

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМ. ІГОРЯ СІКОРСЬКОГО»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМ. ІГОРЯ СІКОРСЬКОГО»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова праця
на правах рукопису

ПРОГОНОВ ДМИТРО ОЛЕКСАНДРОВИЧ

УДК 004.[056.5+932.2]

ДИСЕРТАЦІЯ
СТРУКТУРНИЙ СИНТЕЗ ТА ПАРАМЕТРИЧНА ОПТИМІЗАЦІЯ
МЕТОДІВ ПОБУДОВИ СТЕГОДЕТЕКТОРІВ ДЛЯ ЦИФРОВИХ
ЗОБРАЖЕНЬ

Спеціальність 05.13.21 – Системи захисту інформації

Подається на здобуття наукового ступеня доктора технічних наук

Дисертація містить результати власних досліджень. Використання ідей,
результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Д.О. Прогонов

Науковий консультант: Мачуський Є.А., доктор технічних наук, професор

Київ – 2024

АНОТАЦІЯ

Прогонов Д.О. Структурний синтез і параметрична оптимізація методів побудови стегодетекторів для цифрових зображень. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 «Системи захисту інформації». – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» МОН України, Київ, 2024.

Дисертаційна робота присвячена вирішенню актуальної науково-прикладної проблеми розробки високоточних методів виявлення стеганограм, здатних надійно працювати в умовах відсутності апріорних даних щодо особливостей використаних стеганографічних методів, малого ступеня заповнення зображення-контейнеру стегоданими (менше 10%) та при значній варіативності параметрів досліджуваних цифрових зображень.

У **першому розділі** проведено огляд сучасних моделей, методів та підходів до приховання повідомлень в мультимедійних даних, зокрема цифрових зображеннях (ЦЗ), а також методів виявлення сформованих стеганограм. Особлива увага приділена новітнім методам як вбудовування стегоданих до зображень-контейнерів (ЗК), так і виявлення стеганограм із застосуванням методів статистичного, спектрального та структурного аналізу, а також штучних нейронних мереж. Встановлено, що особлива увага при розробці сучасних стеганографічних методів приділяється мінімізації змін статистичних, спектральних та структурних параметрів ЗК при формуванні стеганограм.

За результатами порівняльного аналізу точності виявлення стеганограм, сформованих згідно новітніх адаптивних стеганографічних методів (АСМ), при використанні стегодетекторів (СД) на основі потужних статистичних моделей $\max\text{SRM}$, DCTR та PSRM встановлено, що висока (більше 90%) імовірність виявлення прихованих повідомлень досягається лише у випадку середнього ($\Delta_{\alpha}^S > 10\%$) ступеня заповнення ЗК стегоданими.

При цьому збільшення точності роботи СД в області слабкого ($\Delta_{\alpha}^S < 10\%$) ступеня заповнення ЗК потребує суттєвого ускладнення процедури попередньої обробки ЦЗ (а саме збільшення кількості використовуваних фільтрів високих частот), що унеможлиблює швидко адаптацію налаштованих стегодетекторів для виявлення нових типів стеганографічних методів (СМ). Застосування СД на основі штучних нейронних мереж (ШНМ) дозволяє подолати виявлене обмеження статистичних стегодетекторів, проте лише у випадку обробки пакетів ЦЗ, статистичні характеристики котрих несуттєво відрізняються від відповідних характеристик вихідної (навчальної) вибірки зображень. Також, дані СД потребують використання прикладів стеганограм при проведенні налаштування ШНМ для забезпечення високої (більше 95%) точності виявлення стеганограм. Це унеможлиблює використання даних СД у випадку виявлення апріорно невідомих стеганографічних методів.

Результати першого розділу дозволили обґрунтувати необхідність розробки нової концепції побудови стегодетекторів для проведення «сліпого» стегоаналізу ЦЗ, що здатні забезпечити надійне виявлення стеганограм в умовах відсутності апріорних даних щодо використаних АСМ. Досягнення поставленої мети потребує визначення факторів, що мають найбільший вплив на точність роботи існуючих СД, експериментальної оцінки межі вірогідності виявлення стеганограм в залежності від наявних апріорних даних щодо використаного СМ та статистичних параметрів досліджуваних зображень, розробки методів, що дозволяють забезпечити точність роботи СД, яка є близькою до отриманих оцінок межі вірогідності виявлення стеганограм навіть в умовах відсутності апріорних даних щодо використаного стеганографічного методу.

Другий розділ присвячено дослідженню межі вірогідності виявлення стеганограм в залежності від наявних апріорних даних щодо СМ та статистичних параметрів досліджуваних ЦЗ, та розробці методів, що дозволяють наблизити точність роботи СД до встановленої межі незалежно від типу використаного стеганографічного методу.

Для подолання виявлених обмежень сучасних підходів до побудови СД в роботі запропоновано інтегральну модель оцінки точності роботи стегодетектору. Дана модель заснована на представленні значення помилки класифікації стеганограм P_E як результату композиції впливів функцій, що відповідають: попередній обробці досліджуваних зображень з метою виявлення слабких змін ЗК, обумовлених прихованням повідомлень, визначення статистичних, спектральних та структурних параметрів оброблюваних ЦЗ та віднесення (класифікації) досліджуваного зображення до класів ЗК або стеганограм за результатами обробки обчислених параметрів зображення.

В роботі запропоновано оцінку приросту «інформації» щодо використаного СМ при проведенні стегоаналізу на основі аналізу характеристик кластеру векторів, що відповідають статистичним параметрам стеганограм, які відрізняються лише значенням яскравості окремого пікселю. За результатами дослідження залежності значень помилки P_E виявлення стеганограм при варіації типу методу класифікації параметрів оброблюваних ЦЗ встановлено, що суттєвий вплив на точність роботи СД має взаємне положення кластерів векторів $\mathbf{F}(c)$ і $\mathbf{F}(s)$, які відповідають статистичним параметрам зображень-контейнерів та відповідним їм стеганограмам. Запропоновано використовувати методи оцінки відстані між імовірнісними розподілами P_X та P_Y , що відповідають нормованим гістограмам розподілу значень яскравості пікселів ЗК та сформованої стеганограми, а саме відстані Хеллінгера D_H , Бхаттачарая D_B , χ^2 -квадрат D_{χ^2} та спектр відстаней Реньї D_R^α для забезпечення високої точності оцінки взаємного положення кластерів $\mathbf{F}(c)$ і $\mathbf{F}(s)$ для довільної статистичної моделі \mathcal{M} оброблюваних зображень. За результатами порівняльного аналізу точності оцінки відстані між кластерами $\mathbf{F}(c)$ та $\mathbf{F}(s)$ при використанні АСМ виявлено, що застосування відстані Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ дозволяє суттєво (до двох разів) підвищити точність оцінювання відмінностей між розподілами значень яскравості

пікселів ЗК та стеганограм у порівнянні іншими підходами, зокрема використанням відстані Кульбака-Лейблера $D_{KL}(\mathbf{X}, \mathbf{Y})$.

В дисертаційній роботі показано, що оптимальними методами попередньої обробки $\mathcal{K}_{opt}(\cdot)$ досліджуваних ЦЗ за критерієм мінімізації значення помилки класифікації стеганограм P_E в умовах обмеженості апріорних даних щодо особливостей використаного СМ є методи $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ для відновлення (реконструкції) вихідного виду ЗК за наявними (зашумленими) зображеннями, а також методи $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$, спрямовані на вилучення спотворень ЗК, обумовлених прихованням повідомлень. Методи, що відносяться до першої групи дозволяють проводити реконструкцію вихідного виду ЗК навіть в умовах відсутності апріорних даних щодо використаного СМ, що становить інтерес для розробки методів деструкції стеганограм, які характеризуються мінімальними змінами статистичних параметрів ЦЗ та дозволяють маскувати факт втручання в канал зв'язку. Практичне застосування методів $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ є обмеженим з огляду на необхідність формування стеганограм на основі оброблюваного ЦЗ, що є неможливим у випадку обмеженості апріорних даних щодо використаного СМ. Проте дані методи можуть становити інтерес для порушення роботи стеганографічних каналів зв'язку за рахунок формування та передачі хибних (підроблених) стеганограм.

За результатами проведених автором досліджень отримано експериментальні оцінки досяжної точності роботи СД при використанні запропонованого методу \mathcal{K}_{opt}^{CE} для новітніх стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD на зображеннях зі стандартних пакетів ALASKA (80,000 зображень), VISION (11,700 зображень) та MIRFlickr (близько 1 мільйона зображень). Показано, що застосування запропонованих методів $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ та векторів векторів \mathbf{F}_{DF} дозволяє суттєво (на 20%) зменшити значення P_E навіть у найбільш складному випадку слабкого (менше 10%) ступеня заповнення ЗК стегоданими. Вагомою перевагою використання векторів \mathbf{F}_{DF} при налаштуванні СД є слабка залежність отримуваних значень

P_E від значення параметру Δ_α^S , що дозволяє суттєво підвищити точність роботи СД навіть у найбільш складному випадку слабого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$).

Для наближення точності роботи методів стегоаналізу ЦЗ до отриманих оцінок меж точності виявлення стеганограм запропоновано математичний апарат синтезу структури та параметричної оптимізації СД, що заснований на декомпозиції багатовимірних сигналів на основі спеціальних систем функцій (ССФ). В роботі запропоновано метод формування ССФ, що дозволяє формувати системи функцій розкладу ЦЗ в залежності від наявних даних щодо параметрів ЗК та стеганограм, а також з врахуванням варіативності статистичних та спектральних параметрів досліджуваних ЦЗ, що становить особливий інтерес для побудови високоточних стегодетекторів. Результати експериментальних досліджень точності виявлення стеганограм, сформованих згідно стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD, при обробці ЦЗ з використання запропонованого методу формування ССФ підтвердили ефективність даного підходу. Зокрема, зменшення значень P_E ($\Delta P_E \cong 40\%$) досягається як в області сильного ($\Delta_\alpha^S > 20\%$), так і слабого ($\Delta_\alpha^S < 10\%$) ступеня заповнення ЗК стегоданими, що є одним з найбільш складних випадків при проведенні стегоаналізу ЦЗ.

Запропоноване об'єднання методів попередньої обробки $F_{calib}(\cdot)$ та методів визначення статистичних, спектральних та структурних параметрів оброблюваного зображення $F_{feature}(\cdot)$ дозволило отримати попередньо неочевидні результати щодо синтезу оптимальних СД за критерієм мінімізації значення помилки класифікації P_E . Показано, що використання запропонованого підходу до розробки СД дозволяє наблизити точність виявлення стеганограм до встановлених меж досяжної точності роботи СД навіть для новітніх стеганографічних методів MG та MiPOD. При цьому забезпечуються нові властивості кластерів $\mathbf{F}_r(c)$ та $\mathbf{F}_r(s)$, а саме максимізація відстані між ними в процесі обробки ЦЗ, що суттєво знижує вимоги щодо

модуля класифікатора зображень при збереженні високої точності виявлення стеганограм.

Зважаючи на високу точність роботи стегодетекторів, заснованих на використанні запропонованого методу, у випадку виявлення стеганограм, сформованих згідно відомих СМ, подальший інтерес становить дослідження точності даних СД у найбільш складних випадках стегоаналізу, а саме виявлення апріорно невідомих стеганографічних методів при обробці нових пакетів ЦЗ.

У **третьому розділі** проведено порівняльний аналіз точності роботи новітніх стегодетекторів, а також запропонованого методу синтезу СД в найбільш складних випадках складних випадках проведення стегоаналізу ЦЗ, а саме відсутності апріорних даних щодо особливостей використаного СМ та при високій варіативності значень статистичних, спектральних та структурних параметрів оброблюваних.

На основі запропонованого методу синтезу високоточних СД розроблено та реалізовано програмний комплекс для проведення стегоаналізу ЦЗ. Зважаючи на відсутність необхідності використання апріорних даних щодо використаного СМ при застосуванні запропонованого методу синтезу СД, для розробленого комплексу запропонована назва Blind-Steg. За результатами експериментального дослідження точності виявлення стеганограм при використанні запропонованого комплексу Blind-Steg підтверджена його висока ефективність навіть у найбільш складних випадках проведення стегоаналізу, а саме виявлення стеганограм, сформованих згідно апріорно невідомих АСМ (досягнуто зменшення помилки класифікації стеганограм до чотирьох разів у порівнянні з сучасними СД) при забезпеченні малої тривалості обробки ЦЗ з використанням запропонованого методу (до трьох секунд на зображення). Висока точність реконструкції ЗК при використанні розробленого комплексу Blind-Steg створює потенціал для суттєвого підвищення якості деструкції стеганограм та використання даного комплексу для дослідження новітніх задач в галузі стегоаналізу ЦЗ, зокрема вилучення та підміни прихованих повідомлень.

Четвертий розділ присвячено огляду перспектив використання запропонованого комплексу Blind-Steg для вирішення задач надійної деструкції даних, а також визначення шляхів вирішення задачі екстракції стегоданих.

Показано, що запропонований метод попередньої обробки ЦЗ шляхом декомпозиції зображення із застосуванням ССФ дає можливість до 12 разів (з 89.65% до 7.12%) зменшити кількість пікселів, використаних для приховання стегобітів, значення яскравості котрих не були змінені в процесі деструкції стеганограм, навіть у найбільш складному випадку слабкого заповнення ЗК стегоданими. Це дозволяє забезпечити надійну деструкцію стеганограм при суттєвому зниженні (до шести разів) змін статистичних, спектральних та структурних параметрів оброблюваних стеганограм у порівнянні з сучасними методами деструкції. Отримані результати підтверджують перспективність використання розробленого комплексу Blind-Steg для забезпечення ефективної протидії роботі стеганографічних каналів передачі ІзОД при маскуванні власне факту проведення деструкції від приймальної сторони стеганографічної системи.

Висока точність визначення положення пікселів, використаних для приховання стегобітів, становить інтерес для використання запропонованого методу для вилучення або підміни бітів стегоданих без необхідності деструкції стеганограм. Встановлено, що запропонований метод попередньої обробки ЦЗ дозволяє до чотирьох разів підвищити точність локалізації пікселів, використаних для приховання окремих стегобітів у порівнянні з випадком застосування мережі SR-Net. Висока точність визначення пікселів зберігається навіть у найбільш складному випадку слабкого заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$).

Таким чином, запропоновані методи реконструкції вихідного виду ЗК за наявними (зашумленими) даними, реалізовані в комплексі Blind-Steg, дозволяють відкрити шляхи для вирішення найбільш складних задач стегоаналізу ЦЗ, а саме вилучення та підміни вбудованих повідомлень без необхідності проведення деструкції стеганограм. Забезпечення високої

точності визначення позицій пікселів, використаних для приховання стегобітів (більше 60% навіть у випадку слабого заповнення ЗК стегоданими), підтверджує перспективність застосування запропонованого підходу для роботи з новітніми стеганографічними методами.

Ключові слова: кібербезпека, захист каналів зв'язку, схеми шифрування та приховання повідомлень, стегоаналіз, адаптивні стеганографічні методи, спеціальні системи функцій, виявлення та деструкція стеганограм, методи заміни стегоданих.

ABSTRACT

Progonov D.O. Structural synthesis and parametric optimization of methods for constructing stegodetectors for digital images. – Qualifying scientific work, manuscript.

Thesis for a doctoral degree in technical sciences on the specialty 05.13.21 "Information protection systems". – National Technical University of Ukraine "Ihor Sikorskyi Kyiv Polytechnic Institute" of the Ministry of Education and Culture of Ukraine, Kyiv, 2024.

The dissertation is devoted to solving the topical scientific and applied problem of developing high-precision methods for stego images detecting, capable of working reliably in the absence of a priori data regarding the features of the used steganographic (embedding) methods, a small degree of cover image payload with stego data (less than 10%) and significant variability of the parameters of the processed digital images.

In the **first chapter**, an overview of modern models, methods and approaches to hiding messages in multimedia data, in particular digital images (DI), as well as methods for detecting formed stego images is provided. Particular attention is paid to the newest methods of message embedding into cover images (CI), detection of stego images using methods of statistical, spectral, and structural analysis, as well as artificial neural networks (ANNs). It has been established that special attention in the development of modern steganographic methods is paid to

the minimization of changes in statistical, spectral and structural parameters of CI during the formation of stego images.

According to the results of a comparative analysis of the accuracy of detection of stego images formed according to the novel adaptive embedding methods (AEM), when using stegdetectors (SD) based on statistical models maxSRM, DCTR and PSRM, it was established that a high (more than 90%) probability of detecting hidden messages is achieved only in the case of an average ($\Delta_{\alpha}^S > 10\%$) payload of CI with stego data. At the same time, increasing the accuracy of the SD in the case of a weak ($\Delta_{\alpha}^S < 10\%$) cover image payload requires a significant improvement of the DI pre-processing procedure (namely, an increase the number of high-pass filters used), which makes it impossible to quickly adapt customized stegdetectors to detect new types of embedding methods (EM). The use of SD based on ANNs allows to overcome the mentioned limitation of statistical stegdetectors, but only in the case of processing DI, the statistical characteristics of which do not significantly differ from the corresponding characteristics of the images used during training of neural networks. Also, such SD requires the use of examples of stego images when setting up ANNs to ensure high (more than 95%) accuracy of stego images detection. This makes it impossible to use SD data in case of detection of a priori unknown steganographic methods.

The results of the first section justified the need to develop a new concept of stegdetectors design for conducting "blind" steganalysis, capable of ensuring reliable detection of stego images in the absence of a priori data on the used AEM. Achieving this goal requires determining the factors that have the greatest influence on the accuracy of the existing SD, experimental assessment of the limit of probability of detecting stego images depending on the available a priori data on the used EM and statistical parameters of processed images, development of methods that allow to ensure the accuracy of the SD, which is close to the obtained estimates of the limit even in the absence of a priori data regarding the used steganographic method.

The **second chapter** is devoted to the investigation of the limit of the probability of stego images detection depending on the available a priori data on the EM and the statistical parameters of the investigated images, and the development of methods that allow to bring the accuracy of the SD operation closer to the established limit, regard-less of the type of used EM.

In order to overcome the identified limitations of modern approaches to the design of the SD, an integral model for estimating the accuracy of the stegdetector is proposed. The model is based on the presentation of the value of the classification error of stego images P_E as a composition of the effects of the following functions: pre-processing of the investigated images in order to detect weak changes in the CI due to the message hiding, determination of statistical, spectral and structural parameters of the processed digital images and further classification of them to classes of cover or stego images.

The thesis proposes an assessment of the increase in "information" regarding the used EM based on the analysis of the characteristics of a cluster of vectors corresponding to the statistical parameters of stego images, which differ only in the brightness value of a single pixel. According to the results of investigation the dependence of the values of classification error P_E by variation of the type of used classifier of processed images, it was established that key influence on stegdetector performance has the mutual position of the clusters of vectors $\mathbf{F}(c)$ and $\mathbf{F}(s)$, which correspond to the statistical parameters of cover and stego images. It is proposed to use methods for estimating the distance between the probability distributions P_X and P_Y corresponding to the normalized histograms of the distribution of the brightness values of the cover and stego images, namely Hellinger distances D_H , Bhattacharya D_B , χ^2 -squared D_{χ^2} and the spectrum of Renyi distances D_R^α to ensure high accuracy in estimating the relative position of clusters $\mathbf{F}(c)$ and $\mathbf{F}(s)$ for an arbitrary statistical model \mathcal{M} of processed images. According to the results of a comparative analysis of the accuracy of distance estimation between clusters $\mathbf{F}(c)$ and $\mathbf{F}(s)$ when using AFM, it was found that the use of the Hellinger distance $D_H(\mathbf{X}, \mathbf{Y})$ allows significantly (up to two times)

increasing the accuracy of estimating the differences between the distributions of the pixels brightness values for cover and stego images in comparison with other approaches, in particular using the Kullback-Leibler distance $D_{KL}(\mathbf{X}, \mathbf{Y})$.

In the dissertation, it is shown that the optimal methods of preprocessing $\mathcal{K}_{opt}(\cdot)$ of the processed images according to the criterion of minimizing the value of the classification error of steganograms P_E under limited a priori data regarding the features of used EM are the $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ methods for restoring (reconstructing) the original form CI based on available (noisy) images, as well as $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ methods aimed at removing cover iamges distortions caused by hiding messages. The methods belonging to the first group make it possible to estimate the initial view of CI even in the absence of a priori data on used EM, which is of interest for the development of novel methods of destruction of stego iamges. These methods are characterized by minimal changes in the statistical parameters of DI and allow to mask the fact of interference in the communication channel. The practical application of the $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ methods is limited due to the need to form a stego image based on the processed CI, which is impossible in the case of limited a priori data about used EM. However, these methods can be of interest for disrupting the operation of steganographic communication channels due to the formation and transmission of false (fake) stego images.

According to the results of performance evaluation, experimental estimates of the achievable accuracy of the SD were obtained when using the proposed \mathcal{K}_{opt}^{CE} method for the advanced steganographic methods HUGO, S-UNIWARD, MG and MiPOD on images from the standard packages ALASKA (80,000 images), VISION (11,700 images) and MIRFlickr (about 1 million images). It is shown that the application of the proposed methods $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ and \mathbf{F}_{DF} vectors allows to significantly (up to 20%) reduce the value of P_E even in the most challenging case of a weak (less than 10%) cover image payload. A significant advantage of using \mathbf{F}_{DF} vectors during adjusting the SD parameters is the weak dependence of the obtained P_E values on cover image payload Δ_{α}^S , which allows to significantly

increase the SD accuracy even in the most difficult case of low payload of CI ($\Delta_\alpha^S < 10\%$).

In order to approximate the SD accuracy to the estimated limits of stego images detection, a mathematical apparatus for the synthesis of the structure and parametric optimization of the SD is proposed. The proposed solution is based on decomposition of multidimensional signals based on special systems of functions (SSF). The thesis proposes a method of forming the SSF, which allows to form systems of functions depending on the available data about parameters of cover and stego images, as well as taking into account the variability of the statistical and spectral parameters of DIs, which is of particular interest for the construction of high-precision SD. The results of experimental studies of the accuracy of stego images detection, formed according to the HUGO, S-UNIWARD, MG and MiPOD embedding methods, during the images processing using the proposed method of SSF forming, confirmed the effectiveness of this approach. In particular, the reduction of P_E value ($\Delta P_E \cong 40\%$) is achieved both in the region of high ($\Delta_\alpha^S > 20\%$) and low ($\Delta_\alpha^S < 10\%$) cover image payload, which is one of the most difficult cases of DI steganalysis.

The proposed fusion of preprocessing methods $F_{calib}(\cdot)$ and methods of determining statistical, spectral and structural parameters of the processed image $F_{feature}(\cdot)$ made it possible to obtain previously non-obvious results regarding the synthesis of optimal SDs according to the criterion of minimizing the value of the classification error P_E . It is shown that the use of the proposed approach to the design of SD allows to bring the accuracy of stego images detection much closer to the established limits of the achievable accuracy even for the novel steganographic methods MG and MiPOD. At the same time, new properties of the $\mathbf{F}_r(c)$ and $\mathbf{F}_r(s)$ clusters are provided, namely, the maximization of the distance between them, which significantly reduces the requirements for the image classifier module while maintaining the high accuracy of stego images detection.

Taking into account the high accuracy of stegdetectors based on the proposed method, further interest is in the study of the accuracy of SD in the most

challenging cases of detection of a priori unknown steganographic methods when processing new packets of digital images.

In the **third chapter**, a comparative analysis of the accuracy of the novel stego-detectors, as well as the proposed method of SD synthesis in the most difficult cases of digital images steganalysis, namely the absence of a priori data on the features of the used EM and high variability of the values of statistical, spectral and structural parameters of the processed images, is carried out.

On the basis of the proposed method of synthesis of high-precision SDs, a software suite for performing digital image steganalysis was developed and implemented. Considering the lack of need to use a priori data regarding the used EM when applying the proposed method of SD synthesis, the name Blind-Steg is proposed for the developed software suite. The results of an experimental study of the accuracy of stego images detection by using of proposed Blind-Steg suite confirmed its efficiency even in the most difficult cases of steganalysis, namely, the revealing of a priori unknown AEM (a reduction of the detection error up to four times was achieved in comparison with modern SD), while ensuring a short duration of processing of the image with usage of proposed preprocessing method (up to three seconds per image). The high accuracy of CI reconstruction when using the developed Blind-Steg suite creates the potential for significantly improving the quality of stego images destruction and using the software suite to research the advanced tasks in the field of steganalysis, in particular, the extraction and replacement of hidden messages.

The **fourth chapter** is devoted to the review of the perspectives of using the proposed Blind-Steg suite to solve the problems of reliable destruction of stego data, as well as the determination of ways to solve the problem of messages extraction.

It is shown that the proposed method of DI preprocessing by image decomposition using SSF makes it possible to reduce the number of pixels used for hiding stegobits up to 12 times (from 89.65% to 7.12%), even in the most in the difficult case of low cover image payload ($\Delta_{\alpha}^S < 10\%$). This allows for reliable destruction of stego images with a significant reduction (up to six times) of

changes in statistical, spectral and structural parameters compared to modern destruction methods. The obtained results confirm the perspective of using the developed Blind-Steg suite to provide effective countermeasures to the hidden transmission of sensitive information while masking the actual fact of destruction from the receiving side of the steganographic system.

The high accuracy of determining the position of pixels used to hide stegobits is of special interest for using the proposed Blind-Steg suite for extracting or replacing stegodata without the need to destroy a stego images. It was established that the proposed method of DI preprocessing allows to increase the accuracy of localization of pixels used to hide individual stegobits by up to four times compared to the case of using the novel SR-Net network. The high accuracy of pixel determination is preserved even in the most difficult case of low cover image payload ($\Delta_{\alpha}^S = 5\%$).

Thus, the proposed methods of reconstruction of the original form of a cover images based on the available (noisy) data, implemented in the Blind-Steg software suite, allow us to open up ways to solve the most difficult tasks of digital images steg-analysis, namely the extraction and replacement of embedded messages. Ensuring high accuracy in determining the positions of pixels used to hide stegobits (more than 60% even in the case of low cover image payload) confirms the promising application of the proposed approach for working with the advanced steganographic methods.

Keywords: cyber security, protection of communication channels, schemes for encryption and hiding of messages, stegoanalysis, adaptive steganographic methods, special systems of functions, detection and destruction of stego images, methods of replacing embedded data.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях

1. **Прогонов Д.О.** Аналіз змін χ^2 -квадрат відстані між розподілами яскравості пікселів при фільтрації зображень-контейнерів та стеганограм [Текст] / **Прогонов Д.О.** // Вісник Національного технічного університету України «Київський політехнічний інститут». Серія «Радіотехніка. Радіоапаратобудування». – 2018. – № 75. – с.54–60. – DOI: <https://doi.org/10.20535/RADAP.-2018.75.54-60>. (Фахове видання, індексується базою даних **Web of Science**).
2. **Прогонов Д.О.** Аналіз змін χ^2 -квадрат відстані між розподілами яскравості пікселів при фільтрації стеганограм, сформованих згідно методу UNIWARD [Текст] / **Прогонов Д.О.** // Вісник Національного технічного університету України «Київський політехнічний інститут». Серія – Радіотехніка. Радіоапаратобудування. – № 76, 2019. – с.72-76. – DOI: <https://doi.org/10.20535/RADAP.2019.76.72-76>. (Фахове видання, індексується базою даних **Web of Science**).
3. **Progonov D.** Statistical stegdetectors performance by message re-embedding [Text] / **Progonov D.** // Theoretical and Applied Cybersecurity, Vol.3, No. 1, 2021. – pp. 5-14. – DOI: <https://doi.org/10.20535/tacs.2664-29132021.1.251291> (Фахове видання категорії «Б»).
4. **Progonov D.O.** Influence of digital images preliminary noising on statistical stegdetectors performance [Text] / **D. Progonov** // Radio Electronics, Computer Science, Control. – Vol. 1(56). – 2021. – p. 184-193. – DOI: <https://doi.org/10.15588/1607-3274-2021-1-18> (Фахове видання категорії «А», індексується базою даних **Web of Science**).
5. **Progonov D.O.** Detection Of Stego Images With Adaptively Embedded Data By Component Analysis Methods [Text] / **Progonov D.O.** // Advances in Cyber-Physical Systems (ACPS). Vol. 6, Number 2. – 2021. – pp. 146-154. – DOI: <https://doi.org/10.23939/acps2021.02.146> (Фахове видання категорії «Б»).
6. **Progonov D.O.** Effectiveness of stego images pre-noising with fractional noise for digital image steganalysis [Text] / **Progonov D.O.** // Applied Aspects of Information Technology. – Vol. 4, issue 3, pp. 261-270. – 2021. – DOI: <https://doi.org/10.15276/aait.03.2021.5>. (Фахове видання категорії «Б»).

7. **Progonov Dmytro**. Effectiveness of stego image calibration via feature vectors re-projection into high-dimensional spaces [Text] / **Progonov Dmytro** // Radio Electronics, Computer Science, Control. Vol. 2 (61). – 2022. – pp. 165-174. – DOI: <https://doi.org/10.15588/1607-3274-2022-2-16>. (Фахове видання категорії «А», індексується базою даних **Web of Science**).

8. **Progonov Dmytro**. Investigation of Digital Image Preprocessing Methods Influence on the Accuracy of Stego Images Detection [Text] / **Progonov Dmytro** // Visnyk NTUU KPI Serii A - Radiotekhnika Radioaparotobuduvannia, Vol. (89). – 2022. – pp. 54-60. DOI: <https://doi.org/10.20535/RADAP.2022.89.54-60> (Фахове видання категорії «А», індексується базою даних **Web of Science**).

9. **Progonov Dmytro**. Effectiveness of stego images pre-processing with spectral analysis methods [Text] / **Progonov Dmytro**, Lutsenko Volodymyr // Applied Aspects of Information Technology, Vol. 5, No. 1. – 2022. – pp. 64-75. – DOI: <https://doi.org/10.15276/aait.01.2022.6>. (Фахове видання категорії «Б». *Особистий внесок: аналітичний огляд сучасних методів попередньої обробки цифрових зображень в задачах стегааналізу, аналіз отриманих експериментальних даних точності виявлення стегааногам при використанні методів вейвлет-аналізу та декомпозиції сигналу із застосуванням складних систем функцій*).

10. **Progonov Dmytro**. Performance Analysis Of Stego Image Calibration With Usage Of Denoising Autoencoders [Text] / **Progonov Dmytro** // Advances in Cyber-Physical Systems (ACPS). Volume 7, Number 1. – 2022. – pp. 46-54, DOI: <https://doi.org/10.23939/acps2022.01.046>. (Фахове видання категорії «Б»).

11. **Progonov Dmytro**. Destruction of stego images formed by adaptive embedding methods with dictionary learning methods [Text] / **Progonov Dmytro** // Theoretical and Applied Cybersecurity. Vol. 4 No. 1. – 2022. – DOI: <https://doi.org/10.20535/tacs.2664-29132022.1.254883> (Фахове видання категорії «Б»).

12. **Dmytro Progonov**. Statistical Steganalysis of Multistage Embedding Methods [Text] / **Dmytro Progonov** // Information Theories and Applications. – Volume 5, Number 1. – 2016. – pp. 23-36. (Фахове видання).

13. **Dmytro Progonov**. Multiclass detector for modern steganographic methods [Text] / **Dmytro Progonov** // Information Theories and Applications. – Vol. 24, No. 3. – 2017. – pp. 55-71. (Фахове видання).

14. **Dmytro Progonov**. Information-Theoretic Estimations of Cover Distortion by Adaptive Message Embedding [Text] / **Dmytro Progonov** // Information Theories and Applications. Vol. 25, No. 1. – 2018. – pp. 47-62. (Фахове видання).

15. **Dmytro Progonov**. Analysis of changes the Renyi divergence for pixel brightness distributions by stego images Wiener filtering [Text] / **Dmytro Progonov** // Information Technologies and Knowledge, Vol. 12, No. 2. – 2018. – pp. 3-25. (Фахове видання).

16. **Progonov D.** Steganalysis of adaptive embedding methods by message re-embedding into stego images [Text] / **D. Progonov**, V. Lucenko // Information Theories and Applications, Vol. 27, Issue 4. – 2020. – pp. 3-24. (Фахове видання . *Особистий внесок: порівняльний аналіз точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при проведенні попередньої обробки досліджуваних зображень шляхом повторного вбудовування стегоданих*).

17. **Progonov D.** Multi-Datasets Evaluation Of GB-Ras Network Based Stegdetectors Robustness To Domain Adaptation Problem [Text] / **Progonov D.** // Information Theories and Applications. Volume 28, Number 4. – 2021. – pp. 372-396. (Фахове видання).

18. **Progonov Dmytro**. Performance of stego images calibration using advanced denoising methods [Text] / **Progonov Dmytro** // Information Theories and Applications, Vol. 29, Issue 1. – 2022. – pp. 3-35. – DOI: <https://doi.org/10.54521/ijita29-01-p01>. (Фахове видання).

Статті у виданнях, віднесених до першого - третього кuartилів (Q1-Q3) відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports

19. Progonov Dmytro. Analyzing The Accuracy Of Detecting Steganograms Formed By Adaptive Steganographic Methods When Using Artificial Neural Networks [Text] / Progonov Dmytro, Yarysh Mariia // Eastern-European Journal of Enterprise Technologies. – Vol. 1, Issue 9 (115). – 2022. – pp.45-55. – DOI: <https://doi.org/10.15587/1729-4061.2022.251350>. (Фахове видання категорії «А», **Scopus** Q3. *Особистий внесок: аналітичний огляд сучасних методів виявлення стеганограм з використанням штучних нейронних мереж, аналіз отриманих*

експериментальних даних щодо точності виявлення стеганограм з використання новітніх типів стегодетекторів).

20. Lutsenko Volodymyr. Application of the principle of information objects description formalization for the design of information protection systems [Text] / Lutsenko Volodymyr, Dmytro Progonov // Eastern-European Journal of Enterprise Technologies, Vol. 6 (9 (120)). – 2022. – pp 28–37. – DOI: <https://doi.org/10.15587/1729-4061.2022.269030>. (Фахове видання категорії «А», **Scopus Q3**. *Особистий внесок: аналітичний огляд сучасних методів стегоаналізу цифрових даних та їх застосування для побудови комплексних систем захисту інформації*).

21. Progonov Dmytro. Behavior-based user authentication on mobile devices in various usage contexts [Text] / Progonov Dmytro, Valentyna Cherniakova, Pavlo Kolesnichenko, Andriy Oliynyk // EURASIP J. on Info. Security, Vol. 6. – 2022. – DOI: <https://doi.org/10.1186/s13635-022-00132-x>. (**Scopus Q2**. *Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів*).

Матеріали, що додатково відображають результати дисертації

22. Конахович Г.Ф. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [Текст] / Конахович Г.Ф., **Прогонов Д.О.**, Пузиренко О.Ю. – Підручник. – Київ: «Центр учбової літератури», 2018. – 558 с. – ISBN 978-617-673-741-4. (*Особистий внесок: теоретичні та експериментальні дослідження ефективності використання спеціальних методів структурного аналізу сигналів в задачах виявлення стеганограм, запропоновані методи виявлення стеганограм з даними, вбудованими з використанням багатоступінчатих стеганографічних методів*).

Патенти на винахід

23. User authentication method and device for executing same (2021). Inventors: **Dmytro Progonov**, Oleh Sych, Pavlo Kolesnichenko, Valentyna Cherniakova, Andriy Oliynyk, Veronika Prokhorchuk, Yevhenii Yakishyn. Assignee: Samsung Electronics Co Ltd. (*Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів*. Ідентифікатор документу в міжнародних системах індексації патентів: US20220350869A1 (USA), WO2021149882A1 (WIPO), KR20210095282A (Republic of Korea)).

24. Electronic device and method of controlling the same (2021). Inventors: Dmytro Likhomanov, Oleksandr Shchur, Andriy Oliynyk, **Dmytro Progonov**. Assignee: Samsung Electronics Co Ltd. (*Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів*). Ідентифікатор документу в міжнародних системах індексації патентів: US11575514B2 (USA), US20210320798A1 (USA), KR20210125655A (Republic of Korea)).

25. Device for protecting content by using biometric information and operating method thereof (2023). Inventors: Andriy Oliynyk, **Dmytro Progonov**, Pavlo Kolesnichenko, Valentyna Cherniakova, Yevhenii Yakishyn, Yaroslav Lavrenyuk. Assignee: Samsung Electronics Co Ltd. (*Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів*). Ідентифікатор документу в міжнародних системах індексації патентів: WO2023153637A1 (WIPO), PCT/KR2022/021652 (Republic of Korea)).

Матеріали конференцій

26. **Прогонов Д.О.** Ефективність універсального стегодетектору Фаріда при вбудовуванні даних у цифрові зображення згідно адаптивних методів [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 20-26 березня, 2017. – с. 266-268;

27. **Прогонов Д.О.** Вплив невідповідності областей приховання повідомлень та проведення стеогоаналізу на ефективність статистичних стегодетекторів [Текст] / **Прогонов Д.О.** // XIX Міжнародна науково-технічна конференція «Системний аналіз та інформаційні технології». – Київ, 22-25 травня, 2017. – ННК «ІПСА», НТУУ «КПІ ім. Ігоря Сікорського» – с. 317-318;

28. Дорошенко А.В. Виявлення стеганограм з використанням авторегресійних моделей зображення-контейнеру [Текст] / Дорошенко А.В., **Прогонов Д.О.** // VI міжнародна науково-практична конференція «Обробка сигналів та негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка. – Черкаси: ЧДТУ, 2017. – с. 209-211. (*Особистий внесок: удосконалено виявлення стеганограм з даними, вбудованими в області перетворення зображення-контейнеру, на основі аналізу параметрів авторегресійних моделей кореляції значень яскравості суміжних пікселів цифрових зображень*).

29. **Прогонов Д.О.** Ефективність універсальних стегодетекторів у випадку використання адаптивних методів формування стеганограм [Текст] / **Прогонов Д.О.**, Богайчук В.О., Терещенко Є.М. // VI міжнародна науково-практична конференція «Обробка сигналів та негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка. – Черкаси: ЧДТУ, 2017. – с. 232-234. (*Особистий внесок: аналіз експериментальних даних щодо точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні новітніх типів універсальних стегодетекторів*).

30. Дорошенко А.В. Визначення параметрів стеганограм з використанням авторегресійних моделей цифрових зображень [Текст] / Дорошенко А.В., **Прогонов Д.О.** // XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 25-27 травня 2017 р. – К.: ВПІ ВПК «Політехніка», 2017. – с. 123-125. (*Особистий внесок: метод оцінки ступеня заповнення зображення-контейнеру стегоданими за величиною зміни параметрів авторегресійних моделей цифрових зображень, обумовлених прихованням повідомлень до зображення-контейнеру*).

31. Яцура П.П. Ефективність використання спеціалізованих методів обробки цифрових зображень для деструкції стеганограм [Текст] / Яцура П.П., **Прогонов Д.О.** // XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 25-27 травня 2017 р. – К.: ВПІ ВПК «Політехніка», 2017. – с. 150-152. (*Особистий внесок: аналіз експериментальних даних щодо ступеня деструкції стеганограм, сформованих згідно багатоетапним стеганографічних методів, при використанні методів компонентного аналізу сигналів*).

32. **Прогонов Д.О.** Ефективність варіаційних методів шумоподавлення у задачах активного стегааналізу цифрових зображень [Текст] / **Прогонов Д.О.**, Яцура П.П. // Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». – Київ, 25-26 травня 2017 р. – НДЦ «Тезіс», НТУУ «КПІ ім. Ігоря Сікорського», 2017. – с. 217. (*Особистий внесок: запропоновано метод деструкції стеганограм з даними, вбудованими в частотній області зображення-контейнеру, з використанням варіаційних*

методів шумоподавлення при збереженні статистичних параметрів оброблених зображень).

33. **Прогонов Д.О.** Виявлення стеганограм, сформованих комплексними методами, з використанням стегодетектора Фаріда [Текст] / **Прогонов Д.О.**, Голубничий В.О. // Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». – Київ, 25-26 травня 2017 р. – НДЦ «Тезіс», НТУУ «КПІ ім. Ігоря Сікорського», 2017. – с. 218. *(Особистий внесок: удосконалено універсальний стегодетектор Фаріда для виявлення стеганограм, сформованих згідно комплексних стеганографічних методів).*

34. **Прогонов Д.О.** Порівняльний аналіз точності виявлення стеганограм при використанні статистичних моделей цифрових зображень [Текст] / **Прогонов Д.О.**, Сівкович П.О., Могиліна Ю.В. // Міжнародна науково-практична конференція «Захист інформації і безпека інформаційних систем». – Львів, 1-2 червня 2017 р. – Видавництво Львівської політехніки, 2017. – с. 101-102. *(Особистий внесок: аналіз експериментальних даних щодо точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні сучасних статистичних моделей зображення-контейнеру).*

35. Богайчук В. Виявлення стеганограм, сформованих згідно адаптивного методу SI-UNIWARD, з використанням універсальних стегодетекторів [Текст] / Богайчук В., Терещенко Є., **Прогонов Д.** // Міжнародна науково-практична конференція «Захист інформації і безпека інформаційних систем». – Львів, 1-2 червня 2017 р. – Видавництво Львівської політехніки, 2017. – с. 105-106. *(Особистий внесок: запропоновано метод підвищення точності роботи сучасних стегодетекторів для виявлення стеганограм, сформованих згідно стеганографічного методу SI-UNIWARD).*

36. Голубничий В. Вплив вибору базисних функцій вейвлет-перетворення на ефективність стегодетектору Фаріда [Текст] / Голубничий В., **Прогонов Д.** // Міжнародна науково-практична конференція «Захист інформації і безпека інформаційних систем». – Львів, 1-2 червня 2017 р. – Видавництво Львівської політехніки, 2017. – с. 107-108. *(Особистий внесок: запропоновано метод підвищення точності виявлення стеганограм при використанні універсального сте-*

годетектору Фаріда шляхом вибору оптимальних базисних функцій вейвлет-перетворення за критерієм мінімізації помилки виявлення стеганограм).

37. **Progonov Dmytro**. Structural Stegdetector Performance in case of Side-Informed Message Embedding [Text] / **Progonov Dmytro** // 4th IEEE International Conference “Problems of Infocommunications Science and Technology”. – Kharkiv, 10-13 October, 2017. – pp. 232-236. – DOI: 10.1109/INFOCOMMST.2017.8246386.

38. Бука М.А. Деструкція прихованих повідомлень шляхом масштабування контейнеру [Текст] / Бука М.А., **Прогонов Д.О.** // International Research and Practice Conference “Modern Methods, Innovations, and Experience of Practical Application in the Field of Technical Sciences”. – 27-28 December 2017, Radom, Poland. – pp. 9-13. (*Особистий внесок: удосконалено метод деструкції прихованих повідомлень шляхом використання спеціальних методів масштабування цифрових зображень*).

39. **Прогонов Д.О.** Теоретико-інформаційні оцінки спотворень контейнерів при формуванні стеганограм [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 19-25 березня 2018. – с. 273-275.

40. Богайчук В.О. Деструкція стеганограм з використанням методу головних компонент [Текст] / Богайчук В.О., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 113-115. (*Особистий внесок: удосконалено метод надійної деструкції стеганограм при мінімізації змін статистичних параметрів зображення-контейнеру*).

41. Остапюк Н.В. Виявлення стеганограм з використанням ріджлет-перетворення [Текст] / Остапюк Н.В., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 127-129. (*Особистий внесок: запропоновано метод деструкції стеганограм при використанні новітніх методів вейвлет-аналізу, заснованих на застосуванні спеціальних типів вейвлетів*).

42. Терещенко Є.М. Методи реконструкції контейнерів з використанням розріджених та надлишкових базисів [Текст] / Терещенко Є.М., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інфор-матики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 138-141. (*Особистий внесок: запропоновано методи оцінки статистичних параметрів зображення-контейнеру за наявними зашумленими даними з використанням математичного апарату складних систем функцій*).

43. Чайка Д.В. Виявлення стеганограм, сформованих згідно адаптивних методів, з використанням статистичної моделі PHARM [Текст] / Чайка Д.В., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 144-146. (*Особистий внесок: аналіз результатів експериментального дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі PHARM*).

44. **Прогонов Д.О.** Теоретико-інформаційні оцінки стійкості методів UNWARD до стегоаналізу [Текст] / **Прогонов Д.О.** // XX Міжнародна науково-технічна конференція «Системний аналіз та інформаційні технології». – Київ, 21-24 травня, 2018. – ННК «ІПСА», НТУУ «КПІ ім. Ігоря Сікорського» – с. 256.

45. Yulia Mohylyna. Stego images destruction using a decomposition in the basis formed using K-SVD algorithm [Text] / Yulia Mohylyna, **Dmytro Progonov**, Vladyslav Bohaichuk // 7th International Scientific and Technical Conference “Information Protection and Information Systems Security”. – Lviv, 30-31 May 2019. – pp. 98-99. (*Особистий внесок: запропоновано метод надійної деструкції прихованих повідомлень при збереженні мінімальних візуальних змін зображення-контейнеру із застосуванням математичного апарату спеціальних систем функцій*).

46. Yelizaveta Tereshchenko. Stego images calibration using wavelet transformation [Text] / Yelizaveta Tereshchenko, **Dmytro Progonov** // 7th International Scientific and Technical Conference “Information Protection and Information Systems Security”. – Lviv, 30-31 May 2019. – pp. 106-107. (*Особистий внесок:*

порівняльний аналіз точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при проведенні попередньої обробки цифрових зображень з використанням вейвлет-стиснення).

47. **Прогонов Д.О.** Аналіз точності виявлення стеганограм, сформованих адаптивними методами, при додатковому зашумленні зображень-контейнерів [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 18-24 листопада 2019. – с. 225-227

48. Яриш М.Б. Використання згоржових нейронних мереж для оцінки статистичних характеристик стеганограм [Текст] / Яриш М.Б., **Прогонов Д.О.** // XVIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Київ, 12-13 травня 2020 р. – ВПІ ВПК «Політехніка». – с. 132-134. (*Особистий внесок: аналіз експериментальних результатів дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні сучасних стегодетекторів на основі згоржових нейронних мереж*).

49. **Progonov Dmytro.** Performance of Statistical Stegdetectors in Case of Small Number of Stego Images in Training Set [Text] / **Progonov Dmytro** // IEEE International Scientific-Practical Conference “Problems of Infocommunications Science and Technology”. – Kharkiv, 2020. (індексується базою даних **Scopus**)

50. **Прогонов Д.О.** Вплив попереднього зашумлення на точність виявлення стеганограм, сформованих згідно адаптивних методів MG та MiPOD [Текст] / **Прогонов Д.О.** // X Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». – Запоріжжя: Запорізький національний технічний університет, 2020. – с. 167-168;

51. **Прогонов Д.О.** Ефективність стегоаналізу цифрових зображень у випадку попередньої фільтрації стеганограм, сформованих згідно адаптивних методів MG та MiPOD [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 16-22 листопада 2020.

52. Яриш М.Б. Вплив регуляризації нейронної мережі SRNet на точність виявлення стеганограм, сформованих згідно адаптивних методів [Текст] / Яриш М.Б., **Прогонов Д.О.** // XXV Міжнародний форум «Радіоелектроніка та молодь в XXI столітті», м. Харків, 20-21 квітня 2021 р. – с. 138-139. (*Особистий внесок: аналіз експериментальних даних точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, в залежності від застосовуваних методів регуляризації параметрів нейронної мережі SRNet*).

53. **Dmytro Progonov**. Stego Images Decomposition Using Shallow Denoising Autoencoders [Text] / **Dmytro Progonov** // IEEE International Conference “Problems of Infocommunications Science and Technology”. – Kharkiv, 2021. (індексується базою даних **Scopus**)

54. **Прогонов Д.О.** Виявлення стеганограм з використанням методів адаптивної фільтрації цифрових зображень [Текст] / **Прогонов Д.О.** // VIII Міжнародна науково-практична конференція «Обробка сигналів і негаусівських процесів», присвячена пам’яті професора Ю.П. Кунченка. [Електронний ресурс] – Черкаси: ЧДТУ, 2021 с. 192-194.

55. Маманчук М.М. Локалізація позицій стегобітів, вбудованих до зображень-контейнерів з використанням адаптивних стеганографічних методів HUGO та WOW [Text] / Маманчук М.М., **Прогонов Д.О.** // Всеукраїнська науково-практична конференція “Theoretical and Applied Cybersecurity (TACS-2023)”, присвячена 100-річному ювілею академіка В.М. Глушкова. КПІ ім. Ігоря Сікорського НН ФТІ. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2023. – ISBN 978-966-990-083-8 – с. 42-45. (*Особистий внесок: запропоновано представлення задачі локалізації позиції пікселів зображення-контейнеру, використаних для приховання стегобітів повідомлення, як еквівалентної задачі сегментації зображень з використанням штучних нейронних мереж*).

ЗМІСТ

АНОТАЦІЯ	2
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ	32
ВСТУП	40
РОЗДІЛ 1 ОГЛЯД МЕТОДІВ СТЕГАНОГРАФІЇ ТА СТЕГОАНАЛІЗУ	
ЦИФРОВИХ ЗОБРАЖЕНЬ.....	55
1.1 Основні положення та область використання методів стеганографії і стегоаналізу мультимедійних даних.....	55
1.2 Класифікація методів стеганографії цифрових зображень	59
1.2.1 Методи приховання повідомлень в області перетворення зображення-контейнеру	61
1.2.2 Адаптивні стеганографічні методи	63
1.2.3 Стеганографічні методи, засновані на моделюванні складових зображення-контейнеру.....	65
1.2.4 Стеганографічні методи, засновані на аналізі статистичних та спектральних параметрів зображення-контейнеру	73
1.2.5 Стеганографічні методи, засновані на синхронізації змін значень яскравості пікселів зображення- контейнеру.....	75
1.3 Огляд сучасних методів стегоаналізу цифрових зображень	77
1.3.1 Стегодетектори на основі спеціальних методів попередньої обробки досліджуваних зображень	79
1.3.2 Стегодетектори на основі статистичних моделей контейнеру.....	85

	28
1.3.3 Стегодетектори на основі згорткових нейронних мереж	92
1.3.4 Стегодетектори на основі спеціальних типів нейронних мереж.....	98
1.4 Порівняльний аналіз точності виявлення стеганограм, сформованих згідно новітніх стеганографічних методів, при використанні сучасних типів стегодетекторів	103
1.4.1 Методика проведення досліджень	107
1.4.2 Порівняльний аналіз точності виявлення стеганограм при варіації типу методів попередньої обробки цифрових зображень.....	112
1.4.3 Оцінка точності виявлення стеганограм при використанні стегодетекторів на основі статистичних моделей цифрових зображень	121
1.4.4 Оцінка точності виявлення стеганограм при використанні стегодетекторів на основі штучних нейронних мереж	131
1.5 Постановка задачі дисертаційного дослідження	138
1.6 Висновки за розділом 1	146
РОЗДІЛ 2 МЕТОДИ СИНТЕЗУ СТРУКТУРИ ТА ОПТИМІЗАЦІЇ ПАРАМЕТРІВ СТЕГОДЕТЕКТОРІВ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ	149
2.1 Аналіз факторів впливу на точність виявлення стеганограм при використанні сучасних підходів до побудови стегодетекторів.....	150
2.2. Оцінка досяжної вірогідності виявлення стеганограм в залежності при використанні відомих методів стегоаналізу зображень.....	160

2.2.1 Порівняльний аналіз показників оцінки відстані між імовірнісними розподілами зображень-контейнерів та стеганограм	160
2.2.2 Оцінка досяжної вірогідності виявлення стеганограм в залежності від наявних апріорних даних щодо використаного стеганографічного методу	168
2.2.3 Теоретичний аналіз досяжної точності виявлення стеганограм.....	180
2.3 Розробка методів синтезу та параметричної оптимізації високоточних стегодетекторів для цифрових зображень.....	188
2.4 Висновки за розділом 2	206
РОЗДІЛ 3 АНАЛІЗ ТОЧНОСТІ ВИЯВЛЕННЯ СТЕГАНОГРАМ ПРИ ВИКОРИСТАННІ СУЧАСНИХ ТА ЗАПРОПОНОВАНОГО ПІДХОДУ ДО СИНТЕЗУ СТЕГОДЕТЕКТОРІВ	208
3.1 Сучасні методи синтезу стегодетекторів цифрових зображень.....	208
3.1.1 Методи на основі повторного вбудовування повідомлень до досліджуваних зображень	211
3.1.2 Методи на основі додаткового зашумлення досліджуваних зображень.....	224
3.1.3 Статистичні методи знешумлення цифрових зображень	233
3.1.4 Спектральні методи знешумлення цифрових зображень	238
3.1.5 Варіаційні методи знешумлення цифрових зображень	243
3.1.6 Методи знешумлення цифрових зображень на основі штучних нейронних мереж.....	247
3.1.7 Методи компонентного аналізу для знешумлення цифрових зображень.....	255
3.2 Структура розробленого комплексу прикладних програм.....	262

3.3 Порівняльний аналіз точності роботи стегодетекторів, синтезованих згідно сучасних та запропонованого методів	267
3.3.1 Методика проведення дослідження	267
3.3.2 Аналіз точності роботи стегодетекторів при виявленні апріорно відомих стеганографічних методів	272
3.3.3 Аналіз точності роботи стегодетекторів при обмеженості апріорних даних щодо використаного стеганографічного методу	281
3.3.4 Аналіз точності роботи стегодетекторів при відсутності апріорних даних щодо використаного стеганографічного методу	285
3.4 Висновки за розділом 3	292
РОЗДІЛ 4 АНАЛІЗ ПЕРСПЕКТИВ ВИКОРИСТАННЯ ЗАПРОПОНОВАНОГО ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ПРОВЕДЕННЯ СТЕГОАНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ	
4.1 Дослідження ефективності використання комплексу для вирішення задач стегоаналізу цифрових зображень	294
4.1.1 Оцінка ступеня деструкції стеганограм при використанні запропонованого методу попередньої обробки цифрових зображень	295
4.1.2 Оцінка точності визначення позицій пікселів, використаних для вбудовування окремих стегобітів.....	299
4.2 Висновки за розділом 4	305
ВИСНОВКИ.....	307
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	311
ДОДАТОК А Список опублікованих праць за темою дисертації.....	340

ДОДАТОК Б Документи, що підтверджують впровадження результатів дисертаційної роботи.....	353
ДОДАТОК В Результати дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні статистичних моделей цифрових зображень.....	359
В.1 Результати дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі SPAM цифрових зображень	361
В.2 Результати дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі maxSRMd2 цифрових зображень	373
В.3 Результати дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі maxSRMd2 (EDGE фільтр) цифрових зображень	385
ДОДАТОК Г Результати дослідження досяжної точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні запропонованого методу побудови стегодетекторів.....	397
Г.1 Результати дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні запропонованого підходу до побудови стегодетекторів.....	399

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

- $\mathbf{A}_{M \times N}$ – матриця дійсних чисел розміром $M \times N$ елементів;
- \mathbf{A}_{SRR} – система функцій, що використовується для забезпечення розрідженого представлення сигналів (збереження відносно малої частки відмінних від нуля коефіцієнтів розкладу сигналів);
- $\mathbf{a}_{M \times 1}$ – вектор дійсних чисел розміром $M \times 1$ елементів;
- C_{CH} – показник Калінського-Харабаша ступеня перекриття груп (кластерів) багатовимірних векторів;
- C_{Dunn} – показник Дунна ступеня перекриття груп (кластерів) багатовимірних векторів;
- \mathbf{C}_X^{cov} – емпіричної коваріаційної матриці для матриці даних \mathbf{X} ;
- $d_{C,S}^F$ – відстань між групами векторів $\mathbf{F}(c)$ і $\mathbf{F}(s)$, що відповідають статистичним параметрам зображень-контейнерів та стеганограм;
- d_{preim} – кількість елементів у векторах-прообразах;
- $D_B(C, S)$ – відстань Бхаттачарая між імовірнісними розподілами C та S ;
- $D_H(C, S)$ – відстань Хеллінгера між імовірнісними розподілами C та S ;
- $D_{KL}(C, S)$ – відстань Кульбака-Лейблера між імовірнісними розподілами C та S ;
- $D_R^\alpha(C, S)$ – відстань Реньї між імовірнісними розподілами C та S з ваговим параметром α ;
- $D_T^S(A, B)$ – індекс Тверського для оцінки ступеня подібності множин A та B ;
- $D_{\chi^2}(C, S)$ – хі-квадрат відстань між імовірнісними розподілами C та S ;
- $DSC(A, B)$ – показник Сьоренсена-Дайса ступеня подібності множин A та B ;
- $\mathbb{E}[\cdot]$ – оператор усереднення;
- $F^M(\cdot)$ – оператор отримання параметрів статистичної моделі M для

- вихідного (необробленого) цифрового зображення;
- $F_{cal}^M(\cdot)$ – оператор отримання параметрів статистичної моделі M для обробленого цифрового зображення;
- F_1 – F-міра якості роботи класифікатору;
- $F_{dn}(\cdot)$ – знешумлюючий фільтр для цифрових зображень;
- $F(c)$ – кластери векторів, що відповідають сукупності використовуваних параметрів зображення-контейнеру;
- $F(s)$ – кластери векторів, що відповідають сукупності використовуваних параметрів стеганограми;
- F_{calib} – статистичні параметри обробленого зображення;
- F_{CC} – вектор, що відповідає об'єднанню статистичні параметрів вихідного та обробленого зображень;
- F_{DF} – вектор, що відповідає різниці статистичних параметрів вихідного та обробленого зображень;
- F_{nc} – вектор, що відповідає статистичним параметрам вихідного (необробленого) зображення;
- $g_{jk}(\theta)$ – інформаційна метрика Фішера $g_{jk}(\theta)$ для випадку приросту значень i -того та j -того елементів вектору θ параметрів досліджуваного зображення;
- $H_4(\pi)$ – функція тернарної ентропії для імовірнісного розподілу π ;
- \mathcal{J} – множина цифрових зображень розміром $N \times M$ пікселів, що мають K каналів кольору (наприклад $K = 3$ для кольорових зображень) з глибиною кольору k ($k \geq 1$) біт;
- $\mathbf{I}_{l \times l}$ – одинична матриця розміром $l \times l$ елементів;
- $J(A, B)$ – показник Жаккарта ступеня подібності множин A та B ;
- \mathcal{K}_{opt} – оптимальний метод попередньої обробки цифрових зображень за критерієм максимізації відстані між кластерами векторів, що відповідають статистичним параметрам зображень-контейнерів та стеганограм;

- K_{α}^{OL} – частка пар зображень-контейнерів та стеганограм у навчальній вибірці зображень при налаштуванні стегодетектору;
- M** – приховувані повідомлення (стегодані), представлені у форматі бітової послідовності фіксованої довжини;
- MCC – коефіцієнт кореляції Метьюса;
- $\mathcal{N}(\mu, \sigma^2)$ – гаусовий (нормальний) розподіл з математичним очікуванням μ та дисперсією σ^2 ;
- n_{PCA} – частка компонентів зображення, використаних при оцінці вихідного виду зображення-контейнеру згідно методу головних компонентів;
- N_{UC} – кількість складових розкладу цифрового зображення при використанні методів розрідженого представлення сигналів;
- $P(\lambda)$ – розподіл Пуасона з математичним очікуванням λ ;
- P_E – загальна помилка виявлення стеганограм;
- P_E^{lim} – досяжна імовірність виявлення стеганограм;
- P_{FN} – імовірність помилки другого роду (хибна класифікація стеганограми як зображення-контейнеру);
- P_{FP} – імовірність помилки першого роду (хибна класифікація зображення-контейнеру як стеганограми);
- P_{TN} – імовірність правильної класифікації зображень-контейнерів;
- P_{TP} – імовірність правильної класифікації стеганограм;
- $\Pr(a)$ – імовірність події a ;
- \mathcal{S}_{test} – вибірка цифрових зображень, що використовується при тестуванні стегодетектору;
- \mathcal{S}_{train} – вибірка цифрових зображень, що використовується для налаштування стегодетектору;
- $\mathcal{S}_{train}^{SRR}$ – вибірка сигналів, що використовується для формування спеціальної системи функцій \mathbf{A}_{SRR} ;
- $\text{trunc}(x, T)$ – оператор порогової обробки скалярного значення x з порогом

- T ;
- U** – вихідне (необроблене) зображення;
- $\mathcal{U}(a, b)$ – рівномірний розподіл на інтервалі від a до b ;
- $w_{w \times w}$ – розміри ковзного вікна, пікселів;
- w_{UC} – розмір блоку розбиття зображення, що використовується при формуванні спеціальної системи функцій \mathbf{A}_{SRR} ;
- X** – зображення-контейнер;
- \mathcal{X} – кластер векторів, що відповідають статистичним параметрам зображень-контейнерів;
- Y** – стеганограма;
- \mathcal{Y} – кластер векторів, що відповідають статистичним параметрам стеганограм;
- $[a]_I$ – нотація (дужка) Айверсона, значення котрої рівне одиниці якщо булевий вираз a є істинним, та нулю у протилежному випадку;
- $\langle \cdot, \cdot \rangle$ – скалярний добуток;
- $\langle a, b \rangle_m$ – скалярний добуток m – елементних векторів, що відповідають бінарному представленню аргументів a та b ;
- $\|\cdot\|_2$ – норма (метрика) Евкліда для скалярних та векторних величин;
- $\|\cdot\|_F$ – норма Фробеніуса для матриць;
- γ_2 – коефіцієнт ексцесу імовірнісного розподілу;
- $\delta(\cdot)$ – функція Дірака;
- μ_{η}^2 – оцінка середнього значення яскравості пікселів для поточного положення ковзного вікна фільтра Вінера;
- σ_{η}^2 – оцінка дисперсії значень яскравості пікселів для поточного положення ковзного вікна фільтра Вінера;
- $\sigma_{\mathbf{I}}^2$ – значення дисперсії значень яскравості пікселів цифрового зображення \mathbf{I} ;
- $\sigma_{\mathcal{N}}^2$ – значення дисперсії нормального розподілу $\mathcal{N}(\mu, \sigma_{\mathcal{N}}^2)$;

- Δ_{α}^S – ступінь заповнення зображення-контейнеру стегоданими. Значення даного показника в роботі умовно розділено на три випадки: слабкого ($\Delta_{\alpha}^S < 10\%$), середнього ($10\% \leq \Delta_{\alpha}^S \leq 20\%$) та сильного ($\Delta_{\alpha}^S > 20\%$) заповнення зображення-контейнеру стегоданими;
- \mathcal{J} – множина значень яскравості пікселів, цифрового зображення;
- $\rho(\cdot)$ – функція оцінки змін статистичних характеристик зображення-контейнеру при вбудовуванні окремого стегобіту;
- Φ_{JL} – оператор проєкції векторів з простору \mathbb{R}^k до простору \mathbb{R}^d , $k < d$, згідно швидкого перетворення Джонсона-Лінденштрауса;
- CE – англ. cover estimate, методи попередньої обробки цифрових зображень, спрямовані на оцінку статистичних параметрів зображення-контейнеру за наявними (зашумленими) даними;
- CV – англ. cross-validation, процедура перехрестної перевірки точності роботи систем класифікації;
- DAE – англ. denoising autoencoders, шумоподавляючі автоенкодери, що забезпечують оцінку вихідного (незашумленого) сигналу за наявними (зашумленими) даними;
- DLSR – англ. digital single-lens reflex camera, цифрова однооб'єктивна дзеркальна фотокамера;
- DR – англ. divergent reference, методи попередньої обробки цифрових зображень, спрямовані на посилення відмінностей між статистичними параметрами (векторами) зображень-контейнерів та стеганограм шляхом зсуву відповідних векторів в протилежних напрямках;
- DRM – англ. Digital Right Management, методи протидії несанкціонованому копіюванню, обробці та розповсюдженню мультимедійних даних;

- DSC – англ. *depthwise separable convolution*, роздільна згортка окремих каналів кольору цифрового зображення;
- FRAME – англ. *Filters, Random Fields and Maximum Entropy*, модель аналізу параметрів марківських випадкових полів, заснована на ітеративному підборі методів попередньої фільтрації зображення для максимізації взаємної ентропії між поточним (зашумленим) та обробленим (відновленим) зображеннями;
- ICM – англ. *indirect cover model*, використання інтегральних показників, зокрема статистичних параметрів цифрових зображень, для оцінки стійкості стеганографічних методів до виявлення з використанням статистичних стегадетекторів;
- IQF – англ. *Image Quality Factor*, індекс якості зображення при проведенні JPEG-стиснення з втратами;
- LDA – англ. *linear discriminant analysis*, лінійний дискримінаційний аналіз;
- MLE – англ. *Maximum Likelihood Estimation*, метод максимальної правдоподібності;
- MOD – англ. *method of optimal directions*, метод оптимальних напрямків проєкцій;
- MVG – англ. *multivariate Gaussian*, модель суміші завад, що мають нормальний (гаусовий) розподіл;
- NLM – англ. *non-local means*, метод знешумлення зображення шляхом усереднення подібних областей значень яскравості пікселів;
- RF – англ. *Random Forest*, ансамблевий класифікатор на основі лінійних дискримінантів Фішера;
- SCI – англ. *side channel information*, оцінка імовірності зміни кожного пікселя в процесі приховання повідомлень згідно поширених стеганографічних методів;
- SE – англ. *stego estimate*, методи попередньої обробки цифрових

- зображень, спрямовані на виокремлення спотворень, обумовлених вбудовуванням стегоданих до зображення-контейнеру;
- SEC – англ. methods with synchronized embedding changes, стеганографічні методи з синхронізацією змін яскравості пікселів;
- SIM – англ. side-informed methods, стеганографічні методи на основі аналізу статистичних та спектральних характеристик вихідного виду контейнеру;
- SPP – англ. spatial pyramid pooling, метод об'єднання параметрів зображення на різних масштабах аналізу з використання методу просторових пірамід;
- SRL – англ. Square Root Law, квадратичний закон оцінки значень досяжної імовірності виявлення стеганограм;
- TLU – англ. truncated linear unit, обмежена лінійна функція;
- TVM – англ. Total Variation Minimization, метод знешумлення сигналів шляхом мінімізації загальної варіативності значень елементів сигналу;
- АНМ – автокодувальна нейронна мережа;
- АСМ – адаптивний стеганографічний метод;
- А-ШНМ – автокодувальна штучна нейронна мережа;
- БД-ДКП – блочне двовимірне дискретне косинусне перетворення;
- БФ – білатеральна фільтрація;
- ВФ – вейвлет-фільтрація;
- ДДВП – двовимірне дискретне вейвлет перетворення;
- ДДКП – двовимірне дискретне косинусне перетворення;
- ДДПФ – двовимірне дискретне перетворення Фур'є;
- ЗАЕ – згорткові автоенкодері;
- ЗнАЕ – знешумлюючий автоенкодер;
- ЗК – зображення-контейнер;
- ЗНМ – згорткові нейронні мережі;

ЗПДЛ	– зворотнє перетворення Джонсона-Лінденштрауса;
ЗШ	– згортковий шар;
ІзОД	– інформація з обмеженим доступом;
ІКС	– інформаційно-комунікаційна система;
КВ	– ковзне вікно;
КІ	– критична інформаційна інфраструктура;
КСМ	– комплексні статистичні моделі;
ЛДФ	– лінійний дискримінант Фішера;
МВП	– марківські випадкові поля;
МГК	– метод головних компонентів;
МД	– мультимедійні дані;
МПО	– методи попередньої обробки;
МФЕ	– матриця фоточутливих елементів;
ОПЗК	– область перетворення зображення-контейнеру;
ПА	– перетворення Арнольда;
ПФ	– перетворення Фур'є;
СД	– стегодетектор;
СК	– стегакодер;
СКІ	– система критичної інфраструктури;
СМ	– стеганографічний метод;
ССЗ	– стеганографічна система зв'язку;
ССФ	– спеціальна система функцій;
УПФ	– узагальнене перетворення Фур'є;
УСД	– універсальний стегодетектор;
ФВ	– фільтр Вінера;
ФВЧ	– фільтр високих частот;
ЦЗ	– цифрове зображення;
ЦС	– цифрова стеганографія;
ШНМ	– штучна нейронна мережа.

ВСТУП

Порушення роботи складових систем критичної інфраструктури (СКІ) державних установ і приватних корпорацій може призвести до несанкціонованого витоку інформації з обмеженим доступом (ІзОД), а також суттєвих втрат у економічній та соціальній сферах [1-3]. Особливу небезпеку становить порушення роботи СКІ в умовах воєнних дій, що може бути використано противником (конкурентом) для вирішення політичних або військових задач [4,5]. В якості прикладу можливо навести відомі інциденти з інформаційної безпеки, що призвели до порушення роботи державних установ та приватних корпорацій протягом 2020-2024 років [3,6,7]:

- несанкціонований доступ до державних реєстрів громадян США та республіки Аргентина, а також викрадення персональних даних співробітників (зокрема, баз даних компанії Асер) та користувачів комерційних сервісів (серед яких, бази даних компаній Twitch, Facebook, Telegram);
- викрадення даних, що стосуються роботи державних (наприклад, доступ до реєстрів співробітників МВС США) та військових (а саме, персональні дані співробітників державних агенцій США) установ;
- порушення роботи промислових об'єктів (наприклад, зупинка підприємств енергетичної інфраструктури України, переробних заводів корпорації JBS Foods) та логістичних систем (зокрема, зупинка роботи нафтопроводів в США та Ірані);
- витік фінансових даних (серед яких, звіти корпорацій Experian, Shinsei Bank, JPMorgan Chase, Heartland Payment Systems) та інформації щодо інженерно-технічних розробок (наприклад, конструкторської документації мікропроцесорів корпорації AMD та продуктів компанії Gigabyte) міжнародних корпорацій.

Протидія використанню несилкових методів впливу на СКІ зловмисниками потребує запровадження багаторівневого та всеосяжного захисту кри-

тичної інформаційної інфраструктури (КІІ) державних та приватних організацій. При цьому особлива увага приділяється розробці та впровадженню заходів, що спрямовані на зниження загроз щодо витоку ІзОД при обміні даними в інформаційно-комунікаційних системах (ІКС), зокрема забезпеченню надійного виявлення прихованих (стеганографічних) каналів передачі інформації з обмеженим доступом.

Особливістю прихованих (стеганографічних) каналів зв'язку (СКЗ) є вбудовування повідомлень (стегоданих) до файлів-контейнерів, зокрема цифрових зображень (ЦЗ), та подальшої передачі сформованої стеганограми в ІКС. Сучасні адаптивні стеганографічні методи (АСМ) дозволяють суттєво зменшити ступінь зміни статистичних параметрів зображення-контейнеру (ЗК) у порівнянні з поширеними стеганографічними методами (СМ), зокрема nsF5, OutGuess, StegHide тощо, що ускладнює виявлення сформованих стеганограм при використанні систем протидії витоку ІзОД в ІКС.

Обмеженість апріорних даних щодо новітніх СМ призводить до суттєвого зниження точності роботи модулів виявлення (стегодетекторів, СД) прихованих даних (стеганограм) сучасних систем протидії витоку ІзОД (проблема zero-day). Додатковим фактором щодо зниження ефективності роботи сучасних СД є нелінійна залежність точності їх роботи від статистичних параметрів досліджуваних ЦЗ, що потребує повторного переналаштування СД при обробці нових пакетів зображень [8]. Це обумовлює актуальність та важливість науково-прикладної проблеми розробки високоточних методів виявлення стеганограм, здатних забезпечити високу (більше 95%) імовірність виявлення стеганограм в умовах відсутності апріорних даних щодо використаного СМ, мінімізації ступеня заповнення ЗК стегоданими та зміні в широких межах статистичних, параметрів досліджуваних зображень

Актуальність теми. Забезпечення високої точності виявлення стеганограм (більше 95%) потребує використання апріорних даних щодо особливостей використаного стеганографічного методу [9-11]. При цьому існуючі СД забезпечують надійне виявлення стеганограм лише у випадку середнього

($\Delta_{\alpha}^S > 10\%$) або ж сильного ($\Delta_{\alpha}^S > 20\%$) ступеня заповнення ЗК стегоданими, що унеможливило виявлення прихованих повідомлень у умовах мінімізації значення Δ_{α}^S , зокрема при використанні методів пакетної стеганографії (англ. batch steganography) [12].

Практичне застосування існуючих СД в сучасних системах протидії витоку ІЗОД при обміні даними в ІКС потребує забезпечення надійного виявлення стеганограм при обробці значних об'ємів ЦЗ, що характеризуються широким діапазоном зміни статистичних, спектральних та структурних параметрів зображень. Проте нелінійна залежність точності роботи СД від характеристик оброблюваних зображень призводить до необхідності використання ансамблю стегодетекторів, або ж постійній адаптації СД для роботи на нових вибірках зображень. Це потребує використання обчислювально складних процедур переналаштування стегодетектору, що призводить до зростання тривалості обробки ЦЗ.

З іншого боку, використання методів деструкції стеганограм в якості превентивної міри призводить до суттєвих змін статистичних, спектральних та структурних параметрів оброблених ЦЗ. Це демаскує втручання в роботу стеганографічного каналу зв'язку та може призвести до зміни типу та/або параметрів використовуваних СМ, зокрема застосування робастних методів приховання повідомлень. Також невирішеною лишаються важливі задачі в галузі стегоаналізу ЦЗ, а саме вилучення та підміни прихованих повідомлень з метою внесення дезінформації в стеганографічний канал зв'язку між зловмисниками.

Таким чином, розробка високоточних СД, здатних працювати в умовах відсутності апріорних даних щодо використаного СМ, мінімізації ступеня заповнення ЗК стегоданими та при значній варіативності спектральних, статистичних та структурних параметрів досліджуваних зображень, наразі є невирішеною науково-практичною проблемою, для якої запропоновані рішення лише для окремих (часткових) випадків.

Розробка ефективних систем виявлення стеганограм та протидії роботі ССЗ спирається на такі напрямки наукових досліджень: інформаційні технології та системи (Сергієнко І.В., Андон П.І., Теленик С.Ф., Ланде Д.В., Гроувер Д., Фіпсу Дж.), системний аналіз та моделювання інформаційної інфраструктури підприємств та організацій (Вінер М., Клір Дж., Згуровський М.З., Новіков О.М., Панкратова Н.Д., Томашевський В.М., Биченков В.В., Терейковський І.А.), теорія проектування та управління багаторівневими системами (Лебедев Д.В., Ролик О.І., Снитюк В.Є., Беллман Р., Ліберзон М.І.), методи криптографічного та стеганографічного аналізу даних (Fridrich J., Memon N., Petitcolas F., Савчук М.М., Кудін А.М., Олексійчук А.М., Ковальчук Л.В., Скрипник Л.В., Іванченко С.О., Аграновський А.В.), математичні методи дослідження складних сигналів (Павлов О.А., Бідюк П.І., Кіріченко Л.О., Кузнецов М.Ю., Шелестов А.Ю. Скляр Б., Mandelbrot B., Koller D., Meyer Y., Mallat S., Cressie N.), теорія штучного інтелекту (Хопфілд Д.Д., Голдберг Д., Зайченко Ю.П., Шлезінгер М.І., Гуляницький Л.Ф., Куссуль Н.М., Червоненкіс А.Я., Вапнік В.Н.) та інші.

Пошуком високоточних методів виявлення та протидії роботі ССЗ займаються провідні вітчизняні та закордонні вчені, зокрема Грибунін В.Г. [13, 14], Коначович Г.Ф. [11, 15], Задірака В.К. [16], Лужецький В.А. [17, 18], Кобозева А.А. [19, 20], Кошкіна Н.В. [21, 22], Корольов В.Ю. [23], Кузнецов О.О. [24], Avcibas I. [25, 25], Bas P. [27], Böhme R. [28], Boroumand M. [29-31], Butora J. [8, 32], Cox I. [33], Fridrich J. [10,34], Katzenbeisser S. [35], Ker A. [12, 36, 37], Pevny T. [38], Sullivan K. [39], та інші.

Серед поширених підходів до підвищення точності сучасних методів стегааналізу ЦЗ варто відмітити використання додаткових методів обробки ЦЗ для виявлення слабких змін параметрів ЗК, обумовлених вбудовуванням стегоданих, використання комплексних статистичних моделей ЗК [34] та штучних нейронних мереж (ШНМ) [29, 40] для підвищення точності оцінки статистичних і спектральних параметрів ЦЗ, застосування ансамблів СД тощо. Проте ефективність даних підходів суттєво залежить від наявних

апріорних даних щодо особливостей СМ [9-11], що знижує ефективність їх застосування у випадках, коли можливості щодо визначення типу та параметрів стеганографічного методу є обмеженими або навіть відсутніми. В якості прикладу можливо навести потужні СД на основі статистичних моделей ЗК, зокрема maxSRM [34], PHARM [41], GFR [42]. Особливістю даних СД є використання ансамблю фільтрів високих частот (ФВЧ) для виділення шумових складових зображення на рівні котрих, зазвичай, проводиться приховання повідомлень. Забезпечення високої точності роботи даних СД (більше 95%) при виявленні невідомих СМ, або ж обробці нових пакетів ЦЗ потребує ретельного відбору та тривалого налаштування параметрів кожного елемента ансамблю ФВЧ. Це обмежує практичне застосування використання даного підходу для побудови високоточних СД [30, 43-47].

Для подолання наведених обмежень використовуються спеціальні методи побудови СД, засновані на комплексному використанні декількох статистичних моделей ЗК. Проте вибір та налаштування параметрів кожної статистичної моделі для мінімізації значення помилки виявлення стеганограм при збереженні фіксованої (малої) тривалості налаштування СД наразі є невирішеною задачею, для якої запропоновані евристичні методи вирішення лише для окремих типів СМ. Тому важливою та актуальною науково-практичною проблемою є розробка нової концепції побудови СД, що дозволить забезпечити надійне виявлення довільних стеганографічних методів при варіації в широких межах значень статистичних, спектральних та структурних параметрів оброблюваних ЦЗ.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана згідно вимог щодо забезпечення захищеності та безперебійного функціонування інформаційних та комунікаційних систем об'єктів критичної інфраструктури, визначених в Концепції забезпечення національної системи стійкості, ухваленої Указом Президента України № 479/2021 від 27.09.2021 року. Тематика роботи включена до плану науково-дослідних робіт на кафедрі інформаційної безпеки КПІ ім. Ігоря Сікорського, узгод-

женого з центром досліджень та розробок «Самсунг РнД Інститут Україна» та Інститутом кібернетики ім. В.М. Глушкова НАН України. Результати дисертаційного дослідження були отримані та розвинуті у держбюджетній НДР, в якій автор був виконавцем: «Дослідження та застосування методів криптографічного аналізу важкозворотних перетворень у сучасних криптографічних системах захисту інформації з урахуванням додаткових даних. НДР «Кета» (держ. реєстр. № 0114U004643).

Мета і завдання дослідження. *Метою роботи є розробка методів синтезу стегодетекторів, що забезпечують високу вірогідність виявлення стеганограм в умовах відсутності апріорних даних щодо використаного стеганографічного методу, мінімізації ступеня заповнення ЗК стегоданими та зміні в широких межах статистичних, спектральних і структурних параметрів досліджуваних зображень.*

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Виконати аналітичний огляд існуючих моделей, методів і засобів формування та виявлення стеганограм з даними, вбудованими до зображень-контейнерів;

2. Розробити підходи до модернізації існуючих стегодетекторів для підвищення вірогідності виявлення стеганограм, сформованих згідно невідомих стеганографічних методів та малого (менше 10%) ступеня заповнення ЗК стегоданими;

3. Розробити математичний апарат для синтезу структури та оптимізації параметрів СД, здатних забезпечити надійне виявлення стеганограм в умовах відсутності апріорних даних щодо стеганографічного методу, слабого заповнення ЗК стегоданими (менше 10%) і зміні в широких межах статистичних, спектральних та структурних параметрів оброблюваних ЦЗ;

4. Розробити методи для практичної реалізації запропонованої структури високоточних стегодетекторів, здатні наблизитися до теоретичних оцінок досяжної імовірності виявлення стеганограм;

5. Розробити програмну реалізацію запропонованих методів синтезу та оптимізації параметрів СД у вигляді програмного комплексу для проведення стегааналізу цифрових зображень, що дозволяє з високою вірогідністю виявляти стеганограми незалежно від використаного методу приховання повідомлень та рівня заповнення ЗК стегаданими;

6. Виконати експериментальні дослідження точності виявлення стеганограм з використанням запропонованого, розробленого та реалізованого програмного комплексу в найбільш складних випадках стегааналізу, а саме відсутності апріорних даних щодо використаного стегаграфічного методу та малого ступеня заповнення ЗК стегаданими (менше 10%);

7. Дослідити перспективи використання розробленого програмного комплексу для вирішення найбільш складних задач стегааналізу ЦЗ, а саме надійної деструкції стеганограм при мінімізації змін статистичних, спектральних та структурних параметрів ЦЗ, а також визначення положення (локалізації) пікселів, використаних для приховання стегабітів, для розробки методів екстракції вбудованих повідомлень.

Об'єктом дослідження є процес виявлення стеганограм при обробці, зберіганні та передачі цифрових зображень в інформаційно-комунікаційних системах (ІКС).

Предметом дослідження є методи, моделі та засоби побудови стегадетекторів для надійного виявлення повідомлень, несанкціоновано вбудованих до цифрових зображень, в умовах обмеженості апріорних даних щодо використаного стегаграфічного методу.

Методи дослідження. Для досягнення мети та вирішення завдань дисертаційного дослідження в роботі використано методи спектрального аналізу (двовимірні дискретні косинусне та вейвлет перетворення), методи компонентного аналізу (дослідження змін статистичних, спектральних та структурних параметрів складових ЦЗ при проведенні їх попередньої обробки), методи статистичного моделювання (аналіз кореляційних характеристик матриць яскравості суміжних пікселів ЦЗ, оцінка відмінностей між розподілами

значень яскравості пікселів ЗК та стеганограм), методи теорії оптимізації (вирішення оптимізаційних задач щодо формування систем функцій для проведення декомпозиції цифрових зображень), методи теорії розпізнавання образів (налаштування стегодетекторів та оцінка їх ефективності), методи об'єктно-орієнтованого програмування та комп'ютерного моделювання (програмна реалізація алгоритмів та методів обробки ЦЗ). Дослідження точності виявлення стеганограм при застосуванні відомих та розроблених методів стегааналізу цифрових зображень проводилося із застосуванням програмного комплексу, розробленого з використанням середовища розробки MATLAB® та JetBrains® PyCharm.

Наукова новизна одержаних результатів.

1. Вперше визначено оптимальні методи попередньої обробки (МПО) досліджуваних зображень за критерієм мінімізації помилки виявлення стеганограм при розробці СД, що спрямовані на визначення положення та подальше видалення локальних збурень значень яскравості пікселів ЗК, обумовлених прихованням повідомлень. Застосування запропонованих МПО при синтезі стегодетекторів дозволило наблизити точність їх роботи до теоретичних оцінок досяжної імовірності виявлення стеганограм у всьому діапазоні змін ступеня заповнення ЗК стегоданими, що є недосяжним при використанні відомих типів МПО, заснованих на знешумленні оброблюваних зображень.

2. Вперше розроблено метод для забезпечення надійного виявлення змін статистичних, спектральних та структурних параметрів ЗК, обумовлених вбудовуванням стегоданих, який заснований на реконструкції вихідного виду ЗК із застосуванням спеціальних систем функцій (ССФ) в якості базису перетворення досліджуваного зображення, що дозволяє створювати високоточні СД, здатні надійно працювати в умовах «сліпого» стегааналізу ЦЗ (а саме, відсутності апіорних даних щодо використаного стегаграфічного методу), при збереженні відносно низької обчислювальної складності процедури налаштування стегодетектору.

3. Вперше запропоновано метод визначення положення пікселів ЗК, використаних для приховання окремих стегобітів повідомлення, який заснований на представленні задачі локалізації пікселів як задачі сегментації досліджуваного зображення. Це дозволило не тільки підвищити ефективність методів деструкції стегоданих при забезпеченні мінімального впливу на статистичні та спектральні параметри ЦЗ, а й створити передумови для розробки методів вилучення (екстракції) стегоданих зі стеганограм.

4. Удосконалено метод синтезу структури та оптимізації параметрів високоточних стегодетекторів шляхом заміни декількох складних етапів налаштування стегодетектору на вирішення оптимізаційної задачі максимізації відстані Хеллінгера між кластерами векторів, що відповідають статистичним параметрам ЗК та сформованих стеганограм. Це дало можливість забезпечити високу вірогідність виявлення стеганограм незалежно від способу їх формування.

5. Удосконалено метод робастної оцінки відмінностей між імовірнісними розподілами значень яскравості пікселів ЗК та стеганограм, що відрізняється використанням спеціальних показників, а саме відстані Хеллінгера D_H , відстані Бхаттачарая D_B , χ^2 -квадрат відстані D_{χ^2} та спектру відстаней Реньї D_R^α . Це дозволило суттєво (до двох разів) підвищити точність виявлення стеганограм навіть в умовах обробки пакетів ЦЗ, що характеризуються високим ступенем варіації статистичних, спектральних та структурних параметрів.

6. Удосконалено методи підвищення точності роботи СД у випадку обмеженості апріорних даних щодо використаного СМ шляхом зниження впливу нелінійних зв'язків між статистичними параметрами досліджуваних зображень за рахунок проекції векторів, які відповідають статистичним параметрам ЗК та сформованих стеганограм, до простору вищої розмірності. Це дозволяє збільшити кількість інформативних параметрів ЦЗ при проведенні стегоаналізу та, відповідно, підвищити точність виявлення стеганограм без

необхідності використання обчислювально складних МПО, зокрема потужних ансамблів ФВЧ.

7. Набули подальшого розвитку методи деструкції стеганограм за рахунок використання варіаційних методів аналізу багатовимірних сигналів для зниження впливу адитивних шумів при проведенні реконструкції вихідного виду ЗК за наявними (зашумленими) даними, що дає можливість підвищити точність оцінки параметрів ЗК в широкому діапазоні зміни параметрів адитивних завад та, відповідно, забезпечити надійну деструкцію стеганограм.

Практичне значення отриманих результатів.

1. Показано, що принциповим обмеженням відомих методів стегааналізу ЦЗ є необхідність використання апріорних даних щодо СМ та статистичних параметрів оброблюваних зображень для вибору оптимальних методів попередньої обробки зображень за критерієм мінімізації помилки виявлення стеганограм. Це унеможливує швидку адаптацію налаштованих СД для виявлення нових типів СМ, оскільки потребує тривалого налаштування параметрів МПО на декількох пакетах досліджуваних ЦЗ для забезпечення високої (більше 90%) точності виявлення стеганограм. Запропонований метод синтезу високоточних стегадетекторів дозволяє подолати дане обмеження, оскільки не потребує використання апріорних даних щодо використаних стегаграфічних методів.

2. Розроблено метод формування спеціальних систем функцій для проведення реконструкції вихідного виду ЗК за наявними (зашумленими) даними. Особливістю методу є забезпечення високої точності реконструкції ЗК в умовах наявності значних адитивних завад та обробки ЦЗ, статистичні та спектральні параметри котрих суттєво різняться. При цьому формування ССФ згідно запропонованого методу можливе при використанні відносно малої кількості прикладів вихідних (непотворених) сигналів (в межах 15-30), що обумовлює перспективність використання даного методу в задачах аналізу даних різної природи, зокрема акустичних та біометричних сигналів, де формування потужних пакетів тестових сигналів є неможливим.

3. Показано перспективність використання запропонованого методу реконструкції вихідного виду ЗК на основі обробки досліджуваного зображення із застосуванням ССФ в найбільш складних випадках деструкції стегограм, а саме маскуванню факту втручання в стеганографічний канал передачі даних. Зокрема, запропонований метод дозволяє мінімізувати зміни статистичних, спектральних та структурних параметрів оброблюваних зображень у порівнянні з відомими методами деструкції при забезпеченні надійного знищення вбудованих стегоданих.

4. Запропоновано, розроблено та реалізовано програмний комплекс проведення стегоаналізу ЦЗ для вирішення широкого спектру задач щодо виявлення, вилучення та деструкції повідомлень, вбудованих до зображень-контейнерів. Вагомою перевагою розробленого комплексу є забезпечення надійної роботи навіть в умовах «сліпого» стегоаналізу ЦЗ. Дана особливість дозволяє використовувати запропонований комплекс в якості універсального рішення для виявлення та протидії роботі стеганографічних каналів передачі ІзОД в інформаційно-комунікаційних системах.

5. Опубліковані результати досліджень, проведених в дисертаційній роботі, використано в центрі досліджень та розробок «Самсунг РнД Інститут Україна» при виконанні науково-дослідних у галузі перевірки автентичності цифрових зображень. Реалізація напрацювань дисертаційної роботи дозволила отримувати важливу інформацію, що стосується оцінки статистичних та спектральних параметрів ЦЗ, для вирішення задач Управління оперативного зв'язку та електронних комунікацій ДСНС України. Запропоновані методи локалізації положення слабких локальних збурень на цифрових зображеннях в умовах обмеженості апріорних даних щодо параметрів джерела збурень були використані в конструкторському бюро «Шторм» КПІ ім. Ігоря Сікорського при виконанні робіт за міжнародними контрактами. Розроблені методи визначення характеристик цифрових сигналів впроваджено в навчальний процес механіко-математичного факультету КНУ ім. Тараса Шевченка, кафедри телекомунікаційних та радіоелектронних систем Націо-

нального авіаційного університету, кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського.

Особистий внесок здобувача. Всі положення дисертації, що виносяться до захисту, отримані автором особисто. У наукових працях опублікованих у співавторстві, що висвітлюють питання дисертаційного дослідження, здобувачу належить авторство на:

- 1) Оригінальні результати порівняльного аналізу сучасних методів стеганографії та стегоаналізу цифрових зображень, отримані з використанням:
 - a) Методів авторегресійного аналізу в задачах виявлення стеганограм та оцінки їх параметрів [48-50];
 - b) Універсальних стегодетекторів (УСД), зокрема розроблених модифікацій УСД Авкібаса [51-57];
 - c) Стегодетекторів, заснованих на використанні статистичних [58-62] та структурних [11, 63-67] параметрів досліджуваних ЦЗ;
 - d) Методів деструкції стеганограм [68-70];
- 2) Дослідження впливу на точність роботи статистичних СД невідповідності типу перетворень ЗК, що використовуюються для приховання повідомлень та проведення стегоаналізу ЦЗ [71];
- 3) Дослідження відмінностей між імовірнісними розподілами значень яскравості пікселів ЗК і стеганограм, сформованих з використанням новітніх адаптивних стеганографічних методів [72-77];
- 4) Дослідження взаємного положення кластерів векторів, що відповідають статистичним параметрам ЗК та стеганограм, сформованих згідно поширених стеганографічних методів [78];
- 5) Дослідження методів попередньої обробки цифрових зображень в задачах стегоаналізу з використанням додаткового зашумлення зображень [79-82], шляхом повторного приховання повідомлень [83, 84], застосування методів підвищення візуальної якості зображень [85-88], зокрема варіаційних методів знешумлення сигналів [89, 90],

методів компонентного аналізу сигналів [91], штучних нейронних мереж [92-96], методів декомпозиції ЦЗ з використанням спеціальних систем функцій в задачах стегоаналізу ЦЗ [97];

- 6) Побудову комплексних систем захисту інформації [98];
- 7) Застосування запропонованого методу формування складних систем функцій для зменшення впливу нестационарних завад у біометричних сигналах, що використовуються в системах автентифікації користувачів [99-106];
- 8) Запропонований метод локалізації позиції пікселів зображення-контейнеру, використаних для приховання стегобітів повідомлення [107];
- 9) Програмний комплекс, на основі якого проведено порівняльний аналіз імовірності виявлення стеганограм з даними, вбудованими в ОПЗК, при використанні відомих та запропонованих СД [108-110].

Апробація результатів дисертації. Основні положення дисертації розглядалися і обговорювалися на засіданнях кафедри фізико-технічних засобів захисту інформацій та кафедри інформаційної безпеки Навчально-наукового Фізико-технічного інституту НТУУ «КПІ ім. Ігоря Сікорського», науковому семінарі «Методи обчислювальної математики», що проводиться в Інституті кібернетики ім. В.М. Глушкова НАН України під керівництвом акад. Задіраки В.К. та акад. Хіміча О.М., а також 22 Міжнародних та 5 Всеукраїнських науково-практичних конференціях: IEEE International Scientific-Practical Conference “Problems of Infocommunications Science and Technology” (Харків, Україна, 2017, 2020, 2021); International Research and Practice Conference “Modern Methods, Innovations, and Experience of Practical Application in the Field of Technical Sciences” (Радом, Польща, 2017); Міжнародної науково-практичної конференції «Обробка сигналів та негаусівських процесів», присвяченої пам’яті професора Ю.П. Кунченка (Черкаси, Україна, 2017-2022); Міжнародної науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи» (Київ, Україна, 2017-2020); Міжнародної науково-тех-

нічної конференції «Системний аналіз та інформаційні технології» (Київ, Україна, 2017-2018); X Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій» (Запоріжжя, Україна, 2020); Міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах» (Київ, Україна, 2017); 25-го Міжнародного форуму «Радіоелектроніка та молодь в XXI столітті» (Харків, Україна, 2021); Міжнародної науково-практичної конференції «Захист інформації і безпека інформаційних систем» (Львів, Україна, 2017, 2019); Всеукраїнська науково-практична конференція “Theoretical and Applied Cybersecurity (TACS-2023)”, присвячена 100-річному ювілею академіка В.М. Глушкова (Київ, Україна, 2023); Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики» (Київ, Україна, 2017-2020).

Публікації. За результатами дисертаційного дослідження опубліковано 55 наукових праць, в тому числі: 21 стаття у фахових виданнях (з них п'ять у міжнародних наукових журналах, що індексуються в наукометричних базах даних Web of Science, Google Scholar, Index Copernicus та три у міжнародних наукових журналах, які індексуються в наукометричній базі даних Scopus), три міжнародні патенти на винахід (zareєстровані в Всесвітній організації інтелектуальної власності (WIPO), організаціях реєстрації патентів та торгових марок США і Республіки Корея), 30 публікацій у збірниках матеріалів Міжнародних (22 матеріалів, з них два у матеріалах конференцій, що індексуються в наукометричних базах даних Scopus та Web of Science) та Всеукраїнських (8 матеріалів) науково-практичних конференцій, один підручник, що додатково відображає результати дисертації.

Структура дисертації. Дисертаційна робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел зі 255 найменувань (81 робота вітчизняних та 174 роботи закордонних вчених) та чотирьох додатків. Загальний обсяг роботи становить 434 сторінки з яких 266 сторінок

основного тексту, 28 сторінок переліку використаної літератури та 95 сторінок додатків. В роботі наведено 76 рисунків та 14 таблиць.

РОЗДІЛ 1 ОГЛЯД МЕТОДІВ СТЕГАНОГРАФІЇ ТА СТЕГОАНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Особливістю сучасних атак на критичну інформаційну інфраструктуру державних установ та приватних організацій є проведення тривалого попереднього аналізу елементів та систем КІІ з метою визначення їх вразливостей [111, 112]. Вирішення даної задачі потребує формування надійних каналів зв'язку для обміну повідомленнями між зловмисниками на етапі як підготовки, так і проведення атаки на КІІ. Для ускладнення виявлення даних каналів зв'язку при використанні сучасних систем протидії витоку ІзОД, формування даних каналів проводиться з використанням методів цифрової стеганографії, що дозволяють приховати власне факт передачі повідомлень [9-11, 13].

В даному розділі проведено аналітичний огляд сучасних моделей, методів та підходів до приховання повідомлень в мультимедійних даних, зокрема цифрових зображеннях (ЦЗ), а також методів виявлення сформованих стеганограм. Особлива увага приділена новітнім методам як вбудовування стегоданих до зображень-контейнерів (ЗК), так і виявлення сформованих стеганограм із застосуванням методів статистичного аналізу та штучних нейронних мереж.

1.1 Основні положення та область використання методів стеганографії і стегоаналізу мультимедійних даних

Стеганографія (грец. *steganos* (στεγανός) «прихований» та *graphein* (γράφειν) «пишу») – наука, що вивчає способи та методи приховання даних [9-11,13,14,33,35]. В якості носіїв (контейнерів) для приховання повідомлень (стегоданих) широко використовуються цифрові дані, зокрема текст, мультимедійні файли, програми та вихідний код [9-11, 13].

До основних галузей застосування методів стеганографії цифрових даних можливо віднести [9,13,33,113]:

1. Вбудовування додаткової інформації до аудіо та відео даних, зокрема відомостей щодо авторства, використаних методів обробки мультимедійних даних, посилань на додаткові матеріали та web-ресурси [114-117];
2. Внесення міток (водяних знаків) до цифрових даних з метою протидії їх несанкціонованому копіюванню, модифікації та розповсюдженню в ІКС [13,33,113], перевірці цілісності даних, або ж підтверженні авторства (англ. zero watermarking) [118];
3. Вбудовування спеціалізованих (службових) даних до мультимедійних файлів з метою протидії їх обробці (наприклад відтворення, копіювання) на неліцензованих мультимедійних програвачах (англ. Digital Right Management, DRM) [9,33];
4. Прихованої анотації документів в медичних закладах, наприклад згідно стандарту DICOM [119];
5. Захисту приватних каналів зв'язку між дисидентами або ж несанкціонованій передачі ІзОД зловмисниками [9-11, 113].

Особливу увагу фахівців в галузі інформаційної та кібернетичної безпеки привертають випадки використання методів стеганографії для формування прихованих каналів передачі ІзОД і обміну даними між зловмисниками [113,120,121]. В якості прикладу можливо навести дослідження провідних аналітичних компаній в галузі кібербезпеки щодо використання зловмисниками стеганографічних каналів зв'язку при проведенні атак на КІІ приватних організацій [120], вбудовування ІзОД до мультимедійних даних, що циркулюють в соціальних мережах [122], поширення шкідливого забезпечення [123], прихованої передачі ІзОД державних та приватних установ (наприклад, з використанням програмних засобів Shamoan, ZeusVM, NetTraveler) [124] тощо.

Зростання уваги до галузі стеганографії та стегааналізу цифрових даних в останні роки підтверджується збільшенням кількості публікацій в даній галузі, що індексуються у бібліографічній системі IEEEExplore (рис. 1.1):

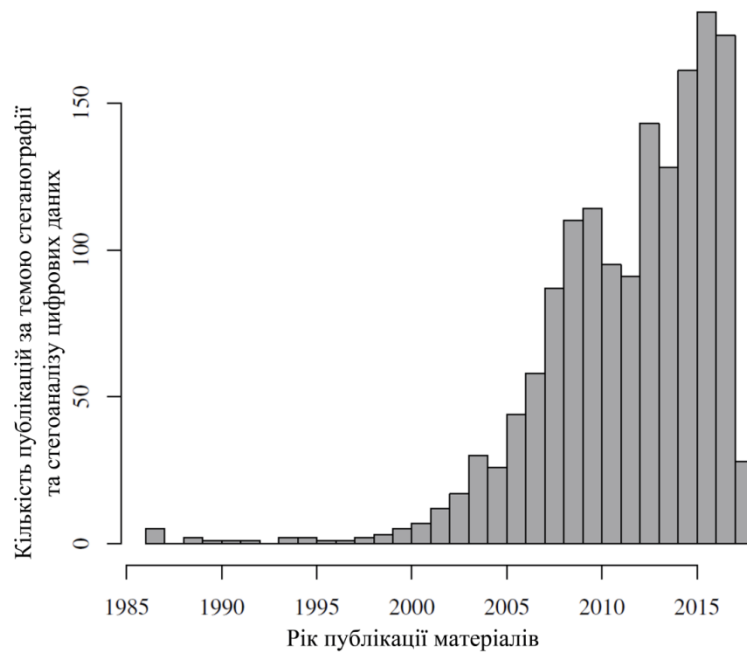


Рисунок 1.1 – Кількість публікацій за напрямком стеганографії та стегоаналізу цифрових даних у бібліографічній системі IEEExplore.

За матеріалами роботи [125].

Відмітимо суттєве зростання кількості публікацій в галузі стеганографії та стегоаналізу цифрових даних з 2010 року (рис. 1.1). Це обумовлено появою нових підходів як до формування стеганограм (наприклад, із застосуванням адаптивних стеганографічних методів), так і побудови високоточних СД з використанням методів статистичного моделювання та штучних нейронних мереж (ШНМ) [30,44,126,127].

Сучасні методи цифрової стеганографії, що використовуються для формування прихованих каналів передачі даних, можливо розділити на наступні групи [9-11, 13,113]:

1. З використанням особливостей обробки даних в автоматизованих системах [128] – зокрема, використання службових полів (атрибутів) ІР-датаграм [129], прихованих файлових систем [130] тощо;
2. Шляхом вбудовування стегоданих до файлів-контейнерів, що циркулюють в ІКС [120] – наприклад, цифрові зображення, аудіо та відео-дані, які передаються у соціальних мережах, сервісах обміну даними тощо.

Відмітимо, що практичне застосування методів, що відносяться до першої групи, наразі є обмеженим [120]. Це обумовлено широким впровадженням методів виявлення несанкціонованих змін атрибутів даних, зокрема модифікації або підміни службової інформації.

Методи цифрової стеганографії, що відносяться до другої групи, набули широкого розповсюдження. Зокрема, значна увага дослідників в галузі стеганографії ЦЗ приділяється розробці новітніх СМ, що дозволяють суттєво зменшити рівень демаскуючих ознак сформованих стеганограм у порівнянні з поширеними підходами. Також, все більшого поширення набувають спеціалізовані стеганографічні методи, засновані на розділенні стегоданих на декілька частин та їх приховання з використанням послідовності ЗК (англ. batch steganography) [12,36,131], шляхом синхронізації змін яскравості суміжних пікселів ЗК [132] та інші

В якості файлів-контейнерів для приховання повідомлень в сучасних СМ широко використовуються ЦЗ, що обумовлено [9-11, 13]:

1. Надлишковістю цифрового представлення ЦЗ – дозволяє приховувати значні об'єми стегоданих, або ж підвищувати стійкість (робастність) отримуваних стеганограм до методів стегоаналізу;
2. Наявністю у більшості ЦЗ областей, що мають шумоподібну структуру (наприклад, зображення трави, піску, хвиль) – висока складність моделювання даних областей з використанням методів статистичного та спектрального аналізу дозволяє ефективно маскувати зміни параметрів ЗК, обумовлені вбудовуванням стегоданих;
3. Висока варіативність статистичних, спектральних та структурних параметрів реальних ЦЗ – що призводить до зниження точності роботи СД, налаштованих з використанням стандартних пакетів зображень BOWS-2 [133], BOSS [27] та ALASKA [134], при роботі на нових пакетах зображень (проблема domain mismatch).

Широке використання ЦЗ в якості файлів-контейнерів в стеганографічних системах зв'язку протягом 2010-2020 років призвело до появи значної кі-

лькості моделей, методів та підходів до приховання повідомлень [9-11,13]. Тому становить інтерес аналітичний огляд даних методів, що дозволить визначити переваг та обмеження практичного застосування новітніх СМ.

1.2 Класифікація методів стеганографії цифрових зображень

Зважаючи на значну кількість розроблених стеганографічних методів для вбудовування стегоданих до ЦЗ, в літературі запропоновано декілька класифікації даних методів в залежності від особливостей процедури формування стеганограм [9,10,13,35]:

- За областю приховання повідомлень – в залежності від способу обробки елементів ЦЗ для приховання окремих стегобітів сучасні стеганографічні методи можливо розділити на наступні класи:
 - Приховання з використанням службових атрибутів – засновані на заміщенні службових атрибутів (наприклад даних EXIF та XMP), що використовуються у поширених форматах графічних даних, зокрема PNG, GIF, JPEG, PSD та TIFF. Дані методи набули широкого поширення у 2000-2010 роках, зважаючи на простоту їх використання [10,11]. Для виявлення стеганограм, сформованих згідно даних стеганографічних методів, запропоновано низку високоточних методів сигнатурного стегоаналізу.
 - Приховання в просторовій області зображення-контейнеру – засновані на зміні (модифікації) значень яскравості пікселів ЗК. Дана група методів наразі є однією з найбільш розповсюджених, зважаючи на широке поширення адаптивних СМ, зокрема методів HUGO, S-UNIWARD та WOW.
 - Приховання в області перетворення зображення-контейнеру (ОПЗК) – засновані на модифікації значень коефіцієнтів розкладу ЗК, отриманих за результатами застосування поширених типів спектральних перетворень. В якості даних перетворень широко використовуються двовимірне дискретне косинусне перетво-

рення (ДДКП) та двовимірне дискретне вейвлет-перетворення (ДДВП) [10,11].

- За кількістю етапів обробки (перетворень) зображення-контейнеру в процесі формування стеганограм запропоновані СМ можливо розділити на наступні групи:
 - Одноетапні методи – засновані на застосуванні заданого (фіксованого) перетворення ЗК в процесі вбудовування стегоданих, наприклад ДДКП. Відносно низька обчислювальна складність даних методів дозволяє використовувати їх для пакетної обробки ЦЗ при формуванні стеганограм (англ. batch steganography).
 - Багатоетапні методи – запропоновані для додаткового зниження рівня демаскуючих ознак у порівнянні з одноетапними методами шляхом використання послідовності перетворень ЗК. Проте практичне застосування даних методів потребує визначення типу та послідовності застосування перетворень ЗК, що дозволяють мінімізувати зміни статистичних, спектральних та структурних параметрів контейнеру в процесі формування стеганограм.
- За способом приховання стегобітів повідомлення до ЗК можливо виокремити наступні групи стеганографічних методів:
 - Статичні методи – засновані на використанні фіксованого алгоритму дій, що не враховує особливостей ЗК при формуванні стеганограм. Дані методи є одними з найбільш поширених, зважаючи на простоту реалізації та робастність до поширених методів стегоаналізу ЦЗ. Тим не менше, використання фіксованих значень параметрів даних СМ, отриманих емпіричним чином, може призводити до суттєвого збільшення рівня демаскуючих ознак при обробці нових вибірок зображень.
 - Адаптивні методи – особливістю даних методів є представлення процесу формування стеганограм як вирішення оптимізаційної

задачі щодо мінімізації спотворень статистичних параметрів ЗК при фіксованій довжині бітового представлення стегоданих. Це дозволяє суттєво підвищити стійкість отримуваних стеганограм до методів статистичного та структурного стегоаналізу у порівнянні з поширеними стеганографічними методами, проте потребує використання обчислювально складних методів оцінки змін статистичних параметрів ЗК.

Наразі, одними з найбільш поширених СМ є багатоетапні та адаптивні методи приховання повідомлень до ЗК, зокрема засновані на вбудовуванні повідомлень в просторовій області, або ж в області перетворення ЗК. Це обумовлено високою стійкістю стеганограм, сформованих згідно даних методів, по відомих типів СД. Відповідно, становить інтерес аналіз особливостей процесу приховання повідомлень до ЗК згідно багатоетапних та адаптивних СМ для визначення демаскуючих ознак сформованих стеганограм, та їх використання при розробці високоточних стегодетекторів.

1.2.1 Методи приховання повідомлень в області перетворення зображення-контейнеру

Одним з найбільш відомих підходів до вбудовування стегоданих в ОПЗК є методи приховання повідомлень в частотній області ЗК [10,135], наприклад багатоетапні методи Джозефа [136], Хана [137] та комплексні методи Елайона [138] і Гунджаля [139]. Використання декількох етапів обробки ЗК при вбудовуванні повідомлень згідно даних СМ дозволяє забезпечити високу робастність отримуваних стеганограм до поширених методів стегоаналізу ЦЗ при забезпеченні стійкості стегоданих до випадкових (наприклад, вплив шумів каналу зв'язку), або навмисних (зокрема, застосування методів деструкції) змін стеганограм. Для комплексних методів приховання повідомлень в ОПЗК характерна наявність етапу попередньої обробки стегоданих з метою наближення їх виду до псевдовипадкового сигналу, що ускладнює виявлення сформованих стеганограм [11,140].

В більшості випадків, формування стеганограм згідно багатоетапних СМ проводиться шляхом вагового додавання коефіцієнтів розкладу зображення-контейнеру $W(I)$ та стегоданих $W(D)$, представлених у вигляді ЦЗ, в обраному базисі перетворення $W(\cdot)$ з ваговим коефіцієнтом $G > 0$, що залежить від енергії приховуваних повідомлень:

$$W(S) = W(I) + G \times W(D), \quad (1.1)$$

де $W(S)$ – матриця коефіцієнтів заповненого ЗК. Перетворення приховуваних повідомлень, представлених у вигляді бітової послідовності, до форми ЦЗ відбувається шляхом представлення стегоданих у вигляді матриці фіксованого розміру, заповнення рядків/стовпчиків даної матриці окремими бітами повідомлення, та подальшого заповнення нулями невикористаних елементів матриці для забезпечення заданого розміру (наприклад, за розміром ЗК).

Обробка окремих каналів кольору ЗК та стегоданих згідно виразу (1.1) проводиться з використанням стандартних або спеціальних спектральних перетворень, а саме двовимірного дискретного вейвлет [141,142] та косинусного [141,143] перетворень, сингулярного розкладу [144] тощо.

Для отримання стеганограми в просторовій області, до отриманих коефіцієнтів $W(S)$ (1.1) застосовується обернене перетворення – $W^{-1}(W(S))$. Вилучення (екстракція) стегоданих з отриманої стеганограми \tilde{S} проводиться згідно наступної формули:

$$W(D) = (W(\tilde{S}) - W(I))/G.$$

Для мінімізації спотворень кольорів ЗК при прихованні повідомлень в комплексних СМ [138,139] проводиться зміна системи кольору як зображення-контейнеру (з RGB на YCbCr або YIQ), так і стегоданих, представлених у вигляді кольорових ЦЗ (з RGB на Grayscale) [139,141,143]. При цьому вбудовування стегоданих проводиться з використанням Y-складової яскравості ЗК (метод Елайона) або різницевої колірної I-складової (метод Гунджалля) зображення-контейнеру.

Багатоетапні стеганографічні методи дозволяють суттєво підвищити стійкість отримуваних стеганограм до методів статистичного стегоаналізу у порівнянні з поширеними одноетапними СМ [137,145,146]. Проте нелінійний характер змін статистичних параметрів ЗК при зміні порядку та типу перетворень ЗК суттєво ускладнює визначення композиції перетворень зображення-контейнеру, що дозволяє забезпечити малий рівень демаскуючих ознак (змін статистичних параметрів ЗК) при формуванні стеганограм. Для подолання даного обмеження запропоновано адаптивні стеганографічні методи (АСМ) [147], що засновані на мінімізації загального рівня спотворень ЗК при формуванні стеганограм [147-150]. Дана особливість дозволяє корегувати (адаптувати) параметри СМ при вбудовуванні повідомлень з врахуванням змін статистичних, спектральних та структурних параметрів ЗК та, відповідно, зменшувати рівень демаскуючих ознак. Це обумовлює широке використання даних методів при розробці новітніх ССЗ, що використовуються злоумисниками при проведенні атак на КІІ державних та приватних установ [1,3].

1.2.2 Адаптивні стеганографічні методи

Значна кількість новітніх СМ заснована на представленні процесу формування стеганограм як вирішення однокритеріальної оптимізаційної задачі з обмеженнями [9,10,13,113], а саме мінімізації значення емпіричної функції оцінки спотворень зображення-контейнеру \mathbf{X} при вбудовуванні повідомлення \mathbf{M} , що має фіксовану довжину бітового представлення [147-150]:

$$D(\mathbf{X}, \mathbf{Y}) = \sum_{i,j} \rho_{i,j}(\mathbf{X}, \mathbf{Y}) \xrightarrow{|\mathbf{M}|=const} \min, \quad (1.2)$$

де \mathbf{X}, \mathbf{Y} – відповідно, зображення-контейнер та сформована стеганограма розміром $M \times N$ пікселів; $\mathbf{M} \in \{0; 1\}^m$ – стегодані, представлені у вигляді бітової послідовності довжиною m бітів; $\rho_{i,j}(\cdot)$ – функція оцінки змін статистичних характеристик ЗК при зміні яскравості пікселю зображення-контейнеру з координатами (i, j) ; $D(\mathbf{X}, \mathbf{Y})$ – функція оцінки спотворень параметрів ЗК при вбудовуванні повідомлення \mathbf{M} .

За результатами вирішення оптимізаційної задачі (1.2) визначається група пікселів ЗК, зміни яскравості котрих дозволять мінімізувати зміни статистичних характеристик ЦЗ при вбудовуванні стегоданих [147]. Таке представлення процесу формування стеганограм дозволяє застосовувати потужний математичний апарат методів оптимізації для мінімізації рівня демаскуючих ознак вбудованих повідомлень при формуванні стеганограм [132,147].

В більшості випадків, вбудовування стегобітів згідно виразу (1.2) проводиться шляхом зміни (маніпуляції) значення яскравості пікселів ЗК [9-11]. Для зменшення кількості даних змін при збереженні високої робастності отримуваних стеганограм до відомих методів стегоаналізу ЦЗ, використовуються методи попередньої обробки ЗК та стегоданих, зокрема визначення послідовності пікселів зображення-контейнеру для вбудовування окремих стегобітів [7, 10]. Особливий випадок становить використання пікселів ЗК, значення яскравості котрих є близькими до 0 або $(2^k - 1)$, де k – глибина кольору ЗК (в бітах). Для обробки даних пікселів ЗК можуть використовуватися наступні методи [7, 10]:

- Величина зміни яскравості пікселю v обирається згідно значення яскравості пікселю ЗК: $v = (+1)$ при обробці пікселя з яскравістю рівною нулю, та $v = (-1)$ для пікселя з яскравістю $(2^k - 1)$;
- Використання лише пікселів ЗК, значення яскравості котрих лежать в діапазоні від нуля до $(2^k - 1)$ та не рівні даним значенням;
- Вилучення з переліку пікселів для вбудовування повідомлень елементів, що мають граничні значення яскравості (нуль або $(2^k - 1)$).

Відмітимо, що величина змін статистичних параметрів ЗК при формуванні стеганограм згідно АСМ суттєво залежить від особливостей розподілу значень яскравості пікселів зображення-контейнеру [151]. Відповідно, визначення послідовності пікселів ЗК, зміни яскравості котрих при вбудованні стегобітів призведуть до найменших змін статистичних параметрів зображення-контейнеру, є нетривіальною та обчислювально складною задачею. Вирі-

шення даної задачі потребує повного перебору всіх можливих послідовностей пікселів зображення-контейнеру для визначення значення функції $\rho_{i,j}(\cdot)$ у виразі (1.2). Для вирішення даної задачі запропоновано наступні групи стеганографічних методів:

1. Стеганографічні методи, засновані на моделюванні складових зображення-контейнеру – ґрунтуються на побудові функції $\rho_{i,j}(\cdot)$ у виразі (1.2) з використанням статистичних моделей шумових складових ЗК;
2. Спеціалізовані стеганографічні методи – спрямовані на додаткове зниження рівня демаскуючих ознак стеганограм шляхом використання спеціальних методів обробки ЗК та стегоданих.

Відмітимо, що практичне застосування наведених груп СМ дозволяє суттєво зменшити рівень демаскуючих ознак сформованих стеганограм у порівнянні з поширеними типами стеганографічних методів [9,13]. Тому становить інтерес дослідження особливостей даних стеганографічних методів, що дозволяють забезпечити високу стійкість сформованих стеганограм до відомих методів стегоаналізу ЦЗ.

1.2.3 Стеганографічні методи, засновані на моделюванні складових зображення-контейнеру

Одним з найбільш поширених підходів до побудови АСМ є використання спеціалізованих функцій $\rho_{i,j}(\cdot)$ у виразі (1.2), що дозволяють врахувати зміни статистичних параметрів окремих складових ЗК при вбудовуванні стегоданих [147,152-154]. Розробка даних функцій $\rho_{i,j}(\cdot)$ потребує дослідження нелінійної залежності статистичних, спектральних та структурних параметрів окремих складових ЗК від змін значень яскравості пікселів зображення-контейнеру, що є нетривіальною задачею для вирішення котрої запропоновано лише емпіричні методи [9,13,155]. Для зниження обчислювальної складності вирішення задачі синтезу функцій $\rho_{i,j}(\cdot)$ при збереженні фіксованого

(малого) рівня демаскуючих ознак отримуваних стеганограм широко використовуються наступні припущення [147,152,153,156]:

1. Імовірності зміни яскравості пікселів ЗК є однаковими незалежно від значенням вбудовуваного стегобіту. Відповідно, значення функції оцінки змін статистичних характеристик ЗК при вбудовуванні окремого стегобіту є рівними: $\rho_{i,j}(-1) = \rho_{i,j}(+1)$.
2. Оцінка загального рівня спотворень статистичних параметрів ЗК при вбудовуванні стегоданих **M** проводиться з використанням принципу суперпозиції. Відповідно, значення функції $D(\mathbf{X}, \mathbf{Y})$ у виразі (1.2) може бути представлено, як сума спотворень, що відповідають прихованню окремих стегобіт.
3. Статистичні та спектральні параметри власних шумів ЗК, обумовлені фізичними процесами на етапі формування зображення, не залежать від просторового положення пікселю, що використовується для приховання бітів повідомлення. Це дозволяє провести оцінку параметрів даних шумів за результатами аналізу розподілу значень яскравості пікселів ЗК в заданому околі поточного пікселя (i, j) .

Використання наведених припущень при розробці АСМ дозволяє забезпечити високу точність оцінки змін параметрів ЗК при формуванні стеганограм, та не потребує використання обчислювально складних методів статистичного аналізу розподілів значень яскравості пікселів зображення-контейнеру. В якості прикладів АСМ, заснованих на врахуванні змін статистичних параметрів окремих складових ЗК при вбудовуванні стегоданих, можливо навести методи HUGO [147], S-UNIWARD [135], MG [152] та Mi-POD [153]. Ці методи дозволяють забезпечити високий ступінь заповнення ЗК стегоданими ($\Delta_{\alpha}^S > 20\%$) при збереженні малого рівня спотворень зображення-контейнеру. Розглянемо особливості формуванні стеганограм згідно даних методів більш детально.

Формування стеганограм згідно методу HUGO проводиться шляхом мінімізації середнього рівня спотворень статистичних параметрів ЗК на вибірці тестових ЦЗ за умови фіксованого розміру стегоданих $|\mathbf{M}| = H(\pi)$ [147]:

$$\min_{\pi} E_{\pi}[D] = \sum_{\mathbf{Y} \in \Upsilon} \pi(\mathbf{Y}) \cdot D(\mathbf{X}, \mathbf{Y}), \quad (1.3)$$

де $y \in \Upsilon$ – поточна стеганограма \mathbf{Y} з множини можливих стеганограм Υ ; π – функція розподілу імовірності вибору заданої стеганограми \mathbf{Y} з множини Υ ; $E_{\pi}[D]$ – оператор усереднення значень функції $D(\mathbf{X}, \mathbf{Y})$ при використанні розподілу π ; $H(\pi) = -\sum_{\mathbf{Y} \in \Upsilon} \pi(\mathbf{Y}) \cdot \log(\pi(\mathbf{Y}))$ – функція визначення інформаційної ентропії розподілу π .

В роботі [147] показано, що використання розподілу Гіббса для вибору стеганограм \mathbf{Y} з множини Υ дозволяє мінімізувати значення оператора $E_{\pi}[D]$ у виразі (1.3) для довільного ЗК:

$$\pi_{\lambda_G}(\mathbf{Y}) = \frac{\exp(-\lambda_G D(\mathbf{Y}))}{\sum_{\mathbf{y} \in \Upsilon} \exp(-\lambda_G D(\mathbf{y}))}, \quad (1.4)$$

де $\lambda_G > 0$ – масштабуючий скаляр. При використанні припущення щодо незалежності змін статистичних параметрів ЗК, обумовлених прихованням окремих стегобітів, значення $\pi_{\lambda_G}(\mathbf{Y})$ у виразі (1.4) може бути представлено як добуток відповідних значень $\pi_{\lambda_G}(\mathbf{Y}_i)$ для кожної стеганограми \mathbf{Y}_i з множини можливих стеганограм Υ :

$$\pi_{\lambda_G}(\mathbf{Y}) = \prod_i \pi_{\lambda_G}(\mathbf{Y}_i) = \frac{\prod_i \exp(-\lambda_G \rho_i(\mathbf{Y}_i))}{\sum_{j \in \mathcal{J}} \exp(-\lambda_G \rho_j(\mathbf{Y}_j))},$$

де $\mathcal{J} = \{0, 1, \dots, 2^k - 1\}$ – діапазон значень яскравості пікселів ЗК з глибиною кольору k (біт).

Для оцінки спотворень ЗК при вбудовуванні окремого стегобіту T . Філлером запропоновано застосовувати математичний апарат статистичної фізики, а саме функцію локального потенціалу $V_C(\mathbf{X}_{ij})$ [147]. Значення потенціалу $V_C(\mathbf{X}_{ij})$ відповідає ступеню кореляції значень яскравості суміжних пікселів в околі C поточного пікселю ЗК з координатами (i, j) [147]. Це дозволяє

використовувати $V_C(\mathbf{X}_{ij})$ в якості функції $\rho_{i,j}(\cdot)$ у виразі (1.2) для оцінки змін статистичних характеристик ЗК при вбудовуванні окремого стегобіту. При цьому можливе використання матрицю суміжності $\mathbf{C}_{k,l}(\mathbf{X})$ для чисельної оцінки значень функції $V_C(\mathbf{X}_{ij})$ [147]:

$$\mathbf{C}_{k,l}(\mathbf{X}) = \sum_{i,j} [x_{i,j} = k]_I \cdot [x_{i+\Delta_i, j+\Delta_j} = l]_I, \quad (1.5)$$

де $x_{i,j}$ – значення яскравості пікселю ЗК з координатами (i, j) ; $[a]_I$ – нотація (дужка) Айверсона, що рівна одиниці якщо булевий вираз a є істинним, та нулю в протилежному випадку; $\Delta_i, \Delta_j \in \{-1, 0, +1\}$ – величина зсуву між положенням поточного та наступного пікселів ЗК.

Розглянемо приклад обчислення матриці суміжності $\mathbf{C}_{k,l}(\mathbf{X})$ (1.5) при обробці ЗК по рядкам та скануванні пікселів зліва-направо. В даному випадку елементи матриці $\mathbf{C}_{k,l}(\mathbf{X})$ можуть бути обчислені наступним чином [147]:

$$\mathbf{C}_{k,l}^{\rightarrow}(\mathbf{X}) = \frac{1}{N \cdot (M - 2)} \cdot \sum_{i,j} [(\mathbf{D}_{i,j}^{\rightarrow}, \mathbf{D}_{i,j+1}^{\rightarrow})(\mathbf{X}) = (k, l)]_I,$$

$$(\mathbf{D}_{i,j}^{\rightarrow}, \mathbf{D}_{i,j+1}^{\rightarrow})(\mathbf{X}) = (k, l) \Leftrightarrow \mathbf{D}_{i,j}^{\rightarrow}(\mathbf{X}) = k \wedge \mathbf{D}_{i,j+1}^{\rightarrow}(\mathbf{X}) = l,$$

де $\mathbf{D}_{i,j}^{\rightarrow}(\mathbf{X}) = (\mathbf{X}_{i,j+1} - \mathbf{X}_{i,j})$ – матриця різниць значень яскравості суміжних пікселів зображення. При формуванні стеганограми значення яскравості пікселів ЗК змінюється на величину (± 1) в залежності від значень стегобіт. Відповідно, для оцінки ступеня кореляції значень яскравості суміжних пікселів ЗК та сформованої стеганограми використовується нормалізована матриця суміжності яскравості пікселів $\mathbf{H}_{(k,l)}^{\rightarrow}$ [147]:

$$\mathbf{H}_{(k,l)}^{\rightarrow}(\mathbf{X}, \mathbf{Y}) = \frac{1}{N \cdot (M - 2)} \cdot \sum_{i,j} |(\mathbf{D}_{i,j}^{\rightarrow}, \mathbf{D}_{i,j+1}^{\rightarrow})(\mathbf{Y}) = (k, l) - (\mathbf{D}_{i,j}^{\rightarrow}, \mathbf{D}_{i,j+1}^{\rightarrow})(\mathbf{X}) = (k, l)|, \quad (1.6)$$

для кожного типу околу поточного пікселю

$$\mathcal{C}^{\rightarrow} = \{c: c = \{(i, j), (i, j + 1), (i, j + 2)\}\}.$$

Тоді оцінка загального спотворення ЗК при вбудовуванні стегоданих згідно методу HUGO може бути обчислена згідно наступного виразу [147]:

$$D(\mathbf{Y}) = \sum_{c \in \mathcal{C}} \sum_{(k,l) \in \mathcal{J}} \omega_{k,l} \mathbf{H}_{(k,l)}^c(\mathbf{Y}), \mathcal{J} = \{0,1, \dots, 255\},$$

де $\mathcal{C} = \mathcal{C}^{\rightarrow} \cup \mathcal{C}^{\leftarrow} \cup \mathcal{C}^{\uparrow} \cup \mathcal{C}^{\downarrow}$ – множина трьох-елементних послідовностей пікселів $(x_{i-\Delta_i, j-\Delta_j}; x_{i,j}; x_{i+\Delta_i, j+\Delta_j})$, $\Delta_i, \Delta_j \in \{-1, +1\}$, суміжних з поточним пікселем ЗК, що має координати (i, j) ; $\omega_{k,l} > 0$ – ваговий коефіцієнт; $\mathbf{H}_{(k,l)}^c$ – нормалізована матриця суміжності яскравості пікселів ЦЗ, що обчислюється для кожного типу околу \mathcal{C} поточного пікселю згідно виразу (1.6).

Використання математичного апарату локальних потенціалів $V_c(\mathbf{X}_{ij})$ при формуванні стеганограм згідно стеганографічному методу HUGO дозволяє суттєво зменшити рівень демаскуючих ознак сформованих стеганограм у порівнянні з поширеними типами СМ [147]. Відмітимо, що оцінка значень $V_c(\mathbf{X}_{ij})$ проводиться з використанням матриць суміжностей $\mathbf{H}_{(k,l)}^c$ (1.6) лише для малого околу поточного пікселю (в межах ковзного вікна розміром 3×3 пікселів) [147]. Внаслідок цього даний СМ не враховує зміни статистичних параметрів ЗК на більших масштабах аналізу, що потребувало б використання обчислювально складних методів статистичного аналізу, зокрема математичного апарату марківських випадкових полів (МВП).

На відміну від стеганографічного методу HUGO, оцінка спотворень параметрів ЗК, обумовлених прихованням повідомлень, для методу S-UNI-WARD проводиться з використанням спектральних перетворень ЗК, а саме ДДВП. При цьому значення функції $D(\mathbf{X}, \mathbf{Y})$ для даного СМ розраховується згідно наступного виразу [135]:

$$D(\mathbf{X}, \mathbf{Y}) = \sum_{k \in \{H, V, D\}} \sum_{u, v} \frac{|\mathbf{W}_{uv}^k(\mathbf{X}) - \mathbf{W}_{uv}^k(\mathbf{Y})|}{\sigma_{UNI} + |\mathbf{W}_{uv}^k(\mathbf{X})|}, \quad (1.7)$$

де $\mathbf{W}_{uv}^k(\mathbf{X})$, $\mathbf{W}_{uv}^k(\mathbf{Y})$ – відповідно, коефіцієнти ДДВП зображення-контейнеру та стеганограми з просторовими координатами (u, v) ; $k \in \{H, V, D\}$ – тип коефіцієнтів ДДВП досліджуваних зображень (горизонтальні, вертикальні та

діагональні деталізуючі коефіцієнти); $\sigma_{UNI} > 0$ – константа для стабілізації обчислень $D(\mathbf{X}, \mathbf{Y})$ при малих значеннях коефіцієнтів ДДВП зображення-контейнеру ($|\mathbf{W}_{uv}^k(\mathbf{X})| \rightarrow 0$).

Вибір базисних функцій ДДВП у виразі (1.7) дозволяє гнучко підходити до виявлення специфічних спотворень ЗК, обумовлених прихованням повідомлень. З іншого боку, визначення оптимальних базисних функцій ДДВП за критерієм мінімізації помилки виявлення стеганограм, сформованих згідно методу S-UNIWARD, є нетривіальною задачею, зважаючи на значну варіативність статистичних та спектральних параметрів реальних ЦЗ. Внаслідок цього в якості базису перетворення ЦЗ у виразі (1.7) використовуються поширені типи вейвлетів та відповідних їм скейлінг-функцій, зокрема вейвлети Добеші [135]. Це призводить до появи характерних спотворень спектральних параметрів стеганограм, обумовлених впливом спектру використаних вейвлет-функцій на вейвлет-спектр ЗК, що використовується для підвищення точності роботи СД.

Відмітимо, що розглянуті стеганографічні методи HUGO та S-UNIWARD засновані на використанні емпіричних функцій $D(\mathbf{X}, \mathbf{Y})$ (1.2) для оцінки спотворень параметрів ЗК при вбудовуванні повідомлення. Це дозволяє суттєво зменшити рівень демаскуючих ознак тестових ЦЗ зі стандартних пакетів зображень, зокрема BOSS [27] та ALASKA [134], що характеризуються відносно низьким рівнем власних шумів. Внаслідок цього рівень демаскуючих ознак стеганограм, сформованих згідно розглянутих СМ, може суттєво змінюватися у випадку обробки реальних ЦЗ, що характеризуються значною варіативністю статистичних та спектральних параметрів.

Одним з сучасних підходів до забезпечення високої стійкості стеганограм, сформованих з використанням реальних ЦЗ, є використання спеціальних статистичних моделей власних шумів зображення-контейнеру [9]. Зокрема, авторами стеганографічних методів MG та MiPOD запропоновано використовувати моделі суміші завад, що мають нормальний (гаусовий) розподіл

(англ. multivariate Gaussian, MVG), для моделювання шумових складових ЗК [152,153]. Це дозволяє враховувати зміни статистичних параметрів ЗК при формуванні стеганограм з метою вибору оптимальних методів попередньої обробки стегоданих \mathbf{M} за критерієм мінімізації рівня демаскуючих ознак сформованих стеганограм.

Формування стеганограм згідно методів MG та MiPOD проводиться в декілька етапів [152,153]. На першому етапі проводиться оцінка шумових складових \mathbf{r} зображення-контейнеру \mathbf{X} з використанням знешумлюючого фільтру $F_{dn}(\cdot)$:

$$\mathbf{r} = \mathbf{X} - F_{dn}(\mathbf{X}). \quad (1.8)$$

Згідно рекомендацій [152,153], в якості фільтру $F_{dn}(\cdot)$ використовуються ФВЧ. Це дозволяє виокремити високочастотні складові ЗК на рівні котрих, зазвичай, проводиться приховання повідомлень.

На другому етапі проводиться оцінка статистичних параметрів обчислених складових \mathbf{r} (1.8) з використанням моделі MVG для кожного положення ковзного вікна (КВ) розміром $w_{p \times p}$ (пікселів) [152,153]. Модель MVG заснована на представленні досліджуваного сигналу як суміші декількох шумів, що мають гаусовий (нормальний) розподіл:

$$\mathbf{r}_l = \mathbf{G}\mathbf{a}_l + \boldsymbol{\xi}, l \in [1; M \cdot N], \quad (1.9)$$

де \mathbf{r}_l – шумові складові для поточного положення ковзного вікна; l – індекс елемента, розташованого в центрі ковзного вікна; $\mathbf{G}_{p^2 \times p}$ – матриця змішування складових, що використовуються для моделювання \mathbf{r}_l ; $\mathbf{a}_{p \times 1}$ – вектор елементів складових змішування; $\boldsymbol{\xi}_{p^2 \times 1}$ – шуканий сигнал, що відповідає шумовим компонентам ЗК. Значення елементів матриці $\mathbf{G}_{p^2 \times p}$ визначаються за результатами налаштування моделі MVG, а саме мінімізації помилки апроксимації значень \mathbf{r}_l (1.9) для поточного положення КВ.

На третьому етапі проводиться попередня обробка (кодування) повідомлення \mathbf{M} з використанням трелліс-кодів [152,153]. Дані методи кодування потребують використання апріорної інформації щодо ваги (впливу зміни

яскравості на відповідні спотворення статистичних параметрів ЦЗ) кожного пікселю ЗК для вибору підмножини пікселів для приховання повідомлення [152,153]:

$$\rho_l = -\ln(\beta_l - 2).$$

де ρ_l – значення ваги l –того елементу \mathbf{r}_l для поточного положення ковзного вікна; β_l – імовірність зміни яскравості l –того пікселю при вбудовуванні окремого стегобіту. Значення β_l визначається шляхом вирішення оптимізаційної задачі мінімізації коефіцієнту розбіжності ζ^2 між розподілами значень яскравості пікселів ЗК та стеганограми [152,153]:

$$\zeta^2(\beta_l) = 2 \cdot \sum_{l=1}^{M \cdot N} \beta_l^2 \sigma_l^{-4} \xrightarrow{H_4(\beta_l)=const} \min, \quad (1.10)$$

$$H_4(z) = (-2)z \log(z) - (1 - 2z) \log(1 - 2z),$$

де $H_4(z)$ – функція оцінки тернарної ентропії імовірнісного розподілу; σ_l^2 – дисперсія значень елементів \mathbf{r}_l для поточного положення ковзного вікна.

Для вирішення оптимізаційної задачі (1.10) застосовується метод множників Лагранжа [152,153]. Згідно даного методу, шукане значення β_l та множників Лагранжу λ_L визначається з використанням чисельних методів при вирішенні наступної системи рівнянь:

$$\begin{cases} \beta_1^2 \sigma_1^{-4} = \frac{1}{2\lambda_L} \ln\left(\frac{1 - 2\beta_1}{\beta_1}\right), \\ \dots, \\ \beta_{M \cdot N}^2 \sigma_{M \cdot N}^{-4} = \frac{1}{2\lambda_L} \ln\left(\frac{1 - 2\beta_{M \cdot N}}{\beta_{M \cdot N}}\right). \end{cases}$$

Відмінність між стеганографічними методами MG та MiPOD полягає у підході до оцінки значення параметру σ_l^2 у виразі (1.10). Для методу MiPOD визначення значення σ_l^2 проводиться з використанням методу максимальної правдоподібності (англ. Maximum Likelihood Estimation, MLE) [152,153]:

$$\sigma_l^2 = \frac{\|\mathbf{P}_G^\perp \mathbf{r}_l\|}{p^2 - q}, \quad (1.11)$$

$$\mathbf{P}_G^\perp = \mathbf{I}_l - \mathbf{G}(\mathbf{G}^T \mathbf{G})^{-1} \mathbf{G}^T,$$

де \mathbf{P}_G^\perp – матриця ортогональної проєкції \mathbf{r}_l у виразі (1.9) на $(p^2 - q)$, $q \in \mathbb{N}$, вимірний простір, сформований лівими власними векторами матриці \mathbf{G} . Використання виразу (1.11) дозволяє забезпечити високу точність оцінки параметру σ_l^2 та, відповідно, мінімізацію змін статистичних параметрів ЗК за рахунок суттєвого зростання обчислювальної складності процедури приховання повідомлень. Для методу MG використовується спрощена оцінка параметру σ_l^2 у рівнянні (1.9), що дозволяє зменшити обчислювальну складність процедури приховання повідомлень до ЗК [152,153]:

$$\sigma_l^2 = \frac{\|\mathbf{r}_l - \tilde{\mathbf{r}}_l\|}{p^2 - q},$$

$$\tilde{\mathbf{r}}_l = \mathbf{G}(\mathbf{G}^T \mathbf{G})^{-1} \mathbf{G}^T \mathbf{r}_l.$$

Вагомою перевагою застосування моделі MVG в задачах стеганографії ЦЗ є висока точність оцінки статистичних параметрів шумів ЗК. Це дозволяє використовувати зміни параметрів моделі MVG, обумовлені прихованням повідомлень до ЗК, для оцінки рівня демаскуючих ознак (спотворень статистичних параметрів ЗК) сформованих стеганограм [152,153]. З іншого боку, використання суміші лише гаусових шумів в моделі MVG призводить до зниження точності моделювання нестационарних шумів, зокрема локальних збурень яскравості пікселів ЗК [144]. Відповідно, становить інтерес використання спеціалізованих методів обробки ЦЗ для виокремлення та аналізу нестационарних шумів досліджуваного зображення, що дозволить підвищити рівень демаскуючих ознак стеганограм у порівнянні з методами MG та Mi-POD при проведенні стегоаналізу ЦЗ.

1.2.4 Стеганографічні методи, засновані на аналізі статистичних та спектральних параметрів зображення-контейнеру

Особливістю новітніх АСМ є використання статистичних, спектральних та структурних параметрів для зображення-контейнеру, представленому у форматі стиснення без втрат, наприклад PGM, TIFF тощо. Відповідно ефективність даних стеганографічних методів може суттєво змінюватися у випад-

ку обробки ЦЗ, представлених у форматах стиснення зі втратами, наприклад JPEG, JPEG-2000 [31]. Також АСМ спрямовані на приховання кожного стегобіту без врахування взаємного впливу змін значень яскравості суміжних пікселів ЗК на відповідні зміни статистичних параметрів зображення-контейнеру. Це призводить до явища посилення рівня демаскуючих ознак, що зменшує робастність сформованих стеганограм до методів стегоаналізу ЦЗ.

Для додаткового зниження рівня демаскуючих ознак стеганограм, сформованих згідно АСМ, були запропоновані спеціальні типи стеганографічних методів, а саме [31]:

- Методи на основі аналізу статистичних та спектральних характеристик вихідного виду контейнеру (англ. side-informed methods, SIM) – засновані на використанні даних щодо змін характеристик ЗК при використанні поширених методів обробки, зокрема фільтрації, стиснення з втратами та підвищення візуальної якості. Врахування даної інформації дозволяє додатково підвищити робастність стеганограм до методів стегоаналізу за рахунок вибору пікселів ЗК, значення яскравості котрих несуттєво змінюються при обробці зображення;
- Методи з синхронізацією змін яскравості пікселів (англ. methods with synchronized embedding changes, SEC) – приховання повідомлень проводиться за умови синхронізації змін значень яскравості суміжних пікселів ЗК, що дозволяє додатково зменшити спотворення контейнеру.

Прикладом SIM-методів є стеганографічний метод Synch [132]. Особливістю даного методу є врахування відмінностей $\Delta x_{i,j}$ між значеннями яскравості пікселів зображення-контейнеру \tilde{X} , отриманого після застосування поширених методів обробки ЦЗ, та сформованої стеганограми Y . Значення $\Delta x_{i,j}$ для даного методу змінюються у діапазоні $\Delta x_{i,j} \in \{-1; 0; +1\}$, що призводить до порушення припущення щодо рівності імовірностей приховання

окремих стегобітів. Тому для оцінки спотворень статистичних параметрів ЗК при вбудовуванні стегоданих \mathbf{M} в методі Synch використовується наступна апроксимація функції $D(\mathbf{X}, \mathbf{Y})$ у виразі (1.2) [132]:

$$\tilde{D}(\mathbf{X}, \mathbf{Y}) = \sum_{(x_{i,j}-y_{i,j}) \neq (\tilde{x}_{i,j}-y_{i,j})} D(\mathbf{X}, \mathbf{Y}_{\sim ij}), \quad (1.12)$$

де $x_{i,j}$, $\tilde{x}_{i,j}$ та $y_{i,j}$ відповідають значенням яскравості пікселя з координатами (i, j) для вихідного \mathbf{X} та обробленого $\tilde{\mathbf{X}}$ зображення-контейнеру, а також відповідної стеганограми \mathbf{Y} ; $\mathbf{Y}_{\sim ij}$ відповідає стеганограмі, що сформована шляхом зміни яскравості лише одного пікселя ЗК з координатами (i, j) . Приховання повідомлень згідно методу Synch потребує використання спеціальних методів кодування стегоданих \mathbf{M} , а саме багаторівневих трелліс-кодів [156], аналогічно до стеганографічних методів MG [152] та MiPOD [153].

Використання SIM-методів дозволяє додатково підвищити стійкість сформованих стеганограм до спотворень, обумовлених використанням поширених методів обробки ЦЗ, при збереженні низького рівня демаскуючих ознак прихованих повідомлень [156]. Проте практичне застосування даних методів є обмеженим внаслідок високої обчислювальної складності мінімізації функції $\tilde{D}(\mathbf{X}, \mathbf{Y})$ (1.12) та необхідності використання вихідних (необроблених) ЗК, що не завжди є можливим. Внаслідок цього особлива увага розробників АСМ приділяється методам, заснованим на синхронізації змін яскравості пікселів ЗК, що розглянуті у наступному розділі.

1.2.5 Стеганографічні методи, засновані на синхронізації змін значень яскравості пікселів зображення-контейнеру

Методи на основі синхронізації змін яскравості пікселів ЗК є частковим випадком більш загального класу методів групування змін, внесених до ЗК при вбудовуванні повідомлення (англ. Clustering Modification Direction steganography) [157]. Особливістю SEC-методів є використання явища синхронізації змін ЗК в процесі формування стеганограм – формування груп пікселів

ЗК, значення яскравості котрих можуть бути змінені на однакову величину v ($v \neq 0$) при забезпеченні фіксованих (малих) змін статистичних параметрів зображення-контейнеру. При цьому вбудовування окремих бітів повідомлення проводиться з використанням поширених АСМ, наприклад методів HUGO [147], S-UNIWARD [135], MG [152], тощо.

Приховання стегоданих згідно SEC-методів, зазвичай, проводиться в декілька етапів. В якості прикладу розглянемо випадок аналізу пікселів ЗК, що є суміжними по горизонталі та вертикалі. На першому етапі приховання стегоданих проводиться формування груп пікселів $\mathcal{L}_i, i \in [1; 4]$, що є суміжними по вертикалі/горизонталі до поточного пікселю з координатами (i, j) , згідно наступних правил [31]:

$$\mathcal{L}_1 = \{(i, j) | \text{mod}(i, 2) = 1 \wedge \text{mod}(j, 2) = 1\}, \quad (1.13)$$

$$\mathcal{L}_2 = \{(i, j) | \text{mod}(i, 2) = 1 \wedge \text{mod}(j, 2) = 0\}, \quad (1.14)$$

$$\mathcal{L}_3 = \{(i, j) | \text{mod}(i, 2) = 0 \wedge \text{mod}(j, 2) = 0\}, \quad (1.15)$$

$$\mathcal{L}_4 = \{(i, j) | \text{mod}(i, 2) = 0 \wedge \text{mod}(j, 2) = 1\}, \quad (1.16)$$

де $\text{mod}(a, b)$ – операція отримання залишку від ділення числа a ($a \in \mathbb{N}$) на число b ($b \in \mathbb{N}$).

На другому етапі, повідомлення \mathbf{M} розбивається на чотири частини $\mathbf{M} = \{\mathbf{M}_m : m \in [1; 4]\}$. Вбудовування кожної частини \mathbf{M}_m проводиться шляхом модифікації значень яскравості відповідної групи пікселів \mathcal{L}_m (1.13)-(1.16) з використанням попередньо обраного АСМ. Для зниження спотворень статистичних параметрів ЗК при формуванні стеганограм, вбудовування стегобіту до пікселю з координатами (i, j) для поточної групи \mathbf{M}_m відбувається з врахуванням змін значень яскравості суміжних пікселів, що належать до інших груп $\mathbf{M}_k, k \in [1; 4] \setminus \{m\}$. Це призводить до появи явища синхронізації змін – додаткового зниження змін статистичних характеристик ЗК $\rho_{i,j}$ в q ($q > 0$) разів. Відмітимо, що значення параметру q визначається емпіричним чином – шляхом порівняння значень функції $D(\mathbf{X}, \mathbf{Y})$ при використанні «синхронізованих» змін та випадку застосування лише АСМ. За результата-

ми експериментальних досліджень в роботі [157] встановлено, що значення параметру q для SEC-методів може сягати дев'яти при використанні поширених типів АСМ для приховання окремих бітів повідомлення \mathbf{M} .

Використання явища синхронізації змін для SEC-методів дозволяє суттєво знизити відмінності між значеннями яскравості суміжних пікселів стеганограм у порівнянні з поширеними СМ. Це призводить до відповідного зниження точності роботи методів кореляційного та статистичного стегоаналізу ЦЗ [157]. Проте обмеженням практичного використання даного підходу є висока обчислювальна складність – необхідність повного перебору всіх можливих комбінацій змін яскравості пікселів в кожній групі \mathcal{L}_m для отримання явища синхронізації змін. Тому на практиці використовуються лише евристичні методи зниження обчислювальної складності даного підходу для окремих (часткових) випадків.

Висока складність виявлення стеганограм, сформованих згідно АСМ, зокрема у випадку обмеженості апріорних даних щодо особливостей даних методів, обумовлює актуальність та важливості науково-прикладної проблеми побудови високоточних СД. Визначення шляхів вирішення даної проблеми потребує огляду відомих методів стеганографії ЦЗ, зокрема дослідження особливостей даних методів, що негативно впливають на точність роботи стегодетекторів.

1.3 Огляд сучасних методів стегоаналізу цифрових зображень

Сучасний підхід до побудови СД для виявлення повідомлень, вбудованих до ЦЗ, заснований на дослідженні відмінностей між статистичними, спектральними та структурними параметрами зображень з відповідними (очікуваними) характеристиками ЗК, або ж стеганограм [9-11,13]. Для забезпечення високої точності оцінки даних параметрів запропоновано значну кількість методів моделювання ЦЗ, зокрема заснованих на використанні статистичних моделей ЗК та згорткових нейронних мереж (ЗНМ). Основні етапи

обробки досліджуваних зображень при використанні даних методів наведені на рис. 1.2.



Рисунок 1.2 – Основні етапи обробки цифрових зображень в сучасних стегодетекторах, заснованих на використанні статистичних моделей ЦЗ (а) та згорткових нейронних мереж (б).

Обробка досліджуваних ЦЗ з використанням відомих СД проводиться в декілька етапів (рис. 1.2) [158]. На першому етапі, до досліджуваних ЦЗ застосовуються методи попередньої обробки (МПО) для виокремлення слабких змін параметрів ЗК, обумовлених прихованням повідомлень [159] (рис. 1.2). В якості даних методів широко використовуються ансамблі ФВЧ [34], що дозволяють виділяти шумові складові ЗК на рівні котрих, зазвичай, відбувається приховання повідомлень.

На другому етапі проводиться оцінка параметрів виділених складових ЦЗ з використанням методів статистичного [34] [159], спектрального та структурного аналізів [146,160-163] (рис. 1.2). На останньому етапі відбувається віднесення досліджуваного зображення до класів ЗК або ж стеганограм за результатами обробки обчислених параметрів ЦЗ із застосуванням методів теорії розпізнавання образів (рис. 1.2).

На відміну від випадку використання статистичних моделей ЦЗ при обробці зображень (рис. 1.2а), застосування ЗНМ дозволяє об'єднати наведені

етапи обробки ЦЗ (рис. 1.2б) [164,165]. Це досягається за рахунок об'єднання в структурі ЗНМ шарів штучних нейронів для виокремлення шумових складових ЦЗ та подальшої обробки отриманих складових з метою оцінки їх статистичних характеристик [166]. При цьому класифікація досліджуваних зображень проводиться за результатами обробки отриманих характеристик в останніх шарах ЗНМ. Застосування методу зворотнього розповсюдження помилок [46,47] при налаштуванні СД на основі ЗНМ дає можливість суттєво прискорити процедуру налаштування параметрів ФВЧ у вхідних (згорткових) шарах мережі при збереженні фіксованої точності виявлення стеганограм.

Для дослідження переваг та обмежень розглянутих підходів до побудови СД (рис. 1.2), проведемо порівняльний аналіз відомих стегодетекторів, заснованих на даних підходах.

1.3.1 Стегодетектори на основі спеціальних методів попередньої обробки досліджуваних зображень

Одним з найбільш поширених підходів до побудови стегодетекторів є використання методів попередньої обробки ЦЗ, спрямованих на посилення відмінностей ЗК та стеганограмами [9-11]. В якості даних методів, зазвичай, використовується фільтрація оброблюваних зображень для вилучення високочастотних складових, зокрема власних шумів ЦЗ, на рівні котрих проводиться приховання повідомень. Проте вибір оптимальних типів ФВЧ для обробки зображення за критерієм максимізації відношення стегодані/контейнер наразі є невирішеною задачею, для котрої запропоновано рішення лише для часткових випадків [78].

Для подолання даного обмеження в роботі запропоновано метод посилення відмінностей між ЗК та стеганограмами, що заснований на аналізі взаємного положення векторів, які відповідають статистичним параметрам зображень-контейнерів та стеганограм, в просторі вищої розмірності [78]. Основні етапи обробки ЦЗ згідно запропонованого методу зображено на рис. 1.3.

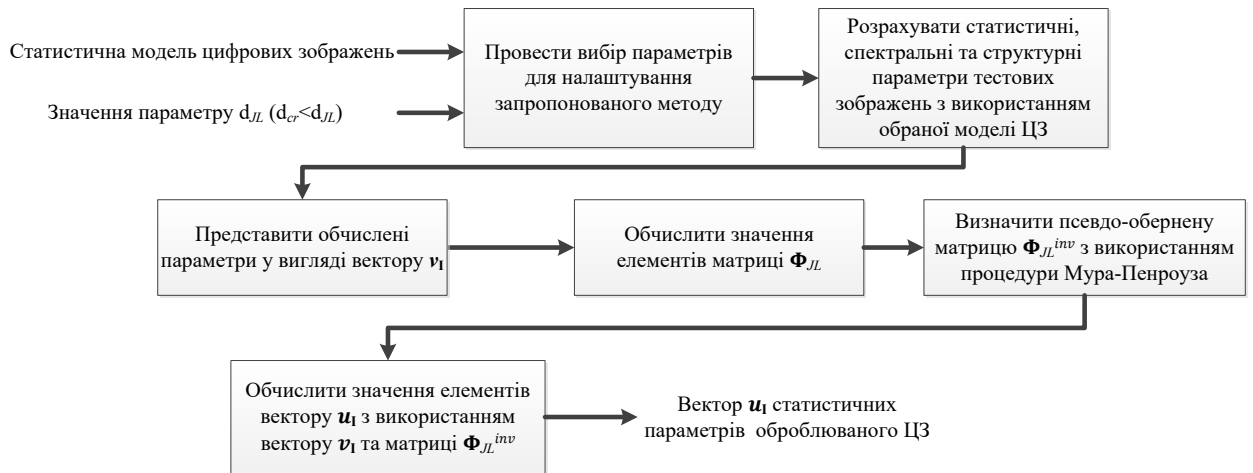


Рисунок 1.3 – Основні етапи обробки цифрових зображень згідно запропонованого методу відмінностей між ЗК та стеганограмами.

Визначення положення векторів, що відповідають статистичним параметрам оброблюваних ЦЗ, проводиться в декілька етапів (рис. 1.3). На першому етапі використовується процедура проєкції багатовимірних векторів до простору меншої розмірності згідно теореми Джонсона-Лінденштрауса [167]. Особливістю даної процедури є збереження взаємного положення багатовимірних векторів (статистичних параметрів досліджуваних ЦЗ) при проєкції до простору меншої розмірності. Відповідно, використання зворотної процедури (визначення векторів-прообразів для заданих груп векторів) дозволить досліджувати відстані між групами (кластерами) векторів-прообразів без необхідності додаткового аналізу ступеня перекриття кластерів векторів, що відповідають зображенням-контейнерам (\mathcal{X}) та стеганограмам (\mathcal{Y}).

В роботі досліджено випадок застосування зворотного перетворення Джонсона-Лінденштрауса (ЗПДЛ) для визначення прообразів векторів (статистичних параметрів ЦЗ) в просторі вищої розмірності. Дане перетворення засновано на використанні матриці трансформації Φ_{JL} [168,169]:

$$\Phi_{JL} = \mathbf{P}_{JL} \times \mathbf{H}_{JL} \times \mathbf{D}_{JL}, \quad (1.17)$$

$$\mathbf{P}_{JL}(i, j) = \begin{cases} \mathcal{N}(0, q^{-1}), & p = q, \\ 0, & p = 1 - q, \end{cases}$$

$$\mathbf{H}_{JL}(i, j) = d^{-1/2} \cdot (-1)^{\langle i-1, j-1 \rangle},$$

де $\mathbf{P}_{\text{JL}} \in \mathbb{R}^{k \times d}$ – стохастична матриця, елементи якої обираються з гаусового (нормального) розподілу $\mathcal{N}(0, q^{-1})$ з імовірністю q та рівні нулю з імовірністю $(1 - q)$; $\mathbf{H}_{\text{JL}} \in \mathbb{R}^{d \times d}$ – нормалізована матриця Адамара; $\langle a, b \rangle_m$ – скалярний добуток m –елементних векторів, що відповідають бінарному представленню аргументів a та b ; $\mathbf{D}_{\text{JL}} \in \mathbb{R}^{d \times d}$ – діагональна матриця, елементи котрої обираються з послідовності $\{-1; +1\}$ з рівною імовірністю.

Використання матриці $\Phi_{\text{JL}} \in \mathbb{R}^{k \times d}$ (1.17) для проекції векторів з простору \mathbb{R}^k до простору \mathbb{R}^d , $k < d$, призводить до внесення змін до взаємного положення векторів, що не перевищують ε^2 [168,169]. Це дозволяє мінімізувати відмінності у взаємному положенні векторів, що відповідають статистичним параметрам ЦЗ, при їх проекції до простору меншої розмірності, що становить особливий інтерес в задачах стегоаналізу ЦЗ. Внаслідок цього застосування оберненої матриці Φ_{JL}^{-1} до заданих векторів дозволить визначити положення відповідних їм векторів у просторі вищої розмірності. Враховуючи, що існування зворотної матриці Φ_{JL}^{-1} не завжди є можливим через стохастичний характер процедури формування складових даної матриці згідно виразу (1.17), запропоновано використовувати процедуру Мура-Пенроуза визначення псевдо-оберненої матриці Φ_{JL}^{inv} [170].

В роботі проведено дослідження ефективності використання ЗПДЛ для оцінки просторового положення векторів, що відповідають параметрам статистичної моделі SPAM для ЗК та стеганограм, сформованих згідно стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153]. За результатами проведеного аналізу побудовано залежності значення помилки класифікації стеганограм P_E від ступеня заповнення ЗК стегоданими та розмірності векторів-прообразів d_{preim} при збільшенні розмірності векторів SPAM-ознак на 10% (рис. 1.4).

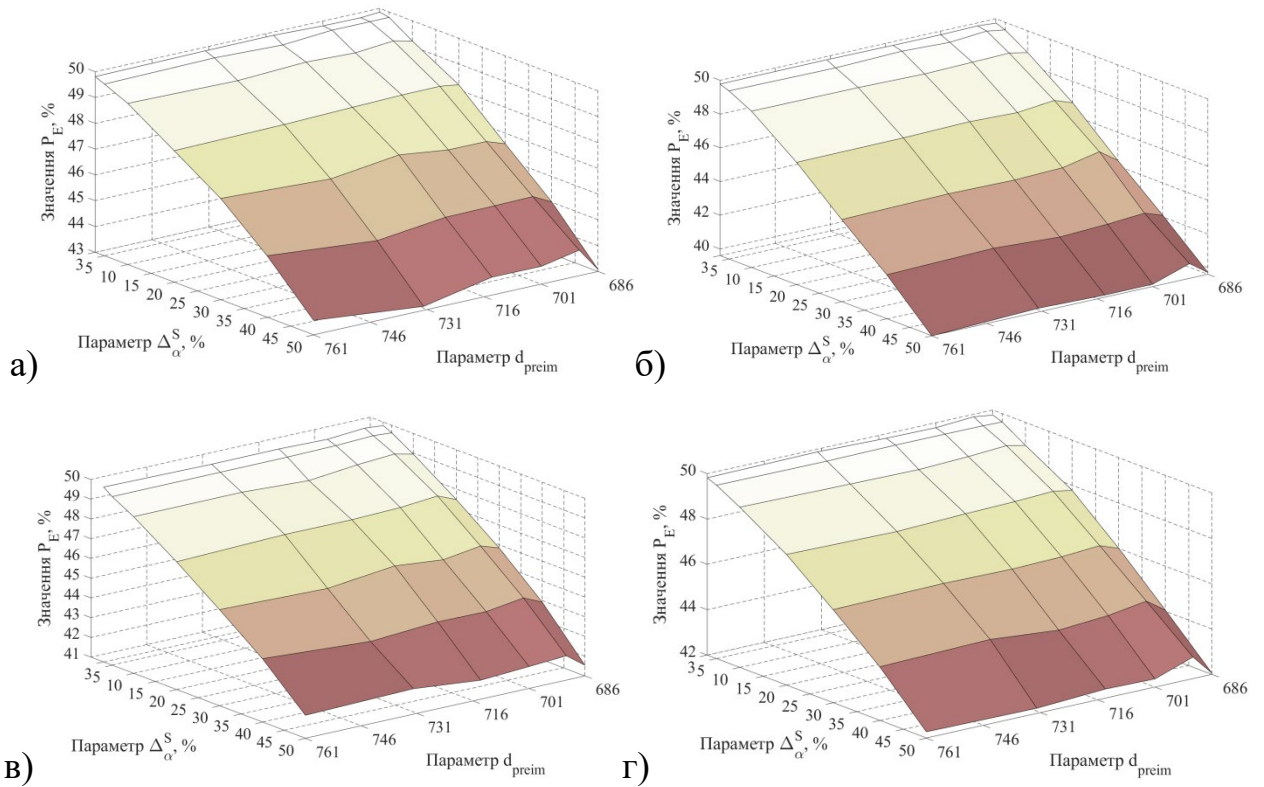


Рисунок 1.4 – Залежності значення помилки класифікації стегограм P_E від ступеня заповнення ЗК стегоданими та розмірності векторів-прообразів d_{preim} для пакету зображень ALASKA та стеганографічних методів:

(а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD.

Використання ЗПДЛ не дозволяє суттєво вплинути на точність виявлення стегограм, сформованих згідно розглянутих ACM (рис. 1.4) – зміни значень значення помилки P_E не перевищують 0.5%. Це може бути пояснено пропорційним збільшенням як відстаней між кластерами векторів, що відповідають ЗК та стегограмам, так і розмірів кластерів при використанні ЗПДЛ. Для перевірки даного припущення були розраховані значення стандартних показників Дунна C_{Dunn} [171] та Калінського-Харабаша C_{CH} [172], що використовуються для оцінки якості кластеризації векторів у багатовимірному просторі:

$$C_{Dunn} = \min_{1 \leq i < j \leq m} \delta(C_i, C_j) / \max_{1 \leq k \leq m} \Delta_k, \quad (1.18)$$

$$\Delta_i = \sum_{\mathbf{x} \in C_i} d(\mathbf{x}, \mu_{C_i}) / |C_i|, \mu_{C_i} = \sum_{\mathbf{x} \in C_i} \mathbf{x} / |C_i|, 1 \leq i < j \leq m,$$

$$C_{CH} = \sum_{i,j} \sigma_d^2(i,j) / \sum_i \sigma_d^2(i), 1 \leq i < j \leq m, \quad (1.19)$$

де $\delta(C_i, C_j)$ – відстань між центрами μ_C кластерів C_i та C_j ; Δ_k – середня відстань від елементів k –того кластеру до його центру μ_{C_k} ; $\sigma_d^2(i,j)$ – дисперсія значень відстаней від векторів i –того до центру j –того кластеру μ_{C_j} ; $\sigma_d^2(i)$ – дисперсія значень відстаней елементів i –того кластеру до його центру μ_{C_i} ; $m > 2$ – кількість кластерів.

За результатами обчислень показників C_{Dunn} (1.18) та C_{CH} (1.19) для розглянутих СМ (рис. 1.4) встановлено, що зміни показників C_{Dunn} і C_{CH} не перевищують 5%. Це підтверджує зроблений раніше висновок щодо пропорційного збільшення як відстаней між кластерами векторів, так і розмірів кластерів.

Для порівняння був також розглянутий випадок використання ЗПЛД у випадку обробки стеганограм, сформованих згідно апріорно невідомого СМ. Отримані залежності значення помилки класифікації стеганограм P_E від ступеня заповнення ЗК стегоданими та розмірності векторів-прообразів d_{preim} при збільшенні розмірності векторів SPAM-ознак на 10% наведені на рис. 1.5.

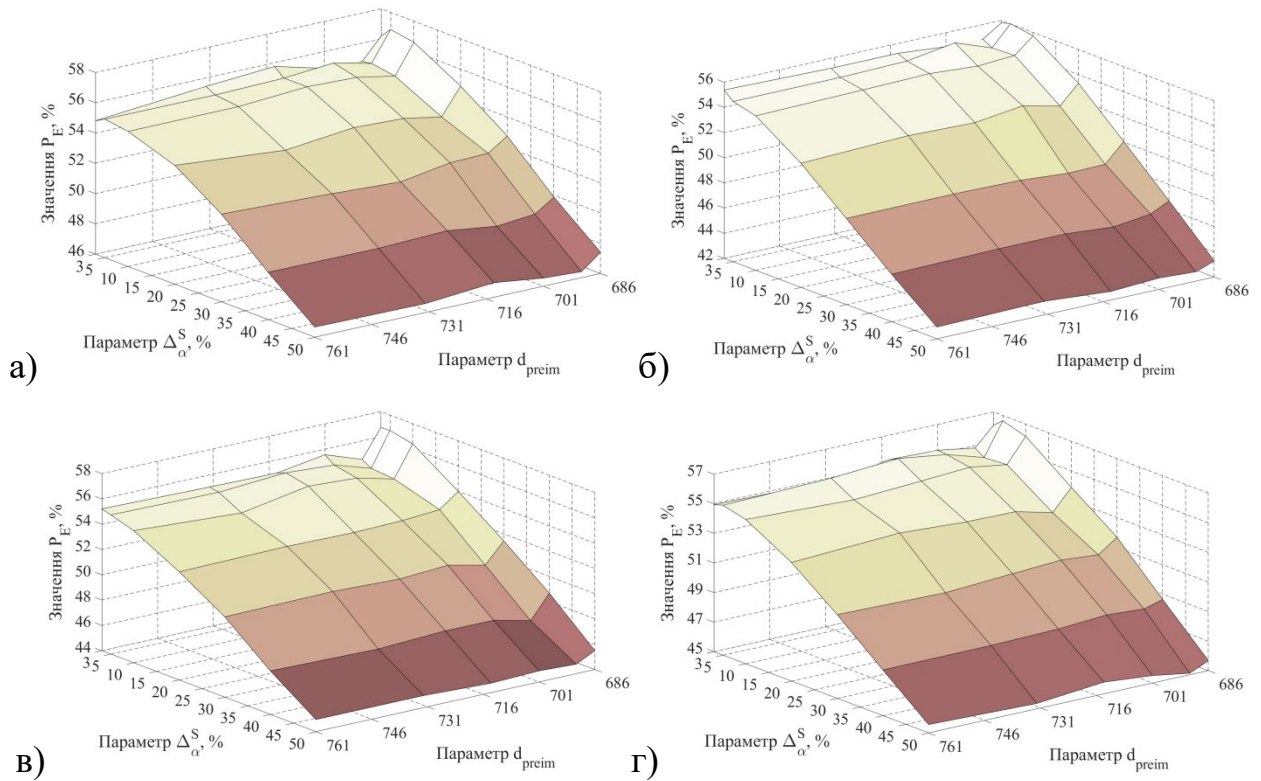


Рисунок 1.5 – Залежності значення помилки класифікації стеганограм P_E від ступеня заповнення ЗК стегоданими та розмірності векторів-прообразів d_{preim} для стегодетектору, налаштованого з використанням стеганографічного методу WOW, пакету зображень ALASKA та тестуванні на стеганографічних методах: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD.

Застосування ЗПДЛ дозволяє зменшити значення помилки класифікації стеганограм P_E до 2% у випадку обмеженості апріорних даних щодо використаного СМ (рис. 1.5). При цьому найбільше зменшення значень помилки класифікації стеганограм P_E досягається в області слабого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$) при несуттєвій зміні (на 0.5%) розмірності векторів у порівнянні з вихідними векторами SPAM-параметрів (рис. 1.4, $d_{SPAM} = 686$ та $d_{preim} = 691$). Подальше збільшення розмірності d_{preim} призводить до несуттєвих змін точності роботи СД ($\Delta P_E < 1\%$). Виявлений ефект зниження значень помилки P_E (рис. 1.5) може бути пояснений несуттєвим збільшенням відстані між векторами-прообразами для ЗК та стеганограм. При цьому зміни в розмірах відповідних кластерів не враховуються на етапі налаштування СД через відсутність пари ЗК та відповідної йому стеганограми.

За результатами аналізу отриманих даних встановлено, що використання методів посилення відмінностей між ЗК та стеганограмами при побудові СД, зокрема заснованих на застосуванні зворотного перетворення Джонсона-Лінденштрауса, не дозволяє суттєво підвищити точність роботи СД. Це обумовлено збереженням взаємного положення кластерів векторів, що відповідають статистичним параметрам ЗК та стеганограм, при їх обробці в просторі вищої розмірності [144,173]. Внаслідок цього підвищення точності роботи СД потребує використання апріорної інформації щодо взаємного положення кластерів векторів, що відповідають ЗК та сформованим стеганограмам, яка є обмеженою або навіть відсутньою у реальних випадках.

1.3.2 Стегодетектори на основі статистичних моделей контейнеру

Використання статистичних моделей ЗК в задачах стегоаналізу ЦЗ дозволило суттєво підвищити точність виявлення стеганограм у порівнянні з методами сигнатурного стегоаналізу [10]. Дані моделі засновані на виявленні та дослідженні слабких змін статистичних характеристик ЗК, обумовлених прихованням повідомлень. Для цього широко використовуються методи статистичного моделювання, зокрема з використанням математичного апарату марківських процесів [34,38,174]. Розглянемо поширені види статистичних моделей ЗК, що використовуються при побудові сучасних СД.

Одними з перших статистичних моделей, запропонованих для вирішення задач стегоаналізу ЦЗ, є моделі SPAM [38] та CC-PEV [175]. Дані моделі засновані на використанні математичного апарату марківських ланцюгів для дослідження ступеня кореляції значень яскравості суміжних пікселів досліджуваного зображення. Розглянемо основні етапи визначення параметрів стандартної статистичної моделі SPAM [38].

На першому етапі обробки ЦЗ з використанням статистичної моделі SPAM проводиться розрахунок різниць яскравості суміжних пікселів досліджуваного зображення при варіації напрямків обробки (сканування) ЦЗ. Наприклад, матриця різниць яскравості суміжних пікселів \mathbf{D} для зображення

\mathbf{U} розміром $N \times M$ пікселів, представленого в градаціях сірого кольору, у випадку сканування по рядкам зліва-направо може бути обчислена згідно наступного виразу [38]:

$$\mathbf{D}_{i,j}^{\rightarrow} = \mathbf{U}_{i,j} - \mathbf{U}_{i,j+1}, i \in [1; M], j \in [1, N - 1], \quad (1.20)$$

де $\mathbf{D}_{i,j}^{\rightarrow}$ – значення різниці яскравостей суміжних пікселів зображення \mathbf{U} з просторовим положенням (i, j) . При цьому значення елементів матриці \mathbf{D} може змінюватися в широкому діапазоні від 0 до $(2^k - 1)$, де k відповідає кількості бітів, виділених для представлення яскравості пікселю.

Практичне використання матриці $\mathbf{D}_{i,j}^{\rightarrow}$ (1.20) потребує використання значних об'ємів пам'яті (пропорційно до $(2^k - 1) \times (2^k - 1)$, $k > 0$), що підвищує складність налаштування СД. Для подолання даного обмеження в роботі [38] запропоновано використовувати оператор порогової обробки $\text{trunc}(x, T)$ елементів матриці $\mathbf{D}_{i,j}^{\rightarrow}$ для зменшення діапазону значень даних елементів при фіксованій втраті точності аналізу різниць яскравості суміжних пікселів ЦЗ:

$$\text{trunc}(x, T) = \begin{cases} (-T), & x < (-T), \\ x, & (-T) \leq x \leq (+T), \\ (+T), & x > (+T), \end{cases}$$

де $T \in \mathbb{N}$ – задане порогове значення.

На другому етапі обробки ЦЗ проводиться аналіз ступеня кореляції значень яскравості суміжних пікселів ЦЗ з використанням марківських ланцюгів першого та другого порядку. Для визначення параметрів даних моделей використовується обчислена матриця \mathbf{D} (1.20). Для розглянутого випадку сканування зліва-направо рядків досліджуваного зображення \mathbf{U} отримуємо:

$$\mathbf{M}_{u,v}^{\rightarrow} = \Pr(\mathbf{D}_{i,j+1}^{\rightarrow} = u | \mathbf{D}_{i,j}^{\rightarrow} = v), \quad (1.21)$$

$$\mathbf{M}_{u,v,w}^{\rightarrow} = \Pr(\mathbf{D}_{i,j+2}^{\rightarrow} = u | \mathbf{D}_{i,j+1}^{\rightarrow} = v, \mathbf{D}_{i,j}^{\rightarrow} = w), \quad (1.22)$$

де $\mathbf{M}_{u,v}^{\rightarrow}, \mathbf{M}_{u,v,w}^{\rightarrow}$ – матриці суміжності для елементів марківських ланцюгів першого та другого порядку відповідно; $u, v, w \in [-T; T]$ – значення різниць яскравості суміжних пікселів ЦЗ, що відповідають можливим станам елемен-

тів марківського ланцюга; $T \in \mathbb{N}$ – порогове значення. Матриці суміжності \mathbf{M} для інших напрямків обробки (сканування) ЦЗ можуть бути обчислені аналогічно до наведених формул (1.21)-(1.22).

На останньому етапі обробки ЦЗ проводиться перетворення отриманих матриць \mathbf{M}^c , $c \in \{\leftarrow, \uparrow, \rightarrow, \downarrow, \nearrow, \nwarrow, \searrow, \swarrow\}$ на відповідні вектори-рядки для використання в якості ознак при налаштуванні СД. Для зниження обчислювальної складності налаштування СД можуть використовуватися методи попередньої обробки отриманих векторів, враховуючи значну кількість елементів матриць (1.21)-(1.22) (пропорційно до T^2 для матриці $\mathbf{M}_{u,v}^{\rightarrow}$, та T^3 для матриці $\mathbf{M}_{u,v,w}^{\rightarrow}$). Зокрема, в роботі [38] запропоновано проводити усереднення отриманих матриць \mathbf{M} :

$$\mathbf{F}_{1,\dots,k} = [\mathbf{M}^{\rightarrow} + \mathbf{M}^{\uparrow} + \mathbf{M}^{\leftarrow} + \mathbf{M}^{\downarrow}]/4,$$

$$\mathbf{F}_{k+1,\dots,2k} = [\mathbf{M}^{\nearrow} + \mathbf{M}^{\nwarrow} + \mathbf{M}^{\searrow} + \mathbf{M}^{\swarrow}]/4,$$

де $k = (2T + 1)^2$ для марківського ланцюга першого порядку та $k = (2T + 1)^3$ для ланцюга другого порядку відповідно. Використання даної процедури дозволяє суттєво знизити обчислювальну складність налаштування СД при збереженні фіксованої точності виявлення стеганограм [38]. Це досягається за рахунок симетрії (незалежності) статистичних ознак ЦЗ при їх афінних перетвореннях (наприклад, повороти, дзеркальні відображення зображення) [141,143].

Застосування статистичних моделей SPAM [38] та CC-PEV [175] при розробці СД дозволило забезпечити високу точність виявлення стеганограм, сформованих згідно поширених стеганографічних методів OutGuess, nsF5, StegHide. Проте вагомим обмеженням даних статистичних моделей ЦЗ є відсутність попередньої обробки ЦЗ для виокремлення слабких змін ЗК, обумовлених прихованням повідомлень. Внаслідок цього точність роботи СД, побудованого з використанням моделей SPAM [38] та CC-PEV [175], суттєво знижується при обробці стеганограм, сформованих згідно новітніх АСМ.

Для подолання наведених обмежень поширених статистичних моделей ЦЗ, були запропоновані комплексні статистичні моделі зображень [34]. Особливістю даних моделей є зменшення впливу ЗК (контексту) на слабкі зміни статистичних параметрів зображення-контейнеру, обумовлені прихованням стегоданих. Це досягається за рахунок використання ансамблю ФВЧ для виділення шумових складових ЗК, на рівні котрих проводиться приховання повідомлень [10, 11].

Однією з найбільш потужних статистичних моделей ЦЗ, що використовується в задачах стегоаналізу ЦЗ, є модель SRM [34]. Визначення параметрів даної моделі проводиться в декілька етапів [34]. На першому етапі проводиться попередня обробка (фільтрація) зображення:

$$\mathbf{r}_{ij} = \tilde{\mathbf{U}}_{ij}(\mathcal{N}_{ij}) - \mathbf{U}_{ij},$$

де $\tilde{\mathbf{U}}_{ij}$ – оцінка вихідного виду досліджуваного зображення \mathbf{U}_{ij} в околі \mathcal{N}_{ij} ($\mathbf{U}_{ij} \notin \mathcal{N}_{ij}$) поточного пікселя з координатами (ij) ; \mathbf{r}_{ij} – виділені лишки (результати придушення контексту досліджуваного зображення в поточному околі). Приклади двовимірних фільтрів, що використовуються для виявлення слабких змін характеристик ЗК, обумовлених прихованням повідомлень, наведені на рис. 1.6.

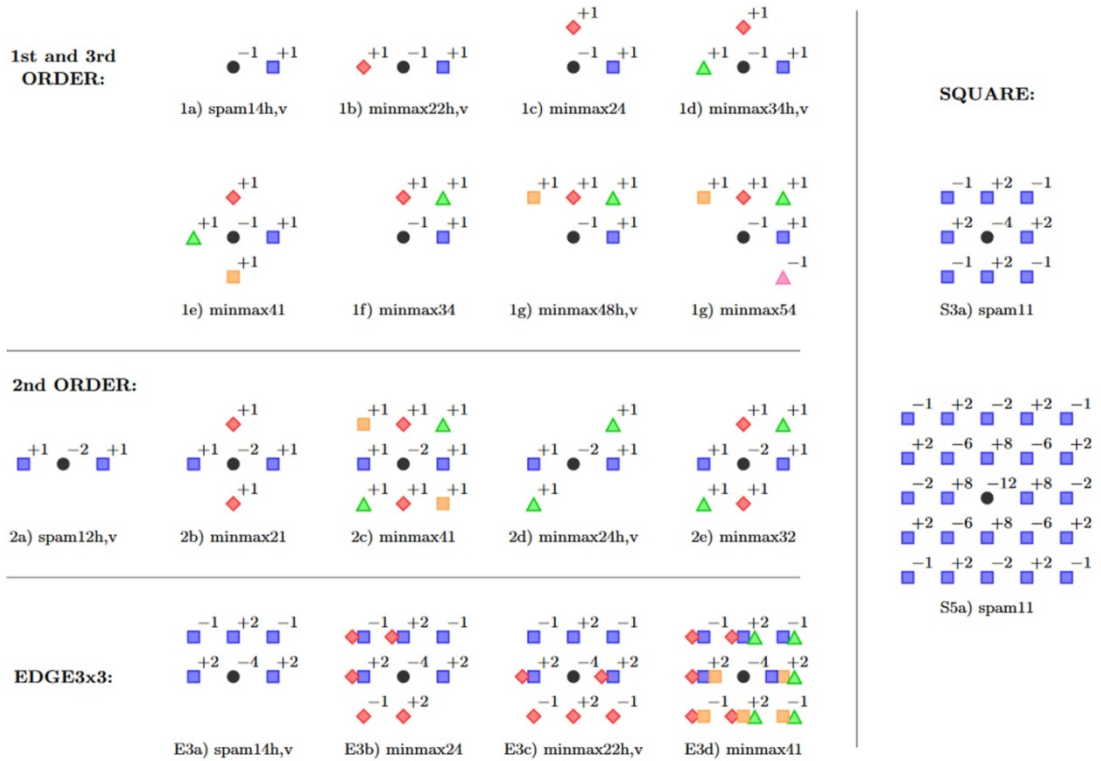


Рисунок 1.6 – Приклади двовимірних ФВЧ, що використовуються для придуження контексту зображення в околі поточного пікселя в моделі SRM.

За матеріалами роботи [34].

Обробка ЦЗ в статистичній моделі SRM проводиться з використанням ФВЧ, налаштованих для виділення змін яскравості лише суміжних пікселів зображення (рис. 1.6). Для підвищення точності виявлення слабких змін значень яскравості пікселів ЗК, обумовлених прихованням повідомлень, також використовуються спеціалізовані типи ФВЧ (наприклад, EDGE та SQUARE, рис. 1.6), що дозволяють досліджувати відмінності значень яскравості як суміжних, так і віддалених груп пікселів.

На наступному етапі, до отриманих лишків \mathbf{r} застосовується оператор порогової обробки $\text{trunc}(\cdot)$ для зменшення діапазону значень елементів лишків [34]:

$$\mathbf{r}_{ij} = \text{trunc}(\mathbf{r}_{ij}/q, T),$$

де $q > 0$ – крок квантування отриманих лишків.

На третьому етапі проводиться побудова матриць суміжності \mathbf{H} елементів \mathbf{r} при варіації напрямків сканування отриманих лишків. Наприклад, у випадку порядково сканування отримуємо [34]:

$$\mathbf{H}_{\mathbf{d}}^{(h)} = \{ \{ (\mathbf{r}_{ij}, \mathbf{r}_{ij+1}, \mathbf{r}_{ij+2}, \mathbf{r}_{ij+3}) | \mathbf{r}_{i,j+k-1} = d_k, k \in [1; 4] \} \} / Z,$$

де Z – нормалізуючий параметр, що забезпечує рівність $\sum_{\mathbf{d} \in \mathcal{T}_4} \mathbf{H}_{\mathbf{d}}^{(h)} = 1$; $\mathbf{d} = (d_1, d_2, d_3, d_4) \in \mathcal{T}_4$ – вектор значень суміжних елементів \mathbf{r} ; $\mathcal{T}_4 = \{-T, \dots, T\}^4$ – множина можливих значень вектору \mathbf{d} . Аналогічним чином розраховується матриця суміжності $\mathbf{H}_{\mathbf{d}}^{(v)}$ при скануванні зображення по кожному стовпчику. При цьому загальна кількість елементів даних матриць суміжності рівна $(2T + 1)^4$.

Статистична модель SRM дозволила суттєво підвищити точність роботи СД у порівнянні з поширеними моделями SPAM та CC-PEV [34]. Проте це досягається за рахунок використання значної кількості ФВЧ для попередньої обробки зображень (загалом 22 фільтрів), що призводить до суттєвого зростання обчислювальної складності процедури визначення параметрів моделі для оброблюваного ЦЗ.

Подальшим розвитком моделі SRM є статистичні моделі J+SRM [176], maxSRM [177], PSRM [174], SCRMQ1 [178] та інші. Дані моделі засновані на підвищенні точності оцінки статистичних параметрів шумових складових ЦЗ, зокрема шляхом використання спеціалізованих методів попередньої обробки зображень (наприклад, моделі maxSRM та PSRM), або ж ансамблю з декількох методів обробки (зокрема, модель J+SRM).

Відмітимо, що формування оптимального ансамблю ФВЧ у моделі SRM за критерієм мінімізації помилки виявлення стеганограм залишається, наразі, невирішеною задачею [177]. Для вирішення даної задачі широко використовуються методи відбору ФВЧ, що мають найбільший вплив на точність виявлення стеганограм при використанні розглянутих статистичних моделей ЦЗ. В якості прикладу можливо навести сучасні моделі PSRM (12,870 параметрів) [174], SCRMQ1 (12,753 параметрів) [178] та maxSRM (12,753 пара-

метрів) [177], що характеризуються суттєвим скороченням кількості параметрів у порівнянні з моделлю SRM (34,671 параметр ФВЧ) при збереженні фіксованої точності виявлення стеганограм [34].

Альтернативним підходом до побудови статистичних моделей ЗК є використання спеціальних типів ФВЧ для забезпечення високої точності виявлення стеганограм при збереженні фіксованої (низької) обчислювальної складності визначення параметрів даних моделей. В якості прикладу можливо навести сучасні статистичні моделі DCTR [179], PHARM [41], GFR [42], а також новітні моделі SCRMQ1 [178] та CFA-CRM [180]. Особливістю даних моделей є врахування кореляційних зв'язків між значеннями яскравості пікселів в окремих каналах кольору ЦЗ, що дозволяє підвищити точність виявлення стеганограм, сформованих з використанням кольорових ЗК.

Незважаючи на появу нових типів статистичних моделей ЗК, обчислювальна складність їх налаштування залишається відносно високою [9,13]. Це обумовлено надзвичайно великою кількістю параметрів моделі, що підвищує вимоги щодо об'єму навчальної вибірки ЦЗ (наприклад, 34,671 параметрів для моделі SRM). З іншого боку, наразі невирішеною лишається задача формування ансамблю оптимальних ФВЧ за критерієм мінімізації помилки виявлення стеганограм [9]. Запропоновані методи дозволяють вирішити дану задачу лише для окремих (часткових) випадків, коли статистичні характеристики досліджуваних ЦЗ є апріорно відомими. Це обмежує використання даних методів при обробці пакетів реальних зображень, що характеризуються зміною в широких межах значень статистичних, спектральних та структурних параметрів.

Одним з шляхів подолання наведених обмежень сучасних статистичних моделей ЦЗ є використання ЗНМ, що дозволяють визначати оптимальні параметри ФВЧ за критерієм мінімізації помилки виявлення стеганограм в процесі налаштування мережі [45]. Огляд сучасних підходів до побудови СД для цифрових зображень з використанням ЗНМ наведено у наступному розділі.

1.3.3 Стегодетектори на основі згорткових нейронних мереж

Сучасні СД на основі згорткових нейронних мереж засновані на використанні потужних ансамблів ФВЧ у вхідних (згорткових) шарах для виявлення слабких змін значень яскравості пікселів ЗК, обумовлених прихованням повідомлень. Відмітимо суттєві відмінності між запропонованими методами формування даних ансамблів ФВЧ [181-183]:

- Залучення ФВЧ, запропонованих для статистичних моделей ЦЗ, зокрема моделі SRM (наприклад, для мереж Ye-Net [184], Yedroudj-Net [44], SR-Net [30]);
- Використання спеціальних типів ФВЧ (наприклад, для мережі QIAN-Net [44]);
- Застосування спеціальних типів методів згортки, наприклад роздільної (поканальної) згортки для кольорових зображень (англ. Depthwise Separable Convolution, DSC [43]) та об'єднання просторових пірамід (англ. spatial pyramid pooling, SPP) [185] для мереж Zhu-Net [43] та GBRAS-Net [44].

Для додаткового підвищення точності роботи СД у випадку обробки стеганограм, сформованих згідно ACM, запропоновано використовувати спеціальні методи регуляризації параметрів ЗНМ [186], ансамблів штучних нейронних мереж [182] та багатошарових (глибоких) ЗНМ, засновані на об'єднанні декількох шарів штучних нейронів. Прикладами СД, що використовуються даний підхід є штучні нейронні мережі IAS-CNN [187], DRHNet [188], SCAE [45], UT-SCA-GAN [189] тощо. Проте висока точність роботи даних СД досягається за рахунок суттєвого підвищення обчислювальної складності налаштування ЗНМ та вимог щодо об'єму тестового пакету ЦЗ. Це обмежує можливості щодо швидкого переналаштування СД для виявлення апріорно невідомих СМ.

Прикладами сучасних ЗНМ, що використовуються при побудові високоточних СД, є мережі Xu-Net [190], Ye-Net [184], Yedroudj-Net [191],

SR-Net [30] та Zhu-Net [43]. Розглянемо особливості сучасних ЗНМ, запропонованих для побудови високоточних СД, більш детально (рис. 1.7).

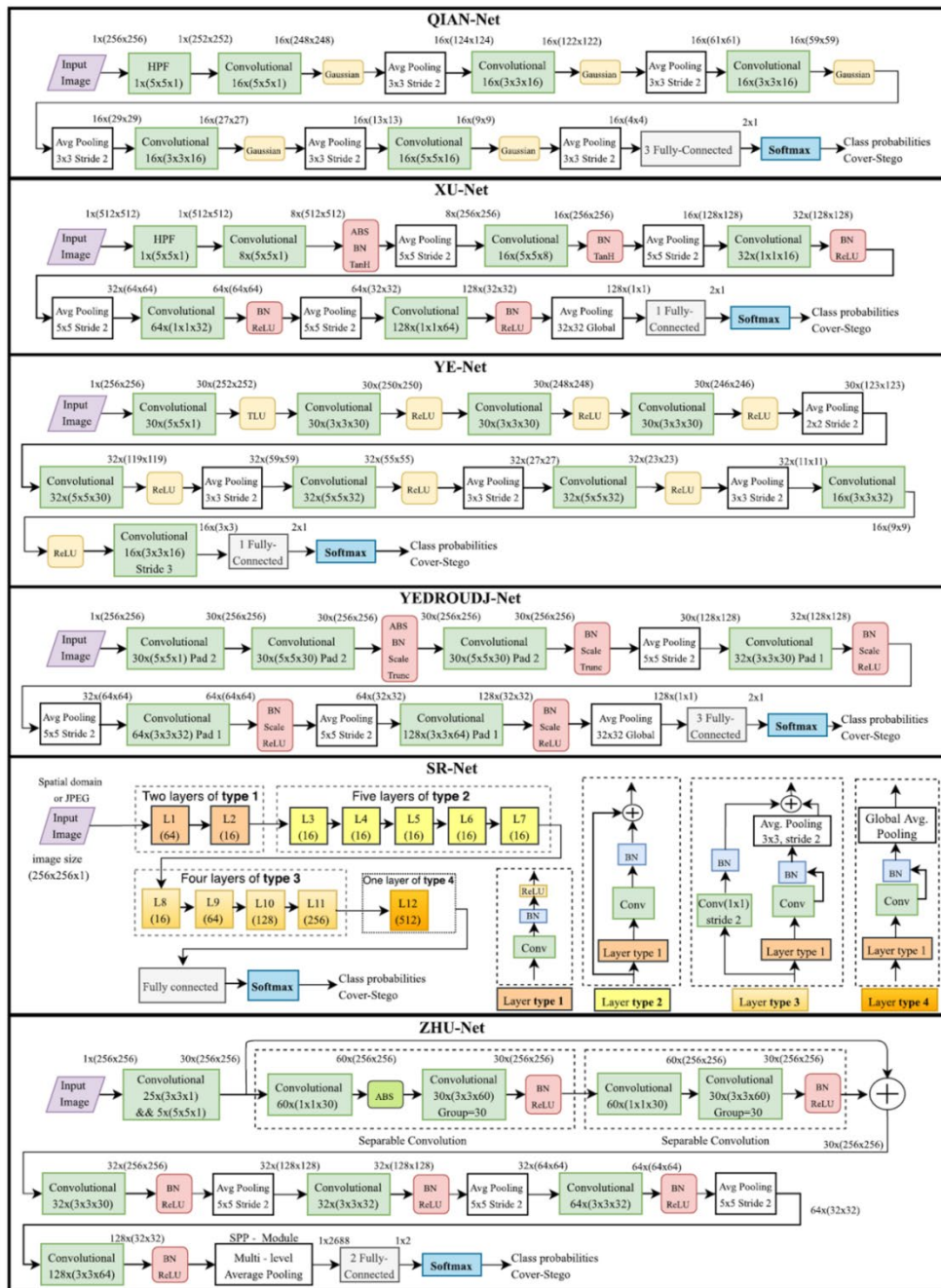


Рисунок 1.7 – Порівняння структури згорткових нейронних мереж, що використовуються при побудові сучасних високоточних стегодетекторів.

За матеріалами роботи [44].

Штучна нейронна мережа QIAN-Net [44] заснована на застосуванні послідовності згорткових шарів, що використовують фільтри Гауса для обробки ЦЗ (рис. 1.7). Для зниження обчислювальної складності налаштування мережі QIAN-Net при збереженні фіксованої точності виявлення стегограм

до векторів на виході згорткових шарів мережі застосовується операція повторної вибірки (субдискретизації, англ. pooling). Подальша класифікація оброблених векторів проводиться з використанням повнозв'язного шару штучних нейронів з нормованою експоненційною функцією активації (англ. softmax).

Для запобігання ефекту перенавчання (зниження точності роботи СД на нових пакетах ЦЗ) мережі QIAN-Net при обробці вибірок реальних зображень була запропонована модель Xu-Net (рис. 1.7) [190]. Особливістю моделі Xu-Net є впровадження додаткових етапів обробки обчислених параметрів досліджуваного зображення, зокрема використання абсолютних значень елементів вихідних векторів у функціях активації проміжних шарів та подальше нормування отримуваних значень (англ. batch normalization)

Подальшим розвитком моделі Xu-Net є згорткова нейронна мережа Ye-Net (рис. 1.7), запропонована в роботі [184]. Дана модель заснована на внесенні суттєвих змін до структури ЗНМ, а саме [184]:

1. Згорткові шари мережі використовують високочастотні фільтри, зокрема запропоновані для статистичної моделі SRM [34], оператори Робертса, фільтри Собеля, оператори Шарра [141,192], замість псевдовипадкової ініціалізації функцій згортки. Це дозволяє зменшити обчислювальну складність налаштування мережі Ye-Net при збереженні високої точності виявлення слабких змін ЗК, обумовлених – прихованням повідомлень.
2. Для зниження негативного впливу явище «перенасичення» значень функції активації (стрибкоподібного зростання значень елементів вихідних векторів), в проміжних шарах мережі Ye-Net використовується обмежена лінійна функція активації штучних нейронів (англ. Truncated Linear Unit, TLU).
3. В процесі обробки ЦЗ проводиться оцінка імовірності зміни кожного пікселя в процесі приховання повідомлень згідно поширених СМ (англ. side channel information, SCI). Обчислення даної імовірності

проводиться шляхом аналізу змін отримуваних векторів-ознак на виході мережі, обумовлених вбудовуванням до досліджуваного ЦЗ тестових повідомлень згідно поширених АСМ.

Наведені особливості мережі Ye-Net дозволили суттєво підвищити точність виявлення стеганограм, сформованих згідно поширених АСМ, при збереженні фіксованої обчислювальної складності налаштування СД. Для додаткового зниження складності налаштування СД при збереженні фіксованої точності виявлення стеганограм була запропонована мережа Yedroudj-Net (рис. 1.7), заснована на модифікації структури мережі Ye-Net [191]. Особливістю мережі Yedroudj-Net є виключення етапу визначення SCI-даних, що знижує точність виявлення стеганограм, сформованих з використанням методів аналізу вихідного виду контейнера та синхронізації змін яскравості пікселів ЗК, наприклад методу Synch [132].

Відмітимо, що наведені згорткові нейронні мережі були запропоновані для виявлення стеганограм з даними, вбудованими в просторовій або ж спектральній області ЗК. Для забезпечення високої точності детектування стеганограм незалежно від області приховання повідомлень запропоновано штучну нейронну мережу SR-Net (рис. 1.7) [30]. Особливістю даної мережі є ініціалізації ядер згортки початкових шарів мережі високочастотними фільтрами з моделі SRM [34], та подальшого оновлення параметрів даних шарів за результатами налаштування ЗНМ. Це дало можливість підвищити точність виявлення стеганограм, сформованих згідно новітніх стеганографічних методів, у порівнянні з розглянутими видами ЗНМ. Проте це було досягнуто за рахунок суттєвого ускладнення архітектури мережі SR-Net, що призвело до суттєвого зростання складності її налаштування.

В роботі [43] запропоновано модифікацію мережі SR-Net, спрямовану на зниження обчислювальної складності налаштування ЗНМ при збереженні високої точності роботи СД. Особливістю розробленої мережі Zhu-Net (рис. 1.7) є зменшення розміру ФВЧ, що використовуються у вхідних шарах ЗНМ, а також застосування спеціалізованої DSC-згортки. Обробка ЦЗ із застосу-

ванням DSC-згортки проводиться в два етапи – використання двовимірної згортки для обробки окремих каналів кольору ЦЗ, та подальше лінійне перетворення результатів згортки, що мають однакові просторові координати. Додаткове підвищення точності виявлення стеганограм при використанні мережі Zhu-Net досягається за рахунок обробки результатів згортки на декількох масштабах з використанням SPP-методу [185].

Подальшим вдосконаленням мережі Zhu-Net є згорткова нейронна мережа GBRAS-Net, запропонована в роботі [44]. Мережа GBRAS-Net дала можливість гнучко обирати компроміс між точністю роботи СД та обчислювальною складністю налаштування ЗНМ за рахунок наступних змін у структурі даної мережі [44]:

- Використання лише 9 згорткових шарів для попередньої обробки досліджуваного зображення. Це дозволяє досягти компромісу між точністю виявлення аномальних змін ЗК, обумовлених прихованням повідомлень, та складністю налаштування мережі GBRAS-Net. Для порівняння, мережа SR-Net забезпечує високу точність виявлення даних змін за рахунок високої обчислювальної складності навчання 25 згорткових шарів, тоді як Zhu-Net дозволяє досягти швидкого навчання з 5 згортковими шарами.
- Збільшення кількості шарів DSC-згортки для підвищення точності виявлення слабких змін ЗК, обумовлених прихованням повідомлень згідно новітніх АСМ.

Розглянемо архітектуру згорткової мережі GBRAS-Net більш детально (рис. 1.8).

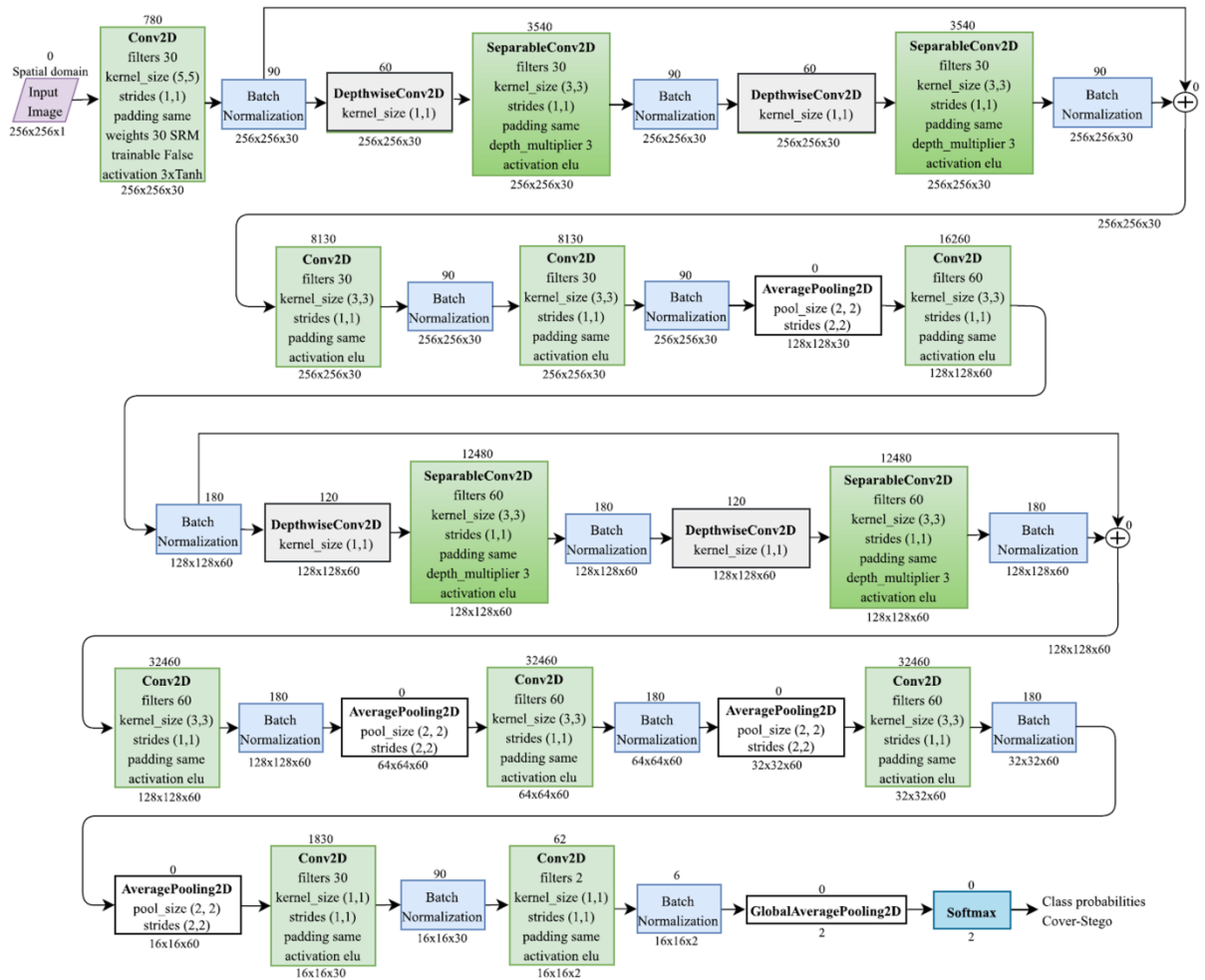


Рисунок 1.8 – Структура стегодетектору на основі згорткової нейронної мережі GBRAS-Net. За матеріалами роботи [44].

Обробка ЦЗ з використання мережі GBRas-Net проводиться в декілька етапів (рис. 1.8). На першому етапі, досліджуване зображення оброблюється з використанням послідовності згорткових шарів. Дані згорткові шари засновані на використанні 30 фільтрів, запропонованих для статистичної моделі SRM, що дозволяє забезпечити високу точність виявлення даних аномальних спотворень ЗК [44].

Наступний етап обробки ЦЗ полягає у застосуванні DSC-згортки, параметри котрої можуть змінюватися в процесі налаштування мережі GBRAS-Net для підвищення точності виявлення стеганограм (рис. 1.8). Для зниження негативного впливу зменшення амплітуди градієнту в процесі оновлення параметрів мережі згідно методу зворотнього розповсюдження помилок, до структури ШНМ включені прямі з'єднання між суміжними шарами мережі.

Для зниження розмірності отримуваних векторів (статистичних параметрів ЦЗ) до них застосовується процедура повторної вибірки [44].

На останньому етапі, отримані статистичні параметри ЦЗ передаються до повнозв'язних шарів для подальшої класифікації. Особливістю даних шарів є використання оператора глобальної субдискретизації та функцій активації softmax для оцінки імовірностей віднесення досліджуваного зображення до класів контейнеру або ж стеганограми.

Наведені особливості мережі GBRas-Net дозволили досягти точності виявлення стеганограм, співставної з високоточними СД на основі статистичних моделей ЗК та ЗНМ, при збереженні відносно низької обчислювальної складності налаштування. За результатами порівняльного аналізу встановлено, що мережа GBRas-Net забезпечує співставну, а в окремих випадках і вищу точність виявлення стеганограм, сформованих згідно новітніх АСМ, у порівнянні зі СД на основі моделей SRM, SR-Net та Zhu-Net на стандартних пакетах зображень BOWS, BOSS і ALASKA [44].

Відмітимо, що досягнення високої точності виявлення стеганограм (більше 95%) при використанні СД на основі ЗНМ потребує використання пакетів тестових зображень значного об'єму (більше 10,000 зображень) [8]. Це обумовлено нелінійною залежністю обчислювальної складності налаштування багат шарових (глибоких) штучних нейронних мереж від кількості шарів [46,47,193], що обмежує можливості щодо швидкого переналаштування СД для виявлення стеганограм, сформованих згідно нових типів АСМ. Тому становить інтерес використання спеціальних типів ШНМ для розробки високоточних СД, що характеризуються відносно низькою обчислювальною складністю налаштування. Результати аналітичного огляду СД на основі спеціальних типів ШНМ наведені в наступному розділі.

1.3.4 Стегодетектори на основі спеціальних типів нейронних мереж

Для зниження обчислювальної складності налаштування багат шарових ЗНМ при збереженні заданої (фіксованої) точності роботи СД широко

використовуються спеціальні методи нормування обчислених параметрів досліджуваних ЦЗ (наприклад, субдискретизації результатів згортки ЦЗ з ФВЧ, включення до структури мережі прямих з'єднань між шарами штучних нейронів тощо) [181,182]. Проте величина зменшення складності налаштування СД при використанні даних методів суттєво залежить від статистичних параметрів оброблюваних зображень. Для подолання даного обмеження було запропоновано змінити структуру ШНМ, зокрема використовувати автокодувальні нейронні мережі (АНМ) [47,127,194,195].

Особливістю АНМ є визначення параметрів досліджуваних ЦЗ, що є нечутливими (робастними) до незначних змін значень яскравості пікселів зображень [46,47]. Це досягається за рахунок використання представлення АНМ як композиції декількох штучних нейронних мереж [47]:

$$\tilde{\mathbf{x}} = g_{dec}(f_{enc}(\mathbf{x})), d(\mathbf{x}, \tilde{\mathbf{x}}) \leq \varepsilon, \quad (1.23)$$

де $\mathbf{x}, \tilde{\mathbf{x}}$ – відповідно, дані на вході та виході АНМ; $f_{enc}(\cdot)$ – функція визначення апроксимації (вектору \mathbf{h}) вхідних даних; $g_{dec}(\cdot)$ – функція відновлення вихідного виду даних \mathbf{x} за результатами обробки отриманого вектору \mathbf{h} ; $d(\cdot, \cdot)$ – функція оцінки відмінностей між вхідними та обробленими даними.

Зазвичай, визначення функцій $f_{enc}(\cdot)$ та $g_{dec}(\cdot)$ у виразі (1.23) проводиться з використанням відповідних штучних нейронних мереж, а саме мереж «кодування» (англ. Encoder) та «декодування» (англ. Decoder) досліджуваних ЦЗ [47]. При цьому для оцінки відмінностей між вхідними та обробленими даними у функції $d(\cdot, \cdot)$ (1.23) широко використовується середньоквадратичне відхилення значень яскравості пікселів вихідного ЦЗ від відповідних значень яскравості пікселів для обробленого зображення. Це дозволяє використовувати поширені методи налаштування ШНМ при збереженні низької обчислюваної складності процедури оновлення параметрів шарів мережі.

Відомі АНМ можливо розділити на наступні групи в залежності від параметрів та особливостей структури даних мереж [47]:

1. Автоенкодері для вирішення задач зниження розмірності вихідних даних (англ. undercomplete autoencoders) – спрямовані на формування «стиснутого» представлення \mathbf{h} у виразі (1.23), кількість елементів котрого є меншою за кількість елементів вхідних даних \mathbf{x} . Мережі даного типу використовуються для підвищення точності роботи систем класифікації даних, зокрема для визначення особливостей оброблюваних класів, що найбільш відрізняють їх один від одного;
2. Розріджені автоенкодері (англ. overcomplete/sparse autoencoders) – цільова функція налаштування для даних мереж додатково враховує ступінь розрідженості (частки нульових елементів) вектору \mathbf{h} . Даний тип мереж застосовується для визначення характеристик оброблюваних даних, що найбільше впливають на точність роботи систем класифікації;
3. Знешумлюючі автоенкодері (англ. denoising autoencoders, DAE) – спрямовані на оцінку початкового (незашумленого) виду вхідних сигналів \mathbf{x} за наявними (зашумленими) даними. Дана особливість широко використовується в сучасних методах підвищення візуальної якості зображень, а також новітніх методах деструкції стеганограм;
4. Стискаючі автоенкодері (англ. contractive autoencoders) – спрямовані на збереження заданого (фіксованого) представлення \mathbf{h} при незначних змінах вхідних даних \mathbf{x} . Це досягається за рахунок включення до цільової функції, що використовується при налаштуванні даних мереж, додаткового члену $\|\partial f_{enc}(\mathbf{x})/\partial \mathbf{x}\|_F^2$, значення котрого є пропорційним до зміни представлення \mathbf{h} при варіації даних \mathbf{x} .

Особлива увага в задачах стегааналізу ЦЗ приділяється DAE-мережам, з огляду на їх властивості оцінки вихідного виду сигналів \mathbf{x} (зокрема ЗК) при несуттєвих змінах значень яскравості оброблюваних зображень. В якості прикладу можливо навести новітні комплексні (гібридні) ШНМ [9], заснованих на поєднанні DAE-мереж та багат шарових нейронних мереж. Дані ме-

режі були запропоновані для підвищення точності виявлення слабких змін ЗК, обумовлених прихованням повідомлень згідно АСМ, при збереженні відносно низької обчислювальної складності налаштування СД.

В якості прикладу гібридних мереж, запропонованих для вирішення задач стегааналізу ЦЗ, можливо навести новітню мережу ASSAF [127]. Дана мережа складається з двої частин, а саме DAE-мережі та дуальної (сіамської) нейронної мережі. Перша мережа використовується для зниження впливу завад (а саме спотворень ЗК, обумовлених прихованням повідомлень), в той час як сіамська мережа застосовується для визначення статистичних параметрів та подальшого віднесення обробленого зображення до класів ЗК або стеганограм. Структура мережі ASSAF наведена на рис. 1.9.

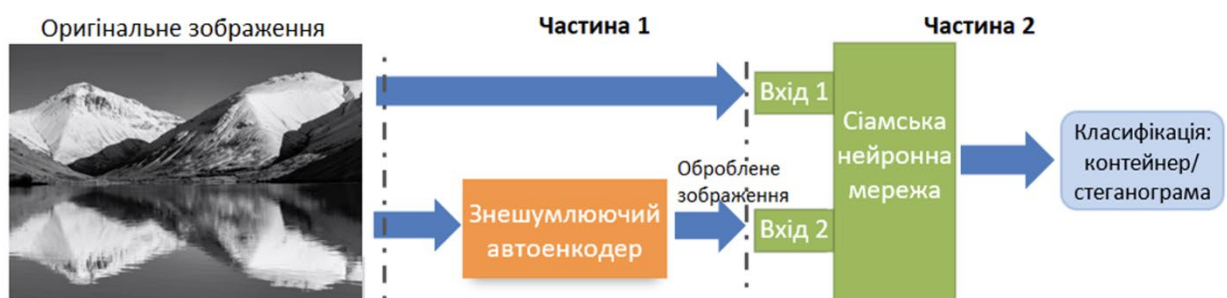


Рисунок 1.9 – Структура штучної нейронної мережі ASSAF для виявлення стеганограм. За матеріалами роботи [127].

Застосування DAE-мережі у складі мережі ASSAF дозволяє зменшити вплив незначних змін значень яскравості пікселів оброблюваного ЦЗ (рис. 1.9), обумовленого прихованням повідомлень [127]. Використання спеціальних типів ШНМ для проведення попередньої обробки досліджуваних ЦЗ суттєво відрізняється від поширеного підходу до побудови СД із застосуванням ансамблю ФВЧ (рис. 1.2).

За результатами порівняльного аналізу [127] встановлено, що мережа ASSAF дозволяє суттєво (до 2-3 разів) скоротити тривалість налаштування стегодетекторів у порівнянні з сучасними СД на основі ЗНМ при збереженні фіксованої точності виявлення стеганограм. Варто зазначити, що дані результати були отримані для випадку використання поширених типів СМ, що ха-

рактикуються суттєвими змінами значень яскравості пікселів ЗК в процесі приховання повідомлень. Використання новітніх АСМ дозволяє мінімізувати дані зміни яскравості пікселів ЗК, що знижує точність визначення (локалізації положення) пікселів ЗК, використаних для приховання окремих стегобітів, при використанні мережі ASSAF. Це обумовлює необхідність подальшого вдосконалення СД на основі DAE-мережі, що є одним з напрямків досліджень в галузі стегоаналізу ЦЗ [9].

Відмітимо, що точність роботи розглянутих СД на основі статистичних моделей ЗК та ШНМ, зазвичай, визначається з використанням стандартних пакетів ЦЗ, зокрема BOSS [27] та ALASKA [134]. Особливістю даних пакетів є використання ЦЗ високої якості, що характеризуються відносно низьким рівнем як власних шумів, так і спотворень, обумовлених застосування поширених процедур обробки зображень (наприклад, стиснення з втратами, методів підвищення візуальної якості). Це ускладнює оцінку значення помилки виявлення стеганограм при обробці ЦЗ, які циркулюють в локальних та глобальних ІКС. Особливістю даних зображень є суттєве зростання енергії власних шумів, а також обмежені дані щодо типу та параметрів використаних методів попередньої обробки ЦЗ.

Також недостатньо уваги при проведенні досліджень сучасних СД приділяється аналізу точності виявлення стеганограм в умовах обмеженості апріорних даних щодо використаного стеганографічного методу. Зокрема в літературі відсутні відомості щодо точності роботи сучасних СД при проведенні їх налаштування з обмеженою кількістю прикладів стеганограм. Тому становить інтерес порівняльний аналіз точності роботи сучасних стегодетекторів при обробці пакетів реальних ЦЗ, що характеризуються значною варіативністю статистичних, спектральних та структурних параметрів в умовах обмеженості апріорних даних щодо особливостей використаного СМ.

1.4 Порівняльний аналіз точності виявлення стеганограм, сформованих згідно новітніх стеганографічних методів, при використанні сучасних типів стегадетекторів

Дослідження проводилося з використанням як стандартного пакету зображень ALASKA, що широко використовується в галузі стегоаналізу ЦЗ, так і більш потужних пакетів VISION, MIRFlickr, що використовуються в галузі обробки цифрових зображень:

- Пакет ALASKA [134] – стандартний тестовий пакет для порівняння точності роботи СД. Пакет складається з 80,000 зображень, отриманих з використанням 40 цифрових камер, включаючи смартфони, планшети, поширені моделі цифрових камер, а також високоякісних цифрових дзеркальних камер (англ. digital single-lens reflex camera, DSLR). Особливістю пакету є використання фіксованої процедури попередньої обробки досліджуваних зображень, для мінімізації варіативності статистичних та спектральних параметрів ЦЗ.
- Пакет VISION [196] – запропонований для оцінки параметрів власних шумів ЦЗ та ідентифікації цифрової камери, використаної для формування зображення. Пакет складається з 34,427 зображень високої якості, представлених після обробки в сервісах YouTube та WhatsApp, соціальній мережі Facebook. Зображення були отримані з використанням 35 мобільних пристроїв (смартфонів) найбільш поширених виробників, зокрема Apple, Samsung, Huawei, Sony тощо.
- Пакет MIRFlickr [197] – є одним зі стандартних пакетів в галузі пошуку подібних зображень в умовах наявності спотворень, обумовлених використанням методів стиснення з втратами. Пакет сформований з використанням близько 1 мільйона цифрових зображень, що циркулюють в сервісі обміну зображеннями Flickr. Відмітимо, що зображення для пакету MIRFlickr характеризуються значною варіативністю типу та параметрів методів попередньої обробки, наприк-

лад, стиснення з втратами, зміни розміру, покращення візуальної якості тощо.

Використання спеціалізованих методів попередньої обробки ЦЗ зі стандартного пакету ALASKA дозволяє суттєво знизити рівень власних шумів, тим самим підвищуючи точність виявлення слабких спотворень ЗК, обумовлених прихованням повідомлень. Використання даного пакету зображень при проведенні досліджень в галузі стегааналізу ЦЗ дозволяє проводити оцінку досяжної точності роботи сучасних СД при обробці високоякісних зображень. З іншого боку, тестові зображення з пакетів VISION та MIRFlickr характеризуються значним рівнем адитивних шумів, що дозволяє «маскувати» спотворення значень яскравості груп пікселів ЗК при вбудовуванні стегаданих. Це призводить до зниження точності роботи запропонованих типів СД, зокрема у випадку використання новітніх АСМ для формування стегаграм.

Порівняння результатів аналізу точності сучасних СД при використанні розглянутих пакетів ЦЗ потребує врахування додаткових даних щодо ступеня «зашумленості» використовуваних ЦЗ (рівня адитивних шумів). Для оцінки даного показника в роботі був використаний фільтр Вінера (ФВ) [198], що дозволяє проводити оцінку енергії адитивних завад шляхом усереднення локальних оцінок σ_I^2 дисперсії значень яскравості пікселів, отриманих з використанням ковзного вікна (КВ) розміром $w_W \times w_W$ (пікселів).

Відмітимо, що вибір розміру КВ суттєво впливає на точність роботи ФВ – використання ковзних вікон відносно малого розміру підвищує чутливість фільтру до локальних збурень (значних відмінностей значень яскравості суміжних пікселів ЦЗ), в той час застосування КВ значного розміру може призвести до зміщеної оцінки значення енергії завад за рахунок збільшення впливу контурів об'єктів на результати роботи фільтру [76]. Внаслідок цього становить інтерес визначення оптимального розміру КВ, що дозволить мінімізувати як вплив локальних збурень значень яскравості пікселів ЦЗ, так і

величини зміщення значення σ_1^2 на точність оцінки енергії завад при використанні фільтру Вінера.

Для вирішення даної задачі було проведено дослідження змін значень дисперсії яскравості пікселів ЗК при варіації розміру КВ фільтру Вінера для псевдовипадкової вибірки з 1,000 зображень зі стандартного пакету ALASKA. Залежності значень дисперсії яскравості пікселів ЦЗ при використанні фільтру Вінера від розміру КВ наведена на рис. 1.10.

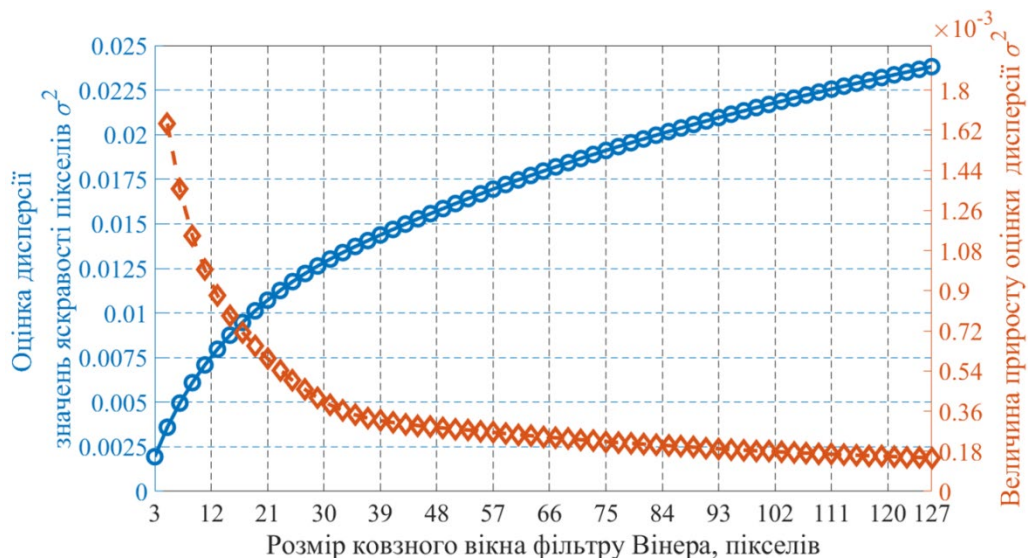


Рисунок 1.10 – Залежність значень дисперсії яскравості пікселів ЦЗ (неперервна лінія, ліва вісь ОУ) та величини приросту даної оцінки (штрихова лінія, права вісь ОУ) від розміру ковзного вікна фільтру Вінера.

Графік залежності значень дисперсії яскравості пікселів ЦЗ від розміру КВ фільтру Вінера має точку перегину (рис. 1.10, $w_W = 35$ пікселів). Наявність даної точки обумовлена зміною впливу локальних збурень (значних змін значень яскравості суміжних пікселів ЦЗ) та контурів об'єктів на зображенні (стабілізація приросту σ_1^2 на рівні $1.8 \cdot 10^{-4}$) на величину приросту значень σ_1^2 . Внаслідок цього можемо зробити висновок, що розмір КВ фільтру Вінера, що відповідає виявленій точці перегину (рис. 1.10), дозволяє оцінити рівень адитивних шумів ЦЗ при мінімізації впливу наведені факторів, а саме локальних збурень значень яскравості пікселів та контурів об'єктів на зображенні.

Для оцінки рівня адитивних завад тестових зображень з пакетів ALASKA, MIRFlickr та VISION була проведена оцінка значення σ_1^2 з використанням фільтру Вінера при розмірі ковзного вікна $w_W = 35$ (пікселів). Діаграма розкиду значень оцінок σ_1^2 для зображень з розглянутих тестових пакетів при використанні фільтру Вінера ($w_W = 35$ (пікселів)) наведена на рис. 1.11.

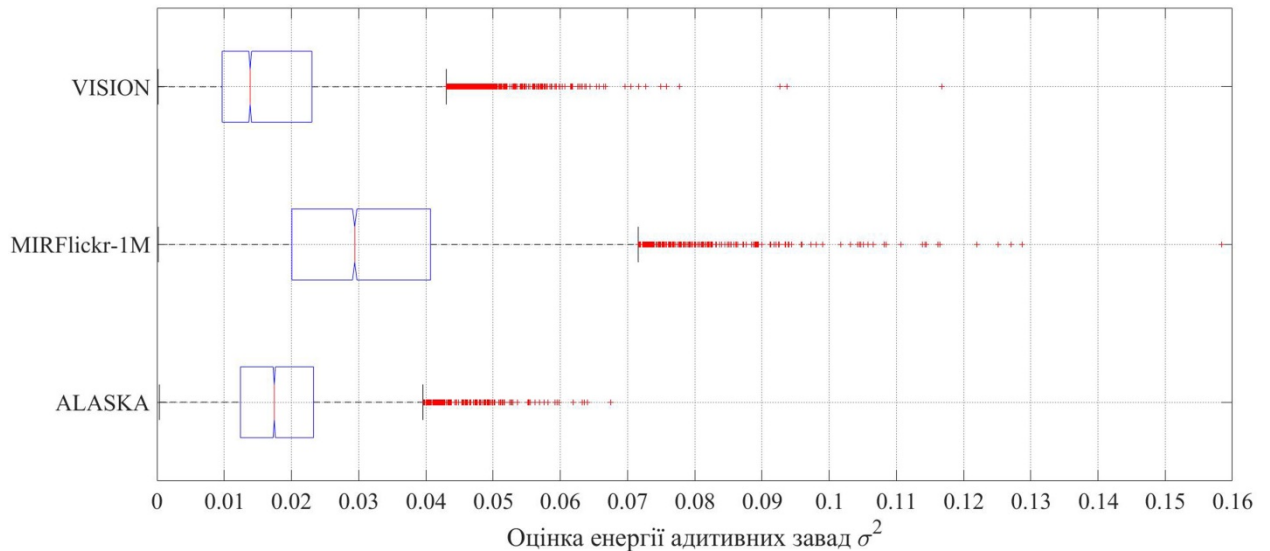


Рисунок 1.11 – Діаграма розкиду значень оцінок σ_1^2 для зображень з тестових пакетів ALASKA, MIRFlickr та VISION при використанні фільтру Вінера з розміром ковзного вікна, рівним $w_W = 35$ (пікселів).

Отримані результати підтверджують зроблені раніше висновки щодо суттєвої відмінності рівня адитивних шумів для зображень з пакетів ALASKA та MIRFlickr (рис. 1.11). Суттєве зростання рівня адитивних завад для тестових зображень з пакету MIRFlickr дозволяє підвищити ефективність роботи АСМ за рахунок «маскування» слабких спотворень ЗК, обумовлених прихованням повідомлень, на фоні значних шумів.

З іншого боку, тестові зображення з пакету VISION, отримані з використанням мобільних пристроїв, характеризуються найменшими значеннями σ_1^2 у порівнянні з розглянутими пакетами зображень (рис. 1.11). Це пояснюється «агресивною» роботою методів зниження шумів матриці фоточутливих елементів (МФЕ) при формуванні ЦЗ. Внаслідок цього знижується ефектив-

ність «маскування» спотворень ЗК, обумовлених прихованням повідомлень, з використанням власних шумів контейнеру.

Враховуючи суттєві відмінності у рівні власних завад тестових ЦЗ з розглянутих пакетів ALASKA, MIRFlickr та VISION (рис. 1.11), подальший інтерес становить дослідження точності виявлення стеганограм, сформованих згідно новітніх АСМ, при використанні сучасних СД.

1.4.1 Методика проведення досліджень

Дослідження точності роботи сучасних СД на вибірках ЦЗ, що характеризуються значною варіативністю статистичних, спектральних та структурних параметрів, проводилося з використанням адаптивних стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153]. Дані методи засновані на прихованні повідомлень шляхом зміни яскравості пікселів ЗК та є одними з найбільш складних СМ до виявлення з використанням сучасних СД [8,9,29,30,32]. Ступінь заповнення ЗК стегоданими Δ_{α}^S варіювалася в наступному діапазоні – від 3% до 5% з кроком 2%, від 5% до 10% з кроком 5 відсотків, та від 10% до 50% з кроком 10%.

Аналіз точності роботи СД проводився згідно стандартної процедури перехресної перевірки (англ. cross-validation, CV) [144]. Дана процедура заснована на розділенні пакету зображень \mathcal{S} псевдовипадковим чином на навчальну (\mathcal{S}_{train}) та контрольну (\mathcal{S}_{test}) вибірки без повторень. Отримані вибірки використовуються, відповідно, для визначення оптимальних параметрів СД, що мінімізують значення помилки виявлення стеганограм, та подальшої оцінки точності налаштованого стегодетектору [47,144]. Для отримання усередненої точності роботи СД, розділення пакету \mathcal{S} повторювалося декілька разів [46,144]. В роботі розглянуто випадок використання процедури перехресної перевірки для порівняльного аналізу точності роботи розглянутих СД, при десятикратному розбитті пакетів тестових зображень на навчальну (70%) та контрольну (30%) вибірки.

Формування вибірок зображень \mathcal{S}_{train} та \mathcal{S}_{test} проводилося з використання розглянутих пакетів ALASKA [134], VISION [196] та MIRFlickr [197]. Відмітимо, що кількість та розмір ЦЗ в даних пакетах суттєво різняться, наприклад, від 34,427 зображень для пакету VISION до одного мільйона зображень для пакету MIRFlickr. Для забезпечення однакових умов тестування СД при використанні даних пакетів ЦЗ, в роботі були використані псевдовипадкові вибірки 10,000 цифрових зображень для кожного пакету.

Застосування зображень різного розміру при налаштуванні та тестуванні СД може призвести до отримання зміщених оцінок точності роботи стегодетектору. Це обумовлено залежністю точності оцінки статистичних характеристик від розміру оброблюваного зображення [10]. В роботі [199] встановлена емпірична залежність величини помилки класифікації стегограм при варіації розміру досліджуваного зображення:

$$P_E(\tilde{\mathbf{U}}) \propto \sqrt{|\tilde{\mathbf{U}}|_s} \cdot P_E(\mathbf{U}), \quad (1.24)$$

де $\mathbf{U}, \tilde{\mathbf{U}}$ – відповідно, вихідне та масштабоване зображення; $|\cdot|_s$ – функція визначення кількості пікселів зображення. Згідно даного виразу (1.24), зростання кількості пікселів в оброблюваному ЦЗ призводить до нелінійної зміни точності роботи СД. Дане явище обумовлено змінами значення інформації Фішера для використовуваної статистичної моделі ЦЗ при варіації розмірів досліджуваного зображення [200].

Для зниження впливу варіації розмірів використовуваних ЦЗ на оцінку точності роботи СД в роботі проводилося масштабування зображень до однакового розміру 512×512 пікселів. Даний розмір ЦЗ, наразі, широко використовується в якості стандартного в дослідженнях ефективності методів стегоаналізу цифрових зображень [9-11,13]. Також проводилося перетворення системи кольору тестових зображень, а саме представлення їх в градація сірого кольору, враховуючи, що більшість сучасних СД засновані на дослідження зображень, представлених в даній системі кольору [9,30,34,127].

Для віднесення досліджуваних зображень до класів ЗК та стеганограм проводилася обробка отриманих статистичних, спектральних та структурних параметрів ЦЗ з використання ансамблю класифікаторів на основі лінійних дискримінантів Фішера (англ. Random Forest, RF) [144,201]. Налаштування даного класифікатора проводилося шляхом мінімізації помилки класифікації стеганограм P_E на \mathcal{S}_{train} вибірці [202]:

$$P_E = \min_{P_{FP}} \frac{1}{2} (P_{FP} + P_{FN}(P_{FP})), \quad (1.25)$$

де P_{FP}, P_{FN} – відповідно, імовірність помилок першого (хибне віднесення ЗК до класу стеганограм) та другого (хибне віднесення стеганограм до класу ЗК) роду.

Вагомий вплив на точність роботи СД має наявність апріорних даних щодо використаного стеганографічного методу, зокрема прикладів стеганограм, сформованих згідно даного методу. Забезпечення високої точності роботи СД потребує використання на етапі налаштування стегодетектору пар ЗК та відповідних їх стеганограм [202]. Для дослідження впливу апріорних даних щодо використаного СМ на точність роботи СД в роботі проводилася варіація кількості відповідних стеганограм в \mathcal{S}_{train} вибірці. Для кількісної оцінки частки стеганограм, використаних при налаштуванні СД, використовувався наступний показник [60]:

$$K_\alpha^{OL} = \frac{|\{(\mathbf{X}, \mathbf{Y}): (\mathbf{X}_i, \mathbf{Y}_i), i \in \mathcal{S}_{train}\}|}{|\mathcal{S}_{train}|} \times 100\%. \quad (1.26)$$

Даний показник відповідає частці пар стеганограм та відповідних ЗК, використаних для їх формування, в навчальній вибірці зображень \mathcal{S}_{train} . Значення показника K_α^{OL} (1.26) змінюється від 0%, що відповідає випадку відсутності у вибірці \mathcal{S}_{train} зображень-контейнерів, використаних для формування стеганограм, до 100%, коли в вибірці \mathcal{S}_{train} наявні пари ЗК та відповідних їм стеганограм.

При проведенні досліджень було розглянуто два граничні випадки значень показника K_α^{OL} (1.25) [60]:

- Наявність стеганогам та відповідних ЗК, використаних для їх формування, у вибірці \mathcal{S}_{train} ($K_{\alpha}^{OL} = 100\%$) – відповідає випадку налаштування СД, коли стегоаналітик має доступ до модуля формування стеганогам та може формувати стеганогам для довільного ЗК.
- Відсутність у вибірці \mathcal{S}_{train} зображень-контейнерів, що були використані для формування наявних стеганогам ($K_{\alpha}^{OL} = 0\%$) – відповідає ситуації, коли стегоаналітик не має доступу до СК та може використовувати лише наявні стеганограми (випадок виявлення невідомих стеганографічних методів, проблема zero-day).

Для оцінки якості роботи налаштованих СД були використані наступні показники [46,47,144,203]: помилки першого P_{FP} та другого P_{FN} роду, загальна помилка класифікації стеганогам P_E (1.25), F_1 -індекс та коефіцієнт кореляції Метьюса (англ. Matthews Correlation Coefficient) MCC . Інтегральний показник F_1 широко використовується для оцінки як точності (частки виявлених стеганогам серед тестової вибірки), так і повноти (частки загального числа стеганогам, що були виявлені в тестовій вибірці) роботи СД [144]:

$$F_1 = \frac{2 \cdot P_{TP}}{2 \cdot P_{TP} + P_{FP} + P_{FN}}, \quad (1.27)$$

де P_{TP} – імовірність правильної класифікації стеганогам. Значення показника F_1 змінюється від 0 (відповідає випадку віднесення ЗК до класу стеганогам та навпаки) до 1 (правильне віднесення ЗК та стеганогам до відповідних класів).

Коефіцієнт кореляції Метьюса MCC використовується для оцінки ступеня кореляції вихідних значень СД та відповідних (істинних) міток класів досліджуваних ЦЗ [203]:

$$MCC = \frac{P_{TP} \times P_{TN} - P_{FP} \times P_{FN}}{\sqrt{(P_{TP} + P_{FP}) \cdot (P_{TP} + P_{FN}) \cdot (P_{TN} + P_{FP}) \cdot (P_{TN} + P_{FN})}}, \quad (1.28)$$

де P_{TN} – імовірність правильної класифікації ЗК. Значення коефіцієнту MCC змінюється від (-1) , що відповідає випадку хибного віднесення стеганогам

до класу ЗК та навпаки, до (+1), що відповідає правильній класифікації як стеганограм, так і зображень-контейнерів. Особливим випадком є значення $MCC = 0$, що відповідає випадку віднесення досліджуваного зображення до класів стеганограм або ЗК випадковим чином ($P_{FN} = P_{FP}$).

При проведенні досліджень розглянуто сучасні підходи до побудови стегодетекторів для цифрових зображень, а саме:

1. Використання поширених методів попередньої обробки ЦЗ з метою виявлення слабких змін статистичних параметрів ЗК, обумовлених вбудовуванням стегоданих – розглянуто випадок використання методів зниження впливу шумів на рівні котрих проводиться прихованням повідомлень, зокрема медіанного фільтру та фільтру Вінера;
2. Застосування статистичних моделей ЗК – заснованих на використанні ансамблю ФВЧ для підвищення точності виявлення слабких змін ЗК, обумовлених прихованням повідомлень, на прикладі застосування сучасної статистичної моделі `maxSRMd2` [177];
3. Побудова СД з використанням новітніх типів ШНМ – зокрема з використанням згорткової нейронної мережі `GB-Ras` [44] та гібридної мережі `ASSAF` [127], для виявлення стеганограм, сформованих згідно АСМ.

Дослідження проводилося з використання персонального комп'ютера з процесором Intel Core i7-3930K (3.20 ГГц), 32 ГБ оперативної пам'яті, відеокарти GeForce RTX 2080 Super (CUDA SDK версії 10.2). Зважаючи на високу складність налаштування СД, частина обчислень проводилася з використання обчислювальних ресурсів кластеру КПІ (10 обчислювальних вузлів). Загальна тривалість обробки пакетів зображень та стеганограм склала 2.5 місяці неперервної роботи комп'ютера. Результати дослідження роботи СД при використанні даних методів наведені в наступних розділах.

1.4.2 Порівняльний аналіз точності виявлення стеганограм при варіації типу методів попередньої обробки цифрових зображень

Особливістю сучасних стеганографічних методів є мінімізація змін статистичних параметрів ЗК в процесу вбудовування стегоданих [147]. Це досягається за рахунок адаптивного вибору пікселів ЗК для приховання бітів стегоданих [9] – визначення груп пікселів зображення-контейнеру зміна яскравості котрих призводить до найменших змін статистичних параметрів контейнеру. Для виявлення даних локальних змін (збурень) значень яскравості пікселів ЦЗ широко використовуються методи адаптивної фільтрації ЦЗ, зокрема фільтрів на основі рангових статистик (наприклад, медіанний фільтр) та фільтру Вінера [76,141,204]. Відмітимо, що в літературі відсутні відомості щодо ефективності використання даних методів для виявлення стеганограм, сформованих згідно новітніх стеганографічних методів, зокрема MG [152] та MiPOD [153]. Тому становить інтерес порівняльний аналіз точності роботи СД при використанні даних методів попередньої обробки ЦЗ для виявлення стеганограм, сформованих згідно АСМ.

Обробка ЦЗ з використанням медіанного фільтру проводиться з використанням ковзного вікна η розміром $w_M \times w_M$ (пікселів) в декілька етапів [141,204]. На першому етапі, відбувається ранжування значень яскравості пікселів в межах поточного положення КВ. На другому етапі проводиться оцінка вихідного значення яскравості центрального пікселю для даного положення КВ з використанням медіани отриманого розподілу значень яскравості пікселів в межах ковзного вікна. Медіанний фільтр дозволяє суттєво зменшувати вплив локальних змін яскравості пікселів ЗК за умови рівномірного розподілу шумів по всьому зображенню.

Для підвищення точності виявлення слабких змін значень яскравості пікселів ЦЗ, обумовлених використанням АСМ, широко використовується фільтр Вінера [76]. Особливістю даного фільтру є визначення оптимальних

параметрів фільтрації для кожного положення КВ за критерієм мінімізації впливу адитивного шуму [141].

Обробка напівтонового зображення \mathbf{I} розмірами $N \times M$ (пікселів) з використанням ФВ проводиться з використанням ковзного вікна η розміром $w_W \times w_W$ (пікселів). Оцінка значення яскравості центрального пікселя $\hat{\mathbf{I}}_{x,y}$ для поточного положення КВ проводиться згідно наступних формул [198]:

$$\hat{\mathbf{I}}_{x,y} = \mu + \frac{\sigma^2 - \nu^2}{\sigma^2} \cdot (\mathbf{I}_{x,y} - \mu),$$

$$\mu = \frac{1}{NM} \sum_{x,y \in \eta} \mathbf{I}_{x,y}, \sigma^2 = \frac{1}{NM} \sum_{x,y \in \eta} (\mathbf{I}_{x,y}^2 - \mu^2),$$

де μ та σ^2 є оцінками середнього значення та дисперсії значень яскравості пікселів зображення \mathbf{I} в межах поточного положення КВ.

Розмір медіанного та вінеровського фільтру при обробці тестових ЦЗ змінювався в наступному діапазоні – 3×3 , 5×5 , 7×7 , 9×9 та 11×11 пікселів. Для оцінки статистичних параметрів оброблених зображень після застосування розглянутих методів фільтрації була використана стандартна статистична модель SPAM [38]. Дана модель заснована на використанні математичного апарату марковських ланцюгів для моделювання кореляції значень суміжних елементів оброблюваного ЦЗ.

Зазначимо, що проведення попередньої обробки ЦЗ дозволяє виявляти та досліджувати зміни статистичних параметрів ЗК, обумовлені прихованням повідомлень. Відповідно, налаштування СД можливо проводити з використанням двох підходів – статистичних параметрів \mathbf{F}_{calib} , обчислених лише для оброблених ЦЗ, а також об'єднання статистичних параметрів \mathbf{F}_{CC} для вихідних та оброблених цифрових зображень. Це дозволяє гнучко обирати тип використовуваних параметрів ЦЗ для мінімізації значення помилки класифікації стеганограм P_E (1.25).

Залежність значення помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими та розміру медіанного фільтру для стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD при використанні \mathbf{F}_{calib}

SPAM-ознак для пакету зображень ALASKA ($K_\alpha^{OL} = 0\%$) наведені на рис. 1.12.

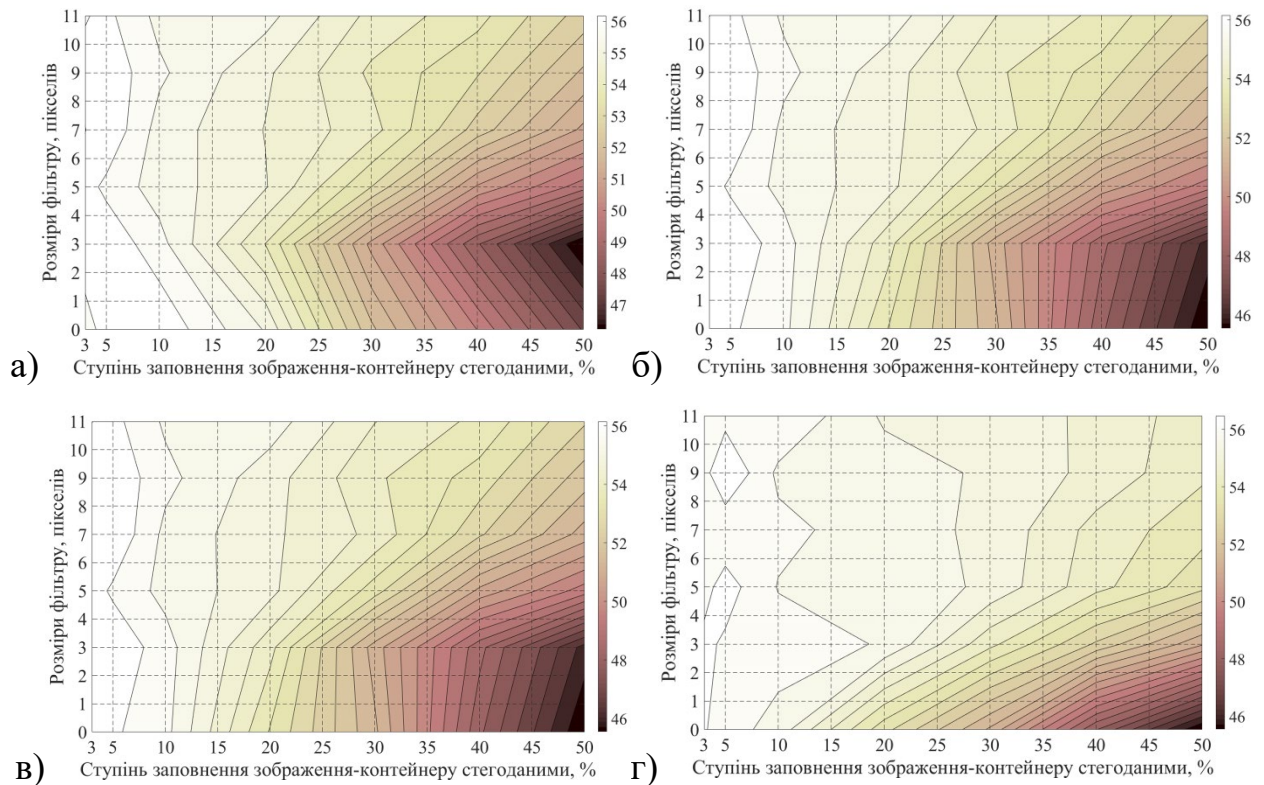


Рисунок 1.12 – Залежність помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими та розміру медіанного фільтру для стеганографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD.

Результати наведено для випадку використання F_{calib} SPAM-ознак для пакету зображень ALASKA ($K_\alpha^{OL} = 0\%$), розмір фільтру рівний «0» пікселів відповідає випадку обробки вихідного ЦЗ.

Використання медіанної фільтрації дозволяє знизити помилку виявлення стеганограм P_E для стеганографічних методів HUGO (до 2%, рис. 1.12а) та S-UNIWARD (до 1.5%, рис. 1.12б) у порівнянні з випадком аналізу необроблених ЦЗ при середньому ($10\% \leq \Delta_\alpha^S \leq 20\%$) та сильному ($\Delta_\alpha^S > 20\%$) ступені заповнення ЗК стегоданими. При цьому найбільша точність виявлення стеганограм досягається при використанні медіанного фільтру з КВ відносно малого розміру ($w_M = 3$ пікселі), а подальше зростання розміру ковзного вікна практично не впливає на зміни значень P_E .

У випадку обробки стеганограм, сформованих згідно стеганографічних методів MG (рис. 1.12в) та MiPOD (рис. 1.12г) застосування медіанного фільтру призводить до підвищення помилки виявлення стеганограм. Це може бути пояснено «агресивним» характером даного фільтру – зниження рівня зашумленості ЦЗ за рахунок внесення змін до більшості текстурних областей оброблюваного зображення. При цьому зазнають спотворень як групи пікселів, використаних для приховання стегоданих, так і власні шуми ЦЗ.

Для порівняння на рис. 1.13 наведено залежність помилки виявлення P_E від ступеня заповнення ЗК стегоданими та розміру вінеровського фільтру для стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD при використанні \mathbf{F}_{calib} SPAM-ознак для пакету зображень ALASKA ($K_\alpha^{OL} = 0\%$).

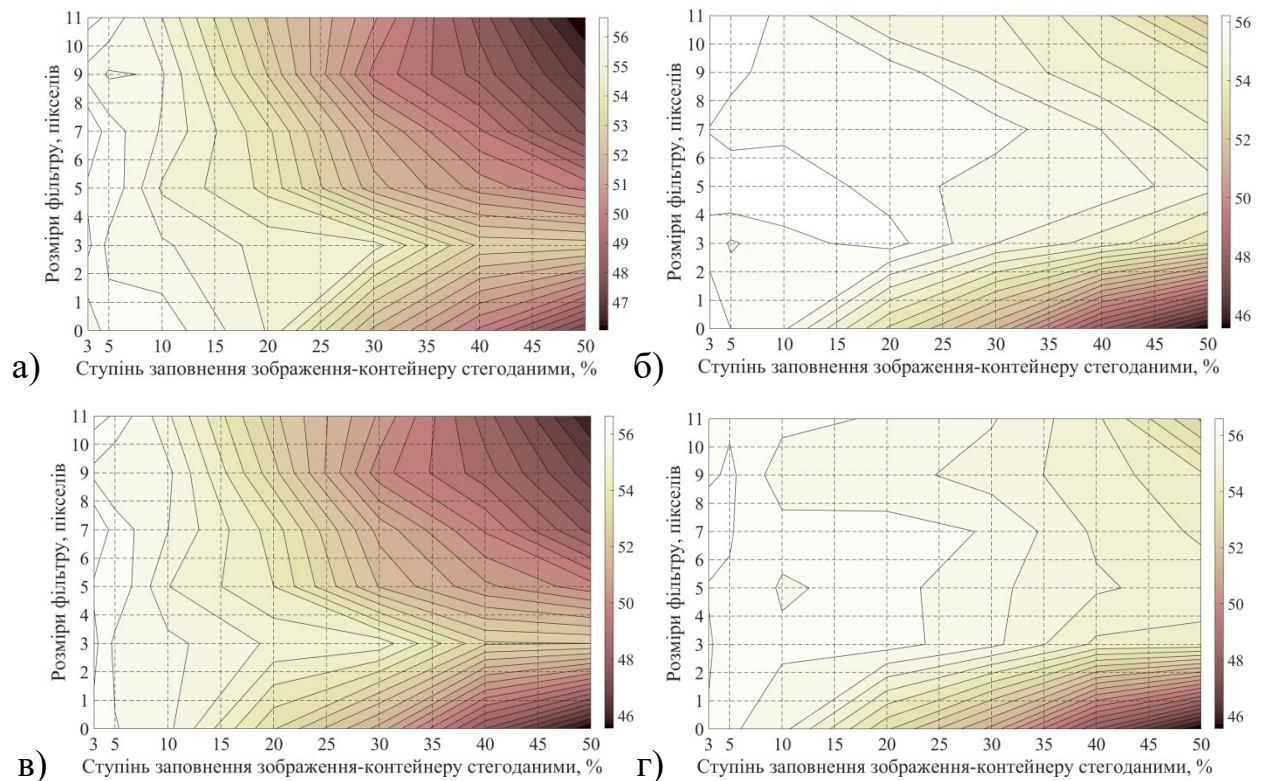


Рисунок 1.13 – Залежність помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими та розміру вінеровського фільтру для стеганографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для випадку використання \mathbf{F}_{calib} SPAM-ознак для пакету зображень ALASKA ($K_\alpha^{OL} = 0\%$), розмір фільтру рівний «0» пікселів відповідає випадку обробки вихідного ЦЗ.

Застосування ФВ для попередньої обробки стеганограм, сформованих згідно стеганографічних методів S-UNIWARD (рис. 1.13б) та MiPOD (рис. 1.13г) призводить до суттєвого зростання значень P_E в області середнього та сильного ступеня заповнення ЗК стегоданими. Це пояснюється ефективним придушення адитивних завад даним фільтром – зниження впливу локальних збурень значень яскравості пікселів ЗК, обумовлених як прихованням повідомлень, так і власних шумів цифрового зображення.

З іншого боку, для стеганографічних методів HUGO (рис. 1.13а) та MG (рис. 1.13в) отримано попередньо неочікувані результати – використання ФВ з ковзним вікном малого розміру ($w_W = 3$ пікселя) призводить до суттєвого зростання значень помилки виявлення стеганограм P_E , в той час як використання КВ більшого розміру практично не впливає на точність виявлення стеганограм. Виявлений ефект може бути пояснений збільшенням впливу яскравості суміжних пікселів при зростанні розміру КВ, що дозволяє «маскувати» локальні збурення значень яскравості пікселів ЦЗ, обумовлені прихованням повідомлень.

Відмітимо, що додаткове підвищення точності виявлення стеганограм може бути досягнуто за рахунок налаштування СД з використанням статистичних параметрів як вихідного, так і обробленого (фільтрованого) ЦЗ. Тому становить інтерес дослідження точності виявлення стеганограм при використанні вектору \mathbf{F}_{CC} , що відповідає об'єднанню наведених характеристик досліджуваних ЦЗ. Залежність помилки виявлення P_E від ступеня заповнення ЗК стегоданими та розміру медіанного фільтру для стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD при використанні \mathbf{F}_{CC} SPAM-ознак для пакету зображень ALASKA ($K_\alpha^{OL} = 0\%$) наведені на рис. 1.14.

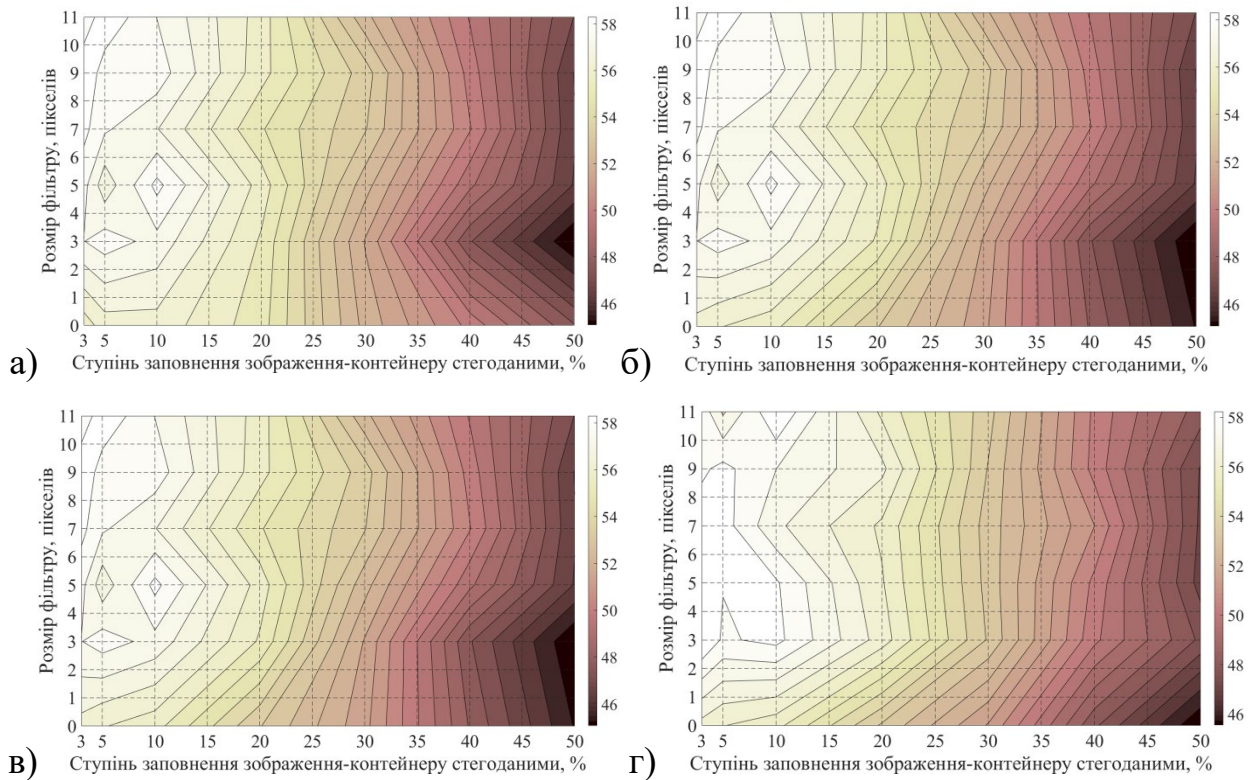


Рисунок 1.14 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими та розміру медіанного фільтру для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD.

Результати наведено для випадку використання F_{CC} SPAM-ознак для пакету зображень ALASKA ($K_{\alpha}^{OL} = 0\%$), розмір фільтру рівний «0» пікселів відповідає випадку обробки вихідного ЦЗ.

Використання F_{CC} SPAM-ознак дозволяє знизити помилку виявлення стегограм в області сильного заповнення ЗК стегоданими ($\Delta_{\alpha}^S \geq 20\%$) до 4% для методу HUGO (рис. 1.14а), та до 2% для методів S-UNIWARD (рис. 1.14б) та MG (рис. 1.14в) у порівнянні з випадком використання вихідних ЦЗ. З іншого боку, використання F_{CC} SPAM-ознак для методу MiPOD (рис. 1.14г) призводить до підвищення значень помилки виявлення стегограм P_E у всьому діапазоні значень ступеня заповнення ЗК стегоданими. Варто зазначити, що виявлені зміни значень точності виявлення стегограм досягається за рахунок подвоєння кількості елементів SPAM-ознак (ознак вихідного та обробленого ЦЗ), що підвищує вимоги щодо об'єму навчальної вибірки зображень та, відповідно, складність налаштування СД.

Для порівняння, на рис. 1.15 наведено залежність помилки виявлення P_E від ступеня заповнення ЗК стегоданими та розміру вінеровського фільтру для стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD при використанні F_{CC} SPAM-ознак для пакету зображень ALASKA ($K_\alpha^{OL} = 0\%$).

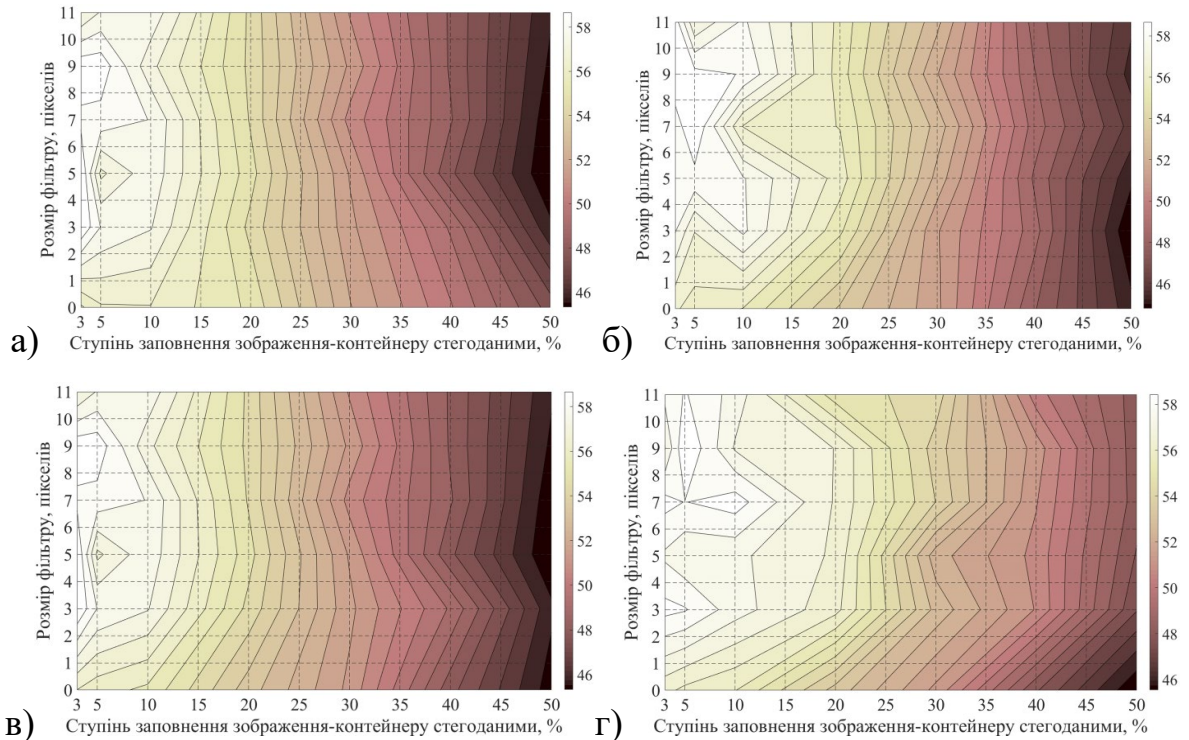


Рисунок 1.15 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими та розміру вінеровського фільтру для стеганографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для випадку використання F_{CC} SPAM-ознак для пакету зображень ALASKA ($K_\alpha^{OL} = 0\%$), розмір фільтру рівний «0» пікселів відповідає випадку обробки вихідного ЦЗ.

На відміну від випадку використання медіанної фільтрації (рис. 1.14), попередня обробка досліджуваних ЦЗ з використанням ФВ призводить до зниження точності виявлення стегограм для F_{CC} SPAM-ознак (рис. 1.15). При цьому, зростання значень P_E виявлено для стеганографічного методу MiPOD (до 4%, рис. 1.14г), в той час як для інших розглянутих методів (рис. 1.15а-в) зростання значень P_E є несуттєвим (до 1%-2%).

Таким чином, можемо зробити висновок, що використання медіанного фільтру та F_{CC} SPAM-ознак дозволяє підвищити точність виявлення стегано-

грам у порівнянні з випадком використання фільтру Вінера для попередньої обробки ЦЗ та F_{calib} SPAM-ознак. Тому становить інтерес використання даних методів попередньої обробки ЦЗ та F_{CC} SPAM-ознак для виявлення стеганограм, сформованих з використанням тестових зображень з пакетів VISION та MIRFlickr. Залежність помилки виявлення P_E від ступеня заповнення ЗК стегоданими та розміру медіанного фільтру для стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD при використанні F_{CC} SPAM-ознак для пакетів зображень VISION та MIRFlickr ($K_{\alpha}^{OL} = 0\%$) наведені на рис. 1.16-1.17.

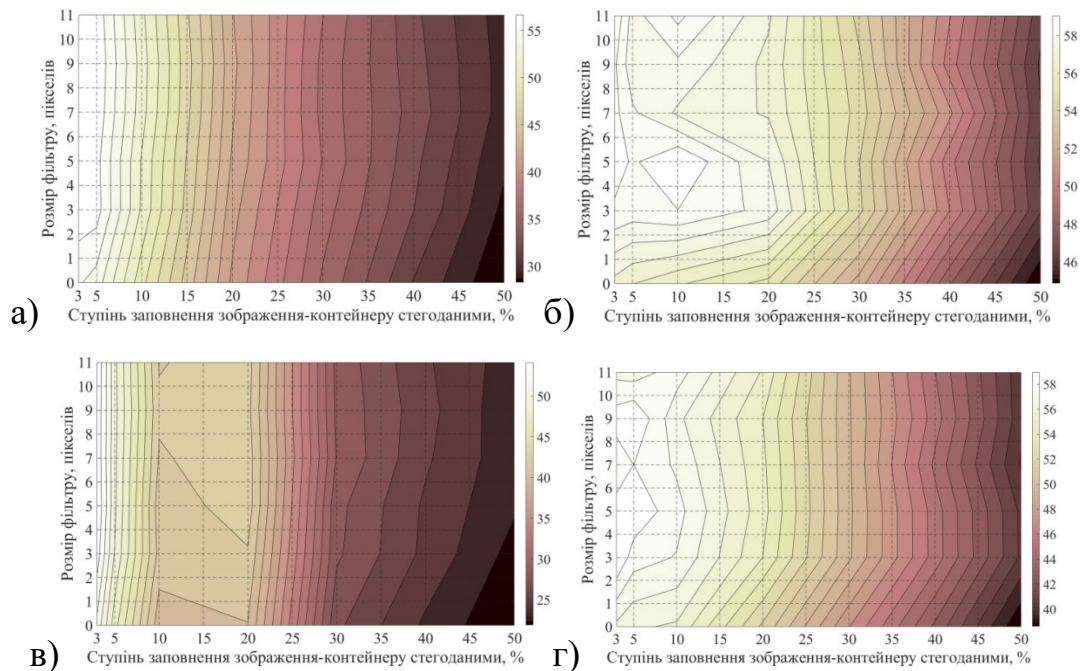


Рисунок 1.16 – Залежність помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими та розміру медіанного фільтру для стеганографічних методів: (а-б) – HUGO; (в-г) – S-UNIWARD. Результати наведені при використанні F_{CC} SPAM-ознак ($K_{\alpha}^{OL} = 0\%$) для пакетів зображень VISION (а, в) та MIRFlickr (б, г), розмір фільтру рівний «0» пікселів відповідає випадку обробки вихідного ЦЗ.

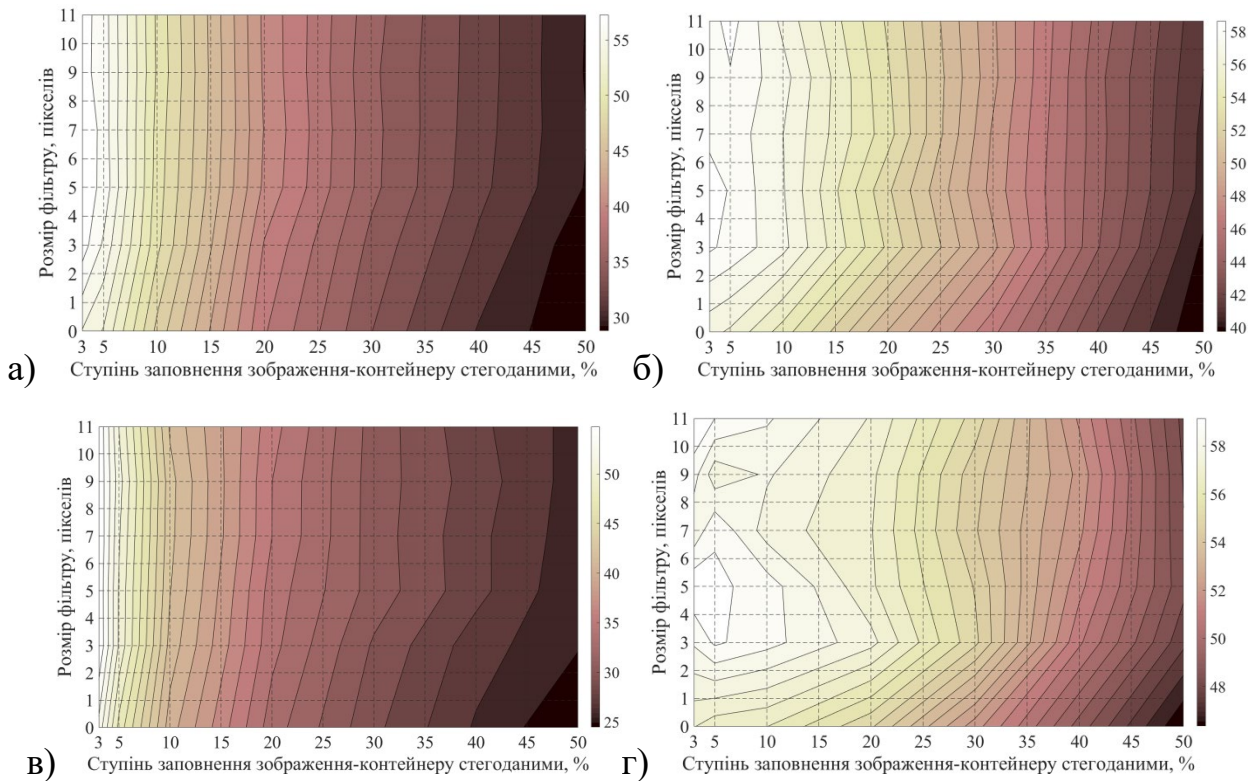


Рисунок 1.17 – Залежність помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими та розміру медіанного фільтру для стеганографічних методів: (а-б) – MG; (в-г) – MiPOD. Результати наведені при використанні F_{CC} SPAM-ознак ($K_{\alpha}^{OL} = 0\%$) для пакетів зображень VISION (а, в) та MIRFlickr (б, г), розмір фільтру рівний «0» пікселів відповідає випадку обробки вихідного (необробленого) ЦЗ.

Відмітимо, що значення помилки P_E практично не змінюються в області слабкого ($\Delta_{\alpha}^S < 10\%$) та середнього ($\Delta_{\alpha}^S \in [10\%; 20\%]$) ступеня заповнення ЗК стегоданими для досліджуваних стеганографічних методів на пакеті VISION (рис. 1.16-1.17). При цьому зміни значень P_E в області сильного заповнення ЗК стегоданими ($\Delta_{\alpha}^S > 20\%$) не перевищують 1.25% для методу HUGO (рис. 1.16а), та 2.00% для інших стеганографічних методів. Це свідчить про несуттєвий вплив розглянутих методів фільтрації ЦЗ у випадку, коли відносно мала частка пікселів ЦЗ використовується для приховання повідомлень ($\Delta_{\alpha}^S \leq 20\%$). Відповідно, приховання повідомлень «маскується» у власних шумах ЗК, що знижує ефективність роботи досліджуваних методів обробки ЦЗ. При зростанні ступеня заповнення ЗК, застосування розглянутих

методів фільтрації призводить до зменшення відмінностей між результатами обробки ЗК та стеганограми. Це підтверджується результатами для методів S-UNIWARD (рис. 1.16в), MG (рис. 1.17а) та MiPOD (рис. 1.17в).

З іншого боку, застосування медіанної фільтрації для попередньої обробки стеганограм, сформованих з використанням зображень з пакету MIRFlickr, призводить до зростання помилки виявлення стеганограм P_E (рис. 1.16-1.17) навіть в області сильного заповнення ЗК стегоданими. Величина зростання значень P_E суттєво варіюється для кожного методу – від 2% для методу S-UNIWARD (рис. 1.16г) до 5% для методу MiPOD (рис. 1.17г). Це може пояснено суттєвими відмінностями у рівні власних шумів ЦЗ для даних пакетів зображень – зображення з пакету MIRFlickr-1M характеризуються більшим рівнем шумів, що призводить до зростання впливу роботи розглянутих фільтрів у порівнянні з пакетом ALASKA (рис. 1.11).

Таким чином, можемо зробити висновок, що використання поширених методів фільтрації для попередньої обробки стеганограм, сформованих згідно АСМ, дозволяє підвищити точність виявлення стеганограм при обробці високоякісних зображень, що характеризуються відносно малим рівнем власних завад. Обробка ЦЗ з високим рівнем власних завад призводить до зниження ефективності даних методів попередньої обробки досліджуваних зображень у порівнянні з випадком аналізу вихідних ЦЗ. Це обумовлює актуальність та важливість проблеми пошуку методів попередньої обробки ЦЗ, здатних підвищити точність виявлення незначних відмінностей між статистичними параметрами ЗК та стеганограм.

1.4.3 Оцінка точності виявлення стеганограм при використанні стегодетекторів на основі статистичних моделей цифрових зображень

В роботі досліджено випадок використання як стандартних, зокрема модель SPAM [38], так і новітніх, а саме модель maxSRMd2 [177], статистичних моделей ЦЗ. Дані моделі засновані на використанні математичного

апарату марківських ланцюгів для дослідження змін яскравості суміжних пікселів ЗК, обумовлених прихованням повідомлень.

Особливістю моделі $\max\text{SRMd2}$ є використання ансамблю ФВЧ для виділення шумових складових досліджуваного ЦЗ, на рівні котрих, зазвичай, проводиться приховання повідомлень. На відміну від моделі SRM, ансамбль ФВЧ для моделі $\max\text{SRMd2}$ включає додаткові типи фільтрів, що дозволяє підвищити точність виявлення слабких змін ЗК, обумовлених прихованням повідомлень згідно ACM [177]. Для дослідження впливу використання ансамблю ФВЧ в моделі $\max\text{SRMd2}$ на точність роботи СД був розглянутий випадок використання лише окремого фільтру типу EDGE при обробці ЦЗ. Згідно досліджень [177], даний тип ФВЧ має найбільший вплив на точність виявлення стегограм при використанні моделі $\max\text{SRMd2}$, в той час як внесок інших типів використовуваних ФВЧ є суттєво меншим. Процедура визначення параметрів статистичної моделі $\max\text{SRMd2}$ є аналогічною до відповідної процедури для моделі SRM [34].

Дослідження точності роботи СД на основі розглянутих статистичних моделей ЦЗ проводилося в декілька етапів. На першому етапі розглянуто випадок аналізу стегограм, сформованих з використанням ЗК зі стандартного пакету ALASKA при варіації значення показника K_{α}^{OL} (1.25) від 0% до 100%.

Залежність значень помилки класифікації P_E від ступеня заповнення ЗК стегоданими при налаштуванні СД з використанням статистичних моделей SPAM та $\max\text{SRMd2}$ для стегограм, сформованих згідно розглянутих ACM, для бази даних ALASKA наведено на рис. 1.18.

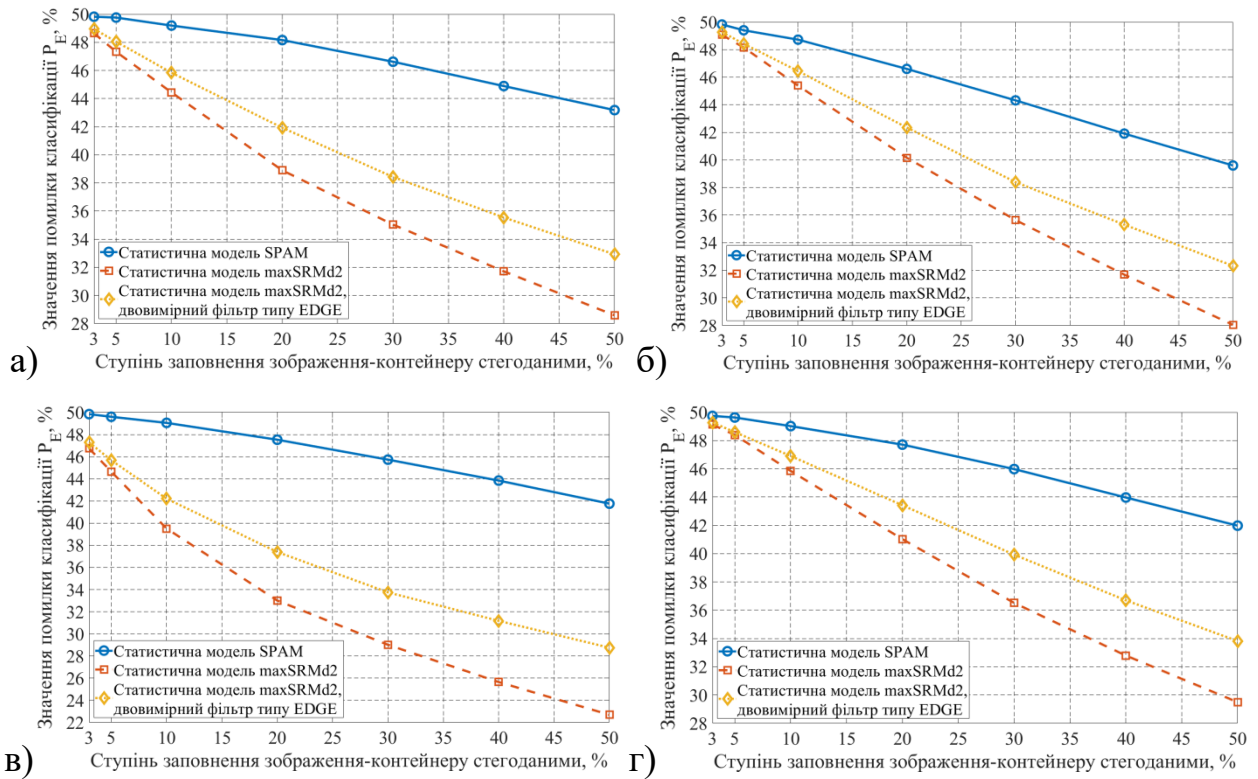


Рисунок 1.18 – Залежність значень помилки виявлення стегонограм P_E від ступеня заповнення ЗК стегоданими при використанні статистичних моделей SPAM та maxSRMd2 для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для бази даних ALASKA та випадку $K_{\alpha}^{OL} = 100\%$.

Використання статистичної моделі maxSRMd2 дозволяє суттєво (на 20%) зменшити значення помилки P_E у порівнянні з випадком використання моделі SPAM (рис. 1.18). При цьому зниження значень P_E досягається лише в області сильного заповнення ЗК стегоданими ($\Delta_{\alpha}^S > 20\%$), в той час як для області слабого заповнення ($\Delta_{\alpha}^S < 10\%$) використання розглянутих статистичних моделей призводить до співставної точності виявлення стегонограм. Це свідчить про обмежені можливості як стандартних, так і новітніх статистичних моделей ЦЗ щодо надійного виявлення слабких спотворень ЗК, обумовлені прихованням повідомлень згідно сучасних АСМ, в найбільш складному випадку стегоаналізу ЦЗ, а саме слабого заповнення ЗК стегоданими.

За результатами аналізу отриманих даних (рис. 1.18) встановлено, що використання ансамблю ФВЧ в моделі maxSRMd2 дозволяє зменшити значе-

ння помилки P_E до 6% у порівнянні з випадком використання лише одного фільтру EDGE. При цьому найбільший вигравш в точності роботи СД досягається в області сильного заповнення ЗК стегоданими ($\Delta_\alpha^S > 20\%$), а в області слабого заповнення ($\Delta_\alpha^S < 10\%$) відмінності в точності роботи СД для даних випадків практично відсутні. Отримані результати підтверджують зроблені раніше висновки щодо екстенсивного характеру сучасних методів підвищення точності роботи СД, а саме суттєвого зростання кількості методів попередньої обробки ЦЗ. При цьому дані методи дозволяють підвищувати точність роботи СД лише в області середнього ($10\% \leq \Delta_\alpha^S \leq 20\%$) та сильного ($\Delta_\alpha^S > 20\%$) заповнення ЗК стегоданими. Це підтверджує актуальність задачі розробки високоточних СД, здатних працювати в умовах слабого ($\Delta_\alpha^S < 10\%$) заповнення ЗК стегоданими.

Відмітимо, що отримані результати (рис. 1.18) відповідають випадку, коли стегоаналітик має доступ до СК та може формувати стеганограми для довільного ЗК ($K_\alpha^{OL} = 100\%$). Проте в більшості реальних випадків проведення стегоаналізу дана можливість є відсутньою, внаслідок чого становить інтерес подальше дослідження точності роботи СД при обмеженості апріорних даних щодо використаного стеганографічного методу. Залежність значення помилки P_E від ступеня заповнення ЗК стегоданими при налаштуванні СД з використанням статистичних моделей SPAM та maxSRMd2 для стеганограм, сформованих згідно розглянутих АСМ, для бази даних ALASKA та $K_\alpha^{OL} = 0\%$ наведено на рис. 1.19.

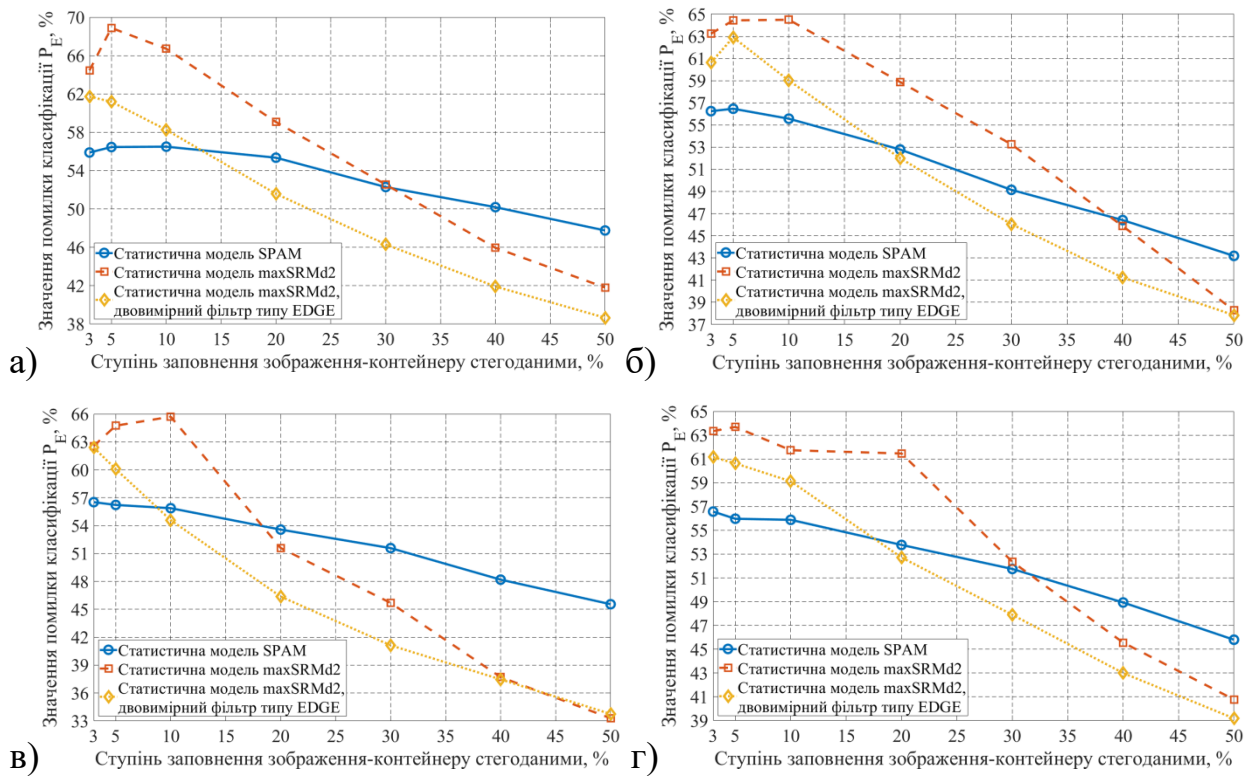


Рисунок 1.19 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими при використанні статистичних моделей SPAM та maxSRMd2 для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для бази даних ALASKA та випадку $K_\alpha^{OL} = 0\%$.

За результатами тестування СД були отримані попередньо неочікувані результати, а саме суттєве підвищення значень помилки P_E при використанні статистичної моделі maxSRMd2 – від 48% для випадку $K_\alpha^{OL} = 100\%$ (рис. 1.18), до 65% для випадку $K_\alpha^{OL} = 0\%$ (рис. 1.19) в області слабого ступеня заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$). При цьому використання лише окремого ФВЧ типу EDGE при проведенні попередньої обробки досліджуваних зображень (рис. 1.19) дозволяє несуттєво зменшити значення помилки P_E ($\Delta P_E \cong 6\%$) у порівнянні з випадком використання всього ансамблю ФВЧ. Це свідчить про низьку ефективність (надлишковість) використання декількох типів ФВЧ для виявлення спотворень ЗК, обумовлених прихованням повідомлень.

Особливий теоретичний та практичний інтерес становлять результати для СД на основі стандартної статистичної моделі SPAM (рис. 1.19) – відсутність етапу попередньої обробки ЦЗ дозволяє зменшити значення помилки P_E ($\Delta P_E \cong 8\%$) при використанні даної моделі у порівнянні з потужною статистичною моделлю maxSRMd2 в найбільш складному випадку слабого заповнення ЗК стегоданими ($\Delta\alpha^S < 10\%$). При зростанні ступеня заповнення ЗК стегоданими відмінності в значеннях помилки P_E для розглянутих статистичних моделей практично нівелюються, а в області сильного заповнення ЗК стегоданими ($\Delta\alpha^S > 20\%$) використання статистичної моделі maxSRMd2 дозволяє суттєво зменшити значення P_E .

Отримані результати свідчать про вагомі обмеження застосування сучасних статистичних моделей ЦЗ, заснованих на обробці ЦЗ з використанням ансамблю ФВЧ, в реальних випадках, коли інформація щодо використаного стеганографічного методу є обмеженою або навіть відсутньою. Тому особливий інтерес становить аналіз точності досліджуваних методів стегоаналізу саме в даному випадку. Внаслідок цього подальші результати досліджень наведені для випадку $K_\alpha^{OL} = 0\%$, а значення точності роботи СД при варіації значення параметру K_α^{OL} наведені у додатках до роботи.

Варто зазначити, що залежності помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими (рис. 1.18-1.19) отримані для випадку обробки високоякісних ЦЗ зі стандартного пакету ALASKA. Тому на другому етапі досліджень проведено аналіз точності роботи СД при обробці реальних зображень, що характеризуються значною варіативністю статистичних та спектральних параметрів. Залежність помилки класифікації P_E від ступеня заповнення ЗК стегоданими при налаштуванні СД з використанням статистичних моделей SPAM та maxSRMd2 для виявлення стеганограм, сформованих згідно розглянутих ACM, при $K_\alpha^{OL} = 0\%$ для пакетів VISION та MIR-Flickr наведено на рис. 1.20-1.21.

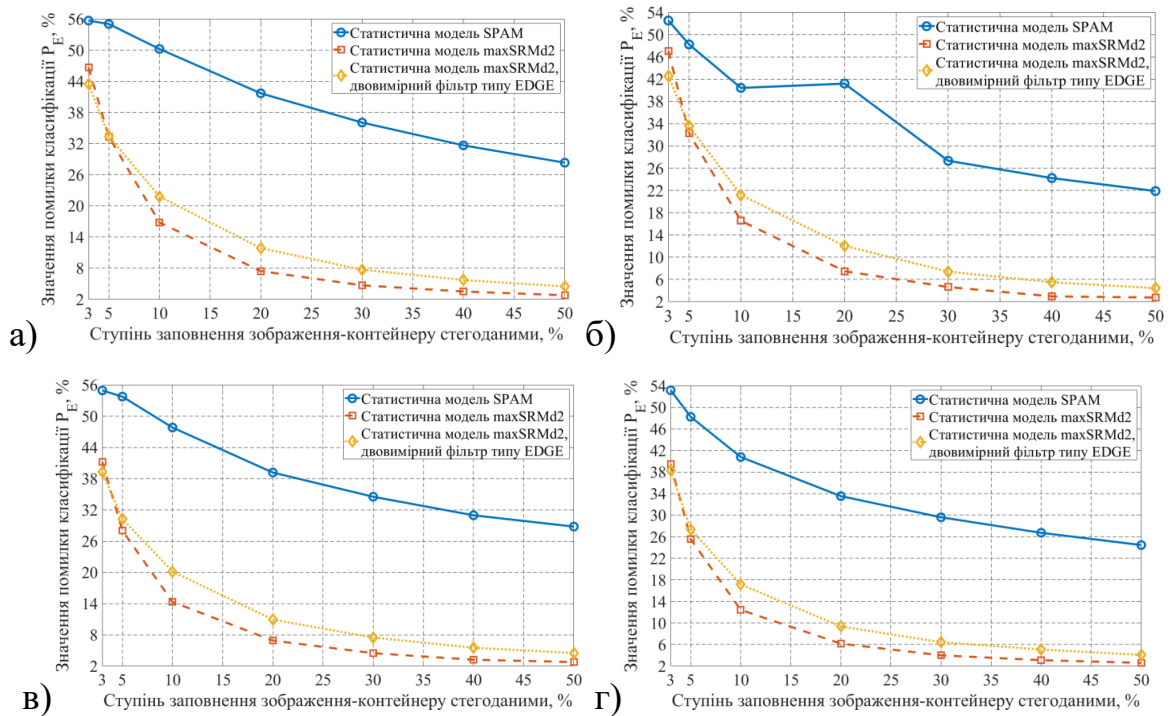


Рисунок 1.20 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими при використанні статистичних моделей SPAM та maxSRMd2 для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для бази даних VISION та випадку $K_\alpha^{OL} = 0\%$.

Отримані результати для зображень з пакету VISION (рис. 1.20) підтверджують зроблені раніше припущення, щодо суттєвого зростання точності роботи СД при обробці зображень з відносно малим рівнем адитивних шумів (рис. 1.19). При цьому використання статистичної моделі maxSRMd2 дозволяє мінімізувати значення помилки P_E ($P_E \cong 2\%$) в області сильного заповнення ЗК стегоданими ($\Delta_\alpha^S > 20\%$) для розглянутих АСМ.

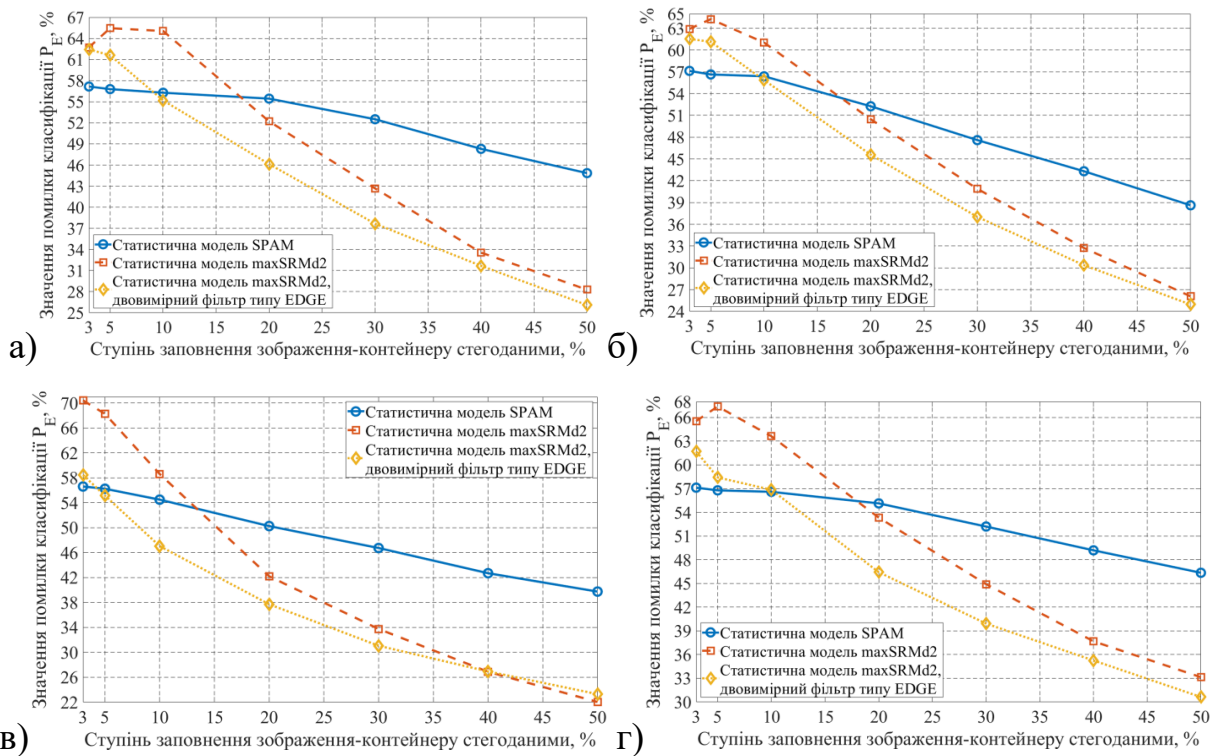


Рисунок 1.21 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими при використанні статистичних моделей SPAM та maxSRMd2 для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для бази даних MIRFlickr та випадку $K_\alpha^{OL} = 0\%$.

З іншого боку, формування стегограм з використанням ЦЗ з пакету MIRFlickr призводить до суттєвого ($P_E \cong 70\%$) зростання значення помилки виявлення стегограм при використанні статистичної моделі maxSRMd2, зокрема в області слабого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$). При цьому для стандартної моделі SPAM отримано попередньо неочікуваний результат (рис. 1.21) – зменшення значень помилки P_E у порівнянні з моделлю maxSRMd2, що найбільше виявляється при ступені заповнення ЗК стегоданими $\Delta_\alpha^S < 10\%$. Це свідчить про обмеження використання ансамблю ФВЧ для обробки ЦЗ з високим рівнем власних шумів, зокрема щодо виявлення слабких спотворень зображення-контейнеру, обумовлених застосуванням АСМ.

Для порівняння, у табл. 1.1 наведені отримані значення P_E при використанні розглянутих статистичних моделей ЗК та пакетів зображень для ви-

падку використання стеганографічного методу MiPOD. Результати наведені для випадку слабкого ($\Delta_\alpha^S = 3\%$), середнього ($\Delta_\alpha^S = 20\%$) та сильного ($\Delta_\alpha^S = 50\%$) заповнень ЗК стегоданими.

Таблиця 1.1 – Значення помилки P_E при застосуванні статистичних моделей SPAM та maxSRMd2 для виявлення стегограм, сформованих згідно стеганографічного методу MiPOD, при використанні пакетів ALASKA, VISION і MIRFlickr та варіації значень параметру K_α^{OL} .

Ступінь заповнення ЗК стегоданими	Параметр K_α^{OL}	Значення помилки класифікації стегограм P_E , %		
		Модель SPAM	Модель maxSRMd2	Модель maxSRMd2 (EDGE фільтр)
Пакет зображень ALASKA				
$\Delta_\alpha^S = 3\%$	$K_\alpha^{OL} = 0\%$	56.57	63.34	61.15
	$K_\alpha^{OL} = 100\%$	49.74	49.13	49.27
$\Delta_\alpha^S = 20\%$	$K_\alpha^{OL} = 0\%$	53.77	61.45	52.71
	$K_\alpha^{OL} = 100\%$	47.71	41.03	43.42
$\Delta_\alpha^S = 50\%$	$K_\alpha^{OL} = 0\%$	45.80	40.78	39.19
	$K_\alpha^{OL} = 100\%$	41.98	29.50	33.82
Пакет зображень VISION				
$\Delta_\alpha^S = 3\%$	$K_\alpha^{OL} = 0\%$	53.17	39.50	38.28
	$K_\alpha^{OL} = 100\%$	46.13	22.67	30.76
$\Delta_\alpha^S = 20\%$	$K_\alpha^{OL} = 0\%$	33.53	6.17	9.37
	$K_\alpha^{OL} = 100\%$	31.39	3.66	8.03
$\Delta_\alpha^S = 50\%$	$K_\alpha^{OL} = 0\%$	24.46	2.61	4.09
	$K_\alpha^{OL} = 100\%$	23.30	1.43	3.68
Пакет зображень MIRFlickr				
$\Delta_\alpha^S = 3\%$	$K_\alpha^{OL} = 0\%$	48.57	65.55	61.70
	$K_\alpha^{OL} = 100\%$	49.91	48.57	48.75

Продовження табл. 1.1

Ступінь заповнення ЗК стегоданими	Параметр K_{α}^{OL}	Значення помилки класифікації стеганограм P_E , %		
		Модель SPAM	Модель maxSRMd2	Модель maxSRMd2 (EDGE фільтр)
Пакет зображень MIRFlickr				
$\Delta_{\alpha}^S = 20\%$	$K_{\alpha}^{OL} = 0\%$	36.58	53.33	46.42
	$K_{\alpha}^{OL} = 100\%$	48.05	36.58	39.50
$\Delta_{\alpha}^S = 50\%$	$K_{\alpha}^{OL} = 0\%$	22.53	33.15	30.64
	$K_{\alpha}^{OL} = 100\%$	42.14	22.53	27.03

Отримані результати (табл. 1.1) підтверджують суттєве зниження точності роботи СД у випадку обмеженості апріорних даних щодо використаного СМ при використанні сучасних статистичних моделей ЗК – значення помилки класифікації стеганограм P_E сягає 65% для сучасної статистичної моделі maxSRMd2 в найбільш складному випадку стегоаналізу ($\Delta_{\alpha}^S < 10\%$). При цьому використання лише одного (фіксованого) ФВЧ при попередній обробці ЦЗ з використанням моделі maxSRMd2 дозволяє зменшити значення P_E на 5% (табл. 1.1), що свідчить про надлишковість використання ансамблю ФВЧ для проведення обробки ЦЗ.

Виявлений ефект також підтверджують результати для стандартної статистичної моделі SPAM (табл. 1.1), що не заснована на проведенні попередньої обробки ЦЗ – застосування даної моделі дозволяє суттєво ($\Delta P_E = 17\%$) зменшити значення помилки класифікації стеганограм P_E у порівнянні з випадком використання моделі maxSRMd2. Це обумовлює необхідність попереднього відбору ФВЧ для мінімізації помилки виявлення стеганограм, що є нетривіальною та обчислювально складною задачею. Це обумовлює актуальність розробки методів попередньої обробки, що дозволять підвищити точність роботи СД на основі сучасних статистичних моделей у випадку обмеженості апріорних даних щодо використаного СМ.

Враховуючи суттєве підвищення значення помилки P_E при використанні фіксованих ансамблів ФВЧ в сучасних статистичних моделях ЗК, подальший становить інтерес дослідження ефективності використання новітніх ШНМ для підвищення точності роботи стегодетектору.

1.4.4 Оцінка точності виявлення стеганограм при використанні стегодетекторів на основі штучних нейронних мереж

Вагомою перевагою використання ШНМ для побудови СД у порівнянні з випадком застосування статистичних моделей ЗК є властивість «адаптації» параметрів нейронної мережі до характеристик досліджуваних ЦЗ. Це досягається за рахунок визначення оптимальних параметрів ФВЧ у вхідних (згорткових) шарах мережі за критерієм мінімізації помилки P_E в процесі налаштування мережі. Тому становить інтерес дослідження ефективності використання ШНМ для побудови високоточних СД, здатних працювати в умовах обмеженості апріорних даних щодо використаного АСМ.

Для вирішення даної задачі був проведений порівняльний аналіз точності роботи СД на основі статистичних моделей SPAM та maxSRMd2, а також новітньої згорткової нейронної мережі GB-Ras [44]. Згідно рекомендацій [44], при проведенні досліджень використовувалася мережа GB-Ras [205], попередньо налаштована з використанням стеганограм, сформованих згідно стеганографічних методів S-UNIWARD [135] та WOW [206] для пакетів BOWS-2 [133], BOSS [27] та ALASKA [134]. Відмітимо, що налаштування мережі проводилося при фіксованих значень ступеня заповнення ЗК стегоданими – $\Delta_\alpha^S = 20\%$ та $\Delta_\alpha^S = 40\%$. Для порівняння результатів роботи СД на основі мережі GB-Ras, налаштованої при варіації типу СМ та значень параметру Δ_α^S , дані характеристики зазначалися в якості параметрів мережі.

Залежності помилки класифікації P_E від ступеня заповнення ЗК стегоданими при налаштуванні СД з використанням статистичних моделей SPAM та maxSRMd2, а також мережі GB-Ras для виявлення стеганограм, сформова-

них згідно розглянутих АСМ, для пакету ALASKA при $K_{\alpha}^{OL} = 0\%$ наведено на рис. 1.22.

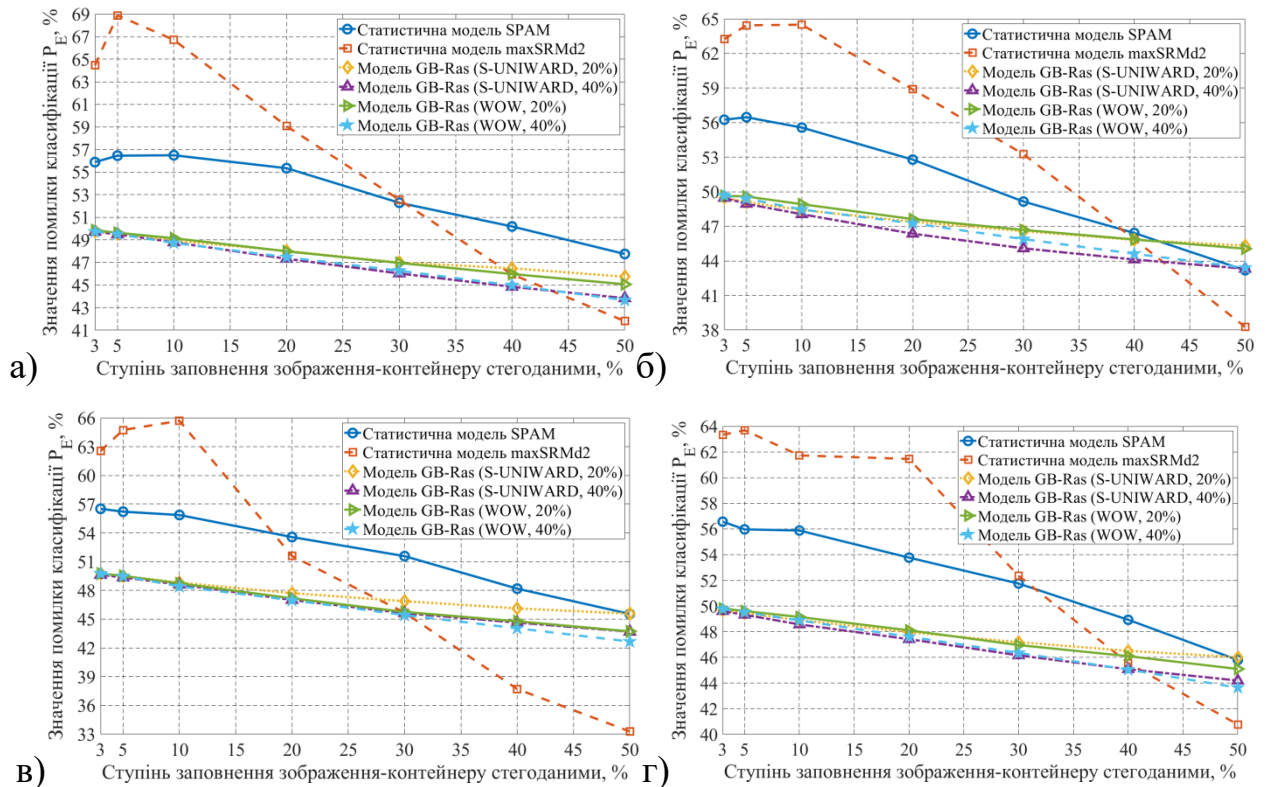


Рисунок 1.22 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими при використанні статистичних моделей SPAM і maxSRMd2, та згорткової нейронної мережі GB-Ras для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для пакету ALASKA та випадку $K_{\alpha}^{OL} = 0\%$.

Використання згорткової мережі GB-Ras дозволяє зменшити значення помилки P_E ($\Delta P_E \cong 7\%$) у порівнянні зі стегодетекторами на основі статистичних моделей ЗК, зокрема в області слабкого ($\Delta_{\alpha}^S < 10\%$) та середнього ($10\% \leq \Delta_{\alpha}^S \leq 20\%$) ступеня заповнення ЗК стегоданими (рис. 1.22). Це свідчить про ефективність використання ЗНМ для підвищення точності роботи СД у випадку обмеженості апріорних даних щодо використаного стегографічного методу ($K_{\alpha}^{OL} = 0\%$).

Відмітимо, що зменшення значень P_E досягається при використанні мережі GB-Ras, налаштованої із застосуванням стегограм, що мають вищий ступінь заповнення (рис. 1.22). При цьому відмінність у значення P_E може

сягати до 2.5% при варіації параметру Δ_{α}^S для стеганограм, використаних для налаштування мережі GB-Ras. Отримані результати можуть бути пояснені суттєвими відмінностями у величині спотворень ЗК, обумовлених формуванням стеганограм з більшим ступенем заповнення ЗК стегоданими. Відповідно, дані відмінності мали більший вплив на зміну параметрів мережі GB-Ras при її налаштуванні.

Зі зростанням ступеня заповнення ЗК стегоданими, точність роботи мережі GB-Ras поступається випадку використання СД на основі статистичної моделі maxSRMd2 (рис. 1.22). Це обумовлено використанням в даній моделі більшої кількості ФВЧ для проведення попередньої обробки ЦЗ, що дозволяє підвищити точність виявлення слабких спотворень ЗК при формуванні стеганограм.

Для порівняння був розглянутий випадок роботи СД на основі мережі GB-Ras на вибірці зображень з пакету VISION. Залежності помилки класифікації P_E від ступеня заповнення ЗК стегоданими при налаштуванні СД з використанням статистичних моделей SPAM та maxSRMd2, а також мережі GB-Ras для виявлення стеганограм, сформованих згідно сучасним АСМ, для пакету VISION при $K_{\alpha}^{OL} = 0\%$ наведено на рис. 1.23.

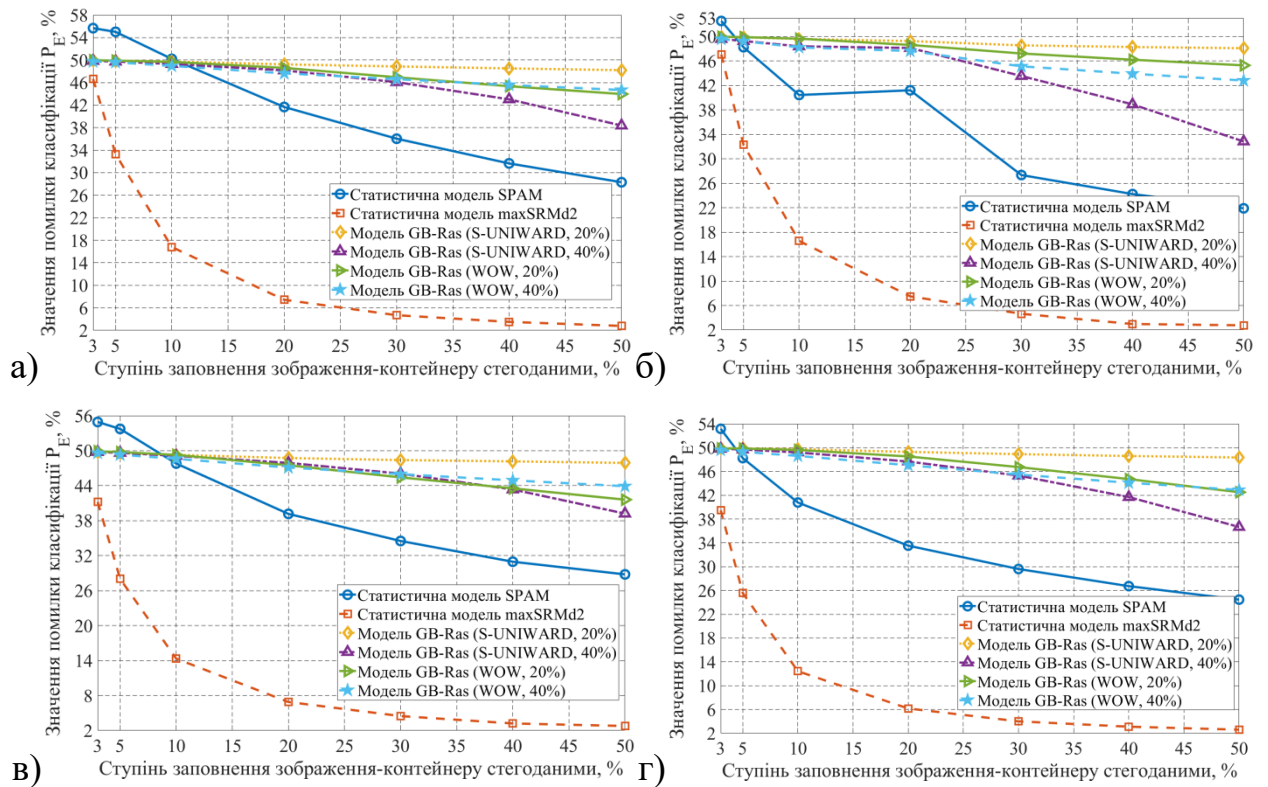


Рисунок 1.23 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими при використанні статистичних моделей SPAM і maxSRMd2, та згорткової нейронної мережі GB-Ras для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для пакету VISION та випадку $K_{\alpha}^{OL} = 0\%$.

Зазначимо, що для моделей GB-Ras були отримані попередньо неочікувані результати (рис. 1.23) – суттєве підвищення значень помилки P_E у порівнянні з розглянутими статистичними моделями (рис. 1.20) в області слабого ($\Delta_{\alpha}^S < 10\%$) та середнього ($10\% \leq \Delta_{\alpha}^S \leq 20\%$) ступеня заповнення ЗК стегоданими. Це може бути пояснено суттєвими відмінностями статистичних параметрів ЦЗ, що використовувалася для налаштування мережі GB-Ras, та зображень з пакету VISION (проблема domain mismatch). Внаслідок цього точність роботи СД на основі мережі GB-Ras лишається порівняно низькою навіть у випадку обробки ЦЗ з малим рівнем адитивних шумів.

Для аналізу точності виявлення стегограм при використанні реальних зображень, що характеризуються високим рівнем адитивних шумів, було проведено тестування СД на основі мережі GB-Ras з використання пакету

MIRFlickr. Залежності помилки класифікації P_E від ступеня заповнення ЗК стегоданими при налаштуванні СД з використанням статистичних моделей SPAM та maxSRMd2, а також мережі GB-Ras для виявлення стегограм, сформованих згідно сучасним ACM, для пакету MIRFlickr при $K_\alpha^{OL} = 0\%$ наведено на рис. 1.24.

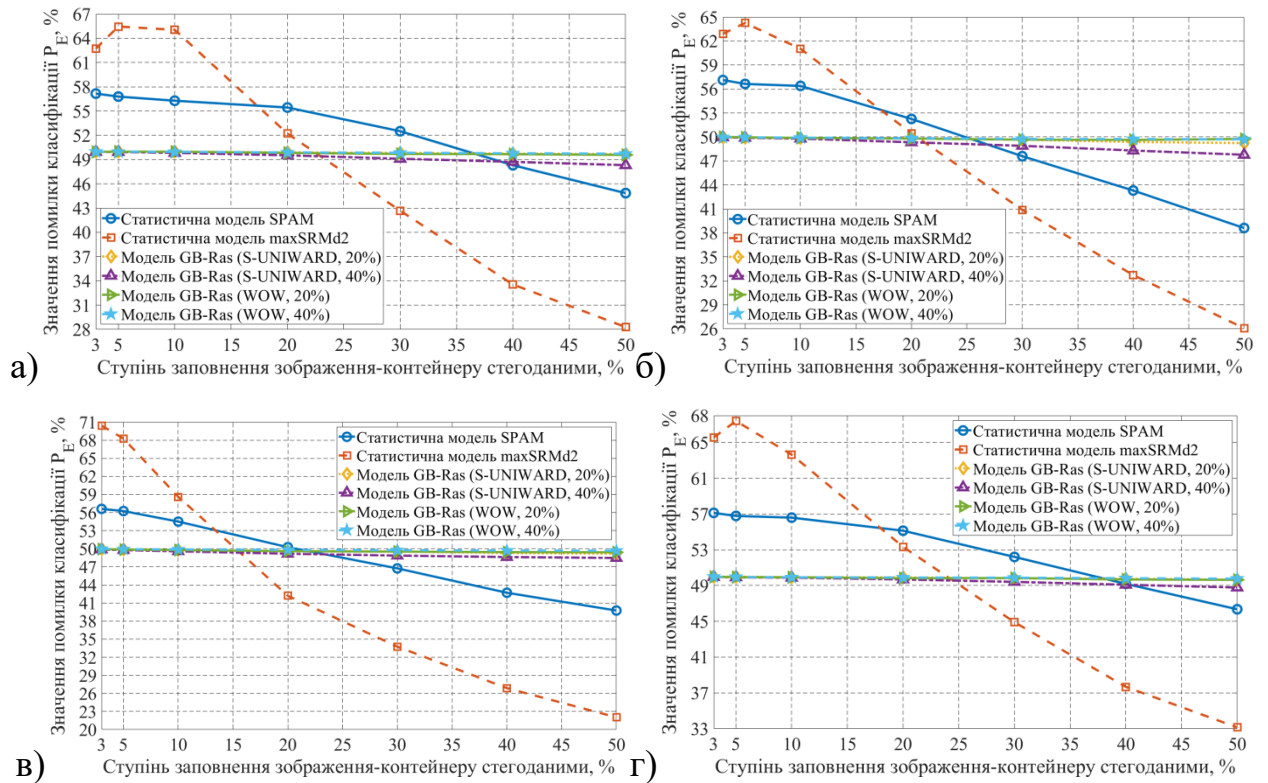


Рисунок 1.24 – Залежність помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими при використанні статистичних моделей SPAM і maxSRMd2, та згорткової нейронної мережі GB-Ras для стегографічних методів: (а) – HUGO, (б) – S-UNIWARD, (в) – MG, (г) – MiPOD. Результати наведено для пакету MIRFlickr та випадку $K_\alpha^{OL} = 0\%$.

Відмітимо збереження негативного впливу проблеми domain mismatch при використанні мережі GB-Ras для обробки тестових зображень з пакету MIRFlickr (рис. 1.24), аналогічно до отриманих раніше результатів для пакету VISION (рис. 1.23). При цьому точність роботи СД на основі мережі GB-Ras практично не залежить від ступеня заповнення ЗК стегоданими (рис. 1.24), що суттєво обмежує використання даної мережі для обробки реальних ЦЗ.

Таким чином, можемо зробити висновок, що використання ЗНМ дозволяє підвищити точність виявлення стеганограм лише при обробці пакетів ЦЗ, статистичні характеристики котрих несуттєво відрізняються від відповідних характеристик навчальної вибірки зображень. В протилежному випадку, точність роботи ШНМ суттєво знижується, що обмежує їх використання у випадку роботи на нових пакетах ЦЗ та обмеженості апріорних даних щодо особливостей використаного АСМ.

Для порівняння також був розглянутий випадок використання гібридної мережі ASSAF [127] для виявлення стеганограм, сформованих з використанням ЗК, що характеризуються значною варіативністю рівня власних шумів. Особливістю даної мережі є використання ЗнАЕ для зниження впливу завад на статистичні параметри досліджуваних цифрових зображень. Значення помилки класифікації стеганограм P_E , сформованих згідно стеганографічного методу HUGO, при використанні СД на основі статистичної моделі maxSRMd2, а також мереж GB-Ras та ASSAF наведені в табл. 1.2.

Таблиця 1.2 – Значення помилки класифікації стеганограм P_E , сформованих згідно стеганографічного методу MiPOD, при використанні СД на основі статистичної моделі maxSRMd2, а також нейронних мереж GB-Ras та ASSAF для пакетів ALASKA і VISION.

Стего-детектор	Параметри налаштування штучних нейронних мереж		Значення помилки класифікації стеганограм P_E , %		
	Метод формування стеганограм	Ступінь заповнення ЗК стего-даними, %	$\Delta_\alpha^S = 3\%$	$\Delta_\alpha^S = 20\%$	$\Delta_\alpha^S = 50\%$
Пакет зображень ALASKA					
max-SRMd2	–	–	49.13	41.03	29.50
GB-Ras	HUGO	20%	49.68	47.96	46.02

Продовження табл. 1.2

Стего-детектор	Параметри налаштування штучних нейронних мереж		Значення помилки класифікації стеганограм P_E , %		
	Метод формування стеганограм	Ступінь заповнення ЗК стего-даними, %	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 50\%$
Пакет зображень ALASKA					
GB-Ras	HUGO	40%	49.60	47.42	44.20
	MiPOD	20%	49.81	48.11	45.10
	MiPOD	40%	49.78	47.61	43.65
ASSAF	HUGO	20%	11.99	12.06	12.14
	HUGO	40%	26.33	26.21	26.43
	MiPOD	20%	13.52	13.59	13.52
	MiPOD	40%	27.67	27.85	27.58
Пакет зображень VISION					
max-SRMd2	–	–	22.67	3.66	1.43
GB-Ras	HUGO	20%	49.92	49.29	48.35
	HUGO	40%	49.81	47.67	36.68
	MiPOD	20%	49.89	48.52	42.51
	MiPOD	40%	49.59	47.05	42.90
ASSAF	HUGO	20%	17.41	17.52	17.35
	HUGO	40%	16.76	16.84	16.40
	MiPOD	20%	50.00	18.12	49.98
	MiPOD	40%	50.02	17.11	50.02

Виявлено, що використання мережі ASSAF дозволяє суттєво зменшити значення помилки P_E ($\Delta P_E \cong 37\%$, табл. 1.2) у порівнянні зі СД на основі статистичної моделі maxSRMd2 та новітньої мережі GB-Ras, навіть у

найбільш складному випадку слабкого заповнення ЗК стегоданими ($\Delta_{\alpha}^S < 10\%$). Зазначимо, що отримані результати досягаються за рахунок суттєвого зростання обчислювальної складності налаштування СД, а саме необхідності налаштування всіх складових частин мережі ASSAF (знешумлюючого автоенкодера та дуальної мережі класифікатора ЦЗ) [127]. При цьому забезпечення ефективності роботи ЗНАЕ щодо виявлення та придушення впливу спотворень ЦЗ, обумовлених прихованням повідомлень, потребує стеганограм та ЗК, використаних для їх формування. Це обмежує використання мережі ASSAF, зокрема коли стегоаналітик не має доступу до стегакодера.

Таким чином, можемо зробити висновок щодо суттєвих обмежень використанням сучасних статистичних моделей ЗК та ШНМ для побудови високоточних СД, здатних працювати в умовах обмеженості апріорних даних щодо АСМ та значної варіативності статистичних параметрів ЦЗ. Дане зниження може бути пояснено низкою факторів, зокрема надлишковістю використання потужних ансамблів ФВЧ для попередньої обробки ЦЗ, особливостями роботи ЗНМ на нових вибірках ЦЗ (проблема domain mismatch), необхідністю використання стеганограм та ЗК для налаштування ЗНАЕ у складі гібридних штучних нейронних мереж.

Відмітимо, що значення точності роботи сучасних СД на основі розглянутих підходів залишається відносно низькою навіть у випадку обробки ЦЗ високої якості та обмеженості апріорних даних щодо СМ. Тому становить інтерес визначення особливостей сучасних методів стегоаналізу, що негативно впливають на точність роботи СД.

1.5 Постановка задачі дисертаційного дослідження

Сучасний підхід до побудови СД заснований дослідженні відмінностей між статистичними, спектральними та структурними параметрами зображень з відповідними характеристиками ЗК, або ж стеганограм [9-11,13]. Враховуючи широке розповсюдження АСМ, значна увага приділяється дослідженню локальних статистичних характеристик ЗК, обчислених для окремих облас-

тей зображення. Для аналізу змін ступеня кореляції значень яскравості суміжних пікселів ЗК, обумовлених прихованням повідомлень, широко використовується математичний апарат марківських випадкових полів (МВП) [9,10,207]:

$$P(f) = e^{-\frac{1}{T_{MRF}}U(f)} / \sum_{f \in \mathbb{F}} e^{-\frac{1}{T_{MRF}}U(f)}, \quad (1.28)$$

де f – поточна конфігурація значень групи елементів МВП, а саме значень яскравості пікселів ЦЗ в заданому околі; \mathbb{F} – простір всіх можливих сполучень (груп) значень елементів МВП; $T_{MRF} > 0$ – константа; $U(f)$ – значення гамільтоніану для заданої конфігурації f , що задає закон зміни параметрів імовірнісного розподілу $P(f)$ при варіації значень обраної групи елементів МВП.

В більшості випадків визначення параметрів розподілу $P(f)$ елементів МВП, що відповідає розподілу значень яскравості пікселів досліджуваного ЦЗ, проводиться згідно емпіричних методів з використанням КВ малого розміру (до 5×5 пікселів) [9,34]. Це обумовлено високою складністю моделювання залежності значень яскравості пікселів для КВ значного розміру (більше 7×7 пікселів) [207]. В якості прикладу можливо навести обчислення матриць суміжності значень яскравості пікселів в групі статистичних моделей SRM [34], або ж використання операції повторної вибірки (субдискретизації) для зниження кількості елементів вихідних даних згорткових шарів ЗНМ [30,43,44].

Враховуючи суттєве зниження точності роботи СД, заснованих на використанні моделі МВП (1.28), становить інтерес визначення чинників, що негативно впливають на ефективність використання даної моделі при проведенні стегоаналізу ЦЗ. Вирішення даної задачі потребує дослідження особливостей методів визначення параметрів статистичної моделі ЗК, наприклад моделей SPAM, SRM, maxSRM, що використовуються при побудові СД.

Сучасні методи стегааналізу ЦЗ засновані на використанні ансамблю ФВЧ для проведення попередньої обробки досліджуваних зображень та подальшого застосування матриць суміжності (1.21)-(1.22) значень яскравості пікселів обробленого зображення. Дана процедура відповідає застосуванню моделі FRAME (англ. Filters, Random Fields and Maximum Entropy) до аналізу параметрів МВП [207]. Модель FRAME заснована на ітеративній обробці досліджуваного ЦЗ з метою зниження впливу завад (шумів) згідно наступної процедури [207]:

1. Фільтрація ЦЗ з метою зниження негативного впливу адитивних завад, наявних в досліджуваному зображенні, на оцінку сумісного розподілу значень яскравості пікселів для поточного положення КВ;
2. Обчислення розподілу значень яскравості пікселів обробленого ЦЗ для кожного положення КВ, що відповідає оцінці параметрів поточної конфігурації f значень заданої (фіксованої) групи елементів МВП у виразі (1.28);
3. Оновлення параметрів методів фільтрації ЦЗ для максимізації взаємної ентропії розподілів значень яскравості пікселів вихідного та обробленого зображень для кожного положення КВ.

Розглянемо наведені етапи обробки ЦЗ для моделі FRAME більш детально для визначення обмежень її застосування в задачах стегааналізу цифрових зображень. На першому етапі проводиться формування набору $G^{(k)}, k \in [1; K]$ з K фільтрів, наприклад фільтрів Габора, що використовується для зниження впливу адитивних завад у зображенні. Відповідно, позначимо результат застосування операції згортки заданого зображення I з k -тим фільтром набору $G^{(k)}$ як $f^{(k)} = I \circledast G^{(k)}$.

На другому етапі проводиться обчислення гістограми розподілу значень яскравості пікселів обробленого зображення $H^{(k)} \in \mathcal{L}^S$ для кожного $f^{(k)}, k \in [1; K]$, згідно наступного виразу [207]:

$$H^{(k)}(\mathbf{I}) = \frac{1}{|\mathcal{S}|} \sum_{i \in \mathcal{S}} \delta(\mathbf{I} - f_i^{(k)}), k \in [1; K], \quad (1.29)$$

де $\delta(a)$ – функція Дірака, значення котрої рівне 1 якщо $a = 0$, та нулю в протилежному випадках; \mathcal{S} – вибірка пікселів для поточного положення КВ, що використовуються при побудові гістограми $H^{(k)}(\mathbf{I})$; \mathcal{L} – діапазон значень яскравості пікселів. Тоді взаємний розподіл значень яскравості пікселів ЦЗ згідно моделі FRAME можливо представити у вигляді [207]:

$$p(f) = \operatorname{argmax}_p \left\{ - \int p(f) \log(p(f)) df \right\} \quad (1.30)$$

за умови

$$\begin{cases} \overline{H_{p(f)}^{(k)}(\mathbf{I})} = \overline{H_{sample}^{(k)}(\mathbf{I})}, \forall k \in [1; K], \\ \int p(f) df = 1, \end{cases}$$

де $\overline{H_{p(f)}^{(k)}(\mathbf{I})} = \int H^{(k)}(f) p(f) df$ – математичне очікування значень елементів гістограми $H^{(k)}$ у виразі (1.29) при варіації імовірності $p(f)$ появи поточної конфігурації f значень фіксованої групи елементів МВП (розподілу значень яскравості пікселів обробленого зображення); $\overline{H_{aver}^{(k)}}$ – гістограма, отримана шляхом усереднення результатів обробки значень яскравостей пікселів досліджуваного зображення для декількох положень КВ з використанням k – того фільтру з набору $G^{(k)}$.

Для вирішення оптимізаційної задачі (1.30), а саме визначення найбільш імовірної конфігурації f для вихідного (незашумленого) ЦЗ за результатами аналізу досліджуваного (зашумленого) зображення, можливо застосувати метод множників Лагранжа [207]:

$$\begin{aligned}
L(p, \theta) = & - \int p(f) \log(p(f)) df \\
& + \int_{\mathbf{I}} \sum_k \theta_1^{(k)} \left\{ \int_{\mathbf{I}} p(f) \sum_i \delta(\mathbf{I} - f_i^{(k)}) df - |\mathcal{S}| \right. \\
& \left. \cdot \overline{H_{sample}^{(k)}(\mathbf{I})} \right\} d\mathbf{I},
\end{aligned} \tag{1.31}$$

де $\theta_1^{(k)}$ – множники Лагранжа. Прирівнюючи до нуля похідну виразу (1.31) ($\partial L(p, \theta) / \partial p = 0$) та враховуючи, що $p(f) = p(f|\mathbf{I})$ при заданому значенні θ , отримуємо рішення вихідної оптимізаційної задачі (1.30):

$ p(f \mathbf{I}) = \frac{e^{-\sum_{k=1}^K \sum_{i \in \mathcal{S}} (\int \theta^{(k)}(\mathbf{I}) \delta(\mathbf{I} - f_i^{(k)}) d\mathbf{I})}}{e^{-\sum_{k=1}^K \sum_{i \in \mathcal{S}_1} (\int \theta^{(k)}(\mathbf{I}) \delta(\mathbf{I} - f_i^{(k)}) d\mathbf{I})}} = \frac{e^{-\sum_{k=1}^K \sum_{i \in \mathcal{S}} (\theta^{(k)}(f_i^{(k)}))}}{e^{-\sum_{k=1}^K \sum_{i \in \mathcal{S}_1} (\theta^{(k)}(f_i^{(k)}))}}, $	(1.32)
--	--------

де \mathcal{S}_1 – множина всіх можливих вибірок пікселів досліджуваного зображення \mathbf{I} для поточного положення КВ, що використовуються для побудови гістограми $H^{(k)}(\mathbf{I})$ у виразі (1.29).

У випадку обробки діапазону значень яскравості пікселів $\mathcal{J} = \{I_1, \dots, I_L\}$ зображення \mathbf{I} , а також використовуючи позначення $I^{(k)} = f_i^{(k)}$ для випадку застосування k -того фільтру з набору $G^{(k)}$, отримуємо наступне представлення виразу (1.32):

$$\begin{aligned}
p(f|\mathbf{I}) &= \frac{e^{-\sum_{k=1}^K \sum_{i \in \mathcal{S}} \sum_{l=1}^L \{\theta_l^{(k)} \delta(I_l^{(k)} - f_i^{(k)})\}}}{e^{-\sum_{k=1}^K \sum_{i \in \mathcal{S}_1} \sum_{l=1}^L \{\theta_l^{(k)} \delta(I_l^{(k)} - f_i^{(k)})\}}} = \frac{e^{-\sum_{k=1}^K \sum_{l=1}^L \theta_l^{(k)} H_l^{(k)}}}{e^{-\sum_{\mathbf{I}} \sum_{k=1}^K \sum_{l=1}^L \theta_l^{(k)} H_l^{(k)}}} \\
&= \frac{e^{-\langle \theta, H \rangle}}{e^{-\sum_{\mathbf{I}} \langle \theta, H \rangle}}, \\
\theta_l^{(k)} &= \theta^{(k)}(\mathbf{I}_l^{(k)}), H_l^{(k)} = H^{(k)}(\mathbf{I}_l^{(k)})
\end{aligned}$$

де $\langle \cdot, \cdot \rangle$ – скалярний добуток. На останньому етапі оцінки параметрів МВП з використанням моделі FRAME проводиться визначення підмножини з N ($N < K$) фільтрів з набору $G^{(k)}$, застосування котрих дозволяє максимізувати значення взаємної ентропії для розподілів значень яскравості пікселів вихідного та обробленого ЦЗ при вирішенні оптимізаційної задачі (1.30).

Забезпечення високої ефективності придушення адитивних шумів, зокрема спотворень ЗК, обумовлених вбудовуванням стегоданих, при використанні моделі FRAME потребує повного перебору всі можливих варіантів наборів фільтрів $G^{(k)}$, $k \in [1; K]$. Для зниження обчислювальної складності вирішення даної задачі, наразі використовуються евристичних методів формування набору фільтрів $G^{(k)}$ для побудови статистичних моделей ЗК в задачах стегоаналізу ЦЗ [207]. Дані набори можуть бути сформовані шляхом відбору поширених типів ФВЧ (наприклад, для групи моделей SRM), або ж за результатами налаштування вхідних (згорткових) шарів штучних нейронних мереж (зокрема, налаштованих мереж SR-Net, Zhu-Net, GB-Ras та інших).

Для додаткового зниження складності формування набору фільтрів $G^{(k)}$, $k \in [1; K]$ при забезпеченні заданої (фіксованої) точності оцінки параметрів МВП, в якості елементів набору використовуються ФВЧ, що характеризуються малими розмірами відповідних КВ (не більше 7×7 пікселів). Це обумовлено високою складністю відбору фільтрів більшого розміру для мінімізації впливу шумів у досліджуваному ЦЗ [30,43,187-189]. Внаслідок цього значна кількість статистичних моделей ЗК, заснованих на використанні моделі FRAME, дозволяють забезпечити високу точність оцінки статистичних характеристик ЦЗ лише в межах малих околів пікселів, в той час як новітні АСМ засновані на мінімізації змін статистичних параметрів ЗК на різних масштабах аналізу цифрових зображень.

Для підтвердження отриманих висновків розглянемо поширений спосіб оцінки спотворень ЗК при формуванні стеганограм $D(\mathbf{X}, \mathbf{Y})$ (1.2), заснований на використанні функції локального потенціалу $V_C(\mathbf{X}_{ij})$. Як було зазначено в розділі 1.2.2, величина потенціалу $V_C(\mathbf{X}_{ij})$ відповідає ступеню кореляції значень яскравості суміжних пікселів в околі C поточного пікселю ЗК з координатами (i, j) [147]. З іншого боку, функція $V_C(\mathbf{X}_{ij})$ є пов'язаною зі значення гамільтоніану $U(f)$ у виразі (1.28), що визначає закон зміни параметрів імовірнісного розподілу $P(f)$ при варіації значень групи елементів МВП [207]:

$$U(f) = \sum_{c \in \mathcal{C}} V_c(f), \quad (1.33)$$

де значення потенціалу $V_c(f)$ залежить від типу використовуваної групи елементів МВП (околів $c \in \mathcal{C}$), а додавання потенціалів окремих околів $V_c(f)$ проводиться по множині всіх можливих околів \mathcal{C} .

У випадку незалежності вибору кожного елемента МВП, розподіл Гіббса (1.28) стає однорідним – значення потенціалів груп пікселів не залежать від відносного положення групи f в межах досліджуваного зображення. Це дозволяє проводити декомпозицію ЦЗ як множини компонентів, що є статистично незалежними. Відповідно, значення гамільтоніану $U(f)$ у виразі (1.33) може бути представлено у вигляді суми потенціалів V_c для кожного типу околу c [207]:

$$U(f) = \sum_{\{i_1\} \in \mathcal{C}_1} V_1(f_{i_1}) + \sum_{\{i_1, i_2\} \in \mathcal{C}_2} V_2(f_{i_1}, f_{i_2}) + \sum_{\{i_1, i_2, i_3\} \in \mathcal{C}_3} V_3(f_{i_1}, f_{i_2}, f_{i_3}) \\ + \dots + \sum_{\{i_1, \dots, i_N\} \in \mathcal{C}_N} V_N(f_{i_1}, \dots, f_{i_N}), \quad (1.34)$$

де i_1, \dots, i_N – множина значень для елементів конфігурації f . Відмітимо, що значення суми потенціалів $V_1(f_{i_1})$ у виразі (1.34) відповідає розподілу шумів ЦЗ, що є незалежними від просторового положення пікселя. Тоді значення суми $V_2(f_{i_1}, f_{i_2})$ відповідає ступеню кореляції значень елементів суміжних околів (властивість локальної «марковості»), а $V_N(f_{i_1}, \dots, f_{i_N})$ – загальної кореляції значень елементів усіх околів ЦЗ (відповідає властивості глобальної «марковості») [207].

Відповідно, використання представлення (1.33) гамільтоніану $U(f)$ розподілу Гіббса (1.28) при оцінці спотворень ЗК, обумовлених прихованням повідомлень, в сучасних СМ дозволяє мінімізувати зміни як локальних (потенціалів $V_1(f_{i_1})$ та $V_2(f_{i_1}, f_{i_2})$), так і глобальних (потенціалів $V_k(f_{i_1}, \dots, f_{i_k})$, $k \in \{3; N\}$) статистичних характеристик ЦЗ. Прикладом застосування потенціалів $V_c(f)$ в задачах стеганографії ЦЗ є методи оцінки спотворень ЗК, що

використовуються у стеганографічному методі HUGO [147]. Враховуючи високу обчислювальну складність безпосередньої оцінки значення потенціалу V_C для всіх типів околів $c \in \mathcal{C}$, в даному методі проводиться наближена оцінка значення $V_C(\mathbf{X}_{ij})$ з використанням матриць суміжності $\mathbf{C}_{k,l}(\mathbf{X})$ (1.5).

Таким чином, можемо зробити висновок, що одним з основних факторів суттєвого зниження точності виявлення стеганограм, сформованих згідно АСМ, при використанні сучасних методів стегааналізу ЦЗ є аналіз змін статистичних параметрів ЗК з використанням КВ лише малого розміру (не більше 7×7 пікселів) [30,43,187-189]. При цьому висока точність роботи СД досягається за рахунок використання потужних ансамблів ФВЧ, що є екстенсивним підходом до вирішення даної задачі. Це призводить до необхідності переналаштування елементів даних ансамблів для мінімізації помилки виявлення стеганограм при появі нових АСМ, або ж зміні пакету оброблюваних ЦЗ.

Вирішення задачі побудови високоточних СД також ускладнюється появою новітніх АСМ, заснованих на врахуванні впливу функцій локальних потенціалів вищих порядків $V_k(f_{i_1}, \dots, f_{i_k})$ у виразі (1.34) при проведенні оцінки спотворень ЗК. Це призводить до мінімізації змін як локальних, так і глобальних статистичних параметрів ЗК. Тому актуальною та важливою науково-прикладною проблемою в галузі стегааналізу ЦЗ є забезпечення високої точності оцінки статистичних параметрів ЗК на різних масштабах аналізу зображень в умовах відсутності апріорних даних щодо використовуваного СМ та при значній варіативності статистичних, спектральних та структурних параметрів досліджуваних ЦЗ.

Враховуючі наведені обмеження сучасних підходів до проведення стегааналізу ЦЗ, становить інтерес розробка нової концепції синтезу високоточних стегадетекторів для надійного виявлення стеганограм, сформованих згідно довільних стеганографічних методів. Вирішення даної задачі потребує дослідження впливу апріорних даних щодо особливостей СМ та характе-

ристик оброблюваних ЦЗ на ефективність роботи як стегодетектору загалом, так і його окремих складових. Це дозволить провести оцінку межі досяжної вірогідності виявлення стеганограм в залежності від наявних апріорних даних щодо використаного СМ та встановити обмеження сучасних моделей, методів та засобів стегааналізу ЦЗ, що не дозволяють наблизитися до даної межі. Зокрема, перспективним є використання методів оцінки статистичних параметрів ЗК за наявними (зашумленими) зображеннями з метою виявлення слабких спотворень ЗК, обумовлених прихованням повідомлень, замість поширених методів виокремлення шумових складових ЦЗ. З огляду на обмеженість апріорних даних щодо особливостей використаного СМ, в більшості випадків проведення стегааналізу ЦЗ, та високу варіативність параметрів реальних зображень становить інтерес використання спеціальних методів деконструкції зображень, що дозволять врахувати дані обмеження (особливості) при проведенні оцінки статистичних параметрів ЗК за наявними (зашумленими) зображеннями.

1.6 Висновки за розділом 1

За результатами критичного аналізу сучасних методів стегаграфії та стегааналізу цифрових зображень встановлено:

1. Переважна кількість новітніх стегаграфічних методів засновані на використанні адаптивних методів обробки зображень-контейнерів з метою мінімізації змін статистичних параметрів ЗК при формуванні стеганограм. Це досягається за рахунок аналізу статистичних параметрів ЗК, зокрема ступеня кореляції значень яскравості пікселів зображення-контейнеру, із використанням математичного апарату МВП, а також застосування спеціалізованих статистичних моделей (зокрема, моделі суміші завад) для оцінки параметрів складових ЗК на рівні котрих проводиться вбудовування стегоданих. Застосування даних методів при формуванні стеганограм дозволяє визначати групи пікселів ЗК, зміни яскравості котрих при вбудовуванні стегобіт призводять до мінімальних змін статистичних параметрів зображення-контейнеру.

Це призводить до суттєвого зниження рівня демаскуючих ознак сформованих стеганограм, що негативно впливає на точність роботи відомих СД.

2. Особливістю сучасних методів стегоаналізу ЦЗ є широке використання статистичних моделей ЗК та новітніх типів ШНМ для виявлення і дослідження демаскуючих ознак стеганограм, сформованих згідно АСМ. Дані методи засновані на використанні потужних ансамблів ФВЧ для попередньої обробки досліджуваних зображень з метою виявлення слабких змін статистичних параметрів ЗК, обумовлених прихованням повідомлень. Формування даних ансамблів для мінімізації помилки виявлення стеганограм є нетривіальною та обчислювально складною задачею, що наразі не має загального вирішення. Запропоновані емпіричні методи побудови ансамблів ФВЧ засновані на результатах аналізу статистичних параметрів потужних пакетів ЦЗ (наприклад, група статистичних моделей SRM), або ж спрямовані на корекцію параметрів ФВЧ в процесі налаштування штучних нейронних мереж.

3. Виявлено суттєві обмеження застосування сучасних високоточних СД для виявлення стеганограм у випадку відсутності апріорних даних щодо використаного стеганографічного методу. Встановлено, що використання потужних статистичних моделей ЗК та новітніх згорткових нейронних мереж не дозволяє забезпечити високу імовірність виявлення стеганограм (більше 95%) при обробці зображень, що характеризуються значним рівнем адитивних завад. Показано, що використання спеціалізованих методів попередньої обробки досліджуваних зображень, а саме знешумлюючого автоенкодера, дозволяє суттєво ($\Delta P_E \cong 40\%$) зменшити значення помилки P_E класифікації стеганограм навіть у випадку слабого заповнення ЗК стегоданими (менше 10%) та обмеженості апріорних даних щодо використаного СМ. При цьому висока точність виявлення стеганограм досягається за рахунок зростання обчислювальної складності налаштування СД, а також обробки стеганограм та відповідних ЗК, використаних для їх формування. Проте отримання даних пар зображень потребує доступу стегоаналітиків до модуля формування стеганограм (стегокодеру), що є неможливим в більшості практичних ситуацій.

4. Показано, що сучасні підходи до формування стеганограм та проведення стегоаналізу ЦЗ широко використовують математичний апарат МВП для аналізу статистичних параметрів ЗК. При цьому сучасні стеганографічні методи засновані на використанні методів оцінки статистичних параметрів на різних масштабах ЗК, на відміну від методів стегоаналізу, які спрямовані на аналіз змін лише локальних статистичних параметрів контейнеру, обумовлених прихованням повідомлень. Це призводить до суттєвого зниження точності роботи відомих СД у випадку аналізу стеганограм, сформованих згідно новітніх АСМ. Для подолання даних обмежень сучасних методів стегоаналізу ЦЗ становить інтерес створення узагальненої теорії побудови стегодетекторів для надійного виявлення стеганограм, сформованих з використанням цифрових зображень. Вирішення даної науково-прикладної проблеми потребує розробки високоточних методів оцінки статистичних параметрів ЗК на різних масштабах аналізу зображень, здатних працювати в умовах обмеженості апріорних даних щодо використовуваного СМ та при значній варіативності статистичних, спектральних та структурних параметрів досліджуваних ЦЗ.

5. Запропоновано використовувати методи оцінки статистичних параметрів ЗК за наявними (зашумленими) ЦЗ з метою виявлення слабких спотворень зображення-контейнеру, обумовлених вбудовуванням стегоданих, замість методів виокремлення шумових складових ЦЗ, що широко використовуються сьогодні. Для забезпечення високої точності оцінки статистичних параметрів ЗК запропоновано проводити попередню обробку досліджуваних зображень з використанням спеціальних методів декомпозиції, що дозволяють враховувати апріорні дані щодо особливостей статистичних, спектральних та структурних параметрів реальних цифрових зображень.

РОЗДІЛ 2 МЕТОДИ СИНТЕЗУ СТРУКТУРИ ТА ОПТИМІЗАЦІЇ ПАРАМЕТРІВ СТЕГОДЕТЕКТОРІВ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ

За результатами огляду сучасних методів стегоаналізу ЦЗ, проведеного в першому розділі, виявлено, що забезпечення високої вірогідності детектування стеганограм (більше 95%) потребує використання потужних ансамблів ФВЧ. Дані ансамблі застосовуються для попередньої обробки досліджуваних зображень, а саме виявлення спотворень (слабких змін) ЗК, обумовлених вбудовуванням стеганограм. При цьому вплив кожного з елементів даного ансамблю на точність виявлення стеганограм є нерівномірним, що обумовлює необхідність ітеративного переналаштування СД при роботі з новими (апріорно невідомими) СМ, або ж суттєвій зміні статистичних характеристик досліджуваних ЗК [34].

Додатковим фактором впливу на точність роботи СД є необхідність повторного визначення оптимальних параметрів його налаштування за критерієм мінімізації значення помилки P_E (1.25) при зміні статистичних характеристик оброблюваного пакету ЦЗ. Це відповідає відомій проблемі адаптації методів класифікації для роботи на вибірках даних, статистичні, спектральні та структурні параметри котрих суттєво відрізняються від відповідних параметрів для вихідної (навчальної) вибірки (проблема domain mismatch) [46,47,208]. При проведенні стегоаналізу ЦЗ, дана проблема призводить до суттєвого зниження точності роботи стегодетекторів при обробці пакетів реальних ЦЗ, які характеризуються значною варіативністю параметрів [9,13].

Внаслідок цього процедура побудови високоточних СД є нетривіальною задачею, що потребує тривалого аналізу стеганограм з метою виділення демаскуючих ознак [9,10]. Це призводить до суттєвого збільшення тривалості налаштування СД, а також зростання обчислювальної складності їх переналаштування для виявлення нових типів СМ. Тому актуальною та важливою науково-прикладною задачею є розробка високоточних методів виявлення стеганограм, здатних надійно працювати в умовах відсутності апріорних да-

них щодо особливостей використаних стеганографічних методів, малого ступеня заповнення ЗК стегоданими (менше 10%) та при значній варіативності параметрів досліджуваних ЦЗ.

Вирішення даної задачі потребує визначення складових СД, що є найбільш чутливими до наявності апріорних даних щодо СМ та змін статистичних параметрів оброблюваних ЦЗ, оцінки досяжної межі точності виявлення стеганограм в залежності від апріорних даних щодо СМ та параметрів досліджуваних зображень, а також розробки методів синтезу високоточних СД, здатних наблизитися до встановленої границі.

2.1 Аналіз факторів впливу на точність виявлення стеганограм при використанні сучасних підходів до побудови стегодетекторів

Точність роботи сучасних СД, залежить від багатьох факторів, зокрема наявності апріорних даних щодо особливостей використаного СМ, статистичних, спектральних та структурних параметрів оброблюваних ЦЗ, методів попередньої обробки досліджуваних ЦЗ тощо [9-11,13]. Нелінійний вплив кожного з даних факторів на вірогідність виявлення стеганограм суттєво ускладнює розробку та/або налаштування високоточних СД. Тому теоретичний та практичний інтерес становить визначення складових стегодетектору, що мають найбільший вплив на точність виявлення стеганограм, та розробка методів підвищення робастності даних складових для роботи в умовах обмеженості апріорних даних щодо використаного СМ та змін параметрів досліджуваних зображень в широких межах.

Сучасні підходи до вирішення даної задачі засновані на виборі певної (фіксованої) структури стегодетектору та подальшої варіації окремих параметрів СД з метою визначення їх впливу на точність роботи СД [9,13]. В якості прикладу можливо навести новітні підходи до розробки високоточних СД, заснованих на зниженні обчислювальної складності переналаштування стегодетектору шляхом: використання попередньо налаштованих ЗНМ [8], врахуванні статистичних параметрів досліджуваних ЦЗ при оптимізації

структури ЗНМ [209], об'єднання (агрегації) результатів роботи ансамблю СД [210] тощо. Практичне застосування даних підходів дозволяє проводити швидко переналаштування СД шляхом зміни лише окремих параметрів стегадетектору. Проте визначення оптимальних значень даних параметрів за критерієм мінімізації значень помилки P_E (1.25) залишається невирішеною задачею, для якої запропоновані евристичні методи для часткових випадків.

Для подолання наведених обмежень відомих методів синтезу високоточних СД в роботі запропоновано об'єднувати (групувати) параметри СД за характером їх впливу на вірогідність виявлення стеганограм. Це дозволяє спростити проведення аналізу точності роботи СД та не потребує повного перебору значень його параметрів. За результатами проведених автором досліджень запропоновано представлення значення загальної помилки класифікації стеганограм P_E (1.25), як результату композиції наступних функцій [80]:

$$P_E = F_{calib}(\mathbf{I}) \circ F_{feature}(\tilde{\mathbf{I}}) \circ F_{class}(\mathbf{f}), \quad (2.1)$$

де $F_{calib}(\cdot)$ – методи попередньої обробки досліджуваного зображення \mathbf{I} , спрямовані на виявлення слабких змін ЗК, обумовлених прихованням повідомлень; $F_{feature}(\cdot)$ – методи визначення демаскуючих ознак стеганограм; $F_{class}(\mathbf{f})$ – методи класифікації досліджуваного зображення за результатами обробки обчислених векторів \mathbf{f} (параметрів зображення). Наведені функції у виразі (2.1) відповідають основним етапам обробки досліджуваних ЦЗ в стегадетекторі. Розглянемо вплив кожної з даних функцій на значення помилки класифікації P_E більш детально.

Функція $F_{feature}(\cdot)$ використовується для визначення відмінностей (демаскуючих ознак) у статистичних, спектральних та структурних параметрах ЗК та стеганограм. При цьому величина змін даних параметрів є пропорційною до рівня спотворень, внесених до ЗК в процесі приховання повідомлень, та може бути оцінена з використання відомих статистичних моделей ЦЗ [10]. Для оцінки якості роботи обраної моделі цифрового зображення можливо

використовувати градієнт зміни параметрів досліджуваних зображень при малих змінах ступеня заповнення ЗК стегоданими Δ_α^S :

$$g_f(\tilde{\mathbf{I}}) \sim \partial \mathbf{f} / \partial \Delta_\alpha^S. \quad (2.2)$$

Для оцінки значення градієнту $g_f(\tilde{\mathbf{I}})$ (2.2) можливо сформуванати тестовий пакет ЗК, що відрізняються один від іншого лише значенням яскравості окремого пікселю. Відповідно, значення $g_f(\tilde{\mathbf{I}})$ (2.2) для зображень з даного пакету буде відповідати елементам поверхні багатовиду \mathcal{F} в рімановському просторі з координатами $\boldsymbol{\theta} = (\theta_1, \dots, \theta_{k_\theta})$, де $\theta_i \in$ значенням i -того елементу вектору параметрів \mathbf{f} досліджуваних ЦЗ. Тоді, оцінку приросту «інформації» щодо використаного СМ при зміні ЗК та варіації значення параметру Δ_α^S можливо представити з використанням інформаційної метрики Фішера $g_{jk}(\boldsymbol{\theta})$ щодо приросту значень i -того та j -того параметрів вектору \mathbf{f} [211]:

$$g_{jk}(\boldsymbol{\theta}) = \int_{\mathcal{X}} \frac{\partial \log p(\mathbf{X}, \boldsymbol{\theta})}{\partial \theta_j} \cdot \frac{\partial \log p(\mathbf{X}, \boldsymbol{\theta})}{\partial \theta_k} \cdot p(\mathbf{X}, \boldsymbol{\theta}) d\mathbf{X}, \quad i, j, k \in [1; k_\theta], \quad (2.3)$$

де $\mathcal{X} = \{\mathbf{X}_1, \dots, \mathbf{X}_n\}$ – множина тестових ЗК, що використовуються в процесі побудови СД; $p(\mathbf{X}, \boldsymbol{\theta})$ – імовірнісний розподіл значень параметрів $\boldsymbol{\theta}$ для зображень-контейнерів \mathbf{X} . Відповідно, використання параметрів ЗК, що зазнають найбільших змін при вбудовуванні повідомлень до ЗК, дозволить максимізувати значення інформаційної метрики Фішера (2.3) та, відповідно, визначити демаскуючі ознаки використаного СМ.

Зазначимо, що фіксація певних елементів вектору $\boldsymbol{\theta}$ може бути представлено, як введення додаткових обмежень, щодо значень імовірності $p(\mathbf{X}, \boldsymbol{\theta})$ у виразі (2.3) у випадку використання МВП для дослідження змін статистичних параметрів ЗК при вбудовуванні стегоданих [207,212,213]. Зокрема наявність у векторі $\boldsymbol{\theta}$ n_θ ($0 \leq n_\theta < k_\theta$) елементів, значення котрих не змінюються при вбудовуванні стегоданих до ЗК, призводить до того, що розмірність простору, в якому розташований багатовид \mathcal{F} може бути скорочена до $(k_\theta - n_\theta)$ [213]. Це пояснює збереження високої точності оцінки параметрів

МВП, що використовуються для аналізу залежності значень яскравості суміжних пікселів у поширених статистичних моделях ЗК, навіть при використанні відносно малого діапазону квантування значень яскравості пікселів зображення [9,10,13]. В даному випадку n_θ елементів вектору θ відповідають значенням яскравості пікселів ЦЗ, що не змінюються після проведення квантування. Враховуючи, що значна кількість новітніх АСМ заснована на мінімізації змін елементів вектору θ у виразі (2.3) [32,148-150], використання МВП для моделювання реальних ЦЗ дозволяє забезпечити високу точність виявлення демаскуючих ознак стеганограм при збереженні відносно низької обчислювальної складності методів обробки.

Внаслідок цього, можемо зробити висновок, що вплив вибору функції $F_{feature}(\cdot)$ на значення помилки класифікації стеганограм P_E (2.1) може бути представлений, як відповідні зміни значення інформаційної метрики Фішера $g_{jk}(\theta)$ (2.3) при фіксованій статистичній моделі ЗК. Тому подальший інтерес становить дослідження впливу функції $F_{class}(\mathbf{f})$ на значення P_E за умови використання заданої (фіксованої) статистичної моделі ЗК.

Точність двокласової (бінарної) класифікації $F_{class}(\mathbf{f})$ досліджуваних ЦЗ можливо оцінити за величиною перекриття відповідних груп (кластерів) векторів, що відповідають використуваним параметрам ЗК та стеганограм [9]. При цьому висока точність класифікації досягається у випадку, коли дані кластери не перетинаються, та суттєво знижується у випадку їх часткового або повного перекриття. Внаслідок цього аналіз впливу функції $F_{class}(\mathbf{f})$ на значення помилки P_E потребує оцінки ступеня перекриття кластерів векторів ЗК та стеганограм.

Вирішення даної задачі потребує апріорних даних щодо використаного СМ для формування стеганограм для заданого набору ЗК. Враховуючи обмеженість даної інформації в реальних випадках, становить інтерес наближена оцінка ступеня перекриття кластерів векторів ЗК та стеганограм з використа-

нням оцінки відстані між імовірнісними розподілами даних векторів, зокрема відстані Кульбака-Лейблера $D_{KL}(\mathbf{X}, \mathbf{Y})$ [10]:

$$D_{KL}(\mathbf{X}, \mathbf{Y}) = \sum_{q \in \mathcal{J}} P_{\mathbf{X}}(q) \cdot \log_2(P_{\mathbf{X}}(q)/P_{\mathbf{Y}}(q)), \quad (2.4)$$

де $P_{\mathbf{X}}$, $P_{\mathbf{Y}}$ – відповідно, нормовані гістограми розподілу значень яскравості пікселів ЗК та сформованої стеганограми; q – поточне значення яскравості пікселів зображення з діапазону яскравості \mathcal{J} . Значення відстані $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4) є близьким до нуля якщо відповідні імовірнісні розподіли перекриваються, та зростає в міру віддалення кластерів один від одного. Особливістю відстані $D_{KL}(\mathbf{X}, \mathbf{Y})$ є несиметричність – залежність значень відстані при зміні порядку використовуваних імовірнісних розподілів [74,76]. Враховуючи обмежені можливості стегоаналітиків щодо доступу до СК, в більшості випадків значення відстані $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4) розраховується відносно імовірнісного розподілу зображень-контейнерів \mathbf{X} , обраних зі стандартних тестових пакетів ЦЗ. Це знижує складність аналізу точності роботи класифікатору у складі СД, оскільки не потребує повторної оцінки відстані між імовірнісними розподілами ЗК та стеганограм при аналізі нових типів СМ.

Таким чином, величину помилки класифікації P_E (2.1) можливо представити як композицію функцій $F_{feature}(\cdot)$ та $F_{class}(\cdot)$, що залежать від: відстані Кульбака-Лейблера $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4) між кластерами векторів ЗК і стеганограм, інформаційної метрики Фішера $g_{jk}(\boldsymbol{\theta})$ (2.3), яка відповідає приросту інформації щодо використаного СМ внаслідок обробки ЦЗ, а також впливу методів попередньої обробки $F_{calib}(\cdot)$. Сучасним підходом до побудови СД є використання математичного апарату МВП для аналізу статистичних параметрів зображень [34]. Для цього випадку запропоновані аналітичні оцінки змін значень $g_{jk}(\boldsymbol{\theta})$ при внесенні спотворень до ЗК, обумовлених прихованням стегоданих [30]. З іншого боку, для віднесення досліджуваних ЦЗ до класів ЗК або стеганограм широко використовуються ансамблеві класифікатори [202]. Це дозволяє мінімізувати значення помилки P_E (2.1) навіть для

випадків, коли взаємне положення кластерів, що відповідають статистичним параметрам зображенням-контейнерам (\mathcal{X}) та стеганограмам (\mathcal{Y}), відомо частково (наприклад, обмежена кількість ЗК або ж стеганограм для отримання достовірної оцінки) та малих значень відстані Кульбака-Лейблера. Тому істотний вплив на точність роботи СД мають методи попередньої обробки, що дозволяють збільшувати відстань $D_{KL}(\mathbf{X}, \mathbf{Y})$ шляхом виокремлення складових ЗК, на рівні котрих проведено приховання стегоданих.

Застосування методів обробки, що виокремлюють лише складові ЗК, використані для вбудовування повідомлень, призводить до зростання відмінностей між імовірнісними розподілами контейнерів та стеганограм. Це відповідає формуванню лінії перегину багатовиду \mathcal{F} для значення інформаційної метрики Фішера $g_{jk}(\boldsymbol{\theta})$ (2.3) є найбільшим, що спрощує вимоги до класифікаторів у складі СД. Це дозволяє суттєво зменшити вимоги щодо точності використовуваної статистичної моделі ЦЗ при збереженні фіксованої вірогідності виявлення стеганограм. Тому становить інтерес розробка процедури вибору оптимальних методів попередньої обробки ЦЗ за критерієм мінімізації помилки класифікації стеганограм P_E (1.25) при заданій (фіксованій) статистичній моделі ЗК та класифікатору у складі СД.

В якості методів попередньої обробки досліджуваного зображення $F_{calib}(\cdot)$ у виразі (2.1) широко використовуються методи високочастотної фільтрації ЦЗ з використанням ансамблів ФВЧ, наприклад в групі моделей SRM [34], згорткових нейронних мережах Zhu-Net [43], SR-Net [30], GB-Ras [44] тощо. Дані методи спрямовані на виділення шумових складових ЦЗ на рівні котрих проводиться приховання повідомлень. Проте варіативність рівня адитивних шумів у реальних ЦЗ призводить до суттєвих змін результатів застосування ансамблю ФВЧ для обробки ЗК та стеганограм, зокрема відмінностей у відстані між статистичними параметрами вихідних та оброблених зображень, що ускладнює переналаштування СД для виявлення нових СМ. Внаслідок цього можемо зробити висновок, що вибір оптимальної функції

$F_{calib}(\cdot)$ у виразі (2.1) за критерієм мінімізації значення помилки P_E суттєво залежить від наявних апріорних даних щодо використаного СМ та відмінностей між статистичними параметрами навчальної та поточної вибірки ЦЗ. Тому становить інтерес дослідження змін взаємного положення векторів, що відповідають статистичним параметрам ЗК та стеганограм, при варіації методу попередньої обробки ЦЗ.

В роботі [159] досліджено поширені методи попередньої обробки ЦЗ та запропоновано представлення впливу даних методів на точність роботи СД, як внесення відповідних змін до розташування кластерів векторів \mathcal{X} та \mathcal{Y} . Схематичне представлення зміни взаємного положення векторів, що відповідають вихідним та обробленим зображенням-контейнерам та стеганограмами наведено на рис. 2.1.

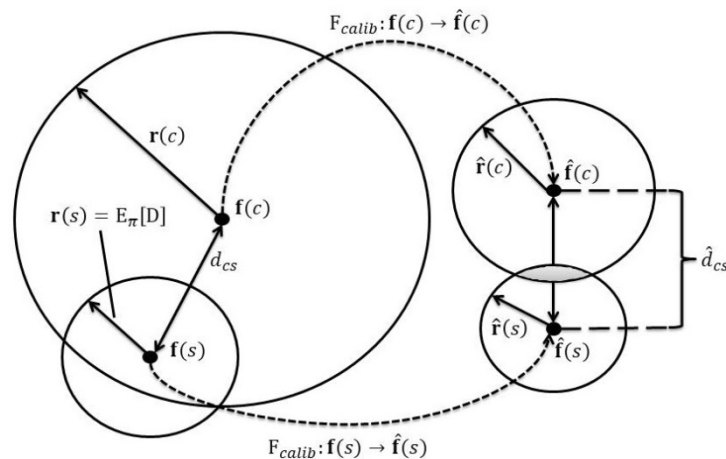


Рисунок 2.1 – Схематичне представлення впливу методів попередньої обробки досліджуваних зображень на взаємне розташування кластерів векторів, що відповідають статистичним параметрам ЗК та стеганограм.

Приховання повідомлень до ЗК призводить до зсуву положення вектору $\mathbf{f}(c)$, що відповідає статистичним параметрам зображення-контейнеру, на величину d_{cs} до нового положення $\mathbf{f}(s)$ (рис. 2.1). При цьому розмір кластеру $\mathbf{f}(c)$ залежить від ступеня варіації значень параметрів ЗК:

$$\|\mathbf{r}(c)\|_2 = \max_{\mathbf{f}_c(i)} \|\mathbf{f}(c) - \mathbf{f}_c(i)\|_2, i \in [1; N_{\mathbf{f}(c)}],$$

де $\mathbf{f}_c(i)$ – вектори, що відносяться до кластеру ЗК; $N_{\mathbf{f}(c)}$ – кількість елементів у кластері $\mathbf{f}(c)$. З іншого боку, розмір кластеру $\mathbf{f}(s)$ (рис. 2.1) відповідає статистичним параметрам сформованих стеганограм та рівний $\|\mathbf{r}(s)\|_2 = E_{\pi}[D]$ згідно виразу (1.3). Застосування функції $F_{calib}(\cdot)$ до $\mathbf{f}(c)$ та $\mathbf{f}(s)$ призводить до формування кластерів, що відповідають обробленим зображенням-контейнерам $\hat{\mathbf{f}}(c)$ і стеганограмам $\hat{\mathbf{f}}(s)$ (рис. 2).

Таким чином, мінімізація значення помилки P_E при фіксованих методах $F_{feature}(\cdot)$ та $F_{class}(\cdot)$ у виразі (2.1) потребує вибору $F_{calib}(\cdot)$, що максимізує значення відстані між кластерами векторів оброблених ЗК та стеганограм при фіксованих змінах розміру даних кластерів. За результатами порівняльного аналізу методів попередньої обробки ЦЗ в залежності від впливу на зміни просторового положення кластерів векторів $\hat{\mathbf{f}}(c)$ та $\hat{\mathbf{f}}(s)$ в роботі [159] запропоновано наступну класифікацію даних методів:

1. Методи паралельного переносу ознак (англ. parallel reference) – застосування методів попередньої обробки ЦЗ призводить лише до паралельного зсуву векторів ЗК та стеганограм, що не підвищує точність роботи СД;
2. Методи підсилення відмінностей ЗК та стеганограм (англ. divergent reference, DR) – спрямовані на посилення відмінностей між ЗК та стеганограмами шляхом підвищення відстані між відповідними векторами;
3. Методи нівелювання відмінностей між векторами-ознак (англ. eraser) – в результаті застосування даних методів відстань між векторами ЗК та стеганограм суттєво знижується, аж до їх повного збігу;
4. Методи оцінки вихідного виду ЗК (англ. cover estimate, CE) – спрямовані на оцінку статистичних ознак зображення-контейнеру за наявним ЦЗ. У випадку обробки ЗК, зміни відповідного вектору ознак є несуттєвими, в той час як обробка стеганограм призводить до суттєвих змін відповідного вектору ознак;
5. Методи оцінки параметрів стеганограм (англ. stego estimate, SE) – спрямовані на виділення спотворень, обумовлених прихованням стегоданих.

В даному випадку обробка стеганограм згідно даного методу призводить до несуттєвих змін відповідного вектору ознак, в той час як обробка ЗК призводить до суттєвих змін відповідного йому вектору ознак.

Схематичне представлення взаємного положення векторів-ознак ЗК та стеганограм при використанні наведених типів методів попередньої обробки зображень наведено на рис. 2.2.

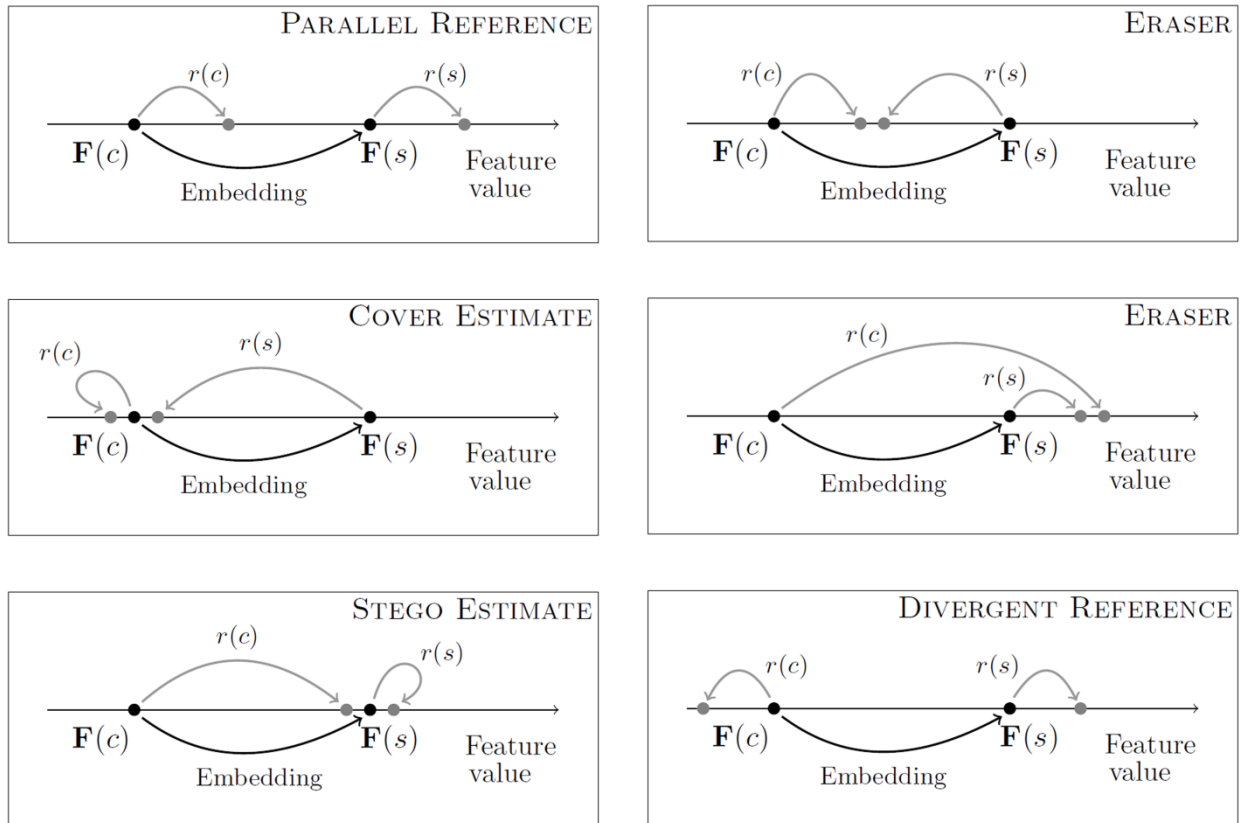


Рисунок 2.2 – Схематичне зображення впливу методів попередньої обробки ЦЗ на зміни відстані r між векторами, що відповідають зображенням-контейнерам $F(c)$ та стеганограмам $F(s)$. За матеріалами роботи [159].

Наведені в першому розділі роботи методи зниження спотворень ЦЗ, обумовлених JPEG-стисненням, можливо віднести до групи методів, спрямованих на відновлення вихідного виду ЗК за наявними (спотвореними JPEG-стисненням) зображеннями. В той же час методи на основі ФВЧ, характерні для групи моделей SRM, спрямовані на підсилення аномальних змін статистичних параметрів ЗК, обумовлених прихованням повідомлень, що дозволяє віднести їх до групи SE-методів.

Сучасні дослідження методів попередньої обробки ЦЗ в галузі стегоаналізу цифрових зображень спрямовані на розробку та практичну реалізацію DR-методів, що дозволяють максимізувати відстань між кластерами \mathcal{X} та \mathcal{Y} в заданому евклідовому просторі. Відповідно, дані методи попередньої обробки дозволяють використовувати прості (лінійні) алгоритми віднесення оброблюваного ЦЗ до класів ЗК та стеганограм (рис. 2.2).

Таким чином, можемо зробити висновок, що основним фактором негативного впливу на точність роботи СД є нелінійна залежність ефективності використання методів попередньої обробки ЦЗ від наявних апріорних даних щодо стеганографічного методу та особливостей статистичних, спектральних та структурних параметрів досліджуваних ЦЗ. При цьому вплив методів визначення демаскуючих ознак стеганограм $F_{feature}(\cdot)$ (2.1) на точність роботи СД залежить лише від обраної статистичної моделі ЗК, зокрема зміни значень інформаційної метрики Фішера $g_{jk}(\boldsymbol{\theta})$ (2.3) при варіації ступеня заповнення ЗК стегоданими. З іншого боку, вплив методів класифікації ЦЗ $F_{class}(\mathbf{f})$ (2.1) на значення помилки P_E визначається лише ступенем перекриття кластерів векторів, що відповідають ЗК та стеганограмам. При цьому вплив методів $F_{class}(\mathbf{f})$ (2.1) може бути оцінений з використанням відстані Кульбака-Лейблера $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4), враховуючи неможливість точної оцінки взаємного положення даних кластерів в умовах обмеженості апріорних даних щодо використаного СМ.

Відповідно, розробка нової концепції синтезу високоточних СД потребує створення математичного апарату вибору оптимальних методів попередньої обробки досліджуваних ЦЗ за критерієм мінімізації значення помилки P_E , здатних працювати в умовах обмеженості апріорних даних щодо використаного СМ. Вирішення даної науково-прикладної проблеми потребує вдосконалення методів оцінки взаємного положення кластерів векторів, що відповідають ЗК $\mathbf{F}(c)$ та стеганограмам $\mathbf{F}(s)$, а саме підвищення точності їх роботи при обробці пакетів ЦЗ, що характеризуються значною варіативністю пара-

метрів досліджуваних ЦЗ [29]. Це дозволить встановити межі зсуву кластерів векторів $\mathbf{F}(c)$ і $\mathbf{F}(s)$ при використанні «ідеалізованих» методів попередньої обробки ЦЗ. Отримані результати дадуть можливість провести оцінку досяжної точності виявлення стеганограм в залежності від наявних апріорних даних щодо СМ та варіативності параметрів досліджуваних ЦЗ, що становить особливий теоретичний та практичний інтерес в задачах стегоаналізу цифрових зображень.

2.2. Оцінка досяжної вірогідності виявлення стеганограм в залежності при використанні відомих методів стегоаналізу зображень

2.2.1 Порівняльний аналіз показників оцінки відстані між імовірнісними розподілами зображень-контейнерів та стеганограм

Розробка високоточних СД, здатних працювати в умовах обмеженості апріорних даних щодо використаного СМ, потребує оцінки взаємного положення кластерів векторів $\mathbf{F}(c)$ і $\mathbf{F}(s)$. Сучасним підходом до оцінки взаємного положення кластерів є використання відстані $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4) між імовірнісними розподілами векторів, що відповідають параметрам ЗК та стеганограм, наприклад елементів гістограм яскравості пікселів досліджуваного ЦЗ [9, 10, 13]. В більшості випадків, показник $D_{KL}(\mathbf{X}, \mathbf{Y})$ використовується для оцінки відстані між імовірнісними розподілами векторів, а саме статистичних параметрів ЦЗ, отриманих з використанням математичної моделі F досліджуваного зображення. В даному випадку, значення відстані $D_{KL}(\mathbf{X}, \mathbf{Y})$ може бути розраховано згідно наступного виразу [74]:

$$D_{KL}^F(\mathbf{X}, \mathbf{Y}) = \sum_{i \in n_F} \sum_{q_i^F \in J_i^F} P_X^F(q_i^F) \cdot \log_2 \left(\frac{P_X^F(q_i^F)}{P_Y^F(q_i^F)} \right), \quad (2.5)$$

де P_X^F, P_Y^F – відповідно, вектори, що відповідають сукупності параметрів ЗК та стеганограм; n_F – кількість параметрів ЦЗ, що використовуються в моделі F ; q_i^F – поточне значення i -того параметру моделі F ; J_i^F – діапазон значень i -того параметру моделі F .

В якості прикладу, розглянемо залежності відстаней $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4) та $D_{KL}^F(\mathbf{X}, \mathbf{Y})$ (2.5) від ступеня заповнення ЗК стегоданими при використанні як стандартної статистичної моделі SPAM [38] та новітньої моделі maxSRMd2 [177] для стеганограм, сформованих згідно сучасних АСМ (рис. 2.3).

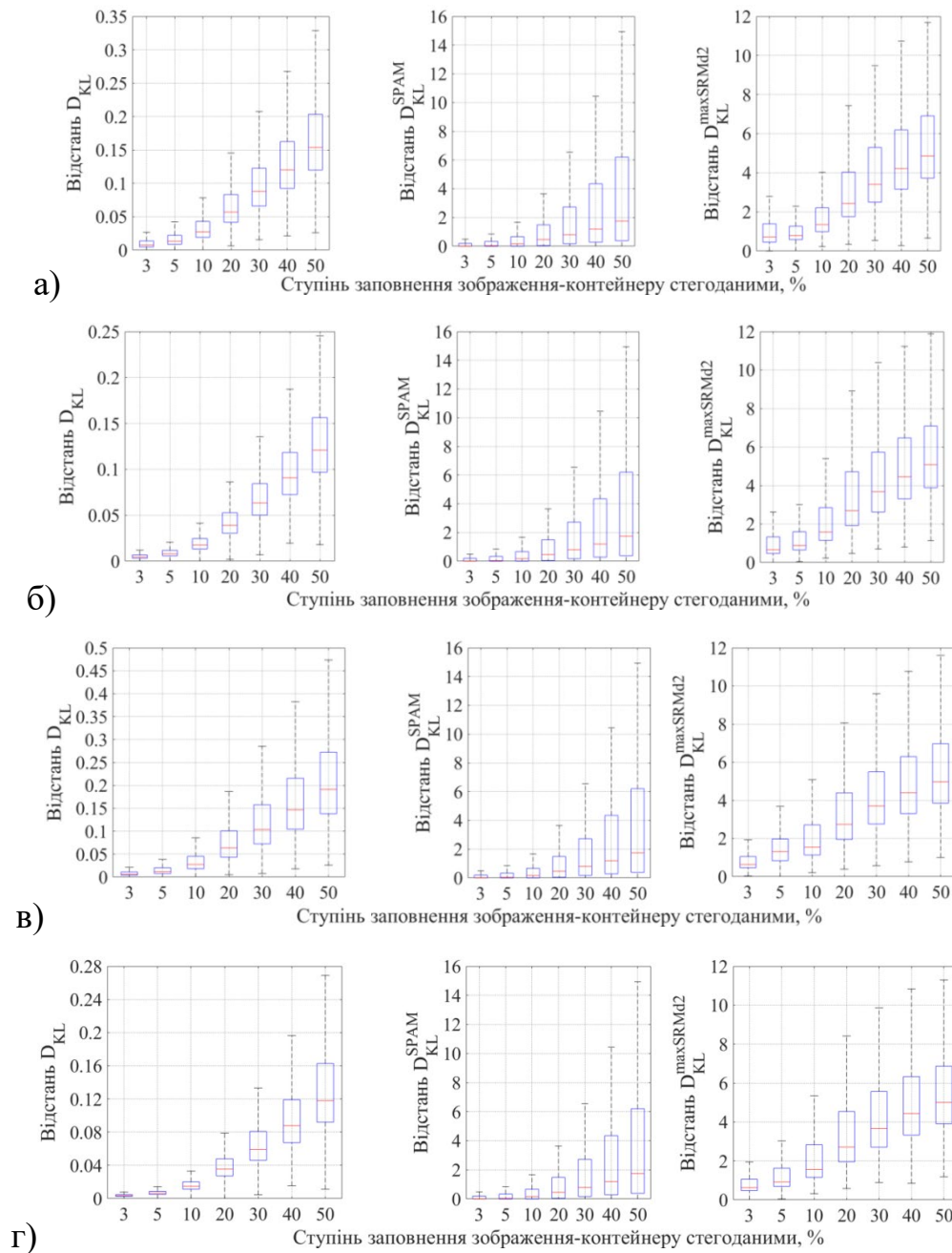


Рисунок 2.3 – Діаграми розмаху значень відстаней D_{KL} (зліва), D_{KL}^{SPAM} (по центру) та $D_{KL}^{maxSRMd2}$ (справа) від ступеня заповнення ЗК стегоданими для пакету зображень ALASKA при формуванні стеганограм з використанням стеганографічних методів HUGO (а), S-UNIWARD (б), MG (в) та MiPOD (г).

Відмітимо малі значення відстані D_{KL} для розглянутих методів приховання повідомлень (рис. 2.3) – максимальне даної відстані не перевищує 0.5 у всьому діапазоні значень параметру Δ_α^S . При цьому найбільший розмах значень (висота діаграми) досягається для методу MG ($D_{KL} \leq 0.18$, рис. 2.3в), а найменший – для методу MiPOD ($D_{KL} \leq 0.11$, рис. 2.3г). Це підтверджує високу ефективність новітніх АСМ щодо мінімізації змін значень яскравості пікселів ЗК при вбудовуванні повідомлень.

Використання статистичних моделей SPAM та maxSRMd2 дозволяє виокремити спотворення параметрів ЗК, обумовлені прихованням повідомлень, що призводить до відповідного зростання значень відстані Кульбака-Лейблера $D_{KL}^F(\mathbf{X}, \mathbf{Y})$ (2.5). При цьому отримані діаграми розкиду значень D_{KL}^{SPAM} та $D_{KL}^{maxSRMd2}$ суттєво різняться – діаграми для статистичної моделі SPAM характеризуються значним розмахом значень, в той час як для моделі maxSRMd2 даний розмах є відносно малим у порівнянні з середніми значеннями відстані $D_{KL}^F(\mathbf{X}, \mathbf{Y})$ (серединна лінія діаграм). Це свідчить про значний розкид значень параметрів моделі SPAM для ЗК та стеганограм, сформованих згідно розглянутих АСМ, що призводить до зниження точності роботи СД. З іншого боку, діаграми розмаху значень $D_{KL}^{maxSRMd2}$ є близькими до відповідних діаграм для D_{KL} (рис. 2.3), що підтверджує ефективність використання даної статистичної моделі для виявлення стеганограм.

Значення відстані D_{KL}^F (2.5) залежить від типу використовуваної моделі F цифрового зображення та, відповідно, способу визначення параметрів даної моделі. Тим не менше, відомі статистичні моделі ЦЗ засновані на безпосередньому використанні яскравості пікселів для дослідження параметрів зображення. Внаслідок цього значення відстані D_{KL}^F залежить від відповідних значень D_{KL} (2.4), тому результати отримані для D_{KL} можуть бути узагальнені для відстані D_{KL}^F при зміні використовуваної моделі F зображення. Таким чином, становить інтерес використання саме відстані D_{KL} (2.4) в подальших до-

слідженнях, що дозволить отримати оцінку досяжної точності виявлення стеганограм незалежно від типу використовуваної моделі ЦЗ.

Як зазначалося в розділі 2.1, значення відстані Кульбака-Лейблера (2.4) залежить від порядку аргументів (імовірнісних розподілів) [208], а саме $D_{KL}(\mathbf{X}, \mathbf{Y}) \neq D_{KL}(\mathbf{Y}, \mathbf{X})$. Відповідно, використання відстані $D_{KL}(\mathbf{X}, \mathbf{Y})$ унеможливило оцінку ступеня змін положення окремих векторів, що відповідають ЗК, обумовлених прихованням повідомлень. Для подолання даного обмеження в роботі [74] автором запропоновано використовувати значення відстані $D_{KL}(\mathbf{Y}, \mathbf{X})$ при оцінці взаємного положення кластерів векторів, що відповідають ЗК та стеганограмам (імовірнісних розподілів P_X та P_Y). Зокрема запропоновано використовувати наступне відношення значень відстаней $D_{KL}(\mathbf{X}, \mathbf{Y})$ та $D_{KL}(\mathbf{Y}, \mathbf{X})$ для дослідження змін параметрів ЗК, обумовлених прихованням повідомлень [74]:

$$D_{KL}^r(\mathbf{X}, \mathbf{Y}) = D_{KL}(\mathbf{X}, \mathbf{Y}) / D_{KL}(\mathbf{Y}, \mathbf{X}). \quad (2.6)$$

Для дослідження точності оцінки взаємного положення імовірнісних розподілів P_X та P_Y при використанні відстаней $D_{KL}(\mathbf{X}, \mathbf{Y})$, $D_{KL}(\mathbf{Y}, \mathbf{X})$ та $D_{KL}^r(\mathbf{X}, \mathbf{Y})$ було проведено аналіз змін значень даних відстаней при вбудовуванні стегоданих до ЗК згідно АСМ при варіації ступеня заповнення ЗК стегоданими Δ_α^S . Отримані залежності значень відстаней $D_{KL}(\mathbf{X}, \mathbf{Y})$, $D_{KL}(\mathbf{Y}, \mathbf{X})$ та $D_{KL}^r(\mathbf{X}, \mathbf{Y})$ (2.6) між імовірнісними розподілами P_X та P_Y при формуванні стеганограм згідно досліджуваних стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153] наведено на рис. 2.4.

Виявлено несуттєві відмінності у значеннях відстаней $D_{KL}(\mathbf{X}, \mathbf{Y})$ та $D_{KL}(\mathbf{Y}, \mathbf{X})$ між імовірнісними розподілами P_X та P_Y (рис. 2.4). Це підтверджується малими змінами значень відстані $D_{KL}^r(\mathbf{X}, \mathbf{Y})$ ($D_{KL}^r(\mathbf{X}, \mathbf{Y}) \cong 1.0$, рис. 2.4) при варіації параметру Δ_α^S . При цьому зміни середнього значення відстаней $D_{KL}(\mathbf{X}, \mathbf{Y})$ та $D_{KL}(\mathbf{Y}, \mathbf{X})$ (середні лінії діаграм розмаху, рис. 2.4) не перевищують 0.2, що суттєво ускладнює оцінку взаємного положення імовірнісних розподілів P_X та P_Y . Це обумовлено мінімізацією змін яскравості пікселів ЗК

при формуванні стегограм згідно розглянутих АСМ, що обмежує практичне застосування даних відстаней при проведенні стегоаналізу новітніх СМ.

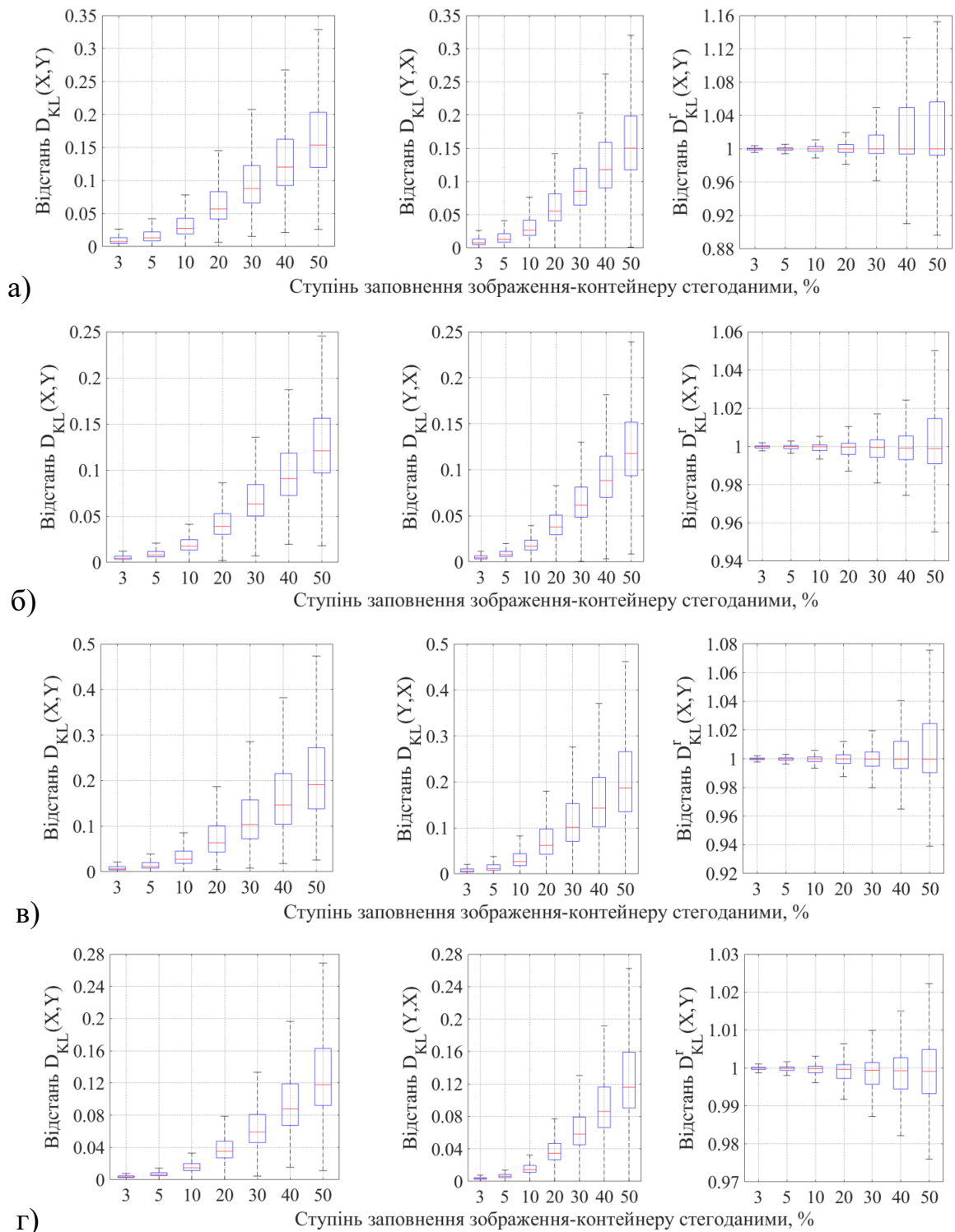


Рисунок 2.4 – Діаграми розмаху значень відстаней $D_{KL}(\mathbf{X}, \mathbf{Y})$ (зліва), $D_{KL}(\mathbf{Y}, \mathbf{X})$ (по центру) та $D_{KL}^r(\mathbf{X}, \mathbf{Y})$ (справа) від ступеня заповнення ЗК стегоданими для пакету зображень ALASKA та стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Для подолання виявленого обмеження використання відстані Кульбака-Лейблера $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4) автором було запропоновано розширити перелік оцінок відстаней між імовірнісними розподілами P_X та P_Y при проведенні стегааналізу ЦЗ, зокрема використовувати відстані Хеллінгера D_H , Бхаттачарая D_B , χ^2 -квадрат D_{χ^2} та спектр відстаней Реньї D_R^α [74]:

$$D_H(\mathbf{X}, \mathbf{Y}) = \sqrt{\frac{1}{2} \cdot \sum_{q \in J} (\sqrt{P_X(q)} - \sqrt{P_Y(q)})^2}, \quad (2.7)$$

$$D_B(\mathbf{X}, \mathbf{Y}) = -\ln(1 - D_H^2(\mathbf{X}, \mathbf{Y})), \quad (2.8)$$

$$D_{\chi^2}(\mathbf{X}, \mathbf{Y}) = \sum_{q \in J} (P_X(q) - P_Y(q))^2 / P_Y(q), \quad (2.9)$$

$$D_R^\alpha(\mathbf{X}, \mathbf{Y}) = \frac{1}{\alpha - 1} \log_2 \left(\sum_{q \in J} P_X^\alpha(q) \cdot P_X^{1-\alpha}(q) \right), \quad (2.10)$$

де $\alpha \in (0; +\infty) \setminus \{1\}$ – ваговий параметр; q – поточне значення яскравості пікселів зображення з діапазону яскравості J . Зміна значення параметру α дозволяє досліджувати вплив груп пікселів з однаковими рівнем яскравості на значення відстані D_R^α [74]. Наприклад, використання діапазону значень $\alpha \in (0; 1)$ дозволяє виокремлювати вплив груп пікселів ЦЗ з малими значеннями яскравості (близькими до чорного кольору), в той час як значення $\alpha > 1$ – вплив груп пікселів з рівнем яскравості, близькими до білого кольору.

За результатами експериментальних досліджень побудовано залежності наведених відстаней (2.7)-(2.10) від ступеня заповнення ЗК стегаданими для сучасних АСМ. Виявлено високу подібність отриманих результатів для розглянутих типів АСМ. Приклади даних залежностей для сучасного стегаграфічного методу HUGO наведені на рис. 2.5.

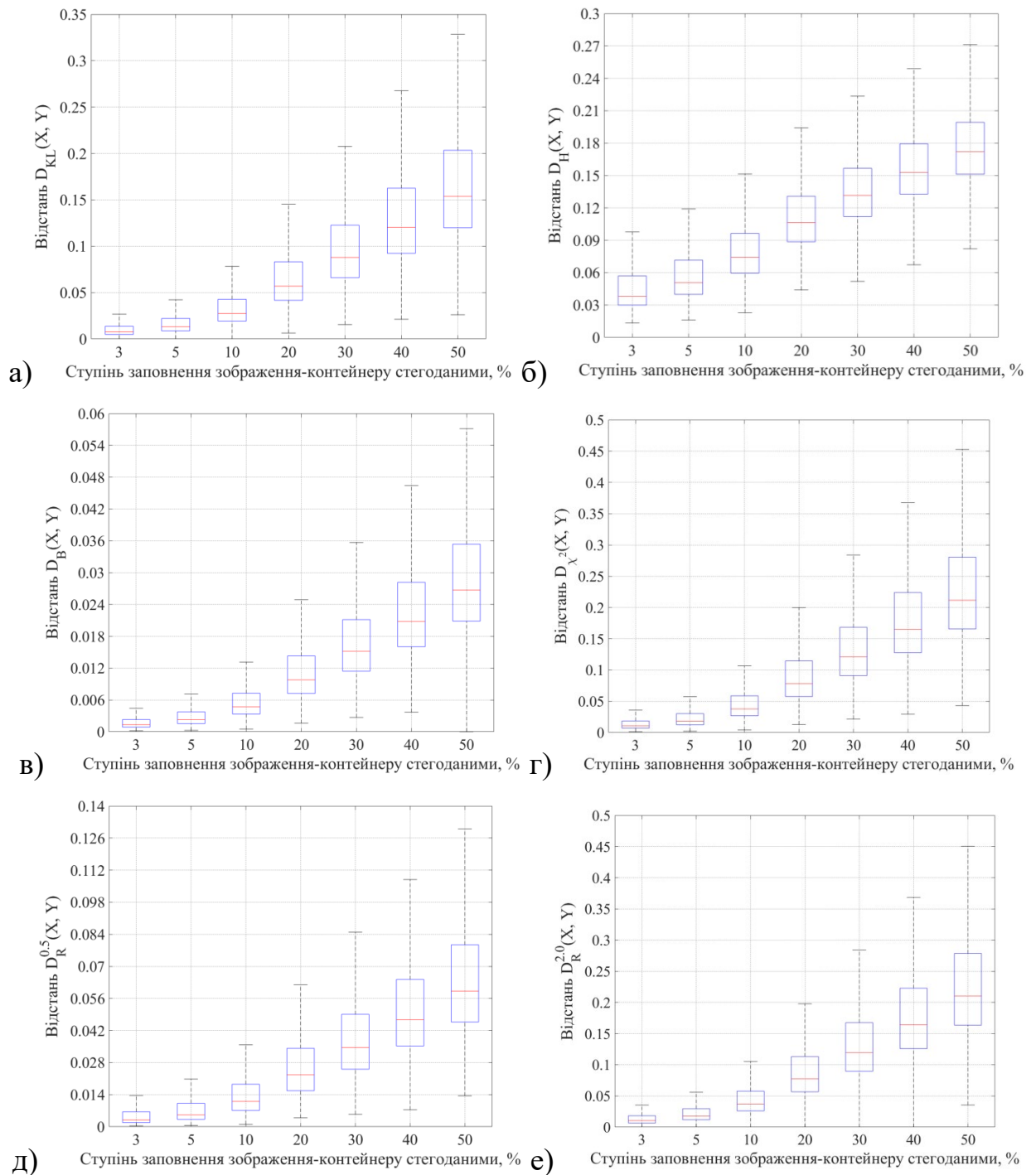


Рисунок 2.5 – Діаграми розмаху значень оцінок відстаней між імовірнісними розподілами P_X та P_Y при варіації ступеня заповнення ЗК стегоданими для пакету зображень ALASKA та стеганографічного методу HUGO:

(а) – $D_{KL}(X, Y)$; (б) – $D_H(X, Y)$; (в) – $D_B(X, Y)$; (г) – $D_{\chi^2}(X, Y)$;

(д) – $D_R^{0.5}(X, Y)$; (е) – $D_R^{2.0}(X, Y)$.

Відмітимо малі значення $D_B(X, Y)$ (рис. 2.5в) та $D_R^{0.5}(X, Y)$ (рис. 2.5д) для стеганограм, сформованих згідно методу HUGO – значення відстаней не

перевищують 0.1 навіть у випадку сильного заповнення ЗК стегоданими ($\Delta_{\alpha}^S > 20\%$), що ускладнює розпізнавання ЗК та сформованих стеганограм. З іншого боку, значення $D_{\chi^2}(\mathbf{X}, \mathbf{Y})$ (рис. 2.5г) та $D_R^{2.0}(\mathbf{X}, \mathbf{Y})$ (рис. 2.5е) суттєві відрізняються при варіації параметру Δ_{α}^S , що дозволяє використовувати прості порогові методи обробки даних відстаней для виявлення стеганограм. Проте практичне застосування даних відстаней $D_{\chi^2}(\mathbf{X}, \mathbf{Y})$ і $D_R^{2.0}(\mathbf{X}, \mathbf{Y})$ має суттєві обмеження, пов'язані зі значним розкидом їх значень (рис. 2.5), що ускладнює налаштування СД.

Виявлено, що використання відстані Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ (рис. 2.5б) дозволяє забезпечити суттєве збільшення відстані між імовірнісними розподілами P_X та P_Y при зростанні значення параметру Δ_{α}^S , що спрощує налаштування СД за рахунок використання ансамблю порогових значень. При цьому розкид значень $D_H(\mathbf{X}, \mathbf{Y})$ при зміні ступеня заповнення ЗК стегоданими залишається відносно малим, що обумовлює інтерес щодо використання даного показника для досягнення поставленої мети.

За результатами аналізу отриманих даних, можемо зробити висновок щодо перспективи застосування відстані Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ (2.7) для оцінки взаємного положення імовірнісних розподілів P_X та P_Y . Відмітимо, що відстань Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ є частковим випадком більш загальної групи показників f – дивергенції, що використовується для оцінок відстаней між імовірнісними розподілами [214]. Вагомою перевагою відстані Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ у порівнянні з іншими показниками (2.8)-(2.10) є формування $D_H(\mathbf{X}, \mathbf{Y})$ метрики на просторі ймовірнісних розподілів [215,216]. Це дозволяє використовувати значення $D_H(\mathbf{X}, \mathbf{Y})$ для оцінки імовірності правильної класифікації ЗК та стеганограм при використанні поширених типів двокласових (бінарних) класифікаторів [217].

Подальший інтерес становить використання відстані $D_H(\mathbf{X}, \mathbf{Y})$ (2.7) для аналізу зсуву кластерів векторів $\mathbf{F}(c)$ і $\mathbf{F}(s)$ (рис. 2.1) при використанні методів попередньої обробки, що дозволять максимізувати відмінності між ста-

тистичними параметрами ЗК та стеганограм. За результатами аналізу величини даних зсувів можливо буде оцінити досяжні межі точності виявлення стеганограм в залежності від наявних апріорних даних щодо СМ та варіативності параметрів досліджуваних ЦЗ.

2.2.2 Оцінка досяжної вірогідності виявлення стеганограм в залежності від наявних апріорних даних щодо використаного стеганографічного методу

Відмітимо, що в літературі відсутні відомості щодо досяжного рівня вірогідності виявлення стеганограм, сформованих згідно новітніх АСМ, при використанні ЗК, що характеризуються значною варіативністю статистичних, спектральних та структурних параметрів. При цьому переважна кількість робіт присвячені дослідженню ефективності використання СЕ- і SE-методів попередньої обробки стеганограм для виявлення лише поширених типів СМ та стандартних пакетів зображень BOSS і ALASKA [44,81-83,91,127]. Тому становить інтерес дослідження досяжної точності виявлення стеганограм при використанні оптимального методу попередньої обробки $\mathcal{K}_{opt}(\cdot)$ ЦЗ за критерієм максимізації відстані $d_{C,S}^F$ між кластерами векторів, що відповідають статистичним параметрам ЗК та стеганограм, в найбільш складному випадку проведення стегааналізу ЦЗ – обмеженості апріорних даних щодо використаних СМ та застосуванням зображень, які характеризуються високою варіативністю статистичних параметрів.

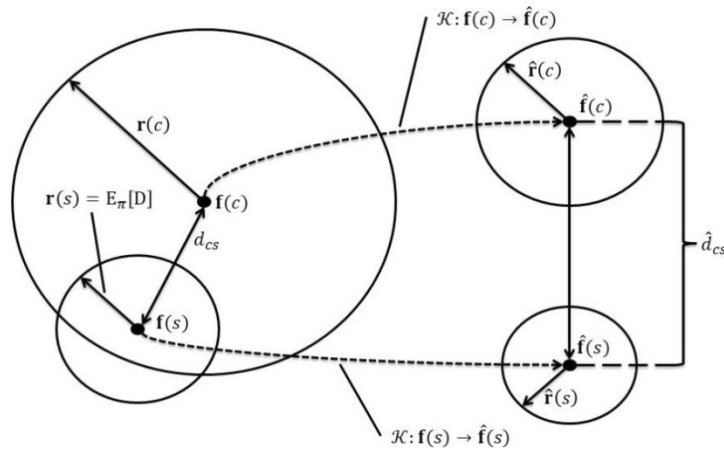


Рисунок 3 – Схематичне представлення зміни положення векторів, що відповідають статистичним параметрам зображення-контейнеру $\mathbf{f}(c)$ та сформованої стеганограми $\mathbf{f}(s)$, при проведенні синтезу стегодетекторів згідно запропонованого методу. Застосування функції попередньої обробки \mathcal{K} , визначеної за результатом вирішення оптимізаційної задачі (18), дозволяє максимізувати значення відстані \hat{d}_{cs} між кластерами $\hat{\mathbf{f}}(c)$ та $\hat{\mathbf{f}}(s)$

Враховуючи обмежені можливості стегоаналітиків щодо визначення особливостей СМ в реальних випадках, положення кластерів векторів $\mathbf{f}(c)$ і $\mathbf{f}(s)$ (рис. 2.1) може бути оцінено лише наближено з використанням доступних (наявних) прикладів стеганограм. В найбільш складному випадку, апріорні дані щодо використаного АСМ є відсутніми, тому стегоаналітик має можливість оцінити лише положення кластеру векторів $\mathbf{F}(c)$, які відповідають статистичним параметрам ЗК. Внаслідок цього суттєво знижується ефективність використання DR-методів попередньої обробки ЦЗ, що дозволяють збільшувати відстань між кластерами векторів $\mathbf{F}(c)$ і $\mathbf{F}(s)$ шляхом оцінки положення відповідних векторів з простору вищої розмірності. Це призводить до того, що оцінка максимального значення відстані $d_{c,s}^{\mathbf{F}}$ при використанні перетворення $\mathcal{K}_{opt}(\cdot)$ буде відповідати величині зсуву вектору ЗК $\mathbf{f}(c)$ до відповідного положення $\mathbf{f}(s, \Delta_{\alpha}^S)$ при формуванні стеганограми зі ступенем заповнення ЗК стегоданим рівним Δ_{α}^S :

$$\max_{\mathbf{F}_{calib}, \Delta_{\alpha}^S} D_H(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)) + \lambda_1 / \|\hat{\mathbf{r}}(c)\|_2 + \lambda_2 / \|\hat{\mathbf{r}}(s)\|_2, \quad (2.11)$$

де $\lambda_1, \lambda_2 > 0$ – множники для відповідних складових виразу регуляризації, а саме впливу розмірів кластерів оброблених зображень-контейнерів ($\hat{\mathbf{f}}(c)$) та стеганограм ($\hat{\mathbf{f}}(s)$). При цьому оцінка значення відстані \hat{d}_{cs} між кластерами $\hat{\mathbf{f}}(c)$ та $\hat{\mathbf{f}}(s)$ проводиться із застосування відстані Хеллінгера D_H (2.7). Використання запропонованого методу синтезу СД дозволяє узгодити вибір типу і параметрів функції $F_{calib}(\cdot)$ та $F_{feature}(\cdot)$ у виразі (2.1) для забезпечення надійного виявлення стеганограм.

Максимальне значення відстані $d_{c,s}^{\mathbf{F}}$ у виразі (2.11) досягається у випадку, коли вектори $\mathbf{f}(c)$ та $\mathbf{f}(s, \Delta_\alpha^S)$ розташовані на протилежних сторонах відповідних кластерів векторів $\mathbf{F}(c)$ і $\mathbf{F}(s)$ (рис. 2.1). Внаслідок цього, оптимальне перетворення $\mathcal{K}_{opt}(\cdot)$ за критерієм максимізації значення $d_{c,s}^{\mathbf{F}}$ у виразі (2.11) буде відповідати оцінці вихідного виду ЗК за наявними (зашумленими) зображеннями (для SE-методів, \mathcal{K}_{opt}^{CE}), або ж вилучення спотворень ЗК, обумовлених прихованням повідомлень (для SE-методів, \mathcal{K}_{opt}^{SE}):

$$\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y}): \mathbf{Y}(\Delta_\alpha^S) \xrightarrow{\forall \Delta_\alpha^S \geq 0} \mathbf{X}, \quad (2.12)$$

$$\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y}): \mathbf{X} \xrightarrow{\forall \Delta_\alpha^S \geq 0} \mathbf{Y}(\Delta_\alpha^S), \quad (2.13)$$

де значення $\Delta_\alpha^S = 0$ відповідає використанню зображення-контейнеру. Застосування запропонованих перетворень (2.12)-(2.13) призводить до зсуву кластерів $\mathbf{F}(c)$ і $\mathbf{F}(s)$ до відповідних положень (рис. 2.1):

- Для перетворення \mathcal{K}_{opt}^{CE} – $\mathbf{F}_r(c) = \mathbf{F}(c)$, $\mathbf{F}_r(s) = \mathbf{F}(c)$;
- Для перетворення \mathcal{K}_{opt}^{SE} – $\mathbf{F}_r(c) = \mathbf{F}(s)$, $\mathbf{F}_r(s) = \mathbf{F}(s)$.

Це призводить до того, що СД може бути налаштований з використанням наступних типів векторів, що відповідають статистичним параметрам досліджуваних ЦЗ [83] [65]:

$$\mathbf{F}_{LF} = a \cdot F_{cal}^{\mathcal{M}}(\mathbf{U}) + b \cdot F^{\mathcal{M}}(\mathbf{U}), \quad (2.14)$$

$$\mathbf{F}_{CC} = \{F^{\mathcal{M}}(\mathbf{U}); F_{cal}^{\mathcal{M}}(\mathbf{U})\}, \quad (2.15)$$

де $a, b \in \mathbb{R}$ – вагові коефіцієнти; $F^{\mathcal{M}}(\mathbf{U}), F_{cal}^{\mathcal{M}}(\mathbf{U})$ – вектори, що відповідають статистичним параметрам вихідного та обробленого зображення \mathbf{U} , отриманим з використанням статистичної моделі \mathcal{M} відповідно; \mathbf{F}_{LF} – вектори, що відповідають лінійній формі векторів (статистичних параметрів) вихідних та оброблених цифрових зображень; \mathbf{F}_{CC} – відповідають випадку використання ознак як вихідного, так і попередньо обробленого ЦЗ.

В загальному випадку значення коефіцієнтів a та b у виразі (2.14) може обиратися довільним чином, проте для практичних застосувань становлять інтерес наступні випадки:

$$\mathbf{F}_{nc} = \mathbf{F}_{LF}|_{a=0, b=(+1)} = F^{\mathcal{M}}(\mathbf{U}), \quad (2.16)$$

$$\mathbf{F}_{calib} = \mathbf{F}_{LF}|_{a=(+1), b=0} = F_{cal}^{\mathcal{M}}(\mathbf{U}), \quad (2.17)$$

$$\mathbf{F}_{DF} = \mathbf{F}_{LF}|_{a=(+1), b=(-1)} = F_{cal}^{\mathcal{M}}(\mathbf{U}) - F^{\mathcal{M}}(\mathbf{U}), \quad (2.18)$$

де вектори \mathbf{F}_{nc} та \mathbf{F}_{calib} відповідають статистичним параметрам вихідного та обробленого зображення \mathbf{U} , а вектор \mathbf{F}_{DF} – різниці даних векторів.

Практичне застосування векторів \mathbf{F}_{nc} (2.16) у відомих СД є обмеженим внаслідок суттєвого зменшення рівня демаскуючих ознак при використанні АСМ [65,83]. Для підвищення точності роботи СД широко використовуються \mathbf{F}_{CC} (2.15) вектори, що характерно для сучасних статистичних моделей ЗК [10,34]. Проте обмеженням практичного використання \mathbf{F}_{CC} векторів є подвоєння кількості елементів даних векторів у порівнянні з \mathbf{F}_{nc} (2.16) векторами, що призводить до підвищення вимог щодо кількості зображень в пакеті \mathcal{S}_{train} .

За результатами використання перетворень \mathcal{K}_{opt}^{CE} (2.12) та \mathcal{K}_{opt}^{SE} (2.13) стає можливим обчислення векторів \mathbf{F}_{calib} (2.17) та \mathbf{F}_{DF} (2.18). Враховуючи, що досліджувані перетворення \mathcal{K}_{opt}^{CE} і \mathcal{K}_{opt}^{SE} спрямовані на визначення статистичних параметрів ЗК, або ж виділення спотворень зображення-контейнеру, обумовлених прихованням повідомлень, значення \mathbf{F}_{calib} та \mathbf{F}_{DF} буде збігатися для ЗК та стеганограм оброблених з використанням даних перетворень. Це

призводить до зниження точності роботи СД при використанні даного типу векторів (2.17)-(2.18).

З іншого боку, довжина векторів $\|\mathbf{F}_{DF}\|_2$ (2.18) буде пропорційною до величини зміни статистичних параметрів ЗК, обумовлених прихованням повідомлень. При цьому значення довжини векторів \mathbf{F}_{DF} буде відмінне від нуля лише для стеганограм при використанні SE-методів. Це дозволяє спростити виявлення стеганограм шляхом використання простих порогових методів обробки значень $\|\mathbf{F}_{DF}\|_2$. Аналогічним чином, значення $\|\mathbf{F}_{DF}\|_2$ буде відмінним від нуля для ЗК при використанні SE-методів, внаслідок чого можемо зробити висновок щодо дуальності перетворень \mathcal{K}_{opt}^{CE} (2.12) та \mathcal{K}_{opt}^{SE} (2.13). Це призводить до того, що застосування даних перетворень для обробки ЦЗ при налаштуванні СД призведе до однакової точності виявлення стеганограм, що буде визначатися лише особливостями використовуваної моделі ЦЗ, а саме значення інформаційної метрики Фішера $g_{jk}(\boldsymbol{\theta})$ (2.3), та відстані Кульбака-Лейблера $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.4) між імовірнісними розподілами оброблених ЗК та стеганограм. Тому в подальших дослідження будуть наведені результати лише для випадку використання перетворення \mathcal{K}_{opt}^{CE} .

За результатами проведених автором досліджень [65,81-83,91] отримано оцінки досяжної точності роботи стегодетектору при використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) для новітніх стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153], розглянутих в розділі 1. Дослідження проводилося при використанні стандартної статистичної моделі SPAM [38] та пакетів зображень ALASKA [134], VISION [196] та MIRFlickr [197].

На першому етапі, проведено дослідження точності виявлення стеганограм, сформованих згідно сучасного стеганографічного методу HUGO, при варіації значення параметру K_{α}^{OL} для стандартного пакету ALASKA. Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно адаптивного методу

HUGO, при використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{nc} (2.16), \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) представлені на рис. 2.6.

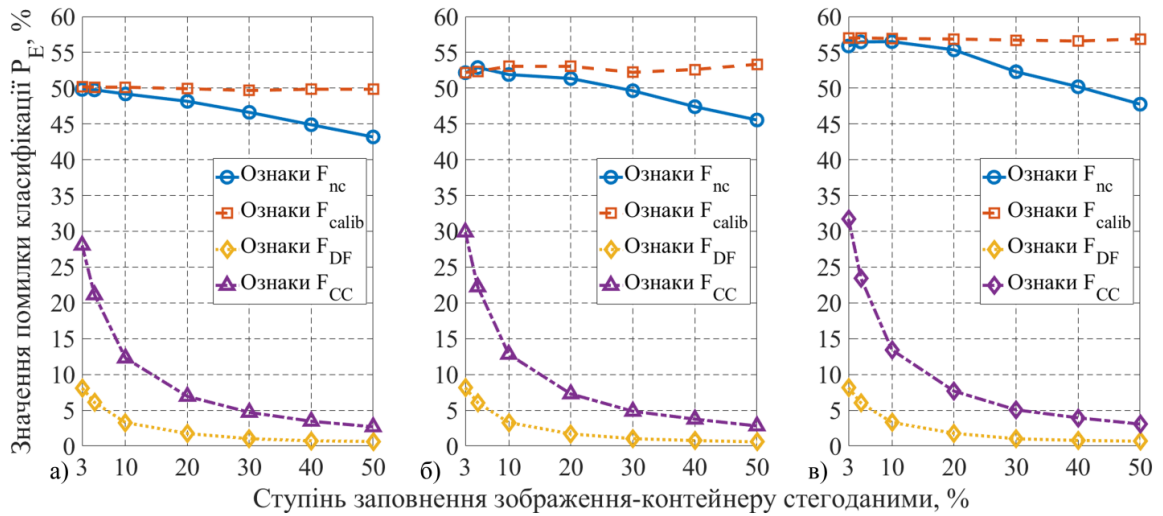


Рисунок 2.6 – Залежності значень помилки виявлення стеганогам P_E від ступеня заповнення ЗК стегоданими для стеганогам, сформованих згідно стеганографічного метод HUGO, при використанні перетворення \mathcal{K}_{opt}^{CE} для бази даних ALASKA та варіації параметру K_α^{OL} : (а) – $K_\alpha^{OL} = 100\%$; (б) – $K_\alpha^{OL} \in \mathcal{U}(0; 100)$; (в) – $K_\alpha^{OL} = 0\%$.

Відмітимо, що зменшення значень параметру K_α^{OL} від 100% (рис. 2.6в) до 0% (рис. 2.6а) призводить до підвищення значень P_E на 5% для всіх типів розглянутих векторів. Це обумовлено поступовим зменшенням кількості пар ЗК та відповідних їм стеганогам у навчальній вибірці \mathcal{S}_{train} , що призводить до зниження точності оцінки розмірів та взаємного розташування кластерів векторів $\mathbf{F}_r(c)$ і $\mathbf{F}_r(s)$.

Варто зазначити, що варіація значень параметру K_α^{OL} в межах від 0% до 100% (рис. 2.6б) не призводить до суттєвих змін P_E у всьому діапазоні значень параметру Δ_α^S . Це свідчить, що висока точність виявлення стеганогам зберігається навіть у випадку використання лише часткових даних щодо особливостей використаного АСМ, що є важливим практичним результатом для стегоаналізу ЦЗ.

Отримані результати для випадку використання \mathbf{F}_{calib} (2.17) підтверджують зроблені раніше висновки щодо суттєвого зниження точності роботи

СД (рис. 2.6), що обумовлено рівністю статистичних параметрів вихідного та обробленого зображень. З іншого боку, застосування векторів \mathbf{F}_{DF} (2.18) дозволяє суттєво зменшити значення P_E (значення P_E є близьким до 0%) у випадку середнього та сильного ступеня заповнення ЗК стегоданими (рис. 2.6). Вагомою перевагою використання векторів \mathbf{F}_{DF} при налаштуванні СД є слабка залежність отримуваних значень P_E від значення параметру Δ_α^S , що дозволяє суттєво підвищити точність роботи СД навіть у найбільш складному випадку слабого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$).

Застосування векторів \mathbf{F}_{CC} (2.15) при налаштуванні СД також призводить до суттєвого зниження значень P_E у порівнянні з випадком використання векторів \mathbf{F}_{nc} (від 47% для векторів \mathbf{F}_{nc} до 8% для векторів \mathbf{F}_{CC} для випадку $\Delta_\alpha^S = 20\%$, рис. 2.6). Тим не менше, отримані значення P_E у випадку використання векторів \mathbf{F}_{CC} перевищують відповідні значення P_E для векторів \mathbf{F}_{DF} – відмінність сягає до 20% у випадку $\Delta_\alpha^S < 10\%$. Отриманий результат свідчить про перспективність використання \mathbf{F}_{DF} векторів для підвищення точності роботи СД у порівнянні з поширеною практикою використання \mathbf{F}_{CC} векторів [34].

Для порівняння, на рис. 2.7 наведено залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно адаптивного методу S-UNIWARD, при використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{nc} (2.16), \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15).

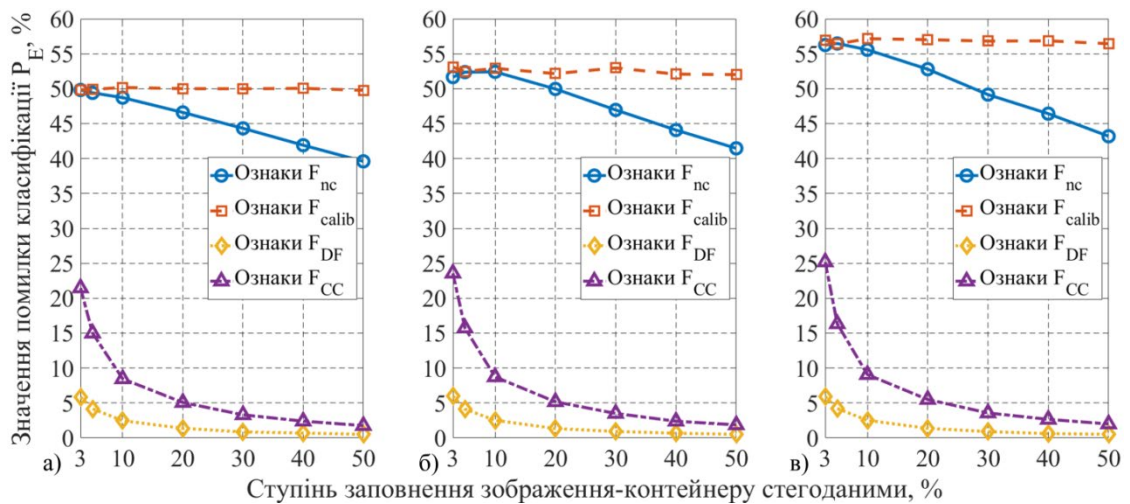


Рисунок 2.7 – Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно стеганографічного методу S-UNIWARD, при використанні перетворення \mathcal{K}_{opt}^{CE} для бази даних ALASKA та варіації параметру K_α^{OL} : (а) – $K_\alpha^{OL} = 100\%$; (б) – $K_\alpha^{OL} \in \mathcal{U}(0; 100)$; (в) – $K_\alpha^{OL} = 0\%$.

Отримані результати для стеганографічного методу S-UNIWARD (рис. 2.7) підтверджують зроблені раніше висновки, щодо високої ефективності використання перетворення \mathcal{K}_{opt}^{CE} для мінімізації значень P_E в широкому діапазоні значень параметру Δ_α^S . Зокрема, зниження значень P_E для стеганографічного методу S-UNIWARD (рис. 2.7) перевищує відповідні результати для методу HUGO (рис. 2.6) – значення ΔP_E сягають 3%-5% в області слабкого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$), та прямують до нуля при зростанні значення параметру Δ_α^S .

Враховуючи отримані результати (рис. 2.6-2.7), становить інтерес дослідження точності виявлення стегограм, сформованих при використанні новітніх адаптивних методів MG та MiPOD, та застосуванні перетворення \mathcal{K}_{opt}^{CE} . Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно адаптивних методів MG та MiPOD, при використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{nc} (2.16), \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) представлені на рис. 2.8.

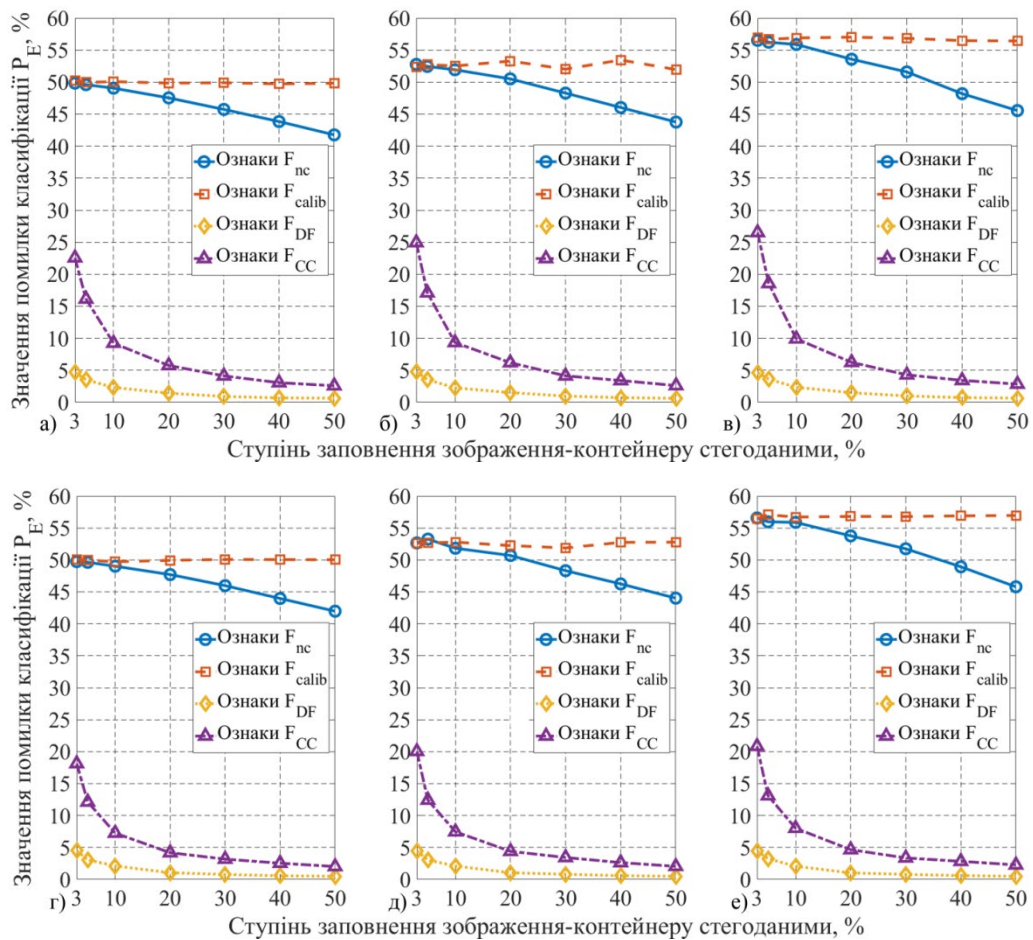


Рисунок 2.8 – Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно стеганографічних методів MG (а-в) та MiPOD (г-е), при використанні перетворення \mathcal{K}_{opt}^{CE} для бази даних ALASKA та варіації параметру K_α^{OL} :

(а, г) – $K_\alpha^{OL} = 100\%$; (б, д) – $K_\alpha^{OL} \in \mathcal{U}(0; 100)$; (в, е) – $K_\alpha^{OL} = 0\%$.

Використання перетворення \mathcal{K}_{opt}^{CE} дозволяє суттєво зменшити значення помилки P_E при використанні векторів \mathbf{F}_{DF} та \mathbf{F}_{CC} (рис. 2.8) для досліджуваних АСМ у порівнянні з отриманими в розділі 1 оцінками точності роботи СД на основі статистичних моделей ЗК (рис. 1.17-1.20) та штучних нейронних мереж (рис. 1.21-1.23). Зменшення значень P_E в області слабого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$) сягає до 60% для статистичної моделі maxSRMd2 (табл. 1.1) та до 12% для мережі ASSAF (табл. 1.2) при використанні векторів \mathbf{F}_{DF} (рис. 2.8). При цьому використання перетворення \mathcal{K}_{opt}^{CE} та векторів \mathbf{F}_{DF} дозволяє наблизити значення помилки P_E практично до нуля

при зростанні значень параметру Δ_{α}^S , що суттєво перевищує відповідні результати для сучасних СД.

Таким чином, можемо зробити висновок, що досяжна точність виявлення стеганограм, сформованих згідно АСМ, при використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{DF} (2.18) суттєво перевищує поточні результати для СД на основі статистичних моделей ЦЗ та ШНМ для зображень-контейнерів зі стандартного пакету ALASKA [134] в широкому діапазоні значень параметрів K_{α}^{OL} та Δ_{α}^S . Внаслідок цього подальший інтерес становить аналіз досяжної точності виявлення стеганограм при використанні запропонованих методів у випадку обробки ЦЗ, що характеризуються значною варіативністю статистичних параметрів, для найбільш складного випадку обмеженості апіорних даних щодо особливостей ($K_{\alpha}^{OL} = 0\%$). Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно розглянутих стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD, при використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{nc} (2.16), \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) представлені на рис. 2.9.

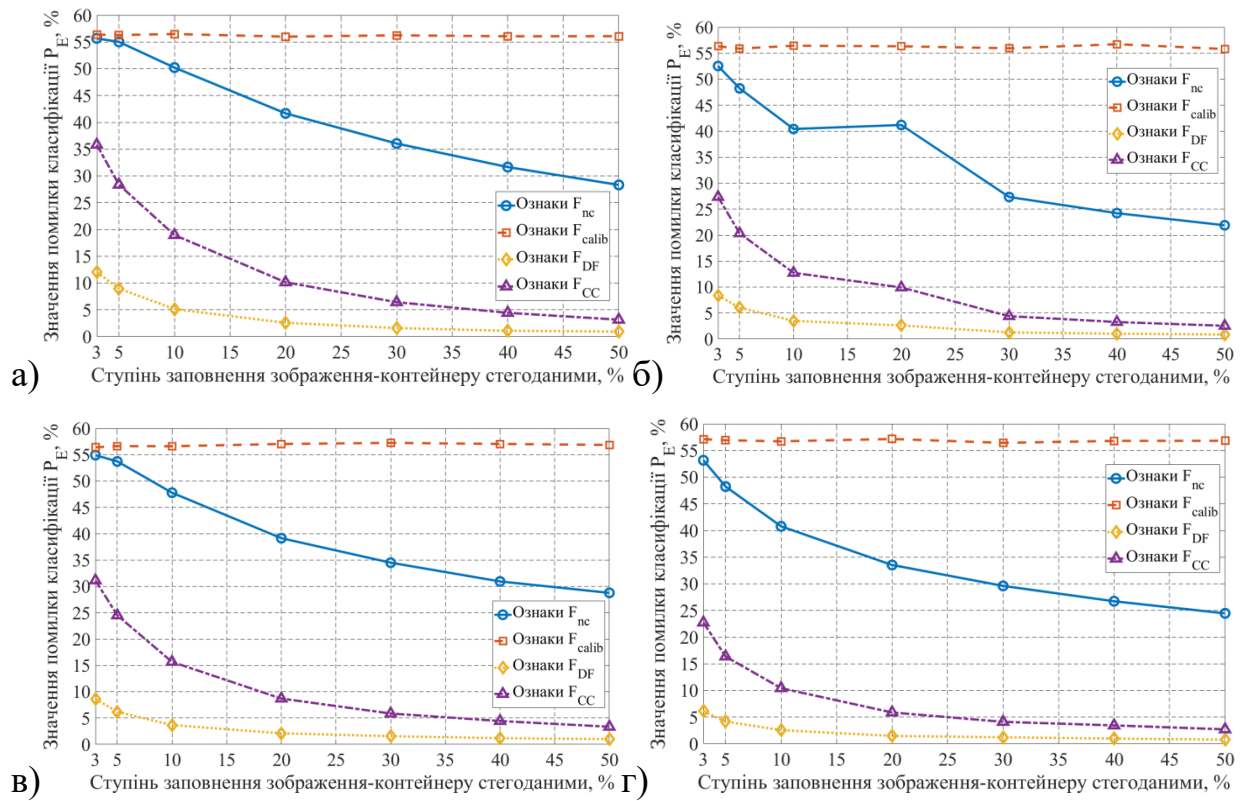


Рисунок 2.9 – Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно стеганографічних методів HUGO (а), S-UNIWARD (б), MG (в) та MiPOD (г), при використанні перетворення \mathcal{K}_{opt}^{CE} для бази даних VISION та значенні параметру $K_\alpha^{OL} = 0\%$.

Попередня обробка досліджуваних зображень із застосуванням перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{DF} (2.18) дозволяє суттєво зменшити значення P_E ($\Delta P_E \cong 50\%$) у порівнянні з випадком використання векторів \mathbf{F}_{nc} (2.16), що відповідають випадку використання вихідних ЦЗ. При цьому зниження значення P_E досягається навіть у найбільш складному випадку слабого заповнення ЗК стегоданими, що становить особливий інтерес для побудови високоточних СД.

Відмітимо, що зменшення значень P_E при використанні векторів \mathbf{F}_{DF} (2.18) для розглянутих пакетів ALASKA (рис. 2.6-2.8) та VISION (рис. 2.9) є співставним в області слабого та середнього ступеня заповнення ЗК стегоданими ($\Delta_\alpha^S \leq 20\%$). З іншого боку, зменшення значень P_E для пакету VISION

($\Delta P_E \cong 30\%$) дещо поступається відповідним результатам для пакету ALASKA ($\Delta P_E \cong 45\%$) у випадку $\Delta \alpha^S > 20\%$. Це пояснюється меншим рівнем власних шумів ЦЗ для бази VISION у порівнянні з пакетом ALASKA (рис. 1.10), що призводить до зниження ефективності АСМ щодо «маскування» приховання повідомлень з використанням власних шумів ЗК.

Для порівняння, також розглянуто випадок використання перетворення \mathcal{K}_{opt}^{CE} (2.12) для обробки реальних ЦЗ з пакету MIRFlickr. Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно розглянутих стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD, при використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{nc} (2.16), \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) представлені на рис. 2.10.

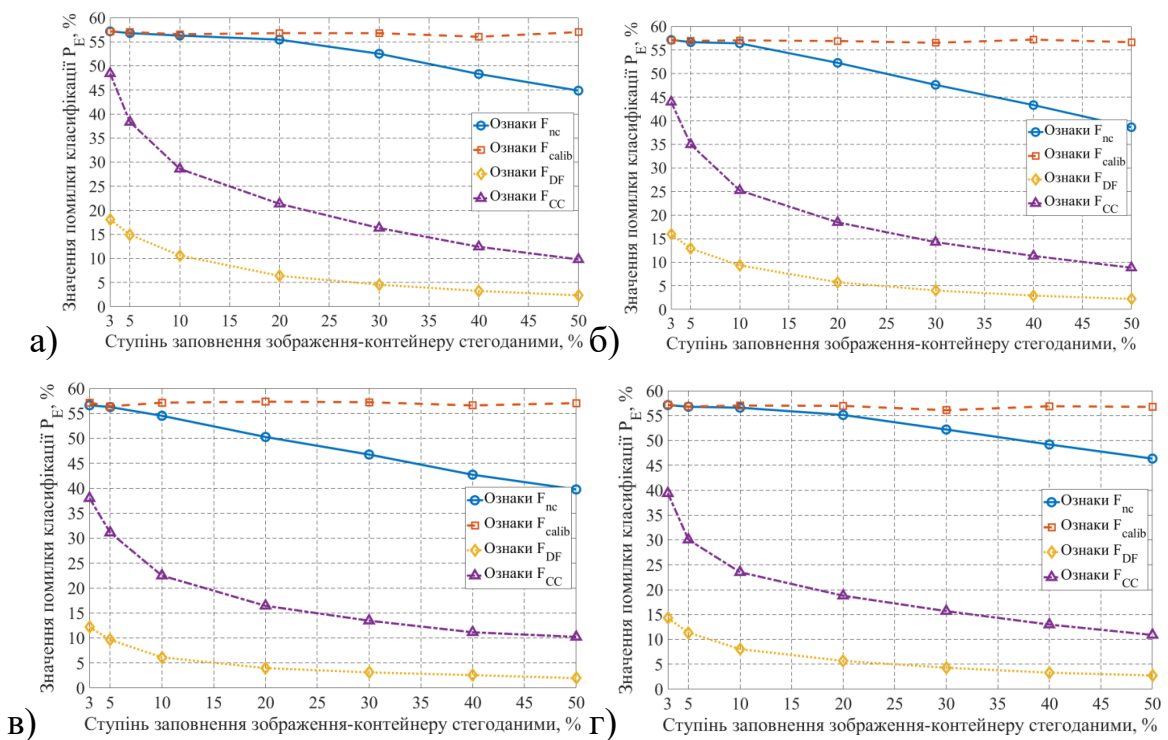


Рисунок 2.10 – Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно стеганографічних методів HUGO (а), S-UNIWARD (б), MG (в) та MiPOD (г), при використанні перетворення \mathcal{K}_{opt}^{CE} для бази даних MIRFlickr та значенні

параметру $K_{\alpha}^{OL} = 0\%$.

Відмітимо, що висока ефективність застосування використанні перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{DF} (2.15) зберігається при обробці реальних ЦЗ, що характеризуються високим рівнем власних шумів (рис. 1.10). При цьому зниження значень P_E є суттєвим ($\Delta P_E \cong 40\%$) у всьому діапазоні значень ступеня заповнення ЗК стегоданими (рис. 2.10) у порівнянні з використанням векторів \mathbf{F}_{nc} (2.16), \mathbf{F}_{calib} (2.17) та \mathbf{F}_{CC} (2.15).

Отримані результати дозволяють оцінити досяжну вірогідність виявлення стеганограм при використанні оптимальних типів методів попередньої обробки $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ (2.12) та $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ (2.13) за критерієм мінімізації значення P_E . Відмітимо суттєве зниження значень помилки виявлення стеганограм P_E при використанні даних методів та векторів \mathbf{F}_{DF} (2.18) у порівнянні з випадком використання поширених типів векторів \mathbf{F}_{nc} (2.16) та \mathbf{F}_{CC} (2.15). Тому становить інтерес розробка математичного апарату побудови оптимальних методів попередньої обробки ЦЗ, що дозволяють мінімізувати значення помилки P_E при обмеженості апріорних даних щодо використаного СМ та значної варіативності статистичних параметрів досліджуваних ЦЗ.

2.2.3 Теоретичний аналіз досяжної точності виявлення стеганограм

Для оцінки стійкості (робастності) стеганографічного методу до відомих методів статистичного аналізу, зазвичай, використовується теоретико-інформаційний підхід [10,35]. Даний підхід заснований на дослідженні відмінностей між імовірнісними розподілами значень яскравості пікселів зображення-контейнеру (P_X) та стеганограм (P_Y) з використання відстані Кульбака-Лейблера (2.4). Згідно теореми Качина встановлюється, що стеганографічний метод є ε –стійким

$$D_{KL}(\mathbf{X}, \mathbf{Y}) \leq \varepsilon, \varepsilon \geq 0, \quad (2.19)$$

до виявлення з використанням статистичних стегодетекторів при виконанні наступної умови [35,218]:

$$H(P_{FA}, P_{MD}) \leq \varepsilon, \quad (2.20)$$

$$H(\alpha, \beta) = \alpha \times \log_2 \frac{\alpha}{1 - \beta} + (1 - \alpha) \times \log_2 \frac{1 - \alpha}{\beta},$$

де P_{FA}, P_{MD} – відповідно, значення імовірність помилки першого (хибне віднесення ЗК до класу стеганограм) та другого (хибна класифікація стеганограм як зображень-контейнерів) роду; $H(\alpha, \beta)$ – функція визначення бінарної ентропії. В частковому випадку, якщо метод виявлення стеганограм дозволяє мінімізувати частку помилок першого роду ($P_{FA} \cong 0$), отримуємо нижню границю оцінки значення кількості помилок P_{MD} :

$$P_{MD} \geq 2^\varepsilon. \quad (2.21)$$

Відповідно, для абсолютно стійкої стеганографічної системи значення константи ε у виразі (2.19) прямує до нуля, наслідком чого є принципова неможливість виявлення стеганограм при використанні методів стегоаналізу ЦЗ – значення P_{MD} у виразі (2.21) буде рівним одиниці.

Вагомим обмеженням практичного застосування теореми Качіна (2.20) є необхідність оцінки відстані Кульбака-Лейблера між нормованими імовірнісними розподілами значень яскравості пікселів ЗК та стеганограм (2.4). Як було зазначено раніше, обмеженням використання відстані Кульбака-Лейблера, зокрема у випадку слабкого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$), є близькість значень $D_{KL}(\mathbf{X}, \mathbf{Y})$ до нуля, що ускладнює перевірку виконання умови (2.19). З іншого боку, побудова нормованих гістограм розподілу значень яскравості пікселів потребує обробки всіх пікселів зображення, що відповідає випадку використання розширеної моделі ЗК (англ. direct cover model). Це призводить до суттєвого зростання обчислювальної складності даної оцінки при обробці зображень значного розміру внаслідок. Для подолання даного обмеження, в роботі Бьоме Р. [28] було запропоновано використовувати статистичні параметри досліджуваного зображення в якості його «інтегральних» характеристики (англ. indirect cover model, ICM):

$$S: \mathcal{J} \rightarrow \mathbb{R}^n, \quad (2.21)$$

де S – метод визначення статистичних параметрів досліджуваного ЦЗ; $\mathcal{J} = \{0; 1; 2; \dots; 2^k\}^{N \times M \times K}$ – множина цифрових зображень розміром $N \times M$

пікселів, що мають K каналів кольору (наприклад $K = 3$ для кольорових ЦЗ) з глибиною кольору k ($k \geq 1$) біт; n ($n \geq 1$) – кількість статистичних параметрів, що використовується для оцінки стійкості стеганограм до статистичних методів виявлення. В роботі Бьоме Р. [28] показано, що застосування статистичних показників дозволяє отримати оцінки робастності стеганографічних методів до виявлення, що аналогічними до випадку використання нормованих розподілів значень яскравості пікселів (2.19). Це обумовлено наступними чинниками [28,35]:

1. Реальні цифрові зображення не є реалізаціями істинно випадкових (стохастичних) процесів – відповідно, розподіл значень яскравості пікселів є результатом впливу ансамблю (суміші) декількох імовірнісних розподілів. Параметри даних розподілів можуть бути оцінені з використанням статистичних параметрів (наприклад, середнє значення та середньо-квандартичне значення яскравості пікселів для нормального розподілу згідно теореми BLUE [144]);
2. Застосування поширених методів обробки ЦЗ, зокрема JPEG-стиснення з втратами, призводить до характерних змін статистичних, спектральних та структурних параметрів – поява даних змін, а також їх величина (інтенсивність) може бути використано для врахування застосування поширених перетворень в стеганографічному каналі передачі з метою підвищення робастності сформованих стеганограм.

Використання ІСМ-моделі при проведенні стегоаналізу ЦЗ дозволяє представити оцінки ε – стійкості (2.19) стеганографічних методів до виявлення у наступному вигляді [28,219-221]:

$$D_{SD}(\mathbf{X}, \mathbf{Y}) = \frac{1}{2} \sum_{\mathbf{X}, \mathbf{Y} \in \mathcal{J}} \|\mathbf{f}(\mathbf{X}) - \mathbf{f}(\mathbf{Y})\|_2 \leq \varepsilon \quad (2.22)$$

$$D_{VD}(\mathbf{X}, \mathbf{Y}) = \max_{\mathbf{X}, \mathbf{Y} \in \mathcal{J}} \|\mathbf{f}(\mathbf{X}) - \mathbf{f}(\mathbf{Y})\| \leq \varepsilon, \quad (2.23)$$

де $\mathbf{f}(\mathbf{X}), \mathbf{f}(\mathbf{Y})$ – вектори, що відповідають статистичним параметрам ЗК та стеганограм відповідно.

Відмітимо, що точність оцінки ступеня стійкості сформованих стеганограм до статистичних методів виявлення у виразах (2.22)-(2.23) залежить від вибору статистичних параметрів при формуванні векторів $\mathbf{f}(\mathbf{X})$ та $\mathbf{f}(\mathbf{Y})$. В більшості випадків, використовується загальне припущення, що розподіл значень яскравості пікселів досліджуваного зображення може бути апроксимований з використанням нормального (гаусового) розподілу [28,36,222]. Це дозволяє використовувати поширені типи статистичних моделей для дослідження параметрів ЗК та стеганограм, зокрема гаусові моделі, моделі суміші імовірнісних розподілів тощо [144]. З іншого боку, даний варіант апроксимації нормованих гістограм розподілу значень яскравості пікселів оброблюваних ЦЗ призводить до того, що побудова СД відповідає вирішенню задачі розрізнення компонентів суміші гаусових процесів, що відрізняються лише значеннями математичного очікування [222]. Внаслідок цього можливо побудувати оптимальний стегодетектор за критерієм мінімізації значень помилок другого роду (P_{MD}) при фіксованому значенні помилок першого роду (P_{FA}) з використанням відношення максимальної правдоподібності L_{ML} [10]:

$$L_{ML}(\mathbf{U}) = \sum_{i=1}^n \log \frac{P_1(\mathbf{U}_i)}{P_0(\mathbf{U}_i)}, \quad (2.24)$$

для перевірки наступних гіпотез:

$$H_0: \Delta_\alpha^S = 0,$$

$$H_1: \Delta_\alpha^S > 0,$$

де $\mathbf{U} \in \mathcal{J}$ – досліджуване зображення; $P_{\Delta_\alpha^S}(\cdot), P_0(\cdot)$ – імовірності віднесення статистичних параметрів зображення до класів ЗК або стеганограм відповідно. В граничному випадку, при мінімізації ступеня заповнення ЗК стегоданими ($\Delta_\alpha^S \rightarrow 0$) отримуємо наступний вираз оцінки відношення максимальної правдоподібності (2.24):

$$L_{ML}(\mathbf{U}) = \begin{cases} \mathcal{N}\left(\left(-\frac{1}{2}\right)(\Delta_\alpha^S)^2\mathfrak{I}(0); \frac{1}{n}(\Delta_\alpha^S)^2\mathfrak{I}(0)\right), H_0 - true, \\ \mathcal{N}\left(\left(+\frac{1}{2}\right)(\Delta_\alpha^S)^2\mathfrak{I}(0); \frac{1}{n}(\Delta_\alpha^S)^2\mathfrak{I}(0)\right), H_1 - true, \end{cases} \quad (2.25)$$

$$\mathfrak{I}(\Delta_\alpha^S) = \sum_{i=1}^n \frac{1}{P_1(\mathbf{U}_i)} \left(\frac{\partial P_1(\mathbf{U}_i)}{\partial \Delta_\alpha^S} \right)^2, \quad (2.26)$$

де $\mathfrak{I}(\Delta_\alpha^S)$ – значення інформації Фішера при аналізі стеганограм, для котрих ступінь заповнення ЗК стегоданими є рівним Δ_α^S . Враховуючи, що використовується припущення щодо гаусового (нормального) розподілу значень яскравості пікселів ЗК, для оцінки точності роботи СД можливо використовувати коефіцієнт розбіжності (англ. deflection coefficient) [10]:

$$d_\zeta^2 = \frac{\left(+\frac{1}{2}\right)(\Delta_\alpha^S)^2\mathfrak{I}(0) - \left(-\frac{1}{2}\right)(\Delta_\alpha^S)^2\mathfrak{I}(0)}{(\Delta_\alpha^S)^2\mathfrak{I}(0)/n} = n \cdot (\Delta_\alpha^S)^2 \cdot \mathfrak{I}(0). \quad (2.27)$$

Запропонований метод синтезу СД шляхом вирішення оптимізаційної задачі (2.11) заснований на використанні встановлених оптимальних типів методів попередньої обробки, що дозволяють мінімізувати значення помилки стеганограм, а саме методи $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ (2.12) та $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ (2.13). З огляду на властивості даних методів, а саме внесення змін лише до стеганограм (при використанні перетворення $\mathcal{K}_{opt}^{CE}: \mathbf{F}_r(c) = \mathbf{F}(c)$), або лише до ЗК (для випадку використання перетворення $\mathcal{K}_{opt}^{SE}: \mathbf{F}_r(s) = \mathbf{F}(s)$), отримуємо що величина зміни векторів \mathbf{F}_{DF} (2.18) є пропорційною до змін параметрів ЗК при формуванні стеганограм. Це дозволяє використовувати методи $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ (2.12) та $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ (2.13), а також вектори \mathbf{F}_{DF} (2.18) для оцінки значення інформації Фішера $\mathfrak{I}(\Delta_\alpha^S)$ (2.26) – оцінки приросту інформації для стегоаналітика щодо використаного стеганографічного методу внаслідок приховання повідомлень.

Отримані результати дозволяють встановити теоретичні оцінки досяжної межі точності виявлення стеганограм при використанні запропонованого методу із застосування коефіцієнту розбіжності d_ζ^2 (2.27). При цьому отримані оцінки інформації Фішера $\mathfrak{I}(\Delta_\alpha^S)$ (2.26) узгоджуються із запропонованими

раніше параметрами $g_f(\mathbf{I})$ (2.2) та $g_{jk}(\boldsymbol{\theta})$ (2.3), що дозволяють характеризувати контур кластерів векторів, що відповідають статистичним параметрам стеганограм.

Для оцінки ступеня наближення точності роботи СД, синтезованих з використанням запропонованого методу (2.11), до теоретичних оцінок в роботі проведено дослідження досяжної імовірності P_E^{lim} виявлення стеганограм згідно квадратичного закону оцінки значень P_E^{lim} (англ. Square Root Law, SRL). Згідно SRL-закону, для сформованих стеганограм забезпечується ϵ -стійкість ($D_{KL}(\mathbf{f}(c), \mathbf{f}(s)) < \epsilon$) до виявлення з використанням статистичних СД при виконанні умови [10,199]:

$$\lim_{n \rightarrow +\infty} \Delta_\alpha^S(n) n / \sqrt{n} = 0,$$

де n – кількість пікселів ЗК, використаних для приховання стегобітів. Оцінка значення P_E^{lim} згідно SRL-закону для випадку виявлення стеганограм, сформованих згідно ACM, була запропонована в роботах Фрідріх Д. [10]:

$$\hat{P}_E^{SRL} \cong 1 - n_s \cdot D_{KL}(\mathbf{X}, \mathbf{Y}) \cdot \Delta_\alpha^S \cdot \log_2(1/\Delta_\alpha^S), \quad (2.28)$$

$$D_{KL}(\mathbf{X}, \mathbf{Y}) = \sum_{q=1}^{2^k-1} P_c(q) \cdot \log_2(P_c(q)/P_s(q)),$$

де $n_s = n/(N \times M)$ – частка пікселів ЗК, використаних для приховання стегобітів; $D_{KL}(\mathbf{X}, \mathbf{Y})$ – відстань Кульбака-Лейблера між нормованими гістограмами розподілу значень яскравості пікселів зображення-контейнеру (P_c) та стеганограм (P_s); q – рівень яскравості пікселю; k – глибина кольору (біт).

Типові залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно адаптивного методу HUGO, при використанні СД, заснованого на використанні перетворення \mathcal{K}_{opt}^{CE} (2.12), векторів \mathbf{F}_{CC} (2.15) та \mathbf{F}_{DF} (2.18) при обробці зображень з тестового пакету ALASKA представлені на рис. 2.11.

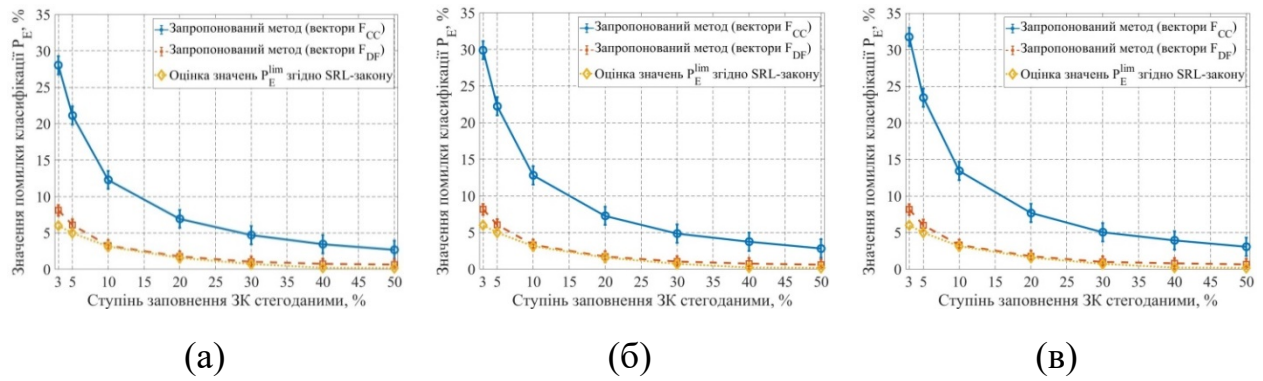


Рисунок 2.11 – Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно методу HUGO, при використанні перетворення \mathcal{K}_{opt}^{CE} для пакету ALASKA та варіації параметру K_α^{OL} : (а) – $K_\alpha^{OL} = 100\%$; (б) – $K_\alpha^{OL} \in \mathcal{U}(0; 100)$; (в) – $K_\alpha^{OL} = 0\%$. Значення P_E наведено для довірчого інтервалу з рівнем довіри 95%

Використання векторів F_{CC} (2.15) відповідає поширеній практиці налаштування сучасних СД із застосуванням статистичних параметрів як вихідних, так і оброблених зображень. Це дозволяє наблизити точність роботи СД до теоретичних оцінок досяжної імовірності виявлення стегограм згідно SRL-закону (2.28) в області сильного заповнення ЗК стегоданими ($\Delta_\alpha^S > 20\%$, рис. 2.11).

Використання запропонованого підходу до синтезу СД дозволяє забезпечити точність роботи стегодетекторів близькою до теоретичних оцінок (2.28) навіть у випадку обробки ЦЗ, що характеризуються високим ступенем варіативності статистичних, спектральних та структурних параметрів. Це підтверджується результатами дослідження точності роботи синтезованих СД для виявлення стегограм, сформованих згідно адаптивних методів HUGO, S-UNIWARD, MG та MiPOD, при обробці зображень з тестового пакету VISION (рис. 2.12).

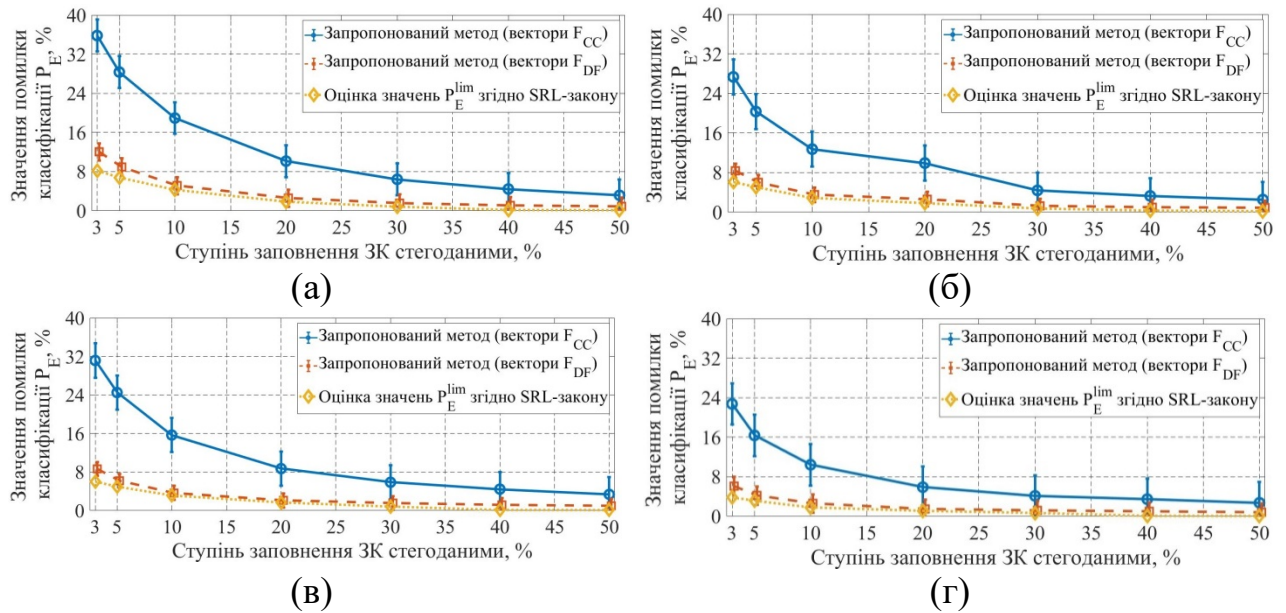


Рисунок 2.12 – Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно методів HUGO (а), S-UNIWARD (б), MG (в) та MiPOD (г), при використанні перетворення \mathcal{K}_{opt}^{CE} для пакету VISION та значенні параметру $K_\alpha^{OL} = 0\%$.

Значення P_E наведено для довірчого інтервалу з рівнем довіри 95%

Результати оцінки точності роботи СД, синтезованих згідно запропонованого методу, на пакеті VISION (рис. 5) підтверджують отримані раніше дані для пакету ALASKA (рис. 4) – застосуванням перетворення \mathcal{K}_{opt}^{CE} (2.12) та векторів \mathbf{F}_{DF} (2.18) дозволяє суттєво (на 25%) зменшити значення P_E у порівнянні з поширеним випадком використання векторів \mathbf{F}_{CC} (2.15). При цьому використання запропонованого методу побудови високоточних СД шляхом вирішення оптимізаційної задачі (2.11) дозволяє наблизити точність виявлення стегограм до теоретичних оцінок (2.28) досяжної точності роботи СД згідно SRL-закону навіть для новітніх стегографічних методів MG та MiPOD (рис. 2.12). Це підтверджує перспективність використання синтезованих стегодетекторів для забезпечення високої точності виявлення стегограм, сформованих згідно новітніх ACM.

2.3 Розробка методів синтезу та параметричної оптимізації високоточних стегодетекторів для цифрових зображень

Сучасні методи попередньої обробки ЦЗ дозволяють підвищити відмінності між векторами, що відповідають статистичним параметрам ЗК та стеганограм (рис. 2.1, відстань \mathbf{m}_{r_s}), лише для окремих випадків, зокрема відомих методів приховання повідомлень [83,84], фіксованого ступеня заповнення ЗК стегоданими [223], застосування поширених процедур обробки ЦЗ, зокрема стиснення з втратами [159] тощо. Дані методи спрямовані на виявлення лише специфічних змін статистичних параметрів ЗК, обумовлених прихованням повідомлень згідно поширених типів СМ [9,10,13], що суттєво обмежує застосування даних методів в умовах обмеженості апріорних даних щодо використаного АСМ. Забезпечення високої точності виявлення стеганограм в даному випадку потребує комплексного застосування декількох методів попередньої обробки ЦЗ, що є екстенсивним підходом та призводить до суттєвого зростання складності налаштування СД.

За результатами аналізу даних, отриманих в попередньому розділі, встановлено, що використання перетворень $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ (2.12) та $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ (2.13), а також векторів \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) дозволяє суттєво зменшити значення P_E навіть у найбільш складних випадках слабого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$) та обмеженості апріорних даних щодо використаного АСМ ($K_\alpha^{OL} = 0\%$). Проте практичне застосування даних перетворень має суттєві обмеження, оскільки потребує визначення статистичних параметрів ЗК або ж стеганограм за наявними (зашумленими) ЦЗ, що є неможливим в більшості практичних випадків.

Для подолання даного обмеження, в роботі розроблено підхід до практичної реалізації перетворень \mathcal{K}_{opt}^{CE} та \mathcal{K}_{opt}^{SE} , що дозволяє адаптивним чином обирати параметри даних перетворень, в залежності від наявних апріорних даних щодо особливостей використаного СМ, а також статистичних, спектральних та структурних параметрів досліджуваних ЦЗ (рис. 2.13).

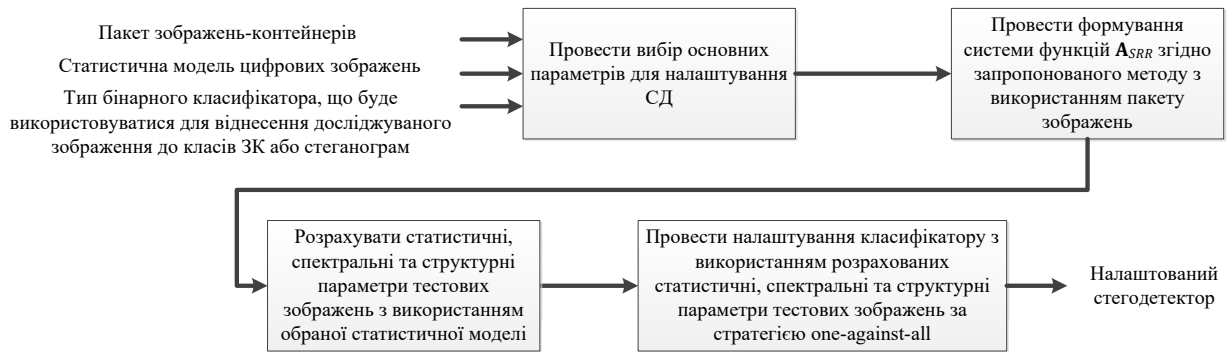


Рисунок 2.13 – Запропонований метод синтезу високоточних стегодетекторів шляхом вирішення оптимізаційної задачі (2.11).

Відмітимо, що розглянуті перетворення \mathcal{K}_{opt}^{CE} та \mathcal{K}_{opt}^{SE} засновані на оцінці вихідного виду ЗК за наявними (зашумленими) зображеннями (для \mathcal{K}_{opt}^{CE}), або ж вилучення спотворень ЗК, обумовлених прихованням повідомлень (для \mathcal{K}_{opt}^{SE}). При цьому практичне застосування перетворення \mathcal{K}_{opt}^{SE} потребує детектування спотворень ЗК, обумовлених вбудовуванням стегоданих, що в більшості випадків проводиться на рівні власних шумів ЗК [11,34]. Також дане перетворення потребує доступу стегоаналітиків до СК для формування стеганограм, що є неможливим в реальних випадків проведення стегоаналізу ЦЗ.

Для забезпечення надійного детектування спотворень ЗК, обумовлених вбудовуванням стегоданих, запропоновано використовувати новітні методи зменшення рівня власних шумів ЦЗ (рис. 2.13), зокрема ЗнАЕ в стегодетекторі на основі моделі ASSAF [127] (розділ 1.3.4). Це дало можливість суттєво підвищити вірогідність виявлення стеганограм, сформованих згідно новітніх АСМ. Проте ефективність даних методів суттєво залежить від статистичних параметрів пакетів досліджуваних зображень, що потребує постійного переналаштування СД для роботи на нових вибірках зображень.

В роботі запропоновано використовувати математичний апарат методів оцінки вихідного виду ЗК на основі спеціальних систем функцій (ССФ) для подолання наведених обмежень сучасного підходу до побудови високоточних СД. Дані методи засновані на представленні досліджуваного сигналу $\mathbf{S} = \{s_1, s_2, \dots, s_S\}$ із застосуванням лише M ($M > 0$) найбільших коефіцієнтів

розкладу сигналу (M – елементної апроксимації) [224] при використанні надлишкової системи функцій (словника) \mathbf{A}_{SRR} .

Задачу побудови ССФ для пакету сигналів $\mathcal{S}_{train}^{SRR} = \{\mathbf{s}_i\}_{i=1}^M$ можливо представити як вирішення наступної оптимізаційної задачі [224,225]:

$$\min_{\mathbf{A}_{SRR}, \{\mathbf{x}_i\}_{i=1}^M} \sum_{i=1}^M \|\mathbf{x}_i\|_0, \|\mathbf{s}_i - \mathbf{A}_{SRR}\mathbf{x}_i\|_2 \leq \epsilon, i \in [1; M], \epsilon \geq 0, \quad (2.29)$$

де \mathbf{s}_i – поточний сигнал з вибірки $\mathcal{S}_{train}^{SRR}$; \mathbf{x}_i – вектор коефіцієнтів декомпозиції сигналу \mathbf{y}_i при використанні системи функцій \mathbf{A}_{SRR} ; \mathbf{A}_{SRR} – матриця розкладу сигналів, що утворення шляхом об'єднання (конкатенації) елементів системи функцій (векторів-стовпчиків).

В більшості випадків, кількість коефіцієнтів розкладу M є суттєво меншою за кількість елементів (відліків) досліджуваного сигналу ($M \ll \|\mathbf{x}_i\|_0, \forall i \in [1; M]$), що забезпечує «розрідженість» представлення сигналу \mathbf{S} при використанні словнику \mathbf{A}_{SRR} (значну частку нульових коефіцієнтів розкладу) [224]. Вирішення оптимізаційної задачі (2.29) дозволяє визначити як оптимальний вигляд матриці \mathbf{A} за критерієм мінімізації похибки реконструкції сигналу, так і визначити найбільш розріджене представлення сигналу \mathbf{y}_i .

Особливістю методів побудови ССФ є врахування варіативності статистичних та спектральних параметрів досліджуваних ЦЗ в процесі вирішення оптимізаційної задачі (2.29) [224,226,227]. Це дозволяє формувати системи функцій розкладу ЦЗ в залежності від наявних даних щодо параметрів ЗК та стеганограм [65]. Відповідно, запропонований метод дозволяє узагальнити поширений підхід до побудови методів попередньої обробки ЦЗ, заснованих на застосуванні спектральних та спеціалізованих перетворень з фіксованим базису розкладу сигналу, або ж використанні лише окремих статистичних параметрів ЦЗ, наприклад на основі методів компонентного аналізу [226,227].

Вибору систем функцій \mathbf{A}_{SRR} для декомпозиції сигналу згідно виразу (2.29) приділяється особлива увага [224]. Одним з напрямків вирішення даної

задачі є використання спеціалізованих типів базисів, зокрема курвлетів (англ. curvelets), контурлетів (англ. contourlets) тощо [142,224,225]. Особливістю даних базисів є забезпечення високої гладкості отримуваних сигналів, зокрема ЦЗ, що становить інтерес щодо вирішення задач зниження впливу шумів та завад для зашумлених зображень [142,225]. Застосування даних методів призводить до суттєвого зниження загального рівня шумів в оброблюваному ЦЗ, що унеможлиблює виділення та придушення локальних слабких змін (спотворень) значень яскравості пікселів ЗК, обумовлених вбудовуванням бітів приховуваного повідомлення \mathbf{M} [91].

Альтернативним підходом до побудови \mathbf{A}_{SRR} є формування ССФ за результатами аналізу заданого пакету тестових сигналів. Прикладом даного підходу є спектральні перетворення сигналів, засновані на використанні пакетів вейвлетів та бандлетів (англ. bandlet) [142,228]. Дані функції були запропоновані в роботах Койфмана Р. та Маллата С. [142] щодо формування систем функцій, які дозволяють забезпечити компроміс між частотною та часовою або просторовою роздільною здатністю перетворення. Бандлети засновані на афінних перетвореннях відомих вейвлетів, що дозволяє підвищити точність просторової локалізації контурів об'єктів на ЦЗ [142,228]. Застосування вейвлет-перетворення забезпечує високу точність відновлення (реконструкції) сигналів при збереженні відносно малої обчислювальної складності $\mathcal{O}(n \log n)$, де n рівне кількості відліків досліджуваного сигналу. З іншого боку, дані системи функцій налаштовані для обробки сигналів з заданими статистичними властивостями, зокрема властивості гладкості функцій, кінцевої дисперсії значень елементів сигналу тощо [142]. Це знижує ефективність даного підходу при обробці сигналів, що не володіють даними властивостями, зокрема ЦЗ з високим рівнем дисперсії власних завад.

В загальному випадку, задача (2.29) може мати декілька рішень (систем функцій \mathbf{A}_{SRR}) які забезпечують M –елементну апроксимацію пакету сигналів $\mathcal{S}_{train}^{SRR}$ [224]. В роботах Ахарона М. [229] теоретично доведено існува-

ння єдиного (унікального) рішення оптимізаційної задачі (2.29) для часткового випадку, коли $\epsilon = 0$ та використанні набору $\mathcal{S}_{train}^{SRR}$ з лінійно-незалежних сигналів. Тоді можливо визначити не більше $k_0 < spark(\mathbf{A}_{SRR})/2$ функцій для проведення декомпозиції сигналу згідно виразу (2.19), де $spark(\mathbf{A}_{SRR})$ – кількість лінійно-залежних стовпчиків матриці \mathbf{A}_{SRR} [224]. При цьому отримувана матриця \mathbf{A}_{SRR} є єдиною, без врахування масштабування та зміни порядку векторів-стовпчиків (отриманого набору функцій розкладу пакету сигналів $\mathcal{S}_{train}^{SRR}$). Відмітимо, що наведені вимоги щодо характеристик пакету $\mathcal{S}_{train}^{SRR}$ обмежують використання даного підходу для аналізу довільної вибірки сигналів. Це пов'язано з необхідністю повного перебору всіх можливих матриць \mathbf{A}_{SRR} , що відповідає вирішенню NP -повної задачі в загальному випадку. Тому для вирішення практичних задачах широко використовуються емпіричні методи побудови матриці \mathbf{A}_{SRR} .

Одним з поширених методів побудови матриці \mathbf{A}_{SRR} є блочно-координатний релаксаційний метод (англ. Method of optimal directions, MOD), запропонований в роботі Енгана [230], що дозволяє вирішити оптимізаційну задачу (2.29) ітеративним чином. На k –тому кроці роботи методу проводиться вирішення M оптимізаційних задач щодо мінімізації похибки реконструкції кожного \mathbf{s}_i сигналу з пакету $\mathcal{S}_{train}^{SRR}$ при використанні матриці $\mathbf{A}_{SRR}^{(k-1)}$ з попереднього $(k - 1)$ кроку. На наступному кроці, отримана матриця розкладу тестових сигналів $\mathbf{X}_{SRR}^{(k)}$ використовується для корегування елементів матриці $\mathbf{A}_{SRR}^{(k)}$ з використанням методу найменших квадратів [230]:

$$\begin{aligned} \mathbf{A}_{SRR}^{(k)} &= \underset{\mathbf{A}_{SRR}}{\operatorname{argmin}} \left\| \mathbf{S} - \mathbf{A}_{SRR} \mathbf{X}_{SRR}^{(k)} \right\|_F^2 = \\ &= \mathbf{S} \left(\mathbf{X}_{SRR}^{(k)} \right)^T \left(\mathbf{X}_{SRR}^{(k)} \left(\mathbf{X}_{SRR}^{(k)} \right)^T \right)^{-1} = \mathbf{S} \left(\mathbf{X}_{SRR}^{(k)} \right)^+ \end{aligned} \quad (2.30)$$

де $\|\cdot\|_F$ – норма Фробеніуса. Наведені кроки повторюються аж до досягнення критерію збіжності рішення, зокрема забезпечення M –елементної апроксимації навчальної вибірки сигналів (2.19).

Обмеженням практичного застосування методу MOD є відносно велика кількість кроків оптимізації у випадку обробки вибірки сигналів, статистичні параметри котрих суттєво різняться [224,225]. Це обумовлено низькою збіжністю оптимізаційної задачі (2.30) за рахунок оптимізації одночасно всіх елементів матриці \mathbf{A}_{SRR} на кожному кроці алгоритму [224,230]. Для подолання даного обмеження запропоновано вдосконалення методу K-SVD [229] (рис. 2.14) для послідовного визначення кожного елементу словника (вектору-стовпчика матриці \mathbf{A}_{SRR}). Це дозволяє підвищити швидкість роботи даного методу у випадку аналізу наборів сигналів, що характеризуються значною варіативністю параметрів [224].

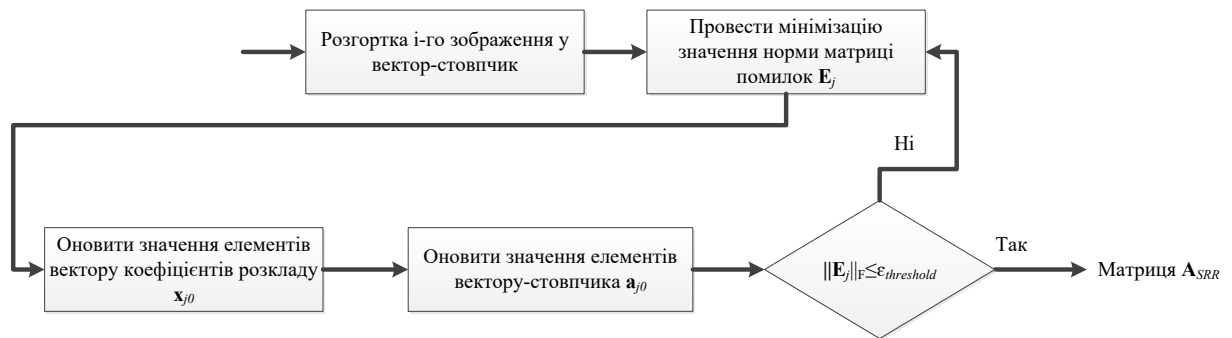


Рисунок 2.14 – Запропонований метод синтезу визначення елементів матриці \mathbf{A}_{SRR} .

Побудова словника \mathbf{A}_{SRR} згідно методу K-SVD проводиться ітеративним чином (рис. 2.14) [229]. Зокрема, визначення j_0 – тої функції розкладу (стовпчика матриці \mathbf{A}_{SRR}) проводиться шляхом використання лише \mathbf{a}_{j_0} стовпчика при обробці пакету $\mathcal{S}_{train}^{SRR}$. Це досягається за рахунок модифікації виразу (2.30) наступним чином [229]:

$$\begin{aligned}
 \|\mathbf{S} - \mathbf{A}_{SRR} \mathbf{X}_{SRR}\|_F^2 &= \left\| \mathbf{S} - \sum_{j=1}^m \mathbf{a}_j \mathbf{x}_j^T \right\|_F^2 = \\
 &= \left\| \left(\mathbf{S} - \sum_{j \neq j_0} \mathbf{a}_j \mathbf{x}_j^T \right) - \mathbf{a}_{j_0} \mathbf{x}_{j_0}^T \right\|_F^2
 \end{aligned} \tag{2.31}$$

де \mathbf{x}_j^T – відповідає j –тому рядку матриці \mathbf{X}_{SRR} . Вирішення даної оптимізаційної задачі відповідає мінімізації норми матриці \mathbf{E}_{j_0} шляхом оновлення значень \mathbf{a}_j та \mathbf{x}_j^T :

$$\|\mathbf{E}_{j_0}\|_F^2 = \left\| \left(\mathbf{s} - \sum_{j \neq j_0} \mathbf{a}_j \mathbf{x}_j^T \right) \right\|_F^2 \rightarrow \min \quad (2.32)$$

Оптимальні значення \mathbf{a}_j та \mathbf{x}_j^T , що дозволяють мінімізувати значення виразу (2.31), можуть бути отримані шляхом сингулярного розкладу матриці помилок \mathbf{E}_{j_0} (2.32). Проте в більшості випадків, це призводить до зниження ступеня розрідженості вектору \mathbf{x}_j^T , що порушує умови вихідної оптимізаційної задачі (2.29) – визначення словника \mathbf{A}_{SRR} , що забезпечує найбільш розріджене представлення тестової вибірки сигналів $\mathcal{S}_{train}^{SRR}$. Для подолання даного обмеження в роботі [229] було запропоновано використовувати лише окремий стовпчик матриці \mathbf{E}_{j_0} , що відповідає j_0 –тому елементу шуканого словника \mathbf{A}_{SRR} , та фіксації інших елементів матриці $\mathbf{E}_j, j \neq j_0$. Даний підхід дозволяє забезпечити задані властивості розкладу сигналів, зокрема розрідженість їх представлення при використанні словника \mathbf{A}_{SRR} [229].

Для отримання j_0 –того стовпчика матриці \mathbf{E}_{j_0} запропоновано використовувати оператор проєкції матриці (2.32) в простір \mathbf{P}_{j_0} . Даний оператор може бути представлений у вигляді матриці, що множиться на матрицю \mathbf{E}_{j_0} для занулення j –того стовпчику ($\forall j \neq j_0$). Матриця \mathbf{P}_{j_0} має розмір M рядків (кількість елементів у пакеті $\mathcal{S}_{train}^{SRR}$) та $M_{j_0} = M - 1$ стовпчиків (кількість елементів пакету $\mathcal{S}_{train}^{SRR}$, необхідних для визначення j_0 –того елементу шуканого словника \mathbf{A}_{SRR}).

Позначимо результат застосування оператору \mathbf{P}_{j_0} до матриці помилок \mathbf{E}_{j_0} як $(\mathbf{x}_{j_0}^R)^T = \mathbf{x}_{j_0}^T \mathbf{P}_{j_0}$. Тоді добуток матриць $\mathbf{E}_{j_0} \mathbf{P}_{j_0}$ може бути апроксимований матрицею з рангом рівним одиниці, отриманої шляхом застосування сингулярного розкладу до матриці \mathbf{E}_{j_0} (2.32). Дана апроксимація використо-

ується для оновлення значень як \mathbf{a}_{j_0} елемента словника \mathbf{A}_{SRR} , так і коефіцієнтів розкладу поточного вектору $\mathbf{x}_{j_0}^T$ при використанні \mathbf{A}_{SRR} . Відмітимо, що обчислення всіх елементів сингулярного розкладу добутку матриць $\mathbf{E}_{j_0} \mathbf{P}_{j_0}$ є надлишковою процедурою, оскільки для визначення елемента \mathbf{a}_{j_0} використовується лише апроксимація матрицею з рангом, рівним одиниці [229]. Тому для прискорення обчислень в методі K-SVD, аналогічно до методу MOD, може бути використаний блочно-координатний метод визначення елементів словника \mathbf{A}_{SRR} з використанням методу найменших квадратів. При цьому вектор коефіцієнтів розкладу $\mathbf{x}_{j_0}^T$ може бути оновлений шляхом вирішення наступної оптимізаційної задачі при фіксації поточного значення вектору \mathbf{a}_{j_0} [229]:

$$\min_{\mathbf{x}_{j_0}^R} \left\| \mathbf{E}_{j_0} \mathbf{P}_{j_0} - \mathbf{a}_{j_0} (\mathbf{x}_{j_0}^R)^T \right\|_F^2 \Rightarrow \mathbf{x}_{j_0}^R = \mathbf{P}_{j_0}^T \mathbf{E}_{j_0}^T \mathbf{a}_{j_0} / \|\mathbf{a}_{j_0}\|_2^2$$

На наступному етапі аналогічним чином проводиться оновлення вектору \mathbf{a}_{j_0} [229]:

$$\min_{\mathbf{x}_{j_0}^R} \left\| \mathbf{E}_{j_0} \mathbf{P}_{j_0} - \mathbf{a}_{j_0} (\mathbf{x}_{j_0}^R)^T \right\|_F^2 \Rightarrow \mathbf{a}_{j_0} = \mathbf{E}_{j_0} \mathbf{P}_{j_0} \mathbf{x}_{j_0}^R / \|\mathbf{x}_{j_0}^R\|_2^2$$

Метод K-SVD дозволяє суттєво зменшити обчислювальну складність формування словника \mathbf{A}_{SRR} у порівнянні з поширеними методами вирішення оптимізаційної задачі (2.30) при забезпеченні заданого ступеня розрідженості векторів розкладу \mathbf{x}_i та точності реконструкції сигналів [224,225,229]. Внаслідок цього становить інтерес застосування даного методу в якості перетворення \mathcal{K}_{opt}^{CE} (2.12) з метою оцінки вихідного виду ЗК за наявними (зашумленими) даними.

Для дослідження ефективності запропонованого методу попередньої обробки ЦЗ в роботі проведено аналіз точності роботи СД при використанні словника \mathbf{A}_{SRR} , сформованого з використанням вибірки 10,000 зображень з пакету ALASKA, що не використовувалися в попередніх розділах роботи. Враховуючи високу обчислювальну складність формування \mathbf{A}_{SRR} при оброб-

ці ЦЗ значного розміру (більше 256×256 пікселів), проведено розділення ЦЗ з тестової вибірки частини фіксованого розміру w_{UC} (пікселів), що не перекриваються. Розмір вікна розбиття w_{UC} варіювався в наступних межах – 8×8 , 16×16 , 32×32 та 64×64 (пікселів). На наступному етапі проводилося «розгортання» (перетворення) отриманих частин (матриць) у вектори-рядки, що впорядковувалися як рядки матриці \mathbf{X}_{SRR} . Загальна кількість функцій декомпозиції сигналів у словнику \mathbf{A}_{SRR} (векторів-стовпчиків) була обрана рівною N_{UC} .

Сформований словник \mathbf{A}_{SRR} використовувався для оцінки вихідного виду ЗК при обробці стеганограм, сформованих згідно стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153]. Для оцінки відмінностей між розподілами значень яскравості пікселів ЗК та стеганограм при застосуванні запропонованого методу попередньої обробки ЦЗ була використана відстань Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ (2.7). Залежності значень відстані Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно розглянутих АСМ, за відсутності методів попередньої обробки ЦЗ наведені на рис. 2.15.

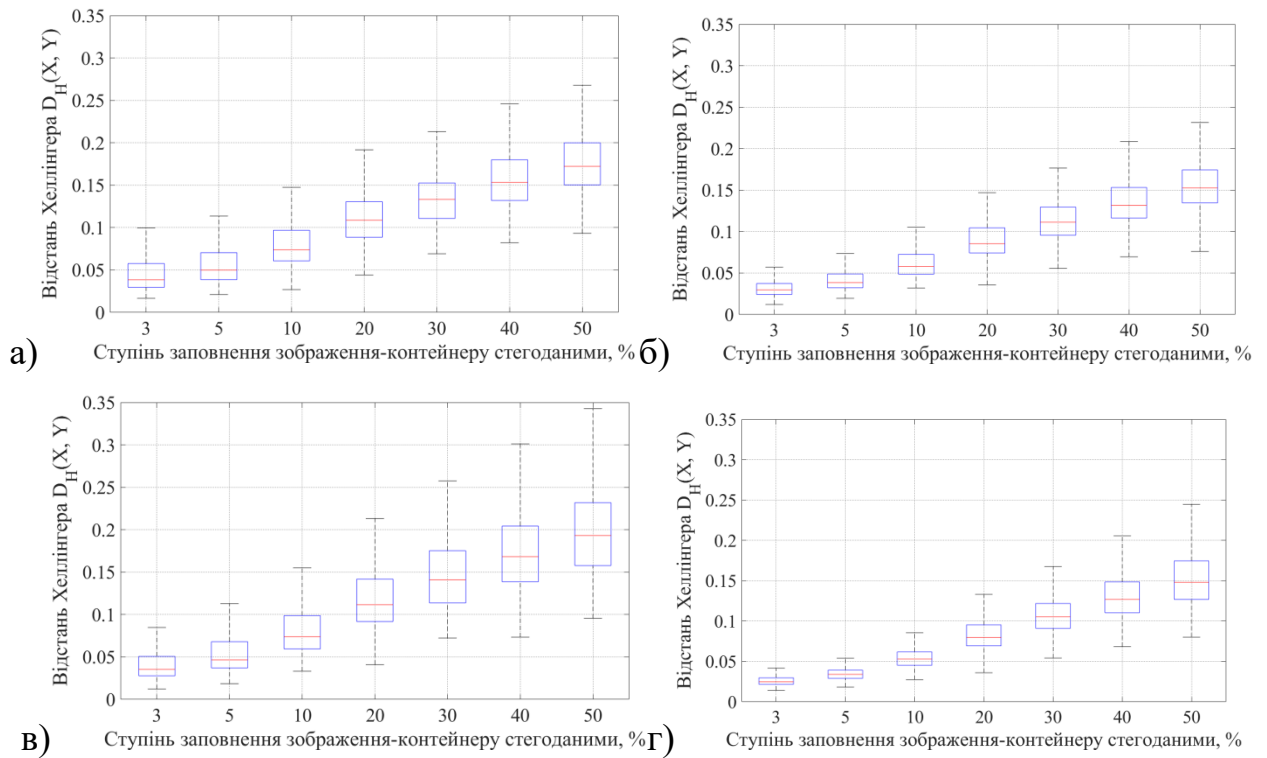


Рисунок 2.15 – Залежності значень відстані Хеллінгера $D_H(X, Y)$ між розподілами значень яскравості пікселів ЗК та стегограм від ступеня заповнення ЗК за відсутності методів попередньої обробки досліджуваних зображень для стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Відмітимо суттєві відмінності значень відстані Хеллінгера D_H для досліджуваних стеганографічних методів – відомий метод HUGO (рис. 2.15а) характеризується більшими значеннями D_H у порівнянні з новітнім методом MiPOD (рис. 2.15г). Це підтверджує зроблений раніше висновок (розділ 2.2.1) щодо високої точності оцінки відмінностей між змінами статистичних параметрів ЗК, обумовлених прихованням повідомлень при використанні сучасних АСМ. Для порівняння на рис. 2.16 наведені залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стегограм при використанні запропонованого підходу до проведення попередньої обробки ЦЗ ($w_{UC} = 16$, $N_{UC} = 512$).

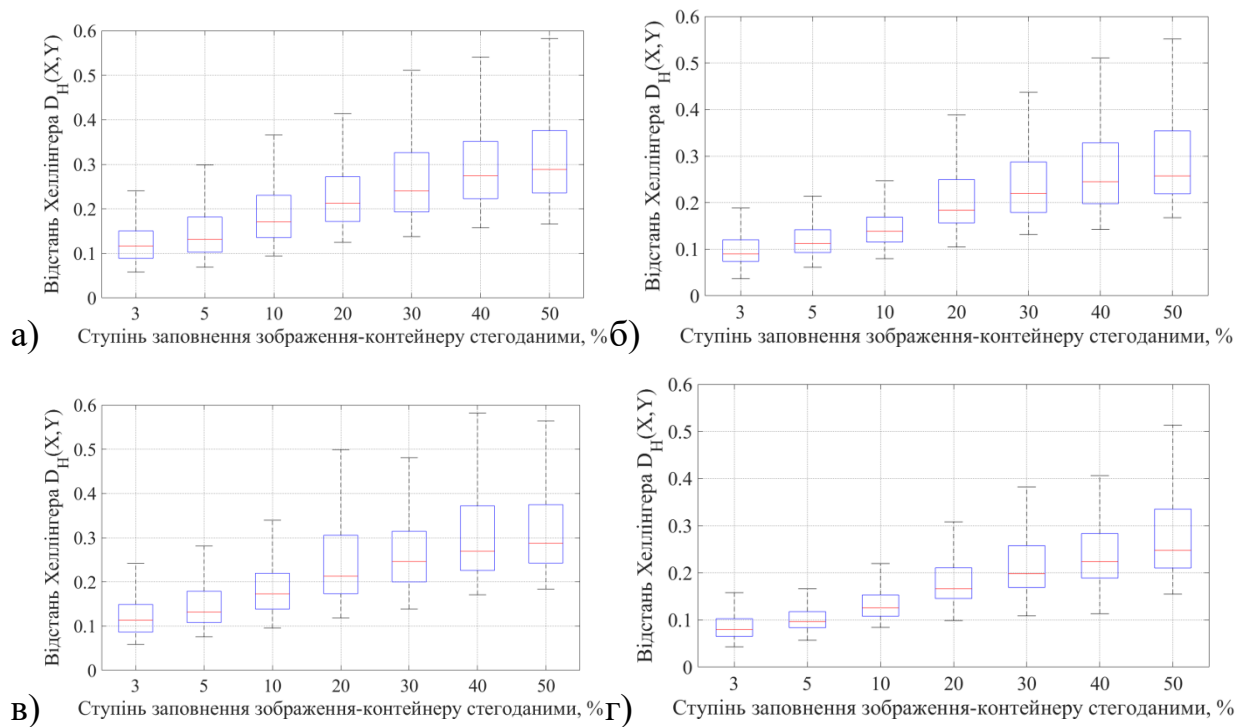


Рисунок 2.16 – Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм від ступеня заповнення ЗК стегоданими при використанні запропонованого підходу до проведення попередньої обробки ЦЗ ($w_{UC} = 16$, $N_{UC} = 512$) для стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Використання запропонованого підходу дозволяє суттєво (до двох разів) збільшити значення відстані D_H між розподілами значень яскравості пікселів ЗК та стеганограм навіть у випадку слабкого заповнення ЗК стегоданими (рис. 2.16). Це є вагомою перевагою у порівнянні з розглянутим випадком відсутності методів попередньої обробки ЦЗ (рис. 2.15). При цьому суттєві відмінності між отриманими значеннями D_H (рис. 2.16) зберігаються у всьому діапазоні значень ступеня заповнення ЗК стегоданими та всіх розглянутих АСМ. Це свідчить про ефективність використання сформованих словників \mathbf{A}_{SRR} для зниження впливу спотворень ЗК, обумовлених прихованням повідомлень, що дозволяє забезпечити високу точність оцінки статистичних параметрів ЗК за наявними (зашумленими) ЦЗ незалежно від типу використаних АСМ.

Відмітимо, що отримані результати (рис. 2.16) відповідають випадку використання блоків ЦЗ відносно малого розміру ($w_{UC} = 16$). Внаслідок цього становить інтерес дослідження змін відстані D_H між розподілами значень яскравості пікселів ЗК та стегограм при варіації розміру блоків розбиття w_{UC} . Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стегограм при варіації значень w_{UC} для запропонованого підходу до попередньої обробки ЦЗ ($N_{UC} = 512$) та стеганографічного методу HUGO наведені на рис. 2.17.

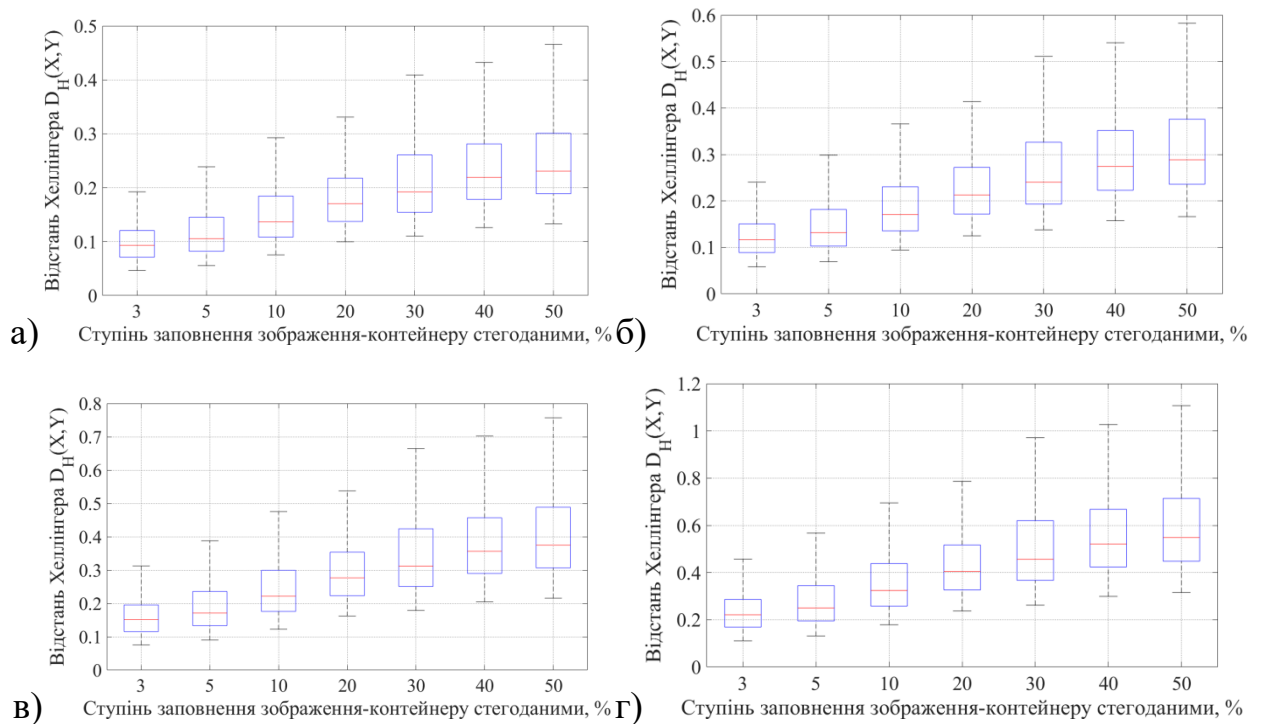


Рисунок 2.17 – Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стегограм від ступеня заповнення ЗК стегоданими при варіації значень w_{UC} для запропонованого підходу до попередньої обробки ЦЗ ($N_{UC} = 512$) для стеганографічного методу HUGO:

(а) – $w_{UC} = 8 \times 8$; (б) – $w_{UC} = 16 \times 16$; (в) – $w_{UC} = 32 \times 32$;

(г) – $w_{UC} = 64 \times 64$.

Варіація значень розміру блоків розбиття зображення w_{UC} (рис. 2.17) не призводить до суттєвих змін значень D_H при зміні ступеня заповнення ЗК стегоданими. Збільшення значень w_{UC} призводить до суттєвого ($\Delta D_H \cong 90\%$) зростання значень D_H , зокрема в області слабого заповнення ЗК стегодани-

ми ($\Delta_{\alpha}^S < 10\%$). Це дозволяє суттєво (до двох разів) підвищити значення відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм (рис. 2.15-2.17). Тому становить інтерес дослідження точності роботи СД при використанні запропонованого підходу, зокрема для випадку виявлення стеганограм, сформованих згідно сучасних АСМ.

Аналіз точності виявлення стеганограм, сформованих згідно стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153], проводився при варіації розмірів w_{UC} блоків розбиття та кількості компонентів N_{UC} розкладу досліджуваних ЦЗ. Визначення статистичних параметрів оброблених ЦЗ проводилося з використанням стандартної статистичної моделі SPAM. Залежності значень помилки виявлення стеганограм P_E , сформованих згідно стеганографічних методів HUGO та S-UNIWARD, при використанні запропонованого підходу до попередньої обробки ЦЗ та векторів \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) для зображень зі стандартного пакету ALASKA наведені на рис. 2.18.

Застосування запропонованого методу попередньої обробки ЦЗ призводить до несуттєвих змін значень P_E при використанні векторів \mathbf{F}_{calib} у всьому діапазоні значень ступеня заповнення ЗК стегоданими (рис. 2.16а-б). Це свідчить про малі відмінності у статистичних параметрах оброблених зображень, що узгоджується з отриманими раніше результатами оцінки досяжної точності виявлення стеганограм при використанні \mathbf{F}_{calib} векторів (рис. 2.6-2.8).

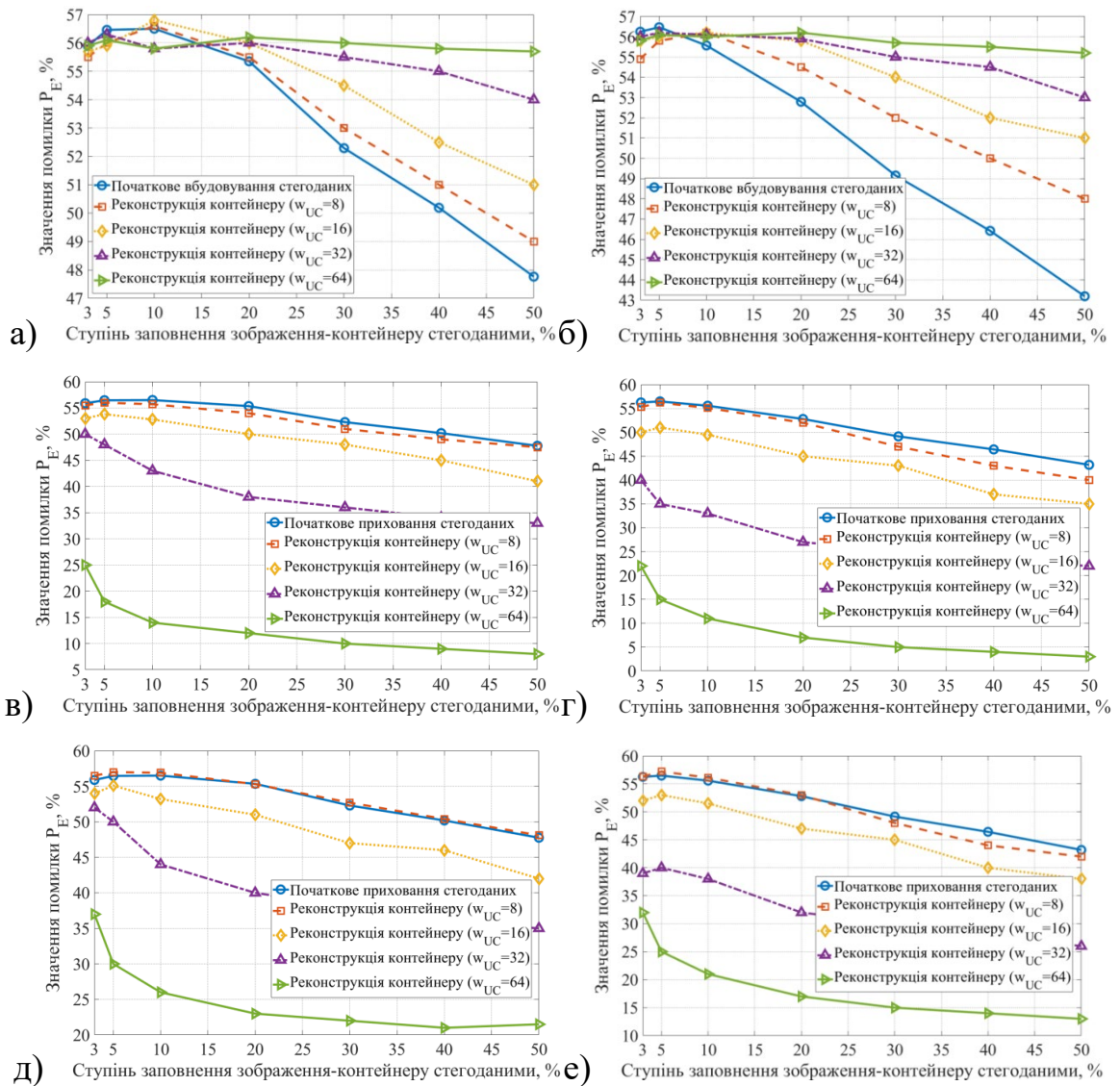


Рисунок 2.18 – Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно стегографічних методів HUGO (а, в, д) та S-UNIWARD (б, г, е), при використанні запропонованого методу попередньої обробки ЦЗ ($N_{UC} = 512$) та векторів \mathbf{F}_{calib} (а-б), \mathbf{F}_{DF} (в-г) та \mathbf{F}_{CC} (д-е) для бази даних ALASKA ($K_{\alpha}^{OL} = 0\%$).

Відмітимо, що зростання розміру w_{UC} блоків розбиття ЦЗ призводить до суттєвого ($\Delta P_E \cong 40\%$) зниження значень P_E при використанні векторів \mathbf{F}_{DF} (рис. 2.18в-г). При цьому виявлене зменшення значень P_E досягається як в області сильного ($\Delta_{\alpha}^S > 20\%$), так і слабого ($\Delta_{\alpha}^S < 10\%$) ступеня заповнення ЗК стегоданими, що є одним з найбільш складних випадків при проведенні стегоаналізу ЦЗ.

З іншого боку, отримані результати для випадку використання векторів \mathbf{F}_{CC} (рис. 2.18д-е) поступаються ($\Delta P_E \cong 3\%$) відповідним значенням при використанні векторів \mathbf{F}_{DF} (рис. 2.18в-г). Це обумовлено подвоєнням кількості елементів векторів \mathbf{F}_{CC} у порівнянні з векторами \mathbf{F}_{DF} , що ускладнює налаштування СД при використанні фіксованої кількості ЦЗ в навчальній вибірці.

Таким чином, виявлено, що використання запропонованого підходу до попередньої обробки ЦЗ дозволяє наблизити точність виявлення стеганограм до встановлених меж досяжної точності роботи СД (рис. 2.6-2.8) для адаптивних стеганографічних методів HUGO та S-UNIWARD. Тому становить інтерес використання запропонованого підходу для виявлення стеганограм, сформованих згідно новітніх методів MG та MiPOD. Як і в попередньому випадку, визначення статистичних параметрів оброблених ЦЗ проводилося з використанням стандартної статистичної моделі SPAM. Залежності значень помилки виявлення стеганограм P_E , сформованих згідно стеганографічних методів MG та MiPOD, при використанні запропонованого підходу до попередньої обробки досліджуваних зображень та векторів \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) для зображень зі стандартного пакету ALASKA наведені на рис. 2.19.

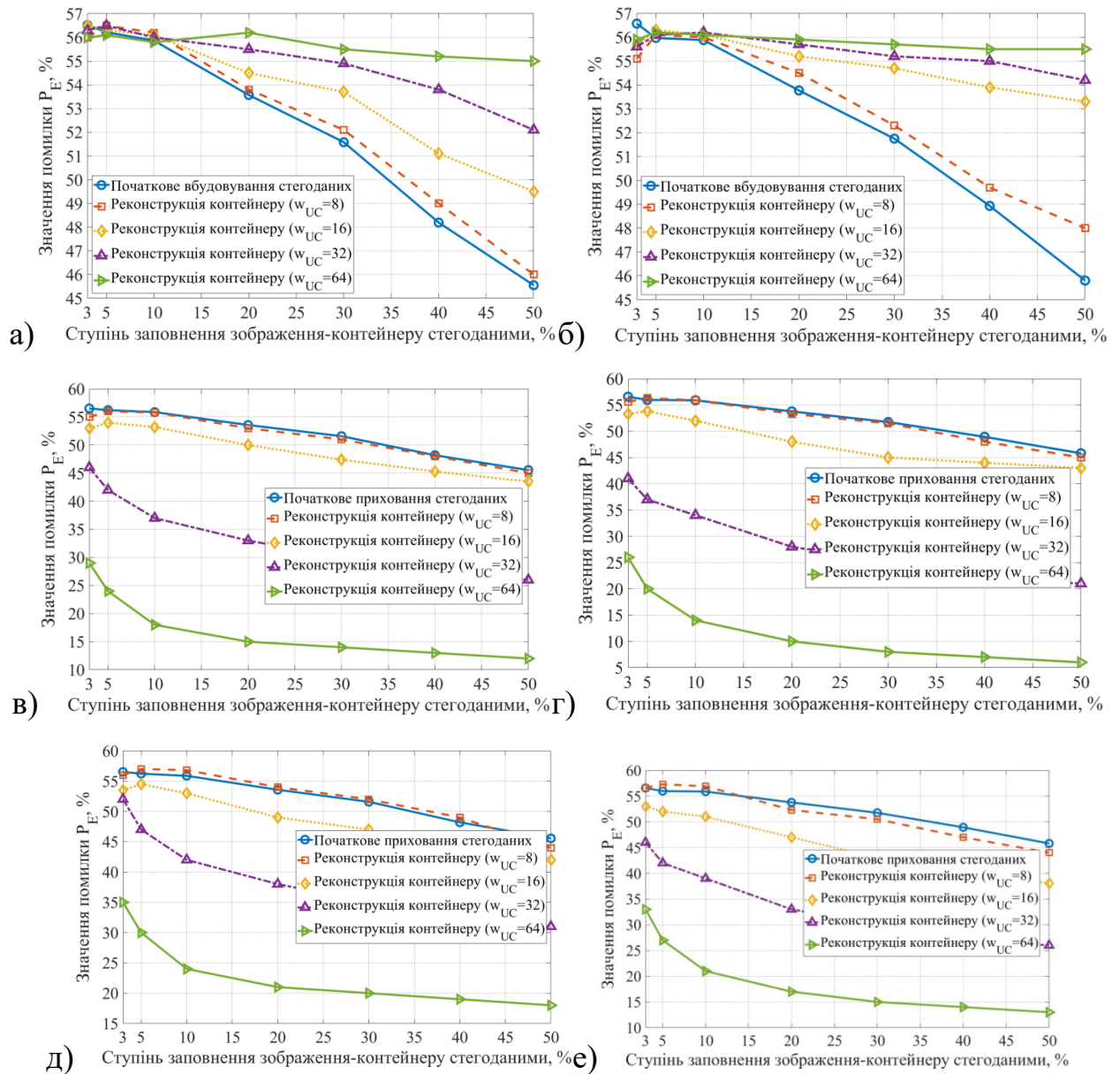


Рисунок 2.19 – Залежності значень помилки виявлення стегограм P_E від ступеня заповнення ЗК стегоданими для стегограм, сформованих згідно стеганографічних методів MG (а, в, д) та MiPOD (б, г, е), при використанні запропонованого методу попередньої обробки ЦЗ ($N_{UC} = 512$) та векторів \mathbf{F}_{calib} (а-б), \mathbf{F}_{DF} (в-г) та \mathbf{F}_{CC} (д-е) ознак для бази даних ALASKA ($K_{\alpha}^{OL} = 0\%$).

Відмітимо суттєве зменшення значень помилки виявлення стегограм ($\Delta P_E \cong 25\%$ при застосуванні запропонованого методу та векторів \mathbf{F}_{DF} , рис. 2.19в-г) навіть в області слабкого заповнення ЗК стегоданими ($\Delta S_{\alpha} < 10\%$). Це підтверджує отримані раніше результати для стеганографічних методів

HUGO та S-UNIWARD (рис. 2.18) щодо суттєвого зниження значень P_E при використанні запропонованого методу попередньої обробки ЦЗ.

Практичне застосування запропонованого методу у сучасних системах виявлення та протидії роботі прихованих каналів витоку ІзОД потребує оцінки обчислювальної складності формування словника \mathbf{A}_{SRR} при варіації розміру блоку розбиття зображення w_{UC} та кількості функцій у даному словнику. Для вирішення даної задачі було проведено оцінку тривалості побудови словника \mathbf{A}_{SRR} при використанні тестових ЦЗ зі стандартного пакету ALASKA [134] та варіації значень w_{UC} та кількості елементів M у словнику \mathbf{A}_{SRR} (рис. 2.20).

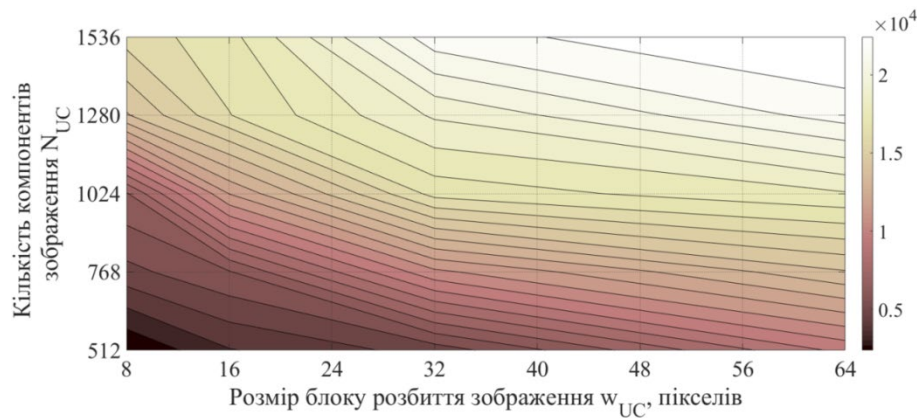


Рисунок 2.20 – Залежність тривалості формування словника \mathbf{A}_{SRR} (секунд) при використанні методу K-SVD для вибірки з 10,000 зображень з пакету ALASKA від розмірів блоку розбиття w_{UC} та кількості компонентів розкладу k_{UC} .

Збільшення розмірів блоку розбиття ЦЗ при налаштуванні словника \mathbf{A}_{SRR} призводить до лінійного зростання тривалості обробки пакету зображень (рис. 2.20). З іншого боку, зростання значень параметру k_{UC} призводить до нелінійного зростання тривалості обробки зображень, що пояснюється обчислювальною складністю визначення заданої кількості компонентів при формуванні словника \mathbf{A}_{SRR} .

Таким чином, можемо зробити висновок, що запропонований підхід до попередньої обробки ЦЗ дозволяє суттєво підвищити точність виявлення слабких змін статистичних параметрів ЗК, обумовлених прихованням пові-

домлень. Відмітимо, що вагомими перевагами даного підходу у порівнянні з сучасними методами попередньої обробки ЦЗ є:

- Формування системи функцій \mathbf{A}_{SRR} для розкладу сигналу за результатами аналізу тестової вибірки зображень – дослідження відмінностей у коефіцієнтах розкладу ЗК та стеганограм при використанні \mathbf{A}_{SRR} дозволяє визначати складові ЗК, використані при формуванні стеганограм. Це дає можливість підвищити ефективність методів деструкції стеганограм за рахунок вилучення даних компонентів;
- Врахування статистичних параметрів вибірки зображень при побудові словників \mathbf{A}_{SRR} – сучасні методи попередньої обробки ЦЗ потребують повторної оцінки параметрів (наприклад, переналаштування згорткових шарів ЗНМ) для мінімізації помилки P_E при роботі на нових пакетах ЦЗ. Властивість «розрідженості» представлення ЦЗ [224,225] дозволяє забезпечити несуттєві зміни коефіцієнтів розкладу ЦЗ при зміні їх статистичних параметрів, що суттєво зменшує тривалість переналаштування СД при роботі на нових пакетах зображень.
- Забезпечення високої точності роботи СД навіть в умовах обмеженості апріорних даних щодо використаного АСМ – досягається за рахунок «розрідженості» представлення ЗК при використанні сформованої системи функції \mathbf{A}_{SRR} , що дозволяє забезпечити високу точність оцінки статистичних параметрів ЗК за наявним (зашумленим) зображеннями.
- Збереження високої точності виявлення стеганограм в умовах зміни методів приховання повідомлень – формування словника \mathbf{A}_{SRR} за результатами обробки тестової вибірки ЗК забезпечує високу ефективність придушення спотворень, обумовлених прихованням повідомлень. Забезпечення даної властивості для сучасних СД на основі ЗНМ потребує використання ансамблю ШНМ, що суттєво підвищує обчислювальну складність процедури налаштування стегадетектору.

Варто зазначити, що потенційним обмеженням практичного використання запропонованого підходу до проведення попередньої обробки ЦЗ є висока обчислювальна складність процедури формування системи функцій \mathbf{A}_{SRR} . Це обумовлено необхідністю обробки потужної вибірки ЗК для забезпечення наведених властивостей запропонованого підходу. Тим не менше, процедура налаштування \mathbf{A}_{SRR} може проводитися лише один раз на значній вибірці ЗК без необхідності переналаштування для нової вибірки даних. Для забезпечення компромісу між точністю оцінки статистичних параметрів ЗК за наявними (зашумленими) ЦЗ та обчислювальною складністю формування \mathbf{A}_{SRR} можливо варіювати значення розміру блоків розбиття ЦЗ. Зокрема, використання малих значень блоків розбиття ($w_{UC} < 25$, рис. 2.20) дозволяє забезпечити несуттєві зміни коефіцієнтів розкладу ЗК при формуванні стеганограм за рахунок відповідного зростання тривалості формування \mathbf{A}_{SRR} .

2.4 Висновки за розділом 2

За результатами дослідження факторів впливу на точність роботи сучасних СД запропоновано нову концепцію синтезу високоточних стегодетекторів в задачах стегааналізу цифрових зображень та отримано наступні наукові та практичні результати:

1. Встановлено досяжні межі точності роботи СД у випадку використання «ідеалізованих» методів попередньої обробки досліджуваних зображень. Виявлено обмеження використання поширеного підходу до налаштування стегодетекторів, заснованого на використанні статистичних ознак \mathbf{F}_{CC} (2.15) як вихідного, так і каліброваного зображень. Показано, що використання різниці векторів-ознак вихідного та каліброваного зображень \mathbf{F}_{DF} (2.18) дозволяє суттєво ($\Delta P_E \cong 50\%$) зменшити значення помилки виявлення стеганограм у порівнянні з поширеним підходом до побудови СД з використання статистичних параметрів обробленого зображення або \mathbf{F}_{CC} векторів.

2. Виявлено, що використання відстані Хеллінгера $D_H(\mathbf{X}, \mathbf{Y})$ (2.7) дозволяє підвищити точність оцінювання відмінностей між розподілами значень яскравості пікселів ЗК та стеганограм у порівнянні з поширеним випадком використання відстані Кульбака-Лейблера $D_{KL}(\mathbf{X}, \mathbf{Y})$ (2.5). Вагомою перевагою $D_H(\mathbf{X}, \mathbf{Y})$ є властивість метрики імовірнісного простору, що дозволяє інтерпретувати отримувані значення $D_H(\mathbf{X}, \mathbf{Y})$ як оцінки імовірності правильної класифікації ЗК та стеганограм при використанні поширених типів бінарних класифікаторів [144,208,231].

3. Виявлені суттєві обмеження використання методів попередньої обробки ЦЗ, заснованих на підвищенні відстані між векторами, що відповідають статистичним параметрам вихідних та оброблених ЦЗ. Забезпечення суттєвого підвищення даних відстаней потребує використання апріорних даних щодо використаного СМ, що обмежує практичне застосування даних методів для виявлення апріорно невідомих стеганографічних методів.

4. Запропоновано концепцію побудови високоточних СД в задачах стегааналізу ЦЗ, що заснована на використанні математичного апарату декомпозиції багатовимірних сигналів з використанням надлишкових систем функцій. Вагомою перевагою запропонованого методу попередньої обробки досліджуваних зображень у порівнянні з існуючими підходами є використання лише ЗК в процесі формування системи функцій для проведення декомпозиції ЦЗ. Це підвищує стійкість запропонованого методу до змін процедури формування стеганограм згідно новітніх АСМ. За результатами дослідження змін відмінностей між розподілами значень яскравості пікселів ЗК та стеганограм при використанні запропонованого методу виявлено суттєве (до двох разів) підвищення значень відстані Хеллінгера D_H для розглянутих АСМ у всьому діапазоні значень Δ_α^S , що свідчить про високу точність оцінки статистичних параметрів ЗК за наявними (зашумленими) даними.

РОЗДІЛ 3 АНАЛІЗ ТОЧНОСТІ ВИЯВЛЕННЯ СТЕГАНОГРАМ ПРИ ВИКОРИСТАННІ СУЧАСНИХ ТА ЗАПРОПОНОВАНОГО ПІДХОДУ ДО СИНТЕЗУ СТЕГОДЕТЕКТОРІВ

Запропонована концепція побудови високоточних СД дозволяє суттєво збільшити відмінності між статистичними параметрами ЗК та стеганограм у порівнянні з розповсюдженими підходами, що засновані на використанні ансамблю ФВЧ. Це досягається за рахунок використання спеціальних типів МПО, а саме SE- та SE-методів, наприклад, методів попереднього зашумлення, повторного вбудовування стегоданих, застосування новітніх методів зниження впливу адитивних спотворень, запропонованого методу декомпозиції ЦЗ з використанням ССФ тощо. Проте в літературі відсутні відомості щодо оцінок даних змін, що ускладнює проведення порівняльного аналізу точності роботи СД, побудованого на основі розглянутих та запропонованого методу попередньої обробки зображень. Тому становить інтерес проведення порівняльного аналізу точності роботи СД, синтезованих на основі відомих та запропонованого підходів, зокрема у випадку виявлення стеганограм, сформованих згідно новітніх АСМ. Особливий інтерес складає аналіз точності виявлення стеганограм у найбільш складному випадку проведення стеогоаналізу ЦЗ, а саме відсутності апріорних даних щодо особливостей використаного стеганографічного методу.

3.1 Сучасні методи синтезу стегодетекторів цифрових зображень

При розробці високоточних СД широко використовуються методи попередньої обробки досліджуваних зображень, спрямовані на оцінку статистичних параметрів ЗК за наявними (зашумленими) даними (SE-методи,) або визначення статистичних параметрів стеганограм (SE-методи). Особливості практичного використання даних груп методів попередньої обробки ЦЗ було розглянуто у розділі 2.1. Відомі SE- та SE-методи попередньої обробки ЦЗ можуть бути класифіковані наступним чином [81,82,91]:

1. Методи посилення змін статистичних параметрів ЗК, обумовлених прихованням повідомлень:
 - a. Повторне вбудовування стегоданих до ЗК згідно відомих СМ – застосовується для підсилення відмінностей між статистичними параметрами ЗК та стеганограм за рахунок підвищення енергії спотворень, обумовлених прихованням повідомлень;
 - b. Внесення додаткових шумів до досліджуваного ЦЗ – дозволяє підсилити відмінності між власними (стаціонарними) шумами ЦЗ та внесеними (локальними) спотвореннями, обумовленими прихованням повідомлень. В якості шумів, що застосовуються для посилення відмінностей між ЗК та стеганограмами широко використовуються наступні:
 - i. Гаусовий шум – відповідає випадку впливу теплового шуму на МФЕ при формуванні зображення;
 - ii. Пуасоновий шум – відповідає впливу дробових шумів на електронні прилади реєстрації та обробки ЦЗ у цифрових камерах;
 - iii. Фрактальний шум – відповідає локальному впливу шумів, зокрема неоднорідностей характеристик окремих комірок МФЕ, при формуванні зображення у цифрових камерах.
2. Методи оцінки статистичних параметрів ЗК за наявними зашумленими зображеннями:
 - a. Статистичні методи – засновані на використанні статистичних моделей сигналів для визначення параметрів вихідних (неспотворених) ЦЗ або ж характеристик завад. Прикладами даних методів є рангові фільтри (зокрема медіанний фільтр), фільтр Вінера, білатеральний фільтр, методи анізотропної фільтрації тощо.
 - b. Спектральні методи – засновані на застосуванні спектральних перетворень до досліджуваних ЦЗ (наприклад ДДПФ, ДДВП тощо), для отримання їх представлення в частотній області. Зниження впливу завад відбувається шляхом порогової обробки коефіцієнтів

розкладу сигналів в базисі перетворення. При цьому вибір коефіцієнтів проводиться з врахуванням апріорних даних щодо параметрів неспотворених ЦЗ або ж завад.

- c. Варіаційні методи – засновані на представленні процесу оцінки вихідного виду ЦЗ, як вирішення оптимізаційної задачі мінімізації загальної варіативності значень елементів сигналу (англ. Total Variation Minimization, TVM).
- d. Методи компонентного аналізу – засновані на представленні сигналу як адитивної суміші компонентів, що відповідають складовим вихідного (незашумленого) зображення та впливу завад [226]. Прикладами даних методів є метод головних компонентів, метод незалежних компонентів, розклад сигналу по емпіричним модам (перетворення Гільберта-Хуанга) тощо.
- e. Методи на основі штучних нейронних мереж – використовують властивості ШНМ щодо оцінки параметрів та реконструкції вихідних (неспотворених) сигналів за наявними зашумленими даними [232]. Прикладом даних методів є згорткові нейронні мережі, знешумлюючі автоенкодера тощо.

Наведені методи попередньої обробки ЦЗ спрямовані на виявлення та вилучення характерних спотворень, обумовлених прихованням повідомлень до ЗК. Незважаючи на значну кількість запропонованих підходів щодо практичної реалізації даних типів МПО, у літературі відсутні відомості щодо порівняння точності виявлення стеганограм при використанні СД на основі даних методів, зокрема для випадку формування стеганограм згідно АСМ. Це ускладнює порівняльний аналіз ефективності відомих та запропонованого підходу до синтезу високоточних СД. Тому становить інтерес аналітичний огляд відомих підходів до побудови SE- та SE-методів попередньої обробки цифрових зображень. В розділі представлено результати дослідження впливу розглянутих методів обробки ЦЗ на зміни відстані між даними кластерами параметрів ЗК та стеганограм з використанням відстані Хеллінгера D_H (2.7).

3.1.1 Методи на основі повторного вбудовування повідомлень до досліджуваних зображень

Даний тип МПО заснований на використанні поширеного в стегааналізі ЦЗ припущення, що множина пікселів, які використовується при початковому та повторному прихованні повідомлень до ЗК, повністю або частково співпадає [223]. Відповідно, повторне вбудовування стегоданих до стеганограми призведе до збільшення зміни яскравості пікселів, використаних для приховання початкового повідомлення до ЗК, що призводить до відповідного зростання відмінностей між статистичними характеристиками ЗК та стеганограм. Приклади повторного приховання повідомлень до стеганограми, сформованої згідно методу HUGO ($\Delta_{\alpha}^S = 10\%$), наведені на Рис 3.1.

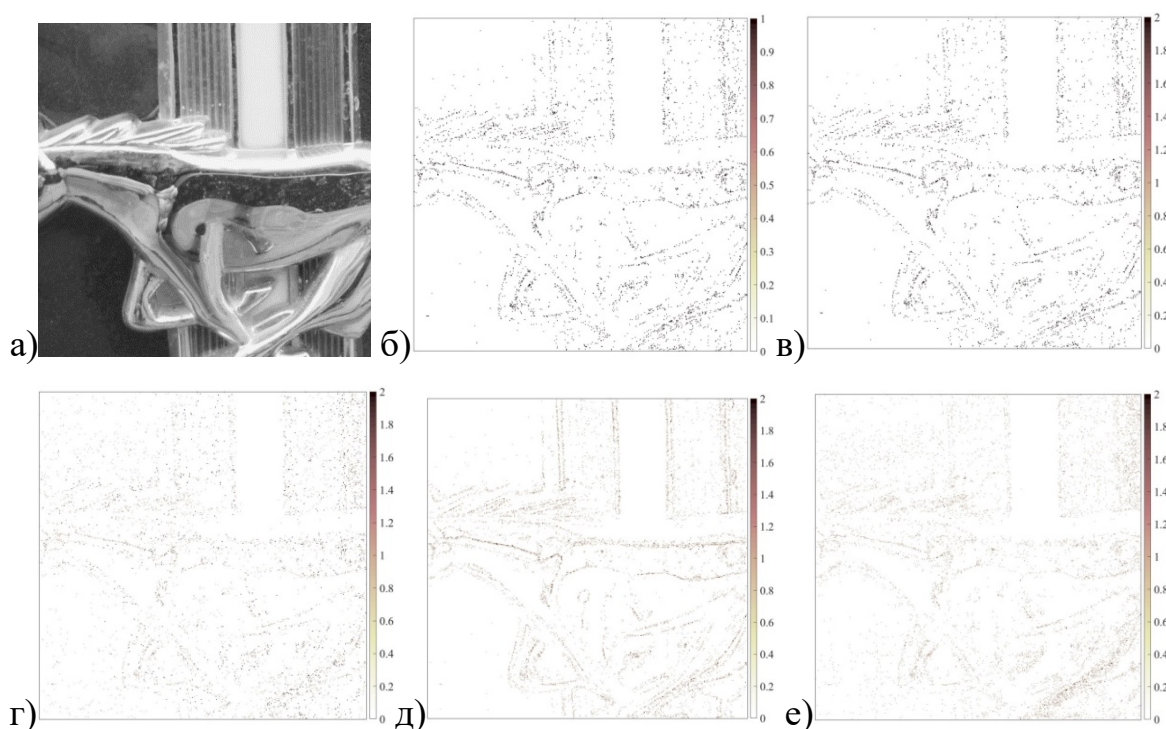


Рисунок 3.1 – Відмінності між зображенням-контейнером (а) та стеганограмами, сформованими при початковому (б) вбудовуванні стегоданих згідно стеганографічного методу HUGO та повторному вбудовуванні згідно методів: (в) – HUGO, (г) – S-UNIWARD, (д) – MG, (е) – MiPOD. Стеганограми наведені для фіксованого ступеня заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 10\%$).

Відмітимо, що повторне приховання повідомлень призводить до посилення змін яскравості пікселів відносно ЗК у порівнянні з випадком обробки вихідної стеганограми (рис. 3.1). Проте дане посилення є нерівномірним та залежить від параметрів СМ, використаного при повторному вбудовуванні – найбільші зміни досягаються у випадку використання СМ, тип та параметри котрого співпадають з початковим методом формування стеганограм (рис. 3.1в). При цьому значення даних змін суттєво знижується у випадку використання СМ (рис. 3.1г-3.1е), процедура вбудовування повідомлень для котрого відрізняється від стеганографічного методу, використаного для формування вихідної стеганограми (рис. 3.1б).

Для чисельної оцінки спотворень ЗК внаслідок початкового та повторного вбудовування в дослідженні використано значення середньоквадратичне відхилення σ_I змін яскравості пікселів ЗК при формуванні стеганограм, наведені в табл. 3.1.

Таблиця 3.1 – Значення середньоквадратичне відхилення σ_I яскравості пікселів ЦЗ при формуванні стеганограм згідно стеганографічного методу HUGO та повторного вбудовування повідомлень до отриманих стеганограм при фіксованому ступені заповнення ЗК стегоданими ($\Delta_\alpha^S = 10\%$).

		Оцінка змін яскравості пікселів ЦЗ при формуванні стеганограм		
		σ_I	$\Delta\sigma_I$	$\Delta\sigma_I, \%$
Початкове приховання повідомлень згідно стеганографічного методу HUGO		0.1274	0.0000	0.00%
Повторне приховання повідомлень згідно стеганографічного методу	HUGO	0.2461	0.1187	93.17%
	S-UNIWARD	0.1768	0.0494	38.78
	MG	0.1837	0.0563	44.19
	MiPOD	0.1715	0.0441	34.62%

Повторне вбудовування повідомлень згідно методу HUGO призводить до зростання значення σ_1 на 93% у порівнянні з випадком аналізу початкової стеганограми (табл. 3.1). При цьому змін зазнають саме пікселі, що були використані при початковому прихованні повідомлень (рис. 3.1б-в). Повторне вбудовування згідно стеганографічних методів S-UNIWARD, MG та MiPOD призводить до зростання значень σ_1^2 від 39% до 44%, причому внесені зміни розпорошуються по всьому ЦЗ (рис. 3.1г- рис. 3.1е).

Розглянутий випадок (рис. 3.1) відповідає ситуації, коли стегоаналітик може визначити ступінь заповнення ЗК стегоданими Δ_α^S та провести повторне приховання повідомлень при збереженні даного показника. Проте в більшості випадків оцінка значення показника Δ_α^S є неможливою, оскільки потребує використання апріорних даних щодо СМ. Внаслідок цього можливо виділити наступні підходи до проведення повторного приховання повідомлень до досліджуваного зображення – вбудовування стегоданих з малим ($\Delta_\alpha^S < 10\%$), високим ($\Delta_\alpha^S > 20\%$) або ж псевдовипадково обраним ступенем заповнення ЗК ($\Delta_\alpha^S \in \mathcal{U}(1; 100)$), де $\mathcal{U}(a, b)$ – рівномірний розподіл в діапазоні значень від a до b .

Приклади повторного приховання повідомлень до стеганограми, сформованої згідно методу HUGO, при малому та сильному ступенях заповнення ЗК стегоданими наведені на Рис 3.2.

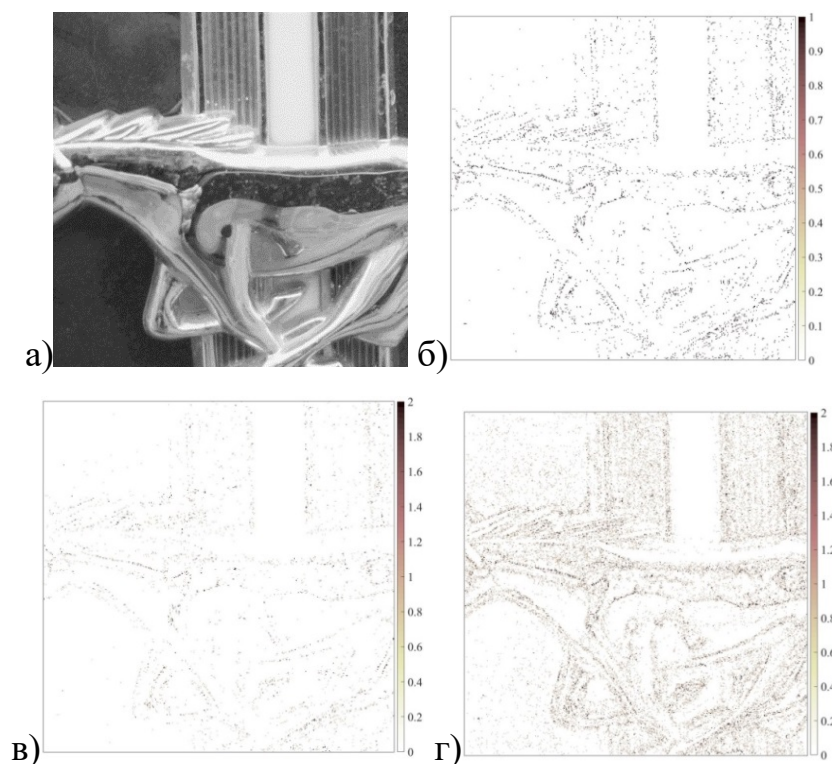


Рисунок 3.2 – Відмінності між зображенням-контейнером (а) та стеганограмами, сформованими при початковому (б, $\Delta_{\alpha}^S = 10\%$) та повторному вбудовуванні стегоданих згідно стеганографічного методу HUGO при варіації ступеня заповнення ЗК стегоданими: (в) – $\Delta_{\alpha}^S = 3\%$; (г) – $\Delta_{\alpha}^S = 50\%$.

Повторне приховання повідомлень з малим ступенем заповнення ЗК стегоданими (рис. 3.2в) призводить до змін яскравості лише малої частки пікселів, використаних для приховання стегобіт. З іншого боку, внесені спотворення розпорощуються по всьому зображенню у випадку $\Delta_{\alpha}^S > 20\%$ (Рис 3.14г) тим самим маскуючи спотворення обумовлені початковим прихованням повідомлень.

Дослідження впливу методів повторного вбудовування стегоданих до досліджуваного ЦЗ на зміни відстані між кластерами векторів, що відповідають статистичним параметрам ЗК та сформованих стеганограм, проводилося в декілька етапів. На першому етапі дослідження, розглянуто випадок повторного вбудовування повідомлень з малим ступенем заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$), до стеганограм, сформованих згідно стеганографічного методу HUGO. Залежності відстані Хеллінгера D_H між розподілами значень

яскравості пікселів ЗК та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta\alpha^S = 5\%$) наведені на рис. 3.3.

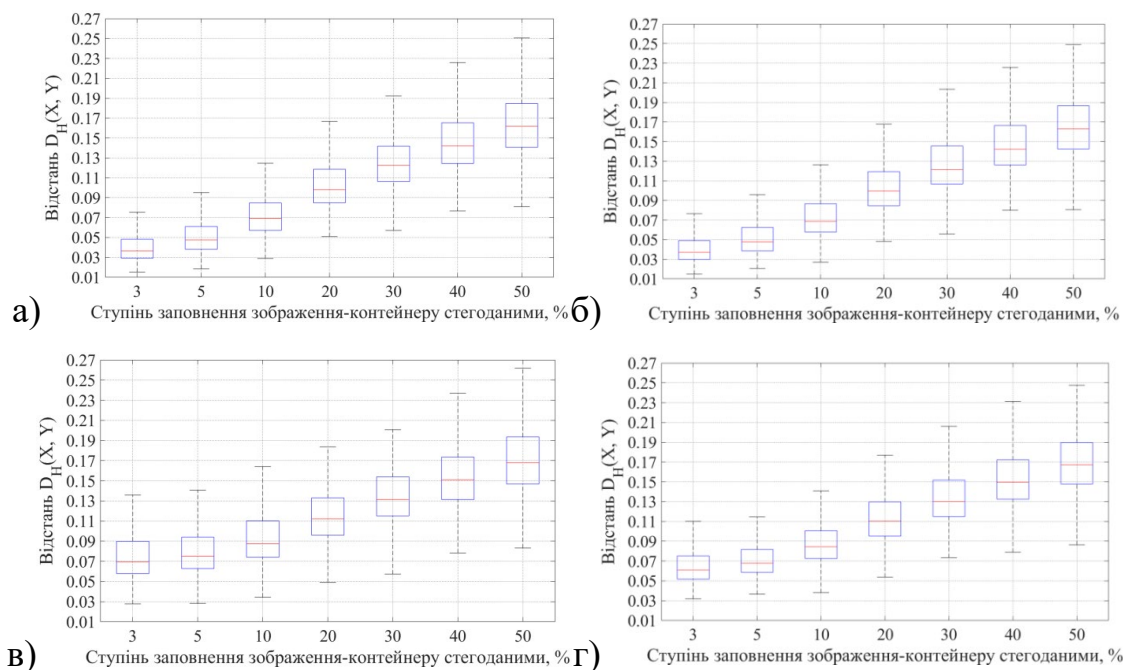


Рисунок 3.3 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta\alpha^S = 5\%$) згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Повторне вбудовування стегоданих з використанням стеганографічних методів HUGO (рис. 3.3а) та S-UNIWARD (рис. 3.3а) практично не змінює значення відстані D_H між розподілами значень яскравості пікселів ЗК та стеганограм у порівнянні з випадком обробки вихідних стеганограм (рис. 2.5). Це пояснюється «стохастичністю» вибору пікселів для приховання повідомлень, внаслідок чого спотворення, обумовлені повторним вбудовування стегоданих, «розпорошуються» по зображенню.

З іншого боку, використання стеганографічних методів MG (рис. 3.3в) та MiPOD (рис. 3.3г) призводить до зростання відстані Хеллінгера між розподілами значень яскравості пікселів ЗК та стеганограм, зокрема в області слабкого ($\Delta D_H \cong 40\%$) та середнього ($\Delta D_H \cong 8\%$) ступені заповнення ЗК стегода-

ними. Отримані результати можуть бути поясненими частковим підсиленням вихідних спотворень ЗК, обумовлених прихованням повідомлень, за рахунок повторного використання пікселів ЦЗ для вбудовування тестових повідомлень (псевдовипадкових бітових послідовностей).

Варто зазначити, що розглянутий випадок відповідає ситуації слабкого заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$), що обумовлює відносно малі зміни відстані Хеллінгера D_H в розглянутих випадках (рис. 3.3). Тому становить інтерес дослідження випадку повторного приховання повідомлень з тим самим значенням ступеня заповнення ЗК стегоданими, що використовувався при початковому вбудовуванні ($\Delta_{\alpha}^S = \Delta_{\alpha_{init}}^S$). Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_{\alpha}^S = \Delta_{\alpha_{init}}^S$) наведені на рис. 3.4.

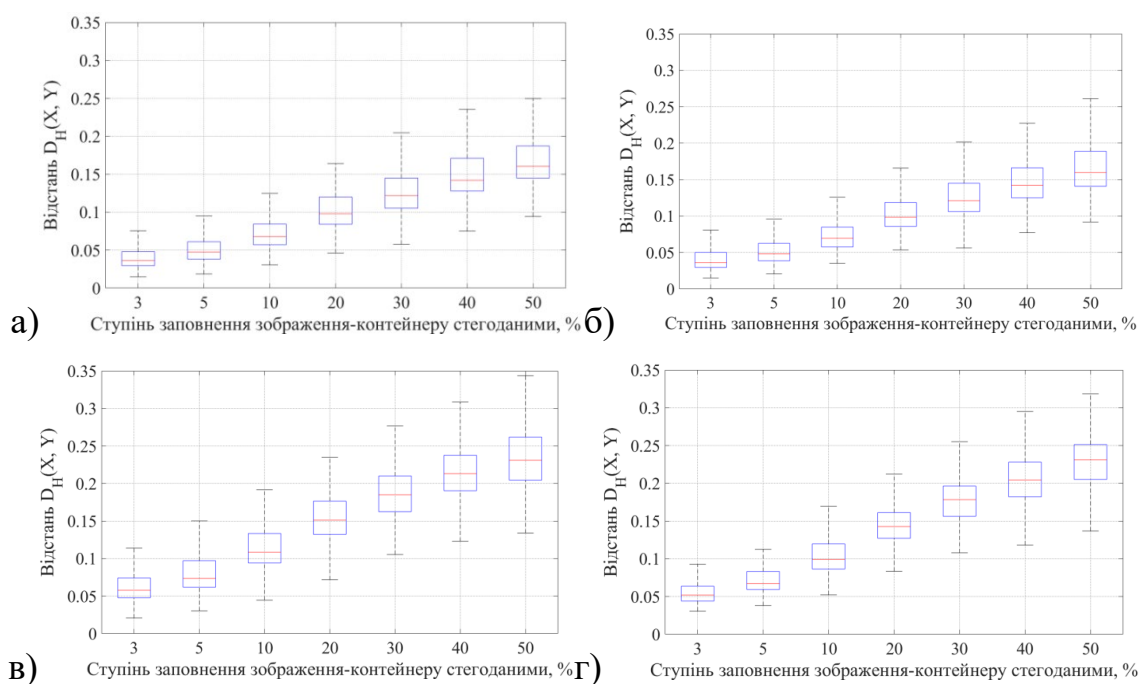


Рисунок 3.4 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_{\alpha}^S = \Delta_{\alpha_{init}}^S$) згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Як і в попередньому випадку (рис. 3.3), повторне приховання повідомлень згідно методів HUGO (рис. 3.4а) та S-UNIWARD (рис. 3.4б) призводить до несуттєвих змін значення відстані D_H між розподілами значень яскравості пікселів ЗК та стеганограм у порівнянні випадком аналізу необроблених ЦЗ (рис. 2.5). Таким чином, псевдовипадковий вибір пікселів при формуванні стеганограм маж незначний вплив на ефективність повторного вбудовування стегоданих в задачах виявлення повідомлень.

Повторне приховання повідомлень згідно стеганографічних методів MG (рис. 3.4в) та MiPOD (рис. 3.4г) призводить до суттєвого ($\Delta D_H \cong 35\%$) збільшення відстані D_H в усьому діапазоні значень параметру Δ_α^S у порівнянні з розглянутим випадком слабкого заповнення ЗК стегоданими (рис. 3.3). Таким чином зростання значення Δ_α^S при повторному вбудовуванні стегоданих згідно розглянутих CM дозволяє збільшувати відстань між розподілами значень яскравості пікселів ЗК та стеганограм, що підвищує точність виявлення стеганограм.

Також розглянуто випадок повторного вбудовування стегоданих за умови сильного заповнення ЗК стегоданими ($\Delta_\alpha^S > 20\%$). Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$) наведені на рис. 3.5.

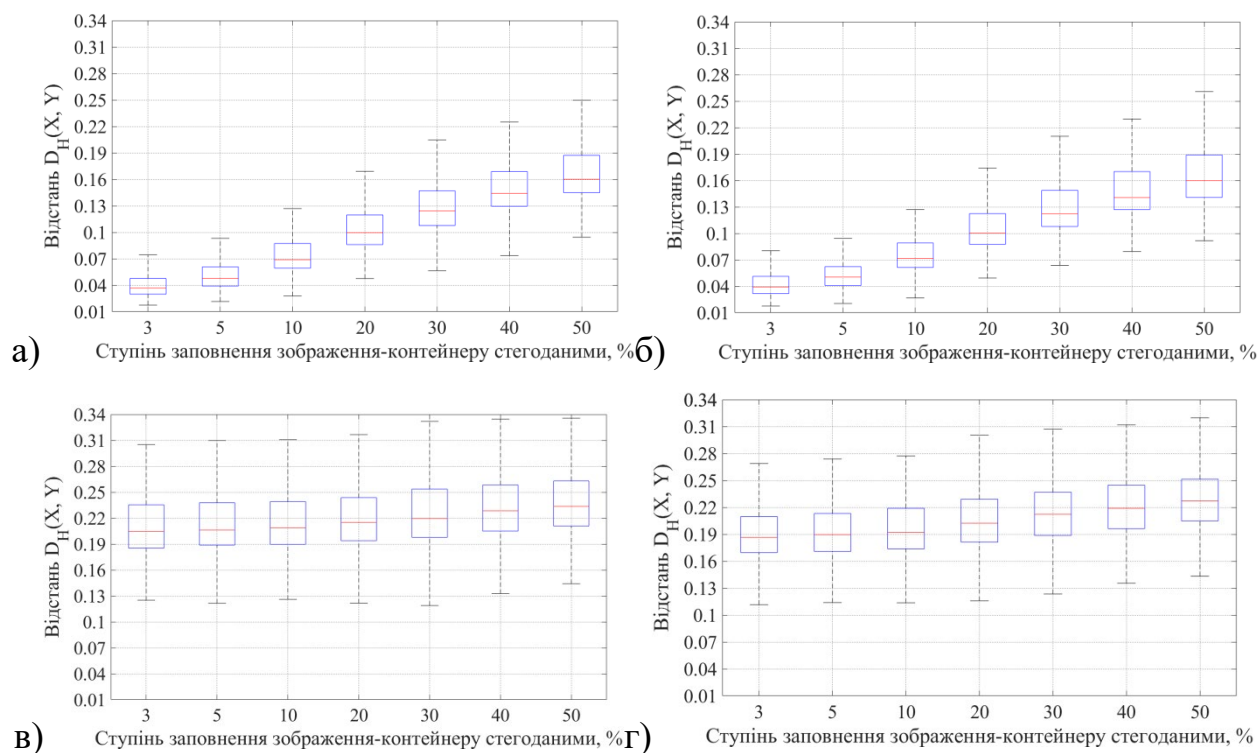


Рисунок 3.5 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$) згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Повторне приховання повідомлень у випадку $\Delta_\alpha^S = 50\%$ призводить до малих змін значення відстані Хеллінгера D_H ($\Delta D_H \cong 5\%$) при використанні методів HUGO (рис. 3.5а) та S-UNIWARD (рис. 3.5а) в області слабкого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$). Для інших значень ступеня заповнення Δ_α^S , значення відстані Хеллінгера D_H залишається практично без змін. Це суттєво обмежує використання методів HUGO та S-UNIWARD для попередньої обробки стеганограм для підсилення спотворень, обумовлених прихованням повідомлень.

На відміну від стеганографічних методів HUGO та S-UNIWARD, повторне приховання стегоданих згідно методів MG (рис. 3.4в) та MiPOD (рис. 3.5г) призводить до зростання значень відстані Хеллінгера D_H до трьох разів у порівнянні з розглянутими випадками (рис. 3.3-3.4) у всьому діапазоні

значень ступеня заповнення ЗК стегоданими. Виявлений ефект має вагоме значення для підвищення точності роботи СД, оскільки дозволяє збільшити відмінності між класами ЗК та стеганограм без необхідності використання обчислювально складних видів СД.

Варто зазначити, що в більшості випадків стегоаналітик має обмежені можливості щодо оцінки ступеня заповнення ЗК стегоданими, зокрема використання значних значень Δ_α^S при повторному прихованні повідомлень. Тому становить інтерес дослідження випадку приховання повідомлень з псевдовипадково обраним значенням параметру $\Delta_\alpha^S \in \mathcal{U}(3; 50)$, де $\mathcal{U}(a; b)$ відповідає рівномірному розподілу значень Δ_α^S від a до b . Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$) наведені на рис. 3.6.

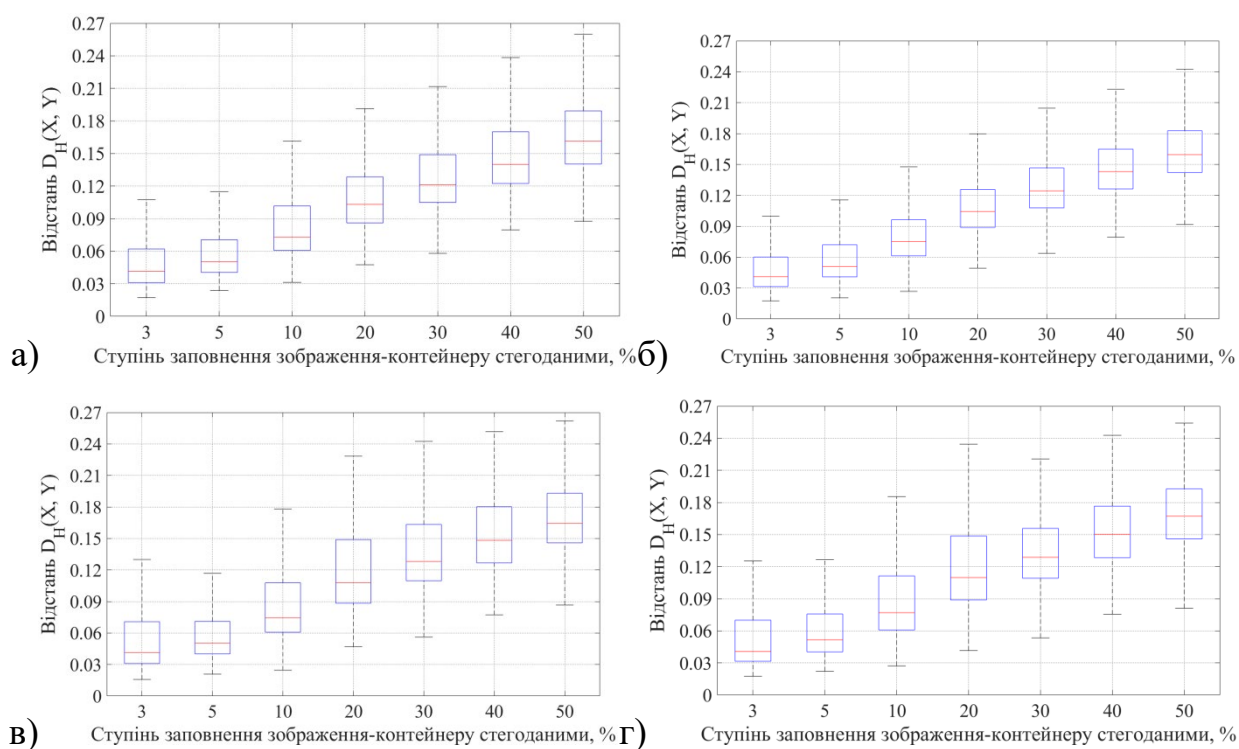


Рисунок 3.6 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, сформованих згідно методу HUGO, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S \in \mathcal{U}(3; 50)$) згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

В розглянутому випадку значення Δ_{α}^S при повторному прихованні тестових стегоданих до досліджуваних зображень обирається з рівною імовірністю з діапазонів слабкого ($\Delta_{\alpha}^S < 10\%$), середнього ($10\% \leq \Delta_{\alpha}^S \leq 20\%$) та сильного ($\Delta_{\alpha}^S > 20\%$) ступеня заповнення ЗК стегоданими. Внаслідок цього виявлене зростання значень відстані Хеллінгера D_H при використанні стеганографічних методів MG (рис. 3.4в) та MiPOD (рис. 3.4г) не спостерігається – отримані значення D_H несуттєво відрізняються від випадку аналізу вихідних стеганограм (рис. 2.5).

Таким чином, можемо зробити висновок, що повторне приховання повідомлень з використання стеганографічних методів MG та MiPOD при сильному заповненні ЗК стегоданими ($\Delta_{\alpha}^S > 20\%$) дозволяє суттєво підвищити значення відстані Хеллінгера D_H . Для перевірки отриманих результатів, становить інтерес дослідження ефективності даного підходу при обробці стеганограм, сформованих згідно інших стеганографічних методів. Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу S-UNIWARD, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_{\alpha}^S = 50\%$) наведені на рис. 3.7.

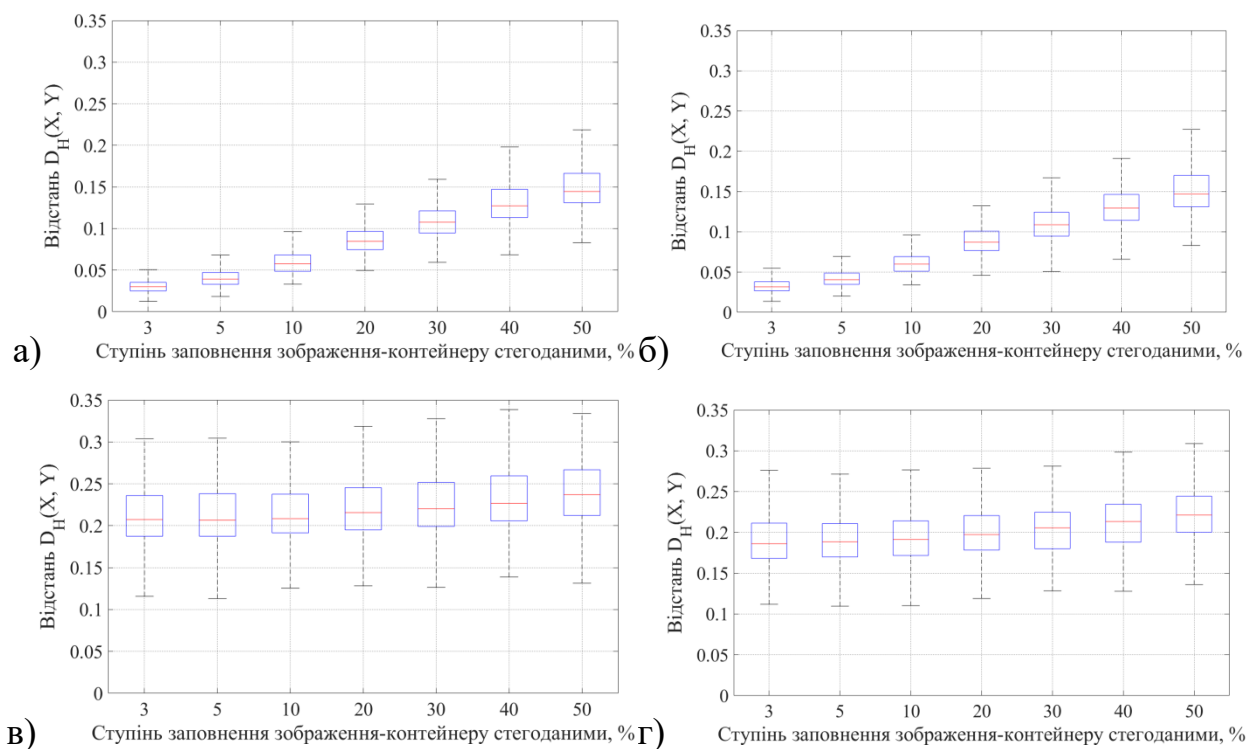


Рисунок 3.7 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, сформованих згідно методу S-UNIWARD, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$) згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Аналогічно до розглянутого випадку для методу HUGO (рис. 3.5), повторне вбудовування стегоданих до ЦЗ згідно методів MG (рис. 3.7в) та MiPOD (рис. 3.7г) дозволяє суттєво підвищити значення відстані D_H у порівнянні з випадком використання методів HUGO (рис. 3.7а) та S-UNIWARD (рис. 3.7б). При цьому виявлене зростання значень D_H зберігається у всьому діапазоні значень Δ_α^S , що підтверджує ефективність даного підходу.

Для порівняння, на рис. 3.8 наведені залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу MG, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$).

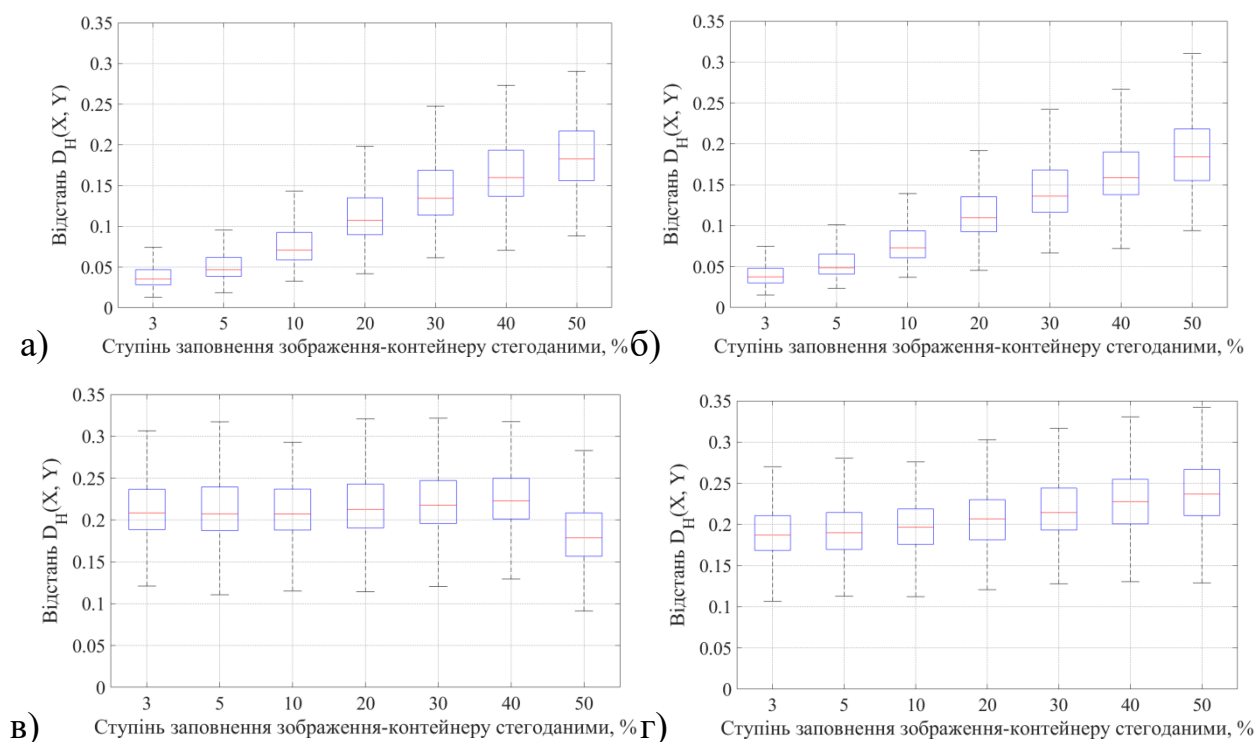


Рисунок 3.8 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, сформованих згідно методу MG, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$) згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Аналогічно до розглянутих випадків (рис. 3.5, рис. 3.7) використання методів MG (рис. 3.8в) та MiPOD (рис. 3.8г) дає можливість суттєво (до чотирьох разів) збільшити значення відстані Хеллінгера D_H у порівнянні з випадком використання методів HUGO (рис. 3.8а) та S-UNIWARD (рис. 3.8б). Проте, виявлене зростання досягається лише в області слабкого ($\Delta_\alpha^S < 10\%$) та середнього ($10\% \leq \Delta_\alpha^S \leq 20\%$) ступеня заповнення ЗК стегоданими.

Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу MiPOD, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$) наведені на рис. 3.9.

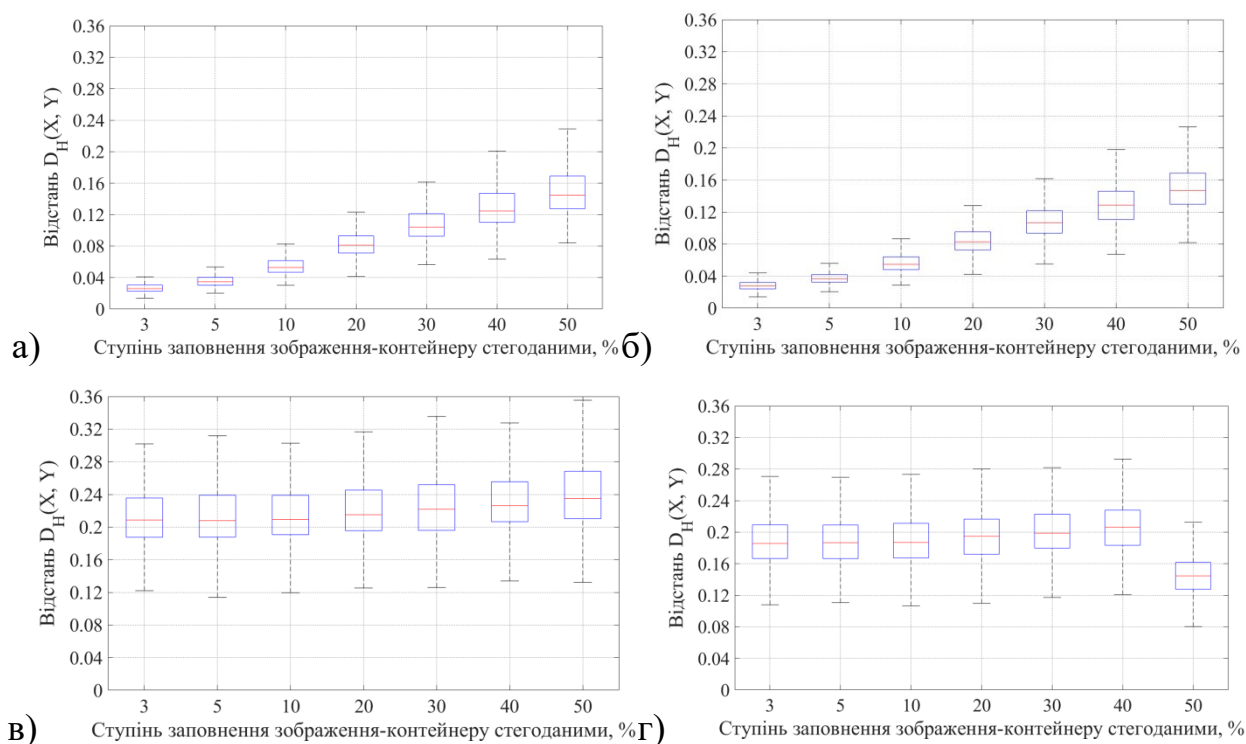


Рисунок 3.9 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, сформованих згідно методу MiPOD, з пакету зображень ALASKA при повторному вбудовуванні повідомлень ($\Delta_\alpha^S = 50\%$) згідно стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Повторне приховання повідомлень згідно методів MG (рис. 3.9в) та MiPOD (рис. 3.9г) дозволяє до п'яти разів збільшити значення відстані Хеллінгера D_H у порівнянні з випадком використання методів HUGO (рис. 3.9а) та S-UNIWARD (рис. 3.9б). Зростання значення D_H досягається лише в області малого та середнього ступеня заповнення ЗК стегоданими, в той час як в області сильного заповнення ($\Delta_\alpha^S > 20\%$), розглянуті методи повторного приховання повідомлень не дозволяють суттєво зміни значення D_H .

Таким чином, можемо зробити висновок, що повторне приховання повідомлень до ЗК призводить до посилення спотворень, обумовлених початковим вбудовуванням стегоданих до зображення-контейнеру. Відмітимо, що даний результат зберігається навіть у випадку, коли повторне приховання стегоданих проводиться згідно CM, що відрізняється від стеганографічного методу, використаного для формування вихідної стеганограми.

В більшості випадків апіорні дані щодо виду та особливостей використаного СМ є обмеженими, що знижує ефективність використання методів попередньої обробки ЦЗ на основі повторного вбудовування стегоданих. Для подолання даного обмеження становить інтерес використання особливостей сучасних підходів до побудови АСМ, а саме приховання повідомлень на рівні шумів ЗК. Дані шуми відповідають впливу теплового, дробового та фрактального шумів на етапі формування ЦЗ [81].

3.1.2 Методи на основі додаткового зашумлення досліджуваних зображень

При розробці сучасних методів зниження впливу адитивних шумів у ЦЗ вплив сторонніх шумів та завад на МФЕ, зокрема теплового, дробового та фрактального шумів [141], обумовлених флуктуаціями значень параметрів комірок МФЕ та дискретної природи світла. Для моделювання впливу даних шумів на значення яскравості пікселів отримуваних ЦЗ широко використовуються поширені типи статистичних розподілів, зокрема гаусового (нормального) та пуасонового розподілів. Вбудовування стегоданих до ЗК призводить до локальних збурень значень яскравості пікселів зображення-контейнеру, що порушує параметри наведених шумів в певному околі пікселів, використаних для приховання стегобітів. Виявлення локальних змін параметрів теплового, дробового та фрактального шумів може бути використано для підвищення точності роботи СД. Розглянемо вплив даних шумів на статистичні параметри ЗК більш детально.

Тепловий шум відповідає впливу теплових завад на елементи МФЕ та, зазвичай, моделюється з використанням нормального розподілу $\mathcal{N}(0, \sigma_N^2)$ з нульовим значенням математичного очікування та дисперсією σ_N^2 , пропорційною до енергії завад. Для оцінки значення σ_N^2 для напівтонового зображення \mathbf{U} розміром $N \times M$ (пікселів) використовується фільтр Вінера [198]:

$$\begin{aligned}\sigma_{\eta}^2 &= \frac{1}{NM} \sum_{n,m \in \eta} \mathbf{U}_{n,m}^2 - \mu_{\eta}^2, \\ \mu_{\eta}^2 &= \frac{1}{NM} \sum_{n,m \in \eta} \mathbf{U}_{n,m},\end{aligned}\tag{3.1}$$

де η – поточне положення КВ розміром $w_w \times w_w$ (пікселів); $\mu_{\eta}^2, \sigma_{\eta}^2$ – відповідно, середнє значення та дисперсія значень яскравості пікселів в межах поточного положення КВ. Оцінка дисперсії σ_N^2 проводиться шляхом усереднення значень σ_{η}^2 (3.1), отриманих при варіації положення КВ фільтру Вінера.

Дробовий шум відповідає впливу явища флуктуації кількості електронів, що циркулюють в елементах МФЕ під впливом зовнішнього опромінювання [10,145]. Спектральні характеристики дробового шуму можливо визначити з використанням теореми Кемпбелла [233] – дисперсія даного шуму є пропорційною до енергії окремих імпульсів, що створюються хаотичним рухом електронів в елементах МФЕ. В більшості практичних застосувань, дробовий шум моделюється з використанням розподілу Пуассона [234]:

$$\text{Pr}(x = k, \lambda) = \frac{\lambda^k}{k!} e^{-\lambda},$$

де x – випадкова величина; $k \geq 0$ – кількість подій; $\lambda > 0$ – математичне очікування кількості подій за фіксований проміжок часу; $a!$ – факторіал числа $a, a \geq 0$. Для оцінювання параметру λ розподілу Пуассона при обробці цифрових зображень може використовуватися ковзне середнє значення яскравості пікселів ЦЗ [235].

Відмітимо, що розглянуті типи шумів відповідають впливу лише стаціонарних завад на елементи МФЕ при формуванні ЦЗ. Для моделювання впливу локальних збурень, що відповідають нерівномірності ступеня чутливості окремих елементів МФЕ, а також нерівномірності падіння світла на дані елементи широко використовуються дробові (фрактальні) шуми. Особливістю даного типу завад є концентрація спектру потужності в певному діапазоні частот [236]:

$$S(\mathbf{U}) \propto f^{-\beta_f}, \quad (3.2)$$

де \mathbf{U} – напівтонове зображення розміром $N \times M$ (пікселів); $\beta_f \in (0; 2)$ – масштабуючий показник. Випадок $\beta_f = 0$ відповідає впливу білого гаусового шуму, в той час як $\beta_f = 2$ відповідає впливу броунівського шуму. В більшості випадків, значення параметру β_f приймається рівним одиниці, що відповідає впливу рожевого шуму [236].

Для моделювання фрактального шуму зазвичай використовується метод Перліна [237]. Даний метод заснований на генерації білого гаусового шуму, та подальшого застосування до нього фільтру, характеристика пропускання котрого є пропорційною до $f^{-\beta_f}$. Це дозволяє забезпечити швидку генерацію фрактального шуму з фіксованим значенням масштабуючого показника β_f (3.2).

Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при попередній обробці досліджуваних ЦЗ шляхом додавання нормального (гаусового) шуму від розмірів w_w ковзного вікна, що використовується для оцінки дисперсії завад, для тестових зображень з пакету ALASKA наведені на рис. 3.10.

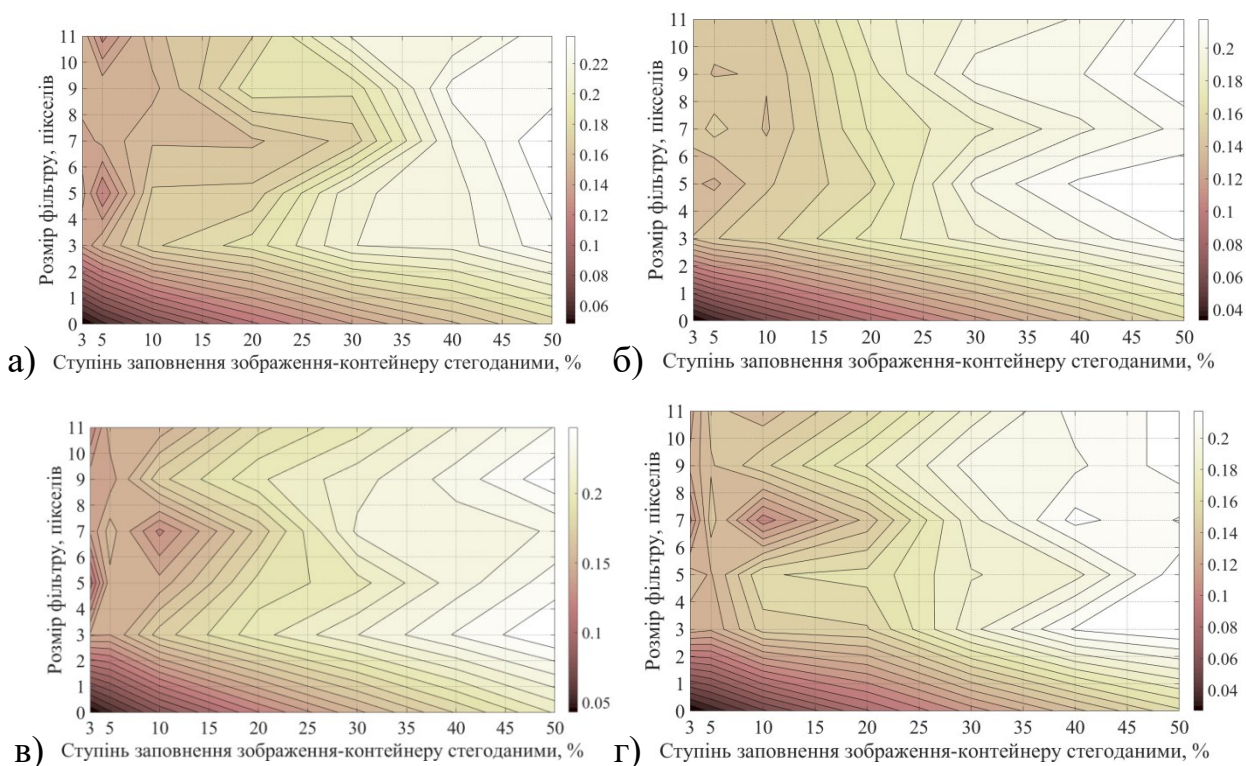


Рисунок 3.10 – Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при калібруванні зображень з пакету зображень ALASKA шляхом додаткового зашумлення з використанням нормального (гаусового) шуму від розмірів КВ, що використовуються для оцінки дисперсії завад, для стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD. Значення розміру рівне нулю відповідає випадку аналізу необроблених зображень.

Додаткове зашумлення стеганограм з використанням нормального (гаусового) розподілу дозволяє суттєво (до 4.75 разів) збільшити середнє значення відстані D_H між розподілами значень яскравості пікселів ЗК та стеганограм для всіх розглянутих стеганографічних методів (рис. 3.10). Значення зміни відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при варіації значень ступеня заповнення ЗК стегоданими наведені в табл. 3.2.

Таблиця 3.2 – Величина зміни відстані Хеллінгера D_H (разів) між розподілами значень яскравості пікселів ЗК та стеганограм при додатковому зашумленні зображень з використанням гаусового шуму у порівнянні з випадком обробки вихідних (необроблених) зображень.

		Стеганографічний метод			
		HUGO	S-UNIWARD	MG	MiPOD
Ступінь заповнення ЗК стегоданими	$\Delta_\alpha^S = 3\%$	3.17	4.43	3.40	4.75
	$\Delta_\alpha^S = 20\%$	1.66	1.99	1.66	2.07
	$\Delta_\alpha^S = 50\%$	1.36	1.37	1.22	1.37

Виявлено, що додавання гаусових шумів до стеганограм дозволяє посилити слабкі зміни значень яскравості пікселів (рис. 3.10), причому величина змін значень D_H залежить від параметру Δ_α^S . Найбільші зміни відстані Хеллінгера D_H (до п'яти разів) виявлені в області слабого заповнення ЗК стегоданими ($\Delta_\alpha^S = 3\%$, табл. 3.2), що є одним з найбільш складних випадків проведення стегоаналізу. В області середнього ($\Delta_\alpha^S = 20\%$) та сильного ($\Delta_\alpha^S = 50\%$) ступеня заповнення ЗК стегоданими зміни відстані Хеллінгера сягають до двох разів (табл. 3.2) навіть для новітнього стеганографічного методу MiPOD (рис. 3.10г), що є одним з найбільш складних для виявлення.

Варто зазначити, що виявлені зміни відстані D_H у випадку зашумлення досліджуваного ЦЗ з використання гаусового шуму практично не залежать від розміру КВ (рис. 3.10). Це дозволяє використовувати ковзні вікна відносно малого розміру (3×3 пікселів, рис. 3.10) для зниження обчислювальної складності МПО.

Таким чином, можемо зробити висновок, що зашумлення досліджуваних ЦЗ з використанням гаусового шуму дозволяє підвищити відмінності між розподілами значень яскравості пікселів ЗК та стеганограм. Тому становить інтерес дослідження використання інших типів завад, зокрема дробового шуму, для додаткового підсилення даних відмінностей.

Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при зашумленні зображень з використанням шумів, що мають пуасоновий розподіл, для тестових зображень з пакету ALASKA наведені на рис. 3.11.

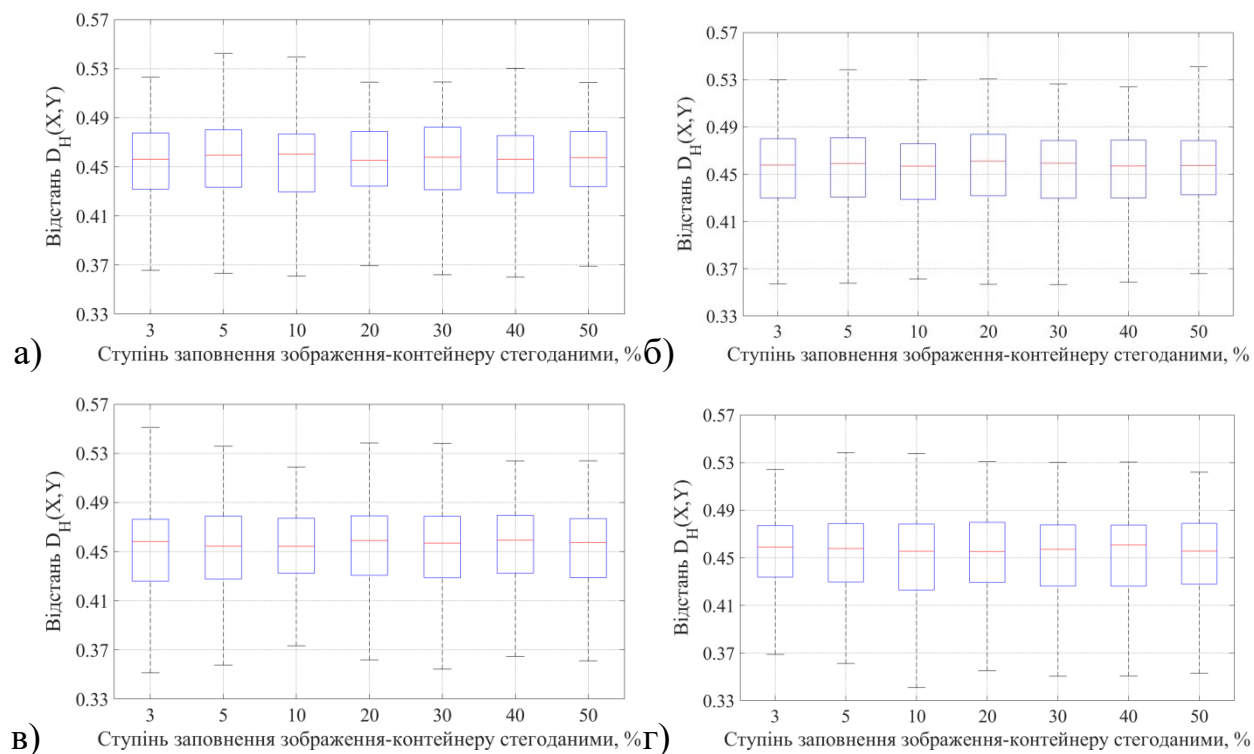


Рисунок 3.11 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при додатковому зашумленні зображень з використанням розподілу Пуассона пікселів для зображень-контейнерів та стеганограм, сформованих згідно стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Використання шумів, що мають пуасоновий розподіл (рис. 3.11), для обробки досліджуваних ЦЗ дозволяє суттєво (до трьох разів) підвищити значення відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм у порівнянні з випадком аналізу необроблених зображень (рис. 2.5). Проте отримані значення D_H практично не залежать від значення параметру Δ_α^S , внаслідок чого можемо зробити висновок, що використання даного типу завад суттєво спотворює досліджуване зображення та практично нівелює слабкі зміни, обумовлені прихованням повідомлень.

Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при зашумленні зображень з використанням фрактального шуму від масштабуючого показника β_f для тестових зображень з пакету ALASKA наведені на рис. 3.12.

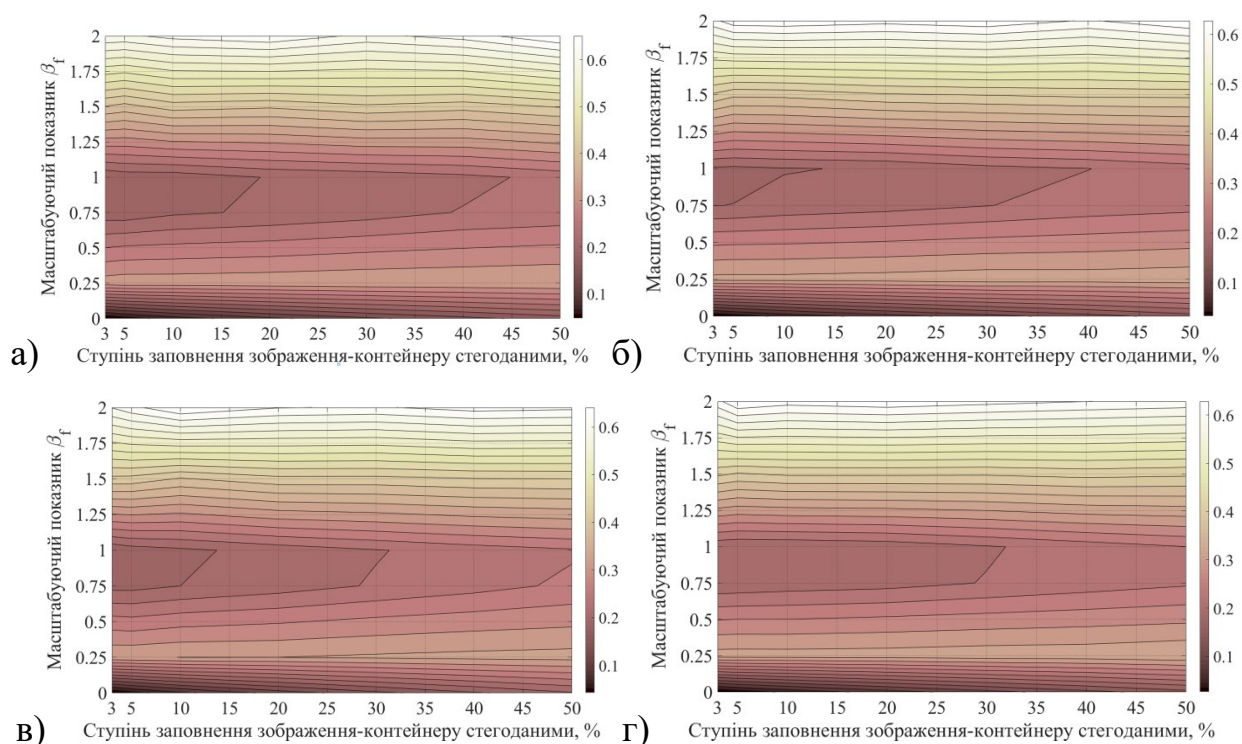


Рисунок 3.12 – Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при зашумленні зображень з пакету зображень ALASKA з використанням фрактального шуму від масштабуючого показника β_f для стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD. Значення $\beta_f = 0$ відповідає випадку аналізу необроблених зображень.

Використання фрактальних шумів з малими значеннями масштабуючого показника β_f ($\beta_f < 0.25$) призводить до зростання значень D_H до трьох разів (рис. 3.12), що є аналогічним до отриманих раніше результатів для випадку додавання гаусових завад (рис. 3.10). Подальше зростання значення β_f ($0.25 < \beta_f < 1.50$) не призводить до суттєвих змін значення D_H для розглянутих СМ (рис. 3.12). Використання високих значень показника β_f ($\beta_f \geq 1.50$) призводить до суттєвого зростання D_H (до 10 разів). Це свідчить, що викорис-

тання роунівського шуму для обробки ЦЗ дозволяє підсилювати відмінності між ЗК та стеганограмами. Проте відсутність змін значень відстані Хеллінгера D_H при високих значень показника β_f та варіації значення параметру Δ_α^S свідчить, що дані завади практично нівелюють вплив спотворень ЗК, обумовлених вбудовуванням стегоданих.

Для порівняння також розглянуто випадок використання завад, що створюються з врахуванням особливостей досліджуваних ЦХ, зокрема неоднорідності значень яскравості пікселів в текстурних областях, що становить інтерес для задач підсилення спотворень ЗК, обумовлених прихованням повідомлень. Одним з найбільш відомих прикладів даних шумів є шуми Перліна, запропоновані в роботі [237]. Процедура генерування даних шумів складається з двох етапів. На першому етапі проводиться розбиття вхідного ЦЗ на комірки рівного розміру, при цьому в кожній комірці проводиться генерування псевдовипадкових векторів з двох (для напівтонових ЦЗ), або ж трьох (для кольорових зображень) елементів. На другому етапі проводиться інтерполяція значень яскравості пікселів між суміжними комірками.

Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при зашумленні зображення з використанням шуму Перліна для тестових зображень з пакету ALASKA наведені на рис. 3.13.

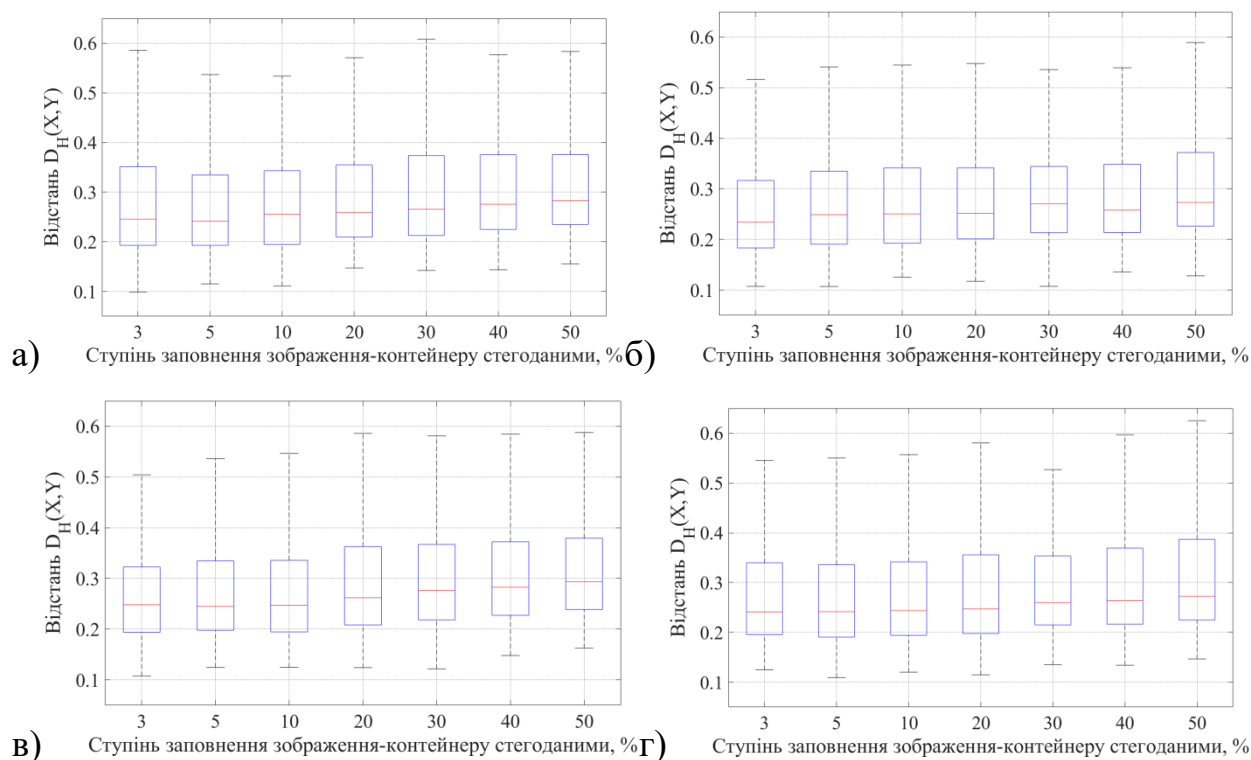


Рисунок 3.13 Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при додатковому зашумленні зображень з пакету зображень ALASKA з використанням шуму Перліна для ЗК та стеганограм, сформованих згідно стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Використання шуму Перліна дозволяє суттєво (на 40%) підвищити значення відстані D_H між розподілами значень яскравості пікселів ЗК та стеганограм у порівнянні з випадком аналізу необроблених зображень (рис. 2.5). Дані результати є аналогічними до розглянутого випадку використання пуасонового шуму (рис. 3.11). Проте, отримані значення D_H практично не залежать від значення параметру Δ_α^S , що свідчить про суттєві спотворення досліджуваного ЦЗ та нівелювання слабких змін, обумовлених прихованням стегоданих.

Таким чином, можемо зробити висновок що використання методів посилення спотворень, обумовлених прихованням повідомлень до ЗК, зокрема повторного вбудовування стегоданих та зашумлення, дозволяє підвищити відмінності між розподілами значень яскравості пікселів ЗК та стеганограм. Найбільших змін дані розподіли зазнають у випадку повторного приховання

повідомлень згідно стеганографічних методів MG та MiPOD (рис. 3.6-3.9), а також зашумлення з використанням гаусового шуму (рис. 3.10).

Проте обмеженням практичного застосування даного підходу є необхідність комплексного застосування декількох методів для забезпечення суттєвої зміни статистичних параметрів стеганограм [82,83]. При цьому визначення оптимального ансамблю даних методів за критерієм мінімізації значення помилки P_E (1.25) наразі є невирішеною задачею, що потребує використання апріорних даних щодо використаного СМ. Тому становить інтерес застосування методів попередньої обробки ЦЗ, що дозволяють проводити оцінку статистичних параметрів ЗК за наявними (зашумленими) зображеннями та не потребують апріорних відомостей щодо використаного СМ.

3.1.3 Статистичні методи знешумлення цифрових зображень

Вбудовування повідомлень до ЗК згідно новітніх АСМ проводиться з використанням областей ЗК, що характеризуються високим рівнем дисперсії значень яскравості пікселів, зокрема шумоподібні області, текстури об'єктів тощо [9]. Використання поширених методів фільтрації ЦЗ, зокрема медіанного та вінеровського фільтрів для обробки даних областей є неефективним [91], що підтверджується результатами досліджень, наведених у розділі 1.4.2. Це обумовлено малими відмінностями між результатами обробки ЗК та стеганограми при використанні даних МПО, що суттєво знижує ефективність роботи СД. Тому становить інтерес використання спеціальних методів зниження впливу завад у ЦЗ, зокрема анізотропної фільтрації [141]. Особливістю даних методів є врахування величини дисперсії значень яскравості в поточному околі для корегування параметрів фільтрації.

Прикладом сучасних методів анізотропної фільтрації ЦЗ є білатеральна фільтрація (БФ), що заснована на зниженні впливу адитивних завад при збереженні контурів об'єктів на зображенні [141]:

$$\begin{aligned}
 F_{BF}(\mathbf{U}_{x,y}) &= \frac{1}{N_{BF}(i,j)} \\
 &\cdot \sum_{k=-\frac{h_k-1}{2}}^{\frac{h_k-1}{2}} \sum_{n=-\frac{h_n-1}{2}}^{\frac{h_n-1}{2}} \mathbf{U}_{x+k,y+n} \cdot h(k,n) \cdot g(\mathbf{U}_{x+k,y+n} - \mathbf{U}_{x,y}), \\
 N_{BF}(i,j) &= \sum_{k=-\frac{h_k-1}{2}}^{\frac{h_k-1}{2}} \sum_{n=-\frac{h_n-1}{2}}^{\frac{h_n-1}{2}} h(k,n) \cdot g(\mathbf{U}_{x+k,y+n} - \mathbf{U}_{x,y}),
 \end{aligned} \tag{3.3}$$

де $h(k,n)$ – фільтр розміром $h_k \times h_n$ (пікселів), що використовується для зменшення впливу локальних збурень значень яскравості пікселів ЦЗ; $g(\cdot)$ – функція, що дозволяє враховувати відмінності між значеннями яскравості поточного та інших пікселів ЦЗ в межах фіксованого положення КВ з метою зниження спотворень контурів об'єктів; $N_{BF}(i,j)$ – нормуючий множник для поточного положення КВ.

Відмітимо, що у випадку обробки областей зображення для яких варіація значень яскравості пікселів є відносно малою, значення функції $g(\cdot)$ є близьким до одиниці та суттєво не впливає на результати роботи фільтру $h(k,n)$ (3.3). При обробці областей зображення, що містять контури об'єктів, значення $g(\cdot)$ знижується, що дозволяє зменшити вплив фільтру $h(k,n)$ на значення яскравості пікселів в межах КВ [141]. В якості фільтру $h(k,n)$ широко використовуються ФНЧ на основі гаусової функції, що дозволяє мінімізувати вплив адитивних завад при збереженні статистичних параметрів текстурних областей ЦЗ [141].

Використання БФ дає можливість знизити вплив локальних збурень значень яскравості пікселів ЗК, обумовлених прихованням повідомлень, що становить інтерес для виявлення слабких змін ЗК, обумовлених стегоданих. Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при використанні білатерального фільтру

($h_k = h_n = 5$ пікселів) для тестових зображень з пакету ALASKA наведені на рис. 3.14.

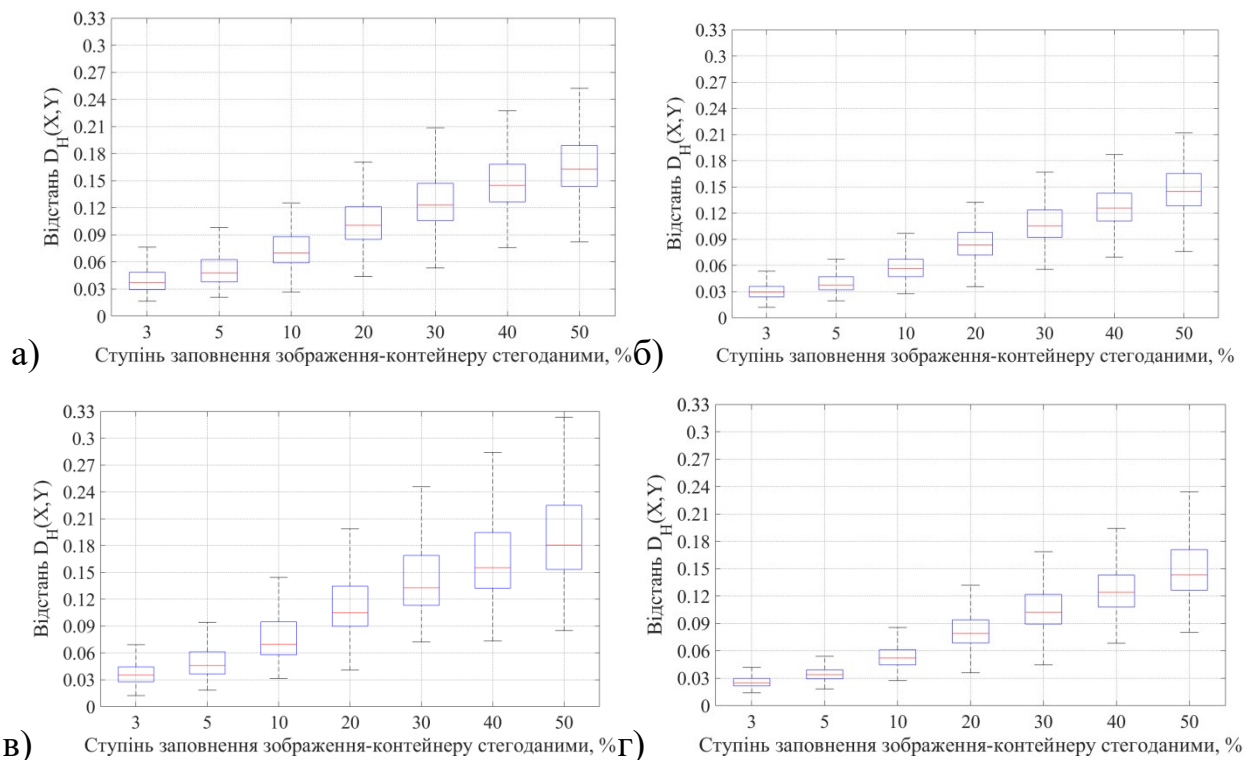


Рисунок 3.14 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стегограм при використанні білатеральної фільтрації ($h_k = h_n = 5$ пікселів, $h(k, n)$ на основі гаусової функції) для зображень-контейнерів з пакету ALASKA та стегограм, сформованих згідно стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Застосування БФ призводить до суттєвих змін відстані Хеллінгера D_H ($\Delta D_H \cong 20\%$) в області слабого заповнення ЗК стегограмими ($\Delta \alpha^S < 10\%$, рис. 3.14) у порівнянні з випадком аналізу необроблених зображень (рис. 2.5). Це свідчить про мінімізацію відмінностей між ЗК та стегограмами після застосування БФ, що негативно впливає на точність роботи СД.

В області сильного заповнення ЗК стегограмими ($\Delta \alpha^S > 20\%$, рис. 3.14) виявлено зростання відстані D_H ($\Delta D_H \cong 7\%$), що свідчить про ефективність «придушення» впливу спотворень, обумовлених прихованням повідомлень, при використанні БФ. Проте, отримані результати суттєво поступаються ви-

падку повторного приховання повідомлень до ЦЗ (рис. 3.5), що свідчить про обмеження використання БФ в якості МПО при побудові стегодетектору.

Для додаткового зниження впливу локальних збурень значень яскравості пікселів широко використовуються методи обробки, спрямовані на пошук областей ЦЗ, статистичні параметри котрих несуттєво різняться (англ. non-local means, NLM). Дані методи засновані на мінімізації дисперсії значень яскравості пікселів оброблюваного зображення шляхом аналізу відмінностей між значеннями яскравості поточного пікселя та середньої яскравості ЦЗ в межах ковзного вікна [238]:

$$F_{NLM}(\mathbf{u}_{x,y}) = \frac{1}{N_{NLM}(i,j)} \cdot \sum_{(x,y) \in w_n} \mathbf{u}_{x,y} \cdot w(x,y),$$

$$N_{NLM}(i,j) = \sum_{(x,y) \in w_n} w(x,y),$$

де $w(x,y)$ – масштабуюча функція, що мінімізує відмінності між яскравістю поточного пікселя з координатами (x,y) в межах КВ та середнього значення яскравості для поточного положення ковзного вікна; $N_{NLM}(i,j)$ – нормуючий множник для поточного значення ковзного вікна NLM-фільтру. В якості функції $w(x,y)$ широко використовується гаусова функція для мінімізації впливу локальних збурень значень яскравості пікселів на оброблене ЦЗ [238].

Зважаючи на адаптивний підхід до масштабування значення яскравості пікселів для NLM-фільтру, становить інтерес його використання для зниження спотворень ЗК, обумовлених вбудовування стегоданих. Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при використанні NLM-фільтру для тестових зображень з пакету ALASKA наведені на рис. 3.15.

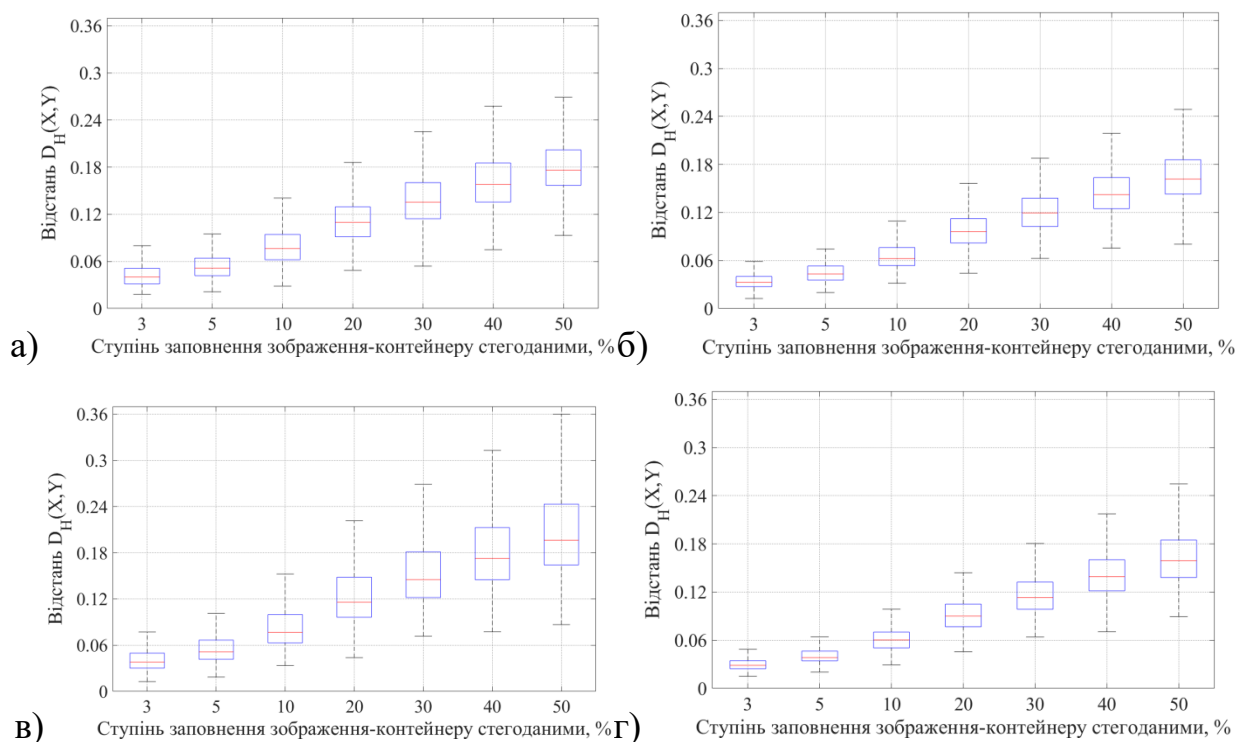


Рисунок 3.15 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при використанні NLM-фільтрації для ЗК з пакету ALASKA та стеганограм, сформованих згідно стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Застосування методів NLM-фільтрації досліджуваних ЦЗ дозволяє підвищити значення відстані D_H для розглянутих стеганографічних методів (рис. 3.15) – зміни D_H сягають від 5% в області слабого ($\Delta_\alpha^S < 10\%$) до 9% в області сильного ($\Delta_\alpha^S > 20\%$) заповнення ЗК стегоданими у порівнянні з випадком обробки вихідних ЦЗ (рис. 2.5). Це свідчить про ефективність використання NLM-фільтру для підсилення відмінностей між розподілами значень яскравості пікселів ЗК та стеганограм. Проте практичне застосування даного методу обробки ЦЗ при побудві СД може бути обмеженим внаслідок використання КВ значного розміру (більше 9×9 пікселів) для підвищення ефективності використання NLM-фільтру щодо зниження впливу локальних збурень яскравості пікселів.

Розглянуті методи анізотропної фільтрації дозволяють суттєво зменшувати вплив локальних збурень яскравості пікселів ЦЗ. Проте це може призводити до суттєвих змін спектральних параметрів оброблюваних зображень, що

ускладнює виявлення демаскуючих ознак стеганограм. Відмітимо, що приховання повідомлень проводиться на рівні власних шумів ЦЗ, а саме шляхом зміни високочастотних складових ЗК [10] [9] [11]. Тому становить інтерес використання методів спектрального аналізу для виявлення та посилення даних слабких змін спектарльних складових зображення-контейнеру.

3.1.4 Спектральні методи знешумлення цифрових зображень

Для зниження впливу адитивних шумів на зображенні широко використовуються як статистичні, так і спектральні методи обробки ЦЗ. На відміну від розглянутих в попередньому розділі статистичних методів, спектральні методи засновані на представленні оброблюваного ЦЗ як суми спектральних складових [142]. Це дозволяє зменшити вплив завад шляхом простої порогової обробки коефіцієнтів розкладу ЦЗ в заданому базисі перетворення, без необхідності використання обчислювально складних методів статистичного моделювання для кожного типу шумів/завад.

Сучасним підходом до зниження впливу адитивних шумів у ЦЗ є використання ДДВП. Дане перетворення засноване на використанні вейвлету $\psi(\cdot)$ та відповідної йому скейлінг-функцій $\varphi(\cdot)$ для декомпозиції оброблюваного зображення \mathbf{U} [141,142]:

$$\begin{aligned} \mathbf{U}_{x,y} &= \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \mathbf{W}_{xy}^A(\mathbf{U}_{x,y}) \cdot \varphi_x \varphi_y + \mathbf{W}_{xy}^H(\mathbf{U}_{x,y}) \cdot \psi_x \varphi_y \\ &\quad + \mathbf{W}_{xy}^V(\mathbf{U}_{x,y}) \cdot \varphi_x \psi_y + \mathbf{W}_{xy}^D(\mathbf{U}_{x,y}) \cdot \psi_x \psi_y \\ \mathbf{W}_{xy}^k(\mathbf{U}_{x,y}) &= \langle \mathbf{U}_{x,y}, \Psi_{x,y}^k \rangle = \frac{1}{MN} \cdot \sum_{x=0}^{N-1} \sum_{y=0}^{M-1} \sum_{k \in \{A,H,V,D\}} \mathbf{U}_{x,y} \cdot \Psi_{x,y}^k, \end{aligned}$$

де \mathbf{W}_{xy}^A – апроксимуючі коефіцієнти, що відповідають низькочастотним складовим ЦЗ, наприклад контурам об'єктів; \mathbf{W}_{xy}^H , \mathbf{W}_{xy}^V , \mathbf{W}_{xy}^D – високочастотні складові, що відповідають текстурованим областям зображення.

Важливою особливістю ДДВП є формування систем базисних функцій, а саме вейвлету $\psi(\cdot)$ та відповідної скейлінг-функцій $\varphi(\cdot)$, для виявлення та

локалізації локальних збурень значення яскравості пікселів ЦЗ [142]. Це дозволяє проводити обробку лише окремих складових зображення, та мінімізувати спотворення інших компонентів ЦЗ, що становить інтерес для побудови високоточних СД. Тому становить інтерес використання методів вейвлет-фільтрації (ВФ) сигналів в задачах попередньої обробки ЦЗ. Особливістю даних методів є адаптивний підбір порогових значень для коефіцієнтів \mathbf{W}_{xy}^H , \mathbf{W}_{xy}^V та \mathbf{W}_{xy}^D за критерієм мінімізації впливу адитивних завад [142]:

$$T_{hard}(x, T) = \begin{cases} x, & |x| \geq T, \\ 0, & |x| < T, \end{cases} \quad (3.4)$$

$$T_{soft}(x, T) = \max(1 - T/|x|, 0), \quad (3.5)$$

$$T_{DJ}(\mathbf{x}) = \sigma_x \sqrt{2 \cdot \ln N_x}, \quad (3.6)$$

де T_{hard} , T_{soft} – функції жорсткої та м'якої порогової обробки відповідно; $T > 0$ – порогове значення; $T_{DJ}(\mathbf{x})$ – порогова функція Донохо-Джонсона для обробки послідовності \mathbf{x} з N_x елементів; σ_x – середньоквадратичне відхилення значень елементів послідовності \mathbf{x} . Відмітимо, що функції (3.4)-(3.6) можуть застосовуватися для обробки як окремих коефіцієнтів розкладу ДДВП (локальна порогова обробка), наприклад для заданого частотного діапазону, так і до всіх коефіцієнтів розкладу (глобальна порогова обробка) з метою зниження впливу адитивних шумів та завад.

Дослідження ефективності використання методів ВФ для попередньої обробки ЦЗ проведено з використанням вейвлету Хаара та відповідної скейлінг-функції в якості базисів вейвлет-перетворення. Даний вейвлет широко використовується в обробці ЦЗ, зокрема локалізації та зниження впливу імпульсних завад, що відповідають локальним змінам яскравості пікселів при вбудовуванні стегобіт [142]. Дослідження проводилося в декілька етапів при використанні розглянутих методів визначення порогових значень.

На першому етапі, розглянуто випадок калібрування ЦЗ шляхом застосування ВФ з глобальним порогом $T = \text{median}(|\mathbf{W}_{xy}^k|)$ для всіх рівнів декомпозиції зображення. Залежності значень відстані Хеллінгера D_H між розподі-

лами значень яскравості пікселів ЗК та стеганограм при ВФ досліджуваних зображень з єдиним (глобальним) порогом для тестових зображень з пакету ALASKA наведені на рис. 3.16.

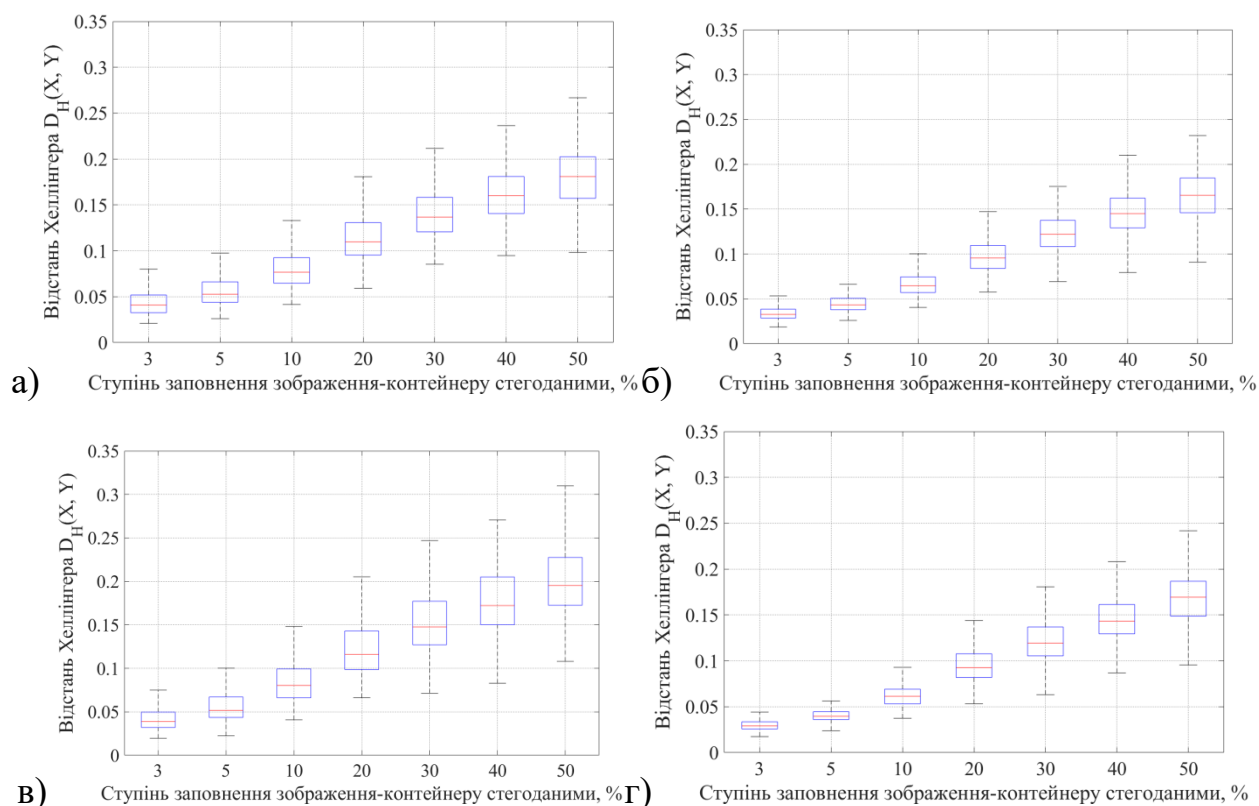


Рисунок 3.16 Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при вейвлет-фільтрації досліджуваних зображень з єдиним (глобальним) порогом для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Використання єдиного глобального порогу для обробки коефіцієнтів декомпозиції ЗК та стеганограм призводить до несуттєвого зростання значень відстані Хеллінгера D_H ($\Delta D_H \leq 5\%$) для досліджуваних стеганографічних методів (рис. 3.16) у порівнянні з випадком обробки вихідних ЦЗ (рис. 2.5). Це свідчить про відносно малі зміни розподілів значень яскравості пікселів ЗК та стеганограмами, що не дозволяє підвищити точність виявлення стеганограм. Тому становить інтерес використання порогових значень, що обчислюються для кожного рівня декомпозиції досліджуваного ЦЗ. В якості прикладу розглянемо використання порогової функції Донохо-Джонсона T_{DJ}

(3.6) для мінімізації емпіричної оцінки параметрів адитивних завад на кожному рівні декомпозиції зображення [142], а також методу Бірге-Массарта [239]. Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при ВФ досліджуваних зображень з пороговою функцією Донохо-Джонсона T_{DJ} для тестових зображень з пакету ALASKA наведені на рис. 3.17.

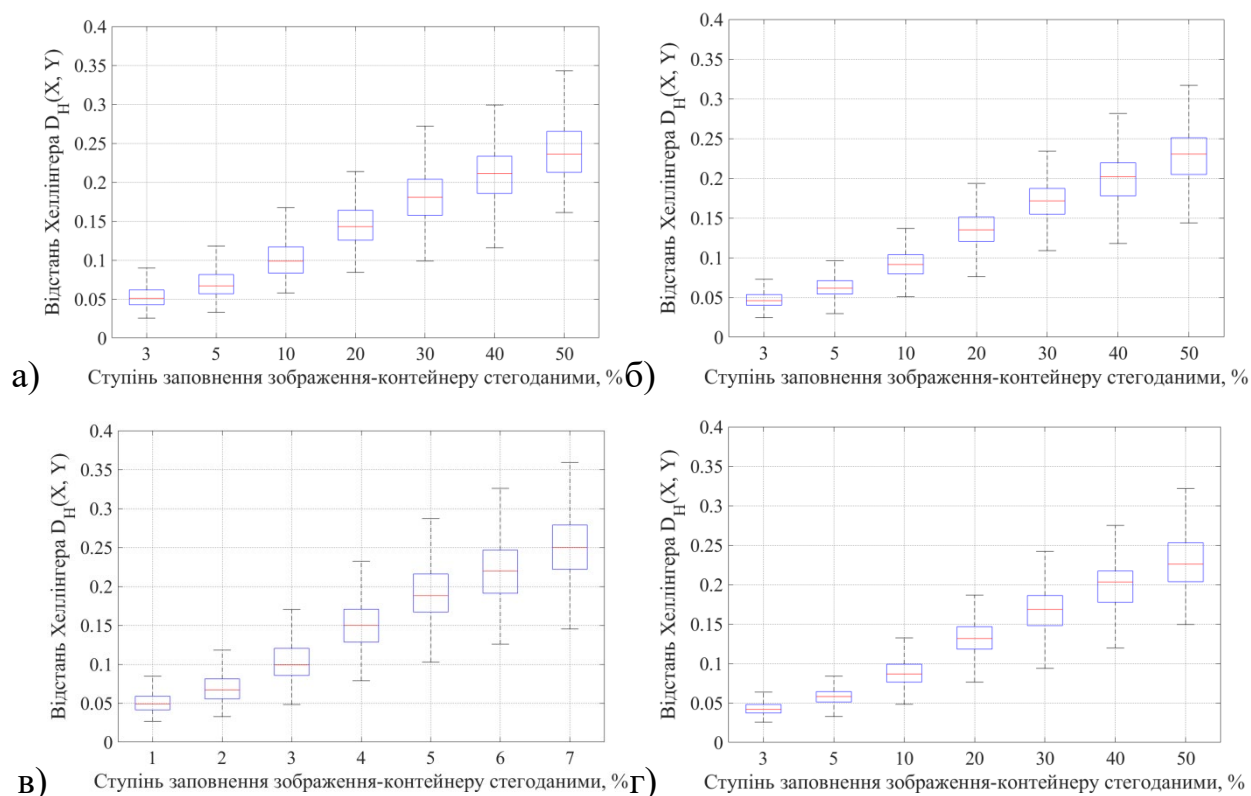


Рисунок 3.17 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при ВФ досліджуваних зображень з пороговою функцією Донохо-Джонсона T_{DJ} для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічних методів: (а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Використання порогової функції T_{DJ} дозволяє підвищити значення D_H ($\Delta D_H \cong 25\%$) між розподілами значень яскравості пікселів ЗК та стеганограм для розглянутих СМ (рис. 3.17) у порівнянні з випадком обробки вихідних ЦЗ (рис. 2.5). Виявлене зростання значень D_H отримано в області середнього ($10\% \leq \Delta_\alpha^S \leq 20\%$) та сильного ($\Delta_\alpha^S > 20\%$) заповнення ЗК стегоданими, що свідчить про ефективність придушення спотворень, обумовлених прихова-

нням повідомлень, при проведенні ВФ. В області слабого заповнення ЗК стегоданими ($\Delta\alpha^S < 10\%$) зміни відстані Хеллінгера D_H при використанні порогової функції Донохо-Джонсона T_{DJ} є несуттєвими ($\Delta D_H \leq 5\%$), що свідчить про обмеження даного підходу щодо зниження впливу відносно малої кількості спотворень яскравості пікселів ЗК при вбудовуванні стегоданих.

Для порівняння розглянемо використання спеціалізованих методів ВФ, а саме метод Бірге-Массарта для обчислення порогових значень на кожному рівня розкладу досліджуваного ЦЗ [239]. Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при вейвлет-фільтрації досліджуваних зображень з пороговою функцією Бірге-Массарта для тестових зображень з пакету ALASKA наведені на рис. 3.18.

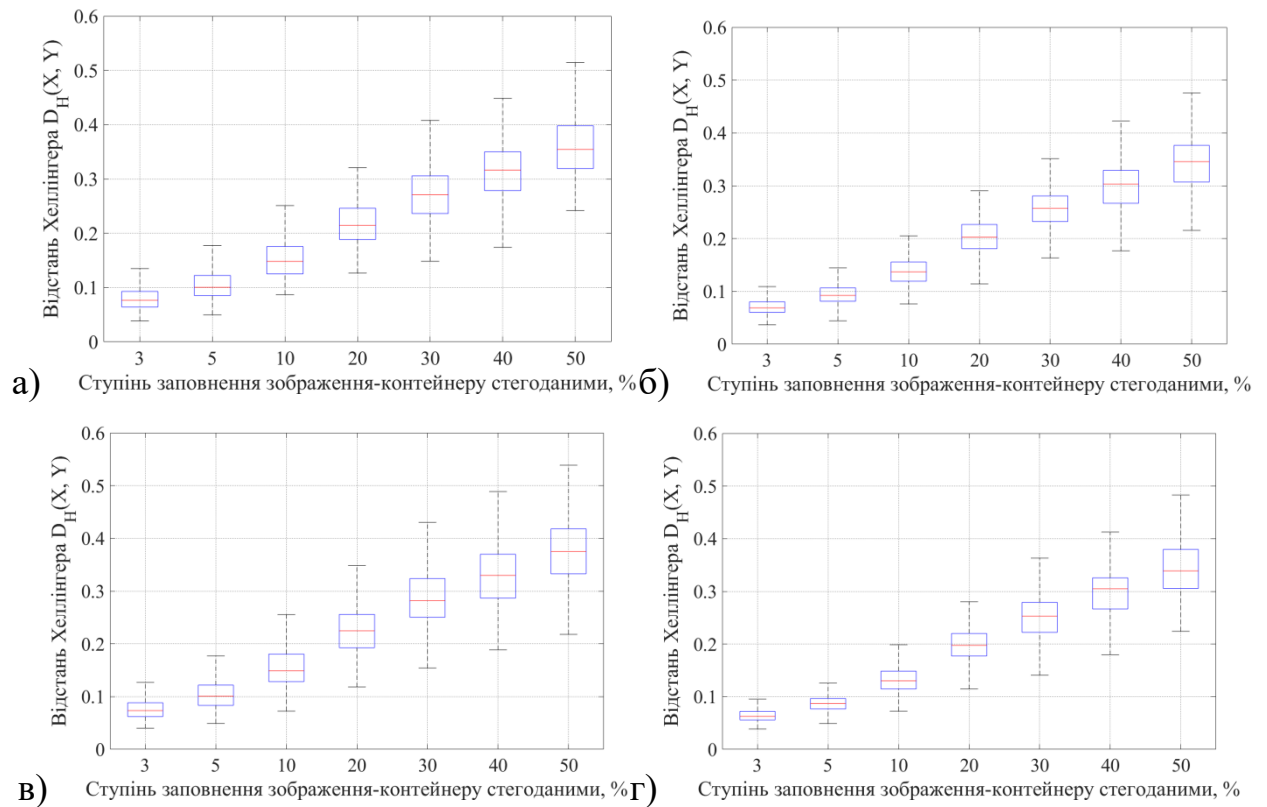


Рисунок 3.18 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при ВФ досліджуваних зображень з пороговою функцією Бірге-Массарта для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Використання спеціалізованого методу Бірге-Массарта для визначення порогових значень для коефіцієнтів ДДВП досліджуваних зображень (рис. 3.18) дозволило підвищити значення відстані Хеллінгера D_H ($\Delta D_H \cong 70\%$) у порівнянні з випадком обробки вихідних ЦЗ (рис. 2.5). При цьому найбільші зміни значень D_H отримані в області сильного заповнення ЗК стегоданими ($\Delta \alpha^S > 20\%$), в той час як для малих значень $\Delta \alpha^S$ ($\Delta \alpha^S < 10\%$) зміни значень D_H сягають лише 10% для розглянутих СМ. Таким чином, використання методу Бірге-Массарта дозволяє підвищити точність реконструкції ЗК за наявними зашумленими даними, проте ефективність даного методу суттєво знижується при зменшенні ступеня заповнення ЗК стегоданими.

Розглянуті методи спектральної обробки ЦЗ засновані на використанні припущення, що статистичні параметри завад є апріорно відомими, наприклад енергія завад рівномірно розподілена по окремим частотним діапазонам. Це дозволяє ефективно придушувати вплив завад з використанням порогових методів обробки коефіцієнтів розкладу ЦЗ. Проте обробка ЗК з використанням новітніх СМ призводить до мінімізації змін статистичних та спектральних параметрів ЩК, обумовлених локальними збуреннями значень яскравості пікселів внаслідок приховання стегобітів. Тому коефіцієнти розкладу ДДВП, які відповідають даним спотворенням можуть бути нерівномірно розділеними між декількома частотними діапазонами, що знижує ефективність використання спектральних методів обробки ЗК [95].

3.1.5 Варіаційні методи знешумлення цифрових зображень

Для подолання наведених обмежень спектральних методів зниження впливу завад становить інтерес застосування TVM-методів обробки ЦЗ, заснованих на мінімізації дисперсії σ_I^2 значень яскравості пікселів зображення. Для оцінки значення σ_U^2 для напівтонового зображення \mathbf{U} розміром $N \times M$ пікселів може бути використана наступна формула [142,240]:

$$V(\mathbf{U}) = \sum_{x,y} \sqrt{|\mathbf{U}_{x+1,y} - \mathbf{U}_{x,y}|^2 + |\mathbf{U}_{x,y+1} - \mathbf{U}_{x,y}|^2}. \quad (3.7)$$

Тоді задача зниження впливу адитивних завад для поточного ЦЗ може бути представлена як оптимізаційна задача мінімізації загального рівня варіації значень яскравості пікселів зображення [240]:

$$\min_{\mathbf{U}} (\|\mathbf{U}\|_2^2 + \lambda V(\mathbf{U})), \quad (3.8)$$

де $\|\mathbf{U}\|_2^2$ – оцінка енергії зображення; $\lambda > 0$ – ваговий параметр регуляризації впливу варіації $V(\mathbf{U})$ значень яскравості пікселів ЦЗ на загальну енергію ЦЗ. Відмітимо, що функція (3.7) не є диференційною, що обмежує використання відомих методів оптимізації для вирішення задачі (3.8). Тому в більшості випадків використовується наступна оцінка $V_{anis}(\mathbf{U})$ значення $\sigma_{\mathbf{U}}^2$ [241]:

$$V_{anis}(\mathbf{U}) = \sum_{x,y} |\mathbf{U}_{x+1,y} - \mathbf{U}_{x,y}| + |\mathbf{U}_{x,y+1} - \mathbf{U}_{x,y}|.$$

Для вирішення оптимізаційної задачі (3.8) при використанні наведеної оцінки $V_{anis}(\mathbf{U})$ дисперсії значень яскравості пікселів ЦЗ запропоновано значну кількість методів, наприклад методи Чамболлі [241] та Брегмана [242]. Особливістю даних методів є вирішення оптимізаційної задачі (3.8) як еквівалентної задачі [242]:

$$\min_{\mathbf{U} \in BV(\Omega)} \|\mathbf{U}\|_{TV(\Omega)} + \frac{\lambda}{2} \int_{\Omega} (\tilde{\mathbf{U}} - \mathbf{U})^2 dx dy, \quad (3.9)$$

де $BV(\Omega)$ – множина функцій з обмеженою варіацією значень в області Ω ; $TV(\Omega)$ – оператор оцінки загальної дисперсії сигналу в області Ω ; $\lambda > 0$ – ваговий параметр регуляризації; $\tilde{\mathbf{U}}$ – оцінка значень яскравості пікселів ЦЗ після застосування TVM-методу.

У випадку обробки сигналів, що характеризуються високим ступенем гладкості, зокрема цифрових зображень, оператор $TV(\Omega)$ у виразі (3.9) є еквівалентним до обчислення градієнту сигналу:

$$\|\mathbf{U}\|_{TV(\Omega)} = \int_{\Omega} \|\nabla \mathbf{U}\|_2 dx dy.$$

Тоді оптимізаційна задача (3.9) може бути розв’язана з використанням чисельних методів, зокрема шляхом вирішення наступного рівняння згідно методу Ейлера-Лагранжа [242]:

$$\begin{cases} \nabla \cdot \left(\frac{\nabla \mathbf{U}}{\|\nabla \mathbf{U}\|_2} \right) + \lambda(\tilde{\mathbf{U}} - \mathbf{U}) = 0, & \mathbf{U} \in \Omega, \\ \frac{\partial \mathbf{U}}{\partial x \partial y} = 0, & \mathbf{U} \in \partial\Omega. \end{cases} \quad (3.10)$$

В роботі досліджено випадки використання розглянутих методів Брегмана та Чамболлі для TVM-обробки досліджуваних ЦЗ при використанні чисельних методів для вирішення оптимізаційної задачі (3.10). Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при використанні TVM-методу знемушлення Брегмана для тестових зображень з пакету ALASKA наведені на рис. 3.19.

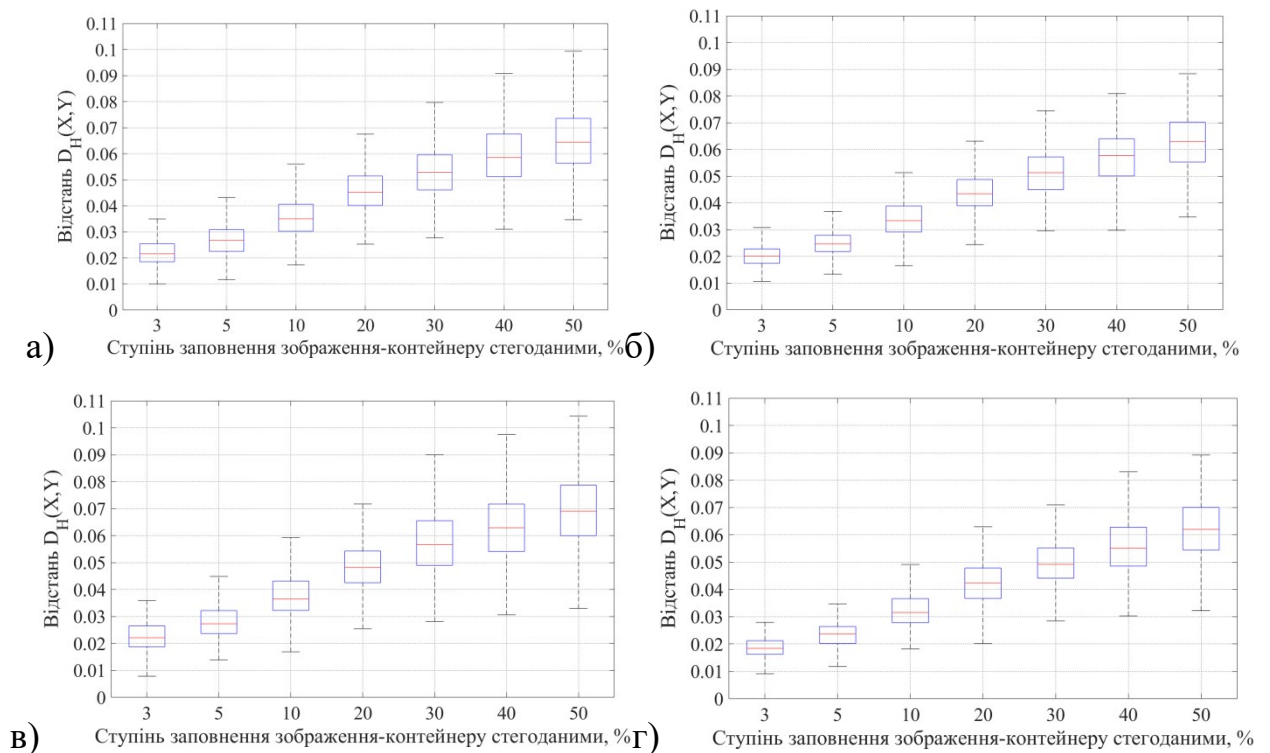


Рисунок 3.19 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при використанні TVM-методу знемушлення Брегмана для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Використання TVM-методу знемушення Брегмана (рис. 3.19) призводить до суттєвого зменшення значень відстані Хеллінгера D_H у порівнянні з випадком обробки вихідних ЦЗ (рис. 2.5). Це негативно впливає на точність віднесення ЦЗ до класів ЗК або стеганограм класифікатором при налаштуванні СД. Отримані результати можуть бути пояснені мінімізацією загального рівня варіації значень яскравості пікселів ЦЗ, що зменшує вплив як локальних спотворень, обумовлених прихованням повідомлень, так і власних шумів ЗК (наприклад, локальних збурень значень яскравості пікселі внаслідок дефектів елементів МФЕ).

Для порівняння був розглянутий випадок використання TVM-методу знемушення Чамболлі для проведення попередньої обробки ЗК та стеганограм. Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при використанні TVM-методу Чамболлі для тестових зображень з пакету ALASKA наведені на рис. 3.20.

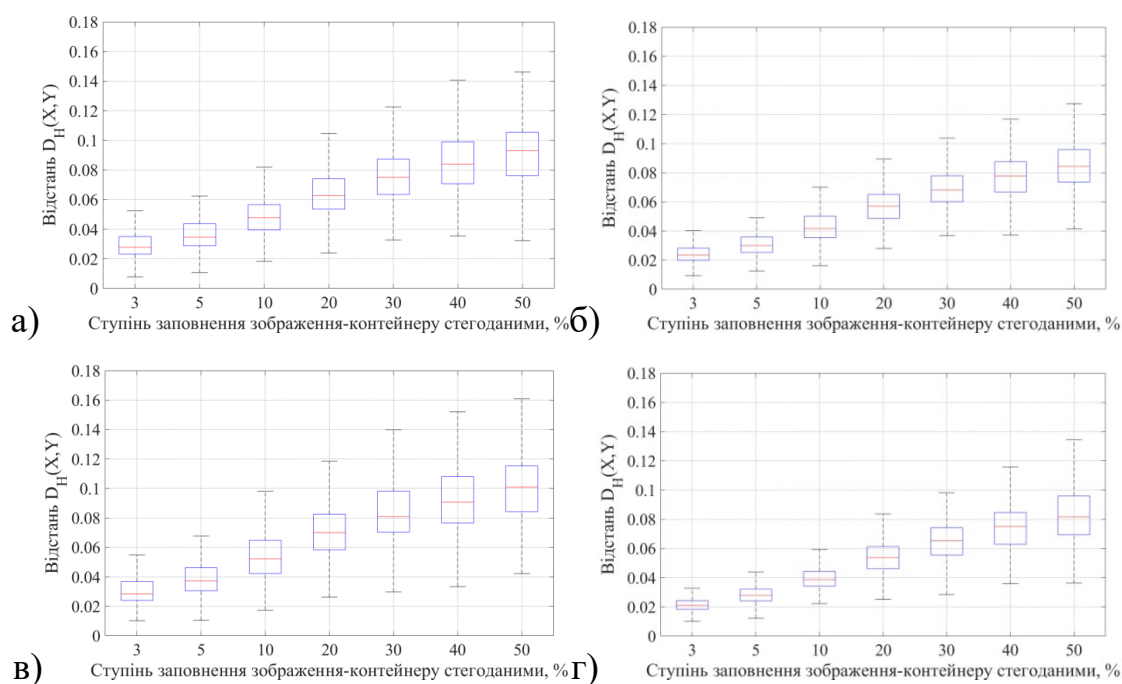


Рисунок 3.20 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при використанні TVM-методу знемушення Чамболлі для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічних методів:

(а) – HUGO; (б) – S-UNIWARD; (в) – MG; (г) – MiPOD.

Отримані значення відстані Хеллінгера при використанні TVM-методу знемушення Чамболлі (рис. 3.20) суттєво перевищують отримані раніше результати при використанні TVM-методу Брегмана (рис. 3.19). Проте, результати для методу Чамболлі також суттєво поступаються значенням відстані D_H при обробці вихідних зображень (рис. 2.5).

Тому можемо зробити висновок, що використання TVM-методу для калібрування ЦЗ не дозволяє посилити відмінності між розподілами значень яскравості пікселів ЗК та стеганограм. Особливістю розглянутих методів обробки ЦЗ є використання спектральних, статистичних або ж енергетичних характеристик спотворень ЗК, обумовлених прихованням повідомлень до ЗК [226], для визначення та вилучення компонентів (складових) досліджуваних ЦЗ. Проте суттєвий вплив на ефективність використання даних методів має використання апріорних даних щодо використаного СМ, які можуть бути обмеженими або навіть відсутніми у більшості випадків. Тому становить інтерес використання новітніх методів обробки сигналів, зокрема ШНМ та методів компонентного аналізу, здатних працювати в умовах обмеженості апріорних даних щодо змін статистичних та спектральних параметрів ЗК, обумовлених вбудовуванням стегоданих.

3.1.6 Методи знешумлення цифрових зображень на основі штучних нейронних мереж

Для подолання наведених обмежень поширених типів МПО, спрямованих на оцінку статистичних, спектральних та енергетичних параметрів ЗК, було запропоновано використовувати ШНМ [45]. Забезпечення високої точності виявлення стеганограм при використанні штучних нейронних мереж досягається за рахунок налаштування параметрів шарів штучних нейронів для мінімізації значення помилки P_E (1.25) на заданому пакеті тестових ЗК та стеганограм [8]. Це потребує використання стегоаналітиком апріорних даних щодо СМ для формування прикладів стеганограм, що є неможливим у випадку виявлення невідомих стеганографічних методів.

Одним з методів подолання даного обмеження є використання спеціальних видів штучних нейронних мереж, зокрема АНМ [46,47]. Особливістю даних мереж є використання двох модулів (кодера та декодера) для відтворення вхідного зображення на виході мережі при накладанні певних умов щодо структури та параметрів проміжних шарів штучних нейронів. Приклад структури АНМ для обробки цифрових зображень наведено на рис. 3.21.

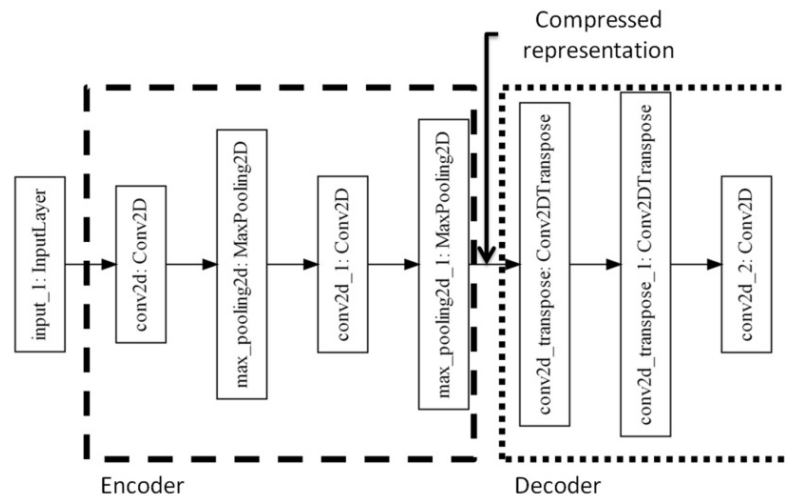


Рисунок 3.21 – Приклад структури автокодувальної нейронна мережа для проведення попередньої обробки цифрових зображень.

Перша частина автокодувальної мережі (мережа кодера, рис. 3.21) дозволяє проводити проєкцію заданого багатовимірного сигналу (а саме, цифрового зображення) в простір меншої розмірності, зберігаючи його статистичні параметри. Відновлення вихідного виду зображення за отриманим представленням (вектором \mathbf{h}) проводиться мережею декодера (рис. 3.21).

Використання додаткових вимог щодо параметрів кодера та декодера (рис. 3.3) дозволяє забезпечити спеціальні властивості АНМ, зокрема оцінку вихідного виду ЦЗ за наявними (зашумленими) даними, що становить особливий інтерес в задачах стегааналізу ЦЗ [127]:

$$-\mathbb{E}_{\mathbf{U} \sim \hat{p}_{data}(\mathbf{U})} \mathbb{E}_{\tilde{\mathbf{U}} \sim C(\tilde{\mathbf{U}}|\mathbf{U})} \log \left(p_{decoder}(\mathbf{U}|\mathbf{h} = f(\tilde{\mathbf{U}})) \right) \rightarrow \min,$$

де $\mathbf{U}, \tilde{\mathbf{U}}$ – відповідно, вихідне та зашумлене (спотворене) цифрове зображення; $C(\tilde{\mathbf{U}}|\mathbf{U})$ – функція внесень спотворених до зображення \mathbf{U} ; $\hat{p}_{data}(\mathbf{U})$ – імовірнісний розподіл ЦЗ, що використовуються для налаштува-

ння ЗНАЕ; $p_{decoder}(\cdot)$ – імовірнісний розподіл зображень на виході мережі декодера ЗНАЕ.

В роботі досліджено використання багат шарових ЗНАЕ в задачах визначення статистичних параметрів ЗК за наявними (зашумленими) даними. В якості прикладу такої мережі розглянуто використання знешумлюючого автоенкодера з моделі ASSAF [127] (розд. 1.2.3). Структура ЗНАЕ моделі ASSAF наведена на рис. 3.22.

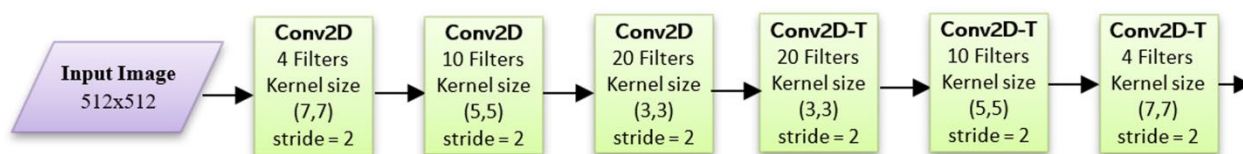


Рисунок 3.22 – Структура знешумлюючого автоенкодера для нейронної мережі моделі ASSAF. За матеріалами роботи [127].

Особливістю даного ЗНАЕ є використання згорткових шарів штучних нейронів для визначення та обробки статистичних параметрів оброблюваного зображення. Це дозволяє зменшити вимоги щодо об'єму тестової вибірки ЦЗ, а також складності налаштування ЗНАЕ у порівнянні з випадком використання повнозв'язних шарів нейронів [46,47]. Розмір вхідного зображення мережі (рис. 3.22) обрано рівним 512×512 пікселів, що дозволяє оброблювати тестові ЦЗ з використанням розглянутих пакетів ALASKA, VISION та MIRFlickr без необхідності зміни розмірів зображень.

Для дослідження ефективності використання ЗНАЕ в задачах попередньої обробки ЦЗ в роботі проведено налаштування знешумлюючого автоенкодера на основі штучної нейронної мережі ASSAF з використанням вибірки зображень з пакету ALASKA та відповідних стеганограм, сформованих згідно стеганографічного методу S-UNIWARD при варіації ступеня заповнення ЗК стегоданими [127]. Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу HUGO, при використанні ЗНАЕ на основі моделі ASSAF для тестових зображень з пакету ALASKA наведені на рис. 3.23.

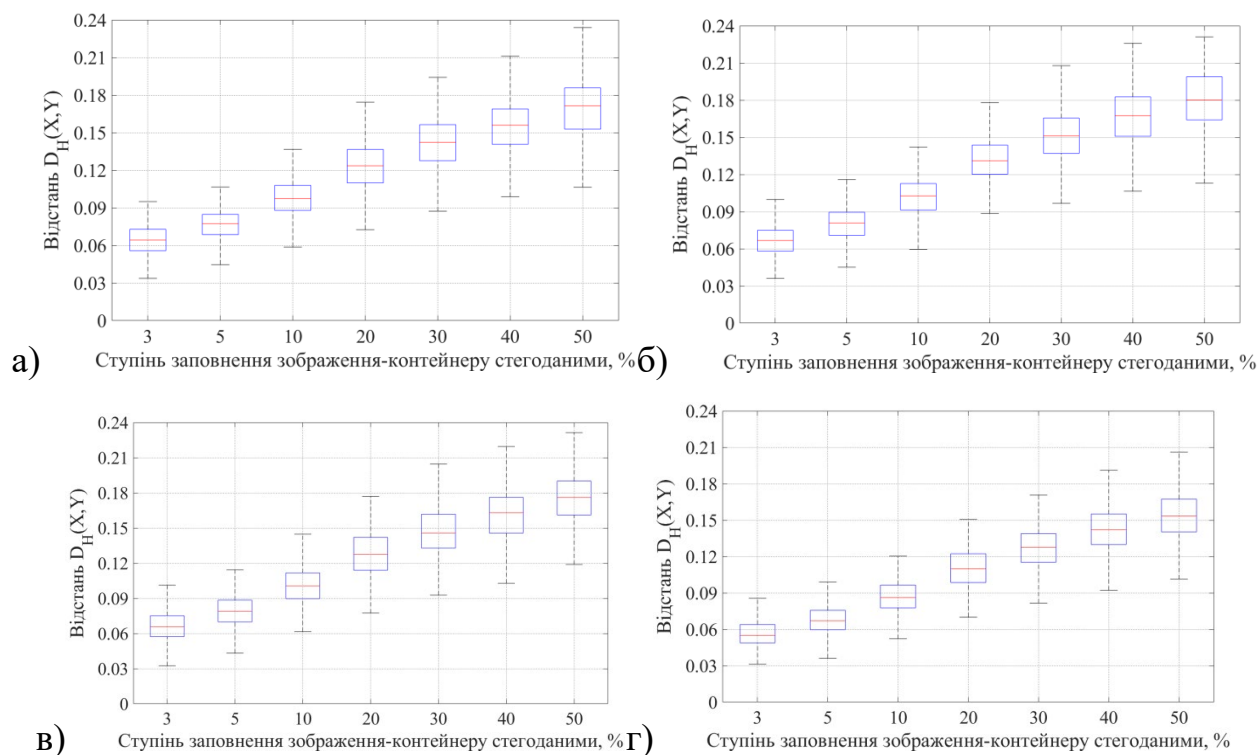


Рисунок 3.23 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічного методу HUGO. Знешумлюючий автоенкодер на основі моделі ASSAF, налаштований з використанням стеганографічного методу S-UNIWARD при ступені

заповнення ЗК стегоданими: (а) – $\Delta_{\alpha}^S = 20\%$; (б) – $\Delta_{\alpha}^S = 30\%$;

(в) – $\Delta_{\alpha}^S = 40\%$; (г) – $\Delta_{\alpha}^S = 50\%$.

Застосування ЗНАЕ дозволяє суттєво збільшити значення D_H ($\Delta D_H \cong 20\%$) у порівнянні з випадком відсутності МПО (рис. 2.5), особливо в області слабого заповнення ЗК стегоданими (рис. 3.23). Зміни значень D_H в області середнього ($10\% \leq \Delta_{\alpha}^S \leq 20\%$) та сильного ($\Delta_{\alpha}^S > 20\%$) заповнення ЗК стегоданими не перевищують 5% (рис. 3.23). Це свідчить про високу вибірковість роботи ЗНАЕ щодо виявлення та придушення локальних збурень яскравості пікселів ЗК, обумовлених прихованням повідомлень. Зростання ступеня заповнення ЗК стегоданими призводить до «розпорощення» даних змін по досліджуваному зображенню, що знижує ефективність використання ЗНАЕ.

Враховуючи отримані результати, становить інтерес дослідження ефективності застосування ЗНАЕ для обробки стеганограм, сформованих згідно ACM. Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу S-UNIWARD, при використанні ЗНАЕ на основі моделі ASSAF для тестових зображень з пакету ALASKA наведені на рис. 3.24.

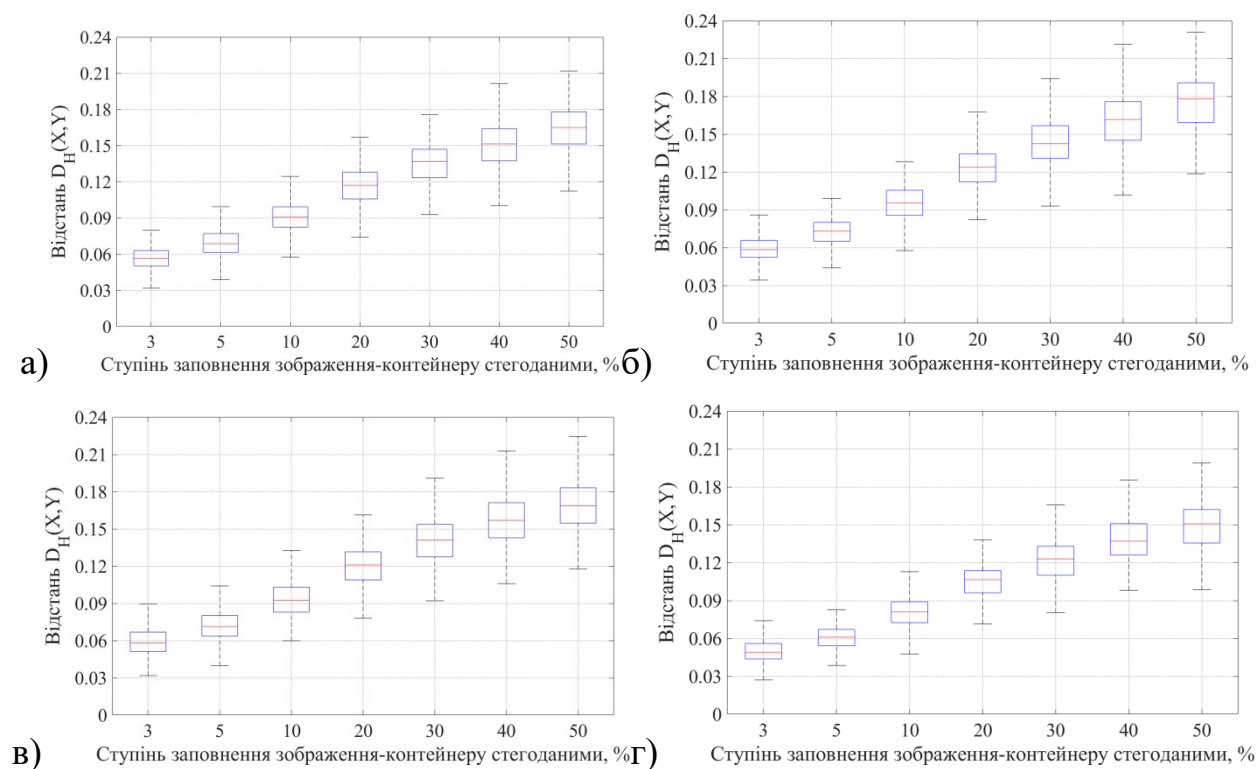


Рисунок 3.24 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічного методу S-UNIWARD. Знешумлюючий автоенкодер з моделі ASSAF, налаштований з використанням стеганографічного методу S-UNIWARD при ступені

заповнення ЗК стегоданими: (а) – $\Delta_{\alpha}^S = 20\%$; (б) – $\Delta_{\alpha}^S = 30\%$;

(в) – $\Delta_{\alpha}^S = 40\%$; (г) – $\Delta_{\alpha}^S = 50\%$.

Аналогічно до попереднього випадку (рис. 3.23), застосування ЗНАЕ дозволяє суттєво підвищити значення відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм (рис. 3.24). На відміну від результатів для методу HUGO (рис. 3.23), застосування ЗНАЕ дозволяє підвищити

значення D_H у всьому діапазоні значень Δ_α^S (рис. 3.24). При цьому, найбільші зміни значень D_H досягаються при використанні навчальної вибірки стеганограм з середнім ступенем заповнення (рис. 3.24в).

Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу MG, при використанні ЗНАЕ на основі моделі ASSAF для тестових зображень з пакету ALASKA наведені на рис. 3.25.

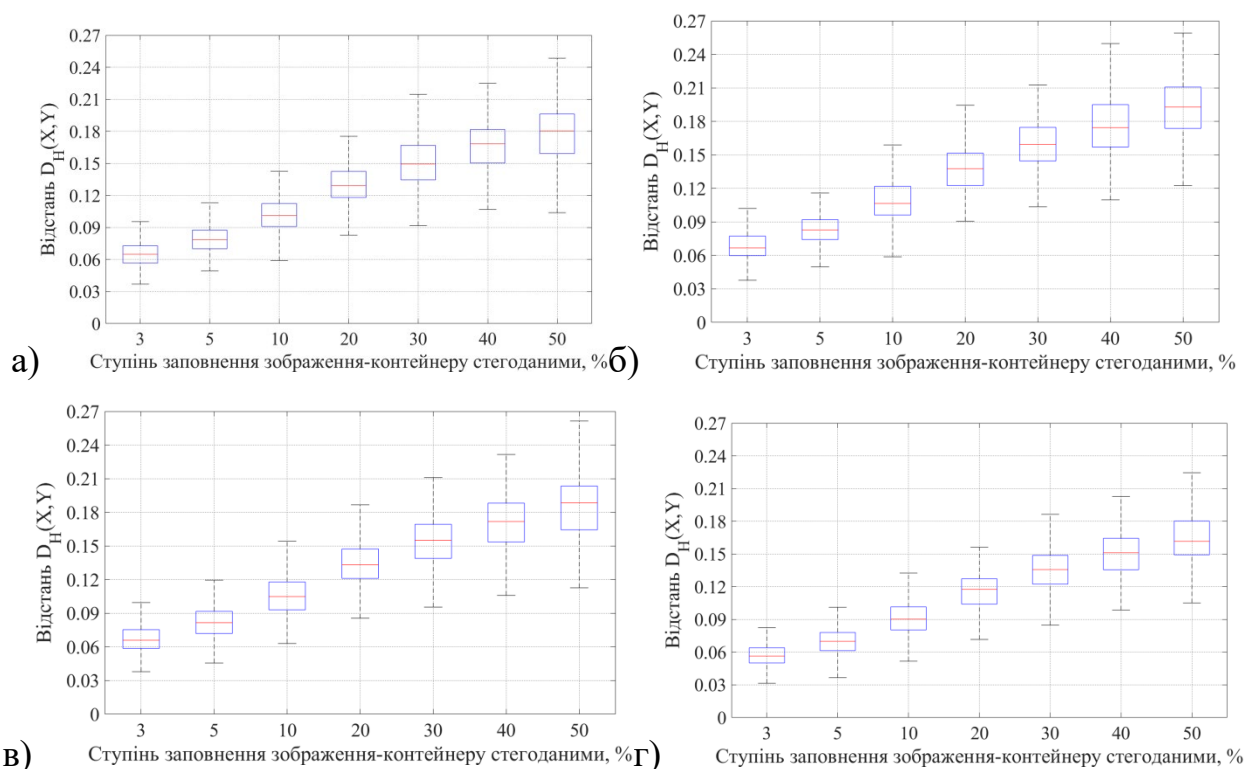


Рисунок 3.25 – Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічного методу MG.

Знешумлюючий автоенкодер з моделі ASSAF, налаштований з використанням стеганографічного методу S-UNIWARD при ступені

заповнення ЗК стегоданими: (а) – $\Delta_\alpha^S = 20\%$; (б) – $\Delta_\alpha^S = 30\%$;

(в) – $\Delta_\alpha^S = 40\%$; (г) – $\Delta_\alpha^S = 50\%$.

Ефективність використання ЗНАЕ при обробці стеганограм, сформованих згідно стеганографічного методу MG (рис. 3.25), суттєво поступається попереднім результатам (рис. 3.23-3.24). Зокрема, збільшення значень D_H до-

сягається лише в області слабого заповнення ЗК стегоданими ($\Delta_{\alpha}^S < 10\%$, рис. 3.25). Це свідчить про обмеження використання ЗНАЕ для виявлення локальних змін значень яскравості ЗК, обумовлених прихованням повідомлень згідно методу MG.

Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу MiPOD, при використанні ЗНАЕ на основі моделі ASSAF для тестових зображень з пакету ALASKA наведені на рис. 3.26.

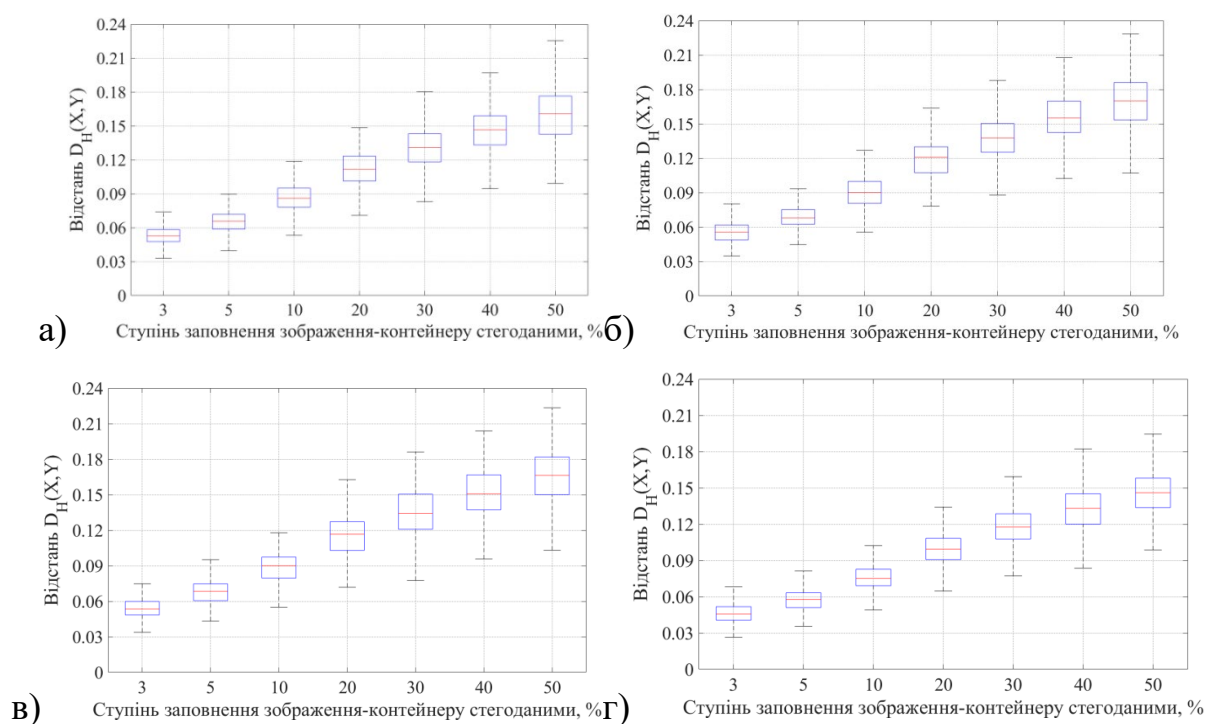


Рисунок 3.26 Залежності відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм для зображень-контейнерів з пакету ALASKA та стеганограм, сформованих згідно стеганографічного методу MiPOD. Знешумлюючий автоенкодер з моделі ASSAF, налаштований з використанням стеганографічного методу S-UNIWARD при ступені

заповнення ЗК стегоданими: (а) – $\Delta_{\alpha}^S = 20\%$; (б) – $\Delta_{\alpha}^S = 30\%$;

(в) – $\Delta_{\alpha}^S = 40\%$; (г) – $\Delta_{\alpha}^S = 50\%$.

На відміну від результатів, отриманих для стеганографічного методу MG (рис. 3.25), застосування ЗНАЕ дозволяє підвищити значення D_H ($\Delta D_H \cong 10\%$) для методу MiPOD (рис. 3.26) у всьому діапазоні значень Δ_{α}^S . Даний

результат є попередньо неочікуваним, оскільки метод MiPOD дозволяє додатково зменшити зміни статистичних та спектральних параметрів ЗК у порівнянні з методом MG [152,153].

Таким чином, застосування ЗНАЕ дозволяє збільшити відмінності між розподілами значень яскравості пікселів ЗК та стеганограм, проте потребує переналаштування даної ШНМ для кожного стеганографічного методу. Це може бути нетривіальною задачею у випадку обмеженої кількості прикладів стеганограм для попередньо невідомого стеганографічного методу. З іншого боку, розглянутий ЗНАЕ (рис. 3.22) відноситься до класу малих штучних нейронних мереж, що складаються з декількох шарів штучних нейронів. Це дозволяє швидко проводити його налаштування для застосування в задачах стегоаналізу. Використання більш глибоких автоенкодерних мереж дає можливість виявляти нелінійні взаємозв'язки між елементами зображення для вибору «стиснутого» представлення за рахунок суттєвого підвищення складності налаштування даних мереж [46,47].

Важливою перевагою використання ЗНАЕ при побудові високоточних СД є можливість оцінки вихідного виду ЗК за наявними (зашумленими) даними. Це досягається за рахунок тривалого налаштування даної штучної нейронної мережі на потужних вибірках ЦЗ для виокремлення складових (компонентів) оброблюваного зображення, що були використані в процесі вбудовування стеганограм. Проте висока гнучкість використання ЗНАЕ для виявлення стеганограм, сформованих згідно новітніх типів СМ, потребує повторного переналаштування параметрів мережі, що ускладнює адаптацію СД. Тому становить інтерес використання спеціальних типів спектрального аналізу, зокрема компонентного аналізу для забезпечення високої точності виокремлення складових ЗК, на рівні котрих проводиться приховання окремих стегобітів, при збереженні фіксованої тривалості налаштування стегодетектору.

3.1.7 Методи компонентного аналізу для знешумлення цифрових зображень

Обробка ЦЗ з використанням спектральних перетворень дозволяє зменшувати вплив спотворень, обумовлених прихованням повідомлень [91]. Проте вибір системи функцій для мінімізації впливу даних спотворень є нетривіальною задачею [142], що вирішена лише для часткових випадків, зокрема зменшення впливу гаусових шумів, дробових шумі тощо.

Для подолання даного обмеження спектральних методів обробки ЦЗ автором запропоновано використовувати методи компонентного аналізу ЦЗ [91,243], що набули широкого поширення в задачах підвищення візуальної якості ЦЗ. Особливістю даних методів є декомпозиція зображення за критерієм максимізації відмінностей статистичних характеристик отримуваних компонентів (складових зображення). Це дозволяє формувати системи функцій для проведення декомпозиції ЦЗ за результатами аналізу тестового набору сигналів з використанням методу формування словників.

Одним з найбільш відомих методів компонентного аналізу зображень є метод головних компонентів (МГК) [144,226]. Даний метод заснований на декомпозиції ЦЗ на ортогональні складові за критерієм максимізації енергії (дисперсії) даних компонентів [226,227]:

$$\sum_{i=1}^m \|\mathbf{x}_i - L_k\|_2^2 \rightarrow \min, \quad (3.11)$$

де $\mathbf{x}_i \in \mathbb{R}^N, i \in [1; m]$ – i -тий елемент множини векторів; $L_k \subset \mathbb{R}^N$ – апроксимація набору векторів з використання гіперплощин; $d(\cdot, \cdot)^2$ – евклідова відстань.

Кожний компонент розкладу L_k у виразі (3.11) може бути представлений k -вимірним лінійним многовидом в просторі \mathbb{R}^N , а саме множиною лінійних комбінацій елементів $\{\mathbf{a}_0 \cdots \mathbf{a}_k\} \subset \mathbb{R}^N$ ортонормованого набору векторів – $L_k = \{\mathbf{a}_0 + \beta_1 \mathbf{a}_1 + \cdots + \beta_k \mathbf{a}_k | \beta_i \in \mathbb{R}\}$. Тоді вираз (3.11) можна представити у наступній формі:

$$\|\mathbf{x}_i - L_k\|_2^2 = \left\| \mathbf{x}_i - \mathbf{a}_0 - \sum_{j=1}^k \mathbf{a}_j \langle \mathbf{a}_j, \mathbf{x}_i - \mathbf{a}_0 \rangle \right\|_2^2, \quad k \in (0; n), \quad (3.12)$$

Розв'язок оптимізаційної задачі (3.22) може бути представлений набором вкладених многовидів $L_0 \subset L_1 \subset \dots \subset L_{n-1}$. Дані многовиди визначаються ортонормованим набором векторів (векторами головних компонентів) $\{\mathbf{a}_1, \dots, \mathbf{a}_{n-1}\}$ та вектором \mathbf{a}_0 . Кожен з векторів \mathbf{a}_i може бути знайдений як розв'язок задачі мінімізації для L_i з використанням узагальненого методу найменших квадратів:

$$\mathbf{a}_i = \operatorname{argmin}_{\mathbf{a}_i \in \mathbb{R}^N} \left(\sum_{j=1}^n \|\mathbf{x}_j - L_i\|_2^2 \right). \quad (3.13)$$

Тому задача пошуку головних компонентів (3.13) може бути зведена до еквівалентної задачі діагоналізації коваріаційної матриці матриці \mathbf{C} :

$$c_{ij} = \frac{1}{m-1} \sum_{l=1}^m (x_{li} - \bar{X}_i)(x_{lj} - \bar{X}_j),$$

де $\mathbf{X} = \{\mathbf{x}_1, \dots, \mathbf{x}_m\}^T$, $\mathbf{x}_i \in \mathbb{R}^N$ – матриця, сформована з векторів-рядків даних; \bar{X}_k – середнє значення елементів матриці \mathbf{X}_k . Тоді МГК відповідає спектральному розкладу коваріаційної матриці \mathbf{C} , а саме представлення матриці \mathbf{C} як лінійної комбінації ортогональних операторів проекції на взаємно ортогональні підпростори C_i з ваговими коефіцієнтами $\lambda_i \geq 0, i \in [1; m]$. Внаслідок цього задача спектрального розкладу емпіричної коваріаційної матриці матриці

$$\mathbf{C}_{\bar{\mathbf{X}}}^{cov} = \frac{1}{m-1} \mathbf{X}^T \mathbf{X} \quad (3.14)$$

є еквівалентною до задачі сингулярного розкладу матриці даних \mathbf{X} .

Вважатимемо, що число $\sigma \geq 0$ є сингулярним числом матриці \mathbf{X} тоді і тільки тоді, коли існують правий (m – вимірний вектор-рядок \mathbf{b}_σ) і лівий (n – вимірний вектор-стовпчик \mathbf{a}_σ) сингулярні вектори одиничної довжини, для яких виконуються наступні рівності:

$$\mathbf{X} \mathbf{a}_\sigma = \sigma \mathbf{b}_\sigma^T; \quad \mathbf{b}_\sigma \mathbf{X} = \sigma \mathbf{a}_\sigma^T.$$

Позначимо $p = \text{rank } \mathbf{X} \leq \min(n, m)$ – ранг матриці даних. Сингулярний розклад даної матриці може бути представлений у вигляді:

$$\mathbf{X} = \sum_{l=1}^p \sigma_l \mathbf{b}_l^T \mathbf{a}_l^T, \quad (3.15)$$

де $\sigma_l > 0$ – сингулярне число; $\mathbf{a}_l, \mathbf{b}_l$ – відповідно, правий та лівий сингулярні вектори. Праві сингулярні вектори, що беруть участь у даному розкладі, є векторами головних компонентів та власними векторами емпіричної коваріаційної матриці \mathbf{C}_X^{cov} (3.14), що відповідають додатнім власним числам $\lambda_l = \sigma_l^2 / (m - 1)$, $l \in [1; p]$.

Оскільки приховання повідомлень проводиться на рівні власних шумів зображення, що характеризуються малою енергією, в роботі досліджено вплив обробки ЦЗ з використанням МГК на відстань Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при видаленні компонентів зображення, що відповідають найменшим сингулярним числам σ_l . Для позначення частки сингулярних чисел розкладу ЦЗ (3.15), що лишилися без змін, використовувався параметр Δ_σ ($\Delta_\sigma \in [0; 100]$). Значення $\Delta_\sigma = 100\%$ відповідає випадку використання всіх компонентів зображення, в той час як при $\Delta_\sigma = 0\%$ вихідне зображення не відновлюється (отримується матриця, що складається з нільових елементів).

Залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу HUGO та використанні МГК для тестових зображень з пакету ALASKA наведені на рис. 3.27.

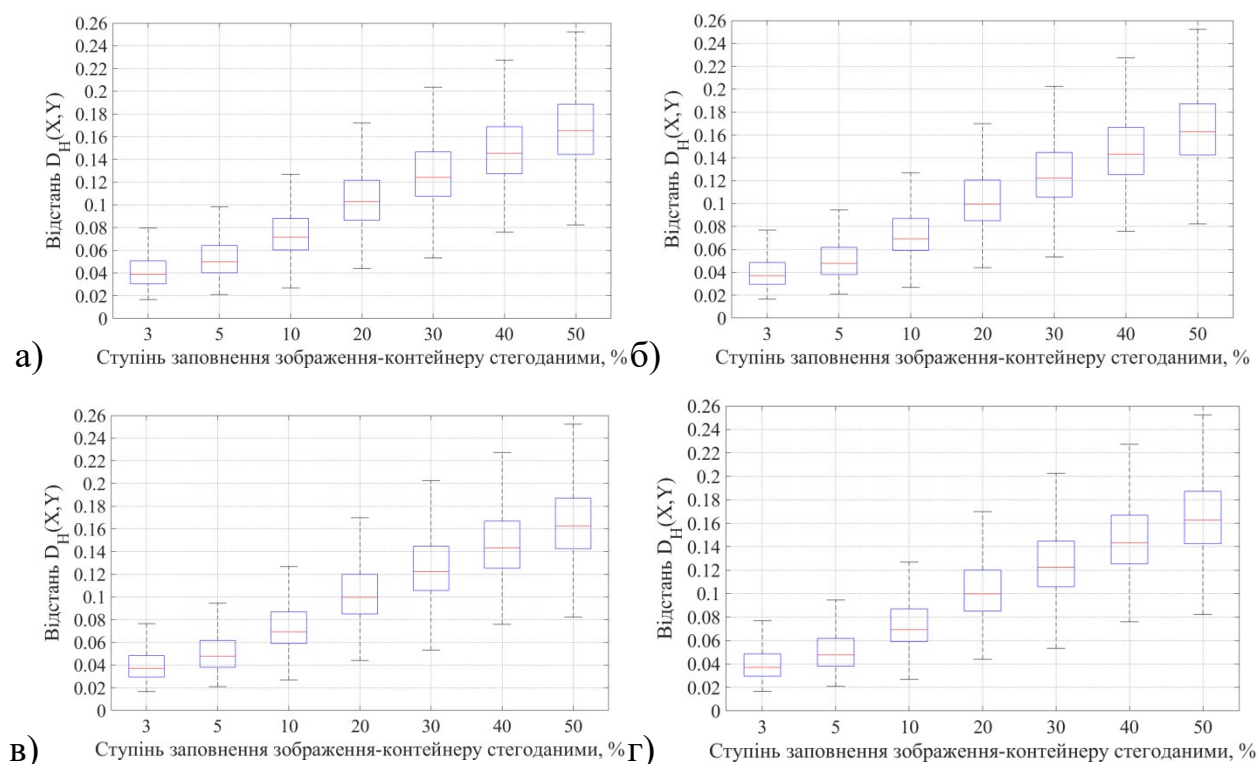


Рисунок 3.27 – Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу HUGO та використанні МГК: (а) – $\Delta\sigma = 90\%$; (б) – $\Delta\sigma = 95\%$; (в) – $\Delta\sigma = 97\%$; (г) – $\Delta\sigma = 99\%$.

Використання методу головних компонентів для попередньої обробки ЦЗ дозволяє підвищити значення відстань Хеллінгера D_H ($\Delta D_H = 7\%$) між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу HUGO (рис. 3.27). При цьому, найбільших змін зазнають значення D_H в області малого ($\Delta\alpha^S < 10\%$) та середнього ($10\% \leq \Delta\alpha^S \leq 20\%$) ступеня заповнення ЗК стегоданими. З іншого боку, варіація значення параметру $\Delta\sigma$ практично не впливає на зміни відстань Хеллінгера (рис. 3.27), що свідчить про вбудовування стегоданих в компоненти з найменшими значеннями сингулярних чисел σ_l – відповідні компоненти видаляються при проведенні реконструкції ЦЗ для обраного діапазону значень $\Delta\sigma$.

Для порівняння, на рис. 3.28 наведені залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм

при формуванні стеганограм згідно методу HUGO та використанні МГК для тестових зображень з пакету ALASKA.

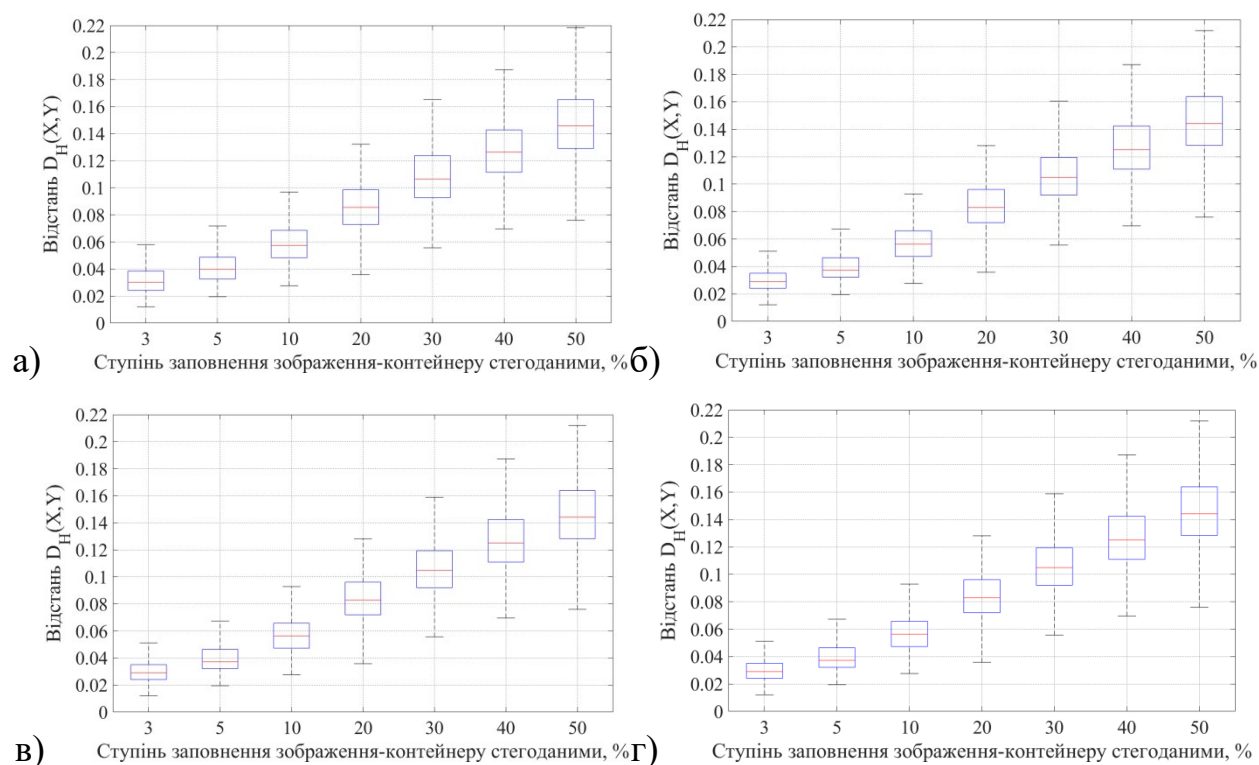


Рисунок 3.28 – Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу S-UNIWARD та використанні МГК: (а) – $\Delta_\sigma = 90\%$; (б) – $\Delta_\sigma = 95\%$; (в) – $\Delta_\sigma = 97\%$; (г) – $\Delta_\sigma = 99\%$.

Аналогічно до попереднього випадку (рис. 3.27), застосування МГК дозволяє збільшити значення D_H ($\Delta D_H = 5\%$) для стеганограм, сформованих згідно методу S-UNIWARD. Проте зростання значень D_H виявлено лише в області слабкого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$), та практично нівелюється при збільшенні значення параметру Δ_σ . Це свідчить, що приховання повідомлень згідно методу S-UNIWARD проводиться в компоненти ЗК, що характеризуються більшою енергією у порівнянні з випадком використання стеганографічного методу HUGO (рис. 3.28).

Враховуючи отримані результати, становить інтерес застосування МГК для попередньої обробки стеганограм, сформованих з використанням новітніх стеганографічних методів MG та MiPOD. Залежності значень відстані

Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу MG та використанні МГК для тестових зображень з пакету ALASKA наведені на рис. 3.29.

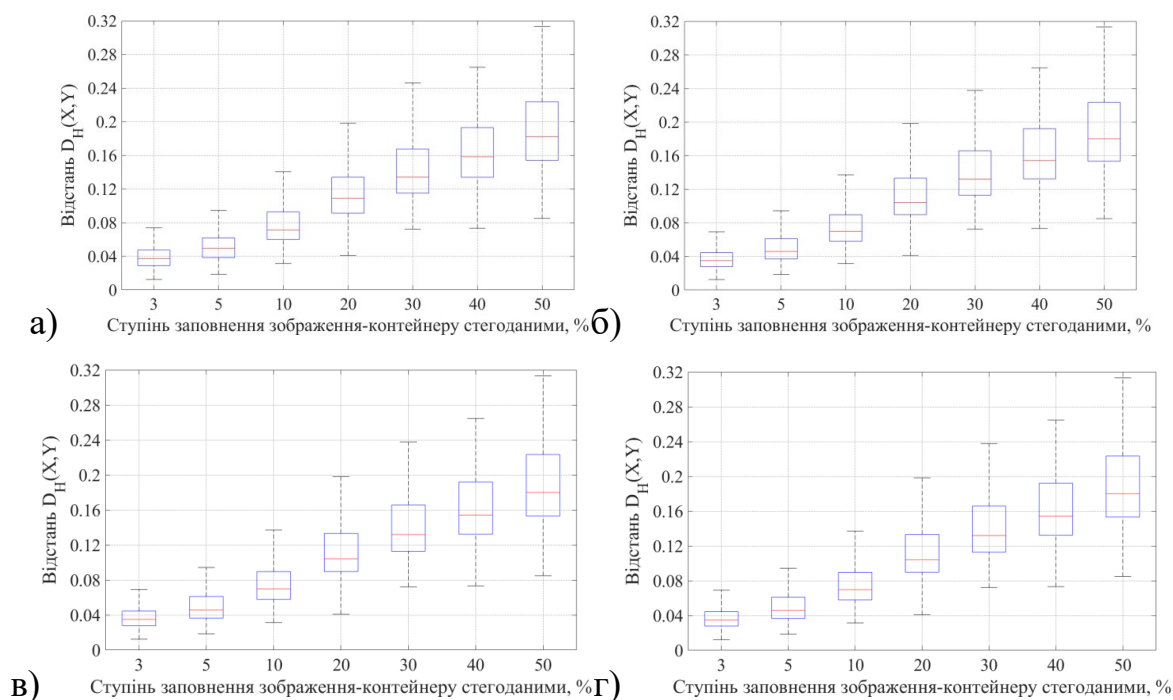


Рисунок 3.29 Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу MG та використанні МГК: (а) – $\Delta_\sigma = 90\%$; (б) – $\Delta_\sigma = 95\%$; (в) – $\Delta_\sigma = 97\%$; (г) – $\Delta_\sigma = 99\%$.

Відмітимо, що використання МГК призводить до незначних змін відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм, сформованих згідно методу MG (рис. 3.29) у порівнянні з випадком аналізу необроблених зображень (рис. 2.5). Це свідчить про обмежені можливості МГК щодо зниження впливу спотворень, обумовлених прихованням повідомлень згідно розглянутого АСМ.

Відповідні залежності значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу MiPOD та використанні МГК для тестових зображень з пакету ALASKA наведені на рис. 3.30.

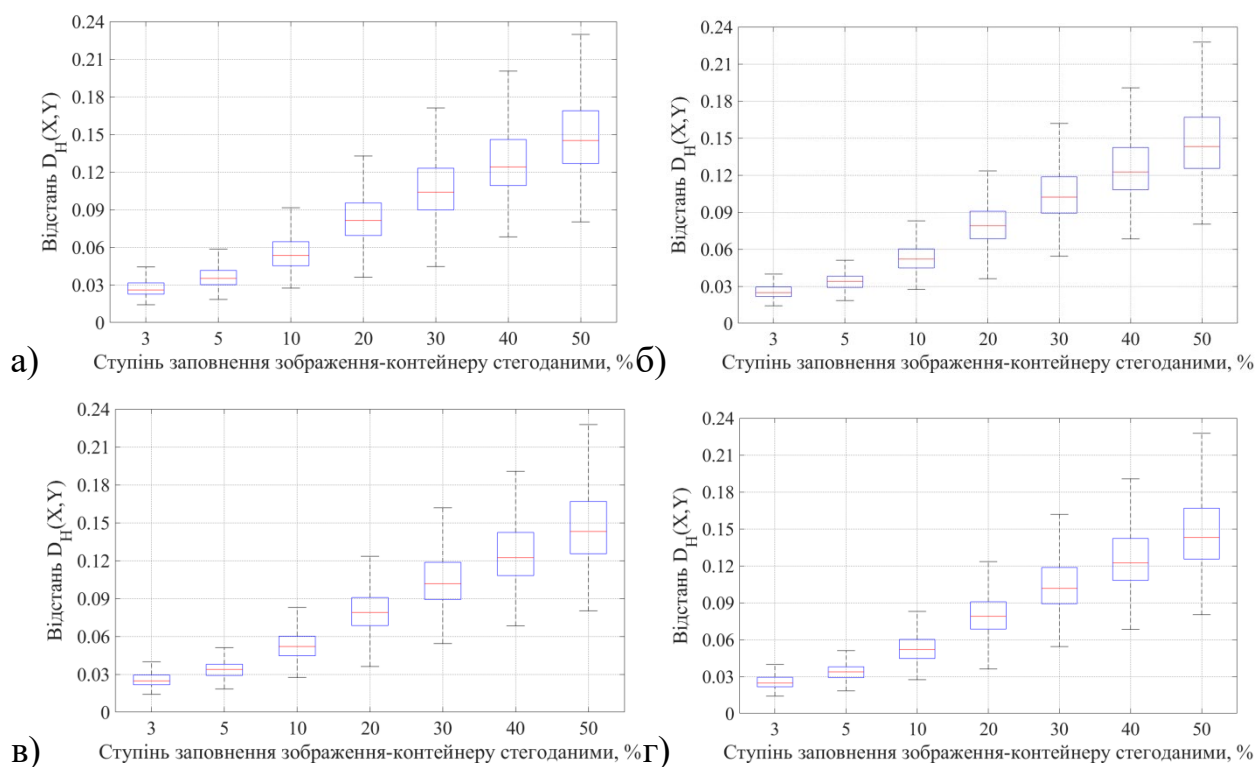


Рисунок 3.30 – Залежності середніх значень відстані Хеллінгера D_H між розподілами значень яскравості пікселів ЗК та стеганограм при формуванні стеганограм згідно методу MiPOD та використанні МГК: (а) – $\Delta_\sigma = 90\%$; (б) – $\Delta_\sigma = 95\%$; (в) – $\Delta_\sigma = 97\%$; (г) – $\Delta_\sigma = 99\%$.

Попередня обробка стеганограм, сформованих згідно методу MiPOD, із застосування МГК (рис. 3.30) практично не впливає на значення відстані Хеллінгера D_H у порівнянні з випадком обробки вихідних зображень (рис. 2.5). Це свідчить про використання набору з декількох компонентів ЗК при вбудовуванні стегоданих згідно даного АСМ, що знижує ефективність використання МГК оскільки потребує визначення даного набору компонентів ЗЦ для подальшого вилучення при проведенні попередньої обробки зображень.

Метод головних компонентів широко використовується в задачах знешумлення ЦЗ, оскільки не потребує апріорних даних щодо статистичних особливостей зображення [226,227]. При цьому шумам/завадам, внесеним до оброблюваного ЦЗ, будуть відповідати компоненти \mathbf{a}_i (3.13), що відповідають найменшим додатнім сингулярними числами. Це дозволяє використовувати прості порогові методи обробки сингулярних чисел для виокремлення

та придушення шумів, навіть в умовах обмеженості апріорних даних щодо їх статистичних характеристик. Враховуючи дані особливості МГК становить інтерес його використання в задачах попередньої обробки цифрових зображень при проведенні стегоаналізу.

3.2 Структура розробленого комплексу прикладних програм

Забезпечення високої точності виявлення стеганограм в умовах обмеженості апріорних даних щодо типу та параметрів СМ потребує використання УСД, або ж ансамблю з декількох СД, налаштованих для виявлення окремих типів СМ [11]. Сучасні УСД дозволяють забезпечити виску (більше 95%) точність виявлення стеганограм, сформованих згідно поширених СМ, проте точність роботи даних стегодетекторів суттєво знижується при використанні новітніх АСМ [56]. Тому становить інтерес практичне застосування розробленого методу побудови СД для підвищення ефективності сучасних систем виявлення та протидії витоку ІзОД при обміні повідомленнями в ІКС.

В роботі запропоновано програмний комплекс проведення стегоаналізу ЦЗ, заснований на використанні розроблених методів обробки ЦЗ. Зважаючи на відсутність необхідності використання апріорних даних щодо використаного СМ при вирішенні оптимізаційної задачі (2.11), для розробленого комплексу запропонована назва Blind-Steg. Основні етапи обробки зображень із застосуванням розробленого комплексу наведені на рис. 3.31.

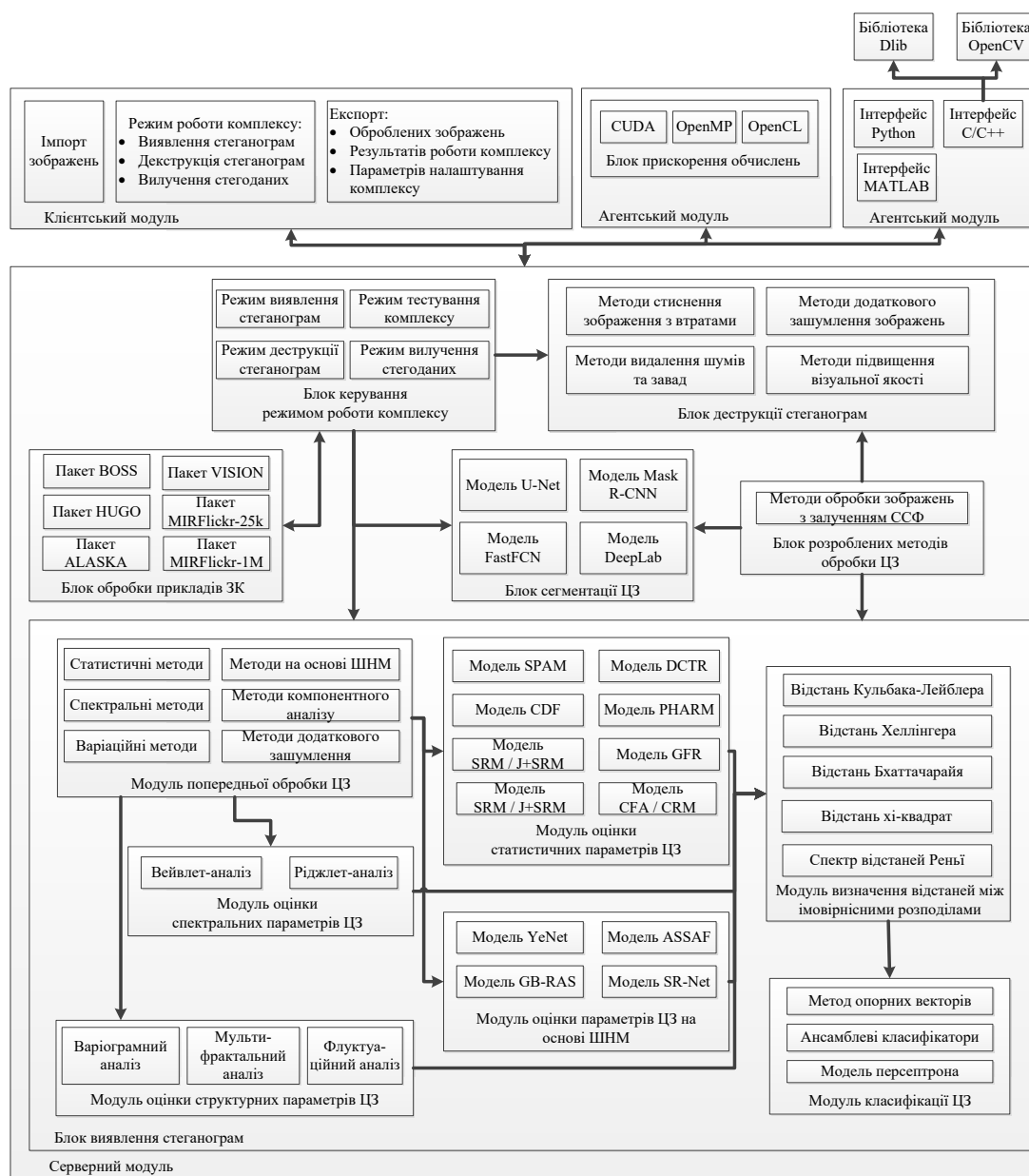


Рисунок 3.31 – Основні етапи обробки зображень з використанням розробленого комплексу проведення стегоаналізу цифрових зображень.

Комплекс Blind-Steg складається з декількох підсистем та баз даних, що використовуються при проведенні стегоаналізу ЦЗ (рис. 3.31):

1. Клієнтський модуль – забезпечує взаємодію з клієнтом, а саме імпорт цифрових зображень для проведення стегоаналізу, налаштування роботи комплексу та експорт оброблених ЦЗ після проведення декструкції або ж локалізації положення пікселів, використаних для приховання стегобітів;

2. Агентський модуль – використовується для взаємодії та інтеграції зі сторонніми системами, зокрема залучення методів прискорення обчислень (наприклад, з використанням програмних бібліотек CUDA, OpenCL);
3. Серверний модуль – використовується для реалізації основних функцій комплексу, а саме виявлення та деструкції стеганограм, визначення пікселів, використаних для приховання стегобітів. До складу даного модуля входять наступні блоки:
 - a. Блок виявлення стеганограм – використовується для детектування зображень, що імовірно містять приховані повідомлення. До складу даного блоку входять модулі проведення попередньої обробки досліджуваних зображень, обчислення статистичних, спектральних та структурних параметрів оброблених ЦЗ та класифікації зображень
 - b. Блок деструкції стеганограм – використовується для внесення незворотніх спотворень до ЦЗ з метою порушення роботи стеганографічного каналу зв'язку. Даний блок включає модулі деструкції прихованих повідомлень шляхом підвищення візуальної якості оброблюваних зображень, стиснення з втратами, видалення шумів та завад із зображення тощо;
 - c. Блок сегментації ЦЗ – спрямований на визначення позицій пікселів, що були використані для приховання окремих стегобітів. Блок проводить обробку ЦЗ після застосування запропонованого методу реконструкції вихідного виду ЗК, а також базу даних штучних нейронних мереж, що проводяться сегментацію зображення (а саме, розмітку пікселів як таких, що використовувалися в процесі формування стеганограм);
 - d. Блок керування режимом роботи комплексу – використовується для включення та налаштування параметрів підсистем комплексу Blind-Steg в залежності від обраного режиму роботи (наприклад, виявлення та деструкція стеганограм, вилучення стегоданих).

Відмітимо, що блок проведення попередньої обробки ЦЗ включає модуль посилення спотворень ЗК, внаслідок приховання повідомлень (рис. 3.31). Даний модуль заснований на використанні розглянутих методів повторного вбудовування стегоданих до ЦЗ згідно апріорно відомих СМ (дозволяють посилити відмінності між статистичними параметрами ЗК та стеганограм за рахунок підвищення енергії спотворень, обумовлених прихованням повідомлень) та внесення додаткових шумів до досліджуваного ЗК (спрямовані на посилення відмінностей між параметрами ЗК та стеганограм шляхом підвищення енергії спотворень, обумовлених вбудовування стегоданих). Дані методи, зазвичай, використовуються для виявлення відомих СМ, для котрих параметри внесених спотворень є апріорно відомими. В роботі досліджено випадок використання методів посилення спотворень ЗК, внаслідок приховання повідомлень, для виявлення невідомих стеганографічних методів, якому не приділено достатньо уваги в літературі. Встановлено обмеження практичного застосування методів посилення спотворень ЗК, обумовлені необхідністю підбору типу та параметрів внесених шумів для мінімізації значення помилки класифікації P_E (1.25).

Для обробки досліджуваних ЦЗ з використанням запропонованого комплексу також залучаються загальнодоступні (відкриті) програмні модулі. Дані модулі поширюються згідно дозвільної ліцензії (зокрема, ліцензій MIT, BSD та GNU GPL) для вільного використання при проведенні досліджень. Залучені програмні модулі використовуються у складі комплексу Blind-Steg для прискорення проведення обчислень (із застосуванням бібліотек CUDA, OpenMP, OpenCL, DLib, OpenCV), обчислення статистичних параметрів та подальшої сегментації оброблюваних зображень з використанням ШНМ (рис. 3.31).

Обробка ЦЗ з використанням розробленого комплексу проводиться в декілька етапів (рис. 3.31). На першому етапі проводиться попередня обробка зображень з метою визначення слабких спотворень ЗК, обумовлених прихованням повідомлень, та їх вилучення для подальшого аналізу. Розроблений

комплекс дозволяє обирати методи попередньої обробки ЦЗ в залежності від умов роботи СД (наприклад, у випадку наявності апріорних даних щодо особливостей використаного СМ), так і параметрів оброблюваних ЦЗ. Це досягається за рахунок налаштування відповідних параметрів блоку вибору режиму роботи комплексу.

На другому етапі роботи комплексу проводиться визначення статистичних, спектральних та структурних параметрів оброблених ЦЗ:

- Статистичні параметри ЦЗ – з використанням математичного марківських ланцюгів першого та другого порядку (розділ 1.3.2);
- Спектральні параметри ЦЗ – шляхом застосування багаторівневого ДДВП до оброблених ЦЗ, квантування отриманих коефіцієнтів розкладу з використанням методу Ллойда-Макса [244] та подальшого дослідження ступеня кореляції значень суміжних коефіцієнтів розкладу із застосуванням марківських ланцюгів другого порядку;
- Структурні параметри ЦЗ – ступеня кореляції між значеннями яскравості пікселів ЦЗ при варіації відстані між ними, фрактальних характеристик шумових складових зображення шляхом застосування методів варіограмного [245], флуктуаційного [160] та мультифрактального [146] аналізу цифрових зображень

Отримані статистичні, спектральні та структурні параметри ЗК зберігаються в базі даних прикладів параметрів зображень-контейнерів (рис. 3.31) та можуть бути використаними для подальшого налаштування СД.

На останньому етапі проводиться класифікація зображень за результатами порівняння отриманих статистичних, спектральних та структурних параметрів з відповідними параметрами для тестових ЗК, що наявні в базі даних параметрів ЦЗ (рис. 3.31). Порівняння параметрів проводиться з використанням методів бінарної класифікації багатовимірних векторів, зокрема класифікаторів на основі ансамблю лінійних дискримінантів Фішера (ЛДФ)

[144]. За результатами роботи класифікатора, досліджуване зображення відноситься до класу ЗК, або ж стеганограм.

Розроблений комплекс був реалізований програмно з використанням мови програмування Python 3.6 та інтегрованого комплексу розробки програмного забезпечення JetBrains PyCharm (Community Edition).

3.3 Порівняльний аналіз точності роботи стегодетекторів, синтезованих згідно сучасних та запропонованого методів

Для дослідження точності роботи високоточних СД, побудованих на основі запропонованої концепції, проведено порівняння точності їх роботи з сучасними стегодетекторами на основі комплексних статистичних моделей ЗК та ШНМ. Розглянуто як випадок виявлення стеганограм, сформованих згідно відомого стеганографічного методу, так і найбільш складні випадки проведення стегоаналізу апріорно невідомих АСМ.

3.3.1 Методика проведення дослідження

Дослідження точності виявлення стеганограм при використанні розглянутих методів попередньої обробки ЦЗ проводилося згідно стандартної CV-процедури [144]. Зокрема відбувалося розбиття пакету тестових ЦЗ псевдовипадковим чином на навчальну \mathcal{S}_{train} (70%) та контрольну \mathcal{S}_{test} (30%) вибірки. Вибірка зображень \mathcal{S}_{train} використовувалася для налаштування СД, в той час як аналіз точності його роботи проводиться на вибірці \mathcal{S}_{test} . Розбиття пакету тестових ЦЗ проводилося 10 разів для отримання усереднених значень показників якості роботи СД. Формування вибірок \mathcal{S}_{train} та \mathcal{S}_{test} проводилося з використанням стандартних пакетів зображень ALASKA (80,000 зображень) [134], VISION (11,700 зображень) [196] та MIRFlickr (близько 1 мільйона зображень) [197]. Аналогічно до проведених досліджень точності роботи сучасних СД (розділ 1.4.1), в роботі були використані псевдовипад-

кові вибірки з 10,000 зображень в градаціях сірого кольору однакового розміру (512×512 пікселів) для кожного пакету.

Формування стеганограм проводилося згідно новітніх стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153]. Ступінь заповнення ЗК стегоданими Δ_{α}^S варіювалася в наступних межах – від 3% до 5% з кроком 2%, від 5% до 10% з кроком 5 відсотків, та від 10% до 50% з кроком 10%.

Для оцінки статистичних параметрів досліджуваних зображень при використанні розглянутих та запропонованого методів попередньої обробки ЦЗ використовувалася статистична модель SPAM [38]. Відповідно, отримані значення параметрів моделі SPAM використовувалися для формування \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15) векторів.

В якості класифікатору у складі СД був використаний ансамблевий RF-класифікатор [202]. Налаштування класифікатору проводилося шляхом мінімізації помилки виявлення стеганограм P_E (1.25). При налаштуванні СД був розглянутий випадок обмеженості апріорних даних щодо використаного стеганографічного методу ($K_{\alpha}^{OL} = 0\%$), що відповідає найбільш складним випадкам проведення стегааналізу ЦЗ.

В якості показника роботи досліджуваних методів попередньої обробки ЦЗ використано похибка класифікації стеганограм P_E (1.24), що дозволяє порівнювати отримані результати з відповідними результатами роботи сучасних СД (розділ 1.4). Результати при використанні інших показників якості роботи СД наведені в додатках до роботи.

Дослідження проводилося з використанням сучасних стегадетекторів, запропонованих в роботах Кошкіної Н.В. [21,246,247] та Корольова В.Ю. [248]. Стегадетектор Кошкіної Н.В. заснований на повторному вбудовуванні (контрольному вкрапленні) до досліджуваного зображення тестової бітової послідовності (стегоданих) згідно відомого СМ (в роботі досліджено випадок використання стеганографічного методу HUGO). Метод виявлення стегано-

грам, запропонований Корольовим В.Ю., заснований на модифікації потужного RS-CA аналізу стеганограм, а саме дослідження змін статистичних характеристик ЦЗ при обробці його ковзним вікном різного розміру.

Попередня обробка ЗК та стеганограм проводилася згідно розглянутих (розділ 3.1) та запропонованого (розділ 2.3) методів. За результатами проведених автором досліджень [65,81-84,91,94] визначено оптимальні параметри розглянутих методів попередньої обробки ЦЗ за критерієм мінімізації значення похибки класифікації стеганограм P_E (1.24) для виявлення досліджуваних АСМ. Параметри даних методів, що використовувалися при проведенні дослідження наведені в табл. 3.3.

Таблиця 3.3 – Параметри досліджених типів методів попередньої обробки цифрових зображень.

№	Група методів попередньої обробки зображень	Параметри методу
1	Методи на основі повторного вбудовування повідомлень до ЦЗ	Повторне приховання повідомлень проводилося з використанням вихідного методу формування стеганограм. Ступінь заповнення ЗК стегаданними Δ_α^S обиралася псевдовипадковим чином з рівномірного імовірнісного розподілу $\mathcal{U}(5,50)$
2	Методи на основі додаткового зашумлення досліджуваних зображень	Проводилося додаткове зашумлення ЦЗ з використанням гаусового, пуасонового та фрактального шумів. Параметри шумів обиралася з використанням фільтру Вінера (оцінка енергії завад), ваговий параметр β_f обирався з рівномірного імовірнісного розподілу $\beta_f \in \mathcal{U}(0; 2)$.

Продовження табл. 3.3

№	Група методів попередньої обробки зображень	Параметри методу
3	Статистичні методи знешумлення цифрових зображень	Розмір ковзного вікна для білатеральної та NLM-фільтрації змінювався від $w_n = 3 \times 3$ до $w_n = 11 \times 11$ пікселів з кроком 2 пікселі. В якості функцій $h(k, n)$ та $g(\cdot)$ для білатеральної фільтрації (3.3) використовувалися функції Гауса з параметрами $\mu = 0$ і $\sigma = 1$.
4	Спектральні методи знешумлення цифрових зображень	Проводилася вейвлет-фільтрація ЦЗ з використанням вейвлету Хаара та відповідної йому скейлінг-функції в якості базису ДДВП. Розглянуто випадок багаторівневого перетворення при використанні п'яти рівнів декомпозиції ЦЗ. Порогові значення для коефіцієнтів ДДВП обиралися згідно виразів (3.4)-(3.6). Визначення порогових значень проводилося з використанням методу "scarceme";
5	Варіаційні методи знешумлення цифрових зображень	Знешумлення зображень з використанням TVM-методів Брегмана та Чамболлі.
6	Методи знешумлення цифрових зображень на основі штучних нейронних мереж	Знешумлення зображень з використанням ЗнАЕ, структура якого наведена на рис. 3.22. Налаштування ШНМ проводилося аналогічно до моделі ASSAF [127] при використанні вибірки з 10,000 зображень з пакету ALASKA.

Продовження табл. 3.3

№	Група методів попередньої обробки зображень	Параметри методу
7	Методи компонентного аналізу для знешумлення цифрових зображень	Зниження впливу спотворень ЦЗ, обумовлених прихованням повідомлень, проводилося з використанням МГК. При цьому Значення порогу змінювалися від 90% до 99% з кроком 1% щодо оцінки загальної енергії ЦЗ (3.15).
8	Запропонований метод попередньої обробки цифрових зображень	Формування надлишкового словника функцій \mathbf{A}_{SRR} для проведення декомпозиції ЦЗ. Налаштування словника \mathbf{A}_{SRR} проводилося з використання вибірки 10,000 зображень з пакету ALASKA, що не використовувався для формування стеганограм, при значеннях параметрів $N_{UC} = 512$, $w_{UC} = 32$

Дослідження точності роботи СД при використанні розглянутих та запропонованого методів попередньої обробки ЦЗ проводилося для наступних випадків:

1. Виявлення стеганограм, сформованих згідно апріорно відомого СМ – відповідає поширеному підходу до аналізу точності роботи СД, коли тип та параметри використаного СМ є апріорно відомими. В даному випадку СД може досягти точності виявлення стеганограм, близької до визначених меж досяжної точності (розділ 2.2) шляхом відповідного підбору параметрів.
2. Виявлення стеганограм в умовах обмеженості апріорних даних щодо використаного СМ – даний випадок відповідає ситуації, коли стегоаналітик вдосконалює метод виявлення стеганограм, сформованих згідно відомого стеганографічного методу, для роботи на нових ви-

бірках ЦЗ, статистичні параметри котрих відрізняються від використовуваного тестового пакету.

3. Виявлення стеганограм в умовах відсутності даних щодо типу та параметрів використаного СМ – дана ситуація відповідає випадку виявлення апріорно невідомих стеганографічних методів (проблема zero day). Забезпечення високої точності роботи СД в даному випадку становить особливий інтерес для підвищення ефективності роботи сучасних систем протидії витоку конфіденційних даних при обміні повідомленнями в ІКС.

Наведені випадки відповідають найбільш поширеним ситуаціям проведення стегааналізу ЦЗ в реальних системах захисту ІзОД. Результати дослідження точності роботи сучасних та запропонованого методів проведення попередньої обробки ЦЗ для даних випадків наведені в наступних розділах.

3.3.2 Аналіз точності роботи стегодетекторів при виявленні апріорно відомих стеганографічних методів

В даному розділі досліджено випадок формування стеганограм згідно сучасних стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153] для найбільш складного випадку проведення стегааналізу, а саме слабкого ступеня заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$). Результати наведено для випадку використання векторів \mathbf{F}_{DF} (2.18), що дозволяє мінімізувати значення помилки P_e у порівнянні з іншими типами параметрів ЦЗ (розділ 2.2). Отримані значення помилки класифікації стеганограм P_e при використанні СД, налаштованого з використанням поширених та запропонованого методів попередньої обробки стеганограм, для зображень з пакету ALASKA наведені в табл. 3.4.

Таблиця 3.4 – Значення помилки класифікації стеганограм P_e для СД, налаштованого із застосуванням поширених та запропонованого методів попередньої обробки зображень, для випадку використання \mathbf{F}_{DF} векторів при слабкому ступені заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$) та використанні зображень з пакету ALASKA.

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів				Середня тривалість роботи СД, сек
	HUGO	S-UNIWARD	MG	MiPOD	
Стегодетектор Кошкіної Н.В.	21.23	20.87	21.05	22.01	7.58
Стегодетектор Корольова В.Ю.	23.78	22.23	23.54	27.87	9.03
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру					
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_{\alpha}^S = 20\%$)	53.42	52.18	53.91	54.57	8.73
Додаткове зашумлення ЦЗ з використанням фрактального шуму	52.79	51.22	55.95	56.5	9.10

Продовження табл. 3.4

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів				Середня тривалість роботи СД, сек
	HUGO	S-UNIWARD	MG	MiPOD	
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними					
Знешумлення з використанням NLM-фільтрації	55.65	54.57	55.03	57.57	29.13
Вейвлет-фільтрація зображень	12.84	10.91	10.93	15.40	12.45
Знешумлення зображень з використанням TVM-методу Брегмана	48.67	43.87	50.75	52.77	17.51
Знешумлення зображень з використанням ЗНАЕ	47.74	42.31	48.39	51.22	27.07
Застосування МГК	45.65	39.55	48.17	50.12	24.00
<u>Комплекс Blind-Steg</u>	<u>10.70</u>	<u>8.60</u>	<u>9.03</u>	<u>11.18</u>	<u>8.24</u>

Відмітимо, що використання методів вейвлет-фільтрації дозволяє суттєво зменшити значення помилки P_e у порівнянні з поширеними типами МПО (табл. 3.4). Це може бути пояснено ефективністю застосування даного методу обробки для зниження впливу локальних збурень значень яскравості

пікселів ЗК, обумовлених прихованням повідомлень. Використання запропонованого методу дозволяє додатково зменшити значення помилки класифікації стеганограм P_e ($\Delta P_e \cong 2\%$) у порівнянні з випадком використання методів вейвлет-фільтрації (табл. 3.4). При цьому отримані значення помилки P_e є близькими до отриманих раніше оцінок досяжної точності роботи СД (розділ 2.2). Також перевагою запропонованого методу є суттєве (до трьох разів) зменшення тривалості обробки ЦЗ (з 27.07 секунд до 8.24) у порівнянні з дослідженими МПО.

Отримані результати (табл. 3.4) підтверджують високу ефективність використання запропонованого підходу для підвищення точності виявлення стеганограм, сформованих з використанням стандартного пакету зображень ALASKA, що широко використовується для порівняння точності роботи сучасних СД [134]. Зазначимо, що особливістю даного пакету ЦЗ є низький рівень власних шумів ЦЗ (розділ 1.3), що дещо спрощує виявлення стеганограм у порівнянні з випадком використання реальних ЦЗ, які характеризуються значною варіативністю даних показників. Тому становить інтерес дослідження точності виявлення стеганограм при використанні пакетів реальних ЦЗ, зокрема VISION та MIRFlickr. Отримані значення помилки класифікації стеганограм P_e при використанні СД, налаштованого з використанням поширених та запропонованого методів попередньої обробки стеганограм, для зображень з пакету VISION наведені в табл. 3.5.

Таблиця 3.5 – Значення помилки класифікації стеганограм P_e для СД, налаштованого із застосуванням поширених та запропонованого методів попередньої обробки зображень, для випадку використання \mathbf{F}_{DF} векторів при слабкому ступені заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$) та використанні зображень з пакету VISION.

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів				Середня тривалість роботи СД, сек
	HUGO	S-UNIWARD	MG	MiPOD	
Стегодетектор Кошкіної Н.В.	33.08	32.11	32.29	25.06	6.99
Стегодетектор Корольова В.Ю.	46.08	41.72	45.10	48.42	9.37
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру					
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_{\alpha}^S = 20\%$)	57.27	55.69	57.04	58.62	8.11
Додаткове зашумлення ЦЗ з використанням фрактального шуму	56.09	56.71	57.82	55.35	9.84

Продовження табл. 3.5

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів				Середня тривалість роботи СД, сек
	HUGO	S-UNIWARD	MG	MiPOD	
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними					
Знешумлення з використанням NLM-фільтрації	54.69	52.48	54.31	56.71	28.99
Вейвлет-фільтрація зображень	25.95	19.02	23.03	27.44	12.63
Знешумлення зображень з використанням TVM-методу Брегмана	56.43	57.87	56.38	57.16	17.81
Знешумлення зображень з використанням ЗНАЕ	53.76	51.55	54.79	56.52	26.73
Застосування МГК	55.18	53.69	56.48	56.98	25.16
<u>Комплекс Blind-Steg</u>	<u>12.44</u>	<u>10.56</u>	<u>11.64</u>	<u>13.63</u>	<u>9.48</u>

Відмітимо, що значення помилки P_e для пакету VISION (табл. 3.5) є меншими у порівнянні з випадком використання стандартного тестового пакету ALASKA (табл. 3.4). Зміна значень P_e сягає до 10% для досліджених методів попередньої обробки ЦЗ та обумовлена високою ефективністю вико-

ристання розглянутих методів попередньої обробки ЦЗ для зниження впливу власних шумів досліджуваних зображень [196].

Використання запропонованого методу, як і в попередньому випадку (табл. 3.4), дозволяє суттєво підвищити точність роботи СД у порівнянні з сучасними методів попередньої обробки. Для порівняння, в табл. 3.6 наведені значення помилки класифікації стеганограм P_e при використанні СД, налаштованого з використанням поширених та запропонованого методів попередньої обробки стеганограм, для ЦЗ з пакету MIRFlickr.

Таблиця 3.6 – Значення помилки класифікації стеганограм P_e для СД, налаштованого із застосуванням поширених та запропонованого методів попередньої обробки зображень, для випадку використання \mathbf{F}_{DF} векторів при слабкому ступені заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$) та використанні зображень з пакету MIRFlickr.

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів				Середня тривалість роботи СД, сек
	HUGO	S-UNIWARD	MG	MiPOD	
Стегодетектор Кошкіної Н.В.	27.15	25.26	27.03	28.95	7.03
Стегодетектор Корольова В.Ю.	32.19	31.04	33.68	34.12	8.95

Продовження табл. 3.6

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів				Середня тривалість роботи СД, сек
	HUGO	S-UNIWARD	MG	MiPOD	
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру					
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_\alpha^S = 20\%$)	57.65	55.55	56.17	56.12	8.45
Додаткове зашумлення ЦЗ з використанням фрактального шуму	56.18	53.03	54.60	56.70	10.07
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними					
Знешумлення з використанням NLM-фільтрації	57.27	55.69	56.04	57.62	32.12
Вейвлет-фільтрація зображень	15.35	12.82	14.71	14.09	15.74

Продовження табл. 3.6

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів				Середня тривалість роботи СД, сек
	HUGO	S-UNIWARD	MG	MiPOD	
Знешумлення зображень з використанням TVM-методу Брегмана	56.69	55.48	55.31	57.71	16.27
Знешумлення зображень з використанням ЗНАЕ	48.44	44.03	45.02	47.95	29.33
Застосування МГК	52.43	50.87	53.38	50.16	27.68
<u>Комплекс Blind-Steg</u>	<u>11.52</u>	<u>9.79</u>	<u>12.55</u>	<u>11.76</u>	<u>11.31</u>

Пакет зображень MIRFlickr сформований з використанням ЦЗ, що циркулюють в мережі обміну цифровими зображеннями Flickr [197]. Внаслідок цього дані зображення характеризуються значним діапазоном зміни статистичних та спектральних параметрів, що ускладнює налаштування СД у порівнянні з розглянутими пакетами ALASKA (табл. 3.4) та VISION (табл. 3.5). Це призводить до незначного підвищення значень P_e (табл. 3.6) у порівнянні з отриманими раніше результатами (табл. 3.4-3.5) для сучасних методів попередньої обробки ЦЗ.

Відмітимо, що запропонований метод дозволяє суттєво підвищити точність роботи СД у порівнянні з розглянутими методами (табл. 3.6). Це свідчить про високу ефективність використання даного методу у випадках, коли стегоаналітик проводиться оптимізацію параметрів СД для мінімізації значе-

ння помилки класифікації ЦЗ для відомого АСМ. Проте в більшості практичних випадків апріорні дані щодо типу та параметрів використаного АСМ є обмеженими, тому становить інтерес дослідження точності роботи СД для даних випадках.

3.3.3 Аналіз точності роботи стегодетекторів при обмеженості апріорних даних щодо використаного стеганографічного методу

Особливий інтерес при проведенні стегоаналізу ЦЗ становить випадок використання попередньо налаштованих СД для роботи на нових пакетах ЦЗ (проблема domain adaptation). Даний випадок відповідає поширеній ситуації, коли статистичні та спектральні параметри оброблюваних зображень суттєво відрізняються від відповідних параметрів для пакету ЦЗ, використаного для налаштування СД. При цьому швидке переналаштування СД для роботи на нових пакетах ЦЗ є неможливим, наприклад через високу обчислювальну складність.

Аналіз точності роботи СД проводилося при використанні СД, попередньо налаштованих з застосуванням стандартного пакету ALASKA [134]. Дані стегодетектори застосовувалися для виявлення стеганограм, сформованих з використанням ЦЗ з пакетів VISION [196] та MIRFlickr [197]. Отримані значення помилки класифікації стеганограм P_e при використанні СД, налаштованого з використанням поширених та запропонованого МПО, для зображень з пакету VISION наведені в табл. 3.7.

Таблиця 3.7 – Значення помилки класифікації стеганограм P_e для СД, налаштованого із застосуванням поширених та запропонованого методів попередньої обробки зображень, для випадку використання \mathbf{F}_{DF} векторів при слабкому ступені заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$). Розглянуто випадок налаштування СД з застосуванням стандартного пакету ALASKA [134], та подальшого тестування на зображеннях з пакету VISION.

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			
	HUGO	S-UNIWARD	MG	MiPOD
Стегодетектор Кошкіної Н.В.	31.53	37.31	50.08	56.65
Стегодетектор Корольова В.Ю.	52.17	43.28	51.52	54.49
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру				
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_{\alpha}^S = 20\%$)	52.81	53.69	50.43	48.24
Додаткове зашумлення ЦЗ з використанням фрактального шуму	51.63	52.64	50.56	53.44
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними				
Знешумлення з використанням NLM-фільтрації	32.11	28.06	51.52	53.99
Вейвлет-фільтрація зображень	17.97	16.85	16.60	20.27
Знешумлення зображень з використанням TVM-методу Брегмана	45.65	41.68	46.16	48.26
Знешумлення зображень з використанням ЗнАЕ	40.84	37.09	43.90	45.11

Продовження табл.3.7

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			
	HUGO	S-UNIWARD	MG	MiPOD
Застосування МГК	47.83	45.66	42.17	38.35
<u>Комплекс Blind-Steg</u>	<u>15.38</u>	<u>11.04</u>	<u>13.53</u>	<u>15.58</u>

Застосування СД, налаштованого з використанням пакету ALASKA, для обробки ЦЗ з пакету VISION призводить до суттєвого підвищення значень помилки P_e (табл. 3.7) у порівнянні з розглянутим раніше випадком налаштування та тестування стегодетектору на однаковому пакеті ЦЗ (табл. 3.5). Це свідчить про обмеження сучасних методів попередньої обробки, а саме необхідності повторного налаштування даних методів, зокрема визначення оптимальних параметрів для мінімізації помилки виявлення стеганограм P_e .

Застосування запропонованого методу дозволяє ефективно протидіяти даному негативному ефекту за рахунок несуттєвих змін коефіцієнтів розкладу ЗК при використанні надлишкових систем функцій для розглянутих пакетів ЦЗ. Для порівняння, в табл. 3.8 наведені значення помилки класифікації стеганограм P_e при використанні СД, налаштованого з використанням поширених та запропонованого методів попередньої обробки стеганограм, для зображень з пакету MIRFlickr.

Таблиця 3.8 – Значення помилки класифікації стеганограм P_e для СД, налаштованого із застосуванням поширених та запропонованого методів попередньої обробки ЦЗ, для випадку використання \mathbf{F}_{DF} векторів при слабкому ступені заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$). Розглянуто випадок налаштування стегодетекторів з застосуванням стандартного пакету ALASKA [134], та подальшого тестування на зображеннях з пакету MIRFlickr.

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			
	HUGO	S-UNIWARD	MG	MiPOD
Стегодетектор Кошкіної Н.В.	34.11	31.98	32.07	33.39
Стегодетектор Корольова В.Ю.	46.27	41.85	43.48	45.04
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру				
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_{\alpha}^S = 20\%$)	56.81	56.47	55.90	55.58
Додаткове зашумлення ЦЗ з використанням фрактального шуму	55.12	55.70	57.91	56.34
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними				
Знешумлення з використанням NLM-фільтрації	58.63	57.24	57.09	58.75
Вейвлет-фільтрація зображень	21.27	30.85	20.54	22.69
Знешумлення зображень з використанням TVM-методу Брегмана	55.95	54.75	56.96	57.49
Знешумлення зображень з використанням ЗнАЕ	52.15	50.76	53.97	55.06
Застосування МГК	54.95	52.72	55.48	57.54

Продовження табл. 3.8

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			
	HUGO	S-UNIWARD	MG	MiPOD
<u>Комплекс Blind-Steg</u>	<u>13.80</u>	<u>10.03</u>	<u>11.14</u>	<u>12.19</u>

Отримані результати (табл. 3.8) підтверджують високу ефективність використання запропонованого методу проведення попередньої обробки ЦЗ. Зокрема досягнуто суттєвого зниження значень помилки P_e ($\Delta P_e \cong 40\%$) у порівнянні з поширеними МПО, зокрема у найбільш складному випадку слабкого заповнення ЗК стегоданими ($\Delta \alpha^S = 5\%$). Таким чином, запропонований метод синтезу СД дозволяє забезпечити високу точність виявлення стеганограм навіть у випадку обробки пакетів ЦЗ, статистичні та спектральні параметри котрих суттєво відрізняються від відповідних параметрів ЦЗ з δ_{train} вибірки ЦЗ. Це дозволяє використовувати попередньо налаштовані СД для обробки нових вибірок ЦЗ без необхідності їх повторного налаштування.

Враховуючи отримані результати становить інтерес дослідження ефективності використання запропонованого методу у найбільш складному випадку проведення стегоаналізу ЦЗ, а саме виявлення стеганограм, сформованих згідно апріорно невідомих стеганографічних методів.

3.3.4 Аналіз точності роботи стегодетекторів при відсутності апріорних даних щодо використаного стеганографічного методу

Дослідження проводилося для випадку використання СД, налаштованого з використання методів HUGO, S-UNIWARD, MG та MiPOD на пакеті зображень ALASKA, та подальшого тестування на пакеті стеганограм, сформованих згідно новітніх методів Synch [132], UED [249] та HILL [250]. Для наближення умов дослідження точності роботи СД до реальних випадків, тестування СД проводилося на вибірках з 10,000 зображень з пакетів зобра-

жень RAISE [251] та Google Open Image [252], що не використовувалися в попередніх дослідженнях.

Пакет RAISE сформований з використанням ЦЗ, що були підготовлені за результатами професійної обробки вихідних даних з DSLR-камер. Внаслідок цього тестові зображення з даного методу характеризуються низьким рівнем власних шумів. Пакет Google Open Image [252] був сформований за результатами обробки реальних ЦЗ, що індексуються у відкритих (публічних) системах обміну мультимедійними даними, зокрема системою Google. Особливістю даних зображень є висока варіативність їх розмірів, а також спектральних та статистичних параметрів.

Дослідження точності роботи попередньо налаштованих СД проводилося з використанням новітніх стеганографічних методів Synch [132], UED [249] та HILL [250]. Особливістю даних АСМ є використання декількох функцій (1.2) для оцінки рівня спотворень ЗК при формуванні стеганограм, що дозволяє суттєво зменшити рівень демаскуючих ознак у порівнянні з розглянутими раніше СМ. Приховання повідомлень згідно наведених СМ проводиться шляхом «синхронізації» змін яскравості декількох груп пікселів (розділ 1.2.2), що дозволяє додатково зменшити рівень демаскуючих ознак сформованих стеганограм.

Отримані значення помилки класифікації стеганограм P_e при використанні СД, налаштованого з використанням поширених та запропонованого методів попередньої обробки стеганограм, для зображень з пакету RAISE [251] наведені в табл. 3.9.

Таблиця 3.9 – Значення помилки класифікації стеганограм P_e для СД, налаштованого із застосуванням поширених та запропонованого методів попередньої обробки зображень, для випадку використання \mathbf{F}_{DF} векторів при слабкому ступені заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$). Розглянуто випадок налаштування СД з застосуванням стандартного пакету ALASKA [134] та стеганографічного методу MiPOD, та подальшого тестування на зображеннях з пакету RAISE.

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			Середня тривалість роботи СД, сек
	Synch	UED	HILL	
Стегодетектор Кошкіної Н.В.	50.03	49.11	52.01	8.12
Стегодетектор Корольова В.Ю.	53.42	51.08	52.99	10.33
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру				
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_{\alpha}^S = 20\%$)	57.75	55.13	55.25	9.77
Додаткове зашумлення ЦЗ з використанням фрактального шуму	55.60	53.50	52.51	13.98

Продовження табл. 3.9

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			Середня тривалість роботи СД, сек
	Synch	UED	HILL	
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними				
Знешумлення з використанням NLM-фільтрації	58.69	54.91	53.89	42.54
Вейвлет-фільтрація зображень	52.93	50.95	54.09	17.95
Знешумлення зображень з використанням TVM-методу Брегмана	54.54	52.72	53.13	19.93
Знешумлення зображень з використанням ЗНАЕ	53.93	50.14	51.86	48.35
Застосування МГК	47.25	48.75	45.84	32.14
<u>Комплекс Blind-Steg</u>	<u>17.43</u>	<u>14.25</u>	<u>16.07</u>	<u>15.59</u>

Відмітимо, що використання поширених методів попередньої обробки ЦЗ в призводить до суттєвого зростання значень помилки P_e (табл. 3.9) у порівнянні з розглянутими раніше випадками (табл. 3.4-3.7). При цьому дані

методи не дозволяють забезпечити відносно малі значення помилки P_e для розглянутих стеганографічних методів Synch [132], UED [249] та HILL [250].

Використання запропонованого методу попередньої обробки дозволяє суттєво (до трьох разів, табл. 3.9) зменшити значення P_e у порівнянні з поширеними типа МПО. Для порівняння, в табл. 3.10 наведені значення помилки класифікації стеганограм P_e при використанні СД, налаштованого з використанням поширених та запропонованого методів попередньої обробки стеганограм, для зображень з пакету Google Open Image [252].

Таблиця 3.10 – Значення помилки класифікації стеганограм P_e для СД, налаштованого із застосуванням поширених та запропонованого методів попередньої обробки зображень, для випадку використання \mathbf{F}_{DF} векторів при слабкому ступені заповнення ЗК стегоданими ($\Delta_\alpha^S = 5\%$). Розглянуто випадок налаштування СД з застосуванням стандартного пакету ALASKA [134] та стеганографічного методу MiPOD, та подальшого тестування на зображеннях з пакету Google Open Image.

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			Середня тривалість роботи СД, сек
	Synch	UED	HILL	
Стегодетектор Кошкіної Н.В.	53.11	49.92	50.34	9.01
Стегодетектор Корольова В.Ю.	55.65	55.03	57.57	9.78

Продовження табл. 3.10

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			Середня тривалість роботи СД, сек
	Synch	UED	HILL	
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру				
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_\alpha^S = 20\%$)	54.18	54.48	55.98	9.24
Додаткове зашумлення ЦЗ з використанням фрактального шуму	51.93	47.92	45.35	12.57
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними				
Знешумлення з використанням NLM-фільтрації	49.35	48.00	46.19	45.13
Вейвлет-фільтрація зображень	48.11	47.25	50.66	18.02

Продовження табл. 3.10

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_e при використанні стеганографічних методів			Середня тривалість роботи СД, сек
	Synch	UED	HILL	
Знешумлення зображень з використанням TVM-методу Брегмана	50.61	46.60	49.47	20.15
Знешумлення зображень з використанням ЗнАЕ	43.08	40.78	39.33	43.18
Застосування МГК	47.95	48.34	50.04	30.48
<u>Комплекс Blind-Steg</u>	<u>14.58</u>	<u>12.53</u>	<u>12.54</u>	<u>13.21</u>

Як і для попередніх випадків (табл. 3.9), застосування запропонованого методу попередньої обробки ЦЗ дозволяє суттєво зменшити значення помилки класифікації стеганограм P_e , сформованих згідно апріорно невідомих АСМ, у порівнянні з випадком використання поширених методів обробки цифрових зображень (рис. 3.10).

Таким чином, можемо зробити висновок, що використання запропонованого методу дозволяє забезпечити високу точність роботи СД навіть в умовах обробки стеганограм, сформованих згідно апріорно невідомих СМ, та зображень-контейнерів, статистичні та спектральні параметри котрих суттєво відрізняються від відповідних параметрів для навчальної вибірки ЦЗ.

3.4 Висновки за розділом 3

За результатами порівняльного аналізу точності роботи СД при використанні поширених та запропонованого методів попередньої обробки ЦЗ для виявлення стеганограм в умовах обмеженості апріорних даних щодо використаного СМ та значної варіативності статистичних параметрів ЗК отримані наступні результати:

1. Показано, що використання запропонованого методу попередньої обробки ЦЗ дозволяє підвищити точність роботи стегадетекторів на 7% при обробці стеганограм, сформованих з використанням стандартних пакетів зображень. При цьому висока точність роботи СД зберігається навіть у випадку обробки ЦЗ, які характеризуються значною варіативністю статистичних параметрів, що становить особливий практичний інтерес в задачах стегааналізу цифрових зображень.

2. Встановлено, що точність роботи поширених методів попередньої обробки ЦЗ суттєво зменшується у випадку обробки зображень, статистичні та спектральні параметри котрих суттєво відрізняються від відповідних параметрів зображень, використаних для налаштування СД. При цьому використання запропонованого методу дозволяє забезпечити малі значення помилки виявлення стеганограм P_e навіть у випадку обробки зображень, що характеризуються високим рівнем власних шумів, для яких точність роботи сучасних СД суттєво знижується.

3. Виявлено, що застосування запропонованого підходу дозволяє суттєво (на 40%) підвищити точність роботи СД навіть у найбільш складному випадку виявлення стеганограм в умовах відсутності апріорних даних щодо використаного СМ. Запропонований метод дозволяє до трьох разів зменшити значення помилки виявлення стеганограм P_e у порівнянні з випадком використання сучасних методів попередньої обробки ЦЗ. Отримані результати дозволяють суттєво зменшити негативний вплив проблем zero-day на точ-

ність виявлення стеганогам, що становить особливий теоретичний та практичний інтерес в галузі стегоаналізу цифрових зображень.

РОЗДІЛ 4 АНАЛІЗ ПЕРСПЕКТИВ ВИКОРИСТАННЯ ЗАПРОПОНОВАНОГО ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ПРОВЕДЕННЯ СТЕГОАНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ

Результати порівняльного аналізу досліджуваних методів попередньої обробки ЦЗ підтвердили ефективність використання запропонованого методу для забезпечення високої точності роботи СД. Відмітимо, що запропонований метод дозволяє суттєво (на 40%) підвищити точність роботи СД навіть у випадку обмеженості апріорних даних щодо використаного СМ, що становить особливий інтерес при проведенні стегоаналізу ЦЗ.

При цьому даний метод попередньої обробки ЦЗ дозволяє суттєво підвищити точність оцінки статистичних параметрів ЗК за наявними (зашумленими) зображеннями шляхом зниження впливу спотворень, обумовлених прихованням повідомлень. Дана особливість становить інтерес в задачах вилучення (деструкції) стеганограм, зокрема визначення позицій пікселів, використаних для приховання стегобітів. Подальша обробка даних пікселів може бути спрямована на оцінку значень бітів стегоданих, що становить інтерес для новітніх методів вилучення/підміни прихованих повідомлень.

Тому становить інтерес дослідження перспектив використання запропонованого програмного комплексу для вирішення найбільш складних задачах стегоаналізу ЦЗ, а саме надійної деструкції даних, а також визначення шляхів вирішення задачі екстракції стегоданих.

4.1 Дослідження ефективності використання комплексу для вирішення задач стегоаналізу цифрових зображень

Дослідження ефективності роботи запропонованого комплексу стегоаналізу ЦЗ (рис. 3.31) проведено для стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD, а також новітнього методу Synch [132]. Аналіз проводився з використанням пакету зображень ALASKA [134] (вибірка з 10,000 зображень) згідно стандартної CV-процедури при псевдовипадковому

розбитті вибірки тестових ЦЗ на навчальну (70%) та контрольну (30%) вибірки 10 разів.

Стеганографічний метод Synch [132] відноситься до групи методів з синхронізацією змін яскравості пікселів (розділ 1.2.2). Особливістю даного методу є забезпечення однакових (синхронних) змін значень яскравості близьких пікселів ЗК, обраних для приховання стегобітів. Це дозволяє додатково зменшити зміни статистичних параметрів ЗК при формуванні стеганограм та, відповідно, підвищити стійкість до сучасних методів стегоаналізу ЦЗ.

Дослідження ефективності роботи розробленого комплексу Blind-Steg проводилося для наступних випадків – вилучення (деструкція) прихованих повідомлень (стеганограм), а також оцінка позицій пікселів ЗК, використаних для приховання окремих стегобітів. Перша задача відповідає випадку превентивної обробки ЦЗ для протидії витоку ІзОД при передачі даних в ІКС, коли точність роботи використовуваних СД є недостатньою для надійного виявлення стеганограм. Вирішення другої задачі становить особливий інтерес для вирішення завдань щодо вилучення або підміни бітів приховуваного повідомлення без необхідності деструкції стеганограми загалом.

4.1.1 Оцінка ступеня деструкції стеганограм при використанні запропонованого методу попередньої обробки цифрових зображень

Сучасні методи деструкції спрямовані на вилучення виявлених стеганограм з повідомлень, або ж вилучення шумових компонентів ЗК на рівні котрих проводиться приховання повідомлень [13]. Це призводить до суттєвих змін статистичних та спектральних параметрів ЦЗ, що може бути виявлено зловмисниками при дослідженні отриманих стеганограм та, відповідно, розкрити втручання в стеганографічний канал передачі даних. Для протидії даному втручання, зловмисники можуть змінити як тип файлу-контейнеру (наприклад, використання текстових даних замість ЗК), так і параметрів ССЗ, що потребуватиме повторного налаштування СД для виявлення стеганограм. Тому становить інтерес розробка методів деструкції стеганограм, що дозво-

ляють забезпечити надійну деструкцію прихованих повідомлень без внесення суттєвих змін в статистичні характеристик ЦЗ.

Відмітимо, що вагомою перевагою запропонованого методу попередньої обробки ЦЗ є суттєве зниження впливу спотворень досліджуваного зображення, обумовлених прихованням повідомлень до ЗК, навіть в умовах обмеженості апріорних даних щодо використаного стеганографічного методу. Тому становить інтерес дослідження ефективності використання запропонованого методу обробки ЦЗ для проведення деструкції стеганограм.

Для вирішення даної задачі в роботі досліджено зміни параметрів стеганограм при використанні поширених та запропонованого методів попередньої обробки ЦЗ:

- Статистичні параметри – обчислювалися з використання статистичної моделі SPAM [38] для оцінки ступеня кореляції значень яскравості суміжних пікселів ЦЗ;
- Спектральні параметри – обчислювалися шляхом порівняння коефіцієнтів $W_{uv}^{(k)}$ однорівневого ДДВП вихідної та обробленої стеганограми при використанні вейвлету Хаара та відповідної йому скейлінг-функції в якості базисних функцій перетворення;
- Структурні параметри – обчислювалися шляхом порівняння спектру Реньї D_R та мультифрактального спектру $f(\alpha)$ вихідного та обробленого ЦЗ [11,160]. Дані параметри широко використовуються для аналізу статистичних параметри окремих складових (компонентів) досліджуваних зображень.

Дослідження проводилося для вибірки з 250 стеганограм, сформованих згідно новітніх стеганографічних методів MiPOD та Synch, при слабкому ($\Delta_\alpha^S = 3\%$) та середньому ($\Delta_\alpha^S = 10\%$) ступені заповнення ЗК стегоданими. Враховуючи відсутність у відкритих джерелах програмних модулів для вилучення стегоданих зі стеганограм згідно наведених АСМ, оцінка ступеня дест-

рукції проводилося шляхом порівняння змін значень яскравості пікселів, обраних для приховання повідомлень.

Отримані оцінки ступеня зміни статистичних (Δ_F^{SPAM}), спектральних ($\Delta W_{uv}^{(k)}$) і структурних (ΔD_R та $\Delta f(\alpha)$) параметрів стеганограм, а також частки пікселів Δ_p , використаних для приховання стегобітів, що лишилися незміненими при використанні досліджуваних методів обробки ЦЗ, наведені в табл. 4.1.

Таблиця 4.1 – Зміни статистичних, спектральних та структурних параметрів стеганограм, а також частка пікселів Δ_p , використаних для приховання стегобітів, що лишилися незміненими при використанні досліджуваних методів обробки цифрових зображень для зображень з пакету ALASKA

	$\Delta_F^{SPAM}, \%$	$\Delta W_{uv}^{(k)}, \%$	$\Delta D_R, \%$	$\Delta f(\alpha), \%$	$\Delta_p, \%$
Ідеалізований випадок	0.00	0.00	0.00	0.00	0.00
Стеганографічний метод MiPOD ($\Delta_\alpha^S = 3\%$)					
Медіанна фільтрація (5 × 5 пікселів)	96.81	78.12	6.63	3.27	17.95
JPEG-стиснення з втратами (IQF=75%)	87.47	48.70	9.24	7.85	42.75
TVM-обробка зображень	72.90	21.91	2.09	6.54	28.96
Запропонований метод реконструкції ЦЗ	12.58	7.34	0.75	2.69	3.49
Стеганографічний метод MiPOD ($\Delta_\alpha^S = 10\%$)					
Медіанна фільтрація (5 × 5 пікселів)	92.15	82.95	10.80	5.42	23.79
JPEG-стиснення з втратами (IQF=75%)	80.76	53.72	13.03	8.18	18.22
TVM-обробка зображень	66.97	22.48	5.14	8.91	14.95

Продовження табл. 4.1

	$\Delta_F^{SPAM}, \%$	$\Delta W_{uv}^{(k)}, \%$	$\Delta D_R, \%$	$\Delta f(\alpha), \%$	$\Delta_p, \%$
Запропонований метод реконструкції ЦЗ	8.06	4.54	1.19	4.57	1.95
Стеганографічний метод Synch ($\Delta_\alpha^S = 3\%$)					
Медіанна фільтрація (5 × 5 пікселів)	98.54	81.84	7.67	2.74	89.65
JPEG-стиснення з втратами (IQF=75%)	89.57	55.91	8.87	5.31	23.55
TVM-обробка зображень	82.03	17.96	3.75	5.39	12.17
Запропонований метод реконструкції ЦЗ	15.57	13.40	1.77	1.22	7.12
Стеганографічний метод Synch ($\Delta_\alpha^S = 10\%$)					
Медіанна фільтрація (5 × 5 пікселів)	90.70	85.27	9.09	4.67	56.95
JPEG-стиснення з втратами (IQF=75%)	81.60	59.69	12.71	5.48	18.02
TVM-обробка зображень	76.03	22.04	6.82	5.31	10.03
Запропонований метод реконструкції ЦЗ	11.18	10.62	2.35	3.71	4.44

Використання TVM-методу фільтрації ЦЗ дозволяє суттєво (до чотирьох разів) зменшити зміни статистичних та спектральних параметрів ЦЗ у порівнянні з поширеними методами деструкції стеганограм (медіанна фільтрація та JPEG-стиснення з втратами, табл. 4.1). При цьому найменші зміни даних параметрів ЦЗ досягаються у випадку слабого заповнення ЗК стегоданими ($\Delta_\alpha^S = 3\%$), що обумовлено зміною відносно малої частки пікселів ЦЗ в процесі обробки. Зростання значень Δ_α^S призводить до підвищення «демас-

куючого» впливу використаних методів деструкції та, відповідно, більших змін параметрів ЦЗ.

З іншого боку, зміни структурних параметрів досліджуваних ЦЗ, а саме спектру Реньї D_R та мультифрактального спектру $f(\alpha)$, практично збігаються для поширених методів деструкції стеганограм. Це обумовлено нелокальним впливом даних методів, що призводить до змін значної кількості пікселів ЦЗ.

Найменші зміни значень розглянутих параметрів стеганограм досягаються при використанні запропонованого методу попередньої обробки ЦЗ (табл. 4.1). Це обумовлено високою «вибірковістю» даних методів щодо виявлення та придушення лише шумових складових ЦЗ без внесення суттєвих змін до інших компонентів. Внаслідок цього можемо зробити висновок щодо ефективності використання запропонованого методу для мінімізації змін статистичних, спектральних та структурних параметрів при забезпеченні високого ступеня деструкції прихованих повідомлень. Тому становить інтерес застосування даного методу для оцінки точності визначення позиції пікселів, використаних для приховання стегобітів.

4.1.2 Оцінка точності визначення позицій пікселів, використаних для вбудовування окремих стегобітів

Задачу визначення пікселів ЗК, використаних для приховання окремих стегобітів, можливо представити як задачу сегментації зображення з використання класів вихідних (незмінених) та модифікованих пікселів [107]. Це дозволяє використовувати потужний математичний апарат розроблених методів сегментації ЦЗ, та показників (індексів) якості роботи даних методів без необхідності розробки спеціалізованих методів обробки зображення (наприклад, розмітки пікселів з використанням ШНМ).

Для вирішення задачі сегментації цифрових зображень було запропоновано значну кількість методів, заснованих на виділенні як окремих об'єктів на зображенні (англ. *instance segmentation*), так і груп подібних об'єктів (англ. *semantic segmentation*). Сучасні методи для проведення сегментації ЦЗ засно-

вані на використанні автокодувальних нейронних мереж. Прикладом даних методів є відома мережа U-Net [253], структура котрої наведена на рис. 4.1.

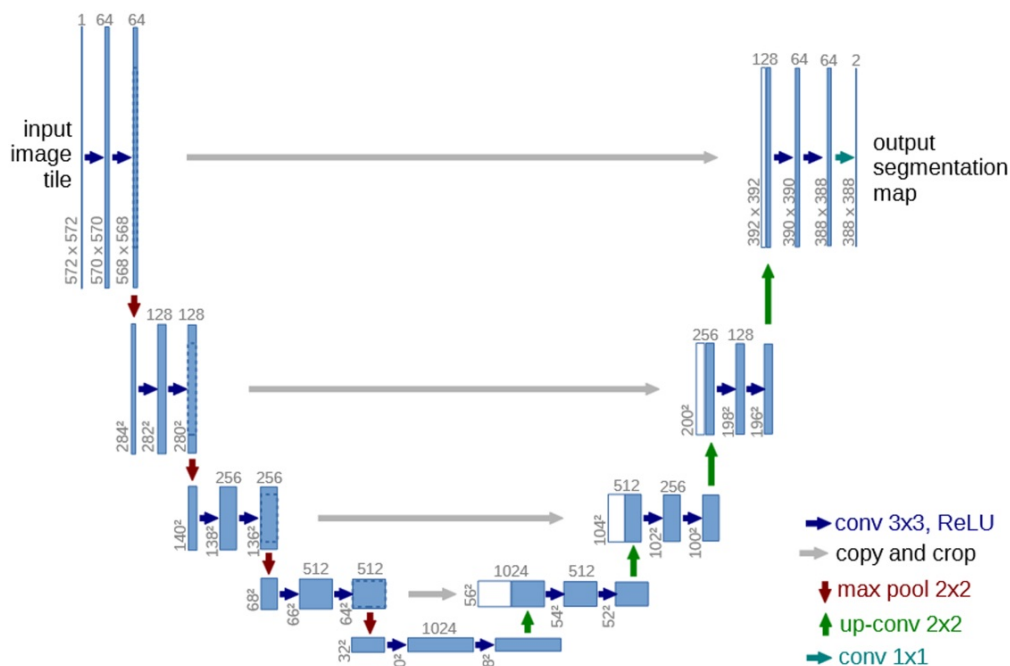


Рисунок. 4.1 – Структура штучної нейронної мережі U-Net, що використовується в задачах сегментації цифрових зображень. За матеріалами роботи [253].

Обробка досліджуваного зображення з використання мережі U-Net проводиться в декілька етапів (рис. 4.1). На першому етапі проводиться попередня обробка вхідного ЦЗ з використанням послідовності згорткових шарів для виділення статистичних параметрів ЦЗ. На другому етапі, відбувається проєкція отриманих векторів, що відповідають отриманим параметрам ЦЗ, до простору меншої розмірності для зниження обчислювальної складності обробки та виділення характерних параметрів для кожного класу (об'єкту сегментації). На останньому етапі проводиться побудова карти сегментації (присвоєння кожному пікселю ЦЗ мітки ЗК або ж стеганограм) ЦЗ шляхом застосування даних операцій в зворотньому порядку. Наявність розробленого математичного апарату для швидкого налаштування АНМ дозволяє суттєво зменшити обчислювальну складність налаштування U-Net мережі (рис. 4.1) при забезпеченні високої якості сегментації зображення [253].

Наведена структура нейронної мережі сегментації ЦЗ була адаптована до вирішення задачі визначення положення пікселів, використаних для при-

ховання окремих стегобітів. Для цього на вхід даної мережі передавалася різниця вихідного та обробленого з використанням запропонованого методу ЦЗ. Дослідження точності роботи запропонованого методу сегментації стеганограм проводилося з використанням псевдовипадкової вибірки 10,000 зображень зі стандартного пакету зображень ALASKA [134]. Зображення були масштабовані до однакового розміру 512×512 (пікселів) та представлені в градація сірого кольору. Формування стеганограм проводилося згідно сучасних стеганографічних методів HUGO [147], MiPOD [153] та Synch [132].

Налаштування мережі U-Net у складі запропонованого методу сегментації стеганограм проводилося на окремій вибірці 10,000 зображень з пакету ALASKA, що не використовувалися в попередніх дослідженнях. За результатами обробки зображень з використанням даної мережі, значення пікселів, що не використовувалися для приховання стегобітів, були рівними (+1) та (-1) в протилежному випадку. Дані значення міток пікселів дозволяють використовувати функцію бінарної кросс-ентропії розподілу q отримуваних значень на виході мережі U-Net відносно очікуваного розподілу міток пікселів p для поточного зображення [46,47]:

$$H(p, q) = -\mathbb{E}_p[\log q], \quad (4.1)$$

де $\mathbb{E}_p(\cdot)$ – оператор визначення математичного очікування за імовірнісним розподілом p . Налаштування мережі U-Net проводилося шляхом мінімізації значення функції бінарної кросс-ентропії (4.1) з використання методу оптимізації Adam [46,47].

Для налаштування мережі U-Net було підготовлено пакет ЗК та стеганограм при виборі ступеня заповнення ЗК стегоданими Δ_α^S згідно рівномірного розподілу з діапазону $\Delta_\alpha^S \in [3; 50]$. Стегодані були сформовані згідно стеганографічних методів HUGO [147], MiPOD [153] та Synch [132].

Для кожного тестового зображення була підготовлена відповідна «маска» (матриця значень міток пікселів), що використовувалася в якості очікуваного (вихідного) значення мережі U-Net (рис. 4.1). Налаштування мережі

проводилося протягом 250 ітерацій (epoch) обробки тестового пакету при використанні вибірок з 16 зображень для оновлення параметрів мережі.

Дослідження точності сегментації стеганограм з використанням розробленого методу відбувалося на початковій вибірці з 10,000 тестових зображень з пакету ALASKA [134]. Оцінка точності сегментації зображення проводилася з використанням наступних показників [144,208]:

$$DSC(M_t, M_p) = 2 \cdot |M_t \cap M_p| / (|M_t| + |M_p|), \quad (4.2)$$

$$D_T^S(M_t, M_p) = \frac{|M_t \cap M_p|}{|M_t \cap M_p| + \beta(\alpha \cdot a + (1 - \alpha) \cdot b)}, \quad (4.3)$$

$$a = \min(|M_t \setminus M_p|, |M_p \setminus M_t|),$$

$$b = \max(|M_t \setminus M_p|, |M_p \setminus M_t|),$$

де M_t – послідовність «істинних» значень міток пікселів; M_p – послідовність міток пікселів, отриманих за результатами роботи розробленого методу; $DSC(A, B)$ – показник Сьоренсена-Дайса ступеня подібності множин A та B ; $D_T^S(M_t, M_p)$ – симетричний індекс Тверського; $A \setminus B$ – доповнення множини A до множини B ; $\alpha, \beta \geq 0$ – вагові коефіцієнти для індексу Тверського. При проведенні досліджень послідовності M_t та M_p у виразах (4.2)-(4.3) були отримані при об'єднанні всіх рядків матриці, отримуваних за результатами роботи мережі U-Net.

Відмітимо, що значення $DSC(A, B)$ (4.2) змінюється від нуля, що відповідає випадку коли значення елементів послідовностей A та B відрізняються для кожного зсуву (індексу), до (+1) коли послідовності A та B повністю співпадають. При цьому показник Сьоренсена-Дайса (4.2) є тісно пов'язаним з відомим показником Жаккарта [254]:

$$J(M_t, M_p) = \frac{|M_t \cap M_p|}{|M_t| + |M_p| - |M_t \cap M_p|} = \frac{DSC(M_t, M_p)}{2 - DSC(M_t, M_p)}.$$

Вагомою перевагою показника Тверського $D_T^S(M_t, M_p)$ у порівнянні з показником Сьоренсена-Дайса $DSC(A, B)$ є варіація впливу досліджуваних послідовностей. Зокрема, в більшості досліджень приймається припущення,

що α та β відповідають вагам послідовностей M_t та M_p відповідно у виразі (4.3). Це дозволяє досліджувати зміни ступеня подібності множин при відповідних змінах ступеня «довіри» до результатів сегментації ЦЗ.

Згідно рекомендацій [255], значення вагових параметрів α та β для показника Тверського $D_T^S(M_t, M_p)$ (4.3) обиралося з врахуванням залежності $\alpha + \beta = 1$. При проведенні досліджень, більша вага надавалася множині M_t ($\alpha = 0.7$), що відповідає більшому впливу «істинних» міток класів, в той час як для множини M_p відповідний ваговий коефіцієнт був рівним $\beta = 0.3$. Аналогічно до показника Сьоренсена-Дайса (4.2), значення $D_T^S(M_t, M_p)$ змінюється від 0 до (+1), де значення $D_T^S(M_t, M_p) = 0$ відповідає випадку відсутності пікселів, використаних для приховання окремих стегобітів, в послідовності M_p , а значення $D_T^S(M_t, M_p) = 1$ – співпадінню послідовностей M_t та M_p (визначенню позицій всіх пікселів, використаних при формуванні стеганограми).

За результатами досліджень отримано залежності наведених показників (4.2)-(4.3) від ступеня заповнення ЗК стегоданими для стеганографічних методів HUGO [147], MiPOD [153] та Synch [132] для розробленого методу сегментації стеганограм, наведені в табл. 4.2. Для порівняння наведені результати при використанні штучної нейронної мережі SR-Net [30] для попередньої обробки ЦЗ для запропонованого методу сегментації стеганограм.

Таблиця 4.2 – Значення показника Сьоренсена-Дайса $DSC(M_t, M_p)$ та індекса Тверського $D_T^S(M_t, M_p)$ щодо точності локалізації пікселів, використаних для приховання окремих стегобітів, при варіації ступеня заповнення ЗК стегоданими для стеганографічних методів HUGO, MiPOD та Synch.

		Ідеальний випадок	Стеганографічний метод		
			HUGO	MiPOD	Synch
Попередня обробка зображень з використанням мережі SR-Net					
$\Delta_\alpha^S = 5\%$	$DSC(M_t, M_p)$	1.000	0.376	0.199	0.123

Продовження табл. 4.2

		Ідеальний випадок	Стеганографічний метод		
			HUGO	MiPOD	Synch
	$D_T^S(M_t, M_p)$	1.000	0.221	0.127	0.109
$\Delta_\alpha^S = 20\%$	$DSC(M_t, M_p)$	1.000	0.483	0.258	0.196
	$D_T^S(M_t, M_p)$	1.000	0.293	0.187	0.154
$\Delta_\alpha^S = 50\%$	$DSC(M_t, M_p)$	1.000	0.631	0.301	0.211
	$D_T^S(M_t, M_p)$	1.000	0.588	0.295	0.209
Попередня обробка зображень з використанням запропонованого методу ($w_{UC} = 16, N_{UC} = 512$)					
$\Delta_\alpha^S = 5\%$	$DSC(M_t, M_p)$	1.000	0.598	0.481	0.434
	$D_T^S(M_t, M_p)$	1.000	0.521	0.449	0.406
$\Delta_\alpha^S = 20\%$	$DSC(M_t, M_p)$	1.000	0.714	0.622	0.593
	$D_T^S(M_t, M_p)$	1.000	0.698	0.603	0.574
$\Delta_\alpha^S = 50\%$	$DSC(M_t, M_p)$	1.000	0.919	0.882	0.807
	$D_T^S(M_t, M_p)$	1.000	0.883	0.858	0.781

Зазначимо, що значення показників Сьоренсена-Дайса $DSC(M_t, M_p)$ та $D_T^S(M_t, M_p)$ несуттєво відрізняються (табл. 4.2). Це обумовлено відмінностями в точності оцінки ступеня «подібності» послідовностей M_t та M_p – показник $DSC(M_t, M_p)$ широко використовується у випадках, коли важлива точність локалізації об'єктів (груп пікселів). З іншого боку, показник $D_T^S(M_t, M_p)$ дозволяє підвищити точність оцінки результатів сегментації окремих пікселів досліджуваного зображення за рахунок варіації значень вагових параметрів α та β у виразі (4.3).

Відмітимо відносно низьку точність сегментації стеганограм при використанні мережі SR-Net для попередньої обробки ЗК та стеганограм при застосуванні запропонованого методу сегментації модулю (близько 0.5, табл.

4.2). Дані результати досягаються лише у випадку сильного ступеня заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 50\%$) та використання стеганографічного методу HUGO (табл. 4.2). При цьому точність сегментації стеганограм при використанні мережі SR-Net суттєво знижується (до 0.1) у випадку використання новітніх методів MiPOD та Synchron навіть при сильному заповненні ЗК стегоданими.

Використання запропонованого методу попередньої обробки ЦЗ дозволяє суттєво (до чотирьох разів) підвищити точність локалізації пікселів, використаних для приховання окремих стегобітів. При цьому висока точність сегментації стеганограм зберігається навіть у найбільш складному випадку слабого заповнення ЗК стегоданими ($\Delta_{\alpha}^S = 5\%$, табл. 4.2). Відмітимо суттєве зростання точності (значення показників $DSC(M_t, M_p)$ та $D_T^S(M_t, M_p)$ наближаються до одиниці) при обробці стеганограм при середньому ($\Delta_{\alpha}^S = 5\%$) та сильному ($\Delta_{\alpha}^S = 20\%$) ступені заповнення ЗК стегоданими (табл. 4.2). Це дає можливість суттєво підвищити точність локалізації пікселів, використаних для приховання повідомлень та, в окремих випадках ($D_T^S(M_t, M_p) \geq 0.8$), забезпечити визначення значень вбудованих стегобітів.

Таким чином, можемо зробити висновок, що застосування запропонованого методу попередньої обробки ЦЗ дозволяє суттєво підвищити точність локалізації положення пікселів, використаних для приховання бітів повідомлення при формуванні стеганограм. Забезпечення високої точності локалізації даних пікселів дозволяє суттєво розширити можливості сучасних методів стегоаналізу ЦЗ, зокрема щодо вилучення та внесення спотворень (підміни) частин вбудованих стегоданих, що становить особливий інтерес при розробці новітніх комплексів протидії витоку ІзОД.

4.2 Висновки за розділом 4

В розділі наведено результати дослідження ефективності використання розробленого програмного комплексу Blind-Steg в найбільш складних випадках проведення стегоаналізу ЦЗ та отримано наступні результати:

1. Показано високу ефективність деструкції прихованих повідомлень при обробці стеганограм у порівнянні з сучасними методами стегааналізу ЦЗ, зокрема методів анізотропної фільтрації зображень. Застосування запропонованих методів дозволяє забезпечити високу якість деструкції стеганограм при несуттєвих змінах статистичних параметрів ЗК, навіть у найбільш складному випадку слабого заповнення ЗК стегоданими (менше 10%) та використання новітніх методів MiPOD та Synch.

2. Розроблено модуль визначення позиції пікселів ЗК, використаних для приховання окремих стегобітів. Даний модуль заснований на сегментації пікселів досліджуваного ЦЗ за результатами порівняння вихідного та обробленого ЦЗ, отриманого з використанням розроблених методів. За результатами дослідження точності визначення пікселів для стеганограм, сформованих згідно сучасних АСМ, виявлено, що використання запропонованих методів дозволяє суттєво (до чотирьох разів) підвищити точність локалізації пікселів, використаних для приховання стегобітів, у порівнянні з сучасними методами стегааналізу ЦЗ. Отримані результати дозволяють розширити можливості сучасних методів стегааналізу ЦЗ щодо вилучення та внесення спотворень (підміни) частин вбудованих стегоданих, що становить особливий інтерес при розробці новітніх комплексів протидії витоку ІзОД.

3. Модульна структура запропонованого комплексу прикладних програм дозволяє зменшити складність розширення його функціональності та адаптації до умов проведення стегааналізу (наприклад, наявних апріорних даних щодо СМ, статистичних параметрів досліджуваних ЦЗ), що становить інтерес для його інтеграції з сучасними системами протидії витоку ІзОД.

ВИСНОВКИ

У дисертаційній роботі розв'язано актуальну науково-прикладну проблему розробки високоточних методів виявлення стеганограм, здатних надійно працювати в умовах відсутності апріорних даних щодо особливостей використаних стеганографічних методів, малого ступеня заповнення ЗК стегоданими (менше 10%) та при значній варіативності параметрів досліджуваних зображень. Отримано наукові та практичні результати, що мають істотні переваги перед існуючими рішеннями:

1. За результатами комплексного аналізу структури та особливостей роботи існуючих стегодетекторів для ЦЗ виявлено принципові обмеження сучасної парадигми побудови стегодетекторів, обумовлені використанням емпіричних підходів до вибору параметрів процедури обробки досліджуваних ЦЗ. Це стосується необхідності тривалого налаштування методів попередньої обробки ЦЗ, а саме визначення параметрів ансамблів ФВЧ, для забезпечення високої точності виявлення стеганограм (більше 90%). Також, наразі запропоновано вирішення задачі визначення демаскуючих ознак сформованих стеганограм лише для окремих (часткових) випадків, що унеможливило надійне виявлення стеганограм, сформованих згідно апріорно невідомих стеганографічних методів. Для подолання даних обмежень запропоновано суттєві зміни загальної концепції побудови СД, а саме інтеграції етапів попередньої обробки ЦЗ та аналізу статистичних, структурних і спектральних параметрів оброблених зображень, що дозволяє забезпечити високу точність виявлення стеганограм навіть у випадку «сліпого» стегоаналізу при спрощенні структури СД.

2. Враховуючи суттєве зниження точності виявлення стеганограм при роботі СД в умовах обмеженості апріорних даних щодо використаного СМ та при значній варіації статистичних параметрів ЦЗ, запропоновано метод визначення факторів, що мають найбільший вплив на параметри оброблюваних зображень. Метод заснований на використанні теореми Джонсона-Лінден-

штрауса для аналізу взаємного розташування кластерів векторів, що відповідають параметрам ЗК та стеганограм, в просторі вищої розмірності. Запропонований метод дозволив підвищити на 2% точність виявлення стеганограм, проте лише у випадку сильного заповнення ЗК стегоданими ($\Delta_{\alpha}^S > 20\%$). Для забезпечення високої вірогідності виявлення стеганограм в умовах відсутності апріорних даних щодо використаного СМ, мінімізації ступеня заповнення ЗК стегоданими та зміни в широких межах статистичних параметрів досліджуваних зображень запропоновано концепцію побудови методів попередньої обробки досліджуваних зображень, що заснована на використанні спеціальних методів декомпозиції та синтезу зображень, для забезпечення високої точності оцінки параметрів ЦЗ за наявними (зашумленими) даними.

3. Для забезпечення надійного виявлення стеганограм у випадку відсутності апріорних даних щодо використаного стеганографічного методу та при значній варіації значень параметрів ЦЗ запропоновано метод синтезу структури та оптимізації параметрів високоточних СД. Запропонований метод відрізняється представленням задачі побудови стегодетектору як оптимізаційної задачі максимізації відстані Хеллінгера між імовірнісними розподілами значень яскравості пікселів ЗК та стеганограм після проведення їх попередньої обробки. Показано, що значення помилки класифікації стеганограм P_E при синтезі високоточних СД згідно запропонованого методу узгоджуються з теоретичними оцінками досяжної вірогідності виявлення стеганограм у всьому діапазоні зміни значень ступеня заповнення ЗК стегоданими, навіть у випадку проведення «сліпого» стегоаналізу ЦЗ. При цьому відомі підходи до проведення стегоаналізу ЦЗ дозволяють наблизитися до даних оцінок лише в області середнього ($\Delta_{\alpha}^S \in [10; 20]$) та сильного ($\Delta_{\alpha}^S > 20\%$) ступеня заповнення ЗК стегоданими при виявленні апріорно відомих стеганографічних методів.

4. Для практичної реалізації запропонованої структури високоточних СД за критерієм мінімізації значення помилки класифікації стеганограм роз-

роблено метод попередньої обробки ЦЗ, який не потребує використання апріорних даних щодо СМ. Запропонований метод заснований на реконструкції вихідного виду ЗК за наявними (зашумленими) даними із застосуванням спеціальних систем функцій в якості базису перетворення. Використання запропонованого методу попередньої обробки ЦЗ при синтезі СД дозволило на 23% підвищити точність виявлення стеганограм в найбільш складних випадках проведення стегоаналізу ЦЗ, а саме виявлення невідомих стеганографічних методів при слабкому (менше 10%) ступеню заповнення ЗК стегаданими. Висока точність реконструкції ЗК при обробці стеганограм з використанням запропонованого методу дозволяє отримувати важливі дані щодо особливостей роботи використаного стеганографічного методу, а саме визначення положення пікселів, використаних для приховання повідомлень. Практичне використання даних відомостей становить особливий інтерес для підвищення ефективності методів деструкції та вилучення (екстракції) прихованих повідомлень.

5. На основі запропонованого методу синтезу структури та оптимізації параметрів стегодетекторів розроблено та реалізовано програмний комплекс для проведення стегоаналізу ЦЗ. Комплекс дозволяє автоматизувати вирішення широкого спектру задач, що стосуються синтезу високоточних СД для надійного виявлення стеганограм в умовах «сліпого» стегоаналізу, розробки методів локалізації положення пікселів, використаних для вбудовування стегобітів, та вилучення прихованих повідомлень. Також комплекс дає можливість проводити надійну деструкцію стеганограм при забезпеченні мінімальних змін статистичних параметрів оброблюваних ЦЗ, що дозволяє маскувати вплив на стеганографічний канал передачі даних.

6. Проведені експериментальні дослідження підтвердили високу точність роботи СД у складі розробленого стеганографічного комплексу. Зокрема, кількість помилок виявлення стеганограм зменшено в чотири рази у порівнянні з сучасними СД навіть у випадку виявлення апріорно невідомих АСМ. При цьому розроблений комплекс дозволяє зменшити тривалість об-

робки ЦЗ до трьох разів (з 27.07 секунд для випадку використання ШНМ, до 8.24 секунд для запропонованого методу) у порівнянні з існуючими методами синтезу стегодетекторів при забезпеченні фіксованої точності виявлення стеганограм, що становить особливий інтерес для впровадження комплексу у системи моніторингу та контролю ІКС.

7. За результатами експериментальних досліджень підтверджено високу точність локалізації пікселів ЗК, використаних при формуванні стеганограм, при використанні розробленого комплексу (локалізація до 88% пікселів, використаних для приховання стегобітів). Це дозволяє суттєво підвищити ефективність деструкції стеганограм при забезпеченні мінімальних змін статистичних, спектральних та структурних параметрів оброблюваних зображень (досягнуто зниження до трьох разів рівня змін параметрів ЦЗ у порівнянні з сучасними методами деструкції), що становить особливий інтерес для маскування факту втручання в стеганографічний канал передачі ІзОД. Отримані результати дозволяють створити передумови для вирішення найбільш складних задач стегоаналізу ЦЗ, а саме розробки методів екстракції та підміни стегоданих.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

- [1] FireEye, Inc., «HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group,» FireEye, Milpitas, 2015.
- [2] J.-P. A. Yaacoub, O. Salman, H. N. Noura, N. Kaaniche, A. Chehab та M. Malli, «Cyber-physical systems security: Limitations, issues and future trends,» *Microprocessors and Microsystems*, т. 77, 2020.
- [3] Kaspersky Inc., «Steganography in attacks on industrial enterprises,» Kaspersky Inc., Moscow, 2020.
- [4] «Top Cybersecurity Threats In 2023,» 2023. [З мережі]. Available: <https://www.forrester.com/report/top-cybersecurity-threats-in-2023/RES179154>. [Дата звернення: 2024].
- [5] Т. С. С. о. Ukraine, «Gamaredon / Armageddon Group: FSB RF cyber attacks against Ukraine,» The Security Service of Ukraine, Kyiv, 2021.
- [6] Carnegie Endowment for International Peace, «Timeline of Cyber Incidents Involving Financial Institutions,» Carnegie Endowment for International Peace, Washington, 2021.
- [7] Center for strategic & international studies, «Significant Cyber Incidents,» Center for strategic & international studies, Washington, 2022.
- [8] J. Butora, Y. Yousfi та J. Fridrich, «How to Pretrain for Steganalysis,» в *IH&MMSec '21: Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security*, New York, 2021.
- [9] M. Hassaballah, *Digital Media Steganography: Principles, Algorithms, and Advances*, 1st edition ред., New York: Academic Press, 2020.
- [10] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*, Cambridge: Cambridge University Press, 2009.
- [11] Г. Ф. Конахович, Д. О. Прогонов та О. Ю. Пузиренко, Комп'ютерна

- стеганографічна обробка й аналіз мультимедійних даних, Київ: Центр учбової літератури, 2018, р. 558.
- [12] A. D. Ker та T. Pevny, «Batch steganography in the real world,» в *roceedings of the on Multimedia and security*, New York, 2012.
- [13] В. Г. Грибунин, И. Н. Оков та И. В. Туринцев, Цифровая стеганография, 2-е ред., Москва: СОЛОН-Пресс, 2018.
- [14] А. В. Аграновский, А. В. Балакин, В. Г. Грибунин та С. А. Сапожников, Стеганография, цифровые водяные знаки и стегоанализ, Москва: Вузовская книга, 2009.
- [15] Г. Ф. Конахович, «Оценка эффективности методов стенографического встраивания информации в спектральную область изображений,» *Автоматизированные системы управления и приборы авто-матики*, т. 168, pp. 59-63, 2015.
- [16] В. Задирака, І. Сергієнко, І. Коваленко та П. Андон, «Комп'ютерна стеганографія,» в *Стан та перспективи розвитку інформатики в Україні*, Київ, Наукова думка, 2010, pp. 736-747.
- [17] В. Лукічов, В. Лужецький та А. Васюра, Методи та засоби стеганографічного захисту інформації на основі вейвлет-перетворень, Вінниця: ВНТУ, 2014, р. 160.
- [18] В. Лужецький, А. Кожухівський та О. Войтович, Основи інформаційної безпеки, Вінниця: ВНТУ, 2013, р. 220.
- [19] А. Кобозева та В. Хорошко, Анализ информационной безопасности, Киев: ГУИКТ, 2009, р. 251.
- [20] А. Кобозева та М. Козина, «Стеганографический метод двухэтапного декодирования, обеспечивающий аутентификацию контейнера,» *Информика та мат. методи в моделюванні*, т. 3, № 2, pp. 169-178, 2013.
- [21] Н. Кошкина, «Обзор и классификация методов стеганоанализа,» *Управляющие системы и машины*, т. 3, pp. 3-12, 2015.

- [22] N. Koshkina, «Comparison of Efficiency of Statistical Models Used for Formation of Feature Vectors by JPEG Images Steganalysis,» *Theoretical and Applied Cybersecurity*, pp. 22-28, 6 8 2020.
- [23] В. Королёв, В. Полиновский та В. Герасименко, «Стеганография по методу наименее значимого бита на базе персонализированных флеш-накопителей,» *Управляющие системы и машины*, т. 1, № 231, pp. 79-87, 2011.
- [24] О. О. Кузнецов, С. П. Євсєєв та О. Г. Король, Стеганографія, Харків:: ХНЕУ, 2011, p. 232.
- [25] I. Avcibas, N. Memon та B. Sankur, «Steganalysis using image quality metrics,» *Transactions on Image Processing*, т. 12, № 2, p. 221–229, 2003.
- [26] I. Avcibas, M. Kharrazi, N. Memon та B. Sankur, «Image Steganalysis with Binary Similarity Measures,» *EURASIP Journal on Applied Signal Processing*, т. 17, pp. 2749-2757, 2005.
- [27] P. Bas, T. Filler та T. Pevný, «”Break Our Steganographic System”: The Ins and Outs of Organizing BOSS,» в *International Workshop on Information Hiding*, Berlin, 2011.
- [28] R. Böhme, *Advanced Statistical Steganalysis*, London: Springer, 2010.
- [29] M. Boroumand, J. Fridrich та R. Cogranne, «Are we there yet?,» в *Electronic Imaging, Media Watermarking, Security, and Forensics*, New York, 2019.
- [30] M. Boroumand, M. Chen та J. Fridrich, «Deep Residual Network for Steganalysis of Digital Images,» *IEEE Transactions on Information Forensics and Security*, т. 14, № 5, pp. 1181-1193, May 2019.
- [31] M. Boroumand та J. Fridrich, «Synchronizing Embedding Changes in Side-Informed Steganography,» в *Electronic Imaging, Media Watermarking, Security, and Forensics*, Burlingame, 2020.
- [32] J. Butora та J. Fridrich, «Revisiting Perturbed Quantization,» в *IH&MMSec*.

- Workshop*, Brussels, 2021.
- [33] I. J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich та T. Kalker, *Digital Watermarking and Steganography*, Burlington: Elsevier, 2008.
- [34] J. Fridrich та J. Kodovsky, «Rich Models for Steganalysis of Digital Images,» *Transactions on Information Forensics and Security*, т. 7, № 3, pp. 868 - 882, 2012.
- [35] S. Katzenbeisser та P. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, Boston: Artech House, 2000.
- [36] A. D. Ker, «Batch steganography and pooled steganalysis,» в *Proceedings of the 8th international conference on Information hiding*, Berlin, 2007.
- [37] A. D. Ker, P. Bas, R. Böhme, R. Cogranne, S. Craver, T. Filler, J. Fridrich та T. Pevný, «Moving steganography and steganalysis from the laboratory into the real world,» в *IH&MMSec '13: Proceedings of the first ACM workshop on Information hiding and multimedia security*, New York, 2013.
- [38] T. Pevny, P. Bas та J. Fridrich, «Steganalysis by Subtractive Pixel Adjacency Matrix,» *Transactions on Information Forensics and Security*, т. 5, № 2, pp. 215-224, 2010.
- [39] K. Sullivan, U. Madhow, S. Chandrasekaran та B. Manjunath, «Steganalysis for Markov Cover Data With Applications to Images,» *IEEE Transactions On Information Forensics And Security*, т. 1, № 2, pp. 275-287, 2006.
- [40] R. Tabares-Soto, R. Ramos-Pollán та G. Isaza, «Deep Learning Applied to Steganalysis of Digital Images: A Systematic Review,» *IEEE Press*, т. 7, pp. 68970 - 68990, 2019.
- [41] V. Holub та J. Fridrich, «Phase-aware projection model for steganalysis of JPEG images,» в *Media Watermarking, Security, and Forensics*, San Francisco, 2015.
- [42] X. Song, F. Liu, C. Yang, X. Luo та Y. Zhang, «Steganalysis of Adaptive JPEG Steganography Using 2D Gabor Filters,» в *IH&MMSec:3rd*

- Workshop on Information Hiding and Multimedia Security*, New York, 2015.
- [43] R. Zhang, F. Zhu, J. Liu та G. Liu, «Efficient feature learning and multisize image steganalysis based on CNN,» Cornell University, Cornell, 18.
- [44] R. Tabares-Soto, H. B. Arteaga-Arteaga, M. A. Bravo-Ortiz, A. Mora-Rubio, D. Arias-Garzón, J. A. Alzate-Grisales, A. B. Burbano-Jacome, S. Orozco-Arias, G. Isaza та R. Ramos-Pollán, «GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis,» *IEEE Access*, т. 9, pp. 14340 - 14350, 2021.
- [45] S. Tan та B. Li, «Stacked convolutional auto-encoders for steganalysis of digital images,» в *Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, 2014.
- [46] C. C. Aggarwal, *Neural Networks and Deep Learning: A Textbook*, New York: Springer, 2018, p. 520.
- [47] I. Goodfellow, Y. Bengio та A. Courville, *Deep Learning*, Cambridge: The MIT Press, 2016, p. 800.
- [48] А. В. Дорошенко та Д. О. Прогонов, «Виявлення стеганограм з використанням авторегресійних моделей зображення-контейнеру,» в *Праці VI міжнародної науково-практичної конференції «Обробка сигналів та негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка*, Черкаси, 2017.
- [49] А. В. Дорошенко та Д. О. Прогонов, «Визначення параметрів стеганограм з використанням авторегресійних моделей цифрових зображень,» в *Матеріали XV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики»*, Київ, 2017.
- [50] А. В. Дорошенко, «Пасивний стегоаналіз цифрових зображень з

- використанням моделей просторової кореляції,» в *Сборник тезисов участников XVII Международной научно-практической конференции «Безопасность информации в информационно-телекоммуникационных системах»*, Київ, 2016.
- [51] Д. О. Прогонов, «Ефективність універсального стегодетектору Фаріда при вбудовуванні даних у цифрові зображення згідно адаптивних методів,» в *Матеріали Міжнародної науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи»*, Київ, 2017.
- [52] Д. О. Прогонов, В. О. Богайчук та Є. М. Терещенко, «Ефективність універсальних стегодетекторів у випадку використання адаптивних методів формування стеганограм,» в *Праці VI міжнародної науково-практичної конференції «Обробка сигналів та негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка*, Черкаси, 2017.
- [53] Д. О. Прогонов та В. О. Голубничий, «Виявлення стеганограм, сформованих комплексними методами, з використанням стегодетектора Фаріда,» в *Матеріали міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах»*, Київ, 2017.
- [54] В. Богайчук, Є. Терещенко та Д. Прогонов, «Виявлення стеганограм, сформованих згідно адаптивного методу SI-UNIWARD, з використанням універсальних стегодетекторів,» в *Матеріали Міжнародної науково-практичної конференції «Захист інформації і безпека інформаційних систем»*, Львів, 2017.
- [55] В. Голубничий та Д. Прогонов, «Вплив вибору базисних функцій вейвлет-перетворення на ефективність стегодетектору Фаріда,» в *Матеріали Міжнародної науково-практичної конференції «Захист інформації і безпека інформаційних систем»*, Львів, 2017.
- [56] D. Progonov, «Multiclass detector for modern steganographic methods,»

Information Theories and Applications, т. 24, № 3, pp. 55-71, 2017.

- [57] Д. О. Прогонов та Д. О. Панічева, «Виявлення стеганограм з використанням універсальних статистичних моделей контейнеру,» в *Збірник матеріалів Міжнародної науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи»*, Київ, 2016.
- [58] Д. О. Прогонов, П. О. Сівкович та Ю. В. Могиліна, «Порівняльний аналіз точності виявлення стеганограм при використанні статистичних моделей цифрових зображень,» в *Матеріали Міжнародної науково-практичної конференції «Захист інформації і безпека інформаційних систем»*, Львів, 2017.
- [59] Д. В. Чайка та Д. О. Прогонов, «Виявлення стеганограм, сформованих згідно адаптивних методів, з використанням статистичної моделі PHARM,» в *Матеріали XVI Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики»*, Київ, 2018.
- [60] D. Progonov, «Performance of Statistical Stegdetectors in Case of Small Number of Stego Images in Training Set,» в *International Scientific-Practical Conference “Problems of Infocommunications Science and Technology” (PIC S&T 2020)*, Kharkiv, 2020.
- [61] D. Progonov, «Statistical Steganalysis of Multistage Embedding Methods,» *International Journal “Information Models & Analyses”*, т. 5, № 1, pp. 23-36, 2016.
- [62] Д. О. Панічева та Д. О. Прогонов, «Статистичний стегоаналіз цифрових зображень з використанням універсальної моделі CDF,» в *Матеріали XIV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики»*, Київ, 2016.

- [63] D. Progonov, «Structural Stegdetector Performance in case of Side-Informed Message Embedding,» в *International Scientific-Practical Conference “Problems of Infocommunications Science and Technology” (PIC S&T 2017)*, Kharkiv, 2017.
- [64] Н. В. Остапюк та Д. О. Прогонов, «Виявлення стеганограм з використанням ріджлет-перетворення,» в *Матеріали XVI Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики»*, Київ, 2018.
- [65] D. Progonov та V. Lutsenko, «Effectiveness of stego images pre-processing with spectral analysis methods,» *Applied Aspects of Information Technology*, т. 5, № 1, pp. 64-75, 2022.
- [66] Д. О. Прогонов, «Стегодетектор на основі мультифрактального аналізу цифрових зображень,» в *Материалы 18-й Международной научно-практической конференции «System analysis and information technologies»*, Київ, 2016.
- [67] Д. Прогонов, «Мультифрактальний флуктуаційний аналіз стеганограм, сформованих згідно комплексних методів,» в *Матеріали V-тої Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем»*, Львів, 2016.
- [68] М. А. Бука та Д. О. Прогонов, «Деструкція прихованих повідомлень шляхом масштабування контейнеру,» в *Proceedings of International Research and Practice Conference “Modern Methods, Innovations, and Experience of Practical Application in the Field of Technical Sciences”*, Radom, 2017.
- [69] В. О. Богайчук та Д. О. Прогонов, «Деструкція стеганограм з використанням методу головних компонент,» в *Матеріали XVI Всеукраїнської науково-практичної конференції студентів, аспірантів*

та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики», Київ, 2018.

- [70] Y. Mohylina, D. Progonov та V. Bohaichuk, «Stego images destruction using a decomposition in the basis formed using K-SVD algorithm,» в *7th International Scientific and Technical Conference "Information Protection and Information Systems Security"*, Lviv, 2019.
- [71] Д. О. Прогонов, «Вплив невідповідності областей приховання повідомлень та проведення стегааналізу на ефективність статистичних стегадетекторів,» в *Матеріали 19-ї Міжнародної науково-технічної конференції «Системний аналіз та інформаційні технології»*, Київ, 2017.
- [72] Д. О. Прогонов, «Теоретико-інформаційні оцінки спотворень контейнерів при формуванні стеганограм,» в *Матеріали Міжнародної науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи»*, Київ, 2018.
- [73] Д. О. Прогонов, «Теоретико-інформаційні оцінки стійкості методів UNIWARD до стегааналізу,» в *Матеріали XX Міжнародної науково-технічної конференції «Системний аналіз та інформаційні технології»*, Київ, 2018.
- [74] D. Progonov, «Information-Theoretic Estimations of Cover Distortion by Adaptive Message Embedding,» *Information Theories and Applications*, т. 25, № 1, pp. 47-62, 2018.
- [75] Д. О. Прогонов, «Аналіз змін χ^2 -квадрат відстані між розподілами яскравості пікселів при фільтрації зображень-контейнерів та стеганограм,» *Вісник Національного технічного університету України «Київський політехнічний інститут»*. Серія – Радіотехніка. Радіоапаратобудування, т. 75, pp. 54-60, 2018.
- [76] D. Progonov, «Analysis of changes the Renyi divergence for pixel

- brightness distributions by stego images Wiener filtering,» *Information Technologies & Knowledge*, т. 12, № 2, pp. 3-25, 2018.
- [77] Д. О. Прогонов, «Аналіз змін χ^2 -квадрат відстані між розподілами яскравості пікселів при фільтрації стеганограм, сформованих згідно методу UNIWARD,» *Вісник Національного технічного університету України «Київський політехнічний інститут»*. Серія – *Радіотехніка. Радіоапаратобудування*, т. 76, pp. 72-76, 2019.
- [78] D. Progonov, «Effectiveness of stego image calibration via feature vectors re-projection into high-dimensional spaces,» *Radio Electronics, Computer Science, Control*, т. 2, № 61, pp. 165-174, 2022.
- [79] Д. О. Прогонов, «Аналіз точності виявлення стеганограм, сформованих адаптивними методами, при додатковому зашумленні зображень-контейнерів,» в *Матеріали Міжнародної науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи»*, Київ, 2019.
- [80] Д. О. Прогонов, «Вплив попереднього зашумлення на точність виявлення стеганограм, сформованих згідно адаптивних методів MG та MiPOD,» в *Матеріали X Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій»*, Запоріжжя, 2020.
- [81] D. O. Progonov, «Influence of digital images preliminary noising on statistical stegdetectors performance,» *Radio Electronics, Computer Science, Control*, т. 1, № 56, pp. 184-193, 2021.
- [82] D. O. Progonov, «Effectiveness of stego images pre-noising with fractional noise for digital image steganalysis,» *Applied Aspects of Information Technology*, т. 4, № 3, pp. 261-270, 2021.
- [83] D. Progonov та V. Lucenko, «Steganalysis of adaptive embedding methods by message re-embedding into stego images,» *Information Theories and*

- Applications*, т. 27, № 4, pp. 3-24, 2020.
- [84] D. Progonov, «Statistical stegdetectors performance by message re-embedding,» *Theoretical and Applied Cybersecurity*, 2021.
- [85] Y. Tereshchenko та D. Progonov, «Stego images calibration using wavelet transformation,» в *Materials of 7th International Scientific and Technical Conference "Information Protection and Information Systems Security"*, Lviv, 2019.
- [86] Д. О. Прогонов, «Ефективність стегааналізу цифрових зображень у випадку попередньої фільтрації стеганограм, сформованих згідно адаптивних методів MG та MiPOD,» в *Матеріали Міжнародної науково-технічної конференції «Радіотехнічні поля, сигнали, апарати та системи»*, Київ, 2020.
- [87] К. В. Черпахова та Д. О. Прогонов, «Вейвлет-стиснення стеганограм,» в *Матеріали XIV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики»*, Київ, 2016.
- [88] Д. О. Прогонов, «Виявлення стеганограм з використанням методів адаптивної фільтрації цифрових зображень,» в *Праці VIII Міжнародної науково-практичної конференції «Обробка сигналів і негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка: Тези доповідей*, Черкаси, 2021.
- [89] П. П. Яцура та Д. О. Прогонов, «Ефективність використання спеціалізованих методів обробки цифрових зображень для деструкції стеганограм,» в *Матеріали XV Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики»*, Київ, 2017.
- [90] Д. О. Прогонов та П. П. Яцура, «Ефективність варіаційних методів

- шумоподавлення у задачах активного стегааналізу цифрових зображень,» в *Матеріали міжнародної науково-практичної конференції «Безпека інформації в інформаційно-телекомунікаційних системах», Київ, 2017.*
- [91] D. O. Progonov, «Detection Of Stego Images With Adaptively Embedded Data By Component Analysis Methods,» *Advances in Cyber-Physical Systems (ACPS)*, т. 6, № 2, pp. 146-154, 2021.
- [92] М. Б. Яриш та Д. О. Прогонов, «Використання згоркових нейронних мереж для оцінки статистичних характеристик стеганограм,» в *Матеріали XVIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики», Київ, 2020.*
- [93] М. Б. Яриш та Д. О. Прогонов, «Вплив регуляризації нейронної мережі SRNet на точність виявлення стеганограм, сформованих згідно адаптивних методів,» в *Матеріали 25-го Міжнародного форуму «Радіoeлектроніка та молодь в XXI столітті», Харків, 2021.*
- [94] D. Progonov, «Stego Images Decomposition Using Shallow Denoising Autoencoders,» в *International Scientific-Practical Conference “Problems of Infocommunications Science and Technology” (PIC S&T 2021)*, Kharkiv, 2021.
- [95] D. Progonov, «Multi-Datasets Evaluation Of GB-Ras Network Based Stegdetectors Robustness To Domain Adaptation Problem,» *Information Models & Analyses*, т. 28, № 4, pp. 372-396, 2021.
- [96] D. Progonov, «Performance Analysis Of Stego Image Calibration With Usage Of Denoising Autoencoders,» *Advances in Cyber-Physical Systems (ACPS)*, т. 7, № 1, pp. 46-54, 2022.
- [97] Є. М. Терещенко та Д. О. Прогонов, «Методи реконструкції контейнерів з використанням розріджених та надлишкових базисів,» в

Матеріали XVI Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики», Київ, 2018.

- [98] V. Lutsenko та D. Progonov, «Application of the principle of information objects description formalization for the design of information protection systems,» *Eastern-European Journal of Enterprise Technologies*, т. 6, № 9 (120), pp. 28-37, 2022.
- [99] D. Progonov, V. Cherniakova, P. Kolesnichenko та A. Oliynyk, «Behavior-based user authentication on mobile devices in various usage contexts,» *EURASIP J. on Info. Security*, т. 6, 2022.
- [100] D. Progonov, O. Sych, P. Kolesnichenko, V. Cherniakova, A. Oliynyk, V. Prokhorchuk та Y. Yakishyn, «User authentication method and device for executing same». USA Патент US20220350869A1, 2021.
- [101] D. Likhomanov, O. Shchur, A. Oliynyk та D. Progonov, «Electronic device and method of controlling the same». USA Патент US11575514B2, 2021.
- [102] A. Oliynyk, D. Progonov, P. Kolesnichenko, V. Cherniakova, Y. Yakishyn та Y. Lavrenyuk, «Device for protecting content by using biometric information and operating method thereof». WIPO Патент WO2023153637A1, 2023.
- [103] D. Progonov та O. Sokol, «User Authentication on Wearable Devices by Component Analysis of Heartbeat Signals,» в *Who Are You?! Adventures in Authentication Workshop. SOUPS-2021*, 2021.
- [104] D. Progonov та O. Sokol, «Heartbeat-based authentication on smartwatches in various usage contexts,» в *4th Workshop on Emerging Technologies for Authorization and Authentication. European Symposium on Research in Computer Security*, 2021.
- [105] D. Progonov, H. Naumenko, O. Sokol та V. Derkach, «User Authentication on Headset-Like Devices by Bioacoustic Signals,» в *Emerging Technologies*

for Authorization and Authentication. ETAA 2022, 2022.

- [106] P. Kolesnichenko, D. Progonov, V. Cherniakova, A. Oliynyk та O. Sokol, «Biometric-Based Password Management,» в *Security and Trust Management. STM 2023*, Hague, 2023.
- [107] М. Маманчук та Д. Прогонов, «Локалізація позицій стегобітів, вбудованих до зображень-контейнерів з використанням адаптивних стеганографічних методів HUGO та WOW,» в *Всеукраїнська науково-практична конференція “Theoretical and Applied Cybersecurity (TACS-2023)”*, присвячена 100-річному ювілею академіка В.М. Глушкова, Київ, 2023.
- [108] D. Progonov, «Investigation of Digital Image Preprocessing Methods Influence on the Accuracy of Stego Images Detection,» *Visnyk NTUU KPI Serii - Radiotekhnika Radioaparobuduvannia*, т. 89, pp. 54-60, 2022.
- [109] D. Progonov, «Destruction of stego images formed by adaptive embedding methods with dictionary learning methods,» *Theoretical and Applied Cybersecurity*, т. 4, № 1, 2022.
- [110] D. Progonov, «Performance of stego images calibration using advanced denoising methods,» *Information Theories and Applications*, т. 29, № 1, pp. 3-35, 2022.
- [111] K. Lamshöft, T. Neubert, C. Krätzer, C. Vielhauer та J. Dittmann, «Information Hiding in Cyber Physical Systems: Challenges for Embedding, Retrieval and Detection using Sensor Data of the SWAT Dataset,» в *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '21)*, 2021.
- [112] M. Hildebrandt, K. Lamshöft, J. Dittmann, T. Neubert та C. Vielhauer, «Information Hiding in Industrial Control Systems: An OPC UA based Supply Chain Attack and its Detection,» в *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec*

- '20), 2020.
- [113] Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, С. С. Войтусік, А. Я. Горпенюк, О. А. Нємкова, І. М. Журавель, Б. М. Березюк, Є. І. Яковенко, В. І. Отенко та І. Я. Тишик, Інформаційна безпека, Львів: Львівська політехніка, 2019.
- [114] Digimarc Inc., «<http://www.digimarc.com/home>,» Digimarc Inc., New York, 2021.
- [115] MarkAny Inc., «<http://www.markany.com/eng/>,» New York, 2021.
- [116] The Coalition for Content Provenance and Authenticity (C2PA), «Technical specification for multimedia data,» January 2022. [З мережі]. Available: <https://c2pa.org/>. [Дата звернення: May 2022].
- [117] Н. Т. Sencar та N. Мемон, Ред., Digital Image Forensics. There is More to a Picture than Meets the Eye, New York: Springer, 2013, p. 382.
- [118] A. Roček, M. Javorník, K. Slaviček та O. Dostál, «Zero Watermarking: Critical Analysis of Its Role in Current Medical Imaging,» *Digital Imaging*, т. 34, № 1, 7 January 2021.
- [119] DICOM Inc., «<https://www.dicomstandard.org/>,» Boston, 2021.
- [120] «Kaspersky Inc.,» Moscow, 2020.
- [121] A. Shulmin, «Steganography in contemporary cyberattacks,» 3 August 2017. [З мережі]. Available: <https://securelist.com/steganography-in-contemporary-cyberattacks/79276/>. [Дата звернення: 25 October 2021].
- [122] W. Wei, «New Malware Takes Commands From Memes Posted On Twitter,» 18 December 2018. [З мережі]. Available: <https://thehackernews.com/2018/12/malware-twitter-meme.html>. [Дата звернення: 25 October 2021].
- [123] M. Kumar, «Hacking Millions with Just an Image — Recipe: Pixels, Ads & Exploit Kit,» 7 December 2016. [З мережі]. Available: <https://thehackernews.com/2016/12/image-exploit-hacking.html>. [Дата

- звернення: 25 October 2021].
- [124] Kaspersky Inc., «Steganograph in attacks on industrial enterprises,» Kaspersky Inc., Moscow, 2020.
- [125] S. Wendzel, «Get Me Cited, Scotty!: Analysis of Citations in Covert Channel/Steganography Research,» в *ARES 2018: Proceedings of the 13th International Conference on Availability, Reliability and Security*, Hamburg, 2018.
- [126] M. Chen, V. Sedighi, M. Boroumand та J. Fridrich, «JPEG-Phase-Aware Convolutional Neural Network for Steganalysis of JPEG Images,» в *IH&MMSec '17: Proceedings of the 5th ACM Workshop on Information Hiding and Multimedia Security*, New York, 2017.
- [127] A. Cohen, A. Cohen та N. Nissim, «ASSAF: Advanced and Slim StegAnalysis Detection Framework for JPEG images based on deep convolutional denoising autoencoder and Siamese networks,» *Neural Networks*, т. 131, pp. 64-77, 2020.
- [128] Cisco Inc., «Security Outcomes Study,» 2021. [З мережі]. Available: <https://www.cisco.com/c/dam/en/us/products/collateral/security/2020-outcomes-study-main-report.pdf>. [Дата звернення: 26 10 2021].
- [129] S. M. Thampi, «Information Hiding Techniques: A Tutorial Review,» *ISTE-STTP on Network Security & Cryptography*, 2004.
- [130] E. Zielinska, W. Mazurczyk та K. Szczypiorski, «Development Trends in Steganography,» *Communications of the ACM*, т. 57, № 3, pp. 86-95, 2014.
- [131] Y. Yousfi, E. Dworetzky та J. Fridrich, «Detector-Informed Batch Steganography and Pooled Steganalysis,» 2022. [З мережі]. Available: <http://www.ws.binghamton.edu/fridrich/Research/BS-revision-jf.pdf>. [Дата звернення: 03 06 2022].
- [132] T. Denemark та J. Fridrich, «Improving Steganographic Security by Synchronizing the Selection Channel,» в *IH&MMSec '15: Proceedings of*

- the 3rd ACM Workshop on Information Hiding and Multimedia Security*, 2015.
- [133] P. Bas та T. Furon, «Break Our Watermarking System,» Watermarking Virtual Laboratory (Wavila) of the European Network of Excellence ECRYPT, July 2007. [З мережі]. Available: <http://bows2.ec-lille.fr/index.php?mode=VIEW&tmpl=credits>. [Дата звернення: 15 April 2022].
- [134] R. Cograanne, Q. Giboulot та P. Bas, «The ALASKA Steganalysis Challenge: A First Step Towards Steganalysis,» в *IH&MMSec'19: Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, New York, 2019.
- [135] V. Holub, J. Fridrich та T. Denemark, «Universal distortion function for steganography in an arbitrary domain,» *EURASIP Journal on Information Security*, т. 1, № 1, 2014.
- [136] A. Joseph та K. Anusudha, «Robust Watermarking Based on DWT-SVD,» *International Journal on Signal&Image Security*, т. 1, № 1, 2013.
- [137] M. Khan, M. Rahman та I. Sarker, «Digital Watermarking for Image Authentication Based on Combined DCT, DWT and SVD Transformation,» *International Journal of Computer Science Issues*, т. 10, № 3, 2013.
- [138] A. Elahian, M. Khalili та S. Shokouhi, «Improved robust DWT–watermarking in YCbCr color space,» *Global journal of computer application and technology*, т. 1, № 3, pp. 300-304, 2011.
- [139] B. L. Gunjal та S. N. Mali, «Secured color image watermarking technique in DWT-DCT domain,» *International Journal of Computer Science, Engineering and Information Technology*, т. 1, № 3, pp. 36-44, 2011.
- [140] J. Nance, «Periods of the discretized Arnold Cat Map and its extension to N dimensions,» *ArXiv preprints*, pp. 1-11, 2011.
- [141] R. C. Gonzalez та R. E. Woods, *Digital Image Processing*, 4th edition ред.,

- London: Pearson, 2017, p. 1192.
- [142] S. Mallat, *A Wavelet Tour of Signal Processing: The Sparse Way*, 3rd edition ред., New York: Academic Press, 2008, p. 832.
- [143] S. J. Prince, *Computer Vision: Models, Learning, and Inference*, 1st edition ред., Cambridge: Cambridge University Press, 2012, p. 598.
- [144] K. P. Murphy, *Machine Learning: A Probabilistic Perspective*, Cambridge: The MIT Press, 2012, p. 1104.
- [145] D. Progonov та S. Kushch, «Passive Steganalysis of Multidomain Embedding Methods,» *Information Theories & Applications*, т. 22, № 1, pp. 86-99, 2015.
- [146] Д. А. Прогонов та С. Н. Куш, «Спектральный анализ стеганограмм,» *Радиоэлектроника, информатика, управление*, т. 2, № 33, pp. 71-81, 2015.
- [147] T. Filler та J. Fridrich, «Gibbs Construction in Steganography,» *IEEE Transactions on Information Forensics and Security*, т. 5, № 4, pp. 705-720, 2010.
- [148] S. Bernard, P. Bas, T. Pevný та J. Klein, «Optimizing Additive Approximations of Non-additive Distortion Functions,» в *Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '21)*, 2021.
- [149] C. Kin-Cleaves та A. D. Ker, «Simulating Suboptimal Steganographic Embedding,» в *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '20)*, 2020.
- [150] J. Butora, Y. Yousfi та J. Fridrich, «Turning Cost-Based Steganography into Model-Based,» в *Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security (IH&MMSec '20)*, 2020.
- [151] V. Sedighi та J. Fridrich, «Effect of saturated pixels on security of steganographic schemes for digital images,» в *International Conference on*

- Image Processing (ICIP)*, Phoenix, 2016.
- [152] V. Sedighi, J. Fridrich та R. Cogranne, «Content-adaptive pentary steganography using the multivariate generalized Gaussian cover model,» в *Media Watermarking, Security, and Forensics*, San Francisco, 2015.
- [153] V. Sedighi, R. Cogranne та J. Fridrich, «Content-Adaptive Steganography by Minimizing Statistical Detectability,» *Transactions on Information Forensics and Security*, т. 11, № 2, 2015.
- [154] T. Denmark та J. Fridrich, «Model Based Steganography with Precover,» *Electronic Imaging*, т. 7, pp. 56-66, 2017.
- [155] T. Denmark, P. Bas та J. Fridrich, «Natural Steganography in JPEG Compressed Images,» в *IS&T, Electronic Imaging, Media Watermarking, Security, and Forensics*, Burlingame, 2018.
- [156] T. Filler, J. Judas та J. Fridrich, «Minimizing Additive Distortion in Steganography Using Syndrome-Trellis Codes,» *Transactions on Information Forensics and Security*, т. 6, № 3, pp. 920-935, 2011.
- [157] B. Li, M. Wang, X. Li, S. Tan та J. Huang, «A Strategy of Clustering Modification Directions in Spatial Image Steganography,» *Transactions on Information Forensics and Security*, т. 10, № 9, pp. 1905-1917, 2015.
- [158] D. Progonov та M. Yarysh, «Analyzing The Accuracy Of Detecting Steganograms Formed By Adaptive Steganographic Methods When Using Artificial Neural Networks,» *Eastern-European Journal of Enterprise Technologies*, т. 1, № 9 (115), pp. 45-55, 2022.
- [159] J. Kodovsky та J. Fridrich, «Calibration revisited,» в *Multimedia and Security Workshop*, Princeton, 2009.
- [160] Д. А. Прогонов та С. Н. Куш, «Мультифрактальный флуктуационный анализ стеганограмм,» *Системные исследования и информационные технологии*, т. 4, pp. 39-47, 2015.
- [161] F. Li, X. Zhang, H. Cheng та J. Yu, «Digital image steganalysis based on

- local textural features and double dimensionality reduction,» *Security and communication networks*, 2014.
- [162] D. D. Shankar та V. K. Shukla, «Effect of Principal Component Analysis in Feature based Uncalibrated Steganalysis using Block Dependency,» *SSRN Electronic Journal*, 2019.
- [163] А. А. Большаков та Р. Н. Каримов, Методы обработки многомерных данных и временных рядов, Москва: Горячая линия-Телеком, 2007, р. 522.
- [164] J. Lwowski, I. Corley та J. Hoffman, «Neural Steganalysis with Spatial Rich Models for Image Steganography Detection,» 2020. [3 мережі]. Available: https://www.techrxiv.org/articles/preprint/Neural_Steganalysis_with_Spatial_Rich_Models_for_Image_Steganography_Detection/11949762/1. [Дата звернення: 10 11 2021].
- [165] Y. Qian, J. Dong, W. Wang та T. Tan, «Deep learning for steganalysis via convolutional neural networks,» в *Proc. IS T Int. Symp. Electron. Imag. (EI)*, 2015.
- [166] F. Y. He, S. P. Zhong та K. Z. Chen, «JPEG Steganalysis Based on Feature Fusion by Principal Component Analysis,» *Applied Mechanics and Materials*, pp. 2933-2938, 2012.
- [167] S. Dasgupta та A. Gupta, «An elementary proof of a theorem of Johnson and Lindenstrauss,» *Random Structures & Algorithms*, т. 22, pp. 60-65, 2003.
- [168] X. Lv та Z. Wang, «An Extended Image Hashing Concept: Content-Based Fingerprinting Using FJLT,» *EURASIP Journal on Information Security*, 2009.
- [169] N. Ailon та B. Chazelle, «Approximate nearest neighbors and the fast johnson-lindenstrauss transform,» в *Proceedings of the 38th Annual Symposium on the Theory of Computing (STOC '06)*, Seattle, 2006.

- [170] B.-I. Adi та T. Greville, *Generalized inverses: Theory and applications*, New York: Springer, 2003.
- [171] J. Dunn, «Well-Separated Clusters and Optimal Fuzzy Partitions,» *Journal of Cybernetics*, т. 4, № 1, pp. 95-104, 1974.
- [172] T. Caliński та J. Harabasz, «A dendrite method for cluster analysis,» *Communications in Statistics*, т. 3, № 1, pp. 1-27, 1974.
- [173] C. C. Aggarwal, *Data Mining*, Luxembourg: Springer, 2015.
- [174] V. Holub та J. Fridrich, «Random Projections of Residuals for Digital Image Steganalysis,» *Transactions on Information Forensics and Security*, т. 8, № 12, pp. 1996-2006, 2013.
- [175] T. Pevny та J. Fridrich, «Merging Markov and DCT features for multi-class JPEG steganalysis,» в *Security, Steganography, and Watermarking of Multimedia Contents IX*, San Jose, 2007.
- [176] J. Kodovský та J. Fridrich, «Steganalysis of JPEG images using rich models,» в *Media Watermarking, Security, and Forensics*, San Francisco, 2012.
- [177] T. Denemark, V. Sedihi, V. Holub, R. Cogranne та J. Fridrich, «Selection-channel-aware rich model for Steganalysis of digital images,» в *International Workshop on Information Forensics and Security (WIFS)*, Atlanta, 2014.
- [178] M. Goljan, J. Fridrich та R. Cogranne, «Rich model for Steganalysis of color images,» в *International Workshop on Information Forensics and Security (WIFS)*, Atlanta, 2014.
- [179] V. Holub та J. Fridrich, «Low-Complexity Features for JPEG Steganalysis Using Undecimated DCT,» *Transactions on Information Forensics and Security*, т. 10, № 2, pp. 219-228, 2015.
- [180] M. Goljan та J. Fridrich, «CFA-aware features for steganalysis of color images,» в *Media Watermarking, Security, and Forensics*, San Francisco,

- 2015.
- [181] P. Singh, V. K. Verma та P. Rai, «HetConv: heterogeneous kernel-based convolutions for deep CNNs,» Cornell University, Cornell, 2019.
- [182] G. Xu, H.-Z. Wu та Y. Q. Shi, «Ensemble of CNNs for steganalysis: An empirical study,» в *Workshop Inf. Hiding Multimedia Secur.*, Atlanta, 2016.
- [183] M. Procházka, Z. Oplatková, J. Holoska та V. Gerlich, «Optimization Of Neural Network Inputs By Feature Selection Methods,» в *ECMS-2011*, 2011.
- [184] J. Ye, J. Ni та Y. Yi, «Deep Learning Hierarchical Representations for Image Steganalysis,» *Transactions on Information Forensics and Security*, т. 12, № 11, pp. 2545-2557, 2017.
- [185] K. He, X. Zhang, S. Ren та J. Sun, «Spatial Pyramid Pooling in Deep Convolutional Networks for Visual Recognition,» *Transactions on Pattern Analysis and Machine Intelligence*, т. 37, № 9, pp. 1904-1916, 2015.
- [186] E. Bisong, «Regularization for Deep Learning,» *Building Machine Learning and Deep Learning Models on Google Cloud Platform*, pp. 415-421, 2019.
- [187] Z. Jin, Y. Yu, Y. Chen та Y. Chen, «IAS-CNN: Image adaptive steganalysis via convolutional neural network combined with selection channel,» *International Journal of Distributed Sensor Networks*, т. 16, № 3, 2020.
- [188] Y. Xu, Z. Fu, G. Xu, S. Zhang та X. Xie, «DRHNet: A Deep Residual Network Based on Heterogeneous Kernel for Steganalysis,» *Secur. Commun. Networks*, т. 20, 2020.
- [189] J. Yang, K. Liu, X. Kang, E. K. Wong та Y.-Q. Shi, «Spatial image steganography based on generative adversarial network,» Cornell University, Cornell, 2018.
- [190] G. Xu, H.-Z. Wu та Y.-Q. Shi, «Structural design of convolutional neural networks for steganalysis,» *Signal Process. Lett.*, т. 23, № 5, pp. 708-712, 2016.

- [191] M. Yedroudj, F. Comby та M. Chaumont, «Yedroudj-Net: An efficient CNN for spatial steganalysis,» в *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, 2018.
- [192] B. Jähne, H. Scharr, S. Körkel, H. Haußecker та P. Geißler, «Principles of Filter Design,» в *Handbook of Computer Vision and Applications*, Academic Press, 1999, pp. 125-151.
- [193] Y. Bengio, *Learning Deep Architectures for AI*, New York: Now Foundations and Trends, 2009.
- [194] R. A. Mallikarjuna, R. K. Sudheer, R. K. Srinivasa та R. C. Sudharshan, «Efficient steganalysis using convolutional auto encoder network to ensure original image quality,» *PeerJ Computer Science*, т. 7, 2021.
- [195] «Image Steganography Using Auto Encoder-Decoder Based Deep Learning Method,» в *International Conference on Interactive Collaborative and Blended Learning*, 2020.
- [196] D. Shullani, M. Fontani, M. Iuliani, O. Al Shaya та A. Piva, «VISION: a video and image dataset for source identification,» *EURASIP Journal on Information Security*, т. 15, 2017.
- [197] M. Huiskes та M. Lew, «The MIR Flickr Retrieval Evaluation,» в *ACM International Conference on Multimedia Information Retrieval*, 2008.
- [198] J. S. Lim, *Two-Dimensional Signal and Image Processing*, 1st edition ред., Prentice Hall PTR, 1989.
- [199] A. D. Ker, T. Pevný, J. Kodovský та J. Fridrich, «The square root law of steganographic capacity,» в *Proceedings of the 10th ACM workshop on Multimedia and security (MM&Sec '08)*, 2008.
- [200] A. D. Ker, «Estimating Steganographic Fisher Information in Real Images,» в *International Workshop on Information Hiding*, 2009.
- [201] J. Kodovský та J. Fridrich, «Steganalysis in high dimensions: fusing classifiers built on random subspaces,» в *Proceedings of Media*

- Watermarking, Security, and Forensics*, San Francisco, 2011.
- [202] J. Kodovsky, J. Fridrich та V. Holub, «Ensemble Classifiers for Steganalysis of Digital Media,» *Trans. Inf. Forensics Security*, т. 7, № 2, pp. 432-444, 2012.
- [203] D. Chicco та G. Jurman, «The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation,» *BMC Genomics*, т. 21, 2020.
- [204] Н. Н. Красильников, Цифровая обработка 2D- и 3D-изображений, Санкт-Петербург: БХВ-Петербург, 2011.
- [205] T.-S. Reinel, A.-A. H. Brayan, B.-O. M. Alejandro, M.-R. Alejandro, A.-G. Daniel, A.-G. J. Alejandro, B.-J. A. Buenaventura, O.-A. Simon, I. Gustavo та R.-P. Raúl, «Repository of GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis,» [з мережі]. Available: <https://github.com/BioAITeam/Steganalysis>. [Дата звернення: 20 4 2022].
- [206] V. Holub та J. Fridrich, «Designing steganographic distortion using directional filters,» в *International Workshop on Information Forensics and Security (WIFS)*, Costa Adeje, 2012.
- [207] S. Z. Li, *Markov Random Field Modeling in Image Analysis*, New York: Springer, 2009, p. 384.
- [208] C. M. Bishop, *Pattern Recognition and Machine Learning*, New York: Springer, 2016, p. 758.
- [209] Y. Yousfi, J. Butora, J. Fridrich та C. F. Tsang, «Improving EfficientNet for JPEG Steganalysis,» в *Proceedings of the Workshop on Information Hiding and Multimedia Security (IH&MMSec '21)*, 2021.
- [210] H. Jang, T.-W. Oh та K. Kim, «Feature Aggregation Networks for Image Steganalysis,» в *Proceedings of the Workshop on Information Hiding and Multimedia Security (IH&MMSec '20)*, 2020.

- [211] J. G. Dowty, «Chentsov's theorem for exponential families,» *Information Geometry*, т. 1, p. 117–135, 2018.
- [212] S.-i. Amari та H. Nagaoka, «Chentsov's theorem and some historical remarks,» в *Methods of Information Geometry*, New York, Oxford University Press, 2000, pp. 37-40.
- [213] T. M. Cover та J. A. Thomas, *Elements of Information Theory*, 2nd ed. ред., Hoboken: John Wiley & Sons, 2006.
- [214] F. Liese та I. Vajda, «On divergences and informations in statistics and information theory,» *IEEE Transactions on Information Theory*, т. 52, № 10, pp. 4394-4412, 2006.
- [215] A. W. v. d. Vaart, *Asymptotic Statistics*, Cambridge: Cambridge University Press, 1998.
- [216] L. Le Cam та G. Lo Yang, *Asymptotics in Statistics: Some Basic Concepts*, Springer, 2000.
- [217] D. A. Cieslak, T. R. Hoens, N. V. Chawla та W. P. Kegelmeyer, «Hellinger distance decision trees are robust and skew-insensitive,» *Data Mining and Knowledge Discovery*, т. 24, pp. 136-158, 2012.
- [218] C. Cachin, «An information-theoretic model for steganography,» *Information and Computation*, т. 192, № 1, pp. 41-56, 2004.
- [219] S. Katzenbeisser та F. A. P. Petitcolas, «Defining security in steganographic systems,» в *Proc. SPIE 4675, Security and Watermarking of Multimedia Contents IV*, 2002.
- [220] N. J. Hopper, J. Langford та L. von Ahn, «Provably Secure Steganography,» *Cryptology ePrint Archive*, 2002.
- [221] W. Zhang та S. Li , «Security Measurements of Steganographic Systems,» в *International Conference on Applied Cryptography and Network Security*, 2004.
- [222] R. Anderson, «Stretching the limits of steganography,» в *International*

- Workshop on Information Hiding (IH-1996)*, 1996.
- [223] M. Yoan, P. Bas та L. Amaury, «Using multiple re-embeddings for quantitative steganalysis and image reliability estimation,» Aalto University, Aalto, 2010.
- [224] M. Elad, *Sparse and Redundant Representations: From Theory to Applications in Signal and Image Processing*, Berlin: Springer, 2010.
- [225] Y. C. Eldar та G. Kutyniok, *Compressed Sensing: Theory and Applications*, Cambridge: Cambridge University Press, 2012.
- [226] P. Comon та C. Jutten, *Handbook of Blind Source Separation: Independent Component Analysis and Applications*, Cambridge: Academic Press, 2010.
- [227] A. Cichocki та S.-i. Amari, *Adaptive Blind Signal and Image Processing*, New York: Wiley, 2002.
- [228] C. R. S. Rao та M. V. Prasad, *Digital Watermarking Techniques in Curvelet and Ridgelet Domain*, Berlin: Springer, 2016.
- [229] M. Aharon, M. Elad та A. Bruckstein, «K-SVD: An algorithm for designing overcomplete dictionaries for sparse representation,» *IEEE Transactions on Signal Processing*, т. 54, № 11, pp. 4311-4322, 2006.
- [230] K. Engan, S. O. Aase та J. Hakon Husoy, «Method of optimal directions for frame design,» в *International Conference on Acoustics, Speech and Signal Processing*, Phoenix, 1999.
- [231] L. Pardo, *Statistical Inference Based on Divergence Measures*, Chapman and Hall/CRC, 2005, p. 512.
- [232] A. E. Ilesanmi та T. O. Ilesanmi , «Methods for image denoising using convolutional neural network: a review,» *Complex & Intelligent Systems volume*, т. 7, p. 2179–2198, 2021.
- [233] Д. Мак-Доналд, *Введение в физику шумов и флуктуаций*, Москва: Мир, 1964.
- [234] Е. С. Вентцель та Л. А. Овчаров, *Теория вероятностей и её инженерные*

- приложения, 2-е ред., Москва: Высшая школа, 2000, p. 480.
- [235] К. Ikeuchi, Ред., *Computer Vision*, Boston: Springer Science+Business Media, 2014.
- [236] М. Weissman, « $1/f$ noise and other slow, nonexponential kinetics in condensed matter,» *Reviews of Modern Physics*, т. 60, № 2, pp. 537-571, 1988.
- [237] К. Perlin, «An Image Synthesizer,» *Computer Graphics*, т. 19, № 3, pp. 287-296, 1985.
- [238] А. Buades, «A non-local algorithm for image denoising,» *Computer Vision and Pattern Recognition*, т. 2, p. 60–65, 2005.
- [239] L. Birgé та P. Massart, «From Model Selection to Adaptive Estimation,» в *Festschrift for Lucien Le Cam: Research Papers in Probability and Statistics*, E. Torgersen, D. Pollard та G. Yang, Ред., New York, Springer-Verlag, 1997, p. 55–88.
- [240] L. I. Rudin, S. Osher та E. Fatemi, «Nonlinear total variation based noise removal algorithms,» *Physica D*, т. 60, p. 259–268, 1992.
- [241] А. Chambolle, «An algorithm for total variation minimization and applications,» *Journal of Mathematical Imaging and Vision*, т. 20, p. 89–97, 2004.
- [242] P. Getreuer, «Rudin-Osher-Fatemi Total Variation Denoising using Split Bregman,» *Image Processing On Line*, т. 2, pp. 74-95, 2012.
- [243] А. А. Miranda, Y.-A. Le Borgne та G. Bontempi, «New Routes from Minimal Approximation Error to Principal Components,» *Neural Processing Letters*, т. 27, № 3, pp. 197-207, 2008.
- [244] P. Chou, T. Lookabaugh та R. Gray, «Entropy-constrained vector quantization,» *IEEE Transactions on Acoustics, Speech, and Signal Processing*, т. 37, № 1, pp. 31-42, 1989.
- [245] Д. О. Прогонов та С. М. Куш, «Варіограмний аналіз стеганограм,

- сформованих на основі комплексних методів приховання даних,» *Вісник Національного університету «Львівська політехніка». Серія «Комп'ютерні системи та мережі», т. 806, pp. 226-232, 2014.*
- [246] Н. В. Кошкіна, «Стеганоанализ бесключевых стеганосистем на основе атаки контрольным внедрением,» *Международный научно-технический журнал «Проблемы управления и информатики», № 6, pp. 137-144, 2014.*
- [247] Н. В. Кошкіна, «Стеганоанализ изображений в формате jpeg на базе атаки контрольным внедрением,» *Управляющие системы и машины, № 4, pp. 3-17, 2014.*
- [248] В. Ю. Корольов, В. В. Поліновський, В. А. Герасименко та М. Л. Горінштейн, «Планування досліджень методів стеганографії та стегоаналізу,» *Вісник Хмельницького національного університету, № 4, pp. 187-195, 2011.*
- [249] L. Guo, J. Ni та Y. Q. Shi, «An efficient JPEG steganographic scheme using uniform embedding,» в *International Workshop on Information Forensics and Security (WIFS), Costa Adeje, 2012.*
- [250] B. Li, M. Wang, J. Huang та X. Li, «A new cost function for spatial image steganography,» в *International Conference on Image Processing (ICIP), Paris, 2014.*
- [251] D.-T. Dang-Nguyen, C. Pasquini, V. Conotter та G. Boato, «RAISE: a raw images dataset for digital image forensics,» в *The 6th Multimedia Systems Conference (MMSys '15), 2015.*
- [252] I. Krasin, T. Duerig, N. Alldrin, V. Ferrari, S. Abu-El-Haija, A. Kuznetsova, H. Rom, J. Uijlings, S. Popov, S. Kamali, M. Mallocci, J. Pont-Tuset, A. Veit, S. Belongie, V. Gomes, A. Gupta, C. Sun, G. Chechik, D. Cai, Z. Feng, D. Narayanan та K. Murphy, «OpenImages: A public dataset for large-scale multi-label and multi-class image classification,» 2017. [3

мережі].

Available:

<https://storage.googleapis.com/openimages/web/index.html>.

[Дата

звернення: 02 May 2022].

- [253] O. Ronneberger, P. Fischer та T. Brox, «U-Net: Convolutional Networks for Biomedical Image Segmentation,» Cornell University Repository (ArXiv), Cornell, 2015.
- [254] T. Sørensen, «A method of establishing groups of equal amplitude in plant sociology based on similarity of species and its application to analyses of the vegetation on Danish commons,» *Kongelige Danske Videnskabernes Selskab*, т. 5, № 4, pp. 1-34, 1948.
- [255] Daylight Chemical Information Systems, Inc., «Fingerprints - Screening and Similarity,» Daylight Chemical Information Systems, Inc., 2019.

ДОДАТОК А СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях

1. **Прогонов Д.О.** Аналіз змін χ^2 -квадрат відстані між розподілами яскравості пікселів при фільтрації зображень-контейнерів та стеганограм [Текст] / **Прогонов Д.О.** // Вісник Національного технічного університету України «Київський політехнічний інститут». Серія «Радіотехніка. Радіоапаратобудування». – 2018. – № 75. – с.54–60. – DOI: <https://doi.org/10.20535/RADAP.2018.75.54-60>. (Фахове видання, індексується базою даних **Web of Science**).

2. **Прогонов Д.О.** Аналіз змін χ^2 -квадрат відстані між розподілами яскравості пікселів при фільтрації стеганограм, сформованих згідно методу UNIWARD [Текст] / **Прогонов Д.О.** // Вісник Національного технічного університету України «Київський політехнічний інститут». Серія – Радіотехніка. Радіоапаратобудування. – № 76, 2019. – с.72-76. – DOI: <https://doi.org/10.20535/RADAP.2019.76.72-76>. (Фахове видання, індексується базою даних **Web of Science**).

3. **Progonov D.** Statistical stegdetectors performance by message re-embedding [Text] / **Progonov D.** // Theoretical and Applied Cybersecurity, Vol.3, No. 1, 2021. – pp. 5-14. – DOI: <https://doi.org/10.20535/tacs.2664-29132021.-1.251291> (Фахове видання категорії «Б»).

4. **Progonov D.O.** Influence of digital images preliminary noising on statistical stegdetectors performance [Text] / **D. Progonov** // Radio Electronics, Computer Science, Control. – Vol. 1(56). – 2021. – p. 184-193. – DOI: <https://doi.org/10.15588/1607-3274-2021-1-18> (Фахове видання категорії «А», індексується базою даних **Web of Science**).

5. **Progonov D.O.** Detection Of Stego Images With Adaptively Embedded Data By Component Analysis Methods [Text] / **Progonov D.O.** // Advances in

Cyber-Physical Systems (ACPS). Vol. 6, Number 2. – 2021. – pp. 146-154. – DOI: <https://doi.org/10.23939/acps2021.02.146> (Фахове видання категорії «Б»).

6. **Progonov D.O.** Effectiveness of stego images pre-noising with fractional noise for digital image steganalysis [Text] / **Progonov D.O.** // Applied Aspects of Information Technology. – Vol. 4, issue 3, pp. 261-270. – 2021. – DOI: <https://doi.org/10.15276/aait.03.2021.5>. (Фахове видання категорії «Б»).

7. **Progonov Dmytro.** Effectiveness of stego image calibration via feature vectors re-projection into high-dimensional spaces [Text] / **Progonov Dmytro** // Radio Electronics, Computer Science, Control. Vol. 2 (61). – 2022. – pp. 165-174. – DOI: <https://doi.org/10.15588/1607-3274-2022-2-16>. (Фахове видання категорії «А», індексується базою даних **Web of Science**).

8. **Progonov Dmytro.** Investigation of Digital Image Preprocessing Methods Influence on the Accuracy of Stego Images Detection [Text] / **Progonov Dmytro** // Visnyk NTUU KPI Serii A - Radiotekhnika Radioaparaturbuduvannia, Vol. (89). – 2022. – pp. 54-60. DOI: <https://doi.org/10.20535/RADAP.2022.89.54-60> (Фахове видання категорії «А», індексується базою даних **Web of Science**).

9. **Progonov Dmytro.** Effectiveness of stego images pre-processing with spectral analysis methods [Text] / **Progonov Dmytro, Lutsenko Volodymyr** // Applied Aspects of Information Technology, Vol. 5, No. 1. – 2022. – pp. 64-75. – DOI: <https://doi.org/10.15276/aait.01.2022.6>. (Фахове видання категорії «Б»).
Особистий внесок: аналітичний огляд сучасних методів попередньої обробки цифрових зображень в задачах стегааналізу, аналіз отриманих експериментальних даних точності виявлення стеганограм при використанні методів вейвлет-аналізу та декомпозиції сигналу із застосуванням складних систем функцій).

10. **Progonov Dmytro.** Performance Analysis Of Stego Image Calibration With Usage Of Denoising Autoencoders [Text] / **Progonov Dmytro** // Advances in Cyber-Physical Systems (ACPS). Volume 7, Number 1. – 2022. – pp. 46-54, DOI: <https://doi.org/10.23939/acps2022.01.046>. (Фахове видання категорії «Б»).

11. **Progonov Dmytro**. Destruction of stego images formed by adaptive embedding methods with dictionary learning methods [Text] / **Progonov Dmytro** // Theoretical and Applied Cybersecurity. Vol. 4 No. 1. – 2022. – DOI: <https://doi.org/10.20535/tacs.2664-29132022.1.254883> (Фахове видання категорії «Б»).

12. **Dmytro Progonov**. Statistical Steganalysis of Multistage Embedding Methods [Text] / **Dmytro Progonov** // Information Theories and Applications. – Volume 5, Number 1. – 2016. – pp. 23-36. (Фахове видання).

13. **Dmytro Progonov**. Multiclass detector for modern steganographic methods [Text] / **Dmytro Progonov** // Information Theories and Applications. – Vol. 24, No. 3. – 2017. – pp. 55-71. (Фахове видання).

14. **Dmytro Progonov**. Information-Theoretic Estimations of Cover Distortion by Adaptive Message Embedding [Text] / **Dmytro Progonov** // Information Theories and Applications. Vol. 25, No. 1. – 2018. – pp. 47-62. (Фахове видання).

15. **Dmytro Progonov**. Analysis of changes the Renyi divergence for pixel brightness distributions by stego images Wiener filtering [Text] / **Dmytro Progonov** // Information Technologies and Knowledge, Vol. 12, No. 2. – 2018. – pp. 3-25. (Фахове видання).

16. **Progonov D.** Steganalysis of adaptive embedding methods by message re-embedding into stego images [Text] / **D. Progonov**, V. Lucenko // Information Theories and Applications, Vol. 27, Issue 4. – 2020. – pp. 3-24. (Фахове видання). *Особистий внесок: порівняльний аналіз точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при проведенні попередньої обробки досліджуваних зображень шляхом повторного вбудовування стегоданих).*

17. **Progonov D.** Multi-Datasets Evaluation Of GB-Ras Network Based Stegdetectors Robustness To Domain Adaptation Problem [Text] / **Progonov D.** // Information Theories and Applications. Volume 28, Number 4. – 2021. – pp. 372-396. (Фахове видання).

18. **Progonov Dmytro**. Performance of stego images calibration using advanced denoising methods [Text] / **Progonov Dmytro** // Information Theories and Applications, Vol. 29, Issue 1. – 2022. – pp. 3-35. – DOI: <https://doi.org/10.54521/ijita29-01-p01>. (Фахове видання).

**Статті у виданнях, віднесених до першого - третього квартилів (Q1-Q3)
відповідно до класифікації SCImago Journal and Country Rank або
Journal Citation Reports**

19. Progonov Dmytro. Analyzing The Accuracy Of Detecting Steganograms Formed By Adaptive Steganographic Methods When Using Artificial Neural Networks [Text] / Progonov Dmytro, Yarysh Mariia // Eastern-European Journal of Enterprise Technologies. – Vol. 1, Issue 9 (115). – 2022. – pp.45-55. – DOI: <https://doi.org/10.15587/1729-4061.2022.251350>. (Фахове видання категорії «А», **Scopus** Q3. *Особистий внесок: аналітичний огляд сучасних методів виявлення стеганограм з використанням штучних нейронних мереж, аналіз отриманих експериментальних даних щодо точності виявлення стеганограм з використання новітніх типів стегадетекторів*).

20. Lutsenko Volodymyr. Application of the principle of information objects description formalization for the design of information protection systems [Text] / Lutsenko Volodymyr, Dmytro Progonov // Eastern-European Journal of Enterprise Technologies, Vol. 6 (9 (120)). – 2022. – pp 28–37. – DOI: <https://doi.org/10.15587/1729-4061.2022.269030>. (Фахове видання категорії «А», **Scopus** Q3. *Особистий внесок: аналітичний огляд сучасних методів стегааналізу цифрових даних та їх застосування для побудови комплексних систем захисту інформації*).

21. Progonov Dmytro. Behavior-based user authentication on mobile devices in various usage contexts [Text] / Progonov Dmytro, Valentyna Cherniakova, Pavlo Kolesnichenko, Andriy Oliynyk // EURASIP J. on Info. Security, Vol. 6. – 2022. – DOI: <https://doi.org/10.1186/s13635-022-00132-x>. (**Scopus** Q2. *Особис-*

тий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів).

Матеріали, що додатково відображають результати дисертації

22. Конахович Г.Ф. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних [Текст] / Конахович Г.Ф., **Прогонов Д.О.**, Пузиренко О.Ю. – Підручник. – Київ: «Центр учбової літератури», 2018. – 558 с. – ISBN 978-617-673-741-4. (*Особистий внесок: теоретичні та експериментальні дослідження ефективності використання спеціальних методів структурного аналізу сигналів в задачах виявлення стеганограм, запропоновані методи виявлення стеганограм з даними, вбудованими з використанням багатоступінчастих стеганографічних методів).*

Патенти на винахід

23. User authentication method and device for executing same (2021). Inventors: **Dmytro Progonov**, Oleh Sych, Pavlo Kolesnichenko, Valentyna Cherniakova, Andriy Oliynyk, Veronika Prokhorchuk, Yevhenii Yakishyn. Assignee: Samsung Electronics Co Ltd. (*Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів.* Ідентифікатор документу в міжнародних системах індексації патентів: US20220350869A1 (USA), WO2021149882A1 (WIPO), KR20210095282A (Republic of Korea)).

24. Electronic device and method of controlling the same (2021). Inventors: Dmytro Likhomanov, Oleksandr Shchur, Andriy Oliynyk, **Dmytro Progonov**. Assignee: Samsung Electronics Co Ltd. (*Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів.* Ідентифікатор документу в міжнародних системах індексації патентів: US11575514B2 (USA), US20210320798A1 (USA), KR20210125655A (Republic of Korea)).

25. Device for protecting content by using biometric information and operating method thereof (2023). Inventors: Andriy Oliynyk, **Dmytro Progonov**, Pavlo Kolesnichenko, Valentyna Cherniakova, Yevhenii Yakishyn, Yaroslav

Lavrenyuk. Assignee: Samsung Electronics Co Ltd. (*Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів*). Ідентифікатор документу в міжнародних системах індексації патентів: WO2023153637A1 (WIPO), PCT/KR2022/021652 (Republic of Korea)).

Матеріали конференцій

26. **Прогонов Д.О.** Ефективність універсального стегодетектору Фаріда при вбудовуванні даних у цифрові зображення згідно адаптивних методів [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 20-26 березня, 2017. – с. 266-268;

27. **Прогонов Д.О.** Вплив невідповідності областей приховання повідомлень та проведення стеогоаналізу на ефективність статистичних стегодетекторів [Текст] / **Прогонов Д.О.** // XIX Міжнародна науково-технічна конференція «Системний аналіз та інформаційні технології». – Київ, 22-25 травня, 2017. – ННК «ІПСА», НТУУ «КПІ ім. Ігоря Сікорського» – с. 317-318;

28. Дорошенко А.В. Виявлення стеганограм з використанням авторегресійних моделей зображення-контейнеру [Текст] / Дорошенко А.В., **Прогонов Д.О.** // VI міжнародна науково-практична конференція «Обробка сигналів та негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка. – Черкаси: ЧДТУ, 2017. – с. 209-211. (*Особистий внесок: удосконалено виявлення стеганограм з даними, вбудованими в області перетворення зображення-контейнеру, на основі аналізу параметрів авторегресійних моделей кореляції значень яскравості суміжних пікселів цифрових зображень*).

29. **Прогонов Д.О.** Ефективність універсальних стегодетекторів у випадку використання адаптивних методів формування стеганограм [Текст] / **Прогонов Д.О.**, Богайчук В.О., Терещенко Є.М. // VI міжнародна науково-практична конференція «Обробка сигналів та негаусівських процесів», присвяченої пам'яті професора Ю.П. Кунченка. – Черкаси: ЧДТУ, 2017. – с.

232-234. *(Особистий внесок: аналіз експериментальних даних щодо точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні новітніх типів універсальних стегадетекторів).*

30. Дорошенко А.В. Визначення параметрів стеганограм з використанням авторегресійних моделей цифрових зображень [Текст] / Дорошенко А.В., **Прогонов Д.О.** // XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 25-27 травня 2017 р. – К.: ВПІ ВПК «Політехніка», 2017. – с. 123-125. *(Особистий внесок: метод оцінки ступеня заповнення зображення-контейнеру стегаданими за величиною зміни параметрів авторегресійних моделей цифрових зображень, обумовлених прихованням повідомлень до зображення-контейнеру).*

31. Яцура П.П. Ефективність використання спеціалізованих методів обробки цифрових зображень для деструкції стеганограм [Текст] / Яцура П.П., **Прогонов Д.О.** // XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 25-27 травня 2017 р. – К.: ВПІ ВПК «Політехніка», 2017. – с. 150-152. *(Особистий внесок: аналіз експериментальних даних щодо ступеня деструкції стеганограм, сформованих згідно багатоетапним стеганографічних методів, при використанні методів компонентного аналізу сигналів).*

32. **Прогонов Д.О.** Ефективність варіаційних методів шумоподавлення у задачах активного стегааналізу цифрових зображень [Текст] / **Прогонов Д.О.**, Яцура П.П. // Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». – Київ, 25-26 травня 2017 р. – НДЦ «Тезіс», НТУУ «КПІ ім. Ігоря Сікорського», 2017. – с. 217. *(Особистий внесок: запропоновано метод деструкції стеганограм з даними, вбудованими в частотній області зображення-контейнеру, з викорис-*

танням варіаційних методів шумоподавлення при збереженні статистичних параметрів оброблюваних зображень).

33. **Прогонов Д.О.** Виявлення стеганограм, сформованих комплексними методами, з використанням стегодетектора Фаріда [Текст] / **Прогонов Д.О.**, Голубничий В.О. // Міжнародна науково-практична конференція «Безпека інформації в інформаційно-телекомунікаційних системах». – Київ, 25-26 травня 2017 р. – НДЦ «Тезіс», НТУУ «КПІ ім. Ігоря Сікорського», 2017. – с. 218. (*Особистий внесок: удосконалено універсальний стегодетектор Фаріда для виявлення стеганограм, сформованих згідно комплексних стеганографічних методів*).

34. **Прогонов Д.О.** Порівняльний аналіз точності виявлення стеганограм при використанні статистичних моделей цифрових зображень [Текст] / **Прогонов Д.О.**, Сівкович П.О., Могиліна Ю.В. // Міжнародна науково-практична конференція «Захист інформації і безпека інформаційних систем». – Львів, 1-2 червня 2017 р. – Видавництво Львівської політехніки, 2017. – с. 101-102. (*Особистий внесок: аналіз експериментальних даних щодо точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні сучасних статистичних моделей зображення-контейнеру*).

35. Богайчук В. Виявлення стеганограм, сформованих згідно адаптивного методу SI-UNIWARD, з використанням універсальних стегодетекторів [Текст] / Богайчук В., Терещенко Є., **Прогонов Д.** // Міжнародна науково-практична конференція «Захист інформації і безпека інформаційних систем». – Львів, 1-2 червня 2017 р. – Видавництво Львівської політехніки, 2017. – с. 105-106. (*Особистий внесок: запропоновано метод підвищення точності роботи сучасних стегодетекторів для виявлення стеганограм, сформованих згідно стеганографічного методу SI-UNIWARD*).

36. Голубничий В. Вплив вибору базисних функцій вейвлет-перетворення на ефективність стегодетектору Фаріда [Текст] / Голубничий В., **Прогонов Д.** // Міжнародна науково-практична конференція «Захист

інформації і безпека інформаційних систем». – Львів, 1-2 червня 2017 р. – Видавництво Львівської політехніки, 2017. – с. 107-108. (*Особистий внесок: запропоновано метод підвищення точності виявлення стеганограм при використанні універсального стегодетектору Фаріда шляхом вибору оптимальних базисних функцій вейвлет-перетворення за критерієм мінімізації помилки виявлення стеганограм*).

37. **Progonov Dmytro**. Structural Stegdetector Performance in case of Side-Informed Message Embedding [Text] / **Progonov Dmytro** // 4th IEEE International Conference “Problems of Infocommunications Science and Technology”. – Kharkiv, 10-13 October, 2017. – pp. 232-236. – DOI: 10.1109/INFO-COMMST.2017.8246386.

38. Бука М.А. Деструкція прихованих повідомлень шляхом масштабування контейнеру [Текст] / Бука М.А., **Прогонов Д.О.** // International Research and Practice Conference “Modern Methods, Innovations, and Experience of Practical Application in the Field of Technical Sciences”. – 27-28 December 2017, Radom, Poland. – pp. 9-13. (*Особистий внесок: удосконалено метод деструкції прихованих повідомлень шляхом використання спеціальних методів масштабування цифрових зображень*).

39. **Прогонов Д.О.** Теоретико-інформаційні оцінки спотворень контейнерів при формуванні стеганограм [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 19-25 березня 2018. – с. 273-275.

40. Богайчук В.О. Деструкція стеганограм з використанням методу головних компонент [Текст] / Богайчук В.О., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 113-115. (*Особистий внесок: удосконалено метод надійної деструкції стеганограм при мінімізації змін статистичних параметрів зображення-контейнеру*).

41. Остапюк Н.В. Виявлення стеганограм з використанням ріджлет-перетворення [Текст] / Остапюк Н.В., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 127-129. (*Особистий внесок: запропоновано метод деструкції стеганограм при використанні новітніх методів вейвлет-аналізу, заснованих на застосуванні спеціальних типів вейвлетів*).

42. Терещенко Є.М. Методи реконструкції контейнерів з використанням розріджених та надлишкових базисів [Текст] / Терещенко Є.М., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 138-141. (*Особистий внесок: запропоновано методи оцінки статистичних параметрів зображення-контейнеру за наявними зашумленими даними з використанням математичного апарату складних систем функцій*).

43. Чайка Д.В. Виявлення стеганограм, сформованих згідно адаптивних методів, з використанням статистичної моделі PHARM [Текст] / Чайка Д.В., **Прогонов Д.О.** // XVI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Том. 1 – Київ, 26-27 квітня 2018 р. – ВПІ ВПК «Політехніка». – с. 144-146. (*Особистий внесок: аналіз результатів експериментального дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі PHARM*).

44. **Прогонов Д.О.** Теоретико-інформаційні оцінки стійкості методів UNIWARD до стегоаналізу [Текст] / **Прогонов Д.О.** // XX Міжнародна науково-технічна конференція «Системний аналіз та інформаційні технології». –

Київ, 21-24 травня, 2018. – ННК «ІПСА», НТУУ «КПІ ім. Ігоря Сікорського» – с. 256.

45. Yulia Mohylina. Stego images destruction using a decomposition in the basis formed using K-SVD algorithm [Text] / Yulia Mohylina, **Dmytro Progonov**, Vladyslav Bohaichuk // 7th International Scientific and Technical Conference “Information Protection and Information Systems Security”. – Lviv, 30-31 May 2019. – pp. 98-99. (*Особистий внесок: запропоновано метод надійної деструкції прихованих повідомлень при збереженні мінімальних візуальних змін зображення-контейнеру із застосуванням математичного апарату спеціальних систем функцій*).

46. Yelizaveta Tereshchenko. Stego images calibration using wavelet transformation [Text] / Yelizaveta Tereshchenko, **Dmytro Progonov** // 7th International Scientific and Technical Conference “Information Protection and Information Systems Security”. – Lviv, 30-31 May 2019. – pp. 106-107. (*Особистий внесок: порівняльний аналіз точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при проведенні попередньої обробки цифрових зображень з використанням вейвлет-стиснення*).

47. **Прогонов Д.О.** Аналіз точності виявлення стеганограм, сформованих адаптивними методами, при додатковому зашумленні зображень-контейнерів [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 18-24 листопада 2019. – с. 225-227

48. Яриш М.Б. Використання згоркових нейронних мереж для оцінки статистичних характеристик стеганограм [Текст] / Яриш М.Б., **Прогонов Д.О.** // XVIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні та прикладні проблеми фізики, математики та інформатики». – Київ, 12-13 травня 2020 р. – ВПІ ВПК «Політехніка». – с. 132-134. (*Особистий внесок: аналіз експериментальних результатів дослідження точності виявлення стеганограм, сформованих згідно адап-*

тивних стеганографічних методів, при використанні сучасних стегодетекторів на основі згорткових нейронних мереж).

49. **Progonov Dmytro**. Performance of Statistical Stegdetectors in Case of Small Number of Stego Images in Training Set [Text] / **Progonov Dmytro** // IEEE International Scientific-Practical Conference “Problems of Infocommunications Science and Technology”. – Kharkiv, 2020. (індексується базою даних **Scopus**)

50. **Прогонов Д.О.** Вплив попереднього зашумлення на точність виявлення стеганограм, сформованих згідно адаптивних методів MG та MiPOD [Текст] / **Прогонов Д.О.** // X Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». – Запоріжжя: Запорізький національний технічний університет, 2020. – с. 167-168;

51. **Прогонов Д.О.** Ефективність стегоаналізу цифрових зображень у випадку попередньої фільтрації стеганограм, сформованих згідно адаптивних методів MG та MiPOD [Текст] / **Прогонов Д.О.** // Міжнародна науково-технічна конференція «Радіотехнічні поля, сигнали, апарати та системи». – Київ, 16-22 листопада 2020.

52. Яриш М.Б. Вплив регуляризації нейронної мережі SRNet на точність виявлення стеганограм, сформованих згідно адаптивних методів [Текст] / Яриш М.Б., **Прогонов Д.О.** // XXV Міжнародний форум «Радіоелектроніка та молодь в XXI столітті», м. Харків, 20-21 квітня 2021 р. – с. 138-139. (*Особистий внесок: аналіз експериментальних даних точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, в залежності від застосовуваних методів регуляризації параметрів нейронної мережі SRNet*).

53. **Dmytro Progonov**. Stego Images Decomposition Using Shallow Denoising Autoencoders [Text] / **Dmytro Progonov** // IEEE International Conference “Problems of Infocommunications Science and Technology”. – Kharkiv, 2021. (індексується базою даних **Scopus**)

54. **Прогонов Д.О.** Виявлення стеганограм з використанням методів адаптивної фільтрації цифрових зображень [Текст] / **Прогонов Д.О.** // VIII Міжнародна науково-практична конференція «Обробка сигналів і негаусівських процесів», присвячена пам'яті професора Ю.П. Кунченка. [Електронний ресурс] – Черкаси: ЧДТУ, 2021 с. 192-194.

55. Маманчук М.М. Локалізація позицій стегобітів, вбудованих до зображень-контейнерів з використанням адаптивних стеганографічних методів HUGO та WOW [Text] / Маманчук М.М., **Прогонов Д.О.** // Всеукраїнська науково-практична конференція “Theoretical and Applied Cybersecurity (TACS-2023)”, присвячена 100-річному ювілею академіка В.М. Глушкова. КПІ ім. Ігоря Сікорського НН ФТІ. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2023. – ISBN 978-966-990-083-8 – с. 42-45. *(Особистий внесок: запропоновано представлення задачі локалізації позиції пікселів зображення-контейнеру, використаних для приховання стегобітів повідомлення, як еквівалентної задачі сегментації зображень з використанням штучних нейронних мереж).*

ДОДАТОК Б ДОКУМЕНТИ, ЩО ПІДТВЕРДЖУЮТЬ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ

«ЗАТВЕРДЖУЮ»

директор з інформаційної безпеки,
Самсунг РнД Інститут Україна,
український центр досліджень та
розробок Samsung, к.ф.-м.н.

Можонько Олександр Анатолійович



«08» грудня 2023 року

АКТ

впровадження результатів досліджень дисертаційної роботи
Прогонова Дмитра Олександровича на тему «Структурний синтез та параметрична
оптимізація методів побудови стегодетекторів для цифрових зображень» на здобуття
наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту
інформації

Підрозділ із досліджень та розробок у галузі кібербезпеки Самсунг РнД Інститут Україна інформує, що, у контексті вирішення завдань щодо обробки мультимедійних даних, були використані результати дисертаційної роботи Прогонова Д.О. за темою «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень».

При виконанні робіт Підрозділу із досліджень та розробок у галузі кібербезпеки були використані запропоновані Прогоновим Д.О. процедури синтезу надлишкових систем функцій для обробки цифрових зображень. Особливістю даних процедур є забезпечення високої якості відновлення вихідного виду зображення за наявною (зашумленою) копією при збереженні малої тривалості процедури обробки. Застосування даних процедур дозволило підвищити якість попередньої обробки цифрових зображень для вирішення задач знешумлення, перевірки цілісності та аутентичності зображень. Розглянуті та запропоновані у дисертаційній роботі методи використано і при розробці пропозицій щодо майбутніх проектів.

к.т.н., старший інженер
Самсунг РнД Інститут Україна,
керівник лабораторії "Security AI"

Сінельнікова Ольга Ігорівна

«07» грудня 2023 року

ЗАТВЕРДЖУЮ
 Начальник Управління оперативного зв'язку та електронних комунікацій ДСНС України



Сергій МИЦЮК
 _____ 2022 р.


АКТ
 впровадження результатів дисертаційної роботи
 Прогонова Дмитра Олександровича

Управління оперативного зв'язку та електронних комунікацій ДСНС України інформує, що у рамках вирішення завдань щодо стеганоаналізу цифрових зображень у моделі пасивного порушника були використані результати дисертаційної роботи докторанта Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Прогонова Д.О. за темою «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень».

Запропоновані в дисертаційній роботі методи синтезу універсальних стегодетекторів для цифрових зображень, що засновані на розкладі (декомпозиції) досліджуваних зображень із застосуванням надлишкових систем функцій, дають змогу з високою точністю виявляти широкий клас стеганографічних методів в умовах обмеженості апріорних даних щодо використаних методів приховання повідомлень та значної варіативності статистичних і спектральних параметрів зображень-контейнерів.

Реалізація напрацювань дисертаційної роботи Прогонова Д.О. дозволила отримувати важливу інформацію, що стосується оцінки статистичних та спектральних параметрів зображення-контейнеру за наявними (зашумленими) даними та визначення пікселів контейнеру, використаних для вбудовування бітів повідомлення. Отримані результати планується використовувати в подальшій роботі Управління оперативного зв'язку та електронних комунікацій ДСНС України.

Начальник відділу спеціальних досліджень та захисту державних інформаційних ресурсів Управління оперативного зв'язку та електронних комунікацій ДСНС України


 Олександр МИКОЛАЄНКО



УКРАЇНА
 МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
 НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
 «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
 ОСОБЛИВЕ КОНСТРУКТОРСЬКЕ БЮРО «ШТОРМ»

03056, Київ-56
 вул. Політехнічна, 16, корп.11

Тел. (044) 204-90-16
 Тел./факс (044) 236-20-91
 sipulka@kpi.ua

Висновок

Про застосування наукових розробок доцента кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського Прогонова Дмитра Олександровича, що були розроблені при підготовці матеріалів дисертаційної роботи на тему «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень» на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

В період 2017 – 2018 років ОКБ «Шторм» виконував два контракти в інтересах Інозамовника. Перший контракт передбачав розробку комплексу програмного забезпечення та методики лабораторних випробувань малогабаритної гідроакустичної станції (Договір комісії №USE-16.2-101-D/K-18 від 18.06.2018 року). Другий контракт передбачав розробку конструкторської документації на повітряні акустичні екрани та методик натурних випробувань Гідроакустичної станції (Договір комісії №USE-16.2-98-D/K-18 від 18.06.2018 року).

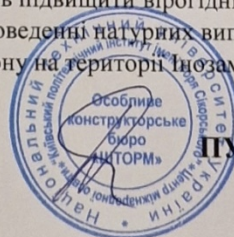
Обидва контракти передбачали розробку алгоритмів аналізу гідроакустичних сигналів в реальному часі частотно-фазового та частотно-амплітудного простору надводних та підводних об'єктів, що знаходились в межах морського випробувального полігону. Частотно-фазовий та частотно-амплітудний простір фактично представляє собою цифрове 3D зображення гідроакустичних сигналів, аналіз яких дає можливість виявляти, ідентифікувати та класифікувати морські об'єкти в ближній та дальній зоні (від сотень метрів до сотень кілометрів). Саме для розробки таких алгоритмів і було застосовані матеріали наукової дисертації Прогонова Д.О., а саме:

- розробка математичного апарату методів синтезу та параметричної оптимізації високоточних детекторів слабких локальних збурень статистичних, спектральних та структурних параметрів цифрових зображень;
- розробка методів локалізації положення слабких локальних збурень на цифрових зображеннях в умовах обмеженості апріорних даних щодо параметрів джерела збурень.

Інтеграція вказаних наукових матеріалів Прогонова Д.О. в програмне забезпечення обробки гідроакустичних сигналів дало можливість підвищити вірогідність виявлення надводних та підводних морських об'єктів при проведенні натурних випробувань гідроакустичної станції в умовах морського полігону на території Інозамовника, особливо по такому параметру як класифікація.

Головний інженер ОКБ «Шторм»

ПУХА Сергій



«ЗАТВЕРДЖУЮ»

Декан
 механіко-математичного
 факультету
 Київського національного
 університету імені Тараса
 Шевченка
 Оксана БЕЗУЦЬКА



« 20 вересня » 2022 року

АКТ

впровадження результатів досліджень дисертаційної роботи
 Прогонова Дмитра Олександровича на тему «Структурний синтез та
 параметрична оптимізація методів побудови стегодетекторів для цифрових
 зображень» на здобуття наукового ступеня доктора технічних наук за
 спеціальністю 05.13.21 – системи захисту інформації

Науково-методична комісія механіко-математичного факультету Київського національного університету імені Тараса Шевченка цим Актом засвідчує, що результати досліджень дисертаційної роботи Прогонова Дмитра Олександровича на тему «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень» впроваджені у навчальний процес кафедри алгебри і комп'ютерної математики. Запропоновані Прогоновим Д.О. методи побудови стегодетекторів для виявлення несанкціонованої передачі інформації з обмеженим доступом в умовах обмеженості апріорних даних щодо типу та параметрів стеганографічних методів використовуються при викладанні навчальної дисципліни «Криптографічні протоколи».

Голова
 науково-методичної комісії
 механіко-математичного факультету,
 професор

Андрій ОЛІЙНИК

«ЗАТВЕРДЖУЮ»

Декан Факультету
аеронавігації, електроніки та
телекомунікацій

Національного авіаційного
університету

Сергій ЗАВГОРОДНІЙ



« 14 » листопада 2022 року

АКТ

впровадження результатів досліджень дисертаційної роботи
Проконова Дмитра Олександровича на тему «Структурний синтез та
параметрична оптимізація методів побудови стегодетекторів для цифрових
зображень» на здобуття наукового ступеня доктора технічних наук за
спеціальністю 05.13.21 – системи захисту інформації

Методична Рада ФАЕТ, цим Актом засвідчує, що результати дослідже-
нь дисертаційної роботи Проконова Дмитра Олександровича на тему
«Структурний синтез та параметрична оптимізація методів побудови
стегодетекторів для цифрових зображень» впроваджені у навчальний процес
кафедри Телекомунікаційних та радіоелектронних систем. Розроблені
Проконовим Д.О. методи повідомлень, несанкціоновано вбудованих до
цифрових зображень, а також методи визначення позицій пікселів
зображень-контейнерів, використаних для приховання бітів повідомлення,
застосовуються при викладанні навчальної дисципліни «Захист інформації в
інформаційно-телекомунікаційних системах критичних інфраструктур»,
«Безпека інформаційних мереж та систем», «Захист безпроводних
телекомунікаційних та радіотехнічних систем».

Завідувач кафедри ТКРС

Роман ОДАРЧЕНКО

« 14 » листопада 2022 року

«ЗАТВЕРДЖУЮ»

Директор Навчально-наукового
Фізико-технічного інституту
Національного технічного
університету України
«Київський політехнічний
інститут імені Ігоря Сікорського»
Олексій НОВІКОВ



«18» січня 2024 року


АКТ


впровадження результатів досліджень дисертаційної роботи
Проконова Дмитра Олександровича на тему «Структурний синтез та
параметрична оптимізація методів побудови стегодетекторів для цифрових
зображень» на здобуття наукового ступеня доктора технічних наук за
спеціальністю 05.13.21 – системи захисту інформації

Методична комісія Навчально-наукового Фізико-технічного інституту, затверджена розпорядженням №44/2023 ввід 16 жовтня 2023 року, цим Актом засвідчує, що результати досліджень дисертаційної роботи Проконова Дмитра Олександровича на тему «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень» впроваджені у навчальний процес кафедри інформаційної безпеки. Запропоновані Проконовим Д.О. методи обробки та класифікації складних сигналів, побудови стегодетекторів для виявлення несанкціонованої передачі інформації з обмеженим доступом в умовах обмеженості апріорних даних щодо типу та параметрів стегаграфічних методів використовуються при викладанні навчальних дисциплін «Основи стегааналізу мультимедійних даних», «Основи структурного аналізу сигналів», «Вейвлет-аналіз сигналів» та «Захист конфіденційної інформації з використанням методів машинного навчання».

Голова Методичної комісії,
к.ф.-м.н., доцент

Зав. кафедри інформаційної
безпеки, д.т.н., професор


Сергій СМІРНОВ


Дмитро ЛАНДЕ

«16» січня 2024 року

ДОДАТОК В РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ТОЧНОСТІ ВИЯВЛЕННЯ СТЕГANOГРАМ, СФОРМОВАНИХ ЗГІДНО АДАПТИВНИХ СТЕГANOГРАФІЧНИХ МЕТОДІВ, ПРИ ВИКОРИСТАННІ СТАТИСТИЧНИХ МОДЕЛЕЙ ЦИФРОВИХ ЗОБРАЖЕНЬ

Для дослідження точності роботи сучасних методів статистичного стегааналізу при обробці стеганограм, сформованих згідно адаптивних стегаанографічних методів, було проведено налаштування стегадетекторів SD_{SPAM} та $SD_{maxSRMd2}$. Дані СД засновані на застосуванні, відповідно, статистичних моделей SPAM та maxSRMd2. Зважаючи на високу складність налаштування $SD_{maxSRMd2}$, розглянуто випадок використання лише фільтру високих частот типу EDGE (стегадетектор $SD_{maxSRMd2-EDGE}$), що має найбільший вплив на точність виявлення стеганограм за результатами дослідження [177].

Ступінь заповнення зображення-контейнеру стегаданними змінювалася в наступному діапазоні – 3%, 5%, 10%, 20%, 30%, 40% та 50%. Формування стеганограм проводилося згідно адаптивних стегаанографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153].

Аналіз точності роботи СД проводився згідно стандартної процедури перехресної перевірки [144]. В якості тестового пакету цифрових зображень використано стандартні пакети ALASKA [134], VISION [196] та MIRFlickr [197]. Зважаючи на суттєві відмінності у кількості зображень в даних пакетах ЦЗ, в роботі були використані псевдовипадкові вибірки 10,000 цифрових зображень для кожного пакету.

Проведено аналіз змін точності роботи СД для наступних випадків:

- Наявність у вибірці \mathcal{S}_{train} пари ЗК та відповідних їм стеганограм ($K_{\alpha}^{OL} = 0\%$) – відповідає випадку, що широко використовується при проведенні досліджень в галузі стегааналізу, а саме використання апріорних даних щодо особливостей АСМ при налаштуванні СД.

- Наявність у вибірці \mathcal{S}_{train} лише окремих пар ЗК та відповідних їм стеганограм ($K_{\alpha}^{OL} \sim \mathcal{U}(0; 100)$) – відповідає поширеній практичній ситуації, коли стегоаналітик може використовувати лише низку пар ЗК та відповідних їм стеганограм при налаштуванні СД.
- Відсутність у вибірці \mathcal{S}_{train} зображень-контейнерів, використаних для формування стеганограм ($K_{\alpha}^{OL} = 0\%$) – відповідає найбільш складному випадку проведення стегоаналізу (проблема zero day), коли стегоаналітик не має можливості формувати стеганограми для довільного ЗК.

Для інтегральної оцінки точності роботи досліджуваних стегодетекторів SD_{SPAM} , $SD_{maxSRMd2}$ та $SD_{maxSRMd2-EDGE}$ в роботі були використані наступні метрики якості: помилки першого P_{FP} та другого P_{FN} роду, F_1 -індекс (1.27) та коефіцієнт кореляції Метьюса (1.28). Для оцінки середньої значення та розкиду значень даних показників процедура перехресної перевірки [144] повторювалася десять разів при розбитті тестового пакету зображень на навчальну (70%) та контрольну (30%) вибірки.

Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індекс та коефіцієнт кореляції Метьюса при використанні стегодетекторів SD_{SPAM} , $SD_{maxSRMd2}$ та $SD_{maxSRMd2-EDGE}$ для методів HUGO, S-UNIWARD, MG та MiPOD наведені у додатках В.1-В.3.

В.1 Результати дослідження точності виявлення стеганогам, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі SPAM цифрових зображень

Таблиця В.1а – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегадетектору SD_{SPAM} для виявлення стеганогам, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,8	49,8	49,3	48,4	47,1	45,7	44,2	52,2	52,8	51,8	51,3	49,7	47,7	46,1	56,1	56,2	56,5	55,5	52,2	50,2	47,9
	σ	0,13	0,09	0,14	0,24	0,16	0,21	0,34	1,17	1,73	0,42	0,55	0,45	0,38	0,31	1,27	0,65	0,62	0,47	1,03	0,57	0,57
$P_{FN}, \%$	μ	49,8	49,7	49,1	47,9	45,9	43,7	41,8	52,3	53,0	52,0	51,4	49,5	46,9	44,8	55,7	56,7	56,5	55,3	52,4	50,2	47,5
	σ	0,15	0,11	0,17	0,27	0,37	0,46	0,33	1,10	1,79	0,59	0,39	0,65	0,63	0,63	1,45	0,69	0,86	0,60	1,12	0,58	0,84
F_1	μ	0,49	0,47	0,48	0,48	0,49	0,51	0,53	0,47	0,46	0,47	0,47	0,47	0,49	0,51	0,45	0,42	0,43	0,45	0,47	0,49	0,50
	σ	0,02	0,02	0,01	0,02	0,02	0,01	0,01	0,07	0,02	0,03	0,04	0,03	0,03	0,01	0,03	0,02	0,02	0,01	0,02	0,01	0,01
MCC	μ	0,00	0,00	0,02	0,04	0,07	0,10	0,14	-0,04	-0,06	-0,04	-0,03	0,01	0,05	0,09	-0,12	-0,13	-0,13	-0,11	-0,05	0,00	0,05
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,04	0,01	0,01	0,01	0,01	0,01	0,03	0,01	0,01	0,01	0,02	0,01	0,01

Таблиця В.16 – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,8	49,5	48,8	47,2	45,3	43,5	41,8	51,8	52,3	52,3	50,0	47,4	45,3	43,1	56,3	56,7	55,5	52,7	49,3	46,7	44,1
	σ	0,17	0,11	0,14	0,17	0,26	0,40	0,31	0,63	1,46	1,18	0,66	0,44	0,49	0,61	0,92	1,11	0,72	0,75	0,53	0,65	0,63
$P_{FN}, \%$	μ	49,8	49,3	48,6	45,5	42,8	39,1	35,6	51,6	52,6	52,6	50,0	46,1	41,5	38,5	56,2	56,3	55,7	52,9	49,0	46,0	42,0
	σ	0,14	0,15	0,29	0,45	0,67	0,95	1,11	0,78	1,26	1,39	0,82	0,59	1,87	1,67	1,12	1,05	0,75	0,59	0,77	0,91	0,86
F_1	μ	0,48	0,47	0,49	0,47	0,50	0,52	0,54	0,50	0,45	0,46	0,48	0,47	0,49	0,53	0,44	0,44	0,44	0,46	0,47	0,51	0,53
	σ	0,05	0,03	0,02	0,02	0,02	0,02	0,01	0,04	0,03	0,03	0,03	0,04	0,04	0,03	0,02	0,02	0,02	0,01	0,02	0,02	0,01
MCC	μ	0,00	0,01	0,03	0,07	0,12	0,17	0,22	-0,03	-0,05	-0,05	0,00	0,06	0,12	0,18	-0,12	-0,13	-0,11	-0,06	0,02	0,07	0,14
	σ	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,03	0,03	0,01	0,01	0,01	0,01	0,02	0,02	0,01	0,01	0,01	0,01	0,01

Таблиця В.1в – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,9	49,6	49,2	47,8	46,4	44,8	43,0	52,7	52,4	51,8	50,5	48,5	46,4	44,5	56,6	56,3	55,8	53,5	51,6	48,3	45,9
	σ	0,12	0,13	0,11	0,24	0,29	0,21	0,37	1,67	0,81	0,80	0,39	0,50	0,45	0,41	1,19	1,26	1,00	0,95	0,78	0,68	0,68
$P_{FN}, \%$	μ	49,8	49,6	48,9	47,2	44,9	42,4	39,9	52,8	52,6	52,0	50,6	48,0	45,5	42,8	56,5	56,2	56,0	53,7	51,6	48,0	45,2
	σ	0,13	0,18	0,26	0,32	0,52	0,52	0,73	1,58	1,10	0,96	0,40	0,81	1,09	0,64	0,95	1,17	0,87	0,88	0,78	0,97	0,97
F_1	μ	0,49	0,48	0,48	0,50	0,50	0,52	0,54	0,46	0,46	0,46	0,48	0,49	0,52	0,53	0,43	0,44	0,43	0,46	0,48	0,50	0,53
	σ	0,02	0,03	0,02	0,01	0,01	0,01	0,01	0,03	0,03	0,04	0,02	0,02	0,02	0,02	0,01	0,02	0,02	0,02	0,01	0,01	0,02
MCC	μ	0,00	0,01	0,02	0,05	0,09	0,13	0,17	-0,06	-0,05	-0,04	-0,01	0,03	0,08	0,13	-0,13	-0,12	-0,12	-0,07	-0,03	0,04	0,09
	σ	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,03	0,02	0,02	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,02	0,02	0,02	0,02

Таблиця В.1г – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,7	49,7	49,2	48,1	46,7	45,1	43,8	52,5	53,2	51,8	50,7	48,5	46,8	45,1	56,5	56,2	55,8	53,7	51,7	49,1	46,3
	σ	0,15	0,18	0,18	0,13	0,22	0,27	0,31	1,42	1,25	0,87	0,46	0,20	0,32	0,43	0,78	0,94	0,92	1,12	1,07	0,59	0,83
$P_{FN}, \%$	μ	49,7	49,6	48,8	47,0	44,8	42,0	38,6	52,9	53,4	51,8	50,8	48,0	45,3	42,3	56,7	55,9	56,0	53,9	51,8	48,7	45,0
	σ	0,17	0,22	0,36	0,53	0,68	0,45	0,92	1,49	1,43	0,90	0,46	0,49	0,86	1,16	0,77	1,35	1,06	1,02	1,14	1,03	1,27
F_1	μ	0,49	0,48	0,45	0,46	0,48	0,50	0,51	0,45	0,46	0,48	0,46	0,48	0,49	0,51	0,43	0,45	0,44	0,45	0,47	0,48	0,51
	σ	0,02	0,04	0,03	0,02	0,02	0,02	0,01	0,04	0,03	0,03	0,04	0,02	0,03	0,02	0,02	0,03	0,02	0,02	0,02	0,02	0,03
MCC	μ	0,01	0,01	0,02	0,05	0,08	0,12	0,17	-0,05	-0,07	-0,04	-0,01	0,03	0,08	0,12	-0,13	-0,12	-0,12	-0,08	-0,04	0,02	0,09
	σ	0,00	0,00	0,00	0,01	0,01	0,00	0,01	0,03	0,03	0,02	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,02	0,02	0,02

Таблиця В.1д – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,4	48,4	45,4	39,4	34,4	31,1	28,8	52,3	52,5	47,8	40,5	35,6	31,9	29,7	55,7	55,0	50,2	41,7	36,6	32,9	29,7
	σ	0,07	0,17	0,26	0,45	0,85	0,47	0,66	0,88	0,55	0,35	0,49	0,59	0,80	0,85	0,93	0,99	0,56	0,69	0,72	0,63	0,82
$P_{FN}, \%$	μ	49,3	48,4	45,0	36,9	32,1	27,7	24,5	52,2	52,7	47,7	39,3	33,4	29,5	25,0	55,6	55,1	50,2	41,6	35,4	30,1	26,6
	σ	0,09	0,18	0,51	0,62	0,82	0,74	0,97	0,89	0,49	0,42	0,81	0,96	0,94	1,13	0,73	1,21	0,53	0,35	0,91	0,76	0,94
F_1	μ	0,49	0,51	0,54	0,60	0,65	0,69	0,72	0,48	0,46	0,52	0,59	0,64	0,68	0,71	0,44	0,45	0,50	0,58	0,63	0,67	0,71
	σ	0,01	0,02	0,01	0,01	0,01	0,00	0,01	0,04	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01
MCC	μ	0,01	0,03	0,10	0,24	0,33	0,41	0,46	-0,04	-0,05	0,05	0,20	0,31	0,39	0,45	-0,11	-0,10	0,00	0,17	0,28	0,37	0,44
	σ	0,00	0,00	0,00	0,00	0,01	0,00	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,01	0,01	0,01	0,01	0,01

Таблиця В.1е – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	46,5	43,4	38,4	39,3	27,5	24,6	22,8	49,9	46,0	39,4	40,4	27,7	25,1	23,4	52,5	48,2	40,8	41,7	28,4	25,9	23,4
	σ	0,22	0,39	0,50	0,26	0,57	0,46	0,62	0,48	0,48	0,74	0,45	1,13	0,83	0,71	0,43	0,59	0,79	0,55	1,02	0,98	1,42
$P_{FN}, \%$	μ	46,1	43,3	36,2	37,1	24,6	21,6	18,9	49,9	45,8	38,8	39,2	25,7	22,2	19,2	52,5	48,2	39,9	40,6	26,0	22,2	20,0
	σ	0,31	0,41	0,63	0,50	0,75	0,61	0,59	0,51	0,63	0,57	0,94	1,30	1,11	1,38	0,43	0,61	0,78	0,93	1,69	1,27	1,68
F_1	μ	0,52	0,56	0,61	0,60	0,73	0,76	0,78	0,49	0,53	0,60	0,59	0,73	0,76	0,78	0,48	0,52	0,59	0,57	0,72	0,75	0,77
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,02	0,01	0,01	0,01	0,01	0,01
MCC	μ	0,07	0,13	0,25	0,24	0,48	0,54	0,58	0,00	0,08	0,22	0,20	0,47	0,53	0,57	-0,05	0,04	0,19	0,18	0,45	0,52	0,56
	σ	0,00	0,00	0,01	0,00	0,00	0,01	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01

Таблиця В.1ж – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	48,4	46,9	43,2	37,2	33,3	30,4	28,7	51,9	51,0	45,6	38,7	34,3	31,0	29,2	54,9	53,6	47,9	39,6	35,3	32,3	30,4
	σ	0,17	0,14	0,31	0,49	0,33	0,53	0,55	0,77	0,37	0,45	0,62	1,00	0,99	0,74	0,94	0,53	0,85	0,91	0,78	0,94	0,90
$P_{FN}, \%$	μ	48,3	46,8	42,4	35,3	30,6	27,5	24,9	52,0	51,0	45,4	36,8	31,3	29,1	26,3	55,0	53,9	47,7	38,6	33,6	29,2	26,8
	σ	0,17	0,29	0,45	0,77	0,71	0,51	0,78	0,91	0,38	0,49	0,79	1,17	1,02	1,45	0,80	0,57	0,90	0,38	1,58	1,69	1,13
F_1	μ	0,51	0,53	0,56	0,62	0,67	0,70	0,72	0,47	0,48	0,54	0,61	0,66	0,69	0,71	0,45	0,45	0,51	0,60	0,65	0,68	0,70
	σ	0,02	0,01	0,01	0,01	0,00	0,00	0,00	0,04	0,02	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,01	0,01	0,01	0,01
MCC	μ	0,03	0,06	0,14	0,27	0,36	0,42	0,46	-0,04	-0,02	0,09	0,24	0,34	0,40	0,44	-0,10	-0,07	0,04	0,22	0,31	0,38	0,43
	σ	0,00	0,00	0,00	0,00	0,01	0,00	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,02	0,01	0,01	0,01	0,01

Таблиця В.1и – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	46,1	43,4	38,2	32,8	29,2	26,9	25,3	49,9	45,9	39,1	33,5	29,7	27,4	25,4	53,2	48,3	41,0	34,2	30,2	28,0	25,9
	σ	0,30	0,36	0,53	0,69	0,48	0,40	0,65	0,39	0,31	0,87	0,49	0,89	0,80	0,76	0,58	0,61	0,72	0,64	0,91	1,05	1,14
$P_{FN}, \%$	μ	46,1	42,9	36,6	29,7	25,9	23,4	20,9	49,9	45,9	39,0	31,3	27,0	24,3	22,4	53,2	48,2	40,5	32,8	28,9	25,2	22,8
	σ	0,29	0,31	0,63	0,59	0,64	0,71	1,04	0,40	0,35	0,76	0,92	0,69	0,94	1,32	0,50	0,67	0,93	0,48	1,11	1,29	0,87
F_1	μ	0,54	0,56	0,61	0,67	0,71	0,74	0,76	0,49	0,54	0,61	0,66	0,71	0,73	0,75	0,47	0,51	0,59	0,66	0,70	0,72	0,75
	σ	0,01	0,01	0,01	0,01	0,00	0,00	0,00	0,02	0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01
MCC	μ	0,08	0,14	0,25	0,37	0,45	0,50	0,54	0,00	0,08	0,22	0,35	0,43	0,48	0,52	-0,06	0,04	0,18	0,33	0,41	0,47	0,51
	σ	0,00	0,00	0,01	0,01	0,00	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01

Таблиця В.1к – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,9	49,7	49,5	48,1	46,2	44,0	41,6	53,6	52,3	52,6	52,4	49,3	46,2	43,2	57,2	56,7	56,2	55,4	52,6	48,3	45,1
	σ	0,13	0,14	0,19	0,17	0,17	0,26	0,34	1,38	1,28	1,53	0,69	0,33	0,39	0,41	0,45	0,65	1,40	0,32	0,57	0,61	0,53
$P_{FN}, \%$	μ	49,9	49,7	49,5	48,2	45,9	42,9	38,7	53,7	52,5	52,4	52,4	49,4	46,1	41,7	57,1	56,9	56,3	55,5	52,5	48,3	44,6
	σ	0,13	0,14	0,17	0,13	0,30	0,35	0,55	1,29	1,21	1,45	0,63	0,34	0,44	0,50	0,68	0,58	1,06	0,41	0,48	0,63	0,62
F_1	μ	0,49	0,49	0,51	0,53	0,53	0,55	0,56	0,46	0,46	0,48	0,47	0,51	0,53	0,55	0,43	0,43	0,43	0,44	0,48	0,52	0,54
	σ	0,02	0,02	0,01	0,01	0,01	0,01	0,01	0,04	0,04	0,03	0,02	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01
MCC	μ	0,00	0,01	0,01	0,04	0,08	0,13	0,19	-0,07	-0,05	-0,05	-0,05	0,01	0,08	0,15	-0,14	-0,14	-0,13	-0,11	-0,05	0,03	0,10
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,03	0,02	0,03	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01

Таблиця В.1л – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апіорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,8	49,6	48,8	46,1	43,1	40,2	38,1	53,3	52,4	52,4	49,9	45,5	41,8	38,9	57,2	56,6	56,3	52,3	47,5	43,6	39,7
	σ	0,16	0,15	0,23	0,23	0,41	0,29	0,40	1,45	1,38	1,07	0,41	0,46	0,35	0,53	0,68	0,79	0,65	0,81	0,90	0,72	0,56
$P_{FN}, \%$	μ	49,8	49,6	48,9	46,4	42,0	38,0	33,0	53,1	52,2	52,5	49,9	45,2	40,6	35,0	57,1	56,6	56,5	52,2	47,7	42,9	37,3
	σ	0,15	0,15	0,17	0,30	0,43	0,77	0,84	1,68	1,52	0,82	0,39	0,62	0,73	1,27	0,63	0,69	0,53	0,75	0,87	0,94	0,72
F_1	μ	0,50	0,51	0,52	0,55	0,56	0,59	0,61	0,48	0,49	0,46	0,51	0,54	0,57	0,60	0,43	0,43	0,43	0,48	0,53	0,56	0,59
	σ	0,02	0,02	0,02	0,01	0,01	0,01	0,01	0,04	0,04	0,03	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01
MCC	μ	0,00	0,01	0,02	0,08	0,15	0,22	0,28	-0,06	-0,05	-0,05	0,00	0,09	0,18	0,26	-0,14	-0,13	-0,13	-0,05	0,05	0,13	0,23
	σ	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,03	0,03	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,01

Таблиця В.1м – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,3	48,8	47,3	44,5	42,2	39,8	37,7	53,2	52,1	51,6	47,6	44,4	41,4	38,9	56,5	56,3	54,4	50,2	46,8	42,9	40,5
	σ	0,13	0,14	0,13	0,21	0,30	0,40	0,24	0,96	0,87	0,48	0,43	0,43	0,31	0,68	0,89	0,78	0,78	0,67	0,71	0,44	0,31
$P_{FN}, \%$	μ	49,0	48,5	47,0	44,1	41,0	37,9	34,5	53,3	52,3	51,6	47,6	44,1	40,5	36,8	56,8	56,2	54,6	50,3	46,7	42,5	38,9
	σ	0,25	0,18	0,22	0,33	0,42	0,52	0,52	1,11	0,90	0,39	0,45	0,30	0,45	0,90	0,87	0,83	0,65	0,74	0,85	0,62	1,04
F_1	μ	0,46	0,48	0,51	0,55	0,57	0,59	0,61	0,47	0,47	0,47	0,52	0,55	0,58	0,60	0,43	0,44	0,45	0,49	0,53	0,57	0,59
	σ	0,02	0,01	0,01	0,01	0,01	0,01	0,00	0,02	0,02	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01
MCC	μ	0,02	0,03	0,06	0,11	0,17	0,22	0,28	-0,07	-0,04	-0,03	0,05	0,11	0,18	0,24	-0,13	-0,12	-0,09	-0,01	0,07	0,15	0,21
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,02	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,01	0,01	0,02	0,01	0,01

Таблиця В.1н – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SPAM} для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апіорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,9	49,8	49,3	48,0	46,4	44,4	42,9	52,7	52,2	51,8	51,8	49,4	47,0	44,6	57,1	56,8	56,6	55,1	52,2	49,2	46,4
	σ	0,20	0,16	0,16	0,15	0,27	0,29	0,27	1,22	1,49	1,08	0,66	0,30	0,41	0,46	0,69	0,86	0,61	0,63	0,65	0,73	0,74
$P_{FN}, \%$	μ	49,9	49,8	49,2	48,0	46,1	43,8	41,2	53,0	52,2	52,0	51,8	49,4	47,0	43,8	57,2	56,8	56,6	55,2	52,2	49,2	46,3
	σ	0,23	0,14	0,19	0,25	0,24	0,39	0,39	1,36	1,53	1,09	0,51	0,24	0,47	0,43	0,72	1,04	0,91	0,61	0,62	0,70	0,71
F_1	μ	0,49	0,50	0,50	0,52	0,53	0,55	0,56	0,46	0,48	0,46	0,48	0,51	0,53	0,54	0,43	0,43	0,43	0,45	0,48	0,51	0,53
	σ	0,02	0,02	0,02	0,01	0,01	0,01	0,01	0,02	0,03	0,06	0,03	0,02	0,01	0,01	0,01	0,02	0,02	0,02	0,01	0,02	0,01
MCC	μ	0,00	0,00	0,01	0,04	0,07	0,12	0,16	-0,06	-0,04	-0,04	-0,04	0,01	0,06	0,12	-0,14	-0,14	-0,13	-0,10	-0,04	0,02	0,07
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,03	0,03	0,02	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01

В.2 Результати дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі $\maxSRMd2$ цифрових зображень

Таблиця В.2а – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{\maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету ALASKA, в залежності від наявних апіорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	48,8	47,6	44,9	39,4	35,7	32,6	29,4	51,9	51,7	51,6	47,1	42,8	39,3	36,2	64,2	68,7	66,5	58,9	52,5	46,0	42,1
	σ	0,22	0,20	0,67	0,62	0,48	0,55	0,54	0,48	0,65	0,61	0,34	0,46	0,68	0,42	3,72	7,67	4,23	4,24	1,74	1,22	1,30
$P_{FN}, \%$	μ	48,5	47,0	43,8	38,3	34,3	30,7	27,7	51,9	51,7	51,9	46,5	41,6	37,3	33,1	64,8	69,1	67,0	59,3	52,6	45,9	41,5
	σ	0,28	0,32	0,33	0,39	0,43	0,61	0,47	0,50	0,86	0,60	0,47	0,76	0,93	0,88	3,75	7,57	4,17	4,35	1,76	1,27	1,39
F_1	μ	0,48	0,50	0,53	0,60	0,64	0,67	0,71	0,48	0,49	0,46	0,51	0,56	0,60	0,63	0,35	0,31	0,33	0,40	0,47	0,54	0,57
	σ	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,03	0,03	0,03	0,01	0,01	0,01	0,01	0,04	0,07	0,04	0,04	0,02	0,01	0,01
MCC	μ	0,03	0,05	0,11	0,22	0,30	0,37	0,43	-0,04	-0,03	-0,03	0,06	0,16	0,23	0,31	-0,29	-0,38	-0,33	-0,18	-0,05	0,08	0,16
	σ	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,07	0,15	0,08	0,09	0,03	0,02	0,03

Таблиця В.2б – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,2	48,4	45,8	40,7	36,5	32,9	29,2	51,6	52,0	51,2	47,5	42,9	38,7	34,7	63,1	64,3	64,4	58,7	53,2	46,1	38,8
	σ	0,24	0,34	0,65	0,60	0,55	0,84	0,62	0,59	0,98	0,41	0,37	0,34	0,40	0,56	4,08	4,40	4,99	5,61	2,87	2,48	0,77
$P_{FN}, \%$	μ	48,9	47,8	44,8	39,5	34,6	30,3	26,7	51,7	51,8	51,4	46,9	41,1	35,7	31,2	63,5	64,6	64,7	59,1	53,3	45,7	37,6
	σ	0,25	0,32	0,38	0,59	0,25	0,41	0,48	0,64	0,68	0,44	0,51	0,85	0,90	0,88	4,31	4,42	4,41	5,27	2,86	2,70	1,38
F_1	μ	0,47	0,48	0,52	0,59	0,63	0,67	0,71	0,47	0,49	0,47	0,50	0,55	0,60	0,65	0,36	0,35	0,35	0,40	0,46	0,53	0,61
	σ	0,03	0,02	0,03	0,01	0,01	0,01	0,01	0,04	0,05	0,02	0,01	0,01	0,01	0,01	0,04	0,05	0,04	0,05	0,02	0,03	0,01
MCC	μ	0,02	0,04	0,09	0,20	0,29	0,37	0,44	-0,03	-0,04	-0,03	0,06	0,16	0,25	0,34	-0,27	-0,29	-0,29	-0,18	-0,07	0,08	0,24
	σ	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,08	0,09	0,09	0,11	0,06	0,05	0,02

Таблиця В.2в – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	47,0	44,9	39,8	33,4	29,5	26,2	23,3	52,1	52,3	49,8	42,3	36,6	32,4	28,5	62,4	64,7	65,7	51,6	45,8	38,0	33,8
	σ	0,39	0,57	0,63	0,59	0,34	0,82	0,61	0,98	0,98	0,47	0,33	0,66	0,59	0,74	3,49	7,74	2,64	2,72	2,26	1,23	1,18
$P_{FN}, \%$	μ	46,5	44,4	39,2	32,6	28,5	25,1	22,0	52,1	52,6	49,8	41,1	35,5	30,6	27,0	62,8	64,8	65,8	51,6	45,6	37,4	32,8
	σ	0,31	0,40	0,47	0,63	0,46	0,57	0,43	1,10	1,05	0,65	0,38	0,46	0,50	0,52	4,15	7,34	2,63	2,75	2,39	1,21	1,70
F_1	μ	0,51	0,54	0,60	0,67	0,71	0,74	0,77	0,47	0,46	0,49	0,57	0,63	0,68	0,72	0,37	0,35	0,34	0,48	0,54	0,62	0,66
	σ	0,01	0,01	0,01	0,01	0,00	0,01	0,00	0,06	0,01	0,02	0,01	0,01	0,01	0,01	0,05	0,07	0,03	0,02	0,02	0,01	0,01
MCC	μ	0,07	0,11	0,21	0,34	0,42	0,49	0,55	-0,04	-0,05	0,00	0,17	0,28	0,37	0,44	-0,25	-0,29	-0,31	-0,03	0,09	0,25	0,33
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,00	0,02	0,02	0,01	0,00	0,01	0,01	0,01	0,08	0,15	0,05	0,05	0,05	0,02	0,03

Таблиця В.2г – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганогам, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,2	48,5	46,2	41,5	37,3	33,6	30,8	51,8	51,5	51,6	48,2	44,0	39,6	35,8	63,3	63,4	61,6	61,3	52,3	45,8	41,1
	σ	0,17	0,33	0,27	0,81	0,78	0,70	0,90	0,47	0,40	0,73	0,44	0,62	0,46	0,42	4,75	4,02	3,49	2,67	2,45	1,62	1,74
$P_{FN}, \%$	μ	49,0	48,2	45,4	40,5	35,6	31,9	27,9	51,8	51,5	51,8	47,7	42,2	37,2	33,3	63,4	64,0	61,8	61,6	52,4	45,3	40,4
	σ	0,16	0,32	0,29	0,38	0,46	0,32	0,46	0,64	0,57	0,89	0,63	0,36	0,71	0,78	4,67	4,30	3,35	2,67	2,62	1,93	2,22
F_1	μ	0,48	0,49	0,52	0,58	0,62	0,66	0,69	0,49	0,48	0,47	0,49	0,54	0,59	0,64	0,36	0,36	0,38	0,38	0,47	0,53	0,58
	σ	0,01	0,02	0,02	0,01	0,01	0,01	0,01	0,03	0,03	0,02	0,02	0,01	0,01	0,01	0,05	0,04	0,03	0,03	0,02	0,02	0,02
MCC	μ	0,02	0,03	0,08	0,18	0,27	0,34	0,41	-0,04	-0,03	-0,03	0,04	0,14	0,23	0,31	-0,27	-0,27	-0,23	-0,23	-0,05	0,09	0,18
	σ	0,00	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,09	0,08	0,07	0,05	0,05	0,04	0,04

Таблиця В.2д – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	26,1	17,5	9,0	4,7	2,9	2,2	1,6	36,2	25,8	13,6	6,4	4,0	3,2	2,4	46,6	33,4	17,1	7,7	4,9	3,8	3,0
	σ	0,72	0,40	0,55	0,30	0,29	0,28	0,25	0,72	0,83	0,72	0,59	0,56	0,34	0,33	1,76	1,62	0,79	0,80	0,54	0,50	0,47
$P_{FN}, \%$	μ	26,9	18,5	9,3	4,3	2,8	2,1	1,7	36,4	25,3	12,5	5,5	3,5	2,4	2,0	46,7	33,2	16,5	7,2	4,5	3,2	2,6
	σ	0,48	0,42	0,37	0,33	0,36	0,23	0,29	0,51	0,56	0,55	0,49	0,48	0,42	0,43	1,73	1,56	1,00	0,38	0,48	0,62	0,48
F_1	μ	0,74	0,82	0,91	0,96	0,97	0,98	0,98	0,64	0,74	0,87	0,94	0,96	0,97	0,98	0,54	0,67	0,83	0,93	0,95	0,96	0,97
	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,02	0,02	0,01	0,00	0,00	0,00	0,00
MCC	μ	0,47	0,64	0,82	0,91	0,94	0,96	0,97	0,27	0,49	0,74	0,88	0,92	0,94	0,96	0,07	0,33	0,66	0,85	0,91	0,93	0,94
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,03	0,03	0,01	0,01	0,01	0,00	0,00

Таблиця В.2е – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	27,1	18,2	9,7	4,8	2,9	1,8	1,8	36,8	25,9	13,3	6,5	3,9	2,6	2,5	47,0	32,5	16,9	7,6	4,6	3,0	2,8
	σ	0,52	0,42	0,59	0,56	0,35	0,26	0,19	0,48	1,01	0,89	0,78	0,57	0,44	0,40	1,70	1,47	0,86	0,90	0,93	0,37	0,46
$P_{FN}, \%$	μ	27,2	18,8	9,2	4,4	2,7	1,8	1,5	36,6	25,5	12,4	5,4	3,7	2,4	1,9	47,0	32,1	16,2	7,4	4,6	2,9	2,7
	σ	0,42	0,45	0,39	0,33	0,28	0,13	0,22	0,49	0,66	0,62	0,57	0,49	0,47	0,27	1,69	1,77	0,92	0,71	0,85	0,57	0,41
F_1	μ	0,73	0,82	0,91	0,95	0,97	0,98	0,98	0,63	0,74	0,87	0,94	0,96	0,98	0,98	0,53	0,68	0,83	0,93	0,95	0,97	0,97
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,02	0,01	0,01	0,00	0,00	0,00	0,00
MCC	μ	0,46	0,63	0,81	0,91	0,94	0,96	0,97	0,27	0,49	0,74	0,88	0,92	0,95	0,96	0,06	0,35	0,67	0,85	0,91	0,94	0,95
	σ	0,01	0,01	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,01	0,00	0,00	0,03	0,03	0,01	0,01	0,01	0,00	0,00

Таблиця В.2ж – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	23,7	15,9	8,6	4,1	2,7	2,0	1,6	32,5	22,8	11,6	5,9	3,9	2,7	2,4	41,1	28,1	14,5	7,1	4,5	3,5	2,5
	σ	0,52	0,62	0,49	0,36	0,30	0,32	0,16	0,73	0,90	0,67	0,68	0,63	0,42	0,44	2,12	1,31	0,71	0,87	0,78	0,48	0,45
$P_{FN}, \%$	μ	24,4	16,5	8,2	3,8	2,7	1,9	1,5	32,3	22,1	10,8	5,0	3,3	2,6	2,1	41,3	27,9	14,1	6,7	4,4	2,9	3,0
	σ	0,66	0,58	0,36	0,28	0,26	0,22	0,13	0,49	0,66	0,69	0,44	0,54	0,46	0,35	1,90	1,54	0,89	0,58	0,81	0,67	0,44
F_1	μ	0,76	0,84	0,92	0,96	0,97	0,98	0,98	0,67	0,77	0,89	0,95	0,96	0,97	0,98	0,59	0,72	0,86	0,93	0,96	0,97	0,97
	σ	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,01	0,01	0,01	0,00	0,00	0,00
MCC	μ	0,52	0,68	0,83	0,92	0,95	0,96	0,97	0,35	0,55	0,78	0,89	0,93	0,95	0,95	0,18	0,44	0,71	0,86	0,91	0,94	0,94
	σ	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,04	0,03	0,01	0,01	0,01	0,01	0,00

Таблиця В.2и – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	22,6	14,7	7,3	3,6	2,4	2,0	1,5	30,9	20,5	10,5	4,8	3,6	2,7	2,5	39,5	25,8	12,8	6,5	4,0	3,0	2,7
	σ	0,62	0,64	0,51	0,22	0,28	0,26	0,27	0,57	0,58	0,65	0,59	0,48	0,37	0,40	1,91	1,17	0,72	0,60	0,53	0,69	0,55
$P_{FN}, \%$	μ	22,8	14,9	7,3	3,7	2,5	1,8	1,4	30,8	19,4	9,1	4,7	3,0	2,4	1,7	39,5	25,3	12,0	5,8	4,0	3,2	2,6
	σ	0,38	0,60	0,33	0,27	0,21	0,24	0,11	0,77	0,81	0,45	0,38	0,35	0,34	0,35	1,98	1,22	1,20	0,64	0,62	0,70	0,59
F_1	μ	0,77	0,85	0,93	0,96	0,98	0,98	0,99	0,69	0,80	0,90	0,95	0,97	0,97	0,98	0,61	0,74	0,88	0,94	0,96	0,97	0,97
	σ	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,01	0,01	0,00	0,00	0,00	0,00
MCC	μ	0,55	0,70	0,85	0,93	0,95	0,96	0,97	0,38	0,60	0,80	0,90	0,93	0,95	0,96	0,21	0,49	0,75	0,88	0,92	0,94	0,95
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,04	0,02	0,01	0,01	0,00	0,00	0,00

Таблиця В.2к – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	48,9	47,4	43,0	34,5	29,0	23,9	20,7	51,9	51,9	51,0	41,8	35,2	29,6	25,0	63,0	65,2	65,2	52,3	42,6	33,9	28,7
	σ	0,37	0,29	0,53	0,28	1,02	0,45	0,76	0,75	0,88	0,42	0,73	0,60	0,55	0,74	4,53	2,86	2,96	2,58	2,67	1,41	1,73
$P_{FN}, \%$	μ	49,0	47,6	43,5	35,0	27,9	22,7	18,0	51,8	51,9	51,1	42,0	32,9	26,5	20,8	62,5	65,7	64,9	52,2	42,7	33,2	27,9
	σ	0,28	0,44	0,32	0,51	0,52	0,56	0,47	0,86	0,62	0,40	0,28	0,67	0,86	0,88	4,42	3,01	2,86	2,41	2,71	2,17	2,75
F_1	μ	0,52	0,54	0,58	0,66	0,71	0,76	0,80	0,49	0,47	0,48	0,58	0,65	0,71	0,76	0,38	0,34	0,35	0,49	0,58	0,66	0,72
	σ	0,02	0,01	0,01	0,00	0,01	0,00	0,00	0,04	0,03	0,01	0,01	0,01	0,00	0,01	0,05	0,03	0,03	0,03	0,02	0,01	0,02
MCC	μ	0,02	0,05	0,14	0,31	0,43	0,53	0,61	-0,04	-0,04	-0,02	0,16	0,32	0,44	0,54	-0,26	-0,31	-0,30	-0,04	0,15	0,33	0,43
	σ	0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,09	0,06	0,06	0,05	0,05	0,04	0,04

Таблиця В.2л – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,5	48,3	44,8	36,4	29,6	23,7	19,8	51,8	51,9	50,8	42,1	35,4	29,2	24,0	63,0	64,1	61,1	50,5	41,0	33,0	27,0
	σ	0,17	0,18	0,60	0,34	0,76	0,69	0,51	0,38	0,87	0,43	0,45	0,44	0,89	0,40	6,54	5,49	5,66	1,46	2,63	1,20	1,21
$P_{FN}, \%$	μ	49,5	48,5	44,8	36,0	28,0	22,1	17,2	51,8	52,2	50,8	41,8	32,7	24,6	19,1	62,9	64,4	60,9	50,5	40,7	32,4	25,1
	σ	0,17	0,14	0,43	0,50	0,52	0,50	0,55	0,32	1,31	0,45	0,62	0,70	1,05	0,77	6,82	5,18	5,70	1,47	3,01	1,87	2,31
F_1	μ	0,51	0,53	0,55	0,64	0,71	0,77	0,81	0,48	0,47	0,51	0,58	0,64	0,71	0,77	0,37	0,35	0,39	0,49	0,59	0,67	0,73
	σ	0,02	0,01	0,01	0,00	0,01	0,00	0,00	0,03	0,05	0,03	0,01	0,01	0,01	0,00	0,07	0,05	0,06	0,01	0,02	0,01	0,01
MCC	μ	0,01	0,03	0,10	0,28	0,42	0,54	0,63	-0,04	-0,04	-0,02	0,16	0,32	0,46	0,57	-0,26	-0,29	-0,22	-0,01	0,18	0,35	0,48
	σ	0,00	0,00	0,01	0,01	0,01	0,01	0,00	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,13	0,11	0,11	0,03	0,06	0,03	0,03

Таблиця В.2м – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	44,2	40,6	34,6	26,1	21,2	18,0	15,5	51,8	51,4	43,9	33,5	27,6	22,6	19,6	70,4	68,5	58,7	42,2	33,7	27,4	22,7
	σ	0,51	0,46	0,50	0,50	0,49	0,69	0,47	0,44	0,75	0,76	0,58	0,68	0,54	0,77	3,09	6,32	3,35	2,33	1,42	1,22	0,87
$P_{FN}, \%$	μ	44,7	41,1	35,2	26,1	20,7	16,9	13,8	52,0	51,3	44,5	33,2	26,1	20,0	16,4	70,5	68,0	58,6	42,2	33,8	26,4	21,3
	σ	0,57	0,48	0,33	0,35	0,60	0,28	0,40	0,50	0,78	0,36	0,90	0,58	0,55	0,82	3,67	6,38	3,25	2,38	1,62	2,01	1,51
F_1	μ	0,57	0,60	0,65	0,74	0,79	0,82	0,85	0,47	0,49	0,57	0,66	0,73	0,78	0,81	0,30	0,32	0,42	0,58	0,66	0,73	0,78
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,03	0,02	0,01	0,01	0,01	0,00	0,00	0,04	0,06	0,03	0,02	0,01	0,01	0,01
MCC	μ	0,11	0,18	0,30	0,48	0,58	0,65	0,71	-0,04	-0,03	0,12	0,33	0,46	0,57	0,64	-0,41	-0,37	-0,17	0,16	0,32	0,46	0,56
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,07	0,13	0,07	0,05	0,03	0,03	0,02

Таблиця В.2н – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апіорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	48,5	47,1	43,1	36,6	30,8	26,7	23,5	52,0	51,6	50,6	43,1	37,1	32,5	28,8	65,7	67,6	63,8	53,4	44,9	37,8	33,4
	σ	0,14	0,25	0,34	1,05	0,75	0,48	1,21	0,60	0,45	0,56	0,49	0,47	0,90	0,65	5,67	6,71	4,31	2,69	2,62	1,56	1,36
$P_{FN}, \%$	μ	48,6	47,3	43,3	36,5	30,3	25,6	21,4	52,0	51,6	50,6	43,0	35,6	29,8	25,0	65,5	67,2	63,4	53,2	44,9	37,6	32,9
	σ	0,16	0,14	0,34	0,39	0,33	0,58	0,69	0,69	0,56	0,53	0,50	0,66	0,71	0,77	6,10	6,43	4,44	2,54	2,71	1,69	1,94
F_1	μ	0,52	0,53	0,57	0,63	0,69	0,73	0,77	0,48	0,49	0,49	0,57	0,63	0,68	0,72	0,35	0,33	0,37	0,48	0,56	0,62	0,67
	σ	0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,04	0,03	0,03	0,01	0,01	0,01	0,01	0,07	0,07	0,05	0,03	0,02	0,02	0,01
MCC	μ	0,03	0,06	0,14	0,27	0,39	0,48	0,55	-0,04	-0,03	-0,01	0,14	0,27	0,38	0,46	-0,31	-0,35	-0,27	-0,07	0,10	0,25	0,34
	σ	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,12	0,13	0,09	0,05	0,05	0,03	0,03

В.3 Результати дослідження точності виявлення стеганогам, сформованих згідно адаптивних стеганографічних методів, при використанні статистичної моделі maxSRMd2 (EDGE фільтр) цифрових зображень

Таблиця В.3а – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганогам, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,1	48,2	46,4	42,3	38,9	36,3	34,0	51,8	51,5	50,5	46,5	42,8	39,5	36,6	61,7	61,1	58,1	51,5	46,4	42,3	39,1
	σ	0,14	0,19	0,47	0,38	0,24	0,57	0,40	0,77	0,40	0,46	0,35	0,29	0,51	0,59	3,16	2,91	2,78	1,55	1,23	0,93	0,69
$P_{FN}, \%$	μ	48,8	47,8	45,0	41,4	37,8	34,6	31,7	51,7	51,8	50,6	45,6	41,8	38,1	34,4	61,8	61,3	58,4	51,6	46,2	41,4	38,2
	σ	0,26	0,33	0,58	0,50	0,40	0,54	0,65	0,89	0,48	0,53	0,62	0,62	0,48	0,65	3,21	2,86	2,60	1,62	1,42	1,05	0,79
F_1	μ	0,48	0,49	0,50	0,57	0,61	0,63	0,66	0,49	0,46	0,46	0,51	0,56	0,60	0,63	0,38	0,38	0,41	0,47	0,53	0,57	0,61
	σ	0,02	0,02	0,03	0,01	0,00	0,01	0,00	0,04	0,02	0,03	0,02	0,01	0,01	0,01	0,03	0,03	0,02	0,02	0,01	0,01	0,01
MCC	μ	0,02	0,04	0,08	0,16	0,23	0,29	0,34	-0,03	-0,03	-0,01	0,08	0,15	0,22	0,29	-0,23	-0,22	-0,17	-0,03	0,07	0,16	0,23
	σ	0,00	0,00	0,01	0,01	0,00	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,06	0,06	0,05	0,03	0,03	0,02	0,01

Таблиця В.3б – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,3	48,5	46,8	42,9	39,2	36,6	33,8	51,6	51,8	50,8	47,0	43,0	39,6	36,1	60,7	62,8	59,0	52,0	46,3	41,7	38,4
	σ	0,19	0,21	0,37	0,47	0,51	0,47	0,49	0,51	0,65	0,33	0,42	0,32	0,48	0,73	2,48	2,53	2,42	1,48	0,96	0,40	0,39
$P_{FN}, \%$	μ	49,2	48,3	46,0	41,6	37,4	33,8	30,5	51,7	51,8	51,0	46,0	41,2	36,8	32,9	60,5	63,0	59,1	52,1	45,8	40,6	37,2
	σ	0,17	0,22	0,33	0,43	0,38	0,89	0,71	0,53	0,63	0,43	0,45	0,82	1,21	0,56	2,66	2,38	2,46	1,50	1,15	0,99	1,12
F_1	μ	0,48	0,49	0,51	0,56	0,60	0,63	0,66	0,47	0,48	0,46	0,50	0,55	0,59	0,63	0,40	0,37	0,41	0,47	0,53	0,57	0,61
	σ	0,03	0,01	0,02	0,01	0,01	0,01	0,01	0,06	0,03	0,03	0,02	0,01	0,01	0,01	0,03	0,02	0,03	0,01	0,01	0,01	0,00
MCC	μ	0,01	0,03	0,07	0,15	0,23	0,30	0,36	-0,03	-0,04	-0,02	0,07	0,16	0,23	0,31	-0,21	-0,26	-0,18	-0,04	0,08	0,18	0,24
	σ	0,00	0,00	0,01	0,00	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,05	0,05	0,05	0,03	0,02	0,01	0,01

Таблиця В.3в – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	47,4	45,9	42,5	38,1	34,4	32,2	29,8	51,7	51,5	48,2	42,2	38,0	35,0	32,4	62,2	59,9	54,6	46,4	41,3	37,8	34,6
	σ	0,36	0,26	0,25	0,48	0,46	0,53	0,68	0,50	0,58	0,57	0,29	0,63	0,44	0,77	3,22	2,03	1,72	0,72	0,78	0,81	0,57
$P_{FN}, \%$	μ	47,1	45,4	41,8	36,6	33,1	30,1	27,5	51,7	51,7	48,0	41,2	37,1	33,2	30,3	62,6	60,3	54,6	46,3	40,9	37,2	32,7
	σ	0,23	0,34	0,26	0,45	0,48	0,57	0,60	0,58	0,55	0,59	0,53	0,75	0,67	0,67	3,23	1,93	1,75	0,81	0,70	0,81	1,06
F_1	μ	0,51	0,53	0,57	0,61	0,66	0,68	0,70	0,48	0,47	0,51	0,57	0,62	0,65	0,68	0,37	0,39	0,45	0,53	0,58	0,62	0,65
	σ	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,05	0,02	0,02	0,01	0,01	0,01	0,01	0,03	0,02	0,02	0,01	0,01	0,01	0,01
MCC	μ	0,05	0,09	0,16	0,25	0,33	0,38	0,43	-0,03	-0,03	0,04	0,17	0,25	0,32	0,37	-0,25	-0,20	-0,09	0,07	0,18	0,25	0,33
	σ	0,01	0,01	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,06	0,04	0,03	0,02	0,01	0,01	0,01

Таблиця В.3г – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,3	48,7	47,2	43,8	40,7	37,8	35,3	51,6	51,3	51,0	47,6	44,1	40,8	37,7	61,0	60,5	59,0	52,7	48,0	43,5	39,7
	σ	0,13	0,16	0,31	0,29	0,49	0,55	0,38	0,34	0,52	0,59	0,37	0,35	0,47	0,41	3,51	4,28	2,44	1,59	1,04	0,64	0,80
$P_{FN}, \%$	μ	49,2	48,4	46,5	42,9	39,0	35,4	32,0	51,8	51,5	51,0	46,9	42,2	38,2	34,7	61,3	60,7	59,3	52,8	47,7	42,4	38,6
	σ	0,17	0,29	0,39	0,57	0,60	0,57	0,36	0,36	0,61	0,48	0,74	0,56	1,06	0,47	3,71	4,27	2,54	1,63	1,26	1,22	0,92
F_1	μ	0,49	0,48	0,50	0,55	0,58	0,62	0,64	0,47	0,46	0,48	0,50	0,53	0,58	0,61	0,38	0,39	0,40	0,46	0,51	0,55	0,60
	σ	0,01	0,02	0,02	0,01	0,01	0,01	0,00	0,02	0,05	0,02	0,02	0,01	0,01	0,01	0,04	0,04	0,03	0,01	0,01	0,01	0,01
MCC	μ	0,01	0,03	0,06	0,13	0,20	0,27	0,33	-0,03	-0,03	-0,02	0,06	0,13	0,21	0,27	-0,22	-0,21	-0,18	-0,05	0,04	0,14	0,22
	σ	0,00	0,00	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,07	0,09	0,05	0,03	0,02	0,02	0,02

Таблиця В.3д – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	34,3	27,5	18,6	10,4	6,8	5,0	4,0	38,3	30,5	20,5	11,2	7,2	5,3	4,4	43,3	33,5	22,0	12,1	7,9	6,1	4,5
	σ	0,55	0,57	0,38	0,48	0,27	0,33	0,21	0,54	0,67	0,56	0,53	0,66	0,35	0,29	1,65	0,88	1,01	0,86	0,59	0,59	0,49
$P_{FN}, \%$	μ	34,2	27,0	18,0	10,0	6,6	4,7	3,7	38,3	30,1	19,1	10,7	7,2	5,2	3,9	43,5	33,3	21,6	11,6	7,5	5,4	4,4
	σ	0,41	0,72	0,76	0,31	0,40	0,35	0,29	0,61	0,74	0,59	0,55	0,44	0,39	0,21	1,63	0,70	0,84	0,49	0,36	0,57	0,44
F_1	μ	0,66	0,73	0,82	0,90	0,93	0,95	0,96	0,62	0,69	0,80	0,89	0,93	0,95	0,96	0,57	0,67	0,78	0,88	0,92	0,94	0,96
	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,02	0,01	0,01	0,00	0,00	0,00	0,00
MCC	μ	0,32	0,46	0,63	0,80	0,87	0,90	0,92	0,23	0,39	0,60	0,78	0,86	0,90	0,92	0,13	0,33	0,56	0,76	0,85	0,89	0,91
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,01	0,01	0,00	0,00	0,03	0,01	0,01	0,01	0,00	0,00	0,00

Таблиця В.3е – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	34,9	27,4	18,0	10,2	6,5	5,0	3,9	38,2	30,2	19,7	11,3	6,6	5,3	4,1	42,4	34,0	21,4	12,3	7,6	5,7	4,5
	σ	0,39	0,46	0,53	0,30	0,26	0,42	0,26	0,47	0,71	0,73	0,68	0,78	0,42	0,43	1,31	0,59	0,87	0,65	0,48	0,44	0,48
$P_{FN}, \%$	μ	34,7	26,9	17,3	9,9	6,3	4,4	3,5	38,4	29,4	18,7	10,8	7,0	4,9	4,0	42,7	33,1	20,9	11,8	7,2	5,3	4,4
	σ	0,56	0,63	0,34	0,40	0,39	0,40	0,23	0,34	0,76	0,66	0,67	0,74	0,45	0,37	1,30	1,12	1,33	0,48	0,52	0,61	0,36
F_1	μ	0,65	0,73	0,82	0,90	0,94	0,95	0,96	0,62	0,70	0,81	0,89	0,93	0,95	0,96	0,58	0,66	0,79	0,88	0,93	0,94	0,96
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,00	0,00	0,00
MCC	μ	0,30	0,46	0,65	0,80	0,87	0,91	0,93	0,23	0,40	0,62	0,78	0,86	0,90	0,92	0,15	0,33	0,58	0,76	0,85	0,89	0,91
	σ	0,01	0,01	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,00	0,01	0,00	0,00	0,00	0,03	0,01	0,02	0,01	0,00	0,00	0,00

Таблиця В.3ж – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	31,9	25,6	17,0	9,6	6,7	4,6	3,9	35,2	28,0	18,5	10,5	7,0	5,2	4,3	39,2	30,4	20,5	11,4	7,6	5,6	4,6
	σ	0,39	0,47	0,49	0,25	0,35	0,35	0,28	0,47	0,51	0,52	0,46	0,41	0,47	0,47	1,27	0,68	0,44	0,46	0,51	0,50	0,67
$P_{FN}, \%$	μ	31,9	24,9	16,2	9,2	6,1	4,8	3,6	35,5	27,1	17,6	9,7	6,6	5,0	3,8	39,3	30,2	19,8	10,4	7,4	5,4	4,4
	σ	0,52	0,55	0,56	0,42	0,27	0,38	0,24	0,48	0,52	0,75	0,38	0,47	0,46	0,44	1,08	0,81	0,54	0,87	0,76	0,64	0,52
F_1	μ	0,68	0,75	0,83	0,91	0,94	0,95	0,96	0,65	0,72	0,82	0,90	0,93	0,95	0,96	0,61	0,70	0,80	0,89	0,93	0,94	0,95
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00
MCC	μ	0,36	0,49	0,67	0,81	0,87	0,91	0,93	0,29	0,45	0,64	0,80	0,86	0,90	0,92	0,21	0,39	0,60	0,78	0,85	0,89	0,91
	σ	0,01	0,01	0,00	0,01	0,00	0,01	0,00	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,02	0,01	0,01	0,01	0,01	0,00	0,00

Таблиця В.3и – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	30,8	23,2	14,9	8,1	5,8	4,5	3,8	33,8	25,3	16,4	9,1	5,9	4,8	4,2	38,3	27,8	17,7	9,8	7,1	5,3	4,3
	σ	0,54	0,48	0,69	0,36	0,26	0,32	0,30	0,61	0,43	0,84	0,65	0,55	0,52	0,48	1,49	1,01	0,69	0,38	0,59	0,68	0,50
$P_{FN}, \%$	μ	30,7	22,7	14,2	8,0	5,4	4,2	3,6	34,0	25,3	15,3	8,1	6,1	4,5	3,7	38,3	27,0	16,6	9,0	5,8	4,8	3,8
	σ	0,48	0,63	0,40	0,30	0,44	0,30	0,34	0,52	0,39	0,80	0,60	0,64	0,50	0,40	1,27	0,91	0,82	0,52	0,54	0,51	0,49
F_1	μ	0,69	0,77	0,85	0,92	0,94	0,96	0,96	0,66	0,75	0,84	0,91	0,94	0,95	0,96	0,62	0,72	0,83	0,91	0,93	0,95	0,96
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,02	0,01	0,00	0,00	0,00	0,00	0,00
MCC	μ	0,38	0,54	0,71	0,84	0,89	0,91	0,93	0,32	0,49	0,68	0,83	0,88	0,91	0,92	0,23	0,45	0,66	0,81	0,87	0,90	0,92
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,01	0,00	0,00	0,00	0,03	0,02	0,01	0,01	0,00	0,01	0,00

Таблиця В.3к – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,1	48,1	44,6	38,2	33,1	29,2	25,1	51,5	51,8	49,1	41,5	35,4	31,0	26,9	62,3	61,6	55,3	46,1	37,8	32,4	27,9
	σ	0,25	0,15	0,28	0,31	0,40	0,53	0,55	1,11	1,12	0,55	0,49	0,68	0,70	0,64	2,96	2,58	2,01	1,49	0,75	0,72	0,46
$P_{FN}, \%$	μ	49,1	48,2	45,0	37,7	31,2	25,5	21,1	52,0	52,1	49,2	41,0	34,0	27,8	22,3	62,7	61,6	55,1	46,2	37,5	30,9	23,9
	σ	0,16	0,16	0,34	0,45	0,58	0,78	0,59	0,86	1,04	0,49	0,68	0,83	1,11	1,01	2,42	2,54	1,88	1,51	1,09	0,98	0,96
F_1	μ	0,51	0,53	0,56	0,62	0,67	0,71	0,76	0,43	0,45	0,52	0,58	0,64	0,69	0,74	0,37	0,38	0,45	0,54	0,62	0,68	0,73
	σ	0,02	0,01	0,01	0,00	0,00	0,00	0,00	0,04	0,04	0,03	0,01	0,01	0,01	0,00	0,02	0,03	0,02	0,02	0,01	0,01	0,00
MCC	μ	0,02	0,04	0,10	0,24	0,36	0,45	0,54	-0,03	-0,04	0,02	0,18	0,31	0,41	0,51	-0,25	-0,23	-0,10	0,08	0,25	0,37	0,48
	σ	0,00	0,00	0,01	0,01	0,01	0,00	0,01	0,02	0,02	0,01	0,01	0,01	0,01	0,01	0,05	0,05	0,04	0,03	0,02	0,02	0,01

Таблиця В.3л – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	49,6	48,9	46,0	39,2	33,7	28,8	24,8	51,6	51,5	49,7	41,4	35,6	30,4	25,4	61,4	61,1	56,0	45,7	37,6	31,4	26,2
	σ	0,20	0,18	0,18	0,30	0,52	0,51	0,52	0,41	0,46	0,51	0,82	0,52	0,71	0,62	3,41	3,61	3,33	1,52	0,79	0,83	0,79
$P_{FN}, \%$	μ	49,6	49,0	46,1	38,0	30,6	24,1	19,2	51,6	51,6	49,7	41,5	32,6	24,9	21,0	61,7	61,2	55,7	45,4	36,4	29,2	23,5
	σ	0,18	0,17	0,30	0,43	0,76	0,85	0,94	0,54	0,31	0,41	0,74	0,96	0,95	1,03	3,83	3,35	3,18	1,91	1,52	1,46	1,42
F_1	μ	0,51	0,51	0,54	0,60	0,66	0,72	0,77	0,48	0,47	0,51	0,59	0,64	0,70	0,76	0,38	0,39	0,45	0,54	0,62	0,69	0,74
	σ	0,02	0,01	0,01	0,01	0,01	0,00	0,00	0,04	0,02	0,03	0,01	0,01	0,01	0,00	0,05	0,03	0,03	0,01	0,01	0,01	0,01
MCC	μ	0,01	0,02	0,08	0,23	0,36	0,47	0,56	-0,03	-0,03	0,01	0,17	0,32	0,44	0,53	-0,23	-0,22	-0,12	0,09	0,26	0,39	0,50
	σ	0,00	0,00	0,00	0,00	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,07	0,07	0,06	0,03	0,02	0,02	0,01

Таблиця В.3м – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRMd2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	45,2	42,3	37,8	32,0	27,9	24,6	22,0	51,3	48,8	42,2	34,8	29,7	26,8	23,3	58,5	55,1	47,0	38,0	31,6	27,8	24,5
	σ	0,24	0,18	0,45	0,35	0,31	0,37	0,65	0,24	0,24	0,68	0,52	0,49	0,70	0,70	1,07	1,08	1,10	1,02	0,67	0,61	0,70
$P_{FN}, \%$	μ	45,6	43,1	38,5	30,9	25,8	21,7	18,7	51,4	48,9	43,1	34,4	28,2	22,7	19,5	58,4	55,2	47,1	37,4	30,4	26,0	22,0
	σ	0,24	0,29	0,65	0,51	0,51	0,57	0,61	0,26	0,31	0,65	0,89	0,81	1,06	0,79	1,10	1,08	1,07	1,14	0,87	1,12	0,74
F_1	μ	0,55	0,58	0,62	0,68	0,72	0,76	0,79	0,48	0,53	0,59	0,65	0,71	0,74	0,78	0,42	0,45	0,53	0,62	0,68	0,73	0,76
	σ	0,01	0,00	0,01	0,00	0,00	0,00	0,00	0,01	0,02	0,01	0,01	0,00	0,00	0,00	0,01	0,02	0,01	0,01	0,01	0,01	0,01
MCC	μ	0,09	0,15	0,24	0,37	0,46	0,54	0,59	-0,03	0,02	0,15	0,31	0,42	0,50	0,57	-0,17	-0,10	0,06	0,25	0,38	0,46	0,53
	σ	0,00	0,00	0,01	0,00	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,02	0,02	0,01	0,01	0,01

Таблиця В.3н – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору $SD_{maxSRM d2-EDGE}$ для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо ACM

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	48,7	47,8	44,9	39,8	35,5	32,2	29,2	51,8	51,7	48,9	42,1	37,6	33,8	30,9	61,6	58,6	57,0	46,4	40,1	35,6	31,7
	σ	0,21	0,27	0,29	0,31	0,51	0,56	0,53	0,47	0,58	0,53	0,59	0,46	0,75	0,56	4,01	2,09	2,56	1,39	0,78	0,89	0,44
$P_{FN}, \%$	μ	48,8	47,9	45,2	39,2	33,2	28,6	24,2	51,8	51,6	48,9	42,5	36,2	30,9	25,6	61,8	58,3	56,7	46,5	39,7	34,9	29,5
	σ	0,19	0,30	0,24	0,42	0,96	0,77	1,16	0,65	0,63	0,54	0,46	0,80	1,01	1,15	3,98	2,43	2,67	1,32	1,07	1,17	1,10
F_1	μ	0,52	0,53	0,56	0,60	0,64	0,68	0,71	0,48	0,49	0,51	0,58	0,62	0,66	0,70	0,38	0,42	0,44	0,54	0,60	0,64	0,68
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,00	0,05	0,03	0,02	0,01	0,01	0,01	0,01	0,04	0,03	0,03	0,02	0,01	0,01	0,00
MCC	μ	0,03	0,04	0,10	0,21	0,31	0,39	0,46	-0,04	-0,03	0,02	0,15	0,26	0,35	0,43	-0,23	-0,17	-0,14	0,07	0,20	0,30	0,39
	σ	0,00	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,08	0,04	0,05	0,03	0,02	0,02	0,01

ДОДАТОК Г РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ ДОСЯЖНОЇ ТОЧНОСТІ ВИЯВЛЕННЯ СТЕГАНОГРАМ, СФОРМОВАНИХ ЗГІДНО АДАПТИВНИХ СТЕГANOГРАФІЧНИХ МЕТОДІВ, ПРИ ВИКОРИСТАННІ ЗАПРОПОНОВАНОГО МЕТОДУ ПОБУДОВИ СТЕГОДЕТЕКТОРІВ

Для аналізу досяжної точності роботи стегодетекторів, заснованих на використанні запропонованих методів структурного синтезу та параметричної оптимізації, проведено налаштування стегодетектору SD_{SRR} . Даний СД заснований на використанні запропонованого методу попередньої обробки (розд. 2.3), стандартної моделі SPAM [38] для аналізу статистичних параметрів оброблюваних ЦЗ та ансамблевого класифікатора на основі ЛДФ [202].

Ступінь заповнення зображення-контейнеру стегоданими змінювалася в наступному діапазоні – 3%, 5%, 10%, 20%, 30%, 40% та 50%. Формування стеганограм проводилося згідно адаптивних стеганографічних методів HUGO [147], S-UNIWARD [135], MG [152] та MiPOD [153].

Аналіз точності роботи СД проводився згідно стандартної процедури перехресної перевірки [144]. В якості тестового пакету цифрових зображень використано стандартні пакети ALASKA [134], VISION [196] та MIRFlickr [197]. Зважаючи на суттєві відмінності у кількості зображень в даних пакетах ЦЗ, в роботі були використані псевдовипадкові вибірки 10,000 цифрових зображень для кожного пакету.

Проведено дослідження точності роботи СД для наступних випадків:

- Наявність у вибірці \mathcal{S}_{train} пари ЗК та відповідних їм стеганограм ($K_{\alpha}^{OL} = 0\%$) – відповідає випадку, що широко використовується при проведенні досліджень в галузі стегоаналізу, а саме використання апріорних даних щодо особливостей використаного АСМ при налаштуванні СД.

- Наявність у вибірці \mathcal{S}_{train} лише окремих пар ЗК та відповідних їм стеганограм ($K_{\alpha}^{OL} \sim \mathcal{U}(0; 100)$) – відповідає поширеній ситуації, коли стегоаналітик може використовувати лише низку пар ЗК та відповідних їм стеганограм при налаштуванні СД.
- Відсутність у вибірці \mathcal{S}_{train} зображень-контейнерів, використаних для формування стеганограм ($K_{\alpha}^{OL} = 0\%$) – відповідає найбільш складному випадку проведення стегоаналізу (проблема zero day), а саме стегоаналітик не має можливості формувати стеганограми для довільного ЗК.

Зважаючи на залежність точності роботи запропонованого методу від виду використаних векторів (статистичних параметрів оброблюваних ЦЗ), досліджено випадки використання запропонованих типів векторів \mathbf{F}_{calib} (2.17), \mathbf{F}_{DF} (2.18) та \mathbf{F}_{CC} (2.15).

Для інтегральної оцінки точності роботи досліджуваних стегодетекторів SD_{SPAM} , $SD_{maxSRMd2}$ та $SD_{maxSRMd2-EDGE}$ в роботі були використані наступні метрики якості: помилки першого P_{FP} та другого P_{FN} роду, F_1 -індекс (1.27) та коефіцієнт кореляції Метьюса (1.28). Для оцінки середньої значення та розкиду значень даних показників процедура перехресної перевірки [144] повторювалася десять разів при розбитті тестового пакету зображень на навчальну (70%) та контрольну (30%) вибірки.

Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індекс та коефіцієнт кореляції Метьюса при використанні стегодетекторів SD_{SPAM} , $SD_{maxSRMd2}$ та $SD_{maxSRMd2-EDGE}$ для стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD наведені у додатку Г.1.

Г.1 Результати дослідження точності виявлення стеганогам, сформованих згідно адаптивних стеганографічних методів, при використанні запропонованого підходу до побудови стегодетекторів

Таблиця Г.1а – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганогам, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету ALASKA, в залежності від наявних апріорних даних щодо ACM і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,2	50,1	50,1	49,9	49,7	49,8	49,8	52,2	52,3	53,0	53,1	52,2	52,5	53,2	56,9	56,9	56,8	56,8	56,7	56,5	56,8	
	σ	0,65	0,23	0,41	0,61	0,48	0,44	0,42	1,10	1,10	1,55	1,74	0,84	1,20	1,82	0,64	0,87	0,98	0,39	1,24	1,56	1,09	
$P_{FN}, \%$	μ	50,2	50,1	50,1	49,9	49,7	49,8	49,8	52,2	52,5	53,2	53,0	52,4	52,7	53,5	57,1	57,1	57,1	57,0	56,8	56,7	57,0	
	σ	0,63	0,23	0,41	0,61	0,48	0,44	0,43	0,85	1,11	1,63	1,57	0,84	1,32	1,68	0,99	1,06	0,96	0,68	1,48	1,44	1,06	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,47	0,47	0,46	0,47	0,46	0,46	0,45	0,43	0,43	0,42	0,43	0,43	0,43	0,43	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
		σ	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,04	0,05	0,03	0,03	0,05	0,03	0,01	0,02	0,02	0,01	0,02	0,03	0,02
MCC	μ	0,00	0,00	0,00	0,00	0,01	0,00	0,00	-0,04	-0,05	-0,06	-0,06	-0,04	-0,05	-0,07	-0,14	-0,14	-0,14	-0,14	-0,13	-0,13	-0,14
	σ	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,02	0,02	0,03	0,03	0,01	0,02	0,04	0,02	0,02	0,02	0,01	0,03	0,03	0,02
Випадак використання векторів \mathbf{F}_{DF}																						
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
$P_{FN}, \%$	μ	14,0	10,9	6,2	3,4	2,0	1,4	1,2	14,0	10,8	6,2	3,3	2,0	1,5	1,1	14,0	10,7	6,2	3,4	2,0	1,5	1,3
	σ	0,53	0,37	0,29	0,24	0,12	0,14	0,20	0,33	0,34	0,25	0,18	0,24	0,18	0,12	0,25	0,46	0,27	0,20	0,15	0,14	0,09
F_1	μ	0,92	0,94	0,97	0,98	0,99	0,99	0,99	0,92	0,94	0,97	0,98	0,99	0,99	0,99	0,92	0,94	0,97	0,98	0,99	0,99	0,99
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
MCC	μ	0,85	0,88	0,94	0,97	0,98	0,99	0,99	0,85	0,89	0,94	0,97	0,98	0,98	0,99	0,85	0,89	0,94	0,97	0,98	0,98	0,99
	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00
Випадак використання векторів \mathbf{F}_{CC}																						

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
$P_{FP}, \%$	μ	0,7	1,2	2,1	3,0	2,6	1,9	1,3	2,8	2,5	3,0	3,6	2,8	2,5	1,6	8,4	5,5	4,2	4,3	3,1	2,8	2,2
	σ	0,19	0,41	0,67	0,46	0,56	0,31	0,25	0,69	1,05	0,87	0,42	0,50	0,55	0,38	1,78	1,50	0,75	1,06	0,66	1,00	0,56
$P_{FN}, \%$	μ	35,9	29,5	18,9	10,2	6,7	4,9	4,0	37,2	30,4	19,2	10,4	6,8	4,9	4,0	38,3	31,1	19,5	10,6	6,8	5,0	3,9
	σ	0,42	0,50	0,43	0,43	0,28	0,19	0,24	0,61	0,45	0,56	0,31	0,34	0,27	0,18	0,55	0,37	0,63	0,36	0,26	0,48	0,23
F_1	μ	0,78	0,82	0,89	0,93	0,95	0,97	0,97	0,77	0,82	0,88	0,93	0,95	0,96	0,97	0,75	0,80	0,88	0,93	0,95	0,96	0,97
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00
MCC	μ	0,53	0,63	0,77	0,86	0,91	0,93	0,95	0,49	0,61	0,76	0,86	0,90	0,93	0,94	0,44	0,58	0,75	0,85	0,90	0,92	0,94
	σ	0,01	0,01	0,00	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,00	0,01	0,00

Таблиця Г.1б – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегадетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стегаграфічного методу S-UNIWARD та тестових зображень з пакету ALASKA, в залежності від наявних апіорних даних щодо ACM і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	49,9	49,9	50,2	50,0	50,0	50,0	49,8	53,3	52,5	53,0	52,3	53,2	52,2	51,9	56,9	56,3	57,2	57,1	56,8	56,9	56,3	
	σ	0,51	0,48	0,68	0,24	0,58	0,57	0,63	1,72	1,16	1,48	0,71	1,36	0,96	0,59	0,73	0,98	0,55	0,81	0,89	1,19	1,06	
$P_{FN}, \%$	μ	49,8	49,9	50,2	50,0	50,0	50,1	49,8	53,0	52,5	52,8	52,1	52,8	52,1	52,2	57,1	56,5	57,1	56,9	56,9	56,8	56,6	
	σ	0,51	0,49	0,69	0,24	0,57	0,56	0,64	1,95	1,15	1,67	0,91	1,52	1,14	0,82	0,88	1,19	0,63	0,77	1,06	1,29	1,20	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,49	0,47	0,48	0,50	0,49	0,49	0,46	0,43	0,43	0,43	0,43	0,43	0,43	0,43	
	σ	0,00	0,01	0,01	0,00	0,01	0,01	0,01	0,04	0,04	0,03	0,04	0,04	0,04	0,05	0,02	0,02	0,02	0,01	0,02	0,02	0,02	
MCC	μ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-0,06	-0,05	-0,06	-0,04	-0,06	-0,04	-0,04	-0,14	-0,13	-0,14	-0,14	-0,14	-0,14	-0,13	
	σ	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,04	0,02	0,03	0,01	0,03	0,02	0,01	0,01	0,02	0,01	0,01	0,02	0,02	0,02	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів F_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	10,5	7,7	4,7	2,7	1,7	1,4	1,0	10,7	7,6	4,8	2,6	1,8	1,3	1,0	10,6	7,8	4,8	2,7	1,8	1,2	1,0	
	σ	0,29	0,27	0,20	0,21	0,13	0,12	0,09	0,37	0,19	0,32	0,16	0,14	0,13	0,12	0,15	0,32	0,30	0,20	0,21	0,20	0,11	
F_1	μ	0,94	0,96	0,98	0,99	0,99	0,99	0,99	0,94	0,96	0,98	0,99	0,99	0,99	0,99	0,94	0,96	0,98	0,99	0,99	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,89	0,92	0,95	0,97	0,98	0,99	0,99	0,89	0,92	0,95	0,97	0,98	0,99	0,99	0,89	0,92	0,95	0,97	0,98	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів F_{CC}																							
$P_{FP}, \%$	μ	0,4	0,3	1,4	1,7	1,3	0,9	0,6	2,0	0,8	1,9	2,1	2,0	0,9	0,8	5,3	2,2	2,3	2,7	1,9	1,4	1,0	
	σ	0,22	0,24	0,24	0,45	0,13	0,18	0,15	0,93	0,65	0,43	0,33	0,33	0,33	0,26	1,56	0,95	0,83	0,73	0,70	0,44	0,41	
P_{FN}	μ	30,0	23,0	13,7	8,0	5,2	3,8	2,9	31,8	23,7	13,9	7,8	5,0	3,8	2,9	32,8	24,0	14,1	8,0	5,2	3,9	3,0	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,73	0,48	0,39	0,41	0,23	0,16	0,20	0,75	0,67	0,47	0,25	0,25	0,35	0,29	0,66	0,69	0,26	0,49	0,19	0,30	0,23
	μ	0,82	0,87	0,92	0,95	0,97	0,98	0,98	0,81	0,86	0,92	0,95	0,97	0,98	0,98	0,79	0,86	0,92	0,95	0,96	0,97	0,98
MCC	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
	μ	0,63	0,73	0,84	0,90	0,93	0,95	0,96	0,59	0,72	0,83	0,90	0,93	0,95	0,96	0,55	0,71	0,83	0,89	0,93	0,95	0,96
	σ	0,01	0,01	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,00

Таблиця Г.1в – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету ALASKA, в залежності від наявних апіорних даних щодо АСМ і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,3	50,0	50,1	49,8	49,9	49,7	49,8	52,3	52,8	52,5	53,3	51,9	53,5	52,0	56,8	56,6	56,9	57,1	56,8	56,5	56,3	
	σ	0,59	0,37	0,56	0,48	0,60	0,48	0,46	1,25	1,19	1,77	1,43	0,68	1,64	1,01	1,20	1,09	0,52	0,89	0,61	0,64	1,16	
$P_{FN}, \%$	μ	50,3	50,0	50,1	49,8	49,9	49,7	49,8	52,4	52,7	52,7	53,3	52,2	53,5	52,1	57,0	56,8	56,9	57,0	56,9	56,5	56,5	
	σ	0,57	0,38	0,56	0,48	0,61	0,48	0,46	1,38	1,20	1,69	1,38	0,79	1,50	1,07	1,35	1,38	0,44	1,05	0,82	1,12	1,20	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,47	0,48	0,45	0,47	0,46	0,46	0,47	0,43	0,43	0,43	0,43	0,43	0,44	0,43	
	σ	0,01	0,00	0,01	0,00	0,01	0,01	0,01	0,04	0,02	0,06	0,03	0,04	0,04	0,06	0,02	0,03	0,01	0,02	0,02	0,03	0,01	
MCC	μ	-0,01	0,00	0,00	0,00	0,00	0,01	0,00	-0,05	-0,05	-0,05	-0,07	-0,04	-0,07	-0,04	-0,14	-0,13	-0,14	-0,14	-0,14	-0,13	-0,13	
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,03	0,02	0,03	0,03	0,01	0,03	0,02	0,02	0,02	0,01	0,02	0,01	0,02	0,02	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів F_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	8,6	6,6	4,4	2,8	1,8	1,4	1,3	8,7	6,6	4,3	2,9	1,9	1,4	1,2	8,5	6,7	4,5	2,9	1,9	1,5	1,3	
	σ	0,35	0,28	0,20	0,19	0,16	0,12	0,08	0,24	0,32	0,18	0,19	0,14	0,16	0,12	0,35	0,23	0,18	0,13	0,15	0,13	0,12	
F_1	μ	0,96	0,97	0,98	0,99	0,99	0,99	0,99	0,95	0,97	0,98	0,99	0,99	0,99	0,99	0,96	0,97	0,98	0,99	0,99	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,91	0,93	0,95	0,97	0,98	0,99	0,99	0,91	0,93	0,96	0,97	0,98	0,99	0,99	0,91	0,93	0,95	0,97	0,98	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів F_{CC}																							
$P_{FP}, \%$	μ	0,7	0,8	1,4	2,4	1,8	1,4	1,2	3,5	2,2	1,8	3,0	1,9	2,0	1,3	7,8	4,1	2,8	3,0	2,1	2,1	1,7	
	σ	0,28	0,27	0,63	0,35	0,35	0,44	0,41	0,85	0,97	0,57	0,73	0,46	0,43	0,25	1,89	1,26	0,88	0,88	0,40	0,50	0,40	
P_{FN}	μ	31,0	24,2	14,9	8,7	6,2	4,6	3,9	32,8	24,9	14,8	9,0	6,2	4,7	3,8	33,7	26,1	15,1	9,1	6,2	4,7	3,9	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,52	0,64	0,57	0,38	0,24	0,26	0,32	0,68	0,68	0,51	0,38	0,18	0,26	0,24	0,40	0,43	0,59	0,33	0,32	0,21	0,18
	μ	0,82	0,86	0,91	0,94	0,96	0,97	0,97	0,80	0,85	0,91	0,94	0,96	0,97	0,97	0,78	0,84	0,91	0,94	0,96	0,97	0,97
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
	μ	0,61	0,71	0,83	0,89	0,92	0,94	0,95	0,56	0,69	0,82	0,88	0,92	0,93	0,95	0,52	0,66	0,81	0,88	0,92	0,93	0,94
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,00	0,00

Таблиця Г.1г – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету ALASKA, в залежності від наявних апіорних даних щодо ACM і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,1	50,0	49,7	49,9	50,1	50,1	50,0	52,7	52,6	52,9	52,1	51,8	52,8	52,8	56,4	57,0	56,5	56,9	56,9	56,6	56,8	
	σ	0,49	0,46	0,79	0,39	0,46	0,43	0,42	1,10	1,54	1,07	1,18	0,89	1,49	1,48	1,58	1,20	0,87	1,11	0,63	1,03	1,37	
$P_{FN}, \%$	μ	50,1	50,0	49,7	49,9	50,1	50,1	50,0	52,5	52,8	52,7	52,4	52,0	52,8	52,9	56,5	57,2	56,9	56,8	56,7	57,3	57,1	
	σ	0,49	0,45	0,79	0,39	0,46	0,43	0,42	1,13	1,66	0,84	1,18	0,54	1,84	1,21	1,49	1,10	1,19	0,98	0,61	0,97	0,93	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,49	0,46	0,47	0,46	0,46	0,47	0,45	0,43	0,42	0,43	0,43	0,43	0,42	0,42	
	σ	0,01	0,01	0,01	0,00	0,01	0,00	0,01	0,03	0,05	0,03	0,04	0,04	0,06	0,04	0,01	0,02	0,02	0,02	0,01	0,01	0,01	
MCC	μ	0,00	0,00	0,01	0,00	0,00	0,00	0,00	-0,05	-0,05	-0,06	-0,05	-0,04	-0,06	-0,06	-0,13	-0,14	-0,13	-0,14	-0,14	-0,14	-0,14	
	σ	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,02	0,03	0,02	0,02	0,01	0,03	0,03	0,03	0,02	0,02	0,02	0,01	0,02	0,02	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	8,3	5,8	4,1	2,1	1,5	1,1	1,0	8,2	5,7	4,0	2,1	1,6	1,2	1,0	8,2	6,1	4,0	2,0	1,6	1,2	1,0	
	σ	0,24	0,29	0,22	0,15	0,14	0,12	0,12	0,23	0,26	0,18	0,19	0,12	0,15	0,10	0,24	0,30	0,23	0,16	0,08	0,16	0,11	
F_1	μ	0,96	0,97	0,98	0,99	0,99	0,99	1,00	0,96	0,97	0,98	0,99	0,99	0,99	1,00	0,96	0,97	0,98	0,99	0,99	0,99	1,00	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,91	0,94	0,96	0,98	0,98	0,99	0,99	0,91	0,94	0,96	0,98	0,98	0,99	0,99	0,91	0,94	0,96	0,98	0,98	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	0,1	0,4	1,6	1,7	1,3	1,1	1,0	1,3	1,1	2,0	2,1	1,9	1,4	1,2	2,9	2,2	3,0	2,6	1,7	1,8	1,5	
	σ	0,14	0,32	0,38	0,22	0,36	0,30	0,15	0,78	0,60	0,80	0,61	0,45	0,32	0,45	0,51	1,02	0,40	0,93	0,40	0,63	0,50	
P_{FN}	μ	26,6	19,4	11,7	6,4	4,9	3,9	3,0	28,4	19,5	11,8	6,5	4,9	3,8	2,9	28,9	20,0	12,1	6,5	4,9	3,8	3,0	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	1,04	0,48	0,32	0,35	0,24	0,22	0,25	0,76	0,40	0,36	0,25	0,33	0,28	0,21	0,83	0,35	0,32	0,25	0,19	0,22	0,26
	μ	0,85	0,89	0,93	0,96	0,97	0,97	0,98	0,83	0,89	0,93	0,96	0,97	0,97	0,98	0,82	0,88	0,92	0,95	0,97	0,97	0,98
	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00
MCC	μ	0,68	0,78	0,86	0,92	0,94	0,95	0,96	0,65	0,77	0,86	0,91	0,93	0,95	0,96	0,63	0,76	0,84	0,91	0,93	0,94	0,95
	σ	0,01	0,00	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,00

Таблиця Г.1д – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегадетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо АСМ і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,1	50,0	50,1	50,0	49,8	50,1	50,1	52,6	52,4	52,2	52,8	52,8	53,0	53,0	56,3	56,3	56,5	56,1	56,4	55,9	56,2	
	σ	0,53	0,60	0,38	0,33	0,50	0,46	0,43	1,19	1,41	1,10	1,60	1,09	1,81	1,49	0,73	0,77	0,72	0,64	1,02	0,86	0,92	
$P_{FN}, \%$	μ	50,1	50,0	50,1	50,0	49,8	50,1	50,1	52,5	52,7	52,4	52,8	52,8	52,9	52,9	56,5	56,3	56,5	55,9	56,1	56,3	56,0	
	σ	0,52	0,60	0,38	0,33	0,50	0,46	0,43	1,23	1,42	1,13	1,29	1,12	1,80	1,45	0,68	0,74	1,21	0,97	1,06	0,75	1,17	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,48	0,46	0,47	0,46	0,47	0,48	0,47	0,43	0,44	0,44	0,45	0,45	0,43	0,45	
	σ	0,00	0,01	0,00	0,00	0,01	0,01	0,00	0,04	0,03	0,04	0,04	0,03	0,03	0,03	0,01	0,01	0,03	0,02	0,02	0,02	0,03	
MCC	μ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-0,05	-0,05	-0,05	-0,05	-0,06	-0,06	-0,06	-0,13	-0,13	-0,13	-0,12	-0,12	-0,12	-0,12	
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,03	0,02	0,03	0,02	0,04	0,03	0,01	0,01	0,02	0,01	0,02	0,01	0,02	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	19,5	15,6	9,4	5,0	3,0	2,1	1,8	19,5	15,3	9,4	5,0	3,0	2,1	1,9	19,4	15,2	9,3	4,9	3,1	2,1	1,8	
	σ	0,32	0,33	0,38	0,15	0,15	0,13	0,13	0,24	0,42	0,31	0,27	0,16	0,12	0,16	0,28	0,26	0,29	0,27	0,19	0,16	0,21	
F_1	μ	0,89	0,92	0,95	0,97	0,98	0,99	0,99	0,89	0,92	0,95	0,97	0,98	0,99	0,99	0,89	0,92	0,95	0,97	0,98	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,78	0,83	0,90	0,95	0,97	0,98	0,98	0,78	0,83	0,90	0,95	0,97	0,98	0,98	0,78	0,83	0,90	0,95	0,97	0,98	0,98	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	0,9	1,4	1,7	1,5	1,3	0,9	0,6	5,5	4,0	2,3	2,2	2,0	1,8	0,9	13,9	7,4	4,1	3,3	2,6	2,1	1,1	
	σ	0,21	0,29	0,31	0,21	0,32	0,21	0,20	1,74	0,78	0,61	0,79	0,36	0,58	0,23	1,68	1,10	0,75	1,28	0,66	1,08	0,40	
P_{FN}	μ	38,6	33,7	25,6	14,9	9,6	6,5	5,2	40,2	34,8	26,4	14,9	9,4	6,7	5,1	41,2	35,5	26,5	15,2	9,7	6,6	5,1	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,38	0,59	0,61	0,53	0,34	0,16	0,25	0,61	0,49	0,63	0,51	0,30	0,17	0,27	0,45	0,80	0,56	0,35	0,17	0,20	0,17
	μ	0,76	0,80	0,85	0,91	0,94	0,96	0,97	0,74	0,78	0,84	0,91	0,94	0,96	0,97	0,73	0,77	0,84	0,91	0,94	0,96	0,97
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,01	0,00	0,00	0,00
	μ	0,47	0,56	0,69	0,83	0,89	0,93	0,94	0,42	0,53	0,67	0,82	0,88	0,91	0,94	0,36	0,50	0,66	0,81	0,87	0,91	0,94
	σ	0,01	0,01	0,01	0,01	0,01	0,00	0,00	0,02	0,01	0,01	0,00	0,00	0,01	0,00	0,01	0,02	0,01	0,01	0,01	0,01	0,00

Таблиця Г.1е – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,0	49,9	49,8	50,0	50,2	49,9	50,4	53,1	52,3	52,6	52,9	53,5	53,0	52,8	56,5	55,8	56,3	56,4	56,0	56,8	55,8	
	σ	0,50	0,22	0,43	0,43	0,46	0,35	0,49	1,27	1,25	1,56	1,67	1,52	1,57	1,38	0,66	1,04	0,61	0,52	1,49	0,50	0,91	
$P_{FN}, \%$	μ	50,0	49,9	49,8	50,0	50,2	49,9	50,4	53,1	52,2	52,7	52,8	53,7	52,9	52,7	56,2	56,1	56,6	56,3	55,9	56,7	55,9	
	σ	0,49	0,22	0,43	0,42	0,46	0,35	0,49	1,63	1,21	1,66	1,56	1,26	1,73	1,43	0,76	1,12	0,76	0,53	0,95	0,59	0,60	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,48	0,48	0,46	0,47	0,45	0,48	0,48	0,44	0,43	0,43	0,44	0,44	0,43	0,44	
	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,04	0,05	0,03	0,03	0,04	0,03	0,02	0,02	0,02	0,01	0,01	0,02	0,02	0,01	
MCC	μ	0,00	0,00	0,00	0,00	0,00	0,00	-0,01	-0,06	-0,04	-0,05	-0,06	-0,07	-0,06	-0,05	-0,13	-0,12	-0,13	-0,13	-0,12	-0,13	-0,12	
	σ	0,01	0,00	0,01	0,01	0,01	0,01	0,01	0,03	0,02	0,03	0,03	0,03	0,03	0,03	0,01	0,02	0,01	0,01	0,02	0,01	0,01	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	14,4	10,7	6,2	5,0	2,5	2,0	1,7	14,3	10,7	6,4	5,0	2,6	2,0	1,7	14,3	10,8	6,5	5,0	2,5	2,0	1,7	
	σ	0,26	0,32	0,18	0,20	0,24	0,15	0,16	0,30	0,19	0,22	0,22	0,15	0,15	0,11	0,32	0,36	0,22	0,33	0,19	0,11	0,20	
F_1	μ	0,92	0,94	0,97	0,97	0,99	0,99	0,99	0,92	0,94	0,97	0,97	0,99	0,99	0,99	0,92	0,94	0,97	0,97	0,99	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,84	0,89	0,94	0,95	0,97	0,98	0,98	0,84	0,89	0,93	0,95	0,97	0,98	0,98	0,84	0,89	0,93	0,95	0,97	0,98	0,98	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	2,2	1,2	0,7	1,4	0,8	0,7	0,5	6,9	2,4	1,4	2,3	1,7	1,1	0,9	12,0	5,2	3,1	2,9	1,5	1,2	1,0	
	σ	0,51	0,34	0,22	0,32	0,30	0,36	0,11	2,12	0,64	0,52	0,73	0,77	0,58	0,44	2,01	1,56	1,21	0,63	0,45	0,44	0,65	
P_{FN}	μ	31,2	25,9	18,2	14,9	7,1	5,0	4,1	32,9	27,1	18,7	14,9	6,9	4,9	3,9	33,8	27,8	19,1	15,1	7,0	5,2	4,0	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,57	0,34	0,30	0,39	0,28	0,26	0,30	0,78	0,48	0,48	0,46	0,19	0,23	0,19	0,58	0,55	0,48	0,37	0,27	0,21	0,18
	μ	0,81	0,85	0,90	0,91	0,96	0,97	0,98	0,79	0,84	0,89	0,91	0,96	0,97	0,98	0,77	0,83	0,88	0,91	0,96	0,97	0,97
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00
	μ	0,60	0,69	0,79	0,83	0,92	0,94	0,95	0,54	0,66	0,78	0,82	0,91	0,94	0,95	0,50	0,63	0,76	0,81	0,91	0,94	0,95
	σ	0,01	0,00	0,00	0,00	0,01	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,00	0,00	0,02	0,01	0,01	0,01	0,01	0,01	0,01

Таблиця Г.1ж – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету VISION, в залежності від наявних апіорних даних щодо ACM і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,2	50,3	50,3	50,1	49,8	50,0	50,0	53,1	53,1	52,6	52,5	53,2	52,7	53,5	56,4	56,6	56,8	57,1	57,2	57,0	57,0	
	σ	0,49	0,30	0,45	0,36	0,51	0,64	0,35	1,60	1,58	1,47	1,39	1,79	1,37	1,59	1,08	0,87	0,69	0,58	0,36	0,39	0,71	
$P_{FN}, \%$	μ	50,2	50,3	50,3	50,1	49,8	50,0	50,0	53,3	52,9	52,5	52,8	53,1	52,9	53,7	56,5	56,7	56,5	57,1	57,4	57,2	56,8	
	σ	0,48	0,31	0,45	0,36	0,50	0,65	0,36	1,63	1,54	1,80	1,35	1,72	1,45	1,70	1,30	1,16	0,52	0,50	0,53	0,47	0,74	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,46	0,48	0,49	0,45	0,47	0,46	0,46	0,43	0,43	0,44	0,43	0,42	0,43	0,44	
	σ	0,01	0,01	0,00	0,00	0,01	0,01	0,01	0,03	0,03	0,04	0,06	0,03	0,03	0,03	0,03	0,02	0,01	0,01	0,01	0,01	0,01	
MCC	μ	0,00	-0,01	-0,01	0,00	0,00	0,00	0,00	-0,06	-0,06	-0,05	-0,05	-0,06	-0,06	-0,07	-0,13	-0,13	-0,13	-0,14	-0,15	-0,14	-0,14	
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,03	0,03	0,03	0,03	0,04	0,03	0,03	0,02	0,02	0,01	0,01	0,01	0,01	0,01	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	14,7	10,8	6,8	4,2	3,0	2,4	1,9	14,5	10,9	6,8	4,2	3,0	2,3	1,9	14,7	11,0	6,8	4,0	3,0	2,3	1,9	
	σ	0,26	0,39	0,30	0,20	0,21	0,21	0,13	0,40	0,36	0,11	0,19	0,18	0,13	0,10	0,34	0,52	0,24	0,26	0,13	0,15	0,18	
F_1	μ	0,92	0,94	0,96	0,98	0,98	0,99	0,99	0,92	0,94	0,96	0,98	0,98	0,99	0,99	0,92	0,94	0,96	0,98	0,98	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,84	0,89	0,93	0,96	0,97	0,98	0,98	0,84	0,88	0,93	0,96	0,97	0,98	0,98	0,84	0,88	0,93	0,96	0,97	0,98	0,98	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	2,0	1,1	0,8	1,2	0,9	0,9	1,4	7,9	4,1	2,6	1,9	1,6	2,0	1,6	14,7	8,6	2,9	2,7	2,1	2,0	1,7	
	σ	0,49	0,36	0,25	0,21	0,21	0,36	0,38	1,50	1,19	1,24	0,45	0,44	0,52	0,74	2,76	1,45	1,02	1,21	1,00	0,96	0,71	
P_{FN}	μ	33,8	29,2	21,0	12,7	8,6	6,6	4,7	35,7	31,0	22,0	12,9	8,6	6,5	4,8	37,1	31,6	23,0	13,3	9,1	6,7	4,9	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,59	0,52	0,61	0,49	0,30	0,18	0,24	0,53	0,64	0,67	0,56	0,33	0,17	0,42	0,62	0,55	0,41	0,30	0,35	0,26	0,25
	μ	0,79	0,83	0,88	0,93	0,95	0,96	0,97	0,77	0,81	0,87	0,92	0,95	0,96	0,97	0,75	0,79	0,86	0,92	0,94	0,96	0,97
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,01	0,00
	μ	0,56	0,64	0,76	0,85	0,90	0,92	0,94	0,49	0,59	0,73	0,84	0,89	0,91	0,94	0,43	0,55	0,71	0,83	0,89	0,91	0,93
	σ	0,01	0,01	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,02	0,02	0,01	0,01	0,01	0,01	0,01

Таблиця Г.1и – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету VISION, в залежності від наявних апріорних даних щодо ACM і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,1	50,1	49,9	49,8	49,8	49,9	50,0	53,1	53,3	53,4	52,7	52,9	52,9	52,5	57,2	56,9	56,8	57,2	56,4	56,9	56,7	
	σ	0,50	0,44	0,48	0,49	0,45	0,79	0,30	1,66	1,58	1,59	1,26	1,70	1,88	1,52	0,82	0,45	0,85	0,64	1,24	0,95	1,08	
$P_{FN}, \%$	μ	50,0	50,1	49,8	49,8	49,8	49,9	50,0	53,1	53,5	53,4	52,6	52,6	52,7	52,4	57,1	57,0	56,7	57,1	56,4	56,8	57,0	
	σ	0,50	0,44	0,48	0,49	0,45	0,79	0,30	1,63	1,45	1,48	1,17	1,87	1,66	1,54	0,79	0,57	0,96	0,53	1,36	0,97	1,03	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,47	0,45	0,46	0,47	0,49	0,47	0,47	0,43	0,43	0,44	0,43	0,44	0,43	0,43	
	σ	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,03	0,05	0,03	0,06	0,04	0,04	0,04	0,01	0,01	0,02	0,01	0,02	0,01	0,02	
MCC	μ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-0,06	-0,07	-0,07	-0,05	-0,05	-0,05	-0,05	-0,14	-0,14	-0,13	-0,14	-0,13	-0,14	-0,14	
	σ	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,03	0,03	0,03	0,02	0,04	0,03	0,03	0,01	0,01	0,02	0,01	0,03	0,02	0,02	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	11,0	7,4	4,8	3,0	2,4	1,9	1,4	10,9	7,7	4,8	2,9	2,5	1,9	1,4	10,9	7,7	4,9	2,9	2,4	1,9	1,5	
	σ	0,52	0,35	0,30	0,10	0,21	0,15	0,16	0,29	0,29	0,20	0,17	0,19	0,17	0,11	0,25	0,31	0,28	0,17	0,19	0,17	0,15	
F_1	μ	0,94	0,96	0,98	0,98	0,99	0,99	0,99	0,94	0,96	0,98	0,99	0,99	0,99	0,99	0,94	0,96	0,98	0,99	0,99	0,99	0,99	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,88	0,92	0,95	0,97	0,98	0,98	0,99	0,88	0,92	0,95	0,97	0,97	0,98	0,99	0,88	0,92	0,95	0,97	0,98	0,98	0,98	
	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	1,4	0,7	0,6	0,5	0,6	0,4	0,4	5,3	2,1	1,7	2,1	1,4	0,9	0,8	9,4	3,9	3,6	1,9	1,6	1,6	0,9	
	σ	0,51	0,29	0,11	0,21	0,19	0,19	0,13	1,36	0,70	0,91	0,75	0,66	0,62	0,42	2,56	1,44	1,09	1,25	0,74	0,60	0,38	
P_{FN}	μ	26,7	21,8	15,0	9,1	6,1	4,8	4,1	28,5	22,7	15,3	9,0	6,3	4,8	4,2	29,4	23,5	15,5	9,3	6,4	5,2	4,3	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,62	0,60	0,35	0,31	0,30	0,28	0,15	0,47	0,63	0,42	0,32	0,28	0,20	0,25	0,57	0,78	0,44	0,31	0,34	0,29	0,26
	μ	0,84	0,88	0,92	0,95	0,97	0,97	0,98	0,82	0,87	0,91	0,94	0,96	0,97	0,97	0,80	0,86	0,90	0,94	0,96	0,97	0,97
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,01	0,00	0,00	0,00
	μ	0,67	0,75	0,83	0,90	0,93	0,95	0,95	0,62	0,72	0,82	0,89	0,92	0,94	0,95	0,58	0,70	0,80	0,89	0,92	0,93	0,95
	σ	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,01	0,01	0,01	0,00	0,02	0,01	0,01	0,01	0,01	0,01	0,00

Таблиця Г.1к – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу HUGO та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апіорних даних щодо АСМ і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	49,9	49,9	50,2	50,0	50,0	50,1	50,3	52,7	53,0	52,5	52,9	53,1	52,3	53,3	57,2	56,9	56,4	56,8	57,0	56,0	57,0	
	σ	0,49	0,68	0,54	0,44	0,38	0,42	0,33	1,41	1,51	1,44	1,39	1,40	1,40	1,68	0,35	0,69	1,81	1,29	1,03	1,80	0,76	
$P_{FN}, \%$	μ	49,9	49,9	50,2	50,0	50,0	50,1	50,3	52,6	52,9	52,6	52,8	53,1	52,2	53,3	57,1	57,2	56,8	56,8	56,7	56,1	57,0	
	σ	0,49	0,68	0,54	0,44	0,39	0,42	0,33	1,27	1,61	1,53	1,71	1,43	1,54	1,69	0,57	0,49	1,14	0,94	1,26	1,61	0,62	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,47	0,47	0,47	0,49	0,47	0,48	0,47	0,43	0,42	0,42	0,43	0,44	0,43	0,43	
	σ	0,01	0,01	0,01	0,00	0,00	0,00	0,00	0,03	0,07	0,04	0,04	0,03	0,05	0,04	0,01	0,01	0,02	0,01	0,02	0,02	0,01	
MCC	μ	0,00	0,00	0,00	0,00	0,00	0,00	-0,01	-0,05	-0,06	-0,05	-0,06	-0,06	-0,04	-0,07	-0,14	-0,14	-0,13	-0,14	-0,14	-0,12	-0,14	
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,01	0,01	0,03	0,02	0,02	0,03	0,01	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	26,4	22,9	17,5	11,4	8,3	6,2	4,4	26,6	22,8	17,5	11,5	8,3	6,1	4,4	26,5	23,0	17,5	11,3	8,3	6,1	4,4	
	σ	0,27	0,24	0,36	0,35	0,22	0,28	0,18	0,36	0,33	0,51	0,37	0,27	0,34	0,29	0,26	0,43	0,23	0,23	0,34	0,27	0,21	
F_1	μ	0,85	0,87	0,90	0,94	0,96	0,97	0,98	0,85	0,87	0,90	0,94	0,96	0,97	0,98	0,85	0,87	0,90	0,94	0,96	0,97	0,98	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,69	0,74	0,81	0,88	0,91	0,94	0,96	0,68	0,74	0,81	0,88	0,91	0,94	0,95	0,69	0,73	0,81	0,88	0,91	0,94	0,95	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	0,3	0,5	2,6	10,4	10,9	9,2	7,9	30,8	9,3	6,4	13,2	12,1	10,0	8,2	46,4	20,0	11,6	14,4	12,9	10,4	8,7	
	σ	0,21	0,15	0,38	1,12	0,65	0,62	0,38	5,36	2,45	1,24	1,26	0,96	0,55	0,68	2,45	4,02	1,40	1,07	1,15	0,51	0,76	
P_{FN}	μ	41,1	37,8	32,9	24,9	18,2	13,5	10,1	46,4	41,4	34,2	25,3	18,9	14,1	10,6	49,0	42,7	35,2	26,0	19,1	14,2	10,8	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,42	0,73	0,20	0,28	0,38	0,42	0,54	0,66	0,44	0,27	0,35	0,39	0,34	0,56	0,59	0,64	0,44	0,35	0,54	0,37	0,55
	μ	0,74	0,77	0,80	0,83	0,86	0,89	0,91	0,67	0,73	0,78	0,81	0,85	0,88	0,91	0,62	0,71	0,77	0,81	0,84	0,88	0,90
MCC	σ	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,01	0,01	0,00	0,00
	μ	0,42	0,49	0,57	0,63	0,71	0,77	0,82	0,17	0,37	0,53	0,60	0,69	0,76	0,81	0,04	0,29	0,48	0,58	0,68	0,75	0,80
	σ	0,01	0,01	0,00	0,01	0,00	0,00	0,00	0,04	0,02	0,01	0,01	0,01	0,00	0,00	0,02	0,03	0,01	0,01	0,01	0,01	0,01

Таблиця Г.1л – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу S-UNIWARD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,0	50,2	50,0	50,0	50,1	49,8	50,1	52,6	51,9	52,5	52,0	53,2	52,3	52,1	57,1	56,8	57,0	56,8	56,4	57,3	56,7	
	σ	0,60	0,41	0,79	0,45	0,52	0,28	0,48	1,48	0,80	1,51	1,22	1,65	1,32	1,24	0,97	1,07	1,27	1,22	0,89	0,42	1,61	
$P_{FN}, \%$	μ	50,0	50,2	49,9	50,0	50,1	49,8	50,1	52,7	51,9	52,5	52,1	53,2	52,4	52,3	56,9	57,1	57,1	57,0	56,6	57,1	56,6	
	σ	0,61	0,41	0,79	0,45	0,52	0,28	0,49	1,45	0,57	1,51	0,96	1,41	1,35	1,11	0,92	1,14	1,08	1,30	0,78	0,40	1,42	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,46	0,47	0,47	0,47	0,46	0,46	0,46	0,43	0,42	0,43	0,43	0,43	0,43	0,43	
	σ	0,01	0,01	0,01	0,01	0,01	0,00	0,01	0,05	0,05	0,04	0,04	0,03	0,05	0,04	0,02	0,02	0,01	0,02	0,01	0,01	0,01	
MCC	μ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-0,05	-0,04	-0,05	-0,04	-0,06	-0,05	-0,04	-0,14	-0,14	-0,14	-0,14	-0,13	-0,14	-0,13	
	σ	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,03	0,01	0,03	0,02	0,03	0,03	0,02	0,02	0,02	0,02	0,02	0,02	0,01	0,03	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадак використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	24,3	20,6	15,7	10,4	7,5	5,7	4,3	24,4	20,6	15,6	10,5	7,5	5,7	4,3	24,2	20,5	15,7	10,3	7,4	5,5	4,3	
	σ	0,31	0,32	0,37	0,31	0,21	0,30	0,26	0,42	0,28	0,28	0,23	0,17	0,21	0,37	0,26	0,20	0,27	0,17	0,32	0,31	0,28	
F_1	μ	0,86	0,88	0,91	0,94	0,96	0,97	0,98	0,86	0,89	0,92	0,94	0,96	0,97	0,98	0,86	0,89	0,91	0,95	0,96	0,97	0,98	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,72	0,77	0,83	0,89	0,92	0,94	0,96	0,72	0,77	0,83	0,89	0,92	0,94	0,96	0,72	0,77	0,83	0,89	0,92	0,94	0,96	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадак використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	0,4	0,4	3,7	10,0	9,6	8,5	6,6	16,9	4,0	6,7	11,4	10,5	8,8	7,2	33,5	13,6	10,2	11,5	11,5	9,7	7,3	
	σ	0,32	0,24	1,02	0,77	0,68	0,52	0,70	2,24	1,31	2,17	1,16	0,98	0,49	0,54	3,61	3,37	2,05	1,12	1,42	0,37	0,63	
P_{FN}	μ	40,0	36,1	30,3	22,3	16,1	12,1	9,8	44,4	39,1	31,2	22,9	16,4	12,6	9,9	46,3	40,5	32,0	23,3	16,7	12,8	10,3	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,63	0,35	0,50	0,57	0,73	0,57	0,51	0,59	0,50	0,32	0,48	0,55	0,28	0,71	0,56	0,66	0,62	0,53	0,45	0,45	0,51
	μ	0,75	0,78	0,81	0,84	0,87	0,90	0,92	0,70	0,75	0,80	0,83	0,87	0,89	0,92	0,67	0,73	0,79	0,83	0,86	0,89	0,91
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,01	0,01	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,01	0,00	0,00
	μ	0,44	0,53	0,60	0,67	0,74	0,79	0,83	0,27	0,45	0,57	0,65	0,73	0,79	0,83	0,16	0,37	0,54	0,64	0,72	0,77	0,82
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,02	0,01	0,01	0,00	0,01	0,03	0,03	0,02	0,01	0,01	0,01	0,00

Таблиця Г.1м – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу MG та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,3	50,0	50,0	49,9	50,1	50,0	50,0	52,9	53,6	53,1	52,6	53,2	52,0	52,7	57,1	56,3	57,2	57,3	57,3	56,5	57,0	
	σ	0,41	0,34	0,49	0,48	0,40	0,54	0,40	1,41	1,52	1,49	1,48	1,40	1,31	1,47	0,70	1,28	0,68	0,78	0,51	1,50	1,30	
$P_{FN}, \%$	μ	50,3	50,0	50,0	49,9	50,1	50,0	50,0	52,6	53,2	53,1	52,6	53,0	52,1	53,0	57,2	56,6	57,1	57,4	57,2	56,6	57,1	
	σ	0,41	0,33	0,48	0,48	0,40	0,54	0,40	1,45	1,80	1,44	1,56	1,73	1,35	1,34	0,73	1,37	0,77	0,83	0,43	1,33	1,25	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,49	0,49	0,47	0,47	0,48	0,47	0,45	0,43	0,43	0,43	0,43	0,43	0,43	0,43	
	σ	0,01	0,00	0,01	0,01	0,00	0,01	0,01	0,03	0,04	0,03	0,05	0,04	0,06	0,03	0,02	0,02	0,02	0,01	0,01	0,02	0,02	
MCC	μ	-0,01	0,00	0,00	0,00	0,00	0,00	0,00	-0,05	-0,07	-0,06	-0,05	-0,06	-0,04	-0,06	-0,14	-0,13	-0,14	-0,15	-0,14	-0,13	-0,14	
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,03	0,03	0,03	0,03	0,03	0,03	0,03	0,01	0,03	0,01	0,01	0,01	0,03	0,02	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	19,8	16,6	10,8	7,6	5,9	4,7	3,9	19,6	16,4	10,9	7,4	5,8	4,8	4,0	19,6	16,2	10,9	7,4	5,9	4,9	3,8	
	σ	0,46	0,28	0,13	0,27	0,27	0,30	0,19	0,39	0,42	0,35	0,36	0,27	0,37	0,23	0,38	0,41	0,23	0,24	0,41	0,31	0,17	
F_1	μ	0,89	0,91	0,94	0,96	0,97	0,98	0,98	0,89	0,91	0,94	0,96	0,97	0,98	0,98	0,89	0,91	0,94	0,96	0,97	0,97	0,98	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,78	0,82	0,89	0,92	0,94	0,95	0,96	0,78	0,82	0,88	0,92	0,94	0,95	0,96	0,78	0,82	0,88	0,92	0,94	0,95	0,96	
	σ	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів \mathbf{F}_{CC}																							
$P_{FP}, \%$	μ	2,5	2,4	6,7	8,7	8,3	7,9	7,4	16,3	8,5	8,2	9,8	9,4	8,3	7,7	25,5	15,2	11,5	11,6	10,4	8,5	8,7	
	σ	0,85	0,78	0,93	0,75	0,45	0,61	0,55	3,09	1,54	0,84	0,52	0,56	0,79	0,31	2,45	2,23	1,80	0,90	1,28	0,76	0,67	
P_{FN}	μ	36,2	32,9	26,4	19,0	15,5	12,6	10,8	40,2	35,5	27,5	19,6	16,1	13,0	11,4	42,0	37,0	28,6	20,2	16,0	13,4	11,6	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,36	0,42	0,60	0,37	0,63	0,51	0,42	0,48	0,48	0,39	0,70	0,57	0,43	0,48	0,22	0,58	0,37	0,54	0,61	0,47	0,53
	μ	0,78	0,80	0,83	0,86	0,88	0,90	0,91	0,73	0,77	0,82	0,86	0,87	0,89	0,91	0,70	0,75	0,80	0,85	0,87	0,89	0,90
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,01	0,00	0,00	0,00	0,00
	μ	0,51	0,57	0,64	0,72	0,76	0,79	0,82	0,36	0,49	0,61	0,70	0,74	0,79	0,81	0,28	0,42	0,57	0,68	0,73	0,78	0,80
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,00	0,02	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01

Таблиця Г.1н – Середні значення (μ) та середньоквадратичне відхилення (σ) значень метрик P_{FP} , P_{FN} , F_1 -індексу та MCC при використанні стегодетектору SD_{SRR} для виявлення стеганограм, сформованих згідно стеганографічного методу MiPOD та тестових зображень з пакету MIRFlickr-1M, в залежності від наявних апріорних даних щодо АСМ і виду запропонованих векторів (статистичних параметрів оброблюваних зображень)

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів \mathbf{F}_{calib}																							
$P_{FP}, \%$	μ	50,1	50,1	49,8	49,8	50,1	50,1	50,2	52,8	52,2	53,0	52,0	52,2	52,5	53,1	57,1	56,6	57,0	57,0	56,1	56,8	56,7	
	σ	0,47	0,46	0,36	0,50	0,47	0,44	0,42	1,72	0,92	1,74	1,06	1,73	1,22	1,49	1,05	0,85	0,69	0,77	1,33	0,84	1,23	
$P_{FN}, \%$	μ	50,1	50,1	49,8	49,8	50,1	50,1	50,2	53,0	52,0	52,8	51,9	52,5	52,6	53,0	57,3	57,0	57,0	56,9	56,1	57,0	56,9	
	σ	0,47	0,46	0,37	0,50	0,47	0,44	0,43	1,79	1,02	1,57	1,17	1,72	1,49	1,44	1,17	0,84	1,06	1,03	1,30	0,85	0,77	
F_1	μ	0,50	0,50	0,50	0,50	0,50	0,50	0,50	0,45	0,49	0,47	0,49	0,45	0,47	0,47	0,43	0,42	0,43	0,43	0,44	0,43	0,43	
	σ	0,00	0,00	0,00	0,01	0,00	0,01	0,00	0,05	0,04	0,04	0,05	0,05	0,04	0,03	0,02	0,01	0,02	0,02	0,02	0,01	0,01	
MCC	μ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	-0,06	-0,04	-0,06	-0,04	-0,05	-0,05	-0,06	-0,14	-0,14	-0,14	-0,14	-0,12	-0,14	-0,14	
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,03	0,02	0,03	0,02	0,03	0,03	0,03	0,02	0,02	0,02	0,02	0,03	0,02	0,02	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim U(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$							
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	
Випадок використання векторів F_{DF}																							
$P_{FP}, \%$	μ	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	0,0	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
$P_{FN}, \%$	μ	22,0	18,5	13,9	10,0	8,0	6,1	5,1	21,8	18,6	13,9	10,0	8,0	6,1	5,1	22,2	18,5	13,9	10,2	7,9	6,2	5,2	
	σ	0,45	0,46	0,32	0,35	0,24	0,35	0,27	0,36	0,30	0,31	0,20	0,26	0,25	0,30	0,46	0,48	0,34	0,27	0,23	0,27	0,29	
F_1	μ	0,88	0,90	0,93	0,95	0,96	0,97	0,97	0,88	0,90	0,93	0,95	0,96	0,97	0,97	0,87	0,90	0,93	0,95	0,96	0,97	0,97	
	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	
MCC	μ	0,75	0,79	0,85	0,89	0,92	0,94	0,95	0,75	0,79	0,85	0,89	0,92	0,94	0,95	0,75	0,79	0,85	0,89	0,92	0,94	0,95	
	σ	0,01	0,01	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,01	0,00	0,00	0,00	0,00	0,00	
Випадок використання векторів F_{CC}																							
$P_{FP}, \%$	μ	0,4	0,7	6,2	10,6	9,8	8,8	8,3	5,8	3,4	8,4	12,1	10,6	9,6	8,4	21,0	7,0	10,6	12,4	12,3	10,5	8,9	
	σ	0,17	0,29	0,65	0,56	0,59	0,65	0,31	1,84	1,01	1,59	1,46	0,73	0,56	0,62	3,42	1,82	1,78	1,16	1,12	0,65	0,75	
P_{FN}	μ	38,7	34,1	28,5	22,0	17,6	14,4	12,3	41,8	36,1	29,3	22,7	18,2	14,8	12,8	43,5	37,0	30,0	23,3	18,5	15,1	12,7	

		$K_{\alpha}^{OL} = 100\%$							$K_{\alpha}^{OL} \sim \mathcal{U}(0; 100), \%$							$K_{\alpha}^{OL} = 0\%$						
		$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$	$\Delta_{\alpha}^S = 3\%$	$\Delta_{\alpha}^S = 5\%$	$\Delta_{\alpha}^S = 10\%$	$\Delta_{\alpha}^S = 20\%$	$\Delta_{\alpha}^S = 30\%$	$\Delta_{\alpha}^S = 40\%$	$\Delta_{\alpha}^S = 50\%$
F_1	σ	0,29	0,47	0,34	0,31	0,46	0,38	0,37	0,43	0,49	0,25	0,29	0,39	0,30	0,64	0,49	0,33	0,46	0,51	0,43	0,56	0,67
	μ	0,76	0,79	0,82	0,84	0,87	0,89	0,90	0,73	0,77	0,81	0,83	0,86	0,88	0,90	0,70	0,76	0,80	0,83	0,85	0,87	0,89
MCC	σ	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,01	0,00	0,00	0,00	0,01	0,00	0,01	0,00	0,01	0,00	0,00
	μ	0,47	0,56	0,61	0,66	0,72	0,77	0,79	0,38	0,51	0,59	0,64	0,71	0,75	0,79	0,27	0,47	0,56	0,63	0,69	0,74	0,78
	σ	0,01	0,01	0,01	0,01	0,01	0,01	0,00	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,02	0,01	0,01	0,01	0,01