

Міністерство освіти і науки України
Одеський національний політехнічний університет

Міністерство освіти і науки України
Одеський національний політехнічний університет

Кваліфікаційна наукова
праця на правах рукопису

Ахмаметьєва Ганна Валеріївна

УДК 004.056.5

ДИСЕРТАЦІЯ

Підвищення ефективності стеганоаналізу для цифрових зображень і відео

(назва дисертації)

05.13.21 — Системи захисту інформації

(шифр і назва спеціальності)

Технічні науки

(галузь знань)

Подається на здобуття наукового ступеня кандидата технічних наук

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

(підпис, ініціали та прізвище здобувача)

Науковий керівник Кобозєва Алла Анатоліївна, доктор технічних наук, професор

Одеса — 2017

АНОТАЦІЯ

Ахмаметьєва Г.В. Підвищення ефективності стеганоаналізу для цифрових зображень та відео. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) за спеціальністю 05.13.21 «Системи захисту інформації» (125 – Кібербезпека). – Одеський національний політехнічний університет, Одеса, 2017.

В роботі вирішено важливу науково-практичну задачу, що полягає в підвищенні ефективності стеганоаналізу цифрових зображень та цифрових відео шляхом розробки ефективних стеганоаналітичних методів виявлення наявності додаткової інформації, вбудованої методом LSB у цифрові зображення та відео, у тому числі при малих значеннях пропускну здатності прихованого каналу зв'язку (ППС).

Для організації стеганоаналізу обґрунтований вибір просторової області цифрових контентів завдяки можливості уникнути накопичення обчислювальної похибки, що в значній мірі впливає на ефективність стеганоаналізу за умови малих значень ППС.

Отримав подальший розвиток загальний підхід до аналізу стану і технології функціонування інформаційних систем шляхом отримання критерію належності єдиного ненульового сингулярного числа блоку множині натуральних чисел, що дозволило встановити відповідність між просторовою областю та областю перетворень цифрових контентів. Це дозволило розробити теоретичний базис, на основі якого запропоновані стеганоаналітичні методи виявлення вкладень додаткової інформації у цифрових відео. Розроблені методи, засновані на врахуванні відмінностей у кількості блоків з однаковими значеннями яскравості в результаті первинної та повторної вбудови додаткової інформації, забезпечують високу ефективність виявлення вкладень додаткової інформації, вбудованої методом LSB за умови ППС 0.167 біт/піксель та вище у цифрові відео, у тому числі малого розміру: ефективність стеганоаналізу підвищено максимально на 7.5%.

На основі аналізу послідовних тріад колірних триплетів у матриці унікальних кольорів цифрових зображень розроблено метод виявлення вкладень додаткової інформації, вбудованої методом LSB в одну постійну колірну складову цифрових зображень (окремих кадрів цифрових відео), що дозволило з високою ефективністю виявляти стеганоповідомлення, сформовані при малій ППС: при ППС 0.05 біт/піксель помилки першого роду максимально склали 7.96% при відсутності помилок другого роду. Розроблений метод адаптовано для виявлення вкладень додаткової інформації у цифрових відео, що дозволило підвищити ефективність стеганоаналізу максимально на 14.93%.

На основі отриманих оцінок ефективності для розроблених методів, сформульовані практичні рекомендації щодо їх застосування, на основі яких розроблено комплексний метод виявлення вкладень додаткової інформації у цифрових відео, ефективний, у тому числі при малих значеннях ППС, при різній кількості заповнених колірних складових контейнерів, в якості яких можуть виступати як кольорові відео, так і відео в градаціях сірого, незалежно від формату (з/без втрат).

Ключові слова: стеганоаналітичний метод, цифрове зображення, цифрове відео, просторова область контентів, метод модифікації найменшого значущого біту, LSB

Список публікацій здобувача:

1. Ахмаметьєва, А.В.: Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров. Информатика та математичні методи в моделюванні. Т.5, № 4, 367-375 (2015)
2. Ахмаметьєва, А.В.: Стеганоанализ цифровых изображений, хранящихся в формате с потерями. Захист інформації. Випуск 23, 135-145 (2016)
3. Ахмаметьєва, Г.В.: Стеганоаналітичний алгоритм для цифрових контейнерів, збережених в форматах з втратами. Сучасна спеціальна техніка. № 3 (46), 31-38 (2016)

4. Akhmametiyeva, A.: Method of detection the fact of compression in digital images as an integral part of steganalysis. Інформатика та математичні методи в моделюванні. Т.6, №4, 357-364 (2016)
5. Кобозева, А.А., Ахмаметьева, А.В., Ефименко, А.А.: Стеганоаналитический метод для цифровых контейнеров, хранящихся в формате без потерь. Інформаційна безпека. №1(13), 31-42 (2014)
6. Маєвський, Д.А., Ахмаметьева, Г.В.: Стеганоаналітичний алгоритм, заснований на аналізі просторової області цифрових контейнерів. Інформатика та математичні методи в моделюванні. Т.6, №1, 52-60 (2016)
7. Ахмаметьева, А.В.: Выявление области применения стеганоаналитического подхода, основанного на анализе пространственной области цифровых контентов. Problemele energeticii regionale. Электронный журнал Академии наук Республики Молдова. № 2 (31), 104-111 (2016)
8. Ахмаметьева, А.В.: Стеганоаналитический метод, основанный на анализе пространственной области цифровых контентов. Международная научно-техническая конференция «Современные информационно-телекоммуникационные технологии», Т. II, 83-84, Киев, 17-20 ноября 2015
9. Ахмаметьева, Г.В.: Детектування стеганоповідомлень, вбудованих методом LSB Matching у цифрові контейнери в форматах з втратами. V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», 106-107, Львів, 2-3 червня 2016
10. Ахмаметьева, Г.В.: Виявлення області застосування стеганоаналітичного алгоритму, що аналізує просторову область цифрових зображень. V Міжнародна науково-технічна конференція «Інформаційні системи та технології» (ICT-2016), 287-288, Харків-Коблево, 12-17 вересня 2016
11. Ахмаметьева, А.В.: Стеганоанализ цифровых видео, основанный на анализе пространственной области. V Міжнародна науково-практична конференція «Інформаційні управляючі системи та технології» (ІУСТ-Одеса - 2016), 161-163, Одеса, 20-22 вересня 2016

ABSTRACT

Akhmametieva A. Improving the efficiency of steganalysis for digital images and video. – Manuscript.

Thesis for a candidate's degree (Ph.D.) by specialty 05.13.21 – Information security system (125 – Cybersecurity) – Odessa National Polytechnic University, Odessa, Ukraine, 2017.

The paper is devoted the development of complex steganalytic method, aimed to detect the fact of presence of additional information, embedded by LSB method in digital images and video with different values of hidden capacity including small values. This method led to improving the efficiency of steganalysis.

Steganalysis of digital contents is realized without presence of original container in spatial domain of content, that allows avoid additional accumulation of a computing error. It was reached high efficiency of detection stego, formed by embedding of additional information into one random color component of digital images, by analyzing of sequential triads of triplets in the matrix of unique colors: for digital images at the hidden capacity 0.05 bpp the first type errors reaches 7.96% as maximum in the absence of the second kind errors; for digital videos the detection efficiency is maximally increased by 14.96% (for hidden capacity 0.0625 bpp).

To provide steganalysis of digital video it was developed methods, based on the accounting of differences in the change of the number of blocks with the equal color brightness values of matrices of frames of a video sequence as a result of primary and repeated embedding of additional information, that provide high detection efficiency of attachment of additional information embedded by LSB method with hidden capacity 0.167 bpp and higher into digital videos, including small size of the frame: the efficiency of steganalysis increased maximally by 7.5%.

Based on the estimated efficiency for the developed methods it was formulated practical recommendations for their use, based on which a complex method of detecting the attachments of additional information in digital video was

developed, that is effective, including for small values of hidden capacity, at different number of filled color components of containers, as which can serve as a color and grayscale videos, regardless of format (with/without losses).

Key words: steganalytic method, digital image, digital video, spatial domain of contents, least significant bit method, LSB

List of publications of the author:

1. Ахмаметьева, А.В.: Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров. Информатика та математичні методи в моделюванні. Т.5, № 4, 367-375 (2015)
2. Ахмаметьева, А.В.: Стеганоанализ цифровых изображений, хранящихся в формате с потерями. Захист інформації. Випуск 23, 135-145 (2016)
3. Ахмаметьева, Г.В.: Стеганоаналітичний алгоритм для цифрових контейнерів, збережених в форматах з втратами. Сучасна спеціальна техніка. № 3 (46), 31-38 (2016)
4. Akhmetieva, A.: Method of detection the fact of compression in digital images as an integral part of steganalysis. Информатика та математичні методи в моделюванні. Т.6, №4, 357-364 (2016)
5. Кобозева, А.А., Ахмаметьева, А.В., Ефименко, А.А.: Стеганоаналитический метод для цифровых контейнеров, хранящихся в формате без потерь. Інформаційна безпека. №1(13), 31-42 (2014)
6. Маєвський, Д.А., Ахмаметьева, Г.В.: Стеганоаналітичний алгоритм, заснований на аналізі просторової області цифрових контейнерів. Информатика та математичні методи в моделюванні. Т.6, №1, 52-60 (2016)
7. Ахмаметьева, А.В.: Выявление области применения стеганоаналитического подхода, основанного на анализе пространственной области цифровых контентов. Problemele energeticii regionale. Электронный журнал Академии наук Республики Молдова. № 2 (31), 104-111 (2016)

8. Ахмаметьева, А.В.: Стеганоаналитический метод, основанный на анализе пространственной области цифровых контентов. Международная научно-техническая конференция «Современные информационно-телекоммуникационные технологии», Т. II, 83-84, Киев, 17-20 ноября 2015
9. Ахмаметьева, Г.В.: Детектування стеганоповідомлень, вбудованих методом LSB Matching у цифрові контейнери в форматах з втратами. V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», 106-107, Львів, 2-3 червня 2016
10. Ахмаметьева, Г.В.: Виявлення області застосування стеганоаналітичного алгоритму, що аналізує просторову область цифрових зображень. V Міжнародна науково-технічна конференція «Інформаційні системи та технології» (ICT-2016), 287-288, Харків-Коблево, 12-17 вересня 2016
11. Ахмаметьева, А.В.: Стеганоанализ цифровых видео, основанный на анализе пространственной области. V Міжнародна науково-практична конференція «Інформаційні управляючі системи та технології» (ІУСТ-Одеса - 2016), 161-163, Одеса, 20-22 вересня 2016

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	11
ВСТУП.....	12
РОЗДІЛ 1. АНАЛІЗ СУЧАСНОГО СТАНУ РІШЕННЯ ЗАДАЧІ ДЕТЕКТУВАННЯ НАЯВНОСТІ ДОДАТКОВОЇ ІНФОРМАЦІЇ В ЦИФРОВИХ КОНТЕНТАХ.....	22
1.1. Основні поняття та принципи стеганографії. Задачі стеганоаналізу....	22
1.2. Класифікація методів стеганоаналізу.....	25
1.3. Стеганоаналітичні методи виявлення вбудови додаткової інформації у цифрових зображеннях.....	29
1.4. Стеганоаналітичні методи виявлення вбудови додаткової інформації у цифрових відео.....	37
1.5. Висновки до розділу 1.....	41
РОЗДІЛ 2. РОЗРОБКА СТЕГАНОАНАЛІТИЧНИХ МЕТОДІВ, ЩО ЗДІЙСНЮЮТЬ АНАЛІЗ ПОСЛІДОВНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ І ЦИФРОВОГО ВІДЕО.....	43
2.1. Розробка теоретичного базису для стеганоаналітичних методів, що аналізують просторову область цифрових контентів.....	44
2.1.1. Відповідність між характерними особливостями сингулярних чисел деяких $n \times n$ -блоків матриці зображення і значеннями яскравості пік селів цих блоків.....	45
2.1.2. Кількісна оцінка наявності блоків спеціального виду в матрицях оригінальних цифрових зображень.....	50
2.2. Аналіз зміни кількості блоків з однаковими значеннями яскравості в матриці зображення в результаті стеганоперетворення.....	53
2.3. Стеганоаналітичний метод для аналізу відеопослідовності, послідовності зображень, заснований на кількісному аналізі зміни числа блоків з однаковими значеннями яскравості.....	60

2.4. Стеганоаналітичний метод, заснований на врахуванні характеру зміни кількості блоків з однаковими значеннями яскравості в результаті первинної і повторної вбудови додаткової інформації.....	65
2.5. Висновки до розділу 2.....	71
РОЗДІЛ 3. РОЗРОБКА СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ ДЛЯ АНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ.....	74
3.1. Удосконалення стеганоаналітичного підходу, заснованого на аналізі кольорів.....	75
3.2. Стеганоаналітичний метод виявлення вбудови додаткової інформації у цифрове зображення/кадр цифрового відео, заснований на аналізі послідовних колірних тріад.....	89
3.3. Адаптація стеганоаналітичного методу SAM3 для виявлення вбудови додаткової інформації в цифрових відео за умови заповнення усіх кадрів.....	92
3.4. Метод визначення формату контейнера, що використовується в процесі стеганоперетворення.....	95
3.5. Висновки до розділу 3.....	99
РОЗДІЛ 4. АНАЛІЗ ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ СТЕГАНОАНАЛІТИЧНИХ МЕТОДІВ.....	102
4.1. Розробка і аналіз стеганоаналітичних алгоритмів, що реалізують розроблені методи.....	104
4.1.1. Розробка і аналіз ефективності алгоритму, що реалізує стеганоаналітичний метод, заснований на врахуванні відносних змін кількості блоків з однаковими значеннями яскравості в результаті первинного і повторного стеганоперетворення.....	107
4.1.2. Розробка і аналіз ефективності алгоритму, що реалізує метод врахування характеру змін кількості блоків з однаковими значеннями яскравості в результаті первинного і повторного стеганоперетворення.....	113

4.1.3. Розробка і аналіз ефективності алгоритмів, що реалізують стеганоаналітичні методи, засновані на аналізі послідовних тріад триплетів.....	117
4.1.4. Розробка і аналіз ефективності алгоритму, що виявляє факт стиску цифрових контентів.....	123
4.2. Порівняльний аналіз розроблених стеганоаналітичних алгоритмів з сучасними аналогами.....	125
4.2.1. Порівняльний аналіз ефективності розроблених стеганоаналітичних алгоритмів, направлених на виявлення додаткової інформації в цифровому відео з сучасними аналогами.....	125
4.2.2. Порівняльний аналіз ефективності алгоритмів, направлених на виявлення додаткової інформації в цифрових зображеннях.....	128
4.3. Практичні рекомендації використання розроблених стеганоаналітичних методів і алгоритмів.....	133
4.4. Комплексний метод виявлення наявності додаткової інформації в цифрових відео.....	136
4.5. Висновки до розділу 4.....	137
ВИСНОВКИ.....	140
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	143
Додаток А. АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ.....	158
Додаток Б. СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ.....	160
Додаток В. ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ.....	162

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

LSB	метод модифікації найменшого значущого біту (Least Significant Bit)
БН	блоки з натуральним сингулярним числом
БЦВ	база цифрових відео
БЦЗ	база цифрових зображень
ДІ	додаткова інформація
ДКП	дискретне косинусне перетворення
ЗПАІС	загальний підхід до аналізу стану і технології функціонування інформаційних систем
ППС	пропускна спроможність прихованого каналу зв'язку
САА	стеганоаналітичний алгоритм
САМ	стеганоаналітичний метод
СНВ	сингулярний вектор
СНЧ	сингулярне число
СП	стеганоповідомлення
ЦВ	цифрові відео
ЦЗ	цифрові зображення
ЦК	цифрові контенти

ВСТУП

Актуальність теми. Бурхливий розвиток інформаційних і комунікаційних технологій призводить до їх широкого розповсюдження в державних, суспільних і побутових сферах, легкої та швидкої передачі будь-якої інформації на великі відстані. Такі відкриті канали зв'язку як електронна пошта, соціальні мережі дозволяють обмінюватися зовнішньо безвинними даними, які можуть містити вбудовану в них цінну конфіденційну інформацію, не виключаючи можливості її використання зі зловмисними намірами. Відкритий доступ до мережі Internet і наукових ресурсів дає можливість відстежувати новітні розробки в області захисту інформації, стеганографії і стеганоаналізу не тільки особам, що використовують їх «на благо», але й тим, хто переслідує небезвинні для суспільства цілі. Застосування стеганографічних методів і алгоритмів дозволяє передавати додаткову інформацію (ДІ), вбудовуючи її в контейнер, що не привертає увагу, в якості якого сьогодні найчастіше виступають цифрові зображення (ЦЗ), аудіо- або відеопослідовності (ЦВ), по відкритих каналах зв'язку, приховуючи сам факт її присутності у контенті, що передається. Результат вбудови ДІ в контейнер будемо називати стеганоповідомленням (СП), а процес вбудови – стеганоперетворенням.

В умовах найжорсткішої конкуренції, розповсюдження тероризму прихована комунікація може призвести до значних збитків для компаній та до катастрофічних наслідків терактів для суспільства в цілому.

З метою попередження зловмисних дій з використанням стеганографічних каналів зв'язку актуальною задачею сьогодні є підвищення ефективності стеганоаналізу, основною задачею якого є виявлення факту наявності/відсутності прихованої інформації у будь-якому інформаційному контенті.

Розробки в області стеганоаналізу ведуть вчені всього світу: І.І. Бобок, А.А. Кобозева, І.А. Узун, А.Д. Кер, J. Fridrich, Udit Budhia, Q.Z. Liu, D. Alimoradi, S.R. Visavalia, Xikai Xu, Jing Dong та інші.

Стеганоаналіз сьогодні розвивається у двох основних напрямках: розробка алгоритмів, що детектують результати вбудови ДІ конкретними стеганометадами, та універсальних, або сліпих (blind), що дозволяють зробити висновок про наявність/відсутність ДІ в контенті без врахування конкретики використаного стеганографічного методу. Однак з появою все нових і нових стеганоалгоритмів задача створення універсального стеганоаналітичного методу стає все більш складною, а результат її рішення викликає певну недовіру. На сьогоднішній день на перший план виходить розробка алгоритмів, що дозволяють детектувати результати роботи конкретних стеганометодів.

Широке розповсюдження в стеганографії отримав метод модифікації найменшого значущого біту (LSB), який і у теперішній час залишається одним з самих використовуваних при організації прихованого каналу зв'язку, залишаючи актуальною задачу детектування результатів його роботи. Постійне удосконалення стеганоаналітичних розробок забезпечило на сьогоднішній день можливість ефективного виявлення вкладення ДІ методом LSB, проведених з високою пропускнуною спроможністю прихованого каналу зв'язку (ППС). Тому для підвищення ймовірності забезпечення приховування таємної комунікації особливістю сучасного використання метода модифікації найменшого значущого біту є застосування його в умовах малої ППС (менше 0.25 біт/піксель), що значно знижує ефективність роботи існуючих стеганоаналітичних комплексів. Сучасні стеганоаналітичні методи часто виявляються неідеальними в умовах $ППС \leq 0.25$ біт/піксель, і навіть не тестуються в таких умовах.

Велика кількість сучасних стеганоаналітичних розробок направлені на детектування наявності/відсутності ДІ, вбудованої методом LSB, у цифрових зображеннях. Існують ефективні стеганоаналітичні методи, що здійснюють аналіз ЦЗ в області перетворень (областях сингулярного/спектрального розкладання відповідних матриць, частотній області, тощо), однак переведення цифрових контентів в область перетворень і назад призводить

до додаткового накопичення обчислювальної похибки, що значно ускладнює процес виявлення ними СП, сформованих при малих значеннях ППС, залишаючи задачу стеганоаналізу у цих умовах невирішеною, а просторову область цифрових контентів найбільш перспективною для організації стеганоаналізу.

Стеганоаналітичні методи, що аналізують просторову область цифрових контентів (ЦК), дозволяють уникнути як додаткових часових витрат, так і накопичення обчислювальної похибки, однак існуючі розробки часто мають невисоку ефективність, якщо при вбудові ДІ використовувався метод LSB з малою ППС.

Застосування цифрових відео в якості контейнеру в стеганографії дозволяє за рахунок великої кількості кадрів передавати значний об'єм даних, використовуючи при цьому малу ППС. Виявити наявність ДІ у цих умовах вісьма проблематично. Однак, незважаючи на переваги використання ЦВ, кількість і якість розробок, присвячених стеганоаналізу відео, є недостатніми, існуючі стеганоаналітичні методи не забезпечують бажану ефективність, зокрема в умовах малої ППС, практично не розглядається задача стеганоаналізу ЦВ у випадку, коли стеганоперетворення зазнають лише деякі кадри ЦВ. Все це можна пояснити тільки значною складністю задачі та неспроможністю існуючих підходів до її рішення.

Таким чином, задача розробки нових ефективних стеганоаналітичних методів і алгоритмів, направлених на виявлення вкладення ДІ, вбудованої методом LSB, у тому числі, при малих значеннях ППС, у ЦЗ та ЦВ є важливою, а тема дисертації «Підвищення ефективності стеганоаналізу для цифрових зображень і відео» актуальною.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконувалася відповідно до пп. 1.2.1.1, 1.2.1.2, 1.2.3.4, 1.2.6.9 і 1.2.8 «Основних наукових напрямів та найважливіших проблем фундаментальних досліджень у галузі природничих, технічних і гуманітарних наук Національної академії наук України на 2014–2018 роки»,

визначених постановою Президії НАН України від 20.12.2013 № 179; відповідає переліку пріоритетних тематичних напрямків наукових досліджень і науково-технічних розробок на період до 2015 року, затверджену Постановою Кабінету Міністрів України №942 від 7 вересня 2011р. Обраний напрямок дослідження відповідає пп. 4.11, 4.12 «Стратегії національної безпеки України», затвердженої Указом Президента України № 287/2015 від 26 травня 2015 р.

Дисертаційна робота виконана в Одеському національному політехнічному університеті відповідно до планів науково-дослідної роботи на тему «Розробка методів підвищення ефективності комплексної системи захисту інформації» (№ держреєстрації 0115U000834).

Мета і задачі дослідження. Метою роботи є підвищення ефективності стеганоаналізу для цифрових зображень і цифрових відео шляхом розробки методів, що детектують в них вкладення конфіденційної інформації LSB-методом, ефективних, у тому числі, при малих значеннях пропускну здатності прихованого каналу зв'язку.

Ефективність стеганоаналізу в роботі оцінюється за допомогою наступних параметрів: помилок першого (пропуск СП) та другого (визначення незаповненого контейнеру як СП) роду; точності детектування вкладення ДІ в ЦК (AD), формальний вираз якої наведений нижче; інтегрального параметра ρ , що визначається за допомогою метода аналізу ROC-кривих. При цьому розглядаються СП, сформовані за допомогою LSB-методу.

Під малими значеннями ППС розуміються значення, не більші 0.25 біт/піксель.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1. Провести аналіз сучасного стану рішення задачі детектування наявності додаткової інформації, вбудованої в цифрові зображення/відео методом LSB;

2. Розробити теоретичний базис для методів детектування наявності додаткової інформації, вбудованої методом LSB в цифрових контентах, у тому числі, з малими значеннями пропускної спроможності прихованого каналу зв'язку, в ході чого обґрунтувати вибір області цифрових контентів для здійснення процесу стеганоаналізу;

3. Розробити стеганоаналітичні методи, направлені на виявлення наявності додаткової інформації у цифрових відео та стеганоаналітичний метод, що здійснює стеганоаналіз окремих кадрів цифрових відео та окремих цифрових зображень, за умови вбудови додаткової інформації методом LSB в одну постійну колірну складову контейнера, ефективні, у тому числі, в умовах малої пропускної спроможності прихованого каналу зв'язку, такі, що здійснюють аналіз просторової області контенту;

4. Розробити метод, який використовує для аналізу просторову область контенту, що дозволяє відокремлювати цифрові контенти, перезбережені з формату з втратами у формат без втрат, від контентів, що спочатку зберігалися у форматі без втрат, який є складовою частиною розроблюваного комплексного стеганоаналітичного методу;

5. Провести аналіз ефективності алгоритмічних реалізацій розроблених стеганоаналітичних методів, у тому числі, порівняльний, на основі якого розробити практичні рекомендації для застосування окремих методів, з врахуванням яких розробити комплексний стеганоаналітичний метод виявлення результатів вбудови додаткової інформації LSB-методом в цифрових відео.

Об'єкт дослідження – процеси організації й виявлення стеганографічного каналу зв'язку.

Предмет дослідження – стеганоаналітичні методи для цифрових зображень і відео.

Методи дослідження. При формуванні теоретичного базису розроблюваних методів використані загальний підхід до аналізу стану і технології функціонування інформаційних систем (ЗПАІС), матричний

аналіз, теорія збурень, чисельні методи, методи обробки ЦЗ. При розробці методів, направлених на виявлення наявності ДІ у ЦВ за умови вбудови ДІ методом LSB в одну постійну колірну складову контейнера, використані матричний аналіз, теорія збурень. При розробці метода, направлено на детектування вкладення ДІ в окремих кадрах ЦВ та окремих ЦЗ за умови вбудови ДІ методом LSB в одну довільну колірну складову контейнера, використані методи обробки ЦЗ. Для оцінки обчислювальної складності алгоритмічних реалізацій розроблених методів використовувалася теорія алгоритмів.

Наукова новизна одержаних результатів полягає у наступному:

1. *Отримав подальший розвиток* загальний підхід до аналізу стану і технології функціонування інформаційних систем шляхом отримання критерію приналежності ненульового сингулярного числа блоку матриці одиничного рангу цифрового зображення/кадру відеопослідовності множині натуральних чисел, що визначає відповідність між характерними властивостями параметрів просторової області і області перетворення цифрових контентів. Це дозволило побудувати теоретичний базис для розроблених стеганоаналітичних методів для цифрових відео, які здійснюють аналіз просторової області контенту, що забезпечило їх високу ефективність при виявленні вкладень додаткової інформації LSB-методом, у тому числі в умовах малих значень пропускну здатності прихованого каналу зв'язку, за рахунок відсутності додаткового накопичення обчислювальної похибки при переведенні цифрових контентів в область перетворень.

2. *Вперше* на основі побудованого теоретичного базису з врахуванням виявлених відмінностей у відносних змінах середньої кількості блоків з однаковими значеннями яскравості у колірній складовій в послідовності цифрових зображень/кадрів цифрових відео в результаті первинної та повторної вбудови додаткової інформації LSB-методом розроблені стеганоаналітичні методи для відеопослідовностей, ефективність яких перевищує ефективність сучасних аналогів, у тому числі при малій

пропускній спроможності прихованого каналу зв'язку і малому розмірі кадрів, що дозволило підвищити ефективність стеганоаналізу цифрового відео.

3. *Вперше* на основі виявлених характерних властивостей послідовних триад колірних триплетів для оригінальних цифрових зображень та зображень-стеганоповідомлень, побудованих за допомогою методу LSB, розроблено стеганоаналітичний метод, ефективність якого для цифрових зображень та окремих кадрів відеопослідовності в умовах вбудови додаткової інформації в одну довільну колірну складову контейнера, у тому числі, з малою пропускною спроможністю прихованого каналу зв'язку, перевищує сучасні аналоги, що дозволило підвищити ефективність стеганоаналізу для цифрових зображень/окремих кадрів цифрових відео.

4. *Вперше* на основі розроблених практичних рекомендацій щодо застосування побудованих методів стеганоаналізу цифрових зображень і відео, заснованих на отриманих оцінках їх ефективності, і розробленого методу відокремлення цифрових контентів, Perezбережених в формат без втрат з формату з втратами, від контентів, що спочатку зберігалися в форматі без втрат, розроблений комплексний стеганоаналітичний метод виявлення вкладень додаткової інформації LSB-методом в цифрові відео, який, на відміну від існуючих, залишається ефективним для малих значень пропускної спроможності прихованого каналу зв'язку, при різній кількості колірних складових контейнера, що використовуються для стеганоперетворення, у тому числі, для контейнерів в градаціях сірого, незалежно від формату цифрового відео-контейнеру (з/без втрат).

Практичне значення одержаних результатів. Практична цінність роботи полягає у доведенні здобувачем отриманих наукових результатів до конкретних методів та алгоритмів, що можуть бути використані як складові комплексних систем захисту інформації будь-яких підприємств, організацій, тощо.

Алгоритм, що реалізує розроблений стеганоаналітичний метод для ЦВ (як кольорових, так і в градаціях сірого), заснований на врахуванні відмінностей у відносних змінах середньої кількості блоків з однаковими значеннями яскравості колірної складової послідовності ЦЗ/кадрів ЦВ в результаті первинної і повторної вбудови ДІ, забезпечує ефективне виявлення стеганоповідомлення, у тому числі, сформованого з малою ППС (аж до 0.125 біт/піксель) в одну (дві, три) колірні складові ЦВ, отриманих камерами мобільних пристроїв (AD для ППС 0.125 біт/піксель досягає 0.94, що на 1.2% перевищує найкращий з існуючих аналогів) та з ППС аж до 0.167 біт/піксель у випадку інших ЦВ (ефективність підвищено максимально на 7.5% (ППС 0.2 біт/піксель) у порівнянні з сучасними аналогами).

Стеганоаналітичний алгоритм виявлення результатів вбудови ДІ методом LSB з незначною ППС для ЦВ (як кольорових, так і в градаціях сірого), заснований на врахуванні відмінностей характеру змін кількості блоків з однаковими значеннями яскравості колірних складових послідовності ЦЗ/кадрів ЦВ в результаті первинної і повторної вбудови ДІ, забезпечує абсолютну ефективність ($AD=1$) виявлення стеганоповідомлень, сформованих вбудовою ДІ з ППС не менше 0.167 біт/піксель в одну (дві, три) колірні складові ЦВ, що не досягалось сучасними аналогами. У випадку ЦВ з малим розміром кадрів висока ефективність забезпечується і для ППС 0.125 біт/піксель: помилки першого роду складають 6.12%, помилки другого роду 5.1%, що не забезпечується жодним з існуючих аналогів.

Алгоритм, що здійснює стеганоаналіз кольорових ЦЗ та окремих кадрів ЦВ забезпечує високу ефективність навіть при ППС 0.05-0.1 біт/піксель. Ефективність виявлення ДІ у ЦЗ при ППС 0.05/0.1 біт/піксель підвищена на 4.5/2.19 % відповідно (показник AD) і у 3.7/2.3 рази відповідно (показник ρ) у порівнянні з кращими аналогами. При стеганоаналізі ЦВ за допомогою стеганоаналітичного алгоритму, заснованому на аналізі послідовних триад колірних триплетів, ефективність підвищено на 2.3% у порівнянні з кращими аналогами для ППС 0.1 біт/піксель, для ППС 0.0625 біт/піксель - на 14.93%,

для ППС 0.05 біт/піксель досягається висока ефективність ($AD = 0.9391$), що не забезпечується жодним сучасним аналогом. У випадку покадрового стеганоаналізу ЦВ ефективність розробленого алгоритму на 5.5% перевищує сучасні аналоги у випадку ППС 0.1 біт/піксель при ступені заповнення кадрів 60-80%, та на 18/32% при ступені заповнення кадрів 40/20% відповідно.

Розроблені стеганоаналітичні алгоритми, засновані на врахуванні змін у кількості блоків з однаковими значеннями яскравості, є поліноміальними степеня 2, алгоритми, засновані на аналізі послідовних тріад триплетів в матриці унікальних кольорів ЦК, є поліноміальними степеня 4.

Акти впровадження. Практичне значення отриманих результатів підтверджене актами впровадження у діяльність компанії «Планета Юг»; в навчальний процес кафедри інформатики та управління захистом інформаційних систем ОНПУ.

Особистий внесок здобувача. Результати дисертаційної роботи отримані автором самостійно. Роботи [134-135, 137-138, 141-143, 145-146] виконані без співавторів. В роботах, опублікованих у співавторстві, автору належить: встановлення властивостей блоків матриці ЦК у просторовій області, що відповідають наявності ненульового натурального сингулярного числа блока; розробка основних кроків стеганоаналітичного методу для виявлення результатів вбудови ДІ методом LSB з незначною ППС у випадку, коли в якості контейнера використовуються ЦВ або послідовність ЦЗ [126]; визначення порогових значень характеру змін кількості блоків з однаковими значеннями яскравості у ЦВ/послідовності ЦЗ, отриманих первинною вбудовою ДІ, у порівнянні з СП, отриманими в результаті повторної вбудови ДІ; розробка основних кроків стеганоаналітичного алгоритму та оцінка його ефективності шляхом визначення помилок першого та другого роду [136]; проведення обчислювальних експериментів [126, 136].

Апробація результатів дисертації. Наукові результати і основні положення дисертаційної роботи доповідалися та обговорювалися на Міжнародних конференціях та семінарах:

- Міжвідомчому міжрегіональному семінарі при Вченій Раді НАН України «Технічні засоби захисту інформації» (Одеса 2014);
- Міжнародної науково-технічної конференції «Сучасні інформаційно-телекомунікаційні технології», Київ, 2015;
- V Міжнародної науково-технічної конференції «Захист інформації і безпека інформаційних систем», Львів, 2016;
- V Міжнародної науково-технічної конференції «Інформаційні системи та технології», Харків-Коблево, 2016;
- V Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології», Одеса, 2016.

Публікації. Матеріали дисертаційної роботи викладено в 11 публікаціях: 7 статей, 6 з яких опубліковано в журналах, які включені у Перелік наукових спеціалізованих видань України; 6 статей – в журналах, включених до міжнародних наукометричних баз (Index Copernicus, РИНЦ, EBSCO, Google Scholar, Ulrich); 5 статей – без співавторів; 1 стаття – у зарубіжному періодичному виданні, 4 тези доповідей на міжнародних наукових конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, чотирьох розділів, загальних висновків, списку використаної літератури з 146 найменувань, 3 додатків на 5 сторінках, 13 рисунків і 18 таблиць – всього 162 сторінки. Основний текст дисертації складається з 130 сторінок (5.42 авторських аркушів).

РОЗДІЛ 1

АНАЛІЗ СУЧАСНОГО СТАНУ РІШЕННЯ ЗАДАЧІ ДЕТЕКТУВАННЯ НАЯВНОСТІ ДОДАТКОВОЇ ІНФОРМАЦІЇ В ЦИФРОВИХ КОНТЕНТАХ

1.1. Основні поняття та принципи стеганографії. Задачі стеганоаналізу

За останнє десятиліття завдяки розвитку інформаційних і телекомунікаційних технологій, а також їх масовому розповсюдженню в суспільних сферах стрімкий розвиток отримали розробки в області комп'ютерної стеганографії, що забезпечує приховування, зберігання і передачу конфіденційних даних у цифрових контейнерах (зображеннях, аудіо, відео, текст, тощо), не викликаючи при цьому підозр про наявність конфіденційної інформації в таких контентях.

Стеганографія – наука про способи передачі прихованої інформації, при яких прихований канал організується на базі і всередині відкритого каналу з використанням особливостей сприйняття інформації [1].

Серед основних призначень стеганографії розрізняють [2]:

- організацію прихованого каналу зв'язку для передачі конфіденційної інформації, приховуючи сам факт її присутності у контенті, що передається, для подолання системи моніторингу мережевими ресурсами і організації каналів витоку інформації;
- вбудова цифрових водяних знаків для забезпечення захисту авторських прав на інтелектуальну власність та захисту конфіденційної інформації від несанкціонованого доступу;
- вбудова ідентифікаційних номерів та заголовків.

Якщо у випадку використання цифрових водяних знаків при забезпеченні захисту авторських прав, як правило, передбачається можливість їх присутності у ЦК, то при організації прихованих каналів зв'язку контенту, що передаються, не повинні викликати ніяких підозр стосовно вмісту в них прихованої інформації.

В стеганографії основними є поняття контейнера, повідомлення, ключа, стеганоповідомлення, стеганоперетворення [1, 2].

Контейнером називається несекретна інформація, яка використовується для приховування повідомлення. В комп'ютерній стеганографії в якості контейнерів можуть виступати оцифровані дані: графічні зображення, цифрові аудіо, відео, текстові та інші електронні документи. Контейнери підрозділяються на фіксовані та потокові, прикладом фіксованого контейнеру є зображення, прикладом потокового контейнеру може служити відео.

Повідомлення (додаткова інформація) – конфіденційна інформація, яку необхідно приховати.

Повідомлення вбудовують в контейнер за допомогою стеганографічного алгоритму з використанням секретного ключа – інформації, що визначає спосіб вбудови ДІ, локалізацію повідомлення та інші параметри, пов'язані з стеганоперетворенням – процесом приховування повідомлення у контейнері, - і відомою лише користувачу, що здійснює вбудову ДІ, та адресату, якому контейнер з ДІ (стеганоповідомлення) передається по відкритому каналу зв'язку.

Під стеганографічною системою (стеганосистемою) розуміють систему, яка представляє собою сукупність повідомлень, секретних ключем, контейнерів та стеганоперетворень, що їх зв'язують [1].

При вбудові ДІ у контейнер модифікуватися можуть не всі елементи контейнера (пікселі ЦЗ, часові відліки аудіо-сигналів), а лише деякі, що впливає на обсяг даних, що передаються приховано (пропускну спроможність прихованого каналу зв'язку). Під пропускну спроможністю прихованого каналу зв'язку розуміють максимальну кількість інформації, яка може бути вбудована в один елемент контейнера [3].

При організації прихованого каналу зв'язку за допомогою стеганографії повинен виконуватися ряд вимог [3]:

- безпека стеганосистеми повинна повністю визначатися секретністю ключа (принцип Керхгоффа);
- знання порушником факту наявності повідомлення у будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах;
- заповнений контейнер повинен бути візуально не відрізнятися від незаповненого;
- повинна забезпечуватися необхідна пропускна спроможність прихованого каналу зв'язку;
- стеганосистема повинна мати прийнятну обчислювальну складність реалізації;
- стеганоалгоритм, що використовується, повинен бути стійким до атак проти вбудованого повідомлення;
- стеганосистема повинна бути стійкою до стеганоаналізу.

Потенційний порушник може мати повне уявлення про стеганосистему, може виявити факт наявності прихованих даних у контенті, однак при відсутності ключа він не в змозі буде встановити зміст конфіденційної інформації, при цьому в сучасних стеганосистемах частиною секретного ключа можуть виступати і координати модифікованих пікселів, і колірна складова, в яку здійснюється вбудова ДІ, і ППС.

Активізація наукової діяльності в області стеганографії, публікації нових результатів у відкритому друці призвели до зростання можливостей використання одержуваних розробок різними антидержавними, терористичними структурами. В силу цього надзвичайно важливим у теперішній момент є рішення питань, пов'язаних з підвищенням ефективності стеганоаналізу, який є складовою частиною стеганографії.

Основною задачею стеганоаналізу [1, 4] є виявлення факту наявності або доказ відсутності у тому чи іншому інформаційному контенті вбудованої інформації, що передається приховано.

1.2. Класифікація методів стеганоаналізу

З огляду на велике розмаїття стеганографічних методів при стеганоаналізі часто є невідомим, який саме метод був використаний для вбудови ДІ. Знання або хоч припущення про використаний стеганографічний метод сприяє вибору методів детектування вбудови ДІ у ЦК: направлених проти конкретних алгоритмів або програм, або універсальних, що дозволяють виявляти наявність ДІ, вбудованої різними методами. Існують різноманітні класифікації стеганоаналітичних методів в залежності від направленості, вхідних даних, способу визначення ДІ, тощо.

Наведені нижче класифікації стеганоаналітичних методів є загальними для ЦЗ та ЦВ, оскільки відео можна представити у виді послідовності окремих кадрів (зображень), таки чином, будь-який стеганоаналітичний алгоритм для ЦЗ принципово може бути адаптований для виявлення ДІ у ЦВ.

Згідно класифікації, запропонованої І.В. Швидченко у [5, 6] в залежності від використовуваних вхідних даних методи стеганоаналізу поділяються на:

1. *направлені*, призначені для роботи з конкретними заздалегідь відомими стеганографічними методами та алгоритмами;
2. *універсальні*, призначені для виявлення вкладення ДІ, вбудованої будь-якими методами стеганографії. Більшість алгоритмів цієї групи засновані на попередньому «навчанні» з використанням пустих і заповнених контейнерів.

Інша, більш детальна класифікація запропонована А.А. Смірновим, Є.В. Мелешко у [7], де методи стеганоаналізу підрозділяються за наступними ознаками:

1. В залежності від наявності інформації про метод стеганографії: направлені та універсальні (сліпі).
2. В залежності від вхідних даних:
 - методи пасивного стеганоаналізу, направлені на виявлення факту наявності або відсутності ДІ в інформаційному контенті;

- методи активного стеганоаналізу, що дозволяють визначити довжину, розташування ДІ у стеганоповідомленні та її вилучення.

3. В залежності від способу визначення прихованої інформації:

- візуальні методи;
- статистичні методи;
- методи, засновані на стиску даних;
- нейромережеві методи.

Візуальні методи базуються на спроможності зорової системи людини аналізувати зорові образи та виявляти суттєві відмінності у зображеннях, кадрах відео, що зіставляються. Найбільш розповсюдженим є метод візуального аналіз бітових зрізів ЦЗ [5], заснований на зіставленні бінарних шарів, які формуються відповідними бітами значень яскравості матриці ЦЗ з зображенням цілком, де шукаються видимі порушення міжпиксельної та внутрішньопиксельної кореляції. В окремих випадках інформативним є візуальний контроль однотонних фрагментів зображення або аналіз артефактів стиску у збільшеному масштабі [8].

Статистичні методи засновані на оцінці відмінностей статистичних характеристик оригінального контейнера та СП, однак, у стеганоаналітика, як правило, оригінальний контейнер є відсутнім для порівняння, а самі статистичні характеристики різних зображень можуть відрізнятися дуже сильно і залежать від специфіки самого контейнера, що є суттєвим недоліком статистичних методів [5-6, 8].

Ідея методів стиску заснована на принципах стиску і архівування даних: потік випадкових даних стискається гірше, ніж потік, в якому зустрічаються повторювані послідовності. При вбудові секретних даних кількість повторюваних послідовностей скорочується, а, відтак, стиск такого контейнера суттєво не змінить його розмір. У [9, 10] пропонується порівняти коефіцієнти стиску досліджуваного контенту і СП, сформованого повторним заповненням довільною бінарною послідовністю. Якщо отримані коефіцієнти стиску є близькими, то можна говорити про наявність прихованої інформації

в досліджуваному контенті. Такий метод є ефективним за умови пропускну́ї спроможності прихованого каналу зв'язку більше 35%. У [10] наводиться точність виявлення ДІ, вбудованої при різних значеннях ППС методом LSB. З врахуванням мети дисертації, наведені результати будуть використані при порівнянні ефективностей розробленого алгоритму детектування ЦЗ з сучасними аналогами. Пошуки в цьому напрямку продовжуються, і у 2012 році В.А. Монарьовим був запропонований більш ефективний зсувний метод виявлення прихованої інформації [11], заснований на операції логічного побітового зсуву вправо.

Методи стеганоаналізу, засновані на використанні нейронних мереж, передбачають використання статистичних методів в поєднанні з можливостями навчання нейронних мереж, на основі якого здійснюється відокремлення незаповнених контейнерів від СП. Дані методи значно розширюють можливості статистичних методів за рахунок можливості комбінування різних технік стеганоаналізу, наприклад, характеристик просторової області, коефіцієнтів дискретного косинусного перетворення і дискретного вейвлетного перетворення, як це описано в [12].

Класифікація А.А. Смірнова і Є.В. Мелешко в достатньої степені відображає загальні напрями розвитку стеганоаналізу. Також загальні класифікації наведені у [13, 14]. Проте, сучасні методи стеганоаналізу розрізняються великою кількістю використовуваних технік для виявлення прихованої інформації, що було відображено в класифікації, запропонованої Rita Chhikara, Latika Singh в роботі [15], де методи класифіковані за особливостями техніки вилучення. Згідно [15] стеганоаналіз поділяється на сигнатурний і спеціальний статистичний, причому обидва види можуть бути направленими і універсальними. Статистичні методи підрозділяються на техніки в залежності від того, в яку область (просторову або перетворень) здійснювалась вбудова ДІ.

Сигнатурні методи засновані на виявленні у ЦК «слідів» - сигнатур (специфічних бітових послідовностей, нетипових значень у службових полях

і полях даних файлів, невідповідностей формату, тощо), які залишаються деякими програмами, що реалізують стеганоперетворення, такими як, наприклад, HideandSeek, JPegX [16-19].

До основних статистичних методів належать [15]: метод аналізу розподілу пар значень на основі критерію χ^2 (Chi square Attack) [20-23], RQP метод (Raw Quick Pair) [24]; RS-стеганоаналіз [25]; апроксимація B-сплайном (B-spline fitting) [26]; аналіз гістограм (Histogram Analysis Attack) [27]; процедура калібрування [28].

Надзвичайно привабливою на сьогоднішній день є ідея універсальних стеганоаналітичних методів, що дозволяють шляхом виявлення або констатації відсутності визначених характерних ознак в контенті, що аналізується, робити висновок про здійснену вбудову секретної інформації або її відсутності, не прив'язуючись до конкретики використовуваного стеганографічного методу. Універсальний стеганоаналіз використовує наступні особливості для виявлення прихованих даних [15]: Марковські особливості (Markov Features) [29-32], метрики якості зображення (Image Quality Metrics) [33], особливості вейвлет-перетворення (Wavelet Transform Features) [34-39], суміжні матриці (Co-occurrence Matrix) [40-44], особливості гістограм (Histogram Features) [45-48], бінарні критерії подоби (Binary Similarity Measure) [49-50], особливості контурного перетворення (Contourlet Transform Features) [51-55], особливості дискретного косинусного перетворення (DCT) [56-58].

Проте, часто формування характеристичного вектору на основі особливостей лише одного конкретного виду не дає бажаних результатів детектування, тому за останні декілька років різко зросла кількість розробок з використанням комбінованого аналізу особливостей різноманітного характеру (наприклад, особливості гістограм, вейвлет-перетворення, дискретного косинусного перетворення), які формують характеристичний вектор [59-76]. На основі незаповнених контейнерів і СП здійснюється навчання за допомогою методу опорних векторів, нейронних мереж,

генетичних алгоритмів, тощо. Таке комбінування різних технік дозволило покращити результати виявлення СП, сформованих при ППС 0.25 біт/піксель та вище.

1.3. Стеганоаналітичні методи виявлення вбудови додаткової інформації у цифрових зображеннях

Більшість робіт, присвячених стеганоаналізу, направлена на виявлення вбудови ДІ у ЦЗ, що обумовлено наступними причинами [3]:

- відносно великим обсягом цифрового представлення зображень, що дозволяє вбудовувати ДІ великого об'єму;
- заздалегідь відомим розміром контейнера;
- наявністю у більшості ЦЗ текстурних областей, що мають шумову структуру і добре підходять для вбудови інформації;
- слабкою чутливістю зорової системи людини до незначних змін кольорів, яскравості, контрастності зображення;
- добре розробленим в останній час методам цифрової обробки зображень.

Найчастіше використовуваним стеганографічним методом був і залишається на сьогоднішній день метод заміни найменших значущих біт. Незважаючи на значний «вік» цього методу, він залишається широко використовуваним. Потенційна можливість заміни молодших біт байтів контейнера бітами ДІ обумовлена присутністю в зображенні структурної надмірності. Фактично, стеганоперетворення методом LSB тотожно накладанню шуму. Найраніші стеганографічні схеми, які використовувались LSB-методом, фокусувалися на вбудові інформації за допомогою внесення незначного спотворення у вихідне зображення, враховуючи положення про те, що чим менше вноситься спотворень при вбудові, тим більш стійкою до стеганоаналізу є стеганографічна система. У зв'язку з цим специфіка сьогоднішнього використання стеганометодів, у тому числі і LSB, з врахуванням удосконалення методів стеганоаналізу, полягає у поверненні до

принципу «чим менше спотворення, тим більш стійка стеганосистема», робить актуальною задачу виявлення стеганоперетворень, здійснених при малій пропускній спроможності прихованого каналу зв'язку.

В багатьох сучасних роботах [32, 61, 63, 68, 72-74], направлених на розробку ефективних стеганоаналітичних методів і алгоритмів, проводиться аналіз СП, сформованих за допомогою метода LSB, який є основою таких програм вбудови ДІ, як JSTEG, Outguess, JPHIDE, Steghide:

- JSTEG – програма вбудови ДІ у ЦЗ в форматі JPEG, алгоритм якої полягає у послідовній заміні молодших бітів усіх ненульових квантова них коефіцієнтів блоків зображення на біти повідомлення [1];

- Outguess – приховування інформації здійснюється у надмірні біти контейнера (для ЦЗ в форматі JPEG під надмірними бітами розуміються молодші біти елементів блока спектру після квантування) [1];

- JPHIDE використовує для приховування молодші біти квантова них коефіцієнтів [1];

- Steghide – програма вбудови ДІ у просторову область ЦЗ, а також аудіо-формати WAV AU, заміною молодших біт контейнера на біти повідомлення [1].

Також на основі метода LSB розроблені такі методи і програми як F5 (та її різновиди) [77-78], PQ (Perturbed Quantization) [53].

При оцінці ефективності запропонованих розробок використовують метод аналізу ROC-кривих, однією з складових якого є визначення точності детектування [79-81], що характеризує долю правильно виявлених СП і незаповнених контейнерів.

Серед статистичних методів стеганоаналізу найчастіше використовують RS-стеганоаналіз [25], запропонований колективом вчених під керівництвом Дж. Фридрих, що дозволяє крім виявлення самого факту наявності прихованої інформації оцінити приблизну пропускну спроможність прихованого каналу зв'язку і довжину повідомлення. Однак даний метод є

мало придатним для зашумлених контентів і ЦЗ, що містять велику кількість дрібних деталей, що знижує точності виявлення СП [82-84].

Метод «аналіз пар» [85-89] заснований на пошуку закономірностей у ймовірностях появи значень яскравості у незаповнених контейнерах і СП. Метод здійснює аналіз просторової області і направлений, перш за все, на виявлення наявності ДІ, вбудованої методом модифікації найменшого значущого біту у просторову область ЦК, і багато в чому базується на особливостях вбудови ДІ методом LSB. При використанні метода LSB значення яскравості колірної складової ЦК в результаті стеганоперетворення або зберігає своє значення, або змінюється на одиницю. Для виявлення вкладень ДІ здійснюється аналіз закономірностей у частотах появи «сусідніх» («лівих», найменший значущий біт яких дорівнює 0, і «правих», найменший значущий біт яких дорівнює 1) значень яскравості. Виходячи з припущення, що ймовірності появи «лівих» і «правих» номерів кольору у незаповнених контейнерах суттєво відрізняються між собою у всіх парах, а в СП ці ймовірності є рівними, робиться висновок про наявність або відсутність вбудованої ДІ в ЦК, що аналізується. В роботах [85-86] тестування запропонованих розробок здійснюється для ЦЗ в форматі без втрат, для яких забезпечується точність детектування більше 0.9 для будь-яких категорій ЦЗ при ППС, що перевищує 0.2 біт/піксель. В роботах [87-89] проводяться дослідження, у тому числі, і для ЦЗ, що початково зберігалися в форматі з втратами, для яких досягається висока ефективність детектування при ППС, не меншої 0.2 біт/піксель (помилки першого і другого роду складають 0.5% [89]), у випадку ЦЗ в форматі без втрат висока ефективність досягається лише при ППС 1 біт/піксель. Проте, метод «аналіз пар», хоч і здійснює аналіз просторової області, однак не дозволяє виявляти наявність ДІ, вбудованої при ППС, меншої за 0.2 біт/піксель.

Ще один варіант статистичного стеганоаналізу передбачає побудову гістограму значень квантованих дискретних косинусних коефіцієнтів [90-94]. Експериментально встановлено, що огинаюча гістограми незаповненого

контейнера має більш гладкий характер, у порівнянні з гістограмами СП, які можуть мати ступінчастий характер при значних обсягах вкладень ДІ, що не властиве для оригінальних ЦЗ в форматі з втратами. Зокрема, в роботі [90] отримані високі результати детектування за умови вбудови ДІ у ЦЗ в форматі без втрат при ППС 0.5 біт/піксель, однак у випадку ЦЗ в форматі з втратами навіть при ППС 0.5 біт/піксель ефективність є недостатньою, що видно з наведених у роботі ROC-кривих.

В сучасній теорії і практиці сигналів активно використовуються сигнали спеціального виду – вейвлети. Вони показали свою ефективність у спектральному аналізі і стисненні сигналів. В роботах [95-96] наводиться теорія і практичне застосування різних вейвлетів. В роботах [97-100], присвячених стеганоаналізу, заснованому на вейвлет-розкладанні ЦЗ, спостерігається невисока ефективність у випадку ППС, меншої за 0.5 біт/піксель. В роботі [97] характеристичний вектор формують особливості вейвлет-перетворення ЦЗ, на основі якого за допомогою метода опорних векторів проводиться навчання і тестування, однак високі результати детектування отримані лише для ППС 1 біт/піксель, при менших значеннях ППС (0.78, 0.2, 0.05 біт/піксель) точність виявлення вкладень ДІ монотонно зменшується. В роботі [98] проводиться аналіз СП, сформованих при малих значеннях ППС, для яких помилки першого роду складають 11.33% (ППС 0.02 біт/піксель) і 12.19% (ППС 0.05 біт/піксель), однак із зростанням ППС ефективність детектування погіршується – для ППС 0.25 біт/піксель помилки першого роду складають вже 30.76%.

Найчисельніший клас статистичних методів – це методи класифікації з навчанням, які є, як правило, універсальними. Загальна схема стеганоаналізу для них може бути описана наступним чином [16]:

1. Визначення характеристичних векторів контейнерів.
2. Вибір і навчання класифікатора, на вхід якого подаються характеристичні вектори контейнерів навчальної вибірки, що формується з

репрезентативної кількості пустих і заповнених контейнерів, для кожного з яких відомо, до якого з двох класів вони належать.

3. Класифікація ЦЗ, що підлягають перевірці.

Характеристичний вектор повинен бути чутливим до змін, які вносяться стеганоперетворенням, але при цьому незалежним від вмісту контейнерів. Елементи характеристичних векторів пустих і заповнених контентів повинні відрізнятися. Чим більше відмінностей між ними спостерігається, тим краще такий елемент підходить для цілей стеганоаналізу.

Основним недоліком методів класифікації з навчанням є те, що контенти навчальної вибірки повинні мати максимально схожі характеристики з контентами, класифікація яких є метою стеганоаналізу, що потребує проводити навчання для різних категорій ЦЗ (природа, будівлі, тварини, люди, тощо), однак на практиці, як правило, один і той же ЦК може відноситися одночасно до різних категорій, що призводить до обмежень на застосування методів класифікації.

В більшості сучасних джерел [32, 59-69] навчання класифікатора здійснюється за допомогою метода опорних векторів, при цьому характеристичний вектор включає в себе різноманітні техніки вилучення особливостей ЦЗ (дискретне косинусне перетворення, вейвлет-перетворення, особливості гістограм, тощо).

В роботі [32] здійснюється формування характеристичного вектора на основі Марковських особливостей, особливостей дискретного косинусного перетворення. Для навчання і подальшого детектування використовуються незаповнені контейнери в форматі JPG і СП, сформовані програмами, заснованими на LSB – Jphide, Outguess (область дискретного косинусного перетворення), Steghide (просторова область) для малих значень ППС (0.05, 0.1 і 0.2 біт/піксель), для яких отримана достатньо висока точність детектування (0.97 для ППС 0.05 біт/піксель). Також в роботі проводиться порівняння точності детектування з аналогами [59, 70-71] для різних методів вбудови ДІ і для різних значень ППС, зокрема, результати для програми

Steghide будуть використані при порівнянні ефективності метода СААЗ, розробленого в роботі, і сучасних аналогів.

В роботі [59] розроблений метод аналізу як ЦЗ в форматі без втрат, так і в форматі з втратами для різних значень ППС (0.5 біт/піксель і менше), отримана висока точність детектування при ППС 0.1 і 0.2 біт/піксель. Результати, отримані в даній роботі, будуть використані для порівняння ефективності розроблених в дисертаційному дослідженні методів.

В роботі [61] характеристичний вектор враховує особливості гістограм, побудованих для коефіцієнтів дискретного косинусного перетворення, вбудова ДІ здійснюється за допомогою стеганографічних програм Nsf5, PQ при значеннях ППС 0.1, 0.25, 0.5, 1 біт/піксель. Висока точність детектування спостерігається лише для метода PQ незалежно від значення ППС, у випадку вбудови ДІ програмою Nsf5 (різновид F5) висока точність детектування спостерігається лише для ППС 0.5 і 1 біт/піксель, при малих значеннях ППС запропонований алгоритм є неефективним.

В роботі [63] здійснюється спроба виявлення наявності ДІ, вбудованої за допомогою програм Outguess, F5, Jsteg при малих значеннях ППС (0.05, 0.1, 0.2 біт/піксель), однак точність детектування є низькою: від 0.65 до 0.695. В роботі [64] авторами проводиться аналіз ефективності запропонованих розробок за допомогою метода аналізу ROC-кривих. Кращі результати, представлені у виді ROC-кривих, для малих значень ППС будуть використовуватися для порівняння інтегральних параметрів при оцінці ефективності методів, розроблених в роботі.

В роботі [68] проводиться детектування ЦЗ за допомогою методу опорних векторів і байєсовського класифікатора на основі характеристичного вектора, що формується особливостями коефіцієнтів дискретного косинусного перетворення, для незаповнених контейнерів и СП, сформованих програмою F5 при значеннях ППС 0.1, 0.2, 0.3, 0.5 біт/піксель. Краща точність детектування досягається байєсовським класифікатором і складає 0.55-0.59.

Цікавий підхід до стеганоаналізу у просторовій області представлений в роботі [72], де розроблений алгоритм заснований на розбитті матриці зображення на блоки з подальшою їх сегментацією, що є основою для навчання і подальшого відокремлення СП від незаповнених контейнерів за допомогою метода опорних векторів. Запропонований алгоритм дозволяє виявляти локалізацію пікселів, в які вбудовувалась ДІ за допомогою програм Outguess, F5, заснованих на LSB, і оцінити приблизну довжину повідомлення. По результатам тестування алгоритму при ППС 0.05 і 0.1 біт/піксель точність виявлення складає від 0.89 до 0.95 в залежності від програми вбудови ДІ і значення ППС.

Таким чином, як витікає з вищесказаного, зроблені спроби по розробці стеганоаналітичних методів виявлення наявності ДІ, вбудованої методом LSB і за допомогою програм, заснованих на LSB, з малою ППС, не забезпечує бажану ефективність стеганоаналізу.

Менш розповсюдженим на сьогоднішній день стосовно до стеганоаналізу є навчання за допомогою нейронних мереж [73-75], кластеризації [76, 101] і генетичних алгоритмів [102], однак і в даних розробках спостерігається невисока ефективність при виявленні СП, сформованих при малій ППС.

В роботі [73] для відокремлення контейнерів від СП, сформованих програмами JSTEG, Outguess, F5, JPHIDE (однак без зазначення значень ППС при вбудові ДІ), проводиться навчання за допомогою нейронних мереж на основі характеристичного вектора, що формується з врахуванням особливостей коефіцієнтів дискретного косинусного перетворення, вейвлет-перетворення, Марковських особливостей. По результатам детектування правильно виявлено 85.4% СП, 75% незаповнених контейнерів, що говорить про недостатню ефективність запропонованого методу.

В роботі [74] характеристичний вектор формується з врахуванням енергії, ентропії, кореляції, контрасту відповідних матриць ЦЗ, на основі незаповнених контейнерів і СП, сформованих програмами F5 (заснована на

LSB), S-TOOLS, JPHS05, що здійснюють вбудову ДІ в область дискретного косинусного перетворення, Steghide (у просторову область за допомогою LSB) без зазначення ППС, проводиться тестування алгоритму, розробленого на основі запропонованого підходу, по результатам якого правильно виявлено 75.68% СП, сформованих програмою Steghide, і 93.23% незаповнених контейнерів.

В роботі [76] запропонований алгоритм, заснований на навчанні за допомогою нейронних мереж, виявлення наявності ДІ, вбудованої методами LSB Replacement і LSB Matching при значеннях ППС 0.25, 0.5 і 1 біт/піксель, однак для малих значень ППС результати не наводяться, що може говорити про неспроможність розробленого метода в зазначених умовах стеганоперетворення. Для ППС 0.25 біт/піксель точність детектування складає 0.9388/0.9167 відповідно для методів вбудови ДІ LSB Replacement і LSB Matching.

Останнім часом для вирішення задач, пов'язаних з виявленням порушення цілісності цифрових контентів, зокрема для стеганоаналізу, добре зарекомендував себе ЗПАІС, заснований на теорії збурень і матричному аналізі [103]. Згідно з ЗПАІС будь-яка інформаційна система (ЦЗ, ЦВ) формально представляється у виді кінцевої множини двовимірних матриць, а зміна стану системи – у виді сукупності збурень повного набору параметрів: сингулярних чисел і сингулярних векторів відповідних матриць. ЗПАІС ліг в основу одного з найбільш ефективних сучасних стеганоаналітичних методів виявлення вбудованої методом LSB інформації в контейнер, що зберігається в форматі з втратами, з малою ППС [104]. Аналіз ефективності розробленого методу проводився в роботі [105] за допомогою аналізу ROC-кривих для різних значень ППС, у тому числі і малих (0.05 і 0.1 біт/піксель), вбудови ДІ методом LSB. Для розробленого методу SAVV значення інтегрального параметра перевищує 0.9 при ППС, не меншої за 0.4 біт/піксель, для ППС 0.2/0.25/0.3 біт/піксель значення інтегрального параметра складає 0.8/0.85/0.884 відповідно, однак при малих значеннях ППС ефективність

детектування є невисокою (значення інтегрального параметра складає 0.42/0.188 відповідно для ППС 0.1/0.05 біт/піксель). Тут же наводиться порівняння інтегрального параметра, що характеризує роботу методу SAVV, з аналогами [106-108], які зовсім не тестувались в силу їх неспроможності у випадках ППС нижче 0.25 біт/піксель. Результати аналізу ефективності методу SAVV і результатів аналогів, наведених в [106-108], використовуються в роботі для порівняння ефективності розробленого методу виявлення вбудови ДІ у ЦЗ за допомогою методу аналізу ROC-кривих.

Як видно з наведеного огляду, переважна більшість стеганоаналітичних методів при виявленні вбудови ДІ здійснює аналіз області перетворень ЦЗ, що негативно позначається на ефективності детектування при малих значеннях ППС.

1.4. Стеганоаналітичні методи виявлення вбудови додаткової інформації у цифрових відео

Використання ЦВ в якості контейнера в стеганографії має ряд переваг у порівнянні з ЦЗ, зокрема за рахунок великої кількості кадрів можна передати значний обсяг даних навіть за умови малої ППС, що значно ускладнює процес стеганоаналізу. Проте, незважаючи на переваги використання ЦВ, відеостеганоаналіз менш розвинений, ніж стеганоаналіз ЦЗ. Розглянемо існуючі у відкритому доступі розробки в області відеостеганоаналізу, зупинившись докладніше на виявленні СП, сформованих за допомогою метода LSB. Слід зазначити, що в роботах, присвячених виявленню вкладень ДІ в ЦВ, на відміну від ЦЗ, рідко згадується безпосередньо метод LSB як такий, а вбудова ДІ описується як вбудова цифрового водяного знаку за допомогою адитивної атаки, що описується формулою $y_k = x_k + w_k$ [109], де x_k - k -ий оригінальний кадр ЦВ, w_k - ДІ, що представляється у виді бінарної матриці, y_k - k -ий кадр-СП. Така адитивна атака призводить або до зміни

значень яскравості пікселів відповідного кадру на 1, або до незмінного значення яскравості, що, по суті, є методом LSB.

В роботах [110-111] був запропонований метод для відеостеганоаналізу, заснований на аналізі надмірної інформації, присутньої в часовій області, як інформації, найбільш чутливої до збурень, зокрема вбудови ДІ (в роботі розглядаються цифрові водяні знаки). Запропонований метод заснований на впливі на ЦВ, що аналізується, адитивною атакою, в результаті якої здійснюється збурення матриці кадрів ЦВ, після чого на основі ЦВ, що аналізується, і ЦВ, отриманого впливом адитивної атаки, формуються характеристичні вектори, що включають Марковські особливості першого порядку (область перетворень), на основі яких здійснюється навчання і відокремлення СП від незаповнених контейнерів. В роботах наведені результати обчислювального експерименту, що проводився на основі 27 ЦВ в градаціях сірого, збережених в форматі без втрат, у кожному відео у середньому по 40 кадрів, де точність детектування за допомогою запропонованого метода складає близько 0.7, що очевидно не є задовільним результатом.

Розробки на основі врахування часової кореляції кадрів ЦВ були продовжені в роботі [109], де автором пропонується адаптація підходів, запропонованих в [38, 112] для ЦЗ, які здійснюють аналіз області перетворень зображень, стосовно до ЦВ. В роботі проводиться тестування як для запропонованого метода, так і окремо для кожного з методів, заснованих на підходах з [38, 112] на основі 10 ЦВ в градаціях сірого, в кожному відео по 124 кадри, для різних значень ППС. Результати обчислювальних експериментів будуть використовуватися для порівняння ефективності розроблених методів виявлення вкладень ДІ у ЦВ з сучасними аналогами. При ППС 0.2 біт/піксель та вище точність детектування запропонованого в [109] підходу вище 0.9, при ППС 0.1 біт/піксель точність детектування складає 0.89.

Одними з різновидів MPEG є кодеки H.264, H.265, які розглядають відео як послідовність I-, P- і B-кадрів, де I-кадри представляють собою незалежні кадри, на які посилаються P- і B-кадри, що робить I-кадри пріоритетними для вбудови ДІ, яка завдяки посилальним кадрам дублюється у відповідних P- і B-кадрах. Стеганоаналіз, що враховує таке представлення ЦВ і, як наслідок, особливості вбудови ДІ у I-кадри, представлений роботами [113-114].

В роботі [113] пропонується формувати характеристичний вектор з врахуванням статистичних особливостей I-кадрів (кореляції між елементами блоків матриці кадрів ЦВ у просторовій області), на основі якого проводиться навчання і відокремлення СП, сформованих за допомогою адитивної атаки, від незаповнених контейнерів. Обчислювальний експеримент для апробації запропонованого методу проводився для ППС 0.0625, 0.125, 0.25, 0.5, 0.75 і 1 біт/піксель на основі 9 ЦВ з кількістю кадрів від 150 до 494. Запропонований метод є найбільш ефективним при ППС 0.25 біт/піксель та вище, при ППС 0.125 біт/піксель точність детектування складає 0.928, при ППС 0.0625 біт/піксель – лише 0.794, що говорить про невисоку ефективність при малих значеннях ППС. Результати запропонованого методу будуть використані для порівняльного аналізу ефективності розроблених в роботі методів.

В роботі [114] при тестуванні розробленого стеганоаналітичного методу ДІ вбудовувалась методом LSB з різними значеннями ППС 0.1, 0.25, 0.5, 0.75, 1 біт/піксель у 26 ЦВ, по 100 кадрів у кожному. Слід зазначити, що обчислювальні експерименти проводились як за умови повного заповнення кадрів, так і за умови часткового заповнення кадрів, що не розглядалося ні в одній з попередніх робіт. Запропонований метод заснований на виявленні особливостей кореляції пікселів кадрів ЦВ, які формують характеристичний вектор, на основі якого проводиться навчання за допомогою метода опорних векторів. Отримані високі значення точності детектування для різних значень ППС – більше 0.97 за умови повного заповнення кадрів, і при ППС 0.25 біт/піксель і вище за умови часткового заповнення кадрів – більше 0.98.

Результати, отримані в роботі [114] будуть використані для порівняння ефективності розроблених методів з сучасними аналогами.

В роботі [115] запропонований стеганоаналітичний алгоритм для ЦВ, направлений проти СП, сформованих програмою MSUstego [116], що здійснює вбудову ДІ адитивною атакою з врахуванням кореляції між сусідніми кадрами ЦВ [114]. Обчислювальний експеримент проводився на основі 20 відео, при цьому кожний кадр (всього 962) аналізувався окремо, в результаті був обраний порог, для якого помилки другого роду склали 5.4% при помилках першого роду 5.3%. Однак в даній роботі не зазначена ППС, з якою здійснювалась вбудова ДІ, що не дозволяє використовувати дані експериментів для порівняння ефективності розроблених методів з сучасними аналогами.

В роботі [117] пропонується відеостеганоаналіз, заснований на навчанні за допомогою методу опорних векторів. Характеристичний вектор формується на основі особливостей просторової області і області перетворень кадрів ЦВ, на основі відмінностей між незаповненим контейнером і СП за допомогою навчання робиться висновок про наявність / відсутність ДІ у ЦВ, що аналізується. Обчислювальний експеримент проводився на основі 50 ЦВ, вбудова ДІ здійснюється адитивною атакою за допомогою методів, запропонованих в [118-119], і програмою MSUstego [116] без зазначення ППС, по результатам експерименту точність детектування перевищує значення 0.94.

Метод LSB є складовою частиною стеганографічного методу вбудови ДІ у вектори руху, заснованого на схемі кодування MPEG і представленні ЦВ у виді послідовності I-, P- і B-кадрів. У сусідніх кадрах аналізуються блоки, які співпадають за значеннями яскравості і приблизному розташуванню, якщо блок змінив своє розташування, на основі координат його початкового і теперішнього розташування визначаються магнітуда та фазовий кут, куди і здійснюється вбудова ДІ методом LSB, при цьому ППС складає 1 біт/піксель. Стеганоаналіз СП, сформованих описаним методом, представлений роботами

[120-124], однак вбудова ДІ у вектори руху відрізняється від звичної модифікації просторової області, тому результати таких методів не можуть використовуватися для коректного порівняння в даній роботі.

Таким чином, серед робіт, присвячених відеостеганоаналізу, широке розповсюдження отримали методи, що здійснюють аналіз просторово-часової області ЦВ, а саме векторів руху, а також спеціалізовані, що враховують особливості представлення ЦВ схемою MPEG та її різновидами. При цьому слід врахувати, що у випадку ЦВ запропоновані стеганоаналітичні методи в основному розглядають просторову область, однак ефективність виявлення СП, сформованих при малих значеннях ППС, є низькою, що говорить про неспроможність існуючих підходів для виявлення наявності ДІ, вбудованої за таких умов.

1.5. Висновки до розділу 1

На основі проведеного аналізу наукових джерел за темою дисертаційного дослідження, доступних з відкритого друку, можна зробити наступні висновки:

1. Стеганографічний метод LSB був і залишається на сьогоднішній день одним з найвикористовуваних методів при організації прихованого каналу зв'язку, однак особливістю його використання стає забезпечення малої пропускної спроможності прихованого каналу зв'язку.

2. Більшість стеганоаналітичних розробок здійснюють аналіз області перетворень ЦК, що призводить до накопичення додаткової обчислювальної похибки, а це в свою чергу знижує ефективність виявлення вкладень ДІ, вбудованої за умови малих значень ППС (в багатьох джерелах зовсім не проводиться аналіз ЦК при ППС, меншій за 0.25 біт/піксель, або спостерігається низька ефективність запропонованих розробок при малих значеннях ППС).

3. Якість і кількість розробок в області відеостеганоаналізу є недостатньою, що можна пояснити складністю задачі і неспроможністю існуючих підходів до її рішення.

4. В сучасних стеганоаналітичних розробках майже не розглядається питання покадрового аналізу у випадку, коли вбудова ДІ здійснюється лише у частину кадрів відеопослідовності.

5. Для існуючих стеганоаналітичних методів, що використовуються для аналізу ЦВ, оцінка їх ефективності проводиться, як правило, на основі малої кількості відеопослідовностей, що тестуються (до 26 ЦВ), що ускладнює об'єктивну оцінку реального стану відеостеганоаналізу.

6. При всьому різноманітті існуючих для детектування LSB стеганоаналітичних методів проблема стеганоаналізу відповідних ЦЗ, ЦВ не є повністю вирішеною. Актуальною залишається задача детектування вбудови конфіденційної інформації, що здійснюється при малій пропускній спроможності прихованого каналу зв'язку.

Таким чином, в розділі 1 вирішена задача 1 з переліку задач дисертаційної роботи; показано, що задача розвитку і підвищення ефективності стеганоаналізу, направленою на виявлення факту наявності / відсутності прихованої інформації у цифрових контентях (ЦЗ, ЦВ), є актуальною.

РОЗДІЛ 2

РОЗРОБКА СТЕГАНОАНАЛІТИЧНИХ МЕТОДІВ, ЩО ЗДІЙСНЮЮТЬ АНАЛІЗ ПОСЛІДОВНОСТІ ЦИФРОВИХ ЗОБРАЖЕНЬ І ЦИФРОВОГО ВІДЕО

Переважаюча кількість існуючих стеганоаналітичних методів здійснює аналіз ЦК в області перетворень: частотної, області сингулярного розкладання відповідної матриці/матриць, тощо. Однак переведення ЦЗ або кадрів ЦВ в область перетворень не тільки потребує додаткових часових затрат, але й призводить до додаткового накопичення обчислювальної похибки, що не має ніякого відношення безпосередньо до процесу стеганоперетворення. Це, в свою чергу, може знизити ефективність стеганоаналізу, що особливо помітно при виявленні СП, сформованих при малої ППС стеганографічного каналу.

Мета розділу: розробка стеганоаналітичних методів виявлення результатів вбудови ДІ методом LSB в цифрові контенті (ЦВ і послідовність ЦЗ), що використовують для аналізу просторову область.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. Розробити теоретичний базис для стеганоаналітичних методів, що аналізують просторову область цифрових контентів, в ході чого виявити і встановити відповідність між характерними особливостями сингулярних чисел деяких $n \times n$ – блоків ЦЗ і значеннями яскравості пікселів цих блоків;
2. Вибрати розмір блока матриці контейнера, найбільш інформативний з точки зору встановлених в ході рішення задачі 1 особливостей значень яскравості його пікселів;
3. Отримати кількісні оцінки для блоків матриць оригінальних ЦЗ, що мають встановлені характеристики;

4. Розробити стеганоаналітичний метод, заснований на врахуванні змін кількості блоків матриці ЦЗ, що мають встановлені характеристики, при первинної і повторної вбудові ДІ, спроможний в умовах малої ППС.

2.1. Розробка теоретичного базису для стеганоаналітичних методів, що аналізують просторову область цифрових контентів

Як вже було відзначено у розділі 1, в останній час для рішення задач стеганоаналізу добре зарекомендував себе ЗПАІС, у відповідності з яким результат стеганоперетворення ЦЗ, кадру ЦВ формально представляється у виді сукупності збурень СНЧ і СНВ відповідних матриць. На основі такого представлення був розроблений один з найбільш ефективних, у тому числі в умовах малої ППС, сучасних стеганоаналітичних методів виявлення вбудованої методом LSB інформації у контейнер, що зберігається в форматі з втратами [104].

При практичному аналізі особливостей СНЧ $n \times n$ – блоків матриць R , G , B оригінальних зображень (колірна схема RGB), отриманих шляхом стандартного розбиття [125], з використанням ЗПАІС практично в кожному ЦЗ була виявлена [126] наявність блоків, що мають єдине ненульове СНЧ, причому яке належить множині натуральних чисел, кратне розміру блока n (блоки з натуральним СНЧ, далі позначаються БН), що раніше не відзначалось в роботах, пов'язаних з використанням ЗПАІС для задачі стеганоаналізу [104]. Кількість БН монотонно зменшувалась в межах одного ЦЗ зі зростанням розміру блока. Така особливість оригінальних ЦЗ є надзвичайно важливою у світлі розв'язуваної задачі: приналежність єдиного ненульового СНЧ множині натуральних чисел (якщо така має місце, а не є результатом накопичення обчислювальної похибки, що відбувається в процесі побудови сингулярного розкладання матриці блока) буде особливістю, чутливою до малих збурень, що відбуваються в ЦЗ, у тому числі, до результатів стеганоперетворення, і може бути використана в процесі стеганоаналізу, оскільки в загальному випадку СНЧ для довільного

ЦЗ (довільної матриці) є невід’ємними дійсними числами [127]. Однак аналіз інформаційного контенту з використанням інструментів ЗПАІС потребує переведення його в область перетворень – область сингулярного розкладання відповідних матриць. У зв’язку з цим необхідно встановити відповідність між виявленими характерними особливостями СНЧ БН (область сингулярного розкладання відповідних матриць) і особливостями значень яскравості пік селів (просторова область ЦЗ) цих блоків.

2.1.1. Відповідність між характерними особливостями сингулярних чисел деяких $n \times n$ -блоків матриці зображення і значеннями яскравості пікселів цих блоків

Розглядаються кольорові ЦЗ, що зберігаються у відповідності з колірною схемою RGB і формально представляються у виді сукупності трьох двовимірних матриць R , G і B - червоної, зеленої і синьої колірних складових ЦЗ відповідно. Кожна матриця стандартним чином розбивається на блоки розміром $n \times n$, що не перетинаються.

Має місце наступна теорема.

Теорема 2.1 (необхідна умова належності ненульового сингулярного числа матриці одиничного рангу множині натуральних чисел). Нехай A - $n \times n$ - матриця, $\sigma_1, \sigma_2, \dots, \sigma_n$ - сингулярні числа A , при цьому

$$\sigma_1 > 0, \sigma_2 = \dots = \sigma_n = 0, \sigma_1 \in \mathbb{N}, \sigma_1 : n, \quad (2.1)$$

де \mathbb{N} - множина натуральних чисел, $\sigma_1 : n$ позначає, що σ_1 кратне n , тоді A має наступний вид:

$$A = \begin{pmatrix} a & a & \dots & a \\ a & a & \dots & a \\ \dots & \dots & \ddots & \dots \\ a & a & \dots & a \end{pmatrix}, a \neq 0. \quad (2.2)$$

Доведення. Побудуємо для A нормальне сингулярне розкладання [103]:

$$A = U\Sigma V^T, \quad (2.3)$$

де U, V - $n \times n$ - ортогональні матриці, стовпці яких є лексикографічно додатними лівими та правими сингулярними векторами матриці A відповідно, $\Sigma = \text{diag}(\sigma_1, \sigma_2, \dots, \sigma_n)$ - матриця сингулярних чисел. В загальному випадку $\sigma_1 \geq \sigma_2 \geq \dots \geq \sigma_n \geq 0$.

Сингулярне розкладання матриці (2.3) можна подати у формі зовнішніх добутків [127]:

$$A = \sum_{k=1}^n \sigma_k u_k v_k^T, \quad (2.4)$$

де $u_k, v_k, k = \overline{1, n}$, - стовпці матриць U, V відповідно.

З врахуванням (2.1) відношення (2.4) буде мати вид:

$$A = \sigma_1 u_1 v_1^T. \quad (2.5)$$

Оскільки, як показано в [128], для матриці (блоку матриці) ЦЗ розміру $n \times n$ лівий і правий сингулярні вектори u_1, v_1 , що відповідають максимальному сингулярному числу σ_1 , мало відрізняються від n -оптимального вектора простору R^n , що має вид: $n^o = \left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, \dots, \frac{1}{\sqrt{n}} \right)^T \in R^n$,

тобто

$$u_1 \approx n^o, v_1 \approx n^o,$$

то співвідношення (2.5) приймає вид:

$$A = \sigma_1 u_1 v_1^T = \sigma_1 n^o (n^o)^T = \sigma_1 \left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, \dots, \frac{1}{\sqrt{n}} \right)^T \left(\frac{1}{\sqrt{n}}, \frac{1}{\sqrt{n}}, \dots, \frac{1}{\sqrt{n}} \right) =$$

$$= \begin{pmatrix} \frac{\sigma_1}{n} & \frac{\sigma_1}{n} & \dots & \frac{\sigma_1}{n} \\ \frac{\sigma_1}{n} & \frac{\sigma_1}{n} & \dots & \frac{\sigma_1}{n} \\ \dots & \dots & \dots & \dots \\ \frac{\sigma_1}{n} & \frac{\sigma_1}{n} & \dots & \frac{\sigma_1}{n} \end{pmatrix},$$

звідки, з врахуванням, що σ_1 кратне n , безпосередньо витікає висновок теореми.

В ході обчислювального експерименту, проведеного з метою практичного підтвердження висновку теореми 2.1, було встановлено, що у просторовій області більше 99% $n \times n$ -БН мають вид (2.2), де $a \in \{1, 2, 3, \dots, 255\}$.

Зв'язок між встановленою властивістю єдиного ненульового СНЧ матриці (блока матриці) ЦЗ та її (його) видом (2.2) носить не лише необхідний, але і достатній характер. Має місце наступна теорема [126].

Теорема 2.2 (достатня умова належності єдиного ненульового сингулярного числа матриці ЦЗ множині натуральних чисел). Для $n \times n$ -матриці A виду (2.2) максимальне СНЧ буде визначатися як $\sigma_1 = na \in \mathbb{N}$, а для інших СНЧ виконується умова $\sigma_2 = \dots = \sigma_n = 0$.

Доведення. Виконання умови $\sigma_2 = \dots = \sigma_n = 0$ для матриці (2.2) витікає з того, що $\text{rank}(A) = 1$ [129-130].

Енергії $En(A)$ сигналу, формальним представленням якого є деяка $n \times n$ -матриця A з елементами a_{ij} , $i, j = \overline{1, n}$, і СНЧ $\sigma_1 \geq \dots \geq \sigma_n \geq 0$, може бути обчислена у відповідності з наступними формулами [103]:

$$En(A) = \sum_{i,j=1}^n a_{ij}^2, \quad (2.6)$$

$$En(A) = \sum_{i=1}^n \sigma_i^2. \quad (2.7)$$

З урахуванням виду (2.2) матриці A формула (2.6) має вид:

$$En(A) = n^2 a^2, \quad (2.8)$$

а з врахуванням того, що $\sigma_2 = \dots = \sigma_n = 0$, формула (2.7) перетворюється:

$$En(A) = \sigma_1^2. \quad (2.9)$$

Дорівнявши (2.8) і (2.9), отримаємо:

$$n^2 a^2 = \sigma_1^2,$$

Звідки з врахуванням (2.3):

$$\sigma_1 = na \in \mathbb{N},$$

що й потрібно було довести.

Зміна лише одного елемента матриці (2.2), яка може виникнути в результаті стеганоперетворення, призведе до того, що висновок теореми 2.2 не буде мати місця. Дійсно, матриця виду:

$$\bar{A} = \begin{pmatrix} a & a & a & \dots & a & \dots & a \\ a & a & a & \dots & a & \dots & a \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a & a & a & \dots & a + \Delta a & \dots & a \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a & a & a & \dots & a & \dots & a \end{pmatrix}, a \in \{1, 2, \dots, 255\},$$

отримана з (2.2) збуренням єдиного елемента на Δa , має ранг, більший за одиницю (що дорівнює двом), а значить, не задовольняє теоремі 2.2, оскільки буде мати два ненульових СНЧ. Звісно, варіант збуреної матриці \bar{A} , що має одиничний ранг, можливий, наприклад:

$$\bar{A} = \begin{pmatrix} a & a & a & \dots & a + \Delta a & \dots & a \\ a & a & a & \dots & a + \Delta a & \dots & a \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a & a & a & \dots & a + \Delta a & \dots & a \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a & a & a & \dots & a + \Delta a & \dots & a \end{pmatrix}$$

або

$$\bar{A} = \begin{pmatrix} a & a & a & \dots & a & \dots & a \\ a & a & a & \dots & a & \dots & a \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a + \Delta a & a + \Delta a & a + \Delta a & \dots & a + \Delta a & \dots & a + \Delta a \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a & a & a & \dots & a & \dots & a \end{pmatrix},$$

однак мало ймовірний у випадку стеганоперетворення, оскільки стеганошлях, як правило, визначається за допомогою генератора псевдо довільної послідовності чисел [1], крім того, тут явно буде порушене співвідношення $\sigma_1 = na \in \mathbb{N}$ для максимального СНЧ.

Теореми 2.1 і 2.2 дають можливість отримати критерій належності єдиного ненульового СНЧ матриці (блоку матриці) ЦЗ множині натуральних чисел:

Твердження 2.1. Для того, щоб єдине ненульове СНЧ σ_1 $n \times n$ -матриці (блоку матриці) A ЦЗ належало множині натуральних чисел, необхідно і достатньо, щоб A мала вид (2.2), при цьому $\sigma_1 = na \in \mathbb{N}$.

Належність $\sigma_1 \in \mathbb{N}$ є важливим показником для констатації оригінальності блоків виду (2.2) ЦК. Будь-які зміни A , що зачіпають такі блоки, призведуть в них до $\sigma_1 \notin \mathbb{N}$, що може служити показником порушення цілісності цифрового контенту (ЦЗ, кадру відео), зокрема показником стеганоперетворення.

2.1.2. Кількісна оцінка наявності блоків спеціального виду в матрицях оригінальних цифрових зображень

Проведемо кількісну оцінку наявності блоків виду (2.2) різного розміру (4×4 , 6×6 , 8×8 , 10×10 і 12×12) в оригінальних ЦЗ, що зберігаються як в форматі без втрат (TIFF), так і в форматі з втратами (JPG), шляхом обчислювального експерименту. В цьому і подальших експериментах, що проводяться з ЦЗ, використовується база зображень (БЦЗ), що включає 1019 кольорових ЦЗ (схема RGB):

- 200 ЦЗ з бази NRCS Photo Gallery [131] в форматі TIFF (група 1);
- 200 зображень в форматі TIFF, отриманих непрофесійними фотокамерами (група 2);
- 203 ЦЗ з бази NRCS Photo Gallery [131] в форматі JPG (група 3);
- 201 високоякісних ЦЗ в форматі JPG, взятих з [132] (група 4);
- 215 зображень в форматі JPG, отриманих непрофесійними фотокамерами (група 5).

Необхідно зазначити, що найбільш ймовірним при організації прихованого каналу зв'язку, очевидно, буде використання зображень груп 2 і

5, оскільки пересилання зображень (відео) по каналу загального використання буде менш привертати увагу у випадку, коли контенти мають безпосереднє відношення до відправника/отримувача. В силу цього основна увага при проведенні подальших обчислювальних експериментів приділяється саме групам 2 і 5.

В ході експерименту кожна колірна складова оригінального зображення досліджувалась окремо. Результати експерименту наведені в табл. 2.1, де стовпець I несе інформацію про колірну складову ЦК; II – про максимальне значення кількості блоків виду (2.2), що маються (у процентному відношенні стосовно загальної кількості блоків в матриці ЦЗ) у відповідній колірній складовій серед всіх ЦЗ відповідної групи; III – середнє значення кількості (%) блоків виду (2.2) по відповідній колірній складовій відповідної групи ЦЗ.

Середнє значення кількості (%) блоків виду (2.2) розраховується наступним чином:

1. для кожного ЦЗ визначається кількість блоків з однаковими значеннями яскравості k_R, k_G, k_B відповідно для червоної, зеленої і синьої складової;

2. для кожного ЦЗ визначається відсоток блоків виду (2.2) у кожній колірній складовій: $\overline{k_R} = \frac{k_R}{k_B} \cdot 100\%$, $\overline{k_G} = \frac{k_G}{k_B} \cdot 100\%$, $\overline{k_B} = \frac{k_B}{k_B} \cdot 100\%$, де k_B - загальна кількість $n \times n$ -блоків виду (2.2) у колірній складовій;

3. обчислюється середнє значення кількості (%) $n \times n$ -блоків з однаковими значеннями яскравості по всім ЦЗ:

$$av_R = \frac{1}{P} \sum_{i=1}^P \overline{k_{R_i}}, \quad av_G = \frac{1}{P} \sum_{i=1}^P \overline{k_{G_i}}, \quad av_B = \frac{1}{P} \sum_{i=1}^P \overline{k_{B_i}}, \quad (2.10)$$

де P - кількість ЦЗ відповідної групи.

Таблиця 2.1 – Кількість блоків виду (2.2) у колірних складових оригінальних ЦЗ відносно загального числа блоків серед всіх ЦЗ відповідної групи, %

I	Група 1		Група 2		Група 3		Група 4		Група 5	
	II	III	II	III	II	III	II	III	II	III
4×4										
<i>R</i>	25.67	1.29	6.17	0.76	44.02	5.97	30.43	1.84	27.78	2.81
<i>G</i>	17.65	0.65	13.77	0.67	44.21	5.94	28.42	1.84	29.89	2.82
<i>B</i>	74.34	3.88	9.18	0.62	46.41	5.99	26.55	2.04	31.39	3.07
6×6										
<i>R</i>	25.61	1.07	5.19	0.61	38.77	4.79	24.18	1.25	22.35	1.83
<i>G</i>	17.54	0.55	12.19	0.52	38.86	4.79	20.77	1.22	24.77	1.81
<i>B</i>	69.37	3.19	5.19	0.47	41.82	4.83	21.23	1.31	26.49	2.08
8×8										
<i>R</i>	25.52	0.96	4.42	0.51	35.53	3.43	14.84	0.93	20.58	1.68
<i>G</i>	17.43	0.50	10.99	0.44	35.12	3.33	14.78	0.94	23.53	1.71
<i>B</i>	65.09	2.80	5.17	0.38	37.18	3.46	14.75	1.02	25.38	1.88
10×10										
<i>R</i>	25.43	0.88	3.89	0.44	27.37	1.52	13.01	0.50	15.16	1.09
<i>G</i>	17.35	0.46	9.93	0.38	26.82	1.44	13.04	0.50	17.78	1.11
<i>B</i>	61.01	2.54	4.72	0.33	28.43	1.55	12.87	0.54	20.01	1.24
12×12										
<i>R</i>	25.39	0.83	3.42	0.38	26.59	1.40	12.71	0.46	14.85	1.02
<i>G</i>	17.29	0.43	9.12	0.33	26.05	1.33	12.74	0.46	16.73	1.03
<i>B</i>	57.24	2.33	4.33	0.29	27.73	1.43	12.53	0.49	19.11	1.17

З табл. 2.1 видно, що кількість блоків з однаковими значеннями яскравості в матрицях *R*, *G*, *B* оригінальних зображень монотонно зменшується зі зростанням розміру блока незалежно від групи ЦЗ, таким чином, найбільш вираженим факт наявності блоків виду (2.2) виявився при використанні 4×4-блоків.

В табл. 2.1 не наведені мінімальні значення блоків виду (2.2) у колірних складових серед всіх ЦЗ відповідних груп, оскільки у будь-якій групі були такі ЦЗ, в яких зовсім були відсутні блоки з однаковими значеннями яскравості (будь-якого розміру). Виняток складають ЦЗ з групи 5 при розмірі блоку 4×4 , де мінімальне значення блоків серед всіх ЦЗ в червоній і зеленій колірних складових складає 0.0015%, в синьої колірної складової – 0.0005%.

Для ЦЗ в форматі TIFF було встановлено: біля 9% загальної кількості колірних матриць (в експерименті їх кількість всього $400 \times 3 = 1200$) зовсім не мають 4×4 -блоків виду (2.2); кількість блоків виду (2.2) залежить від специфіки ЦЗ: чим більше дрібних деталей на зображенні, тим менше блоків виду (2.2) у його матрицях. Такий ефект є очікуваним. Дійсно, якщо всі значення яскравості блока однакові, то він не може містити частини контурів об'єктів ЦЗ, що характеризуються перепадами яскравості прилеглих пікселів.

У випадку ЦЗ в форматі JPG в 2.2% від загальної кількості колірних матриць (з $619 \times 3 = 1857$ матриць) не міститься 4×4 -блоків виду (2.2), що суттєво нижче аналогічного показника для зображень в форматах без втрат. Така відмінність пояснюється стиском ЦЗ: округлення коефіцієнтів ДКП до найближчого цілого після квантування призводить до уніфікації сусідніх близьких за значеннями яскравостей до їх середнього значення.

Очевидно, що вбудова ДІ методом LSB в просторову область цифрових контентів змінить кількість блоків з однаковими значеннями яскравості в тої колірної складової, куди здійснювалась вбудова ДІ, що буде використано при розробці стеганоаналітичного методу, що аналізує просторову область цифрових контентів.

2.2. Аналіз зміни кількості блоків з однаковими значеннями яскравості в матриці зображення в результаті стеганоперетворення

Виходячи з припущення, що в результаті вбудови ДІ у ЦЗ кількість блоків з однаковими значеннями яскравості в СП відносно контейнера зменшиться, а також з врахуванням того, що більшість оригінальних ЦЗ

містять 4×4 -блоки виду (2.2), встановимо оцінку зміни кількості 4×4 -блоків виду (2.2) після вбудови ДІ методом LSB у всі колірні складові ЦЗ шляхом обчислювального експерименту, де СП формуються на основі контейнерів з БЦЗ при ППС 0.5, 0.25 і 0.1 біт/піксель. Результати експерименту наведені в табл. 2.2, де стовпець з позначенням I відповідає використуваному значенню ППС (біт/піксель); II – колірній складовій ЦЗ; III_i – середньому значенню відносної (по відношенню до загальної кількості блоків у матриці колірної складової ЦЗ (%)) кількості блоків з однаковими значеннями яскравості по всім СП з *i*-ої групи відповідно (формула (2.8)); IV_i – відносної зміни середнього значення кількості блоків з однаковими значеннями яскравості у сформованих СП у порівнянні з оригінальним ЦЗ для *i*-ої групи відповідно (%).

Зміни середнього значення кількості блоків виду (2.2) $\bar{R}, \bar{G}, \bar{B}$ відповідно для червоної, зеленої та синьої колірної складової оригінального контейнера у порівнянні з СП обчислюються за формулами:

$$\begin{aligned}\bar{R} &= \frac{|av_R^{(C)} - av_R^{(S)}|}{av_R^{(C)}} \cdot 100\%, \\ \bar{G} &= \frac{|av_G^{(C)} - av_G^{(S)}|}{av_G^{(C)}} \cdot 100\%, \\ \bar{B} &= \frac{|av_B^{(C)} - av_B^{(S)}|}{av_B^{(C)}} \cdot 100\%,\end{aligned}\tag{2.11}$$

де $av_R^{(C)}, av_G^{(C)}, av_B^{(C)}$ – середні значення кількості блоків у послідовності оригінальних ЦЗ у червоної, зеленої і синьої складових відповідно;

$av_R^{(S)}, av_G^{(S)}, av_B^{(S)}$ – середні значення кількості блоків у послідовності СП, сформованих вбудовою ДІ з однаковою ППС в оригінальний контейнер, у червоної, зеленої і синьої складових відповідно.

Таблиця 2.2 – Кількість 4×4 -блоків з однаковими значеннями яскравості у колірних складових ЦЗ-СП, сформованих для різних значень ППС, відносно загального числа блоків колірних складових зображення (%)

I	II	Група 1		Група 2		Група 3		Група 4		Група 5	
		III ₁	IV ₁	III ₂	IV ₂	III ₃	IV ₃	III ₄	IV ₄	III ₅	IV ₅
0.5	R	1.24	3.4	1.94	18.5	0.52	91.3	0.67	63.6	0.56	80.1
	G	0.60	7.8	2.19	33	0.46	92.2	0.69	62.6	0.69	75.5
	B	3.85	0.8	3.16	10.7	0.52	91.2	1.05	48.6	0.88	71.2
0.25	R	1.23	4.1	1.94	18.8	0.51	91.4	0.66	64	0.55	80.3
	G	0.59	8.5	2.18	15.4	0.46	92.3	0.68	63	0.69	75.6
	B	3.82	1.7	3.15	11	0.52	91.3	1.03	49.7	0.88	71.5
0.1	R	1.23	4.1	1.95	18.1	0.75	87.4	0.70	61.9	0.66	76.5
	G	0.60	8.1	2.20	14.7	0.68	88.5	0.74	59.7	0.77	72.6
	B	3.81	1.9	3.16	10.9	0.80	86.6	1.07	47.5	0.98	68.1

Як показує обчислювальний експеримент, абсолютна кількість блоків виду (2.2) в межах матриці як оригінального ЦЗ, так і СП, може бути дуже незначною, більш того, указані блоки в ЦЗ можуть бути зовсім відсутніми. Абсолютна кількість блоків виду (2.2) в оригінальному ЦЗ може співпадати з кількістю таких блоків в ЦЗ-СП, побудованого на основі іншого контейнеру, що не дає принципіальної можливості відокремлювати контейнер від СП за такою характеристикою.

При проведенні аналізу більш інформативним є те, як зміниться ця кількість при вбудові ДІ, у порівнянні з оригінальним ЦЗ-контейнером (см. IV_i в табл. 2.2). Як видно з табл. 2.2, зміни, що відбуваються, залежать від групи ЦЗ з БЗЦ: ці зміни будуть найбільш помітними в групах ЦЗ, зроблених непрофесійними фотокамерами (групи 2, 3, 5). Більш того, в оригінальних ЦЗ з груп 2, 3 і 5 початково кількість блоків виду (2.2) більша, що є очікуваним в силу гіршої початково якості ЦЗ цих груп. Однак необхідно відзначити, що в межах однієї групи фіксуємо зміни кількості блоків виду (2.2) майже не

залежать від значення ППС (для тих значень, які були використані і навмисно визначають незначну ППС). Зміни, які отримуються для ЦЗ з груп 1 і 4 в результаті стеганоперетворення, не настільки значні у порівнянні з іншими групами відповідних форматів, що пояснюється більш високою якістю ЦЗ. Слід відзначити, що відносні зміни в форматах з втратами на порядок вище, ніж в форматі без втрат, що очікувано і пояснюється, як вже відзначалося вище, особливостями стиску зображень.

Отже, в реальних умовах стеганоаналіз проводиться, як правило, при відсутності оригінального зображення-контейнера.

З'ясуємо, як зміниться кількість блоків виду (2.2) в ЦЗ-СП при повторної вбудові ДІ методом LSB з різними значеннями ППС. Результати експерименту наведені в табл. 2.3, де стовпець з позначенням I відповідає значенню ППС (біт/піксель) при первинній вбудові ДІ; II – значенню ППС (біт/піксель) при повторній вбудові ДІ; III – колірній складовій ЦЗ-СП; V_i – середньому значенню кількості блоків з однаковими значеннями яскравості в СП, сформованих в результаті повторної вбудови ДІ методом LSB в ЦЗ-СП з i -ої групи відповідно (формула (2.10)); V_i – зміні середнього значення кількості блоків з однаковими значеннями яскравості у порівнянні з СП, сформованими в результаті повторної вбудови ДІ методом LSB в ЦЗ-СП з i -ої групи відповідно (%). Тут зміни середнього значення кількості блоків виду (2.2) $\bar{R}, \bar{G}, \bar{B}$ відповідно для червоної, зеленої та синьої колірної складової ЦЗ-СП у порівнянні з СП, сформованим повторною вбудовою ДІ, обчислюються за формулами:

$$\begin{aligned}\bar{R} &= \frac{|av_R^{(S)} - av_R^{(\bar{S})}|}{av_R^{(S)}} \cdot 100\%, \\ \bar{G} &= \frac{|av_G^{(S)} - av_G^{(\bar{S})}|}{av_G^{(S)}} \cdot 100\%, \\ \bar{B} &= \frac{|av_B^{(S)} - av_B^{(\bar{S})}|}{av_B^{(S)}} \cdot 100\%,\end{aligned}\tag{2.12}$$

де $av_R^{(\bar{s})}$, $av_G^{(\bar{s})}$, $av_B^{(\bar{s})}$ – середні значення кількості блоків у послідовності СП, сформованих повторною вбудовою ДІ в ЦЗ-СП, у червоної, зеленої і синьої складових відповідно.

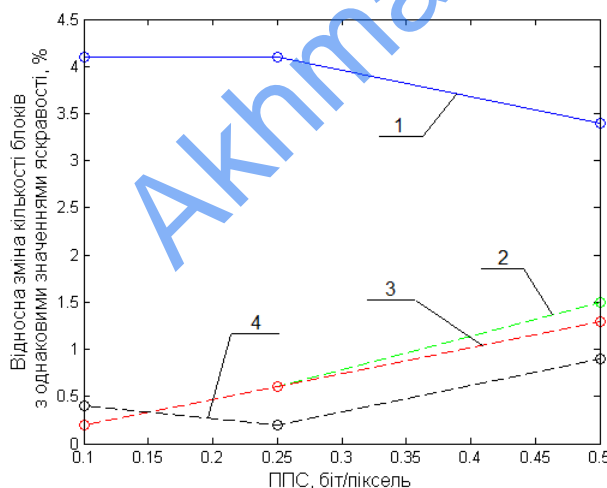
Таблиця 2.3 – Оцінки для абсолютної і відносної кількості 4×4 -блоків з однаковими значеннями яскравості у колірних складових ЦЗ-СП, сформованих шляхом повторної вбудови ДІ в СП, отримані методом LSB для різних значень ППС, усереднені по всіх зображеннях з груп 1-5 (%)

I	II	III	Група 1		Група 2		Група 3		Група 4		Група 5	
			IV ₁	V ₁	IV ₂	V ₂	IV ₃	V ₃	IV ₄	V ₄	IV ₅	V ₅
0.5	0.5	R	1.26	1.5	1.96	0.8	0.54	3.7	0.69	3.1	0.58	3.3
		G	0.61	1.4	2.20	0.6	0.48	3.9	0.71	3.3	0.71	1.9
		B	3.91	1.7	3.18	0.5	0.54	3.6	1.10	5.2	0.91	2.2
	0.25	R	1.25	0.6	1.95	0.3	0.52	0.5	0.68	1	0.56	0.7
		G	0.60	0.6	2.19	0.3	0.46	0.4	0.69	1.1	0.70	0.6
		B	3.87	0.6	3.17	0.3	0.52	0.4	1.07	1.9	0.89	0.9
	0.1	R	1.25	0.2	1.95	0.1	0.52	0.2	0.67	0.4	0.56	0.3
		G	0.60	0.2	2.19	0.1	0.46	0.1	0.69	0.4	0.69	0.2
		B	3.86	0.3	3.17	0.1	0.52	0.2	1.06	0.8	0.89	0.4
0.25	0.5	R	1.25	1.3	1.95	0.7	0.52	1.2	0.68	2.3	0.56	1.8
		G	0.60	1.3	2.19	0.7	0.46	1	0.69	2.3	0.70	1.1
		B	3.88	1.6	3.17	0.6	0.53	1	1.07	4.3	0.89	2.1
	0.25	R	1.24	0.6	1.95	0.5	0.58	12.4	0.67	1.9	0.57	3.7
		G	0.60	0.5	2.19	0.3	0.49	6.1	0.70	2.9	0.71	2.7
		B	3.84	0.6	3.17	0.4	0.58	11.6	1.05	2.4	0.89	2.1
	0.1	R	1.24	0.2	1.94	0.1	0.51	0.2	0.66	0.4	0.56	0.3
		G	0.60	0.3	2.18	0.1	0.46	0.2	0.68	0.4	0.69	0.2
		B	3.83	0.3	3.16	0.1	0.52	0.2	1.03	0.8	0.88	0.4

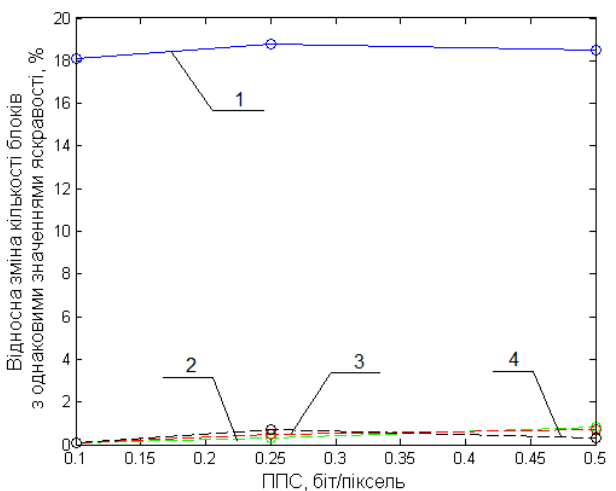
Продовження табл. 2.3

I	II	III	Група 1		Група 2		Група 3		Група 4		Група 5	
			IV ₁	V ₁	IV ₂	V ₂	IV ₃	V ₃	IV ₄	V ₄	IV ₅	V ₅
0.1	0.5	R	1.25	0.9	1.95	0.3	0.52	30.8	0.67	4.1	0.56	15
		G	0.60	0.6	2.19	0.3	0.46	32.3	0.69	6.8	0.69	10.5
		B	3.86	1.4	3.17	0.3	0.52	34.7	1.06	1.2	0.89	9.4
	0.25	R	1.24	0.2	1.94	0.7	0.51	31.3	0.66	5.3	0.56	15.7
		G	0.60	0.2	2.18	0.7	0.46	32.6	0.68	8	0.69	10.9
		B	3.83	0.5	3.16	0.01	0.52	35.1	1.03	3.5	0.88	10.4
	0.1	R	1.24	0.4	1.96	0.1	1.09	45.6	0.74	5.1	0.78	18.8
		G	0.61	1.6	2.22	1.1	1.15	68.2	0.78	5.6	0.83	6.9
		B	3.82	0.4	3.16	0.2	1.11	38.4	1.13	5.9	1.07	9.5

Наглядною ілюстрацією змін середнього значення кількості блоків виду (2.2) в результаті первинної і повторної вбудови ДІ служить рис. 2.1, побудований для червоної колірної складової зображень (червона колірна складова обрана для прикладу).



а



б

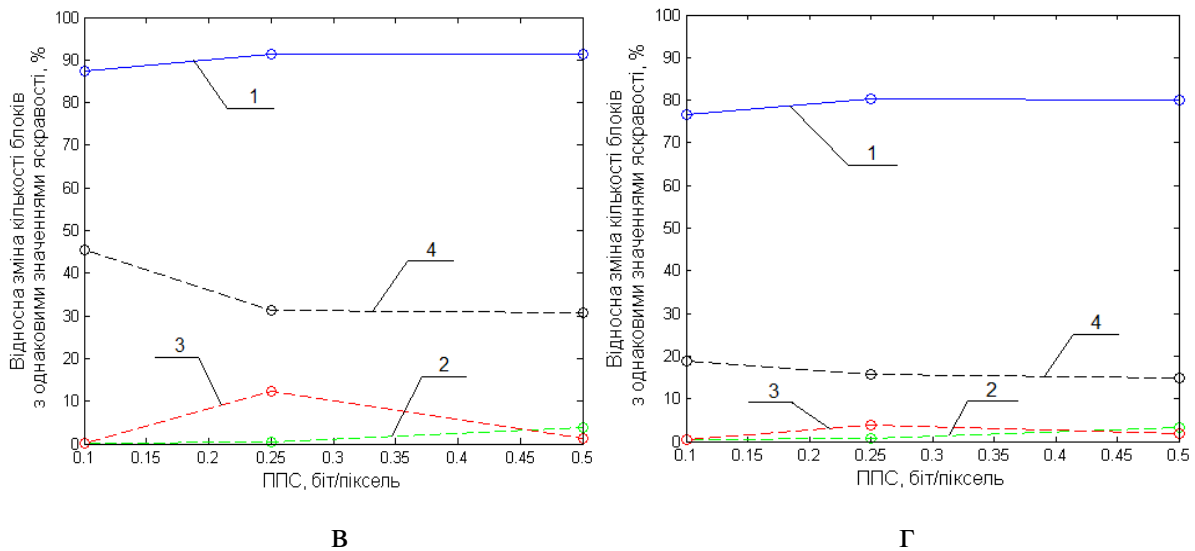


Рис. 2.1 - Залежність відносної зміни середнього значення кількості (%) 4×4 - блоків виду (2.2) в матрицях ЦЗ від ППС метода LSB, що використовується для стеганоперетворення: 1 – для СП, отриманого в результаті однократної вбудови ДІ у порівнянні з оригінальним ЦЗ; 2 – для СП, отриманого шляхом повторної вбудови ДІ у СП, сформоване методом LSB з ППС 0.5 біт/піксель; 3 – для СП, отриманого повторною вбудовою ДІ у СП, сформоване методом LSB з ППС 0.25 біт/піксель; 4 – для СП, отриманого повторною вбудовою ДІ у СП, сформоване методом LSB з ППС 0.1 біт/піксель; а – ЦЗ з групи 1; б – ЦЗ з групи 2; в – ЦЗ з групи 3; г – ЦЗ з групи 5

З табл. 2.2, 2.3 і рис. 2.1 випливає, що результати первинного і повторного стеганоперетворення кількісно (для БН виду (2.2)) відрізняються один від одного настільки, що дають можливість відокремити послідовність незаповнених контейнерів-зображень від послідовності ЦЗ-СП. Послідовність ЦЗ (кадрів ЦВ) впливає з формули (2.10), де середні значення кількості блоків з однаковими значеннями яскравості обчислюються по всім ЦЗ в групі.

З рис. 2.1 видно, що відносні зміни при первинній вбудові ДІ в ЦЗ з групи 2 (рис. 2.1, б) зіставні з відносними змінами при повторній вбудові ДІ в ЦЗ з групи 5 (рис. 2.1, г), при цьому в першому випадку в якості контейнерів виступають ЦЗ в форматі без втрат (TIFF), а у другому – ЦЗ в форматі з

втратами (JPG). Очевидно, що при розробці стеганоаналітичного методу, що дозволяє відокремлювати незаповнені контейнери від СП, слід визначати і використовувати різні порогові значення для різних форматів, а, отже, безпосередньо перед процесом стеганоаналізу необхідно з'ясувати, в якому форматі початково зберігався оригінальний контейнер, адже в результаті вбудови ДІ у просторову область цифрових контентів методом LSB всі СП зберігаються в форматі без втрат. Можливість відокремлення ЦЗ, які початково зберігалися в форматі без втрат, від ЦЗ, Perezбережених в формат без втрат після стиску з втратами, обґрунтована в роботі [133], алгоритмічна реалізація запропонованого в [133] підходу може бути використана як складова частина розроблюваного стеганоаналітичного методу, однак запропонований в [133] підхід здійснює аналіз області перетворень цифрових контентів, що може призвести до накопичення додаткової обчислювальної похибки, і є небажаним, тому в розділі 3 буде розроблений метод виявлення формату (з/без втрат) оригінального контейнера, що аналізує просторову область цифрових контентів. Застосування метода виявлення формату контейнерів дозволить покращити результати стеганоаналізу розробленим в роботі методом завдяки вибору різних порогових значень для форматів без втрат і форматів з втратами.

2.3. Стеганоаналітичний метод для аналізу відеопослідовності, послідовності зображень, заснований на кількісному аналізі зміни числа блоків з однаковими значеннями яскравості

До теперішнього часу стеганоаналітичні методи, комплекси у більшості своїй були розраховані на окремо взяті ЦЗ, залишаючи підходи для рішення задачі стеганоаналізу відеопослідовності, послідовності ЦЗ менш розробленими, а саму задачу актуальною.

Розглянемо можливість використання для стеганоаналізу цифрового відео підходу, заснованого на врахуванні зміни кількості блоків виду (2.2), запропонованого вище.

Нехай стеганоперетворення кадрів цифрового відео (послідовності ЦЗ) здійснюється з незмінним значенням ППС.

З отриманих результатів обчислювального експерименту (табл. 2.2, 2.3, рис. 2.1) випливає, що результати первинного і повторного стеганоперетворення послідовності ЦЗ (см. середні значення (стовпці IV_i в табл.2.2, V_i в табл.2.3)) кількісно відрізняються одне від одного настільки, що дають можливість відокремити незаповнені контейнери від СП (найбільш яскраво ця відмінність проявляється для ЦЗ груп 2-5). З урахуванням цього проведення стеганографічного аналізу здійснюється шляхом стеганоперетворення послідовності, що аналізується, методом LSB. По відносній зміні кількості блоків виду (2.2) в отриманому СП, у порівнянні з контентом, що аналізується, робиться висновок про те, первинним або повторним було це стеганоперетворення, тобто здійснюється детектування наявності або констатація відсутності вбудованої ДІ у послідовності кадрів ЦВ, ЦЗ, що аналізуються.

Необхідно відзначити, що, як видно з табл. 2.3, зміни кількості блоків виду (2.2), що фіксуються в ЦЗ в форматах без втрат при повторному стеганоперетворенні, порівняні одне з одним при різних використаних при проведенні експерименту значеннях ППС (як при первинної, так і при повторної вбудові ДІ). Якщо в якості контейнерів виступають ЦЗ в форматі з втратами, значення відносної зміни порівняні одне з одним для ППС 0.5 и 0.25 біт/піксель. У випадку ППС 0.1 біт/піксель ці значення декілька вище, що, проте, не вплине на висновок про наявність/відсутність ДІ, оскільки навіть такі значення набагато нижче тих, які отримуються при первинній вбудові ДІ.

У відповідності до отриманих результатів обчислювального експерименту, сформулюємо основні кроки стеганоаналітичного методу для виявлення наявності/відсутності вкладення ДІ у ЦВ/послідовності ЦЗ.

Для послідовності з P кадрів ЦВ (послідовності P ЦЗ) C_1, C_2, \dots, C_P з кольорними складовими $R_i^{(c)}, G_i^{(c)}, B_i^{(c)}$ основні кроки стеганоаналітичного

методу (CAM1) детектування наявності/відсутності ДІ, вбудованої методом LSB, наступні:

Крок 1. Визначення формату оригінального контейнеру для вибору порогових значень, що використовуються на наступних кроках.

Крок 2. Вбудова ДІ (випадково сформованої бінарної послідовності). Для кожного C_i , $i = \overline{1, P}$: вбудувати у $Y_i^{(C)} \in \{R_i^{(C)}, G_i^{(C)}, B_i^{(C)}\}$ - колірні складові C_i методом LSB ДІ з ППС t біт/піксель, $t \in \{0.5, 0.25, 0.1\}$. Результат - S_i^t з колірними складовими $Y_i^{(t)} \in \{R_i^{(t)}, G_i^{(t)}, B_i^{(t)}\}$.

Крок 3. Для $i = \overline{1, P}$:

- 3.1. Визначити $ky_i^{(C)}$, $ky_i^{(C)} \in \{kr_i^{(C)}, kg_i^{(C)}, kb_i^{(C)}\}$ - кількість 4×4 -блоків виду (2.2) у $Y_i^{(C)} \in \{R_i^{(C)}, G_i^{(C)}, B_i^{(C)}\}$ відповідно;
- 3.2. Визначити $ky_i^{(t)}$, $ky_i^{(t)} \in \{kr_i^{(t)}, kg_i^{(t)}, kb_i^{(t)}\}$, $t \in \{0.5, 0.25, 0.1\}$ - кількість 4×4 -блоків виду (2.2) у $Y_i^{(t)} \in \{R_i^{(t)}, G_i^{(t)}, B_i^{(t)}\}$ відповідно.

Крок 4. Для $i = \overline{1, P}$:

- 4.1. Обчислити $ry_i^{(C)}$, $ry_i^{(C)} \in \{rr_i^{(C)}, rg_i^{(C)}, rb_i^{(C)}\}$ - відносну кількість 4×4 -блоків у $Y_i^{(C)} \in \{R_i^{(C)}, G_i^{(C)}, B_i^{(C)}\}$ відповідно (у %);
- 4.2. Обчислити $ry_i^{(t)}$, $ry_i^{(t)} \in \{rr_i^{(t)}, rg_i^{(t)}, rb_i^{(t)}\}$, $t \in \{0.5, 0.25, 0.1\}$ - відносну кількість 4×4 -блоків у $Y_i^{(t)} \in \{R_i^{(t)}, G_i^{(t)}, B_i^{(t)}\}$ відповідно (у %).

Крок 5. Визначити:

$$\overline{ry}^{(C)} = \frac{1}{P} \sum_{i=1}^P ry_i^{(C)}; \overline{ry}^{(t)} = \frac{1}{P} \sum_{i=1}^P ry_i^{(t)},$$

де $\overline{ry}^{(C)}$, $\overline{ry}^{(t)}$ - середні значення кількості (%) 4×4 -блоків виду (2.2) по всім ЦЗ/кадрам ЦВ відповідно для C_i та S_i^t , $\overline{ry}^{(C)} \in \{\overline{rr}^{(C)}, \overline{rg}^{(C)}, \overline{rb}^{(C)}\}$, $\overline{ry}^{(t)} \in \{\overline{rr}^{(t)}, \overline{rg}^{(t)}, \overline{rb}^{(t)}\}$, $t \in \{0.5, 0.25, 0.1\}$.

Крок 6. Обчислити:

$$\bar{Y}_t = \frac{|\overline{ry}^{(C)} - \overline{ry}^{(t)}|}{\overline{ry}^{(C)}} \cdot 100\%,$$

де \bar{Y}_t - зміни середнього значення кількості 4×4 -блоків виду (2.2) відповідних колірних складових C_i у порівнянні з S_i^t , $\bar{Y}_t \in \{\bar{R}_t, \bar{G}_t, \bar{B}_t\}$, $t \in \{0.5, 0.25, 0.1\}$.

Крок 7. Детектування наявності ДІ.

Якщо

$$\begin{aligned} & (\bar{Y}_{t_1} < T_Y \text{ AND } \bar{Y}_{t_2} < T_Y) \text{ OR } (\bar{Y}_{t_1} < T_Y \text{ AND } \bar{Y}_{t_3} < T_Y) \text{ OR} \\ & (\bar{Y}_{t_2} < T_Y \text{ AND } \bar{Y}_{t_3} < T_Y) \text{ OR } (\bar{Y}_{t_1} < T_Y \text{ AND } \bar{Y}_{t_2} < T_Y \text{ AND } \bar{Y}_{t_3} < T_Y), \end{aligned}$$

де $\bar{Y}_t \in \{\bar{R}_t, \bar{G}_t, \bar{B}_t\}$, $t_j \in t \in \{0.5, 0.25, 0.1\}$, $T_Y \in \{T_R, T_G, T_B\}$,

то C_1, C_2, \dots, C_p містять вбудовану ДІ у Y -ій колірній складовій, $Y \in \{R, G, B\}$,

інакше ДІ відсутня у Y -ій колірній складовій C_1, C_2, \dots, C_p ,

де $T_Y \in \{T_R, T_G, T_B\}$ – порогові значення для кожної колірної складової, які визначаються на основі результатів обчислювального експерименту у відповідності з табл. 2.3. Для контейнерів в форматах з втратами та контейнерів в форматах без втрат (рис. 2.1, б, г) ці значення повинні відрізнятися. Порогові значення T_R , T_G , T_B рекомендується приймати однаковими для різних значень ППС, оскільки, по-перше, при стеганоаналізі початково невідомо значення ППС, з яким здійснювалась вбудова ДІ, а по-друге, відносні зміни кількості блоків виду (2.2) при первинній вбудові ДІ в один контейнер можуть співпадати з відносними змінами блоків в СП, сформованого на основі іншого контейнеру. Це, в свою чергу, призведе до неоднозначності результатів детектування і додатковому виникненню помилок першого і другого роду. Значення порогів T_R , T_G , T_B будуть визначені в розділі 4 на основі експериментальної апробації стеганоаналітичного алгоритму, що реалізує запропонований метод.

Реалізація кроку 1 може відбуватися за рахунок використання методу відокремлення ЦЗ, Perezбереженого в формат без втрат з формату з втратами, від ЦЗ, що зберігалося в форматі без втрат початково, розробленого в розділі 3, у випадку кольорових цифрових контентів, а також метода, запропонованого в [133], для випадків цифрових контейнерів в градаціях сірого.

Слід відзначити, що аналіз кількості 4×4 -блоків виду (2.2) здійснюється окремо для матриці кожної колірної складової кадру ЦВ незалежно від двох інших, таким чином, розроблений метод може використовуватися для детектування як кольорових ЦВ, так і відеопослідовностей в градаціях сірого.

Основним недоліком запропонованого методу є залежність кількості блоків з однаковими значеннями яскравості від виду контейнеру. Для ЦЗ, навіть у випадку великого розміру, яке містить дуже багато дрібних деталей, кількість блоків виду (2.2) є дуже незначною (аж до 0), що значно ускладнює процес стеганоаналізу. Для ЦВ з малим розміром кадрів запропонований підхід може виявитися недостатньо ефективним, зважаючи на початково порівняно невелику кількість блоків у кадрі. Згідно САМ1 для ЦВ спочатку визначаються відносні зміни кількості блоків виду (2.2) для кожного кадру, після чого обчислюється їх середнє значення, що, з врахуванням початково невисокої кількості блоків в кадрі, може не дати очікуваної відмінності значень відносних змін при первинній і повторній вбудові ДІ. З урахуванням вище сказаного запропонований підхід необхідно удосконалити з метою можливості виявлення вкладень ДІ у ЦВ з малим розміром кадру, що буде зроблено в наступному підрозділі.

Ефективність алгоритмічної реалізації стеганоаналітичного методу досліджується в розділі 4.

2.4. Стеганоаналітичний метод, заснований на врахуванні характеру зміни кількості блоків з однаковими значеннями яскравості в результаті первинної і повторної вбудови додаткової інформації

У минулому підрозділі розроблено стеганоаналітичний метод, заснований на порівнянні зміни відносної кількості блоків з однаковими значеннями яскравості в результаті первинної і повторної вбудови ДІ у послідовність ЦЗ/відеопослідовність, однак, як було зазначено вище, область застосування методу САМ1 обмежена розмірами кадрів ЦВ.

З метою розширення області застосування запропонованого стеганоаналітичного підходу, а саме коректного виявлення вкладень ДІ в ЦВ з кадрами малого розміру, визначимо параметр, що якісно характеризує зміни кількості блоків з однаковими значеннями яскравості (зменшення, збільшення або незмінність) в результаті первинної та повторної вбудови ДІ в цифрові контенти. Далі таку якісну характеристику будемо називати *характером зміни кількості блоків виду (2.2)*.

Проведемо обчислювальний експеримент, що аналізує характер змін кількості 4×4 -блоків з однаковими значеннями яскравості у послідовності ЦЗ/відеопослідовності в результаті первинної і повторної вбудови ДІ.

На першому етапі обчислювального експерименту проводилась оцінка характеру зміни (зменшення, збільшення чи незмінність) кількості 4×4 -блоків з однаковими значеннями яскравості в колірних складових оригінальних ЦЗ після вбудови ДІ методом LSB. Кожна колірна складова контейнера досліджувалась окремо, однак характер змін для будь-яких колірних складових виявився аналогічний, тому в подальшому будемо мати на увазі, що результати обчислювального експерименту застосовні як для червоної, так і для зеленої та синьої колірних матриць. Результати першого етапу експерименту представлені у табл. 2.4, де стовпець I відповідає ППС при первинній вбудові ДІ; II – характеру зміни кількості блоків виду (2.2); позначення \downarrow - зменшенню кількості блоків виду (2.2), \uparrow - збільшенню

кількості блоків виду (2.2), \leftrightarrow - незмінної кількості блоків виду (2.2).
Кількісний показник характеру змін визначається за формулами:

$$p_{\downarrow} = \frac{k_{\downarrow}}{P} \cdot 100\%, p_{\uparrow} = \frac{k_{\uparrow}}{P} \cdot 100\%, p_{\leftrightarrow} = \frac{k_{\leftrightarrow}}{P} \cdot 100\%, \quad (2.13)$$

де $p_{\downarrow}, p_{\uparrow}, p_{\leftrightarrow}$ – відсоток матриць, у яких кількість 4×4 -блоків з однаковими значеннями яскравості при вбудові ДІ зменшується, збільшується та залишається незмінним відповідно;

$k_{\downarrow}, k_{\uparrow}, k_{\leftrightarrow}$ – кількість матриць у послідовності ЦЗ/кадрах ЦВ, у яких кількість 4×4 -блоків з однаковими значеннями яскравості при вбудові ДІ зменшується, збільшується та залишається незмінним відповідно;

P – загальна кількість матриць у послідовності, що аналізується.

Таблиця 2.4 – Характер зміни кількості 4×4 -блоків з однаковими значеннями яскравості при первинній вбудові ДІ по всьому набору зображень, %

I	II	Група 1	Група 2	Група 3	Група 4	Група 5
0.5	↓	34.9301	40.3134	92.2824	82.2554	91.6279
	↑	40.9182	47.1510	4.9261	12.2720	7.9070
	↔	24.1517	12.5356	2.7915	5.4726	0.4651
0.25	↓	39.7206	43.4473	92.7750	86.2355	93.9535
	↑	33.9321	40.5983	4.5977	8.4577	5.4264
	↔	26.3473	15.9544	2.6273	5.3068	0.6201
0.1	↓	43.7126	46.0114	92.7750	88.8889	96.2791
	↑	27.3453	34.4729	3.4483	4.8093	2.6356
	↔	28.9421	19.5157	3.7767	6.3018	1.0853

Як видно з табл. 2.4 при первинній вбудові ДІ у контейнери в форматах без втрат (групи 1, 2) незалежно від ППС у середньому в 40% матриць спостерігається зменшення кількості 4×4 -блоків виду (2.2). У зображеннях в форматах з втратами (групи 3-5) доля матриць зі зменшеною кількістю 4×4 -блоків досягає 80% та вище.

На другому етапі обчислювального експерименту проводилась оцінка характеру змін кількості 4×4 -блоків виду (2.2) у колірних складових СП, отриманих в результаті первинної вбудови ДІ у контейнер методом LSB, та СП, отриманих в результаті повторної вбудови ДІ у дане СП. Результати експерименту представлені у табл. 2.5, де стовпець I відповідає ППС при первинній вбудові ДІ; II – ППС при повторній вбудові ДІ; III - характеру зміни кількості блоків виду (2.2). Характер змін визначається за формулою (2.13).

Таблиця 2.5 – Характер зміни кількості 4×4 -блоків з однаковими значеннями яскравості при повторній вбудові ДІ по всьому набору зображень, %

I	II	III	Група 1	Група 2	Група 3	Група 4	Група 5
0.5	0.5	↓	0	0	0	0	0
		↑	55.8882	72.0798	71.5928	73.6318	81.7054
		↔	44.1118	27.9202	28.4072	26.3682	18.2946
	0.25	↓	0	0	0	0	0
		↑	52.4950	65.6695	33.9901	63.1841	56.8992
		↔	47.5050	34.3305	66.0099	36.8159	43.1008
	0.1	↓	0	0	0	0	0
		↑	46.5070	60.2564	26.7652	55.7214	51.1628
		↔	53.4930	39.7436	73.2348	44.2786	48.8372

Продовження табл. 2.5

I	II	III	Група 1	Група 2	Група 3	Група 4	Група 5
0.25	0.5	↓	0.1996	0	0.1642	0	2.0155
		↑	57.2854	73.7892	41.2151	71.4760	67.1318
		↔	42.5150	26.2108	58.6207	28.5240	30.8527
	0.25	↓	0.3992	0	0.1642	0	1.7054
		↑	54.0918	68.0912	39.4089	67.1642	65.8915
		↔	45.5090	31.9088	60.4269	32.8358	32.4031
	0.1	↓	0.1996	0	0	0	1.7054
		↑	49.1018	60.8262	29.5567	55.2239	54.2636
		↔	50.6986	39.1738	70.4433	44.7761	44.0310
0.1	0.5	↓	20.3593	20.2279	64.5320	41.4594	63.4109
		↑	50.4990	62.9630	18.8834	45.2736	31.6279
		↔	29.1417	16.8091	16.5846	13.2670	4.9612
	0.25	↓	21.7565	22.6496	68.1445	48.0929	67.4419
		↑	46.7065	55.6980	13.7931	35.1575	25.8915
		↔	31.5370	21.6524	18.0624	16.7496	6.6666
	0.1	↓	15.7685	17.6638	41.3793	34.1625	44.1860
		↑	46.9062	54.2735	45.8128	50.9121	51.4729
		↔	37.3253	28.0627	12.8079	14.9254	4.3411

З табл. 2.5 видно, що після повторної вбудови ДІ у СП помітно знижується відсоток колірних матриць зі зменшеною кількістю 4×4 -блоків з однаковими значеннями яскравості (аж до 0%, особливо, якщо ППС при первинній вбудові складала 0.5 і 0.25 біт/піксель), що призводить до зростання відсотку матриць зі збільшеною та незмінною кількістю 4×4 -блоків виду (2.2). Притому, це спостереження характерне як для контейнерів в форматах без втрат, так і для контейнерів в форматах з втратами.

У випадку, коли первинна вбудова здійснювалась з ППС 0.5 біт/піксель, а також для деяких груп при ППС 0.25 біт/піксель, після повторної вбудови ДІ зменшення кількості блоків виду (2.2) не спостерігалось зовсім (у табл. 2.5 значення 0 для ↓). Це пов'язано з великою щільністю вкладення ДІ при первинній вбудові, в результаті чого 4×4-блоків виду (2.2) в матрицях колірних складових практично не залишається, адже при ППС 0.5 біт/піксель в 4×4-блоці виду (2.2) змінюються до 8-ми значень з 16, а при ППС 0.25 біт/піксель – до 4-х значень. І якщо у випадку вбудови ДІ з ППС 0.25 біт/піксель зберігається ймовірність того, що 4×4-блок з однаковими значеннями яскравості не зміниться і при повторній вбудові ДІ кількість таких блоків ще може зменшитися, то у випадку ППС 0.5 біт/піксель ймовірність збереження в матриці колірних складових блоків виду (2.2) практично нульова, тому в результаті повторної вбудови ДІ не спостерігається зменшення кількості 4×4-блоків з однаковими значеннями яскравості.

Однак у випадку малих значень ППС (0.125 біт/піксель та менше) після первинної вбудови ДІ в матрицях колірних складових залишається достатня кількість 4×4-блоків виду (2.2), в результаті повторної вбудови ДІ таких блоків стане ще менше, що видно в табл. 2.5 у випадку ППС 0.1 біт/піксель при первинній вбудові ДІ. Це може служити основою недостатньої ефективності виявлення ДІ, вбудованої при малих значеннях ППС, оскільки із-за залежності кількості блоків виду (2.2) від специфіки контейнера можлива ситуація, коли характер зміни кількості 4×4-блоків з однаковими значеннями яскравості для різних контейнерів буде зіставним у випадку первинної і повторної вбудови ДІ.

Проте, на основі характеру змін кількості 4×4-блоків виду (2.2) більшості елементів (ЦЗ, кадрів ЦВ) послідовності можна зробити висновок про наявність/відсутність ДІ у цифровому контенті, що аналізується. З врахуванням проведених досліджень характеру зміни кількості блоків виду (2.2) основні кроки стеганоаналітичного методу (SAM2) наступні:

Кроки 1, 2 відповідають крокам 2, 3 відповідно методу САМ1.

Крок 3. Визначення характеру змін кількості 4×4 -блоків виду (2.2) у кожній колірній складовій.

Для $i = \overline{1, P}$:

$$dY_i^{(t)} = ky_i^{(C)} - ky_i^{(t)},$$

де $dY_i^{(t)} \in \{dR_i^{(t)}, dG_i^{(t)}, dB_i^{(t)}\}$, $t \in \{0.5, 0.25, 0.1\}$, $ky_i^{(C)} \in \{kr_i^{(C)}, kg_i^{(C)}, kb_i^{(C)}\}$,
 $ky_i^{(t)} \in \{kr_i^{(t)}, kg_i^{(t)}, kb_i^{(t)}\}$.

Крок 4. Визначити загальну кількість матриць ЦЗ/кадрів ЦВ, у яких спостерігається зменшення кількості 4×4 -блоків з однаковими значеннями яскравості у кожній колірній складовій.

Для $i = \overline{1, P}$:

Якщо $dY_i^{(t)} > 0$, то $kY_i^{(t)} = kY_i^{(t-1)} + 1$ ($kY_i^{(t)}$ - кількість матриць у послідовності зі зменшенням кількості 4×4 -блоків виду (2.2)), де $t \in \{0.5, 0.25, 0.1\}$, $dY_i^{(t)} \in \{dR_i^{(t)}, dG_i^{(t)}, dB_i^{(t)}\}$, при цьому відповідно $kY_i^{(t)} \in \{kR_i^{(t)}, kG_i^{(t)}, kB_i^{(t)}\}$, початкові значення $kY_i^{(0)} = 0$.

Крок 5. Обчислити:

$$pY_i^{(t)} = \frac{kY_i^{(t)}}{P} \cdot 100\%,$$

де $pY_i^{(t)} \in \{pR_i^{(t)}, pG_i^{(t)}, pB_i^{(t)}\}$, $kY_i^{(t)} \in \{kR_i^{(t)}, kG_i^{(t)}, kB_i^{(t)}\}$, $t \in \{0.5, 0.25, 0.1\}$.

Крок 6. Детектування вкладення ДІ.

Якщо

$$\begin{aligned} & (pY_i^{(t_1)} \leq T \text{ AND } pY_i^{(t_2)} \leq T) \text{ OR } (pY_i^{(t_1)} \leq T \text{ AND } pY_i^{(t_3)} \leq T) \text{ OR} \\ & (pY_i^{(t_2)} \leq T \text{ AND } pY_i^{(t_3)} \leq T) \text{ OR} \end{aligned}$$

$$(pY_i^{(t_1)} \leq T \text{ AND } pY_i^{(t_2)} \leq T \text{ AND } pY_i^{(t_3)} \leq T),$$

де $pY_i^{(t)} \in \{pR_i^{(t)}, pG_i^{(t)}, pB_i^{(t)}\}$, $t_j \in \{t_1 = 0.5, t_2 = 0.25, t_3 = 0.1\}$,

то C_1, C_2, \dots, C_P містять вбудовану ДІ у Y -ій колірній складовій,
 $Y \in \{R, G, B\}$;

інакше ДІ відсутня у Y -ій колірній складовій C_1, C_2, \dots, C_P ,

де T – порогове значення, яке визначається з врахуванням результатів, наведених в табл. 2.5.

Поріг T використовується для оцінки кількості кадрів (%) в ЦВ (зображень в послідовності ЦЗ), у яких спостерігалось зменшення кількості блоків при повторної вбудові ДІ. Порогове значення T буде визначено в розділі 4 на основі експериментальної апробації стеганоаналітичного алгоритму, що реалізує запропонований метод.

Слід зазначити, що аналіз кількості 4×4 -блоків виду (2.2) здійснюється окремо для кожної матриці кожної колірної складової кадру ЦВ незалежно від двох інших, таким чином, розроблений метод може використовуватися для детектування як кольорових ЦВ, так і відеопослідовностей в градаціях сірого. І SAM1, і SAM2 дозволяють виявляти ДІ у послідовностях ЦЗ/кадрах ЦВ за умови заповнення усіх кадрів/ЦЗ при постійній колірній складовій, однак для забезпечення прихованості ДІ може вбудовуватися лише в частину кадрів відеопослідовності, що потребує удосконалення розроблених методів, направлених на забезпечення можливості покадрового аналізу ЦВ, аналізу ЦЗ, що буде зроблено в розділі 3.

І метод SAM1, і SAM2 мають однакові можливості для стеганоаналізу, а саме: дозволяють аналізувати окремі колірні складові кольорових ЦВ і ЦВ в градаціях сірого, виявляти наявність ДІ, вбудованої у декілька колірних складових, крім цього SAM2, на відміну від SAM1, дозволяє детектувати вбудову ДІ у ЦВ з малим розміром кадру. Формулювання практичних рекомендацій для застосування розроблених методів і розробка на їх основі комплексного методу виявлення вкладення ДІ в ЦВ будуть проведені в розділі 4.

2.5. Висновки до розділу 2

В розділі 2 розроблені стеганоаналітичні методи виявлення результатів вбудови ДІ методом LSB у цифрові контенти (ЦВ і послідовності ЦЗ) шляхом аналізу їх просторової області.

Отримані наступні результати:

1. Отриманий критерій належності єдиного ненульового СНЧ блока матриці ЦЗ множині натуральних чисел, на основі якого розроблений теоретичний базис для стеганоаналітичних методів, що аналізують просторову область цифрових контентів.
2. Отримані кількісні оцінки вмісту блоків з однаковими значеннями яскравості у колірних складових оригінальних ЦЗ. Встановлено, що зі зростанням розміру блока незалежно від групи, формату, колірної складової ЦЗ кількість блоків, що мають єдине ненульове сингулярне число, що належить множині натуральних чисел, в матриці монотонно зростає.
3. Обраний і обґрунтований розмір блоку матриці ЦЗ (кадру ЦВ) - 4×4 , найбільш інформативний з точки зору використання встановленого критерію належності єдиного ненульового СНЧ блока матриці ЦЗ множині натуральних чисел для рішення задач стеганоаналізу.
4. Розроблений стеганоаналітичний метод, направлений на виявлення наявності/відсутності ДІ в цифрових відеопослідовностях, послідовностях ЦЗ за умови її вбудови методом LSB в одну постійну колірну складову контейнера. Метод заснований на врахуванні відносних змін кількості 4×4 -блоків з однаковими значеннями яскравості в матрицях колірних складових кадрів ЦВ при первинній і повторній вбудові ДІ і може застосовуватися для детектування як кольорових ЦВ, так і відеопослідовностей в градаціях сірого, однак може виявитися недостатньо ефективним у випадку використання в якості контейнера ЦВ з малим розміром кадру, а також окремих ЦЗ.
5. Для розширення можливості стеганоаналізу ЦВ з малим розміром кадру розроблений стеганоаналітичний метод, заснований на врахуванні характеру змін кількості 4×4 -блоків з однаковими значеннями яскравості в матрицях колірних складових при первинній і повторній вбудові ДІ у цифрові відеопослідовності за умови вбудови ДІ методом

LSB в одну постійну колірну складову контейнера. Метод може використовуватись для детектування як кольорових ЦВ, так і відеопослідовностей в градаціях сірого.

Таким чином, в розділі 2 частково вирішені задачі 2 і 3 з переліку задач дисертаційної роботи. Основні результати даного розділу опубліковані в роботах [126, 134-138].

Акһтаметіева Анна

РОЗДІЛ 3

РОЗРОБКА СТЕГАНОАНАЛІТИЧНОГО МЕТОДУ ДЛЯ АНАЛІЗУ ЦИФРОВИХ ЗОБРАЖЕНЬ

У розділі 2 був запропонований стеганоаналітичний підхід виявлення вбудованої інформації, заснований на врахуванні кількості блоків з однаковими значеннями яскравості, однак розроблені на його основі методи можуть недостатньо ефективно детектувати вкладення ДІ в окремих ЦЗ/кадрах цифрових відео.

Як показав обчислювальний експеримент, багато ЦЗ як в форматах без втрат, так і в форматах з втратами або не містять блоки з однаковими значеннями яскравості, або містять незначну їх кількість, що при повторній вбудові ДІ помітно не впливає на відносну зміну кількості блоків виду (2.2). Такі ЦЗ характеризуються високим вмістом контурів і дрібних деталей, в результаті чого в їх матрицях відсутні блоки з однаковими значеннями яскравості. Крім того, якщо первинна вбудова ДІ здійснювалась з малою ППС (0.05-0.125 біт/піксель) можлива ситуація, коли блоки з однаковими значеннями яскравості залишаються неторкнутими, або в результаті стеганоперетворення такі блоки випадковим чином можуть з'явитися. Більш того, в проведеному обчислювальному експерименті середнє значення кількості блоків з однаковими значеннями яскравості визначається по всім ЦЗ у групі, тобто для послідовності ЦЗ (формула (2.10)), однак, якщо розглядати вміст 4×4 - блоків виду (2.2) в окремих ЦЗ, то їх кількість напряму залежить від специфіки контейнера – чим більше контурів і дрібних деталей є в зображенні, тим менше зустрічається блоків з однаковими значеннями яскравості, що в свою чергу, може негативно сказатися на ефективності детектування окремих ЦЗ (як з точки зору помилок першого роду, так і помилок другого роду), якщо основою для цього детектування буде виступати виключно аналіз зміни кількості блоків виду (2.2).

Мета розділу: розробка стеганоаналітичного методу виявлення наявності/відсутності ДІ, вбудованої методом LSB, в окремих ЦЗ/кадрах відеопослідовності, що здійснює аналіз просторової області контенту, ефективний, у тому числі, в умовах малої ППС.

В даному розділі в якості контейнера, цифрового контенту розглядається окремо взяте кольорове ЦЗ або кадр ЦВ (схема RGB).

Для досягнення мети необхідно вирішити *задачі*:

1. Установити в просторовій області таке сукупне представлення пікселів цифрового контенту, яке забезпечувало б виявлення модифікацій значень яскравості пікселів ЦЗ/кадру ЦВ при вбудові ДІ методом LSB в одну довільну колірну складову контейнеру;
2. Виявити характерні особливості збурення матриці унікальних кольорів СП, сформованих вбудовою ДІ методом LSB в одну довільну колірну складову контейнеру;
3. Розробити стеганоаналітичний метод, що здійснює аналіз просторової області кольорових контентів в умовах вбудови ДІ методом LSB в одну довільну колірну складову контейнера, заснований на врахуванні вмісту послідовних тріад триплетів в матриці унікальних кольорів, спроможний, у тому числі, для малих значень ППС;
4. Розробити метод, що використовує для аналізу просторову область та дозволяє відокремлювати цифрові контенти, Perezбережені з формату з втратами у формат без втрат, від цифрових контентів, що початково зберігалися в форматі без втрат.

3.1. Удосконалення стеганоаналітичного підходу, заснованого на аналізі кольорів

Сучасні стеганоаналітичні методи, що здійснюють аналіз кольорового ЦЗ у просторовій області, часто використовують аналіз пар кольорів [85-89], де кожний колір визначається пікселем $pc(i, j)$, $i = \overline{1, M}$, $j = \overline{1, N}$, ЦЗ розміру $M \times N$, що представляється значеннями яскравості червоної, зеленої і синьої

колірних складових в діапазоні $[0, 255]$, тобто триплетом значень (r_{ij}, g_{ij}, b_{ij}) .

В указаному підході обчислюються і порівнюються відношення $R_{CP} = \frac{P_{CP}}{U}$ і

$R'_{CP} = \frac{P'_{CP}}{U'}$, де P_{CP} і P'_{CP} – число близьких пар кольорів в оригінальному ЦЗ і

СП відповідно; U і U' – число різних триплетів (r_{ij}, g_{ij}, b_{ij}) в оригінальному

ЦЗ і СП відповідно. Під близькими парами кольорів для ЦЗ розуміють такі

два триплети (r_{ij}, g_{ij}, b_{ij}) і (r_{kl}, g_{kl}, b_{kl}) , для яких виконуються співвідношення

[89]:

$$\begin{cases} |r_{ij} - r_{kl}| \leq 2, \\ |g_{ij} - g_{kl}| \leq 2, \\ |b_{ij} - b_{kl}| \leq 2 \end{cases} \Leftrightarrow (r_{ij} - r_{kl})^2 + (g_{ij} - g_{kl})^2 + (b_{ij} - b_{kl})^2 \leq 12 \quad (3.1)$$

для ЦЗ в форматі з втратами і

$$\begin{cases} |r_{ij} - r_{kl}| \leq 1, \\ |g_{ij} - g_{kl}| \leq 1, \\ |b_{ij} - b_{kl}| \leq 1 \end{cases} \Leftrightarrow (r_{ij} - r_{kl})^2 + (g_{ij} - g_{kl})^2 + (b_{ij} - b_{kl})^2 \leq 3 \quad (3.2)$$

для ЦЗ в форматі без втрат.

Недоліком даного підходу є неможливість точного визначення порога відношень R_{CP} для всіх зображень в силу різних варіацій унікальних кольорів U , яке може суттєво відрізнятись для ЦЗ з високою і низькою ступеню стиску. Крім того, існуюче до теперішнього моменту поняття близьких пар є дуже узагальненим. Якщо розглянути, наприклад, варіанти триплетів виду (r_{ij}, g_{ij}, b_{ij}) і $(r_{ij} + 1, g_{ij}, b_{ij})$ або виду (r_{ij}, g_{ij}, b_{ij}) і $(r_{ij} + 2, g_{ij} - 2, b_{ij} + 1)$, то очевидно, що у першому випадку кольори ближче

один до одного, ніж у другому випадку, при цьому обидві пара будуть визнані близькими згідно формули (3.1).

Для удосконалення стеганоаналітичного підходу, основанийого на аналізі кольорів, проведемо аналіз того, які модифікації зазнає піксель цифрового контенту при вбудові ДІ методом LSB в одну колірну складову.

Нехай стеганоперетворення здійснюється методом LSB Matching, реалізованим у відповідності до формули [139]:

$$c'(i, j) = \begin{cases} c(i, j) + 1, & \text{if } b \neq LSB(c(i, j)) \ \& \ r > 0, \\ c(i, j), & \text{if } b = LSB(c(i, j)), \\ c(i, j) - 1, & \text{if } b \neq LSB(c(i, j)) \ \& \ r < 0, \end{cases} \quad (3.3)$$

де $c(i, j)$, $c'(i, j)$ – значення яскравості пікселя у колірній складовій оригінального ЦЗ і СП відповідно; b – біт секретного повідомлення; r – випадкова величина в діапазоні $[-1;1]$; $LSB(c(i, j))$ – найменший значущий біт $c(i, j)$ [139]. Таким чином, при вбудові ДІ значення яскравості пікселя оригінальної матриці або збільшиться на 1, або зменшиться на 1, або залишиться незмінним.

У випадку, коли вбудова ДІ здійснюється в одну довільну колірну складову триплету (r_{ij}, g_{ij}, b_{ij}) , модифікується лише один його елемент, наприклад при вбудові ДІ у червону колірну складову модифікований триплет представляє собою $(r'_{ij}, g_{ij}, b_{ij})$. Якщо триплет (r_{ij}, g_{ij}, b_{ij}) , що розглядається, зустрічається у зображенні неодноразово, зростає ймовірність того, що перша його складова може бути змінена всіма трьома способами: $+1, -1, 0$. Аналогічно з двома іншими колірними складовими триплету.

Для виявлення можливої наявності/відсутності ДІ в контенті, що аналізується, розміром $M \times N$ формується матриця CT (color triplets) розміром $L \times 3$, $L = MN$, що містить триплети $(r_{ij}, g_{ij}, b_{ij}) = (\tilde{r}_l, \tilde{g}_l, \tilde{b}_l)$, що зустрічаються в ЦЗ, де перетворення $(i, j) \rightarrow l$ індексів елементів матриці

колірної складової здійснюється за формулою $l = N(i-1) + j$, $i = \overline{1, M}$, $j = \overline{1, N}$, $l = \overline{1, L}$. При цьому слід зазначити, що триплети можуть повторюватись, в залежності від того, скільки разів вони зустрічаються в зображенні. Вбудова ДІ тягне за собою зміни значень складових триплету, що може призвести до появи нових триплетів, що формують нові кольори, та зникненню тих, що мають, тому з метою виявлення модифікацій триплетів, що відбуваються при вбудові ДІ, потребується матриця, що містить усі триплети, що мають в ЦЗ, без урахування їх повторів.

Визначення 3.1. Усі різні триплети значень $(r_{i,j}, g_{i,j}, b_{i,j})$, $i = \overline{1, M}$, $j = \overline{1, N}$, в межах ЦЗ будемо називати унікальними кольорами.

Кількість унікальних кольорів позначимо U .

Визначення 3.2. Матрицею унікальних кольорів UCT (unique color triplets) будемо називати матрицю розміром $U \times 3$ унікальних кольорів $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$.

Таким чином, матриця UCT представляє собою послідовність унікальних кольорів, які хоч раз зустрічаються в ЦЗ, що аналізується. При цьому матриця унікальних кольорів не враховує частоту появи триплету $(\check{r}_k, \check{g}_k, \check{b}_k) \in UCT$ в ЦЗ.

В результаті вбудови ДІ змінюються значення яскравостей пікселів, ці зміни відображаються на вмісті матриці унікальних кольорів, оскільки вбудова ДІ призводить не лише до появи нових триплетів, а й модифікації існуючих триплетів, які в початковому виді можуть бути відсутніми в UCT . Для ілюстрації зробленого припущення розглянемо на прикладі триплетів $(\check{r}_k, \check{g}_k, \check{b}_k - 3)$, $(\check{r}_k, \check{g}_k, \check{b}_k)$, $(\check{r}_k, \check{g}_k, \check{b}_k + 2)$, як відіб'ється на матриці унікальних кольорів їх модифікація при вбудові ДІ. Нехай ДІ вбудовується у синю колірну складову, і триплети модифікуються у відповідності з рис. 3.1, в результаті в матриці унікальних кольорів СП з'явилися додаткові кольори, що утворюють дві послідовні (з урахуванням третьої складової) тройки

триpletів: $(\check{r}_k, \check{g}_k, \check{b}_k - 2)$, $(\check{r}_k, \check{g}_k, \check{b}_k - 1)$, $(\check{r}_k, \check{g}_k, \check{b}_k)$ – обведені жовтогарячим кольором, і $(\check{r}_k, \check{g}_k, \check{b}_k - 1)$, $(\check{r}_k, \check{g}_k, \check{b}_k)$, $(\check{r}_k, \check{g}_k, \check{b}_k + 1)$ – обведені червоним кольором. Слід відзначити, що такі послідовні тройки триpletів (тріади триpletів) можуть перетинатися: триплети $(\check{r}_k, \check{g}_k, \check{b}_k - 1)$ і $(\check{r}_k, \check{g}_k, \check{b}_k)$ входять в обидві утворені в результаті стеганоперетворення послідовні тройки. Таким чином, можна припустити, що матриця унікальних кольорів СП буде містити більше послідовних тріад триpletів, ніж матриця унікальних кольорів контейнера, що може сигналізувати про модифікації яскравості кольорних складових ЦЗ.

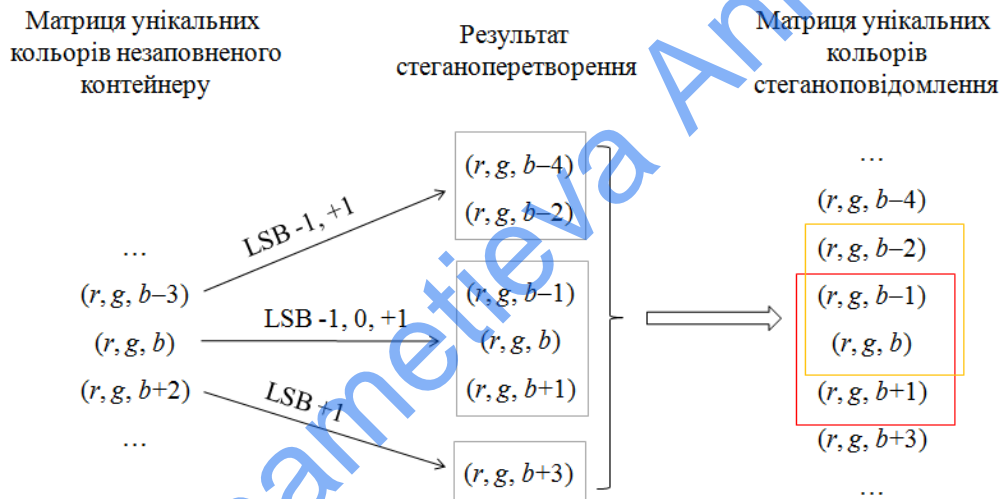


Рис. 3.1 – Модифікація унікальних кольорів в результаті вбудови ДІ у синю колірну складову

Введемо наступні визначення.

Визначення 3.3. Послідовними Red- (Green-, Blue-) тріадами триpletів у матриці унікальних кольорів будемо називати тріади:

$$(\check{r}_k, \check{g}_k, \check{b}_k) \in UCT \ \& \ (\check{r}_k - 1, \check{g}_k, \check{b}_k) \in UCT \ \& \ (\check{r}_k + 1, \check{g}_k, \check{b}_k) \in UCT, \ k = \overline{1, U}; \quad (3.4)$$

$$(\check{r}_k, \check{g}_k, \check{b}_k) \in UCT \ \& \ (\check{r}_k, \check{g}_k - 1, \check{b}_k) \in UCT \ \& \ (\check{r}_k, \check{g}_k + 1, \check{b}_k) \in UCT, \ k = \overline{1, U}; \quad (3.5)$$

$$(\check{r}_k, \check{g}_k, \check{b}_k) \in UCT \ \& \ (\check{r}_k, \check{g}_k, \check{b}_k - 1) \in UCT \ \& \ (\check{r}_k, \check{g}_k, \check{b}_k + 1) \in UCT, \ k = \overline{1, U}; \quad (3.6)$$

відповідно. При підрахуванні кількості послідовних триад триплетів будемо асоціювати послідовну триаду з $(\check{r}_k, \check{g}_k, \check{b}_k) \in UCT$, для якого виконуються умови (3.4), (3.5) або (3.6) в залежності від виду триади. Триплет $(\check{r}_k, \check{g}_k, \check{b}_k) \in UCT$ будемо називати *середнім*, якщо для нього існує послідовна триада.

Визначення 3.4. Основними триадами триплетів будемо називати послідовні триади, що відповідають тій колірній складовій контейнера, у яку здійснюється вбудова ДІ.

Визначення 3.5. Супутніми триадами триплетів будемо називати такі послідовні триади, які відповідають незаповненим ДІ колірним складовим контейнера.

Проведемо обчислювальний експеримент, що аналізує вміст послідовних Red-, Green- і Blue-триад триплетів у незаповнених цифрових контейнерах. В якості контейнерів виступають ЦЗ з БЦЗ. В обчислювальному експерименті для кожного незаповненого ЦЗ відповідної групи формується матриця унікальних кольорів, у якої для кожного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$, проводиться перевірка умов (3.4)-(3.6), при виконанні яких виконується підрахунок кількості середніх триплетів v_r, v_g, v_b (%) по відношенню до загальної кількості унікальних кольорів U для послідовних Red-, Green- і Blue-триад триплетів відповідно. В табл. 3.1 наведені результати обчислювального експерименту, де стовпець I відповідає видам послідовних триад триплетів (R – Red-тріадам триплетів, G – Green-тріадам триплетів, B – Blue-тріадам триплетів); Π_i – максимальним значенням v_r, v_g, v_b відповідно по i -ої групі ЦЗ з БЦЗ; III_i – середнім значенням v_r, v_g, v_b відповідно по i -ої групі.

Таблиця 3.1 – Кількість послідовних тріад триплетів в матриці унікальних кольорів незаповнених ЦЗ, %

I	Група 1		Група 2		Група 3		Група 4		Група 5	
	II ₁	III ₁	II ₂	III ₂	II ₃	III ₃	II ₄	III ₄	II ₅	III ₅
R	76.40	46.83	81.66	54.29	5.57	0.69	8.88	1.24	4.13	1.03
G	76.06	46.27	81.77	54.12	9.08	1.26	11.25	1.79	4.69	1.37
B	76.53	46.53	79.55	54.74	4.87	0.78	7.27	0.71	3.74	0.99

Як видно з табл. 3.1, матриця унікальних кольорів незаповнених ЦЗ в форматі з втратами (групи 3-5) містить у середньому не більше 3% послідовних тріад триплетів, при цьому максимальний вміст середніх триплетів не перевищує 12%. Зовсім інша ситуація спостерігається для груп 1-2 (формат без втрат TIFF), де вміст середніх триплетів, на відміну від формату з втратами, початково високий (у середньому 40-60%), що пояснюється відсутністю стиску і, як наслідок, великою різноманітністю унікальних кольорів. Слід відзначити, що кількість Red-, Green- і Blue-тріад триплетів у матриці унікальних кольорів незаповнених ЦЗ є зіставною за значеннями: різниця між ними складає не більше 1-1.5%.

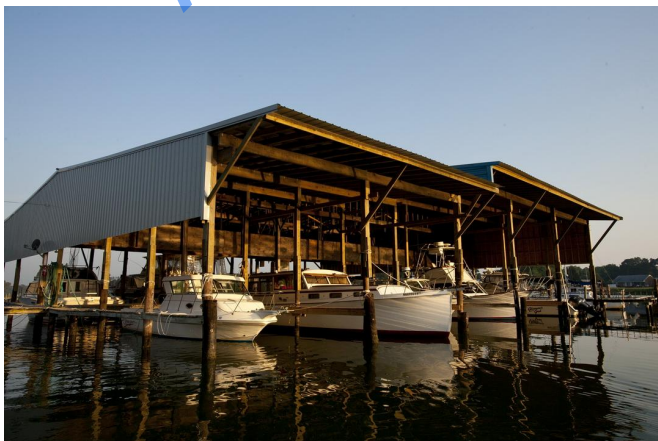
Проаналізуємо, як зміниться кількість послідовних тріад триплетів у матриці унікальних кольорів СП, сформованих вбудовою ДІ в одну довільну колірну складову контейнерів з БЦЗ з ППС 0.5 біт/піксель, при цьому для різних ЦЗ колірна складова обирається довільно. Результати експерименту наведені в табл. 3.2, де стовпець I відповідає видам послідовних тріад триплетів; II_i – максимальним значенням v_r, v_g, v_b відповідно по *i*-ої групі ЦЗ з БЦЗ; III_i – середнім значенням v_r, v_g, v_b відповідно по *i*-ої групі.

Таблиця 3.2 – Кількість послідовних тріад триплетів в матриці унікальних кольорів СП, сформованих вбудовою ДІ в одну довільну колірну складову цифрових контентів з ППС 0.5 біт/піксель, %

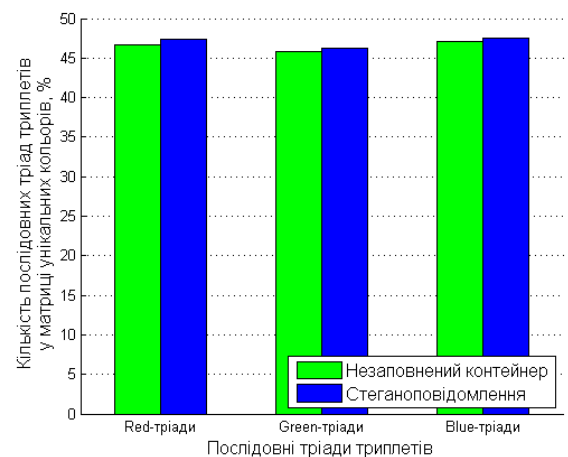
I	Група 1		Група 2		Група 3		Група 4		Група 5	
	II ₁	III ₁	II ₂	III ₂	II ₃	III ₃	II ₄	III ₄	II ₅	III ₅
R	76.51	52.75	81.60	55.67	39.26	15.23	38.99	14.62	39.91	15.89
G	76.25	52.95	81.72	56.30	45.68	22.99	45.63	21.07	46.72	24.15
B	76.53	53.29	79.45	57.34	56.94	23.24	54.57	21.31	55.08	23.40

З табл. 3.2 видно, що вбудова ДІ в контейнери призводить до зростання кількості послідовних тріад триплетів по всім групам, однак найбільш помітне відносне зростання характерне для груп 3-5, що відповідають формату з втратами. У випадку контейнерів в форматі без втрат (група 1-2) зміни у кількості тріад триплетів кожного окремого ЦЗ незначні.

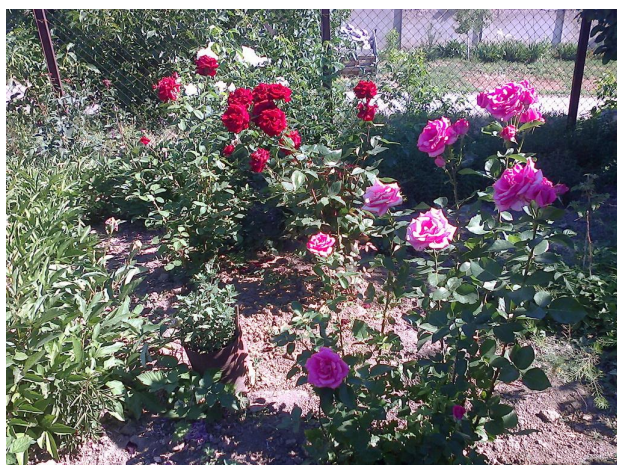
Наглядною ілюстрацією зміни кількості послідовних тріад у матриці унікальних кольорів служить рис. 3.2, де в ЦЗ (рис. 3.2, а, в) ДІ вбудовувалась лише в червону (для прикладу) колірну складову з ППС 0.5 біт/піксель. Стовпці діаграми (рис. 3.2, б, г) відображають зміни кількості Red-, Green-, Blue-тріад триплетів у СП у порівнянні з незаповненими контейнерами.



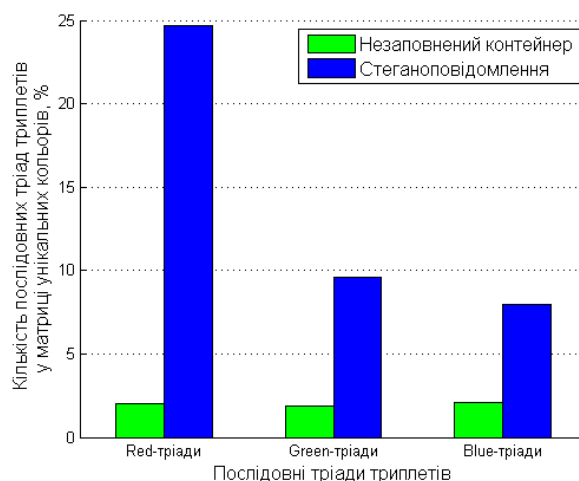
а



б



В



Г

Рис. 3.2 – Кількість послідовних тріад триплетів в зображенні: а – ЦЗ в форматі TIFF з групи 1; б – кількість тріад в контейнері і СП; в – ЦЗ в форматі JPG з групи 5; г – кількість тріад в контейнері і СП

Проаналізуємо, за рахунок чого спостерігається така значна розбіжність у зміні кількості послідовних тріад триплетів в матрицях унікальних ЦЗ, що зберігаються в форматі без втрат, і ЦЗ в форматі з втратами в результаті стеганоперетворення.

Для ЦЗ в форматі без втрат (TIFF) внаслідок відсутності квантування частотних коефіцієнтів блоків матриця унікальних кольорів містить велику кількість унікальних кольорів, які незначно відрізняються один від одного (не більше ніж на 1). У ЦЗ в форматі з втратами (JPG) в результаті квантування і округлення коефіцієнтів ДКП блоків, отриманих в результаті стандартного розбиття матриці, обнуляються СНЧ, що відповідають високим і (можливо) середнім частотам [140], що при переході у просторову область відображається на значеннях яскравості колірних складових, зменшуючи кількість різних триплетів.

Для ілюстрації вище сказаного розглянемо матрицю унікальних кольорів ЦЗ (рис. 3.2, а) в форматі TIFF (оригінал) і отриманого на його основі зображення в форматі JPG при максимальній якості стиску ($Q=100$).

Фрагменти матриці унікальних кольорів наведені на рис. 3.3, де вертикальні лінії синього кольору указують на Blue-тріади триплетів.

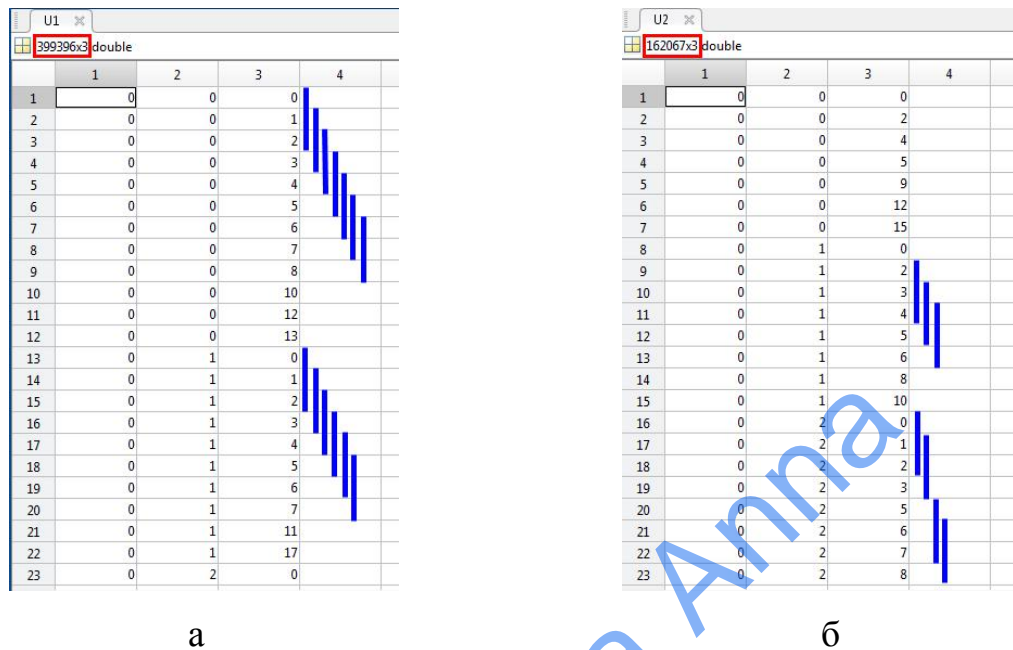


Рис. 3.3 – Матриця унікальних кольорів (фрагмент) ЦЗ: а – оригінала в форматі без втрат; б – оригінала, перезбереженого в форматі з втратами

У даному прикладі матриця унікальних кольорів оригіналу містить 399396 унікальних кольорів, 46.73% середніх триплетів Red-тріад, 45.8% середніх триплетів Green-тріад, 47.1% середніх триплетів Blue-тріад, у той час як матриця унікальних кольорів отриманого на його основі Jpeg-ЦЗ містить лише 162067 унікальних кольорів, що в 2.464 рази менше оригіналу, і зовсім незначну, у порівнянні з оригіналом, кількість середніх триплетів: 1.88% Red-тріад, 2.74% Green-тріад, 1.05% Blue-тріад. Наведений приклад відображає типічну картину стану послідовних тріад триплетів для ЦЗ, збережених в форматі з/без втрат.

При вбудові ДІ в контейнер, що початково зберігається в форматі з втратами (рис. 3.2, в), відбувається помітне зростання кількості послідовних тріад триплетів в матриці унікальних кольорів (рис. 3.2, г), особливо сильним є зростання кількості послідовних Red-тріад триплетів, що відповідають червоної колірної складової, куди здійснювалась вбудова ДІ. Якщо такі

збурення кількості послідовних тріад триплетів при вбудові ДІ характерні для всіх ЦЗ в форматах з втратами, то на основі виявлення подібних збурень можна буде відокремлювати незаповнені контейнери від СП.

З метою відокремлення ЦЗ, які початково зберігалися в форматі з втратами, від СП, сформованих вбудовою ДІ в одну колірну складову ЦЗ, у тому числі з малою ППС, необхідно визначити діапазони для кількості середніх триплетів відносно до загального числа унікальних кольорів (%) в незаповнених контейнерах, адже, як вже говорилось вище, різниця між кількістю середніх триплетів Red-, Green- і Blue-тріад в матриці унікальних кольорів незаповнених ЦЗ складає не більше 1-1.5%. Розподіл кількості середніх триплетів (%) для всіх незаповнених ЦЗ з груп 3-5 відображає рис. 3.4.



Рис. 3.4 – Кількість послідовних тріад триплетів в матрицях унікальних кольорів оригінальних ЦЗ: а – з групи 3; б – з групи 4; в – з групи 5

Як видно з рис. 3.4, у більшості незаповнених контейнерів в форматі з втратами кількість середніх триплетів (всіх видів) складає від 0 до 3% від загальної кількості унікальних кольорів, на основі чого можна зробити висновок, що низький вміст послідовних тріад триплетів характерний для контейнерів в форматі з втратами.

Розглянемо детальніше, як буде змінюватися кількість послідовних тріад при вбудові ДІ з малими значеннями ППС. Для цього проведемо обчислювальний експеримент, що аналізує вміст послідовних тріад триплетів в матриці унікальних кольорів СП, сформованих вбудовою ДІ з ППС 0.5, 0.25, 0.167, 0.125, 0.1 и 0.05 біт/піксель. В експерименті здійснюється підрахунок кількості Red-, Green- і Blue-тріад триплетів, що обумовлено тим, що в процесі стеганоаналізу, як правило, невідомо, в яку саме колірну складову була вбудована ДІ. З урахуванням того, що матриця унікальних кольорів незаповнених ЦЗ в форматі з втратами містить в основному від 0 до 3% середніх триплетів (рис. 3.4), і кількість Red-, Green- і Blue-тріад є зіставними за значеннями, детальніше розглянемо, як розподіляються по діапазнам - $[0, 1)$, $[1, 2)$, $[2, 3)$ або $[3, 100]$ кількість послідовних тріад триплетів в матрицях унікальних кольорів незаповнених контейнерів і СП, сформованих вбудовою ДІ в одну довільну колірну складову (для різних ЦЗ використовувались різні колірні складові). Для цього здійснюється підрахунок кількості Red-, Green- і Blue-тріад триплетів в матриці унікальних кольорів всіх незаповнених ЦЗ і всіх СП, сформованих вбудовою ДІ в одну довільну колірну складову з різними значеннями ППС, по кожній групі ЦЗ. Після чого визначається, скільки значень кількості послідовних тріад триплетів відносно загального числа значень належить діапазнам $[0, 1)$, $[1, 2)$, $[2, 3)$ або $[3, 100]$ у відповідній групі ЦЗ. Результати експерименту наведені в табл. 3.3 для різних значень ППС відповідних груп ЦЗ.

Таблиця 3.3 – Кількість значень вмісту послідовних тріад триплетів, що входять в діапазони [0, 1), [1, 2), [2, 3) або [3,100] в залежності від групи ЦЗ і значень ППС відносно загального числа значень, %

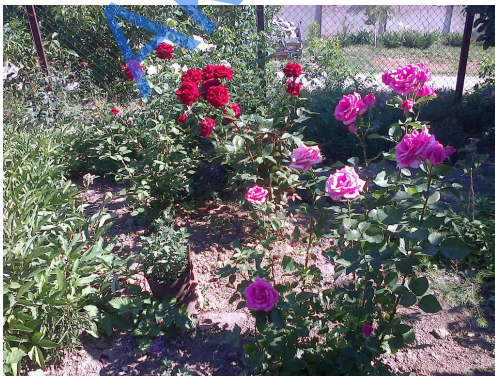
	Діапазон	ППС, біт/піксель						
		0.5	0.25	0.167	0.125	0.1	0.05	0
Група 3	[0, 1)	0	0.16	0.33	0.49	1.48	4.60	64.04
	[1, 2)	0.49	3.12	6.08	6.57	6.57	6.57	25.94
	[2, 3)	6.24	3.78	1.97	2.30	3.28	6.73	6.90
	[3,100]	93.27	92.94	91.63	90.64	88.67	82.10	3.12
Група 4	[0, 1)	0	0	0.50	0.83	2.82	5.14	57.88
	[1, 2)	1.33	3.65	3.15	6.30	5.31	8.62	20.07
	[2, 3)	3.15	4.31	5.31	5.47	6.30	10.78	13.10
	[3,100]	95.52	92.04	91.04	87.40	85.57	75.46	8.96
Група 5	[0, 1)	0	0	0	0	0	1.24	52.09
	[1, 2)	0.16	1.09	2.95	4.03	6.51	5.74	29.30
	[2, 3)	4.34	4.81	3.72	3.26	2.95	5.74	14.73
	[3,100]	95.50	94.11	93.33	92.71	90.54	87.29	3.88

Як видно з табл. 3.3, більшість значень кількості послідовних тріад (як основних, так і супутніх) в матриці унікальних кольорів СП перевищує 3%, на відміну від незаповнених контейнерів, де число значень, що входять в діапазон [3,100] не перевищує 9% від усіх значень кількості послідовних тріад триплетів. Таким чином, при вбудові ДІ в контейнери, що зберігаються в форматі з втратами, навіть з малими значеннями ППС відбувається значне зростання кількості послідовних тріад триплетів, що дозволить виявляти наявність/відсутність ДІ в цифровому контенті, що аналізується.

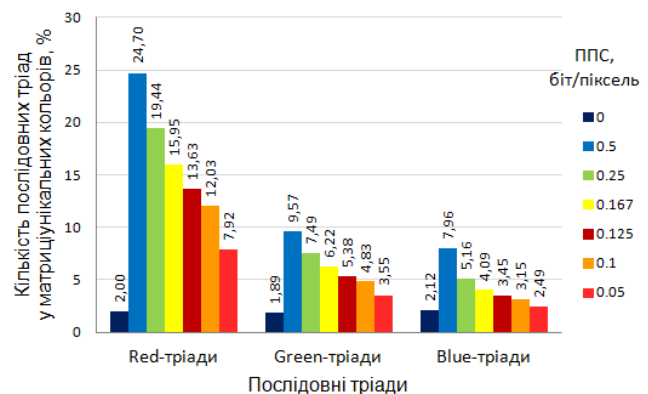
Наглядною ілюстрацією зробленого висновку служить рис. 3.5, де в ЦЗ (рис. 3.5, а) ДІ вбудовувалась лише в червону колірну складову з різними значеннями ППС. В матриці унікальних кольорів сформованого СП

проведений підрахунок кількості Red-, Green- і Blue-триад. Вміст середніх триплетів Red-, Green- і Blue-триад по відношенню до загальної кількості унікальних кольорів для СП, сформованого вбудовою ДІ в червону колірну складову з різними значеннями ППС, наведено на рис. 3.5, б. Аналогічно, визначений вміст Red-, Green- і Blue-триад в матрицях унікальних кольорів СП, сформованих вбудовою ДІ лише в зелену колірну складову (рис. 3.5, в) і лише в синю колірну складову (рис. 3.5, г).

Як видно з рис. 3.5, вбудова ДІ в одну довільну колірну складову викликає найбільше зростання вмісту основних триад. При цьому зростає і кількість супутніх триад, однак помітно менше у порівнянні з вмістом основних триад в матриці унікальних кольорів СП (супутніх триад приблизно в 1.5-2 рази менше основних). Таке зростання пов'язане зі збільшенням кількості унікальних кольорів при вбудові ДІ. Наприклад, при вбудові ДІ у синю колірну складову унікальний триплет (10, 158, 74) модифікований у Blue-триаду (10, 158, 73), (10, 158, 74) і (10, 158, 75), при цьому в матриці унікальних кольорів контейнера існують триплети (11, 158, 75) і (12, 158, 75). У цьому випадку новий триплет (10, 158, 75) разом з існуючими триплетами (11, 158, 75) і (12, 158, 75) утворює Red-триаду, притому, що в червону колірну складову вбудова не відбувалася.



а



б

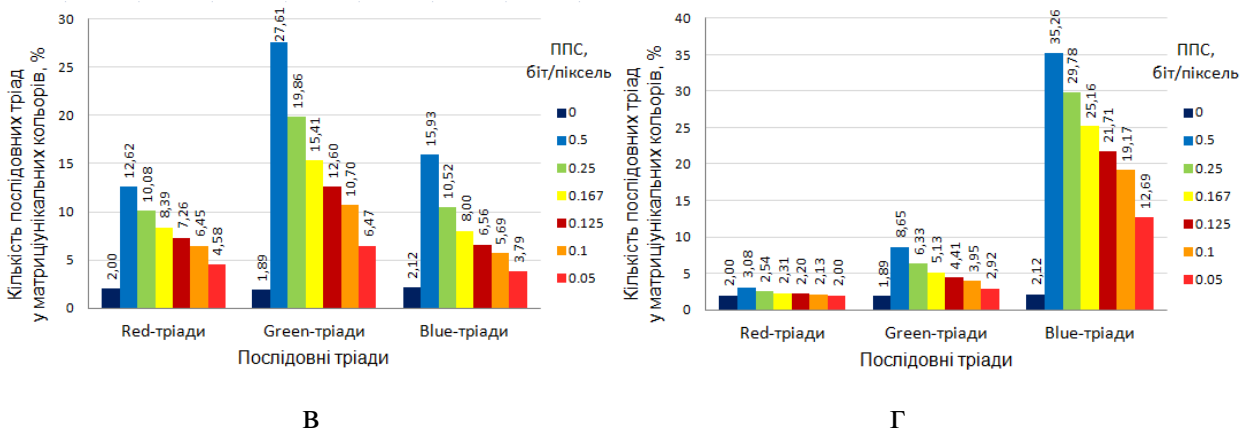


Рис. 3.5 – Кількість послідовних колірних тріад в зображенні: а – оригінальне ЦЗ; б – кількість тріад у СП, сформованому вбудовою ДІ методом LSB в червону колірну складову; в – кількість тріад у СП, сформованому вбудовою ДІ методом LSB в зелену колірну складову; г – кількість тріад у СП, сформованому вбудовою ДІ методом LSB в синю колірну складову

Таким чином, враховуючи незначний вміст послідовних тріад триплетів у незаповнених контейнерах в форматі з втратами і значне збільшення основних тріад після вбудови в контейнер ДІ, можна розраховувати на ефективне виявлення наявності/відсутності ДІ в ЦЗ/окремих кадрах ЦВ (причому з визначенням конкретної колірної складової, яка зазнала стеганоперетворення), засноване на аналізі просторової області контенту – кількості послідовних тріад триплетів.

3.2. Стеганоаналітичний метод виявлення вбудови додаткової інформації у цифрове зображення/кадр цифрового відео, заснований на аналізі послідовних колірних тріад

На основі встановлених особливостей зміни кількості колірних тріад в матриці унікальних кольорів сформулюємо основні кроки стеганоаналітичного методу (САМЗ) для виявлення вкладки ДІ методом LSB в ЦЗ I розміром $M \times N$ з колірними складовими R, G, B :

Крок 1. Формування матриці UCT розміром $U \times 3$ унікальних триплетів кольорів $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ для ЦЗ I .

Крок 2. Підрахування кількості послідовних тріад триплетів для кожної колірної складової.

2.1. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k + 1, \check{g}_k, \check{b}_k)$ і $(\check{r}_k - 1, \check{g}_k, \check{b}_k)$, то $countR = countR + 1$, $countR$ – кількість Red-тріад в UCT;

2.2. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k, \check{g}_k + 1, \check{b}_k)$ і $(\check{r}_k, \check{g}_k - 1, \check{b}_k)$, то $countG = countG + 1$, $countG$ – кількість Green-тріад в UCT;

2.3. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k, \check{g}_k, \check{b}_k + 1)$ і $(\check{r}_k, \check{g}_k, \check{b}_k - 1)$, то $countB = countB + 1$, $countB$ – кількість Blue-тріад в UCT.

Крок 3. Обчислити кількість середніх триплетів послідовних тріад відносно загальної кількості унікальних кольорів (%):

$$pR = \frac{countR}{U} \cdot 100, \quad pG = \frac{countG}{U} \cdot 100, \quad pB = \frac{countB}{U} \cdot 100;$$

$$p_{\max} = \max(pR, pG, pB),$$

де p_{\max} – максимальне значення серед pR, pG, pB .

Крок 4. Детектування наявності/відсутності ДІ.

4.1. Якщо $(pR = p_{\max}) \text{ AND } (pR > T_{up})$,

то I містить вбудовану ДІ у червоній колірній складовій;

інакше якщо

$$((pR > T_{low}) \text{ OR } (pG > T_{low}) \text{ OR } (pB > T_{low})) \text{ AND}$$

$$((pR > 1.5 \cdot pG) \text{ AND } (pR > 1.5 \cdot pB))$$

то I містить вбудовану ДІ у червоній колірній складовій;

інакше ДІ відсутня у червоній колірній складовій;

4.2. Якщо $(pG = p_{\max}) \text{ AND } (pG > T_{up})$,

то I містить вбудовану ДІ у зеленій колірній складовій,

інакше якщо

$$\begin{aligned} & ((pR > T_{low}) \text{ OR } (pG > T_{low}) \text{ OR } (pB > T_{low})) \text{ AND} \\ & ((pG > 1.5 \cdot pR) \text{ AND } (pG > 1.5 \cdot pB)) \end{aligned}$$

то I містить вбудовану ДІ у зеленій колірній складовій;

інакше ДІ відсутня у зеленій колірній складовій;

4.3. *Якщо* $(pB = p_{max}) \text{ AND } (pB > T_{up}),$

то I містить вбудовану ДІ у синій колірній складовій,

інакше якщо

$$\begin{aligned} & ((pR > T_{low}) \text{ OR } (pG > T_{low}) \text{ OR } (pB > T_{low})) \text{ AND} \\ & ((pB > 1.5 \cdot pR) \text{ AND } (pB > 1.5 \cdot pG)) \end{aligned}$$

то I містить вбудовану ДІ у синій колірній складовій,

інакше ДІ відсутня у синій колірній складовій;

де T_{low} і T_{up} – порогові значення. Порогове значення T_{low} характеризує максимальну кількість середніх триплетів (%) у незаповнених контейнерах і обирається з урахуванням табл. 3.3, неперевикнення T_{low} усіма послідовними тріадами триплетів зображення, що аналізується, свідчить про оригінальне ЦЗ. Порог T_{up} характеризує мінімальну кількість середніх триплетів (%) в СП, перевищення T_{up} усіма послідовними тріадами триплетів зображення, що аналізується, свідчить про СП. Значення порогів T_{low} і T_{up} будуть визначені у розділі 4 на основі експериментальної апробації ефективності стеганоаналітичного алгоритму, що реалізує запропонований метод.

Запропонований стеганоаналітичний метод не тільки дозволяє виявляти вкладення ДІ в окремих ЦЗ, але й розширює можливості детектування ЦВ, здійснюючи покадровий стеганоаналіз відеопослідовностей, що особливо актуально у випадках, коли в результаті стеганоперетворення заповнюється лише частина кадрів.

Ефективність алгоритмічної реалізації стеганоаналітичного методу для ЦЗ досліджується в розділі 4.

3.3. Адаптація стеганоаналітичного методу SAM3 для виявлення вбудови додаткової інформації в цифрових відео за умови заповнення усіх кадрів

Для забезпечення можливості використання розробленого методу SAM3 для ЦВ за умови вбудови ДІ у всі кадри відео послідовності (далі таке стеганоперетворення будемо називати повним), адаптуємо його, позначаючи далі результат адаптації як стеганоаналітичний метод SAM3v, для виявлення вкладення ДІ у ЦВ.

Позначення, що використовуються в SAM3v:

$F_z, z = \overline{1, P}$ – кадр відеопослідовності V , що аналізується та містить P кадрів розміром $M \times N$.

$resultF$ – матриця розміром $P \times 3$, що містить результат детектування по кожному кадру відеопослідовності. Перший стовпець матриці $resultF$ відповідає червоної, другий – зеленої, третій – синьої колірним складовим. Значення елементів матриці $resultF_z, j \in \{1, 2, 3\}, z = \overline{1, P}$, відповідають 1, при наявності ДІ у відповідній (j -ої) колірної складової кадру F_z , 0 – при її відсутності.

UCT – матриця унікальних кольорів кадру F_z розміром $U \times 3$, що містить унікальні триплети $(\check{r}_k, \check{g}_k, \check{b}_k), k = \overline{1, U}$.

$countR, countG, countB$ – кількість послідовних триад триплетів в UCT для червоної, зеленої і синьої колірних складових кадру F_z відповідно.

pR, pG, pB – відносний вміст середніх триплетів в UCT по відношенню до загальної кількості унікальних кольорів для червоної, зеленої та синьої колірних складових відповідно.

p_{\max} – максимальне значення серед pR, pG, pB .

$kY_{pos}^j \in \{kR_{pos}, kG_{pos}, kB_{pos}\}$ – кількість кадрів, визнаних як таких, що містять вбудовану ДІ, у j -ій, $j \in \{1, 2, 3\}$, колірної складової кадрів.

$kY_{neg}^j \in \{kR_{neg}, kG_{neg}, kB_{neg}\}$ – кількість кадрів, визнаних як таких, що не містять вбудовану ДІ, у j -ій, $j \in \{1, 2, 3\}$, колірної складової кадрів, де 1, 2, 3 асоціюються з червоною, зеленою та синьою колірними складовими відповідно.

Стеганоаналітичний метод САМЗv:

Крок 1. Для кожного кадру F_z , $z = \overline{1, P}$, здійснюється детектування наявності в ньому ДІ:

1.1. Формування матриці унікальних кольорів UCT .

1.2. Підрахунок кількості Red-, Green-, Blue-триад триплетів.

1.2.1. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k + 1, \check{g}_k, \check{b}_k)$ и $(\check{r}_k - 1, \check{g}_k, \check{b}_k)$, то $countR = countR + 1$;

1.2.2. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k, \check{g}_k + 1, \check{b}_k)$ и $(\check{r}_k, \check{g}_k - 1, \check{b}_k)$, то $countG = countG + 1$;

1.2.3. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k, \check{g}_k, \check{b}_k + 1)$ и $(\check{r}_k, \check{g}_k, \check{b}_k - 1)$, то $countB = countB + 1$.

1.3. Обчислити:

$$pR = \frac{countR}{U} \cdot 100, \quad pG = \frac{countG}{U} \cdot 100, \quad pB = \frac{countB}{U} \cdot 100,$$

$$p_{\max} = \max(pR, pG, pB).$$

1.4. Детектування наявності/відсутності ДІ в окремому кадрі відеопослідовності.

1.4.1. Якщо $(pR = p_{\max}) \text{ AND } (pR > T_{up})$

$$\text{то } result_{F_{z,1}} = 1,$$

інакше якщо

$$\left((pR > T_{low}) \text{ OR } (pG > T_{low}) \text{ OR } (pB > T_{low}) \right) \text{ AND} \\ \left((pR > 1.5 \cdot pG) \text{ AND } (pR > 1.5 \cdot pB) \right)$$

то $resultF_{z,1} = 1$,

інакше $resultF_{z,1} = 0$;

1.4.2. Якщо $(pG = p_{max}) \text{ AND } (pG > T_{up})$

то $resultF_{z,2} = 1$,

інакше якщо

$$\left((pR > T_{low}) \text{ OR } (pG > T_{low}) \text{ OR } (pB > T_{low}) \right) \text{ AND} \\ \left((pG > 1.5 \cdot pR) \text{ AND } (pG > 1.5 \cdot pB) \right)$$

то $resultF_{z,2} = 1$,

інакше $resultF_{z,2} = 0$;

1.4.3. Якщо $(pB = p_{max}) \text{ AND } (pB > T_{up})$

то $resultF_{z,3} = 1$,

інакше якщо

$$\left((pR > T_{low}) \text{ OR } (pG > T_{low}) \text{ OR } (pB > T_{low}) \right) \text{ AND} \\ \left((pB > 1.5 \cdot pR) \text{ AND } (pB > 1.5 \cdot pG) \right)$$

то $resultF_{z,3} = 1$,

інакше $resultF_{z,3} = 0$.

Крок 2. Підрахування кількості позитивних (1) та негативних (0) результатів детектування у кадрах відеопослідовності окремо для кожної колірної складової в матриці $resultF$:

Якщо $resultF_{z,j} = 1$

то $kY_{pos}^j = kY_{pos}^j + 1$,

інакше $kY_{neg}^j = kY_{neg}^j + 1$.

Крок 3. Детектування наявності ДІ у відеопослідовності:

Якщо $kY_{pos}^j \geq kY_{neg}^j$

то ДІ міститься у j -ій колірній складовій,
інакше ДІ відсутня у j -ій колірній складовій.

Розроблений метод може бути використаний для стеганоаналізу ЦВ, послідовностей ЦЗ, збережених в форматах з втратами.

Ефективність алгоритмічної реалізації стеганоаналітичного методу досліджується в розділі 4.

3.4. Метод визначення формату контейнера, що використовується в процесі стеганоперетворення

В процесі стеганоперетворення в якості контейнерів можуть виступати цифрові контенти як в форматі з втратами, так і в форматі без втрат. Після вбудови ДІ у просторову область контейнеру методом LSB СП зберігаються в форматі без втрат, тобто при стеганоаналізі мається, як правило, цифровий контент в форматі без втрат при відсутності оригінального контейнеру. Можливість відокремлення ЦЗ, збереженого в форматі без втрат початково, від ЦЗ, перезбережених в форматі без втрат з формату з втратами, може підвищити ефективність стеганоаналізу, указавши на проведену з ЦЗ дію.

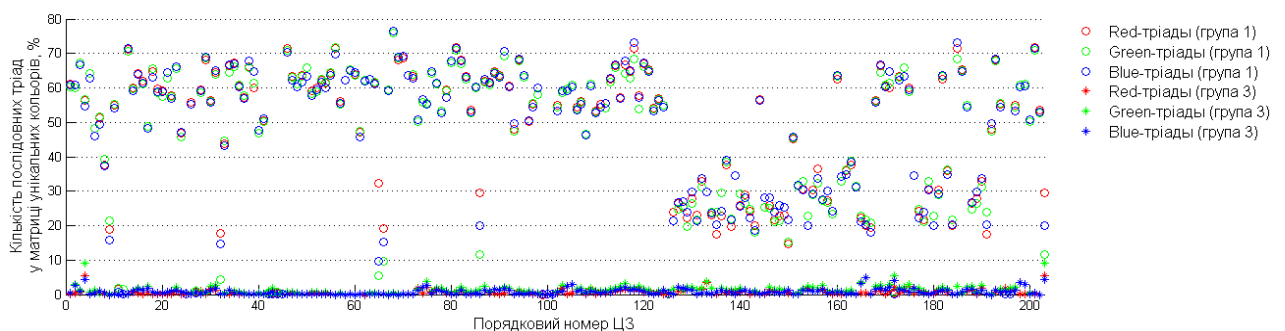
Задача визначення формату вхідного контейнеру є суттєвою в даній роботі: для розробленого методу SAM1 (розділ 2.3) потребується вибір різних порогових значень T_R , T_G , T_B в залежності від формату контейнеру; розроблені методи SAM3 і SAM3v (розділ 3.2, 3.3) розраховані на контейнери в форматі з втратами. В роботі [133] запропонований підхід для відокремлення ЦЗ, перезбережених в формат без втрат з формату з втратами, від ЦЗ, початково збережених в форматі без втрат, однак, як показав обчислювальний експеримент, проведений автором, для різних технічних пристроїв з різними матрицями квантування отримані протилежні результати, що потребує наявності даних про матриці квантування різних пристроїв і відповідних до них співвідношень для забезпечення ефективної роботи алгоритму, що реалізує даний підхід. Крім того, запропонований в [133] метод передбачає перехід в область перетворень, що може призвести до

накопичення обчислювальної похибки, тому розробка аналогічного методу, що здійснює аналіз просторової області, є актуальною задачею. Проте, перевагою запропонованого підходу є можливість його застосування для цифрових контентів в градаціях сірого.

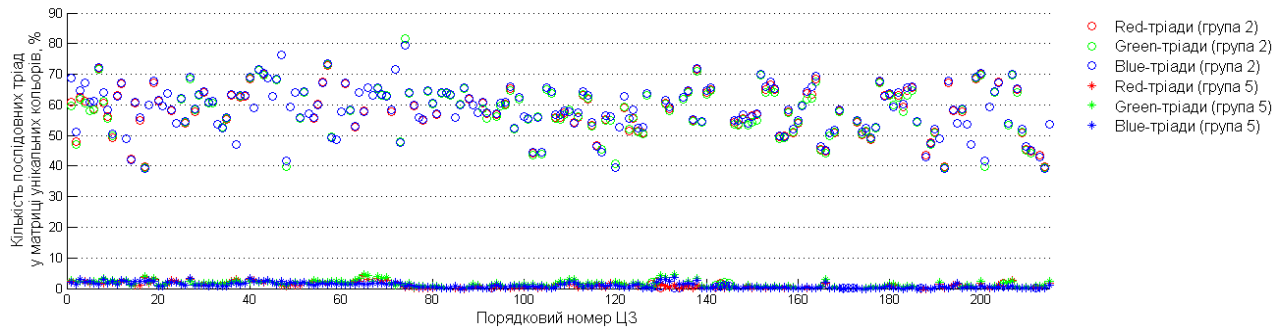
В результаті дослідження, направлено на виявлення збурень кількості послідовних тріад триплетів у матриці унікальних кольорів після вбудови ДІ у порівнянні з незаповненими контейнерами, була виявлена характерна відмінність форматами з втратами і форматами без втрат. Як показали обчислювальні експерименти, матриця унікальних кольорів незаповнених контейнерів в форматі з втратами містить незначну кількість середніх триплетів (в основному до 3%) (рис. 3.4), для контейнерів в форматі без втрат характерний високий вміст середніх триплетів (табл. 3.1), причому кількість Red-, Green-, Blue-тріад триплетів незначно відрізняються одна від одної.

На рис. 3.6 наведений розподіл кількості послідовних тріад триплетів у матриці унікальних кольорів для ЦЗ з груп 1 (TIFF) і 3 (JPG) з бази NRCS [131] (рис. 3.6, а), і для ЦЗ з груп 2 (TIFF) і 5 (JPG), отриманих непрофесійними камерами (рис. 3.6, б).

Як показує рис. 3.6, підхід, заснований на аналізі послідовних тріад триплетів у матриці унікальних кольорів, дозволяє відокремлювати ЦЗ, перезбережені в формат без втрат з формату з втратами, від ЦЗ, що спочатку зберігалися в форматі без втрат. Особливо суттєво відрізняються ЦЗ з груп 2 і 5, де практично відсутні перетини.



а



б

Рис. 3.6 – Порівняння розподілу кількості послідовних триад триплетів у матриці унікальних кольорів оригінальних ЦЗ: а – з груп 1 (TIFF) і 3 (JPG); б – з груп 2 (TIFF) і 5 (JPG)

Однак виникає питання: чи можна подібним чином відокремити контейнери в форматі з втратами від контейнерів в форматі без втрат у випадку, коли контент, що аналізується, не є оригінальним, а є СП, побудованим методом LSB. Для відповіді на це питання був проведений додатковий обчислювальний експеримент на базі ЦЗ з БЦЗ, що аналізує вміст послідовних триад триплетів у матрицях унікальних кольорів, сформованих вбудовою ДІ з різним ступенем заповнення з різними значеннями ППС: в одну довільну колірну складову, в дві довільні колірні складові, у всі три колірні складові контейнеру. Порівняльна характеристика кількості послідовних триад триплетів для форматів JPG і TIFF наведена в табл. 3.4.

З табл. 3.4, а також з рис. 3.5 випливає, що в результаті вбудови ДІ у контейнери, що спочатку зберігалися в форматі з втратами, кількість послідовних триад триплетів зростає нерівномірно, для таких СП характерні значні перепади значень кількості послідовних триад навіть у випадках, коли ДІ вбудовувалась в дві або три колірні складові. Для СП, сформованих на основі контейнерів в форматі без втрат, характерний стабільний, практично незмінний, високий вміст послідовних триад триплетів незалежно від ступеня заповнення, що є відмінною рисою ЦЗ в форматі без втрат, яку можна

використовувати для виявлення формату оригінального цифрового контенту-контейнеру.

Таблиця 3.4 – Порівняльна характеристика вмісту послідовних триад триплетів у матриці унікальних кольорів ЦЗ і СП, сформованих з різним ступенем заповнення

		TIFF	JPG
Незаповнені контейнери		Високий вміст ($\approx 20-70\%$) послідовних триад триплетів, кількість Red-, Green-, Blue-триад триплетів є зіставною за значеннями	Низький вміст (до 5%) послідовних триад триплетів, кількість Red-, Green-, Blue-триад триплетів є зіставною за значеннями
СП, сформоване вбудовою ДІ в:	одну колірну складову	Кількість Red-, Green-, Blue-триад триплетів є зіставною за значеннями і чисельно майже не відрізняється від контейнерів (не більше ніж на 1-2%)	Кількість Red-, Green-, Blue-триад триплетів нерівномірно зростає у порівнянні з контейнером (основних триад $\approx 20-50\%$, супутніх – до 15%)
	дві колірні складові	Кількість Red-, Green-, Blue-триад триплетів є зіставною за значеннями і чисельно майже не відрізняється від контейнерів (не більше ніж на 1-2%)	Кількість Red-, Green-, Blue-триад триплетів нерівномірно зростає у порівнянні з контейнером (основних триад $\approx 5-50\%$, супутніх – до 35%)
	три колірні складові	Кількість Red-, Green-, Blue-триад триплетів є зіставною за значеннями і чисельно майже не відрізняється від контейнерів (не більше ніж на 1-2%)	Кількість Red-, Green-, Blue-триад триплетів нерівномірно зростає у порівнянні з контейнером (всі триади є основними, їх кількість варіюється в межах від 5 до 50%)

На основі результатів проведених експериментів сформулюємо основні кроки методу виявлення формату контейнеру (МВФКА), що дозволяє відокремити кольорові ЦЗ, перезбережені в формат без втрат з формату з втратами, від кольорових ЦЗ, початково збережених в форматі без втрат. Для кольорового ЦЗ/кадру ЦВ I розміром $M \times N$ з колірними складовими R, G, B :

Кроки 1-3. Кроки відповідають крокам 1-3 метода САМЗ.

Крок 4. Визначення формату ЦК.

Якщо $((pR > T_{lim}) \& (pG > T_{lim}) \& (pB > T_{lim}))$ при $pR \approx pG \approx pB$,

то оригінальним форматом I є формат без втрат,

інакше оригінальним форматом I є формат з втратами,

де T_{lim} – порогове значення, що відокремлює цифрові контенти в форматі без втрат від цифрових контентів в форматі з втратами. Виходячи з рис. 3.6 і табл. 3.4, можна приймати значення T_{lim} з діапазону [5,10].

Алгоритм, що реалізує запропонований метод, буде застосовуватися як складова частина стеганоаналітичного методу САМ1, хоч може використовуватися і самостійно. При цьому слід відзначити, що метод МВФКА призначений для виявлення оригінального формату тільки кольорових цифрових контентів, для ЦЗ або ЦВ в градаціях сірого його використання неможливе.

3.5. Висновки до розділу 3

В розділі 3 розроблений стеганоаналітичний метод для виявлення результатів роботи LSB-методу, у тому числі в умовах малої ППС організованого прихованого каналу зв'язку, в ЦЗ/кадрах відеопослідовності, що здійснює аналіз просторової області контенту.

Отримані наступні результати:

1. Для матриці кольорового ЦЗ у просторовій області визначений параметр – кількість послідовних колірних тріад, відносно зменшення якого, що

визначається з використанням матриці унікальних кольорів, дозволяє виявляти модифікації значень яскравості пікселів зображення, що відбуваються в результаті вбудови ДІ методом LSB в одну довільну колірну складову контейнеру.

2. Виявлені характерні особливості збурення матриці унікальних кольорів СП, сформованих вбудовою ДІ методом LSB в одну довільну колірну складову контейнеру, збереженого в форматі з втратами: незаповнений контейнер містить не більше 3% послідовних тріад триплетів, в результаті вбудови ДІ значно зростає кількість основних тріад, що відповідають тої колірної складової, куди відбувалась вбудова ДІ.
3. Розроблений стеганоаналітичний метод, що здійснює у просторовій області ЦЗ детектування результатів стеганоперетворення, проведеного за допомогою LSB-методу, у тому числі при малій пропускній спроможності прихованого каналу зв'язку, аж до 0.05 біт/піксель. Метод заснований на врахуванні кількості послідовних Red-, Green- і Blue-тріад триплетів в матриці унікальних кольорів ЦЗ і застосовний за умови використання в якості контейнерів кольорових ЦЗ в форматі з втратами.
4. Розроблена ефективна адаптація стеганоаналітичного методу, заснованого на врахуванні кількості послідовних Red-, Green- і Blue-тріад триплетів у матриці унікальних ЦЗ, на випадок ЦВ за умови вбудови ДІ в одну довільну колірну складову всіх кадрів відеопослідовності, при цьому обрана колірна складова є постійною для всіх кадрів.
5. Розроблений метод, що дозволяє відокремлювати цифрові контенти, перезбережені з формату з втратами у формат без втрат, від цифрових контентів, початково збережених в форматі без втрат, що здійснює аналіз просторової області контенту. Метод може використовуватись для аналізу кольорових цифрових контентів і заснований на відмінності кількості послідовних тріад триплетів при вбудові ДІ у цифрових контентях в форматі без втрат і в форматі з втратами. Розроблений метод

може використовуватися як складова частина стеганоаналітичного методу, а також самостійно для виявлення порушення цілісності цифрових контентів.

Таким чином, в розділі 3 знайшли своє остаточне рішення задачі 2 і 3, вирішена задача 4 з переліку задач дисертаційної роботи. Основні результати даного розділу опубліковані в роботах [141-143].

Акһтамәтйева Анна

РОЗДІЛ 4

АНАЛІЗ ЕФЕКТИВНОСТІ РОЗРОБЛЕНИХ СТЕГАНОАНАЛІТИЧНИХ МЕТОДІВ

Метою розділу є розробка комплексного методу виявлення ДІ в ЦВ, ефективного при різних умовах вбудови ДІ на основі аналізу і оцінки, у тому числі порівняльній (з сучасними аналогами), ефективності стеганоаналітичних алгоритмів, що реалізують розроблені вище методи.

Оскільки розроблені вище стеганоаналітичні методи направлені на виявлення ДІ в ЦЗ, ЦВ, ефективність алгоритмів, що їх реалізують, буде оцінюватися шляхом визначення помилок першого роду (пропуск СП) і другого роду (визначення незаповненого контейнеру як СП) для кожного з алгоритмів.

Порівняльний аналіз ефективності розроблених алгоритмів з сучасними аналогами буде здійснюватися:

- шляхом оцінки значення інтегрального параметру ρ , що визначається за допомогою методу аналізу ROC-кривих, і точності детектування AD для алгоритму, що аналізує окремі ЦЗ і кадри ЦВ;
- шляхом оцінки точності детектування AD для алгоритмів, що аналізують послідовність ЦЗ/кадрів ЦВ.

Точність детектування AD визначається наступним чином. Для всіх цифрових контентів (ЦЗ, ЦВ) визначаються: TP - відсоток правильно виявлених СП, $TP = 100 - FN$, FN - помилки першого роду, TN - відсоток правильно виявлених незаповнених контейнерів, $TN = 100 - FP$, FP - помилки другого роду, після чого визначається точність детектування AD , що характеризує долю правильно виявлених подій [79-81]:

$$AD = \frac{TP + TN}{TP + FN + TN + FP}. \quad (4.1)$$

Метод аналізу ROC-кривих стосовно до стеганоаналізу полягає у проведенні тестування групи цифрових контентів, до якої входять як незаповнені контейнери, так і СП, причому відомо, яким саме є кожний контент. Серед ЦК, що аналізуються, в тестовій групі необхідно виявити СП (клас V_1) і оригінальні контейнери (клас V_2) за допомогою розробленого стеганоаналітичного алгоритму, в результаті виконання якого приймаються позитивне $\delta = 1$ або негативне $\delta = 0$ рішення. По результатах тестування визначаються TP , TN , FP , FN (пояснення наведено вище). Отримані результати детектування представляються в двовимірному ROC-просторі, де по осі абсцис відкладаються значення специфічності $1 - Sp$, що характеризують помилки другого роду:

$$Sp = \frac{TN}{TN + FP} \quad (4.2)$$

а по осі ординат – значення чутливості Se , що характеризують помилки першого роду:

$$Se = \frac{TP}{TP + FN} \quad (4.3)$$

На основі побудованих ROC-кривих обчислюється площа під ROC-кривою A та визначається інтегральний параметр ρ , що характеризує ефективність алгоритму, що досліджується за допомогою ROC-аналізу:

$$\rho = 2A - 1. \quad (4.4)$$

Результати аналізу ефективності розроблених стеганоаналітичних алгоритмів будуть використані для розробки комплексного

стеганоаналітичного методу, що здійснює аналіз просторової області контенту, для виявлення вкладення ДІ методом LSB в ЦВ, послідовності ЦЗ.

Для досягнення поставленої мети необхідно вирішити наступні *задачі*:

1. Розробити і оцінити ефективність стеганоаналітичних алгоритмів, що реалізують розроблені методи, для різних значень ППС;
2. Оцінити ефективність методу, направлено на виявлення факту стиску цифрових контентів, збережених в форматі без втрат, який виступає як складова частина стеганоаналізу;
3. Провести порівняльний аналіз ефективності розроблених стеганоаналітичних алгоритмів з сучасними аналогами;
4. Розробити комплексний метод виявлення ДІ в ЦВ, ефективний при різних умовах вбудови ДІ, а саме:
 - при різних значеннях ППС;
 - при різній степені заповнення контейнерів (в одну, дві або три колірні складові);
 - використанні в якості контейнерів кольорових або полутонових (в градаціях сірого) ЦВ;
 - використанні в якості контейнерів ЦВ в форматах з втратами або без втрат.

4.1. Розробка і аналіз стеганоаналітичних алгоритмів, що реалізують розроблені методи

Для спрощення викладення матеріалу далі використовуються наступні позначення:

- САА1 – стеганоаналітичний алгоритм виявлення вкладення ДІ в ЦВ, заснований на врахуванні відносних змін кількості блоків з однаковими значеннями яскравості, що реалізує метод САМ1;
- САА2 – стеганоаналітичний алгоритм виявлення вкладення ДІ в ЦВ, заснований на врахуванні характеру змін кількості блоків з однаковими значеннями яскравості, що реалізує метод САМ2;

- СААЗ – стеганоаналітичний алгоритм виявлення вкладення ДІ в ЦЗ, заснований на аналізі послідовних тріад триплетів в матриці унікальних кольорів, що реалізує метод САМЗ;
- СААЗv – стеганоаналітичний алгоритм виявлення вкладення ДІ в ЦВ, заснований на аналізі послідовних тріад триплетів в матриці унікальних кольорів, що реалізує метод САМЗv.

Для визначення ефективності розроблених алгоритмів проводяться обчислювальні експерименти для ЦЗ з БЦЗ, а також наступних ЦВ (тут і далі БЦВ):

1. Набір 1: 200 відеопослідовностей розміром кадру 320×240 , отриманих камерами мобільних пристроїв, з розширенням *.3gp або *.mp4 (при стиску використовуються кодеки H.263 або H.264);
2. Набір 2: 167 відеопослідовностей розміром кадру 320×240 , отриманих відеокамерою, з розширенням *.avi (при стиску використовується кодек Xvid);
3. Набір 3: 49 відеопослідовностей розміром кадру 176×144 , отриманих камерою застарілої моделі мобільного телефону (Sony Ericsson W700i – 2006 року випуску), з розширенням *.3gp.

Кожний відеоролик містить по 250 кадрів, після вбудови ДІ відео зберігаються без втрат в форматі *.avi.

Далі при обчислювальних експериментах для ЦЗ з БЦЗ будемо використовувати термін «група», для ЦВ з БЦВ – термін «набір», що відповідають описам БЦЗ і БЦВ.

У всіх подальших експериментах для ЦВ вбудова ДІ здійснюється в одну постійну колірну складову, що обирається довільно для кожного ЦВ, з різними значеннями ППС. Вбудова ДІ в одну постійну колірну складову обумовлена тим, що у сусідніх кадрах можуть відрізнятися тільки ділянки, що відповідають руху, а фон майже не змінюється, тому якщо здійснювати вбудову ДІ в різні колірні складові кадрів, можна виявити наявність ДІ в ЦВ простим порівнянням колірних складових сусідніх кадрів. Одним з методів

стійкості до стеганоаналізу, від з великою долею ймовірності в якості контейнера обере постійну колірну складову кадрів ЦВ.

4.1.1. Розробка і аналіз ефективності алгоритму, що реалізує стеганоаналітичний метод, заснований на врахуванні відносних змін кількості блоків з однаковими значеннями яскравості в результаті первинного і повторного стеганоперетворення

Для розробки алгоритму САА1 необхідно визначити порогові значення T_R , T_G , T_B для кожної колірної складової.

З табл. 2.2 (стовпці IV_i) і 2.3 (стовпці V_i) видно, що значення відносних змін кількості блоків виду (2.2) в результаті первинної і повторної вбудови ДІ у цифрові контенти відрізняються для форматів з втратами і форматів без втрат, тому і порогові значення T_R , T_G , T_B повинні бути різними для відповідних форматів.

Як правило, при отриманні камерами мобільних чи інших пристроїв ЦВ зазнають стиск з втратами, таким чином, припускається, що ЦВ, що використовуються в якості контейнерів при стеганоперетворенні, початково зберігаються в форматі з втратами. Використання в якості контейнера послідовності ЦЗ без втрат, з врахуванням специфіки організації сучасного обміну цифровою інформацією (як правило, у стиснутому стані) може привернути додаткову увагу, у тому числі і стеганоаналітика, в чому не зацікавлені організатори стеганографічного каналу зв'язку. З врахуванням наведених міркувань, розроблюваний алгоритм націлений, перш за все, на детектування ЦВ, оригінальні контейнери яких зберігаються в форматах з втратами.

Проведемо обчислювальний експеримент, направлений на підбір порогових значень T_R , T_G , T_B для виявлення вкладення ДІ в ЦВ, що спочатку зберігалися в форматі з втратами.

З урахуванням табл. 2.3, що містить відносну кількість 4×4 -блоків виду (2.2) (стовпці V_i для ЦЗ з груп 3-5) у колірних складових ЦЗ-СП, сформованих повторною вбудовою ДІ методом LSB в СП з різними значеннями ППС, усереднене по всіх ЦЗ з відповідних груп, оберемо максимальну відносну зміну кількості блоків виду (2.2) для кожної колірної складової відповідної групи: для червоної колірної складової максимальними значеннями є 31.3 (група 3), 5.3 (група 4), 18.8 (група 5); для зеленої колірної складової - 32.6 (група 3), 8 (група 4), 10.9 (група 5); для синьої колірної складової - 35.1 (група 3), 5.9 (група 4), 10.4 (група 5). Значення, більші за 36 можуть призвести до збільшення помилок детектування, тому при підборі порогових значень до уваги не беруться. На основі отриманих значень здійсимо визначення порогових значень для кожної колірної складової наступним чином:

1. В ЦВ з наборів 1 і 2 вбудуємо ДІ в одну довільну колірну складову з різними значеннями ППС, обрана колірна складова постійна для всіх кадрів ЦВ;
2. Для кожного ЦВ-СП для кожної колірної складової визначимо відносні зміни кількості блоків виду (2.2) в результаті повторної вбудови ДІ у всі колірні складові кадрів ЦВ-СП (формула (2.11));
3. Визначимо кількість помилок першого і другого роду окремо для кожної колірної складової ЦВ з наборів 1 і 2 при різних порогових значеннях (етап 1).

На першому етапі порогові значення змінюються з кроком 2: для червоної колірної складової від 6 до 32; для зеленої колірної складової від 8 до 34; для синьої колірної складової від 6 до 36. По результатам експерименту для кожного набору ЦВ для кожної колірної складової виділяються кращі показники детектування – мінімум помилок першого роду при мінімальних помилках другого роду, після чого обирається «перетин» кращих показників для наборів 1 і 2 при різних значеннях ППС. В результаті даної перевірки був уточнений діапазон порогових значень: для червоної

колірної складової від 28 до 30; для зеленої колірної складової від 18 до 20; для синьої колірної складової від 12 до 14.

4. Визначимо кількість помилок першого і другого роду окремо для кожної колірної складової ЦВ з наборів 1 і 2 при різних порогових значеннях, уточнених в результаті етапу 1 (етап 2).

На другому етапі порогові значення змінюються з кроком 0.5: для червоної колірної складової від 27 до 31; для зеленої колірної складової від 17 до 21; для синьої колірної складової від 11 до 15. Для більш точного визначення порогового значення відбувається розширення діапазонів на 1 в більшу та меншу сторони, оскільки на першому етапі при кроці, що дорівнює 2, не були захоплені непарні значення. Аналогічно для кожного набору ЦВ для кожної колірної складової виділяються кращі показники детектування, після чого знову обирається «перетин» кращих показників для наборів 1 і 2 при різних значеннях ППС.

По результатам другого етапу підбору порогових значень для ЦВ, що початково зберігалися в форматі з втратами, приймемо порогові значення $T_R = 27.5$, $T_G = 19.5$, $T_B = 11.5$.

Проте, не можна виключати варіант, коли в якості контейнера все ж таки буде виступати послідовність ЦЗ, збережених в форматі без втрат. У цьому випадку, з врахуванням табл. 2.2 (стовпці IV_i для ЦЗ з груп 1-2) і 2.3 (стовпці V_i для ЦЗ з груп 1-2) можна визначити порогові значення $T_R = 1.6$, $T_G = 1.7$, $T_B = 1.6$, як максимальні відносні зміни кількості блоків виду (2.2) для кожної колірної складової ЦЗ з групи 1 (значення відносних змін при повторній вбудові ДІ для ЦЗ з групи 2 менше обраних, що указує на повторну вбудову ДІ).

З урахуванням встановлених порогових значень T_R , T_G , T_B сформулюємо основні кроки стеганоаналітичного алгоритму САА1, що реалізує метод САМ1.

Для послідовності з P кадрів ЦВ (послідовності ЦЗ) C_1, C_2, \dots, C_P з колірними складовими $R_i^{(C)}$, $G_i^{(C)}$, $B_i^{(C)}$:

Крок 1. Визначення формату f оригінального контейнеру для вибору порогових значень, різних для випадків форматів з втратами і форматів без втрат, де $f \in \{losses, lossless\}$, $losses$ - формат з втратами, $lossless$ - формат без втрат.

Крок 2. Визначення порогових значень:

Якщо $f = losses$, то $T_R = 27.5$, $T_G = 19.5$, $T_B = 11.5$,

інакше $T_R = 1.6$, $T_G = 1.7$, $T_B = 1.6$.

Кроки 3-8 відповідають крокам 2-7 методу SAM1 відповідно.

Для апробації розробленого стеганоаналітичного алгоритму в середовищі MathWorks MatLAB (License number: 21808, Platform: All, License option: Group Term: Perretual, Use: Classroom) був проведений обчислювальний експеримент для ЦВ з БЦВ, по результатам якого визначені помилки першого та другого роду, наведені в табл. 4.1, при цьому слід відзначити, що підрахунок правильно виявлених СП (контейнерів) здійснюється як підрахунок кількості правильно виявлених заповнених (незаповнених) колірних складових (червоної, зеленої і синьої) для кожного ЦВ, що аналізується. Для порівняння ефективності виявлення вкладення ДІ в ЦВ з наборів 1-3 помилки першого і другого роду наведені для трьох наборів порогових значень:

1. $T_R = 27.5$, $T_G = 19.5$, $T_B = 11.5$ (результат двох етапної процедури визначення значень);

2. $T_R = 32$, $T_G = 33$, $T_B = 35.5$ (максимальні порогові значення для кожної колірної складової);

3. $T_R = 13$, $T_G = 7$, $T_B = 12$ (мінімальні порогові значення для кожної колірної складової при ППС 0.25-0.5 біт/піксель).

Таблиця 4.1 – Ефективність детектування наявності/відсутності ДІ в ЦВ алгоритмом САА1, %

Порогові значення	Помилки	ППС, біт/піксель				
		0.5	0.25	0.167	0.125	0.1
Набір 1						
$T_R = 32, T_G = 33, T_B = 35.5$	1-го роду	0	0	1.46	10.95	34.31
	2-го роду	3.28	3.28	3.28	2.19	2.55
$T_R = 13, T_G = 7, T_B = 12$	1-го роду	0	2.92	3.65	16.79	67.15
	2-го роду	0.36	0.36	0.36	0	0.36
$T_R = 27.5,$ $T_G = 19.5, T_B = 11.5$	1-го роду	0	0	2.19	11.68	51.09
	2-го роду	0.36	0.36	0.36	0.36	0.73
Набір 2						
$T_R = 32, T_G = 33, T_B = 35.5$	1-го роду	0	0	19.13	98.26	100
	2-го роду	0	0	0	0	0
$T_R = 13, T_G = 7, T_B = 12$	1-го роду	0	0	20.43	98.69	100
	2-го роду	0	0	0	0	0
$T_R = 27.5, T_G = 19.5,$ $T_B = 11.5$	1-го роду	0	0	19.56	98.26	100
	2-го роду	0	0	0	0	0
Набір 3						
$T_R = 32, T_G = 33, T_B = 35.5$	1-го роду	0	0	0	0	0
	2-го роду	98.98	98.98	98.98	97.96	97.96
$T_R = 13, T_G = 7, T_B = 12$	1-го роду	0	0	0	0	0
	2-го роду	90.82	89.79	90.82	86.73	89.79
$T_R = 27.5, T_G = 19.5,$ $T_B = 11.5$	1-го роду	0	0	0	0	0
	2-го роду	94.90	94.90	94.90	91.84	91.84

Як видно з табл. 4.1, ефективність стеганоаналітичного алгоритму САА1 різна для різних наборів ЦВ: найкращі результати детектування характерні для ЦВ, отриманих мобільними пристроями (набір 1) при значеннях ППС 0.125-0.5 біт/піксель, у випадку ЦВ з набору 2 алгоритм ефективний при

значеннях ППС 0.167 біт/піксель і вище. В результаті проведеного експерименту підтверджено, що порогові значення $T_R = 27.5$, $T_G = 19.5$, $T_B = 11.5$ можуть розглядатися як такі, що дають краще співвідношення між помилками першого та другого роду, що підтверджується результатами виявлення вкладень ДІ в ЦВ з набору 1 при ППС 0.125 біт/піксель: при мінімальних помилках другого роду помилки першого роду також невисокі і незначно (не більше 1%) відрізняються від мінімальних помилок першого роду при більш високих помилках другого роду при порогових значеннях $T_R = 32$, $T_G = 33$, $T_B = 35.5$.

Крім того, як видно з табл. 4.1, стеганоповідомленнями були визначені майже всі колірні складові кадрів ЦВ малого розміру, у тому числі і незаповнені, що підтверджує припущення, висунуте в розділі 2.3, про неефективність застосування розробленого методу для ЦВ з малим розміром кадру, і говорить про низьку ефективність алгоритму САА1 для таких відео. Це можна пояснити незначною кількістю блоків виду (2.2) у матриці колірної складової (для розміру кадра 176×144 загальна кількість 4×4 -блоків складає всього 1584, а для розміру 320×240 - 4800). Як показав проведений обчислювальний експеримент, алгоритм САА1 ефективно виявляє СП, сформовані вбудовою ДІ з ППС 0.125-0.5 біт/піксель в ЦВ з набору 1, де розмір кадрів складає 320×240 .

Таким чином, експериментально встановлено достатня для організації ефективного детектування наявності ДІ в цифрових відео кількість 4×4 -блоків в кадрі - 4800. З урахуванням зроблених спостережень можна припустити, що при великих значеннях розміру кадру ЦВ ефективність виявлення вкладень ДІ буде зростати. Таким чином, в результаті обчислювального експерименту встановлено, що при загальній кількості 4×4 -блоків кадрів ЦВ, що перевищує 4800, спостерігається висока ефективність виявлення вкладень ДІ в ЦВ, при зниженні кількості 4×4 -блоків внаслідок зменшення розміру кадрів буде знижуватись і ефективність детектування вкладень ДІ.

Визначимо обчислювальну складність алгоритму САА1. В матриці ЦЗ (кадру ЦВ) I розміром $M \times M$ при стеганоаналізі необхідно перевірити $\left\lceil \frac{M}{n} \right\rceil \cdot \left\lceil \frac{M}{n} \right\rceil$ блоків розміром $n \times n$, при цьому розмір блоків є константою і не залежить від розміру вхідної матриці контейнеру. Для кожного блоку проводиться $n^2 - 1$ операцій порівняння, необхідних для виявлення блоків з однаковими значеннями яскравості, ця кількість операцій є постійною для всіх блоків і також не залежить від розміру матриці I . Тому обчислювальна складність для однієї колірної складової оцінюється як $O(M^2)$, а з урахуванням кольорових ЦЗ (кадрів ЦВ), що містять три колірні матриці, як $3 \cdot O(M^2)$. Таким чином, обробка всієї відеопослідовності, що містить P кадрів розміром $M \times M$, потребує $3 \cdot P \cdot O(M^2)$ операцій. Оскільки кількість колірних складових кадрів є константою і не залежить від M , то обчислювальна складність розробленого алгоритму оцінюється як $P \cdot O(M^2)$.

4.1.2. Розробка і аналіз ефективності алгоритму, що реалізує метод врахування характеру змін кількості блоків з однаковими значеннями яскравості в результаті первинного і повторного стеганоперетворення

З метою розширення області застосування стеганоаналітичного підходу, заснованого на врахуванні кількості блоків з однаковими значеннями яскравості в розділі 2.4 був розроблений стеганоаналітичний метод, спроможний детектувати вкладення ДІ, у тому числі, в ЦВ з малим розміром кадру. Для розробки САА2 необхідно визначити порогове значення T , що використовується для оцінки кількості кадрів (%) в ЦВ (зображень в послідовності ЦЗ), у яких спостерігалось зменшення кількості блоків при вбудові ДІ, що проводиться в ході аналізу.

Виходячи з того, що після первинної вбудови ДІ у більшості ЦЗ всіх груп спостерігалось зменшення кількості 4×4 -блоків виду (2.2) (у табл. 2.4

до 50% ЦЗ з груп 1-2 (без втрат) зі зменшенням кількості блоків виду (2.2) і в понад 80% ЦЗ груп 3-5 (з втратами)), а у випадку повторної вбудови ДІ зменшення таких блоків майже не відбувалось (для первинних ППС 0.5 і 0.25 біт/піксель у середньому до 2%, за винятком випадку, коли первинна вбудова ДІ складає 0.1 біт/піксель (табл. 2.5)), визначимо таке порогове значення T , яке забезпечувало б високу ефективність виявлення вкладень ДІ в ЦВ з малим розміром кадру. Для цього проведемо наступний обчислювальний експеримент:

1. В ЦВ з наборів 1, 2 і 3 вбудуємо ДІ в одну довільну колірну складову з різними значеннями ППС, обрана колірна складова є постійною для всіх кадрів ЦВ;

2. Для кожного ЦВ-СП для кожної колірної складової визначимо характер зміни кількості блоків виду (2.2) в результаті повторної вбудови ДІ у всі колірні складові кадрів ЦВ-СП;

3. Визначимо кількість помилок першого і другого роду в результаті використання алгоритму САА2 для виявлення вкладень ДІ в ЦВ з наборів 1, 2 і 3 при різних порогових значеннях. З урахуванням табл. 2.5, де кількість колірних складових зі зменшенням блоків виду (2.2) для первинних значень ППС 0.25-0.5 біт/піксель при повторній вбудові ДІ складала не більше 3% від загальної кількості колірних матриць ЦЗ у відповідних групах, порогові значення змінюються від 0.5 до 5 з кроком 0.5.

В результаті проведеного обчислювального експерименту було встановлено, що найменша кількість помилок першого роду при допустимій, як свідчать відкриті наукові джерела з теми дисертації, кількості помилок другого роду (до 5%) при аналізі ЦЗ з набору 3 досягається при порогових значеннях $T \in [2,3]$. У випадку ЦВ з наборів 1 і 2 при значеннях ППС 0.167-0.5 біт/піксель при відсутності помилок другого роду помилок першого роду майже не спостерігалось, а у випадку ППС 0.1-0.125 біт/піксель зі збільшенням порогового значення T зменшується кількість помилок першого роду, в той же час, збільшення порогового значення T призводить

до монотонного збільшення помилок другого роду для ЦВ з набору 3 (з малим розміром кадру). Залежність помилок першого і другого роду від значення порогу T на прикладі ППС 0.125 біт/піксель наведена на рис. 4.2.

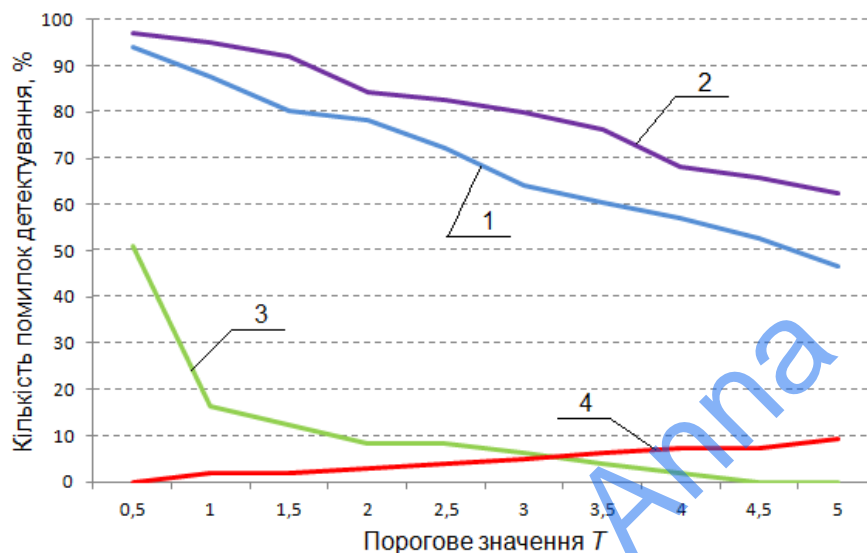


Рис. 4.2 – Залежність помилок першого і другого роду від значення порогу T : 1 – помилки першого роду для ЦВ з набору 1; 2 – помилки першого роду для ЦВ з набору 2; 3 – помилки першого роду для ЦВ з набору 3; 4 – помилки другого роду для ЦВ з набору 3

Таким чином, виходячи з проведеного обчислювального експерименту, можна зробити висновок, що подальше збільшення порогового значення T з метою підвищення ефективності виявлення вкладень ДІ в ЦВ-СП, сформованих при малих значеннях ППС, спричинить за собою зниження ефективності детектування ЦВ малого розміру кадру, оскільки призведе до збільшення помилок другого роду.

На основі отриманого порогового значення розроблений стеганоаналітичний алгоритм САА2, кроки якого співпадають з кроками методу САМ2, на кроці 6 в якості порогового значення T приймемо $T = 3$.

Для апробації розробленого стеганоаналітичного алгоритму САА2 у середовищі MathWorks MatLAB був проведений обчислювальний

експеримент для ЦВ з БЦВ, по результатам якого визначені помилки першого і другого роду, наведені в табл. 4.2.

Таблиця 4.2 – Ефективність детектування наявності/відсутності ДІ у цифрових контентах алгоритмом САА2, %

	Порогове значення	Помилки	ППС, біт/піксель				
			0.5	0.25	0.167	0.125	0.1
Набір 1 (ЦВ)	$T = 2.5$	1-го роду	0	0	0	72.26	98.54
		2-го роду	0	0	0	0	0
	$T = 3$	1-го роду	0	0	0	64.23	97.08
		2-го роду	0	0	0	0	0
Набір 2 (ЦВ)	$T = 2.5$	1-го роду	0	0	0	82.61	100
		2-го роду	0	0	0	0	0
	$T = 3$	1-го роду	0	0	0	80	100
		2-го роду	0	0	0	0	0
Набір 3 (ЦВ)	$T = 2.5$	1-го роду	0	0	0	8.16	40.82
		2-го роду	4.08	4.08	4.08	3.06	4.08
	$T = 3$	1-го роду	0	0	0	6.12	40.82
		2-го роду	5.10	5.10	5.10	5.10	5.10

Як видно з табл. 4.2, запропонований стеганоаналітичний алгоритм САА2 ефективний у випадку ППС 0.5, 0.25, 0.167 біт/піксель при порогових значеннях $T \in [2.5, 3]$, а для ЦВ малого розміру кадру і у випадку 0.125 біт/піксель. Таким чином, обчислювальний експеримент підтвердив, що запропонований метод САМ2, заснований на врахуванні характеру змін кількості блоків виду (2.2) є ефективним при виявленні вбудованої ДІ в ЦВ з малим розміром кадрів.

Як і для САА1, обчислювальна складність розробленого алгоритму САА2 при обробці відеопослідовності, що містить P кадрів розміром $M \times M$, визначається як $P \cdot O(M^2)$ операцій.

4.1.3. Розробка і аналіз ефективності алгоритмів, що реалізують стеганоаналітичні методи, засновані на аналізі послідовних тріад триплетів

Для розробки алгоритмів СААЗ і СААЗv необхідно визначити порогові значення T_{low} , що характеризують максимальну кількість середніх триплетів послідовних тріад (%) в незаповнених контейнерах, і T_{up} , що характеризує мінімальну кількість середніх триплетів послідовних тріад (%) в СП, сформованих при різних значеннях ППС.

З урахуванням того, що матриця унікальних кольорів незаповнених ЦЗ в форматі з втратами у середньому містить не більше 3% послідовних тріад триплетів (табл. 3.1), а також того факту, що кількість супутніх тріад триплетів у матриці унікальних кольорів СП зростає у середньому до 8-12% (рис. 3.5), прийmemo попередні пороги вмісту послідовних тріад $T_{low} = 2.5$ і $T_{up} = 8$. На базі ЦЗ з груп 3-5 проведений обчислювальний експеримент, що визначає кількість Red-, Green- і Blue-тріад триплетів у матрицях унікальних кольорів оригінальних контейнерів (ППС 0 біт/піксель) і СП, сформованих вбудовою ДІ тільки в одну довільну колірну складову з різними значеннями ППС. Результати експерименту наведені в табл. 4.3, де ν - вміст (в %) всіх послідовних тріад триплетів (і основних, і супутніх) у матрицях унікальних кольорів всіх цифрових контентів відповідних груп, $\nu \in \{\nu_{r_q}, \nu_{g_q}, \nu_{b_q}\}$, $q = \overline{1, X}$, X - кількість ЦЗ в групі, $\max \nu$ - максимальний відсоток послідовних тріад триплетів у матрицях унікальних кольорів всіх цифрових контентів відповідних груп (для ППС 0.05-0.5 біт/піксель $\max \nu$ відповідає максимальному вмісту серед всіх основних тріад триплетів відповідних груп ЦЗ-СП).

Таблиця 4.3 – Кількість значень вмісту послідовних тріад триплетів, що задовольняють умовам $v \leq T_{low}$, $v > T_{up}$, в залежності від групи ЦЗ і значень

ППС відносно загального числа значень, %

	Умова	ППС, біт/піксель						
		0.5	0.25	0.167	0.125	0.1	0.05	0
Група 3	$v \leq T_{low}$	3.613	6.240	8.210	8.703	9.195	13.300	94.417
	$v > T_{up}$	89.655	80.788	72.578	64.368	56.486	35.796	0.328
	max v	56.941	47.444	47.682	45.333	43.216	31.365	9.077
Група 4	$v \leq T_{low}$	3.151	5.307	6.302	8.624	11.609	18.242	86.236
	$v > T_{up}$	84.245	69.983	64.179	55.887	53.566	31.012	0.829
	max v	54.576	51.674	48.757	46.210	41.470	36.024	11.248
Група 5	$v \leq T_{low}$	1.395	4.651	5.892	6.822	7.597	9.923	92.248
	$v > T_{up}$	90.698	85.736	77.364	68.217	61.240	46.977	0
	max v	55.079	51.649	48.279	45.319	43.803	38.531	4.689

Таким чином, обчислювальний експеримент показав, що у середньому 90% цифрових контейнерів, збережених в форматі з втратами, містять не більше 2.5% (умова $v \leq T_{low}$, $T_{low} = 2.5$, в табл. 4.3 для ППС 0 біт/піксель) Red-, Green- і Blue-тріад, їх кількість значно зростає при вбудові ДІ (умова $v > T_{up}$, $T_{up} = 8$, в табл. 4.3 для ППС 0.05-0.5 біт/піксель). Тому умовою для оригінального контейнеру є виконання співвідношення:

$$(pR \leq T_{low}) \text{ AND } (pG \leq T_{low}) \text{ AND } (pB \leq T_{low}), \quad (4.5)$$

і для СП:

$$(pR > T_{low}) \text{ OR } (pG > T_{low}) \text{ OR } (pB > T_{low}), \quad (4.6)$$

де pR – відсотковий вміст Red-тріад триплетів у матриці унікальних кольорів ЦЗ (кадру ЦВ); pG – відсотковий вміст Green-тріад триплетів у матриці унікальних кольорів ЦЗ (кадру ЦВ); pB – відсотковий вміст Blue-тріад триплетів у матриці унікальних кольорів ЦЗ (кадру ЦВ).

На основі результатів проведеного експерименту в якості порогу T_{low} , що дозволяє відокремити пустий контейнер від заповненого, для форматів з втратами приймемо $T_{low} = 2.5$. Зменшення даного значення порогу недоцільно, оскільки воно призведе до зростання кількості «помилкових тривог» при детектуванні пустих контейнерів.

Крім того, в оригінальних ЦЗ майже не спостерігалось значень вмісту тріад триплетів (%) у матриці унікальних кольорів більшого за 8% (лише у 0.38% колірних матриць контейнеру значення v перевищило 8%), що дозволяє прийняти значення порогу T_{up} , що сприяє правильному детектуванню незаповнених контейнерів, забезпечуючи захист від виникнення «помилкових тривог», що дорівнює 8. Якщо максимальне зі значень v_r, v_g, v_b , що відповідають колірної складової з вбудованою інформацією, перевищить значення $T_{up} = 8$, то можна говорити, що аналізоване зображення є СП.

Додатковим параметром при детектуванні наявності ДІ у цифрових контентях виступає різниця між максимальним зі значень v_r, v_g, v_b і двома іншими значеннями. Як правило, при ППС 0.5 і 0.25 біт/піксель максимальне зі значень v_r, v_g, v_b більше двох інших в 2 рази, однак при менших значеннях ППС це співвідношення зменшується до 1.5. Тому, якщо значення v_r, v_g, v_b знаходяться в діапазоні $(2.5, 8]$, визначається співвідношення між максимальним зі v_r, v_g, v_b ($v^{\max} = \max(v_r, v_g, v_b)$) і двома меншими значеннями з v_r, v_g, v_b ($v^{(1)}, v^{(2)}$)

$$\theta' = \frac{v^{\max}}{v^{(1)}}; \theta'' = \frac{v^{\max}}{v^{(2)}}. \quad (4.7)$$

Якщо отримані співвідношення θ' і θ'' перевищують 1.5, то має місце СП. Як правило, перевірка умови (4.7) настає при вбудові ДІ з малими значеннями ППС (0.05-0.125 біт/піксель), при значеннях ППС більше 0.125 біт/піксель при стеганоаналізі спрацьовує умова (4.6), при відсутності ДІ у цифровому контенті – умова (4.5).

На основі встановлених порогових значень T_{low} і T_{up} сформулюємо основні кроки стеганоаналітичного алгоритму СААЗ для ЦЗ (кадру ЦВ) I розміром $M \times N$ з кольорними складовими R, G, B :

Крок 1. Формування матриці UCT розміром $U \times 3$ унікальних триплетів кольорів $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ для ЦЗ I .

Крок 2. Підрахування кількості послідовних триад триплетів для кожної кольорної складової.

2.1. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k + 1, \check{g}_k, \check{b}_k)$ і $(\check{r}_k - 1, \check{g}_k, \check{b}_k)$, то $countR = countR + 1$, $countR$ – кількість Red-триад в UCT ;

2.2. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k, \check{g}_k + 1, \check{b}_k)$ і $(\check{r}_k, \check{g}_k - 1, \check{b}_k)$, то $countG = countG + 1$, $countG$ – кількість Green-триад в UCT ;

2.3. Якщо для поточного триплету $(\check{r}_k, \check{g}_k, \check{b}_k)$, $k = \overline{1, U}$ в UCT одночасно існують триплети $(\check{r}_k, \check{g}_k, \check{b}_k + 1)$ і $(\check{r}_k, \check{g}_k, \check{b}_k - 1)$, то $countB = countB + 1$, $countB$ – кількість Blue-триад в UCT .

Крок 3. Обчислити кількість середніх триплетів послідовних триад відносно загальної кількості унікальних кольорів (%):

$$pR = \frac{countR}{U} \cdot 100, \quad pG = \frac{countG}{U} \cdot 100, \quad pB = \frac{countB}{U} \cdot 100;$$

$$p_{\max} = \max(pR, pG, pB),$$

де p_{\max} – максимальне значення серед pR, pG, pB .

Крок 4. Детектування наявності/відсутності ДІ.

4.1. Якщо $(pR = p_{\max}) \text{ AND } (pR > 8)$,

то I містить вбудовану ДІ у червоній колірній складовій;

інакше якщо

$$((pR > 2.5) \text{ OR } (pG > 2.5) \text{ OR } (pB > 2.5)) \text{ AND}$$

$$((pR > 1.5 \cdot pG)) \text{ AND } ((pR > 1.5 \cdot pB))$$

то I містить вбудовану ДІ у червоній колірній складовій;

інакше ДІ відсутня у червоній колірній складовій;

4.2. Якщо $(pG = p_{\max}) \text{ AND } (pG > 8)$,

то I містить вбудовану ДІ у зеленій колірній складовій I ,

інакше якщо

$$((pR > 2.5) \text{ OR } (pG > 2.5) \text{ OR } (pB > 2.5)) \text{ AND}$$

$$((pG > 1.5 \cdot pR)) \text{ AND } ((pG > 1.5 \cdot pB))$$

то I містить вбудовану ДІ у зеленій колірній складовій;

інакше ДІ відсутня у зеленій колірній складовій I ;

4.3. Якщо $(pB = p_{\max}) \text{ AND } (pB > 8)$,

то I містить вбудовану ДІ у синій колірній складовій,

інакше якщо

$$((pR > 2.5) \text{ OR } (pG > 2.5) \text{ OR } (pB > 2.5)) \text{ AND}$$

$$((pB > 1.5 \cdot pR)) \text{ AND } ((pB > 1.5 \cdot pG))$$

то I містить вбудовану ДІ у синій колірній складовій,

інакше ДІ відсутня у синій колірній складовій I .

Для аналізу ЦВ кроки стеганоаналітичного алгоритму САА3v співпадають з відповідними кроками методу САМ3v при порогових значеннях $T_{low} = 2.5$ і $T_{up} = 8$.

Для оцінки ефективності розроблених стеганоаналітичних алгоритмів СААЗ і СААЗv в середовище MatLAB був проведений обчислювальний експеримент на основі зображень з БЦЗ (групи 3-5) і відео з БЦВ, результати якого наведені в табл. 4.4, при цьому для ППС 0 біт/піксель (незаповнені контейнери) наведені тільки помилки другого роду.

Таблиця 4.4 – Ефективність детектування наявності/відсутності ДІ в цифрових контентів алгоритмами СААЗ і СААЗv, %

	Помилки	ППС, біт/піксель						
		0.5	0.25	0.167	0.125	0.1	0.05	0
Група 3 (ЦЗ)	1-го роду	0	0	0	0	0	1.97	-
	2-го роду	0	0	0	0	0	0	1.15
Група 4 (ЦЗ)	1-го роду	0	0	0.50	0	2.99	7.96	-
	2-го роду	0	0	0	0	0	0	1.66
Група 5 (ЦЗ)	1-го роду	0	0	0	0	0	2.32	-
	2-го роду	0	0	0	0	0	0	0.31
Набір 1 (ЦВ)	1-го роду	0	0	0	0.73	2.19	32.12	-
	2-го роду	0	0	0	0	0	0	0
Набір 2 (ЦВ)	1-го роду	0	0	0	0	0	10	-
	2-го роду	0	0	0	0	0	0	0
Набір 3 (ЦВ)	1-го роду	79.59	83.67	85.71	95.92	93.88	85.71	-
	2-го роду	1.02	7.14	5.10	13.27	12.24	6.12	18.37

Як видно з табл. 4.4, запропоновані стеганоаналітичні алгоритми є ефективними для контейнерів, збережених в форматі з втратами, навіть при вбудові в них ДІ з малою ППС (0.1 і 0.05 біт/піксель) за винятком ЦВ з малим розміром кадрів.

Визначимо обчислювальну складність алгоритмів СААЗ і СААЗv. На основі ЦЗ/кадру ЦВ розміром $M \times M$ з трьома колірними складовими формується матриця ST розміром $M^2 \times 3$, що потребує $3M^2$ операцій.

Матриця CT є вхідною для матриці унікальних кольорів UCT , що формується у два етапи:

1. У матрицю UCT копіюється матриця CT - $3M^2$ операцій;
2. З матриці UCT убираються повторні рядки (триплети), для цього для кожного з M^2 триплетів необхідно M^2-1 порівнянь, тобто M^4 операцій.

В результаті сформована матриця UCT розміром $U \times 3$, $U < M^2$, причому U (кількості унікальних кольорів) не залежить від M , оскільки характеризує кількість різних кольорів ЦЗ/кадру ЦВ, а кількість унікальних кольорів залежить від вмісту цифрового контенту, а не від його розміру.

Для підрахунку кількості одного виду послідовних тріад триплетів необхідно по 2 операції порівняння для кожного елементу, тобто для всіх трійок потрібно $3 \cdot 2 \cdot U = 6U$ операцій. А оскільки U не залежить від M , то для обробки одного ЦЗ/кадру ЦВ обчислювальна складність визначається як $\underline{O}(M^4)$. Обробка всієї відеопослідовності, що містить P кадрів розміром $M \times M$, потребує $P \cdot \underline{O}(M^4)$ операцій.

4.1.4. Розробка і аналіз ефективності алгоритму, що виявляє факт стиску цифрових контентів

Для підвищення ефективності виявлення вкладень ДІ в цифрових контентях за допомогою розроблених стеганоаналітичних методів і алгоритмів, що їх реалізують, виникла необхідність розробки методу, що дозволяє відокремлювати цифрові контенті, Perezбережені з формату з втратами в формат без втрат, від контентів, початково збережених в форматі без втрат, що було зроблено у розділі 3.4. Проведемо аналіз ефективності алгоритму, що реалізує метод МВФКА, що здійснює аналіз просторової області цифрових контентів, шляхом визначення помилок першого і другого роду, де стосовно до алгоритму, що аналізується, під помилками першого роду будемо розуміти пропуск факту стиску за його наявності, під помилками другого роду – визначення нестиснутого контенту як того, що зазнав стиск.

Сформулюємо основні кроки алгоритмічної реалізації методу МВФКА, де в якості порогового значення T_{lim} , що відокремлює цифрові контенти в форматі без втрат від цифрових контентів в форматі з втратами, приймемо $T_{\text{lim}} = 7.5$, під умовою $pR \approx pG \approx pB$ будемо розуміти випадок, коли $\max(pR, pG, pB) - \min(pR, pG, pB) \leq 6$.

Для кольорового ЦЗ/кадру ЦВ I розміром $M \times N$ з колірними складовими R, G, B :

Кроки 1-3. Кроки аналогічні крокам 1-3 алгоритму СААЗ.

Крок 4. Визначення формату цифрового контенту:

Якщо

$$((pR > 7.5) \text{ AND } (pG > 7.5) \text{ AND } (pB > 7.5)) \text{ AND} \\ \max(pR, pG, pB) - \min(pR, pG, pB) \leq 6,$$

то оригінальним форматом I є формат без втрат ($f = \text{lossless}$),

інакше оригінальним форматом I є формат з втратами ($f = \text{losses}$).

В обчислювальному експерименті, направленому на аналіз ефективності розробленого алгоритму, використовувались 400 ЦЗ з груп 1-5 (200 в форматі без втрат, 200 в форматі з втратами), з яких $\frac{1}{4}$ частина усіх зображень представляє собою незаповнені контейнери, $\frac{1}{2}$ - СП, сформовані вбудовою ДІ в одну довільну колірну складову ЦЗ з різними значеннями ППС, $\frac{1}{4}$ - СП, сформовані вбудовою ДІ в дві або три колірні складові ЦЗ з різними значеннями ППС.

По результатам проведеного експерименту помилки першого роду склали 3%, помилки другого роду – 4.5%, що дозволяє говорити про високу ефективність розробленого методу. Слід відзначити, що помилки першого роду спостерігались лише у випадку СП, сформованих вбудовою ДІ у всі три колірні складові ЦЗ, що початково зберігалися в форматі з втратами. У випадку, коли факт стиску виявлений в ЦЗ, що початково зберігалися в форматі без втрат, при вбудові ДІ в одну довільну колірну складову збурення

матриці унікальних кольорів аналогічні, як і при використанні в якості контейнерів ЦЗ в форматі з втратами, що допускає можливість визначити факт наявності/відсутності ДІ в таких цифрових контентах.

4.2. Порівняльний аналіз розроблених стеганоаналітичних алгоритмів з сучасними аналогами

4.2.1. Порівняльний аналіз ефективності розроблених стеганоаналітичних алгоритмів, направлених на виявлення додаткової інформації в цифровому відео з сучасними аналогами

Для порівняльного аналізу ефективності розроблених стеганоаналітичних алгоритмів САА1, САА2, САА3_v, направлених на виявлення наявності/відсутності ДІ, вбудованої методом LSB в ЦВ, використовувались ефективні сучасні аналоги.

Введемо позначення для стеганоаналітичних методів і алгоритмів, що використовуються для порівняння:

- V1 (2005) [38] (10 відео по 124 кадри);
- V2 (2005) [112] (10 відео по 124 кадри);
- V3 (2007) [109] (10 відео по 124 кадри);
- V4 (2013) [113] (9 відео по 150-300 кадрів);
- V5 (2015) [114] (26 відео по 100 кадрів).

У дужках представлена інформація про обсяг обчислювальних експериментів, що використовувались авторами відповідних алгоритмів при оцінці їх ефективності.

Порівняльний аналіз ефективності розроблених алгоритмів САА1, САА2, САА3_v для ЦВ та САА3 для виявлення наявності ДІ в окремих кадрах ЦВ з сучасними аналогами буде здійснюватися шляхом оцінки точності детектування AD , що обчислюється за формулою (4.1). Результати порівняння точності детектування AD розроблених стеганоаналітичних алгоритмів з обраними аналогами наведені в табл. 4.5. Слід відзначити, що в роботі [109] тестування проводиться лише для 10 ЦВ за допомогою

удосконаленого в даній роботі стеганоаналітичного підходу, а також за допомогою методів, розроблених в [38] і [112], початково направлених на детектування наявності вбудови в ЦЗ. Тому в табл. 4.5 методи V1 і V2 указані 2005 роком, однак результати детектування наведені з роботи [109]. Більш того, всі указані методи їх авторами перевірялись на основі дуже малої кількості ЦВ, що не дозволяє достовірно оцінити реальну ефективність наведених методів. Для алгоритмів САА1, САА2, САА3v в табл. 4.5 наведені результати тестування для 367 ЦВ з наборів 1-2, при цьому ДІ вбудовувалась у всі кадри ЦВ.

Таблиця 4.5 – Порівняння AD для розроблених стеганоаналітичних методів і сучасних аналогів

ППС, біт/піксель	V1 2005	V2 2005	V3 2007	V4 2013	V5 2015	САА1	САА2	САА3v
0.5	0.925	0.955	0.98	1	0.9991	0.9991	1	1
0.4	0.885	0.94	0.97	-	-	0.9991	1	1
0.3	0.825	0.92	0.945	-	-	0.9991	1	1
0.25	-	-	-	0.996	0.9988	0.9991	1	1
0.2	0.68	0.875	0.925	-	-	0.9691	1	1
0.167	-	-	-	-	-	0.9537	1	1
0.125	-	-	-	0.928	-	0.7757	0.7530	0.9991
0.1	0.555	0.755	0.89	-	0.9744	0.7139	0.6703	0.9973
0.0625	-	-	-	0.794	-	0.5157	0.5	0.9433
0.05	-	-	-	-	-	0.5074	0.5	0.9391

Для випадку, коли при вбудові ДІ заповнюється лише деяка частина кадрів ЦВ (часткова вбудова), проводиться по кадровий аналіз ЦВ за допомогою алгоритму САА3. Результати порівняння ефективності алгоритму САА3 з сучасним аналогом [114] в умовах часткової вбудови ДІ наведені в табл. 4.6. Порівняння здійснюється лише з аналогом [114], оскільки тільки в

даному джерелі проводився експеримент за умови заповнення частини кадрів ЦВ.

Таблиця 4.6 – Порівняння AD для стеганоаналітичного алгоритму САА3 і сучасного аналогу за умови часткового заповнення кадрів ЦВ

ППС окремих кадрів ЦВ, біт/піксель	Кількість заповнених кадрів							
	80%		60%		40%		20%	
	V5 2015	САА3	V5 2015	САА3	V5 2015	САА3	V5 2015	САА3
0.5	1	1	0.9978	1	1	1	0.9932	1
0.25	1	1	1	1	0.9926	1	0.9843	0.9999
0.167	-	0.9998	-	0.9998	-	0.9998	-	0.9999
0.125	-	0.9959	-	0.9948	-	0.9948	-	0.9991
0.1	0.9381	0.9897	0.9276	0.9867	0.7974	0.9867	0.6688	0.9974
0.05	-	0.9232	-	0.9048	-	0.9048	-	0.9811

В результаті порівняння значень AD можна зробити висновок, що розроблені стеганоаналітичні алгоритми є ефективнішими, ніж аналоги. Якщо вбудова ДІ здійснювалась з ППС 0.167-0.5 біт/піксель, алгоритмами САА3v і САА2 досягнутий абсолютний результат для точності детектування - $AD = 1$. У випадку малих значень ППС найбільш ефективним є алгоритм САА3v: результати детектування за допомогою САА3v на 2.3% перевищують аналог 2015 року [114] і більше ніж на 10% аналоги 2005-2007 років (для ППС 0.1 біт/піксель) [38, 109, 112]. Найбільше підвищення ефективності досягається при виявленні ДІ, вбудованої зі значеннями ППС, меншими за 0.1 біт/піксель: точність детектування САА3v на 14.93% перевищує аналог 2013 року [113] при значенні ППС 0.0625 біт/піксель. Точність детектування алгоритмів САА1 і САА2 нижче аналогів, оскільки порівняльний аналіз враховує результати аналізу ЦВ з наборів 1 і 2, однак у випадку використання САА1 для стеганоаналізу ЦВ, отриманих камерами

мобільних пристроїв (набір 1), точність детектування при ППС 0.125 біт/піксель досягає 0.94, що на 1.2% перевищує аналог 2013 року [113].

Також у випадку часткової вбудови ДІ (у випадку, коли заповнюється тільки частина кадрів) розроблений алгоритм СААЗ (стосовно до кадрів ЦВ) значно ефективніше сучасного аналогу [114] при вбудові ДІ з малою ППС. При ППС 0.25-0.5 біт/піксель результати порівняні при різній степені заповнення кадрів, однак у випадку ППС 0.1 біт/піксель при степені заповнення кадрів 60-80% результати СААЗ на 5.5% перевищують аналог, при степені заповнення кадрів 40% і 20% відповідно на 18% і 32%.

4.2.2. Порівняльний аналіз ефективності алгоритмів, направлених на виявлення додаткової інформації в цифрових зображеннях

Порівняння ефективності алгоритму СААЗ з існуючими аналогами здійснюється за допомогою інтегрального параметру ρ , що обчислюється на основі побудованих ROC-кривих за формулою (4.4), а також порівнянням значень точності детектування AD (формула (4.1)).

В даному дослідженні значення Sp і Se , що обчислюються за формулами (4.2) і (4.3) відповідно, визначені для різних порогових значень, на основі яких побудовані ROC-криві для значень ППС 0.5, 0.25, 0.167, 0.125, 0.1 і 0.05 біт/піксель, наведені на рис. 4.3, 4.4. На рис. 4.3 наведений ROC-простір для $1 - Sp \in \overline{0,1}$, $Se \in \overline{0,1}$, на рис. 4.4 наведений фрагмент ROC-простору для $1 - Sp \in \overline{0, 0.025}$, $Se \in \overline{0.8, 1}$.

На основі побудованих ROC-кривих був отриманий інтегральний параметр ρ (формула (4.4)). Значення площі під ROC-кривими і параметру ρ для різних значень ППС наведені в табл. 4.7.

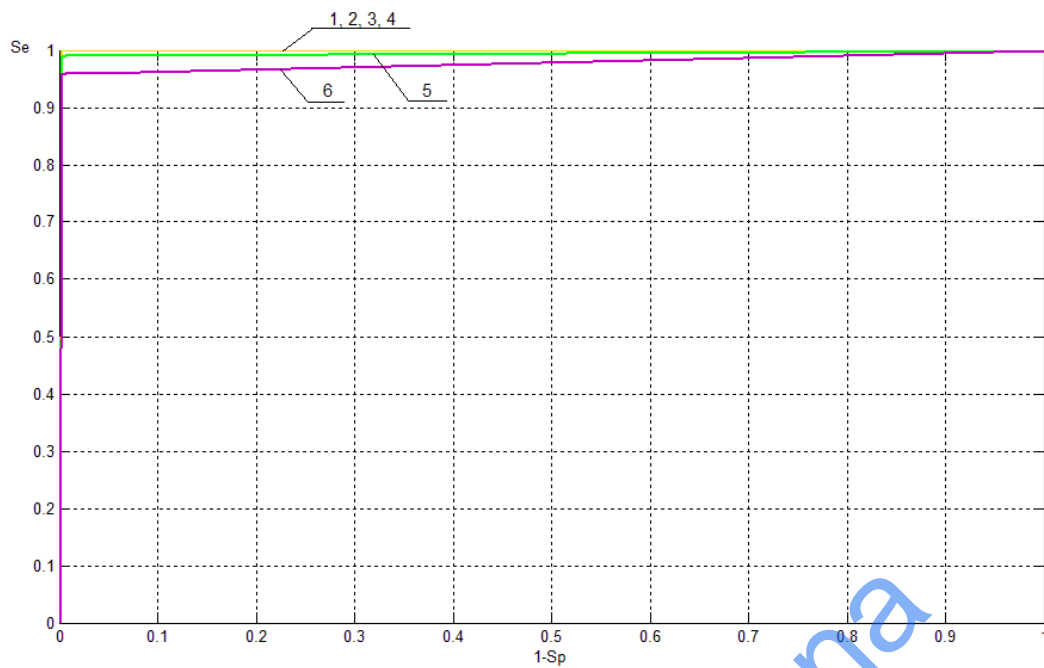


Рис. 4.3 – ROC-криві, що характеризують роботу стеганоаналітичного алгоритму СААЗ для різних значень ППС: 1 – 0.5; 2 – 0.25; 3 – 0.167; 4 – 0.125; 5 – 0.1; 6 – 0.05 біт/піксель

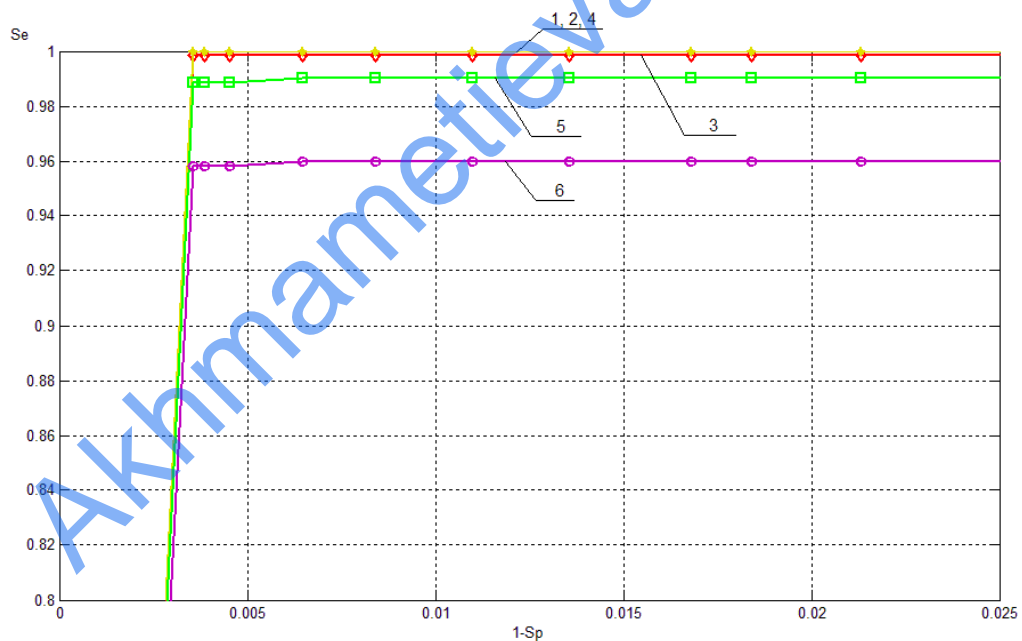


Рис. 4.4 – Фрагмент ROC-кривих у ROC-просторі на ділянці $1 - Sp \in \overline{0, 0.025}$, $Se \in \overline{0.8, 1}$, що характеризують роботу стеганоаналітичного алгоритму СААЗ для різних значень ППС: 1 – 0.5; 2 – 0.25; 3 – 0.167; 4 – 0.125; 5 – 0.1; 6 – 0.05 біт/піксель

Таблиця 4.7 – Значення інтегрального параметру ρ для оцінки ефективності стеганоаналітичного алгоритму СААЗ

ППС, біт/піксель	A	ρ
0.5	0.99822294	0.99644588
0.25	0.99822294	0.99644588
0.167	0.997393263	0.994786526
0.125	0.99822294	0.99644588
0.1	0.993238873	0.986477747
0.05	0.977475004	0.954950008

Для порівняння розробленого стеганоаналітичного алгоритму СААЗ, направлено на виявлення наявності/відсутності ДІ в ЦЗ, використовувались ефективні сучасні стеганоаналітичні методи.

Введемо позначення для стеганоаналітичних методів і алгоритмів, що використовуються для порівняння:

- Ker's (2005) [106];
- Liu's (2008) [107];
- HGE (2011) [108];
- NDH COM (2011) [108];
- RLH COM (2011) [108];
- Fused feature (2011) [108];
- Joint feature set (2011) [108];
- SAVV (2012) [105];
- BS (2016) [64].

Результати порівняння інтегральних параметрів ρ розробленого стеганоаналітичного алгоритму СААЗ з сучасними аналогами наведені на рис. 4.5.

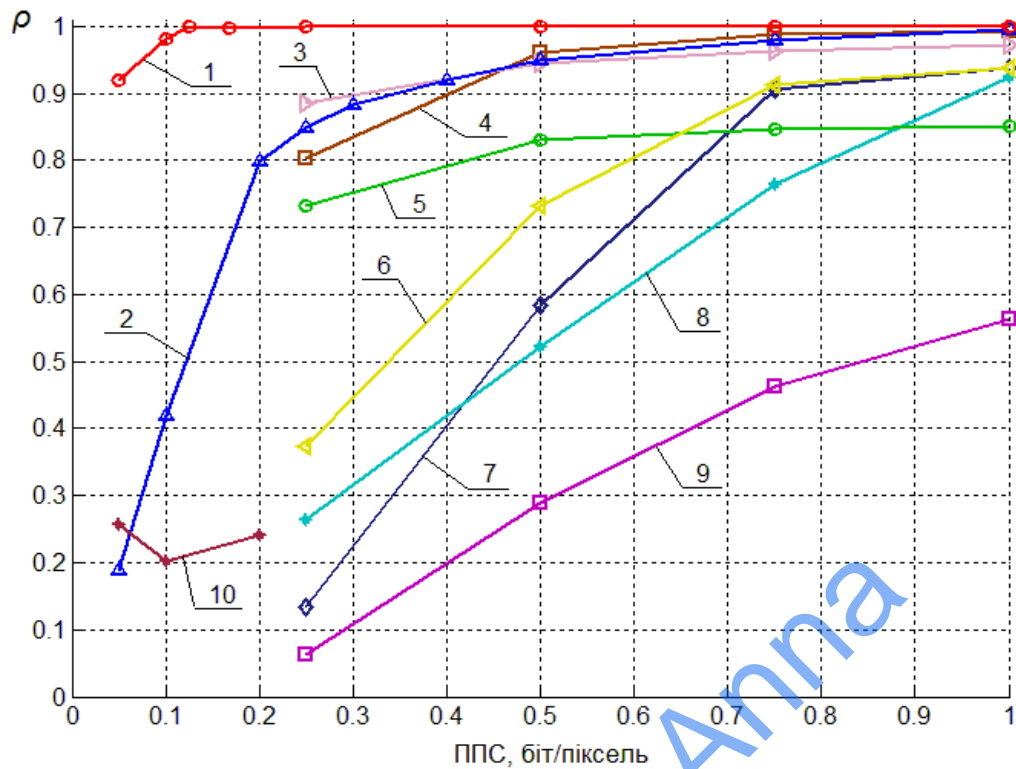


Рис. 4.5 – Результати порівняння інтегрального параметру ρ стеганоаналітичного алгоритму СААЗ з існуючими аналогами: 1 – СААЗ, 2 – SAVV, 3 – Joint feature set, 4 – Liu's, 5 – RLH COM, 6 – Fused feature, 7 – Ker's, 8 – NDH COM, 9 – HGE, 10 – BS

Як видно з рис. 4.5, результати алгоритму СААЗ значно перевищують сучасні аналоги, особливо у випадку малої ППС (0.25 біт/піксель і менше). Найбільш показовим є порівняння розробленого алгоритму з методами SAVV і BS, що аналізують цифрові зображення з малою ППС, значення інтегрального параметру ρ алгоритму СААЗ при ППС 0.05 біт/піксель перевищує аналог SAVV в 5 разів, аналог BS в 3.7 рази, при ППС 0.1 біт/піксель перевищує аналог SAVV в 2.3 рази, аналог BS в 3.7 рази.

Оскільки в різних джерелах точність детектування оцінюється по-різному – в одних випадках за допомогою ROC-кривих, в інших визначається точність детектування AD за формулою (4.1), наведемо результати порівняння значень AD алгоритму СААЗ з наступними сучасними аналогами:

- 31 (2008) [10];
- 32 (2008) [70];
- 33 (2009) [71];
- 34 (2010) [59];
- 35 (2015) [32].

Результати порівняння наведені в табл. 4.8.

Таблиця 4.8 – Порівняння *AD* для розробленого стеганоаналітичного алгоритму САА3 і сучасних аналогів

ППС, біт/піксель	31 2008	32 2008	33 2009	34 2010	35 2015	САА3
0.5	0.9975	-	-	-	-	1
0.4	0.995	-	-	-	-	1
0.3	0.982	-	-	-	-	1
0.25	-	-	-	-	-	1
0.2	0.98	0.9985	0.9993	0.9992	0.9999	1
0.167	-	-	-	-	-	0.9995
0.125	-	-	-	-	-	1
0.1	0.922	0.9943	0.9937	0.9924	0.9971	0.9968
0.05	-	0.9283	0.9319	0.9404	0.9770	0.9865

Як видно з табл. 4.8, і у випадку порівняння точності детектування *AD* алгоритм САА3 є ефективнішим, ніж сучасні аналоги. Максимальна перевага алгоритму САА3 досягається при детектуванні СП, сформованих вбудовою ДІ з ППС 0.05 біт/піксель, де точність виявлення на 1% перевищує аналог 35, і максимально на 5.82% інші аналоги.

4.3. Практичні рекомендації використання розроблених стеганоаналітичних методів і алгоритмів

В підрозділі 4.1 були проведені обчислювальні експерименти, направлені на виявлення ефективності детектування стеганоаналітичних алгоритмів, що реалізують стеганоаналітичні методи, розроблені в розділах 2 і 3. Кожний з алгоритмів (CAA1, CAA2, CAA3v) має як переваги, так і обмеження, пов'язані з форматом використовуваного контейнеру, розміром кадру ЦВ, специфікою ЦВ (повнокольорове або в градаціях сірого). Ці обмеження змушують застосовувати визначені алгоритми в залежності від характеристик ЦВ, що аналізується, тому для ефективного виявлення наявності ДІ в ЦВ рекомендується розробити комплексний метод, що буде реалізовано в наступному підрозділі. З цією метою для кожного з алгоритмів, що реалізують розроблені методи, необхідно оцінити їх переваги і недоліки, область застосування. Порівняння алгоритмів CAA1, CAA2, CAA3v (CAA3) між собою за різними критеріями, що відображають область застосування розроблених алгоритмів, наведені в табл. 4.9.

Таблиця 4.9 – Порівняльний аналіз алгоритмів CAA1, CAA2, CAA3v

Критерій порівняння	CAA1	CAA2	CAA3 / CAA3v
Колірне представлення ЦВ	кольорові, в градаціях сірого		кольорові
Формат контейнерів ЦВ	формати з втратами, формати без втрат		формати з втратами
Обмеження на розмір кадрів	є неефективним при малому розмірі кадрів	ні	є неефективним при малому розмірі кадрів
Заповнення кадрів	повне		часткове / повне
Кількість колірних складових кольорових ЦВ, які використовуються для вбудови ДІ	1, 2 або 3 колірні складові		лише 1 колірна складова

Продовження табл. 4.9

Критерій порівняння		САА1	САА2	САА3 / САА3v
Категорія цифрових контентів з кращою ефективністю детектування		ЦВ, отримані камерами мобільних пристроїв (множина V_1)	ЦВ з множини V_3 (з малим розміром кадрів)	ЦЗ з множин I_3 , I_5 , ЦВ з множини V_2
Висока ефективність виявлення ДІ, вбудованої з ППС (біт/піксель):	0.5	так	так	так
	0.25	так	так	так
	0.167	так	так	так
	0.125	ні / так *	ні / так **	так
	0.1	ні	ні	так
	0.05	ні	ні	так

* для ЦВ, отриманих камерами мобільних пристроїв;

** для ЦВ с малим розміром кадрів.

Таким чином, на основі проведених досліджень можна зробити висновок, що кожний з розроблених методів (САМ1, САМ2, САМ3v) має переваги, яких не мають інші:

- САА1 дозволяє з високою ефективністю виявляти СП, сформовані вбудованою ДІ з ППС не менше 0.125 біт/піксель в одну (дві, три) кольорні складові ЦВ, отриманих камерами мобільних пристроїв, і з ППС не менше 0.167 біт/піксель у випадку інших ЦВ;
- САА2 ефективно виявляє СП, сформовані вбудованою ДІ з ППС не менше 0.167 біт/піксель при інших аналогічних умовах, що гірше, ніж САА1, однак САМ2 є єдиним з розроблених методів, що дозволяє ефективно детектувати ЦВ з малим розміром кадру;
- САА3 і САА3v застосовні лише для кольорових цифрових контентів і ефективні при детектуванні СП, сформованих вбудованою ДІ тільки в одну кольорну складову, у тому числі, з малою ППС.

На основі виявлених переваг і недоліків сформулюємо практичні рекомендації щодо застосування розроблених алгоритмів:

1. Якщо ЦВ (як кольорове, так і в градаціях сірого), що аналізується, має малий розмір кадрів (менше ніж 320×240) слід використовувати алгоритмічну реалізацію методу SAM2.
2. Якщо при стеганоаналізі маються послідовності ЦЗ/кадрів ЦВ в градаціях сірого рекомендується використовувати алгоритмічні реалізації методів САА1 і САА2.
3. При первинному аналізі кольорового ЦВ (послідовності ЦЗ) середнього і великого розміру кадрів слід використовувати алгоритмічні реалізації методів САМ1 і САМ2, що дозволяють виявити вкладення ДІ в однієї, двох і трьох колірних складових.
4. При використанні в процесі стеганоаналізу методу САМ1, на першому кроці його алгоритмічної реалізації слід використовувати методи, що визначають формат оригінального контейнеру: для ЦВ в градаціях сірого – алгоритмічну реалізацію методу МВФКБ [133], для кольорових ЦВ – алгоритмічну реалізацію методу МВФКА.
5. Якщо передбачається, що в якості контейнерів використовуються ЦВ, отримані камерами мобільних пристроїв, пріоритетним є використання алгоритмічної реалізації методу САМ1.
6. Якщо для кольорового ЦВ, що аналізується, алгоритмічною реалізацією методу МВФКА форматом оригінального контейнеру визначений формат з втратами та в результаті первинного аналізу вкладення ДІ виявлено тільки в однієї колірної складової, або зовсім не виявлено, для перевірки отриманого на попередньому етапі результату слід застосовувати алгоритмічну реалізацію методу САМ3v.
7. Якщо передбачається, що у кольоровому ЦВ заповнені не всі кадри, а тільки частина, слід здійснювати покадровий аналіз ЦВ за допомогою алгоритмічної реалізації методу САМ3.

8. Якщо передбачається, що кольорове ЦЗ, для якого оригінальним форматом визначений формат з втратами, містить вкладення лише в однієї колірної складової, необхідно використовувати алгоритмічну реалізацію методу САМЗ.

4.4. Комплексний метод виявлення наявності додаткової інформації в цифрових відео

З урахуванням проведеного порівняння розроблених вище методів і обмежень на їх застосування розроблений комплексний метод виявлення ДІ в ЦВ, що реалізує двох етапний аналіз відеопослідовностей (послідовності ЦЗ):

Крок 1. Визначення кількості кадрів, розміру кадрів ЦВ (M, N), обчислення загальної кількості 4×4 -блоків в кадрі

$$cb = \left[\frac{M}{4} \right] \cdot \left[\frac{N}{4} \right]$$

Крок 2. (Детектування ЦВ з малим розміром кадрів)

Якщо $cb < T_{cb}$, $T_{cb} = 4800$,
то САМ2, перехід на крок 6,
інакше крок 3.

Крок 3. (Детектування ЦВ в градаціях сірого).

Якщо ЦВ має лише одну колірну складову, то:

- 3.1. Визначення формату оригінального контейнеру за допомогою МВФКБ.
- 3.2. Вибір порогових значень T_R , T_G , T_B в залежності від визначеного формату контейнера;
- 3.3. Стеганоаналіз ЦВ за допомогою методів САМ1 та САМ2.
- 3.4. Прийняття рішення щодо наявності/відсутності ДІ у ЦВ (за умови протилежних результатів детектування перевага надається методу, найефективнішому для ймовірного джерела ЦВ – для ЦВ, отриманих камерами мобільних пристроїв перевага надається методу САМ1), перехід на крок 6.

Інакше крок 4.

Крок 4. (Детектування кольорових ЦВ).

- 4.1. Визначення формату оригінального контейнеру за допомогою МВФКА.
- 4.2. Вибір порогових значень T_R , T_G , T_B в залежності від визначеного формату контейнера;
- 4.3. Стеганоаналіз ЦВ за допомогою методу САМ1.
- 4.4. *Якщо* ДІ виявлена у двох або трьох колірних складових ЦВ або визначений у кроці 4.1 формат контейнера без втрат, *то* додаткова перевірка здійснюється методом САМ2, *інакше* додаткова перевірка здійснюється методом САМ3v.
- 4.5. Прийняття рішення щодо наявності/відсутності ДІ у ЦВ (за умови порівняння результатів САМ1 та САМ3v перевага надається останньому; при порівнянні результатів САМ1 і САМ2 перевага надається методу, найефективнішому для ймовірного джерела ЦВ), перехід на крок 6.

Крок 5 (необов'язковий). (Покадровий аналіз ЦВ).

Якщо в п. 4.1 виявлено формат з втратами та в п. 4.3 ДІ виявлена в одній колірній складовій або не виявлена, *то* для кожного кадру ЦВ здійснюється аналіз за допомогою методу САМ3.

Крок 6. Виведення кінцевого результату.

Оцінки ефективності комплексного методу виявлення наявності ДІ в ЦВ співпадають для конкретних випадків з отриманими вище оцінками для його складових.

4.5. Висновки до розділу 4

В розділі розроблені з подальшим аналізом і оцінкою ефективності стеганоаналітичні алгоритми, що реалізують розроблені в розділах 2, 3

методи, на основі чого розроблений комплексний метод виявлення вкладень ДІ в ЦВ (послідовності ЦЗ).

Встановлено:

1. Метод, заснований на врахуванні відносних змін кількості 4×4 -блоків виду (2.2) при первинній і повторній вбудові ДІ (САМ1), дозволяє з високою ефективністю виявляти СП, сформовані вбудовою ДІ методом LSB з ППС не менше 0.125 біт/піксель в одну (дві, три) кольорні складові ЦВ або в кадри ЦВ в градаціях сірого, отриманих камерами мобільних пристроїв (точність детектування при ППС 0.125 біт/піксель досягає 0.94, що на 1.2% перевищує кращий сучасний аналог), в з ППС не менше 0.167 біт/піксель у випадку інших ЦВ – ефективність детектування покращена на 4.41% у порівнянні з кращим аналогом при ППС 0.2 біт/піксель.
2. Метод, заснований на врахуванні характеру змін кількості 4×4 -блоків виду (2.2) при первинній і повторній вбудові ДІ (САМ2), ефективно виявляє СП, сформовані вбудовою ДІ з ППС не менше 0.167 біт/піксель, є єдиним з розроблених методів, що дозволяє ефективно детектувати ЦВ з малим розміром кадру: при ППС 0.167-0.5 біт/піксель помилки другого роду складають 5.1% при відсутності помилок першого роду, при ППС 0.125 біт/піксель помилки першого роду складають 6.12%, помилки другого роду – 5.1%. Метод САМ2 забезпечує високу точність виявлення ДІ в ЦВ при значеннях ППС 0.167-0.5 біт/піксель і на 0.15% перевищує кращий сучасний аналог.
3. Методи, засновані на врахуванні послідовних тріад триплетів (САМ3 і САМ3v), дозволяють виявляти вбудову ДІ як в ЦВ, так і в окремих ЦЗ/кадрах ЦВ з високою ефективністю навіть при малих значеннях ППС (0.05-0.1 біт/піксель). У випадку стеганоаналізу ЦЗ значення інтегрального параметру ρ алгоритму САА3 при ППС 0.05 біт/піксель перевищує аналог SAVV в 5 разів, аналог BS в 3.7 рази, при ППС 0.1 біт/піксель перевищує SAVV в 2.3 рази, BS в 3.7 рази. При

порівнянні точності детектування СААЗ максимально на 2% перевищує аналоги при ППС 0.2-0.5 біт/піксель, на 2.19% при ППС 0.1 біт/піксель і на 4.5% при ППС 0.05 біт/піксель. При виявленні вбудови ДІ в ЦВ результати детектування для ППС 0.1 біт/піксель на 2.3% перевищують кращі з аналогів. максимальна перевага методу СААЗ досягається при виявленні ДІ, вбудованої зі значеннями ППС, меншими за 0.1 біт/піксель: точність детектування перевищує кращий з сучасних аналогів на 14.93% при значенні ППС 0.0625 біт/піксель.

4. Метод СААЗ дає високу ефективність детектування ЦВ у випадку часткового заповнення кадрів, що краще аналогу, особливо у випадку малих значень ППС (0.05-0.1 біт/піксель): при ППС 0.25-0.5 біт/піксель результати є зіставними при різній степені заповнення кадрів, у випадку ППС 0.1 біт/піксель при степені заповнення кадрів 60-80% результати СААЗ на 5.5% перевищують аналог, при степені заповнення кадрів 40% і 20% відповідно на 18% і 32%.

В ході роботи розроблені:

1. Практичні рекомендації використання розроблених стеганоаналітичних методів і алгоритмів, що дає змогу застосовувати конкретні алгоритми в залежності від характеристик ЦВ, що аналізується;
2. Ефективний комплексний метод виявлення ДІ в ЦВ, оцінки ефективності якого співпадають для конкретних випадків з отриманими вище оцінками для його складових.

Таким чином, в розділі 4 показана висока ефективність розроблених стеганоаналітичних методів та їх алгоритмічних реалізацій.

В розділі 4 вирішена задача 5 з переліку задач дисертаційної роботи.

Результати розділу опубліковані в [135-136, 139, 141-143, 145-146].

ВИСНОВКИ

В роботі вирішена важлива науково-практична задача, що полягає у підвищенні ефективності стеганоаналізу для ЦЗ і ЦВ шляхом розробки методів, що детектують в них вкладення конфіденційної інформації LSB-методом, ефективних, у тому числі, при малих (не більше 0.25 біт/піксель) значеннях ППС.

Практична цінність роботи полягає у доведенні здобувачем отриманих наукових результатів до конкретних методів та алгоритмів, що можуть бути використані як складові комплексних систем захисту інформації будь-яких підприємств, організацій, тощо.

В роботі одержані наступні результати:

1. *Отримав подальший розвиток* загальний підхід до аналізу стану і технології функціонування інформаційних систем шляхом встановлення відповідності між властивостями параметрів $n \times n$ -блоку ЦЗ у просторовій області і області сингулярного розкладання відповідної матриці. Доведено, що необхідною і достатньою умовою належності єдиного ненульового сингулярного числа блоку множині натуральних чисел та його кратності n є співпадіння значень яскравості пікселів, що належать блоку. Показано, що виявлена властивість є чутливою до будь-яких збурних дій, а тому використовується як основа теоретичного базису розроблених стеганоаналітичних методів SAM1 і SAM2 для аналізу ЦВ, який проводиться у просторовій області контенту, що забезпечує їх високу ефективність, у тому числі в умовах ППС, меншій за 0.25 біт/піксель.
2. *Вперше* на основі аналізу змін кількості блоків з однаковими значеннями яскравості в матрицях ЦК в результаті стеганоперетворення LSB-методом послідовності ЦЗ/кадрів ЦВ розроблені стеганоаналітичні методи SAM1 і SAM2, ефективні, у тому числі, для малої ППС, кадрів малого розміру, незалежно від пристрою, за допомогою якого отримане ЦВ, його формату зберігання (з/без втрат) та кількості колірних

складових, що були задіяні при стеганоперетворенні. Метод САМ1 дозволив підвищити ефективність стеганоаналізу для ЦВ, отриманих камерами мобільних пристроїв в умовах ППС 0.125 біт/піксель на 1.2%. При стеганоаналізі з використанням САМ2 ЦВ з малим розміром кадрів в умовах ППС 0.167-0.5 біт/піксель помилки першого роду відсутні, при ППС 0.125 біт/піксель вони складають 6.12%; помилки другого роду – 5.1%. Методом САМ2 досягнутий абсолютний результат детектування наявності ДІ у ЦВ з середнім і великим розміром кадрів – $AD=1$ при ППС 0.167-0.5 біт/піксель, що не досягалось аналогами та дозволило підвищити ефективність стеганоаналізу ЦВ максимально на 7.5% (при ППС 0.2 біт/піксель).

3. *Вперше* на основі аналізу зміни кількості послідовних тріад кольорних триплетів у матриці унікальних кольорів ЦЗ/кадрів ЦВ в результаті вбудови ДІ методом LSB в одну довільну кольірну складову ЦК, які початково зберігалися в форматах з втратами, розроблено метод САМ3, ефективний, в тому числі, для малої ППС, ефективність якого перевищує сучасні аналоги: для ППС 0.05/0.1 біт/піксель точність детектування підвищена на 4.5/2.19% відповідно, інтегральний параметр у 3.7/2.3 рази відповідно. Метод САМ3v, що є результатом адаптації САМ3 для ЦВ, дозволив підвищити ефективність стеганоаналізу для малих значень ППС максимально на 14.93% (ППС 0.0625 біт/піксель), та забезпечив високу ефективність стеганоаналізу ЦВ ($AD = 0.9391$) в умовах, де сучасні аналоги є недієздатними (ППС 0.05 біт/піксель).
4. *Вперше* на основі отриманих практичних рекомендацій застосування розроблених стеганоаналітичних методів, які забезпечують вибір конкретного методу в залежності від характеристик ЦВ, що аналізується, і ефективного удосконалення стеганоаналітичного методу САМ3 з метою використання його для визначення формату (з/без втрат) оригінального контейнеру, для якого помилки першого роду склали 3%, другого роду – 4.5%, розроблено комплексний метод виявлення

вкладень ДІ в ЦВ, ефективний, у тому числі при малих значеннях ППС, при різній кількості заповнених колірних складових контейнерів, в якості яких можуть виступати як кольорові ЦВ, так і відео в градаціях сірого, незалежно від формату (з/без втрат); різній степені заповненості кадрів цифрового відео.

5. Алгоритмічні реалізації всіх розроблених методів мають поліноміальну обчислювальну складність: для САА1 і САА2 обчислювальна складність визначається як $P \cdot \underline{O}(M^2)$, де $M \times M$ – розмір матриці ЦЗ/кадру ЦВ, P – кількість зображень/кадрів у послідовності ЦЗ/ЦВ; для алгоритмічних реалізацій методів САМЗ, МВФКА – $\underline{O}(M^4)$; для алгоритму САА3v – $P \cdot \underline{O}(M^4)$, що дає можливість для їх практичного використання для стеганоаналізу ЦЗ/ЦВ будь-якого, у тому числі значного, розміру.

Акхматметієва А.І.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аграновский, А.В., Балакин, А.В., Грибунин, В.Г., Сапожников, С.А.: Стеганография, цифровые водяные знаки и стеганоанализ. Москва, Вузовская книга (2009)
2. Конахович, Г.Ф., Пузыренко, А.Ю.: Компьютерная стеганография: теория и практика. Киев, «МК-Пресс» (2006)
3. Грибунин, В.Г., Оков, И.Н., Туринцев, И.В.: Цифровая стеганография. Киев, Солон-Пресс (2002)
4. Bohme, R.: Advanced statistical steganalysis. Springer (2010)
5. Швидченко, И.В. Методы стеганоанализа для графических файлов. Искусственный интеллект. № 4, 697-705 (2010)
6. Швідченко, І.В.: Методи виявлення стеганографічного приховування інформації у зображеннях. Автоматика, вимірювання та керування. 198-203 (2012)
7. Смірнов, О.А., Мелешко, Є.В.: Дослідження методів стегоаналізу цифрових зображень. Наука і техніка Повітряних Сил Збройних Сил України. №2 (8), 92 – 99 (2012)
8. Кошкина, Н.В.: Стеганоанализ изображений в формате jpeg на базе атаки контрольным внедрением. Управляющие системы и машины. № 4, 3–17 (2014)
9. Жилкин, М.Ю., Меленцова, Н.А., Рябко, Б.Я.: Метод выявления скрытой информации, базирующийся на сжатии данных. Вычислительные технологии. Том 12, Специальный выпуск 4, 26-31 (2007)
10. Жилкин, М.Ю.: Стеганоанализ графических данных в различных форматах. Доклады Томского государственного университета систем управления и радиоэлектроники. №2 (18), 63-64 (2008)
11. Монарев, В.А.: Сдвиговой метод обнаружения скрытой информации. Вестник Сибирского государственного университета телекоммуникаций и информатики. № 4, 62-68 (2012)

12. Мерков, А.Б.: Введение в методы статистического обучения: конспект лекций <http://www.recognition.mccme.ru/pub/RecognitionLab.html/slbook.pdf> (2014). Дата обращения 30.10.2015
13. Jina Chanu Yambem, Kh. Manglem Singh, Themrichon Tuithung: Image steganography and steganalysis: a Surveyю. International Journal of Computer Applications. Volume 52, No.2, 1-11 (2012)
14. Manveer Kaur, Gagandeep Kaur: Review of Various Steganalysis Techniques. International Journal of Computer Science and Information Technologies. Vol. 5(2), 1744-1747 (2014)
15. Rita Chhikara, Latika Singh: A review on digital image steganalysis techniques categorized by features extracted. International Journal of Engineering and Innovative Technology. Volume 3, Issue 4, 203 -213 (2013)
16. Кошкина, Н.В.: Обзор и классификация методов стеганоанализа. Управляющие системы и машины. № 3, 3-12 (2015)
17. Швідченко І.В.: Аналіз програмного забезпечення зі стеганоаналізу. Искусственный интеллект. № 3, 487–495 (2012)
18. Hawi T.A., Qutayari M.A., Barada H.: Steganalysis attacks on stego images using stego-signatures and statistical image properties In: TENCON'2004, Region 10 Conf. No. 2, 104–107 (2004)
19. M. Niimi, T. Ei, H. Noda et al.: An attack to BPCS-steganography using complexity histogram and countermeasure. In: Int. Conf. on Image Processing, ICIP. No. 5, 733–736 (2004)
20. Westfeld, A., Pfitzmann, A.: Attacks on steganographic systems. In: Proc. of Information Hiding, Third Int. Workshop, 61-75, Dresden, Germany, September 28 – October 1, 1999
21. Fridrich, J., Goljan, M.: Practical steganalysis of digital images-state of the art. In: Proc. SPIE Photonics West, Electronic Imaging (2002), Security and Watermarking of Multimedia Contents, Vol. 4675, San Jose, CA, Jan 2002

22. Chandramouli, R., Kharrazi, M., Memon, N.: Image steganography and steganalysis: Concepts and practices. In: Proc. 2nd Int. Workshop Digital Watermarking, 35-49, Seoul, Korea, January 2003
23. Zhang, T., Ping, X.: A fast and effective steganalytic technique against JSteg-like algorithms. In: ACM Symposium on Applied Computing, 307-311, Florida, USA, March 9 – 12, 2003
24. Fridrich, J., Du, R., Meng, L.: Steganalysis of LSB encoding in color images. In: Proc. IEEE Int. Conf. on Multimedia and Expo, New York, July 31–August 2, 2000
25. Fridrich, J., Goljan, M., Du, R.: Detecting LSB steganography in color and gray-scale images. IEEE Multimedia Magaz. Special Issue on Security, 22-28 (2001)
26. Shunquan Tan, Bin Li: Targeted Steganalysis of Edge adaptive Image Steganography Based on LSB Matching Revisited using B-Spline Fitting. IEEE Signal Processing Letters. Vol. 19, No. 6, 336-339 (2012)
27. Yu, X, Wang, Y., Tan, T.: On estimation of secret message length in JSteg-like steganography. In: Proc. of 7th ICPR, 2004
28. Fridrich, J.: Feature-based steganalysis for JPEG images and its implications for future design of steganographic schemes. Proc. Inf. Hiding Workshop, Lecture Notes in Computer Science. Vol. 3200, 67–81 (2004)
29. Shi, Y. Chen, C., Chen, W.: A Markov process based approach to effective attacking JPEG steganography Information Hiding. In: Proceedings of the 8th International Workshop, 249–264, Springer, Berlin, 2006
30. Dekun Zou, Yun Q. Shi, Wei Su, Guorong Xuan: Steganalysis based on Markov model of threshold prediction-error image. IEEE, ICME, 1365-1368 (2006)
31. Wing W. Y NG, Zhi-Min He, Patrick P.K Chan, Daniel S. Yeung: Blind Steganalysis with High Generalization Capability for different Image Databases. In: Proceedings of the 2011 International Conference on Machine Learning and Cybernetics, 1690-1695, Guilin, 10-13 July, 2011

32. Su Jinyang, Zeng Xianting, Wang Lei: Steganalysis using regional correlation and second-order Markov features. *International Journal of Security and Its Applications*. Vol. 9, № 1, 69-76 (2015)
33. Avcibas, I., Memon, N., Sankur, B.: Steganalysis using image quality metrics. *IEEE Transactions on Image Processing*. Vol. 12, No. 2, 221-229 (2003)
34. Minh N. Do, Martin Vetterli: Wavelet-based texture retrieval using generalized Gaussian density and Kullback–Leibler distance. *IEEE Trans. Image Process.* Vol. II, 146–158 (2002)
35. Shaohui Liu, Hongxun Yao, Wen Goa: Steganalysis based on wavelet texture analysis and neural network. In: *Proc. of WCICA 2004, Hangzhou, China, 2004*
36. Farid, H.: Detecting hidden messages using higher-order statistical models. In: *Proc. IEEE Int. Conf. Image Process.*, Vol. 2, 905–908, Rochester, NY, September 2002
37. Lyu, S., Farid, H.: Steganalysis using color wavelet statistics and one-class vector support machines. *Proc. SPIE, Security, Steganography, Watermarking of Multimedia Contents*. Vol. 5306, 35–45 (2004)
38. Xuan, G.: Steganalysis based on multiple features formed by statistical moments of wavelet characteristic functions. *Lecture Notes in Computer Science*. Vol. 3727, 262–277 (2005)
39. Wang, Y., Moulin, P.: Optimized feature extraction for learning based image steganalysis. *IEEE Trans Inf Forensics Secur.* Vol. 2, No. 1, 262-277 (2005)
40. Kodovsky, J., Fridrich, J., Holub, V.: Ensemble classifier for steganalysis of digital media. *IEEE Trans. Inf. Forensics Security*. Vol. 7, No. 2, 432–444 (2012)
41. Fengyong Li, Xinpeng Zhang, Bin Chen, Guorui Feng: JPEG Steganalysis With High-Dimensional Features and Bayesian Ensemble Classifier. *IEEE signal processing letters*. Vol. 20, No. 3, 233-236 (2013)
42. Guorong Xuan, Yun Q. Shi, Cong Huang, Dongdong Fu, Xiuming Zhu, Peiqi Chai, Jianliang Gao: Steganalysis using high-dimensional features derived

- from Co-occurrence matrix and class-wise non-principal components analysis (CNPCA). IWDW. LNCS 4283, 49-60 (2006)
43. Ziwen Sun, Maomao Hui, Chao Guan: Steganalysis Based on Co-occurrence Matrix of Differential Image Intelligent Information Hiding and Multimedia Signal Processing. In: Proc. of International Conference (IIHMSP '08), 1097-1100, 15-17 Aug. 2008
 44. Kerke, H.B., Athawale, A.A., Patki, S.A.: Steganalysis of LSB embedded images using gray level Co-Occurence matrix. International Journal of Image Processing (IJIP). Volume 5, Issue 1, 36-45 (2011)
 45. Kodovský, J. JPEG-Compatibility Steganalysis Using Block-Histogram of Recompression Artifacts. In: Proc. of 14th Information Hiding Conference, Vol. 7692, 78-93, Berkeley, CA, May 15–18, 2012
 46. Deng Qian-lan: The blind detection of information hiding in color image. Computer Engineering and Technology (ICCET), 2nd International Conference on, 2010, Vol. 7, V7-346-V7-348 (2010)
 47. Jing Dong, Tieniu Tan: Blind Image Steganalysis Based on Run-Length Histogram Analysis. In: National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, ICIP 2008, 2064-2067 (2008)
 48. Xiaochuan Chen, Yunhong Wang, Tieniu Tan, Lei Guo: Blind Image Steganalysis Based on Statistical Analysis of Empirical Matrix Pattern Recognition. In: 18th International Conference on ICPR 2006, Vol. 3, 1107-1110 (2006)
 49. Avcibas, I., Kharrazib, M., Memon, N., Sankur, B.: Image Steganalysis with Binary Similarity Measures. EURASIP JASP. No. 17, 2749-2757 (2005)
 50. Jing-Qu Lin, Shang-Ping Zhong: JPEG Image Steganalysis Method Based on Binary Similarity Measures. Proceedings of Eighth International Conference on Machine Learning and Cybernetics, 2238-2243, Baoding, 12-15 July 2009
 51. Hedieh Sajedi, Mansour Jamzad: A Steganalysis Method Based on Contourlet Transform Coefficients. International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2008, 245-248 (2008)

52. Sallee, P.: Model-based steganography. In: Proc. Int. Workshop on Digital Watermarking, 154-167, Seoul, Korea, 2003
53. Fridrich, J., Goljan, M., Soukal, D.: Perturbed quantization steganography with wet paper codes. In: Proc. ACM Multimedia Workshop, Germany, 2004
54. Solanki, K., Sarkar, A., Manjunath B.S.: YASS: Yet another steganographic scheme that resists blind steganalysis. In: 9th Int. Workshop on Info. Hiding, Saint Malo, Brittany, France, 2007
55. Sheikhan, M., Moin, M.S., Pezhmanpour, M.: Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform. Intelligent Systems Design and Applications (ISDA), 10th International Conference on 2010, 368 –372 (2010)
56. Santhosh, S., Arangasamy, S.: Steganalysis in estimation of spatial ± 1 steganography using JPEG 2000 standards. International Journal of Innovative Research in Science, Engineering and Technology. Vol. 4, Iss. 6, 676-681 (2015)
57. Prabhu Kumar, Nikhil Tirpathi, Michael, G.: Pixel steganalysis – a novel approach in image steganography using F5 algorithm. International Journal of Innovative Research in Computer and Communication Engineering. Vol. 3, Iss. 3, 2452-2457 (2015)
58. Tong Qiao, Florent Reiraint, Remi Cogranne, Cathel Zitzmann: Steganalysis of JSteg algorithm using hypothesis testing theory. In: EURASIP Journal on Information Security (2015)
59. Pevny, T., Bas, P., Fridrich, J.: Steganalysis by subtractive pixel adjacency matrix. IEEE Transactions on Information Forensics and Security. No. 2, 215-224 (2010)
60. Yamini, B., Sabitha, R.: Blind steganalysis: to analyse the detection rate of stego images using different steganalytic techniques with support vector machine classifier. International journal of computer applications. No. 2, 22-25 (2014)

61. Ashu, Rita Chhikara: Performance evaluation of first and second order features for steganalysis. *International Journal of Computer Applications*. Vol. 92, No. 16, 17-22 (2014)
62. Tejashree Shinde, Ujwala Chaudhari, Rushali Bodke: Image steganalysis based on statistical evidence by using SVM. *International Journal of Innovative Research in Computer and Communication Engineering*. Vol. 2, Iss. 2, 3007-3012 (2014)
63. Swagota Bera, Monisha Sharma: Blind JPEG steganalysis using statistical moment and second order statistics. *International Journal of Engineering Research and General Science*. Vol. 3, Iss. 5, 632-638 (2015)
64. Swagota Bera, Monisha Sharma: Performance evaluation of universal steganalysis using machine learning tool. *International Journal of Advanced Research in Computer Science and Software Engineering*. Volume 6, Issue 2, 258-263 (2016)
65. Xiuhui Ge, Hao Tian: Dimensionality reduction for classification of blind steganalysis. *Journal of Software Engineering*. No. 9(4), 721-734 (2015)
66. Haodong Li, Weiqi Luo, Xiaoqing Qiu, Jiwu Huang: Identification of image operations based on steganalytic features. Cornell University Library <https://arxiv.org/abs/1503.04718> (2015)
67. Christaline, J.A., Ramesh, R., Vaishali, D.: Bio-inspired computational algorithms for improved image steganalysis. *Indian Journal of Science and Technology*. Vol. 9(10), 1-10 (2016)
68. Christaline, J.A., Ramesh, R., Vaishali, D.: Optimized JPEG steganalysis. *International Journal of Multimedia and Ubiquitous Engineering*. Vol. 11, No. 1, 385-396 (2016)
69. Seongho Cho, Byung-Ho Cha, Martin Gawecki, C.-C. Jay Kuo: Block-based image steganalysis: algorithm and performance evaluation. *J. Vis. Commun. Image R.* No. 24, 846–856 (2013)

70. Chen, C., Shi, Y.Q.: JPEG Image Steganalysis Utilizing both Intrablock and Interblock Correlations. IEEE International Symposium on Circuits and Systems, 3029-3032, Seattle, Washington, USA, 2008
71. Huang, F., Huang, J.: Calibration based universal JPEG steganalysis. Science in China series F: Information sciences. Vol. 52, No. 2, 260-268 (2009)
72. Yamini, B., Sabitha, R.: Universal steganalysis: defend against adaptive steganographic attack using MX-quadtrees neighbor finding mechanism. Indian Journal of Computer Science and Engineering . Vol. 6, No. 6, 173-181 (2015-2016)
73. Rajendraprasad, K., Narasimha, V.B.: Steganography image detection using different Steganalysis techniques with Markov chain features. International Journal of Applied Engineering Research. Vol. 11, No. 1, 392-395 (2016)
74. Nissar, A., Mir, A.H.: Texture based steganalysis of grayscale images using neural network. Signal Processing Research. Vol. 2, Iss. 1, 17-24 (2013)
75. Sujatha, P., Purushothaman, S., Rajeswari, P.: Computational complexity evaluation of ANN algorithms for image steganalysis. International Journal of Latest Trends in Engineering and Technology (IJLTET). Vol. 3, Iss. 3, 229-233 (2014)
76. Sarab M. Hameed, Rasha A. Mohammed, Baraa' A. Attea: Fuzzy based clustering for grayscale image steganalysis. Iraqi Journal of Science. Vol. 56, No. 2A, 1161-1175 (2015)
77. Fridrich, J., Pevný, T., Kodovský J.: Statistically undetectable JPEG steganography: Dead ends, challenges, and opportunities. In J. Dittmann and J. Fridrich, editors, Proceedings of the 9th ACM Multimedia & Security Workshop, 3–14, Dallas, TX, September 20–21, 2007.
78. Westfeld, A.: High capacity despite better steganalysis (F5 – a steganographic algorithm). In I. S. Moskowitz, editor, Information Hiding, 4th International Workshop, volume 2137 of Lecture Notes in Computer Science, 289–302, Pittsburgh, PA, April 25–27, 2001

79. Fawcett, T.: An introduction to ROC analysis. Pattern Recognition Letters. No. 27, 861–874 (2006)
80. Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi: A Survey on Image Steganography and Steganalysis. Journal of Information Hiding and Multimedia Signal Processing. Vol. 2, No. 2, 142-172 (2011)
81. Receiver operating characteristic. From Wikipedia, the free encyclopedia. https://en.wikipedia.org/wiki/Receiver_operating_characteristic Accessed 10.02.2016
82. Зацеркляний, М.М., Кириченко, Г.С.: Дослідження методу RS-стеганоаналізу. Сборник научных трудов "Вестник НТУ "ХПИ": Інформатика і моделювання. № 49, 64-71 (2008)
83. Корольов, В.Ю., Поліновський, В.В., Герасименко, В.А.: RS-стеганоаналіз. Принципи роботи, недоліки та концепція методу його обходу. Вісник Вінницького політехнічного інституту. № 6, 66-71 (2010)
84. Солодуха, Р.А., Атласов, И.В.: Усовершенствование метода RS-стеганоанализа применением его к группам пикселей различного размера. Вестник Воронежского института МВД России. № 2, 1-6 (2012)
85. Geetha, S., Sindhu, S., Kamaraj, N.: Close color pair signature ensemble adaptive threshold based steganalysis for LSB embedding in digital images. Transactions on Data Privacy. Vol.1, Iss.3, 140-161 (2008)
86. Mitra, S., Roy, T., Mazumdar, D., Saha, A.B.: Steganalysis of LSB Encoding in Uncompressed Images by Close Color Pair Analysis. In: Proc. of IT Kanpur Hackers' Workshop 2004 (ИТКНАСК04), 23–24, 23-24 Feb 2004
87. Рудницький, В.Н., Узун, И.А.: Стеганоаналитический алгоритм для изображений, подвергавшихся операции сжатия с потерями. Захист інформації. Том 15, № 2, 122-127 (2013)
88. Рудницький, В.Н., Узун, И.А.: Стеганоаналитический алгоритм детектирования метода модификации наименьшего значащего бита для контейнеров, хранимых в форматах без потерь. Інформатика та математичні методи в моделюванні. Т. 2, № 3, 238-245 (2012)

89. Узун, И.А.: Стеганоанализ цифровых изображений, хранящихся в произвольных форматах. Информатика та математичні методи в моделюванні. Т. 3, № 2, 179-189 (2013)
90. Jun Zhang, Ingemar J. Cox, Gwenael Doerr: Steganalysis for LSB Matching in images with high-frequency noise. In: Proc. IEEE Workshop on Multimedia Signal Processing, 385-388 (2007)
91. Брюханова, Я.А.: Стеганоаналіз на основі статистичних характеристик зображень. Вісник Східноукраїнського національного університету ім. В. Даля. №8 (126), 102-106 (2008)
92. Der-Chyuan Lou, Chen-Hao Hu, Chung-Cheng Chiu: Steganalysis of histogram modification reversible data hiding scheme by histogram feature coding. International Journal of Innovative Computing, Information and Control. Vol. 7, No. 11, 6571-6583 (2011)
93. Dariush Alimoradi, Maryam Hasanzaden: The effect of variance difference of dyadic quantized histograms on universal steganalysis. International Journal of Computer Applications. Vol. 62, No. 8, 19-24 (2013)
94. Sunaina Verma, Sandeep Sood, Sukhjeet Kaur Ranade: Relevance of steganalysis using DIH on LSB steganography. International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 4, Iss. 2, 835-838 (2014)
95. Чуи, Ч.: Введение в вейвлеты. Москва, Мир (2001)
96. Яковлев, А.Н.: Введение в вейвлет-преобразования. Новосибирск, Изд-во НГТУ (2003)
97. Siwei Lyu, Hany Farid: Steganalysis using higher-order image statistics. IEEE Transactions on information forensics and security. Vol. 1, No. 1, 111-119 (2006)
98. Hamed Modagheh, Seyed Aliresa Seyedin: Active steganalysis of transform domain steganography based on sparse component analysis. Journal of Information Systems and Telecommunication. Vol. 3, No. 2, 75-84 (2015)

99. Progonov, D., Kushch, S.: Passive steganalysis of multidomain embedding methods. International Journal “Information Theories and Applications”. Vol. 22, No. 1, 86-99 (2015)
100. Manisha Saini, Rita Chhikara: DWT feature based blind image steganalysis using neural network classifier. International Journal of Engineering Research & Technology (IJERT). Vol. 4, Iss. 04, 776-782 (2015)
101. Ramandeep Kaur, Arshdeep Singh: Steganalysis using hopping cluster algorithm. International Journal Of Engineering And Computer Science. Vol. 4, Iss. 2, 10356-10358 (2015)
102. Sarita R. Visavalia, Amit Ganatra: Improving blind image steganalysis using genetic algorithm and fusion technique. International Conference on Advances in Engineering & Technology – 2014 (ICAEET-2014), 40-46 (2014)
103. Кобозева, А. А., Хорошко, В.А.: Анализ информационной безопасности. Киев, ГУИКТ (2009)
104. Бобок, И.И.: Стеганоаналитический метод для цифрового сигнала-контейнера, хранящегося в формате с потерями. Сучасний захист інформації. №2, 50–60 (2011)
105. Бобок, И.И.: Использование метода анализа гос-кривых для комплексной оценки эффективности стеганоаналитического метода. Інформатика та математичні методи в моделюванні. Т.2, № 3, 221-230 (2012)
106. Ker, A.D.: Steganalysis of LSB matching in grayscale images. IEEE Signal Processing Letters. Vol.12, No.6, 441–444 (2005)
107. Liu, Q.Z., Sung, A.H.: Image complexity and feature mining for steganalysis of least significant bit matching steganography. Information Sciences. Vol.178, No.1, 21-36 (2008)
108. Zhihua Xia, Lincong Yang: A Learning-Based Steganalytic Method against LSB Matching Steganography. Radioengineering. Vol.20, No.1, 102-109 (2011)

109. Vinod Pankajaksan, Ho A.T.S.: Improving video steganalysis using temporal correlation. Third international conference on intelligent information hiding and multimedia signal processing, 2007. Vol. 1, 287-290 (2007)
110. Udit Budhia, Deepa Kundur: Digital video steganalysis exploiting collusion sensitivity. Proc. of SPIE. Vol. 5403, 210-221 (2004)
111. Udit Budhia, Deepa Kundur, Takis Zourntos: Digital video steganalysis exploiting statistical visibility in the temporal domain. IEEE Transactions on information forensics and security. Vol. 1, No. 4, 502-516 (2006)
112. Shi, Y.Q., Xuan, G., Zou, D., Gao, J., Yang, C., Zhang, Z., Chai, P., Chen, W., Chen, C.: Steganalysis based on moments of characteristic functions using wavelet decomposition, prediction-error image, and neural network. In: Proceedings of the IEEE International Conference on Multimedia and Expo, July 2005
113. Songbin Li, Peng Liu, Qiongxing Dai, Xiuhua Ma, Haojiang Deng: Detection of Information Hiding by Modulating Intra Prediction Modes in H.264/AVC. In: Proceedings of the 2nd International Conference on Computer Science and Electronics Engineering (ICCSEE 2013), 590-593 (2013)
114. Kaicheng Wu: Research of Video Steganalysis Algorithm Based on H265 Protocol. MATEC Web of Conferences 25, 2015, 03003-1 - 03003-7 (2015)
115. Su, Y., Zhang, C., Wang, L., Zhang, C.: A New Video Steganalysis based on Mode Detection. In: Proceedings of the International Conference on Audio, Language and Image Processing, 1507-1510, Shanghai, China, July 2008
116. MSU Stego Video http://www.compression.ru/video/stego_video/index.html
Accessed 14.11.2014
117. Xikai Xu, Jing Dong, Tieniu Tan: Universal spatial feature set for video steganalysis. 19th IEEE International Conference, 245-248, 2012
118. Hartung, F., Girod, B.: Watermarking of Uncompressed and Compressed Video. Signal Processing. Vol. 66, Issue 3, 283-301 (1998)
119. Kalker, T. Depovere, G., Haitsma, J.: A Video Watermarking System for Broadcast Monitoring. Proc. of SPIE. Vol. 3657, 103-112 (1999)

120. Jainky, J.S., Kundur, D., Jainky, J.S., Halverson, D.R.: Towards Digital Video Steganalysis using Asymptotic Memoryless Detection. In: Proceedings of the 9th International Workshop on Multimedia and Security, 161-168, 2007
121. Xikai Xu, Jing Dong, Wei Wang, Tieniu Tan: Video steganalysis based on the constraints of motion vectors. ICIP. 4422-4426 (2013)
122. Kasim Tasdemir, Fatih Kurugollu, Sakir Sezer: Spatio-temporal rich model-based video steganalysis on cross sections of motion vectors planes. IEEE Transactions on image processing. Vol. 25, No. 7, 3316-3328 (2016)
123. Venkatarami, Reddy D., Rao T. Narasimha, Rao, K. Saideswara: A novel approach for detection of video steganalysis defenses against covert communications motion vector based steganography by AOSO MV value. International journal of scientific engineering and technology research. Vol. 5, Iss. 4, 622-626 (2016)
124. Punithalatha, M., Amsaveni, A.: Reversion-based features video steganalysis for images and images fusion technique using fuzzy logic. International Conference on Innovations In Intelligent Instrumentation, Optimization And Signal Processing "ICIINOSP-2013", 15-22, 2013
125. Гонсалес, Р., Вудс, Р., Эддинс, С.: Цифровая обработка изображений в среде MATLAB. Москва, Техносфера (2006)
126. Кобозева, А.А., Ахмаметьева, А.В., Ефименко, А.А.: Стеганоаналитический метод для цифровых контейнеров, хранящихся в формате без потерь. Інформаційна безпека. №1(13), 31-42 (2014)
127. Деммель, Дж.: Вычислительная линейная алгебра. Теория и приложения. Москва, Мир (2001)
128. Кобозева, А.А., Мельник, М.А.: Анализ чувствительности сингулярных векторов матрицы изображения-контейнера как основа стеганоалгоритма, устойчивого к сжатию с потерями. Захист інформації. Том 15, №2, 88–96 (2013)

129. Парлетт, Б.: Симметричная проблема собственных значений. Численные методы. Москва, Мир (1983)
130. Гантмахер, Ф.Р.: Теория матриц. Москва, Физматлит (2004)
131. NRCS Photo Gallery. United States Department of Agriculture. Washington, USA. <http://photogallery.nrcs.usda.gov> Дата обращения: 26.07.2012
132. WallpapersCraft: Широкоформатные обои на рабочий стол, картинки, фото. <http://wallpaperscraft.ru/> Дата обращения: 21.11.2014
133. Бобок, И.И.: Выявление цифровых изображений, пересохраненных в формат без потерь из формата с потерями, как составная часть стеганоанализа. Сучасна спеціальна техніка. №3, 64-70 (2013)
134. Ахмаметьева, А.В.: Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров. Информатика та математичні методи в моделюванні. Т.5, № 4, 367-375 (2015)
135. Ахмаметьева, Г.В.: Стеганоаналітичний алгоритм для цифрових контейнерів, збережених в форматах з втратами. Сучасна спеціальна техніка. № 3 (46), 31-38 (2016)
136. Маєвський, Д.А., Ахмаметьева, Г.В.: Стеганоаналітичний алгоритм, заснований на аналізі просторової області цифрових контейнерів. Информатика та математичні методи в моделюванні. Т.6, №1, 52-60 (2016)
137. Ахмаметьева, А.В.: Стеганоаналитический метод, основанный на анализе пространственной области цифровых контентов. Международная научно-техническая конференция «Современные информационно-телекоммуникационные технологии», Т. II, 83-84, Киев, 17-20 ноября 2015
138. Ахмаметьева, А.В.: Стеганоанализ цифровых видео, основанный на анализе пространственной области. V Міжнародна науково-практична конференція «Інформаційні управляючі системи та технології» (ІУСТ-Одеса - 2016), 161-163, Одеса, 20-22 вересня 2016

139. Jun Zhang, Yuping Hu, Zhibin Yuan: Detection of LSB Matching steganography using the envelope of histogram. Journal of computers. Vol.4, No.7, 646-653 (2009)
140. Бобок, И.И., Кобозева, А.А.: Стеганоанализ как частный случай анализа информационной системы. Сучасна спеціальна техніка. № 2 (25), 21-33 (2011)
141. Ахмаметьева, А.В.: Стеганоанализ цифровых изображений, хранящихся в формате с потерями. Захист інформації. Випуск 23, 135-145 (2016)
142. Akhmametiieva, A.: Method of detection the fact of compression in digital images as an integral part of steganalysis. Інформатика та математичні методи в моделюванні. Т.6, №4, 357-364 (2016)
143. Ахмаметьева, Г.В.: Детектування стеганоповідомлень, вбудованих методом LSB Matching у цифрові контейнери в форматах з втратами. V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», 106-107, Львів, 2-3 червня 2016
144. Ferreirf, A.M.: An overview on hiding and detecting stego-data in Video streams. Research project by University of Amsterdam “System & Network Engineering” (2015)
145. Ахмаметьева, А.В.: Выявление области применения стеганоаналитического подхода, основанного на анализе пространственной области цифровых контентов. Problemele energeticii regionale. Электронный журнал Академии наук Республики Молдова. № 2 (31), 104-111 (2016)
146. Ахмаметьева, Г.В.: Виявлення області застосування стеганоаналітичного алгоритму, що аналізує просторову область цифрових зображень. V Міжнародна науково-технічна конференція «Інформаційні системи та технології» (ІСТ-2016), 287-288, Харків-Коблево, 12-17 вересня 2016

Додаток А.

АКТИ ВПРОВАДЖЕННЯ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЙНОЇ РОБОТИ

ЗАТВЕРДЖУЮ

Директор компанії

ТОВ Компанія «Планета-Юг»

О.А. Сиропятов

«12» грудня 2016 р.



АКТ

про впровадження результатів дисертаційної роботи на тему
**«ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СТЕГНОАНАЛІЗУ ДЛЯ
 ЦИФРОВИХ ЗОБРАЖЕНЬ І ВІДЕО»**

отриманих

Ахмаметьєвою Ганною Валеріївною

Члени комісії у складі:

- технічний директор Каліновський Р.Ю.
- начальник виробничо-технічного відділу Лавровський В.М.
- керівник групи монтажників Кисіль А.В.

Результати дисертаційної роботи Ахмаметьєвої Г.В. за темою «Підвищення ефективності стеганоаналізу для цифрових зображень і відео», а саме алгоритми виявлення наявності вбудови додаткової інформації у цифрових контентах (цифрових зображеннях та відео), що аналізують просторову область цифрових контентів, використані у діяльності компанії ТОВ Компанія «Планета-Юг», що дозволило підвищити надійність комплексної системи захисту інформації: використання означених алгоритмів для перевірки цілісності цифрових зображень дозволило зменшити помилки першого роду на 6,7% в умовах порушення цілісності шляхом накладання різноманітних шумів та фільтрації зображення.

Даний акт не є основою для фінансових розрахунків.

Технічний директор

Р.Ю. Каліновський

Начальник виробничо-технічного відділу

В.М. Лавровський

Керівник групи монтажників

А.В. Кисіль

ЗАТВЕРДЖУЮ

Проректор з наукової та науково-педагогічної роботи
Одеського національного політехнічного університету
д.т.н., проф., Дмитришин Д.В.

« ___ » _____ 2016р.

АКТ

про впровадження у навчальний процес кафедри
Інформатики та управління захистом інформаційних систем
результатів дисертаційної роботи
Ахматєєвої Ганни Валеріївни

Члени комісії у складі:

Директор інституту інформаційної безпеки, радіоелектроніки та телекомунікацій
д.т.п. доц. Чечельницький В.Я.

Завідувач кафедри інформатики та управління захистом інформаційних систем
д.т.н. проф. Кобозєва А.А.

Голова методичної ради інституту інформаційної безпеки, радіоелектроніки та
телекомунікацій д.т.н. проф. Казаков А.І.

склали цей акт про те, що в Одеському національному політехнічному університеті для
магістрів спеціальності 122 – Комп'ютерні науки та інформаційні технології спеціалізації
«Інформатика» при вивченні курсу «Стеганографія», аспірантів спеціальності 125 –
Кібербезпека при вивченні курсів «Стеганографія та стеганоаналіз», «Сучасні проблеми
захисту інформації» впроваджено такі результати, отримані Ахматєєвої Г.В.

- стеганоаналітичний метод виявлення наявності додаткової інформації, що
аналізує просторову область цифрових відео, оснований на урахуванні кількості
блоків з однаковими значеннями яскравості;
- стеганоаналітичний метод виявлення наявності додаткової інформації, що
аналізує просторову область цифрових зображень та кадрів відеопослідовностей,
оснований на аналізі послідовних тріад триплетів у матриці унікальних кольорів;
- спосіб відокремлення цифрових зображень, отриманих збереженням у формат
без втрат з формату з втратами, від зображень, що початково зберігалися у
форматі без втрат.

Директор інституту інформаційної безпеки,
радіоелектроніки та телекомунікацій
д.т.н. доц.



В.Я. Чечельницький

Завідувач кафедри інформатики та управління
захистом інформаційних систем
д.т.н. проф.



А.А. Кобозєва

Голова методичної ради
інституту інформаційної безпеки,
радіоелектроніки та телекомунікацій



А.І. Казаков

Підписи членів комісії завіряю
Начальник відділу кадрів



О.І. Гармаш

Додаток Б.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Ахмаметьева, А.В.: Усовершенствование стеганоаналитического метода, основанного на анализе пространственной области цифровых контейнеров. Информатика та математичні методи в моделюванні. Т.5, № 4, 367-375 (2015)
2. Ахмаметьева, А.В.: Стеганоанализ цифровых изображений, хранящихся в формате с потерями. Захист інформації. Випуск 23, 135-145 (2016)
3. Ахмаметьева, Г.В.: Стеганоаналітичний алгоритм для цифрових контейнерів, збережених в форматах з втратами. Сучасна спеціальна техніка. № 3 (46), 31-38 (2016)
4. Akhmetieva, A.: Method of detection the fact of compression in digital images as an integral part of steganalysis. Информатика та математичні методи в моделюванні. Т.6, №4, 357-364 (2016)
5. Кобозева, А.А., Ахмаметьева, А.В., Ефименко, А.А.: Стеганоаналитический метод для цифровых контейнеров, хранящихся в формате без потерь. Інформаційна безпека. №1(13), 31-42 (2014)
6. Маєвський, Д.А., Ахмаметьева, Г.В.: Стеганоаналітичний алгоритм, заснований на аналізі просторової області цифрових контейнерів. Информатика та математичні методи в моделюванні. Т.6, №1, 52-60 (2016)
7. Ахмаметьева, А.В.: Выявление области применения стеганоаналитического подхода, основанного на анализе пространственной области цифровых контентов. Problemele energeticii regionale. Электронный журнал Академии наук Республики Молдова. № 2 (31), 104-111 (2016)
8. Ахмаметьева, А.В.: Стеганоаналитический метод, основанный на анализе пространственной области цифровых контентов. Международная научно-техническая конференция «Современные

информационно-телекоммуникационные технологии», Т. II, 83-84, Киев, 17-20 ноября 2015

9. Ахмаметьева, Г.В.: Детектування стеганоповідомлень, вбудованих методом LSB Matching у цифрові контейнери в форматах з втратами. V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», 106-107, Львів, 2-3 червня 2016
10. Ахмаметьева, Г.В.: Виявлення області застосування стеганоаналітичного алгоритму, що аналізує просторову область цифрових зображень. V Міжнародна науково-технічна конференція «Інформаційні системи та технології» (ІСТ-2016), 287-288, Харків-Коблево, 12-17 вересня 2016
11. Ахмаметьева, А.В.: Стеганоанализ цифровых видео, основанный на анализе пространственной области. V Міжнародна науково-практична конференція «Інформаційні управляючі системи та технології» (ІУСТ-Одеса - 2016), 161-163, Одеса, 20-22 вересня 2016

Додаток В.

ВІДОМОСТІ ПРО АПРОБАЦІЮ РЕЗУЛЬТАТІВ ДИСЕРТАЦІЇ

1. Міжвідомчий міжрегіональний семінар при Вченій Раді НАН України «Технічні засоби захисту інформації», Одеса 2014, очна участь.
2. Міжнародна науково-технічна конференція «Сучасні інформаційно-телекомунікаційні технології», Київ, 2015, заочна участь.
3. V Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», Львів, 2016, очна участь.
4. V Міжнародна науково-технічна конференція «Інформаційні системи та технології», Харків-Коблево, 2016, очна участь.
5. V Міжнародна науково-практична конференція «Інформаційні управляючі системи та технології», Одеса, 2016, очна участь.

Акхматметієва Анна