ВІДГУК

офіційного опонента д.т.н., проф. **Кобозєвої Алли Анатоліївни**
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

В останні роки суттєво зросла роль методів несилового впливу на критичну інформаційну інфраструктуру противника (конкурента) для досягнення переваги в економічній, політичній та військових сферах. Метою даного впливу може бути несанкціонований доступ і передача інформації з обмеженим доступом (ІзОД), порушення роботи виробничих комплексів, елементів комунальної та енергетичної інфраструктури, систем керування військами, поширення дезінформації тощо.

Вагомою складовою успішного проведення атак зловмисниками на інформаційну інфраструктуру державних установ і приватних підприємств є забезпечення надійного зв'язку для обміну повідомленнями та несанкціонованої передачі ІзОД. Це потребує застосування систем прихованого (стеганографічного) зв'язку, здатних долати сучасні програмно-апаратні комплекси для моніторингу інформаційно-комунікаційних систем (ІКС). В якості файлів-контейнерів для приховання повідомлень широко використовуються мультимедійні дані, зокрема цифрові зображення (ЦЗ), які циркулюють в ІКС. Результатом використання новітніх методів стеганографії ЦЗ є, як правило, досить незначні зміни (статистичних, спектральних) параметрів зображень-контейнерів при вбудовуванні стегоданих, наслідком чого є зниження ефективності виявлення сформованих стеганограм існуючими системами моніторингу ІКС.

Для забезпечення надійного виявлення стеганограм запропоновано широкий спектр методів стегоаналізу ЦЗ, заснованих на використанні статистичних моделей зображень-контейнерів (ЗК), спеціальних методів спектрального аналізу ЦЗ, штучних нейронних мереж тощо. Проте практичне застосування даних стегодетекторів (СД) є наразі обмеженим. Це обумовлено тим, що СД часто налаштований в своїй роботі на використання апріорних даних щодо стеганографічного методу, врахування особливостей статистичних та спектральних параметрів оброблюваних зображень, точність виявлення стеганограм СД значно знижується при малому (менше 10%) ступені заповнення ЗК стегоданими. Також висока, як правило, обчислювальна складність налаштування СД утруднює його адаптацію до виявлення стеганограм, сформованих новими стеганографічними методами.

На сьогодні лишаються невирішеними остаточно задачі, пов'язані з вилученням або підміною прихованих повідомлень, розв'язок яких хоча і не входить в безпосередні функції СД, але дасть змогу зменшити ефективність процесу комунікації супротивника, і може бути досягнутий шляхом застосування методів деструкції в якості превентивної міри навіть в тих випадках, коли «висновки» СД викликають недовіру.

Вищенаведене обумовлює актуальність науково-прикладної проблеми підвищення ефективності виявлення стеганограм шляхом побудови високоточних експертних методів, здатних надійно працювати в умовах відсутності апріорних даних щодо особливостей використаних стеганографічних методів, малого ступеня заповнення ЗК стегоданими (менше 10%) та значній варіативності параметрів досліджуваних ЦЗ.

Зв'язок роботи з науковими програмам, планами, темами

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 отриманих Прогоновим Д.О. результатів забезпечується значним обсягом проведених експериментальних досліджень точності роботи сучасних та запропонованих стегодетекторів в різних умовах їх практичного застосування. Про достовірність результатів дисертаційного дослідження свідчить узгодженість отриманих результатів з розрахунковими та експериментальними даними інших дослідників. Отримані наукові положення та експериментальні результати опубліковані в рецензованих фахових виданнях та пройшли апробацію на авторитетних наукових конференціях і семінарах.

Достовірність практичних рекомендацій щодо розробки високоточних СД, розроблених методів обробки сигналів підтверджена міжнародними патентами та актами впровадження у промисловості (зокрема в центрі досліджень та розробок «Самсунг РнД Інститут Україна»), та навчальному процесі провідних навчальних закладів освіти України.

Структура та зміст дисертації

Зміст дисертації узгоджується з її темою, відповідає науковій спеціальності. У дисертації стисло, логічно та аргументовано представлено зміст і результати роботи з посиланнями на публікації інших авторів.

Дисертаційна робота та реферат оформлені згідно чинних вимог ВАК України. Зміст та суть реферату відповідає змісту дисертації і дає повне уявлення про наукову цінність та практичну значущість роботи.

Загальний обсяг роботи становить 434 сторінки з яких 266 сторінок основного тексту, 28 сторінок переліку використаних джерел та 95 сторінок до-

датків. Дисертаційна робота складається з анотації двома мовами, вступу, чотирьох розділів, висновків, списку використаних джерел з 255 найменувань (81 робота вітчизняних та 174 роботи закордонних вчених) та чотирьох додатків, що відповідає чинним вимогам до докторських дисертацій.

У ***вступі*** обґрунтовано актуальність роботи, сформульовано мету та задачі дисертаційного дослідження, висвітлено наукову новизну і практичне значення отриманих результатів. Також охарактеризовано особистий внесок здобувача у наукових публікаціях, де викладено основний зміст роботи.

У ***першому розділі*** проведено структурований та критичний аналіз сучасних наукових публікацій щодо досліджуваної проблеми. Проведено аналіз світового досвіду щодо розробки високоточних стеганодетекторів для ЦЗ та їх практичного використання в системах моніторингу ІКС. За результатами аналізу виявлено вагомі обмеження практичного застосування сучасних СД, зокрема у випадку відсутності апріорних даних щодо використаного стеганографічного методу. Показано доцільність застосування обраних моделей, методів та засобів до синтезу та параметричної оптимізації високоточних стегодетекторів.

У ***другому розділі*** дисертаційного дослідження досліджено фактори впливу на точність роботи сучасних СД при виявленні стеганограм, сформованих згідно новітніх типів стеганографічних методів. Отримано кількісні характеристики точності роботи СД в залежності від умов їх функціонування, зокрема використання апріорних даних щодо стеганографічного методу (СМ), статистичних параметрів оброблюваних ЦЗ, ступеня заповнення зображення-контейнеру стегоданими. Проведено теоретичну оцінку досяжної межі точності роботи СД при варіації структури та параметрів стегодетекторів. Представлено концепцію побудови високоточних СД та методи математичної обробки ЦЗ для її практичного використання.

В ***третьому розділі*** дисертації наведено результати комплексного аналізу точності роботи СД, синтезованих згідно сучасних та запропонованого методу. Досліджено ефективність застосування даних СД в найбільш

складних випадках проведення стегоаналізу, а саме в умовах обмеженості апріорних даних щодо використаного СМ та варіативності статистичних параметрів ЗК. Показано, що застосування запропонованого підходу дозволяє підвищити точність роботи СД на 40% в порівнянні з сучасними аналогами, навіть в умовах відсутності апріорних даних щодо використаного СМ та обробці зображень, які характеризуються високим рівнем власних шумів.

В ***четвертому розділі*** роботи розглянуто перспективи використання запропонованих моделей, методів та засобів для вирішення найбільш складних задач в галузі стегоаналізу ЦЗ. Проведено оцінку змін статистичних параметрів ЗК при використанні сучасних методів деструкції та запропоновано методу відновлення вихідного виду зображення-контейнеру. Показано, що запропонований метод дозволяє забезпечити надійну деструкцію вбудованих повідомлень при малих змінах статистичних параметрів ЗК. Отримані результати зберігаються навіть у найбільш складному випадку слабкого заповнення ЗК стегоданими (менше 10%) та використання новітніх методів MiPOD та Synch. Показано перспективи використання запропонованих моделей, методів та засобів для вирішення задачі локалізації пікселів, використаних для приховання стегобітів у випадку стеганоперетворення в просторовій області ЗК. Отримані результати становлять особливий практичний інтерес для розширення можливостей комплексів протидії витоку ІзОД щодо вилучення та підміни частин прихованих повідомлень.

У ***висновку*** сформульовані основні результати дисертаційного дослідження, які дозволили оцінити вклад здобувача в подальший розвиток методів синтезу та параметричної оптимізації високоточних стегодетекторів.

У ***додатках*** наведені відомості щодо опублікованих праць за темою дисертаційної роботи, копії документів, які підтверджують впровадження результатів дослідження.

Наукова новизна отриманих в роботі результатів, сформульованих положень та висновків

Аналіз представленого до захисту наукового дослідження та публікацій дозволяють дійти висновку про наукову обґрунтованість і достовірність викладених здобувачем результатів. Основні результати, викладені в дисертаційній роботі, відповідають критерію новизни в даній галузі. Серед найважливіших результатів слід зазначити визначення оптимальних методів обробки ЦЗ за критерієм мінімізації помилки виявлення стеганограм, що узгоджуються з теоретичними напрацюваннями в галузі стегоаналізу, а також розробку ефективних методів для їх практичного застосування.

1. *Вперше* розроблено оптимальні методи попередньої обробки 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.

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 в якості базису перетворення досліджуваного зображення.

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.

4. *Удосконалено* метод синтезу структури та оптимізації параметрів високоточних стегодетекторів, що 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.

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.

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.

Практична значимість роботи

Практичну значимість дисертаційного дослідження підтверджують успішні результати впровадження запропонованих методів обробки сигналів в центрі досліджень та розробок «Самсунг РнД Інститут Україна», Управлінні оперативного зв'язку та електронних комунікацій ДСНС України та конструкторському бюро «Шторм» КПІ ім. Ігоря Сікорського. Особливістю представленої роботи є наявність суттєвого масиву експериментальних досліджень. Всі представлені результати досліджень спрямовані на вирішення конкретних практичних задач. Обсяг та рівень опрацювання матеріалу, представленого у дисертації, свідчить про потужну експериментальну роботу, проведену Прогоновим Д.О.

Повнота викладення результатів роботи у наукових працях

Основні положення і висновки дисертаційного дослідження повністю викладені в 55 опублікованих наукових працях, серед яких: 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.

Мова та стиль дисертації

Дисертація написана державною мовою. Текст дисертації викладено аргументовано. Представлений в роботі матеріал має логічну послідовність, наукова термінологія є загальновизнаною. Розділи дисертації взаємопов'язані та цілком розкривають поставлену мету. Стиль викладення результатів дослідження, наукових положень та висновків легко сприймається. Результати проілюстровані високоякісними рисунками та графіками. Використані ідеї, результати і тексти інших авторів мають належні посилання на відповідне джерело, що підтверджується звітом подібності за результатами перевірки дисертаційної роботи на текстові співпадіння.

Дискусійні положення та зауваження щодо дисертаційної роботи:

1. Розробка ефективних стеганодетекторів в межах цифрової стеганографії, зокрема для аналізу цифрових зображень, є сучасною проблемою, яка розглядається вже не одне десятиріччя фахівцями-стеганографами, результатом чого є розробка багатьох високоефективних стеганоаналітичних методів (зокрема українськими вченими https://www.semanticscholar.org/paper/General-Principles-of-Integrity-Checking-of-Digital-Kobozeva-Bobok/5564b647911e2dbf37f42f6f2a0c4137efec66ce; https://nure.ua/wp-content/uploads/2018/Scientific_editions/rvmnts_2018_194_10.pdf; http://dspace.op.edu.ua/jspui/bitstream/123456789/2836/1/aref_Akhmametieva_A.pdf тощо), в тому числі «сліпих», а також працездатних в умовах незначної пропускної спроможності прихованого (стеганографічного) каналу. Взагалі основна задача стеганоаналізу (виявлення в інформаційному контенті наявності прихованої інформації) може розглядатися як частковий випадок задачі експертизи його цілісності, для виявлення порушення якої існують новітні ефективні методи, що працюють без наявності інформації про

безпосередню збурну дію (вид, силу тощо) і можуть застосовуватися в якості стеганоаналітичних (https://uacademic.info/ua/document/0520U100387#!). Враховуючи це, формулювання мети дисертаційного дослідження як «розробки методів синтезу стегодетекторів, що забезпечують високу вірогідність виявлення стеганограм в умовах .....» потребує уточнення.

2. Огляд методів стеганографії та стегоаналізу цифрових зображень (розділ 1) не в повній мірі враховую здобутки вітчизняних фахівців в цій області, зокрема Ахмаметьєвої Г.В., Бобок І.І., Костирки О.В., Мельник М.О. та ін.

3. В роботі серед умов використання СД фігурує забезпечення його ефективної роботи при «малому ступені заповнення ЗК стегоданими (менше 10%)», але не конкретизується, що тут мається на увазі під «ступенем заповнення»: пропускна спроможність стеганографічного каналу; відносна кількість пікселів ЗК, які отримали збурення в результаті вбудови додаткової інформації? Ці поняття можуть відрізнятися кількісно дуже значно. Наприклад, якщо мається блоковий стеганометод (блоки 8×8 пікселів), який проводе вбудову інформації (саме 1 біт) в області сингулярного розкладання блоку (пропускна спроможність стеганоканалу тут 1/64 біт/піксель за умови задіювання всіх блоків ЗК), це може привести до збурення (майже) всіх пікселів ЗК, результатом чого може бути значна вірогідність виявлення такого каналу зв'язку СД навіть при наявній незначній пропускній спроможності. І навпаки, принципово можлива ситуація, коли зображення-контейнер є обраним і вже містить в собі додаткову інформацію, вбудовану у відповідності з секретним ключем навіть зі значною пропускною спроможністю стеганоканалу. В останньому випадку виявлення такої стеганограми програмно-технічними засобами є неможливим.

4. З обзору літературних джерел, проведеного в розділі 1 дисертаційного дослідження, складається враження, що вбудова приховуваної інформації зазвичай проводиться в високочастотну складову зображення-контенера

(стор. 73, 82, Висновки до розділу 1), що не відповідає дійсності. Така область стеганоперетворення буде забезпечувати одну з необхідних вимог для стеганосистеми: надійність сприйняття формованого стеганоповідомлення. Але на практиці стеганосистема повинна мати низку властивостей, серед яких, зокрема, забезпечення стійкості до атак проти вбудованого повідомлення, для чого вбудова інформації не може відбуватися у високочастотну складову, але в літературного огляді увага цьому питанню не приділяється.

5. При описі методики проведення досліджень (п.1.4.1) зазначено, що дослідження точності роботи сучасних СД проводилося з використанням адаптивних стеганометодів, що здійснюють стеганоперетворення лише в просторовій області ЗК. Просторова область ЗК також «виділяється» і в п.1.4.2, присвяченому порівняльному аналізу точності виявлення стеганограм при варіації типу методів попередньої обробки цифрових зображень, де зазначається, що «особливістю сучасних стеганографічних методів є мінімізація змін статистичних параметрів ЗК в процесі вбудовування стегоданих, яка досягається за рахунок адаптивного вибору пікселів ЗК для приховання бітів стегоданих». Просторовій області вбудовування додаткової інформації присвячений також і аналіз перспектив використання запропонованого програмного комплексу для проведення стегоаналізу цифрових зображень (розділ 4). Але, як показує практика, вибір просторової області для сучасних стеганоперетворень не є пріоритетним, більше того, саме область перетворення, зокрема частотна, є такою, де забезпечення певних вимог до стеганосистеми, зокрема згаданих у попередньому зауваженні, досягається більш точно і легко. При цьому в роботі йдеться про розробку «сліпого» СД, для якого його ефективність не повинна залежити від конкретики використаного стеганометоду, тобто і від області стеганоперетворення. Таким чином, мало б сенс у якості стеганометодів, що використовувались при будь-яких дослідження в роботі та при аналізі перспектив, розглянути такі, що використовують різні області

ЦЗ для стеганоперетворення, інакше складається враження про обмеженість області застосування відповідного СД.

6. При оцінці точності роботи СД для зниження впливу варіації розмірів використовуваних ЦЗ в дисертаційному дослідженні використовувалися ЦЗ однакового розміру (512×512 пікселів), отриманих шляхом масштабування (стор.112). Масштабування ЦЗ найчастіше передбачає застосування процесу інтерполяції. Це вносить спотворення в параметри оригінальних ЗК, кількісний (і якісний) вираз яких буде залежити від конкретики використаного фільтру. При цьому первісні ЦЗ будуть відрізнятися по своїх параметрах (статистичних, спектральних тощо) від тих, які після обробки відіграють роль ЗК. Чи не впливає це на результати проведених в роботі експериментів, зокрема, коли йдеться про аналіз та співставлення векторів, що відповідають статистичним параметрам ЗК і стеганограм?

7. В роботі неявно припускається, зокрема при аналізі факторів впливу на точність виявлення стеганограм при використанні сучасних підходів до побудови стегодетекторів (розділ 2), що при вбудові в ЗК додаткової інформації це обов'язково приведе до збурення матриці контейнера, тим самим ніяк не враховується можливість використання обраного контейнера, який у відповідності з секретним ключем вже несе в собі додаткову інформацію, при цьому чим менше пропускна спроможність стеганоканалу (чим менша кількість пікселів, які б потрібно було залучити до вбудови додаткової інформації (якщо розглядати просторову область ЗК як область стеганоперетворення)), тим більше ймовірність того, що потрібний ЗК буде знайдено за практичний час. Саме цей варіант є критичним для стеганоаналізу, але він в роботі навіть не згадується.

8. В п.2.2.2 роботи проводиться оцінка досяжної вірогідності виявлення стеганограм в залежності від наявних апріорних даних щодо використаного стеганографічного методу, в ході якої стеганоаналітик оцінює положення лише кластеру векторів, які відповідають статистичним параметрам ЗК, при відсутності у нього апріорних даних про використаний адаптивний

стеганометод, що найчастіше має місце на практиці. Але на практиці стеганоаналітик може не мати інформації і про ЗК.

9. Одним з етапів запропонованого в роботі СД є етап попередньої обробки досліджуваного ЦЗ, що підвищує ефективність вирішення основної задачі стеганоаналізу – виявлення стеганограм. Але, якщо стеганограма була отримана стеганометодом, що є нестійким до атак проти вбудованого повідомлення (а переважна більшість просторових стеганометодів є такими), її попередня обробка призведе до спотворення прихованої цифрової інформації разом зі статистиками стеганограми, тобто може просто «витерти слід» від вбудованої інформації. Чи враховується така можливість (нестійкість використаного стеганометода до атак проти вбудованого повідомлення) при роботі запропонованого стеганодетектора?

10. Обчислювальна складність роботи стеганодетектора є одною з його основних характеристик. В роботі запропоновані стеганодетектори, «здатні надійно працювати в умовах «сліпого» стегоаналізу цифрового зображення при збереженні відносно низької обчислювальної складності процедури налаштування стегодетектору», але відсутня безпосередня оцінка цієї обчислювальної складності, що утруднює сприйняття значущості отриманого результату.

Відповідність реферату змісту дисертаційної роботи

Реферат за структурою та оформленням відповідає встановленим чинним вимогам. В рефераті відображено головні результати дисертаційного дослідження та наукові здобутки автора. За змістом реферат є ідентичним до тексту дисертаційної роботи.

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 підвищення ефективності стеганоаналізу ЦЗ шляхом розробки високоточних методів виявлення стеганограм.

За актуальністю, практичною цінністю та науковою новизною, змістом та оформленням дисертаційна робота повністю відповідає вимогам пп. 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,

професор кафедри технічної
кібернетики й інформаційних
технологій Одеського національного
морського університету
д.т.н., проф. Алла КОБОЗЄВА
(до 12 серпня 2024 року - професор кафедри комп'ютерних систем і технологій Одеського національного університету імені І.І.Мечникова)

Підпис офіційного опонента
Кобозєвої А.А. засвідчую:

Міністерство освіти і науки України
Національний морський університет
ВІДДІЛ КАДРІВ
Фахівець відділу кадрів
ОНМУ