МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
(повне найменування факультету)

Кафедра «Інформаційної безпеки та наноелектроніки»
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)
магістра
(ступінь вищої освіти)

на тему «Аналіз зображень при стеганографічної передачі»
(назва теми)

Виконав: студент 2 курсу, групи БКз-813м
Спеціальності 125 – «Кібербезпека та захист
(код і найменування спеціальності)
інформації»

Освітня програма (спеціалізація)
Безпека інформаційних і комунікаційних систем

КУЛІКОВ
Д.О.
(ПРІЗВИЩЕ та ініціали)

Керівник КОЗІНА Г.Л.
(ПРІЗВИЩЕ та ініціали)

Рецензент МОРОЗ Г.В.
(ПРІЗВИЩЕ та ініціали)

2025
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій
Кафедра інформаційної безпеки та наноелектроніки
Ступінь вищої освіти магістр
Спеціальність 125 – «Кібербезпека та захист інформації»
(код і найменування)
Освітня програма (спеціалізація) Безпека інформаційних і комунікаційних систем
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
Завідувач кафедри ІБтаН, к.ф.-м.н., доцент
Андрій КОРОТУН
«_____» _____20___року

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

КУЛІКОВА Дениса Олександровича
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) «Аналіз зображень при стеганографічної передачі»
Керівник проєкту (роботи) кандидат фіз.-мат. наук, доцент КОЗІНА Галина Леонидівна,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «05» грудня 2024 року №507

2. Строк подання студентом проєкту (роботи) «21» січня 2025 року

3. Вихідні дані до проєкту (роботи) алгоритм Дея, передача секретного цільового зображення набір контейнерів для передачі, статистичні розрахункові показники викривлення зображення

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) специфіка стеганографічної передачі зображення, методи приховування зображення, характеристики цифрових зображень, дослідження алгоритму Дея, порівняння результатів вбудовування зображення, аналіз статистичних показників викривлення зображення.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація PowerPoint (16 слайдів)

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
Основні розділи	Козіна Г.Л., доцент		
Нормоконтроль	Корольков Р.Ю., доцент		

7. Дата видачі завдання «_____» _____2024 року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Приміпка
1	Складання та затвердження завдання на дипломний проект	05.12-07.12.2024	Виконано
2	Пошук літературних джерел	08.12-10.12.2024	Виконано
3	Ознайомлення з принципом роботи алгоритму Дея	11.12-12.12.2024	Виконано
4	Проведення вбудовування цільового зображення в набір контейнерів з різними параметрами	13.12-16.12.2024	Виконано
5	Проведення розрахунків статистичних показників	17.12-19.12.2024	Виконано
6	Узагальнення результатів вбудовування та проведених розрахунків	20.12-21.12.2024	Виконано
7	Оформлення пояснювальної записки	22.12-29.12.2024	Виконано

Студент(ка) _____ Денис КУЛІКОВ
(підпис) (Ім'я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ Галина КОЗІНА

(підпис) (Ім’я ПРІЗВИЩЕ)

АНОТАЦІЯ

Пояснювальна записка до магістерської роботи: 67 с., 12 табл., 5 рис., 11 джерел.

АЛГОРИТМ ДЕЯ, СТЕГОКОНТЕЙНЕР, АЛЬФА ЗМІШУВАННЯ, ДИСКРЕТНЕ КОСИНУСНЕ ПЕРЕТВОРЕННЯ

Об'єкт дослідження – алгоритм Дея.

Предмет дослідження – стеганографічна передача цифрових зображень за допомогою алгоритму Дея.

Мета роботи – дослідження алгоритму Дея для обробки цифрових зображень у контексті стеганографічної передачі даних, а також оцінка його ефективності у приховуванні та виявленні прихованої інформації.

В процесі роботи обрано найбільш підходящій контейнер, який найкраще приховує цільове зображення при його передачі, забезпечуючи достатню якість витягнутого зображення.

Метод дослідження – у роботі використовуються методи цифрової обробки зображень, стеганографічного аналізу, математичного моделювання та експериментального дослідження. Для реалізації алгоритму використовуються сучасні програмні середовища, зокрема MathCad та Excel.

ABSTRACT

Explanatory note to the master's thesis: 67 p., 12 tables, 5 figures, 11 sources.

DEY ALGORITHM, STEGO-CONTAINER, ALPHA BLENDING, DISCRETE COSINE TRANSFORM

The object of research is the Dey algorithm.

The subject of the research is the steganographic transmission of digital images using the Dey algorithm.

The aim of the work is to investigate the Dey algorithm for processing digital images in the context of steganographic data transmission, as well as to evaluate its effectiveness in hiding and detecting hidden information.

In the course of the work, the most suitable container was chosen, which best conceals the target image during its transmission, ensuring sufficient quality of the extracted image.

Research Method – The work utilizes methods of digital image processing, steganographic analysis, mathematical modeling, and experimental research. Modern software environments, such as MathCad and Excel, are used to implement the algorithm.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

C – порожній контейнер;

S – стегоконтейнер;

T – оригінальне цільове зображення;

V – витягнуте цільове зображення;

DCT (Discrete Cosine Transform) – дискретне косинусне перетворення;

LSB (Least Significant Bit) – метод найменш значущого біта;

DWT (Discrete Wavelet Transform) – метод хвильового перетворення.

ВСТУП

Сучасні інформаційні технології стрімко розвиваються, створюючи нові можливості для передачі та збереження даних. Одним із важливих напрямків є стеганографія — методика приховування інформації у цифрових носіях, таких як зображення, аудіо чи відео. В умовах зростаючих вимог до конфіденційності та безпеки стеганографія отримує особливу увагу як інструмент захисту даних. Проте з розвитком методів приховування інформації вдосконалюються й технології її виявлення. У цьому контексті аналіз ефективності стеганографічних алгоритмів є критично важливим завданням.

Алгоритм Дея, як один із поширених підходів до аналізу зображень, набув популярності завдяки своїй здатності виявляти приховані зміни в цифрових медіа. Його використання в стеганографічному аналізі дозволяє підвищити точність виявлення прихованих повідомлень, що особливо важливо для протидії несанкціонованому використанню стеганографії в кібербезпеці.

Актуальність теми обумовлена поширеним використанням стеганографії, яка часто використовується як для легальних цілей (наприклад, захист авторських прав), так і для несанкціонованої діяльності. У таких умовах ефективний аналіз зображень для виявлення прихованої інформації стає ключовим завданням у сфері інформаційної безпеки. Алгоритм Дея, будучи потужним інструментом для аналізу цифрових зображень, надає унікальні можливості для вирішення цього завдання. Вивчення його ефективності та застосування у стеганографічному аналізі дозволяє значно покращити методи виявлення прихованих повідомлень.

Ціллю даної роботи є вибір оптимального контейнеру для якісного приховування цільового зображення за допомогою алгоритму Дея, а також щоб витягнуте цільове зображення не значно відрізнялось від оригінального.

В першій главі роботи описується стеганографія як наука, визначаються її цілі та принципи. Описується цифрова стеганографія та методи приховування інформації у цифрових зображеннях, робиться акцент на характеристиках цих зображень. Цифрові зображення стали однією з найбільш популярних платформ для стеганографічного приховування інформації, завдяки їхній великій поширеності, доступності, великій ємності для вміщення даних та можливості мінімізувати візуальні зміни. Для стеганографії використовуються різні методи, такі як метод найменш значущого біта, метод стего-блоків, дискретне косинусне перетворення та дискретне хвильове перетворення. Кожен метод має свої переваги та недоліки, що робить їх придатними для різноманітних застосувань.

В другій главі описується принцип роботи алгоритму Дея, його використання для обробки зображень та перспективи оптимізації. Алгоритм Дея є важливим інструментом для стеганографічного приховування інформації у зображеннях. Він базується на аналізі частотних характеристик даних з використанням дискретного косинусного перетворення (DCT), перетворення Фур'є та дискретного хвильового перетворення (DWT). Основна мета алгоритму — виявлення аномальних частотних компонентів, які можуть

вказувати на наявність прихованої інформації. DCT дозволяє перетворювати сигнал з просторової області у частотну, допомагаючи виявити приховані частотні компоненти. Перетворення Фур'є дозволяє представити сигнал у вигляді суми синусоїдальних компонентів, а DWT забезпечує чудову локалізацію у просторі та частоті, що дозволяє ефективно приховувати інформацію у високочастотних піддіапазонах без помітного впливу на зображення. Метод α-змішування використовується для об'єднання двох зображень, забезпечуючи контроль якості змішування та стійкість до атак.

Загалом, оптимізація алгоритму Дея має великий потенціал, включаючи підвищення стійкості до атак, оптимізацію обчислювальних процесів, покращення якості прихованої інформації та адаптацію до нових форматів даних. Модернізація алгоритму, інтеграція з частотними та криптографічними методами, а також використання апаратного прискорення забезпечать високий рівень безпеки та конфіденційності інформації. Ці дослідження мають прикладне значення для забезпечення інформаційної безпеки, кібербезпеки, судової експертизи та захисту інтелектуальної власності.

В третій главі розглядаються результати вбудовування цільового зображення в запропоновані контейнери та робиться оцінка отриманих результатів вбудовування з різними параметрами. Також проводяться розрахунки відповідних статистичних показників, робиться їх детальне порівняння та узагальнення для формування висновків по результатам вбудовування та витягання цільового повідомлення. Обгрунтовується вибір оптимального контейнеру, який є ціллю нашого дослідження за різними параметрами.

1 ТЕОРЕТИЧНІ ОСНОВИ СТЕГАНОГРАФІЇ

1.1 Основи стеганографії: цілі, принципи, сучасні підходи

Стеганографія — це наука та мистецтво приховування інформації в такому вигляді, щоб саме її існування залишалося непомітним для сторонніх осіб. Основна мета стеганографії полягає у забезпеченні таємності передачі даних, шляхом вбудовування прихованого повідомлення в носій (зображення, аудіо, відео, текст тощо) таким чином, щоб носій інформації виглядав незмінним або не викликав підозри.

На відміну від криптографії, яка приховує зміст повідомлення, стеганографія приховує сам факт його існування. Обидва методи можуть використовуватися разом для підвищення безпеки передачі інформації.

Як зазначає В.О. Хорошко та співавтори у посібнику «Комп’ютерна стеганографія: навчальний посібник» [1] – стеганографія являє собою сукупність методів та засобів їхньої реалізації, які базуються на різних

принципах і дозволяють приховувати сам факт існування секретної інформації в тому або іншому середовищі.

Стеганографія як метод прихованого передавання інформації має широкий спектр цілей, які спрямовані на забезпечення конфіденційності даних і захист від стороннього доступу. Нижче ми розглянемо її основні завдання та умовно поділимо їх на декілька категорій.

Прихована передача інформації. Як вже зазначалось – основна мета стеганографії полягає в забезпеченні можливості передавання інформації таким чином, щоб факт її наявності залишався непомітним для сторонніх осіб. Це досягається шляхом вбудовування прихованих повідомлень у звичайні, не викликаючі підозри носії, такі як цифрові зображення, аудіо файли, відео або текстові документи. У разі правильного застосування стеганографії сторонні спостерігачі не можуть навіть запідозрити наявність прихованого повідомлення.

Захист конфіденційної інформації. У сучасному світі, де загроза кіберзлочинності постійно зростає, стеганографія є важливим інструментом для захисту конфіденційних даних. Вона може використовуватися для передачі приватної інформації між сторонами, уникаючи виявлення її під час перехоплення даних.

Забезпечення авторських прав і накладання «водяних знаків». Одним із популярних напрямів застосування стеганографії є створення цифрових «водяних знаків» для захисту авторських прав. У цьому випадку в мультимедійний файл (наприклад, зображення чи відео) вбудовуються метадані, які підтверджують право власності або джерело походження файлу. Такі «водяні знаки» не помітні для звичайних користувачів, але можуть бути виявлені за допомогою спеціальних програм.

Військове та розвідувальне застосування. Стеганографія має довгу історію використання у військових та розвідувальних операціях. Вона дозволяє передавати секретну інформацію через звичайні, на перший погляд, повідомлення або файли, мінімізуючи ризик викриття. Сучасні технології

дозволяють приховувати повідомлення навіть у шумі аудіо чи відеозаписів, що ускладнює їх виявлення.

Інтеграція з іншими методами захисту. Стеганографія часто використовується разом із криптографією для створення багаторівневих систем безпеки. У таких системах спочатку дані шифруються, а потім приховуються у вибраному носії. Цей підхід забезпечує додатковий рівень захисту, оскільки навіть у разі виявлення прихованого повідомлення його вміст залишиться недоступним без ключа дешифрування.

Обхід цензури. В умовах, коли доступ до певної інформації може бути обмежений цензурою, стеганографія надає можливість безпечного розповсюдження матеріалів, уникаючи блокування чи виявлення контролюючими органами.

Таким чином, цілі стеганографії охоплюють широкий спектр завдань, починаючи від забезпечення приватності у спілкуванні і закінчуючи використанням у промислових і військових цілях. Її застосування є важливим як у захисті інформації, так і в гарантуванні безпеки у сучасному цифровому світі.

Виходячи з завдань можемо зазначити, що стеганографія ґрунтується на використанні спеціальних методів і технік для приховування інформації таким чином, щоб її існування було невидимим для сторонніх осіб.

На наш погляд основні принципи стеганографії включають такі аспекти:

1. Використання носіїв для прихування даних.

Стеганографія передбачає використання різних типів носіїв, у які вбудовується прихована інформація. Це можуть бути зображення, найбільш популярний носій завдяки його великим розмірам і широкому використанню у цифровому середовищі, аудіо- та відео файли, які використовуються для приховування значних обсягів даних, при цьому забезпечуючи високий рівень маскування, текстові документи, які використовуються для передачі невеликих обсягів інформації через зміну символів, пробілів або форматування, тощо.

2. Непомітність прихованої інформації.

Одним із ключових принципів є забезпечення непомітності повідомлення для сторонніх осіб. Для цього використовуються методи, що мінімально впливають на зовнішній вигляд або властивості носія. Наприклад у цифрових зображеннях інформація вбудовується у найменш значущі біти (метод LSB — Least Significant Bit), а в аудіо файлах дані можуть бути приховані у спектральних або фазових характеристиках.

3. Збереження якості носія.

Приховування даних не повинно суттєво змінювати характеристики носія. Це важливо, щоб уникнути підозри з боку сторонніх осіб. Наприклад, у стеганографії зображень важливо, щоб зміни у кольорах пікселів не були помітні людському оку.

4. Захист прихованої інформації.

Щоб забезпечити додатковий рівень безпеки, приховані дані можуть шифруватися перед вбудовуванням у носій. Це створює додаткові труднощі для сторонніх осіб навіть у разі виявлення прихованої інформації.

5. Статистична стійкість.

Приховані дані повинні бути стійкими до стеганоаналізу — процесу, спрямованого на виявлення або витягування прихованої інформації. Для цього розробляються методи, які маскують статистичні ознаки вбудованих даних.

6. Реверсивність процесу.

Інформація, що була прихована, повинна бути коректно витягнута з носія без втрати даних. Це забезпечується використанням чітких алгоритмів кодування та декодування.

7. Адаптація до типу носія.

Ефективність приховування залежить від типу і характеристик носія. Наприклад у зображеннях із низьким рівнем шуму використовуються менш помітні методи вбудовування, а в аудіо файлах приховані дані можуть маскуватися під природний шум.

Отже, як ми можемо помітити основні принципи стеганографії спрямовані на забезпечення надійного та непомітного передавання інформації.

Вони базуються на ефективному використанні носіїв, збереженні їхньої якості, а також застосуванні методів для підвищення стійкості до виявлення. Сучасна стеганографія продовжує розвиватися, вдосконалюючи свої алгоритми та методи для забезпечення максимальної безпеки та конфіденційності даних.

Розвиток інформаційних технологій значно вплинув на методи та підходи, які застосовуються в стеганографії. Сучасна стеганографія поєднує традиційні принципи приховування інформації з новітніми алгоритмами та техніками її приховування для забезпечення високого рівня конфіденційності.

До основних сучасних підходів можна віднести наступні види стеганографії:

1. Цифрова стеганографія.

Сучасні технології зосереджені на використанні цифрових носіїв, таких як зображення, аудіо, відео та текстові файли. Це може бути використання такого методу як LSB (Least Significant Bit), який ґрунтується на вбудовуванні інформації у найменш значущі біти пікселів цифрових зображень або аудіо сигналів, дозволяючи зберегти зовнішній вигляд носія незмінним.

Фазове кодування використовується в аудіо стеганографії, де інформація приховується у фазі сигналу, що робить її непомітною для людського слуху.

Спектральні методи застосовуються у відео- та аудіо файлах для приховування інформації у частотних характеристиках.

2. Адаптивна стеганографія.

Цей підхід враховує статистичні та візуальні властивості носія для зменшення помітності вбудованих даних. Адаптивна стеганографія передбачає проведення аналізу носія перед вбудовуванням інформації, щоб уникнути змін, які можуть бути виявлені стеганоаналізом, або динамічне коригування алгоритмів залежно від типу носія.

3. Інтеграція стеганографії з криптографією.

Поєднання стеганографії та криптографії дозволяє створювати багаторівневі системи захисту інформації. У таких системах дані спочатку шифруються, а потім приховуються у вибраному носії. Це забезпечує

додатковий рівень безпеки, оскільки навіть у разі виявлення стеганографічного повідомлення його зміст залишиться захищеним.

4. Стеганографія у мультимедіа.

Сучасні мультимедійні формати, такі як JPEG, MP3, MP4, є популярними середовищами для приховування даних. Як приклад у зображеннях формату JPEG може бути використання особливостей алгоритму компресії, що дозволяє вбудовувати дані у коефіцієнти дискретного косинусного перетворення (DCT). У відео файлах інформація може бути прихована у межах кадрів або у кольорових каналах.

5. Стеганографія в мережах.

У мережевому середовищі стеганографія використовується для приховування даних у пакетах даних, що передаються. Це може включати маніпуляції з полями заголовків протоколів (наприклад, IP чи TCP), або використання надлишкової інформації у пакунках для вбудовування повідомлень.

6. Стеганографія з використанням штучного інтелекту.

Сучасні підходи активно впроваджують методи машинного навчання та штучного інтелекту, так можливе використання нейронних мереж для адаптивного вбудовування даних, що зменшує помітність змін, розробка алгоритмів, які аналізують носії на предмет оптимальних місць для приховування даних.

7. Розподілена стеганографія.

Цей підхід передбачає розподіл прихованого повідомлення між кількома носіями. Такий метод підвищує безпеку, оскільки навіть у разі виявлення одного носія повідомлення залишається неповним і незрозумілим.

Як ми бачимо з розвитком стенографії відкриваються певні перспективні напрямки для подальшого вдосконалення. Це і подальша інтеграція зі штучним інтелектом, розвиток розподілених систем, нові формати носіїв та використання квантових технологій.

Проте ці ж фактори можуть кидати і певні виклики використанню стенографії.

Розвиток стеганоаналізу дозволяє сучасним методам аналізу носіїв, таким як статистичні тести і машинне навчання, значно ускладнювати приховування інформації. Виявлення навіть малопомітних змін у цифрових носіях становить серйозну проблему для стеганографічних методів.

Обмеження ресурсів носіїв, коли не всі цифрові файли мають достатньо місця для приховування великих обсягів даних без помітних змін, це обмежує використання деяких форматів файлів.

Забезпечення непомітності викликає потребу в постійному вдосконаленні алгоритмів, які забезпечують високий рівень маскування, що є досить складним завданням в умовах зростання якості стеганоаналізу.

1.2 Методи приховування інформації у цифрових зображеннях

Як вже зазначалось стеганографія є важливим елементом сучасних технологій захисту інформації, що дозволяє приховувати дані у звичайних медіа-файлах, таких як зображення, аудіо чи відео. Серед них цифрові зображення є одними з найбільш зручних для вбудовування прихованої інформації завдяки їхній великій ємності, популярності та повсякмісному використанні. Для реалізації стеганографічних операцій існує широкий спектр методів, які дозволяють забезпечити ефективне приховування даних з різним рівнем стійкості до виявлення.

На наш погляд можна класифікувати методи стеганографії зображень наступним чином.

Методи приховування інформації в цифрових зображеннях можна розділити на дві основні категорії:

1) Методи просторового домену, ці методи працюють безпосередньо з пікселями зображення, модифікуючи їхні значення для приховування даних.
2) Методи частотного домену, вони використовують перетворення зображення в частотній області (наприклад, за допомогою дискретного косинусного або хвильового перетворення) для вбудовування інформації.

В свою чергу методи просторового домену можна поділити на метод найменш значущого біта (LSB, англ. Least Significant Bit) та метод стего-блоків.

Метод найменш значущого біта (LSB) є одним із найпоширеніших і найпростіших методів стеганографії у цифрових зображеннях. Цей підхід базується на зміні найменш значущих бітів у пікселях зображення для вбудовування прихованих даних, таких як текст, зображення або інші форми цифрової інформації.

У посібнику «Комп'ютерна стеганографія: навчальний посібник» В.О. Хорошко та співавторів зазначається, що LSB-метод є базовим у практичних реалізаціях стеганографії, особливо для цифрових зображень у форматі BMP, завдяки простій структурі цього формату, яка дозволяє зберігати всі бітові дані без втрат. [1]

Суть роботи методу полягає в тому, що кожен піксель цифрового зображення у стандартних цифрових форматах файлів (наприклад BMP або PNG файли) зазвичай описується трьома кольоровими компонентами – червоним (R), зеленим (G) і синім (B). Кожен з цих компонентів кодується 8 бітами. LSB-метод замінює останній, найменш значущий, біт у значеннях R, G або B на біт прихованого повідомлення.

Завдяки цій мінімальній зміні кольорова інтенсивність пікселя змінюється так незначно, що людське око не помічає різниці, а отже приховані дані залишаються непомітними.

Перевагами методу є простота реалізації, метод LSB є технічно нескладним і може бути легко реалізований за допомогою програмного

забезпечення, та низький рівень спотворень, завдяки зміні лише одного біта у кожному кольоровому компоненті пікселя, зміни у зображенні залишаються практично непомітними для людського зору. Також вбудовування можливе у кожен піксель зображення, що забезпечує високу щільність прихованої інформації, що забезпечує високу ємність інформації.

Кузнецов О.О. у посібнику «Стеганографія» наголошує, що LSB-метод є одним із перших і найменш складних способів приховування даних. Однак, він підкреслює його обмеження у стійкості до атак, зокрема до аналізу гістограм і модифікацій зображення [2].

До недоліків методу відноситься чутливість до обробки зображення. LSB-метод дуже вразливий до таких операцій, як стискання (наприклад, у формат JPEG), фільтрація або зміна розмірів зображення.

Простота реалізації робить метод вразливим до стеганоаналізу і доступним для виявлення. Інструменти аналізу можуть легко визначити підозрілі зміни у найменш значущих бітах.

Метод найкраще працює з незжатими або мало зжатими форматами, такими як BMP чи PNG. У форматах із втратами, наприклад JPEG, приховані дані можуть бути пошкоджені через процедуру стискання, що робить цей метод обмеженим у форматах.

У роботах Конаховича Г.Ф. зазначається, що для підвищення ефективності LSB-методу використовуються комбіновані алгоритми, які адаптують вбудовування даних до особливостей зображення або використовують ключове шифрування для захисту даних від стороннього доступу [3] [4].

З метою підвищення стійкості та безпеки LSB-методу можливо використовувати певні вдосконалення.

Псевдовипадкове вбудовування – використання ключа для визначення позицій пікселів, у які буде вбудовано дані, це ускладнює виявлення прихованої інформації.

Використання тільки синіх компонентів – через менш помітну для ока зміну у синіх каналах деякі алгоритми працюють виключно із цими компонентами.

Динамічне вбудовування – інформація розподіляється нерівномірно по зображенню, а залежно від його текстурних особливостей.

Наступним в класифікації можна виділити метод стего-блоків, який є ефективним підходом у стеганографії, що базується на розподілі зображення на блоки пікселів та виборі певних блоків для вбудовування прихованої інформації. Цей метод спрямований на підвищення стійкості до стеганоаналізу, зокрема за рахунок зменшення впливу прихованих даних на загальну структуру зображення.

Згідно з посібником «Стеганографія» О. Кузнецова та співавторів, метод стего-блоків є важливим елементом сучасної стеганографії завдяки його високій стійкості до аналізу гістограм і атак на основі частотного розподілу. Автори також наголошують на доцільності використання цього методу у поєднанні з іншими підходами для підвищення безпеки стеганографічних даних [2].

Принцип роботи методу можна описати наступним чином:

- розбиття зображення на блоки, вихідне зображення поділяється на невеликі блоки однакового розміру (наприклад, 4×4 або 8×8 пікселів);
- вибір блоків для вбудовування інформації, що здійснюється з використанням псевдовипадкового генератору (на основі ключа);
- модифікація блоків, коли у вибраних блоках дані вбудовуються у пікселі за допомогою різних методів, таких як зміна найменш значущих бітів (LSB) або частотних компонентів блоку.

Перевагами методу є:

- стійкість до стеганоаналізу, завдяки розподілу прихованої інформації між різними блоками, метод робить виявлення стеганографічних даних складнішим;

- гнучкість, розмір блоків і стратегія вибору блоків можуть бути адаптовані до конкретних вимог, таких як розмір прихованого повідомлення або рівень безпеки;
- мінімальні спотворення, зміни вносяться лише у вибрані блоки, залишаючи більшу частину зображення незмінною.

Недоліки методу:

- чутливість до атак, якщо зловмисник отримує ключ або алгоритм розподілу блоків, приховані дані стають вразливими до виявлення;
- нижча ємність, порівняно з методами, які використовують усі пікселі зображення, метод стего-блоків має обмежену ємність, оскільки не всі блоки використовуються для приховування інформації;
- складність реалізації, необхідність розподілу блоків і використання ключів збільшує складність реалізації у порівнянні з простішими методами, такими як LSB.

В роботі «Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних» Г.Ф. Конаховича зазначено, що метод стего-блоків ефективно застосовується у сценаріях, де необхідна висока стійкість до спотворень зображення, таких як стискання або фільтрація. Автори підкреслюють, що випадковий вибір блоків суттєво ускладнює виявлення прихованих даних за допомогою автоматизованих засобів стеганоаналізу [3].

Для підвищення ефективності методу стего-блоків застосовуються такі вдосконалення як адаптивний вибір блоків, використання інформації про текстуру зображення для вибору блоків, які найменше помітно змінюються під час вбудовування даних, та шифрування даних, тобто використання криптографічних алгоритмів для шифрування прихованої інформації перед її вбудовуванням, що підвищує загальний рівень безпеки. Також його комбінують з частотними методами, тобто вбудовують інформацію у частотні компоненти блоків після їх перетворення, наприклад, за допомогою дискретного косинусного перетворення (DCT).

Нижче ми докладніше розглянемо методи частотного домену.

Дискретне косинусне перетворення (DCT) – є потужним інструментом у стеганографії, особливо для роботи з цифровими зображеннями. Воно використовується для перетворення даних із просторової області (пікселів) у частотну, що дозволяє приховувати інформацію у частотних компонентах зображення. Цей підхід є одним із найпоширеніших у стеганографії, оскільки він поєднує високу стійкість до атак із низьким рівнем помітності змін.

Принцип роботи методу:

- розділення зображення на блоки, вихідне зображення поділяється на невеликі блоки, зазвичай розміром 8×8 пікселів;
- перетворення блоків у частотну область, для кожного блоку виконується дискретне косинусне перетворення, що перетворює значення пікселів у набір частотних коефіцієнтів;
- вибір коефіцієнтів для вбудовування прихованої інформації обираються, зазвичай обираються середньо частотні коефіцієнти. Низькочастотні коефіцієнти не змінюються, щоб не спотворювати загальну якість зображення, а високочастотні часто ігноруються, оскільки вони можуть бути втрачені під час стиснення;
- модифікація коефіцієнтів при якій бітові значення прихованої інформації змінюють значення вибраних коефіцієнтів відповідно до заданих правил, наприклад, шляхом зміни їх найменш значущих бітів;
- зворотне перетворення – модифіковані коефіцієнти перетворюються назад у просторову область за допомогою зворотного дискретного косинусного перетворення.

У навчальному посібнику «Стеганографія» О.О. Кузнецова та співавторів метод DCT описується як один із ключових для роботи з скомпресованими зображеннями. Автори зазначають, що метод DCT дозволяє досягти високого рівня захисту інформації, одночасно зберігаючи якість зображення на прийнятному рівні [2].

Перевагами використання методу DCT є стійкість до стискання, оскільки метод працює з частотними компонентами, прихована інформація залишається

непошкодженою після стиснення зображення форматами, що базуються на DCT, такими як JPEG. Також він забезпечує мінімальні спотворення зображення завдяки модифікації середньо частотних коефіцієнтів, при якому зміни у зображенні залишаються непомітними для людського ока. Використання частотної області значно ускладнює стеганоаналіз і виявлення прихованих даних.

Г.Ф. Конахович у підручнику «Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних» звертає увагу на те, що використання методу DCT є перспективним для створення адаптивних стеганографічних систем, які враховують особливості людського зору та природні характеристики зображень [3].

До недоліків методу відносять складність реалізації - перетворення між просторовою та частотною областями вимагає більших обчислювальних ресурсів у порівнянні з простішими методами, такими як LSB. Обмежена ємність через використання лише середньо частотних коефіцієнтів, через що метод має обмежений обсяг для приховування даних. Також інтенсивне стиснення або інші форми обробки можуть призводити до втрати прихованої інформації.

Метод DCT знайшов широке застосування у практичних системах стеганографії, зокрема для приховування даних у фотографіях, відео та «водяних знаках». Для підвищення рівня безпеки він також використовується у поєднанні з іншими методами такими як LSB. Цей метод є ідеальним для роботи з форматами, які застосовують стиснення із втратами, і продовжує розвиватися завдяки вдосконаленню алгоритмів вибору та модифікації коефіцієнтів.

Хвильове перетворення DWT є одним із сучасних методів стеганографії, який дозволяє працювати з частотною областю зображень. На відміну від дискретного косинусного перетворення DCT, DWT забезпечує як просторову, так і частотну локалізацію сигналу. Ця властивість робить його особливо

ефективним для роботи із цифровими зображеннями, зберігаючи високу якість зображення та прихованість даних.

Розглянемо принцип роботи методу хвильового перетворення (DWT) який складається з трьох етапів. Спочатку проходить розділення сигналу зображення на чотири частини, названі субсмугами:

- LL (низькі частоти за обома напрямами — відображають основну структуру зображення);

- LH (низькі частоти за горизонталлю та високі за вертикаллю);

- HL (високі частоти за горизонталлю та низькі за вертикаллю);

- HH (високі частоти за обома напрямами — відображають деталі зображення).

Потім проходить модифікація субсмуг. Для вбудовування прихованих даних зазвичай використовують субсмуги LH, HL або HH. Це дозволяє зберігати основні візуальні характеристики зображення, представлені в LL.

Завершує процес зворотне хвильове перетворення. Після вбудовування інформації виконується зворотне перетворення для отримання модифікованого зображення.

Особливості методу:

- ітеративність, хвильове перетворення може виконуватися кілька разів (багаторівневе DWT), що дозволяє отримувати додаткові субсмуги із глибшою частотною деталізацією;
- адаптивність, DWT дозволяє адоптивно вибирати ділянки для приховування інформації, орієнтуючись на важливість частотних компонентів.

Г.Ф. Конахович і співавтори у підручнику «Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних» наголошує, що хвильове перетворення є основою для побудови сучасних адаптивних алгоритмів стеганографії, які враховують особливості людського зору та характеристики сигналу [3].

Перевагами методу DWT є висока стійкість до стиснення, він є сумісним із форматами, що використовують компресію з втратами (наприклад, JPEG

2000), низька помітність змін, завдяки локалізації сигналу зміни залишаються малопомітними для людського ока та гнучкість у налаштуванні, тобто можливість вибору рівня деталізації дозволяє регулювати обсяг прихованої інформації та її вплив на якість зображення.

Недоліки методу це складність реалізації, метод вимагає значних обчислювальних ресурсів та обмеження ємності прихованих даних, який залежить від кількості вибраних субсмуг і рівнів перетворення. Також цей метод чутливий до атак. Хоча DWT стійкий до стиснення, інтенсивні фільтрації або трансформації зображення можуть знищити приховану інформацію.

В стеганографії метод DWT часто використовується для вбудовування водяних знаків у зображення, захисту авторських прав на мультимедійний контент, створенні стеганографічних систем із підвищеною стійкістю до компресії та фільтрації.

Метод хвильового перетворення (DWT) є перспективним підходом для стеганографії, оскільки забезпечує баланс між прихованістю даних і якістю зображення. Використання цього методу дозволяє ефективно приховувати інформацію навіть у складних мультимедійних середовищах, роблячи його актуальним у різних галузях, таких як захист авторських прав і конфіденційне передавання даних.

Останнім часом набувають популярності гібридні методи. Гібридні методи стеганографії поєднують кілька технік для приховування інформації, щоб максимально використовувати переваги кожного з методів і мінімізувати їх недоліки. Це підхід, який дозволяє адаптувати систему стеганографії до різних середовищ передачі даних і підвищує її стійкість до виявлення та атак.

Принцип роботи гібридних методів:

- поєднання методів різних областей, наприклад, комбінування методів із просторової області (наприклад, метод LSB) з методами з частотної області (наприклад, DWT або DCT);

- використання додаткових алгоритмів, гібридні методи часто включають криптографію, хешування або інші механізми для посилення захисту прихованих даних;

- адаптивний підхід, під час приховування враховуються характеристики носія, наприклад, текстури або кольорові властивості зображення, для вибору найкращої техніки стеганографії.

Особливості гібридних методів:

- мультиплатформенність, гібридні методи можуть застосовуватися до різних типів носіїв, включаючи зображення, аудіо, відео тощо;

- баланс між прихованістю та ємністю, завдяки комбінуванню методів можна оптимізувати приховування, забезпечуючи як непомітність змін, так і достатню ємність для вбудовування даних;

- стійкість до атак, поєднання технік підвищує стійкість до виявлення прихованої інформації за допомогою статистичних, спектральних або інших видів аналізу.

Переваги гібридних методів це висока якість носія, тобто приховування інформації незначно впливає на візуальні характеристики зображення, підвищена стійкість до стиснення, яка досягається завдяки використанню частотних перетворень, що дозволяє зберігати інформацію навіть після стиснення із втратами та складність виявлення завдяки комбінуванню методів.

Недоліки гібридних методів це висока обчислювальна складність та значна потреба в ресурсах, складність налаштування, при якому вибір оптимальних методів для комбінування залежить від характеристик даних і цілей, та ризик конфлікту між методами, коли не всі методи добре інтегруються, що може вплинути на ефективність стеганографії.

Прикладом гібридного методу може бути поєднання LSB і DWT коли інформація спочатку вбудовується у субсмуги частотного перетворення (DWT), а потім модифікації виконуються на рівні просторових даних (LSB), що зберігає якість зображення та стійкість до атак.

Використання DCT і криптографії коли перед приховуванням інформація шифрується криптографічним алгоритмом, а вже зашифровані дані вбудовуються у низькочастотні компоненти, отримані за допомогою DCT.

Комбінація DWT і DCT дозволяє одночасно скористатися локалізацією сигналу (DWT) та ефективним використанням частотного спектра (DCT).

Гібридні методи стеганографії є ефективним інструментом для досягнення високої якості приховання інформації при збереженні стійкості до атак. Вони дозволяють поєднувати переваги кількох методик, що робить їх універсальним рішенням для різних завдань і середовищ.

1.3 Загальні характеристики цифрових зображень як середовища стеганографічної передачі

Цифрові зображення є одним із найбільш популярних середовищ для стеганографічної передачі інформації завдяки їхній широкій доступності, високій ємності для приховування даних та можливості мінімізації змін, які можуть бути помітними для людського ока. Однак їхнє використання у стеганографії передбачає врахування ряду характеристик, які впливають на ефективність та прихованість переданої інформації.

На наш погляд до основних характеристик цифрових зображень можна віднести наступні аспекти:

1. Структура цифрового зображення.

Цифрове зображення є дискретним представленням візуальної інформації у вигляді масиву пікселів, кожен із яких характеризується:

- розміром (роздільною здатністю), кількістю пікселів на ширину та висоту зображення. Зображення з вищою роздільною здатністю зазвичай мають більшу ємність для приховування даних;

- глибиною кольору, кількість бітів, що використовуються для представлення кольору одного пікселя. Наприклад, зображення з глибиною 24 біти (RGB) може приховувати більше даних порівняно із зображенням із глибиною 8 бітів (монохромні зображення).

2. Формати зображень.

Для стеганографії використовуються різні формати зображень, серед яких можна виділити наступні:

- BMP (Bitmap), не містить стиснення, що забезпечує точну передачу даних, але призводить до великого розміру файлу;

- JPEG (Joint Photographic Experts Group), використовує стиснення з втратами, що може призводити до спотворення прихованих даних;

- PNG (Portable Network Graphics), підтримує стиснення без втрат, що робить його зручним для стеганографії. Вибір формату залежить від вимог до прихованості та стійкості даних до стиснення.

3. Кольорові моделі.

Цифрові зображення можуть використовувати різні кольорові моделі, наприклад такі як:

- RGB (Red, Green, Blue), поширена модель, в якій кожен піксель представлений трьома компонентами;

- YCbCr, часто використовується в стиснених зображеннях (наприклад, JPEG) і дозволяє працювати з яскравістю (Y) та кольоровими компонентами (Cb і Cr) окремо;

- Grayscale (відтінки сірого), використовується для зображень із одним каналом, що обмежує ємність для приховування даних.

4. Статистичні характеристики.

Цифрові зображення мають набір статистичних характеристик, таких як середнє значення яскравості, дисперсія, частотний спектр, які можуть змінюватися після вбудовування даних. Важливо, щоб ці зміни залишалися непомітними для аналізу.

Цифрові зображення як середовище для стеганографії повинні відповідати певним вимогам:

- висока ємність. Цифрові зображення мають значну кількість пікселів, що дозволяє приховувати велику кількість інформації. Наприклад, у зображенні розміром 1024×768 із глибиною кольору 24 біти можна вбудовувати інформацію, використовуючи метод найменш значущого біта (LSB);

- можливість використання різних областей. Використання просторової області, тобто безпосереднє вбудовування даних у пікселі зображення, або частотна область, коли застосовуються методи перетворення (DCT, DWT), що підвищує стійкість прихованих даних до атак;

- сумісність із стисненням. Для стиснених форматів (наприклад, JPEG) використовуються спеціальні алгоритми, які зберігають стеганографічні дані навіть після стиснення.

До переваг цифрових зображень як середовища стеганографії можемо віднести наступні:

- візуальна непомітність, зміни у пікселях можуть бути настільки мінімальними, що їх не можна помітити без спеціального аналізу;

- універсальність використання, зображення є звичним форматом файлів, що не викликає підозри;

- різноманітність алгоритмів, можливість використання різних методів залежно від цілей.

Недоліками цифрових зображень можна вважати:

- обмежену стійкість до агресивного редагування, тобто фільтрація, перекодування або масштабування можуть знищити приховані дані;

- залежність від формату, стиснення з втратами (JPEG) може спотворювати вбудовану інформацію;

- статистичний аналіз, зміни у характеристиках зображення можуть бути виявлені за допомогою спеціальних алгоритмів.

Зважаючи на вказані характеристики цифрових зображень можемо навести ряд рекомендації щодо їх вибору для потреб стеганографії:

- використання зображень із високою роздільною здатністю, це дає можливість збільшити ємність для приховування даних;

- робота з форматами без втрат, наприклад, BMP або PNG забезпечують вищу точність передачі даних;

- застосування частотних методів для стиснених форматів, доцільно використовувати наприклад DCT або DWT.

З огляду на наведену інформацію можемо зробити висновок, що цифрові зображення є дуже підходящім середовищем для стеганографії завдяки їхнім характеристикам. Однак під час роботи із зображеннями необхідно враховувати їхні особливості, такі як розмір, формат і кольорова модель, щоб обрати оптимальний метод приховування даних.

Проте варто врахувати, що розробка нових методів приховування інформації вимагає врахування низки викликів:

- протидія стеганоаналізу, інструменти виявлення стеганографічних даних стають дедалі ефективнішими, що підвищує потребу в удосконаленні алгоритмів приховування;

- адаптація до нових форматів зображень, які з’являються з розвитком цифрових технологій та які потребують адаптації методів приховування інформації.

2 ВИКОРИСТАННЯ АЛГОРИТМУ ДЕЯ ДЛЯ ОБРОБКИ ТА ПЕРЕДАЧІ ЗОБРАЖЕНЬ

2.1 Опис роботи алгоритму Дея

Алгоритм Дея базується на аналізі частотних характеристик даних. Основна ідея полягає в тому, щоб розкласти сигнал на складові частоти та

виявити аномальні частотні компоненти, які можуть вказувати на наявність прихованої інформації.

Дискретне косинусне перетворення (DCT) є одним з найважливіших інструментів для обробки сигналів, особливо в контексті стеганографії. Воно дозволяє перетворити сигнал з часової області у частотну, виявляючи його частотні компоненти [5]. Формула DCT для 1D сигналу x(n) виглядає так (2.1):

$$X(k) = \sum_{n=0}^{N-1} x(n) * cos\left[\frac{\pi}{N}\left(n + \frac{1}{2}\right)k\right],\ k = 0,1,\dots,N-1 \qquad (2.1)$$

де *X(k)* – коефіцієнт DCT;

N – довжина сигналу;

n – індекс вхідного сигналу;

k – індекс частотної компоненти.

Одним з ключових інструментів, що використовується для цього аналізу, є перетворення Фур'є.

У мультимедійних файлах (зображеннях, аудіо) приховані дані часто змінюють частотні характеристики. Алгоритм Дея може бути застосований до частотних компонентів, виділених за допомогою перетворення Фур'є або дискретного косинусного перетворення (DCT). Це математичне перетворення дозволяє представити сигнал у вигляді суми синусоїдальних компонентів, кожна з яких має свою частоту, амплітуду та фазу.

Перетворення Фур'є визначається як (2.2):

$$X(k) = \sum_{n=0}^{N-1} x(n) * e^{-j2\pi kn/N} \qquad (2.2)$$

де: *X(k)* – спектральна компонента сигналу на частоті *k*;

x(n) – оригінальний сигнал у часовій області,

N – кількість точок у сигналі;

j – уявна одиниця.

Окрім перетворення Фур'є, для аналізу частотних характеристик також використовується перетворення Вейвлета.

Вейвлет перетворення.

Перетворення на основі хвиль описує процес поступової декомпозиції зображення через його розклад на набір базисних функцій хвильового перетворення. Дискретне хвильове перетворення (DWT) забезпечує чудову локалізацію в просторі та частоті. Застосування DWT до двовимірних зображень відповідає фільтрації зображення у кожному вимірі.

Вхідне зображення розділяється на 4 неперекриваючі один одного багатороздільні піддіапазони за допомогою фільтрів: (LL1), (LH1), (HL1) і (HH1). Піддіапазон (LL1) обробляється далі для отримання наступного більш грубого масштабу коефіцієнтів хвильового перетворення, поки не буде досягнутий певний кінцевий масштаб «N». Коли масштаб «N» досягнутий, ми отримуємо 3N+1 піддіапазони, включаючи багатороздільні піддіапазони (LLN), а також (LHX), (HLX) і (HHX), де «X» змінюється від 1 до «N». Як правило, зображення великої енергії зберігається в цих піддіапазонах.

Пряме дискретне хвильове перетворення (DWT) є надзвичайно підходящім для визначення областей у контейнерному зображенні, де секретне зображення може бути ефективно приховане завдяки добрим властивостям локалізації в просторі та частоті. чому, ці властивості використовують ефект маскування, пов'язаний із людською системою зору. Якщо змінюється коефіцієнт DWT, ця зміна не містить зображення області, яка відповідає цьому коефіцієнту.

Однак приховування секретного зображення в піддіапазоні низької частоти (LLX) може значно погіршити якість зображення, так як саме в цих піддіапазонах остаточно зберігається основна частина видимого зображення. З іншого боку, використання низькочастотних піддіапазонів для отримання інформації може значно підвищити її стійкість до атак.

З іншого боку, краї та текстури зображення, які належать до високочастотних піддіапазонів (HHX), не настільки чутливі до змін з точки зору сприйняття людським оком. Це дозволяє вбудовувати секретне зображення в ці піддіапазони без помітного впливу на стегоконтейнер.

Більшість алгоритмів, які базуються на DWT, вибирають компромісний підхід для досягнення прийнятого рівня непомітності та стійкості: секретне зображення вбудовується в середньо частотні піддіапазони (LHX) або (HLX) і (HHX).

Для формування остаточного зображення використовують спосіб змішування двох зображень разом з відповідним ваговим коефіцієнтом змішування. Коефіцієнт змішування або відсоток кольорів із першого вихідного зображення, використаного в змішаному зображення називається – «альфа», а сама техніка - альфа-змішування (або α-змішування). Ця техніка широко застосовується у комп'ютерній графіці, обробці зображень та стеганографії, де необхідно приховати одне зображення всередині іншого. Завдяки коефіцієнту α можна контролювати ступінь змішування двох зображень [6].

α -змішування можна реалізувати в комп'ютерній графіці шляхом змішування кожного пікселя з першого вихідного зображення з відповідним пікселем у другому вихідному зображенні. Процес проведення α-змішування можемо описати наступним чином – кожне зображення з тих, що будуть змішуватись, розбивається на окремі пікселі де кожен піксель має свої кольорові значення. Далі кінцевий піксель стегозображення отримується множенням вихідного пікселя першого зображення на коефіцієнт α та додається добуток вихідного пікселя другого зображення на значення (1,0 - коефіцієнт α). Значення «альфа», що використовується в змішуванні, знаходиться в діапазоні від 0,0 до 1,0 що відповідає значенню від 0% до 100% значення пікселю першого зображення в порівнянні з другим.

Математична модель або ж основна формула техніки α-змішування виглядає так (2.3):

$$P_{final}=\alpha\cdot P_{source1}+(1-\alpha)\cdot P_{source2}, \qquad (2.3.)$$

де: P_{final} — значення пікселя у фінальному зображенні (стегоконтейнері);

$P_{source1}$ — значення пікселя першого джерела (порожнього контейнера);

$P_{source2}$ — значення пікселя другого джерела (цільового зображення);

α — коефіцієнт змішування ($0\leq\alpha\leq1$).

Значення α задає пропорцію, з якою кожне зображення впливає на результат.

При значенні α=0 - результат є повною копією другого зображення.

При значенні α=1 - результат дорівнює першому зображенню.

При значеннях 0<α<1 - зображення змішуються.

У стеганографії α-змішування застосовується для приховування секретного зображення всередині контейнера.

До особливостей та переваг техніки α-змішування можемо віднести наступне:

- контроль якості змішування, що відбувається завдяки параметру α, яким можна точно налаштовувати співвідношення між контейнером і прихованими даними. Це дозволяє досягати балансу між якістю стегозображення та стійкістю прихованої інформації;

- непомітність змін в стегоконтейнері, при α-змішуванні вони мінімально помітні для людського ока, особливо якщо приховані дані розподілені у високочастотних компонентах;

- стійкість до атак техніки α-змішування забезпечує базову стійкість до втрат інформації під час стискання (наприклад, JPEG) або фільтрації;

- гнучкість застосування методу робить його підходящим як для просторової області (змішування пікселів), так і для частотної області (під час роботи з перетвореннями, такими як DCT або DWT).

При цьому слід звернути увагу на можливі виклики та обмеження методу.

Необхідно вибрати оптимальне значення α, так як воно впливає на якість витягнутого зображення. Надто низьке значення може погіршити видимість контейнера, а надто високе — знизити якість витягнутих даних.

Складність обробки великих даних у випадку великих зображень або відео, через що обчислювальні витрати на обробку можуть зростати.

Стійкість до спеціалізованих атак, техніка α-змішування може бути вразливою до атак, які використовують спектральний аналіз для виявлення прихованої інформації.

Теоретичні основи алгоритму Дея базуються на аналізі частотних характеристик даних з використанням перетворення Фур'є та перетворення Вейвлета. Ці методи дозволяють виявляти приховану інформацію, аналізуючи складові частоти сигналу та виявляючи аномальні компоненти [6].

На рисунку 2.1 наведена узагальнена схема пропонованого алгоритму вбудовування секретного цільового повідомлення в контейнер, яка складається з наступних послідовних етапів:

- зображення порожній контейнер та секретне цільове зображення, які мають бути однакового розміру, розділяються на індивідуальні кольорові RGB-площини;

- до кожної з індивідуальних кольорових RGB-площин застосовується дискретне косинусне перетворення (DCT);

- кожна індивідуальна кольорова RGB-площина цільового зображення приховуються всередині відповідної за кольором індивідуальної кольорової RGB-площини контейнера за допомогою техніки α-змішування;

- усі три кольорові RGB-площини після α-змішування знову комбінуються разом для створення стегоконтейнера.

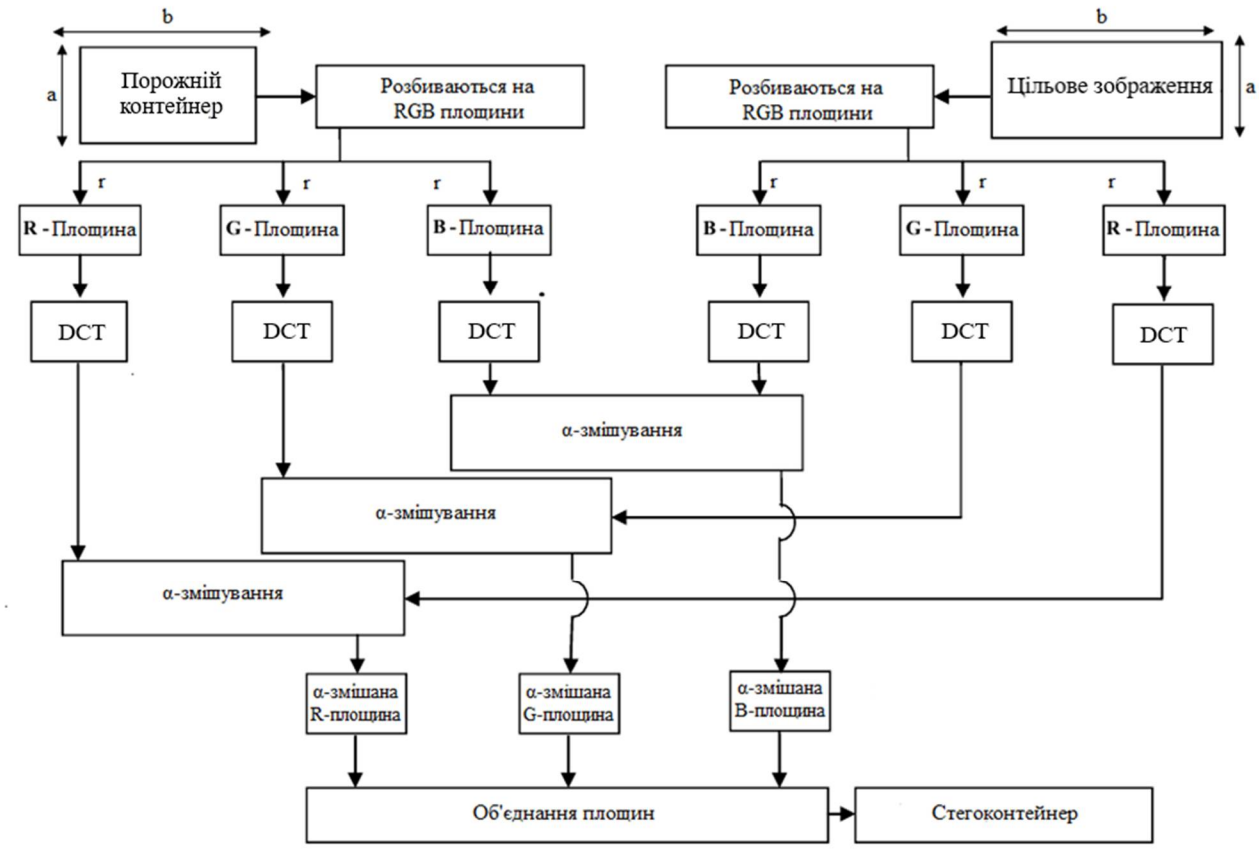


Рисунок 2.1 – Алгоритм приховування цільового зображення

На рисунку 2.2 наведена узагальнена схема пропонованого алгоритму витягування секретного цільового повідомлення зі тегоконтейнеру, вона схожа на процес вбудовування та складається з наступних послідовних етапів:

- зображення порожній контейнер, яке застосовувалось для вбудовування та отриманий стегоконтейнер, розділяються на індивідуальні кольорові RGB-площини;

- до кожної з індивідуальних кольорових RGB-площин застосовується дискретне косинусне перетворення (DCT);

- кожна індивідуальна кольорова RGB-площина порожнього контейнеру проходить α-змішування з відповідною за кольором індивідуальною кольоровою RGB-площиною стегоконтейнера, з коефіцієнтом α-змішування таким точно як при вбудовуванні;

- усі три кольорові RGB-площини після α-змішування знову комбінуються разом для отримання витягнутого зображення.

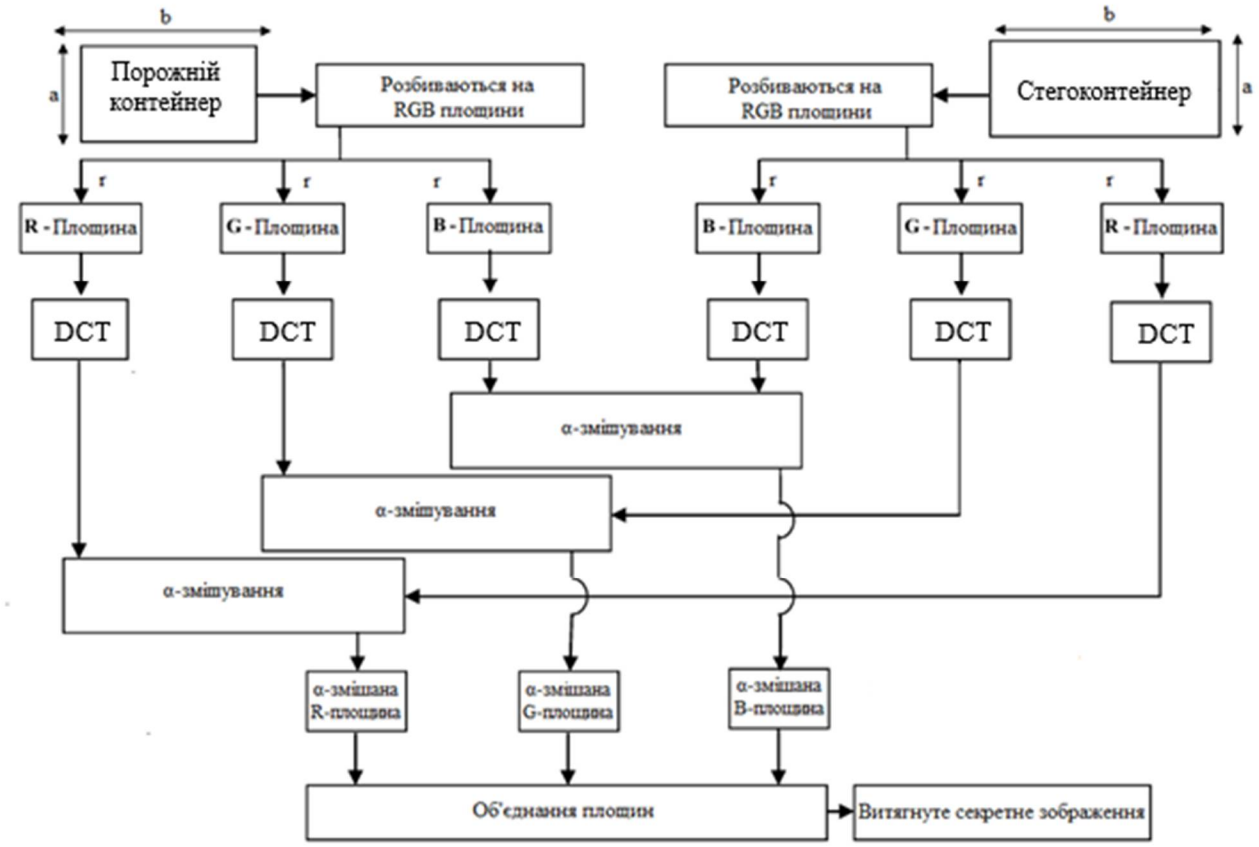


Рисунок 2.2 - Алгоритм витягнення цільового зображення

2.2 Перспективи оптимізації алгоритму Дея

Алгоритм Дея є ефективним інструментом для стеганографічного приховування інформації у зображеннях. Однак, з розвитком технологій і потребою у підвищенні рівня безпеки та якості прихованої інформації, виникає необхідність оптимізації алгоритму для роботи зі складними стеганографічними методами. Розглянемо кілька перспективних напрямків для оптимізації цього алгоритму.

Підвищення стійкості до сучасних атак та оптимізація для роботи у складних умовах може бути досягнута завдяки:

- використанню адаптивних методів, таких як адаптивне налаштування коефіцієнта змішування α залежно від характеристик контейнера та цільового зображення може значно ускладнити виявлення прихованої інформації, тощо;

- захист від атак на основі частотного аналізу для цього на основі частотного аналізу можна використовувати методи, що дозволяють приховувати інформацію у низькочастотних компонентах, які менш помітні для атак, наприклад, комбінація методів DCT та Вейвлет-перетворення може підвищити таку стійкість;

- захист від статистичних атак через створення більш рівномірного розподілу зашифрованих даних;

- врахування параметрів мультимедійного контейнера для запобігання змін, що викликають підозру.

Підвищення ефективності роботи алгоритму може досягатися завдяки:

- оптимізації обчислювальних процесів, що може значно зменшити час виконання алгоритму, наприклад, використання паралельних обчислень на основі графічних процесорів (GPU) дозволяє прискорити обробку великих обсягів даних;

- використанню сучасних алгоритмів машинного навчання для автоматичного налаштування параметрів алгоритму, що може значно підвищити його ефективність, як приклад можемо навести нейронні мережі які можуть бути використані для оптимізації параметрів змішування залежно від характеристик зображення.

Для підвищення якості приховування інформації пропонується застосовувати:

- використання методів покращення якості зображення, для зменшення спотворень прихованої інформації, таких як супер резолюція та згладжування, ці методи дозволяють зберігати високу якість як цільового зображення, так і стегоконтейнера;

- комбінація стеганографії з іншими методами захисту, такими як криптографія, що дозволяє забезпечити додатковий рівень безпеки, коли перед

стеганографічним приховуванням інформації її можна зашифрувати, що забезпечить захист навіть у випадку виявлення прихованої інформації.

Також потрібно постійно адаптуватись до нових форматів даних. Оптимізація алгоритму Дея для роботи з новими форматами зображень, такими як HEIF та AVIF, може підвищити його актуальність і придатність для сучасних потреб. Ці формати забезпечують вищу якість зображення при менших обсягах даних, що є важливим для стеганографії.

Перспективним напрямком є і розширення алгоритму Дея на інші типи мультимедійних даних, таких як аудіо та відео. Це дозволить використовувати стеганографію для приховування інформації у різних типах файлів.

Оптимізація алгоритму Дея для роботи зі складними стеганографічними методами має великий потенціал. Підвищення стійкості до атак, оптимізація обчислювальних процесів, покращення якості прихованої інформації та адаптація до нових форматів даних – це лише кілька напрямків, які можуть значно покращити ефективність алгоритму. Також не слід забувати про модернізацію його архітектури, інтеграцію з частотними та сучасними криптографічними методами, а також використання апаратного прискорення. Розвиток цих напрямків дозволить забезпечити високий рівень безпеки та конфіденційності інформації у сучасному цифровому світі [8].

Результати дослідження можуть бути використані для покращення методів аналізу цифрових зображень у системі забезпечення інформаційної безпеки. Практична реалізація застосування алгоритму Дея дозволяє використати його як інструмент для виявлення стеганографічних змін у зображеннях, що має прикладне значення в кібербезпеці, судовій експертизі та захисті інтелектуальної власності.

3 ВИБІР КОНТЕЙНЕРУ ДЛЯ ПЕРЕДАЧІ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ АЛГОРИТМУ ДЕЯ

3.1 Постановка задачі

Передача секретної інформації через зображення з використанням стеганографії вимагає вибору відповідного контейнера, який забезпечує мінімальну помітність змін, високу якість відновлення прихованих даних і стійкість до атак. Вибір контейнеру який би максимально відповідав даним вимогам і є основною метою нашої роботи.

Для ефективного виконання поставленої задачі нам необхідно досягнути певних цілей:

- забезпечення якісного приховування зображення, вибрати контейнер таким чином, щоб приховане зображення було важко виявити навіть за допомогою статистичного або спектрального аналізу;
- мінімізація спотворень у контейнері, тобто контейнерне зображення повинно зберігати візуальну схожість із початковим навіть після внесення змін.
- забезпечення високої якості відновлення, після вилучення прихованого зображення його відмінності від оригіналу мають бути мінімальними;
- вибір оптимального коефіцієнта змішування α, так як його значення впливає на співвідношення між контейнером і секретними даними, тому необхідно знайти баланс між непомітністю і точністю відновлення.

Вхідні дані – маємо цільове зображення (секретне) форматі BMP файлу розміром 128 на 128 пікселів для приховування і його наступної передачі.

Також пропонується набір контейнерів, які будуть використовуватися для приховування. В якості контейнерів будемо використовувати кольорові зображення в тому ж форматі BMP файлів розміром 128 на 128 пікселів.

Цільове зображення та контейнери наведені на рисунку 3.1. Як бачимо в якості контейнерів ми будемо використовувати різні за стилістикою та

кольоровою гамою зображення. Контейнери повинні мати досить велику місткість для приховування секретного зображення, бути стійкими до стискання, обробки і інших маніпуляцій та забезпечувати мінімальну помітність змін в результаті вбудовування даних. Для того, щоб в подальшому було легше орієнтуватись в контейнерах кожному з них буде присвоєний відповідний номер.

Цільове зображення

Запропоновані контейнери

Перший контейнер (С1) Другий контейнер (С2) Третій контейнер (С3)

Рисунок 3.1 – Цільове зображення та варіанти контейнерів

В роботі будуть застосовуватись різні коефіцієнти α – змішування для отримання оптимального стегоконтейнеру.

Після отримання стегоконтейнерів з різними коефіцієнтами α – змішування буде проведена оцінка візуальної якості зображення та розраховані додаткові статистичні показники викривлення стегоконтейнера в порівнянні з вихідним контейнером.

Основні моменти які можна виділити при виборі контейнеру:

- баланс між непомітністю і стійкістю - використання низькочастотних компонент підвищує стійкість, але може спричиняти помітні спотворення, робота з високочастотними компонентами знижує вплив на зображення, але зменшує стійкість;
- складність статистичного аналізу, для запобігання виявленню прихованої інформації необхідно уникати утворення закономірностей у змінених даних;
- оптимальний вибір контейнера, контейнер має бути адаптованим до типу секретного зображення, щоб зберегти його характеристики після вбудовування.

Постановка задачі вибору контейнера для стеганографії включає розв'язання багатокритеріальної задачі: забезпечення високої непомітності, збереження якості контейнера, стійкості до атак і точності відновлення прихованих даних. У наступних частинах аналізуються методи розв'язання цієї задачі та критерії оцінки ефективності.

3.2 Використання алгоритму Дея для приховування зображення

Алгоритм Дея є одним з ефективних стеганографічних методів для приховування зображень. Він базується на використанні дискретного косинусного перетворення (DCT) та методу α-змішування для вбудовування цільового зображення у контейнер. Ми будемо використовувати його для вбудовування секретного зображення в кольоровий BMP-файл. Обидва файли повинні бути однакового розміру.

В якості програмного забезпечення для реалізації поставленої задачі будемо застосовувати пакет математичних обчислень MathCad.

Розглянемо поетапно процес приховування зображення:

1. Підготовка зображень

1.1. Вибір цільового зображення та контейнера

Перший крок включає вибір цільового зображення, яке потрібно приховати, і контейнера, у який буде приховано цільове зображення. Обидва зображення мають бути однакового розміру і зберігатися у форматі BMP файлу.

1.2. Розбиття на кольорові площини

Цільове зображення та контейнер розбиваються на три окремі кольорові площини: червону (R), зелену (G) та синю (B). Кожна площина зображення розбивається на блоки розміром 8x8 пікселів.

2. Дискретне косинусне перетворення (DCT)

2.1. Перетворення блоків

До кожного блоку зображення застосовується DCT. Це перетворення дозволяє розкласти блоки на частотні компоненти, де високочастотні компоненти можуть бути змінені без значної втрати якості зображення.

3. Приховування інформації (α-змішування)

3.1 Формула α-змішування

Цільове зображення приховується у контейнері за допомогою методу α-змішування. Формула змішування виглядає так (3.1):

$$S = \alpha * C + (1 - \alpha) * T , \qquad (3.1)$$

де: S – стегоконтейнер;

C – пустий контейнер;

T – оригінальне цільове зображення;

α - коефіцієнт змішування ($0 < \alpha < 1$).

3.2. Зворотне DCT

Після змішування даних у частотній області, виконується зворотне DCT для повернення блоків у часову область.

4. Формування стегоконтейнера

4.1. Отримання стегоконтейнера

Після застосування зворотного DCT, отримане зображення містить приховану інформацію цільового зображення. Це зображення називається стегоконтейнером.

5. Витягнення прихованого зображення

5.1. Необхідні компоненти

Для витягнення цільового зображення необхідно мати стегоконтейнер, початковий контейнер та значення коефіцієнта змішування α яка застосовувалось при його формуванні.

5.2. Процес витягнення

З використанням стегоконтейнера та початкового контейнера, а також значення α, виконується зворотний процес змішування для відновлення цільового зображення.

Тепер розглянемо результати вбудовування нашого цільового зображення в запропоновані контейнери використовуючи пакет математичних обчислень MathCad в якому для приховування інформації був застосований коефіцієнт α-змішування який дорівнює 0,5.

Результати цього вбудовування, а саме отримані стегоконтейнери (S-0,5) та витягнуті цільові зображення (V-0,5) наведені на рисунку 3.2. Як можемо побачити, всі три отримані нами стегоконтейнери не відповідають необхідним нам вимогам, через що ми не досягли поставлених раніше цілей, а саме стегоконтейнери не забезпечують якісного приховування цільового зображення та мінімального спотворення стегоконтейнеру. На отриманих зображеннях (стегоконтейнерах S-0,5) чітко проглядаються обриси цільового зображення, а також самі зображення контейнерів значно змінили кольорову насиченість, зображення стало дуже тьмяним, напівпрозорим.

Витягнуте зображення (V-0,5) з даних стегоконтейнерів відповідає цільовому, маючи незначні спотворення в порівнянні з оригіналом, незначні зміни відтінку кольору при повністю збережених обрисах. Незважаючи на це отриманий результат при обраному коефіцієнті α-змішування 0,5 не можна вважати позитивним, так як ми не досягли основної мети нашої робот, а саме

непомітності самого факту передачі секретного повідомлення, яким в нашому випадку є цільове зображення.

Отримавши такі результати ми не будемо використовувати для подальшого розгляду та поглибленого аналізу різниці між різними контейнерами коефіцієнті α-змішування 0,5.

Цільове зображення (T)

↓

1 2 3

Контейнери для вбудовування зображення (C)



↓ ↓ ↓

Стегоконтейнери з вбудованим цільовим зображенням (S-0,5)



↓ ↓ ↓

Витягнуті цільові зображення (V-0,5)



Рисунок 3.2 – Вбудовування цільового зображення в контейнери з коефіцієнтом α-змішування = 0,5

Наступним кроком ми збільшуємо коефіцієнт α-змішування в наших розрахунках до 0,8. Результати вбудовування нашого цільового зображення в запропоновані контейнери, це стегоконтейнери S-0,8 та витягнуті цільові зображення V-0,8, з використанням пакету математичних обчислень MathCad в якому для приховування інформації застосований коефіцієнт α-змішування який дорівнює 0,8 наведені на рисунку 3.3.

Цільове зображення (T)

↓

1 2 3

Контейнери для вбудовування зображення (C)



↓ ↓ ↓

Стегоконтейнери з вбудованим цільовим зображенням (S-0,8)



↓ ↓ ↓

Витягнуті цільові зображення (V-0,8)

Рисунок 3.3 – Вбудовування цільового зображення в контейнери з коефіцієнтом α-змішування = 0,8.

При збільшенні коефіцієнту α-змішування до 0,8 нам вдалось досягти значно кращих результатів, а саме отримані стегоконтейнери S-0,8 з усіх трьох контейнерів C1, C2 та C3 без значних спотворень, вбудоване повідомлення майже не помітне, що і є основним нашим заданням, непомітно передати секретне повідомлення.

Витягнуті з цих стегоконтейнерів S-0,8 секретне повідомлення V-0,8 також має добру якість, має чіткі риси та незначну зміну початкового кольору. Тому для подальших розрахунків та поглибленого аналізу будуть використовуватись результати саме цього вбудовування з коефіцієнтом α-змішування 0,8. Розрахунки статистичних показників відхилення якості цільового повідомлення та витягнутого повідомлення та їх детальний аналіз будуть наведені в наступному розділі.

3.3 Аналіз отриманих результатів та вибір оптимального контейнеру

Для оцінки спотворення стегоконтейнера в порівнянні з порожнім контейнером будемо використовувати такі статистичні показники викривлення:

- максимальна різниця;
- середня абсолютна різниця;
- нормована середня абсолютна різниця;
- нормована середньоквадратична похибка;

- відношення сигнал/шум;
- якість зображення;
- структурний склад [3] [9].

Розглянемо кожний з них більш детально.

1. Максимальна різниця (Maximum Difference, MaxDiff) – визначає найбільше відхилення значень пікселів між порожнім контейнером (C) та стегоконтейнером (*S)*. Цей показник дозволяє виявити найкритичнішу точку спотворення.

Для розрахунку будемо використовувати наступну формулу (3.2):

$$\max_{x,y} \left| C_{x,y} - S_{x,y} \right|, \tag{3.2}$$

де: $C_{x,y}$ — значення пікселя в оригінальному зображенні (порожньому контейнері);

$S_{x,y}$ — значення пікселя у зображенні з повідомленням (стегоконтейнері).

Даний показник використовується для швидкого виявлення та оцінки найбільшої втрати даних у конкретному пікселі.

Низьке значення MaxDiff свідчить про те, що візуальна якість зображення майже не змінена.

Ідеально коли значення MaxDiff наближається до 0. Занадто високе значення навпаки вказує на значну локальну зміну.

2. Середня абсолютна різниця (Mean Absolute Difference, MAD) - цей показник розраховує середнє відхилення значень пікселів між двома зображеннями, відображаючи загальний рівень викривлення.

Розраховується за формулою (3.3):

$$\frac{1}{XY} \sum_{x,y} |C_{x,y} - S_{x,y}|, \tag{3.3}$$

де: $C_{x,y}$ — значення пікселя в оригінальному зображенні (порожньому контейнері);

$S_{x,y}$ — значення пікселя у зображенні з повідомленням (стегоконтейнері).

Використовується для оцінки загальної схожості між двома зображеннями. Низьке значення MAD свідчить про високу якість відновлення.

Як і з максимальною різницею значення близьке до нуля свідчить про мінімальні викривлення.

3. Нормована середня абсолютна різниця (Normalized Mean Absolute Difference, NAD) – це нормалізована версія середньої абсолютної різниці NAD, яка враховує динамічний діапазон значень пікселів. Використовується для порівняння зображень із різними характеристиками.

Розраховується за формулою (3.4):

$$\frac{\sum_{x,y}|C_{x,y} - S_{x,y}|}{\sum_{x,y}|C_{x,y}|}, \quad (3.4)$$

де: $C_{x,y}$ — значення пікселя в оригінальному зображенні (порожньому контейнері);

$S_{x,y}$ — значення пікселя у зображенні з повідомленням (стегоконтейнері).

MaxValue — максимальне можливе значення пікселя (наприклад, 255 для 8-бітного зображення).

Застосовується для полегшення порівняння якості різних зображень. Забезпечує масштабованість оцінки. Ідеально коли значення NAD близьке до нуля.

4. Нормована середньоквадратична похибка (Normalized Mean Squared Error, NMSE) – цей показник вимірює середньоквадратичну різницю між пікселями оригінального і витягнутого зображень, нормалізовану до динамічного діапазону.

Розраховується за формулою (3.5):

$$\frac{\sum_{x,y}(C_{x,y} - S_{x,y})^2}{\sum_{x,y}(C_{x,y})^2}, \quad (3.5)$$

де: $C_{x,y}$ — значення пікселя в оригінальному зображенні (порожньому контейнері);

$S_{x,y}$ — значення пікселя у зображенні з повідомленням (стегоконтейнері).

Використовується для детального аналізу спотворень зображення. Чутливий до великих відхилень. Значення близьке до нуля означає мінімальні втрати якості.

5. Відношення сигнал/шум (Peak Signal-to-Noise Ratio, SNR) – показник оцінює рівень шуму в зображенні відносно його сигналу. Це найбільш поширений показник для оцінки якості зображень. Відношення сигнал/шум - вказує рівень шуму в отриманому зображенні відносно цільового, чим більше це відношення, тим менше шум спотворює зображення.

Розраховується за формулою (3.6):

$$\frac{\sum_{x,y}(C_{x,y})^2}{\sum_{x,y}(C_{x,y}-S_{x,y})^2}, \tag{3.6}$$

де: $C_{x,y}$ — значення пікселя в оригінальному зображенні (порожньому контейнері);

$S_{x,y}$ — значення пікселя у зображенні з повідомленням (стегоконтейнері).

6. Якість зображення (Information Fidelity, IF) – показник, який також можна назвати «якість зображення», використовується для оцінки ступеня збереження інформації при обробці зображення. Цей показник базується на порівнянні інформації, що міститься в оригінальному зображенні, із відновленим або модифікованим зображенням, оцінюючи втрати, спричинені обробкою.

Розраховується за формулою (3.7):

$$1-\frac{\sum_{x,y}\left(C_{x,y}-S_{x,y}\right)^2}{\sum_{x,y}\left(C_{x,y}\right)^2}, \tag{3.7}$$

де: $C_{x,y}$ — значення пікселя в оригінальному зображенні (порожньому контейнері);

$S_{x,y}$ — значення пікселя у зображенні з повідомленням (стегоконтейнері).

Якість вважається високою, якщо відновлене зображення майже не відрізняється від оригіналу. Ці метрики дозволяють оцінити ефективність

стеганографічного алгоритму та визначити, наскільки приховані дані вплинули на візуальну якість контейнера, забезпечити порівняння різних підходів до приховування інформації [11].

7. Структурний склад (Structure Content, SC) – оцінює структурну схожість між двома зображеннями. Цей показник враховує не тільки рівні яскравості пікселів, але й їх розподіл у зображенні, що дозволяє краще оцінити візуальну якість.

Розраховується за формулою (3.8):

$$\frac{\sum_{x,y}(C_{x,y})^2}{\sum_{x,y}(S_{x,y})^2}, \tag{3.8}$$

де: $C_{x,y}$ — значення пікселя в оригінальному зображенні (порожньому контейнері);

$S_{x,y}$ — значення пікселя у зображенні з повідомленням (стегоконтейнері).

SC використовується для вимірювання структури та розподілу пікселів у зображеннях. Значення SC близькі до 1 вказують на високу структурну схожість між оригінальним і модифікованим зображенням.

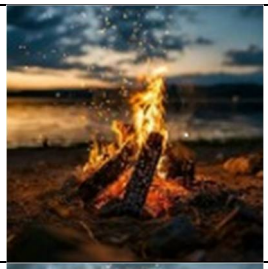
Кожний з цих статистичних показників грає важливу роль у оцінці якості зображення порожнього контейнера (C) та стегоконтейнера (*S)* при використанні стеганографічних методів. Показники викривлення є критично важливими для розробки та вдосконалення стеганографічних алгоритмів, особливо тих, які використовуються для передачі мультимедійних даних.

Використовуючи розглянуті вище статистичні показники ми можемо з їх допомогою додатково переконатись в необхідності збільшення коефіцієнта α-змішування з 0,5 до 0,8. Для цього ми зробимо розрахунки на прикладі першого контейнеру для кожного кольору з палітри RGB окремо. Першим етапом розрахунків є формування масивів необхідних даних. За допомогою пакету математичних обчислень MathCad ми формуємо файли в форматі XLS в яких в першу вкладку будуть записані значення пікселя кожного кольору з палітри RGB для порожнього контейнеру (C1), а в другу вкладку для стегоконтейнеру

(S1). В результаті ми отримуємо три файли в форматі XLS, відповідно до кількості кольорів, кожний з яких містить по дві книги з масивами даних 128 стовбців на 128 рядків, відповідно до розширення BMP файлів які ми використовуємо в нашій роботі. Далі за допомогою вбудованих математичних функцій Microsoft Excel проводяться розрахунки за наведеними вище формулами.

Результати проведених розрахунків по першому контейнеру (C1) по кожному кольору наведені відповідно в таблиці 3.1 для червоного кольору, в таблиці 3.2 для зеленого кольору та в таблиці 3.3 для синього кольору.

Таблиця 3.1 – Порівняння статистичних показників першого контейнера для різних коефіцієнтів α-змішування для червоного кольору.

№	Розрахунковий параметр	Значення при накладенні 0,5	Значення при накладенні 0,8	Зміна розрахункових параметрів про збільшенні коефіцієнту накладання
	Порожній контейнер (C1)			
	Отриманий стегоконтейнер (S1)			
1	MD – максимальна різниця	129,000	56,000	-73,000
2	AD – середня абсолютна різниця	57,586	25,509	-32,077
3	NAD – нормована середня абсолютна різниця	0,716	0,320	-0,396

4	NMSE – нормована середньоквадратична похибка	0,455	0,088	-0,367
5	SNR – відношення «сигнал/шум»	2,199	11,377	+9,179
6	IF – якість зображення	0,545	0,912	+0,367

Таблиця 3.2 – Порівняння статистичних показників першого контейнера для різних коефіцієнтів α-змішування для зеленого кольору.

№	Розрахунковий параметр	Значення при накладенні 0,5	Значення при накладенні 0,8	Зміна розрахункових параметрів про збільшенні коефіцієнту накладання
	Порожній контейнер (C1)			
	Отриманий стегоконтейнер (S1)			
1	MD – максимальна різниця	134,000	56,000	-78,000
2	AD – середня абсолютна різниця	57,351	24,488	-32,863
3	NAD – нормована середня абсолютна різниця	1,008	0,434	-0,574
4	NMSE – нормована середньоквадратична похибка	0,790	0,143	-0,647
5	SNR – відношення «сигнал/шум»	1,265	6,983	+5,718

6	IF – якість зображення	0,210	0,857	+0,647

Таблиця 3.3 – Порівняння статистичних показників першого контейнера для різних коефіцієнтів α-змішування для синього кольору.

№	Розрахунковий параметр	Значення при накладенні 0,5	Значення при накладенні 0,8	Зміна розрахункових параметрів про збільшенні коефіцієнту накладання
	Порожній контейнер (C1)			
	Отриманий стегоконтейнер (S1)			
1	MD – максимальна різниця	132,000	55,000	-77,000
2	AD – середня абсолютна різниця	57,355	23,488	-33,866
3	NAD – нормована середня абсолютна різниця	1,886	0,779	-1,107
4	NMSE – нормована середньоквадратична похибка	2,127	0,361	-1,766
5	SNR – відношення «сигнал/шум»	0,470	2,770	+2,300

6	IF – якість зображення	-1,127	0,639	+1,766

Як можемо побачити з наведених таблиць при збільшенні коефіцієнту α-змішування у всіх кольорових площинах спостерігається зниження максимальної та середньої різниці між відповідними пікселями порожнього контейнеру (C1) та стегоконтейнеру (S1), що свідчить про менші зміни у зображені, а отже і зменшені помітності вбудованого зображення. Якість зображення та відношення сигналу до шуму навпаки зростає у всіх випадках, що також відповідає нашій меті.

Зважаючи на незадовільну якість отриманих стегоконтейнерів (S-0,5) з коефіцієнтом α-змішування = 0,5 в подальшому для розгляду, аналізу значень та вибору оптимального контейнеру будемо розглядати стегоконтейнери отримані з коефіцієнтом α-змішування = 0,8.

Розрахунки також будемо проводити для кожного кольору з палітри RGB окремо. В таблиці 3.4 наведені розрахунки статистичних показників для червоного кольору по всім трьом запропонованим контейнерам. В цій таблиці, а також наступних по зеленому (таблиця 3.5) та синьому (таблиця 3.6) кольором будемо виділяти оптимальні значення по кожному розрахунковому показнику.

Таблиця 3.4 – Порівняння статистичних показників по трьом контейнерам для коефіцієнтів α-змішування 0,8 для червоного кольору.

№	Розрахунковий параметр	Значення для першого контейнера	Значення для другого контейнера	Значення для третього контейнера
1	MD – максимальна різниця	56,000	53,000	64,000
2	AD – середня абсолютна різниця	25,509	24,590	35,028
3	NAD – нормована середня абсолютна різниця	0,320	0,234	0,421

4	NMSE – нормована середньоквадратична похибка	0,088	0,049	0,189
5	SNR – відношення «сигнал/шум»	11,377	20,383	5,280
6	IF – якість зображення	0,912	0,951	0,811
7	SC – структурний склад	0,763	0,970	0,552

Розглянемо кожен показник більш докладно, щоб краще зрозуміти характеристики трьох контейнерів.

Максимальна різниця (MD) представляє максимальне відхилення між значеннями в порожньому контейнері та стегоконтейнері. Для першого контейнера максимальна різниця становить 56,000, для другого – 53,000, а для третього – 64,000. Це вказує на те, що найбільші коливання значень спостерігаються у третьому контейнері, що може свідчити про менш стабільні дані.

Середня абсолютна різниця (AD) вимірює середнє абсолютне відхилення значень від середнього. Значення AD для першого контейнера – 25,509, для другого – 24,590, а для третього – 35,028. Найменше значення AD у другого контейнера свідчить про те, що його значення більш згруповані біля середнього, тобто він має найбільш стабільні показники.

Нормована середня абсолютна різниця (NAD) нормує середню абсолютну різницю щодо середнього значення. Для першого контейнера значення NAD – 0,320, для другого – 0,234, а для третього – 0,421. Знову ж таки, другий контейнер демонструє найменше відхилення від середнього значення, що підкреслює його стабільність.

Нормована середньоквадратична похибка (NMSE) оцінює середньоквадратичну похибку між значеннями в порожньому контейнері та стегоконтейнері. Показники NMSE для першого контейнера – 0,088, для другого – 0,049, а для третього – 0,189. Найменша похибка у другого контейнера свідчить про високу точність даних.

Відношення «сигнал/шум» (SNR) визначає відношення потужності сигналу до рівня шуму. Значення SNR для першого контейнера – 11,377, для другого – 20,383, а для третього – 5,280. Високе значення SNR у другого контейнера означає, що він має кращу якість передачі сигналу з мінімальним шумом.

Якість зображення (IF) оцінює якість зображення. Значення IF для першого контейнера – 0,912, для другого – 0,951, а для третього – 0,811. Другий контейнер демонструє найвищу якість зображення.

Структурний склад (SC) оцінює схожість з оригіналом. Значення SC для першого контейнера – 0,763, для другого – 0,970, а для третього – 0,552. Найвище значення SC для другого контейнера свідчить про найбільшу схожість порожнього контейнера з стегоконтейнером.

Загалом, другий контейнер має найкращі показники стабільності, точності та якості серед трьох контейнерів, що робить його найоптимальнішим вибором для задач, де потрібна висока якість даних. Третій контейнер має найгірші показники, що може свідчити про велику кількість шуму і менш стабільні дані. Перший контейнер займає проміжне положення, маючи деякі характеристики, схожі на обидва контейнери.

Таблиця 3.5 – Порівняння статистичних показників по трьом контейнерам для коефіцієнтів α-змішування 0,8 для зеленого кольору.

№	Розрахунковий параметр	Значення для першого контейнера	Значення для другого контейнера	Значення для третього контейнера
1	MD – максимальна різниця	56,000	61,000	64,000
2	AD – середня абсолютна різниця	24,488	26,495	29,573
3	NAD – нормована середня абсолютна різниця	0,434	0,338	0,344
4	NMSE – нормована середньоквадратична похибка	0,143	0,104	0,130

5	SNR – відношення «сигнал/шум»	6,983	9,605	7,695
6	IF – якість зображення	0,857	0,896	0,870
7	SC – структурний склад	0,647	0,714	0,610

По зеленій кольоровій площині з таблиці 3.5 максимальна різниця найбільша у третього контейнера (64,000), трохи менша у другого (61,000) і найменша у першого (56,000). Це вказує на те, що третій контейнер має найбільші відхилення в значеннях, тоді як перший - найменші. Показники для зеленого кольору вище, ніж найкращий показник для червоного кольору, що свідчить про більші відхилення в значеннях для зеленого кольору.

Середня абсолютна різниця найменша у першого контейнера (24,488), середня у другого (26,495) і найбільша у третього (29,573). Це свідчить про те, що перший контейнер має більш згруповані значення навколо середнього, тоді як третій контейнер має найбільші відхилення. AD для першого контейнера зеленого кольору трохи менша, ніж найкращий показник для червоного кольору, що свідчить про більш згруповані значення навколо середнього.

Значення NAD найменше у другого контейнера (0,338), трохи більше у третього (0,344) і найбільше у першого (0,434). Це свідчить про те, що другий контейнер має найменші відхилення від середнього значення, тоді як перший контейнер має найбільші. Значення для зеленого кольору вища, ніж найкращий показник для червоного кольору, що свідчить про більші відхилення від середнього значення.

Нормована середньоквадратична похибка найменша у другого контейнера (0,104), середня у третього (0,130) і найбільша у першого (0,143). Це означає, що другий контейнер має найвищу точність, тоді як перший контейнер - найменшу. Як і попередній показник для зеленого кольору значення вище, ніж найкращий показник для червоного кольору, що свідчить про більші відхилення від середнього значення.

Відношення сигнал/шум найвище у другого контейнера (9,605), середнє у третього (7,695) і найнижче у першого (6,983). Це означає, що другий контейнер має найкращу якість передачі сигналу, тоді як перший контейнер – найгіршу. Відношення «сигнал/шум» для зеленого кольору значно нижче, ніж показники для червоного кольору, що вказує на гіршу якість передачі сигналу.

Якість зображення, в цій кольоровій площині, найвища у другого контейнера (0,896), трохи менша у третього (0,870) і найнижча у першого (0,857). Це свідчить про те, що другий контейнер забезпечує найкращу якість зображення. Загалом якість зображення для зеленого кольору нижча, в порівнянні з червоним.

Структурний склад найвищий у другого контейнера (0,714), середній у першого (0,647) і найнижчий у третього (0,610). Це означає, що другий контейнер має найбільшу схожість з оригіналом, тоді як третій контейнер - найменшу. Структурний склад для зеленого кольору значно нижчий, ніж найкращий показник для червоного кольору, що свідчить про меншу схожість з оригіналом.

Другий контейнер знову демонструє найкращі показники стабільності, точності та якості серед трьох контейнерів для зеленого кольору. Перший контейнер має деякі переваги у меншому відхиленні значень, але поступається за іншими показниками. З аналізу видно, що показники для зеленого кольору загалом гірші, ніж найкращі показники для червоного кольору з таблиці 3.4. Другий контейнер для зеленого кольору все ж демонструє найкращі результати серед трьох контейнерів, але йому все ще бракує досягнення найвищих показників, які ми бачимо для червоного кольору у другому контейнері.

Таблиця 3.6 – Порівняння статистичних показників по трьом контейнерам для коефіцієнтів α-змішування 0,8 для синього кольору.

№	Розрахунковий параметр	Значення для першого контейнера	Значення для другого контейнера	Значення для третього контейнера

1	MD – максимальна різниця	55,000	55,000	64,000
2	AD – середня абсолютна різниця	23,488	18,614	30,917
3	NAD – нормована середня абсолютна різниця	0,779	0,281	0,768
4	NMSE – нормована середньоквадратична похибка	0,361	0,070	0,470
5	SNR – відношення «сигнал/шум»	2,770	14,263	2,128
6	IF – якість зображення	0,639	0,930	0,530
7	SC – структурний склад	0,497	0,794	0,448

Як бачимо з таблиці 3.6 у всіх трьох контейнерів максимальна різниця для синього кольору є досить високою, але не відрізняється суттєво між контейнерами.

Середня абсолютна різниця (AD) другого контейнеру має значно менше значення порівняно з іншими контейнерами, що вказує на більшу стабільність даних.

Другий контейнер має найнижчу нормовану середню абсолютну різницю (NAD), що свідчить про найменші відхилення від середнього значення.

Показники нормованої середньоквадратичної похибки також найменші у другого контейнера, що вказує на високу точність даних.

Другий контейнер демонструє найвище відношення «сигнал/шум», що свідчить про кращу якість передачі сигналу з мінімальним шумом. Також в нього найкраща якість зображення та вища схожість з оригіналом.

Проаналізувавши всі показники для червоного, зеленого та синього кольорів з трьох таблиць, можна зробити узагальнений висновок, що другий контейнер постійно демонструє найкращі результати у більшості параметрів для всіх трьох кольорів. Він має найменші відхилення, високу точність та найкращу якість зображення. Це свідчить про те, що другий контейнер забезпечує найбільш стабільні і точні дані, а також має найменше шумів і

найвищу якість сигналу. Його структурний склад також показує високу схожість з оригіналом, що важливо для збереження візуальної якості.

Таким чином, другий контейнер є найкращим вибором серед трьох контейнерів для роботи зі стеганографією, оскільки він забезпечує найвищу якість та стабільність даних для різних кольорів. Якщо вам потрібно зберегти високу якість зображень та точність даних, другий контейнер буде найоптимальнішим вибором.

Якість витягнутих повідомлень (V) відіграє дуже важливу роль в виборі контейнера, тому ми також розглянемо статистичні показники і по ним. Хоча ми і відкинули формування стегоконтейнерів з коефіцієнтом α-змішування = 0,5 через їх не відповідність умовам непомітності та незначного викривлення стегоконтейнера, проте вони забезпечують найкращу якість витягнутого зображення. Для наочності ми порівняємо значення статистичних показників між цільовим зображенням (T) та витягнутими зображеннями зі стегоконтейнерів (S-0,5) в таблиці 3.7 для червоного кольору, в таблиці 3.8 для зеленого кольору та в таблиці 3.9 для синього кольору.

Таблиця 3.7 – Порівняння статистичних показників витягнутих зображень по трьом контейнерам для коефіцієнтів α-змішування 0,5 для червоного кольору.

№	Розрахунковий параметр	Значення для V з першого контейнера	Значення для V з другого контейнера	Значення для V з третього контейнера
1	MD – максимальна різниця	13,000	18,000	55,000
2	AD – середня абсолютна різниця	3,972	4,918	15,101
3	NAD – нормована середня абсолютна різниця	0,022	0,034	0,107
4	NMSE – нормована середньоквадратична похибка	0,001	0,001	0,019
5	SNR – відношення	1469,878	666,889	52,034

	«сигнал/шум»			
6	IF – якість зображення	0,999	0,999	0,981

На основі проведеного аналізу можна зробити висновок, що перший контейнер демонструє найкращі показники для витягнутих зображень при коефіцієнті α-змішування 0,5 для червоного, зеленого та синього кольорів. Він забезпечує найвищу стабільність, точність, менші відхилення значень, мінімальний рівень шуму та високу якість зображення.

Таким чином, для витягнутих зображень перший контейнер є найкращим вибором серед трьох контейнерів, особливо при роботі з червоним кольором, де він демонструє максимальні показники якості.

Таблиця 3.8 – Порівняння статистичних показників витягнутих зображень по трьом контейнерам для коефіцієнтів α-змішування 0,5 для зеленого кольору.

№	Розрахунковий параметр	Значення для V з першого контейнера	Значення для V з другого контейнера	Значення для V з третього контейнера
1	MD – максимальна різниця	41,000	54,000	78,000
2	AD – середня абсолютна різниця	11,609	14,415	20,804
3	NAD – нормована середня абсолютна різниця	0,073	0,114	0,167
4	NMSE – нормована середньоквадратична похибка	0,009	0,020	0,044
5	SNR – відношення «сигнал/шум»	105,728	49,344	22,515
6	IF – якість зображення	0,991	0,980	0,956

Таблиця 3.9 – Порівняння статистичних показників витягнутих зображень по трьом контейнерам для коефіцієнтів α-змішування 0,5 для синього кольору.

№	Розрахунковий параметр	Значення для V з першого контейнера	Значення для V з другого контейнера	Значення для V з третього контейнера
1	MD – максимальна різниця	33,000	31,000	54,000
2	AD – середня абсолютна різниця	9,810	7,988	14,259
3	NAD – нормована середня абсолютна різниця	0,054	0,078	0,140
4	NMSE – нормована середньоквадратична похибка	0,005	0,008	0,027
5	SNR – відношення «сигнал/шум»	183,639	130,514	37,525
6	IF – якість зображення	0,995	0,992	0,973

Тепер розглянемо аналогічні показники для витягнутого зображення з стегоконтейнерів для формування яких використовувався коефіцієнт α-змішування 0,8 для врахування його при остаточному виборі контейнеру для передачі секретного зображення. Ці показники будуть наведені в таблиці 3.10 для червоного кольору, в таблиці 3.11 для зеленого кольору та в таблиці 3.12 для синього кольору.

Таблиця 3.10 – Порівняння статистичних показників витягнутих зображень по трьом контейнерам для коефіцієнтів α-змішування 0,8 для червоного кольору.

№	Розрахунковий параметр	Значення для V з першого контейнера	Значення для V з другого контейнера	Значення для V з третього контейнера
1	MD – максимальна різниця	37,000	14,000	96,000
2	AD – середня абсолютна різниця	12,938	4,382	26,349
3	NAD – нормована середня абсолютна різниця	0,074	0,032	0,193
4	NMSE – нормована середньоквадратична	0,007	0,001	0,051

	похибка			
5	SNR – відношення «сигнал/шум»	151,395	845,564	19,449
6	IF – якість зображення	0,993	0,999	0,949

Для показників витягнутих зображень з коефіцієнтом α-змішування 0,8, перший і другий контейнери показують найкращі результати. Другий контейнер домінує за якістю передачі сигналу і точністю даних для червоного кольору, тоді як перший контейнер показує стабільні результати для зеленого і синього кольорів.

Таким чином, для червоного кольору другий контейнер є оптимальним вибором, а для зеленого і синього кольорів перший контейнер демонструє кращі результати.

Таблиця 3.11 – Порівняння статистичних показників витягнутих зображень по трьом контейнерам для коефіцієнтів α-змішування 0,8 для зеленого кольору.

№	Розрахунковий параметр	Значення для V з першого контейнера	Значення для V з другого контейнера	Значення для V з третього контейнера
1	MD – максимальна різниця	37,000	54,000	76,000
2	AD – середня абсолютна різниця	12,938	16,043	19,783
3	NAD – нормована середня абсолютна різниця	0,074	0,103	0,163
4	NMSE – нормована середньоквадратична похибка	0,007	0,016	0,041
5	SNR – відношення «сигнал/шум»	151,395	64,464	24,628
6	IF – якість зображення	0,993	0,984	0,959

Таблиця 3.12 – Порівняння статистичних показників витягнутих зображень по трьом контейнерам для коефіцієнтів α-змішування 0,8 для синього кольору.

№	Розрахунковий параметр	Значення для V з першого контейнера	Значення для V з другого контейнера	Значення для V з третього контейнера
1	MD – максимальна різниця	37,000	42,000	89,000
2	AD – середня абсолютна різниця	12,094	11,068	22,405
3	NAD – нормована середня абсолютна різниця	0,068	0,112	0,229
4	NMSE – нормована середньоквадратична похибка	0,007	0,014	0,046
5	SNR – відношення «сигнал/шум»	147,994	73,196	21,677
6	IF – якість зображення	0,993	0,986	0,954

Отже другий контейнер постійно показує найкращі результати за багатьма критеріями, такими як менша максимальна різниця, менша середня абсолютна різниця, менша нормована середня абсолютна різниця та низька нормована середньоквадратична похибка. Відношення «сигнал/шум» також значно вище у другого контейнера, що вказує на кращу якість передачі сигналу з мінімальним рівнем шуму. Якість зображення також вища у другого контейнера порівняно з іншими контейнерами. Це справедливо для всіх кольорів (червоний, зелений і синій).

Для витягнутих зображень з коефіцієнтом α-змішування 0,5 та 0,8, перший контейнер часто демонструє менші відхилення, більш стабільні дані та високу якість зображення. Це особливо помітно для червоного кольору, де перший контейнер має найкращі показники. Проте, для коефіцієнта α-змішування 0,8 червоного кольору другий контейнер демонструє дуже високі показники якості сигналу, що також варто враховувати.

ВИСНОВКИ

Відповідно до мети роботи було досліджено використання алгоритму Дея в контексті стеганографічної передачі цільового зображення та здійснено вибір оптимального контейнеру з трьох потенційних, який забезпечив мінімальне викривлення стегоконтейнеру та високу якість витягнутого зображення.

Вибір оптимального контейнеру було зроблено не лише на основі суб'єктивної візуальної оцінки отриманих стегоконтейнерів і витягнутих цільових повідомлень, а і на основі аналізу розрахункових статистичних показників. Розрахунки додатково підтвердили вибір контейнеру і додали йому числової вимірюваності. Проаналізувавши показники по всім кольоровим площинам (R, G, B) кожного стегоконтейнера можна зробити висновок, що другий контейнер постійно демонструє найкращі результати по більшості параметрів. Він має найменші відхилення, високу точність та найкращу якість зображення, має найменше шумів. Його структурний склад також показує

високу схожість з оригіналом, що важливо для збереження візуальної якості. Стосовно витягнутих зображень то тут найкращі результати показують перший та другий контейнер. Підсумовуючи можемо дійти загального висновку в оптимальності вибору другого контейнеру для стеганографічної передачі цільового повідомлення забезпечуючи мінімальне спотворення стегоконтейнеру та добру якість витягнутого зображення.

Це дослідження показує ефективність методу Дея в практичних завданнях стеганографії при роботі з цифровими зображеннями які стали однією з найбільш популярних платформ для стеганографічного приховування інформації, завдяки їхній великій поширеності, доступності, великій ємності для вміщення даних та можливості мінімізувати візуальні зміни.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Хорошко В.О. Комп'ютерна стеганографія: навчальний посібник / В.О.Хорошко, Ю.Є. Яремчук, В.В. Карпінець. − Вінниця: ВНТУ, 2017. − 155 с.
2. Кузнецов О. О. Стеганографія : навчальний посібник / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2011. – 232 с.
3. Конахович Г.Ф. Комп'ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник / Г.Ф. Конахович, Д.О. Прогонов, О.Ю. Пузиренко. – Київ: Центр учбової літератури, 2018. – 558 с.
4. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. – Київ: МК-Пресс, 2006. – 288 с.
5. Blossom Kaur, Amandeep Kaur, Jasdeep Singh, Steganographic Approach for Hiding Image in DCT Domain / International Journal of Advances in Engineering & Technology, Issue 3 – No.3, July 2011, pp. 72-78.

6. Nilanjan Dey, Anamitra Bardhan Roy, Sayantan Dey, A Novel Approach of Color Image Hiding using RGB Color planes and DWT / International Journal of Computer Applications, Volume 36 – No.5, December 2011.
7. Дурняк Б. В. Стеганографічні методи захисту документів / Б. В. Дурняк, Д. В. Музика, В. І. Сабат. — Львів: Укр. акад. друкарства, 2014. — 159 с.
8. Денисюк В. О.Стеганографічний алгоритм захисту даних з використанням файлів зображень / Електронний журнал "Ефективна економіка", 2017 р. – № 5.– Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5584.
9. Швідченко І.В. Методи виявлення стеганографічного приховання інформації в зображеннях / Інститут кібернетики імені В.М. Глушкова НАН України, 2015р. – Режим доступу: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3737/shvidchenkoiv.pdf .
10. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави / Мельник С.В., Кондакова С.В. // Актуальні проблеми управління інформаційною безпекою держави : Всеукр. науково-практична конф.: зб. тез наукових доповідей. – К. : Наук.-вид. відділ НА СБ України, 2010. – С. 134-138.
11. Горніцька Д. А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, О.Г. Корченко, В.В. Волянська // Захист інформації. – 2012. – №1. – С. 108 – 121.