Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ПРОГОНОВ ДМИТРО ОЛЕКСАНДРОВИЧ

УДК 004.[056.5+932.2]

СТРУКТУРНИЙ СИНТЕЗ ТА ПАРАМЕТРИЧНА ОПТИМІЗАЦІЯ МЕТОДІВ ПОБУДОВИ СТЕГОДЕТЕКТОРІВ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ

Спеціальність 05.13.21 – системи захисту інформації

РЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2024

Дисертацією є рукопис.
Робота виконана у Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського» на кафедрі інформаційної безпеки.

Науковий консультант: доктор технічних наук, професор
Мачуський Євген Андрійович,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри інформаційної безпеки

Офіційні опоненти: доктор технічних наук, професор
Кобозєва Алла Анатоліївна,
Одеський національний університет імені І.І.Мечникова, професор кафедри комп'ютерних систем і технологій

доктор технічних наук, професор
Халімов Геннадій Зайдулович,
Харківський національний університет радіоелектроніки, завідувач кафедри безпеки інформаційних технологій

доктор технічних наук, професор
Шелест Михайло Євгенович,
Національний університет "Чернігівська політехніка", професор кафедри кібербезпеки та математичного моделювання

Захист відбудеться «31» жовтня 2024 р. о 15 год. на засіданні спеціалізованої вченої ради Д 26.002.29 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» за адресою: 03056, м. Київ, пр. Берестейський, 37, корп. №1, ауд. 05.

Захист транслюватиметься на YouTube-каналі Вченої ради КПІ ім. Ігоря Сікорського: https://www.youtube.com/@vchenaradakpi/streams

З дисертацією можна ознайомитись у Науково-технічній бібліотеці ім. Г.І. Денисенка Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», за адресою: 03056, м. Київ, проспект Берестейський, 37, та на сайті Вченої ради Університету за адресою: https://rada.kpi.ua.

Про дату та місце захисту громадськість проінформовано «___» _____ 20___ р.

Учений секретар
спеціалізованої вченої ради Д.26.002.29
доктор технічних наук, професор Андрій ШЕЛЕСТОВ

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Порушення роботи систем критичної інфраструктури (СКІ) державних установ і приватних корпорацій, особливо в умовах військових дій, може призвести до несанкціонованого витоку інформації з обмеженим доступом (ІзОД), а також суттєвих втрат у економічній, соціальній, політичній та військових сферах. Це підтверджується низкою успішних кібератак на інформаційну інфраструктуру державних установ (а саме державні реєстри громадян США та Аргентини, реєстри співробітників міністерств оборони Великобританії, Німеччини, Франції, Японії, системи керування енергетичною інфраструктурою України), провідних міжнародних корпорацій (серед яких X (Twitter), LinkedIn, CloudFlare, Weibo, Tencent, JBS Foods, Mercedes Benz Group) та фінансових організацій (наприклад, JPMorgan Chase, Shinsei bank, Heartland Payment Systems, Binance) протягом 2020-2024 років.

Ефективна протидія використанню противником (конкурентом) несилових методів впливу для порушення роботи СКІ потребує запровадження багаторівневого та всеосяжного захисту критичної інформаційної інфраструктури державних та приватних організацій. Особлива увага приділяється заходам, спрямованим 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.

Розробкою систем виявлення та протидії роботі стеганографічних каналів зв’язку при обміні даними в ІКС займаються міжнародні та державні установи (наприклад, проект «The Criminal Use of Information Hiding» за підтримки Європейського Союзу, проект «Computer Forensics Tools & Techniques Catalog» Національного інституту стандартів і технології США, Державний центр кіберзахисту Державної служби спеціального зв’язку та захисту інформації України), провідні ІТ-корпорації (серед яких FireEye, Google, Cisco, Trend-Micro), а також групи науковців провідних науково-дослідних установ світу, насамперед університету Бінгемтону (США), Оксфордського університету (Великобританія), Лілльського університету (Франція), Сієнського університету (Італія), Чеського технічного університету, Інституту кібернетики ім. В.М. Глушкова НАН України, Харківського національного університету радіоелектроніки, Національного університету «Одеська політехніка», Національного авіаційного університету. Зусиллями багатьох вчених, насамперед Задіраки В.К., Кошкіної Н.В., Конаховича Г.Ф., Лужецького В.А., Кобозевої А.А., Кузнецова О.О., Fridrich J., Böhme R., Ker A., Boroumand M., Yousfi Y., Zhang R., Tabares-Soto R. та інших, систематизовано відомі методи вбудовування повідомлень (стегоданих) у мультимедійні дані, зокрема цифрові зображення (ЦЗ), запропоновано підходи до побудови високоточних стегодетекторів (СД), зокрема заснованих на застосуванні комплексних статистичних моделей файлу-контейнеру та штучних нейронних мереж (ШНМ).

Відмітимо, що в низці теоретичних досліджень та практичних застосувань СД існують проблеми, обумовлені:

– обмеженістю або навіть відсутністю апріорних даних щодо типу та параметрів стеганографічного методу (СМ), використаного для приховання стегоданих до зображення-контейнеру (ЗК);

– неможливістю надійного виявлення стеганограм в умовах мінімізації ступеня заповнення ЗК стегоданими;

– нелінійною залежністю точності роботи СД від статистичних і спектральних характеристик оброблюваних ЦЗ;

– обмеженими можливостями щодо зниження рівня демаскуючих ознак проведення деструкції стеганограм, а саме мінімізації змін статистичних, спектральних та структурних параметрів оброблених ЦЗ;

– неможливістю визначення положення (локалізації) пікселів ЗК, використаних для приховання стегобітів, для розробки методів вилучення (екстракції) вбудованих повідомлень.

Зокрема, це стосується випадків виявлення стеганограм, сформованих з використанням новітніх адаптивних стеганографічних методів (АСМ), що дозволяють мінімізувати зміни статистичних, спектральних та структурних параметрів ЗК при вбудовуванні повідомлень.

Наведене вище обумовлює актуальність та важливість науково-прикладної проблеми 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 ЦЗ. Вирішення даної проблеми потребує суттєвого вдосконалення існуючих методів синтезу та параметричної оптимізації стегодетекторів для 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, узгодженого 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, слабкого 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, здатних наблизитися до теоретичних оцінок досяжної імовірності виявлення стеганограм;

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

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

7. Дослідити перспективи використання розробленого програмного комплексу для вирішення найбільш складних задач стегоаналізу ЦЗ, а саме надійної деструкції стеганограм при мінімізації змін статистичних, спектральних та структурних параметрів ЦЗ, а також визначення положення (локалізації) пікселів, використаних для приховання стегобітів, 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 стегодетекторів для надійного виявлення повідомлень, несанкціоновано вбудованих до ЦЗ, в умовах обмеженості апріорних даних щодо використаного стеганографічного 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 ЦЗ), 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).

Наукова новизна одержаних результатів, що виносяться до захисту:

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 вилучення локальних збурень значень яскравості пікселів ЗК, обумовлених приховання 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» стегоаналізу ЦЗ (а саме, відсутності апріорних даних щодо використаного стеганографічного 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 Бхаттачарайя 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 полягає в наступному:

1. Показано, що принциповим обмеженням відомих методів стегоаналізу 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 унеможливлює 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 стегодетекторів дозволяє подолати дане обмеження, оскільки не потребує використанням апріорних даних щодо використаних стеганографічних 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 (неспотворених) 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 стеганограм, а саме маскування 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 дисертаційної роботі, використано в центрі досліджень та розробок «Самсунг РнД Інститут Україна» при виконанні науково-дослідних робіт 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 Національного 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 [28,30];
   b) Універсальних стегодетекторів, зокрема розроблених модифікацій стегодетектору Авкібаса [16,26,29,33,35,36];

c) Стегодетекторів, заснованих на використанні статистичних [15,34, 43,49] та структурних [10,22,37,41] параметрів досліджуваних ЦЗ;
d) Методів деструкції стеганограм [38,40,45];

2. Оригінальні результати експериментального дослідження причин зниження точності роботи відомих СД при обробці нових пакетів зображень, зокрема:
a) впливу невідповідності типу перетворень ЗК, що використовуються для приховання повідомлень та проведення стегоаналізу ЦЗ [27];
b) відмінностей між імовірнісними розподілами значень яскравості пікселів ЗК і стеганограм, сформованих з використанням поширених [8] та новітніх [1,2,17,18,39,44] стеганографічних методів;

3. Застосування спеціальних методів попередньої обробки в задачах стегоаналізу ЦЗ для підвищення точності роботи СД, а саме:
a) додаткового зашумлення [4,6,47,50] та повторного приховання повідомлень [3,19] до оброблюваних зображень;
b) методів підвищення візуальної якості ЦЗ [46,51,54], зокрема заснованих на використанні методів компонентного аналізу сигналів [5];
c) зниження впливу шумів [31,32], що засновані на застосуванні варіаційних методів [31,32], штучних нейронних мереж [7,11,20,48,52,53] та декомпозиції ЦЗ з використанням спеціальних систем функцій [42];

4. Запропонований метод локалізації позиції пікселів зображення-контейнеру, використаних для приховання стегобітів повідомлення [55];

5. Застосування запропонованого методу формування ССФ:
a) для зменшення впливу нестаціонарних завад у сигналах, що використовуються в системах біометричної автентифікації користувачів [14, 23-25];

6. Оригінальні методи стеганографічної обробки та аналізу ЦЗ, що запропоновані для підвищення ефективності комплексних систем захисту інформації [13];

7. Програмний комплекс, на основі якого проведено порівняльний аналіз імовірності виявлення стеганограм з даними, вбудованими в ОПЗК, при використанні відомих та запропонованих СД [9,12,21].

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 конфе-

ренції «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-технічної 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 наукових фахових виданнях, з них:

– 13 статей у наукових періодичних виданнях, включених до Переліку наукових фахових видань України (в т.ч. 7 включених до категорії "А", з них 2 статті у виданнях, віднесених до квартилю Q3 відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports);

– 8 статей у наукових періодичних виданнях інших держав з напряму, з якого підготовлено дисертацію, з них 1 стаття у виданні, віднесеному до квартилю Q2 відповідно до класифікації SCImago Journal and Country Rank або Journal Citation Reports;

три міжнародні патенти на винахід (зареєстровані 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.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **вступі** обґрунтовано актуальність теми дисертаційної роботи, сформульовано мету і завдання дослідження, визначено об'єкт, предмет та методи досліджень, визначені наукова новизна та практичне значення отриманих результатів. Наведено дані про впровадження результатів роботи, публікації та особистий внесок автора.

У **першому розділі** проведено аналітичний огляд існуючих моделей, методів та засобів стеганографії та стегоаналізу ЦЗ. Визначено область застосування, переваги і обмеження сучасних методів стегоаналізу цифрових зображень. Наведено вимоги щодо надійності роботи систем виявлення та деструкції стеганограм.

За результатами аналітичного огляду сучасних стеганографічних методів приховання повідомлень до ЦЗ встановлено, що особлива увага при розробці даних методів приділяється мінімізації змін статистичних, спектральних та структурних параметрів ЗК при формуванні стеганограм. Одним з найбільш поширених підходів до вирішення даної задачі є представлення процесу приховання повідомлення **M** до зображення-контейнеру **X** як вирішення оптимізаційної задачі з обмеженнями:

$$\min_{\pi} \mathrm{E}_{\pi}[\mathrm{D}] = \sum\nolimits_{\mathbf{Y}\in\mathcal{Y}} \pi(\mathbf{Y}) \cdot \mathrm{D}(\mathbf{X},\mathbf{Y}), \mathrm{H}(\pi) = m, \quad (1)$$

$$\mathrm{H}(\pi) = -\sum\nolimits_{\mathbf{Y}\in\mathcal{Y}} \pi(\mathbf{Y}) \cdot \log_2 \pi(\mathbf{Y}),$$

$$\mathrm{D}(\mathbf{X},\mathbf{Y}) = \sum_{i=1}^{N}\sum_{j=1}^{M} \rho_{i,j}(\mathbf{X},\mathbf{Y}),$$

де $\mathbf{X} \in \mathcal{J}, \mathbf{Y} \in \mathcal{Y}$ – відповідно, зображення-контейнер та сформована стеганограма; $\mathcal{J} = \{0,1,\cdots,2^k-1\}^{N\times M}$ – множина зображень розміром $N \times M$ пікселів, представлених в градаціях сірого кольору, з глибиною кольору k бітів; $\mathcal{Y} \subset \mathcal{J}$ – множина можливих стеганограм; π – імовірнісний розподіл щодо вибору стеганограми $\mathbf{Y}$ з множини $\mathcal{Y}$ для передачі повідомлення $\mathbf{M}$; $\mathbf{M} \in \{0;1\}^m$ – стегодані, представлені у вигляді бітової послідовності довжиною m бітів; $\mathrm{E}_{\pi}[\cdot]$ – функція визначення математичного очікування для випадкової величини, що характеризується імовірнісним розподілом π; $\mathrm{H}(\pi)$ – інформаційна ентропія для імовірнісного розподілу π; $\mathrm{D}(\mathbf{X},\mathbf{Y})$ – функція оцінки величини змін параметрів ЗК при вбудовуванні повідомлення $\mathbf{M}$; $\rho_{i,j}(\cdot)$ – функція оцінки змін статистичних характеристик ЗК при зміні яскравості пікселю ЗК з координатами (i,j);

Застосування сучасних оптимізаційних методів для вирішення задачі (1) дозволяє створювати СМ, що характеризуються високою робастністю до відомих методів статистичного та структурного стегоаналізу. Для додаткового зниження рівня демаскуючих ознак сформованих стеганограм широко використовуються методи пакетної стеганографії (а саме, приховання частин повідомлення в декількох ЗК), методи синхронізації змін значень яскравості суміжних

пікселів зображення-контейнеру, методи оцінки змін статистичних та спектральних параметрів ЗК, обумовлених використанням поширених методів обробки (наприклад, стиснення з втратами, підвищення візуальної якості зображення тощо) та інші.

За результатами огляду відомих підходів до побудови СД встановлено, що переважна більшість методів синтезу стегодетекторів засновані на використанні фіксованої (стандартної) структури детектору та подальшої оптимізації лише його окремих параметрів за критерієм мінімізації значення помилки класифікації стеганограм P_E. На першому етапі роботи СД, зазвичай, використовуються методи попередньої обробки досліджуваних ЦЗ, зокрема потужні ансамблі ФВЧ. Дані методи спрямовані на виявлення змін значень яскравості пікселів ЗК, обумовлених приховуванням повідомлень. Для визначення демаскуючих ознак стеганограм, сформованих згідно поширених стеганографічних методів, широко використовуються комплексні статистичні моделі, серед яких SRM, J+SRM, GFR та інші. Це дозволяє забезпечити високу точність виявлення стеганограм (в діапазоні 90%-95%), проте лише у випадку використання відомих стеганографічних методів та значного ($\Delta_\alpha^S > 20\%$) 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 ФВЧ), що унеможливлює швидку адаптацію налаштованих стегодетекторів для виявлення нових типів СМ.

Для додаткового підвищення імовірності виявлення стеганограм, сформованих згідно АСМ, досліджено використання спеціальних типів ШНМ, зокрема згорткових нейронних мереж (наприклад, SR-Net, Zhu-Net), автоенкодерних мереж (серед яких, ASSAF). Це дозволяє гнучко підходити до вибору структури та параметрів стегодетектору при налаштуванні ШНМ, наприклад шляхом застосування спеціальних типів ФВЧ для визначення демаскуючих ознак стеганограм, зменшення тривалості налаштування СД за рахунок спрощення структури штучної нейронної мережі та інших.

За результатами порівняльного аналізу точності виявлення стеганограм, сформованих згідно АСМ, встановлено, що застосування СД на основі ШНМ дозволяє подолати наведені обмеження статистичних стегодетекторів. Проте суттєве зниження кількості помилок класифікації стеганограм P_E при використанні ШНМ досягається лише у випадку обробки пакетів ЦЗ, статистичні параметри котрих несуттєво відрізняються від відповідних характеристик ЦЗ з вихідної (навчальної) вибірки $\mathcal{S}_{train}$. Також, стегодетектори на основі ШНМ потребують використання прикладів стеганограм при проведенні налаштування параметрів штучних нейронних мереж для забезпечення високої (більше 95%) точності виявлення стеганограм. Це унеможливлює використання даних СД у випадку виявлення апріорно невідомих стеганографічних методів.

Для підвищення імовірності виявлення стеганограм, сформованих згідно новітніх АСМ, в роботі запропоновано розширити перелік використовуваних

параметрів ЦЗ шляхом врахування факторів, що мають вплив на значення даних параметрів:

$$\boldsymbol{v}_{\mathbf{I}} = \mathrm{F}_{mix}(\boldsymbol{u}_{\mathbf{I}}), \tag{2}$$

де $\boldsymbol{v}_{\mathbf{I}} \in \mathbb{R}^{d_{cr}}$ – вектор з d_{cr} елементів, що відповідає статистичним параметрам оброблюваного зображення $\mathbf{I} \in \mathcal{J}$; $\boldsymbol{u}_{\mathbf{I}} \in \mathbb{R}^{d_{tr}}, d_{cr} < d_{tr}$ – вектор з d_{cr} факторів, що впливають на значення параметрів зображення $\mathbf{I}$; $\mathrm{F}_{mix}\colon \mathbb{R}^{d_{tr}} \to \mathbb{R}^{d_{cr}}$ – функція відображення впливу факторів на параметри досліджуваного ЦЗ.

Відмітимо, що аналітичне визначення функції $F_{mix}(\cdot)$ у виразі (2) наразі лишається невирішеною задачею, враховуючи високу складність моделювання реальних ЦЗ. Для подолання даного обмеження, в роботі запропоновано використовувати наближене представлення впливу даної функції на вектор $\boldsymbol{u}_{\mathbf{I}}$ із застосуванням матриці $\mathbf{A}_{mix}$:

$$\boldsymbol{v}_{\mathbf{I}} = \mathbf{A}_{mix} \times \boldsymbol{u}_{\mathbf{I}}, \tag{3}$$

де $\mathbf{A}_{mix} \in \mathbb{R}^{d_{cr} \times d_{tr}}$ – матриця, що визначає ступінь «змішування» впливу d_{cr} факторів на досліджувані параметри ЦЗ. При цьому оцінку значень елементів матриці $\mathbf{A}_{mix}$ запропоновано проводити із застосуванням теореми Джонсона-Лінденштрауса, а саме представлення $\mathbf{A}_{mix}$ як матриці проекції $\boldsymbol{\Phi}_{\mathrm{JL}}$ векторів $\boldsymbol{u}_{\mathbf{I}}$ з вихідного простору $\mathbb{R}^{d_{tr}}$ до простору $\mathbb{R}^{d_{cr}}$:

$$\boldsymbol{\Phi}_{\mathrm{JL}} = \mathbf{P}_{\mathrm{JL}} \times \mathbf{H}_{\mathrm{JL}} \times \mathbf{D}_{\mathrm{JL}}, \tag{4}$$

$$\mathbf{P}_{\mathrm{JL}}(i,j) = \begin{cases} \mathcal{N}(0, q^{-1}), & \Pr(q), \\ 0, & \Pr(1-q), \end{cases} \tag{5}$$

$$q = \min\{1; \Theta(\varepsilon^{p-2} \log^p n_{\boldsymbol{v}_{\mathbf{I}}}/d_{cr})\},$$

$$\mathbf{H}_{\mathrm{JL}}(i,j) = d_{tr}^{-1/2} \cdot (-1)^{\langle i-1, j-1 \rangle}, \tag{6}$$

де $\mathbf{P}_{\mathrm{JL}} \in \mathbb{R}^{d_{cr} \times d_{tr}}$ – стохастична матриця; $\varepsilon > 0$ – константа, що визначає максимальне значення зміни відстані між векторами $\{\boldsymbol{v}_{\mathbf{I}}^i\}_{i=1}^{n_{\boldsymbol{v}_{\mathbf{I}}}}$ внаслідок їх проекції до простору $\mathbb{R}^{d_{tr}}$; $n_{\boldsymbol{v}_{\mathbf{I}}}$ – кількість оброблюваних векторів $\boldsymbol{v}_{\mathbf{I}}$; $p \in \{1; 2\}$ – тип метрики ℓ_p, що використовується для оцінки відстані між векторами; $\mathbf{H}_{\mathrm{JL}} \in \mathbb{R}^{d_{tr} \times d_{tr}}$ – нормалізована матриця Адамара; $\langle a, b \rangle_m$ – скалярний добуток m –елементних векторів, що відповідають бінарному представленню аргументів a та b; $\mathbf{D}_{\mathrm{JL}} \in \mathbb{R}^{d_{tr} \times d_{tr}}$ – діагональна матриця, елементи котрої обираються з послідовності $\{-1; +1\}$ з рівною імовірністю. Відповідно, оцінка $\widetilde{\boldsymbol{u}}_{\mathbf{I}}$ для векторів $\boldsymbol{u}_{\mathbf{I}}$ у виразі (3) може бути отримана шляхом застосування оберненої матриці $\boldsymbol{\Phi}_{\mathrm{JL}}^{-1}$ до вектору $\boldsymbol{v}_{\mathbf{I}}$:

$$\widetilde{\boldsymbol{u}}_{\mathbf{I}} = \boldsymbol{\Phi}_{\mathrm{JL}}^{-1} \times \boldsymbol{v}_{\mathbf{I}}, \|\boldsymbol{u}_{\mathbf{I}} - \widetilde{\boldsymbol{u}}_{\mathbf{I}}\|_2 \leq \varepsilon^2. \tag{7}$$

Відмітимо неможливість аналітичної оцінки кількості факторів d_{cr}, що мають вплив на статистичні параметри ЦЗ, враховуючи високу складність моделювання реальних зображень. Внаслідок цього, при налаштуванні СД проводиться проекція вектору $\boldsymbol{v}_{\mathbf{I}}$, що відповідає статистичним параметрам оброблюваного ЦЗ, до простору $\mathbb{R}^{d_{JL}}$, $d_{cr} < d_{JL} < d_{tr}$. Значення d_{JL} обирається таким, що дозволяє мінімізувати значення помилки класифікації стеганограм P_E на тестовому пакеті зображень. При цьому застосування швидких методів генерації матриць $\mathbf{P}_{\mathrm{JL}}$ (5) та $\mathbf{H}_{\mathrm{JL}}$ (6) дозволяє забезпечити мінімальні зміни тривалості налаштування СД при використанні запропонованого методу.

За результатами проведених автором досліджень запропонованого методу підвищення точності сучасних СД отримано експериментальні оцінки імовірності виявлення стеганограм, сформованих згідно новітніх стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD. Дослідження проводилося згідно стандартної процедури перехресної перевірки (англ. cross-validation) при розбитті пакету тестових зображень на навчальну $\mathcal{S}_{train}$ (70%) та контрольну $\mathcal{S}_{test}$ (30%) вибірки. В якості тестових ЦЗ використовувалися зображення зі стандартних пакетів ALASKA (80,000 зображень), VISION (34,427 зображень) та MIRFlickr (близько 1 мільйона зображень).

Визначення статистичних параметрів оброблюваних ЦЗ проводилося згідно стандартної процедури з використанням статистичної моделі SPAM. Обробка отриманих статистичних параметрів ЦЗ відбувалася із застосуванням ансамблевого класифікатора, а саме пакету зі 250 класифікаторів на основі лінійних дискримінантів Фішера, налаштованих з використання окремих статистичних параметрів оброблюваних зображень. При цьому віднесення ЦЗ до класів ЗК або стеганограм з використанням ансамблю класифікаторів проводилося за мажоритарним принципом. Налаштування кожного з класифікаторів у складі ансамблю проводилося на $\mathcal{S}_{train}$ вибірці з 8,000 зображень для кожного пакету ЦЗ шляхом мінімізації помилки класифікації стеганограм P_E:

$$P_E = \min_{P_{FP}} \frac{1}{2}\left(P_{FP} + P_{FN}(P_{FP})\right), \tag{8}$$

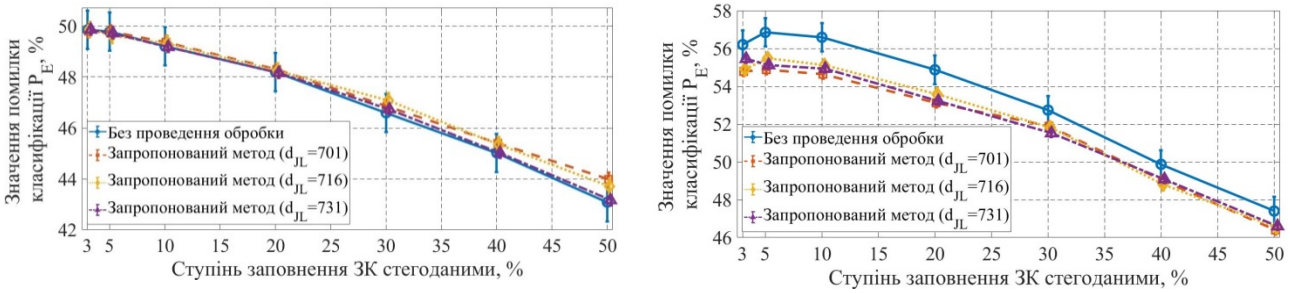
де P_{FP}, P_{FN} – відповідно, імовірність помилок першого (хибне віднесення ЗК до класу стеганограм) та другого (хибне віднесення стеганограм до класу ЗК) роду.

Для дослідження впливу апріорних даних щодо використаного СМ на точність роботи СД в роботі проводилася зміна частки пар ЗК і сформованих на їх основі стеганограм у навчальній вибірці $\mathcal{S}_{train}$. Для кількісної оцінки частки стеганограм, використаних при налаштуванні СД, використовувався наступний показник:

$$K_{\alpha}^{OL} = \frac{|\{(\mathbf{X}, \mathbf{Y})\colon (\mathbf{X}_i, \mathbf{Y}_i), i \in \mathcal{S}_{train}\}|}{|\mathcal{S}_{train}|} \times 100\%. \tag{9}$$

Значення K_α^{OL} змінюється від 0% (відповідає випадку відсутності у вибірці $\mathcal{S}_{train}$ зображень-контейнерів, використаних для формування стеганограм) до 100% (в вибірці $\mathcal{S}_{train}$ наявні пари ЗК та відповідних їм стеганограм).

Типові залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно адаптивного методу HUGO, при використанні запропонованого методу підвищення точності роботи СД та варіації параметру d_{JL} для матриці $\mathbf{\Phi}_{\text{JL}}^{-1}$ у виразі (7) представлені на рис. 1.



(а) (б)

Рисунок 1 – Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими Δ_α^S та значення параметру d_{JL} для матриці $\mathbf{\Phi}_{\text{JL}}^{-1}$ для стеганограм, сформованих згідно метод HUGO. Розглянуто випадок формування стеганограм з використанням тестових ЦЗ з пакету ALASKA та застосування запрононованого методу підвищення точності роботи СД при варіації значення параметру K_α^{OL}: (а) – $K_\alpha^{OL} = 100\%$; (б) – $K_\alpha^{OL} = 0\%$. Значення P_E наведено для довірчого інтервалу з рівнем довіри 95%

Запропонований метод дозволяє зменшити на 2% значення помилки класифікації стеганограм P_E у випадку відсутності апріорних даних щодо використаного СМ ($K_\alpha^{OL} = 0\%$, рис. 1б). Відмітимо, що дане зниження значень P_E досягається лише в області сильного заповнення ЗК стегоданими ($\Delta_\alpha^S > 20\%$).

Таким чином, встановлено, що існуючі методи побудови та вдосконалення стегодетекторів дозволяють забезпечити високу (більше 95%) імовірність виявлення стеганограм лише для випадку дослідження апріорно відомого СМ та сильного заповнення ЗК стегоданими ($\Delta_\alpha^S > 20\%$). Відсутність у літературі теоретичних обґрунтувань щодо вибору оптимальних методів синтезу структури та оптимізації параметрів СД за критерієм мінімізації значення помилки класифікації стеганограм P_E суттєво ускладнює побудову високоточних СД. Вирішення даної науково-прикладної проблеми потребує розробки нового методу побудови високоточних стегодетекторів, здатних надійно працювати в найбільш складних випадках стегоаналізу ЦЗ, а саме за відсутності апріорних даних щодо використовуваного СМ, слабкого ступеня заповнення ЗК стегоданими (менше 10%) та при значній варіативності значень статистичних, спектральних та структурних параметрів досліджуваних зображень.

Результати першого розділу дозволили обґрунтувати необхідність розробки нової концепції побудови ивисокоточних стегодетекторів для проведення

«сліпого» стегоаналізу ЦЗ. Досягнення поставленої мети потребує визначення факторів, що мають найбільший вплив на точність роботи існуючих СД, розробки методів синтезу структури та оптимізації параметрів СД, що здатні забезпечити надійне виявлення стеганограм в умовах відсутності апріорних даних щодо використаних АСМ.

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 методів 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 наступних функцій:

$$P_E = \mathrm{F}_{calib}(\mathbf{I}) \circ \mathrm{F}_{feature}(\tilde{\mathbf{I}}) \circ \mathrm{F}_{class}(\mathbf{f}), \qquad (10)$$

де $\mathrm{F}_{calib}(\mathbf{I})$ – функція попередньої обробки досліджуваного зображення $\mathbf{I} \in \mathcal{J}$ з метою виокремлення змін яскравості пікселів ЗК, обумовлених приховуванням стегоданих; $\mathrm{F}_{feature}(\tilde{\mathbf{I}})$ – функція визначення статистичних, спектральних та структурних параметрів обробленого зображення $\tilde{\mathbf{I}}$ ($\tilde{\mathbf{I}} = \mathrm{F}_{calib}(\mathbf{I})$); $\mathrm{F}_{class}(\mathbf{f})$ – функція віднесення (класифікації) досліджуваного зображення до класів ЗК або стеганограм за результатами обробки обчислених параметрів зображення (векторів $\mathbf{f} = \mathrm{F}_{feature}(\tilde{\mathbf{I}})$).

В роботі проведено дослідження змін значень помилки P_E (10) при формуванні стеганограм згідно новітніх АСМ та побудови стегодетектору з використанням різних типів функцій $\mathrm{F}_{calib}(\cdot)$ (наприклад, потужних ансамблів ФВЧ, застосування спеціальних типів згорткових і автоенкодерних штучних нейронних мереж), $\mathrm{F}_{feature}(\cdot)$ (а саме, визначення статистичних параметрів ЦЗ з використанням статистичних моделей SRM, maxSRM, DCTR, PSRM, PHARM і GFR) та $\mathrm{F}_{class}(\cdot)$ (зокрема, застосування ансамблевих класифікаторів на основі лінійних дискримінантів Фішера, методу опорних векторів, багатошарових ШНМ). За результатом аналізу отриманих даних встановлено, що суттєвий вплив на точність роботи СД має відстань між вектором, що відповідає статистичним параметрам зображення-контейнеру $\mathbf{f}(c)$, та центром кластеру $\mathbf{f}(s)$, який побудовано з використанням відповідних векторів для сформованих стеганограм. Схематичне зображення змін положення даних векторів при використанні функції $\mathrm{F}_{calib}(\cdot)$ наведено на рис. 2.

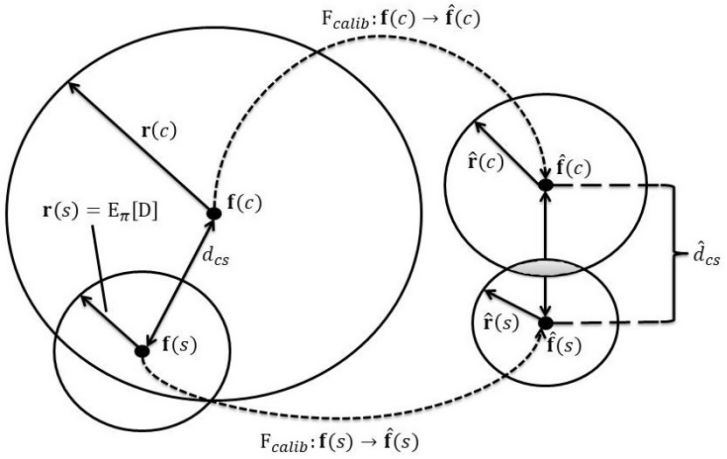


Рисунок 2 – Схематичне представлення зміни положення векторів, що відповідають статистичним параметрам зображення-контейнеру $\mathbf{f}(c)$ та сформованої стеганограми $\mathbf{f}(s)$, внаслідок застосування функції $\mathrm{F}_{calib}(\cdot)$. Забезпечення високої точності роботи СД потребує мінімізації ступеня перекриття кластерів (позначено сірим кольором), що відповідають статистичним параметрам оброблених ЗК ($\hat{\mathbf{f}}(c)$) та стеганограм ($\hat{\mathbf{f}}(s)$).

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). При цьому розмір кластеру $\mathbf{f}(c)$ залежить від ступеня варіації значень параметрів зображень-контейнерів:

$$\|\mathbf{r}(c)\|_2 = \max_{\mathbf{f}_\mathrm{c}(i)} \|\mathbf{f}(c) - \mathbf{f}_\mathrm{c}(i)\|_2 \,, i \in \left[1; N_{\mathbf{f}(c)}\right], \tag{11}$$

де $\mathbf{f}_\mathrm{c}(i)$ – 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) відповідає статистичним параметрам сформованих стеганограм та рівний $\|\mathbf{r}(s)\|_2 = \mathrm{E}_{\pi}[\mathrm{D}]$ згідно виразу (1). Застосування функції $\mathrm{F}_{calib}(\cdot)$ 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). Розмір $\|\hat{\mathbf{r}}(c)\|_2$ і $\|\hat{\mathbf{r}}(s)\|_2$ сформованих кластерів може бути визначений аналогічно до виразу (11).

Для оцінки значення відстані d_{cs} між векторами $\mathbf{f}(c)$ та $\mathbf{f}(s)$ (рис. 2) зазвичай використовується відстань Кульбака-Лейблера:

$$\mathrm{D}_{KL}\big(\mathbf{f}(c), \mathbf{f}(s)\big) = \sum_{q=1}^{|\mathcal{M}|} P_\mathrm{c}(q) \cdot \log_2(P_\mathrm{c}(q)/P_s(q)), \tag{12}$$

де $P_\mathrm{c}(q), P_s(q)$ – нормовані гістограми розподілу значень q –го елементу векторів $\mathbf{f}(c)$ і $\mathbf{f}(s)$; $|\mathcal{M}|$ –кількість параметрів статистичної моделі $\mathcal{M}$, що використовується для аналізу досліджуваних зображень.

Формування стеганограм згідно новітніх АСМ шляхом вирішення оптимізаційної задачі (1) призводить до мінімізації відстані між векторами $\mathbf{f}(c)$ і

$\mathbf{f}(s)$, та, відповідно, значення $\mathrm{D}_{KL}\left(\mathbf{f}(c), \mathbf{f}(s)\right)$ (12). Відмітимо, шо значення відстані $\hat{d}_{cs} = \mathrm{D}_{KL}\left(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)\right)$ також буде близьким до нуля (рис. 2), враховуючи незмінність значення відстані Кульбака-Лейблера у випадку застосування перетворень до імовірнісних розподілів $P_{\mathrm{c}}(q)$ та $P_s(q)$. Це призводить до перекриття кластерів $\hat{\mathbf{f}}(c)$ та $\hat{\mathbf{f}}(s)$ (рис. 2) та, відповідно, зниження точності роботи СД.

Для підвищення точності оцінки відстані $\hat{d}_{cs}$ (рис. 2), зокрема у випадку формування стеганограм згідно АСМ, в роботі запропоновано застосування спеціальних показників, а саме відстані Хеллінгера D_H, відстані Бхаттачарайя D_B, χ^2-квадрат D_{χ^2} та спектру відстаней Реньї D_R^{α}:

$$\mathrm{D}_H\left(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)\right) = \sqrt{\frac{1}{2} \cdot \sum_{q=1}^{|\mathcal{M}|} \left(\sqrt{\hat{P}_{\mathrm{c}}(q)} - \sqrt{\hat{P}_{\mathrm{s}}(q)}\right)^2}, \tag{13}$$

$$\mathrm{D}_B\left(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)\right) = -\ln\left(1 - \mathrm{D}_H^2\left(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)\right)\right), \tag{14}$$

$$\mathrm{D}_{\chi^2}\left(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)\right) = \sum_{q=1}^{|\mathcal{M}|} \left(\hat{P}_{\mathrm{c}}(q) - \hat{P}_{\mathrm{s}}(q)\right)^2 / \hat{P}_{\mathrm{s}}(q), \tag{15}$$

$$\mathrm{D}_R^{\alpha}\left(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)\right) = \frac{1}{\alpha - 1} \log_2 \left(\sum_{q=1}^{|\mathcal{M}|} \hat{P}_{\mathrm{c}}^{\alpha}(q) \cdot \hat{P}_s^{1-\alpha}(q)\right), \tag{16}$$

де $\hat{P}_{\mathrm{c}}(q), \hat{P}_{\mathrm{s}}(q) -$ нормовані гістограми розподілу значень q –го елементу векторів з кластерів $\hat{\mathbf{f}}(c)$ та $\hat{\mathbf{f}}(s)$ відповідно; $\alpha \in (0; +\infty)\backslash\{1\} -$ ваговий параметр. Використання діапазону малих значень параметру α ($\alpha \in (0; 1)$) при визначенні значення D_R^{α} (16) дозволяє виокремлювати вплив груп пікселів ЦЗ з малими значеннями яскравості (близькими до чорного кольору). В той час як при $\alpha > 1$ основний вплив на значення D_R^{α} мають групи пікселів з рівнем яскравості, близькими до білого кольору.

За результатами порівняльного аналізу точності оцінки відстані $\hat{d}_{cs}$ між кластерами $\hat{\mathbf{f}}(c)$ та $\hat{\mathbf{f}}(s)$ (рис. 2) при формуванні стеганограм згідно АСМ виявлено, що застосування відстані Хеллінгера D_H (13) дозволяє суттєво (до двох разів) підвищити точність оцінювання відмінностей між розподілами значень яскравості пікселів ЗК та стеганограм у порівнянні іншими показниками (14)-(16), зокрема використанням відстані Кульбака-Лейблера (12). Це дає можливість підвищити точність виявлення стеганограм навіть у випадку слабкого заповнення ЗК стегоданими ($\Delta_{\alpha}^{S} < 10\%$).

Функція $\mathrm{F}_{feature}(\cdot)$ у виразі (10) використовується для оцінки статистичних, спектральних та структурних параметрів оброблюваних ЦЗ. Визначення демаскуючих ознак сформованих стеганограм потребує виявлення параметрів досліджуваних зображень, що найбільше змінюються внаслідок приховання повідомлень для заданого (фіксованого) ступеня заповнення ЗК стегоданими (Δ_{α}^{S}). Для аналізу залежності значень вектору $\mathbf{f} = F_{feature}(\tilde{\mathbf{I}})$, що відповідає ста-

тистичним параметрам обробленого зображення $\tilde{\mathbf{I}} = F_{calib}(\mathbf{I})$, від параметру Δ_α^S в роботі запропоновано використовувати наступну функцію:

$$g_{\mathbf{f}}(\tilde{\mathbf{I}}) \sim \partial \mathbf{f} / \partial \Delta_\alpha^S. \quad (17)$$

В дисертаційній роботі показано, що функція $g_{\mathbf{f}}(\tilde{\mathbf{I}})$ (17) визначає контур кластеру, сформованого з векторів $\mathbf{f}$ для стеганограм, які відрізняються лише значенням яскравості окремого пікселю. Це дозволяє визначати особливості кластеру $\hat{\mathbf{f}}(s)$, а саме підмножину елементів вектору $\mathbf{f}$, які найбільш змінюються внаслідок формування стеганограм, що становить інтерес для підвищення точності роботи СД.

Новітні типи АСМ дозволяють мінімізувати зміни як відстані $\hat{d}_{cs}$ між кластерами $\hat{\mathbf{f}}(c)$ та $\hat{\mathbf{f}}(s)$ (рис. 2), так і значень функції $g_{\mathbf{f}}(\tilde{\mathbf{I}})$ (17) при вбудовуванні повідомлень до ЗК. Це ускладнює визначення демаскуючих ознак стеганограм та призводить до суттєвого зниження точності роботи СД. Також, вибір методів попередньої обробки $\mathrm{F}_{calib}(\cdot)$ проводиться, зазвичай, емпіричним чином для апріорно відомих СМ. Внаслідок цього не враховуються особливості роботи методів визначення статистичних, спектральних та структурних параметрів ЦЗ, що ускладнює адаптацію існуючих СД для виявлення нових типів стеганографічних методів. Для подолання даних обмежень в роботі запропоновано представити процес синтезу СД як вирішення наступної оптимізаційної задачі:

$$\max_{\mathrm{F}_{calib}, \Delta_\alpha^S} \mathrm{D}_H\left(\hat{\mathbf{f}}(c), \hat{\mathbf{f}}(s)\right) + \lambda_1 / \|\hat{\mathbf{r}}(c)\|_2 + \lambda_2 / \|\hat{\mathbf{r}}(s)\|_2, \quad (18)$$

де $\lambda_1, \lambda_2 > 0 -$ множники для відповідних складових виразу регуляризації, а саме впливу розмірів кластерів оброблених зображень-контейнерів ($\hat{\mathbf{r}}(c)$) та стеганограм ($\hat{\mathbf{r}}(s)$). 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 (13). Використання запропонованого методу синтезу СД дозволяє узгодити вибір типу і параметрів функції $\mathrm{F}_{calib}(\cdot)$ та $\mathrm{F}_{feature}(\cdot)$ у виразі (10) для забезпечення надійного виявлення стеганограм.

Схематичне представлення результату обробки статистичних параметрів зображення-контейнеру $\mathbf{f}(c)$ та сформованої стеганограми $\mathbf{f}(s)$ при синтезі СД згідно запропонованого методу (18) наведено на рис. 3.

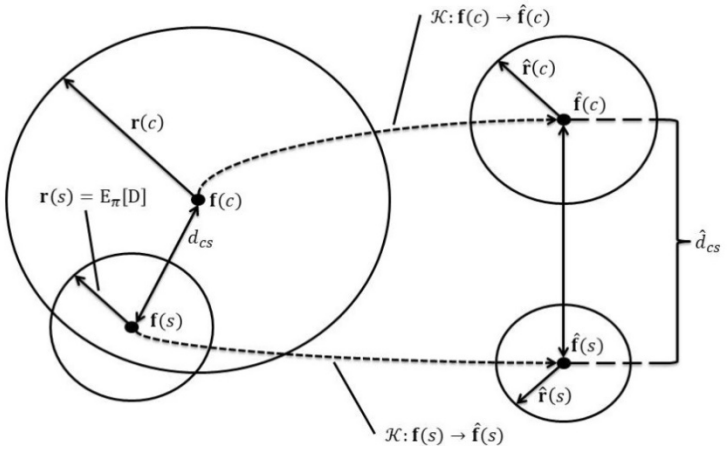


Рисунок 3 – Схематичне представлення зміни положення векторів, що відповідають статистичним параметрам зображення-контейнеру $\mathbf{f}(c)$ та сформованої стеганограми $\mathbf{f}(s)$, при проведенні синтезу стегодететкорів згідно запропонованого методу. Застосування функції попередньої обробки $\mathcal{K}$,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

Запропонований метод синтезу високоточних СД дозволяє підвищити точність виявлення стеганограм за рахунок максимізації значення відстані $\hat{d}_{cs}$ між кластерами векторів оброблених ЗК ($\hat{\mathbf{f}}(c)$) та стеганограм ($\hat{\mathbf{f}}(s)$) при забезпеченні малого розміру даних кластерів (рис. 3). Це дає можливість спростити вимоги до вибору методу $\mathrm{F}_{class}(\cdot)$ у виразі (10), що становить інтерес для розробки СД, здатних працювати в режимі, наближеного до реального часу.

В дисертаційній роботі показано, що оптимальними методами попередньої обробки $\mathcal{K}_{opt}(\cdot)$ досліджуваних ЦЗ у виразі (18) за критерієм мінімізації значення помилки класифікації стеганограм P_E та обмеженості апріорних даних щодо особливостей використаного СМ є наступні:

$$\mathcal{K}_{opt}^{CE}(\mathbf{X},\mathbf{Y})\colon \mathbf{Y}(\Delta_{\alpha}^{S}) \xrightarrow[\forall \Delta_{\alpha}^{S} \geq 0]{} \mathbf{X}, \tag{19}$$

$$\mathcal{K}_{opt}^{SE}(\mathbf{X},\mathbf{Y})\colon \mathbf{X} \xrightarrow[\forall \Delta_{\alpha}^{S} \geq 0]{} \mathbf{Y}(\Delta_{\alpha}^{S}) \tag{20}$$

де метод $\mathcal{K}_{opt}^{CE}(\mathbf{X},\mathbf{Y})$ відповідає відновленню (реконструкції) вихідного виду ЗК за наявними (зашумленими) зображеннями, метод $\mathcal{K}_{opt}^{SE}(\mathbf{X},\mathbf{Y})$ спрямований на вилучення спотворень ЗК, обумовлених приховуванням повідомлень, а значення $\Delta_{\alpha}^{S} = 0$ у виразі (20) відповідає використанню зображення-контейнеру.

Відмітимо, що застосування методу $\mathcal{K}_{opt}^{CE}(\cdot)$ (19) для обробки ЗК не призводить до їх зміни. Аналогічно, обробка стеганограм з використанням методу $\mathcal{K}_{opt}^{SE}(\cdot)$ (20) не змінює значення яскравості пікселів зображення:

$$\mathcal{K}_{opt}^{CE}(\mathbf{X},\mathbf{X})\colon \mathbf{X} \to \mathbf{X}, \mathcal{K}_{opt}^{SE}(\mathbf{Y},\mathbf{Y})\colon \mathbf{Y} \to \mathbf{Y}. \tag{21}$$

Внаслідок цього, застосування функцій $\mathcal{K}_{opt}^{CE}(\cdot)$ (19) та $\mathcal{K}_{opt}^{SE}(\cdot)$ (20) для обробки, відповідно, ЗК або стеганограм є еквівалентним до використання тотожного відображення $\mathcal{F}_{\mathcal{J}}: \mathbf{U} \to \mathbf{U}, \mathbf{U} \in \mathcal{J}$.

Використання методу $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ (19) дозволяє проводити реконструкцію вихідного виду ЗК навіть в умовах відсутності апріорних даних щодо використаного СМ. Це становить інтерес для розробки методів деструкції стеганограм, що характеризуються мінімальними змінами статистичних параметрів ЦЗ та дозволяють маскувати факт втручання в канал зв'язку, а також визначення можливого шляху вирішення задачі вилучення (екстракції) повідомлень зі стеганограм.

Практичне застосування методу $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ (20) є обмеженим з огляду на необхідність формування стеганограм на основі оброблюваного ЦЗ, що є неможливим у випадку обмеженості апріорних даних щодо використаного СМ. Проте метод $\mathcal{K}_{opt}^{SE}(\mathbf{X}, \mathbf{Y})$ може становити інтерес для порушення роботи стеганографічних каналів зв'язку за рахунок формування та передачі хибних (підроблених) стеганограм, сформованих згідно відомих стеганографічних методів.

За результатами застосування статистичної моделі $\mathcal{M}$ до зображення $\mathbf{U} \in \mathcal{J}$, обробленого з використанням оптимальних методів $\mathcal{K}_{opt}(\cdot)$ (19)-(20), отримуються відповідні статистичні параметри, представлені у вигляді вектору $\mathrm{F}_{cal}^{\mathcal{M}}(\mathbf{U})$. Для віднесення оброблюваного зображення $\mathbf{U}$ до класів ЗК, або ж стеганограм до отриманих векторів $\mathrm{F}^{\mathcal{M}}(\mathbf{U})$ та $\mathrm{F}_{cal}^{\mathcal{M}}(\mathbf{U})$, що відповідають статистичним параметрам вихідного та обробленого зображень, застосовується функція $\mathrm{F}_{class}(\cdot)$ (10). В залежності від способу обробки векторів $\mathrm{F}^{\mathcal{M}}(\mathbf{U})$ та $\mathrm{F}_{cal}^{\mathcal{M}}(\mathbf{U})$ з використанням функції $\mathrm{F}_{class}(\cdot)$ можливо виділити наступні випадки:

$$\mathbf{F}_{CC} = \left\{\mathrm{F}^{\mathcal{M}}(\mathbf{U}); \mathrm{F}_{cal}^{\mathcal{M}}(\mathbf{U})\right\}, \tag{22}$$

$$\mathbf{F}_{DF} = \mathrm{F}_{cal}^{\mathcal{M}}(\mathbf{U}) - \mathrm{F}^{\mathcal{M}}(\mathbf{U}), \tag{23}$$

Відмітимо, що значна кількість відомих стегодетекторів заснована на використанні векторі $\mathbf{F}_{CC}$ (22) з метою забезпечення високої точності виявлення стеганограм. Це досягається шляхом збільшення кількості використовуваних параметрів досліджуваних ЦЗ, що призводить до відповідного зростання вимог до об'єму вибірки ЦЗ, які використовуються для налаштування СД

Враховуючи властивість (21) методів $\mathcal{K}_{opt}^{CE}(\cdot)$ (20) та $\mathcal{K}_{opt}^{SE}(\cdot)$ (21), отримуємо, що значення $\|\mathbf{F}_{DF}\|_2$ при використанні даних функцій є рівними нулю у наступних випадках:

$$\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{X}): \mathbf{X} \to \mathbf{X} \Rightarrow \|\mathbf{F}_{DF}\|_2 = \left\|\mathrm{F}_{cal}^{\mathcal{M}}(\mathbf{X}) - \mathrm{F}^{\mathcal{M}}(\mathbf{X})\right\|_2 = 0,$$

$$\mathcal{K}_{opt}^{SE}(\mathbf{Y}, \mathbf{Y}): \mathbf{Y} \to \mathbf{Y} \Rightarrow \|\mathbf{F}_{DF}\|_2 = \left\|\mathrm{F}_{cal}^{\mathcal{M}}(\mathbf{Y}) - \mathrm{F}^{\mathcal{M}}(\mathbf{Y})\right\|_2 = 0.$$

Відповідно, значення $\|\mathbf{F}_{DF}\|_2$ є рівним нулю при застосуванні методу $\mathcal{K}_{opt}^{CE}(\cdot)$ до ЗК, або ж використання методу $\mathcal{K}_{opt}^{SE}(\cdot)$ для обробки стеганограм. В

інших випадках довжина векторів $\|\mathbf{F}_{DF}\|_2$ (23) є пропорційною до величини зміни статистичних параметрів ЗК, обумовлених приховання повідомлень. Внаслідок цього використання простих порогових методів обробки значень $\|\mathbf{F}_{DF}\|_2$ дозволяє забезпечити надійне виявлення стеганограм незалежно від особливостей використовуваної моделі ЦЗ та обраного типу класифікатора.

В роботі показано, що запропонований метод синтезу високоточних СД шляхом вирішення оптимізаційної задачі (18) дозволяє наблизити точність роботи СД до теоретичних оцінок досяжної імовірності виявлення стеганограм P_E^{lim}, а саме квадратичного закону оцінки значень P_E^{lim} (англ. Square Root Law, SRL). Згідно SRL-закону, для сформованих стеганограм забезпечується ϵ-стійкість ($\mathrm{D}_{KL}\big(\mathbf{f}(c), \mathbf{f}(s)\big) < \epsilon$) до виявлення з використанням статистичних СД при виконанні умови:

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

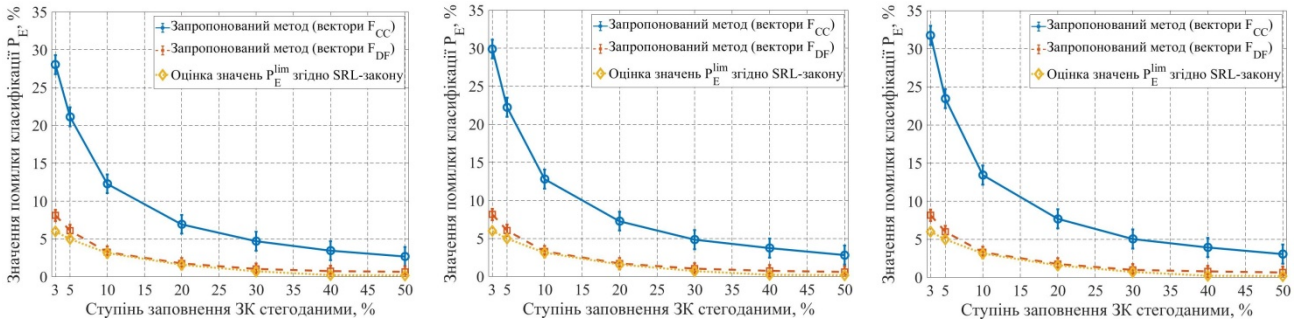
де $n -$ кількість пікселів ЗК, використаних для приховання стегобітів. Оцінка значення P_E^{lim} згідно SRL-закону для випадку виявлення стеганограм, сформованих згідно ACM, була запропонована в роботах Фрідріх Д.:

$$\hat{P}_E^{SRL} \cong 1 - n_s \cdot \mathrm{D}_{KL}(\mathbf{X}, \mathbf{Y}) \cdot \Delta_\alpha^S \cdot \log_2(1/\Delta_\alpha^S), \tag{24}$$

$$\mathrm{D}_{KL}(\mathbf{X}, \mathbf{Y}) = \sum_{q=1}^{2^k-1} P_{\mathrm{c}}(q) \cdot \log_2(P_{\mathrm{c}}(q)/P_s(q)),$$

де $n_s = n/(N \times M) -$ частка пікселів ЗК, використаних для приховання стегобітів; $\mathrm{D}_{KL}(\mathbf{X}, \mathbf{Y}) -$ 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).

Отримані результати підтверджуються експериментальними оцінками досяжної точності роботи СД, синтезованих згідно запропонованого методу, для новітніх стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD. 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 $\mathcal{K}_{opt}^{CE}$ (19), векторів $\mathbf{F}_{CC}$ (22) та $\mathbf{F}_{DF}$ (23) при обробці зображень з тестового пакету ALASKA представлені на рис. 4.



(а) (б) (в)

Рисунок 4 – Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, 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 $\mathbf{F}_{CC}$ (23) 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 стеганограм згідно SRL-закону (24) в області сильного заповнення ЗК стегоданими ($\Delta_\alpha^S > 20\%$, рис. 4).

З іншого боку, виявлено суттєві відмінності між отриманими значеннями помилки виявлення стеганограм P_E при використанні векторів $\mathbf{F}_{CC}$ (22) від теоретичних оцінок (24) у випадку слабкого заповнення ЗК стегоданими ($\Delta_\alpha^S < 10\%$) – зростання значень P_E при виявленні апріорно відомого СМ сягає 20% (рис. 4а), та збільшується до 25% при аналізі невідомих стеганографічних методів (рис. 4в). Це обумовлено поступовим зменшенням кількості пар ЗК та відповідних їм стеганограм у навчальній вибірці $\mathcal{S}_{train}$, що призводить до зниження точності оцінки розмірів та взаємного розташування кластерів $\mathbf{F}_r(c)$ та $\mathbf{F}_r(s)$.

Застосування векторів $\mathbf{F}_{DF}$ (23) дозволяє суттєво (на 20%) зменшити значення помилки виявлення стеганограм P_E навіть у найбільш складному випадку слабкого (менше 10%) ступеня заповнення ЗК стегоданими (рис. 4). 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 забезпечити високу точність виявлення стеганограм у всьому діапазоні значень ступеня заповнення ЗК стегоданими.

Використання запропонованого підходу до синтезу СД дозволяє забезпечити точність роботи стегодетекторів близькою до теоретичних оцінок (24) 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 стеганограм, сформованих згідно адаптивних методів HUGO, S-UNIWARD, MG та MiPOD, при обробці зображень з тестового пакету VISION (рис. 5).

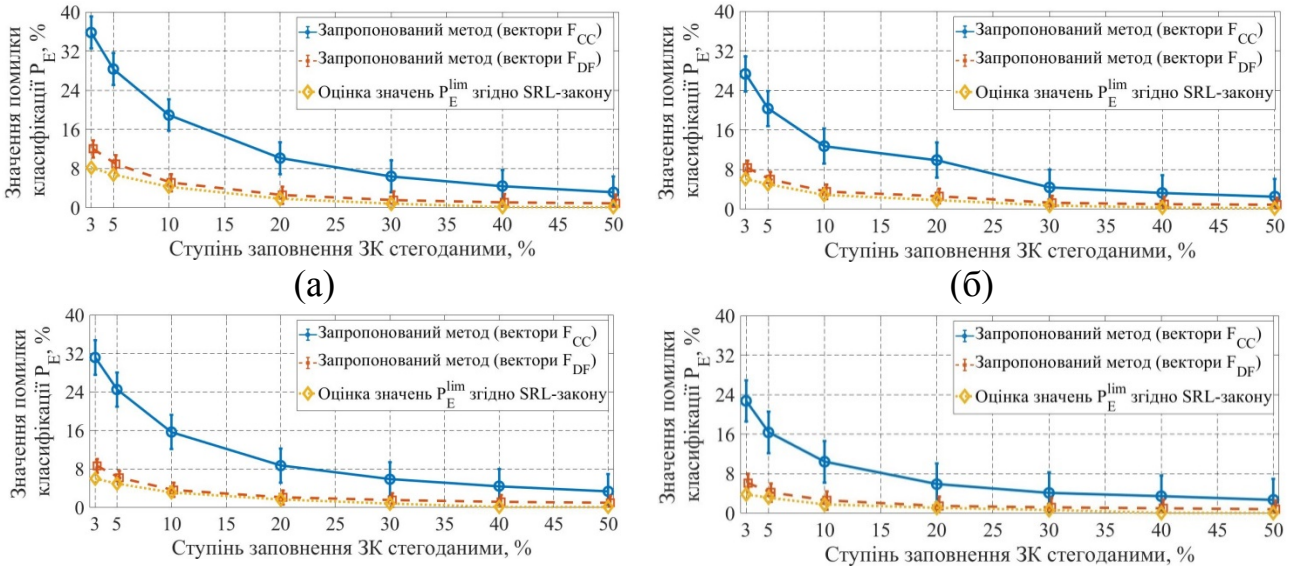


Рисунок 5 – Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно методів HUGO (а), S-UNIWARD (б), MG (в) та MiPOD (г), при використанні перетворення $\mathcal{K}_{opt}^{CE}$ для пакету VISION та значенні параметру $K_\alpha^{OL} = 0\%$. 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 $\mathcal{K}_{opt}^{CE}$ (19) та векторів $\mathbf{F}_{DF}$ (23) дозволяє суттєво (на 25%) зменшити значення P_E у порівнянні з поширеним випадком використання векторів $\mathbf{F}_{CC}$ (22). При цьому використання запропонованого методу побудови високоточних СД шляхом вирішення оптимізаційної задачі (18) дозволяє наблизити точність виявлення стеганограм до теоретичних оцінок (24) досяжної точності роботи СД згідно SRL-закону навіть для новітніх стеганографічних методів MG та MiPOD (рис. 5). Це підтверджує перспективність використання синтезованих стегодетекторів для забезпечення високої точності виявлення стеганограм, сформованих згідно новітніх АСМ.

Наведені результати (рис. 4-5) дозволяють оцінити межі досяжної точності роботи СД, побудованих згідно запропонованого методу, у випадку використання «ідеалізованих» методів попередньої обробки досліджуваних зображень (19)-(20). Для наближення точності роботи методів стегоаналізу ЦЗ до визначених меж запропоновано практичну реалізацію методу $\mathcal{K}_{opt}^{CE}(\mathbf{X}, \mathbf{Y})$ (19), що заснована на декомпозиції багатовимірних сигналів на основі ССФ.

Методи обробки сигналів з використанням ССФ засновані на представленні досліджуваного сигналу $\mathbf{S} = \{s_1, s_2, \cdots, s_S\}$ із застосуванням лише M ($M > 0$) найбільших коефіцієнтів розкладу сигналу при використанні системи базисних функцій (словника) $\mathbf{A}_{SRR}$ спеціального виду. Формування словника $\mathbf{A}_{SRR}$ з використанням пакету сигналів $\mathcal{S}_{train}^{SRR} = \{\mathbf{s}_i\}_{i=1}^{M}$ можливо представити як вирішення наступної оптимізаційної задачі:

$$\min_{\mathbf{A}_{SRR},\{\mathbf{x}_i\}_{i=1}^{M}} \sum_{i=1}^{M} \|\mathbf{x}_i\|_0 , \|\mathbf{s}_i - \mathbf{A}_{SRR}\mathbf{x}_i\|_2 \le \epsilon, i \in [1; M], \epsilon \ge 0, \qquad (25)$$

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

Для побудови матриці $\mathbf{A}_{SRR}$ при збереженні низької обчислювальної складності вирішення задачі (25) в роботі запропоновано використовувати метод K-SVD. Даний метод заснований на представленні виразу (25) у наступному вигляді:

$$\|\mathbf{S} - \mathbf{A}_{SRR}\mathbf{X}_{SRR}\|_F^2 = \left\|\mathbf{S} - \sum_{j=1}^{m} \mathbf{a}_j \mathbf{x}_j^T\right\|_F^2 = \left\|\left(\mathbf{S} - \sum_{j \ne j_0} \mathbf{a}_j \mathbf{x}_j^T\right) - \mathbf{a}_{j_0}\mathbf{x}_{j_0}^T\right\|_F^2. \qquad (26)$$

де $\mathbf{x}_j^T$ – відповідає j –тому рядку матриці $\mathbf{X}_{SRR}$. Вирішення задачі (26) відповідає мінімізації норми матриці $\mathbf{E}_{j_0}$:

$$\left\|\mathbf{E}_{j_0}\right\|_F^2 = \left\|\left(\mathbf{S} - \sum_{j \ne j_0} \mathbf{a}_j \mathbf{x}_j^T\right)\right\|_F^2 \to min. \qquad (27)$$

Для отримання j_0 –того стовпчика матриці $\mathbf{E}_{j_0}$ запропоновано використовувати оператор проекції матриці в простір $\mathbf{P}_{j_0}$. Позначимо результат застосування оператору $\mathbf{P}_{j_0}$ до матриці помилок $\mathbf{E}_{j_0}$ як $\left(\mathbf{x}_{j_0}^R\right)^T = \mathbf{x}_{j_0}^T\mathbf{P}_{j_0}$. Тоді добуток матриць $\mathbf{E}_{j_0}\mathbf{P}_{j_0}$ може бути апроксимований матрицею з рангом рівним одиниці, отриманої шляхом сингулярного розкладу матриці $\mathbf{E}_{j_0}$ (27). Дана апроксимація використовується для ітеративного оновлення значень як елемента $\mathbf{a}_{j_0}$ словника $\mathbf{A}_{SRR}$, так і коефіцієнтів розкладу поточного вектору $\mathbf{x}_{j_0}^T$ з використанням методу найменших квадратів:

$$\mathbf{x}_{j_0}^R = \left(\mathbf{P}_{j_0}^T\mathbf{E}_{j_0}^T\mathbf{a}_{j_0}\right)/\left\|\mathbf{a}_{j_0}\right\|_2^2, \mathbf{a}_{j_0} = \left(\mathbf{E}_{j_0}\mathbf{P}_{j_0}\mathbf{x}_{j_0}^R\right)/\left\|\mathbf{x}_{j_0}^R\right\|_2^2. \qquad (28)$$

Особливістю методів обробки сигналів з використанням ССФ є врахування варіативності статистичних та спектральних параметрів досліджуваних ЦЗ в процесі вирішення оптимізаційної задачі (25). Це дозволяє формувати системи функцій розкладу ЦЗ в залежності від наявних даних щодо параметрів ЗК та стеганограм, що становить особливий інтерес для побудови високоточних СД.

Для дослідження ефективності запропонованого методу синтезу СД в роботі проведено аналіз точності роботи стегодетектору при використанні матриці $\mathbf{A}_{SRR}$, сформованої з використанням вибірки з 10,000 зображень з пакету ALASKA, які не використовувалися в попередніх розділах роботи. Враховуючи високу обчислювальну складність формування $\mathbf{A}_{SRR}$ при обробці ЦЗ значного розміру (більше 256×256 пікселів), проведено розділення ЦЗ на частини фіксованого розміру $w_{UC} \times w_{UC}$ (пікселів), що не перекриваються. Значення пара-

метру w_{UC} варіювалося в наступних межах –16×16, 32×32 та 64×64 (пікселів). Загальна кількість функцій (векторів-стовпчиків у словнику $\mathbf{A}_{SRR}$) для проведення декомпозиції сигналів була обрана рівною N_{UC}.

Аналіз точності виявлення стеганограм, сформованих згідно стеганографічних методів HUGO, S-UNIWARD, MG та MiPOD, при використанні запропонованого методу синтезу СД проводився при варіації значень розмірів w_{UC} блоків розбиття та кількості компонентів N_{UC} розкладу досліджуваних ЦЗ. Визначення статистичних параметрів оброблених ЦЗ проводилося із застосуванням стандартної статистичної моделі SPAM. Залежності значень помилки виявлення стеганограм P_E, сформованих згідно новітніх методів MG та MiPOD, при використанні запропонованого методу синтезу СД та векторів $\mathbf{F}_{CC}$ (22) та $\mathbf{F}_{DF}$ (23) для зображень зі стандартного пакету ALASKA наведені на рис. 6.

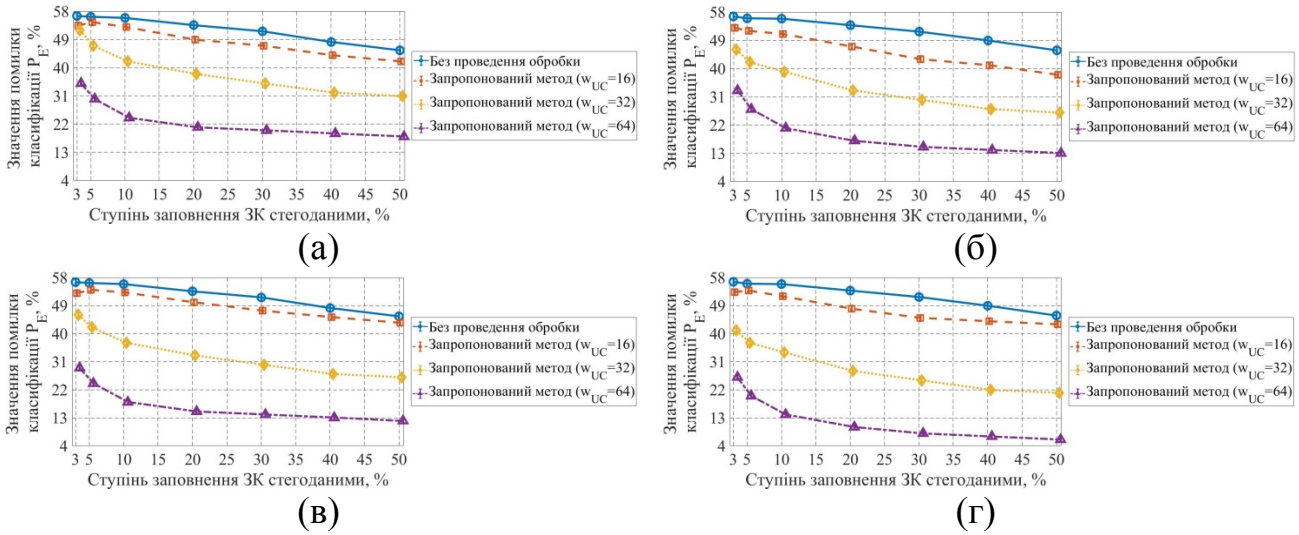


Рисунок 6 – Залежності значень помилки виявлення стеганограм P_E від ступеня заповнення ЗК стегоданими для стеганограм, сформованих згідно методів MG (а, в) та MiPOD (б, г), при використанні запропонованого методу попередньої обробки ЦЗ ($N_{UC} = 512$) та векторів $\mathbf{F}_{CC}$ (а-б) та $\mathbf{F}_{DF}$ (в-г) для пакету ALASKA ($K_{\alpha}^{OL} = 0\%$). Значення P_E наведено для довірчого інтервалу з рівнем довіри 95%

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. 6в-г). При цьому зменшення кількості помилок виявлення стеганограм досягається як в області сильного ($\Delta_{\alpha}^{S} > 20\%$), так і слабкого ($\Delta_{\alpha}^{S} < 10\%$) ступеня заповнення ЗК стегоданими, що є одним з найбільш складних випадків при проведенні стегоаналізу ЦЗ.

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 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. Перевагою запропонованого комплексу у порівнянні з відомими методами виявлення стеганограм є забезпечення надійного виявлення прихованих повідомлень навіть в найбільш складному випадку, а саме відсутності апріорних даних щодо використаного СМ. З огляду на дану особливість комплексу, для нього запропонована назва Blind-Steg. Архітектура комплексу наведена на рис. 7.

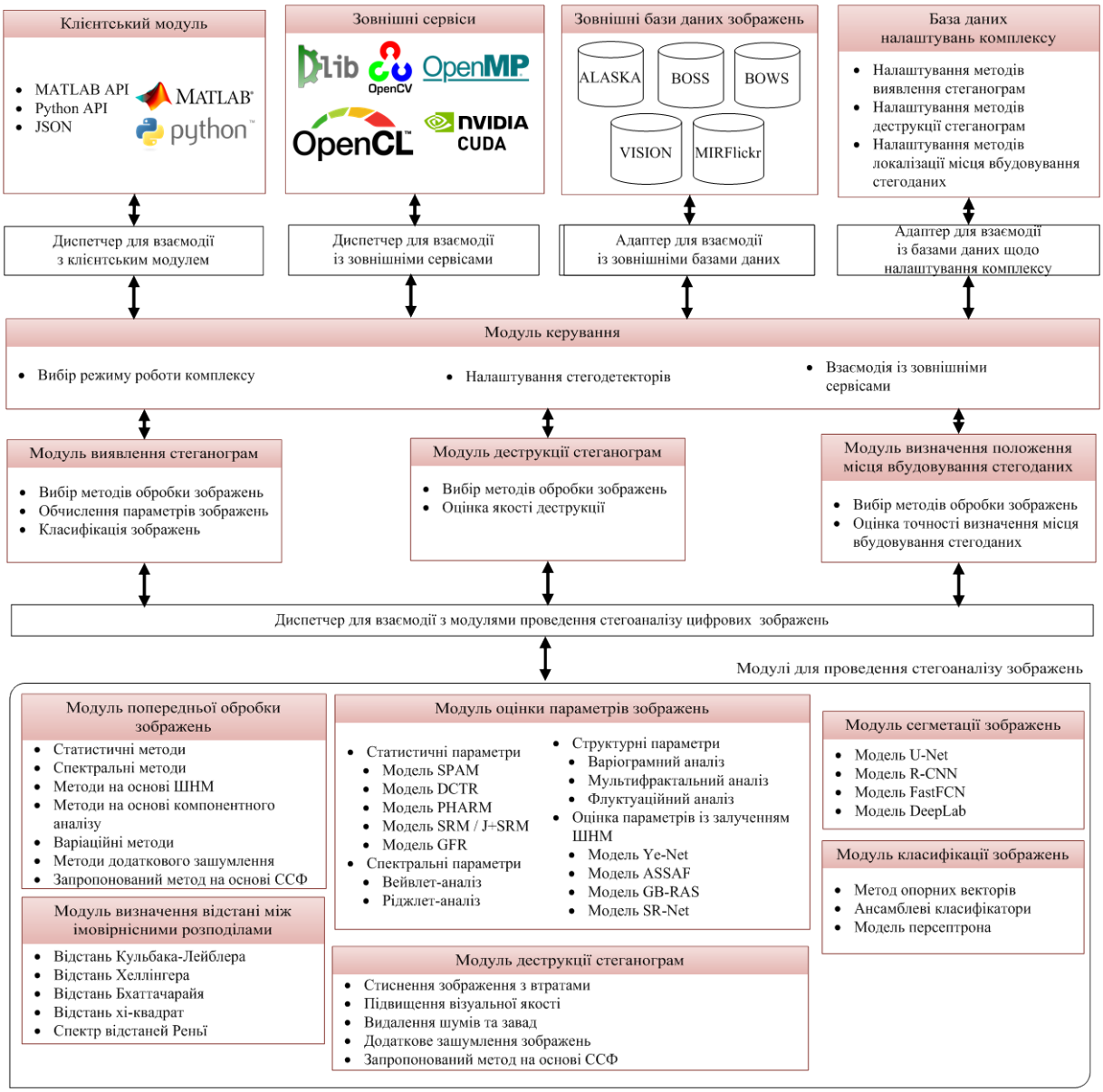


Рисунок 7 – Архітектура запропонованого та реалізованого комплексу Blind-Steg для проведення стегоаналізу цифрових зображень.

Комплекс Blind-Steg побудований з використанням мікросервісної архітектури (рис. 7), що дозволяє гнучко налаштовувати його роботу в залежності від умов проведення стегоаналізу ЦЗ. Для обробки досліджуваних зображень з використанням запропонованого комплексу також залучаються загальнодоступні (відкриті) програмні модулі (рис. 7), зокрема бібліотеки для прискорення проведення обчислень (зокрема, CUDA, OpenMP, OpenCL), використання спеціальних методів обробки зображень (наприклад, DLib, OpenCV), визначення статистичних параметрів ЦЗ (статистичні моделі SPAM, DCTR, SRM тощо), подальшої сегментації оброблюваних зображень з використанням ШНМ (а саме, штучний нейронних мереж U-Net, FastFCN, DeepLab та інші). Дані модулі поширюються згідно дозвільної ліцензії (зокрема, ліцензій MIT, BSD та GNU GPL) для вільного використання при проведенні досліджень.

До складу комплексу входять модулі (диспетчери) для взаємодії з зовнішніми системами, зокрема клієнтським модулем, програмними бібліотеками для прискорення обчислень, а також базами даних зображень, що можуть залучатися при проведенні досліджень (рис. 7). Вибір режиму функціонування (наприклад, виявлення та подальшої деструкції стеганограм, визначення пікселів, використаних для приховання стегобітів) та параметрів налаштування стегодетекторів проводиться модулем керування роботою комплексом згідно з результатами обробки запитів від користувачі комплексу. Дані налаштування передаються до відповідних модулів для проведення стегоаналізу ЦЗ (рис. 7), які використовують загальний реєстр доступних кроків обробки зображень, наприклад для проведення попередньої обробки, визначення статистичних, спектральних та структурних параметрів зображень тощо. Модулі для обробки ЦЗ при проведенні стегоаналізу реалізовані у вигляді окремих сервісів (рис. 7), що дозволяє швидко оновлювати та розширювати перелік можливостей комплексу Blind-Steg. За результатами обробки ЦЗ модулем керування формуються відповіді на запити користувачів комплексу, що включають: результати виявлення стеганограм (зокрема, перелік зображень які було віднесено до класу стеганограм за результатами аналізу), деструкції прихованих повідомлень (наприклад, оцінки змін статистичних, спектральних параметрів ЦЗ після проведення обробки), та локалізації місця вбудовування стегобітів до ЗК (а саме, перелік пікселів, що імовірно були використані для приховання бітів повідомлення).

В роботі досліджено точність роботи відомих СД, зокрема стегодетекторів запропонованих в роботах Кошкіної Н.В. та Корольова В.Ю., а також розробленого комплексу Blind-Steg у випадку формування стеганограм згідно сучасних адаптивних стеганографічних методів HUGO, MG та MiPOD. Стегодетектор Кошкіної Н.В. заснований на повторному вбудовуванні (контрольному вкрапленні) до досліджуваного ЦЗ тестової послідовності згідно відомого СМ (в роботі досліджено випадок використання стеганографічного методу HUGO). Метод виявлення стеганограм, запропонований Корольовим В.Ю., заснований на модифікації RS-CA аналізу стеганограм, а саме дослідження змін статистичних характеристик ЦЗ при обробці його ковзним вікном різного розміру. Для

порівняння розглянуто випадок використання статистичних стегодетекторів, заснованих на застосуванні поширених типів методів попередньої обробки ЦЗ.

Отримані значення помилки класифікації стеганограм P_E при використанні відомих СД та розробленого комплексу Blind-Steg для зображень з пакету ALASKA наведені в табл. 1.

Таблиця 1 – Значення помилки класифікації стеганограм P_E для відомих стегодетекторів та розробленого комплексу Blind-Steg при використанні $\mathbf{F}_{DF}$ векторів. Розглянуто випадок слабкого ступеня заповнення ЗК стегоданими ($\Delta_\alpha^S = 5\%$), та використання пакету зображень ALASKA. Значення P_E наведено для довірчого інтервалу з рівнем довіри 95%

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_E при використанні стеганографічних методів, %			Середня тривалість роботи СД, сек
	HUGO	MG	MiPOD	
Стегодетектор Кошкіної Н.В.	21.2 ± 7.8	21.1 ± 1.7	22.0 ± 7.7	7.58
Стегодетектор Корольова В.Ю.	23.8 ± 0.2	23.5 ± 4.0	27.9 ± 2.8	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 ($\Delta_\alpha^S = 20\%$)	53.4 ± 4.4	53.9 ± 8.3	54.6 ± 4.6	8.73
Додаткове зашумлення ЦЗ з використанням фрактального шуму	52.8 ± 8.7	56.0 ± 5.5	56.5 ± 2.9	9.10
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними				
Вейвлет-фільтрація ЦЗ	12.8 ± 0.8	10.9 ± 5.8	15.4 ± 7.3	12.45
Знешумлення ЦЗ з використанням варіаційного методу Брегмана	48.7 ± 2.2	50.8 ± 8.5	52.8 ± 1.6	17.51
Знешумлення зображень на основі знешумлюючих автоенкодерних мереж	47.7 ± 7.6	48.4 ± 0.7	51.2 ± 7.2	27.07
Обробка ЦЗ із застосуванням методу головних компонентів	45.7 ± 1.4	48.2 ± 3.5	50.1 ± 3.9	24.00
Комплекс Blind-Steg	**10.7 ± 0.8**	**9.0 ± 1.3**	**11.2 ± 2.2**	**8.24**

Виявлено суттєве обмеження практичного використання методів попередньої обробки досліджуваних ЦЗ, заснованих на додатковому зашумленні зображень з використанням фрактального шуму, а саме необхідність тривалого вибору параметрів даного шуму для зменшення значень помилки класифікації P_E.

Зокрема, використання поширених параметрів генерації фрактальних шумів (рис. 7) призводить до незначного посиленням енергії спотворень ЦЗ, обумовлених приховання повідомлень згідно методу MiPOD, що ускладнює виявлення сформованих стеганограм (табл. 1). Це підтверджується отриманими результатами дослідження точності роботи СД (табл. 1) – додаткове зашумлення ЦЗ з використанням фрактального шуму призводить до зростання значення P_E до 55.98% для даного типу МПО, у порівнянні з 15.58% для запропонованого комплексу.

Відмітимо, що використання методів вейвлет-фільтрації дозволяє суттєво зменшити значення помилки P_E у порівнянні з поширеними типами методів попередньої обробки (табл. 1). Використання запропонованого методу синтезу СД дозволяє додатково зменшити значення помилки класифікації стеганограм P_E ($\Delta P_E \cong 5\%$) у порівнянні з випадком використання методів вейвлет-фільтрації (табл. 1). При цьому отримані значення помилки P_E є близькими до отриманих раніше оцінок досяжної точності роботи СД (рис. 4а).

Для порівняння, в роботі досліджено випадок використання розглянутих СД для виявлення стеганограм, сформованих згідно апріорно невідомих СМ. Дослідження точності роботи СД проводилося з використанням адаптивних стеганографічних методів Synch, UED та HILL. Отримані значення помилки класифікації стеганограм P_E при сучасних СД та розробленого комплексу Blind-Steg для зображень з пакету Google Open Image, наведені в табл. 2.

Таблиця 2 – Значення помилки класифікації стеганограм P_E для відомих стегодетекторів та розробленого комплексу Blind-Steg при використанні $\mathbf{F}_{DF}$ векторів та слабкому ступені заповнення ЗК стегоданими ($\Delta_\alpha^S = 5\%$). Розглянуто випадок використання СД, налаштованого із застосуванням пакету зображень ALASKA та стеганографічного методу MiPOD, та подальшого тестування на зображеннях з пакету Google Open Image. Значення P_E наведено для довірчого інтервалу з рівнем довіри 95%

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.	53.1 ± 4.6	49.9 ± 3.4	50.3 ± 0.4	9.01
Стегодетектор Корольова В.Ю.	55.7 ± 6.5	55.0 ± 3.9	57.6 ± 6.2	9.78
Методи попередньої обробки ЦЗ, засновані на виділенні спотворень, обумовлених прихованням стегоданих до зображення-контейнеру				
Повторне приховання повідомлень до ЦЗ згідно стеганографічного методу MiPOD ($\Delta_\alpha^S = 20\%$)	54.2 ± 2.8	54.5 ± 9.7	56.0 ± 6.6	9.24

Таблиця 2 (продовження)

Метод попередньої обробки зображень	Значення помилки виявлення стеганограм P_E при використанні стеганографічних методів, %			Середня тривалість роботи СД, сек
	Synch	UED	HILL	
Додаткове зашумлення ЦЗ з використанням фрактального шуму	51.9 ± 8.8	47.9 ± 4.2	45.4 ± 4.1	12.57
Методи попередньої обробки ЦЗ, засновані на оцінці статистичних параметрів ЗК за наявними (зашумленими) даними				
Вейвлет-фільтрація ЦЗ	48.1 ± 4.0	47.3 ± 9.0	50.7 ± 4.3	18.02
Знешумлення ЦЗ з використанням варіаційного методу Брегмана	50.6 ± 6.4	46.6 ± 2.5	49.5 ± 5.6	20.15
Знешумлення зображень на основі знешумлюючих автоенкодерних мереж	43.1 ± 4.3	40.8 ± 2.8	39.3 ± 7.7	43.18
Обробка ЦЗ із застосуванням методу головних компонентів	48.0 ± 5.7	48.3 ± 4.6	50.0 ± 2.4	30.48
Комплекс Blind-Steg	**14.6 ± 1.2**	**12.5 ± 1.9**	**12.5 ± 3.4**	**13.21**

Застосування запропонованого методу попередньої обробки ЦЗ дозволяє суттєво (до чотирьох разів) зменшити значення помилки класифікації стеганограм P_E, сформованих згідно апріорно невідомих АСМ, у порівнянні з випадком використання поширених методів обробки цифрових зображень (табл. 2). При цьому СД, побудований на основі запропонованого підходу дозволяє скоротити тривалість обробки зображень 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. Отримані результати підтверджують переваги запропонованого підходу у порівнянні з існуючими методами синтезу СД, та перспективність їх практичного впровадження у реальних системах моніторингу та контролю ІКС.

Висока точність реконструкції ЗК при використанні розробленого комплексу Blind-Steg на основі вирішення оптимізаційної задачі (25) з використанням ССФ 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.

Визначальним критерієм якості роботи методів деструкції стеганограм є мінімізація частки пікселів Δ_p зображення-контейнеру, використаних при вбу-

довуванні повідомлень. Проте практичне застосування методів деструкції призводить до значних змін статистичних параметрів оброблюваних зображень, що демаскує роботу стегоаналітика. З огляду на отримані результати щодо високої точності реконструкції ЗК за наявними (зашумленими) даними, становить інтерес використання комплексу Blind-Steg в задачах деструкції стеганограм при забезпеченні маскування факту втручання в канал передачі ЦЗ.

Для оцінки ефективності застосування комплексу Blind-Steg в задачах деструкції стеганограм, сформованих згідно сучасних АСМ, досліджено зміни параметрів оброблених зображень, а саме:

- Статистичні параметри (Δ_F^{SPAM}) – визначалися з використанням стандартної статистичної моделі SPAM для оцінки ступеня кореляції значень яскравості суміжних пікселів цифрового зображення;
- Спектральні параметри ($\Delta W_{uv}^{(k)}$) – визначалися із застосуванням коефіцієнтів $W_{uv}^{(k)}$ двовимірного дискретного вейвлет-перетворення ЦЗ при використанні вейвлету Хаара та відповідної йому скейлінг-функції в якості базисних функцій перетворення;
- Структурні параметри – визначалися з використанням спектру Реньї (ΔD_R) та мультифрактального спектру ($\Delta f(\alpha)$) ЦЗ.

Отримані оцінки ступеня зміни статистичних, спектральних і структурних параметрів стеганограм, а також частки пікселів Δ_p, використаних для приховання стегобітів, що лишилися незміненими при використанні досліджуваних методів обробки ЦЗ наведені в Табл. 3.

Таблиця 3 – Зміни статистичних, спектральних та структурних параметрів стеганограм, а також частка пікселів Δ_p, використаних для приховання стегобітів, що лишилася незміненими, при вбудовуванні повідомлень згідно методу Synch та використанні досліджуваних методів обробки цифрових зображень для зображень з пакету ALASKA

	Δ_F^{SPAM}, %	$\Delta W_{uv}^{(k)}$, %	ΔD_R, %	$\Delta f(\alpha)$, %	Δ_p, %
Ідеалізований випадок	0.00	0.00	0.00	0.00	0.00
Слабкий ступінь заповнення ЗК стегоданими ($\Delta_\alpha^S = 3\%$)					
Медіанна фільтрація (5 × 5 пікселів)	98.65	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 ЦЗ	82.03	17.93	3.75	5.39	12.17
Запропонований метод реконструкції ЗК	**15.57**	**13.40**	**1.77**	**1.22**	**7.12**
Середній ступінь заповнення ЗК стегоданими ($\Delta_\alpha^S = 10\%$)					
Медіанна фільтрація (5 × 5 пікселів)	90.70	85.27	9.09	4.69	56.95
JPEG-стиснення з втратами (IQF=75%)	81.60	59.69	12.71	5.48	18.02

Таблиця 3 (продовження)

	Δ_F^{SPAM}, %	$\Delta W_{uv}^{(k)}$, %	ΔD_R, %	$\Delta f(\alpha)$, %	Δ_p, %
TVM-обробка ЦЗ	76.03	22.04	6.82	5.31	10.03
Запропонований метод реконструкції ЗК	**11.18**	**10.62**	**2.35**	**3.71**	**4.44**

Застосування запронованого методу реконструкції ЦЗ шляхом вирішення оптимізаційної задачі (25) при проведенні деструкції стеганограм дозволяє 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. При цьому зниження частки стегобітів, що лишилися незміненими після проведеня деструкції залишається малою (близько до 7%) навіть у найбільш складному випадку проведення деструкції, а саме слабкого заповнення ЗК стегоданими (табл. 3). Це дозволяє забезпечити надійну деструкцію стеганограм при суттєвому зниженні (до шести разів, табл. 3) 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 прихованні 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. Вирішення даних задач становить особливий інтерес для протидії промисловому шпигунству та військовій розвідці, а саме перехоплення повідомлень противника (конкурента), впровадження дезінформації в стеганографічний канал передачі ІзОД. Проте у відкритій літературі наразі відсутні відомості щодо можливих шляхів вилучення повідомлень в умовах відсутності апріорних даних та малого ($\Delta_\alpha^S < 10\%$) ступеня заповнення ЗК стегоданими, зважаючи на високу складність даної задачі.

В роботі показано ефективність використання запропонованого методу реконструкції ЦЗ шляхом вирішення оптимізаційної задачі (25) для налаштування методу сегментації ЦЗ на основі стандартної штучної нейронної мережі U-Net. Налаштування блоку сегментації ЦЗ комплексу Blind-Steg (рис. 7) для вилучення прихованих повідомлень проводилося з використанням вибірки з 10,000 зображень з пакету ALASKA. Досліджено випадок обробці ЗК та стеганограм, сформованих згідно методів HUGO, MiPOD та Synch. Ступінь заповнення ЗК стегоданими Δ_α^S обиралася псевдовипадковим чином з діапазону $\Delta_\alpha^S \in [3; 50]$.

Оцінка точності сегментації ЦЗ при застосуванні запропонованого підходу проводилася з використанням показника Сьоренсена-Дайса $DSC(M_t, M_p)$ та індексу Тверського $D_T^S(M_t, M_p)$:

$$DSC(M_t, M_p) = 2 \cdot \frac{|M_t \cap M_p|}{|M_t| + |M_p|}, \quad (29)$$

$$D_T^S(M_t, M_p) = \frac{|M_t \cap M_p|}{|M_t \cap M_p| + \beta(\alpha \cdot a + (1-\alpha) \cdot b)}, \quad (30)$$

$$a = \min(|M_t \setminus M_p|, |M_p \setminus M_t|), b = \max(|M_t \setminus M_p|, |M_p \setminus M_t|),$$

де $M_t -$ послідовність «істинних» значень міток пікселів; $M_p -$ послідовність міток пікселів, отриманих за результатами роботи розробленого методу; $A \setminus B -$ доповнення множини A до множини B; $\alpha, \beta \geq 0 -$ вагові коефіцієнти.

Значення показників $DSC(M_t, M_p)$ (29) та $D_T^S(M_t, M_p)$ (30) змінюється від 0 до $(+1)$. При цьому значення даних показників рівне нулю відповідає випадку відсутності в послідовності M_p пікселів, використаних для приховання стегобітів, а значення рівне одиниці – співпадінню послідовностей M_t та M_p (коректному визначенню позицій всіх пікселів ЗК, використаних при формуванні стеганограми).

Значення показників (29)-(30) при обробці стеганограм, сформованих згідно методів HUGO, MiPOD та Synch, з використанням новітньої штучної нейронної мережі SR-Net та запропонованого методу наведені в табл. 4.

Таблиця 4 – 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

		Ідеалізований 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
	$D_T^S(M_t, M_p)$	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 комплексу Blind-Steg ($w_{UC} = 16$, $N_{UC} = 512$)					
$\Delta_\alpha^S = 5\%$	$DSC(M_t, M_p)$	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

Таблиця 4 (продовження)

		Ідеалізований випадок	Стеганографічний метод		
			HUGO	MiPOD	Synch
$\Delta_\alpha^S = 50\%$	$DSC(M_t, M_p)$	1.000	0.919	0.882	0.807
	$D_T^S(M_t, M_p)$	1.000	0.883	0.858	0.781

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 ($\Delta_\alpha^S = 5\%$, табл. 4).

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 слабкого заповнення ЗК стегоданими, табл. 4), підтверджує перспективність застосування запропонованого підходу для роботи з новітніми АСМ.

У **додатках** наведено: перелік публікацій за темою дисертаційного дослідження; результати дослідження точності виявлення стеганограм при використанні сучасних статистичних СД для цифрових зображень, а також отримані оцінки межі вірогідності виявлення стеганограм при використанні стегодетекторів, сформованих на основі запропонованого методу синтезу структури та оптимізації параметрів.

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 унеможливлює 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 спектральній параметрів оброблених зображень. Це дозволило 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-Лінденштрауса 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 середнього заповнення ЗК стегоданими ($\Delta_\alpha^S \geq 10\%$). 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 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 розроблено 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 ме-

тоду 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 та слабкому (менше 10%) ступеню заповнення ЗК стегоданими. 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 обробки 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 дозволило 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 стеганографічній канал передачі ІзОД. Отримані результати дозволяють створити передумови для вирішення найбільш складних задач стегоаналізу ЦЗ, а саме розробки методів екстракції та підміни стегоданих.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України

1. **Прогонов Д.О.** Аналіз змін хі-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. (Категорія «А», включене до наукометричної бази **Web of Science**).

2. **Прогонов Д.О.** Аналіз змін хі-квадрат відстані між розподілами яскравості пікселів при фільтрації стеганограм, сформованих згідно методу UNI-WARD [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/RA-DAP.2019.76.72-76. (Категорія «А», включене до наукометричної бази **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 (Категорія «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/10.155-88/1607-3274-2021-1-18 (Категорія «А», включене до наукометричної бази **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 (Категорія «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. (Категорія «Б»).

7. **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. (Категорія «А», включене до наукометричної бази **Scopus, квартиль Q3**). *Особистий внесок: аналітичний огляд сучасних методів виявлення стеганограм з використанням ШНМ, аналіз отриманих експериментальних даних щодо точності виявлення стеганограм з використання новітніх типів СД.*

8. **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. (Категорія «А», включене до наукометричної бази **Web of Science**).

9. **Progonov Dmytro**. Investigation of Digital Image Preprocessing Methods Influence on the Accuracy of Stego Images Detection [Text] / **Progonov Dmytro** // Visnyk NTUU KPI Seriia - Radiotekhnika Radioaparatobuduvannia, Vol. (89). – 2022. – pp. 54-60. DOI: https://doi.org/10.20535/RADAP.2022.89.54-60 (Категорія «А», включене до наукометричної бази **Web of Science**).

10. **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. (Категорія «Б») *Особистий внесок: аналітичний огляд сучасних методів попередньої обробки ЦЗ в задачах стегоаналізу, аналіз отриманих експериментальних даних точності виявлення стеганограм при використанні методів вейвлет-аналізу та декомпозиції сигналу із застосуванням складних систем функцій*.

11. **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. (Категорія «Б»).

12. **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 (Категорія «Б»).

13. 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. (Категорія «А», включене до наукометричної бази **Scopus, квартиль Q2**). *Особистий внесок: аналітичний огляд сучасних методів стегоаналізу цифрових даних та їх застосування для побудови комплексних систем захисту інформації*.

Статті у іноземних наукових фахових виданнях

14. **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. (включене до наукометричних баз **Scopus** та **Web of Science, квартиль Q2**). *Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів*.

15. **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).

16. **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).

17. **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).

18. **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).

19. **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: оригінальні результати порівняльного аналізу точності виявлення стеганограм при проведенні повторного (контрольного) вбудовування*.

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

21. **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).

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 багатоетапних стеганографічних методів*.

Міжнародні 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. Ідентифікатор документу в міжнародних системах індексації патентів: US20220350869A1 (USA), WO2021149882A1 (WIPO), KR202100952-82A (Republic of Korea). *Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів*

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

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. Ідентифікатор документу в міжнародних системах індексації патентів: WO2023153637A1 (WIPO), PCT/KR2022/021652 (Republic of Korea). *Особистий внесок: розробка методів синтезу спеціальних систем функцій для аналізу та знешумлення даних з біометричних сенсорів.*

Публікації у збірниках наукових праць, матеріалах 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, 2017. – с. 266-268;

27. **Прогонов Д.О.** Вплив невідповідності областей приховання повідомлень та проведення стегоаналізу 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 ЗК, на основі аналізу параметрів авторегресійних моделей кореляції значень яскравості суміжних пікселів ЦЗ.*

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 АСМ, 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 ЗК стегоданими за величиною зміни параметрів авторегресійних моделей ЦЗ, обумовлених прихованням повідомлень до ЗК.*

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, мате-

матики 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 СМ, при використанні методів компонентного аналізу сигналів*.

32. **Прогонов Д.О.** Ефективність варіаційних методів шумоподавлення у задачах активного стегоаналізу 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 ЗК, з використанням 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 СМ.*

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 АСМ, при використанні сучасних статистичних моделей ЗК*.

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 СД 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/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 стегоданих шляхом використання спеціальних методів масштабування ЦЗ.*

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 ЗК.*

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 ЗК 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 ACM, 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 ЗК 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 АСМ, при проведенні попередньої обробки ЦЗ 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 АСМ, 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.

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 ACM, 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.

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*.

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», Київ, 2024.

Дисертаційну роботу присвячено вирішенню актуальної науково-прикладної проблеми забезпечення високої імовірності 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. Запропоновано нову концепцію побудови стегодетекторів, що заснована інтеграції етапів попередньої обробки цифрових зображень та аналізу статистичних, структурних і спектральній параметрів оброблених зображень для зменшення складності налаштування стегодетекторів при забезпеченні високої точності виявлення стеганограм. На основі запропонованого методу синтезу структури та оптимізації параметрів стегодетекторів розроблено та реалізовано програмний комплекс для проведення стегоаналізу цифрових зображень. Комплекс дозволяє автоматизувати вирішення широкого спектру задач, що стосуються синтезу структури високоточних стегодетекторів для надійного виявлення стеганограм в умовах «сліпого» стегоаналізу, розроб-

ки методів локалізації положення пікселів, використаних для вбудовування стегобітів, та вилучення прихованих повідомлень, а також деструкції стеганограм при забезпеченні мінімальних змін статистичних параметрів оброблюваних зображень, що дозволяє маскувати вплив на стеганографічний канал передачі даних.

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.

SUMMARY

Progonov D.O. Structural synthesis and parametric optimization of methods for stegdetectors design for digital images. – Qualifying scientific work, manuscript. Thesis for a doctoral degree in technical sciences, specialty 05.13.21 – information security systems. – National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute», Kyiv, 2024.

Disruption of critical infrastructure systems (CIS) of government institutions and private corporations, especially in the context of military operations, can lead to unauthorized leakage of restricted information, as well as significant losses in the economic, social, political and military spheres. Effective countermeasures against the use of non-forceful methods of influence by the adversary (competitor) to disrupt the operation of the CIS requires the introduction of multi-level and comprehensive protection of the critical information infrastructure of state and private organizations. Special attention is paid to measures aimed at reducing threats related to the leakage of personal data when exchanging multimedia data, such as digital images, in communication systems, in particular, ensuring reliable detection of hidden (steganographic) transmission channels information with limited access.

In a number of theoretical studies and practical applications of the methods for high-precision stegdetectors (SD) design, there are problems caused by: limited or even lack of a priori data regarding the type and parameters of the embedding method, the impossibility of reliable detection of stego images under minimization of cover image payload, non-linear dependence of SD accuracy on the statistical and spectral characteristics of processed digital images. In particular, this applies to cases of detection of stego images formed using the novel adaptive steganographic methods, which allow to minimize changes in the statistical, spectral and structural parameters of the cover image by message hiding.

The thesis is devoted to solving of the actual scientific and applied problem of ensuring a high probability of stego images detecting in the absence of a priori data on the used embedding method, minimizing of cover image payload with stegodata, and changing statistical, spectral, and structural parameters of processed images within wide limits. To solve this problem, the work proposes a new concept for the design of SD that is based on the integration the stages of digital image preprocessing and analysis of statistical, structural and spectral parameters of processed images. This allows reducing the complexity of designed SD while ensuring high accuracy of stego images detection.

In order to solve the researched scientific and applied problem, a new concept of design methods of pre-processing of the investigated images is proposed, which is based

on the use of special methods of image decomposition and synthesis, to ensure high accuracy of the estimation of cover image parameters based on the available (noisy) data.

On the basis of the proposed approaches to the selection of optimal methods of preprocessing of the digital images according to the criterion of minimizing the value of the stego images classification error P_E, experimental estimates of the probability limit of stego images detection were obtained depending on the available a priori data on the used embedding method and statistical parameters of the investigated images. In order to align stegdetector's accuracy with estimated limit of the probability of stego images detection, a method of synthesis of the structure and optimization of the parameters of high-precision detectors is proposed. The proposed method is based on representation the task of a SD design as an optimization task of maximizing the distance between the probability distributions of the brightness values of the pixels of the cover and stego images after their pre-processing.

On the basis of the proposed method of structure synthesis and optimization of parameters of SD, a software complex for carrying out steganalysis of digital images is proposed and developed. The complex allows to automate the solution of a wide range of tasks related to the synthesis of the structure of high-precision SD for the reliable detection of stego images under the conditions of "blind" steganalysis, the design of methods for the localization of the position of pixels used for embedding stegobits, and the extraction of hidden messages, as well as the destruction of stego images while ensuring minimal changes in statistical parameters of processed images, which allows to conceal the influence on the steganographic data transmission channel.

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 imagaes, methods of replacing embedded data.