НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«ДОСЛІДЖЕННЯ СТІЙКОСТІ ДО АТАК СТИСНЕННЯ СТЕГАНОГРАФІЧНИХ ЗАСТОСУНКІВ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ»

Виконав: здобувач 5 курсу
Рівень бакалавр
Галузь знань 12 «Інформаційні технології»,
спеціальність 125 «Кібербезпека»
Пискун Микола Андрійович

Керівник: к.т.н., доцент
Ахмаметьєва Ганна Валеріївна

Рецензент: к.т.н., доцент
Кухаренко Сергій Вікторович

Одеса – 2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Факультет **кібербезпеки та інформаційних технологій**
Кафедра **кібербезпеки**
Галузь знань: **12 Інформаційні технології**
Спеціальність: **125 Кібербезпека**
Назва освітньої програми: **Кібербезпека**

ЗАТВЕРДЖУЮ
Завідувач кафедри кібербезпеки
професор С.А. Горбаченко
_____ «____ »_____ 20__ року

З А В Д А Н Н Я
на кваліфікаційну (бакалаврську) роботу
здобувачу Пискуну Миколі Андрійовичу

1. Тема роботи: «Дослідження стійкості до атак стиснення стеганографічних застосунків для цифрових зображень»
Керівник роботи: к.т.н, доцент Ганна Валеріївна Ахмаметьєва
затверджені наказом НУ ОЮА від «__» _____ 20___ року № _____
2. Строк подання здобувачем роботи «__» _____ 20___ рік
3. Дата видачі завдання«__» _____ 20___ рік

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської роботи	Строк виконання етапів роботи	Примітка

Здобувач _____
(підпис) (прізвище та ініціали)

Керівник роботи _____
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Кваліфікаційна робота на тему “Дослідження стійкості до атак стиснення стеганографічних застосунків для цифрових зображень” на здобуття першого (бакалаврського) рівня вищої освіти за спеціальністю 125 Кібербезпека, освітньою програмою: Кібербезпека, містить 16 рисунків, 1 таблицю, 37 літературних джерел за переліком посилань. Робота виконана на 34 сторінках основного тексту.

Метою роботи є дослідження стійкості програмних реалізації методів стеганографії, які в якості контейнера використовують цифрові зображення, до атак стиснення.

В роботі проаналізовано функціональність стеганографічних застосунків та досліджено стійкість стеганоконтейнерів, сформованих за допомогою реалізованих в програмах алгоритмів, до атаки стиснення. Встановлено, що більшість з запропонованих програм здійснюють вбудовування інформації в просторову область, що в більшості випадків призводить до руйнування вбудованих даних після стиснення.

СТЕГАНОГРАФІЯ, ЦИФРОВІ ЗОБРАЖЕННЯ, АТАКА СТИСНЕННЯМ, ОБЛАСТЬ ПЕРЕТВОРЕНЬ, ПРОСТОРОВА ОБЛАСТЬ

ABSTRACT

Qualification work on the topic “Investigating the resistance to compression attacks of steganographic applications for digital images” for obtaining the first (bachelor's) level of higher education in the specialty 125 Cybersecurity, specialization, educational program: Cybersecurity, contains 16 figures in the main text, 1 table, 37 literature sources on the list of references. The work is performed on 34 pages of general text.

The purpose of the work is to study the resistance of software implementations of steganography methods, which use digital images as a container, to compression attacks.

The work analyzes the functionality of steganographic applications and investigates the resistance of stego-containers formed with the help of algorithms implemented in programs to a compression attack. It was established that most of the proposed programs embed information into the spatial domain, which in most cases leads to the destruction of the embedded data after compression.

STEGANOGRAPHY, DIGITAL IMAGES, COMPRESSION ATTACK, TRANSFORM DOMAIN, SPATIAL DOMAIN

ЗМІСТ

ВСТУП

За останні роки широкого поширення набули технології, що передбачають моніторинг та контроль відкритих каналів зв’язку з метою збирання персональних даних особи, аналізу її області інтересів, кругу спілкування, місцезнаходження, що з одного боку порушує Конституційні права людини, з іншого боку неналежне забезпечення захисту таких даних може спричинити їх виток до зловмисників, які можуть бути використані з метою шантажу, компрометації, крадіжки фінансових ресурсів, махінацій з нерухомістю, як засіб тиску на людину, тощо. Через це виникає потреба застосування засобів, які дозволяють передати конфіденційну інформацію таємно від служб моніторингу. Одним з рішень організації прихованого каналу зв’язку є використання методів стеганографії та їх програмних реалізації для персональних комп’ютерів.

Обмін мультимедійними даними (зображень, відео, аудіо та голосових повідомлень) в месенджерах, соціальних мережах не є чимось підозрюваним, однак передача великої кількості нестиснутих файлів за рахунок їх великого розміру все ж може викликати деякий інтерес, тому при використанні стеганографічних перетворень слід звертати увагу на стійкість до стиснення вбудованих в контейнер даних та можливість їх відновлення. Деякі реалізації стеганографічних перетворень здійснюють вбудовування секретної інформації в просторову область контейнера, що часто не забезпечує стійкості до стиснення. Це в свою чергу вимагає передавати файли в форматі без втрат, отже їх розмір може бути на порядок більшим, ніж у стиснутих файлах. Крім того просторовими маніпуляціями з медіа-файлами, наприклад, накладання шуму, зміна яскравості зображення, нормалізація звуку в аудіо, можна без зайвих проблем зруйнувати вбудовану секретну інформацію.

Метою роботи є дослідження стійкості програмних реалізації методів стеганографії, які в якості контейнера використовують цифрові зображення, до атак стиснення.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

1) навести огляд сучасних програмних реалізацій стеганографічних методів для цифрових зображень;

2) провести експериментальні дослідження стійкості результатів вбудовування до атак стисненням;

3) сформувати рекомендації щодо використання стеганографічних застосунків.

Об’єкт дослідження – процеси організації стеганографічного каналу зв’язку.

Предмет дослідження – стеганографічні методи і алгоритми для цифрових зображень.

Практичне значення отриманих результатів. Результати роботи можуть бути використані звичайними користувачами як керівництво до вибору застосування тих чи інших стеганографічних програм.

В першому розділі наведено основні поняття та визначення стеганографії, класифікації стеганографічних методів для цифрових зображень.

В другому розділі описані можливості програмних реалізацій методів стеганографії, їх переваги, недоліки з точки зору дослідників, застосовані формати і обмеження використання.

В третьому розділі наведені результати експериментальних досліджень стеганографічних програм до атак стиснення та рекомендації щодо їх використання.

1 ОСНОВНІ ВИЗНАЧЕННЯ СТЕГАНОГРАФІЇ ТА СТЕГАНОГРАФІЧНИХ ПЕРЕТВОРЕНЬ

1.1 Поняття і визначення стеганографії

Наука стеганографія розглядає розробку й дослідження методів організації прихованого зв'язку, коли в таємниці залишається сам факт наявності деякої вбудованої конфіденційної інформації в контейнері [1]. Класичними прикладами використання стеганографії в давні часи є симпатичні чорнила (наприклад, написи молоком або соком лимону або цибулі, пізніше спеціальні хімічні з’єднання), які можна проявити нагріванням, освітленням або за допомогою певних хімічних речовин, використання трафаретів, які задають порядок читання певних букв або слів в тексті, жаргонні шифри, де окремі слова мають власне секретне значення, мікрокрапки, в які вкладалися мікроскопічні фотознімки.

Сучасний розвиток і використання стеганографії відбувається завдяки розвитку комп’ютерної техніки, нових засобів і каналів передачі інформації, де вбудовування секретних даних побудовано на цифровому представленні файлів і структурі їх зберігання. Така стеганографія отримала назву комп’ютерної стеганографії, яка охоплює не лише організацію прихованого зв’язку, а й захист інтелектуальної власності шляхом вбудовування невидимих цифрових водяних знаків, підписи медичних знімків, тощо.

Сучасна комп’ютерна стеганографія в якості контейнерів найчастіше використовує мультимедійні дані, що обумовлено несприйнятністю органів почуттів людини до незначних змін в кольорах зображення, відео-кадрів або якості звуку в аудіо-файлах. Сама структура цифрових мультимедійних даних передбачає значний обсяг надлишкової інформації, яку можна змінювати без втрати їх функціональності та тим самим забезпечити можливість вбудовування значного обсягу конфіденційних даних [2].

Комп’ютерна стеганографія є складовою цифрової стеганографії – напрямом, який в якості об’єктів перетворення (як контейнери, так і додаткова інформація) використовує довільні цифрові об’єкти, будь то цифрові документи, поля

заголовків і метаданих файлів довільного формату, мультимедійні дані, модифікації в налаштуваннях мережевих протоколах передачі даних (наприклад, Wireless Local Area Networks (WLAN) – передача повідомлень в бездротових локальних мережах [3], Lost Audio Packets Steganography (LACK) – методи приховування повідомлень під час розмов з використанням IP-телефонії [4], Voice over IP (VoIP) – передбачає передачу мультимедійних даних в реальному часі з використанням протоколів TCP/IP [5], тощо.

Слід зазначити, що для оцифрованих об’єктів характерною є наявність шуму квантування, може з’явитися аналоговий шум, нелінійні спотворення апаратури, все це впливає на якість вихідних даних і за певних умов дозволяє забезпечити більшу непомітність прихованого повідомлення в контейнері.

При розв’язанні задачі організації прихованого каналу зв’язку використовується сукупність засобів і методів перетворення, які утворюють стеганографічну систему, або стеганосистему. Узагальнену структуру стеганографічної системи наведено на рис.1.1.

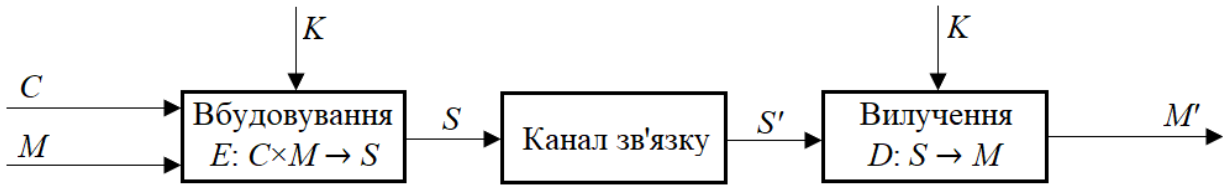

Рисунок 1.1 – Стеганографічна система

Основними компонентами стеганографічної системи є наступні [1].

Повідомлення (Message – *M*) – це будь-яка чутлива (конфіденційна, персональна, додаткова) інформація, яка підлягає захисту та прихованої передачі відкритими каналами зв’язку.

Для прихованої передачі повідомлення використовують контейнер (Container – *C*) – будь-яку інформацію, розмір якої має значно перевищувати розмір повідомлення для забезпечення повного занурення повідомлення в контейнер, а також збереження візуальної (слухової) цілісності самого контейнеру.

Розрізняють контейнери потокові, тобто неможливо визначити початок і кінець такого контейнеру, як правило, потокові контейнери використовуються при вбудовуванні і передачі повідомлення в режимі реального часу, та фіксовані – заздалегідь відомі розмір та характеристики файлу, що дозволяє підібрати найбільш придатний для забезпечення непомітності прихованої інформації.

Вибір типу контейнера залежить від обраного способу передачі повідомлень. Найбільше наукових досліджень присвячені використанню саме фіксованих контейнерів, зокрема зображень.

Стеганографічне перетворення $E: C \times K \rightarrow S$ (вбудовування додаткової інформації) передбачає занурення повідомлення M в контейнер C з використанням ключа K за допомогою обраного стеганографічного методу (алгоритму). Вид і структура ключа K залежить від обраного алгоритму, іноді це послідовність часових (просторових) відліків, які визначають величину пропусків між елементами для вбудовування, іноді послідовність пікселів (часових відліків), які задають місце занурення, іноді це самі параметри стеганоалгоритму.

На виході стеганографічного перетворення $E: C \times K \rightarrow S$ отримуємо заповнений контейнер (стеганоконтейнер, Stego – S), який в подальшому передається відкритим каналом зв'язку та може зазнати деяких спотворень (S').

Перетворення $D: S' \rightarrow M'$ дозволяє вилучити можливо спотворену додаткову інформацію M' з стеганоконтейнеру S'.

1.2 Класифікація стеганографічних методів

Залежно від того, в яку область контейнера відбувається вбудовування інформації методи стеганографії поділяють на просторові і частотні (область перетворень).

Стеганографічні методи в просторовій області зображень здійснюють модифікацію значень яскравості елементів контейнера – пікселів. Найпоширенішими методами є наступні.

- Метод заміни найменшого значущого біту LSB (Least Significant Bit), та

його модифікації. Існують варіанти LSB Replacment, LSB Matching, XOR LSB та деякі інші [6-9], які відрізняються принципом зміни значень яскравості. Окрім того внесення нестандартних відстаней між пікселями або псевдовипадковий вибір пікселів також визначає методи псевдовипадкової перестановки та метод псевдовипадкового інтервалу.

- Метод різниці значень пікселів PVD (Pixel Value Difference). Існує чимало підходів до вбудовування інформації [10-12], зокрема використання різних таблиць вибору регіонів квантування та кількості пікселів вбудовування, можливість приховувати інформацію в окремих матрицях зображення або використовувати колірне представлення пікселів зображення [13-14]. Також існує значна кількість різновидів блочного застосування методів PVD [15-16].

Всі різновиди просторових методів LSB та PVD є найбільш поширеними, оскільки забезпечують можливість вбудовування значного обсягу конфіденційних даних, особливо це стосується методів PVD, які дозволяють в пару пікселів заховати до 6-ти бітів інформації. Однак значні модифікації пікселів призводять до порушення цілісності стеганоконтейнеру, тому слід знайти оптимальне співвідношення між пропускною здатністю та якістю результуючого зображення. Окрім того такі методи є нестійкими до стиснення.

- Метод, заснований на обчисленні хеш-значень блоку [17]. Окремий різновид блокових методів стеганографії, який для блоків розміром 3×3 визначає хеш-значення, яке визначає модифікацію відповідного пікселя. Метод дозволяє вбудувати 1-2 біти інформації в блок колірної матриці, тобто забезпечує малу пропускну здатність, однак за рахунок цього візуальна якість стеганоконтейнера має надвисокі показники (значення PSNR на рівні 60-67 дБ). Метод показав добру стійкість до зашумлення, дослідження стійкості до стиснення не проводились.
- Метод заміни палітри [18]. Зображення представляється як матриця індексів M та палітри кольорів C – вектору, індекс i якого задає індекс кольору у матриці індексів, а значення вектору $C[i]$ задає колір. Для

відновлення зображення порядок кольорів у палітрі *C* не важливий, тому приховати додаткову інформацію можна шляхом перестановки кольорів у палітрі.

- Метод, що застосовує кодове управління вбудовування інформації [19]. Метод здійснює приховування інформації в просторову область зображення та використовує кодове управління частотними складовими, які зазнають спотворення в результаті стеганографічного перетворення. Через вбудовування в просторову область даний підхід забезпечує високу швидкодію та стійкість до атак стиснення.

В більшості наукових досліджень стеганографічних методів працюють в наступних частотних областях цифрових зображень.

- Дискретне косинусне перетворення DCT (Discrete Cosine Transform) [20-22] – стеганоперетворення відбувається шляхом модифікації середньочастотних коефіцієнтів DCT блоків розміром 8×8, який обумовлений стандартом стиснення JPEG. В деяких методах відбувається додаткове квантування коефіцієнтів DCT блоків зображення.
- Дискретне вейвлет-перетворення DWT (Discrete Wavelet Transform) [23] – найчастіше вбудовування інформації здійснюється в низькочастотні (апроксимуючі) коефіцієнти *k*-го рівня DWT (як правило, застосовується не більше трьох рівнів розкладання). Деякі алгоритми маніпулюють високочастотним коефіцієнтами. Вейвлет-перетворення може бути застосоване як до зображення цілком, так і до окремих блоків.
- Дискретне перетворення Фур’є DFT (Discrete Fourie Transform) [24-25]. Найпростіші з точки зору обчислювальної складності методи використовують блоки зображення розміром 2×2 для обчислення коефіцієнтів DFT, якими певним чином маніпулюють для вбудовування біту (бітів) секретного повідомлення.
- Сингулярне розкладання матриць SVD (Singular Value Decomposition) набуло поширення останні роки, для вбудовування використовуються

сингулярні числа або сингулярні вектори блоків зображення.

- Комбіноване застосування вище перерахованих областей перетворень [26-27].

Стеганографічним методами, що працюють в області перетворень, в більшості випадків забезпечується стійкість стеганоконтейнерів до атак, зокрема до атаки стисненням, однак за рахунок високої обчислювальної складності і похибок округлення точність вилучення інформації дещо погіршується. В деяких ситуаціях таким похибками можна знехтувати, наприклад, коли в одиницю контейнера вбудовується не окремий біт, а значення яскравості, тоді похибка вилучення значно не впливає на результат.

В першому розділі визначено основні поняття стеганографії, її компоненти та розглянуто класифікацію стеганографічних методів за областю перетворення.

2 ОГЛЯД СТЕГАНОГРАФІЧНИХ ЗАСТОСУНКІВ ДЛЯ ЦИФРОВИХ ЗОБРАЖЕНЬ

2.1 Програмні застосунки стеганографічних перетворень в просторовій області цифрових зображень

В мережі Інтернет існує чимало програмних застосунків, які реалізують вбудовування додаткової інформації в просторову область цифрових зображень, що призводить формування стеганоконтейнеру в форматі без втрат і потребує його безпомилкової передачі і зберігання. Розглянемо декілька методів, які працюють з просторовою областю зображень.

Hallucinate [28]. Програма не потребує встановлення, має простий зрозумілий інтерфейс (рис.2.1). Працює з зображеннями-контейнерами довільного формату, однак стеганоконтейнер можна зберегти лише в форматі BMP та PNG (останній формат зображень має досить широке поширення, тому такий формат може не привернути особливої уваги систем моніторингу), в якості повідомлення підтримуються довільні формати.

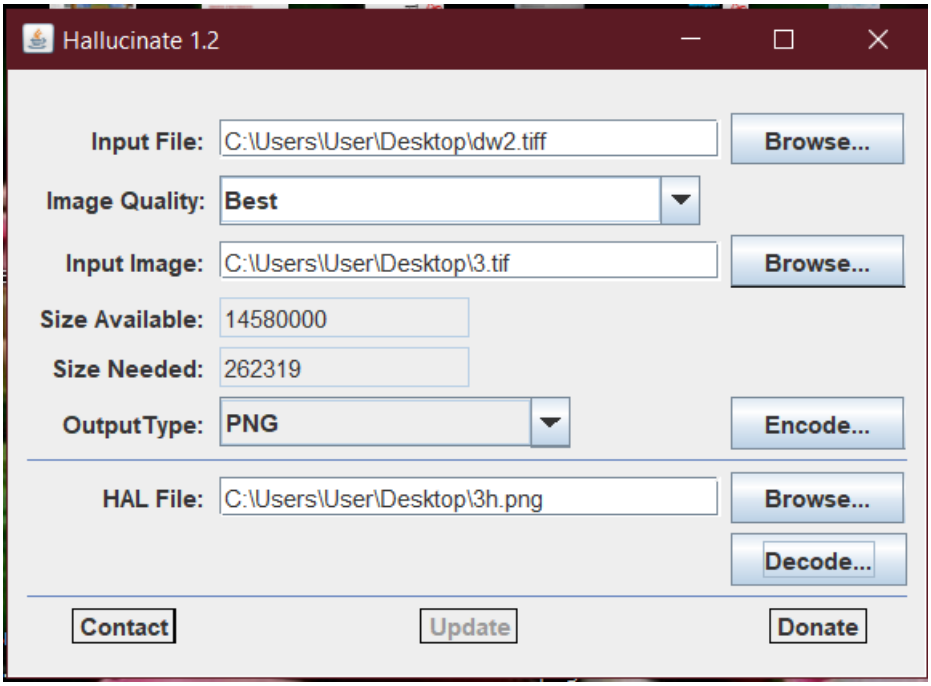

Рисунок 2.1 – Інтерфейс застосунку Hallucinate

Застосунок реалізує стеганографічний метод LSB та дає можливість обрати бажану якість підсумкового зображення, всього доступні вісім варіантів: Best, Better, Good, Fair, Poor, Bad, Worse, None. Чим нижче якість вихідного зображення, тим більше виникає візуальних артефактів, в той же час можна вбудувати більший обсяг конфіденційної інформації.

JHide [29]. Програмний застосунок (рис.2.2) підтримує контейнери в форматі BMP, PNG та TIFF. В якості секретної інформації можна обрати довільний файл, який перед вбудовуванням в зображення підлягає максимальному стисненню в ZIP-архів, тому при вилученні повідомлення результатом завжди буде архів, в якому зберігається секретний файл.

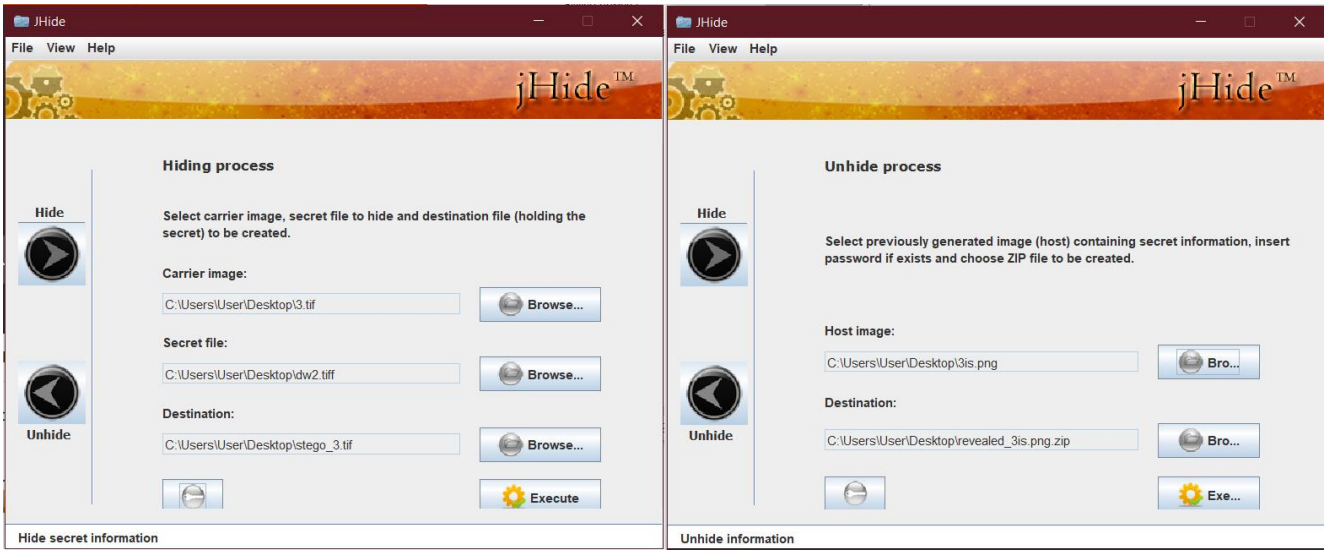

Рисунок 2.2 – Інтерфейс процедур вбудовування/вилучення повідомлення застосунком JHide

Додатковою можливістю програми є захист паролем.

OpenPuff [30]. Застосунок (рис.2.3) реалізує дві задачі стеганографії: вбудовування і вилучення секретного повідомлення в мультимедійні файли – зображення, аудіо і відео (рис.2.4), вбудовування і перевірку цифрового водяного знаку як захист авторських прав. Підтримуються формати контейнеру BMP, JPEG, PCX, PNG, TGA, в якості додаткової інформації виступає будь-який формат. В якості стеганоконтейнеру також можна обрати файли форматів BMP, JPEG, PCX,

PNG, TGA, однак за умови використання методу LSB формат JPEG є неспроможним зберегти секретне повідомлення. Додатковою перевагою програми можна відзначити можливість виділення необхідної кількості ядер процесора і кількість потоків у випадку, коли використовуються великі файли.

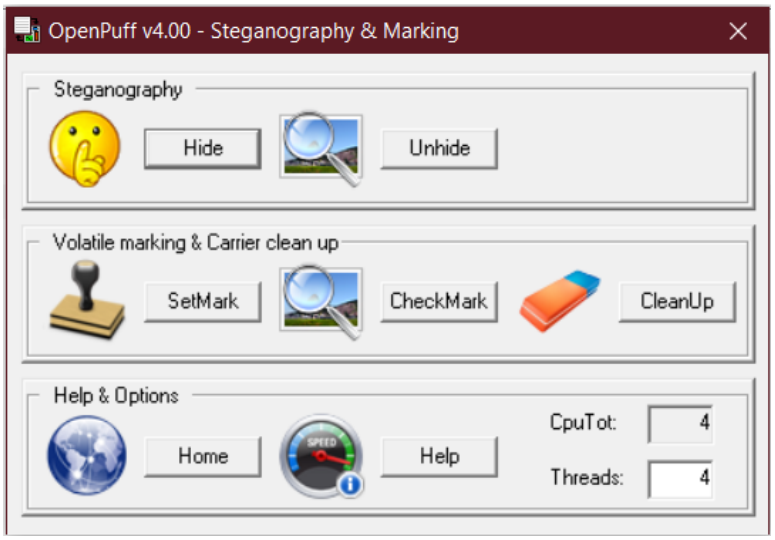

Рисунок 2.3 – Основний інтерфейс застосунку OpenPuff

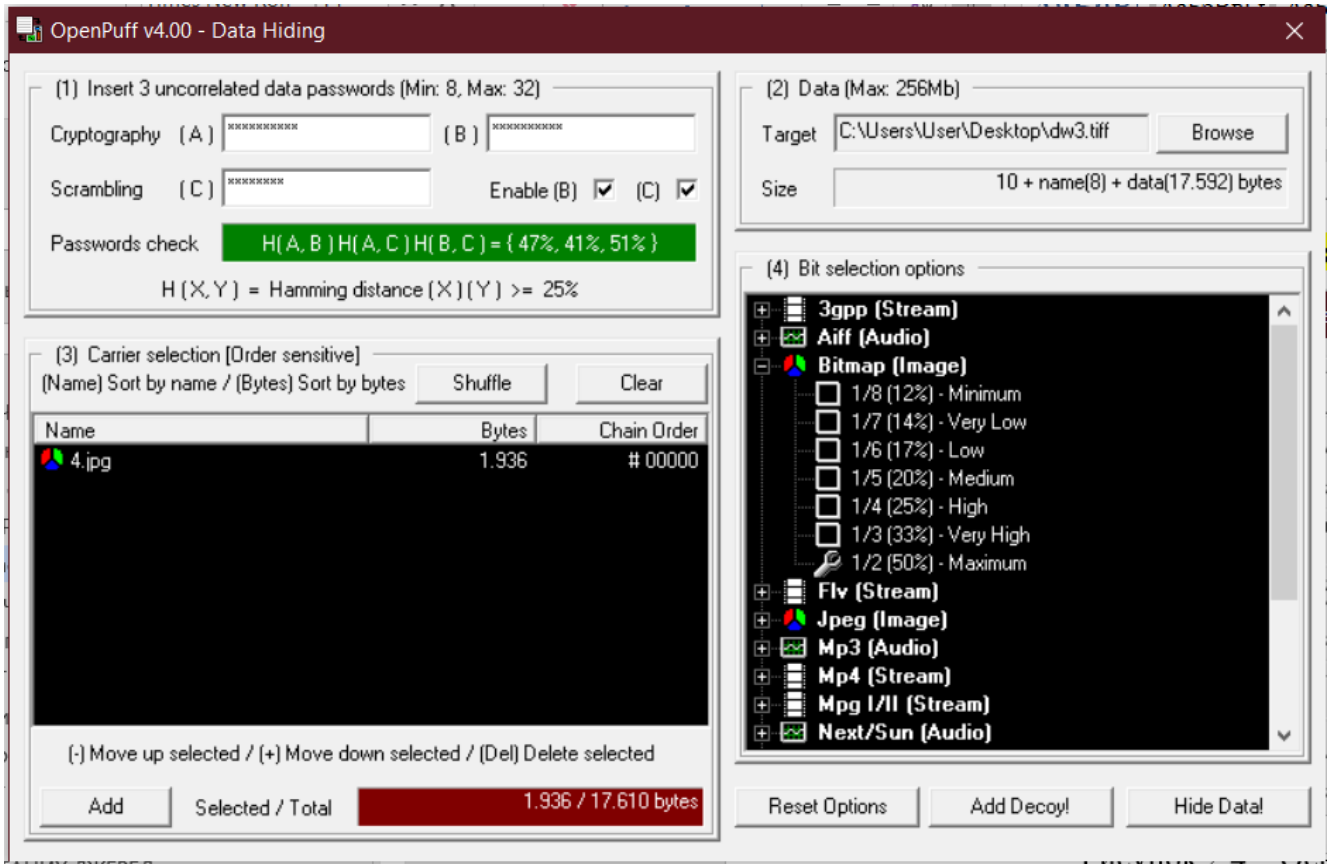

Рисунок 2.4 – Інтерфейс процедури вбудовування повідомлення застосунком OpenPuff

Застосунок реалізує складний парольний захист повідомлень при їх вбудовуванні і вилученні. В режимі звичайного паролю достатньо використовувати поле A (рис.2.4), при застосуванні полів B і C можна ввести три різні паролі довжиною від 8 до 32 символів, на їх основі буде згенерований унікальний ключ за допомогою криптографічно стійкого генератору псевдовипадкових чисел CSPRNG (Cryptographically secure pseudorandom number generator), який задаватиме стеганографічний шлях.

OpenStego [31]. Програма (рис.2.5) працює на операційних системах Windows і Linux та підтримує контейнери в форматі BMP, PNG, JPG, GIF і WBMP, однак заповнений контейнер завжди зберігається ф форматі PNG. В якості повідомлення можна взяти будь-які файли. Застосунок підтримує парольний захист, вбудовування/вилучення прихованих повідомлень і вбудовування/перевірку цифрових водяних знаків.

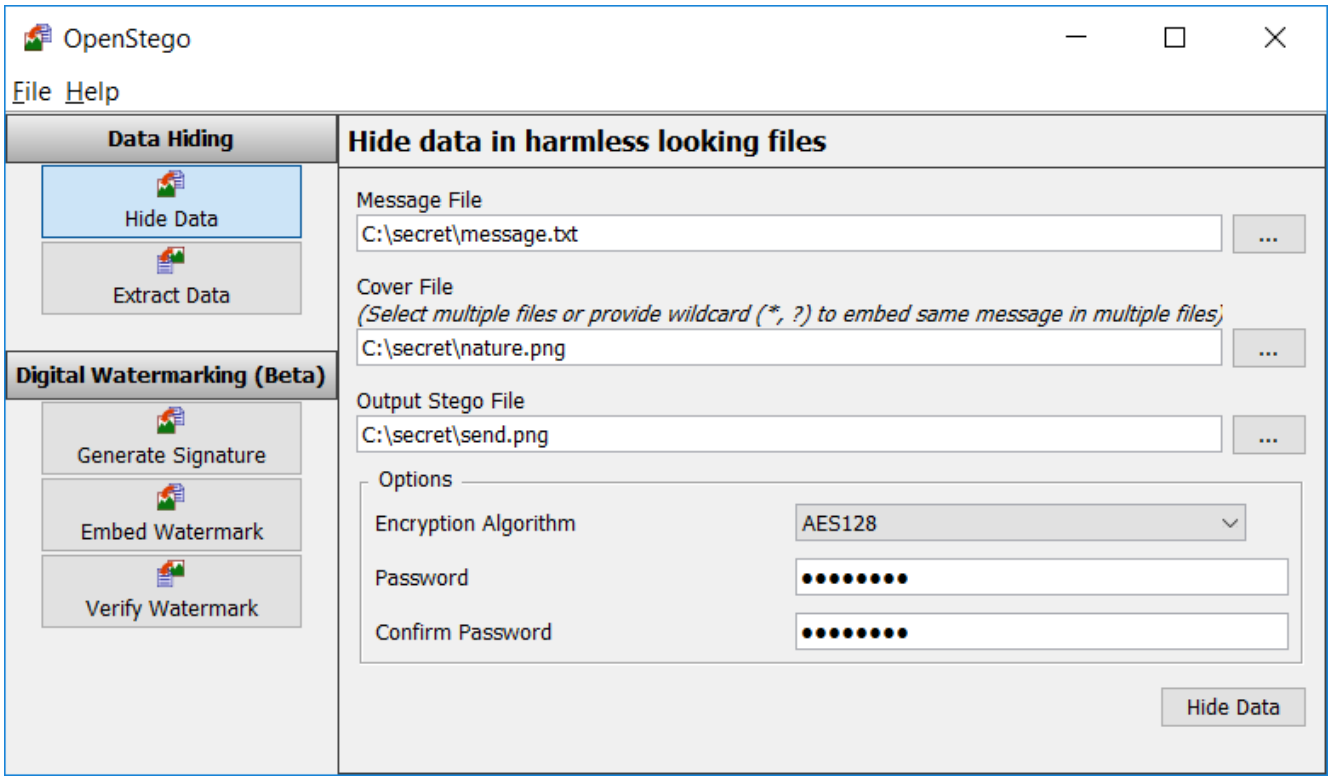

Рисунок 2.5 – Інтерфейс процедури вбудовування повідомлення застосунком OpenStego

Слід зазначити, що парольний захист працює не зовсім коректно. Якщо невірно ввести пароль при вилученні повідомлення, то вилучене повідомлення не буде збережено в файл, хоч програма і виведе повідомлення про успішність виконання операції. Файл буде згенеровано лише у разі співпадіння паролів при вбудовуванні і вилученні повідомлень.

Вбудовування цифрових водяних знаків програмою OpenStego здійснюється непрямим способом, тобто на основі зображення-водяного знаку генерується унікальна бітова послідовність (рис.2.6), яка зберігається в форматі SIG, і вже ця інформації розподіляється стеганографічним алгоритмом по контейнеру.

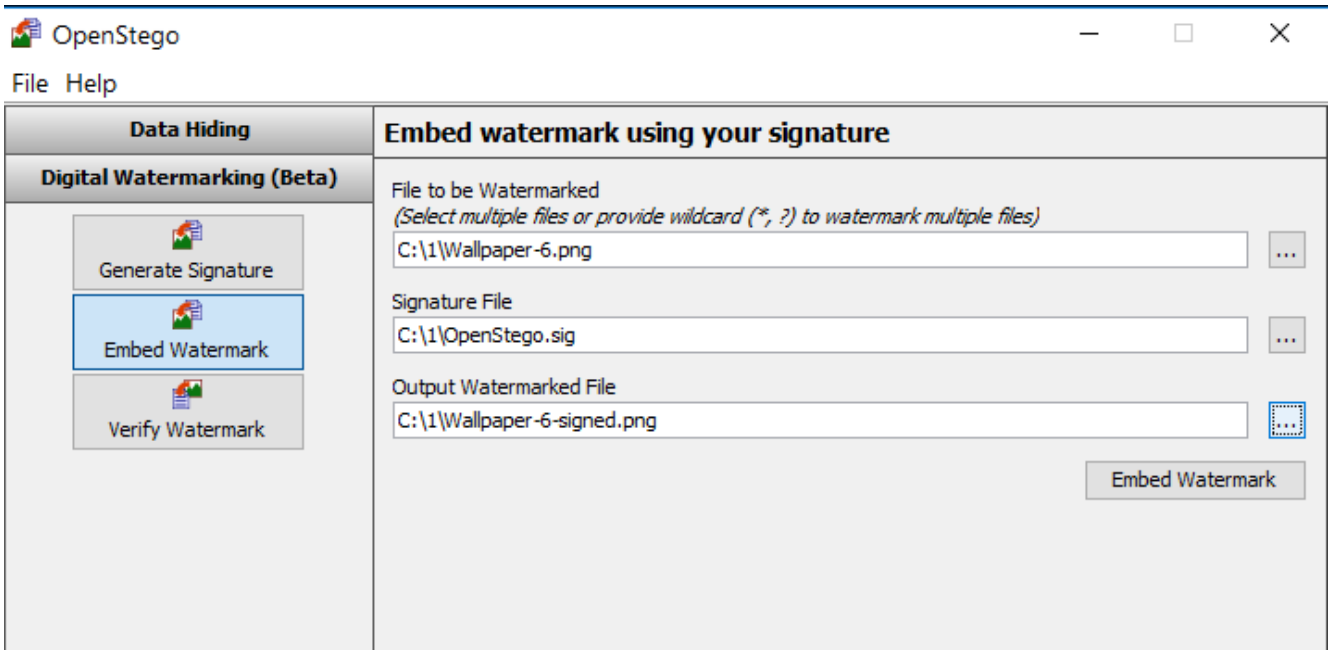

Рисунок 2.6 – Інтерфейс процедури вбудовування цифрового водяного знаку застосунком OpenStego

ImageSpyer G2 [32]. Програмний застосунок (рис.2.7) використовує вбудовування файлів в зображення форматів BMP, JPEG, WMF, EMF, TIFF, на виході отримуємо стеганоконтейнер в форматі BMP і TIFF. Максимальний обсяг прихованих даних дорівнює кількості пікселів контейнера. Додатково можна ввести пароль для шифрування секретного повідомлення (всього підтримується 30 алгоритмів шифрування), а також перевірити цілісність вбудованої інформації

(доступно 25 хеш-функцій). Також можливе попереднє стиснення конфіденційних даних.

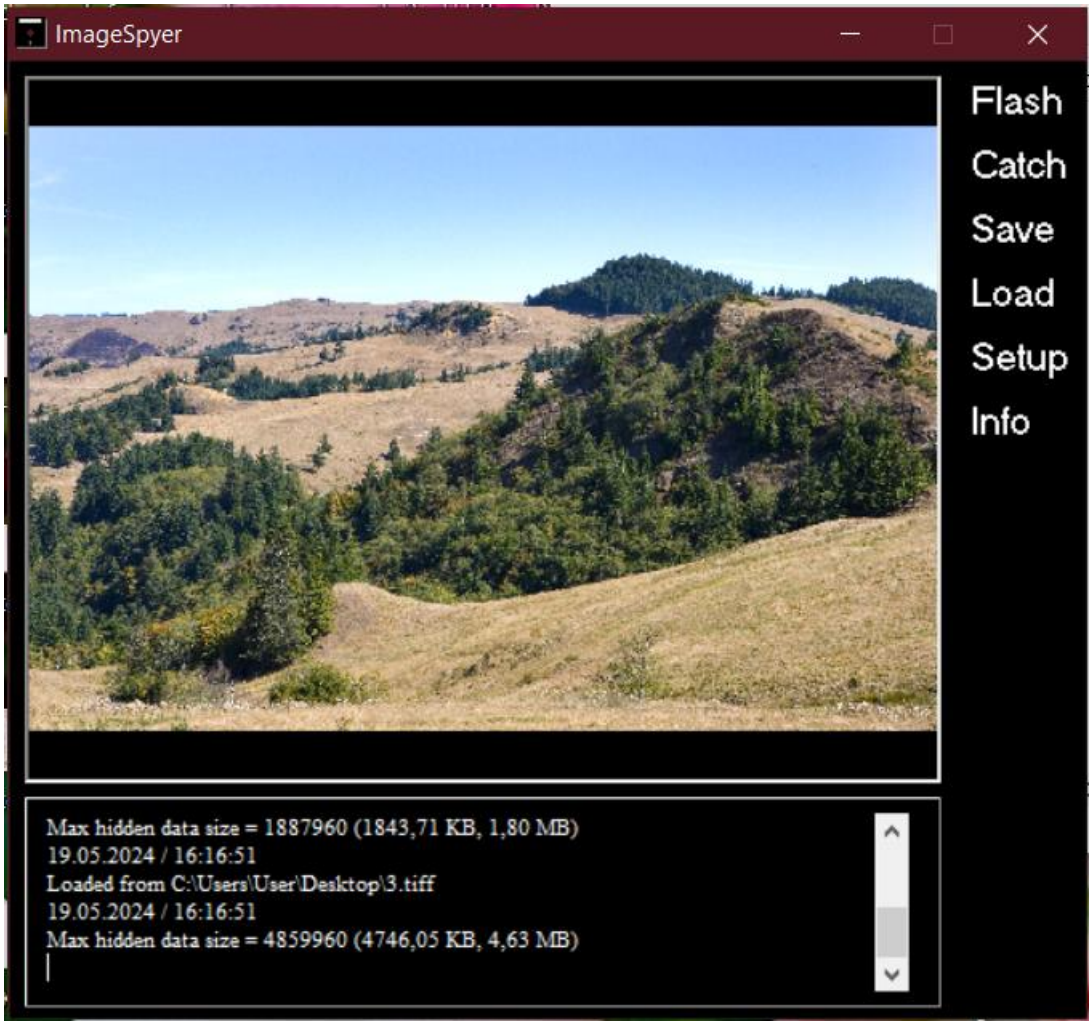

Рисунок 2.7 – Інтерфейс застосунку ImageSpyer G2

Слід зазначити, що у програми зовсім незручний і незрозумілий інтерфейс користувача.

Image Steganography [33]. Програма (рис.2.8) дозволяє вбудувати інформацію в зображення довільного формату, однак на виході можливе збереження лише в форматі PNG. Програма дозволяє шифрувати файли, при цьому необхідно ввести пароль (алгоритм шифрування не зазначений).

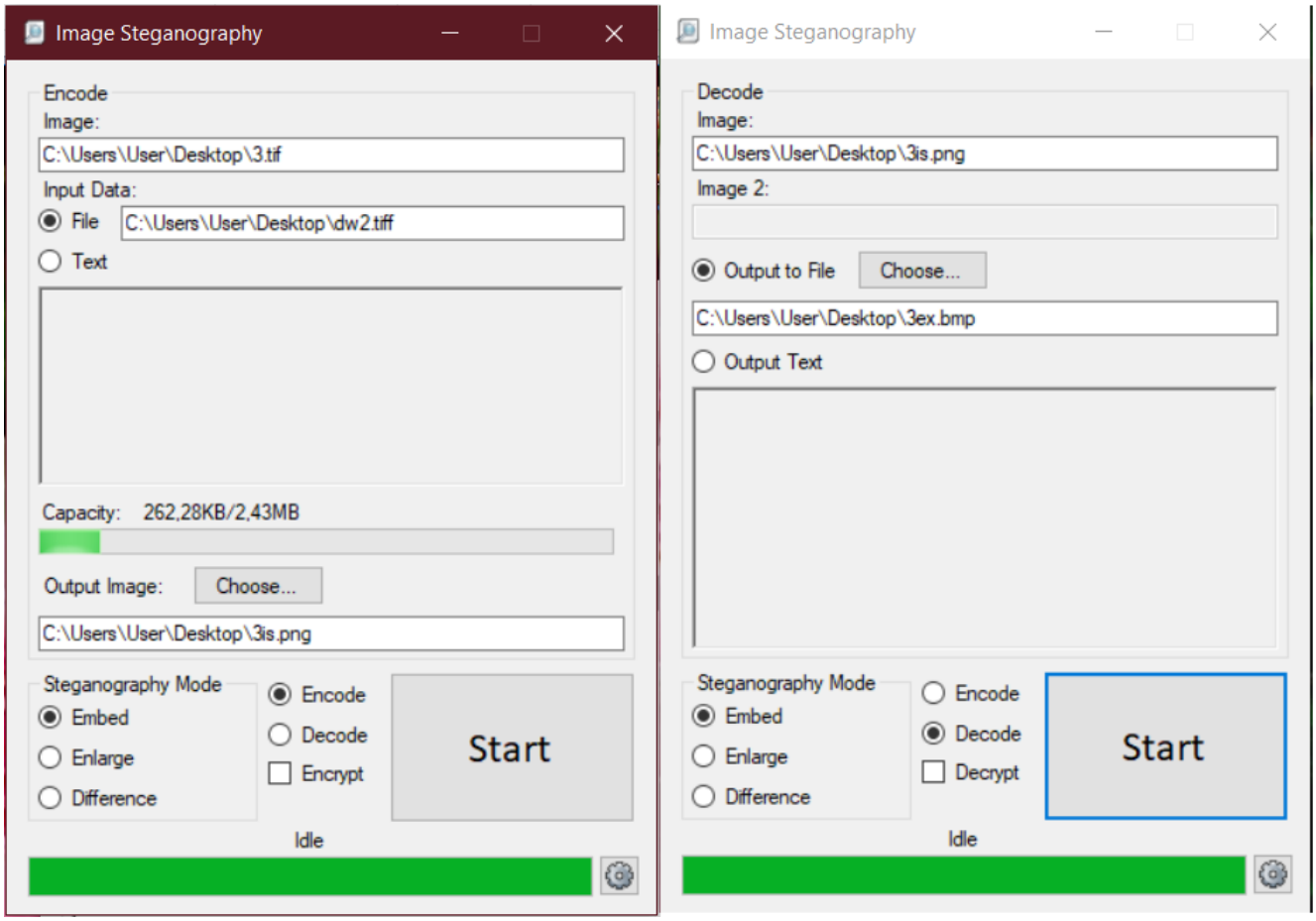

Рисунок 2.8 – Інтерфейс застосунку Image Steganography: Embed-Encode – приховування секретної інформації; Embed-Decode – вилучення секретної інформації

2.2 Стеганографічні програмні застосунки в області перетворень цифрових зображень

RedJPEG [32]. Програма має простий інтерфейс (рис.2.9) та призначена для приховування інформації в файли формату JPEG. Також є можливість використання перевірки цілісності даних, використовуючи алгоритми AMPRNG і Cartman II DDP4 в режимі хеш-функції, і стиснення даних з використанням LZMA-компресії. Обов’язковою умовою стеганографічного перетворення є введення паролю.

Рисунок 2.9 – Інтерфейс застосунку RedJPEG

В програмі є рядок стану, в якому одразу після завантаження файлу відображені назва файлу, наявність або відсутність даних та ємність файлу. При вбудовуванні файлу (можна обрати будь-який формат) в цьому ж рядку відображається розмір даних для приховування та співвідношення розмірів у відсотках, що дозволяє одразу побачити, чи вміститься файл у контейнер. Для збереження стеганоконтейнеру необхідно натиснути “Save JPEG”. Однак жодних налаштувань якості стеганоповідомлення при збереженні програмою не передбачено.

SilentEye [34]. Стеганографічний застосунок (рис.2.10) дозволяє приховувати повідомлення в аудіо та зображення. Форматами стеганоконтейнерів можуть виступати BMP, JPEG, PNG, GIF, TIFF, для запису аудіо – WAV. Є можливість застосування шифрування даних криптоалгоритмом AES.

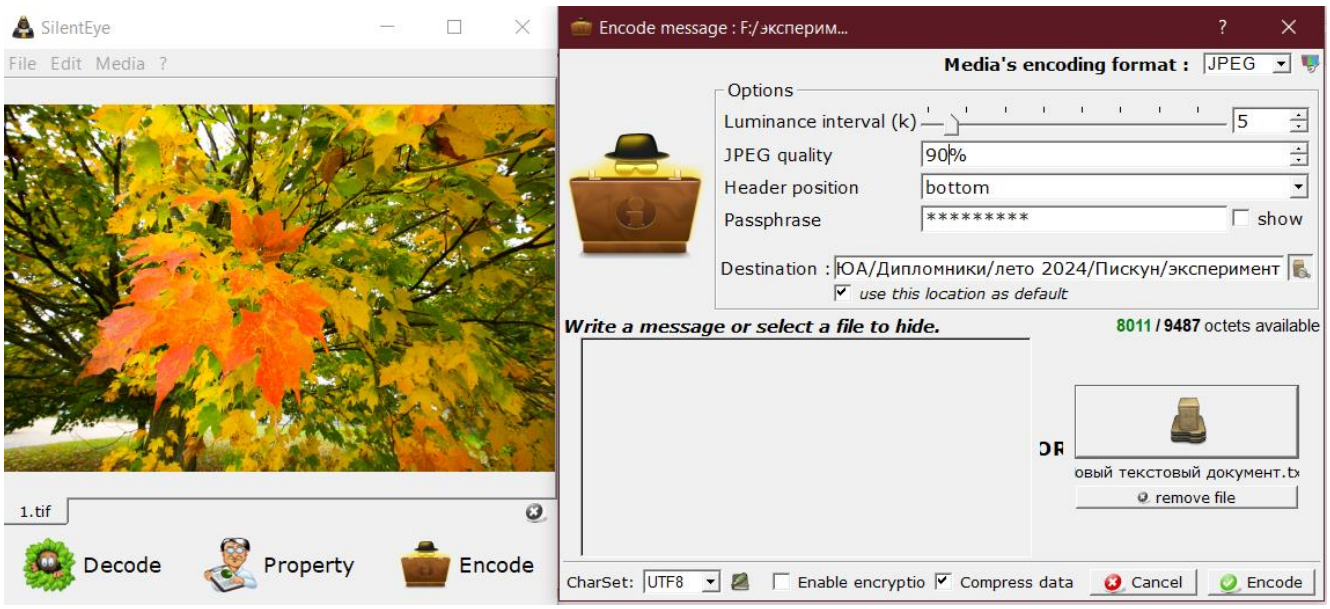

Рисунок 2.10 – Інтерфейс застосунку SilentEye

При вбудовуванні інформації у вікні “Encode” можна обрати формат для збереження стеганоконтейнера (BMP або JPEG), та для формату JPEG задати якість результуючого зображення. В якості секретної інформації можна або ввести текстову інформацію в поле зліва, або обрати файл довільного формату. Також у вікні наявна інформація, скільки октетів доступно для вбудовування, і скільки займає секретний файл, отож можна ще перед приховуванням файлу побачити, чи вміститься повідомлення в контейнер.

Hide ‘N’ Send [35]. Компактний і простий у використанні інструмент (рис.2.11) для вбудовування секретних повідомлень в файлах зображень. Застосунок підтримує кілька алгоритмів приховування (M-F5, M-LSB, F5, LSB), хешування (SHA512, RIPEMD, MD5) і шифрування (AES, RC2, RC4), які зручно вибрати всі з списку, що випадає. Слід зазначити, що можливе лише використання зображень в форматі JPG, під час процесу приховування також можна ввести пароль.

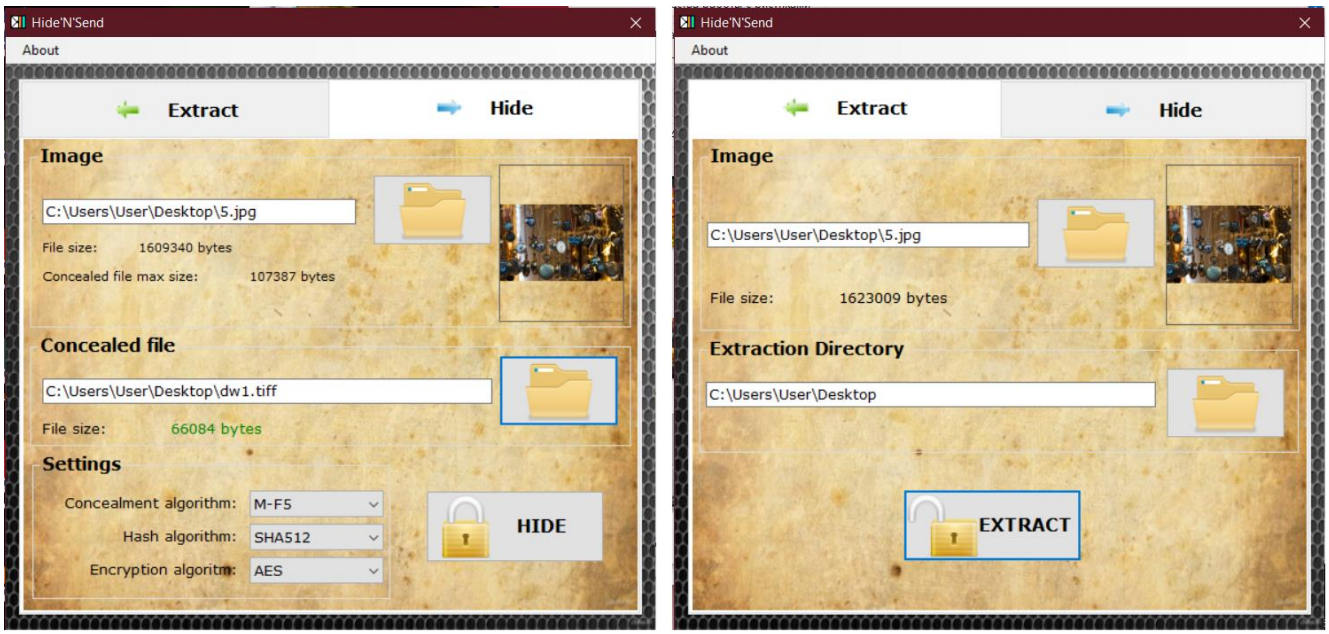

Рисунок 2.11 – Інтерфейс застосунку Hide ‘N’ Send: Hide – приховування секретної інформації; Extract – вилучення секретної інформації

Слід зазначити, що програма Hide ‘N’ Send не дає можливості задати якість результату вбудовування, крім того, під час вбудовування контейнер переписується стеганоконтейнером.

З перевірених комбінацій налаштувань деякі працюють некоректно, зокрема якщо при вбудовуванні були задані параметри “F5” – “RIPEMD” – “RC4”, то незважаючи на успіх приховування даних, вилучити секретне повідомлення не вдалося.

Steghide UI [36]. Програма (рис.2.12), яка дозволяє приховувати конфіденційні дані в зображеннях (BMP, JPG) і аудіо (WAV, AU). Серед параметрів можна задати алгоритм шифрування (Blowfish, Cast-128, Cast-256, DES, Enigma, AES 256/128/192, Saferplus, Serpent, TripleDES, Twofish та інші), режим шифрування, ввести пароль та задати рівень стиснення (0 – без стиснення, 1 – мінімальне стиснення, 9 – максимальне стиснення). Програма дозволяє писати аргументи командного рядка безпосередньо на основній панелі програми, а також коректно працює з будь-якою комбінацією вхідних параметрів.

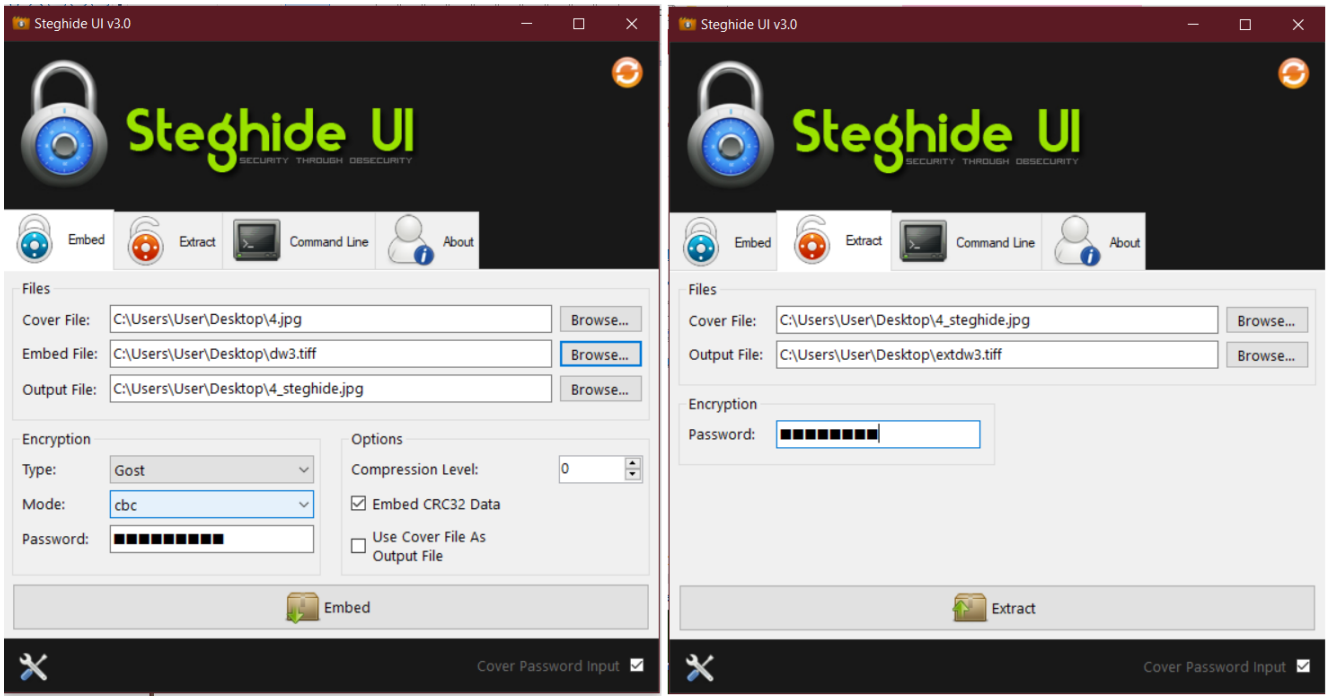

Рисунок 2.12 – Інтерфейс застосунку Steghide UI: Embed – приховування секретної інформації; Extract – вилучення секретної інформації

2.3 Реалізації стеганографічних методів мовами програмування

На сайті [37] наведені різноманітні алгоритмічні реалізації стеганографічних методів, які здійснюють вбудовування як в просторової області (S-UNIWARD, WOW, HUGO, MG, Pentary MVG, MiPOD, Synch), так і в області перетворень (nsF5, J-UNIWARD). Деякі з них реалізовані мовою C++, більшість написані мовою MatLAB – інтегрованого середовища розробки для розв'язання складних технічних, математичних і наукових задач. Система містить потужний набір математичних обчислень та вирішує величезну кількість прикладних задач, зокрема в області робототехніки, обробки звуку, зображень і відео, математичної статистики та інших.

Незважаючи на свою функціональність та широке охоплення поставлених задач, використання системи обмежується її ліцензійним використанням, адже система є платною, та необхідністю потужного комп’ютера (обсяг встановленої програми перевищує 8 ГБ необхідного місця на диску). Використання безкоштовних аналогів, таких як SciLAB або GNU Octave, хоч і схожих за

синтаксисом команд, не дозволяє гарантувати успішне виконання скриптів, написаних мовою MatLAB. Тому в подальшому дослідженні стійкості стеганоконтейнерів до стиснення ці реалізації не прийматимуть участі.

У даному розділі було проведено опис основних можливостей стеганографічних застосунків, які пропонують вбудовування конфіденційної інформації в цифрові зображення.

3 АНАЛІЗ СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ ПРОГРАМ ДО АТАКИ СТИСНЕННЯМ

3.1 Опис експерименту

Для аналізу стійкості стеганоконтейнеру до атак стиснення приведемо обчислювальний експеримент, який полягає в наступному:

1) обраними стеганографічними програмами вбудувати повідомлення в контейнер-зображення, результат зберегти в форматі JPEG з різними значеннями якості (100, 90, 80, 70, 60, 50);

2) вилучити вбудоване повідомлення зі стиснутого стеганоконтейнеру;

3) оцінити відмінності між оригінальним та витягнутим повідомленнями.

Оцінювання якості вилученого повідомлення буде здійснено за допомогою обсягу правильно вилученої інформації, який розраховується за формулою [1]:

$$P = \frac{\textit{Кількість бітів секретного повідомлення, вилучених вірно}}{\textit{довжина секретного повідомлення}}.$$

В експерименті прийматиме участь 20 зображень-контейнерів в форматі TIFF розміром 2700×1800, 20 зображень-контейнерів в форматі JPG розміром 1600×1200, секретною інформацією є довільний файл, який максимально повно вміщується в контейнер.

Вбудовування і вилучення секретної інформації буде здійснено програмами RedJPEG, SilentEye, Hide ‘N’ Send, Steghide UI.

3.2 Результати дослідження стійкості стеганографічних застосунків до стиснення

В ході проведення експерименту виникли деякі проблеми, пов’язані з тим, що такі програми як RedJPEG та Hide ‘N’ Send зберігають стеганоповідомлення, однак не зазначено, яка саме якість зображення була використана при збереженні.

Припустимо, що використовувалась якість 100. Тоді перезбереження стеганоповідомлення з іншими значеннями якості (90, 80, 70, 60, 50) призводить до того, що ці програми в перезбережених повідомленнях взагалі не бачать наявність вбудованої інформації. Це відображено в табл.3.1 та рис.3.1, 3.2. В програмі SilentEye взагалі не вдалося вилучити секретне повідомлення навіть з стеганоконтейнеру, сформованого самою програмою (рис.3.2). І лише в програмі Steghide UI є як можливість задати якість результату, так і коректними є вилучені секретні повідомлення, причому з абсолютною точністю. Результати експерименту наведені в таблиці 3.1.

Таблиця 3.1 – Точність вилучення секретної інформації з стеганоконтейнеру

Назва програми	Якість стеганоконтейнера *Q*, %					
	100	90	80	70	60	50
RedJPEG	1	Після перезбереження з відповідною якістю вбудована інформація не виявлена (рис.3.1)				
SilentEye	Не вдалося вилучити вбудовану інформацію (рис.3.2)					
Hide ‘N’ Send (M-F5)	1	Після перезбереження з відповідною якістю вбудована інформація не виявлена (рис.3.3)				
Steghide UI	1	1	1	1	0.985	0.965

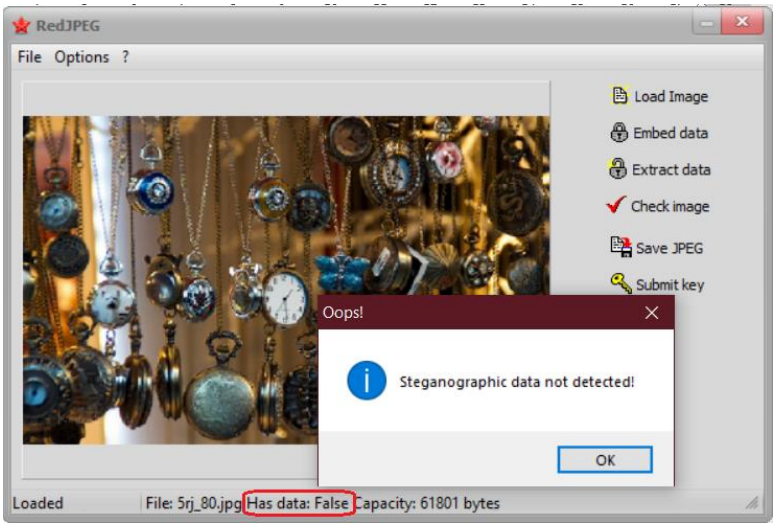

Рисунок 3.1 – Визначення відсутності секретної інформації в стеганоконтейнері програмою RedJPEG

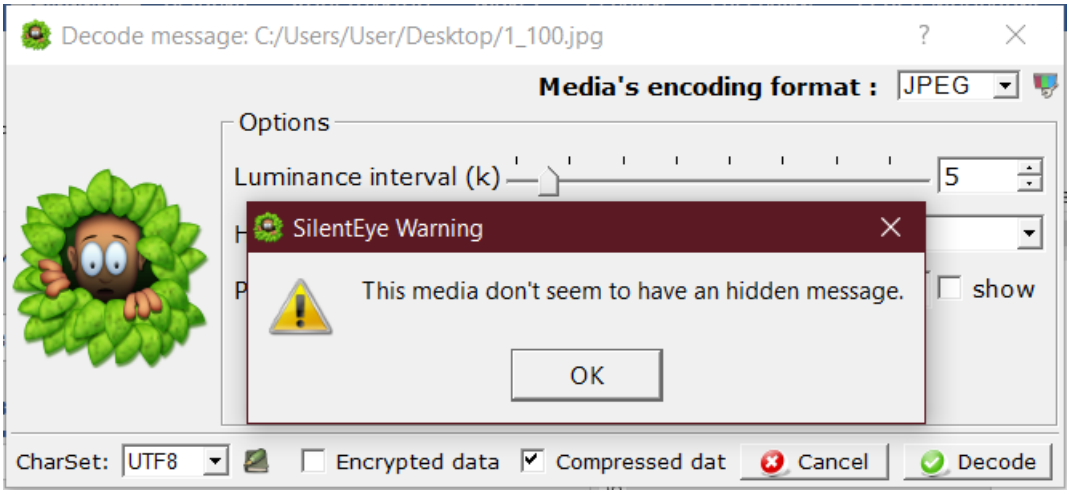

Рисунок 3.2 – Повідомлення про помилку в процесі вилучення секретної інформації програмою SilentEye

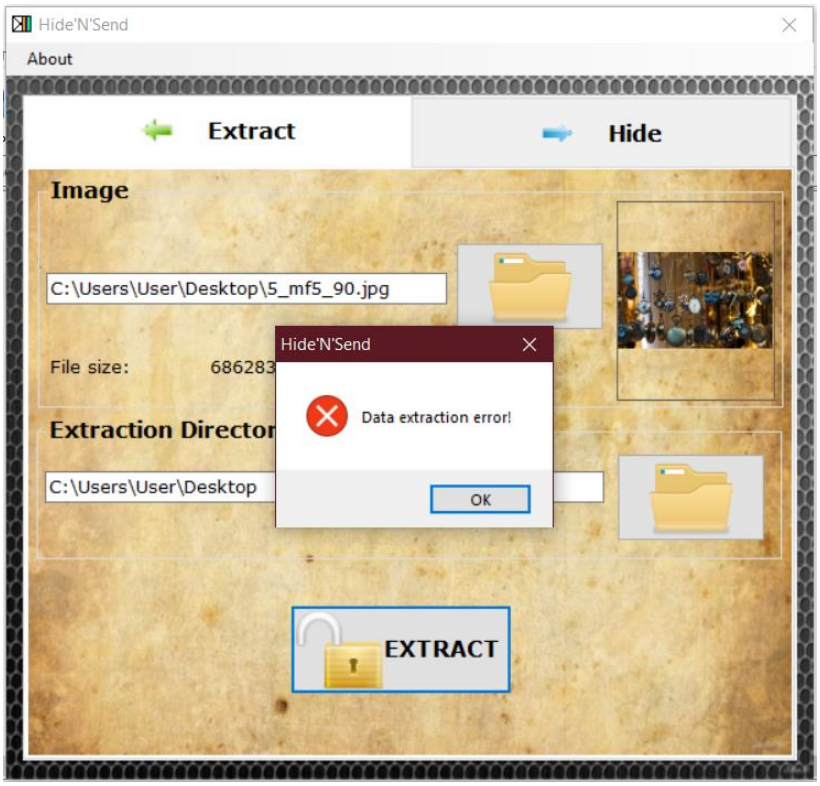

Рисунок 3.3 – Повідомлення про помилку в процесі вилучення секретної інформації програмою Hide ‘N’ Send

3.3 Рекомендації з використання стеганографічних застосунків

Отже, з тих програм, які дозволяють вбудовування конфіденційної інформації з можливістю збереження стеганоконтейнеру в форматі з втратами можна відзначити програми RedJPEG, Hide ‘N’ Send та Steghide UI. Перші дві програми рекомендуються для вбудовування в тому випадку, коли неважливою є якість результуючого зображення, адже ці програми не дають можливості самостійно налаштувати цей параметр. За спостереженнями результатів експериментів якихось помітних артефактів виявлено не було.

Більш серйозною і за функціональністю, і за стійкістю до стиснення можна вважати програму Steghide UI, адже вона якісно вилучає приховане повідомлення за будь-яких заданих параметрах якості. Крім того вона має багато варіантів для шифрування конфіденційної інформації.

В тому випадку, коли достатньо отримати стеганоповідомлення в форматі без втрат, незважаючи на його нестійкість до атак стисненням, корисними будуть програми Hallucinate з коректним алгоритмом вбудовування, OpenPuff з розширеними можливостями шифрування та широким охопленням можливих контейнерів, і OpenStego з можливістю вбудовування цифрового водяного знаку.

Отже в розділі наведено результати експерименту щодо дослідження стійкості стеганоконтейнерів, сформованих за допомогою стеганографічних програм, до атаки стисненням та наведені рекомендації відносно застосування розглянутих застосунків.

ВИСНОВКИ

В кваліфікаційній роботі бакалавра проведено дослідження стійкості застосунків, що реалізують процеси вбудовування та вилучення додаткової інформації в контейнери-зображення, до атак стиснення. Були наведені основні терміни і визначення стеганографії як науки, її основні складові та класифікацію стеганографічних методів залежно від використаної області вбудовування інформації.

В ході огляду стеганографічних застосунків виявлено, що більшість програм реалізують вбудовування методами, які модифікують просторову область контейнеру та не передбачають можливість стиснення стеганоконтейнера. Крім того, характерною є тенденція поєднання криптографічного закриття секретного повідомлення та подальше його приховування в контейнер. Більшість з програм надають широкий вибір криптоалгоритмів для шифрування та хеш-функцій для перевірки цілісності інформації. З тих програм, що є стійкими до стиснення, лише програма Steghide UI має широку функціональність, як з точки зору вибору якості стеганоконтейнеру, можливості коректного вилучення секретної інформації за різних значень якості, так і з точки зору криптографічного закриття чутливих даних.

В ході обчислювального експерименту встановлено, що програми RedJPEG, Hide ‘N’ Send та Steghide UI коректно вилучають приховане повідомлення після стиснення, з поправкою на те, що в застосунках RedJPEG та Hide ‘N’ Send не можна задати якість збереження стеганоповідомлення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конахович Г.Ф., Пузиренко А.Ю. Компьютерная стеганография. Теория и практика. МК-Пресс, 2006. 288 с.
2. Wu D.C., Tsai W.H. A Steganographic method for images by pixel-value differencing. *Pattern Recognition Letters.* 2003. V. 24. P.1613-1626.
3. Kratzer C., Dittmann J., Lang A., Kuhne T. WLAN steganography: A first practical review. *The 8th workshop on Multimedia & Security*. 26-27 September, 2006. Geneva. Pp. 17-22.
4. Mazurczyk W. Lost audio packets steganography: the first practical evaluation. *International Journal of Security and Communication Networks.* December 2012. Vol.5(12). Pp. 1394– 1403.
5. Mazurczyk W. VoIP Steganography and Its Detection – A Survey. *ACM Computing Surveys*. June 2014. Vol. 46, Issue 02, Pp. 1-19.
6. J. Mielikainen, "LSB matching revisited," *Signal Processing Letters*, IEEE, vol. 13, pp. 285-287, 2006.
7. Muhammad, K., Sajjad, M., Mehmood, I. et al. A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. *Multimed Tools Appl* 75, 14867–14893 (2016). https://doi.org/10.1007/s11042-015-2671-9
8. Soukaena H. Hashem, Eman Taleb Zghaer. Review Study among Traditional LSB, Proposed Modified LSB and DWT Steganography Algorith. *Al-Mansour Journal*/ Issue(27) 2017. P.37-56.
9. Marwa M. Emam, Abdelmgeid A. Aly, Fatma A. Omara. A Modified Image Steganography Method based on LSB Technique. *International Journal of Computer Applications* (0975 – 8887) Volume 125 – No.5, September 2015. P.12-17
10. H. C. Wu, N. I. Wu, C. S. Tsai, M. S. Huang. Image steganographic scheme based on pixel-value differencing and LSB replacement methods. *IEE Proceedings Vision Image and Signal Processing*, 2005, vol. 152, no. 5, pp. 611–615.

11. X. Liao, Q.-Y. Wen, J. Zhang. A steganographic method for digital images with four-pixel differencing and modified LSB substitution. *Journal of Visual Communication and Image Representation*, 2011, vol. 22, no. 1, pp. 1–8.
12. G. Swain. Digital image steganography using nine-pixel differencing and modified LSB. *Substitution Indian Journal of Science and Technology*, 2014, vol. 9, no. 7, pp. 1444-1450.
13. Nagaraj V, Vijayalakshmi V, Zayaraz G. Colour image steganography based on pixel value modification method using modulus function. *Int. Conf. on Electronic Engineering and Computer Science*, 2013, pp. 17–24.
14. Yang C-Y, Wang W-F. Block based color image steganography using smart pixel-adjustment. *Adv. Intell. Syst. Comput*, 2015, pp. 145–154.
15. Gandharba Swain. Digital Image Steganography Using Eight-Directional PVD against RS Analysis and PDH Analysis. *Advances in Multimedia*, Volume 2018, 13 pages.
16. Anita Pradhan, K. Raja Sekhar, and Gandharba Swain. Adaptive PVD Steganography Using Horizontal, Vertical, and Diagonal Edges in Six-Pixel Blocks. *Security and Communication Networks*, Volume 2017, 13 pages.
17. Ахмаметьєва Г.В., Гайдук Д.В. Удосконалення стеганографічного методу на основі виділення особливостей блоків цифрового зображення. *Сучасна спеціальна техніка*. 2020. № 4 (63). С. 5-17.
18. Юдін О.К. Аналіз стеганографічних методів приховування інформаційних потоків в контейнери різних форматів *Радіоелектроніка та інформатика*. 2015. № 3. С.13-21.
19. Kobozeva A.A. Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele Energeticii Regionale*. 4 (52), 2021, pp.115-130.
20. Mantoro, T., Alfiah, F. Comparison Methods of DCT, DWT and FFT Techniques Approach on Lossy Image Compression. *International Journal of Computer Techniques*. 2018. Vol. 5. Pp.20-24.

21. Jiansheng M., Sukang L., Xiaomei T. A Digital Watermarking Algorithm Based On DCT and DWT. *International Symposium on Web Information Systems and Applications.* 2009. Pp. 104-107.
22. Roy A.B., Dey, D., Mohanty, B., Banerjee, D. Comparison of FFT, DCT, DWT, WHT Compression Techniques on Electrocardiogram and Photoplethysmography Signals. *IJCA Special Issue on International Conference on Computing, Communication and Sensor Network CCSN*, 2012. Pp. 6-11.
23. Alsayyh M. A., Mohamad D., Saba T., Rehman A., Jarallah S., A Novel Fused Image Compression Technique UsingDFT, DWT, and DCT. *Journal of Information Hiding and Multimedia Signal Processing.* 2017. Vol.8. № 2. Pp. 261-271.
24. Козина М.А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации. *Сучасна спеціальна техніка*. 2014. № 4(39). С.98-106.
25. Ахмаметьєва Г.В., Безсонова М.Д. Розробка стеганографічного методу для цифрових зображень на основі перетворення Фур'є. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. 2020. №69. С. 66-74.
26. Singh N. High PSNR based Image Steganography. *International Journal of Advanced Engineering Research and Science*. 2019. №1. Pp. 109-115.
27. Akter A., Tajnina N. Digital image watermarking based on dwt-dct: evaluate for a new embedding algorithm. *International Conference on Informatics, Electronics & Vision (ICIEV)*. 2014. №10. Pp.1-6.
28. Hallucinate. SourseForge [Електронний ресурс]. Режим доступу: http://sourceforge.net/projects/hallucinate/
29. JHide. SourseForge [Електронний ресурс]. Режим доступу: https://sourceforge.net/projects/jhideapp/
30. OpenPuff. SoftLot [Електронний ресурс]. Режим доступу: https://www.softslot.com/software-1007-openpuff.html
31. OpenStego [Електронний ресурс]. Режим доступу: http://www.openstego.com/

32. Цифровая стеганография: Программы и другие способы. SPY-SOFT.NET [Електронний ресурс]. Режим доступу: https://spy-soft.net/cifrovaya-steganografiya-sposoby-realizacii/
33. Image Steganography. SourseForge [Електронний ресурс]. Режим доступу: https://sourceforge.net/projects/image-steg/
34. SilentEye. SourseForge [Електронний ресурс]. Режим доступу: https://sourceforge.net/projects/silenteye/
35. Hide ‘N’ Send. Softpedia [Електронний ресурс]. Режим доступу: https://www.softpedia.com/get/Security/Encrypting/Hide-N-Send.shtml
36. Steghide UI. Softpedia [Електронний ресурс]. Режим доступу: https://www.softpedia.com/get/Security/Encrypting/Steghide-UI.shtml
37. Steganographic Algorithms [Електронний ресурс]. Режим доступу: http://dde.binghamton.edu/download/