Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: «Стеганографія на базі зображень RAW-формату із цифрових камер»

Виконав: студент VI курсу, групи СБм-61
спеціальності 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

_____ Фаберський А.М.
(підпис) (прізвище та ініціали)

Керівник _____ Козак Р.О.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Стадник М.А.
(підпис) (прізвище та ініціали)

Завідувач кафедри _____ Загородна Н.В.
(підпис) (прізвище та ініціали)

Рецензент _____ Матійчук Л.П.
(підпис) (прізвище та ініціали)

Тернопіль - 2025

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 202_ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Магістр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека та захист інформації
(шифр і назва спеціальності)

Студенту Фаберському Андірю Михайловичу
(прізвище, ім'я, по батькові)

1. Тема роботи Стеганографія на базі зображень RAW-формату із цифрових камер

Керівник роботи Козак Руслан Орестович, к.т.н., доц.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від « 24 » 11 2025 року № 4/7-1024

2. Термін подання студентом завершеної роботи 18.12.2025 р.

3. Вихідні дані до роботи наукові літературні джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
1. RAW зображення та методи стеганографії.
2. Теоретико-проектна частина.
3. Програмна реалізація алгоритму.
4. Охорона праці та безпека в надзвичайних ситуаціях

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Тема роботи. 2. Актуальність. 3. Мета, задачі, об'єкт, предмет дослідження, наукова новизна. 4. Характеристики RAW зображення. 5. Механізм стеганографії. Види стеганоносіїв.
6. Алгоритми стеганографії у цифровому зображенні
7. Програмні рішення стеганографії. 8. Блок-схеми алгоритмів вбудовування в RAW зображення формату CR2 та визначення метаданих. 9. Блок-схеми алгоритмів вбудовування та вилучення даних. 10. Стек технологій. 11. Скріншоти розробленого ПЗ.
12. Демонстрація роботу програми на трьох зображеннях. 13. Показники візуального спотворення при вбудовуванні 100 кб..
14. Показники візуального спотворення при IF >0,9
15. Висновки. Основні результати дослідження

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Осухівська Г.М., зав. каф. КС		
Безпека в надзвичайних ситуаціях			

7. Дата видачі завдання 19.09.2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	19.09 – 22.09	*Виконано*
2.	Підбір джерел про стеганографію на базі зображень		
	RAW-формату з цифрових камер	22.09 – 30.09	*Виконано*
3.	Опрацювання джерел про стеганографію на базі		
	зображень RAW-формату з цифрових камер	01.10 – 15.10	*Виконано*
4.	Виконання дослідження щодо аналізу стеганографії		
	на базі зображень RAW-формату з цифрових камер	16.10 – 22.10	
5	Розробка ПЗ для тестування	23.10 – 02.11	
6.	Оформлення розділу «RAW зображення та методи стеганографії»	03.11 – 13.11	*Виконано*
7.	Оформлення розділу «Теоретико-проектна частина»	14.11 – 28.11	*Виконано*
8.	Оформлення розділу «Програмна реалізація алгоритму»	29.11 – 06.12	*Виконано*
9.	Виконання завдання до підрозділу «Охорона праці та		
	безпека в надзвичайних ситуаціях»	30.11 – 06.12	*Виконано*
10.	Оформлення кваліфікаційної роботи	03.12 – 08.12	*Виконано*
11.	Нормоконтроль	08.12 – 12.12	*Виконано*
12.	Перевірка на плагіат	16.12 – 18.12	*Виконано*
13.	Попередній захист кваліфікаційної роботи	18.12 – 19.12	*Виконано*
14.	Захист кваліфікаційної роботи	23.12	

Студент _____ Фаберський А.М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Козак Р.О.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Стеганографія на базі зображень RAW-формату із цифрових камер // ОР «Магістр» // Фаберський Андрій Михайлович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем та програмної інженерії, кафедра кібербезпеки, група СБм-61 // Тернопіль, 2025 // с. – 72, рис. – 20, табл. – 4, слайд. – 15, бібліогр. –39.

Ключові слова: Декодування, Найменш Значущий Біт, Стеганографія, Стегосистема, RAW Зображення, SSIM

Кваліфікаційна робота виконана з метою реалізації приховування даних за допомогою стеганографії на основі RAW зображень із цифрових камер.

У першому розділі було проведено аналіз RAW зображень, розглянуто механізм формування необроблених даних у цифровій камері, розібрано структуру розширень RAW зображень. Докладно досліджено алгоритм декодування необроблених даних, описані методи стеганографії..

У другому розділі проведено порівняння методів та наводиться обґрунтування обраного методу стеганографії. Описано розроблений алгоритм вбудовування та вилучення даних із RAW зображення. Також представлені параметри для оцінки ефективності вбудовування та обрані підводять для аналізу реалізованих результатів роботи розроблених алгоритмів.

Третій розділ присвячений розробці програми приховування та виявлення даних у RAW зображень. У цьому розділі проведено аналіз результатів з урахуванням параметрів, вибраних у другому розділі, а також їх порівняння із вбудовуванням у зображення форматів PNG та JPEG.

ABSTRACT

Steganography based on RAW images from digital cameras // Thesis of educational level "Master" // Faberskyi Andrii// Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security // Ternopil, 2025 // p. - 72, Fig. – 20, Table - 4, Slides - 15, References - 39.

Keywords: Decoding, LSB, Steganography, Stegosystem, RAW image, SSIM

Thesis was carried out with the aim of implementing data hiding using steganography based on RAW images from digital cameras.

In the first section, an analysis of RAW images was carried out, the mechanism of raw data formation in a digital camera was considered, the structure of RAW image extensions was analyzed. The algorithm for decoding raw data was studied in detail, steganography methods were described. A comparison of methods was carried out and the justification of the selected steganography method was provided.

In the second section, the developed algorithm for embedding and extracting data from RAW images is described. Parameters for assessing the effectiveness of embedding are also presented and selected summaries for analyzing the implemented results of the developed algorithms are selected.

The third section is devoted to the development of a program for hiding and detecting data in RAW images. This section analyzes the results taking into account the parameters selected in the second section, as well as their comparison with embedding in PNG and JPEG format images.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ СКОРОЧЕНЬ І ТЕРМІНІВ

EXIF – стандарт метаданих, який надає інформацію про цифрові зображення та аудіофайли, створені цифровими камерами та іншими пристроями

HVS (англ. Human Visual System) – зоровий аналізатор людини

IF (англ. Image Fidelity) – якість зображення (показник візуального спотворення)

LSB (англ. Least Significant Bit) – найменш значущий біт, використовується в стеганографії для приховування даних шляхом заміни останніх бітів пікселів зображення

PVD (англ. Pixel Value Differencing) – різниця значень пікселів, стеганографічний метод, який вбудовує секретні дані в зображення шляхом зміни різниці між двома сусідніми пікселями

RAW (англ. Raw – сирий) – формат даних, що містить необроблені (або мінімально оброблені) дані, що дозволяє уникнути втрат інформації, і не має чіткої специфікації

SSIM (англ. structure similarity) – індекс структурної подібності

Принцип Керкгоффа (або Керкгоффса) – принцип криптографії, який стверджує, що надійність криптосистеми має залежати виключно від секретності ключа, а не від секретності самого алгоритму шифрування

ПЗ – програмне забезпечення

Стеганографія - мистецтво приховування інформації всередині інших файлів, таких як зображення, аудіо чи текст

ВСТУП

Актуальність теми. На сьогоднішній день прискорення використання Інтернету свідчить про підвищений інтерес до способу передачі прихованої інформації за допомогою різних методів. Однією з визначних і важливих форм приховування інформації є стеганографія. Отже, стеганографія включає наукові методи приховування інформації всередині об'єкта.

Даний об'єкт служить для прихованої передачі інформації, яка має бути передана іншій стороні. Стеганографія задіює безліч форм носіїв інформації, наприклад текст, аудіо, зображення, протокол, які можуть бути використані для приховування даних. Цифрове зображення є приватною формою носіїв інформації через використання в Інтернеті.

У цій роботі розглядаються різні RAW формати з цифрових камер та методи стеганографії зображень. Також реалізовано приховування інформації в необроблених даних із сенсора цифрової камери, які знаходяться у форматі RAW цифрової камери.

Мета дослідження: програмно реалізувати приховування даних у зображенні RAW з цифрових камер, а також розробити для цієї програми алгоритм стеганографії на основі RAW зображення, заснований на відомих методах.

В роботі поставлено та розв’язано **наступні задачі**:

– вивчити можливі алгоритми стеганографії та вибрати відповідний для реалізації у програмі;

– дослідити існуючі у літературі підходи до роботи з RAW зображеннями;

– дослідити аналоги приховування даних за допомогою стенографічних методів та їх застосування до RAW зображень;

– реалізувати приховування даних у RAW зображенні зі збереженням вихідного формату;

– проаналізувати результат приховування даних у RAW зображеннях.

Об’єкт дослідження: RAW зображення із цифрової камери.

Предмет дослідження: метод стеганографії для вбудовування даних в об'єкт цієї роботи.

Наукова новизна отриманих результатів:

– розроблено методи обробки формату RAW зображення, метод вбудовування інформації та метод проявлення інформації з RAW зображення.

Практичне значення одержаних результатів. Створене ПЗ може бути застосованим фотографами, творцями онлайн-картинних галерей, редакціями журналів з інтерактивними зображеннями.

Апробація результатів роботи. Результати дослідження обговорювалися на XIV Міжнародна науково-практична конференція молодих учених та студентів «Актуальні задачі сучасних технологій», Тернопіль, 11-12. Грудня 2025 р.

Публікації. Окремі результати кваліфікаційної роботи опубліковано у працях конференції (Додаток А).

РОЗДІЛ 1 RAW ЗОБРАЖЕННЯ ТА МЕТОДИ СТЕГАНОГРАФІЇ

1.1 Аналіз RAW форматів цифрових камер

RAW файл містить дані, отримані безпосередньо зі світлочутливого сенсора камери. У виробництві матриць використовується дві технології CMOS та CCD або комплементарний метал-оксид напівпровідник (КМОП) та прилад із зарядовим зв'язком (ПЗЗ) відповідно.

Матриця цифрового фотоапарата складається з величезної кількості світлочутливих напівпровідникових елементів прямокутної форми, які називають пікселями, як показано на рис. 1.1. Кожен такий піксель збирає електрони, котрі виникають у ньому під дією фотонів, що прийшли від джерела світла. Структура цих даних відрізняється, але призначення однакове для всіх і є відображенням результату перетворення світлової енергії в електричні сигнали.

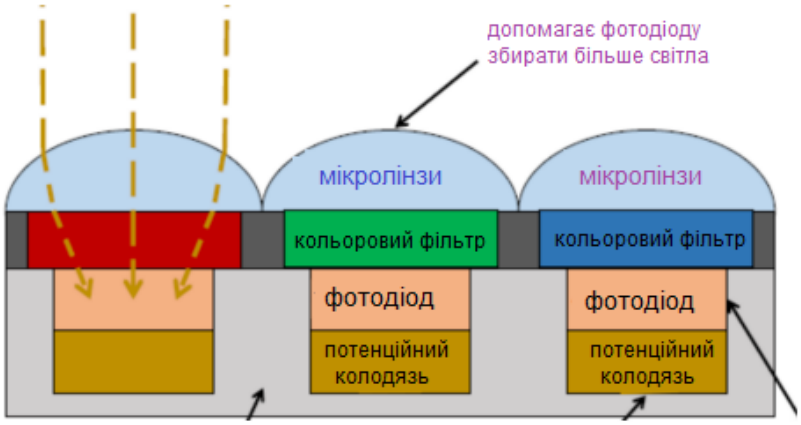

Рисунок 1.1 – Будова пікселя в матриці камери

Більшість цифрових камер, що генерують RAW -файли, відносяться до мозаїчних камер або цифрових фотоапаратів з масивом кольорових фільтрів (color filter array - CFA). Процес формування зображення матрицею фотоапарата залежить від обраного формату. Необроблені файли містять дані в діапазоні, зазвичай 12 або 14 біт, зчитані з кожного пікселя сенсора зображення камери. Основна особливість процесу полягає в тому, що матриця формує зображення у

відтінках сірого, оскільки RAW -файл не містить інформації про колір. Файл RAW - зображень із цифрової камери містить необроблені або мінімально оброблені дані із сенсора цифрової камери. Raw файли названі так тому, що вони ще не оброблені і містять велику кількість потенційно надлишкових даних. Різні виробники цифрових камер для захоплення цифрових зображень використовують модифіковані формати RAW.

Raw формати зображень призначені для захоплення радіометричних характеристик сцени, тобто фізичної інформації про інтенсивність світла та кольору з максимальним отриманням даних від сенсора камери. Більшість форматів необроблених файлів зображень зберігають інформацію, сприйняту відповідно до геометрії окремих фоточутливих елементів сенсора.

Файли RAW містять інформацію, потрібну для створення видимого зображення на основі даних сенсора камери. Структура необроблених файлів часто відповідає загальному шаблону: короткий заголовок файлу, який зазвичай містить індикатор порядку байтів у файлі, ідентифікатор файлу та усунення основних даних файлу. Потім йдуть метадані сенсора, включаючи розмір давача, атрибути CFA та його колірний профіль. Далі йдуть метадані зображення, які можуть бути корисними для включення в будь-яке середовище CMS або базу даних. До них належать налаштування експозиції, модель камери, сканера та об'єктива, дата та місце зйомки та сканування, інформація про автора та інше. Деякі необроблені файли містять стандартизований розділ метаданих із даними у форматі Exif. Після цього надається мініатюра зображення і більшість необроблених файлів містять повнорозмірне перетворення зображення на JPEG, яке використовується для попереднього перегляду файлу на екрані камери. Останніми у структурі формату заповнюються дані зображення давача малюнку.

Багато RAW форматів файлів, включаючи IIQ (Phase One), 3FR (Hasselblad), DCR, K25, KDC (Kodak), CRW CR2 (Canon), ERF (Epson), MEF (Mamiya), MOS (Leaf), NEF NRW (Nikon), ORF (Olymp (Panasonic) та ARW, SRF, SR2 (Sony) засновані на TIFF, форматі файлу зображення з тегами. Ці файли можуть відрізнятися від стандарту TIFF з низки причин, включаючи використання нестандартного заголовка файлу, включення додаткових тегів зображення та

шифрування деяких даних з тегами. Далі у цьому розділі буде детальніше розглянуто формати CR2.

1.1.1 Структура формату CR2

Глобально CR2 починається із заголовка TIFF, потім йде заголовок CR2. Після даних заголовків починаються дані параметрів 4 зображень різних форматів. Також у метаданих для першого зображення розташований покажчик на початок даних Exif, а всередині Exif міститься позначка на покажчик MakerNote. Після всіх цих даних йдуть 4 зображення зашифровані у відповідному форматі. На рис. 1.2 представлена ця структура наочно.

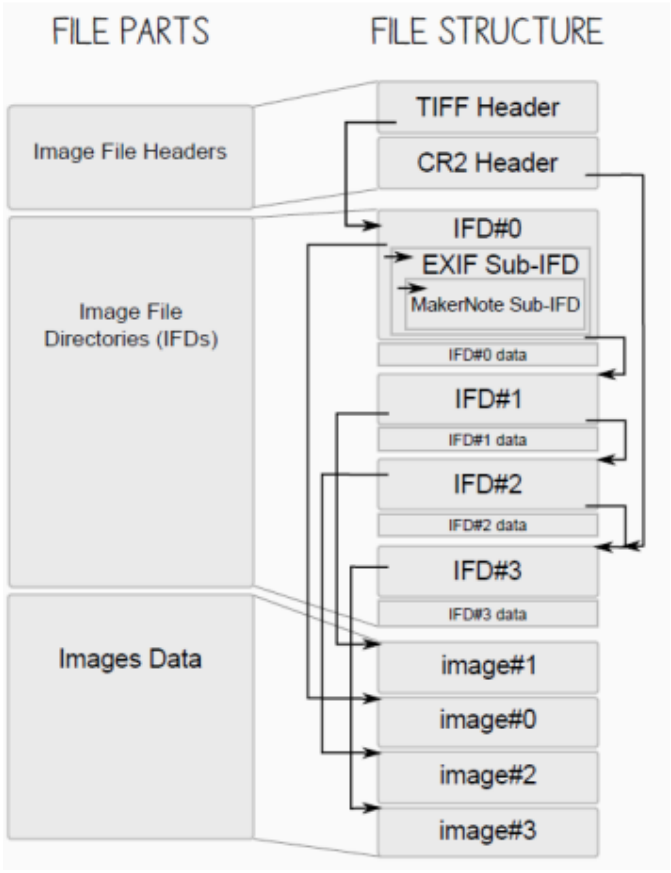

Рисунок 1.2 – Структура формату CR2

Після цих даних наступні 8 байт несуть інформацію заголовка CR2. Два байти за адресою з 0008 по 0009 містять магічне число формату Canon Raw у форматі CR2 значення завжди дорівнює 43 і 52, і це CR у рядковому поданні байт. Наступні

2 байти несуть інформацію версії. Далі йдуть 4 байти інформації, які вказують на розташування даних RAW під міткою IFD3. IFD3 має необроблені дані, і ми можемо отримати необроблені дані без аналізу TIFF.

У IFD0 міститься інформація про зменшену версію зображення одна четверта розміру оригіналу, стиснута у форматі Jpeg, така як ширина і висота, тип стиснення, марка, модель та інша. Також під цим маркером міститься розділ Exif, який містить розділ Makemotes. Інформація про давач знаходиться в Makemote, важливими даними є SensorInfo, маркер 00E0. Цей маркер містить інформацію про межі видимої частини сенсора. Якщо ви хочете отримати лише необроблені дані, достатньо отримати дані SensorInfo. Але якщо ви хочете перетворити необроблені дані на видиме зображення, ви також повинні отримати в цьому розділі інші дані, такі як колірний баланс 4001 і т.д.

Остання мітка IFD0 вказує на перехід до IFD1. Під міткою IFD1 міститься лише два теги. Перший покажчик розміщення зменшеної версії зображення, стиснута в Jpeg. Ще цю версію зображення називають мініатюрою основного зображення. Під другим тегом розташована інформація про кількість байт, які займає мініатюра.

Наприкінці IFD1 знаходиться покажчик IFD2. Цей IFD містить багато інформації для невеликого зображення, яке є стиснутим зображенням з глибиною кольору 16 біт. На рис. 1.3 наведено приклад даних. Кожні дані на 2 байти означають червоне, зелене та синє значення. Тобто перший піксель займає перші 6 байт, по 2 за кожен колір.

Рисунок 1.3 – Структура IFD1 формату CR2

IFD3 зберігається після закінчення IFD2, як і інші IFD. Адреса збігається з адресою в заголовку CR2 файлу. Цей IFD має адресу до необроблених RAW даних. У CR2 RAW дані закодовані за допомогою 16-бітної шкали сірого JPEG

без втрат за стандартом ITU-T T.81

Raw дані сканера розбиті на сегменти, вказані під тегом RawImageSegmentation У цьому тегу розташовано три значення. Нехай ці три значення будуть A, B і C. Для отримання ширини необхідна A x B + C. Для прикладу, значення дорівнюють 2, 1728 і 1888, і ми можемо отримати три області, кожна з яких має ширину 1728, 1728 і 1888 без втрат, як показано на наступному рис. 1.4. Після збереження № 0 ми зберігаємо дані областей № 1 та № 2 однаково.

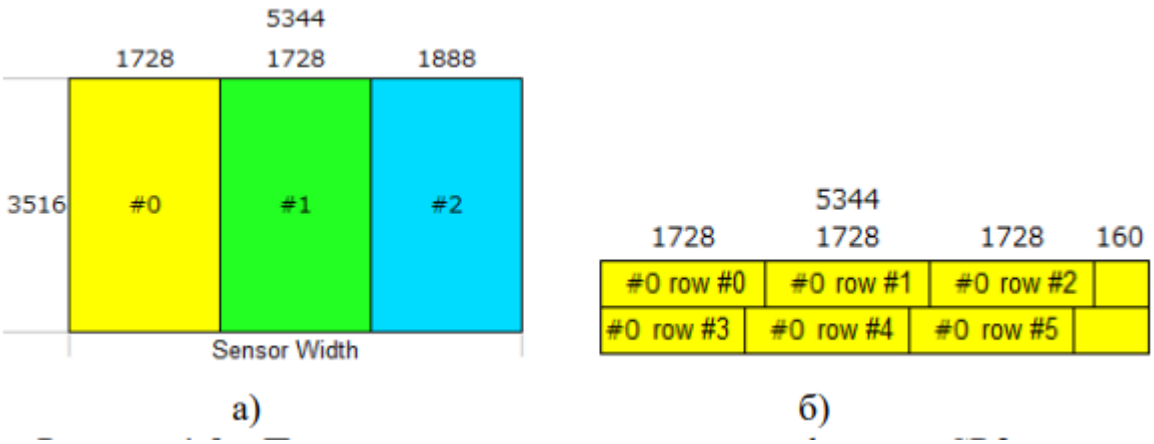

Рисунок 1.4 – Подання даних сенсора у форматі CR2:
а) розподіл даних по ширині; б) порядок зчитування даних

1.1.2 Опис структури форматів NEF, ARW, SRF та SR2

Формат NEF від Nikon використовується для зберігання цифрових зображень, створених їхньою цифровою камерою. Цей формат заснований на форматі TIFF і зазвичай має 2 мітки sublFD, перший для зберігання повного зображення у форматі jpeg із втратами, другий для повного зображення RAW, стислий без втрат. У Makemote є тег NikonImagePreview (0x0011), який містить мініатюру зображення у форматі JPEG із втратами.

IFD#0 також містить мініатюру зображення в стиснутому форматі TIFF розміром 160×120. У Makernote, починаючи з версії 200, тег ColorBalance (0x0097) зашифровано. Це можна розшифрувати за допомогою вмісту тегів 0x1d (серійний номер) та 0x00a7 (кількість затворів) та деяких жорстко заданих значень. Заголовок NEF є стандартним заголовком TIFF. З визначенням порядку читання

байт значення 49,49, що означає прямий від молодшого байта до старшого чи значення 4d,4d, що означає зворотний порядок байт. Наступні 2 байти так званий магічний номер TIFF, значення цих байт завжди дорівнює 002a. Потім йдуть байти адреси IFD0. Далі в IFD0 розміщена інформація про мініатюру у форматі TIFF та покажчики на стисло зображення у форматі jpeg під позначкою subIFD0 та покажчик на RAW дані під покажчиком subIFDl.

Формати файлів RAW, які використовуються камерами Sony, мають розширення SRF, SR2, ARW та ARQ. Всі формати засновані на форматі TIFF з порядком проходження байтів Intel (маркер «II» або 0x4949). SRF з'явився у січні 2004 р. у моделі камери DSC-F828, SR2 у грудні 2005 р. (DSC-R1) та ARW у липні 2006 р. з Alpha DSLR-A100. SRF, ймовірно, означає Sony Raw File, SR2 – це версія 2 SRF, а ARW означає Alpha RAW.

Версії і формати RAW з часом отримали додаткові функції: SRF, SR2 і ARW 1.0: 12 біт без стиснення, ARW 2.1: 12 біт cRAW (11 біт + 7 біт) з втратами, розроблений в 2008 році, ARW 2.3 : 14 біт. стиск без втрат представлений у 2021 році, ARQ, зсув пікселів, з'явився у листопаді 2017 року (A7R III).

Кожен рядок даних розбивається на фрагменти по 32 пікселя, кожен фрагмент містить пікселі, що чергуються, з 2 колірних каналів. У непарних рядках міститься 16 R пікселів та 16 G пікселів (RGRGRG...), у парних рядках міститься 16 G пікселів та 16 B пікселів (GBGBGB...). Структура кожного 16-піксельного блоку даних сенсорних даних наведена на рис. 1.5.

Max	Min	Offset of Max	Offset of Min	Delta01	Delta02	...	Delta13	Delta14
11-bit	11-bit	4-bit	4-bit	7-bit	7-bit	...	7-bit	7-bit

Рисунок 1.5 – Структура 16-піксельного блоку

Тут Max – максимальне значення пікселя в блоці, Min – мінімальне значення в блоці, Offsets – положення пікселів зі значеннями Max та Min щодо початку блоку.

Довжина блоку 2 11+2 4+14 7=128 біт або 16 байт. Таким чином, необроблені

дані, стислі за схемою RAW, ефективно використовують 1 байт на піксель; але загальний розмір файлу ARW2 трохи більший, оскільки він містить не лише дані RAW, але також метадані та попередній перегляд JPEG.

Чим більший діапазон даних у 16 піксельному блоці, тим більший крок, який множиться на значення дельти для відновлення значення пікселя, і, отже, тим більше крок даних. Для діапазону даних, меншого або рівного 128 коефіцієнт дорівнює 1, і при реверсуванні дельта-кодування не виникає помилки заокруглення. Для більшого діапазону схема робить помилку округлення, яка може призвести до пастеризації. Іншими словами, якщо блок 32 пікселів охоплює область з великим розкидом яскравості, дані в блоці не точні, а є приблизними. Під час необробленого перетворення спочатку інвертується дельта-кодування, потім для розпакування даних застосовується тонова крива лінеаризації, що міститься в метаданих файлів Sony ARW2 і, нарешті, рівень чорного, також узятий з метаданих, віднімається від результату.

1.2 Огляд методів стеганографії у цифрові зображення

За останні роки було опубліковано кілька оглядів стеганографії. Найбільш важливими та популярними є дві статті [1, 2]. Ці роботи зосереджені на огляді основних концепцій, різних мірах оцінки, стороні безпеки системи стеганографії зображень та включають літературу, яка була опублікована до моменту публікації статей. Проте цей огляд можна вважати застарілим через те, що з цієї дати опубліковано багато матеріалів, і ці нові публікації обов'язково мають бути зібрані в рамках нового оглядового документа. Варто коротко обговорити деякі інші огляди визначення стеганографії зображень, області, а також методи узагальненої форми, не обговорюючи величезну кількість вкладів у цій галузі щодо оглядових статей.

Етимологія стеганографії походить від пари грецьких лексичних одиниць, Steganos та Graphy, які позначають прихований та письмовий відповідно [3]. Початковий орфографічний доказ, що відноситься до стеганографії, можна простежити приблизно в 440 до н.е., починаючи з твердження грецького історика

Геродота [4]. У минулому застосовувалися різні способи приховування інформації. Стародавні греки писали послання на дерев'яних табличках, які покривали воском, щоб приховати повідомлення. До того ж вони татуювали послання на голених головах посланців і чекали, поки відросте його волосся, щоб покрити і приховати повідомлення, перш ніж ці посланці будуть відправлені як носії секретних повідомлень. Під час Другої світової війни німці винайшли технологію мікроточок у кілька етапів і використовували обкладинки, такі як журнали, щоб не викликати підозри [5]. Також у той час повідомлення писалися невидимим чорнилом між рядками звичайних букв, які не привертали б уваги. Розвиток стеганографії дозволив створити різні та проникливі методи секретних повідомлень, які будуть вбудовані у різні цифрові носії, такі як текстові носії, відео, протоколи та аудіо, з поточною доступністю Інтернету та динамічних комп'ютерів.

Умовно механізм приховування інформації шляхом вбудовування їх дискретним чином називається стеганографією, має на увазі наявність прихованих даних, які є взаємним знанням тільки між конкретними співрозмовниками. Прихована інформація є об'єктним файлом стеганографії. Потім він передається іншому, де прихована інформація витягується та розшифровується приймачем при допомозі алгоритму вилучення [6]. Загальний механізм стеганографії зображено на рис. 1.6.

В основному в моделі стеганографії є чотири компоненти. Зображення, яке використовується для приховування, відоме як зображення обкладинки, буде виступати як контейнер для передачі інформації, прихованої всередині нього. Список повідомлення, прихована інформація може складатися з даних, файлів або зображень та інших даних [7]. Стегоключ, званий секретним ключем, використовується для кодування та декодування при розшифровці прихованої інформації. Стегоносії також відомі як стегооб'єкти. Цей етап досягається внаслідок процесу впровадження прихованої інформації [8].

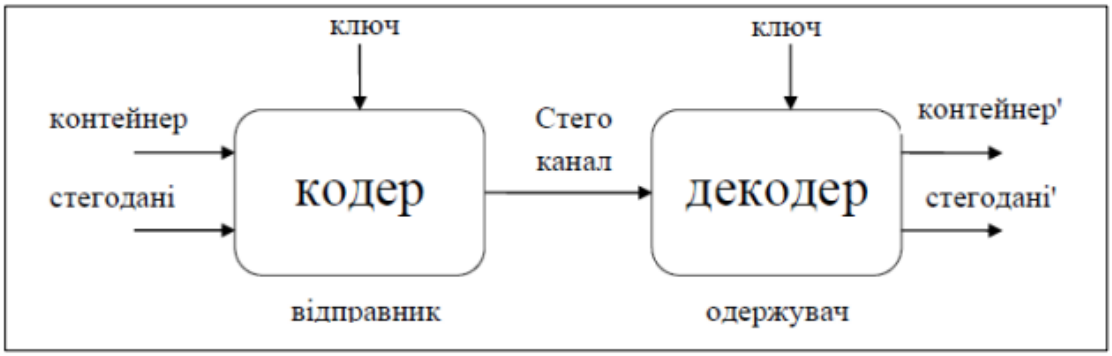

Рисунок 1.6 – Механізм стеганографії

Цифрові зображення є поширеною формою всіх цифрових носіїв у стеганографії через їх регулярність використання та доступність в Інтернеті, хоча також використовуються всі інші формати цифрових файлів [9]. На рис. 1.7 показані формати шести основних категорій файлів, які можна використовувати для стеганографії.

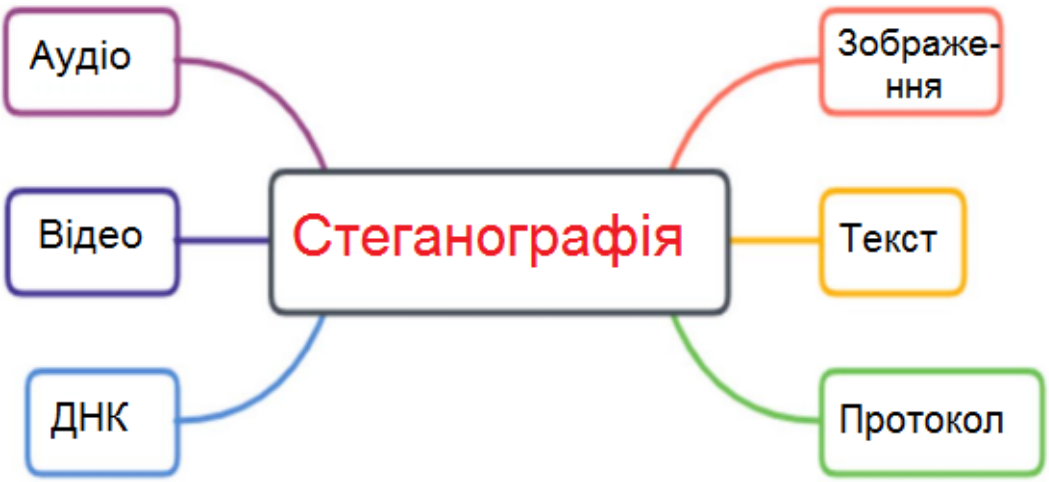

Рисунок 1.7 – Види стеганоносіїв

Стеганографія зображень найбільш популярна з форм об'єктів-обкладинок, яка часто використовується для стеганографії, є цифрові зображення, оскільки вони також є найпоширенішими формами в Інтернеті. Прихована інформація вбудовується в цифрове зображення під час алгоритму за допомогою секретного ключа, що створює стеганографічне зображення. Цей метод в основному включає інтенсивність пікселів, що використовуються для приховування інформації [10].

Приховування інформації у відеоформаті називається відеостеганографією. Відео файли складаються з компіляції зображень та аудіо. Як правило, велику кількість рекомендованих методів роботи із зображеннями та звуком можна застосовувати і до відеофайлів. Це найбільш придатна форма файлу зображення в порівнянні з іншими мультимедійними файлами. Це пов'язано з обсягом простору всередині відеоформату, який може вмістити та приховати величезну кількість даних, які можуть залишитись непоміченими людьми внаслідок нескінченного потоку інформації. Можна використовувати різні відеофайли: H.264, MP4, MPEG, AVI та інші [11].

Приховування інформації у текстовому файлі називається текстовою стеганографією. Файл має крихітний об'єм пам'яті, тому може бути сховищем тільки для текстового формату. Існує безліч форматів, які використовують цей механізм. Табуляція, великі літери та кількість прогалин використовуються для приховування інформації в текстовій стеганографії. Текстова стеганографія рідко використовується, оскільки текстові файли містять величезну кількість надлишкових даних [12].

Стеганографія у протоколі передбачає вбудовування прихованої інформації всередину мережевих протоколів, наприклад, IP, TCP, ICMP, UDP та інших; при цьому протокол використовується як носій. До складу мережного пакета входять дані користувача, заголовки пакетів і трейлери пакетів. Таким чином, стеганографію можна використовувати у шарах мережевої моделі. Ця термінологія визначається як стеганографія протоколу [13].

Цифровий звук, що зазнав прихованого впровадження інформації, відомий як аудіостеганографія, в якій комп'ютер використовується в як основу для функціонування системи. Невелика модифікація, внесена в послідовне розташування двійкового файлу в звуковій системі, що дозволяє вбудовувати в нього приховану інформацію. Деяке ПЗ для звукової стеганографії, доступне в даний час, є засобом включення вбудовування інформації, що дозволяє приховувати інформацію у форматах WAV, AU, та звукові файли MP3 [14]. Завдання впровадження прихованої інформації в цифровий звук є більш складним порівняно з тим самим завданням, котре має бути виконана в інших медіаформах,

таких як зображення у цифрових формах. Різні методи вбудовування даних в цифрове аудіо були введені та ініційовані в звуковому середовищі, кульмінацією чого стала працююча система, яка буде добре приховувати інформацію. Ці варіанти методів працюють у спектрі, який складається із введення даних через форму сигналу-шуму за рахунок використання нескладного алгоритму, аж до сильніших методів, таких як використання високотехнологічних механізмів приховування даних [15].

1.3 Характеристики стеганографії

Існує три основні типи протоколів [16]:

–чиста стеганографія;

–стеганографія з секретним ключем;

–стеганографія з відкритим ключем.

Чиста стеганографія включає систему, в якій співрозмовники, що відправляють та отримують секретні повідомлення, не діляться попередньою інформацією. У цьому випадку дуже важливо, щоб і відправник, і одержувач мали доступ до функцій вбудовування та вилучення, які не повинні бути відомі третій стороні. Насправді чиста стеганографія не захищена через те, що вона суперечить принципу Керкгоффа, що ґрунтується на передумові, що алгоритм вбудовування відомий третій стороні [2].

Стеганографія із секретним ключем. З посиланням на принцип Керкгоффа робиться висновок, що третя сторона має канал для методу вилучення, і, отже, це дозволяє перехоплювати і вилучати приховану інформацію, яка розташована в кожному стеганографічному носії, що передається між відправником і одержувачем. Отже, спільне знання стегоключа відправником та одержувачем впливає на безпеку прихованої інформації. Відсутність цього ключа призведе до повного утруднення доступу будь-якої сторони до секретної інформації з обкладинки стеганографічного носія. Тим не менш, додаткова передача секретного ключа суперечить основним цілям стеганографії. Це непомітний зв'язок, що передбачає, що відправник і одержувач раніше мали загальне знання

стегоключа [2].

Стеганографія з відкритим ключем використовує пару ключів – відкритий ключ та закритий ключ. Відкритий ключ поміщається у базу даних, котра є загальнодоступною, та застосовується алгоритмом вбудовування, у той час як закритий же ключ використовується алгоритмом вилучення для отримання секретного повідомлення. Отже, відкритий ключ може бути створений з використанням загальнодоступної криптосистеми, де відправнику та одержувачу не потрібно обмінюватися секретним ключем. Це може бути виконано з припущення, що відправник і одержувач поділилися своїм відкритим ключем один з одним до їх затримання. Виходячи з гіпотези про те, що третя сторона знає про метод вбудовування, вона може спробувати витягти приховану інформацію в стеганографічному носії. Проте їй не вдасться ідентифікувати секретну інформацію через те, що в результаті шифрування вони виглядатимуть як хаотичні ланцюжки бітів.

Стеганографія пов'язана з більш великою областю, званої приховування інформації, тому загальні характеристики приховування інформації можуть застосовуватися як для стеганографії, так і для цифрових водяних знаків. Проте стеганографія певною мірою відрізняється від водяних знаків з погляду визначення пріоритетів і цих властивостей [17].

Невиявлення. Основними завданнями стеганографії є приховування інформації, що приховує наявність секретної інформації та зберігає її конфіденційність. Отже, невиявлення є найвищою першорядною властивістю всієї системи стеганографії, що означає, що присутність будь-якої прихованої інформації має залишитися непоміченим під час використання будь-яких статистичних методів. У випадку, якщо хтось зможе легко виявити та ідентифікувати стеганографічний носій, можна припустити, що використання конкретної стеганографічної техніки безглуздо [3]. Існує кілька факторів, які можуть безпосередньо вплинути на невиявність, наприклад, вибраний покривний носій, метод вбудовування та кількість модифікацій, що вносяться до покривного носія. Проте існує неіснуючий метод будь-якої стеганографічної техніки, який може вбудовувати інформацію в певний медіафайл, не залишаючи залишкових

артефактів. Таким чином, менша можливість розрізнення цих артефактів має на увазі більш досконалу техніку стеганографії порівняно з іншими.

Непомітність - це одна з властивостей стеганографічної системи, яка визначає обов'язковість стеганографічних носіїв бути вільними від будь-яких залишкових артефактів, що виявляються, котрі виникають в результаті вбудовування секретних даних. Таким чином, при вбудовуванні більшість методів стеганографії враховували обмеження зорової системи людини (HVS) або слухової системи людини (HAS) [18]. Це означає, що як зразок стеганографічне зображення має виглядати невинним і безневинним зображенням HVS. Існує безліч критеріїв оцінки щодо непомітності, які слід брати до уваги з точки зору типу методу стеганографії або типу файлу покриття, що використовується для приховування даних. Наприклад, розмір файлу може вказувати на наявність прихованих даних у текстових файлах або стеганографії на основі вставки. Крім того, у випадку стеганографії зображень якість зображення може вказувати на наявність заснованої на підстановці стеганографії зображень. Однак поширені стеганографічні методи уникають виявлення і мають високий рівень непомітності, однак їхня ідентифікація за допомогою статистичних засобів утруднена.

У літературі з стеганографії термін безпека прирівнюється до невиявлення. Отже, статистичне невиявлення забезпечує безпеку стеганографічного методу. Тим не менш слід зазначити, більшість поширених стеганографічних методів враховують пасивну атаку, проте розгляд активних атак береться до уваги значно менше у дослідженнях, як це обговорюється зокрема у [19].

Місткість вбудовування та стеганографічна ємність - це два варіанти ємності, пов'язані з полем стеганографії. Місткість вбудовування – це максимальна кількість бітів, яку конкретний медіафайл може прийняти для вбудовування [19]. Наприклад, ємність зображення в градаціях сірого, яка має бути впроваджена із заміною LSB, еквівалентна загальній кількості пікселів зображення, що позначає ємність впровадження. Однак стеганографічна ємність відрізняється від ємності вбудовування, оскільки її важко визначити навіть за нескладної техніки вбудовування. Позначається оптимальною кількістю бітів, яка може бути вбудована в конкретний медіафайл з непомітною присутністю, яка не може бути

виявлена зловмисником.

На надійність стеганографії впливають два фактори. З погляду невиявленості, як описано вище. Здатність долати активні атаки, що найважливіше для цифрових водяних знаків [20]. Це означає, що секретна інформація може бути вилучена іншим об'єктом, у тому числі в умовах, коли носії покриття піддавалися певному ступеню обробки даних. Надійність стеганографії пояснюється її здатністю протистояти як виявленню, і знищенню прихованої інформації, що робить обидва завдання важкими для розкриття зловмисником. Однак, як стверджує автор, подолання активної атаки не є головним завданням стеганографії, оскільки майже ніколи не враховується у рівнянні. Це спричинено припущенням, що стеганографічний об'єкт передаватиметься по мережі. Отже, також передбачається, що деградація незначна і що друга сторона отримає повідомлення від першої сторони без змін.

1.4 Висновки до першого розділу

В цьому розділі проаналізовано RAW зображення, досліджено механізм створення необроблених даних у цифровій камері, опрацьовано структуру розширень різних RAW зображень. Докладно розібрано алгоритм декодування необроблених даних, проаналізовані різні методи стеганографії. Здійснено їх порівняння.

За проаналізованими даними можна зробити висновок, що для кожного розширення формату RAW необхідно розробляти окремий алгоритм виявлення необроблених даних, отриманих з сенсора цифрової камери.

Також описано три основні протоколи стеганографії.

РОЗДІЛ 2 ТЕОРЕТИКО-ПРОЕКТНА ЧАСТИНА

2.1 Алгоритми стеганографії у цифровому зображенні

За останні кілька десятиліть було створено та вдосконалено безліч секретних методів зв'язку, при цьому стеганографія зображення становить одну з основних областей прихованого зв'язку. Це пов'язано з тим, що в Інтернеті є мільйони готових і доступних зображень, з яких будь-яка людина, яка бажає спілкуватися таємним чином, може вставляти свої власні повідомлення. Крім того, формат має високу надмірність, а незначні зміни цифрових зображень не виявляються HVS. Більше того, їхня присутність є всюди в Інтернеті, тому їх легко використовувати як прикриття для вбудовування даних без збудження. Отже, цифрові зображення широко використовуються як прикриття для стеганографії. Відносна більшість стеганографічних систем досліджують і використовують знання про недоліки людського зору у методах вбудовування. Таким чином, зашумлені області та краї зображень цікавлять стеганографів, оскільки HVS менш чутливий до зашумлених областей та областей по краях.

Незважаючи на певний прогрес, досягнутий у стеганографії зображень з погляду бінарних зображень та тривимірних зображень, дослідники зосередили свої дослідження на прихованні даних у відтінках сірого та кольорових зображень. Незважаючи на те, що компонент яскравості кольорового зображення ідентичний компоненту яскравості зображення в градаціях сірого, деякі експерти вважають зображення в градаціях сірого оптимальним покриттям для стеганографії. Це пов'язано з тим, що процес вбудовування змінить кореляцію між елементами кольору, і ці зміни можуть викликати сліди артефактів, які спростять виявлення вбудовування.

Як правило, існує два основних типи стеганографії зображень: просторова область та область перетворення. На рис. 2.1 показано два типи методів.

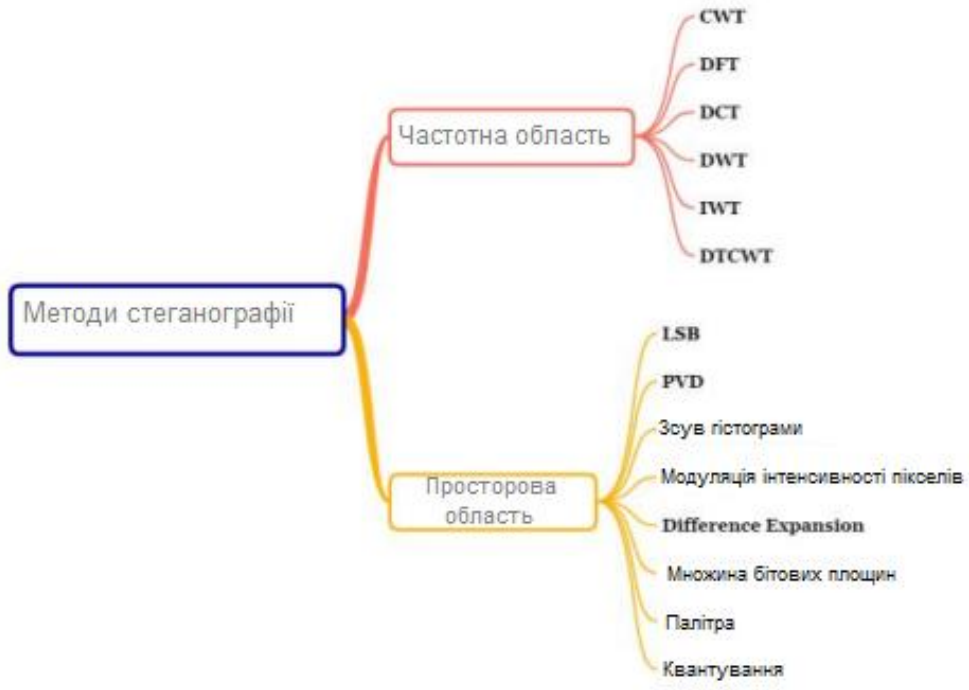

Рисунок 2.1 – Методи стеганографії

У цьому підрозділі буде детально описана просторова область, в той час як область перетворення та адаптивна область, яка є особливою формою методів просторового перетворення та перетворення, будуть пояснені коротко. Таблиця 2.1 пояснює різницю між ними.

Таблиця 2.1 – Відмінності між методами стеганографії

Характеристика	Властивості	Просторова стеганографія		
		Спектральна область	Частотна область	Адаптивне вбудовування
1	2	3	4	5
Тип системи	–	Простий	Складний	Залежить від адаптивного алгоритму
Залежність від формату	–	Залежний	Незалежний	Незалежний
Маніпулювання пікселями	–	Пряме	Непрямий	Залежить від вбудованої техніки

Продовження таблиці 2.1

1	2	3	4	5
Обчислювальна складність	–	Менше час обчислень	Більший час обчислень	Залежний від алгоритму
Здатність до вбудовування	Корисне навантаженн	Високий	Обмежений	Різноманітний
Візуальна якість	Непомітність	Високий	Менш керований	Висока керованість
Цілісність візуальних елементів	Різкість, розмиття, краї	Підтримуваний	Менш підтримуваний	Ремонтопридатний
Стійкість	Стиснення, шум, обрізка, обертання і т.д.	Стійко	Менш схильній	Залежить від внутрішнього алгоритму
Безпека	Геометричні атаки	Вразливий для геометричних атак	Стійкий до геометричних атак	Важко піддаються геометричним атакам
Статистичний аналіз атак за виявленням	Гістограма	Легко викривається/ виявляється	Важко викрити/безуспішно	Важко викрити/безуспішно
Аналіз атак з неструктурним виявленням	Аналіз атак із неструктурним виявленням	Складний/різноманітний	Легко виявляється	Складний/різноманітний

2.1.1 Перетворення стеганографії просторової області

Значення що стосуються області перетворення, використовуються для вставки та комбінації прихованих бітів у зображенні, знайденому в обкладинці. Біти приховані під частотними коефіцієнтами піддіапазону під час використання методів, заснованих на галузі перетворення. Методи просторової області

включають складніший процес впровадження та декодування в порівнянні з методами частотної області. Таким чином, безпека системи буде підвищена. Ще однією перевагою методу перетворення області є те, що він менш сприйнятливий до атак з обертанням, кадруванням, стисненням, масштабуванням, що дозволяє системам, заснованим на перетворенні, бути ефективнішими. Методи області перетворення широко використовуються в області стеганографії, і переважні схеми включають цілочисельне вейвлет-перетворення (IWT), комплексне вейвлет-перетворення (CWT), дискретне перетворення Фур'є (DFT), дискретне косинусне перетворення (DCT), дискретне вейвлет-перестворення. (DWT) та різні версії цих базових перетворень та комплексних вейвлет перетворень Dual -Tree (DTCWT).

2.1.2 Адаптивна стеганографія

Це особлива форма просторових та трансформаційних технік. З іншого боку, це називається вбудовування із урахуванням статистики чи маскування [21]. Величезна частина основної роботи, що стосується стеганографії, може бути віднесена до цього розділу. Введення адаптивного характеру в схему вбудовування може бути виконано у різний спосіб, такими як вибір цільових пікселів у зображенні обкладинки, тип модифікації, яку необхідно виконати. реалізовано, кількість бітів, вбудованих у піксель, та багато інших. Класифікацію систем можна розділити на кілька розділів, і вони ґрунтуються на ознаках та положеннях адаптивних методів через системи. До них відносяться стеганографія на основі регіонів, стеганографія на основі HVS, стеганографія на основі методів машинного навчання та штучного інтелекту [2].

Незважаючи на ці фактори, різні альтернативні види зображень стеганографії використовуються рідко або менш відомі. Одним із таких прикладів є прикріплення секретної інформації до тега кінця файлу (EOF) зображення JPG, що нескладно і в більшості випадків буде пропущено програмами для перегляду зображень. Згаданий тип впровадження даних не вимагає зусиль, не впливає на якість зображення, не змінює гістограму зображення та не може бути сприйнятий

програмами для перегляду зображень. Тим не менш, в умовах, коли доступ до стеганографічного зображення здійснюється через інші програми, такі як Блокнот, будуть відображатися приховані дані через те, що конфігурація Блокнота не налаштована для звернення до тега EOF файл JPG.

Іншим прикладом є прихована інформація, яка була прикріплена до розширеної інформації про файл зображення (EXIF), що є звичайною практикою і використовується виробниками цифрових камер як сховища інформації, такий як марка та модель камери, час захоплення фотографії, її дозвіл та інші дані. Як стверджує [22], інформація, зібрана та відображена за допомогою EXIF, може допомогти у перевірці справжності зображення та перевірці у слідчій процедурі, пов'язаної з дитячою порнографією. Вкрай важливим аспектом, на який слід звернути увагу, є те, що метод додавання прихованих даних до тегів метаданих файлу зображення сприйнятливий і вразливий для будь-яких типів редагування або атак у нескладних та простих механізмах за допомогою методів просторової області чи області зображення. Основні стеганографічні системи, які знаходяться в рамках методу просторової області, складаються з LSB, на основі декількох бітових площин, на основі квантування, додавання значення пікселя, будь-яка форма додавання прихованих даних можна виявити за розміром файлу, що помітно, якщо приховані великі дані.

Легкий і нескладний метод вбудовування зображення в оцифрованих формах - це вбудовування в просторову область, де змінюються значення пікселя зображення обкладинки. Для кодування біт секретної інформації в таких способах використовуються точні або опосередковані рівні значень інтенсивності пікселів зображення обкладинки. Ці методи використовують найпростіший процес щодо складного впровадження та декодування. Реалізація побітових методів, які використовують вставку бітів та маніпулювання шумом за допомогою PVD, зсуву гістограми, розширення на основі палітри, модуляції інтенсивності пікселів та стеганографії на основі шаблонів.

2.1.3 Стеганографія з LSB

Це сприймається як один із простих та кращих методів стеганографії просторового зображення. Робота цього методу заснована на передумові, що менш значущі біти у зображенні втілюють мізерну інформацію, а дрібні зміни в цих бітах не можуть бути помітні і залишатимуться непоміченими для людських очей. У методах просторової області на основі LSB незрозуміла прихована інформація буде вбудована прямо у зображення обкладинки за допомогою модифікації LSB певних пікселів без візуального впливу на якість вихідного зображення обкладинки через спотворення. Використовуючи цей метод у каналах зв'язку, зловмисники не можуть візуально відстежити або виявити погіршення якості зображення, коли вони запускають режим атаки. Проте статистика показує сліди шуму у діапазоні 5 % від середньої швидкості застосування бітів, створеного у процесі застосування. Попередні ранні роботи зі стеганографії LSB були зосереджені на дизайні системи для збільшення ємності корисного навантаження за рахунок використання великої кількості пікселів зображення обкладинки [23]. Після певного періоду область дослідження стегоаналізу набрала сили, щоб зламати такі системи за допомогою статистичного аналізу. Після цього, при вирішенні дослідницької проблеми, дослідники були поглинені і концентрували власне свою увагу на створенні модерних надійних методів LSB, в основі яких лежить криптографія-стеганографія, які можуть уникнути таких атак стеганоаналізу.

Щоб підвищити ефективність, численні дослідження зробили безліч розширених форм стеганографії зображень, заснованих на LSB. Алгоритми зіставлення LSB використовувалися значущими. LSB базується на характеристиках зображення, таких як зміст текстури, інтенсивність чи характеристики крайових пікселів. Оптимізована заміна LSB ґрунтується на методологіях навчання та інших. Крім того, для підвищення здатності вбудовування, розширення LSB може охоплювати до чотирьох площин LSB, що призведе до зниження непомітності. Його простота в процесі вбудовування та декодування є основною перевагою методу LSB. Враховуючи, що у більшості

форматів зображень використовується 8-бітне представлення замість окремих пікселів, молодші біти, зазвичай від шостого до восьмого біта, певного числа або сукупність значень інтенсивності пікселя, що належить зображення на обкладинці, регулюється відповідно до прихованої інформації. Молодші розряди окремих кольорових площин (червона, зелена та синя) змінюються відповідно до кожного з даних під час використання 24 бітного кольорового зображення, яке використовується як носій покриття, оскільки методи LSB вразливі для статистичних атак.

2.1.4 Стеганографія з PVD

Метод використовує приховування прихованої інформації шляхом порівняння невідповідностей між значеннями пікселів пари послідовних пікселів. Прихована інформація, що міститься в елементарних зачатках методу PVD [24], під час процесу вбудовування відокремлюється від обкладинки і зображення на блоки, що не перекриваються, з двома сусідніми пікселями, а потім вставляються різні значення пікселів в окремому блоці на кілька кластерів.

Вибір інтервалів діапазону здійснюється відповідно до характеру HVS до відмінностей значень інтенсивності - від низької точності до високої частоти. Через те, що PVD показує більш високий ступінь точності в порівнянні з методами LSB, що відносяться до продуктивності щільного впровадження, за рахунок того, що використання є більш плавним при використанні методів PVD. Конфігурація конструкції системи диктує, що модифікації визначаються межах певного інтервалу діапазону.

Численні методи були спрямовані на вивчення кореляції пікселів у галузі досліджень стеганографії PVD. Різні схеми сусідства, такі як п'ять, шість, сім та вісім сусідів, використовуються для визначення різниці значень пікселів, щоб передбачити остаточний ідеальний рівень впровадження в пікселі покриття. Візуальні спотворення здаються незначними, порівняно з більшістю альтернативних методів PVD. Основним недоліком методу PVD є безпека, хоча він забезпечує більш високий коефіцієнт сприйняття зображення Численні

додаткові характеристики безпеки включені в типову схему PVD для підвищення цього фактора безпеки підходу з різницею значень пікселів. Наприклад, Хусейн та ін. запропонував використовувати два методи вбудованих процедур для техніки приховування інформації, що підвищує безпеку. Відповідні процедури спричиняють поліпшену заміну правої цифри (iRMDR) і різницю значень пікселів бітів парності (PBPVD). Також наведено ще один приклад підвищеної безпеки, заснований на гістограмному аналізі вразливості PVD. Були запропоновані гібридні схеми вбудовування, щоб інтегрувати переваги різних схем вбудовування, які є методами стеганографії, які реалізують різницю значень пікселів і заміну найменш значущих бітів. Було проведено безліч досліджень розширених форм стеганографії зображень, що ґрунтуються на PVD, щоб підвищити ефективність. Значні з них використовують адаптивний блок PVD, реалізуючи методи псевдовипадкових чисел для вибору блоків та вирішення проблем спадаючих кордонів у PVD шляхом максимізації стратегії.

2.1.5 Стеганографія на основі усунення гістограми

Центральна стратегія, що використовується в цьому методі, включає зміщення рівнів гістограми носія покриття. Виявляються западини та пікові точки на гістограмі зображення покриття, що йде за процесом вбудовування, який включає зміну цих западин та пікових точок [25]. Метод зберігає непомітність та забезпечує більш високу вантажопідйомність. Основна перевага приховування зображення на основі гістограми зводиться до підтримки схемою оборотного приховування даних. Крім того, він також перешкоджає тому, щоб оточуюче середовище не перевищувало значення яскравості > 255 та < 0.

Щоб уникнути проблем з переповненням та не доповненням, а також підвищити здатність приховувати дані, пропонується додаткове рішення для вбудовування точок максимуму та мінімуму в карту гістограми шляхом використання структури «двійкове дерево». Інший підхід, заснований на методі імітації зсуву гістограми. Замість використання встановленого вибору опорної точки на карті гістограми, цей метод включає процес, який робить вибір на основі

інтенсивності пікселів зображення. Перед процесом вбудовування виконується поділ діапазону інтенсивності зображення на сегменти, що не перекриваються. Відповідно до інших методів, заснованих на зміщенні гістограми, вбудовування прихованих даних обробляється шляхом зміни інтенсивності пікселя пікової точки з іншими в межах того ж відрізку вершини. Враховуючи, що випадки перетворення під час процедури вбудовування для кожного окремого пікселя мінімальні, ймовірність багатошарового вбудовування реальна, що не вплине на помітність зображення покриття, крім бездоганного відновлення прихованих даних. У порівнянні з альтернативними методами, заснованими на гістограмі, це система, яка може бути обернена, включаючи можливість отримання зображення обкладинки на додаток до секретної інформації. Сегментований рівень інтенсивності обмежує перетворення при вбудовуванні в безпечний масив, що призводить до високої якості зображення стегомедіа. Місткість корисного навантаження обмежена, тому що під час оцінки з численними тестовими зображеннями вона становила 0,5 біт на піксель. Крім того, він не підходить для використання зі стислим стегозображенням, на додаток до каналу передачі, вразливому для геометричних спотворень, таких як масштабування або додавання шуму.

2.1.6 Стеганографія на основі модуляції інтенсивності пікселів

Впровадження систем стеганографії, заснованих на модуляції чи налаштуванні інтенсивності пікселів, має бути модифікацією процедури вбудовування для налаштування інтенсивності пікселів у стеганографії на основі LSB. В цьому випадку вбудовування прихованих інформаційних бітів виконується в рамках регулювання інтенсивності між найближчими сусідніми пікселями або блоками в безпосередній близькості, що залежить від умов схеми вбудовування. Ці методи допомагають забезпечити більш високу якість стегозображень порівняно із системами модифікації LSB внаслідок непрямого процесу вбудовування. Для досягнення підвищеної безпеки [26] пропонується вибір краю, заснований на модуляції інтенсивності пікселів. З метою підвищення

пропускної спроможності та якості, яка сприймається, пояснюється додатковий складний метод модуляції інтенсивності пікселів. У цьому випадку підблоки основного зображення містять інтегрований секрет. Інтелектуальне налаштування пікселів, засноване на секретних бітах даних, потім оновить середні значення підблоків. Реалізація адекватних порогів закладена у підтримці коригування значень у межах параметрів максимального значення інтенсивності.

Процедура екстракції тягне за собою зворотну фазу вбудовування. Завдяки огляду цих методів було зроблено оцінку переваги методу над стандартним методом модуляції LSB щодо непомітності, безпеки та надійності. Тим не менш, інші системні недоліки найменш значущих бітів, як і раніше, переважають, і для їх усунення потрібне подальше розслідування.

2.1.7 Стеганографія різницевого розширення

Пов’язана із впровадженням прихованої інформації в різні пари пікселів. Розширення варіантів значень реалізується за рахунок використання різних методів, та вбудовування бітів секретних даних виконується в цьому розширеному діапазоні відмінностей [27]. Більшість методів різницевого розширення відносяться до категорії оборотних стегано-систем, і в цьому випадку на стороні одержувача не виходять помилкові вилучення зображення обкладинки та секретні дані. Багато дослідників запропонували безліч досліджень систем стеганографії зображень, заснованих на розширення відмінностей, і деякі з останніх пов'язаних робіт роз'яснюються. У [27] попередня обробка використовується для запобігання проблемам з недоліком та переповненням. Це допомагає обійти обставини у випадку, якщо ймовірність того, що вбудовані пікселі мають вищі значення в порівнянні з найвищим і найнижчим діапазоном зображення обкладинки. Найменш значущі біти обкладинки не пошкоджені, що дозволяє системі бути оборотною. Стиснення розміру найменш значущого біта даних забезпечується за рахунок застосування кодування Хаффмана і ховається разом із прихованою інформацією на етапі впровадження. Схема прогнозування на основі методу GAP [28] використовується для виведення активної частини

вбудовування. Потім виводиться генерація різницевого зображення з фактичного покриття та передбаченого покриття.

Відбувається вбудовування секретної інформації поверх розширеної форми фактичного різницевого зображення. Маніпуляції з розширеним діапазоном дозволяють збільшувати чи зменшувати можливості впровадження. Чим вище значення розширеного діапазону, тим вища швидкість впровадження та зворотний стан погіршення якості зображення. Тому діапазон розширення регулюється для дотримання балансу між непомітністю зображення та вантажопідйомністю. Порогове значення, реалізоване у різницевому зображенні разом із використанням флаг- бітів при великих значеннях різниці, допомагає пригнічувати викиди у нешкідливому інтервалі. Додатковий стеганографічний алгоритм, заснований на розширенні відмінностей, пояснений Юнг та ін. [3]. У цьому випадку стратегія, заснована на розширенні різниці рівнів блоків, використовується на додаток до механізму інтерполяційного прогнозування. Розширення зображення обкладинки виконується до кількох масштабів, а вбудовування виконується відповідно до простору масштабу.

Вхідні зображення поділяються на підблоки кожного рівня масштабування, та біти впровадження визначаються для кожного розширеного підблокування. Використання ключового параметра масштабування може дозволити коригування ємності застосування. Визначення ємності корисного навантаження 4 BPP виконується за межі масштабування 3 та візуальній якості PSNR 30 дБ. Цей метод схильний до вразливостей до геометричних і статистичних атак, а також всіх недоліків оборотних методів.

У [28] представлена додаткова система стеганографії, заснована на оборотному зображенні великої ємності. Основна процедура полягає у встановленні різницевого зображення між фактичними даними обкладинки та прогнозованим зображенням, заснованим на еталонних пікселях з носія обкладинки. Крім того, відбулося вбудовування помилкового зображення в приховану інформацію, яке використовується як стегозображення, з метою зв'язку. Обмеження вбудовування визначається місцезнаходженнями пікселів, в яких різниця знаходиться вище порогового значення, і це регулювання допомагає

підтримувати бездоганну систему щодо переповнення та не доповнення. На стороні одержувача еталонні пікселі можна відрізнити за значеннями пікселів та попередньо налаштованими граничними значеннями. Секретні біти обмежуються за допомогою процедури зворотного вбудовування зі стегозображення. Основна зацікавленість у тому, щоб вбудовування не вимагало вибору руйнівного еталонного піку з карти гістограми. Швидкість вбудовування також може бути змінена відповідно до вимог наслідків нижчої візуальної якості. Загальний висновок тягне у себе обмеження методів розширення відмінностей цільовими додатками, й у разі зображення обкладинки життєво важливо, а канал зв'язку стійкіший до атак зловмисників.

2.1.8 Стеганографія на основі декількох бітових площин

Цей метод був розроблений у 2006 році як розширення стандартного методу підстановки LSB, і в цьому випадку бітові площини використовувалися для приховування секретних бітів даних. Зазвичай стеганосистеми бітової площини використовуються разом з альтернативними методами як підсилювач продуктивності всієї системи. Таким чином, це часто асоціюється з альтернативною класифікацією домінуючого образу стеганографії.

Система стеганографії, заснована на сегментації бітової площини, показана у [29]. І тут складність окремих бітових площин оцінюється до процедури застосування. Це досягається шляхом вибору бітових площин з великим значенням шуму, а потім створюється відповідна матриця Хессенберга, частина розкладеної матриці Q.

Після процедури вбудовування розібрані частини Q і R поєднуються, після чого створюється стегозображення. У разі вибору оптимального зображення обкладинки результуючим ефектом буде ідеальний вибір бітової площини, що дозволяє вбудовувати секретні біти без погіршення візуальної якості. Серйозний системний збій тягне за собою можливість зображення, яке не сприймається, яке може бути анульовано у разі помилкового. вибір бітового зрізу. Він також зазнає негативних наслідків у результаті додаткових похибок висновку, пов'язаних із

середньою методикою LSB. У [30] автори рекомендували зазначений метод за рахунок використання бітових площин значень інтенсивності пікселів для упаковки секретних даних. Перший етап включає поділ системи на множину бітових площин, при цьому необхідна кількість площин вибирається з використанням послідовності ANR255. За збереження вищих цілей безпеки шифрування секретних даних здійснюється до фактичної процедури вбудовування. Він використовує 13-бітний кодувальник ANR площини, і біти секретних даних вбудовуються в ці розширені бітові фрагменти.

Після процедури вбудовування зображення обкладинки повертається до типовому 8-бітному представлення перед використанням його як стегозображення. Кодування бітової площини, що зазнало розширення, дає подвійні переваги. По-перше, дозволяє розміщувати додаткові секретні біти, ніж звичайні 8-бітові методи LSB. З іншого боку, буде високий рівень хаотичного впровадження, що призведе до створення більш надійної системи із стійкою системою захисту, котра протидіє процесу стегоаналізу зловмисника. Додаткова системна перевага спричиняє відсутність необхідності в загальній системі кодування між співрозмовниками. Зв'язок сприйнятливості стегозображення до геометричних атак як серйозної невдачі та найменшої зміни вирівнювання пікселів може призвести до шифрування вбудованої інформації.

2.1.9 Стеганографія на основі палітри

В [31] запропоновано використання зображень на основі палітри в якості обкладинки. Відповідними форматами зображень є PNG, GIF та TIFF. Псевдовипадкові числа генеруються з використанням секретного ключа, і вибраний біт секретних даних буде вставлений в один піксель покриття. Замість вихідного кольору у процесі вбудовування використовується колір із тим самим паритетом, як і секретний біт на палітрі. Як правило, стеганосистема на основі палітри можна розділити на два типи кольору палітри, модифікується для створення спотворення в невеликому діапазоні. У таких системах вбудовуюча здатність виявляється невеликою.

Другий тип підтримує деталі, що стосуються кольору даних обкладинки, але налаштовує елементи палітри відповідно до біт секретних даних і підтримує щільне вбудовування. Основний акцент до використання стеганографії на основі палітри пов'язаний із меншим всебічним спотворенням у стегозображенні порівняно з альтернативними просторовими методами. Вимога, щоб зображення були у певних форматах стиснення без втрат, є основним недоліком цього підходу. Він не застосовується до широко використовуваних форматів зображень, таких як JPEG. В результаті цей підхід менш кращий і менше використовується для реальних програм. Імаїдзумі та ін. [31] запропонували щільну схему вбудовування зображень, яка використовує стеганографічну систему на основі палітри, яка підтримує візуальну якість на адекватному рівні для не відстежуваного зв'язку.

Цей метод дозволяє вбудовувати мультиплексні біти прихованих даних в один піксель, що призводить до оцінки відмінності з використанням методів евклідової відстані, за допомогою чого більшість системи палітри відповідає схемі один біт на піксель. Він використовує перевірку парності для вбудованого зменшення помилок. Попередньою умовою, яка має бути виконана у цій схемі приховування, є спільне використання позицій відображення місця впровадження між співрозмовниками для забезпечення точного отримання секретної інформації. У порівнянні з альтернативними системами, заснованими на палітрі, ємність корисного навантаження знаходиться на межі того, щоб вважатися великою. З метою отримання підвищених характеристик безпеки, вибір пікселів для процедури вбудовування виконувався випадковим чином.

Процедура вбудовування починається з формування фрактальних зображень Жюліа-сета за заданими обмеженнями. Реалізовано вилучення колірних каналів з подальшим компонуванням палітри кольорів відповідно. Потім виконується випадковий вибір пікселя, і індекс палітри підтримується в актуальному стані відповідно до оптимального збігу секретних бітів з подальшим оновленням пікселя стегозображення відповідно. Потрібно, щоб вбудовування було загальним на стороні одержувача, а приховані дані витягувалися шляхом порівняння фактичного індексу з індексом впровадження. Однак це допомагає підтримувати

якість зображення в діапазоні 60 дБ, а альтернативні функції стеганографії в цьому розділі не враховуються. Всебічна оцінка стеганографії на основі палітри неадекватна, якщо взяти до уваги просунуті стеганографічні системи LSB.

2.1.10 Стеганографія на основі квантування

Використовує всі типи системи кодування зі стисненням для приховування бітів прихованої інформації. Система, яка використовується для кодування, може бути знайдена в різних формах типових кодеків, що використовуються для стиснення, таких як JPEG, вектор перетворення та інші. Як правило, прихована інформація поділяється на невеликі блоки підвибірок даних, які виходять шляхом вбудовування цих дрібних фрагментів даних у закодовані зображення обкладинок.

На стороні одержувача виконується точне кодування стегозображення, де пошук прихованих даних стає можливим завдяки використанню процесу вбудовування. Система стеганографії, що використовує зображення, і в цьому випадку приховані дані вбудовуються в JPEG кодувальник. Для процедури стиснення використовується кодер JPEG, який забезпечує блоки розміром 8x8 пікселів, де виконується поділ секретної інформації на невеликі частини, які повинні бути приховані за перетвореними коефіцієнтами. Для прихованих даних може знадобитися множина коефіцієнтів кодувальника розміщення всієї фрагментації. У процесі стиснення кодер JPEG використовує блоки розміром 8 x 8 пікселів, в яких секретні дані поділяються на дрібні фрагменти для маскування цих перетворених коефіцієнтів. Секретним даним може знадобитися кілька коефіцієнтів кодувальника розміщення повного фрагмента.

Аналогічно виконується вбудовування цілих секретних фрагментів в один або додаткові коефіцієнти стиснення, при цьому на стороні одержувача виконується зворотна процедура над стегозображенням, при цьому первісна форма виходить шляхом компіляції секретних бітів . Системі не потрібно жодної інформації, що стосується розташування коефіцієнта, і на адаптивний вибір впливає статистика зображення, щоб встановити місце вбудовування. Цей метод

підходить для використання з будь-якими кодувальниками і пропонує додаткові переваги. Пояснення безлічі удосконалених форм стеганографії зображень на основі квантування знаходиться в галузі досліджень, що стосуються поліпшення пропускної спроможності та зведення до мінімального масштабу спотворення. Серед них один із компонентів цього метод використовує модифіковану таблицю квантування DCT для кольорового зображення та адаптивну приховану стеганографію, засновану на простому оптимальному квантуванні.

2.2 Програмні рішення стеганографії

Розглянемо найбільш поширене на сьогоднішній день ПЗ, що реалізує методи стеганографії.

Anubis – програма, в якій як контейнери використовуються медіафайли формату BMP. Як прихована інформація - текстовий файл. Інформація, що приховується, дописується в кінець файлу. Виявлення таких вкладень здійснюється елементарно.

DeEgger Embedder - як контейнери використовуються медіафайли форматів BMP, PNG, JPG, AVI, MP3. Інформація, що приховується, як і в попередньому випадку, дописується в кінець файлу. Таке вкладення дуже легко виявити.

DeepSound - як вихідні контейнери використовуються файли формату WAV (тільки стиснутий, PCM), MP3, CDA, WMA, APE, FLAC, при цьому на виході, після впровадження інформації, можуть вийти файли тільки форматів WAV, APE, FLAC. Для вкладення інформації у цій програмі використовується алгоритм вкладення. Дана програма дає змогу спершу зашифрувати криптографічний алгоритм AES, що приховується.

Hallucinate – як контейнери використовуються файли формату BMP, PNG. Як стенографічний алгоритм використовується алгоритм LSB.

JHide – як контейнери використовуються файли формату BMP, PNG, TIFF. Як стенографічний алгоритм використовується алгоритм LSB.

OpenPuff - як контейнери використовуються медіафайли з нерухомими картинками, відеопотоком або аудіозаписами (наприклад, MP4, MPG, VOB). Як

стенографічний алгоритм використовується алгоритм LSB. Прихована інформація також захищається стійким криптографічним генератором псевдовипадкових чисел.

OpenStego - як вихідні контейнери використовуються файли формату MP, PNG, JPG, GIF, WBMP. Існує можливість використання шифрування типу AES.

QuickStego - як вихідні контейнери використовуються файли формату BMP, JPG, GIF, при цьому на виході, після впровадження інформації, можуть вийти файли тільки формату BMP. У платній версії програми можна використовувати файли формату WAV, MP3. Як стенографічний алгоритм використовується алгоритм LSB.

Xiao Steganography – як контейнери використовуються файли формату BMP, WAV. Ця програма також дозволяє попередньо зашифрувати криптографічними алгоритмами RC4, Triple DES, DES, Triple DES 112, RC2 і алгоритмами хешування SHA, MD4, MD2, MD5.

SilentEye - як контейнери використовуються файли формату BMP, JPG, PNG, GIF, TIF, WAV. Для шифрування інформації, що вкладається криптографічними методами використовується алгоритм AES.

Steghide - як контейнери використовуються файли формату JPG, BMP, WAV та AU. Як стенографічний алгоритм використовується алгоритм LSB.

SSuite Picsel Security - як контейнери використовуються файли формату BMP, JPG, WMF, PNG.

StegoStick (beta) – як контейнери використовуються файли формату JPG, BMP, GIF, WAV, AVI, PDF, EXE, CHM. Для шифрування інформації, що вкладається криптографічними методами використовуються алгоритми DES, Triple DES, RSA.

Trojan - як вихідні контейнери використовуються файли формату JPG, BMP, TIF, GIF, PNG, MNG, PCS, TGA, при цьому на виході, після впровадження інформації можуть вийти файли тільки форматів BMP, PNG, TIF.

SecurEngine Professional 1.0 – як контейнери використовуються файли формату BMP, GIF, PNG, HTM. Для шифрування інформації, що вкладається криптографічними методами використовуються алгоритми AES, Gost, BlowFish,

ThreeDe.

bmpPacker 1.2a - як контейнери використовуються файли лише формату BMP. Для шифрування інформації, що вкладається криптографічними методами використовуються алгоритми AES, BlowFish, TwoFish.

MP3Stego 1.1.16 - як контейнери використовуються файли тільки формату MP3.

Hide and Seek 5.0 - як контейнери використовуються файли лише формату GIF. Для шифрування інформації, що вкладається криптографічними методами використовується алгоритм BlowFish.

Hide'N'Send - як контейнери використовуються файли лише формату JPEG. Як стенографічні алгоритми використовуються алгоритми LSB і F5. Для шифрування інформації, що вкладається криптографічними методами використовуються алгоритми AES, RC4, RC2.

S-Tools - як контейнери використовуються файли з нерухомими зображеннями або звуком. Для шифрування інформації, що вкладається криптографічними методами використовуються алгоритми DES, Triple DES і IDEA.

Jsteg – як контейнери використовуються файли формату JPG. Як стенографічний алгоритм використовується алгоритм LSB.

StegoDos - як контейнери використовуються файли з нерухомими зображеннями.

Steganos – як контейнери використовуються файли формату BMP, DIB, VOC, WAV, ASCII, HTML. Для шифрування вкладеної інформації криптографічними методами використовується алгоритм AES.

DarkJPEG – як контейнери використовуються файли формату JPEG. Для шифрування інформації, що вкладається криптографічними методами використовується алгоритм AES.

FFEncode - як контейнери використовуються текстові файли.

Проаналізувавши ПЗ, що використовує алгоритми стеганографії, можна зробити висновок, що найбільш часто як контейнери для вкладення використовуються медіафайли з нерухомими зображеннями. Існує кілька причин

популярності саме зображень як контейнери для стеговкладень. Також видно, що жодне із розглянутих рішень не працює із зображеннями RAW.

2.3 Розробка стеганографічного алгоритму в RAW зображення

У цьому підрозділі описана постановка завдання приховування даних у зображенні RAW та алгоритм реалізації вбудовування та виявлення інформації. Також у розділі наведено способи оцінки стенографічних алгоритмів.

2.3.1 Опис алгоритму передачі даних всередині RAW зображення

У підрозділі 2.1 був обраний спосіб LSB. Математичне представлення вбудовування має вигляд (2.1):

$$s_i = x_i - x_i mod(2^k) + m_i, \tag{2.1}$$

де s_i - змінювані і -ті дані RAW зображення; x_i - вихідні і -ті дані RAW зображення; m_i –і-тий біт прихованої інформації; k - номер біта, що замінюється.

Для реалізації вбудовування та отримання прихованої інформації були розроблені такі алгоритми:

– вбудовування даних;
– вилучення даних;
– визначення метаданих;
– одержання інформації для декодування необроблених даних;
– отримання даних сканера.

В роботі розглянуто вбудовування у формат CR2 від компанії Canon. На рис. 2.2 наведено схему роботи алгоритму вбудовування в RAW зображення формату CR2. Для того щоб вбудувати дані у формат RAW зображення для початку необхідно прочитати формат RAW у байтовому вигляді та визначити з якого байта починається директорія даних, захоплених з сенсора.

Заголовки складаються із даних заголовка TIFF, їх розмір становить 8 байт. Перші 2 біти показують порядок читання байт у файлі, можливо читання справа наліво чи навпаки зліва на право. Наступні 2 байти константа з формату TIFF, значення цих байт завжди дорівнює 002a. Наступні 4 байти є вказівником на зміщення до першої директорії зображення у форматі jpeg , що зберігається у форматі CR2.

Рисунок 2.2 – Алгоритм вбудовування в RAW зображення формату CR2

Потім після переходу за покажчиками до даних директорії необхідно обрахувати кількість тегів, що зберігаються в даній директорії зі своїми значеннями. Після прочитання всіх тегів у директорії розташований вказівник на наступну директорію із зберіганням даних про мініатюру зображення у форматі jpeg. У директорії мініатюри дані структуровані так само, як і в попередній директорії, тому зчитуємо всі наступні директорії. Читання директорій

припиняється після того, як покажчик дорівнюватиме нулю.

Для отримання даних із сенсора збережених у CR2 необхідно розробити алгоритм визначення заголовків, директорій файлів зображень та визначити зміщення до директорії необроблених даних сенсор. На рис. 2.3 представлений даний алгоритм.

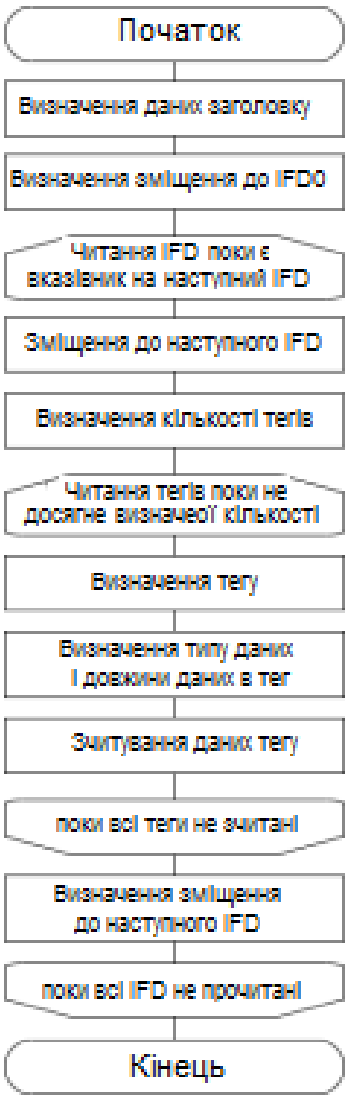

Рисунок 2.3 – Алгоритм визначення метаданих

Після визначення директорії необробленого зображення необхідно опрацювати внутрішні теги стиснення зображення. У даному форматі RAW зображення дані із сенсора цифрової камери знаходяться в стислому вигляді за допомогою коду Хаффмана. На рис. 2.43 продемонстровано алгоритм отримання

інформації про довжину та ширину зображення сканера, а також про кількість компонентів зображення, отримання коду Хаффмана та довжин даних.

Рисунок 2.4 – Алгоритм отримання інформації для декодування необроблених даних

Після визначення коди Хаффмана та зашифрованих в них довжини даних сканера приступаємо до читання необроблених даних із цифрової камери (рис. 2.5). Для подальших обчислень переводимо дані зчитані із зображення в біти і з початку проводимо пошук коди Хаффмана при його знаходженні зіставляємо ключ із зашифрованою довжиною і такі дані зазначеної довжини і є дані сенсора. Продовжуємо пошук кодів Хаффмана та наступних даних сенсора до кінця даних зображення.

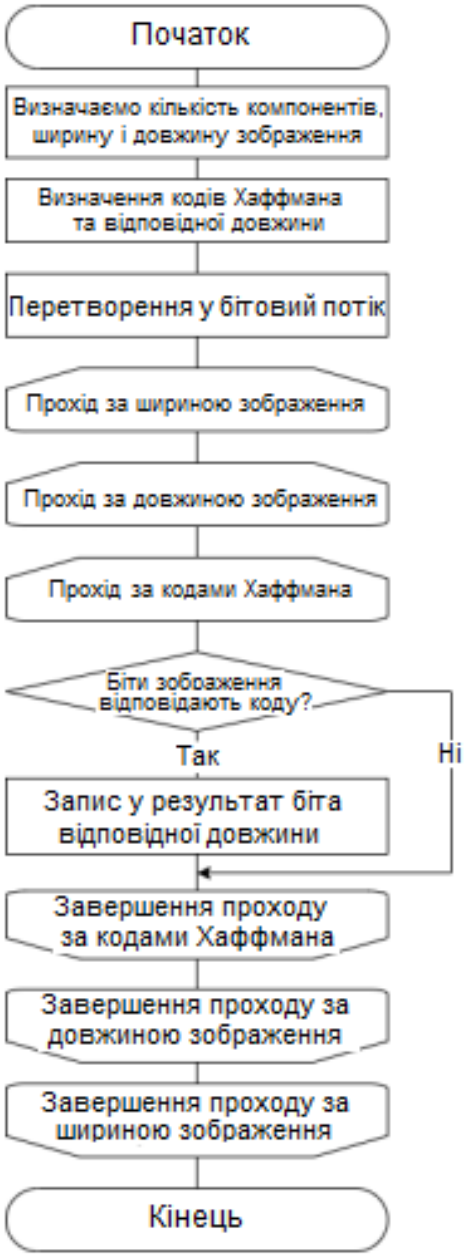

Рисунок 2.5 – Алгоритм отримання необроблених даних

Після обчислення необроблених даних необхідно приступати до приховування інформації в цих даних. На рис. 2.6 показано алгоритм вбудовування даних. Для більшого вбудовування перед безпосереднім приховуванням даних у RAW зображення використовуємо бібліотеку zlib для зменшення кількості байт інформації. Для вбудовування перетворимо дані на бітовий потік для приховання. Також перед інформацією додаємо дані про формат даних та їх розмір.

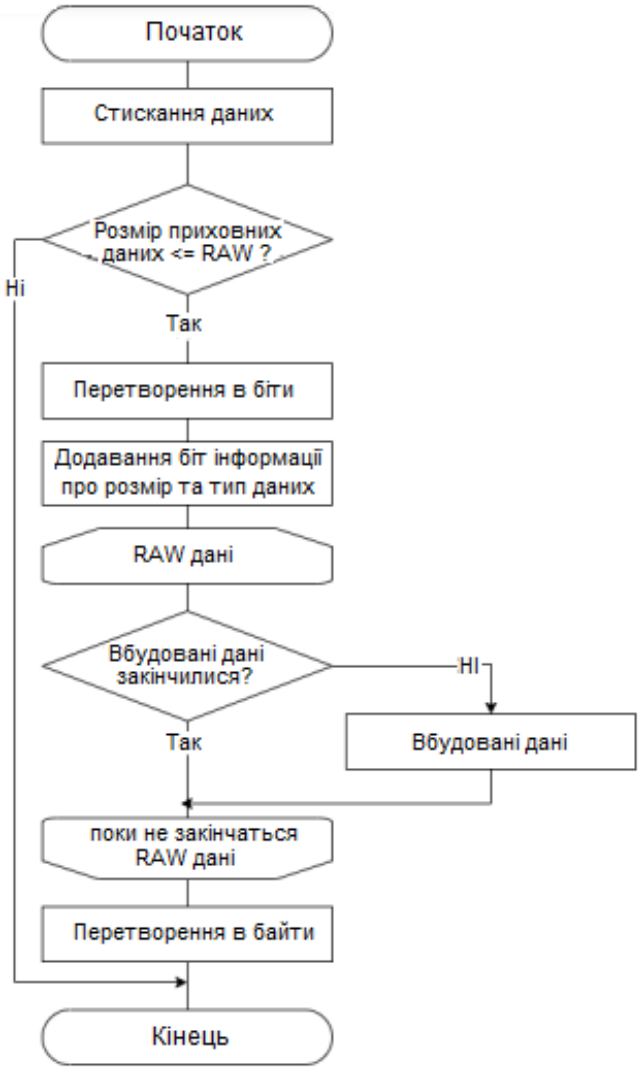

Рисунок 2.6 – Алгоритм вбудовування даних

Для вбудовування необхідно стиснути дані, які будуть вставлені у дані RAW зображення. Після цього необхідно перевести дані приховуваного повідомлення в бітовий потік з додаванням інформації про розмір і тип секретного файлу. Процес вбудовування проходить так обчислюється половина довжини необробленого даного і замінюється менш значні біти інформації. Процес триває остаточно необроблених даних. Необхідно пройтися за всіма даними зображення перетворення їх у бітовий потік подальшого перетворення. Після вбудовування дані переводяться в байтовий потік і записуються у файл розширення CR2.

Для декодування даних, зашифрованих в RAW зображенні, проводиться, як і при приховуванні, аналіз файлу, пошук директорії даних з сенсора і за допомогою таблиці Хаффмана, що зберігається, обчислюється дані сенсора. Після отримання

необроблених даних переходимо безпосередньо до вилучення даних. На рис. 2.7 розглянуто схему алгоритму.

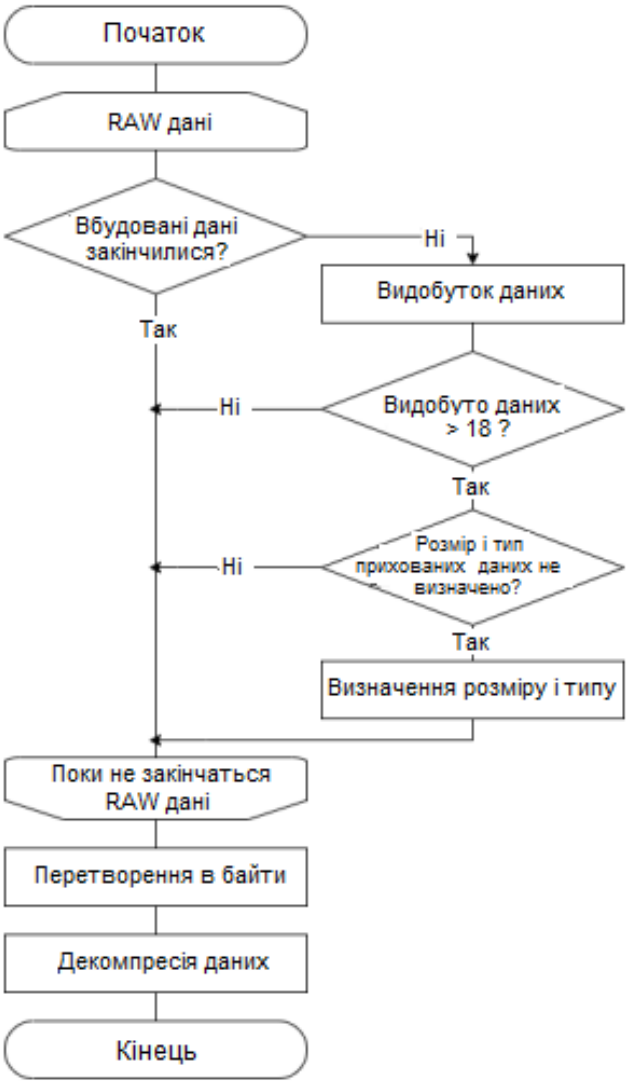

Рисунок 2.7 – Алгоритм вилучення даних

Після отримання необроблених даних необхідно визначити тип прихованої інформації та її розмір. Після обчислення даних показників починається вилучення прихованого повідомлення. Для цього кожна отримана RAW інформація ділиться навпіл. Потім витягується найменша половина справа. Після декатирування повідомлення проводиться перетворення на байтовий потік даних і розархівування за допомогою бібліотеки zlib для збереження в певному форматі даних.

2.3.2 Оцінка ефективності стеганографії у зображеннях

Проведення оцінки визначення візуальної стійкості властиво стеганографічної системи щодо впливів ззовні вважається достатньо складною задачею. З метою оцінки якості власне стеганографічних засобів формуються показники, котрі видають кількісні оцінки. Найбільш часто ці показники працюють із зображеннями тільки на рівні пікселів та, більше того, окремих RGB-складових пікселів. Найважливішими ознаками при аналізуванні міри спотворень, що поміщаються у зображення при приховуванні в ньому інформації, вважаються кореляція сигналу і шуму, обчислена щодо якості зображення, котра визначається у відсотках. На додачу до інших ознак варто виділити середню абсолютну різницю значень пікселів, нормовану середню абсолютну різницю значень пікселів та максимальне відношення сигнал шум. У табл. 2.2 наведено найбільш поширені показники візуального спотворення, засновані на аналізі піксельної структури контейнера, та формули їх обчислення.

Таблиця 2.2 – Показники візуального спотворення

Показники спотворення	Формула для розрахунку	Оригінал	LSB
1	2	3	4
Середня абсолютна різниця (Average Absolute Difference)	$AD = \frac{1}{XY}\sum_{x,y} \lvert C_{x,y} - S_{x,y} \rvert$	0	6,774072
Нормована середня абсолютна різниця (Normalized Average Absolute Difference)	$NAD = \frac{\sum_{x,y} \lvert C_{x,y} - S_{x,y} \rvert}{\sum_{x,y} \lvert C_{x,y} \rvert}$	0	0,096575
Середньоквадратична помилка (Mean Square Error)	$\mathrm{MSE} = \frac{1}{\mathrm{XY}} \cdot \sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2$	0	0,591680
Відношення сигнал/шум (Signal to Noise Ratio)	$SNR = \frac{\sum_{x,y} (C_{x,y})^2}{\sum_{x,y} (C_{x,y} - S_{x,y})^2}$	inf	186,2152

Продовження таблиці 2.2

1	2	3	4
Максимальне відношення сигнал /шум (Peak Signal to Noise Ratio)	$PSNR = 10\log_{10}\left(\frac{\max_{x,y}(C_{x,y})^2}{MSE}\right)$	inf	39,40993
Якість зображення (Image Fidelity)	$IF = 1 - \frac{\sum_{x,y}(C_{x,y} - S_{x,y})^2}{\sum_{x,y}(C_{x,y})^2}$	1	0,994630
Міра структурної подібності	$SSIM = \frac{(\sigma_{xy})(2\bar{X}\bar{Y})(2\sigma_x\sigma_y)}{(\sigma_x\sigma_y)(\bar{X}^2 + \bar{Y}^2)(\sigma_x^2 + \sigma_y^2)}$	1	0,999923

Показники такі розраховуються із використанням різниці контейнерів (оригіналу та стего-). У представлених співвідношеннях через C_{xy} позначено складова пікселя незаповненого контейнера із (x, y) координатами, у котру відбувається вбудовування, тоді як через S_{xy} - певна складова пікселя вже заповненого контейнера, $\bar{X}$ та $\bar{Y}$ - середні значення пікселів, через σ позначається середньоквадратичне відхилення.

Для оцінки погіршення якості raw зображення при стеганографії використовуватиметься параметр IF та SSIM. Ці параметри демонструють спотворення зображення наочно. Стандартні значення PSNR для зображень лежать у межах 30-40. Оскільки це відношення корисного сигналу до шуму, тому чим вище значення PSNR, тим менше шуму створює вбудовування. Вбудовування у зображення вважається прийнятним, якщо SSIM > 0,89, IF > 0,80.

2.4 Висновки до другого розділу

Було узагальнено поширені методів стеганографії зображень у просторовій області. Кожна техніка унікальна та не схожа на іншу. Найменша частина з них займається покращенням якості зображення, в той час як інші займаються дослідженнями, пов'язаними зі здатністю приховувати дані або питаннями

безпеки. Результати розглянутих додатків відрізняються один від одного за якістю та швидкістю роботи. Для проведення подальшої роботи було обрано спосіб стеганографії вбудовування LSB.

Алгоритм LSB володіє низькою обчислювальною складністю, потребує для функціонування мінімального часу, володіє вельми значною прихованою пропускною здатністю, а також вносить найменші візуальні завади. Проте основний його недолік – він є нестійким майже до усіх типів атак. Саме це і ускладнює застосування його у стегоканалах із значною ймовірністю атак. Але в розроблюваному випадку обсяг даних RAW зображення неймовірно великий через це необхідний метод, робота якого займала б найменше часу. Тому було обрано спосіб LSB.

Розібрано алгоритми для застосування стеганографії у RAW зображеннях, що реалізується в даній роботі. Також описано процеси структурування структури формату CR2 RAW зображення. Було розроблено методи обробки формату RAW зображення, метод вбудовування інформації та метод прояву інформації з RAW зображення.

Було розглянуто метрики оцінки ефективності вбудовування даних зображення. За результатом аналізу параметрів було обрано метрики SSIM та IF. Міра структурної подібності має бути більшою, ніж 0,89, а показник якості зображення потрібен більший, ніж 0,80.

РОЗДІЛ 3 ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ

У цьому розділі надається реалізація розроблених алгоритмів у розділі 2. Продемонстровано користувацький інтерфейс. Наведено приклади роботи розробленого ПЗ. Також проаналізовано результати за метриками, вибраними у розділі 2.

3.1 Реалізація стеганографії на основі RAW зображення

При реалізації вбудовування даних в RAW зображення необхідне середовище розробки, в якому можна реалізувати інтерфейс користувача. Крім цього, також знадобиться високорівнева мова програмування, функціонал, якої дозволить досягти кращих результатів роботи програми, а процес розробки коду буде максимально ефективним. Для цього рішення буде доцільний вибір такої мови програмування, як Python. Простий доступ до бібліотек дозволить скоротити час на розробку алгоритму за допомогою наявних у них функцій. Так як, необхідний інтерфейс користувача, а результатом даної роботи буде застосунок під операційні системи Windows, то потрібно середовище розробки, яке підходить під критерії і обрану мову програмування. Таким середовищем розробки є PyCharm, котре було створено спеціально під програмування мовою Python. Розробники цього рішення виділяють кілька переваг:

– автодоповнення, яке працює у режимі реального часу;
– пропозиції щодо покращення читаності коду;
– швидке виправлення помилок;
– проста навігація по коду, що розробляється;
– висока продуктивність та оптимізація програми.

З отриманої інформації можна дійти висновку, що це рішення є досить зручним для його використання у цій роботі. Програмна реалізація даної роботи втілена як застосунок для персональних комп'ютерів. Розглядати системні вимоги в даній ситуації вважатимемо недоцільним тому, що запустити наше програмне рішення можливо навіть на слабкому устаткуванні. Однак, варто враховувати, що

швидкість роботи самого алгоритму та обробки зображення буде різною на обладнанні з різною потужністю.

Інтерфейс програми розроблено за допомогою бібліотеки tkinter. Користувальницький інтерфейс – це вікно програми, в якому є можливість вибору дії приховування та проявлення, яка потрібує натискання кнопки «Encode» для приховування та «Decode» для проявлення, як наведено на рис. 3.1.

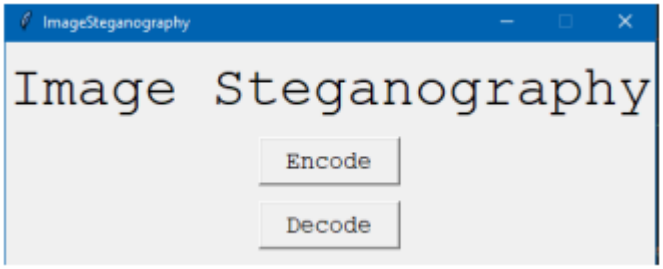

Рисунок 3.1 – Стартове вікно програми

Після переходу по кнопці приховування необхідна вибрати файл RAW зображення для вбудовування даних та файл, дані якого будуть приховані, як показано на рис. 3.2. Після натискання кнопки Hide почнеться процес приховування. Файл результату зберігається автоматично в директорії програми.

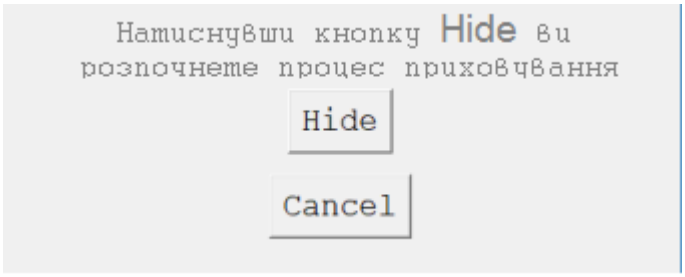

Рисунок 3.2 – Вікно методу приховування даних

Також є процес проявлення прихованих повідомлень. Ця функція доступна за кнопкою «Decode». Після натискання цієї кнопки з'явиться вікно вибору файлу для роботи з ним. Потім після визначення файлу буде доступна кнопка Decode, після натискання на яку починається процес витягування даних із завантаженого файлу. На рис. 3.3 представлений вигляд вікна програми.

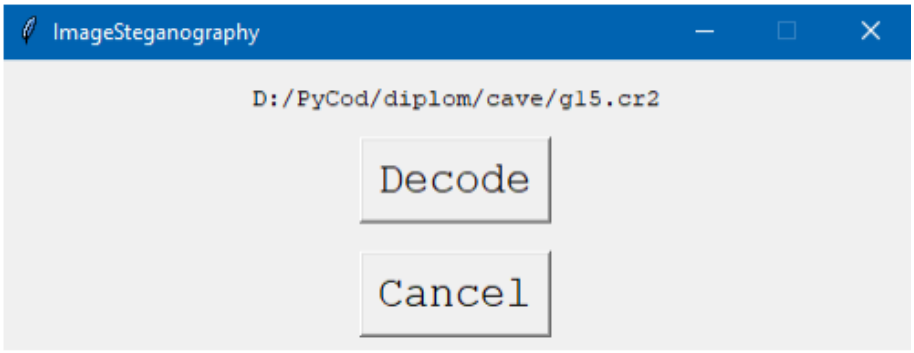

Рисунок 3.3 – Вікно методу проявлення даних

На рис. 3.4 показаний приклад інформації, що вбудовується. Далі продемонстровано роботу програми на трьох зображеннях на рис. 3.5. Основними вимогами для вбудованих даних є переведення даних у бітову послідовність і показник IF не повинен бути нижчим за 0,99 при порівнянні RAW зображення з прихованою інформацією і без неї.

Перед кожним, хто прочитає цю книгу, постане панорама розвитку однієї зі своєрідних літератур світу з моменту її зародження до першої третини XX століття. По суті, книга Н. І. Конрада являє собою першу і поки що єдину історію японської літератури і містить характеристику найважливіших , вузлових етапів її еволюції.

Рисунок 3.4 – Приховувана інформація

а) б) в)

Рисунок 3.5 – Зображення формату CR2 до вбудовування:
а) зображення 28 Мб; б) зображення 11 Мб; в) зображення 14 Мб

Для аналізу результатів приховування спочатку у зображення форматів JPEG, PNG і CR2 вставлявся текст розміром 100 Кб. За результатом приховування виділяються відмінності при вбудовуванні одного розміру даних у різні формати зображення обкладинки. Після отримання результатів при вбудовуванні однакового розміру вбудованих даних проводиться аналіз зображень при вбудовуванні обсягів даних, коли показник IF максимально наближений до граничного значення, яке ми визначили. У цій роботі мінімальне значення IF, яке допустили, дорівнює 0,99. Час роботи програми становив у середньому по всіх зображеннях 30,15 секунди. Це пов'язано з великим обсягом RAW зображення.

RAW зображення після вбудовування з IF не нижче 0,99 показані на рис. 3.6. При розгляді даних зображень можна помітити, що при вбудовуванні людським органом зору практично неможливо виявитися візуальне спотворення в RAW зображеннях.

а) б) в)

Рисунок 3.6 – Зображення формату CR2 після вбудовування:
а) зображення 28 Мб; б) зображення 11 Мб; в) зображення 14 Мб

3.2 Дослідження отриманих результатів роботи програми

Аналіз ефективності вбудовування перевірялося більш, ніж на 10 зображеннях формату CR2 з бази RAW зображень PIXLS.US [32]. Для порівняння отриманих результатів досліджуємо спосіб приховування LSB у форматах JPEG,

PNG та CR2. Для аналізу вбудовування JPEG і PNG були перетворені CR2 зображення. Отримані результати оцінки ефективності усереднені. Одержані величини параметрів візуального спотворення для JPEG, PNG і CR2 зображень при вбудовуванні 100 кб наведено в табл. 3.1.

Таблиця 3.1 – Величини візуального спотворення при вбудовуванні 100 кб

	Роздільна здатність	Розмір до приховання (Мб)	Об'єм прихованих даних (Кб)	Розмір після приховування (Мб)	Час роботи (мс)	SSIM	IF
а. JPEG	5616 на 3744	3,84	100	22,86	1188	0,99985	0,9952
б. JPEG	3000 на 4000	1,28	100	10,79	306	0,99992	0,99463
в. JPEG	2736 на 3648	1,2	100	9,42	270	0,99993	0,99520
а. PNG	5616 на 3744	9,14	100	9,74	3148	0,99981	0,99540
б. PNG	3000 на 4000	7,31	100	7,6	2583	0,99993	0,99391
в. PNG	2736 на 3648	5,77	100	8,52	1982	0,99997	0,99641
а. CR2	5616 на 3744	28,46	100	28,46	38907	0,99999	0,99977
б. CR2	3000 на 4000	11,95	100	11,95	20049	0,99999	0,99870
в. CR2	2736 на 3648	14,06	100	14,06	31504	0,99999	0,99975

У табл. 3.1 наведено дані після вбудовування 100 кб даних у три формату зображення з різною роздільною здатністю та обсягом параметри SSIM та IF в середньому для JPEG рівні відповідно 0,999, 0,995, для PNG рівні відповідно 0,9999, 0,9952, для CR2 рівні відповідно 0,9999, 0,9994.

У табл. 3.2 зібрані дані за середнім значенням даних, які вбудовуються у зображення та зберігають параметр IF на рівні 0,99. У CR2 приховані дані зі збереженням вихідного обсягу та формату. Якщо завдання зберегти вихідний формат і розмір не поставлена, то можливе вбудовування до половини даних по всій ширині та висоті та зберегти зображення у форматі TIFF.

Таблиця 3.2 – Показники візуального спотворення при IF >0,98

	Роздільна здатність	Розмір до приховання (Мб)	Об'єм прихованих даних (Кб)	Розмір після приховування (Мб)	Час роботи (мс)	SSIM	IF
а. JPEG	5616 на 3744	3,84	7200	27,6	2511	0,9999	0,9912
б. JPEG	3000 на 4000	1,28	4000	13,59	370	0,9997	0,9934
в. JPEG	2736 на 3648	1,2	3400	12,69	339	0,9995	0,9957
а. PNG	5616 на 3744	9,14	7200	30,56	6106	0,9998	0,9980
б. PNG	3000 на 4000	7,31	4000	15,2	4683	0,9997	0,9954
в. PNG	2736 на 3648	5,77	3400	14,91	2584	0,9996	0,9900
а. CR2	5616 на 3744	28,46	12000	28,46	37528	0,9999	0,9936
б. CR2	3000 на 4000	11,95	5000	11,95	21524	0,9999	0,9921
в. CR2	2736 на 3648	14,06	8000	14,06	31341	0,9999	0,9932

За результатом роботи програми можна зробити висновок, що чим об'ємніше RAW зображення використовується для приховування, тим довше буде виконуватися програма, як приховування так і розкриття. Також необхідно зазначити, що при прихованні у форматах JPEG та PNG змінюється обсяг зображення із вбудованими даними. Однак при прихованні розробленим алгоритмом приховування RAW зображенні обсяг зображення з вбудованими даними не змінюється.

Досліджуючи функціонування якого-небудь алгоритму одним із ключових його атрибутів ефективності вважається той час, котрий затрачений на роботу. Цей критерій є суттєвим обчислювальним ресурсом, відповідно мінімізація його витрат є істотною проблемою, яка постає перед розробником алгоритму. Було виміряно середній час (в секундах) функціонування алгоритму вмонтовування даних для JPEG, PNG і RAW форматів, що втілено у застосунку на Python. Такий час є середнім арифметичним часів, котрі затрачаються на відкривання RAW зображень, вбудовування даних і зберігання із прихованою інформацією.

Результат (середній час) показаний алгоритмом LSB для вбудовування у

JPEG становить 0,588 секунди, для PNG 1,571 секунди, для CR2 30,15 секунди. Час приховування із виконанням розробленого алгоритму залежить від формату вихідного зображення. Також на час роботи алгоритму впливає розмір зображення, в яке здійснюється вбудовування інформації.

3.3 Висновки до третього розділу

Продемонстровано результат роботи програми на трьох зображеннях різного розміру. Проаналізувавши результати можна зробити висновок про те, що зміна в необроблених даних сенсора несе в собі зміну в яскравості та корекції кольору зображення. При цьому розмір зображення не змінюється. Обсяг даних, який вдалося вбудувати дорівнює одній сьомій кількості байт файлу RAW зображення. Час вбудовування залежить від кількості байт у форматі RAW зображення, задіяного у зберігання необроблених даних із сенсора. Вдалося досягти приховування половини за кількістю байт RAW зображень.

При порівнянні використано метод стеганографії LSB вбудовування у зображеннях стандартних форматів зі стисненням. Було виявлено, що статистичні показники зміни зображення виявляють відхилення схоже з відхиленнями у форматах JPEG і PNG. Основні відмінності приховування RAW від JPEG і PNG в тому, що при вбудовуванні не змінюється обсяг зображення. Також обсяг RAW зображення завжди набагато перевищує обсяг JPEG та PNG. Слід зазначити, що обсяг RAW після вбудовування можна порівняти з обсягом PNG і JPEG після вбудовування. Однак при рівному об'ємі зображення розмір прихованих даних у RAW більше, ніж у PNG та JPEG.

РОЗДІЛ 4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Метою кваліфікаційної роботи магістра є програмна реалізація приховування даних у зображенні RAW з цифрових камер, а також розробка для цієї програми алгоритму стеганографії на основі RAW зображення. Оскільки, програмна реалізація приховування даних у зображенні RAW з цифрових камер, передбачає використання комп’ютерної техніки, зокрема ПК та периферійних пристроїв, то обов’язковим є дотримання вимог з охорони праці і техніки безпеки.

Для ефективної і безпечної роботи колективу працівників із аналізу аналіз алгоритмів, що виявляють спотворення та цілеспрямовану зміну інформації, необхідно організувати безпечні умови праці. При цьому керівник організації несе безпосередню відповідальність за порушення нормативно-правових актів з охорони праці [33]. Окрім цього, на робочих місцях працівників необхідно забезпечити дотримання вимог, затверджених Наказом Мінсоцполітики від 14.02.2018 за № 207 «Про затвердження Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями». Згідно Вимог приміщення, де розміщені робочі місця операторів, крім приміщень, у яких розміщені робочі місця операторів великих ЕОМ загального призначення (сервер), мають бути оснащені системою автоматичної пожежної сигналізації відповідно до цих вимог;

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 22.08.2005 N 161, зареєстрованого в Міністерстві юстиції України 05.09.2005 за N 990/11270 (НАПБ Б.06.004-2005);

– Державних будівельних норм "Інженерне обладнання будинків і споруд. Пожежна автоматика будинків і споруд", затверджених наказом Держбуду України від 28.10.98 N 247 (далі - ДБН В.2.5-56:2014, з димовими пожежними

сповіщувачами та переносними вуглекислотними вогнегасниками.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця операторів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами ДСТУ 4297:2004 «Пожежна техніка. Технічне обслуговування вогнегасників». Загальні технічні вимоги і з урахуванням граничнодопустимих концентрацій вогнегасної рідини відповідно до вимог НАПБ А.01.001-2014. Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.2.5-56:2014, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп’ютера та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники мають відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам НПАОП 40.1-1.01-97.

У приміщенні, де одночасно експлуатуються понад п’ять комп’ютерів, на помітному, доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Комп’ютери повинні підключатися до електромережі тільки за допомогою

справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання фазового та нульового робочого провідників. Порядок роз'єднання при відключенні має бути зворотним. Не допускається підключати комп'ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв. Електромережі штепсельних з'єднань та електророзеток для живлення комп'ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі. Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При підвищенні ефективності контролю доступу в приміщення, де для забезпечення безпеки мешканців, співробітників і збереження майна використовуються ДС, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у НПАОП 0.00-7.15-18. Організація робочого місця фахівця із дослідження методів та програмно-апаратних засобів оптимізаційних процесів на основі ГА повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».

Розміщення принтера або іншого пристрою введення-виведення інформації на робочому місці має забезпечувати добру видимість екрана комп'ютера, зручність ручного керування пристроєм введення-виведення інформації/

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп'ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної

роботи фахівців з програмної реалізації приховування даних у зображенні RAW з цифрових камер, а також розробка для цієї програми алгоритму стеганографії на основі RAW зображення.

4.2. Комп’ютерне забезпечення процесу оцінки радіаційної та хімічної обстановки

Екологічне співтовариство розробило сімейство інструментів комплексної екологічної оцінки. Програмне забезпечення і послуги (ESS), комерційна група IIASA, включаючи AirWare (для повітряних проблеми якості), WaterWare (для якості води), CityWare (якість повітря і води в контексті великих міст) і EIAxpert (для надання допомоги із загальним впливом на навколишнє середовище). Функціональність в цілому схожа на RAISON, хоча з великим акцентом на моделювання і меншим акцентом на керування даними. Знову ж таки, інструменти ESS розроблені як модульні набори інструментів (доступні спеціальні системи для вирішення конкретних завдань). Компоненти включають стандартні імітаційні моделі, включаючи моделі ISC і PBM Агентства з охорони навколишнього середовища США, управління даними, в тому числі ГІС, аналіз даних (наприклад, аналіз часових рядів даних спостережень), візуалізація, а також оптимізація [34].

Іноді немає готових моделей, придатних для конкретного застосування, але тягар розробки нової програми на Фортрані або C / C ++ є надмірним. Розробка моделі оточення може відносно легко реалізувати власні моделі комп'ютерів і не турбуватися про включення процедур для вирішення рівнянь, візуалізації і т. д. Як правило, за допомогою цих інструментів користувач просто повинен вказати свою модель, використовуючи або математичні рівняння, або спеціальні графічні символи або значки, які безпосередньо представляють поведінку системи.

На даний момент є розроблені моделі комп’ютерного забезпечення процесу для оцінки радіаційної та хімічної обстановки.

GEMS – це система на основі моделей, яка підтримує оцінки схильності і ризику, надаючи доступ до одиночних і мультимедійних моделям експозиції, фізико-хімічні властивості методи оцінки, статистичний аналіз, графічні та

картографічні програми з відповідними даними на навколишнє середовище, джерела, рецептори і популяції. У розробці з 1981 року, GEMS надає аналітикам 84 84 інтерактивний, легко досліджуваний інтерфейс для різних моделей, програм і даних, які необхідні для оцінки хімічного впливу і ризику [34].

HSPF – це комплексний пакет для моделювання кількості і якості стоків з багатоцільових водозборів і процесів радіації, що відбуваються в потоках або повністю змішаних озерах. Це дозволяє інтегроване моделювання землі і грунту, процесів забруднення при гідравлічній і осадово-хімічній взаємодії. Результатом моделювання є тимчасові дані витрати стоку, концентрація поживних речовин і пестицидів, а також дані кількості і якості води в будь-якій точці водозбору. Алгоритми якості води включають динаміку BOD / DO, вуглець, азот і фосфор. Процеси трансформації, які включені в модель це: гідроліз, фотоліз, окислення, випаровування, сорбція і биодеградація. Вторинні або «дочірні» хімічні речовини також моделюються.

Вимоги до даних для моделі можуть бути досить широкими в залежності від конкретного застосування.

Модель MMSOILS – це методологія оцінки впливу на людину і ризику для здоров'я, пов'язаних з викидами забруднень з небезпечних відходів. Мультимедійна модель, що стосується перенесення хімічної речовини в ґрунтові води, поверхневі води, атмосферу і накопичення в їжі. Шляхи впливу на людину, які розглянуті в методології включають: потрапляння в грунт, вдихання летких речовин в повітря і тверді частинки, шкірний контакт, прийом питної води і т.д. Ризик, пов'язаний із загальною дозою опромінення, розраховується на основі хімічної токсичності [34].

4.3 Висновки до четвертого розділу

В цьому розділі проаналізовано важливі питання охорони праці та безпеки в надзвичайних ситуаціях, висвітлено питання комп’ютерного забезпечення процесу оцінки радіаційної та хімічної обстановки.

ВИСНОВКИ

Метою даної роботи була розробка програми, яка реалізує вбудовування даних за допомогою методу стеганографії з приховуванням RAW зображень з цифрових камер. Ця проблема була успішно вирішена. У ході роботи було досліджено існуючі у світі методи стеганографії. Розглянуто структури форматів RAW зображень та було обрано відповідний та більш поширений для реалізації у програмі.

За результатами дослідження методів стеганографії в роботі було застосовано алгоритм LSB. Він має низьку обчислювальну складність, затрачає для функціонування мінімальний часовий проміжок, володіє величезною прихованою пропускною здатністю, на додачу ще й вносить найменші візуальні спотворення при вбудовуванні.

Розібрано алгоритм для вбудовування та вилучення інформації в RAW зображеннях на підставі методу стеганографії. Було розглянуто метрики оцінки ефективності вбудовування даних зображення. За результатом аналізу параметрів було обрано метрики SSIM та IF. SSIM має бути більшою ніж 0,998, а IF необхідний понад 0,98.

Реалізовано вбудовування даних збереження вихідного формату та розміру RAW зображення. Після розробки програми було проведено дослідження на вибірці більш, ніж з 10 зображень. Реалізована програма виконує поставлені завдання та показує хороші результати щодо якості зображень. Надалі планується вдосконалити алгоритм для досягнення ще більш непомітного вбудовування.

В результаті програмної реалізації вдалося досягти вбудовування в половину від обсягу RAW зображення. Також необхідно зауважити, що обсяг RAW зображень набагато перевищує JPEG і PNG, що дозволяє приховати більше інформації. При порівнянні використано спосіб приховування LSB у зображеннях стандартних rgb форматах. Результати показників ефективності вбудовування в RAW зображення знаходяться в межах допустимих значень і становлять в середньому: SSIM дорівнює 0,9999 і IF дорівнює 0,9929. Було виявлено, що статистичні показники зміни зображення виявляють відхилення схоже з

відхиленнями у форматах JPEG і PNG.

Також необхідно зазначити, що при прихованні у форматах JPEG та PNG змінюється обсяг зображення із вбудованими даними. Однак при прихованні розробленим алгоритмом RAW зображенні обсяг зображення з вбудованими даними не змінюється.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hashim M., Mohd Rahim M. S., Alwan A. A.. A review and open issues of multifarious image steganography techniques in spatial domain. Journal of Theoretical & Applied Information Technology. 2018. Vol. 96, no. 4 P. 956–977.

2. How to get Raw data from CR2 format. URL: https://www.swetake.com/photo/cr2/cr2-1_en.html (date of access: 21.11.2025).

3. Wu X., Memon N.. CALIC-a context based adaptive lossless image codec. 1996 IEEE international conference on acoustics, speech, and signal processing conference proceedings. 1996. Vol. 4. P. 1890–1893.

4. Dunbar B.. A detailed look at Steganographic Techniques and their use in an Open-Systems Environment. Sans Institute. 2002. Vol. 1. P. 12–20.

5. Kumar A., Pooja K.. Steganography-A data hiding technique. International Journal of Computer Applications. 2010. Vol. 9, no. 7. P. 19–23.

6. Hashim M.. An extensive analysis and conduct comparative based on statistical attach of LSB substitution and LSB matching. International Journal of Engineering & Technology. 2018. Vol. 7, no. 4. P. 4008–4023.

7. Пузиренко О. Ю., Прогонов Д. О., Конахович Г. Ф.. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних. Київ: Центр учбової літератури, 2018. 558 с.

8. Хорошко В. О., Яремчук Ю. Є., Карпінець В. В.. Комп’ютерна стеганографія. Навчальний посібник. Вінниця: ВНТУ, 2017. 155 с.

9. Pan F., Li J., Yang X.. Image steganography method based on PVD and modulus function. 2011 International Conference on Electronics, Communications and Control (ICECC). 2011. P. 282–284.

10. Bashardoost M., A Novel Approach to Enhance the Security of the LSB Image Steganograph. Research Journal of Applied Sciences, Engineering and Technology. 2014. Vol. 7, no. 19. P. 3957–3963.

11. Subhedar M. S., Mankar V. H.. Current status and key issues in image steganography: A survey. Computer science review. 2014. Vol. 13. P. 95–113.

12. Din R.. Evaluating the feature-based technique of text steganography based on capacity and time processing parameters. Advanced Science Letters. 2018. Vol. 24, no. 10. P. 7355–7359.

13. Bobad R., Goudar S. Secure data communication using protocol steganography in IPv6. 2015 International Conference on Computing Communication Control and Automation. 2015. P. 275–279.

14. Han C. A new audio steganalysis method based on linear prediction. Multimedia Tools and Applications. 2018. Vol. 77. P. 15431–15455.

15. Provos N., Honeyman P.. Hide and seek: An introduction to steganography. IEEE security & privacy. 2003. Vol. 1, no. 3. P. 32–44.

16. Khalind O. S.. New methods to improve the pixel domain steganography, steganalysis, and simplify the assessment of steganalysis tools. Diss. University of Portsmouth, 2015. 171 p.

17. Imaizumi S., Ozawa K.. Multibit embedding algorithm for steganography of palettebased images. Springer Berlin Heidelberg. 2014. P. 99–110.

18. Abraham A. Significance of steganography on data security. International Conference on Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. 2004. Vol. 2. P. 347–351.

19. Gao W., Huo Y., Qiao Y.. A security steganography scheme based on hdr image. Proceedings of the 2019 International Conference on Video, Signal and Image Processing. 2019. P. 44–48.

20. Rawat D., Bhandari V.. A steganography technique for hiding image in an image using lsb method for 24 bit color image. International Journal of Computer Applications. 2013. Vol. 64, no. 20. P. 15–19.

21. Rajalakshmi K., Mahesh K.. Robust secure video steganography using reversible patch-wise code-based embedding. Multimedia Tools and Applications. 2018. Vol. 77. P. 27427–27445.

22. Alvarez P.. Using extended file information (EXIF) file headers in digital evidence analysis. International Journal of Digital Evidence. 2004. Vol. 2, no.3. P.1–5.

23. Chandramouli R., Memon N.. Analysis of LSB based image steganography techniques. Proceedings 2001 international conference on image processing. 2001. Vol. 3. P. 1019–1022.

24. Qian Z.. Robust steganography using texture synthesis. Advances in Intelligent Information Hiding and Multimedia Signal Processing. 2017. P. 25–33.

25. Mahdi M. H. Improvement of image steganography scheme based on LSB value with two control random parameters and multi-level encryption. IOP Conference Series: Materials Science and Engineering. 2019. Vol. 518, no. 5. P. 552–554.

26. Chang C. C., Huang Y. H., Lu T. C.. A difference expansion based reversible information hiding scheme with high stego image visual quality. Multimedia Tools and Applications. 2017. Vol. 76. P. 12659–12681.

27. Nasrullah M. A. LSB based audio steganography preserving minimum sample SNR. International Journal of Electronic Security and Digital Forensics. 2018. Vol. 10, no. 3. P. 311–321.

28. Gupta Banik B., Bandyopadhyay S. K.. Image Steganography using BitPlane complexity segmentation and hessenberg QR method. Proceedings of the First International Conference on Intelligent Computing and Communication. 2017. P. 623–633.

29. Collins J., Agaian S. High Capacity Image Steganography Using Adjunctive Numerical Representations With Multiple Bit-Plane Decomposition Methods. International Journal on Cryptography and Information Security. 2016. Vol. 6, no. 1/2. P. 01–21.

30. Islam S., Gupta P.. Robust edge based image steganography through pixel intensity adjustment. 2014 IEEE Intl Conf on High Performance Computing and Communications, 2014 IEEE 6th Intl Symp on Cyberspace Safety and Security, 2014 IEEE 11th Intl Conf on Embedded Software and Syst. 2014. P. 771–777.

31. PIXLS.US Free/Open Source Photography. URL: https://raw.pixls.us (date of access: 21.11.2025).

32. Skorenkyy Y., Kozak R., Zagorodna N., Kramar O., Baran, I. Use of augmented reality-enabled prototyping of cyber-physical systems for improving cybersecurity education. Journal of Physics: Conference Series. 2021. Vol. 1840, no.1.

33. Tymoshchuk D., Yasniy O., Mytnyk M., Zagorodna N., Tymoshchuk V. Detection and classification of DDoS flooding attacks by machine learning method. CEUR Workshop Proceedings. 2024. Vol. 3842. P. 184-195.

34. Lypa B., Horyn I., Zagorodna N., Tymoshchuk D., Lechachenko T. Comparison of feature extraction tools for network traffic data. CEUR Workshop Proceedings. 2024. vol. 3896. P. 1-11.

35. Микитишин А. Г., Митник М. М., Стухляк П. Д. Телекомунікаційні системи та мережі. Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017. 384 с.

36. Palamar A., Karpinski M., Palamar M., Osukhivska H., Mytnyk M. Remote Air Pollution Monitoring System Based on Internet of Things. CEUR Workshop Proceedings, 2nd International Workshop on Information Technologies: Theoretical and Applied Problems (ITTAP 2022), Ternopil, Ukraine, November 22–24, 2022. Vol. 3309. P. 194-204.

37. O. Sedinkin, M. Derkach, I. Skarga-Bandurova, and D. Matiuk, “Eye tracking system based on machine learning”, cit, no. 55, pp. 199-205, Jun. 2024.

38. Derkach, M., Matiuk, D., Skarga-Bandurova, I., Biloborodova, T., & Zagorodna, N. (2024, October). A Robust Brain-Computer Interface for Reliable Cognitive State Classification and Device Control. In 2024 14th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 1-9). IEEE.

39. Деркач, М. В., Остополець, В. Ю., & Дерев’янченко, В. С. (2023). Розробка мобільного додатку для визначення автентичності медіа файлу. *Вісник Східноукраїнського національного університету імені Володимира Даля*, (3 (279)), 5-10.

40. Заікіна Д., Глива В. Основи охорони праці та безпека життєдіяльності. RS Global Sp. z O.O., Warsaw. 2019. 44 с.

41. Безпека в надзвичайних ситуаціях. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання / укл.: Стручок В. С. Тернопіль: ФОП Паляниця В. А., 2022. 156 с.

Додаток А Публікація

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя
Маріборский університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Краківський економічний університет (Польща)
Вроцлавський економічний університет (Польща)
Університет «Опольська Політехніка» (Польща)
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Вінницький національний аграрний університет
Львівський національний університет ім. І. Франка
Головне управління Пенсійного фонду в Тернопільській області
Наукове товариство ім. Шевченка
Тернопільський обласний комунальний інститут післядипломної педагогічної освіти
Сумський державний педагогічний університет
Запорізький національний університет

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

XIV Міжнародної науково-технічної конференції молодих учених та студентів

11-12 грудня 2025 року

УКРАЇНА
ТЕРНОПІЛЬ – 2025

УДК 004.056
А.М.Фаберський, студент гр. СБм-61
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

СТЕГАНОГРАФІЯ ЗОБРАЖЕНЬ

A. M. Faberskyi, student gr. SBm-61

IMAGE STEGANOGRAPHY

За останні кілька десятиліть було створено та вдосконалено безліч секретних методів зв'язку, при цьому стеганографія зображення становить одну з основних областей прихованого зв'язку [1]. Це пов'язано з тим, що в Інтернеті є мільйони готових і доступних зображень, в які будь-яка людина, яка бажає спілкуватися таємним чином, може вставляти свої власні повідомлення. Крім того, формат має високу надмірність, а незначні зміни цифрових зображень не виявляються зоровим аналізатором людини (ЗАЛ). Більше того їх легко використовувати як прикриття для вбудовування даних без збурення. Цифрові зображення широко використовуються як прикриття для стеганографії. Більшість стеганографічних систем досліджують і використовують знання про недоліки людського зору у методах вбудовування. Таким чином, зашумлені області та краї зображень цікавлять стеганографів, оскільки ЗАЛ менш чутливий до зашумлених областей та областей по краях.

Незважаючи на певний прогрес, досягнутий у стеганографії зображень з погляду бінарних зображень та тривимірних зображень, дослідники зосередили свої дослідження на прихованні даних у відтінках сірого та кольорових зображень [1]. Незважаючи на те, що компонент яскравості кольорового зображення ідентичний компоненту яскравості зображення в градаціях сірого, деякі експерти вважають зображення в градаціях сірого оптимальним покриттям для стеганографії. Це пов'язано з тим, що процес вбудовування змінить кореляцію між елементами кольору, і ці зміни можуть викликати сліди артефактів, які спростять виявлення вбудовування.

Як правило, існує два основних типи стеганографії зображень: просторова область та область перетворення. На рисунку1 показано два типи методів.

Рисунок 1 - Види стеганосіїв