Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)
Кафедра *Інформаційно-мережної інженерії*
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження моделей приховування інформації в мультимедійних даних з використанням стеганографічних перетворень
(тема)

Виконав:
здобувач *2* року навчання,
групи *ІМІм-24-1*
Олександр Картушин
(власне ім'я, прізвище)

Спеціальність *172 Електронні комунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *освітньо-професійна*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *проф. Валерій Безрук*
(посада, власне ім'я, прізвище)

Допускається до захисту
Зав. кафедри _____ *Микола Москалець*
(підпис) (власне ім'я, прізвище)

2025 р.

Не містить відомостей заборонених до відкритого публікування.

Студент _____ / Картушин О.А. /

Керівник _____ / Безрук В.М. /

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
Кафедра *Інформаційно-мережної інженерії*
Рівень вищої освіти *другий (магістерський)*
Спеціальність *172 «Електронні комунікації та радіотехніка»*
(код і повна назва)
Тип програми *освітньо-професійна*
Освітня програма *«Інформаційно-мережна інженерія»*
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові *Картушину Олександру Андрійовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Дослідження моделей приховування інформації в мультимедійних даних з використанням стеганографічних перетворень*

затверджена наказом університету від 24 жовтня 2025 р. № 959 Ст

2. Термін подання студентом роботи до екзаменаційної комісії 22 грудня 2025 р.

3. Вихідні дані до роботи *Дослідити методи цифрової стеганографії для приховування інформації при передачі мультимедійного трафіку в інфокомунікаційних мережах. Провести порівняльний аналіз існуючих методів стеганографії для вбудовування інформації в зображення. На основі виявлених недоліків запропонувати рішення, що дозволить підвищити пропускну здатність при передачі мультимедійної інформації без впливу на рівень її захисту. Провести порівняльну оцінку запропонованого методу із класичними найбільш розповсюдженими методами цифрової стеганографії.*

4. Перелік питань, що потрібно опрацювати в роботі
Вступ
1. Основні відомості про цифрову стеганографію
2. Аналіз сучасних рішень приховування інформації в мультимедіа
3. Аналіз та розробка моделі стеганографічних перетворень медіаданих з метою підвищення ефективності приховування інформації
4. Оцінка ефективності запропонованого стеганографічного методу приховування інформації в медіатрафіку
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *назва, мета і актуальність кваліфікаційної роботи; класифікація методів стеганографії; загальна модель стегосистеми; переваги використання зображень для побудови прихованих контейнерів; базові методи стеганографії для приховування інформації у просторовій та частотній областях зображення; ключові характеристики методів цифрової стеганографії; значення кількісних показників базових методів стеганографії; аналіз якісних показників базових методів стеганографії; основні недоліки існуючих методів стеганографії; розробка методу на основі дискретного вейвлет-перетворення; варіант хвильового-перетворення третім каскадом; оцінка ефективності розробленого методу; порівняння пропускної здатності методів цифрової стеганографії, висновки*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	*Ознайомлення із завданням. Уточнення ТЗ.*	*24.10.25*	*виконано*
2	*Підбір літератури за темою роботи.*	*25.10-05.11.25*	*виконано*
3	*Основні відомості про цифрову стеганографію*	*06.11-10.11.25*	*виконано*
4	*Аналіз сучасних рішень приховування інформації в мультимедіа*	*11.11-20.11.25*	*виконано*
5	*Аналіз та розробка моделі стеганографічних перетворень медіаданих з метою підвищення ефективності приховування інформації*	*21.11-09.12.25*	*виконано*
6	*Оцінка ефективності запропонованого стеганографічного методу приховування інформації в медіатрафіку*	*10.12-17.12.25*	*виконано*
7	*Оформлення презентаційного матеріалу, підготовка до захисту в ЕК*	*18.12.25*	*виконано*

Дата видачі завдання _24_ ___жовтня__ 2025 р.

Студент _____
(підпис)

Керівник роботи _____ проф. Валерій Безрук
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка 66 с., 15 рис., 5 табл., 24 джерела, 2 додатки.

Об'єкт дослідження – процеси приховування інформації в мультимедійних даних.

Мета роботи – дослідити існуючі моделі цифрової стеганографії та розробити нову модель підвищення пропускної спроможності каналу передачі відеоінформаційних даних на основі стеганографічного перетворення.

Досліджено різновиди методів цифрової стеганографії, виявлено що вони мають ряд недоліків.

Обґрунтовано необхідність застосування методів цифрової стеганографії для захисту інформації в інфокомунікаційних системах.

Визначено рекомендації щодо підвищення пропускної спроможності при використанні методів вбудовування в область перетворення.

Розроблено метод підвищення пропускної спроможності скритого каналу передачі відеоінформаційних ресурсів на основі використання стеганографічного перетворення.

Розраховано показники якості розробленого стеганографічного методу.

ЦИФРОВА СТЕГАНОГРАФІЯ, ТЕЛЕКОМУНІКАЦІЙНИЙ КАНАЛ, ЗАХИСТ ДАНИХ, СТЕГАНОГРАФІЧНИЙ КАНАЛ, ВІДЕОТРАФІК, ПЕРЕТВОРЕННЯ ХААРА, ПЕРЕТВОРЕННЯ УОЛША-АДАМА.

THE ABSTRACT

Explanatory slip 66 p., 15 figures, 5 tables, 24 sources, 2 attach.

Object of research - information hiding processes in multimedia data.

The purpose of the work - to investigate existing models of digital steganography and develop a new model for increasing the bandwidth of the video data transmission channel based on steganographic transformation.

Various methods of digital steganography have been studied, and it has been found that they have a number of shortcomings.

The need to use digital steganography methods to protect information in infocommunication systems has been substantiated.

Recommendations for increasing throughput when using embedding methods in the transformation domain are determined.

A method for increasing the throughput of a covert channel for the transmission of video information resources based on the use of steganographic transformation has been developed.

The quality indicators of the developed steganographic method are calculated.

DIGITAL STEGANOGRAPHY, TELECOMMUNICATIONS CHANNEL, DATA PROTECTION, STEGANOGRAPHIC CHANNEL, VIDEO TRAFFIC, HAAR TRANSFORM, WALSH-ADAM TRANSFORM.

ЗМІСТ

С.

ПЕРЕЛІК СКОРОЧЕНЬ

БМЕЮ	–	метод Бенгама-Мемона-Ео-Юнга;
ДВП	–	дискретне вейвлет-перетворення;
ДКП	–	дискретно-косинусне перетворення;
ДХП	–	дискретне хвильове перетворення;
СКВ	–	середньоквадратичне відхилення;
ЗК	–	зображення-контейнер;
IF	–	якість візуального сприйняття;
НЗБ	–	найменш значущий біт;
ПСП	–	псевдовипадкова послідовність бітів;
ПВСШ	–	пікове відношення сигнал-шум;
ЦС	–	цифрова стеганографія.

ВСТУП

Обмеження на використання криптографії в багатьох країнах та зростаюча потреба захищати цифрову власність роблять стеганографію надзвичайно важливою галуззю для досліджень. Надійний захист даних від несанкціонованого доступу залишається актуальною, але ще не повністю вирішеною проблемою.

Запровадження обмежень на криптографію, таких як вимога надавати ключі шифрування або обов'язкова реєстрація систем, стало потужним стимулом для розвитку стеганографії. На відміну від криптографії, стеганографія не підпадає під ці обмеження і ефективно приховує передачу даних. Вона ідеально підходить для конфіденційного обміну інформацією, захисту авторських прав та приховування даних без привернення уваги [1].

Сучасні технології зв'язку та автоматизації вимагають швидших та надійніших методів захисту інформації. Тому цифрова стеганографія стає необхідною для забезпечення безпеки даних у сучасному світі.

Актуальність цієї теми підкреслюється тим, що передача інформації в реальному часі часто ускладнюється. Методи стиснення та криптографії можуть порушувати структуру даних, збільшуючи час обробки. Цифрова стеганографія, навпаки, дозволяє вбудовувати інформацію без зміни її обсягу та структури, що робить її більш ефективною.

Таким чином, дослідження, спрямовані на підвищення захисту та достовірності мультимедійної інформації в умовах кіберзагроз, є надзвичайно актуальними.

Мета роботи: розробити модель для збільшення пропускної здатності каналу передачі відеоданих за допомогою стеганографічних методів, забезпечуючи захист від зловмисників.

1 ОСНОВНІ ВІДОМОСТІ ПРО ЦИФРОВУ СТЕГАНОГРАФІЮ

1.1 Поняття та класифікація стеганографії

Проблема безпеки інформації від несанкціонованого доступу є вічною. Ще з давніх часів людство розробляло способи її захисту, серед яких виділяються два ключові напрямки, що залишаються актуальними й сьогодні: криптографія та стеганографія. Якщо криптографія зосереджується на шифруванні змісту повідомлення, то стеганографія, що буквально означає "тайнопис" (з грецької), має на меті приховати сам факт існування секретної інформації. Ці два методи часто використовуються в комплексі, взаємно доповнюючи один одного.

Більшість наукових робіт у сфері стеганографії [2–6] присвячена створенню нових та покращенню існуючих технік приховування даних. Однак, незважаючи на постійне зростання кількості таких методів, у сучасній науковій літературі відсутня уніфікована класифікація, що ускладнює їх систематизацію та ефективне використання.

1.1.1 Класична стеганографія

Згідно з класифікацією О.І. Стасюка, стеганографія поділяється на класичну, цифрову, лінгвістичну та квантову. Класичні методи передбачають використання технічних засобів для приховування інформації, тоді як сучасні підходи охоплюють фізичні та хімічні техніки (рис. 1.1) [2].

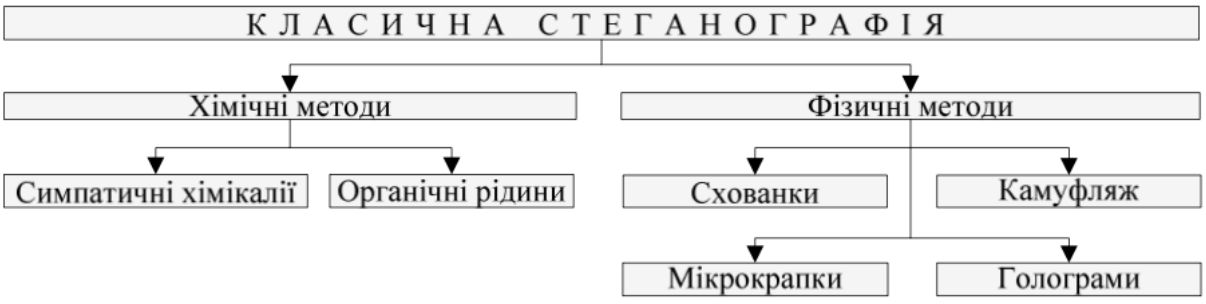

Рисунок 1.1 – Методи класичної стеганографії

В цілому, *хімічні методи* стеганографії базуються на використанні невидимого чорнила. До таких прийомів належать застосування симпатичних речовин і органічних розчинників. Симпатичні хімікати [4] є одними з найпоширеніших традиційних способів прихованого письма. Зазвичай процес записи виглядає так: спочатку наносять важливий текст невидимим чорнилом, а потім – другий, незначущий запис видимим. Повідомлення, написане подібним чином, проявляється лише за певних умов, наприклад, при нагріванні, освітленні або обробці хімічним реактивом. Органічні рідини мають схожі характеристики – під впливом нагріву вони темніють завдяки високому вмісту вуглецю [4].

До *фізичних методів* можна віднести різноманітні схованки, камуфляжні прийоми та використання мікрокрапок. Сьогодні такі методи викликають інтерес у дослідженнях різних носіїв інформації з метою прихованого запису, який не виявляється стандартними способами зчитування. Особливу увагу приділяють стандартним носіям, а також пристроям для обробки обчислювальної, аудіо- та відеоінформації. Окрім того, з’явилися новітні технології, які, спираючись на традиційну стеганографію, використовують досягнення мікроелектроніки, зокрема голографію [6]. Такі схованки для секретних повідомлень застосовувались ще в Стародавній Греції - вони маскувалися у вигляді осей возів, підошв сандалів чи підкладок плащів. Форма схованок може бути дуже різною [3, 4]. Сучасною версією такого прихованого сховку став Інтернет.

Мікрокрапки як засіб стеганографії були розроблені в Німеччині між двома світовими війнами. Згодом вони отримали широке застосування у багатьох країнах для передачі секретної інформації поштою. Замість класичних галогенідів срібла почали використовувати світлочутливі матеріали на основі аніліну, що значно ускладнило їхнє виявлення. Після зведення Берлінської стіни виготовлення мікрокрапок здійснювалося за допомогою спеціальних фотокамер. Ці крапки прикріплювали до непримітних листів і пересилали поштою. Завдяки своєму дуже маленькому розміру, мікрокрапки, як правило, залишалися непоміченими. Одержувач міг прочитати приховане послання за допомогою мікроскопа [7].

Метод на голографічній основі. Його суть полягає у вбудовуванні голограм конфіденційних даних замість самих даних у зображення-контейнер. Цей підхід забезпечує найвищий рівень захисту від несанкціонованого доступу.

Використання голографії дозволяє приховувати секретну інформацію в звичайних фотографіях, як на паперовій, так і на пластиковій основі. Основний недолік полягає в обмеженій місткості для вбудовуваних даних. Тому голографічний підхід найефективніший для приховування невеликих зображень, які можуть витримати незначну втрату якості при відновленні, таких як зразки підписів або відбитків пальців [8].

При використанні *методу камуфляжу* конфіденційне повідомлення приховується шляхом його інтеграції в зовнішній вигляд об'єкта-контейнера, щоб воно стало практично непомітним [4].

Серед переваг класичної стеганографії можна виділити легкість її реалізації, тоді як основними недоліками є складність практичного втілення та ймовірність випадкового виявлення прихованого повідомлення.

1.1.2 Цифрова стеганографія

Цифрова стеганографія [5, 6] (рис. 1.2) полягає у приховуванні або вбудовуванні додаткової інформації в цифрові об'єкти, що призводить до незначних змін у них. Зазвичай, ці об'єкти є мультимедійними, і внесені спотворення настільки малі, що не сприймаються людським оком, не викликаючи помітних змін.

Рисунок 1.2 – Методи цифрової стеганографії

Приховування інформації в зображеннях (стеганографія в просторовій області) може бути реалізовано за допомогою таких підходів [2]:

1) заміна найменш значущих бітів (LSB): Цей метод полягає в тому, що останні, найменш важливі біти кожного пікселя зображення-контейнера замінюються бітами секретного повідомлення;

2) метод псевдовипадкового інтервалу – секретні біти розподіляються по зображенню-контейнеру випадковим чином. Відстань між місцями, куди вбудовується кожен біт секретного повідомлення, визначається за допомогою псевдовипадкової послідовності;

3) метод псевдовипадкової перестановки. Використовується генератор псевдовипадкових чисел для створення послідовності індексів пікселів. Кожен біт секретного повідомлення зберігається у пікселі, що відповідає черговому індексу з цієї послідовності. Це забезпечує рівномірне розподілення секретних даних по всьому зображенню;

4) метод блокового приховування. Зображення розбивається на окремі блоки. Для кожного блоку обчислюється біт парності. Потім один секретний біт вбудовується в кожен блок. Якщо біт парності блоку не збігається з секретним бітом, то один з найменш значущих бітів блоку змінюється так, щоб біт парності став рівним секретному біту;

5) метод заміни палітри. Якщо зображення використовує палітру кольорів, де кожен колір представлений певним індексом, секретна інформація може бути прихована шляхом зміни порядку кольорів у цій палітрі. Оскільки порядок кольорів не впливає на візуальне сприйняття зображення, це дозволяє непомітно вбудувати дані;

6) метод квантування зображення [6]. Цей метод передбачає коригування певних значень у зображенні (наприклад, різницевих сигналів). Секретний ключ у цьому випадку може бути таблицею, яка співвідносить кожне можливе значення коригування з певним бітом секретного повідомлення;

7) метод Куттера-Джордана-Боссена – цей алгоритм зосереджується на вбудовуванні інформації в синій колірний канал зображення. Це робиться тому, що людське око найменш чутливе до змін у синьому кольорі, що робить приховування більш ефективним;

8) метод Дармстедтера-Делейгла-Квісквотера-Макка – цей підхід базується на принципах людського сприйняття. Секретна інформація спочатку перетворюється на послідовність двійкових даних. Потім кожен біт цієї послідовності вбудовується в окремий блок зображення, враховуючи

особливості вмісту цього блоку, щоб зробити вбудовування максимально непомітним [2].

Існує кілька способів *приховати інформацію в частотній області* зображень. Серед них виділяються такі:

1) метод відносної заміни величин коефіцієнтів дискретно косинусного перетворення (ДКП) (метод Коха і Жао) – це один з найпопулярніших методів для вбудовування секретної інформації в частотну сферу зображень. Його суть полягає у відносній зміні значень коефіцієнтів ДКП. Процес починається з розбиття зображення на блоки розміром 8x8 пікселів. Потім до кожного такого блоку застосовується ДКП, що призводить до отримання матриці коефіцієнтів 8x8. Кожен блок призначений для зберігання одного біта прихованої інформації;

2) метод Бенгама-Мемона-Ео-Юнга. Цей метод є вдосконаленою версією попереднього. Оптимізація досягається двома шляхами: використовуються не всі блоки зображення, а лише ті, які найкраще підходять для вбудовування даних; замість двох, для вбудовування в частотній області вибираються три коефіцієнти ДКП;

3) метод Хсу і Ву. Цей метод передбачає вбудовування цифрового водяного знака безпосередньо в масив коефіцієнтів ДКП, отриманих з блоків зображення-контейнера;

4) метод Фрідріха. Цей метод є комбінованим. Він поєднує два алгоритми: один з них вбудовує приховані дані в низькочастотні коефіцієнти ДКП, а інший – у середньочастотні [2].

Методами приховування при розширенні спектру є наступні:

1) метод прямої псевдовипадкової послідовності: цей метод полягає в тому, що інформаційний сигнал, який розширюється за допомогою прямої послідовності, модулюється функцією. Ця функція генерує псевдовипадкові значення в заданих межах і множиться на тимчасову константу, яка визначає швидкість проходження елементів сигналу. Отриманий псевдовипадковий сигнал містить компоненти на всіх частотах. При розширенні ці компоненти модулюють енергію сигналу в широкому діапазоні частот;

2) метод стрибкоподібного перебудовування частот: При використанні цього методу передавач миттєво перемикається з однієї частоти несучого

сигналу на іншу. Секретним ключем для цього процесу є псевдовипадковий закон, за яким відбувається зміна частот;

3) Метод компресії з використанням лінійної частотної модуляції (ЛЧМ): Цей метод базується на тому, що при компресії сигналу за допомогою ЛЧМ, його частота змінюється в часі за певною функцією [2].

Приховування даних в аудіосигналах [6] використовує такі методи:

1) кодування найменш значущих біт (часова область). Цей метод передбачає використання звукового сигналу, де найменш значущі біти (НЗБ) кожної точки вибірки, представленої двійковою послідовністю, замінюються прихованими даними;

2) фазове кодування (частотна область) - суть цього методу полягає в тому, що фаза вихідного звукового сегмента замінюється на опорну фазу. Характер зміни цієї опорної фази відображає приховані дані;

3) розширення спектру (часова область). Цей метод розширює сигнал даних (повідомлення), множачи його на сигнал несучої та псевдовипадкову шумову послідовність, яка має широкий частотний спектр;

4) приховування даних з використанням ехо-сигналу. Дані вбудовуються в аудіосигнал-контейнер шляхом додавання до нього ехо-сигналу. Приховування досягається шляхом зміни трьох параметрів ехо-сигналу: початкової амплітуди, швидкості загасання та зсуву.

Методи приховування даних в тексті [6, 9]:

1) синтаксичні та семантичні методи. Синтаксичні методи включають зміни в пунктуації та модифікації структури й стилю тексту. Семантичні методи подібні до синтаксичних, але вони базуються на виборі двох синонімів, які відповідають значенням приховуваних бітів. Для їх застосування потрібна таблиця синонімів;

2) методи довільного інтервалу. Ці методи використовують вільний простір у тексті для приховування даних. Вони реалізуються трьома способами: зміною інтервалу між реченнями, зміною кількості пробілів в кінці рядків або зміною кількості пропусків між словами у вирівняному за шириною тексті. Деякі джерела відносять ці методи до лінгвістичної стеганографії.

Переваги цифрової стеганографії: простота в реалізації; висока стійкість до атак; візуальна невідмінність модифікованого повідомлення від

оригінального; доступність безкоштовного програмного забезпечення для реалізації методів.

1.1.3 Лінгвістична стеганографія

Напрям лінгвістичної стеганографії зосереджується на розробці та аналізі методів приховування конфіденційних даних у звичайних текстових повідомленнях. Цей процес базується на використанні специфічних мовних властивостей та лінгвістичних ресурсів. Класифікація лінгвістичних методів стеганографії (рис. 1.3) передбачає виділення двох головних категорій: умовного письма та семаграм [6].

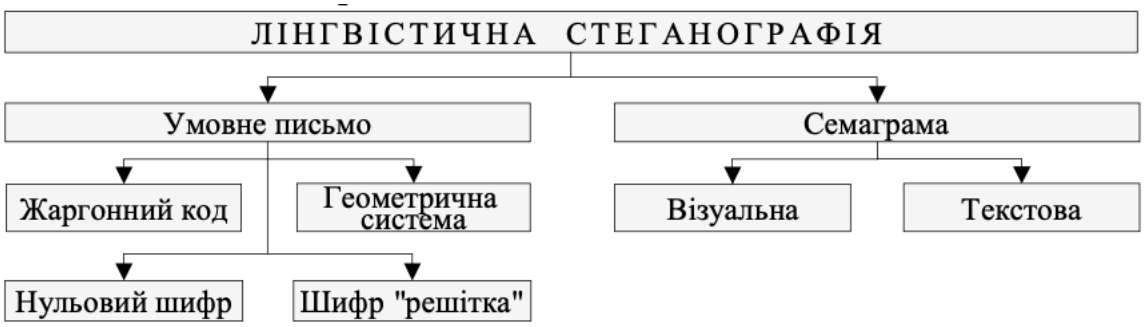

Рисунок 1.3 – Методи лінгвістичної стеганографії

Існують різні способи приховати інформацію, використовуючи мову та текст. Один з них – жаргонний код, де звичайні слова набувають нового, неочевидного значення. Текст при цьому виглядає цілком буденно, щоб не викликати підозр. Такий код може включати спеціальні символи (піктограми), незрозумілу термінологію або типові розмови, які для сторонніх залишаються загадкою, але для обізнаних осіб несуть прихований зміст [2].

Інший підхід – геометрична система. Тут важливе розташування слів на сторінці: їхнє розміщення в певних місцях або на перетині уявних геометричних фігур може вказувати на приховане повідомлення [2].

Нульовий шифр працює за чітко визначеними правилами, які заздалегідь узгоджуються. Наприклад, це може бути інструкція "читати кожне п'яте слово" або "звертати увагу на третю літеру кожного слова".

Шифр "решітка" використовує спеціальний шаблон. Слова, що потрапляють у прорізи цього шаблону, і складають секретне послання, яке ховається за основним текстом.

Окрему групу становлять семаграми. Це таємні повідомлення, де замість літер і цифр використовуються інші символи. Наприклад, послання може бути передане за допомогою крапок і тире, як у азбуці Морзе, оформлених у вигляді малюнка. Візуальні семаграми використовують звичайні, на перший погляд, предмети або дії для передачі інформації. Це може бути певний жест рукою, розташування предметів на столі, або навіть непомітні зміни у дизайні веб-сайту. Текстові семаграми приховують інформацію, змінюючи вигляд самого тексту: ледь помітні відмінності у розмірі чи типі шрифту, зайві пробіли, або витіюваті завитки в рукописному тексті [2].

Головна перевага цих методів полягає в можливості передавати досить об'ємні повідомлення. Однак, існують і суттєві недоліки. По-перше, існує ризик випадкового виявлення прихованого алгоритму, коли людина може помітити невідповідність або незвичність у модифікованому тексті порівняно з оригіналом. По-друге, процес створення такого прихованого повідомлення може бути досить складним і трудомістким.

1.1.4 Квантова стеганографія

Подібно до своїх класичних попередників, квантова стеганографія ставить за мету маскування самого факту передачі даних. Хоча ця галузь ще не досягла широкого застосування, існують дослідження [11], що пропонують архітектури систем штучного інтелекту, які експлуатують квантові феномени. Цей напрямок являє собою інтеграцію класичної та квантової інформатики, що базується на поєднанні принципів квантової механіки та класичної теорії інформації [10]. Класифікація методів квантової стеганографії представлена на рис. 1.4.

Рисунок 1.4 – Методи квантової стеганографії

Інша система кодує два класичних біти в один шуруподібний кубіт шляхом заміни кубіта із щільним кодуванням. Безпека цієї системи базується на тому, що квантовий шум не відрізняється від справжнього білого шуму з точки зору матриці щільності. У третій системі кубіт передається через класичний стеганографічний канал, використовуючи квантову телепортацію. Безпека цієї системи аналогічна безпеці класичної стеганографічної системи. Проте жоден із зазначених протоколів не вирішує завдання передачі непомітних повідомлень через відкритий класичний канал або загальний квантовий канал за умов збереження секретності [12].

Розглядаючи сильні і слабкі сторони квантової стеганографії, можна відзначити, що вона є значно більш захищеною порівняно з класичною, зокрема через те, що теоретично неможливо перехопити й розшифрувати конфіденційну інформацію, закодовану у квантові стани (теоретико-інформаційна стійкість).

1.2 Загальна модель стегосистеми

Суть стеганографії полягає в приховуванні інформації шляхом її інтеграції в інші, так звані, "контейнерні" дані (рис. 1.5). Ці контейнери можуть бути як порожніми (тобто не містити прихованих даних), так і заповненими (що містять секретне повідомлення, яке також називають "стего"). Важливо, щоб візуально або за іншими характеристиками порожній та заповнений контейнер були невідрізними.

Як контейнери можуть виступати різноманітні цифрові об'єкти: це можуть бути комп'ютерні файли, фотографії, аудіо- та відеозаписи. Для

приховування ж найчастіше використовують текстові повідомлення або прості чорно-білі зображення, наприклад, схеми чи креслення [5].

Для передачі таких замаскованих даних використовується "стеганоканал", а для самого процесу приховування – "стегоключ". Стегоключі бувають двох типів: секретні та відкриті.

Системи з секретним ключем передбачають використання одного спільного ключа, який має бути заздалегідь узгоджений між сторонами або переданий безпечним шляхом до початку обміну прихованими повідомленнями [5].

Системи з відкритим ключем використовують два різні ключі: один для вбудовування інформації, а інший – для її вилучення. Ці ключі взаємопов'язані таким чином, що знаючи один, неможливо отримати інший. Це дозволяє безпечно передавати один з ключів (відкритий) навіть через незахищені канали зв'язку, що робить такі системи ефективними навіть між сторонами, які не мають повної довіри одна до одної [5].

Вся сукупність елементів, що забезпечують процес стеганографії – від вибору контейнерів та повідомлень, використання ключів, до алгоритмів вбудовування та вилучення даних – формує так звану "стеганографічну систему".

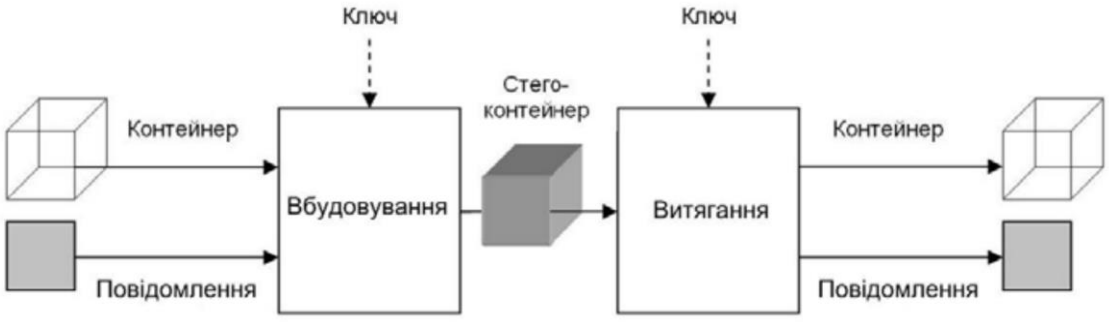

Рисунок 1.5 – Загальна модель стегосистеми

Порожній контейнер – це контейнер, який не містить прихованої інформації. Заповнений контейнер – це контейнер, в якому вже прихована інформація. Важливою умовою є те, що контейнер з вбудованими даними не повинен відрізнятися візуально від оригінального контейнера. Існують два основні типи контейнерів: варіаційний та стаціонарний [5].

Варіаційний контейнер характеризується тим, що його тип визначається динамічними потоками даних, наприклад, послідовністю зображень. У цьому випадку приховування критично важливої інформації відбувається в режимі потокової передачі. Важливо узгодити початок доданих даних із початком маркерів контейнерів і компонентами стиснення. Якщо в послідовності присутні біти синхронізаційних маркерів або заголовки пакетів, то прихована інформація може розміщуватися безпосередньо після них, хоча це належить до складних завдань [5].

Стаціонарний контейнер має заздалегідь відомі розміри та характеристики, що дозволяє здійснювати вкладення даних максимально ефективно. Контейнер може бути вибраним, випадковим або нав’язаним. Вибраний контейнер залежить від вбудованого повідомлення і, у найскладніших випадках, є його функцією.

Приховування переважно великого обсягу інформації висуває суворі вимоги до розміру контейнера, який повинен бути принаймні кілька разів більшим за вбудовані дані. Для підвищення якості процесу обробки спочатку проводять додаткові дії: криптографічне шифрування важливої інформації (наприклад, за допомогою блочних симетричних алгоритмів) і попередню обробку контейнера для зручнішого приховування даних [6].

Слід зауважити, що надійність системи напряму залежить від обсягу вбудованих даних: з ростом розміру прихованої інформації надійність знижується (див. рис. 1.6). Таким чином, у стеганографії існують обмеження на максимальний розмір даних, які можна вбудувати.

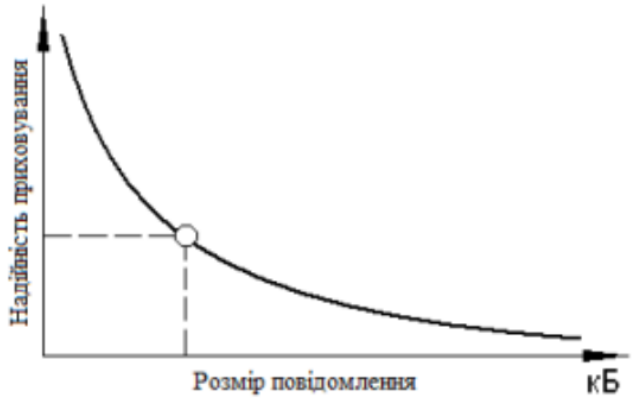

Рисунок 1.6 - Залежність надійності приховування даних від розміру повідомлення

При розробці системи приховування інформації важливо врахувати, що зловмисники можуть намагатися спотворити дані, які містять приховане повідомлення (контейнер). Під час передачі, наприклад, відео або зображень, ці контейнери можуть бути змінені: змінено їх розмір, перетворено на інший формат, або навіть оброблені алгоритмами, що призводять до втрати даних. Щоб приховане повідомлення залишалося неушкодженим, може знадобитися використання спеціальних кодів, які виправляють помилки (завадостійке кодування).

Для того, щоб приховане повідомлення було ще більш захищеним, перед його вбудовуванням часто застосовується попередня обробка за допомогою ключа. Сам процес додавання прихованих даних до контейнера здійснюється безпосередньо за допомогою стеганографічних методів. Алгоритм, який визначає, як саме інформація буде вбудовуватися та приховуватися, керується параметрами ключової послідовності. Саме ця послідовність є вирішальною для успішного приховування даних у контейнері. Ключова ідея полягає в тому, що зловмисник не знає цього ключа.

Існує два основних типи стеганосистем, які відрізняються за типом використовуваного ключа [5]:

- *системи з секретним ключем:* тут ключ відомий лише відправнику та отримувачу;

- *системи з відкритим ключем:* у таких системах використовується пара ключів – один для шифрування (відкритий), а інший для розшифрування (секретний).

Як секретний алгоритм може виступати генератор псевдовипадкової послідовності (ПСП) бітів. У цьому випадку заздалегідь визначаються ті частини контейнера, куди можна вбудовувати інформацію, мінімально впливаючи на якість зображення. Сам процес зміни цих частин контейнера відбувається згідно з обраним стеганографічним методом. Сукупність цих елементів контейнера, визначених ключем та з урахуванням вимог до збереження якості, формує так званий стеганографічний канал. Стеганографічний канал – це, по суті, шлях передачі контейнера, який вже містить приховане повідомлення [5].

У стеганодетекторі, з урахуванням формату даних контейнера, визначається наявність прихованої інформації, навіть якщо контейнер було

змінено. Такі зміни можуть виникати через помилки при передачі сигналу, обробку сигналу або навмисні атаки зловмисників.

Видобування інформації з контейнера зазвичай відбувається у два етапи. Перший етап – це виявлення стеганографічної послідовності, під час якого встановлюється факт присутності прихованих даних. Другий етап – безпосереднє вилучення цих прихованих даних із контейнера. Саме на основі цих двох етапів будується стеганографічна система [5].

В якості одного з детекторів може виступати система розпізнавання прихованого повідомлення, також у процесі може брати участь людина, яка пред’являє до системи передачі складні, важко формалізовані вимоги [4].

При розробці стеганографічної системи слід враховувати такі ключові аспекти:

- вимогу енергоефективності, тобто забезпечення балансу між алгоритмічною складністю та продуктивністю телекомунікацій;

- обмеження на обсяг прихованої інформації у контейнері з урахуванням необхідності передачі даних у режимі реального часу;

- вимогу збереження достовірності та авторства захищеної інформації, яка є важливою для конкретної галузі;

- дотримання принципу закону Кіргофа: алгоритм стеганографії відомий зловмисникові, але ключ залишається таємницею;

- у разі виявлення існування прихованого повідомлення зловмисником, це не має дозволяти йому розшифрувати дані, доки ключ є захищеним;

- необхідність брати до уваги технічні та алгоритмічні можливості потенційного зловмисника у сфері стеганоаналізу.

Найбільш поширеними та добре дослідженими методами цифрової стеганографії є вбудовування даних у зображення-контейнер (ЗК). Переваги такого підходу наглядна ілюструє рис. 1.7.

Застосування стеганографії у системах відеоконференцзв’язку також стає більш актуальним з розвитком технологій, що сприяє підвищенню якості і достовірності переданих даних у різних галузях провідних країн світу.

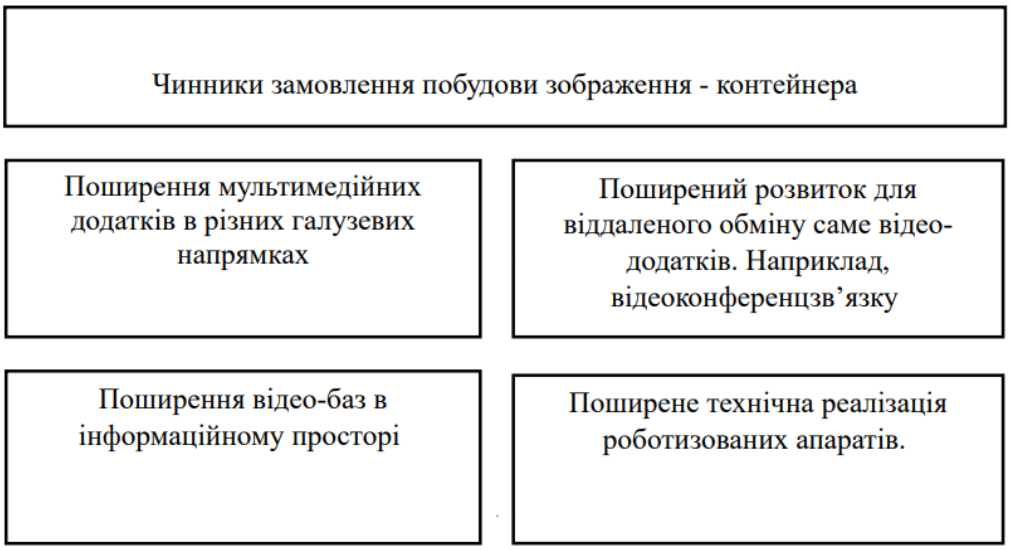

Рисунок 1.7 – Чинники переважного використання зображень для побудови прихованих контейнерів

Інформаційне поле відео отримало широке поширення. Завдяки розвитку інформаційних технологій у стратегічно важливих галузях зросла кількість відеоданих. Цей тип інформації широко застосовується для документування та передачі поточної ситуації. Коректне використання особливостей відеоданих дозволяє надійно приховувати значні обсяги інформації з високим рівнем достовірності [13].

Застосування в мультимедійних додатках також стало поширеним. У сучасних ключових сферах у світі використовують цифрові технології для об'єктивного контролю. За допомогою методів цифрової стеганографії (ЦС) можна передавати важливі відомості про порушників, приховуючи їх у звичайних даних задля забезпечення обмеженого доступу.

Використання на роботизованих пристроях передбачає їх застосування для контролю та спостереження. Методи ЦС забезпечують секретність передачі службових розпоряджень і підвищують надійність інформації.

В розділі обґрунтовано необхідність застосування методів цифрової стеганографії для приховання даних. Найперспективнішим напрямом розвитку цих методів є використання зображень як контейнерів інформації. Цей підхід є складовою загальної стратегії захисту та інформаційної безпеки. У певних випадках стеганографія виступає альтернативою криптографічним методам, тому важливо досліджувати сучасні методи стеганографії як ефективний інструмент захисту інформації.

2 АНАЛІЗ СУЧАСНИХ РІШЕНЬ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В МУЛЬТИМЕДІА

Сучасні методи комп'ютерної стеганографії розвиваються у двох ключових напрямках [6]:

1) використання специфічних особливостей комп'ютерних форматів даних: Ці методи експлуатують унікальні характеристики того, як комп'ютери зберігають інформацію у різних форматах. Наприклад, можна приховати дані у невикористаних частинах файлів, таких як вільний простір на дискових кластерах або порожні поля в розширеннях файлів. Однак, цей підхід має свої обмеження: прихованість інформації може бути не надто надійною, а обсяг даних, які можна таким чином сховати, є досить невеликим;

2) застосування цифрової обробки сигналів, що базується на надлишковості аудіо- та візуальної інформації: Цей напрямок використовує той факт, що цифрові зображення та звукові файли часто містять надлишкову інформацію. Це означає, що вони представлені у вигляді числових даних, які відображають інтенсивність світла (для зображень) або звукових коливань (для аудіо) в певні моменти часу. Надлишковість дозволяє вносити зміни, які залишаються непомітними для людського сприйняття.

Далі детальніше розглянемо методи комп'ютерної стеганографії, класифікуючи їх за типом носія (контейнера), в якому приховується інформація.

2.1 Методи приховування інформації в аудіо

LSB кодування: цей метод полягає у зміні останнього біта кожного байта аудіоданих, щоб непомітно вбудувати прихований текст. Однак, будь-які операції з аудіофайлом, такі як перекодування або стиснення, можуть призвести до втрати цієї прихованої інформації [14].

Паритетне кодування: цей підхід розбиває аудіосигнал на окремі частини і вставляє кожен біт секретного повідомлення в біт парності кожної частини. Він не потребує значних обчислювальних потужностей для реалізації. Проте, у великих аудіофайлах цей метод може збільшити їхній розмір [14].

Фазове кодування: цей метод використовує зміни у фазі аудіосигналу для приховування додаткової інформації. Ці зміни настільки незначні, що не впливають на сприйняття якості звуку людиною. Таким чином, додаткове повідомлення вбудовується у вихідний сигнал, залишаючись непоміченим [14].

Розподіл спектра: прихована інформація передається шляхом розподілу її по широкому діапазону частот аудіофайлу. Це робить інформацію менш помітною, але може обмежити загальний обсяг даних, які можна приховати. Цей метод використовує спеціальний код, який не взаємодіє з основним аудіосигналом [14].

Приховування відлуння: цей метод полягає у додаванні до оригінального аудіосигналу ледь помітного відлуння, в яке вбудовується прихована інформація. Це відлуння майже не відчувається на слух. Однак, якщо аудіофайл буде змінено, це відлуння може бути спотворене або повністю втрачене [14].

2.2 Методи приховування даних у відео

Метод вбудовування на рівні коефіцієнтів. Приховане повідомлення інтегрується шляхом модифікації коефіцієнтів, отриманих після дискретно-косинусного перетворення (ДКП) зображення. Цей підхід забезпечує стійкість прихованої інформації до таких впливів, як фільтрація, додавання випадкового шуму та дискретизація. Виявлення прихованого повідомлення можливе за допомогою статистичних методів, які шукають відхилення або зміни в закономірностях розподілу коефіцієнтів ДКП [15].

Метод вбудовування інформації на рівні бітової площини Цей метод полягає у втручанні в окремі біти або групи бітів (бітові площини) відеосигналу для приховування інформації. Однак, багаторазове застосування цього методу призводить до помітного погіршення якості відео та знищення прихованих даних [15].

Метод вбудовування інформації за рахунок енергетичної різниці між коефіцієнтами. Прихована інформація вбудовується шляхом вибіркового видалення деяких коефіцієнтів, отриманих після дискретно-косинусного перетворення. Цей метод може забезпечити високий рівень захисту від поширених зовнішніх впливів, таких як додавання шуму або стиснення даних [15].

2.3 Методи приховування даних в зображеннях

2.3.1 Дослідження базових методів стеганографії для приховування інформації у просторовій області зображення

Приховування даних у просторовій області може здійснюватися різними способами, такими як заміна найменш значущого біта (НЗБ), використання псевдовипадкових інтервалів, псевдовипадкових перестановок, блокових методів приховування, заміна палітри, квантування зображення, а також методи Куттера-Джордана-Боссена та Дармстедтера-Делейгла-Квісквотера-Макка. Всі ці підходи базуються на ідеї заміни надлишкових або неістотних частин зображення бітами прихованого повідомлення. Для відновлення зашифрованої інформації необхідно знати точний алгоритм, за допомогою якого дані були сховані в контейнері. Головним недоліком цих методів є їх чутливість до різного виду спотворень [16].

Одними з найпоширеніших і найбільш перевірених способів стеганографії є методи приховування інформації у часовій області зображення. Їх суть полягає у вбудовуванні секретних даних безпосередньо в початкову структуру формату зображення. Оскільки кольорове зображення складається з трьох компонент – R, G та B, маємо три окремі яскравісні простори. Такий підхід дозволяє уникнути додаткових етапів трансформації кольорових компонент, що значно скорочує час обробки зображень і приховування інформації.

Кольорове зображення CL можемо розглянути як дискретну функцію, що задає кольоровий вектор clr(x, y) для кожного пікселя (x, y), де значення вектора представляє точки у трикомпонентному колірному просторі. Найпоширенішою моделлю передачі кольору є RGB, в якій базовими квітами є червоний, зелений і синій, а будь-який інший колір формується як комбінація цих трьох основних.

Вектор clr(x, y) в RGB-моделі відображає інтенсивність кожного базового кольору. Вбудовування повідомлень відбувається шляхом зміни кольорових каналів або напряму яскравості пікселів. В цілому такі методи полягають у заміщенні малозначущих, надлишкових елементів зображення бітами секретних даних. Для того, щоб правильно вилучити приховану інформацію,

потрібно мати знання про алгоритм, який було застосовано для її інтеграції в контейнер.

Метод заміщення найменш значущого біта (НЗБ) є найпопулярнішим із методів, що працюють у просторовій області. Наймолодший біт пікселя зображення не несе значної інформації і зазвичай зміни в ньому непомітні для людського ока. Таким чином, можна розглядати цей біт як шум, який використовується для варіацій з метою приховання даних — замість LSB пікселів записуються біти секретного повідомлення. При цьому в зображеннях у відтінках сірого (кожен піксель кодується одним байтом) максимальний об’єм може складати 1/8 від загального об’єму контейнера [16].

Збільшення кількості прихованих бітів на одиницю призводить до подвоєння обсягу даних, які можна приховати. Цей підхід набув широкого поширення завдяки своїй доступності та ефективності у приховуванні значних обсягів інформації навіть у невеликих файлах.

Найчастіше цей метод застосовується до растрових зображень, які не стискаються (наприклад, у форматах GIF та BMP). Такий вибір виключає необхідність складних попередніх обробок зображень і відповідає вимогам стеганографії для бездротових мереж. На рис. 2.1 показано процес приховування даних у зображенні.

Головним обмеженням методу НЗБ є його низька стійкість до спроб виявлення та модифікації з боку як пасивних, так і активних зловмисників. Це пов'язано з його високою чутливістю до будь-яких змін у файлі-контейнері. Для підвищення стійкості часто використовують додаткове завадостійке кодування, яке дозволяє виявляти та виправляти помилки в даних.

Рисунок 2.1 – Схема стеганографічного методу шляхом додавання біту важливої інформації в найменш значущий біт контейнеру

2.3.2 Дослідження базових методів стеганографії для приховування інформації у частотній області зображення

Серед методів стеганографії в частотній області виділяються: підхід на основі відносної заміни значень коефіцієнтів дискретного косинусного перетворення (ДКП); метод Бенгама-Мемона-Ео-Юнга; алгоритм Хсу і Ву; техніка Фрідріха. Процес виділення зон для конфіденційних даних виконується після декомпозиції оригінального сигналу на базові елементи. Вибір конкретного виду трансформації залежить від необхідного ступеня стійкості для секретного повідомлення, хоча це може обмежувати обсяг даних, що вбудовуються [17].

Існує кілька підходів до представлення зображень у частотній області. Найпоширенішими є трансформації двох категорій. Перша група — ортогональні перетворення, де ключовими є дискретне косинусне перетворення (ДКП), перетворення Хаара та дискретне перетворення Уолша-Хадамара. Друга група — хвильові перетворення, які, на відміну від ортогональних, застосовуються не лише до локальних фрагментів зображення, але й до повного кадру одразу [17].

У стеганографії найбільше застосування знайшли вейвлет-перетворення та ДКП, що пояснюється їх широким використанням у компресії зображень.

Метод відносної заміни коефіцієнтів ДКП (Коха-Жао) є одним із найпопулярніших на сьогодні. Алгоритм передбачає поділ зображення на блоки розміром 8×8 пікселів, до кожного з яких застосовується дискретне косинусне перетворення, що дає формування матриці компонентів ДКП аналогічного розміру [19].

Для кодування одного біта інформації використовується один блок. В межах блоку вибираються дві фіксовані компоненти ДКП за певними координатами, які стають основою для вбудовування. Залежно від значення вбудованого біта модифікується різниця між цими двома коефіцієнтами: для біта "0" вона повинна бути більшою за позитивний поріг, а для біта "1" — меншою за деяку від’ємну величину. Таке порогове управління дозволяє реалізувати стійке приховування, що зберігає питання видимих змін у контейнері після зворотного перетворення.

Метод Бенгама-Мемона-Ео-Юнга (БМЕЮ) вдосконалює згаданий алгоритм шляхом відбору найбільш придатних для вбудовування блоків на основі певних критеріїв (наприклад, енергетичної концентрації або текстурності регіону). Це сприяє як покращенню якості зображення після вбудовування, так і підвищенню надійності захованої інформації. Крім того, замість двох коефіцієнтів тут використовуються три, що дозволяє більш гнучко коригувати характеристики блоку за рахунок додаткового ступеня свободи, зменшуючи загальні візуальні спотворення та підвищуючи захищеність [19].

Метод Хсу і Ву базується на аналізі статистичних властивостей коефіцієнтів ДКП, особливо їх розподілу у середньочастотних зонах. Він використовує специфічні правила компресії та модифікації пар коефіцієнтів для вбудовування інформації, забезпечуючи баланс між стійкістю до шумів і малопомітністю.

Метод Фрідріха відрізняється застосуванням кількісних критеріїв добору областей для вбудовування, враховуючи локальні характеристики текстури та структури зображення. У процесі він керує зміною коефіцієнтів ДКП так, щоб уникнути значних спотворень видимих ділянок і одночасно забезпечити відновлення закодованої інформації.

В усіх цих методах суттєвим є вибір зони приховування: низькочастотні коефіцієнти часто не змінюються через вплив на якість зображення, а високочастотні - через схильність до компресії та шумів. Найбільш оптимальними зазвичай виступають середньочастотні компоненти, де можна досягти компромісу між стійкістю і втратами якості.

Варто також зазначити, що прийоми в частотній області здебільшого інтегруються з алгоритмами стиснення (наприклад, JPEG), що додає додаткові вимоги і обмеження до схеми вбудовування, регулюючи ємність та стійкість методу.

Усе це створює основу для розробки ефективних стеганографічних алгоритмів, які враховують як характеристики сигналу, так і потреби та умови захисту інформації в практичних системах.

2.4 Оцінка якості методів цифрової стеганографії

Для того, щоб зрозуміти, наскільки добре працюють різні методи приховування інформації (стеганографії), застосовуються вже розроблені

числові методики. Ці методики зазвичай аналізують зображення, розглядаючи кожен окремий піксель. Однак, після невеликих змін, ці ж методики можна використовувати для аналізу зображень, описаних іншими способами, а також для роботи з аудіофайлами.

Одним з ключових показників ефективності стеганографічної системи є її відносна стеганографічна ємність $\omega_{\text{відн}}$. Цей показник демонструє, яку частку (у відсотках) від загального обсягу вихідного носія $\omega_{\text{поч}}$ (контейнера) займає прихована інформація $\omega_{\text{вбуд}}$ [18].

Таким чином, ми можемо оцінити, наскільки ефективно стеганографічний метод використовує простір контейнера для приховування даних. Чим вище значення відносної стеганографічної ємності, тим більше корисної інформації можна приховати, не надто впливаючи на сам контейнер. Розрахунок цього показника здійснюється за такою формулою [18]:

$$\omega_{\text{відн}} = \frac{\omega_{\text{вбуд}}}{\omega_{\text{поч}}}, \tag{2.6}$$

$$\omega_{\text{вбуд}} = \frac{3 \cdot z_{\text{ряд}} \cdot z_{\text{стовп}}}{\omega}, \tag{2.7}$$

де $z_{\text{ряд}}$ – розмір зображення оригіналу по рядках;

$z_{\text{стовп}}$ – розмір зображення оригіналу по стовпцях;

ω - розмір області контейнеру, яка використовується для приховування одного біту інформації.

Коефіцієнт успішного вилучення даних авторизованим користувачем $P_{\text{вил}}$. Цей показник слугує для кількісної оцінки коректності вилученої інформації в умовах авторизованого доступу. Розрахунок даного коефіцієнта здійснюється за такою формулою [18]:

$$P_{\text{вил}} = \frac{\omega_{\text{вил}}}{\omega_{\text{вбуд}}}, \tag{2.8}$$

де $\omega_{\text{вил}}$ - об’єм безпомилково вилучених даних, біт;

$\omega_{\text{вбуд}}$ – об’єм вбудовуваної інформації, біт.

Пікове відношення сигнал-шум (ПВСШ), що позначається як h і вимірюється в децибелах (дБ), є показником якості зображення з вбудованими даними при несанкціонованому доступі. Ця величина кількісно визначає візуальні спотворення, які виникають у закодованому зображенні (ЗК) під час процесу вбудовування, і розраховується за наведеною нижче формулою [18]:

$$h = 20\lg\left(\frac{255}{СКВ}\right), \tag{2.9}$$

де СКВ – середньоквадратичне відхилення зображення з вбудованими даними відносно ЗК, розраховується за формулою:

$$СКВ = \sqrt{\frac{\sum_{i=1}^{z_{ряд}}\sum_{j=1}^{z_{стовп}}(a_{ij} - a'_{ij})}{z_{ряд}\cdot z_{стовп}}}, \tag{2.10}$$

де a_{ij} – елементи початкового зображення;

a'_{ij} – елементи стеганографічно перетвореного зображення;

$z_{ряд}$ – розмір зображення оригіналу по рядку;

$z_{стовп}$ – розмір зображення оригіналу по стовпцю.

До головних якісних параметрів стеганографічних систем, створених із застосуванням різноманітних методик, належать [21]:

- пропускна здатність;
- стійкість. Це здатність витягувати заховану інформацію після здійснення типових обробних операцій із зображеннями, таких як лінійне і нелінійне фільтрування (розмиття, підвищення різкості, медіанна фільтрація), стиснення із втратою якості, регулювання контрастності, змінювання кольору, масштабування, обертання, додавання шуму, обрізання, друкування, копіювання, сканування, а також перестановка пікселів;
- невидимість. Цей параметр базується безпосередньо на особливостях людської візуальної системи. Поширена методика оцінки — так званий сліпий тест, що часто застосовується у психовізуальних дослідженнях, де учасникам у довільному порядку демонструють велику кількість носіїв із

прихованою інформацією та без неї, і їх просять визначити, які з них містять приховані дані;

- захищеність. Цей параметр включає стійкість до різних процедурних атак, зокрема атак IBM або атак, що базуються на знанні про часткові зміни носія, спричинені вбудованими даними;
- складність вбудовування й вилучення. Мається на увазі кількість стандартних операцій, які потрібно виконати для вбудовування і подальшого виявлення захованого повідомлення.

Варто зазначити, що ці характеристики мають зворотну залежність між собою: покращення одного показника, як правило, супроводжується погіршенням іншого. Наприклад, якщо необхідно заховати великий обсяг інформації у зображенні, не можна одночасно очікувати абсолютної невидимості та високої стійкості. Завжди потрібен оптимальний баланс між параметрами. З іншого боку, якщо система повинна бути дуже стійкою до значних спотворень, то приховане повідомлення не може бути надто об’ємним [21].

На рисунку 2.2 наведено характеристики методів цифрової стеганографії.

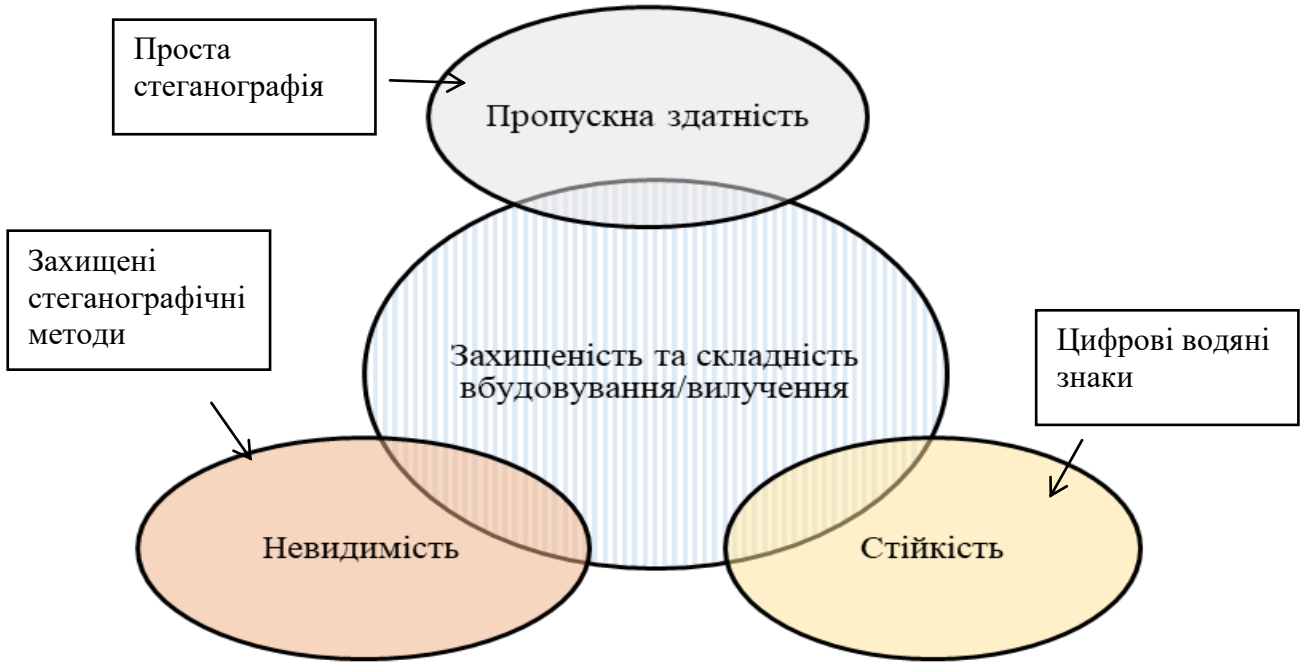

Рисунок 2.2 – Основні характеристики методів цифрової стеганографії

За формулами кількісних показників проведемо розрахунки для найбільш популярних методів:

- найменш значущого біта;
- методу БМЕЮ;
- методу Коха-Жао.

Аналіз таблиці 2.1 свідчить про те, що сучасні стеганографічні методи характеризуються низькою стійкістю до вилучення інформації та невисоким співвідношенням сигнал/шум (ПВСШ). Така вразливість робить створені стеганограми схильними до різноманітних видів атак.

Таблиця 2.1 – Значення кількісних показників методів стеганографії

Показник якості	Методи стеганографії		
	НЗБ	БМЕЮ	Коха-Жао
Відносна ємність, %	6,25	12,5	3,1
Ймовірність вилучення даних	0,5	0,75	0,7
Пікове відношення сигнал шум, дБ	55,67	45,87	51,01

Порівняльний аналіз кількісних показників для обраних методів представлено в табл. 2.2:

- А1 (метод найменш значущого біта);
- А2 (метод Бенгама-Мемона-Ео-Юнга);
- А3 (метод Коха-Жао).

Таблиця 2.2 – Аналіз якісних показників методів стеганографії

	Пропускна спроможність	Складність виявлення	Невидимість	Захищеність	Складність вбудовування
А1	0,058	0,453	0,147	0,018	0,453
А2	0,023	0,072	0,076	0,216	0,072
А3	0,038	0,120	0,044	0,216	0,120

Пропускна спроможність для методу найменш значущого біта залежить від розмірів зображення (h – висота, ω – ширина):

$$C = h \cdot \omega \cdot 3. \qquad (2.11)$$

Метод Коха-Жао та БМЕЮ використовують блоки розміром 8x8. Відповідно пропускна спроможність розраховуватиметься як:

$$C = \frac{h \cdot \omega}{8 \cdot 8}. \quad (2.12)$$

Для оцінки ефективності методів приховування інформації в зображеннях були використані такі показники: якість візуального сприйняття (IF), стійкість до спроб виявлення та складність реалізації процесів вбудовування та вилучення даних. Ці операції розраховувалися на основі кількості стандартних дій, а заповнення стеганографічного контейнера обмежувалося 10% його максимальної місткості. Результати аналізу існуючих методів стеганографії в ЗК, що виявили їхні ключові слабкі сторони, наведені на рис. 2.3.

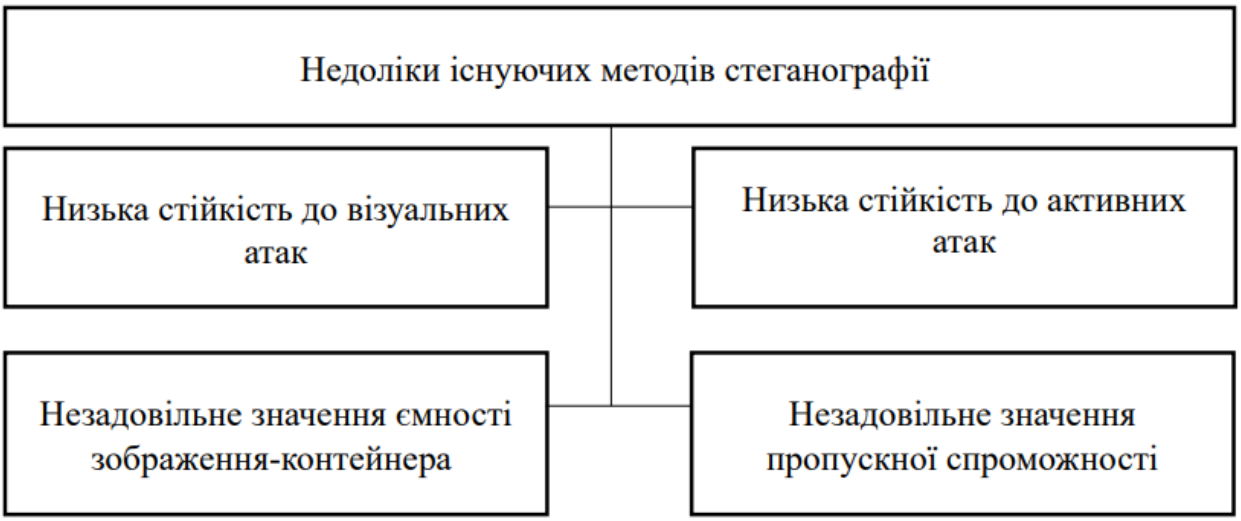

Рисунок 2.3 – Недоліки існуючих методів стеганографії

Низьке значення стійкості стеганограми до візуальних атак зловмисника – якщо стеганографічний метод погано протистоїть візуальним атакам, це означає, що при спробі виявити приховане повідомлення зображення стає помітно спотвореним, його якість погіршується. Якщо зловмисник має оригінал зображення, він може легко помітити, що в ньому щось приховано.

Низька стійкість до активних дій зловмисника, зокрема до компресійних атак, є проблемою. Ці атаки намагаються усунути надлишкову інформацію в зображенні, яка, як виявилося, також використовується для приховування даних.

Недостатня ємність означає, що неможливо приховати багато інформації. Чим більше даних ви намагаєтеся вбудувати, тим більше елементів зображення доводиться змінювати, що призводить до сильніших спотворень.

Незадовільне значення пропускної спроможності – важливо, щоб прихована інформація доходила до отримувача без помилок і була захищена від дій зловмисника. Це включає захист від виявлення самого факту прихованого зв'язку, перехоплення змісту повідомлень, підміни даних або пошкодження прихованої інформації.

Після аналізу існуючих методів приховування інформації в цифрових зображеннях було виявлено, що вони мають суттєві недоліки. Ці методи часто вразливі до атак, мають обмежену здатність приховувати великі обсяги даних і погано справляються з передачею зображень, коли зловмисник активно намагається втрутитися. Збільшення обсягу приховуваної інформації призводить до помітних спотворень зображення, що, в свою чергу, знижує ефективність захисту від візуального аналізу. Були розглянуті як якісні, так і кількісні показники методів стеганографії та їхній вплив на вихідне зображення.

3 АНАЛІЗ ТА РОЗРОБКА МОДЕЛІ СТЕГАНОГРАФІЧНИХ ПЕРЕТВОРЕНЬ МЕДІАДАНИХ З МЕТОЮ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРИХОВУВАННЯ ІНФОРМАЦІЇ

3.1 Стеганографічний метод на базі дискретного вейвлет-перетворення

Методи, які використовують частотну область для приховання даних замість просторової області контейнера, є більш стійкими до різних видів спотворень, зокрема компресії. Існує декілька підходів для перетворення зображення у частотне подання. В основному, їх можна поділити на два типи. Перший полягає в переході зображення у спектральний простір за допомогою ортогональних перетворень. До найпопулярніших серед них відносять дискретне косинусне перетворення (ДКП), перетворення Хаара та дискретне перетворення Уолша-Адамара. Другий підхід передбачає переведення зображення у спектрально-часовий простір, що реалізується за допомогою хвильових (вовнових) перетворень. Базисом для таких перетворень зазвичай слугують початкові компоненти базису Хаара, але можуть застосовуватись також більш складні алгоритмічні базиси, наприклад, базис Добеші. З усіх ортогональних перетворень найбільше розповсюдження у стеганографії здобули хвильові перетворення та ДКП, що пов’язано з їх широким використанням під час компресії зображень [20].

Хвильові перетворення являють собою локалізований інтегральний метод із застосуванням фіксованого розміру вікна і змінної форми аналізуючої функції, що дозволяє якісно визначати низькочастотні складові сигналу у частотній області (основні гармоніки), а високочастотні деталі — у часовій області.

Суть дискретного хвильового перетворення (ДХП) при обробці зображень полягає в його розкладанні на складові, що відповідають різним просторовим та частотним ділянкам**.** Після застосування ДХП, інформація зображення аналізується в чотирьох частотних областях: одна низькочастотна (LL), одна високочастотна (HH) та дві середньочастотні (LH, HL) [22].

Зазвичай для приховування інформації використовують середньочастотні складові, оскільки людське око менш чутливе до змін саме в цих ділянках. Це

пояснюється такими факторами. По-перше, високочастотні компоненти (смуги) застосовуються під час стиснення зображень, і цей процес супроводжується викривленнями їх значень. Внаслідок цього важлива інформація, додана стеганографічним методом, може бути втрачена. По-друге, високочастотні складові відіграють ключову роль у якості відновлених зображень, і додавання сюди стеганографічних даних може викликати помітні візуальні спотворення. Такі дефекти будуть добре помітні й порушуватимуть вимоги до непомітності прихованої інформації [24].

Отже, існує два можливі підходи. Перший — вміщувати важливі дані у високочастотні компоненти, але лише у обмеженій кількості, або ж використовувати середньо-інформативні області зображення. Другий варіант — обмежуватись середньочастотними смугами, де рівень шуму приблизно дорівнює шуму обробки, наприклад, у середніх частотах спектрального простору ДКП або у спектрально-часових областях LH та HL. Ці ділянки є більш стійкими, адже вони представляють собою компроміс між низькочастотними та високочастотними областями спектру чи спектрально-часового простору.

Щоб забезпечити вищу стійкість, дані впроваджують саме в частково перетворене зображення. На рис. 3.1 показано приклади переходу окремих фрагментів зображення у спектральний та спектрально-часовий простір за допомогою ДКП (рис. 3.1а) та вейвлет-перетворення (рис. 3.1б).

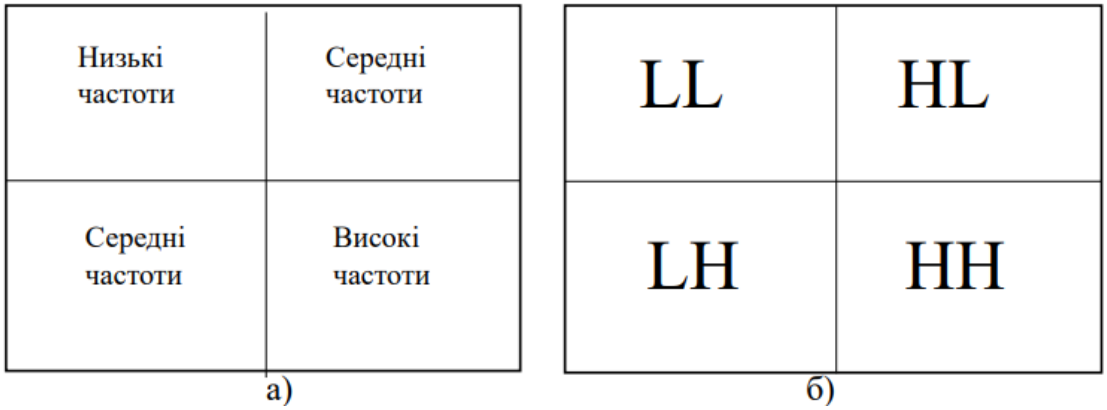

Рисунок 3.1 – Приклади формування простру з областями різних частот спектру

У разі виконання перетворення зображень за допомогою вейвлет-перетворення можливе застосування двох або трьох каскадів вейвлет-перетворень до поточної області низьких частот LL. Це дозволяє зменшити

масштаб цих ділянок та створити умови для подальшого збільшення рівня деталізації. При двоетапному розкладанні спочатку проводиться дискретне вейвлет-перетворення (ДВП) у вертикальному напрямку, а потім – у горизонтальному, для кожного з рівнів. Після першого рівня розкладання виділяються чотири піддіапазони: LL1, LH1, HL1 та HH1. Для наступних рівнів розкладання як вихідне зображення береться піддіапазон LL. На рис. 3.2 наведено приклад двоетапного дискретного вейвлет-розкладання [22].

Таким чином, для другого рівня розкладання ДВП застосовується до LL піддіапазону, в результаті чого він також розбивається на чотири піддіапазони: LL2, LH2, HL2 та HH2 [22].

Якщо ж виконується трирівневе розкладання, то ДВП застосовується до піддіапазону LL2, що дозволяє розбити його на ще чотири піддіапазони (LL3, LH3, HL3, HH3). Загалом, це призводить до утворення десяти піддіапазонів для одного компонента. Піддіапазони LH1, HL1 та HH1 містять найбільш високочастотні компоненти зображення, тоді як LL3 утворює найнижчі частоти. Приклад трирівневого ДХП-розкладання представлений на рис. 3.3 [22].

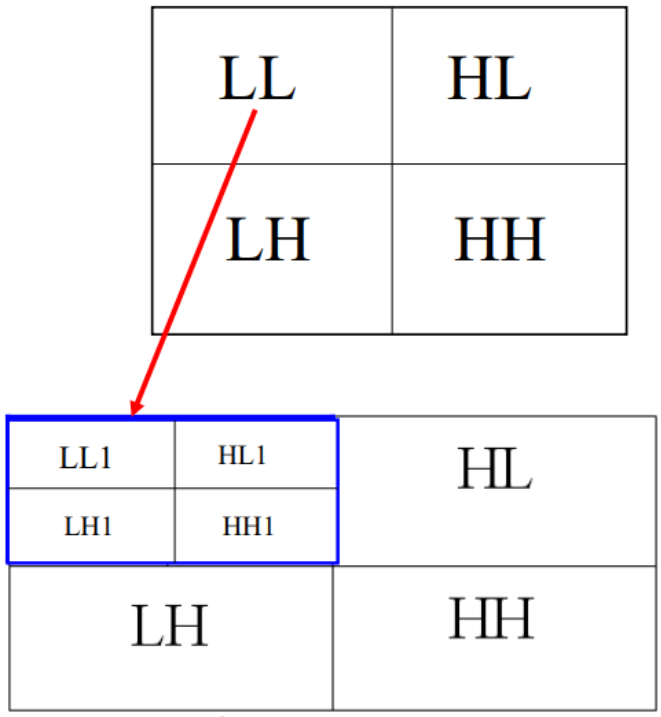

Рисунок 3.2 – Варіант другого рівня масштабування області LL хвилевим-перетворенням

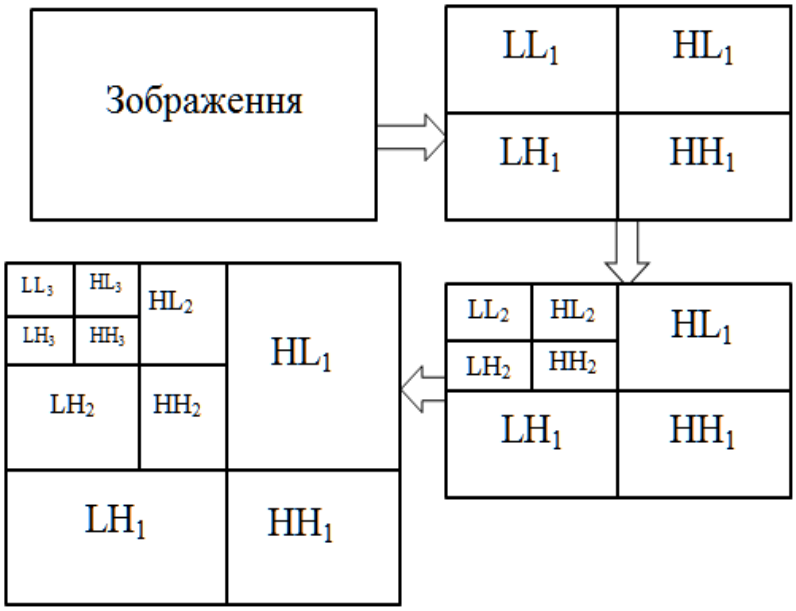

Рисунок 3.3 – Варіант хвилевого-перетворення за третім каскадом

3.2 Рекомендації щодо підвищення ефективності формування прихованого каналу

Для підвищення завадостійкості необхідно збільшити пропускну здатність, оскільки застосування методів завадостійкого кодування або дублювання даних вимагає передачі додаткових бітів. У процесі досліджень було визначено два способи підвищення пропускної здатності при використанні методів вбудовування у область перетворення. Перший спосіб ґрунтується на припущенні, що вбудовування інформації у середньочастотні коефіцієнти ДКП забезпечує достатню стійкість зображення, оскільки ці коефіцієнти зазвичай не піддаються суттєвим змінам або втратам у процесі стиснення. Водночас людське око не настільки чутливе, щоб помітити зміни у цих коефіцієнтах. Відповідно, запропоновано метод, який максимально використовує середньочастотні компоненти зображення. Приклад блоку коефіцієнтів ДКП яскравісної складової наведений на рис. 3.4.

Другий підхід до підвищення стійкості зображення передбачає вбудовування інформації не лише у синю складову кольорового формату, як прийнято в більшості відомих методів, а й у зелену та червону компоненти. Для успішного застосування цього методу рекомендується використовувати зображення, в яких переважають зелені або червоні тони, а також відсутні великі однотонні ділянки.

	1	2	3	4	5	6	7	8
1	1420	220	11	37	-28	-12	-12	-7
2	108	-89	10	43	25	6	8	2
3	-47	-20	-6	16	17	9	3	2
4	54	72	7	-22	-10	-5	-2	-2
5	-29	-19	15	8	3	-4	-5	-3
6	-16	-14	8	2	-4	-2	1	1
7	0	-5	-6	-1	2	3	0	1
8	9	5	-6	-9	0	3	3	1

Рисунок 3.4 – Приклад блоку коефіцієнтів ДКП складової яскравості

Було сформульовано рекомендації щодо підвищення пропускної здатності при застосуванні методів вбудовування інформації у частотну область зображення. Розроблено метод стеганографічного приховування даних, що базується на виборі блоків, які є стійкими до компресійних атак і вносять мінімальні спотворення в зображення, що дає змогу ефективно їх використовувати для приховування інформації.

4 ОЦІНКА ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО СТЕГАНОГРАФІЧНОГО МЕТОДУ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В МЕДІАТРАФІКУ

4.1 Алгоритм методу підвищення ефективності прихованого каналу при передачі медіатрафіку

Моніторинг, безперервне спостереження та своєчасне передавання даних про стан підсистем ключових галузей стали основою успішного розвитку держави. Сучасні телекомунікаційні технології значно сприяють виконанню цих завдань. Спираючись на аналіз переваг та недоліків існуючих методів вбудовування інформації, було створено метод стеганографічного приховування даних. В основі вдосконаленого стеганографічного методу лежать алгоритмічні принципи, які полягають у наступному:

- зображення, обране як контейнер, проходить попередню обробку — перетворення у спектральний або спектрально-часовий простір за допомогою дискретного косинусного перетворення (ДКП) або вейвлет-перетворення;
- важлива галузева інформація також піддається попередній обробці — стисненню для зменшення обсягу бітів та застосуванню завадостійкого кодування; за потреби, після стиснення, інформацію можна зашифрувати криптографічними методами;
- вбудовування інформації здійснюється у двох режимах для одного типу зображень, розміщуючись у компонентах середньочастотних ділянок. Такий підхід використовується для зображень із достатнім рівнем статистичної залежності, тоді як для зображень із середнім рівнем інформативності додаткові дані вставляють у високочастотні компоненти.

Основною вимогою методу є збільшення кількості інформації, що може бути стеганографічно вкладена у вибрані частини зображення. Перед вбудовуванням зображення поділяється на сегменти, розміри яких залежать від типу перетворення в спектральний або спектрально-часовий простір.

Основні етапи удосконаленого методу, запропонованого в роботі, можна описати у п’ять етапів.

Перший етап. Спочатку визначається ступінь статистичної залежності зображення. Якщо цей рівень високий, тоді зображення розбивають на невелику кількість частин із більшими розмірами. До кожної такої частини застосовується вейвлетне перетворення, внаслідок якого виділяються області за типом частотних характеристик: низькочастотна (LL), високочастотна (HH) та дві середньочастотні (LH, HL). Якщо ж області великого розміру характеризуються середнім рівнем ентропії, їх безпосередньо розподіляють на меншого розміру фрагменти, наприклад, 8×8 або 16×16 пікселів. Потім для таких частин здійснюється перехід у частотну область за допомогою дискретного косинусного перетворення (формула (2.2)).

Другий етап. Залежно від параметрів ключової послідовності можливі два варіанти реалізації першого типу перетворень. Варіант 1 передбачає стеганографічне впровадження інформації у елементи високочастотних областей. Варіант 2 передбачає додаткове застосування двовимірного дискретного косинусного перетворення до середньочастотних областей LH, HL. У цьому випадку також використовується алгоритм за формулою (2.2). Ці варіанти можуть застосовуватися окремо або у комбінованому режимі.

Третій етап. На цьому етапі здійснюється вибір певних частин зображення, до яких буде впроваджуватися важлива стеганографічна інформація. Вибір базується на параметрах ключа, що визначають порядок вибору фрагментів, а також на ентропійних характеристиках частин із урахуванням їх статистичного аналізу. Аналіз статистичних залежностей допомагає встановити рівень ентропії, виявити контрастні області (за гістограмою розподілу) та визначити значення емпіричного коефіцієнта кореляції. Для відбору фрагментів зображення за обраними критеріями використовують множини зонально-порогових меж, як нижніх, так і верхніх. Залежно від належності кожного параметра до певної зонально-порогової межі обирається відповідний напрямок та спосіб попередньої обробки частин зображення. Теоретично можливо впроваджувати важливу інформацію у всі обрані частини зображення.

Четвертий етап полягає у виборі алгоритму модифікації, що реалізує стеганографічну передачу важливої інформації, виходячи з принципу чотирьох складових. Наприклад, загалом такими складовими можуть виступати $g(\xi;\gamma)$, $g(\lambda;\psi)$ та $g(u;v)$, $g(\tau;\upsilon)$ з алгоритмічно обраними координатами.

Компоненти можуть бути віднесені до високочастотної або середньочастотної частини спектрального або спектрально-часового аналізу. Класифікація відбувається на основі статистичних показників та їх співвідношення до встановлених зон та порогів. Таким чином, компоненти розділяються на дві категорії. Перша категорія включає компоненти $g(\xi;\gamma)$, $g(\lambda;\psi)$. Друга група $g(u;v)$, $g(\tau;\upsilon)$.

На п'ятому етапі відбувається приховане вбудовування ключового фрагмента даних. Цей процес здійснюється за допомогою наступного алгоритму:

у разі додавання біту «0» сума $S_1 = g(\xi;\gamma)+g(\lambda;\psi)$ значень компонент першої групи повинна бути меншою ніж сума $S_2 = g(u;v)+g(\tau;\upsilon)$ значень компонент другої групи:

$$S_1 < S_2. \tag{4.1}$$

Якщо додається біт "1", то має бути дотримано зворотну залежність: сума компонент першої групи повинна перевищувати суму компонент другої групи:

$$S_1 > S_2.$$

Узагальнено можна подати це у вигляді такого виразу:

$$r_i = \begin{cases} 0 \rightarrow S_1 = g(\xi;\gamma)+g(\lambda;\psi) < S_2 = g(u;v)+g(\tau;\upsilon); \\ 1 \rightarrow S_1 = g(\xi;\gamma)+g(\lambda;\psi) > S_2 = g(u;v)+g(\tau;\upsilon). \end{cases} \tag{4.2}$$

Де r_i - поточний елемент важливої інформації, яку потрібно додати до контейнеру стеганографічним чином.

Вважається, що застосування чотирьох компонентів дозволяє мінімізувати спотворення, які виникають при внесенні даних у спектральний або спектрально-частотний простір. Це забезпечує невидимість доданої інформації для зображення. Крім того, використання чотирьох значень допомагає контролювати складність алгоритму.

Розроблений метод поєднує в собі запропоновані підходи для покращення стійкості, безпеки та пропускної здатності стеганографічних систем. У певних ситуаціях, для зменшення спотворень та спрощення процесу прихованого додавання інформації, можна обмежитися використанням трьох компонентів.

4.2 Оцінка ефективності розробленого методу

За формулами з другого розділу 2.6 – 2.11 проведемо аналіз показників розробленого методу. Результати зведено в табл. 4.1.

Таблиця 4.1 – Оцінка якісних характеристик розробленого методу

	Відносна ємність $w_{відн}$, %	Ймовірність вилучення даних $P_{вил}$	Пікове відношення сигнал шум h, дБ
Розроблений метод	4,6	1	83,56

Для об'єктивного порівняння ефективності стеганографічних методів застосовуються стандартні метрики, які дозволяють отримати числові результати. Ці метрики аналізують зображення на рівні окремих пікселів. Тут $C_{x,y}$ $C_{x,y}$, $S_{x,y}$ $S_{x,y}$ – відповідно компоненти до та після додавання елементів важливої інформації.

- У цій роботі якість стегосистем оцінювалася за низкою параметрів, серед яких було відношення сигнал/шум (SNR) - безрозмірна величина, що визначається як співвідношення корисного сигналу до шуму:

$$SNR = \sum_{x,y} (C_{x,y})^2 \Big/ \sum_{x,y} (C_{x,y} - S_{x,y})^2. \quad (4.3)$$

- показник якості зображення (IF) є однією з ключових метрик оцінювання стегоалгоритмів, що працюють із графічними даними:

$$IF = 1 - \sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2 \Big/ \sum_{x,y} (C_{x,y})^2. \quad (4.4)$$

- середньоквадратична похибка (MSE):

$$MSE = \frac{1}{X \cdot Y} \sum_{x,y} \left(C_{x,y} - S_{x,y}\right)^2. \quad (4.5)$$

- середня абсолютна різниця (AD) показує, наскільки значно відрізняються пікселі порожнього та заповненого контейнера.
Велике значення AD означає, що зображення має багато шумів або артефактів, що призводить до низької якості:

$$AD = \frac{1}{X \cdot Y} \sum_{x,y} \left|C_{x,y} - S_{x,y}\right|. \quad (4.6)$$

Тестування запропонованих методів проводилося на зображеннях розміром 128x128 пікселів, з використанням потужності приховування P = 50 для розробленого алгоритму. Розраховані показники характеристик представлені в табл. 4.2.

Таблиця 4.2 – Значення кількісних показників методів стеганографії

Показник викривлення	Розроблений метод (P=50)	Метод НЗБ	Метод БМЕЮ	Метод Коха-Жао
AD	0,649	0,494	0,042	0,5
IF	1	≈1	0,998	0,995
MSE	2,113	0,404	10,2	9,4

За формулами 2.12 – 2.14 виконаємо розрахунок пропускної здатності представлених методів:

Таблиця 4.3 – Значення пропускної спроможності методів стеганографії

Якісний показник	Розроблений метод	Метод НЗБ	Метод БМЕЮ	Метод Коха-Жао
Пропускна спроможність	0,086	0,058	0,023	0,038

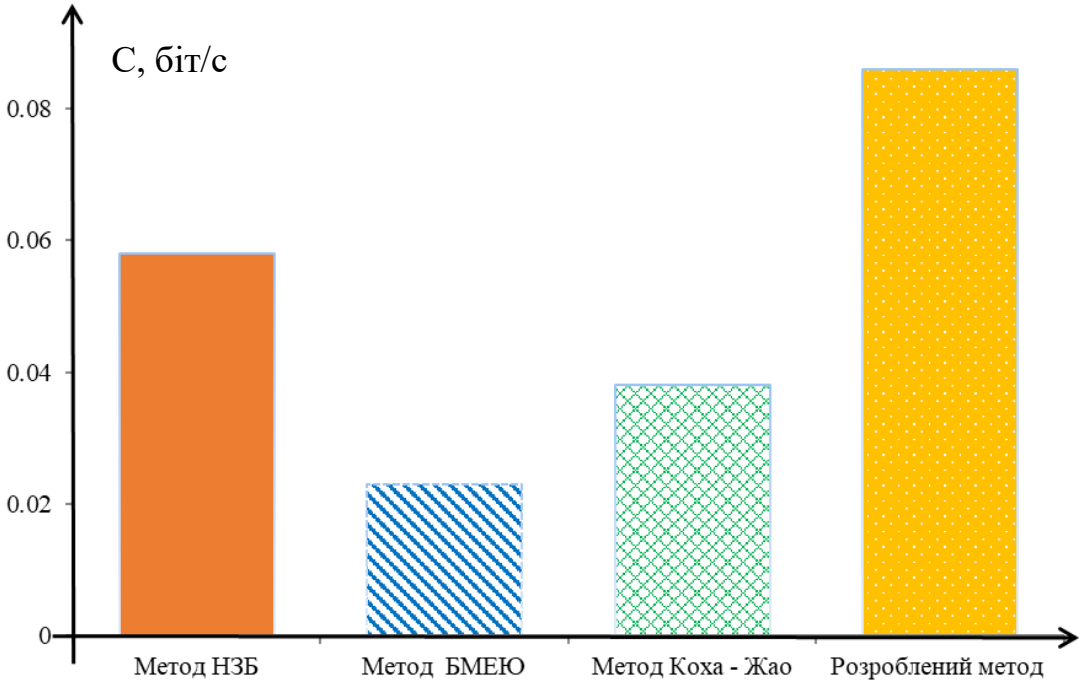

Рисунок 4.1 – Пропускна здатність розробленого та класичних методів цифрової стеганографії

Розроблений метод дозволяє досягти максимального збільшення порогового значення без помітного погіршення якості зображення. Проведено порівняльний аналіз кількісних та якісних характеристик як існуючих, так і запропонованої стеганографічної системи. Результати демонструють перевагу нашого методу над поширеними аналогами та його стійкість до статистичного стеганоаналізу, що підтверджується відсутністю значних відхилень у розрахованих показниках.

ВИСНОВКИ

У кваліфікаційній роботі вирішена актуальна задача підвищення захисту та достовірності мультимедійної інформації в умовах кіберзагроз.

В роботі обґрунтовано необхідність застосування методів цифрової стеганографії для приховання даних. Найперспективнішим напрямом розвитку цих методів є використання зображень як контейнерів інформації. Цей підхід є складовою загальної стратегії захисту та інформаційної безпеки. У певних випадках стеганографія виступає альтернативою криптографічним методам, тому важливо досліджувати сучасні методи стеганографії як ефективний інструмент захисту інформації.

Після аналізу існуючих методів приховування інформації в цифрових зображеннях було виявлено, що вони мають суттєві недоліки. Ці методи часто вразливі до атак, мають обмежену здатність приховувати великі обсяги даних і погано справляються з передачею зображень, коли зловмисник активно намагається втрутитися. Збільшення обсягу приховуваної інформації призводить до помітних спотворень зображення, що, в свою чергу, знижує ефективність захисту від візуального аналізу. Були розглянуті як якісні, так і кількісні показники методів стеганографії та їхній вплив на вихідне зображення.

Було сформульовано рекомендації щодо підвищення пропускної здатності при застосуванні методів вбудовування інформації у частотну область зображення. Розроблено метод стеганографічного приховування даних, що базується на виборі блоків, які є стійкими до компресійних атак і вносять мінімальні спотворення в зображення, що дає змогу ефективно їх використовувати для приховування інформації. Для аналізу були обрані первинні області зображення, зокрема LH та HL. Виявлено, що блоки, оброблені за допомогою нашого методу, демонструють стійкість до компресійних атак та мінімальні візуальні спотворення, що робить їх придатними для стеганографічного приховування даних. Відмінною рисою розробленого підходу є його здатність збільшувати обсяг передаваної прихованої інформації шляхом використання середньочастотних коефіцієнтів зображень-контейнерів. Ці зображення обираються за критерієм відсутності монотонності та різких перепадів яскравості, що досягається за допомогою

комбінованого застосування вейвлет- та дискретного косинусного перетворення.

Розроблений метод дозволяє досягти максимального збільшення порогового значення без помітного погіршення якості зображення. Проведено порівняльний аналіз кількісних та якісних характеристик як існуючих, так і запропонованої стеганографічної системи. Результати демонструють перевагу нашого методу над поширеними аналогами та його стійкість до статистичного стеганоаналізу, що підтверджується відсутністю значних відхилень у розрахованих показниках.

Досліджуваний метод демонструє середню пропускну здатність каналу, що перевищує показники інших методів стеганографії приблизно в 1,5 рази. Крім того, розроблений підхід відзначається високою стійкістю до відомих типів активних атак та стеганографічного аналізу, що застосовуються противником.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Мельник А. С. Інформаційні системи та мережі. Вісник НУ “Львівська політехніка”. – № 673.– Львів, 2017. – С. 365-374.

2. Стасюк О.І., Гнатюк С.О., Довгич Н.І., Літош М.С. Сучасні стеганографічні методи захисту інформації // Науковотехнічний журнал "Захист інформації". – 2011, № 1.

3. Хорошко В.А. Методы и средства защиты информации / В.А. Хорошко, А.А. Чекатков. – К. : Юниор, 2003. – 464 с.

4. Генне О.В. Основные положения стеганографии // Защита информации. Конфидент – 2000. №3 – 56 с.

5. Грибунін В.Г. Цифрова стеганографія – К.: СОЛОН - Пресс, 2017. – 272 с.

6. Конахович Г.Ф. Комп’ютерна стеганографія. Теорія та практика / А. Ю. Пузиренко — Київ: МК - Пресс, 2016. — 288 с.

7. Buckland M., Goldberg E. Emanuel Goldberg and His Knowledge Machine. – Libraries Unlimited. – 2006. – 70 p.

8. Смирнов М. Скрытая передача и хранение конфиденциальной информации в Интернете и сотовой связи [Ел. ресурс]. – Режим доступу: http://www.infocity.kiev.ua/hack/content/hack264.phtml.

9. An Overview of Steganography for the Computer Forensics Examiner. 2004. [Електронний ресурс]. – Режим доступу: http://www.garykessler.net/library/fsc_stego.html.

10. Корченко О.Г., Васіліу Є.В., Гнатюк С.О. Сучасні квантові технології захисту інформації // Науковотехнічний журнал "Захист інформації". – 2010, № 1. – С. 77-89.

11. Bilal A. Shaw. Quantum steganography and quantum error-correction // University of Southern California. – 2010. – P.137.

12. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky Rosen channels / Bennett C.H., Brassard G., Crepeau C., Jozsa R., Peres A., Wootters W.K. – 1993. – 128 p.

13. Barannik, V., Babenko M. *et al.* (2023). A Method of Scrambling for the System of Cryptocompression of Codograms Service Components. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in

the Digital Transformation Age. TCSET 2022. Lecture Notes in Electrical Engineering, vol 965. Springer, Switzerland, Cham. https://doi.org/10.1007/978-3-031-24963-1_26.

14. Головін М., Головіна Н. Навчальний приклад маскування інформації в акустичному сигналі. *Наукові записки Бердянського державного педагогічного університету.* 2021. № 2. С. 203–210.

15. Інформаційна безпека в комп'ютерних мережах : навч. посіб. / Смірнов О. А. та ін. Кропивницький : Вид. Лисенко В. Ф., 2020. 295 с.

16. V. Barannik, M. Babenko, A. Berchanov, V. Barannik, R. Onyshchenko and L. Kolodiichuk, "Method of Mini Segments Encoding in Difference Space Using Haar Wavelet," *2023 IEEE 5th International Conference on Advanced Information and Communication Technologies (AICT)*, Lviv, Ukraine, 2023, pp. 1-4, doi: 10.1109/AICT61584.2023.10452674.

17. . Barannik, V., Babenko Y. *et al.* (2023). Processing Marker Arrays of Clustered Transformants for Image Segments. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transformation Age. TCSET 2022. Lecture Notes in Electrical Engineering, vol 965. Springer, Switzerland, Cham. https://doi.org/10.1007/978-3-031-24963-1_25.

18. . V..Barannik, Y. Babenko, V. Barannik, V. Kolesnyk and D. Zhuikov, "Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 66-71, doi: 10.1109/ATIT58178.2022.10024193.

19. . Barannik V., Barannik N. Indirect information hiding technology on a multiadic basis // Informatyka, Automatyka, Pomiary w Gospodarce i Ochronie Środowiska, 2021, Volume T. 11, nr 4, Pages 14 – 17. DOI 10.35784/iapgos.2812.

20. . V. Barannik, A. Alimpiev, A. Bekirov, D. Barannik and N. Barannik, "Detections of sustainable areas for steganographic embedding," 2017 IEEE East-West Design & Test Symposium (EWDTS), Novi Sad, Serbia, 2017, pp. 1-4, doi: 10.1109/EWDTS.2017.8110028.

21. . D. Barannik and V. Barannik, "Steganographic Coding Technology for Hiding Information in Infocommunication Systems of Critical Infrastructure," 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 88-91, doi: 10.1109/ATIT58178.2022.10024185.

22. . Barannik V., Khimenko V., Barannik N., Method of indirect information hiding in the process of video compression. Radioelectronic and Computer Systems. 2021. №. 4. PP. 119–131. https://doi.org/10.32620/reks.2021.4.

23. Ding Z. GPU accelerated interactive space-time video matting / Z. Ding, H. Chen, Y. Gua, Q. Peng // In Computer Graphics International. – 2010. – pp. 163-168.

24. Гонсалес Р. Цифрова обробка зображень. 3-е видання. / Р. Гонсалес, Р. Вудс. – К.: Техносфера, 2017. – 1104 с.