Міністерство освіти і науки України
Одеський національний політехнічний університет
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення

Безсонова Марія Дмитрівна,
студентка групи РЗ-151

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

Розробка стеганографічного методу для цифрових зображень на основі перетворення Фур'є

Спеціальність:
125 Кібербезпека

Спеціалізація, освітня програма
Кібербезпека

Керівник:
Ахмаметьєва Ганна Валерьївна,
к.т.н

Одеса – 2020

Міністерство освіти і науки України
Одеський національний політехнічний університет
Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій
Кафедра кібербезпеки та програмного забезпечення
Рівень вищої освіти другий (магістерський)
Спеціальність 125 – Кібербезпека
Освітня програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри КБПЗ

_____
д.т.н.,проф. А.А.Кобозєва
____ _____202_р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Безсоновій Марії Дмитрівні

1.Тема роботи: *Розробка стеганографічного методу для цифрових зображень на основі перетворення Фур'є*

керівник роботи *Ахмаметьєва Ганна Валерьївна, к.т.н.*

затверджені наказом ректора ОНПУ від „ 16 ” листопада 2020 р. № 468-в

2.Зміст роботи: *аналіз проблемної області, постановка задачі, розробка стеганографічного методу для цифрових зображень на основі перетворення Фур'є, аналіз ефективності розробленого методу, охорона праці.*

3. Перелік ілюстративного матеріалу: *Схема вбудови та вилучення біт повідомлення з блоку цифрового зображення. Схема вбудови та вилучення трьох біт повідомлення в блок цифрового зображення з корегуванням різниці між коефіцієнтами Фур’є.*

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
Охорона праці	Ярова І.А., к.т.н., доцент	Завдання видав	Завдання прийняв

5. Дата видачі завдання "_____"_____20___ р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
1	*Аналіз джерел з теми випускної кваліфікаційної роботи*	*1.09-15.09.2020*	*виконано*
2	*Обґрунтування вибору рішення. Збір даних*	*15.09-1.10.2020*	*виконано*
3	*Визначення формальних параметрів ЦЗ*	*1.10-20.10.2020*	*виконано*
4	*Розробка стенографічного алгоритму*	*20.10-10.11.2020*	*виконано*
5	*Оцінка ефективності розробленого алгоритму*	*10.11-25.11.2020*	*виконано*
6	*Підготовка тексту роботи*	*25.11-15.11.2020*	*виконано*
7	*Підготовка презентації та доповіді*	*15.11-20.112020*	*виконано*
8	*Попередній захист*	*2.12.2020*	*виконано*
9	*Нормоконтроль, рецензування*	*21.12.2020*	*виконано*
10	*Занесення роботи в електронний архів*	*24.12.2020*	*виконано*
11	*Допуск до захисту у завідувача кафедри*	*24.12.2020*	*виконано*

Здобувач вищої освіти _____ *Безсонова М.Д.*

Керівник роботи _____ *Ахметьєва Г.В.*

ЗАВДАННЯ

на розробку розділу “Охорона праці та безпека в надзвичайних ситуаціях”

Безсоновій Марії Дмитрівні, група РЗ-151

Інститут інформаційної безпеки, радіоелектроніки та телекомунікацій

Кафедра кібербезпеки і програмного забезпечення

Тема роботи: *Розробка стеганографічного методу для цифрових зображень на основі перетворення Фур'є*

Зміст розділу:

1. Аналіз умов праці і вибір заходів і засобів захисту від небезпечних і шкідливих виробничих факторів.
2. Аналіз техногенних небезпек і вибір заходів і засобів забезпечення безпеки у надзвичайних ситуаціях.
3. Вибір первинних засобів пожежогасіння.

Керівник роботи	Консультант з охорони праці та БНС
_____	_____
(прізвище та ініціали)	(прізвище та ініціали)
_____	_____
(підпис)	(підпис)
«____» _____ 2020 р.	«____» _____ 2020 р.

АННОТАЦІЯ

Кваліфікаційна робота магістра на тему "Розробка стеганографічного методу для цифрових зображень на основі перетворення Фур'є" на здобуття освітньо-кваліфікаційного рівня "Магістр" за напрямом 125– Кібербезпека написана об'ємом 55 сторінок і містить 23 рисунків, 3 таблиці, 1 додаток і 50 джерел літератури.

Метою роботи є підвищення візуальної якості стеганоповідомлень при забезпеченні високої пропускної спроможності прихованого каналу зв’язку шляхом розробки стеганографічного методу на основі перетворення Фур’є.

У роботі був запропонований новий стеганографічний метод для цифрових зображень на основі швидкого перетворення Фур’є. Метод дозволяє забезпечити високу пропускну спроможність прихованого каналу зв’язку при збереженні високої якості стеганоповідомлення (середнє значення PSNR становить 58-60 дБ).

В ході проведених обчислювальних експериментів встановлено, що в більшості випадків забезпечується висока точність вилучення додаткової інформації (в 88% заповнених контейнерів з усіх експериментів показник NCC перевищує значення 0,9).

Експерименти, спрямовані на аналіз стійкості до атак, зокрема зашумлення, показали високу стійкість до шуму «Сіль та перець», а також до Гаусового та мультиплікативних шумів при незначних спотвореннях стеганоповідомлень.

СТЕГАНОГРАФІЯ, ШВИДКЕ ПЕРЕТВОРЕННЯ ФУР’Є, ЦИФРОВЕ ЗОБРАЖЕННЯ

ANOTATION

Qualification work on "DEVELOPMENT OF A STEGANOGRAPHIC METHOD FOR DIGITAL IMAGES BASED ON FOURIER TRANSFORM" for the second (Master's) level of higher education in the specialty 125 - Cybersecurity, educational program "Cybersecurity", contains 23 figures, 3 tables, 1 appendix, 50 references. The work is written on 58 pages of the general text and 55 pages of the main text.

The aim of the work is to improve the visual quality of stegos while ensuring high capacity of the covert communication channel by developing a steganographic method based on the Fourier transform.

A new steganographic method for digital images based on Fast Fourier Transform was proposed. The method allows you to provide ensuring high capacity of the covert communication channel while high quality of stegos is provided (average PSNR value is 58-60 DB).

The results of computational experiments have shown that in most cases high accuracy of extracting additional information is ensured (in 88% of filled containers from all experiments, the NCC indicator exceeds the value of 0.9).

Experiments aimed at analyzing resistance to attacks, in particular noise, showed high resistance to attack by the noise "Salt and pepper", as well as the imposition of a Gaussian and a multiplicative noise at imperceptible distortions of stegos.

STEGANOGRAPHY, FAST FOURIER TRANSFORM, DIGITAL IMAGE

ЗМІСТ

ВСТУП

Сучасний розвиток інформаційних технологій сприяє їх широкому поширенню серед населення. В наш час вже неможливо уявити передачу будь-якої інформації без використання мережі Інтернет, обмін інформацією є настільки масштабним процесом, що вже неможливо повністю контролювати весь ланцюжок проходження інформаційним контентом проміжних серверів, які і забезпечують миттєву доставку повідомлень від відправника до отримувача. Ніхто з законних власників інформації не може гарантувати неможливість її несанкціонованого використання сторонніми особами, що потребує додаткового захисту конфіденційної інформації. Оскільки в ряді країн обмежено використання криптографічних засобів, широке поширення отримали розробки в області стеганографії – застосування стеганографічних методів і програм дозволяє зберегти в таємниці сам факт наявності повідомлення (додаткової інформації) в будь-якому інформаційному контенті. В якості контейнера можуть виступати будь-які цифрові дані: текстові документи, зображення, аудіо, відео та інші. Результат вбудови повідомлення в контейнер будемо називати заповненим контейнером або стеганоповідомленням.

При розробці стеганографічних методів увага приділяється наступним важливим умовам:

– забезпечення високої цілісності сприйняття сформованого стеганоповідомлення у порівнянні з оригінальним, відсутністю помітних спотворень, які указували б на наявність додаткової інформації;

– забезпечення надійності вилучення повідомлення з заповненого контейнеру, що є неодмінним компонентом при організації каналу прихованої передачі інформації;

– по можливості забезпечувати високу пропускну спроможність прихованого каналу інформації, оскільки в більшості методів підвищення ємності контейнера призводить до погіршення якості стеганоповідомлення;

– в деякої мірі стеганографічні методи повинні забезпечувати стійкість до навмисних або ненавмисних атак.

Аналіз останніх публікацій показав, що для більшості сучасних розробок залишається проблема співвідношення якості стеганоповідомлення і пропускної спроможності прихованого каналу зв’язку, тому тема роботи є актуальною.

Метою роботи є підвищення візуальної якості стеганоповідомлень при забезпеченні високої пропускної спроможності прихованого каналу зв’язку шляхом розробки стеганографічного методу на основі перетворення Фур’є.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

– проаналізувати стан сучасних розробок в області стеганографічного захисту інформації;
– розробити основні кроки стеганографічного методу;
– провести обчислювальні експерименти, спрямовані на оцінку ефективності запропонованого методу та визначення його стійкості до атак;
– виконати порівняння показників візуальної якості PSNR та пропускної спроможності прихованого каналу зв’язку для запропонованого методу і сучасних аналогів;
– розробити програмний інтерфейс для розробленого стеганографічного методу.

Об'єкт дослідження - процеси організації і створення стеганографічного каналу зв'язку.

Предмет дослідження – стеганографічні методи приховування інформації для цифрових зображень.

Наукова новизна одержаних результатів полягає в наступному.

1. Вперше розроблено стеганографічний метод вбудови додаткової інформації в область перетворення Фур’є, який забезпечує високу якість заповненого контейнеру при забезпеченні високої пропускної спроможності прихованого каналу зв’язку.

2. Проведено дослідження впливу просторових значень яскравості цифрового зображення на результат вилучення додаткової інформації, що дозволило підвищити якість вилученого повідомлення.

Практичне значення отриманих результатів. Практична цінність роботи полягає в розробці нового стеганографічного метода на основі перетворення Фур'є, який забезпечує високу пропускну спроможність прихованого каналу зв'язку та високу якість стеганоповідомлення. Розроблений метод може бути використаний як складова частина комплексних систем захисту інформації будь-яких підприємств, структур, тощо.

У вступі обумовлена актуальність теми, сформульована мета, задачі, об'єкт та предмет досліджень.

В першому розділі були розглянуті основні поняття та визначення стегонографії, розглянуті існуючі стеганографічні системи і методи, та була обумовлена актуальність створення даного метода.

В другому розділі розглянуті теоретичні відомості стеганографічного метода, була проведена оцінка ефективності розробленого стеганографічного методу, та проведено порівняння методи з аналогами.

В третьому розділі розглянуті основні кроки розробки алгоритмічної реалізації стеганографічного метода, та основні моменти роботи з інтерфейсом програми.

В четвертому розділі проведено аналіз ймовірних небезпечних та шкідливих виробничих факторів. Був проведений аналіз причин пожежної небезпеки, яка створюються проектованим об'єктом. Та були розроблені заходи, направлені на усунення або зниження шкідливого впливу виявлених факторів.

В висновках описується отримані результати роботи.

Публікації. Матеріали кваліфікаційної роботи магістра опубліковані в [1].

1 СУЧАСНИЙ СТАН СТЕГАНОГРАФІЇ ЦИФРОВИХ ЗОБРАЖЕНЬ

1.1 Основні поняття та визначення стеганографії

Стеганографія – наука про способи передачі, зберігання прихованої інформації, при яких прихований канал організується на базі і в межах відкритого каналу із застосуванням особливостей сприйняття інформації [2].

Для цієї мети можуть використовуватися такі прийоми [2]:

- повне приховування факту існування прихованого каналу зв'язку;
- створення труднощів для виявлення, вилучення або модифікації переданих прихованих повідомлень всередині відкритих повідомлень-контейнерів;
- маскування прихованої інформації в протоколі.

Стеганографія має такі чотири підрозділи [3]:

- стеганографія зображення. Вбудова додаткової інформаціїї (далі ДІ) відбувається всередину зображення контейнера таким чином, що існування ДІ зникає, а зображення візувльно не відрізнити від оригінального;
- аудіостеганографія. Цифрові звукові файли використовуються для приховування [4];
- відеостеганографія. відеофайли можна визначити як сукупність зображень і звуків, об'єднаних разом. Тому є велика кількість можливостей вбудови ДІ у відео, найбільш популярним форматов для вбудови ДІ в відео є формати MPEG-2 та MPEG_4 [5];
- текстова стеганографія. Текстова стеганографія відноситься до інформації, яка прихована в текстових файлах.

Мета класичної стеганографії - полягає в тому, щоб приховати інформацію в інших відкритих наборах або потоках даних таким способом, який не дозволяє виявити, що в них є якась прихована складова частина, і тим самим виділити ці повідомлення серед інших [6].

Комп'ютерна стеганографія - це розділ стеганографії який вивчає системи прихованої передачі інформації, в яких в якості контейнера і повідомлення виступають апаратне або програмне забезпечення комп'ютера або цифрові дані, які він зберігає і обробляє [7].

В даний час виділяють наступні основні положення комп'ютерної стеганографії [7]:

- методи приховування повинні забезпечувати цілісність файлу.
- передбачається, що противнику повністю відомі можливі стеганографічні методи (згідно з принципом Керкгоффса).
- безпека методів ґрунтується на збереженні стеганографічним перетворенням основних властивостей відкрито переданого файлу при внесенні в нього секретного повідомлення і невідомої противнику інформації - ключа.

Контейнер – носій схованого повідомлення.

Порожній контейнер-це контейнер, який не містить повідомлення.

Заповнений контейнер – це контейнер, який містить повідомлення [2].

Стеганографічна система (стегосистема) – сукупність засобів та методів які використовуються з метою формування прихованого каналу зв’язку [8].

Стегосистема складається з таких основних елементів[9]:

- прекодер-пристрій, призначений для перетворення приховуваного повідомлення до виду, зручного для вбудовування в сигналконтейнер.
- стегокодер-пристрій, призначений для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їх моделі;
- пристрій виділення вбудованого повідомлення;
- стегодетектор-пристрій, призначений для визначення наявності стегоповідомлення;
- декодер-пристрій, що відновлює приховане повідомлення.

Для того, щоб стегосистема була надійною, необхідно притримуватися певному ряду вимог [9]:

- безпека системи повинна повністю визначатися секретністю ключа. Це означає, що порушник може повністю знати всі алгоритми роботи стегосистеми і статистичні характеристики множин повідомлень і контейнерів, і це не дасть йому ніякої додаткової інформації про наявність або відсутність повідомлення в даному контейнері;
- знання порушником факту наявності повідомлення в будь-якому контейнері не повинно допомогти йому при виявленні повідомлень в інших контейнерах;
- заповнений контейнер повинен не відрізняти візуально від незаповненого;
- стегосистема ЦВЗ повинна мати низьку ймовірність помилкового виявлення прихованого повідомлення в сигналі, що його не містить. У деяких додатках таке виявлення може призвести до серйозних наслідків.
- повинна забезпечуватися необхідна пропускна здатність (ця вимога актуальна, в основному, для стегосистем прихованої передачі інформації);
- стегосистема повинна мати прийнятну обчислювальну складність реалізації.

Ключ - псевдовипадкова послідовність біт, створена генератором, що задовольняє певним вимогам (криптографічно безпечний генератор) [6].

Дані, що містять приховане повідомлення, можуть піддаватися навмисним атакам або випадковим перешкодам [9].

Можна розділити на наступні класи такі атаки на стегосистеми [9, 10]:

- атаки зі знанням тільки модифікованого контейнера аналог криптографічної атаки зі знанням шифртексту. Стеганоаналітик в цьому випадку володіє тільки модифікованим контейнером, за яким він намагається визначити наявність прихованого повідомлення. З усіх видів цей вид стеганографічних атак є базовим, за якими оцінюються - стегосистеми;
- атаки зі знанням немодифікованого контейнера можливі в випадку, коли стеганоаналітик також має здатність дізнаватися, який саме немодифікований контейнер був використаний для приховування

повідомлення. Дана атака визначає можливість визначення факту приховування повідомлень в подальшому в залежності від наявності одного разу перехопленого контейнера і розкритого повідомлення;

- про атаки з вибором повідомлення говорять, коли стеганоаналітик має можливість вказувати, які саме повідомлення будуть приховані, але при цьому не має можливості вказати контейнер, який буде для цього використовуватися. Стійкість до даної атаки характеризує стійкість системи до перехоплення і відстеження повідомлень, посланих з використанням одного і того ж контейнера. Даний вид атак іноді також позволяють визначити тип застосованої стеганографічної системи;
- атаки з вибором контейнера, при умові повторного використання одного і того ж повідомлення з різними контейнерами дозволяє визначити стійкість стегосистеми до розкриття;
- атаки про підміни і імітації не покликані визначити факт наявності повідомлення або витягти його, їх застосовують для модифікації прихованої інформації, або імітації такої передачі;
- атаки з протидії передачі інформації використовують для знищення прихованої інформації та зниження пропускної спроможності каналів прихованої передачі даних.

1.2 Класифікація стеганографічних систем

Стегосистеми використовуються для вирішення таких задач [11]:

- захист конфеденційної інформації від несанкціонованого доступу;
- обхід засобів моніторингу;
- захист авторських прав.

При побудові стегосистеми враховують такі вимоги:

- стеганосистема повинна мати прийнятну обчислювальну складність своєї реалізації достатніх для розв’язання поставленої задачі, такої як процес вбудовування/видобування ДІ з контейнера;

- повинна забезпечуватися необхідна пропускна здатність;
- якщо факт існування прихованого повідомлення стає відомим порушнику, це не повинне дозволити йому видобути його до тих пір, доки сам ключ знаходиться в таємниці;
- методи приховання мають забезпечувати автентичність і цілісність секретної інформації для авторизованої особи.
- порушник повинен бути позбавлений будь-яких технічних та інших переваг у детектуванні наявності і, розкритті змісту секретних повідомлень;
- безпека системи повинна повністю визначатися секретністю ключа.

Виділяють чотири вида стеганографічних систем [11]:

- безключові стегосистеми;
- стегосистеми з секретним ключем;
- стегосистеми з відкритим ключем;
- змішані стеганосистеми.

Безключова стегосистема не потребує ніякої ДІ, на зразок стеганоключа. Щоб збільшити стан захищеності процесу зв'язку, на попередньому етапі виконується шифрування прихованої інформації, з метою ускладнення виявлення прихованого повідомлення, однак для «сильних» стеганосистем, цей етап не обов'язковий [11].

У стегосистемі з секретним ключем ключ розподіляється між авторизованими особами за принципом Керкгоффса,

Вбудовуючи секретне повідомлення контейнера відправник використовує стеганоключ. Одержувач зможе видобути інформацію з контейнера, тільки при наявності ключа. Цей тип стегосистем допускає, що обмін стеганоключей відбувається через захищений канал зв'язку [11].

В якості окремого випаду можна виділити системи де використовують відомості про деякі дані, під час видобування ДІ, такі як первинний контейнер, тощо. Тому що, передача первинного контейнера те саме, що й задачі ключового обміну [11].

Стегосистеми з відкритим ключем не потребують додатковий канал ключового обміну [11].

Для роботи з стеганографічними системами з відкритим ключем потрібно мати два стеганоключі. Один секретний, а інший — відкритий [11].

Секретний ключ зберігається в таємниці та використовується для вбудовування ДІ. Відкритий ключ зберігається у доступному для всіх місці та використовується для видобування ДІ [12].

Змішані стегосистеми є найбільш популярними в використанні на сьогоднішній день. Хоча й вони мають певний недолік, в тому, що така система може бути розкрита. За умови, якщо порушник дізнається про метод стеганоперетворення, який застосовувався. Тому в таких системах використовуються особливості особливості систем з відкритим і/або секретним ключем. У роботах [13-15] запропоновані різні види організацій стегосистем під відповідні задачі.

1.3 Огляд стеганографічних методів

Переважна більшість методів комп'ютерної стеганографії базується на двох ключових принципах [10]:

- файли, які не вимагають абсолютної точності (наприклад, файли із зображенням, звуковою інформацією і т. д.), можуть бути візуально змінені (звичайно, до певної міри) без втрати своєї функціональності;
- органи чуття людини нездатні надійно розрізняти незначні зміни в модифікованих таким чином файлах і/або відсутній спеціальний інструментарій, який був би здатний виконувати дане завдання [16].

ДІ може вбудовуватися в такі області:

- просторова область
- частотна область

Метод заміни найменш значущого біта найбільш поширений серед методів заміни в просторовій області.

Молодший значущий біт зображення несе в собі найменше інформації. Помітити зміни в цьому біті, в більшості випадків, людина не здатна. Фактично, найменш значущий біт - це шум, тому його можна використовувати для вбудовування інформації шляхом заміни менш значущих бітів пікселів зображення бітами секретного повідомлення. Цей метод став популярним завдяки його простоті і тим, що він дозволяє приховувати у відносно невеликих файлах досить великі обсяги інформації [10].

Основний його недолік - висока чутливість до найменших спотворень контейнера. Для ослаблення цієї чутливості часто додатково застосовують кодування яке стійке до спотворень. На сьогоднішній день є метод який усуває даний недолік [17].

Також є інші варіанти вдосконалення даного метода [18-20]

Алгоритм Куттера-Джордана-Боссена був запропонований Куттером, Джорданом і Боссеном для вбудовування в канал синього кольору зображення, представленого в схемі RGB. У цифрове зображення вбудовуються окремі біти шляхом зміни значення синього каналу. Ця зміна пропорційна яскравості компонента пікселя і може приймати як позитивні, так і негативні значення в залежності від значення вбудованого біта водяного знака [10].

Даний метод є ефективним виходячі зі статей [21] також присутні його модифікації [22-24].

Так в [25] був розроблений стеганографічний алгоритм, стійкий до збурних дій, який для вбудови ДІ використовує просторову області ЦЗ-контейнера. Але умовою, що забезпечувала його стійкість до збурних дій, вимагала високу обчислювальну складність. Вирішенню цієї проблеми було присвячено роботу [26], у якій зменшення обчислювальної складності досягається відсутністю необхідності проведення перетворення з просторової області у область розкладання та назад при організації занурення та декодування ДІ.

Стеганографічні методи приховування даних в просторовій області зображення є нестійкими до більшості з відомих видів спотворень. Більш стійкими до різноманітних спотворень, в тому числі і компресії, є методи, що

використовують для приховування даних не просторову область контейнера, а частотну.

Найбільшого поширення серед усіх ортогональних перетворень у стеганографії набули вейвлет-перетворення та ДКП.

Метод відносної заміни величин коефіцієнтів ДК також відомий як метод Коха і Жао. Один з найбільш поширених на сьогодні методів приховування конфіденційної інформації в частотній області зображення полягає у відносній заміні величин коефіцієнтів ДКП [10]. На початковому етапі первинне зображення розбивається на блоки 8х8. ДКП застосовується до кожного блоку, в результаті чого отримують матриці 8х8 коефіцієнтів ДКП. Кожен блок при цьому призначений для приховування одного біта даних [10].

У роботі [27,28] була запропонована модифікація методів, що використовують частотну область, а саме дискретно-косинусне перетворення для вбудови ДІ, вчасності метода Коха і Жао. Підвищення ефективності відбувається за рахунок вибору коефіцієнтів ДКП таким чином, аби матриця квантування JPEG, мала найменші значення, тобто низькочастотної складової зображення. Дане рішення показало кращі результати в умовах атаки стиском, але при накладанні шумів, фільтрації та масштабуванні результат не мав значних змін, а за рахунок використання низькочастотних коефіцієнтів можливе порушення надійності сприйняття. В роботі [29] дискретно-косинусне перетворення використовували з розширеною таблицею квантування 32х32, а в [30] використовували таблицю інтерполяційного квантування.

В методі Бенгама-Мемона-Эо-Юнг метод Коха и Жао був обран за основу. Метод відрізняється тим, що в даному методі запропонували використовувати вбудову ДІ тільки в найбільш підходящі для цього блоки, а не в усі. Для вбудови ДІ обирають три коефіцієнта ДКП замість двох. В результаті це призвело до зменшення спотворення контейнера [10]. Однак цей метод є вразливим до сторонніх впливів [11].

Окрім, дискретного-косинусного перетворення стеганографічні методи, що вбудовують ДІ у частотну область використовують дискретне перетворення

Фур'є, дискретне вейвлет-перетворення [10,31] та інші. Так у [32] представлено алгоритм, що використовує для модифікації частотних коефіцієнтів перетворення Адамара, але у якості контейнера можливе використання лише напівтонових зображень. У статті [33,34] виявлено що використання перетворення Адамра може забезпечувати майже повну стійкість до JPEG-стиснення.

Більшість останніх публікацій присвячені розробці стеганографічних методів, заснованих на дискретному косинусному перетворенні [35-36], вейвлет-перетворенні [37-38] або комбінації частотних перетворень [39-40], що хоч і призводить до стійкості до атак, але для даних методів характерно зменшення пропускної спроможності і складність реалізації, крім того не забезпечується висока якість стеганоповідомлення, про що свідчать невисокі значення PSNR. Однак методів, в основу яких покладено перетворення Фур'є, не так багато.

В роботі [41] запропонований стеганографічний метод забезпечує достатньо високу пропускну спроможність, однак значно залежить від обраних параметрів вбудови – висока якість стеганоповідомлень забезпечується лише при малих значеннях α, при значеннях $\alpha > 0.0001$ заповнений контейнер містить помітні спотворення. В роботах [42-43] отримані невисокі значення PSNR (37,6 і 32,8 дБ відповідно) для стеганоповідомлення при забезпеченні високої пропускної спроможності прихованого каналу зв'язку.

В статті [44] наведено теоретичний базис для стеганографічного методу [45], який забезпечує високу надійність вилучення інформації, проте значення PSNR (42 дБ) і пропускна спроможність залишаються недостатньо високими.

Таким чином, аналіз публікацій показав, що для більшості стеганографічних методів характерною є проблема співвідношення якості стеганоповідомлення і пропускної спроможності прихованого каналу зв'язку. Тому метою роботи є розробка стеганографічного методу для цифрових зображень, що забезпечує високу пропускну спроможність прихованого каналу зв'язку при збереженні якості заповненого контейнеру.

2 РОЗРОБКА СТЕГАНОГРАФІЧНОГО МЕТОДУ

2.1 Теоретичні відомості стеганографічного метода

Як контейнер будемо розглядати окрему колірну складову цифрового зображення (ЦЗ), представленого в схемі RGB, або полутонове зображення I розміром $M \times N$. В якості додаткової інформації можна використовувати будь-яку бінарну послідовність, сформовану на основі тексту або зображення.

В основі стеганографічного методу лежить теоретичний базис, наведений в [44], основне положення якого полягає в отриманні цілих частотних коефіцієнтів Фур'є для блоків 2×2. Однак стеганографічний метод, розроблений на основі [44], потребує просторової корекції значень яскравості перед обчисленням перетворення Фур'є та передбачає вбудову лише одного біта інформації в блок. Для методу, що розробляється, будемо використовувати швидке перетворення Фур'є для блоку B розміром 2×2:

$$F(u,v) = \sum_{x=0}^{1} \sum_{y=0}^{1} B(x,y) e^{-2i\pi\left(\frac{ux}{2}+\frac{vy}{2}\right)}, \quad (2.1)$$

де $F(u,v)$ – (u,v) -й коефіцієнт швидкого перетворення Фур'є, $B(x,y)$ – (x,y) -й піксель блоку B, $u = \overline{0,1}$, $v = \overline{0,1}$.

Вбудову додаткової інформації реалізуємо на основі просторового методу PVD [48] шляхом модифікації різниці між двома коефіцієнтами перетворення Фур'є: $F(0,1)$ і $F(1,0)$. Суть вбудови повідомлення полягає в наступному. З бінарної послідовності вибираються l біт, які переводяться в десяткову систему числення - d. Саме це значення і визначає різницю між пікселями, після чого значення коефіцієнтів модифікуються у відповідності з d.

Коефіцієнти $F(0,1)$ і $F(1,0)$ для вбудови інформації були обрані експериментальним шляхом. При аналізі коефіцієнтів було помічено, що коректне вилучення інформації відбувається лише за умови парних значень абсолютної різниці між коефіцієнтами, що обумовлено тим, що у випадку

непарного значення різниці коефіцієнтів обернене перетворення Фур'є призводить до дробових значень яскравості, які потребують округлення до цілих значень. Це в свою чергу веде до некоректної різниці між коефіцієнтами Фур'є при повторному перетворенні. Для уникнення помилок детектування слід подвоювати значення d. Приклад вбудови додаткової інформації в блок наведений на рисунку 2.1.

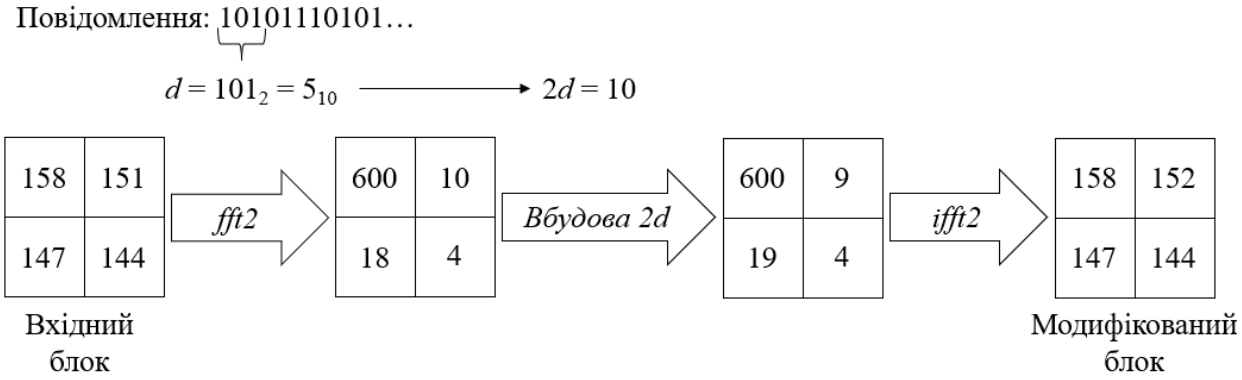

Рисунок 2.1 – Приклад вбудови трьох біт повідомлення в блок цифрового зображення

Ще один недолік пов'язаний з широким діапазоном значень абсолютної різниці між коефіцієнтами $F(0,1)$ і $F(1,0)$ для різних блоків. В класичному методі PVD для пікселів ЦЗ це враховується використанням таблиці діапазонів квантування, однак в даному методі через використання подвійних значень d застосування таблиць ускладнене по причині відсутності непарних значень. Тому ми пропонуємо корегувати десяткове значення абсолютної різниці d на величину $s = k \cdot 2^{l+1}$, де $k = \left\lfloor \frac{d}{2^{l+1}} \right\rfloor$, l - число біт, що вбудовуються в блок. Приклад вбудови додаткової інформації в блок з корегуванням різниці між коефіцієнтами Фур'є наведений на рисунку 2.2.

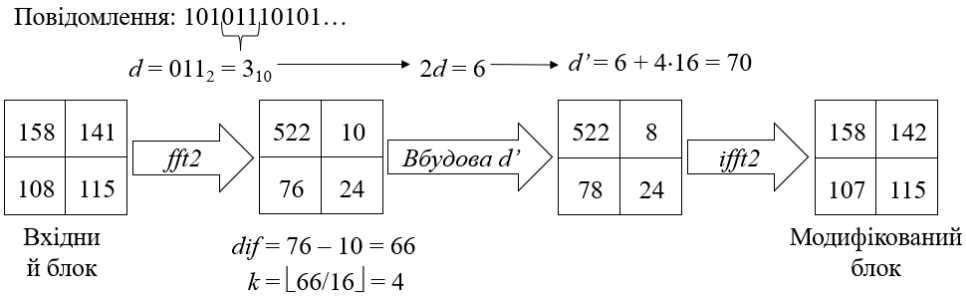

Рисунок 2.2 – Приклад вбудови трьох біт повідомлення в блок цифрового зображення з корегуванням 2.2 різниці між коефіцієнтами Фур'є

Модифікація самих коефіцієнтів відбувається згідно класичного методу PVD [48], після чого виконується обернене швидке перетворення Фур'є:

$$B'(x,y) = \sum_{u=0}^{1}\sum_{v=0}^{1} F'(u,v)e^{2i\pi\left(\frac{ux}{2}+\frac{vy}{2}\right)}, \qquad (2.2)$$

де $F'(u,v)$ - коефіцієнти Фур'є блоку після вбудови інформації, $B'(x,y)$ - значення яскравості модифікованого блоку, $x = \overline{0,1}$, $y = \overline{0,1}$.

Вилучення додаткової інформації відбувається наступним чином. Для блоку обчислюється швидке перетворення Фур'є, між двома коефіцієнтами $F'(0,1)$ і $F'(1,0)$ обчислюється абсолютне значення різниці d'. Якщо $d' > s$, то модифікуємо значення d' за формулою $d' = d' - s$. Знаходимо $b' = \frac{d'}{2}$, де значення b', переведене у двійкову систему числення, представляє собою фрагмент бінарної послідовності. Приклади вилучення додаткової інформації для розглянутих вище випадків наведені на рисунках 2.3 і 2.4 відповідно.

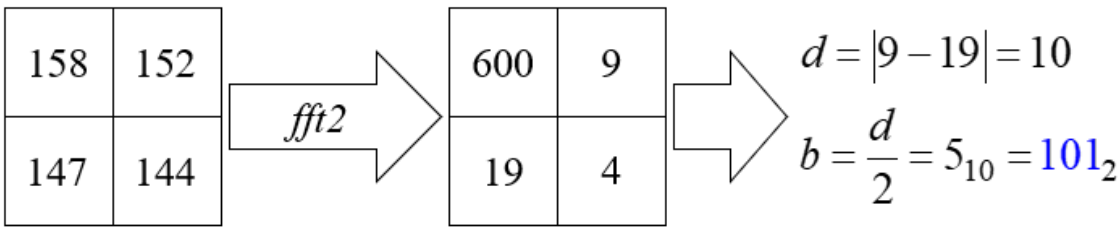

Рисунок 2.3 – Приклад вилучення трьох біт повідомлення з блоку ЦЗ

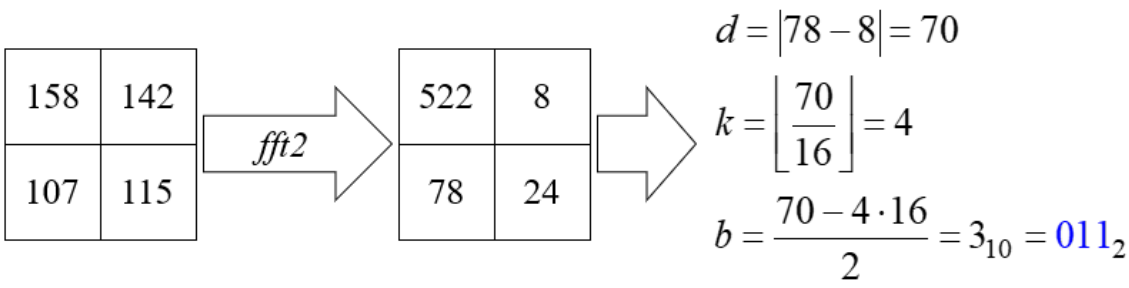

Рисунок 2.4 – Приклад вилучення трьох біт повідомлення з блоку цифрового зображення при корегуванні різниці між коефіцієнтами Фур'є

Нижче наведені основні кроки вбудови і вилучення повідомлення для запропонованого стеганографічного методу.

Вбудова додаткової інформації в контейнер.

Крок 1. Додаткову інформацію AI представити як бінарну послідовність $binAI$ довжиною L.

Крок 2. Виділити колірну складову I ЦЗ розміром $M \times N$, використовувану для вбудови додаткової інформації AI.

Крок 3. Колірну складову I розбити на блоки B розміром 2×2, що не перетинаються.

Для кожного блоку B (кроки 4-10):

Крок 4. Виконати швидке перетворення Фур'є. Результат - B^F.

Крок 5. З послідовності $binAI$ виділити l біт, перевести їх в десяткову систему числення. Результат - b.

Крок 6. Обчислити $d = \left|B^F_{1,2} - B^F_{2,1}\right|$.

Крок 7. Обчислити $b' = 2b + \left\lfloor \frac{d}{2^{l+1}} \right\rfloor \cdot 2^{l+1}$.

Крок 8. Якщо $\left|b' - d\right| < |2b - d|$, то $b = b'$, інакше $b = 2b$.

Крок 9. Модифікувати значення $B^F_{1,2}$ і $B^F_{2,1}$ у відповідності до формули

$$\left(B_{1,2}^{F}{}',\ B_{2,1}^{F}{}'\right) = \begin{cases} \left(B_{1,2}^{F} + \left\lceil \frac{m}{2} \right\rceil,\ B_{2,1}^{F} - \left\lfloor \frac{m}{2} \right\rfloor\right),\ якщо\ B_{1,2}^{F} \geq B_{2,1}^{F}\ \&\ b > d \\ \left(B_{1,2}^{F} - \left\lceil \frac{m}{2} \right\rceil,\ B_{2,1}^{F} + \left\lfloor \frac{m}{2} \right\rfloor\right),\ якщо\ B_{1,2}^{F} < B_{2,1}^{F}\ \&\ b > d \\ \left(B_{1,2}^{F} - \left\lceil \frac{m}{2} \right\rceil,\ B_{2,1}^{F} + \left\lfloor \frac{m}{2} \right\rfloor\right),\ якщо\ B_{1,2}^{F} \geq B_{2,1}^{F}\ \&\ b \leq d \\ \left(B_{1,2}^{F} + \left\lceil \frac{m}{2} \right\rceil,\ B_{2,1}^{F} - \left\lfloor \frac{m}{2} \right\rfloor\right),\ якщо\ B_{1,2}^{F} < B_{2,1}^{F}\ \&\ b \leq d \end{cases}$$

де $m = |b - d|,\ \lfloor \bullet \rfloor$ - округлення до найменшого цілого, $\lceil \bullet \rceil$ - округлення до найбільшого цілого.

Крок 10. Виконати обернене швидке перетворення Фур'є. Результат - $B^{'}$.

Крок 11. Зберегти заповнений контейнер.

Вилучення додаткової інформації з заповненого контейнеру.

Крок 1. Виділити колірну складову I' ЦЗ розміром $M \times N$, яка містить додаткову інформацію.

Крок 2. Обрану колірну складову ЦЗ I' розміром $M \times N$ розбити на блоки B' розміром 2×2, що не перетинаються.

Для кожного блоку $B^{'}$ (кроки 3-6):

Крок 3. Виконати швидке перетворення Фур'є. Результат - $B^{F}{}^{'}$.

Крок 4. Обчислити $d^{'} = \left| B_{1,2}^{F}{}' - B_{2,1}^{F}{}' \right|$.

Крок 5. Якщо $d' \geq \left\lfloor \frac{d'}{2^{l+1}} \right\rfloor \cdot 2^{l+1}$, то $b' = \frac{d' - \left\lfloor \frac{d'}{2^{l+1}} \right\rfloor \cdot 2^{l+1}}{2}$, інакше $b^{'} = \frac{d^{'}}{2}$.

Крок 6. Перевести значення b' в двійкову систему числення довжиною l біт. Додати отримане значення до бінарної послідовності $AI^{'}$.

Крок 7. З бінарної послідовності $AI^{'}$ сформувати вилучене повідомлення.

2.2 Оцінка ефективності розробленого стеганографічного методу

Ефективність розробленого стеганографічного методу будемо оцінювати на основі наступних показників:

– PSNR, що визначає якість заповненого контейнеру у порівнянні з оригінальним ЦЗ;

– NCC [47], що визначає точність вилучення вбудованого повідомлення;

– пропускної спроможності прихованого каналу зв’язку.

Пропускна спроможність прихованого каналу зв’язку розраховується як число біт вбудованого повідомлення на один елемент контейнера. Для запропонованого методу максимальна ємність колірної складової I розміром $M \times N$ оцінюється як

$$v = \left\lfloor \frac{M}{2} \right\rfloor \cdot \left\lfloor \frac{N}{2} \right\rfloor \cdot l,$$

де l - число біт повідомлення, вбудованих в один блок 2×2 ЦЗ.

Пропускна спроможність обчислюється за формулою:

$$capacity = \frac{v}{MN}$$

Відповідно, вбудовуючи 4 біти повідомлення в кожний блок пропускна спроможність буде становити 1 біт/піксель, а при вбудові 3 біт повідомлення – 0,75 біт/піксель. Порівнюючи пропускну спроможність з роботами [41, 45], в яких пропускна спроможність складає 0,7 і 0,25 біт/піксель відповідно), розроблений метод забезпечує високу пропускну спроможність прихованого каналу зв’язку.

Для оцінки якості стеганоповідомлень та якості вилучення додаткової інформації був проведений обчислювальний експеримент на основі 200 цифрових зображень різного розміру. В якості вбудованого повідомлення в експерименті були використані напівтонові ЦЗ. В таблиці 2.1 наведені середні значення показників PSNR та NCC, а також максимальні і мінімальні значення NCC для наступних випадків:

– в кожний блок синьої колірної складової відбувалась вбудова 4-х біт повідомлення (експеримент 1);

– в кожний блок синьої колірної складової відбувалась вбудова 3-х біт повідомлення (експеримент 2);

– в кожний блок зеленої колірної складової відбувалась вбудова 3-х біт повідомлення (експеримент 3).

У всіх трьох експериментах заповнені контейнери були збережені без втрат.

Таблиця 2.1 – Ефективність вилучення додаткової інформації із заповненого контейнеру

	Середнє значення PSNR, дБ	Середнє значення NCC	Максимальне значення NCC	Мінімальне значення NCC
Експеримент 1	58,633282	0,87922645	0,99989	0,2648
Експеримент 2	60,076282	0,9373597	0,9996	0,41737
Експеримент 3	60,024235	0,9721804	0,99994	0,80379

З таблиці 2.1 видно, що при забезпеченні високої пропускної спроможності прихованого каналу зв'язку (1 і 0,75 біт/піксель) забезпечуються високі показники PSNR порівняння оригінального контейнеру і отриманого стеганоповідомлення – середні значення становлять від 58 до 60 дБ. Однак точність вилучення додаткової інформації при використанні синьої колірної складової контейнеру недостатньо висока – середні значення показника NCC становлять 0,87-0,94 через наявність таких стеганоповідомлень, з яких вилучена ДІ дуже відрізняється від вбудованої, про що свідчать дуже низькі мінімальні значення NCC в експериментах 1 і 2. При вбудові 4-х біт в кожний блок погане вилучення повідомлення (NCC менше 0,7) відбувалося в 12,5% заповнених контейнерів, зменшення кількості біт дозволило зменшити долю стеганоповідомлень з поганим вилученням інформації до 5%.

Аналіз причин некоректного вилучення повідомлення показав, що синя колірна складова містить багато блоків зі значеннями яскравості, близьких до 0 та 255, набагато більше, ніж в червоній і зеленій колірних складових. Модифікація коефіцієнтів Фур'є таких блоків призводить до того, що в

результаті оберненого перетворення Фур'є ми отримуємо значення яскравостей, менших нуля або більших 255, що призводить до округлень до граничних значень – 0 або 255. В результаті при вилученні інформації виникають помилки. Нижче наведено приклад некоректного вилучення додаткової інформації:

$$\begin{pmatrix}4 & 0\\ 1 & 1\end{pmatrix} \xrightarrow{fft2} \begin{pmatrix}6 & 4\\ 2 & 4\end{pmatrix} \xrightarrow{\textit{вбудова } 3=011_2} \begin{pmatrix}6 & 6\\ 0 & 4\end{pmatrix} \xrightarrow{ifft2} \begin{pmatrix}4 & -1\\ 2 & 1\end{pmatrix} \rightarrow \begin{pmatrix}4 & 0\\ 2 & 1\end{pmatrix},$$

$$\begin{pmatrix}4 & 0\\ 2 & 1\end{pmatrix} \xrightarrow{fft2} \begin{pmatrix}7 & 5\\ 1 & 3\end{pmatrix} \xrightarrow{\textit{вилучення}} |5-1| = 4 \rightarrow \frac{4}{2} = 2 = 010_2$$

Для порівняння ефективності вилучення повідомлення, вбудованого в іншу колірну складову, був проведений експеримент вбудови 3-х біт додаткової інформації в кожний блок зеленої колірної складової ЦЗ (експеримент 3). В таблиці 2.1 видно, що результати вилучення повідомлення в експерименті 3 набагато краще результатів експерименту 2 – середнє значення NCC становить 0,97, а мінімальне – 0,8. Тому для забезпечення високої точності вилучення додаткової інформації рекомендується проводити аналіз матриць ЦЗ та обирати ту з них, яка містить найменшу кількість блоків зі значеннями, близькими до 0 або 255.

Для оцінки стійкості запропонованого методу до атак зашумленням був проведений обчислювальний експеримент, результати якого наведені в таблиці 2.2.

Таблиця 2.2 – Ефективність вилучення додаткової інформації із заповненого контейнеру після атак

Атака	Параметри	Середнє значення PSNR, дБ	Середнє значення NCC	Максимальне значення NCC	Мінімальне значення NCC
Експеримент 1					

Продовження таблиці 2.2

Атака	Параметри	Середнє значення PSNR, дБ	Середнє значення NCC	Максимальне значення NCC	Мінімальне значення NCC
Гаусів шум	$m = 0$, $d = 0.00001$	48,86962	0,344633	0,44853	0,061157
	$m = 0$, $d = 0.000001$	56,36327	0,802141	0,91876	0,24327
Мультиплікативний шум	$d = 0.00005$	49,40806	0,539976	0,98263	0,093479
	$d = 0.000006$	55,32855	0,787686	0,99989	0,18039
	$d = 0.000001$	58,63328	0,879226	0,99989	0,2648
Шум «Сіль та перець»	$d = 0.01$	24,6721	0,861752	0,97989	0,25954
	$d = 0.005$	26,582	0,870476	0,9901	0,26237
Експеримент 2					
Гаусів шум	$m = 0$, $d = 0.00001$	49,14321	0,288482	0,33804	0,19205
	$m = 0$, $d = 0.000001$	57,49274	0,841496	0,89902	0,38408
Мультиплікативний шум	$d = 0.00005$	49,03103	0,476161	0,88556	0,16396
	$d = 0.000006$	56,01979	0,810879	0,9982	0,29988
	$d = 0.000001$	60,07628	0,93736	0,9996	0,41737
Шум «Сіль та перець»	$d = 0.01$	24,92572	0,918699	0,98018	0,40956
	$d = 0.005$	27,93963	0,928015	0,99017	0,41289
Експеримент 3					
Гаусів шум	$m = 0$, $d = 0.00001$	49,13999	0,296112	0,34005	0,24478
	$m = 0$, $d = 0.000001$	57,46723	0,872095	0,90179	0,72341

Продовження таблиці 2.2

Атака	Параметри	Середнє значення PSNR, дБ	Середнє значення NCC	Максимальне значення NCC	Мінімальне значення NCC
Мультиплі-кативний шум	$d = 0.00005$	49,02722	0,417405	0,90854	0,17678
	$d = 0.000006$	56,00131	0,823811	0,99655	0,49959
	$d = 0.000001$	60,02424	0,97218	0,99994	0,80379
Шум «Сіль та перець»	$d = 0.01$	24,92548	0,952747	0,97987	0,78745
	$d = 0.005$	27,93351	0,962455	0,99	0,79591

З таблиці 2.2 видно, що найгірші результати вилучення повідомлення спостерігаються при помітному зашумленні Гаусовим і мультиплікативним шумами ($m = 0, d = 0.00001$ і $d = 0.00005$ відповідно) – у всіх експериментах спостерігаються низькі значення показника NCC, однак при менших спотвореннях стеганоповідомлення забезпечується досить висока якість вилучення додаткової інформації – середні значення NCC дорівнюють від 0,78 до 0,94. Окремо слід відзначити стійкість запропонованого методу до атаки шумом «Сіль та перець» - навіть при великих спотвореннях заповненого контейнеру (про що свідчать низькі значення PSNR від 24 до 27 дБ) точність вилучення повідомлення з синьої колірної складової при різних значеннях пропускної спроможності становить від 0,86 до 0,93, а при вилученні з зеленої колірної матриці – 0,95-0,96.

На рисунках 2.5 і 2.6 наведені приклади вбудови додаткової інформації (рисунок 2.6, а) в зелену колірну складову контейнеру (рисунок 2.5, а) з пропускною спроможністю 0,75 біт/піксель, а також результатів вилучення повідомлень (рисунок 2.6, б, в) з заповнених контейнерів (рисунок 2.5, б, в). Стеганоповідомлення, наведене на рисунку 2.5, в, зазнало атаки шумом «Сіль та перець» з дисперсією $d = 0.03$, що призвело до помітних спотворень

зображення, однак секретна інформація вилучена з нього з високою точністю (рисунок 2.6, в), хоч і має деякі завади у вигляді чорних і білих точок.

а б в

Рисунок 2.5 –Результати вбудови додаткової інформації: а – контейнер; б – стеганоповідомлення, сформоване вбудовою повідомлення в зелену колірну складову (PSNR=58,5642 дБ); в – стеганоповідомлення, сформоване вбудовою повідомлення в зелену колірну складову, після атаки шумом «Сіль та перець» при $d = 0.03$ (PSNR=20,4152 дБ)

а б в

Рисунок 2.6 –Результати вилучення додаткової інформації: а – оригінальна ДІ; б – повідомлення, вилучене з заповненого контейнеру без атак (NCC=0,98757); в – повідомлення, вилучене з заповненого контейнеру після атаки шумом «Сіль та перець» (NCC=0,92871)

2.3 Порівняння розробленого стеганографічного методу з аналогами

Для порівняння ефективності запропонованого стеганографічного методу з сучасними аналогами обрано сучасні методи на основі перетворення Фур'є. Результати методу [41] наводяться для кольорових зображень, роботи [45, 48] аналізують зображення в градаціях сірого, причому в [48] для аналізу візуальної якості автори використовують стандартні зображення розміром 512×512. В роботі [45] відомості про розмір і ємність контейнеру відсутні, однак з розрахунку вбудови одного біту в блок 2×2 ППС становить 0,25 біт/піксель. В таблиці 2.3 наведено порівняння запропонованого методу з аналогами.

Таблиця 2.3 – Порівняння запропонованого методу з сучасними аналогами

Стеганографічний метод	ППС, біт/піксель	Ємність контейнеру, байт	Розмір контейнеру	PSNR, дБ
На основі контейнеру в градаціях сірого				
SCDFT [48] 2008	0,1172*	3840	512×512	30,1024
QFT [48] 2008	0,1172*	3840	512×512	30,9283

Продовження таблиці 2.3

IATFDDFT [42] 2010	0,75	24576	512×512	37,536
[45] 2014	0,25	8192**	512×512	42
Запропонований метод	1	32768	512×512	43,0097
	0,75	24576	512×512	47,1934
На основі кольорових контейнерів				
[41] 2018	0,71*	125952	1419×1001	43,6913
Запропонований метод	1	177500	1420×1000	45,8848
	0,75	133125	1420×1000	51,7182

* ППС розрахована за даними, наведеними в роботах [41,48]

** Ємність контейнеру розрахована для розміру 512×512

Як видно з таблиці 2.3 при забезпеченні високої пропускної спроможності досягаються високі значення PSNR, які перевищують значення сучасних аналогів.

В ході проведених обчислювальних експериментів встановлено, що в більшості випадків забезпечується висока точність вилучення додаткової інформації (в 88% заповнених контейнерів з усіх експериментів показник NCC перевищує значення 0,9), однак при використанні синьої колірної складової спостерігаються досить високі помилки, пов’язані з характеристиками самого контейнеру, а саме наявністю великої кількості блоків зі значеннями яскравості, близькими до 0 або 255. Мінімізувати помилки вилучення повідомлення можна шляхом вибору тієї колірної складової, яка містить якомога менше таких блоків.

3 РЕАЛІЗАЦІЯ ПРОГРАМНОГО ІНТЕРФЕЙСУ ДЛЯ РОЗРОБЛЕНОГО СТЕГАНОГРАФІЧНОГО МЕТОДУ

3.1 Структура програмного інтерфейсу

У програмі був створений стеганографічний метод для цифрових зображень на основі перетворення Фур'є.

Робота програми починається з завантаження зображення в яке буде завантажуватия ДІ.

З’явиться вікно вибору:

```
try
[number, directory] = uigetfile({'*.tif;*' });
```

Обране зображення зберігається у змінній *I* :

```
I = imread(fullfile(directory, number));
```

Якщо зображення не вибрано, програма поверне помилку:

```
catch
    sms = msgbox('Оберіть зображення');
end
```

Для зручності, зберегання даних зображення реалізовано в глобальній змінній:

```
handles.I = I;
guidata(hObject,handles);
```

Вивід зображения на экран здійснюється наступним чином:

```
axes(handles.axes1);
set(gca,'xtick',[],'ytick',[]);
imshow(I);
```

Завантаження інших зображень відбувається аналогічно.

Коли ми хочемо виконати вбудову ДІ в цифрове зображення, нам потрібно представити додаткову інформацію як бінарну послідовність:

```
b=dec2bin(br,8);
```

Виділити обрану колірну складову ЦЗ, яка буде використана для вбудови додаткової інформації:

```
container_channel_green = container(:,:,2);
pic=container_channel_green;
```

Обрану колірну складову треба розбити на блоки розміром 2×2:

```
x1=x1+4;
if(x1>container_width)
    x1=1;
    y1=y1+2;
end
y2=y1+1;
x2=x1+1;
x3=x1+2;
x4=x1+3;
```

Для кожного блоку зображення виконати швидке перетворення Фур'є:

```
F1=fft2(block1);
```

З отриманої бінарної послідовності виділити потрібну кількість біт, яка переводиться в десяткову систему числення:

```
bb1=extractBetween(b,1,4);
bb2=extractBetween(b,5,8);
b1=bin2dec(bb1);
b2=bin2dec(bb2);
```

Обчислити модуль різниці між коефіцієнтами для кожного блока:

```
d1=abs(Rs1(1,2)-Rs1(2,1));
```

Обчислення кожного блока відбувається за такою формулою:

```
k=floor(d/16);
b1=2*b+k*16;
```

Далі кожний блок обчислюється за таких умов:

```
if abs(b1-d)<abs(b-d)
    b=b1;
```

```
else
    b=2*b;
end
```

Модифікуємо значення коефіциентів:

```
m=abs(b-d);
mu=ceil(m/2);
ml=fix(m/2);
if p1>=p2 && b>d
        ps1=p1+mu;
        ps2=p2-ml;
    else
        if p1<p2 && b>d
            ps1=p1-ml;
            ps2=p2+mu;
        else
            if p1>=p2 && b<=d
                ps1=p1-mu;
                ps2=p2+ml;
            else
                ps1=p1+mu;
                ps2=p2-ml;
            end
        end
end
```

Після перетворень потрібно виконати обернене швидке перетворення Фур’є:

```
Fs2=Rs2+sqrt(-1)*I2;
Blocks1=ifft2(Fs2);
```

Зберігаємо заповнений контейнер:

```
imwrite(rgbimage,'Stegomessage\message_in_4_in_green.tif')
```

Для вилучення додаткової інформації з заповненого контейнеру потрібно виділити колірну складову ЦЗ розміром яка містить додаткову інформацію:

```
container_channel_green = container(:,:,2);
pic=container_channel_green;
```

Розбити на блоки 2×2, обрану колірну складову ЦЗ:

```
x1=x1+4;
if(x1>container_width)
    x1=1;
    y1=y1+2;
end
y2=y1+1;
x2=x1+1;
x3=x1+2;
x4=x1+3;
```

Для кожного блоку виконати швидке перетворення Фур'є:

```
Fss1=fft2(pic(x1:x2,y1:y2));
```

Обчислити модуль різниці коефіцієнтів:

```
bs1=mod(abs(Rss1(1,2)-Rss1(2,1))/2,16);
```

Кожний блок обчислюється за таких умов:

```
if bs1>d1*16
 bs1=(bs1-d1*16)/2;
else
 bs1=bs1/2;
end
```

Перевести отримане значення в двійкову систему числення та додати отримане значення до бінарної послідовності:

```
dbs1=dec2bin(bs1,4);
SM=[SM dbs1];
```

З отриманої бінарної послідовності формуємо вилучене повідомлення:

```
binare_size=strcat(dec2bin(Stego_message(1),8),dec2bi
n(Stego_message(2),8),dec2bin(Stego_message(3),8));
```

3.2 Реалізація програмного інтерфейсу

Після запуску програму з’являється вікно програми, за замовчуванням ми знаходимося в пункті меню «Погрузити інформацію» (рисунок 3.1).

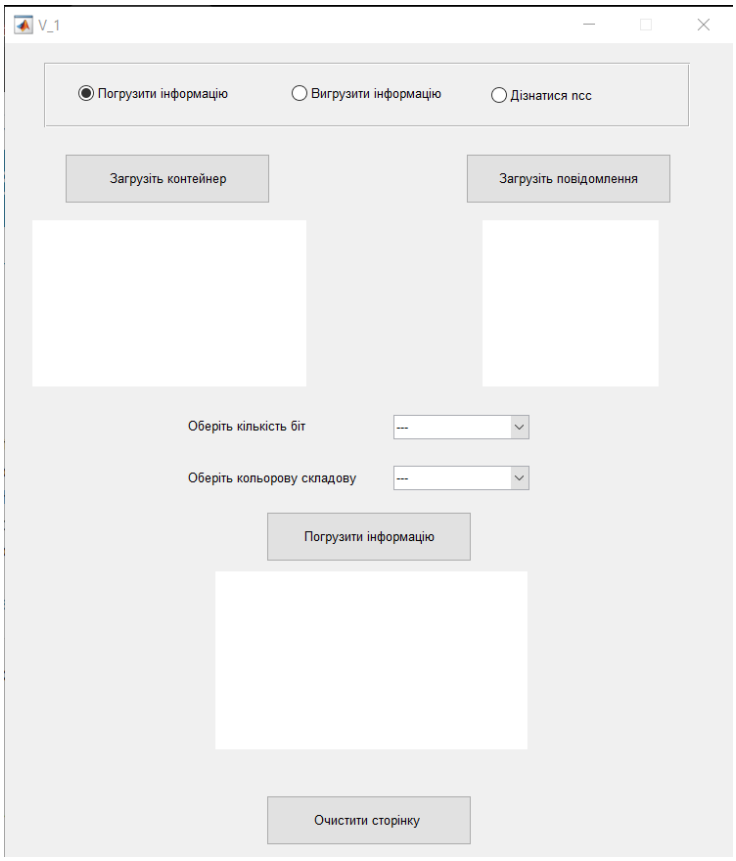

Рисунок 3.1 - Головне вікно

У вікні програми зображені пункти меню:

- погрузити інформацію;
- вигрузити інформацію;
- дізнатися ncc.

Також у вікні програми зображені чотири кнопки:

– загрузіть контейнер;
– загрузіть повідомлення;
– погрузити інформацію;
– очистити сторінку.

Та панель, яка містить випадаючий список для вибору відповідних умов:

– оберіть кількість біт;
– оберіть кольорову складову.

Щоб завантажити контейнер в програму, необхідно натиснути кнопку «Загрузіть контейнер», яка відкриє вікно вибору, де ми можемо вибрати потрібне зображення (рисунок 3.2).

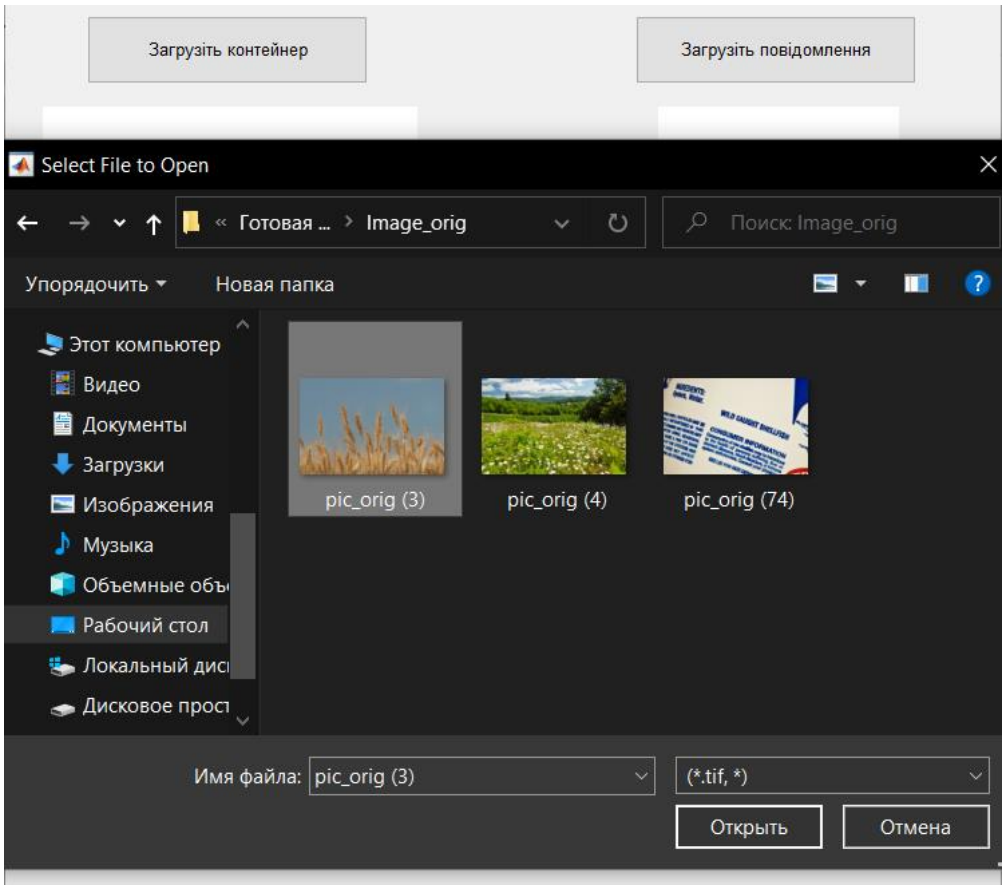

Рисунок 3.2 - Вікно вибору зображення

Коли зображення буде вибрано, воно буде завантажено та відображено на екрані (рисунок 3.3).

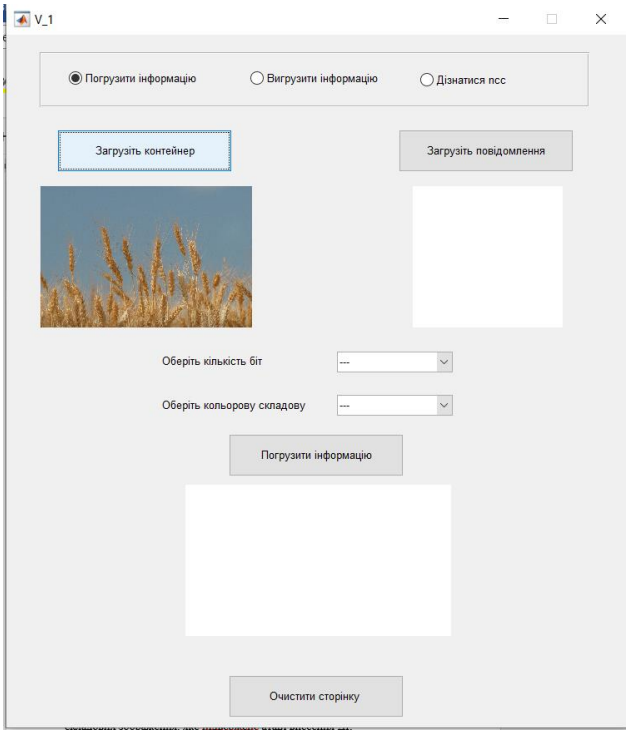

Рисунок 3.3 – Відображення зображення на екрані

Щоб завантажити повідомлення в програму, необхідно натиснути кнопку «Загрузіть повідомлення», яка відкриє вікно вибору, де ми можемо вибрати потрібне зображення (рисунок 3.4).

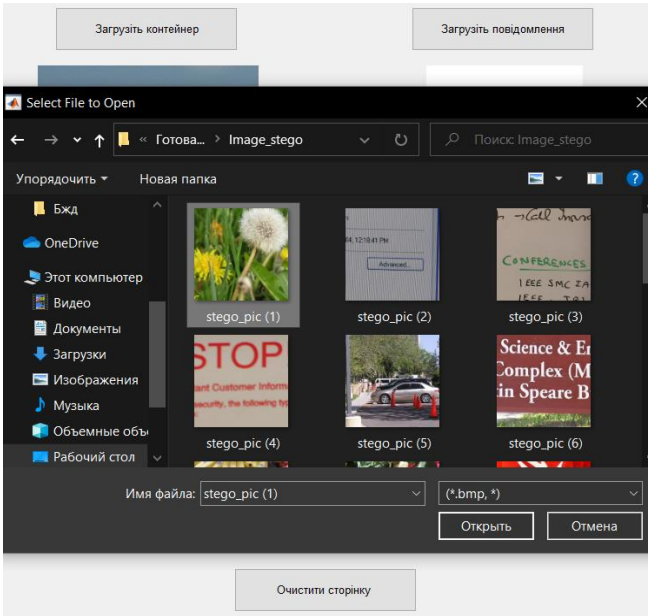

Рисунок 3.4 - Вікно вибору зображення

Коли зображення буде вибрано, воно буде завантажено та відображено на екрані (рисунок 3.5).

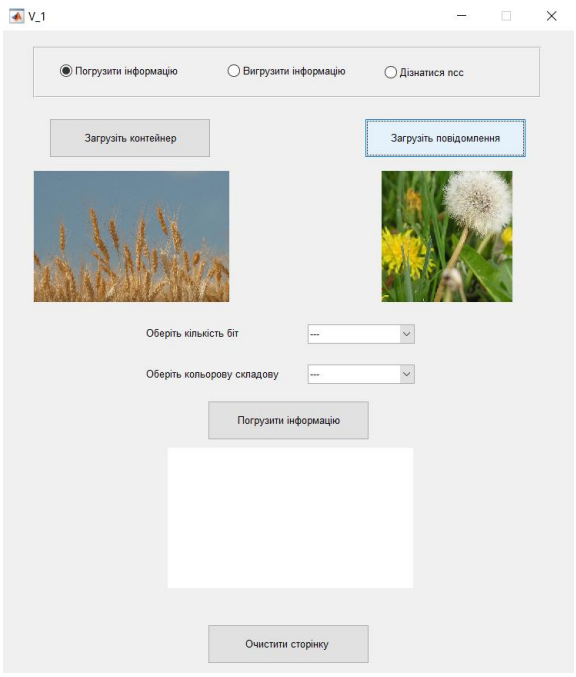

Рисунок 3.5 - Відображення зображення на екрані

Обираемо параметри погруження ДІ за допомогою панелі яка мітить спливаюче меню (рисунок 3.6-3.7).

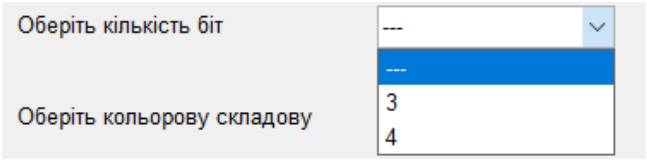

Рисунок 3.6 – Вибір параметрів у спливаючему вікні

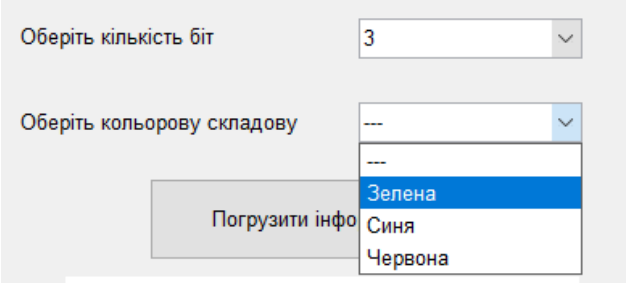

Рисунок 3.7 - Вибір параметрів у спливаючему вікні

Коли зображення відображені в програмі та обрані необхідні параметри ми можемо запустити реалізацію стеганографічного методу, щоб погрузити ДІ в контейнер натиснувши кнопку натиснувши кнопку «Погрузити інформацію», після обробки, програма покаже отримане стеганоповідомлення, та надасть нам інформацію про оцінку якості PSNR (рисунок 3.8).

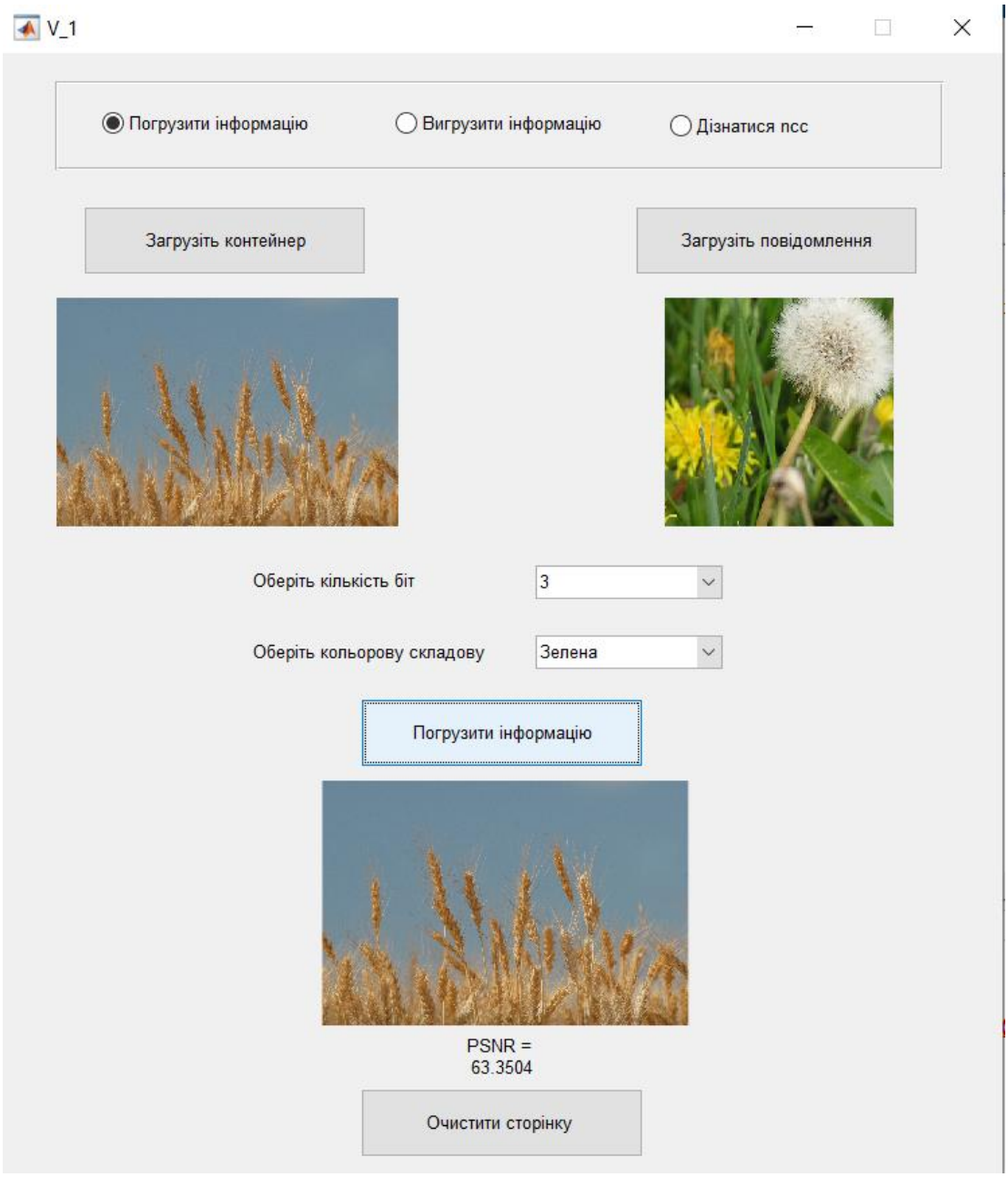

Рисунок 3.8 – Отримані результати

В пункті меню «Вигрузити інформацію» користувач може вигрузути інформацію з стеганоповідомлення(рисунок 3.9).

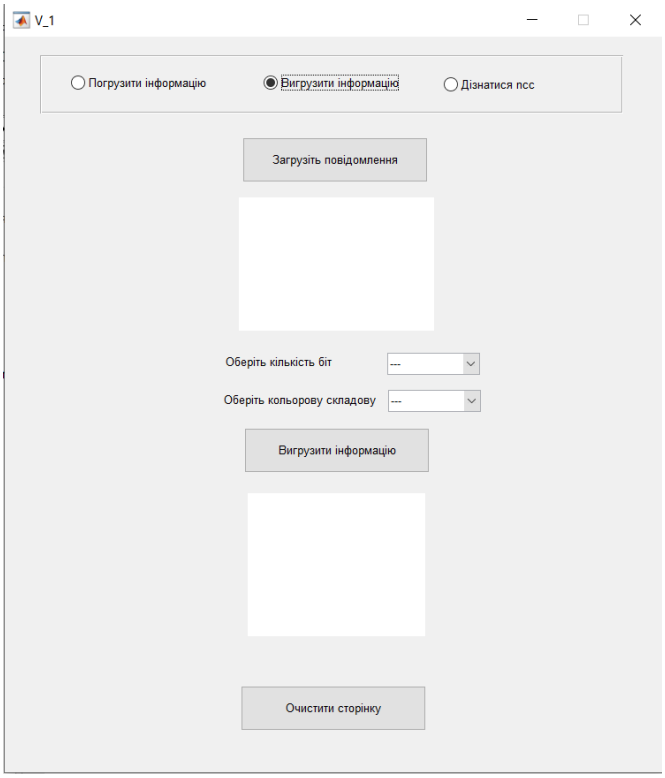

Рисунок 3.9 - Вікно пункта меню «Вигрузити інформацію»

Щоб завантажити стеганоповідомлення в програму, необхідно натиснути кнопку «Загрузіть повідомлення», яка відкриє вікно вибору, де ми можемо вибрати потрібне зображення (рисунок 3.10).

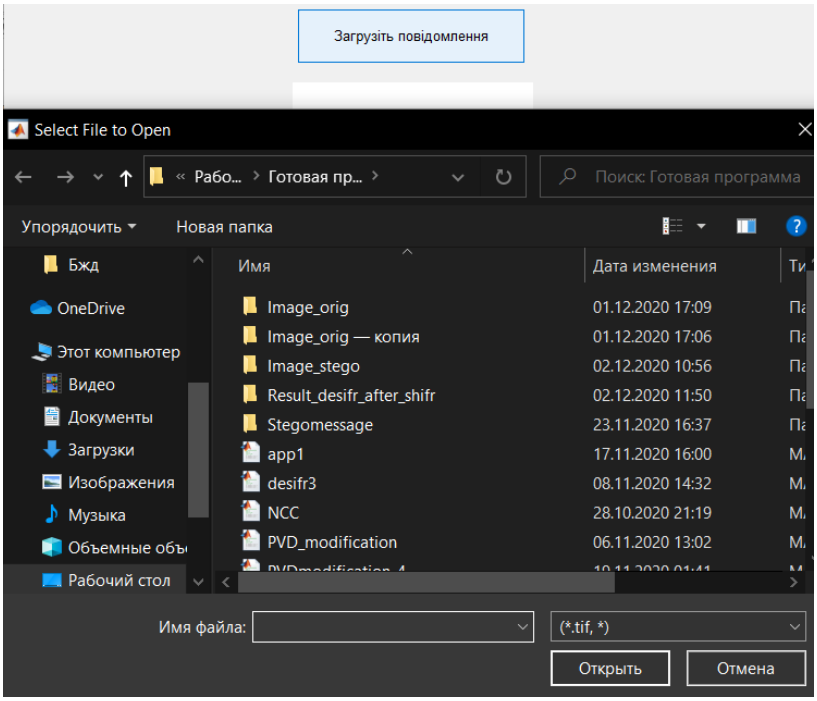

Рисунок 3.10 - Вікно вибору зображення

Коли зображення буде вибрано, воно буде завантажено та відображено на екрані (рисунок 3.11).

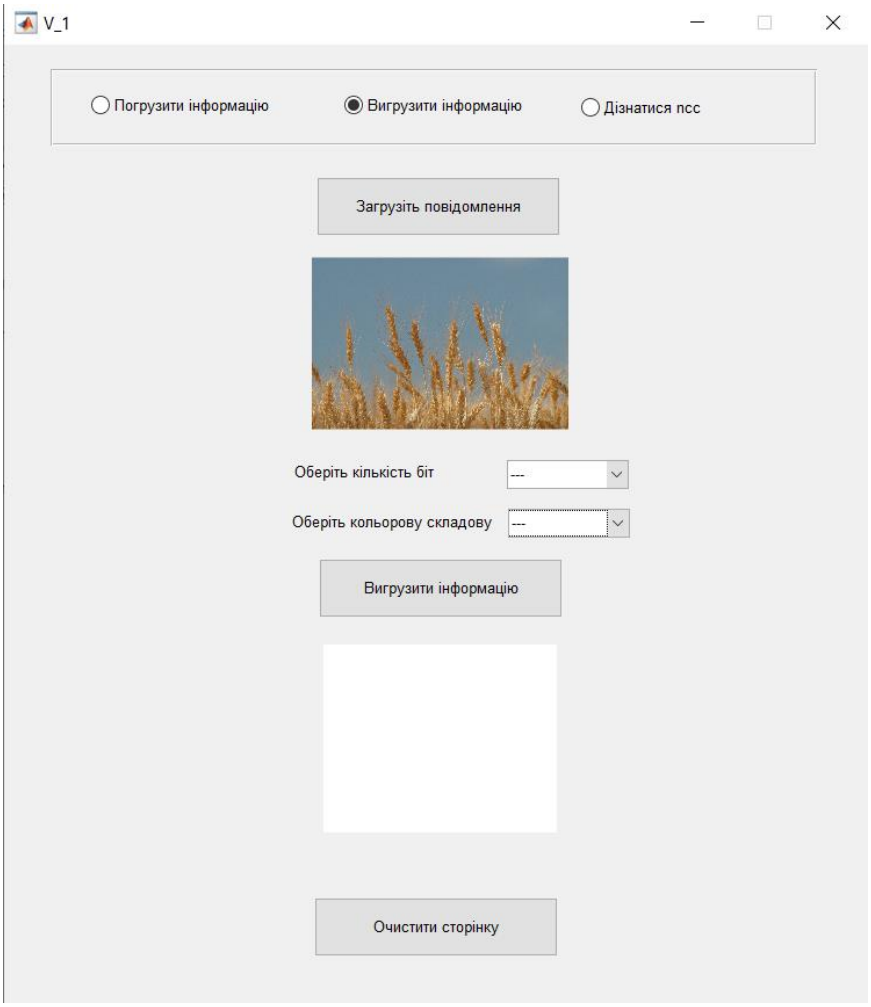

Рисунок 3.11 - Відображення зображення на екрані

Обираемо параметри вигруження ДІ за допомогою панелі яка мітить спливаюче меню (рисунок 3.12-3.13).

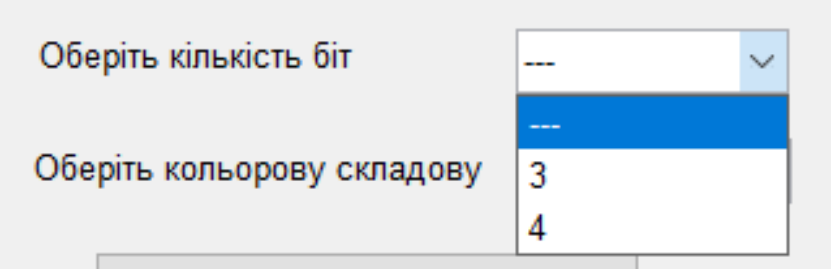

Рисунок 3.12 - Вибір параметрів у вспливаючему вікні

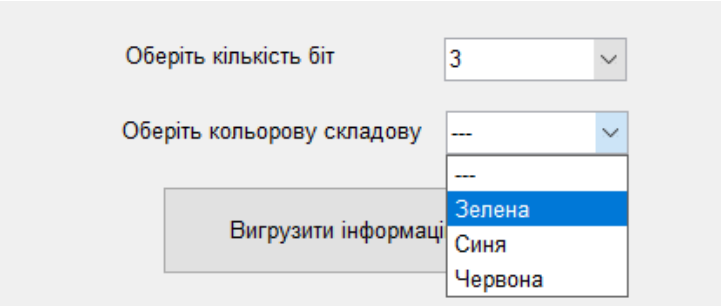

Рисунок 3.13 - Вибір параметрів у вспливаючему вікні

Коли зображення відображені в програмі та обрані необхідні параметри ми можемо запустити реалізацію стеганографічного методу, щоб погрузити ДІ в контейнер натиснувши кнопку «Вигрузити інформацію», після обробки програма покаже вигружену додаткову інформацію (рисунок 3.14).

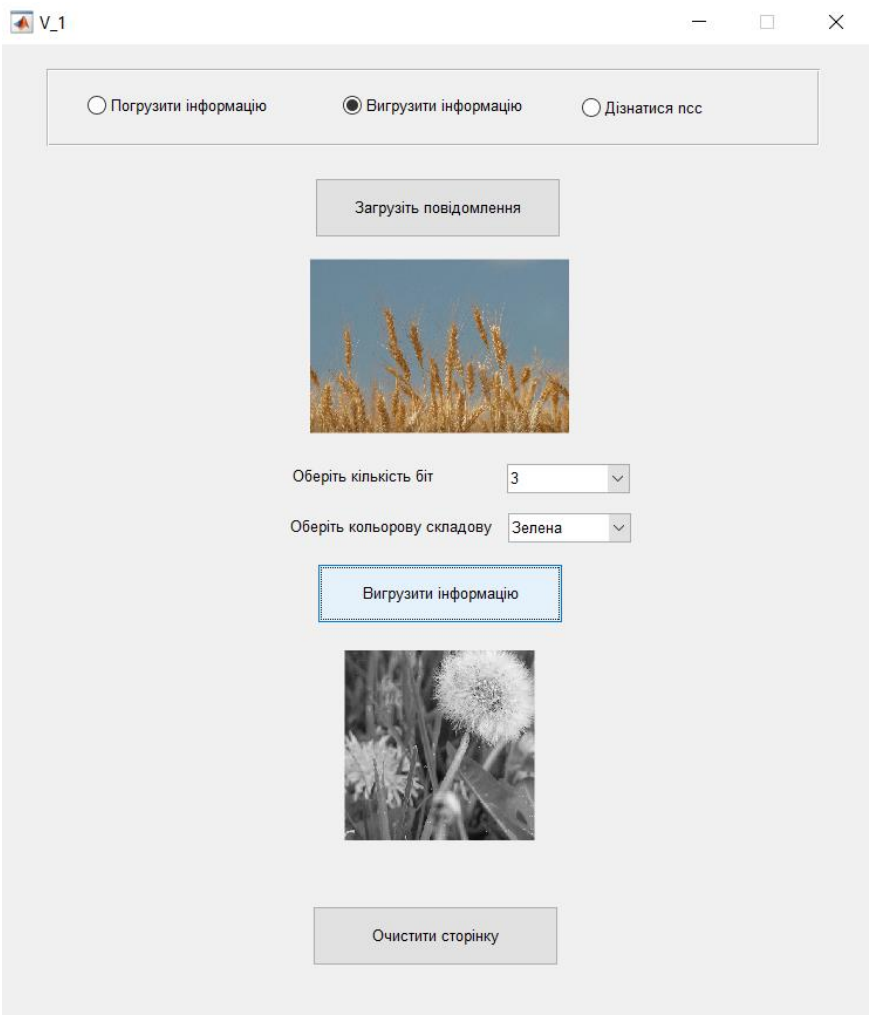

Рисунок 3.14 - Отримані результати

В пункті меню «Дізнатися ncc» корстувач може дізнатися параметр «ncc» (рисунок 3.15).

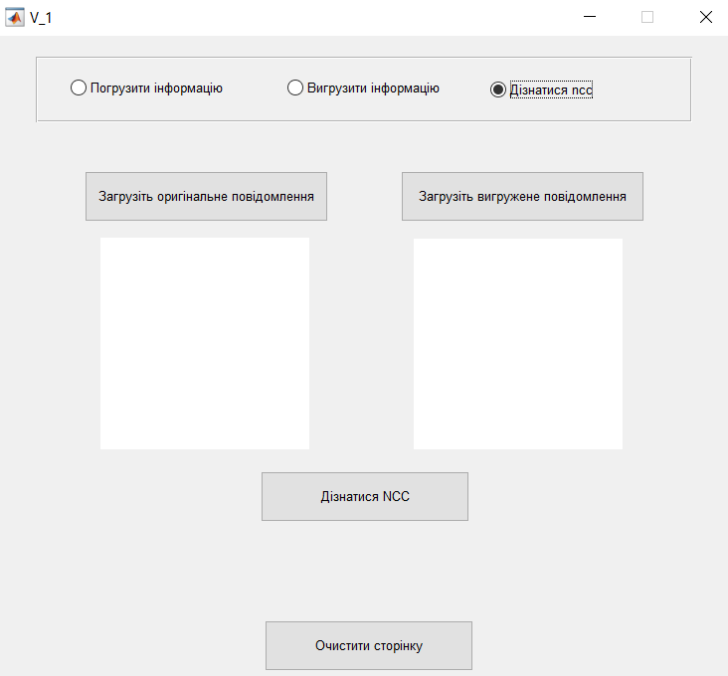

Рисунок 3.15 - Вікно пункта меню «Дізнатися ncc»

Щоб завантажити додаткову інформацію, треба натиснути кнопку «Загрузіть оригінальне повідомлення», яка відкриє вікно вибору, де ми можемо вибрати потрібне зображення (рисунок 3.16).

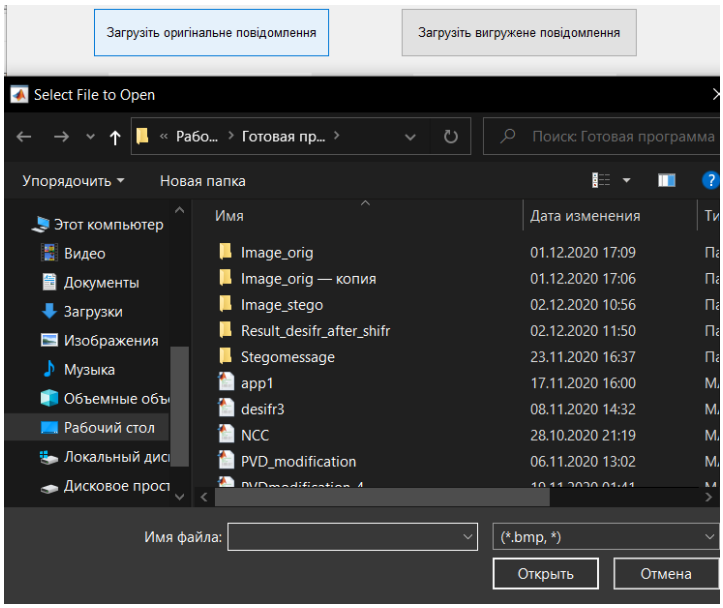

Рисунок 3.16 - Вікно вибору зображення

Щоб завантажити вигружену додаткову інформацію, треба натиснути кнопку «Загрузіть вигружене повідомлення», яка відкриє вікно вибору, де ми можемо вибрати потрібне зображення (рисунок 3.17).

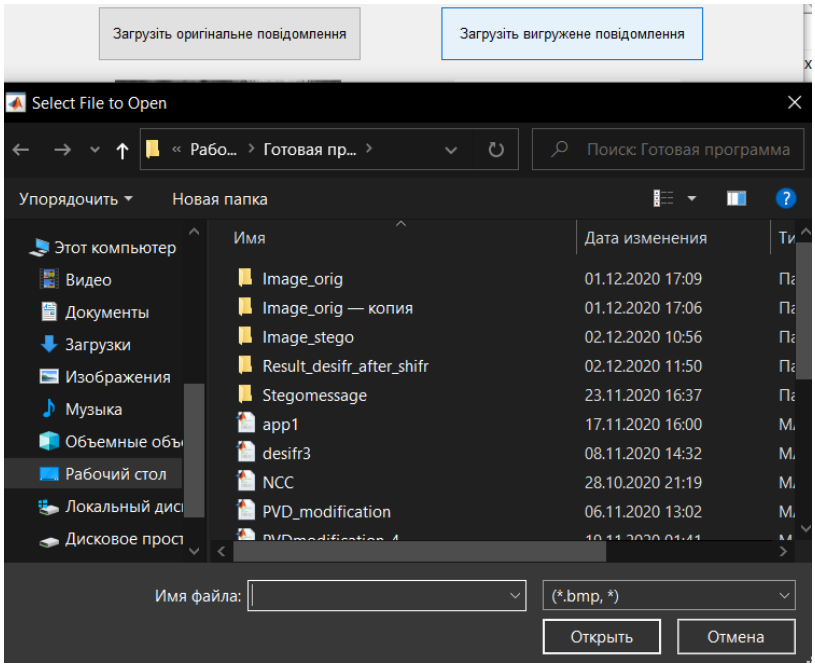

Рисунок 3.17 - Вікно вибору зображення

Коли зображення будуть вибрані, вони будуть завантажені та відображені на екрані (рисунок 3.18).

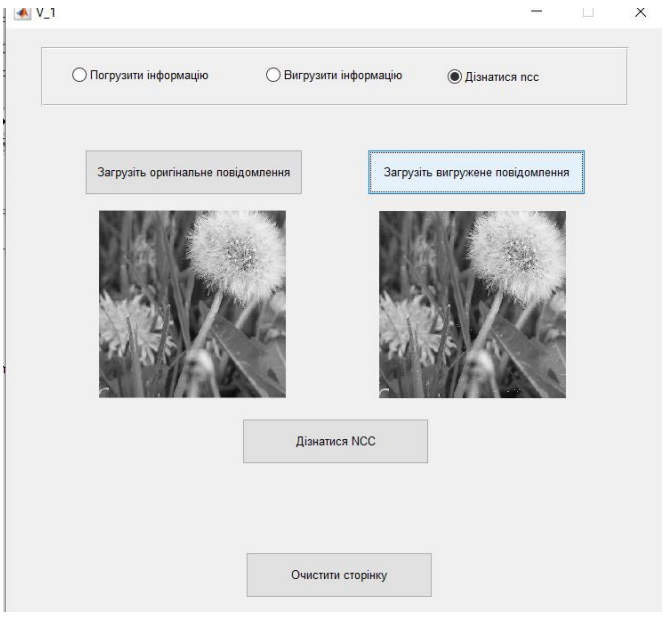

Рисунок 3.18 – Відображення зображеннь на ектрані

Коли зображення відображені в програмі ми можемо запустити реалізацію стеганографічного методу, щоб дізнатися параметр натиснувши кнопку «Дізнатися NCC», після обробки програма надасть нам інформацію про оцінку якості NCC (рисунок 3.19),

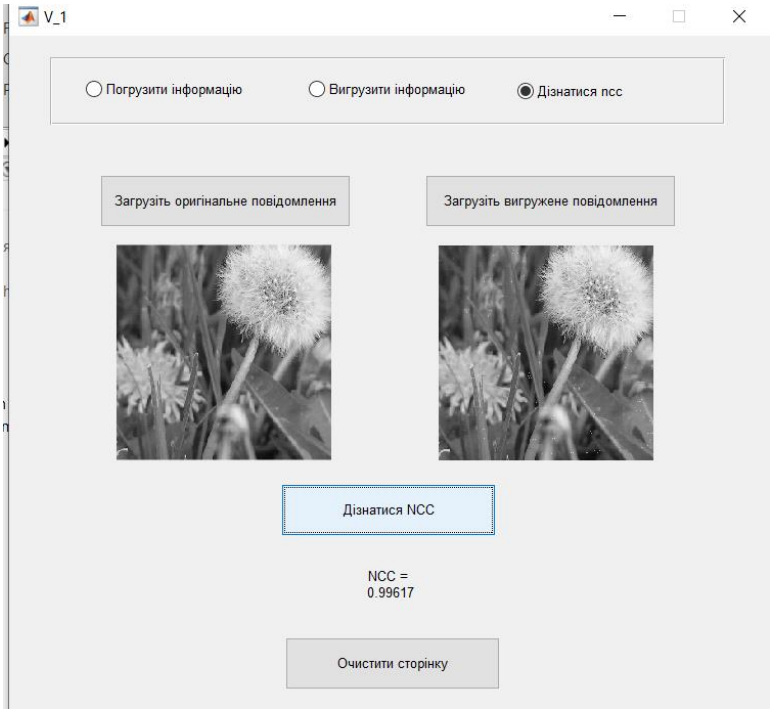

Рисунок 3.19 – Отримані результати

В даному розділі були описані основні моменти реалізації розробленого стеганографічного методу для цифрових зображень на основі перетворення Фур'є. Створена детальна інструкція для зручного користування інтерфейсом програми для користувача.

ВИСНОВКИ

В роботі запропонований новий стеганографічний метод для цифрових зображень на основі швидкого перетворення Фур'є. Вбудова додаткової інформації відбувається в блоки шляхом модифікації різниці між двома коефіцієнтами перетворення Фур'є. В кожний блок можна вбудувати до чотирьох біт повідомлення, що дозволяє забезпечити високу пропускну спроможність прихованого каналу зв'язку при збереженні високої якості стеганоповідомлення (середнє значення PSNR становить 58-60 дБ).

В ході проведених обчислювальних експериментів встановлено, що в більшості випадків забезпечується висока точність вилучення додаткової інформації (в 88% заповнених контейнерів з усіх експериментів показник NCC перевищує значення 0,9), однак при використанні синьої колірної складової спостерігаються досить високі помилки, пов'язані з характеристиками самого контейнеру, а саме наявністю великої кількості блоків зі значеннями яскравості, близькими до 0 або 255. Мінімізувати помилки вилучення повідомлення можна шляхом вибору тієї колірної складової, яка містить якомога менше таких блоків.

Експерименти, спрямовані на аналіз стійкості до атак, зокрема зашумлення, показали високу стійкість до шуму «Сіль та перець», а також до Гаусового та мультиплікативних шумів при незначних спотвореннях стеганоповідомлень.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ахмаметьєва, Г.В. Розробка стеганографічного методу для цифрових зображень на основі перетворення Фур'є / Г.В. Ахмаметьєва, М.Д. Безсонова // *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. – 2020. – №69. – С.
2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации. Белорусский государственный технологический университет, Минск, 2016, 220 с.
3. Kurane S., Harke H., and Kulkarni S., Text and audio data hiding using LSB and DCT a review approach. *Internet of Things: Towards a Smart Future» & «Recent Trends in Electronics & Communication*. Materials National Conference, 17-18 February 2016. India, Pune, 2016.
4. Mishra S., Yadav V. K., Trivedi M.C. Shrimali T. Audio Steganography Techniques: A Survey. *Advances in Computer and Computational Sciences* January, 29 September 2017, Springer, Singapore. P. 581-589
5. Моденова О. В. Стеганография и стегоанализ в видеофайлах. *Прикладна Дискретна Математика. Приложение*. 2010. №3. URL: https://cyberleninka.ru/article/n/steganografiya-i-stegoanaliz-v-videofaylah
6. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. Вузовская книга, 2009. 220 с.
7. Федосєєв В. А. Теоретичні основи стеганографії та цифрових водяних знаків: навч. посібник. Самарський університет, Самара, 2017. 132 с.
8. Вильховский Д.Э. Протоколы квантовой стеганографии. *Математические структуры и моделирование*. 2020. №2 (54). С.100-128 URL: https://cyberleninka.ru/article/n/protokoly-kvantovoy-steganografii
9. Грибунин В.Г., Орков И.Н., Турницев И.В. Цифровая стеганография. М.: «Солон-Пресс», 2002. 261с.

10. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: теория и практика. Киев : МК-Пресс, 2006. 288 с.
11. Юдін О. К., Зюбіна Р.В., Фролов О.В. Аналіз стеганографічних методів приховування інформаційних потоків у контейнери різних форматів. *Радиоэлектроника и информатика.* 2015. №3. URL: https://cyberleninka.ru/article/n/analiz-steganografichnih-metodiv-prihovuvannya-informatsiynih-potokiv-u-konteyneri-riznih-formativ
12. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних. Київ: «Центр учбової літератури», 2018. 558 с.
13. Шипулин П.М., Шниперов А.Н. О возможности организации скрытых временных каналов для защиты информации в открытых компьютерных сетях. *Решетневские чтения.* 2016. №20. URL: https://cyberleninka.ru/article/n/o-vozmozhnosti-organizatsii-skrytyh-vremennyh-kanalov-dlya-zaschity-informatsii-v-otkrytyh-kompyuternyh-setyah
14. Рябинин Ю. Е., Финько О. А. Устойчивая к атакам стеганографическая система в расширенном модулярном коде. *Известия ЮФУ. Технические науки.* 2014. №2 (151). URL: https://cyberleninka.ru/article/n/ustoychivaya-k-atakam-steganograficheskaya-sistema-v-rasshirennom-modulyarnom-kode
15. Ахрамеева К.А., Коржик В.И., Нгуен З.К. Обнаружение видео стегосистем с использованием универсального метода, основанного на использовании nist-тестов. *Труды учебных заведений связи.* 2020. №1. URL: https://cyberleninka.ru/article/n/obnaruzhenie-video-stegosistem-s-ispolzovaniem-universalnogo-metoda-osnovannogo-na-ispolzovanii-nist-testov
16. Шумская О.О., Будков В.Ю. Сравнительное исследование методов классификации в стегоанализе цифровых изображений. *Научный вестник НГТУ.* Том 72, №3. С.121-134.
17. Вишневская Т.И., Уточкина Н.В. Стеганографический метод, устойчивый к повреждению данных. *Информационные технологии в науке,*

образовании и управлении. 2020. №1 (15). URL: https://cyberleninka.ru/article/n/steganograficheskiy-metod-ustoychivyy-k-povrezhdeniyu-dannyh

18. Вахаб А., Романенко Д. М. Методы цифровой стеганографии на основе модификации цветовых параметров изображения. *Труды БГТУ*. Серия 3, 2018. №1 (206). URL: https://cyberleninka.ru/article/n/metody-tsifrovoy-steganografii-na-osnove-modifikatsii-tsvetovyh-parametrov-izobrazheniya
19. Фримучков А. Н. Применение скремблирования для усложнения обнаружения скрытой информации, записанной методом LSB. *Достижения науки и образования.* 2017. №1 (14). URL: https://cyberleninka.ru/article/n/primenenie-skremblirovaniya-dlya-uslozhneniya-obnaruzheniya-skrytoy-informatsii-zapisannoy-metodom-lsb
20. Marwa M., Abdelmgeid A., Fatma A. A Modified Image Steganography Method based on LSB. Technique *International Journal of Computer Applications*. V. 125. No.5. 2015.
21. Лысенко Н. В., Лабков Г. М. Применение стеганографического алгоритма Куттера-Джордана-Боссена в видеопоследовательностях. *Известия вузов России. Радиоэлектроника.* 2015. №4. URL: https://cyberleninka.ru/article/n/primenenie-steganograficheskogo-algoritma-kuttera-dzhordana-bossena-v-videoposledovatelnostyah
22. Дизер А.Е., Дизер Е.С., Опарина Т.М. Модификация метода Куттера-Джордана-Боссена скрытого хранения информации в изображениях формата JPEG. *Матемачиские структуры и моделирование*. 2016. №3 (39). С.177-183. URL: https://cyberleninka.ru/article/n/modifikatsiya-metoda-kuttera-dzhordana-bossena-skrytogo-hraneniya-informatsii-v-izobrazheniyah-formata-jpeg
23. Фомин Д. В. Модификация метода скрытия информации Куттера - Джордана – Боссена. *Вестник Амурского государственного университета. Серия: Естественные и экономические науки*. 2014. №65. URL:

https://cyberleninka.ru/article/n/modifikatsiya-metoda-skrytiya-informatsii-kuttera-dzhordana-bossena

24. Защелкин К.В., Иващенко А.И., Иванова Е.Н. Усовершенствование метода стеганографического скрытия данных Куттера-Джордана-Боссена. *Гарантоздатність та інформаційна безпека комп'ютерних систем і мереж.* 2013. №5 (64) URL: http://nti.khai.edu:57772/csp/nauchportal/Arhiv/REKS/2013/REKS513/Zaschelk.pdf
25. Рудницький В.М., Костирка О.В. Стійке стеганоперетворення в просторовій області зображення-контейнера. *Інформатика та математичні методи в моделюванні.* 2013. Том 3, №4. С.353-360.
26. Костирка О.В., Мельник М.А., Рудницкий В.Н. Стеганопреобразование пространственной области изображения-контейнера, устойчивое к сжатию. *Сучасна спеціальна техніка*. 2014. №1 (36). С.75-84.
27. Прохожев Н.Н., Михайличенко О.В., Коробейников А.Г. Повышение устойчивости стеганоалгоритмов частотной области на основе дискретно-косинусного преобразования к внешним воздействиям. *Научно-технический вестник информационных технологий, механики и оптики.* 2009. №2(60). С.102-106.
28. Жиляков Е.Г., Балабанова Т.Н., Лихогодина Е.С., Лихолоб П.Г. Технология скрытного кодирования геоданных в снимках земной поверхности. *Экономика. Информатика.* 2016. №2 (223). URL: https://cyberleninka.ru/article/n/tehnologiya-skrytnogo-kodirovaniya-geodannyh-v-snimkah-zemnoy-poverhnosti
29. Vongurai, N.; Phimoltares, S. Frequency-based steganography using 32×32 interpolated quantization table and discrete cosine transform. *Modelling and Simulation.* Fourth International Conference on Computational Intelligence. 2012. Pp 249-253

30. Banu, T. S.; Shajeesh, K. U. Secure reversible data hiding technique on textures using double encryption. *Embedded and Communication Systems.* Proceedings of 2017 International Conference on Innovations in Information. 2017. Pp. 1-5.
31. Fan, C.H., Huang H.Y., Hsu W.H. A robust watermarking technique resistant Jpeg compression. *Journal of Information Science and Engineering.* 2011. V. 27, #1. Pp. 163–180.
32. Батура В.А., Тропченко А.Ю. Модифицированный частотный алгоритм цифрового маркирования неподвижных изображений, стойкий к компрессии JPEG. *Наука и образование. МГТУ им.Н.Э. Баумана..* 2015.№ 7. С.235-253.
33. Батура В.А., Тропченко А.Ю. Эффективность алгоритмов маркирования цифровых изображений в частотной области на основе дискретного преобразования Адамара. *Приборостроение.* 2014. №4. URL: https://cyberleninka.ru/article/n/effektivnost-algoritmov-markirovaniya-tsifrovyh-izobrazheniy-v-chastotnoy-oblasti-na-osnove-diskretnogo-preobrazovaniya-adamara
34. Батура В.А. Повышение устойчивости при JPEG-сжатии цифровых водяных знаков, встраиваемых в неподвижные изображения. *Научно-технический вестник информационных технологий, механики и оптики*. 2015. №4. URL: https://cyberleninka.ru/article/n/povyshenie-ustoychivosti-pri-jpeg-szhatii-tsifrovyh-vodyanyh-znakov-vstraivaemyh-v-nepodvizhnye-izobrazheniya
35. Arup Kumar Pal. A Steganography Scheme on JPEG Compressed Cover Image with High Embedding Capacity. *The International Arab Journal of Information Technology*. 2019. V.16. No. 1. Pp.116-124.
36. Saidi, M., Hermassi, H., Rhouma, R. New adaptive image steganography scheme based on DCT and chaotic map. *Multimedia Tools and Applications.* 2017. No. 76. Pp. 13493-13510.

37. Safwat H., Amal K., Ahmed E. A Blind High-Capacity Wavelet-Based Steganography Technique for Hiding Images into other Images. *Advances in Electrical and Computer Engineering*. 2014. V.14. No. 2. Pp.35-42.
38. Kumar, V., Kumar, D. Modified DWT based image steganography technique. *Multimedia Tools and Applications*. 2018. No. 77. – Pp.13279–13308.
39. Akter A., N. Tajnina, M. Digital image watermarking based on dwt-dct: evaluate for a new embedding algorithm. *Electronics & Vision*. International Conference on Informatics. 2014. № 10. С. 1-6.
40. Benoraira A., Benmahammed K., Boucenna N. Blind image watermarking technique based on differential embedding in DWT and DCT domains. *Journal on Advances in Signal Processing*. 2017. №55. С. 1-11.
41. Khalil M.I. Using Quaternion Fourier Transform in Steganography Systems. *International Journal of Communication Networks and Information Security.* 2018. V. 10. No. 2. Pp.425-431.
42. Nabin G., Mandal J. K. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation. 2010. November 19-20. Pp.144-150.
43. Ashish S., Jitendra J., Rakesh R. Image Steganography using Discrete Fractional Fourier Transform. International Conference on Intelligent Systems and Signal Processing. 2013. India. Pp.99-103.
44. Kozina M.O. Discrete Fourier Transform As A Basis For Steganographic Method. *Праці Одеського політехнічного університету*. 2014. Вип. 2(44). С.147-154.
45. Козина М.А. Стеганографический метод организации скрытого канала связи, осуществляющий проверку целостности передаваемой информации *Сучасна спеціальна техніка*. 2014. № 4(39). С.98-106.
46. Wu D.C. A Steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*. 2003. V. 24. Pp. 1613-1626.
47. Мельник, М.А. Методика оценки устойчивости стеганоалгоритма к сжатию. *Збірник наукових праць Військового інституту Київського*

національного університету імені Тараса Шевченка. 2013. Вип. 44. С. 121-128.

48. Tsui T. T., Zhang X.-P., Androutsos D. Color Image Watermarking Usimg Multidimensional Fourier Transfomation, IEEE Trans. on Info. Forensics and Security. , 2008. V. 3, No. Pp. 16-28.
49. ДСанПІН 3.3.2.007-98. Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин
50. ДСТУ 12.0.003-74. Опасные и вредные производственные факторы. Классификация