Рішення щодо присудження наукового ступеня доктора наук

Спеціалізована вчена рада з присудження наукового ступеня доктора наук Д 26.002.29 Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Міністерства освіти і науки України (м. Київ) прийняла рішення про присудження наукового ступеня доктора технічних наук Прогонову Дмитру Олександровичу на підставі прилюдного захисту докторської дисертації «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень» у вигляді рукопису за спеціальністю 05.13.21 – системи захисту інформації 31 жовтня 2024 року, протокол № 3.

Прогонов Дмитро Олександрович, 1991 року народження, громадянин України, освіта вища: закінчив у 2013 році Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» за спеціальністю «Системи технічного захисту інформації, автоматизація її обробки».

Наукові ступені і вчені звання: кандидат технічних наук з 2016 року, доцент кафедри фізико-технічних засобів захисту інформації з 2019 року.

В 2022 р. закінчив докторантуру Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» Міністерства освіти і науки України.

Працює доцентом кафедри інформаційної безпеки в Національному технічному університеті України «Київський політехнічний інститут імені Ігоря Сікорського» Міністерства освіти і науки України (м. Київ) з 2017 р. до теперішнього часу.

Докторська дисертація виконана на кафедрі інформаційної безпеки Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Науковий консультант:

Мачуський Євген Андрійович, доктор технічних наук, професор, Навчально-науковий Фізико-технічний інститут Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського», професор кафедри інформаційної безпеки.

Рекомендовано до захисту 27 червня 2024 року.

Здобувач має 55 наукових публікацій за темою дисертації, з них 21 стаття в наукових фахових виданнях:

– 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, 30 матеріалів та тез конференцій, один підручник, що додатково відображає результати дисертації.

Офіційні опоненти:

Кобозєва Алла Анатоліївна, доктор технічних наук за спеціальністю 05.13.21 – системи захисту інформації, професор за кафедрою інформатики та математичних методів захисту інформаційних систем, Одеський національний морський університет, професор кафедри технічної кібернетики й інформаційних технологій (до 12 серпня 2024 року – професор кафедри комп'ютерних систем і технологій Одеського національного університету імені І.І.Мечникова), дала позитивний відгук із зауваженнями:

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 вбудовування додаткової інформації? Ці поняття можуть відрізнятися кількісно дуже

значно. Наприклад, якщо мається блоковий стеганометод (блоки 8×8 пікселів), який проводить вбудовування 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 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 вбудовування приховуваної інформації зазвичай проводиться в високочастотну складову зображення-контейнера (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 вбудовування 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 процесу 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 залежати 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 вбудовуванні 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 вбудовування 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.

Халімов Геннадій Зайдулович, доктор технічних наук за спеціальністю 05.13.05 – комп'ютерні системи та компоненти, професор за кафедрою безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, завідувач кафедри безпеки інформаційних технологій, дав позитивний відгук із зауваженнями:

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 Фрідріха Д. 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 немає пояснення яким чином визначається поріг і його вплив на імовірність 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.

Шелест Михайло Євгенович, доктор технічних наук за спеціальністю 05.13.21 – системи захисту інформації, професор за кафедрою систем захисту інформації, Національний університет "Чернігівська політехніка", професор кафедри кібербезпеки та математичного моделювання, дав позитивний відгук із зауваженнями:

1. У першому розділі, автор аналізуючи стан наукових досліджень у сфері криптоаналізу обрав у якості об'єкту досліджень найбільш поширені стегометоди: багатоетапні та адаптивні методи приховання повідомлень у цифрові зображення, зокрема засновані на вбудовуванні повідомлень в

просторовій області та в області перетворення зображення-контейнеру. Але це не охоплює весь перелік відомих стегометодів для цифрових зображень, бо існують й інші стегометоди (наприклад, приховування в альфа-каналі, приховування через векторне кодування (VQ Steganography), розсіяного приховування (Spread Spectrum), приховування на основі фракталів та інші), дослідження яких слабо представлено у науковій літературі. За логікою, зловмисник для досягнення своєї мети має обрати один з цих слабо досліджених методів. Тому, при аналізі сучасного стану криптоаналізу зображень, автору доцільне було більш ґрунтовно аргументувати границі свого дослідження стеганометодів, проаналізувати переваги та недоліки інших методів, оцінити можливість застосування розробленої технології синтезу стеганодетекторів або її модифікації до таких методів.

2. Слід було б навести більш детальне обґрунтування використання в якості класифікатору зображень-контейнерів та стеганограм саме ансамблю лінійних дискримінантів Фішера замість поширених методів класифікації, зокрема методу опорних векторів (Support Vector Machine, SVM), багато-шарового персептрона тощо.

3. В дисертації використовується теоретична оцінка досяжної точності виявлення стеганограм при використанні квадратичного закону (англ. Square Root Law), який використовується для дослідження ϵ-стійких методів приховання повідомлень. Зокрема, розглянуто випадок оцінки значення помилки виявлення стеганограм P_E^{lim}, запропонованої в роботах Фрідріх Д., проте не наведено даних щодо результатів дослідження при використанні інших методів оцінок P_E^{lim}.

4. Бажано б було навести оцінки швидкодії запропонованих методів при роботі у реальних системах контролю та моніторингу інформаційно-комунікаційних систем або їх модулів для виявлення прихованих каналів передачі даних.

5. Також становить інтерес дослідження ефективності запропонованих методів виявлення стеганограм при використанні різних пакетів тестових зображень, зокрема пакету BOSS, а також новітніх методів приховання повідомлень у просторовій області (наприклад Synch) та пакетних методів (зокрема J2-UNIWARD, Clustered-SI).

На докторську дисертацію та реферат надійшли відгуки:

1. **Національний університет «Одеська політехніка»**. Відгук підписано професором кафедри інформаційних систем, д.т.н., проф. ***Світланою Антощук.*** Відгук позитивний, є зауваження:

1) З тексту реферату не зрозуміло чи є контур кластеру, сформованого з векторів **f** для стеганограм унікальним (вираз 17, стор. 17) та яким чином новітні типи ACM дозволяють мінімізувати зміни контуру кластеру.

2) Деякі назви рисунків (наприклад, рис. 2, рис.3) та таблиць (№1 та №2) містять пояснення. Було б доцільно навести ці пояснення у тексті відповідних посилань.

2. **Приватне акціонерне товариство «Інститут інформаційних технологій»**. Відгук підписано головою наглядової ради, Лауреатом Державної премії в галузі науки і техніки, д.т.н., проф. ***Іваном Горбенко.*** Відгук позитивний, є зауваження:

1) В роботі наведено результати дослідження точності роботи стего-детекторів, налаштованих з використанням запропонованих методів, для виявлення стеганограм, сформованих згідно новітніх методів MG та MiPOD. Проте відсутні відомості щодо ефективності застосування даних стегодетекторів у випадку застосування спеціалізованих стеганографічних методів, наприклад J-UNIWARD, Synch.

2) Бажано б було навести оцінки швидкодії запропонованих методів деструкції стеганограм та вилучення прихованих повідомлень при роботі у реальних системах протидії витоку конфіденційних даних, або їх модулів для виявлення прихованих каналів передачі даних.

3. **Інститут кібернетики імені В.М. Глушкова НАН України**. Відгук підписано академіком НАН України, д.ф.-м.н., проф. ***Валерієм Задіракою.*** Відгук позитивний, є зауваження:

1) В роботі зазначено, що розроблено низку методів для побудови високоточних стегодетекторів. Проте відомості щодо основних етапів роботи даних методів у рефераті не наведені.

2) В матеріалах реферату представлені результати порівняльного аналізу стегодетекторів, налаштованих з використанням ансамблів класифікаторів на основі лінійних дискримінантів Фішера, проте відсутні дані щодо точності роботи стегодетекторів при використанні інших типів класифікаторів, зокрема методу опорних векторів.

3) В рефераті використовується значна кількість скорочених позначень, що ускладнює сприйняття тексту реферату. Зокрема, є скорочені позначення, які використовуються лише декілька разів, а саме ШНМ – штучна нейронна мережа, МПО – метод попередньої обробки тощо.

4. **Лодзький університет технологій** (м. Лодзь, Республіка Польща). Відгук підписано доцентом інституту математики, д.т.н., проф. ***Людмилою Кіріченко.*** **Відгук** позитивний, є зауваження:

1) В рефераті зазначено, що запропонований метод побудови спеціальних систем функцій був використаний для побудови як високоточних стегодетекторів, так і обробки сигналів різної фізичної природи, а саме акустичних та біометричних сигналів. Проте відсутні відомості щодо тривалості формування спеціальних систем функцій, що становить інтерес для практичного застосування даних методів.

2) У формулюванні наукової новизна п'ятого наукового результату не вказано методів-прототипів, від яких відрізняється запропонований метод робастної оцінки відмінностей між імовірнісними розподілами значень яскравості пікселів зображень-контейнерів та стеганограм.

5. **Національний авіаційний університет**. Відгук підписано професором кафедри телекомунікаційних та радіоелектронних систем,

Заслуженим працівником транспорту України, д.т.н., проф. ***Георгієм Конаховичем.*** Відгук позитивний, є зауваження:

1) Теоретичні та практичні результати, отримані в дисертаційній роботі, дозволяють створювати високоточні стегодетектори для цифрових зображень, як одного з найбільш поширених типів мультимедійних даних. Проте в рефераті відсутні відомості щодо можливості адаптації даних результатів для побудови стегодетекторів для інших типів мультимедійних даних, зокрема аудіо та відеофайлів.

2) В роботі наведено дані щодо середнього часу обробки цифрових зображень при використанні сучасних та запропонованих стегодетекторів, проте у тексті реферату відсутні відомості щодо процедури визначення даного параметру.

6. **Вінницький національний технічний університет**. Відгук підписано завідувачем кафедри захисту інформації, д.т.н., проф. ***Володимиром Лужецьким.*** Відгук позитивний, є зауваження:

1) Автор вживає як синоніми такі поняття: «помилки виявлення стеганограм», «імовірність виявлення стеганограм», «точність виявлення стеганограм» і «вірогідність виявлення стеганограм». При цьому одиницею кількісного вимірювання є %. Для ймовірності така одиниця є некоректною. Доцільно було б вживати поняття «влучність» (precision), яку ґрунтується на розумінні та мірі релевантності та використовується в задачах розпізнавання образів, інформаційного пошуку і класифікації.

2) Мало уваги приділено дослідженню результатів роботи сучасних та запропонованих стегодетекторів у випадку надмалого (менше 5%) ступеня заповнення ЗК стегоданими, що наразі є одним з найбільш складних при проведенні стегоаналізу цифрових зображень.

3) Доцільно було б також навести відомості щодо мови програмування та середовища розробки, в якому був розроблений запропонований комплекс, а також характеристики ПК використаного для проведення тестування досліджених методів стегоаналізу.

7. **ДержНДІ технологій кібербезпеки**. Відгук підписано завідувачем відділу науково-технічної експертизи, д.т.н. ***Євгеном Морщем*** та вченим секретарем інституту д.т.н., проф. ***Олександром Юдіним.*** Відгук позитивний, є зауваження:

1) З тексту реферату незрозуміло, чи аналізувалися в роботі відомості щодо тривалості обробки ЦЗ при застосуванні запропонованих методів визначення позицій пікселів, використаних для приховання окремих стегобітів.

2) В роботі наведені результати експериментального дослідження деструкції стеганограм при використанні поширених методів обробки ЦЗ, а саме методів фільтрації та підвищення візуальної якості зображень. Доцільно було б також навести відомості щодо ступеня деструкції стеганограм при використанні новітніх методів обробки зображень із застосуванням штучних нейронних мереж.

3) В рефераті не відображено алгоритм запропонованого методу синтезу структури та оптимізації параметрів стегодетекторів, на підставі якого реалізовано програмний комплекс для проведення стегоаналізу ЦЗ, що ускладнює сприйняття цього методу та роботи в цілому.

4) В рефераті (стор. 2) зазначається, що «в низці теоретичних досліджень та практичних застосувань стеганодетектора існують проблеми, обумовлені неможливістю визначення положення (локалізації) пікселів зображення-контейнера, використаних для приховання стегобітів, для розробки методів вилучення (екстракції) вбудованих повідомлень», але зазначена задача не є специфічною задачею стеганодетектора, а тому її розгляд в світі обґрунтування актуальності теми дисертації є некоректним. Крім того, локалізація пікселів контейнера та їх конкретна послідовність при вбудовуванні секретної інформації є частиною секретного ключа, а «необізнаність» стеганодетектора порушника в цьому питанні – природнім наслідком принципів побудови стеганографічної системи.

5) Відомо, що обчислювальна складність процесу налаштування, роботи стеганодетектору є одною з його ключових характеристик, зокрема, коли йдеться про стеганоаналіз при використанні потокового контейнеру. В рефераті зазначається, що досягнута «відносно низька обчислювальна складність процедури налаштування стегодетектору» (стор. 4), але безпосередня оцінка обчислювальної складності не наведена. Не наведені також конкретні оцінки обчислювальної склданості (як функції залежності від розміру вхідних даних) вирішення задачі (25) (стор. 23), формування $\mathbf{A}_{SRR}$ при обробці цифрового зображення значного розміру (стор. 23), замість чого в авторефераті використані якісні оцінки «низька», «висока» відповідно, що зменшує розуміння значимості отриманих в роботі певних результатів (кількісні показники результатів досліджень).

8. **Самсунг РнД Інститут Україна, український центр досліджень та розробок Samsung**. Відгук підписано заступником директора з безпеки інформаційних систем, к.ф.-м.н. ***Олексієм Мохонько.*** Відгук позитивний, є зауваження:

1) В роботі зазначена висока ефективність знищення стеганограм при використанні запропонованого методу за мінімальних змін статистичних, спектральних та структурних параметрів оброблюваних ЦЗ. Проте, відсутні відомості щодо оцінок обчислювальної складності процедури обробки ЦЗ при використанні запропонованого підходу, що може мати вагомий вплив при прийнятті рішення щодо його практичного застосування у системах протидії витоку конфіденційних даних.

2) З тексту реферату є незрозумілим, чи забезпечується висока точність виявлення стеганограм при обробці ЦЗ значного розміру. Зокрема, в рефераті наведено результати тестування стегодетекторів при використанні цифрових зображень розміром 256×256 пікселів.

9. **Київський національний університет імені Тараса Шевченка**. Відгук підписано професором кафедри алгебри і комп'ютерної математики, д.ф.-м.н., проф. ***Андрієм Олійником.*** Відгук позитивний, є зауваження:

1) При дослідженнях точності роботи стегодетекторів широко використовуються такі показники, як кількість помилок першого та другого роду, площа під ROC-кривою та інші. В рефераті наведено результати дослідження точності виявлення стеганограм з використанням помилки класифікації стеганограм, тому не зрозуміло, чи використовувалися інші показники ефективності стегодетекторів.

2) Доцільно також було б навести відомості щодо тривалості обробки цифрових зображень при використанні запропонованого програмного комплексу для вирішення задач деструкції стеганограм або ж визначення позицій пікселів, використаних для приховання окремих стегобітів.

10. **Черкаський державний технологічний університет**. Відгук підписано завідувачем кафедри робототехнічних і телекомунікаційних систем та кібербезпеки, д.т.н., проф. ***Володимиром Палагіним.*** Відгук позитивний, є зауваження:

1) В рефераті наведено обмежену інформацію щодо обчислювальної складності запропонованого методу підвищення точності роботи СД, заснованого на використанні теореми Джонсона-Лінденштрауса. Даний метод може становити практичний інтерес для вдосконалення СД у складі існуючих систем моніторингу ІКС без необхідності їх заміни.

2) Автором запропоновано використовувати відстань Хеллінгера для оцінки відмінностей між імовірнісними розподілами значень яскравості пікселів ЗК та стеганограм після проведення їх попередньої обробки. Проте в рефераті відсутні відомості щодо результатів порівняльного аналізу використання інших типів показників, зокрема відстані Кульбака-Лейблера.

11. **Національний університет «Чернігівська політехніка»**. Відгук підписано завідувачем кафедри кібербезпеки та математичного моделювання, д.пед.н., к.т.н., проф. ***Юлією Ткач.*** Відгук позитивний, є зауваження:

1) В рефераті наведено значну кількість досліджених та запропонованих автором статистичних моделей ЦЗ та методів виявлення стеганограм, що перевантажені детальним описом їх роботи. Це ускладнює ознайомлення з результатами дисертаційного дослідження автора.

2) Наведені в рефераті рисунки складаються з кількох графіків малого розміру, що ускладнює їх сприйняття та аналіз. Було б доцільно навести кожен з даних графіком у вигляді окремого рисунку.

У дискусії взяли участь члени докторської ради:

- Сергій ІВАНЧЕНКО, д.т.н., проф., спеціальність 05.13.21, без зауважень;
- Ігор ТЕРЕЙКОВСЬКИЙ, д.т.н., проф., спеціальність 05.13.21, є зауваження:

- Можливим перспективним напрямком подальших досліджень в напрямку дисертації – це визначити, як стегоповідомлення, що є в стегоконтейнері, можна розпізнати за рахунок психоемоційного стану людини, яка дивиться такі зображення із вбудованим повідомлення. Трохи має змінитись, очевидно, вплив цього зображення на психоемоційний стан людини;

- Дмитро ЛАНДЕ, д.т.н., проф., спеціальність 05.13.21, без зауважень;
- Антон КУДІН, д.т.н., проф., спеціальність 05.13.21, без зауважень;
- Євген МАЧУСЬКИЙ, д.т.н., проф., науковий консультант, без зауважень;
- Олексій НОВІКОВ, д.т.н., проф., спеціальність 05.13.21, без зауважень;

та присутні на захисті фахівці

- Валерій ЗАДІРАКА, академік НАН України, д.ф.-м.н., проф., Інститут кібернетики імені В.М. Глушкова НАН України, без зауважень;
- Анатолій КАЧИНСЬКИЙ, д.т.н., проф., професор кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського:
  - Академік Задірака, проф. Іванченко і опоненти говорили щодо визначення точності, імовірності і ефективності. Ви запропонували свої. Якби ви навели результати ROC-аналізу і AUC-показник, тоді цих запитань не виникло б і вам не прийшлося би на них відповідати.

При проведенні таємного голосування виявилося, що із 14 членів докторської ради, які взяли участь у голосуванні (з них 7 докторів наук за профілем дисертації), проголосували:
«За» – 13 членів докторської ради,
«Проти» – немає,
недійсних бюлетенів – немає.

ВИСНОВОК СПЕЦІАЛІЗОВАНОЇ ВЧЕНОЇ РАДИ

Дисертаційна робота Прогонова Д.О. є завершеною науково-дослідною працею, в якій на підставі проведених теоретичних та експериментальних досліджень розв'язано актуальну науково-прикладну проблему забезпечення високої (більше 95%) точності виявлення стеганограм в умовах відсутності апріорних даних щодо особливостей використаних стеганографічних методів, малих значень ступеня заповнення зображення-контейнеру стегоданими (менше 10%) та широкому діапазоні змін статистичних, спектральних та структурних параметрів досліджуваних зображень.

Найбільш суттєві наукові результати, отримані особисто здобувачем, полягають у наступному:

– *вперше* встановлено перелік оптимальних методів попередньої обробки цифрових зображень за критерієм мінімізації помилки виявлення стеганограм при розробці стегодетекторів. Використання даних методів при синтезі стегодетекторів дало можливість наблизити точність роботи стегодетекторів до теоретичних оцінок досяжної імовірності виявлення стеганограм у всьому діапазоні змін ступеня заповнення зображення-контейнеру стегоданими, що є недосяжним при застосуванні сучасних методів попередньої обробки, зокрема заснованих на зниженні впливу адитивних завад в оброблюваних зображеннях.

– *вперше* розроблено метод для надійного виявлення слабких змін статистичних, спектральних та структурних параметрів зображення-контейнеру, обумовлених вбудовуванням стегоданих, що заснований на використанні спеціальних систем функцій в якості базису перетворення досліджуваного зображення. Даний метод забезпечує високу точність реконструкції вихідного виду зображення-контейнеру та здатен надійно працювати в умовах відсутності апріорних даних щодо використаного стеганографічного методу при збереженні відносно низької обчислювальної складності процедури налаштування стегодетектору.

– *вперше* розроблено метод визначення положення пікселів зображення-контейнеру, використаних для приховання окремих бітів повідомлення, що заснований на представленні задачі локалізації пікселів як задачі сегментації досліджуваного зображення. Практичне застосування даного методу дозволило не тільки підвищити ефективність методів деструкції стегоданих (зокрема, забезпечити мінімальний вплив на статистичні та спектральні параметри оброблюваних цифрових зображень), а й створити передумови для розробки методів вилучення стегоданих зі стеганограм.

– *удосконалено* метод синтезу структури та оптимізації параметрів високоточних стегодетекторів шляхом заміни декількох обчилювально складних етапів налаштування стегодетектору на вирішення єдиної оптимізаційної задачі максимізації відстані Хеллінгера між кластерами векторів, що відповідають статистичним параметрам зображення-контейнеру та сформованих стеганограм. Це дозволило забезпечити високу точність виявлення стеганограм незалежно від способу їх формування.

– *удосконалено* метод робастної оцінки відмінностей між імовірнісними розподілами значень яскравості пікселів зображень-контейнерів та стеганограм, особливістю котрого є застосування відстані Хеллінгера D_H, відстані Бхаттачарайя D_B, χ^2-квадрат відстані D_{χ^2} та спектру відстаней Реньї D_R^α. Це дало можливість суттєво (до двох разів) підвищити точність виявлення стеганограм, зокрема у випадку обробки пакетів цифрових зображень, статистичні, спектральні та структурні параметри котрих змінюються в широких межах.

– *удосконалено* методи для додаткового підвищення точності роботи стегодетекторів у випадку обмеженості апріорних даних щодо використаного стеганографічного методу. Це досягається шляхом проекції векторів, які відповідають статистичним параметрам зображення-контейнеру та сформованих стеганограм, до простору вищої розмірності з метою зниження впливу нелінійних зв'язків між статистичними параметрами зображень. Це дозволило збільшити кількість інформативних параметрів оброблюваних зображень при проведенні стегоаналізу без необхідності використання обчислювально складних методів попередньої обробки зображень, зокрема потужних ансамблів фільтрів високих частот.

– *набули подальшого розвитку* методи деструкції стеганограм, засновані на реконструкції вихідного виду зображення-контейнеру за наявними (зашумленими) даними з використанням методів варіаційного аналізу багатовимірних сигналів. Це дало можливість підвищити точність параметрів адитивних завад та, відповідно, забезпечити надійну деструкцію оброблюваних стеганограм.

Оцінка достовірності та новизни наукових результатів

Отримані наукові положення та висновки обґрунтовуються коректним застосуванням математичного апарату статистичного моделювання, методів спектрального аналізу сигналів, використанням поширених методів теорії оптимізації та теорії розпізнавання образів. Отримані теоретичні напрацювання та експериментальні дані не містять результатів, представлених у кандидатській дисертації здобувача.

Достовірність результатів досліджень підтверджується численними результатами комп'ютерного моделювання роботи сучасних стегодетекторів, заснованих на аналізі статистичних та спектральних параметрів зображень. Отримані здобувачем результати узгоджуються з теоретичними результатами та дослідженнями провідних фахівців в галузі стегоаналізу цифрових зображень.

Значення для теорії та практики отриманих результатів

У ході виконання дисертаційної роботи розроблено нові методи, моделі і засоби для проведення синтезу високоточних стегодетекторів в умовах обмеженості апріорних даних щодо використаного стеганографічного методу та зміні статистичних, спектральних і структурних параметрів досліджуваних зображень в широкому діапазоні значень.

Використання запропонованих методів синтезу стегодетекторів дозволило суттєво (на 23%) підвищити точність виявлення стеганограм у найбільш складних випадках проведення стегоаналізу цифрових зображень, а саме виявлення невідомих стеганографічних методів та слабкому (менше 10%) ступеню заповнення зображення-контейнеру стегоданими. Розроблено програмний комплекс для проведення стегоаналізу цифрових зображень, що дозволяє автоматизувати вирішення широкого спектру задач, що стосуються

синтезу високоточних стегодетекторів, надійної деструкції стеганограм при забезпеченні мінімальних змін статистичних параметрів оброблюваних зображень, визначення положення пікселів, використаних для вбудовування стегобітів тощо.

Результати дисертаційної роботи використано в центрі досліджень та розробок «Самсунг РнД Інститут Україна» та конструкторському бюро «Шторм» КПІ ім. Ігоря Сікорського при виконанні науково-дослідних робіт. Розроблені методи реконструкції вихідного виду цифрових зображень за наявними (зашумленими) даними дозволили отримувати робастні оцінки значень статистичних та спектральних параметрів цифрових зображень, для вирішення задач Управління оперативного зв'язку та електронних комунікацій ДСНС України. Розроблені методи визначення параметрів цифрових сигналів впроваджено в навчальний процес механіко-математичного факультету КНУ ім. Тараса Шевченка, кафедри телекомунікаційних та радіоелектронних систем Національного авіаційного університету та кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського.

Пропозиції щодо подальшого використання результатів

Основним досягненням роботи є розробка методів синтезу стегодетекторів, здатних забезпечити високу точність виявлення стеганограм в умовах обмеженості апріорних даних щодо використаного стеганографічного методу та зміні в широких межах статистичних, спектральних і структурних параметрів досліджуваних зображень.

Результати роботи можуть бути використаними для:

– теоретичного та експериментального дослідження проблематики виявлення стеганограм в умовах відсутності апріорних даних щодо використаного стеганографічного методу;

– розробки методів вилучення повідомлень, вбудованих до стеганограм, з метою їх подальшого аналізу або ж підміни;

– вибору ефективних методів деструкції стеганограм при забезпеченні мінімальних змін статистичних та спектральних параметрів зображення-контейнеру;

– створення вітчизняних систем виявлення і протидії роботі стеганографічних систем зв'язку, ефективність котрих не поступається провідним комерційним рішенням;

– підвищення точності роботи сучасних комплексів виявлення прихованих каналів обміну конфіденційними даними між користувачами інформаційно-комунікаційних систем, зокрема соціальних мереж, сервісів електронної пошти, служб зберігання мультимедійних даних тощо.

Загальна оцінка дисертації.

Дисертаційна робота Прогонова Дмитра Олександровича «Структурний синтез та параметрична оптимізація методів побудови стегодетекторів для цифрових зображень» є завершеною науково-дослідною

працею, яка 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 присудження наукового ступеня доктора технічних наук.

На підставі результатів таємного голосування та прийнятого висновку спеціалізована вчена рада присуджує Прогонову Дмитру Олександровичу науковий ступінь доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Головуючий на засіданні
спеціалізованої вченої ради
з присудження наукового
ступеня доктора наук
Д.26.002.29 Олексій НОВІКОВ

Вчений секретар
спеціалізованої вченої ради
з присудження наукового
ступеня доктора наук Андрій ШЕЛЕСТОВ

Вчений секретар
КПІ ім. Ігоря Сікорського Валерія ХОЛЯВКО

М. П. "____" _____ 2024 року