ВІДГУК

офіційного опонента д.т.н., проф. **Халімова Геннадія Зайдуловича**

на дисертаційну роботу **Прогонова Дмитра Олександровича**

«Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень»,

подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Актуальність обраної теми дисертації

Стеганографія являється одним з напрямків криптографії і визначає методи приховування інформації при передачі по відкритим каналам. На даний час цій напрямок активно досліджується в питаннях як розробки ефективних методів приховування, оцінки пропускної властивості таких каналів передачі так і боротьби зі стеганографічними каналами на рівні захисту інтересів держави. Особливістю стеганографічних каналів зв'язку є приховання власне факту передачі інформації, що дозволяє долати існуючі системи протидії витоку як конфіденційних даних так і атак на ресурси країни через інформаційне середовище.

Більшість стеганоканалів побудовано на цифрових контейнерах на основі цифрових зображень. Такий підхід визначається великою ємкістю контейнерів і насиченістю ресурсів інтернет таким даними. Боротьба зі стеганоканалами вимагає вирішення ряду задач на рівні розробки ефективних рішень щодо побудови детекторів стеганоданих, які дозволяють виявляти стеганоканали з високою ймовірністю за короткий час. Сучасні стегодетектори (СД) засновані на комплексному використанні методів статистичного, спектрального та структурного аналізу сигналів що дозволяє виявляти слабкі змін параметрів зображень-контейнерів (ЗК), обумовлених вбудовуванням стегоданих. Для зниження тривалості визначення демаскуючих ознак стеганограм, при забезпеченні високої (більше 95%) точності виявлення прихованих повідомлень все більшого поширення

набуває практика побудови СД з використанням штучних нейронних мереж (наприклад мереж SR-Net, Zhu-Net, ASSAF та інших). Це дає можливість отримувати стегодетектори, здатні виявляти широкий спектр методів приховання повідомлень, шляхом залучення відповідних прикладів сформованих стеганограм на етапі налаштування штучної нейронної мережі.

Незважаючи на значний прогрес в розробці високоточних стегодетекторів в останні роки, наразі лишається невирішеною низка проблем, обумовлених відсутністю апріорних даних щодо: особливостей новітніх адаптивних стеганографічних методів (СМ), використаних для приховання стегоданих до ЗК, суттєве зниження точності роботи СД у випадку мінімізації ступеня заповнення ЗК стегоданими, нелінійною залежністю точності роботи СД від статистичних і спектральних характеристик оброблюваних ЦЗ. Також невирішеною лишається задачі в галузі стегоаналізу ЦЗ, пов'язані з неможливістю вилучення або заміни вбудованих стегоданих, що потребує використання методів деструкції які можуть розкрити факт втручання до стеганографічного каналу.

Існує наукова проблема яка визначається тим що класичні спектральні методи аналізу такі як дискретно косинусні, вейвлет перетворення не дають точні спектральні представлення на малих довжинах перетворень до яких можна віднести сегменти при обробці зображень. Вибір невеликих сегментів визначається необхідністю апроксимації сегментованого зображення стаціонарнім процесом. Модель стаціонарності дозволяє будувати інтерполяційні функції для прогнозування та фільтрації зображення для рішення задачі вичленення стеганотексту і детектування стеганоканалу.

Вирішення задач детектування може бути досягнуто на основі вирішення задачі синтезу дискретних базисних функцій з наближенням до функції яскравості пікселів по критерію максимальної правдоподібності. Таким чином вирішення науково-прикладної проблеми, що пов'язана з розробкою 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 являється актуальною науково прикладною задачею.

Зв'язок роботи з науковими програмам, планами, темами

Дослідження за темою дисертаційної роботи виконано 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).

Ступінь обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертації та їх достовірність

Обґрунтованість наукових положень дисертаційної роботи базується на відповідності з положеннями які вже були відкриті іншими авторами і представлені в наукових публікаціях по напрямку стеганографії та стеганодетектуванні. В дисертації приведено такий аналіз, зіставлені результати і показана спадкоємність, відповідність з вже відомими.

Обґрунтованість наукових результатів підтверджується використанням для вирішення наукових задач методів спектрального аналізу (двовимірні дискретні косинусне та вейвлет перетворення), компонентного аналізу (дослідження змін статистичних, спектральних та структурних параметрів складових ЦЗ при проведенні їх попередньої обробки), статистичного

моделювання (аналіз кореляційних характеристик матриць яскравості суміжних пікселів ЦЗ, оцінка відмінностей між розподілами значень яскравості пікселів ЗК та стеганограм), теорії оптимізації (вирішення оптимізаційних задач щодо формування систем функцій для проведення декомпозиції ЦЗ), теорії розпізнавання образів (налаштування стегодетекторів та оцінка їх ефективності).

Достовірність результатів досліджень підтверджується комп'ютерним моделюванням, численними результатами тестування відомих та запропонованих стегодетекторів на стандартних пакетах тестових зображень ALASKA, VISION та MIRFlickr-1M загальною кількістю близько 1 мільйона зображень.

Отримані теоретичні та практичні результати дослідження мають апробацію на провідних фахових наукових конференціях та опубліковані у рецензованих періодичних виданнях.

Структура та зміст дисертації

Структура дисертації узгоджується з її назвою, метою і завданнями дослідження. Дисертаційна робота складається з анотації двома мовами, вступу, чотирьох розділів, висновків, списку використаних джерел зі 255 найменувань (81 робота вітчизняних та 174 роботи закордонних вчених) та чотирьох додатків. В роботі наведено 76 рисунків та 14 таблиць. Загальний обсяг роботи становить 434 сторінки з яких 266 сторінок основного тексту, 28 сторінок переліку використаної літератури та 95 сторінок додатків, що відповідає чинним вимогам до докторських дисертацій.

У ***вступі*** обґрунтовано актуальність теми роботи, сформульовано мету і завдання наукового дослідження, наведено зв'язок роботи з науковими програмами, планами, темами, вказано об'єкт та предмет дослідження, перелічено методи досліджень. Викладено наукову новизну і практичне значення отриманих результатів, зазначено особистий внесок здобувача, відомості про апробацію результатів роботи, публікації за темою досліджень, структуру та обсяг дисертації.

У ***першому розділі*** проведено критичний аналіз сучасних методів стеганографії та стегоаналізу цифрових зображень. За результатами даного аналізу виявлено суттєві обмеження застосування сучасних високоточних СД для виявлення стеганограм у випадку відсутності апріорних даних щодо використаного стеганографічного методу. Показано, що забезпечення високої (більше 95%) точності виявлення стеганограм потребує використання потужних ансамблів методів попередньої обробки досліджуваних зображень з метою виявлення слабких змін статистичних параметрів ЗК, обумовлених приховання повідомлень, що унеможливлює швидку адаптацію отримуваних стегодетекторів для виявлення нових типів стеганографічних методів.

Другий розділ дисертації присвячено методу оцінки факторів впливу на точність роботи сучасних СД при виявленні стеганограм, сформованих згідно новітніх типів стеганографічних методів. За результатами дослідження виявлені суттєві обмеження використання методів попередньої обробки ЦЗ, заснованих на підвищенні відстані між векторами, що відповідають статистичним параметрам вихідних та оброблених ЦЗ. Проведено теоретичну оцінку досяжної межі точності роботи СД у випадку використання «ідеалізованих» методів попередньої обробки досліджуваних зображень. Запропоновано метод побудови високоточних СД в задачах стегоаналізу ЦЗ, що засновано на використанні математичного апарату декомпозиції багатовимірних сигналів з використанням надлишкових систем функцій, та розроблено програмний комплекс для практичного використання надлишкових систем функцій для синтезу стегодетекторів.

В ***третьому розділі*** дисертаційного дослідження наведено результати порівняльного аналізу точності роботи СД, побудованих згідно сучасних та запропонованого методу, для виявлення стеганограм в умовах обмеженості апріорних даних щодо використаного СМ та значної варіативності статистичних параметрів ЗК. Показано, що застосування розроблених методів стеганодетектування дозволяє суттєво (на 40%) підвищити точність роботи СД навіть у найбільш складному випадку виявлення стеганограм в умовах

відсутності апріорних даних щодо використаного СМ. При цьому використання запропонованого методу дозволяє забезпечити малі значення помилки виявлення стеганограм навіть при обробці зображень, що характеризуються високим рівнем власних шумів, для яких точність роботи сучасних СД суттєво знижується.

Перспективи використання запропонованих методів для вирішення найбільш складних задач в галузі стегоаналізу ЦЗ досліджено в ***четвертому розділі***. Показано, що застосування запропонованих методів дозволяє забезпечити високу якість деструкції стеганограм при малих змінах статистичних параметрів ЗК, навіть у найбільш складному випадку слабкого заповнення ЗК стегоданими (менше 10%) та використання новітніх методів MiPOD та Synch. При цьому запропоновані методи обробки ЦЗ дозволяють суттєво (до чотирьох разів) підвищити точність локалізації пікселів, використаних для приховання стегобітів, у порівнянні з сучасними методами стегоаналізу ЦЗ. Отримані результати становлять особливий інтерес для вдосконалення новітніх комплексів протидії витоку інформації, а саме розширення можливостей щодо вилучення та внесення спотворень (підміни) частин вбудованих стегоданих.

Висновки за розділами, зроблені за результатами досліджень, охоплюють весь обсяг отриманих результатів і є достовірними.

У ***додатках*** наведені відомості щодо опублікованих праць за темою дисертації, копії документів, які підтверджують впровадження результатів дисертаційної роботи, результати дослідження точності виявлення стеганограм, сформованих згідно адаптивних стеганографічних методів, при використанні сучасних та запропонованих методів обробки ЦЗ.

В цілому за змістом дисертація є завершеною роботою, яка забезпечує суттєвий внесок в теорію та практику побудови високоточних стегодетекторів для цифрових зображень. Тема та зміст дисертації відповідають паспорту спеціальності 05.13.21 – системи захисту інформації. Оформлення дисертаційної роботи в цілому відповідає чинним вимогам.

Наукова новизна результатів дисертаційного дослідження полягає в наступному:

1. *Вперше* розроблено модель інтегральної оцінки точності роботи стегодетекторів, яка враховує функціональний зв'язок складових попередньої обробки досліджуваного зображення, визначення демаскуючих ознак стеганограм та класифікацію досліджуваного зображення, що дозволило сформувати цільову функцію дослідження та розробки детекторів для малих рівнів заповнення стегоконтейнеру.

2. *Вперше* розроблено метод 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.

3. *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.

4. *Вперше* запропоновано метод визначення положення пікселів ЗК, використаних для приховання окремих стегобітів повідомлення, який заснований на представленні задачі локалізації пікселів як задачі сегментації дос-

ліджуваного 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.

5. *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.

6. *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 $\bar{D}_{\chi^2}$ 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.

7. *Удосконалено* метод 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 МПЮ, зокрема потужних ансамблів ФВЧ.

Практичне значення роботи полягає у наступному:

1. 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 високих характеристик детектування навіть в умовах «сліпого» стегоаналізу ЦЗ. Дана особливість дозволяє використовувати запропонований комплекс в якості універсального рішення для виявлення та протидії роботі стеганографічних каналів передачі інформації в інформаційно-комунікаційних системах.

2. Отримано чисельні порівняльні оцінки стеганодетекторів існуючих та розроблений в дисертаційній роботі. Показано, що розроблені стеганоконтейнери мають кращі показники, забезпечують зменшення в три рази часу обробки цифрових зображень в порівнянні з методами штучного інтелекту та локалізації до 88% пікселів, використаних для приховання стегобітів.

3. 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.

Повнота викладення результатів роботи у наукових працях підтверджується апробацією результатів дисертаційного дослідження в публікаціях у фахових рецензованих виданнях, оприлюдненням на міжнародних та всеукраїнських науково-практичних конференціях. Результати дисертації опубліковано у 55 наукових роботах, у тому числі: 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; 3 міжнародні патенти на винахід; 30 тез та доповідей на наукових конференціях; 1 підручник, що додатково відображає результати дисертації.

Мова та стиль дисертації

Дисертація написана державною мовою. Текст дисертації викладено аргументовано та логічно. Виклад матеріалу, наукова термінологія є загальновизнаною, розділи взаємопов'язані та цілком розкривають поставлену мету, стиль викладення результатів досліджень, нових наукових положень та висновків забезпечує доступність їх сприйняття. Результати проілюстровані рисунками та графіками.

Розглянувши звіт подібності за результатами перевірки дисертаційної роботи на текстові співпадіння, можна зробити висновок, що дисертаційна робота Прогонова Д.О. є результатом самостійних досліджень і не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело.

Дискусійні положення та зауваження щодо дисертаційної роботи

1. В дисертації використовується цільова функція мінімізації помилки виявлення стеганограм P_E. Функціонально значення P_E визначається формулою по ймовірностям помилок першого та другого роду. Обґрунтування такої формули було дано в роботах Д. Фрідріх. Результати порівняння детекторних схем по параметру P_E представлені в дисертації на декількох графіках і в деяких випадках мають значення більше 0.5. В таких випадках це свідчить про некоректні рішення детекторів, або про неточність цих оцінок.

2. Детекторні схеми визнають свої рішення по порогу. В роботі нема пояснення яким чином визначається поріг і його вплив на ймовірність помилки детектування.

3. По представленому матеріалу в дисертації є відчуття, що дисертація перевантажена оцінками та моделями по іншим стеганодетекторам Це відноситься попередньо до першого розділу і деякі результати важко оцінити, наприклад ізогенії на графіках рис 1.14-1.17.

4. По деяким результатам порушено послідовний порядок викладання наукових та практичних результатів. Спочатку було приведено оцінки ймовірності помилок для методу, а потім викладено сам метод.

5. В роботі заявлено про визначення теоретичної границі досяжної точності виявлення стеганограм, є формула, але будь яка границя повинна мати доказ, асимптоти та збіжність к відомим результатам.

6. Є ряд зауважень загального характеру: орфографічні та стилістичні неточності за текстом дисертації.

Висловлені зауваження не є визначальними і не зменшують загальну наукову новизну та практичну значимість результатів та не впливають на загальну позитивну оцінку дисертаційної роботи Прогонова Д.О.

Відповідність реферату змісту дисертаційної роботи

У тексті реферату відображено основні положення, зміст, результати та висновки здійсненого дослідження. Зміст реферату та основні положення дисертаційної роботи є ідентичними.

Загальний висновок щодо

відповідності дисертації встановленим вимогам

Вважаю, що дисертаційна робота Прогонова Дмитра Олександровича на тему «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень» є завершеною науковою працею, що виконана на високому науковому і методичному рівнях, в якій представлені нові наукові результати, спрямовані на вирішення важливої науково-прикладної проблеми розробки високоточних методів виявлення стеганограм, здатних надійно працювати в умовах відсутності апріорних даних щодо особливостей використаних стеганографічних методів, малого ступеня заповнення зображення-контейнеру стегоданими (менше 10%) та при значній варіативності параметрів досліджуваних цифрових зображень.

Реферат повністю відображає основні положення дисертації. За актуальністю, практичною цінністю та науковою новизною, змістом та оформленням дисертаційна робота повністю відповідає вимогам п. 7, 8, 9 «Порядку присудження та позбавлення наукового ступеня доктора наук» затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 р. № 1197, а її автор Прогонов Дмитро Олександрович заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент

Завідувач кафедри безпеки інформаційних технологій
Харківського національного університету
радіоелектроніки,
доктор технічних наук, професор Геннадій ХАЛІМОВ

«11» 10 2024

Підпис Г.З. Халімова засвідчую

Учений секретар ХНУРЕ, к.т.н. Ірина ЖАРІКОВА