Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Система захисту інформації з використанням стеганографічних методів

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІ-21-3
Олександр ПОЛУПАН
(власне ім’я, прізвище)

Спеціальність
123 «Комп’ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп’ютерна інженерія
(повна назва освітньої програми)

Керівник: ас. Олександр РОМАНЮК
(посада, власне ім’я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім’я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Полупану Олександру Романовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Система захисту інформації з використанням стеганографічних методів

затверджена наказом по університету від “ 26 ” травня 2025 р. № 424 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 16 червня 2025 р.

3. Вхідні дані до роботи захист інформації, стеганографія, криптографія, LSB-метод, AES-шифрування, прихована передача даних,

4. Перелік питань, що потрібно опрацювати у роботі

Теоретичні основи

Методи

Тестування системи

Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 17

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Отримання теми кваліфікаційної роботи	26.05	
2	Аналіз літератури	27.05-29.05	
3	Побудова системи	28.05-10.06	
4	Тестування системи та отримання результатів	11.06-12.06	
5	Формування пояснювальної записки	13.06-14.06	
6	Перевірка на плагіат	15.06-17.06	
7	Рецензування роботи	17.06	
8	Подача роботи в ЕК	18.06	
9	Захист роботи	24.06	

Дата видачі завдання " 26 " травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ас. Олександр РОМАНЮК
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 50 с., 12 рис., 1 дод., 25 джерел.

ЗАХИСТ ІНФОРМАЦІЇ, СТЕГАНОГРАФІЯ, КРИПТОГРАФІЯ, LSB-МЕТОД, AES-ШИФРУВАННЯ, ПРИХОВАНА ПЕРЕДАЧА ДАНИХ.

Метою кваліфікаційної роботи є створення системи захисту інформації з використанням стеганографічних методів.

У ході виконання кваліфікаційної роботи… представлено вдосконалену багаторівневу систему безпеки, що інтегрує стеганографію та криптографію для забезпечення конфіденційного обміну інформацією. Запропонована криптостеганографічна модель поєднує AES-шифрування, QR-коди та метод LSB-стеганографії для безпечного приховування текстових повідомлень у графічних зображеннях. Такий комплексний підхід забезпечує високу стійкість до несанкціонованого доступу, зберігаючи цілісність та непомітність вбудованих даних.

Результати експериментів засвідчили ефективність системи в умовах диференціального криптоаналізу, а також її високу дифузію та плутанину. Проведений аналіз ентропії та стандартного відхилення дозволив оцінити вплив різних методів стеганографії на текстуру зображень та ступінь приховування інформації.

ABSTRACT

Bachelor’s thesis: 50 pages, 12 figures, 1 appendices, 25 sources.

INFORMATION SECURITY, STEGANOGRAPHY, CRYPTOGRAPHY, LSB METHOD, AES ENCRYPTION, HIDDEN DATA TRANSMISSION

The major goal of this thesis is to develop an information security system using steganographic methods.

This bachelor's qualification work presents an advanced multi-level security system that integrates steganography and cryptography to enable confidential information exchange. The proposed cryptosteganographic model combines AES encryption, QR codes, and the LSB steganography method to securely embed textual messages into digital images. This comprehensive approach ensures high resistance to unauthorized access while preserving the integrity and invisibility of the embedded data.

Experimental results confirm the system’s effectiveness under differential cryptanalysis, demonstrating strong diffusion and confusion properties. Entropy and standard deviation analysis was conducted to evaluate the impact of different steganographic techniques on image texture and data concealment.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ІС – Інформаційна система

ЗІ – Захист інформації

LSB –Найменш значущий біт

AES – Advanced Encryption Standard

QR – Quick Response

RSA – Rivest-Shamir-Adleman

ВСТУП

Сучасне суспільство немислиме без інтенсивного обміну даними, який став основою цифрової комунікації, електронної комерції та соціальних взаємодій. Проте стрімкий розвиток інтернет-технологій, окрім беззаперечних переваг, породив критичні виклики, пов’язані із захистом конфіденційної інформації. Особливої уваги потребують методи забезпечення безпеки зображень, що містять приватні або секретні дані, оскільки традиційні підходи шифрування часто виявляються недостатніми для протидії сучасним кіберзагрозам. У цьому контексті стеганографія, яка приховує дані у звичайних на вигляд файлах, набуває ключового значення, забезпечуючи непомітність і стійкість до виявлення.

Сучасні стеганографічні методи стикаються з низкою обмежень, зокрема високою обчислювальною складністю, втратою якості прихованих даних та недостатньою адаптацією до динамічних вимог безпеки. Для подолання цих проблем у даній роботі пропонується інноваційна стеганографічна мережа, яка інтегрує дві взаємодоповнюючі підмережі: мережу приховування та мережу розкриття. Ця архітектура забезпечує окреме вбудовування та відновлення секретних даних, що підвищує гнучкість і надійність системи.

Для оптимізації обчислювальних процесів розроблено каркас мережі зі структурою «знизу вгору», який стискає проміжні карти ознак, зберігаючи при цьому ключові характеристики вхідних даних. Для мінімізації втрати інформації через багатошарові згортки запроваджено метод конкатенації з довгим пропуском, що передає необроблені дані на верхні рівні мережі. Це дозволяє синтезувати високоякісні приховані зображення з деталізованою текстурою. Додатково запропоновано стратегію неактивованого об’єднання ознак (NAFF), яка покращує контроль над синтезом прихованих та відновлених зображень, забезпечуючи точність відтворення.

Важливим елементом системи є модуль на основі механізму уваги, призначений для реконструкції ключових об’єктів на зображенні. Цей модуль підвищує візуальну якість прихованого зображення та зменшує ризик виявлення секретного вмісту. Для досягнення балансу міструктурною цілісністю та непомітністю впроваджено гібридну функцію втрат, що поєднує втрати в піксельному та структурному доменах.

Експериментальні результати підтверджують, що запропонований метод забезпечує високу ступінь непомітності та безпеки, перевершуючи традиційні підходи за показниками якості відновлення даних і стійкості до атак. Актуальність дослідження полягає в комплексному вирішенні проблем сучасної стеганографії, що відкриває нові можливості для захисту конфіденційної інформації в умовах зростання кіберзагроз. Робота має теоретичну та практичну цінність для розвитку галузей, пов’язаних із кібербезпекою, машинним навчанням і обробкою мультимедійних даних.

1 ТЕОРЕТИЧНІ ОСНОВИ

Зі швидким розвитком інтелектуальних технологій поєднання інформаційних технологій та інтелектуальних технологій вступило у стадію швидкого розвитку [1]. Різні взаємопов'язані інформаційні пристрої щодня створюють велику кількість даних зображень. Деякі дані зображень можуть містити конфіденційну або навіть конфіденційну інформацію, таку як зображення посвідчень особи, зображення банківських карток, електронні зображення, що стосуються особистого життя, і навіть деякі конфіденційні військові зображення або зображення дистанційного зондування. В останні роки технології цифрових медіа забезпечили велику зручність для обробки зображень, але вони також створюють серйозні проблеми безпеки під час передачі секретних даних зображень. Розголошення цих секретних даних зображень у загальнодоступній мережі легко приверне увагу зловмисників, що наражає секретні дані зображень на високий ризик перехоплення або крадіжки злочинцями. Тому питання захисту секретних даних зображень та забезпечення їхньої безпеки стало нагальним.

Наразі шифрування [2, 3] є найпоширенішим методом безпеки в галузі цифрового зв'язку, оскільки воно зазвичай використовує складні та добре розроблені алгоритми шифрування для перетворення секретної інформації в певну форму шифротексту. Однак метод шифрування зосереджений лише на безпеці інформаційного контенту; він не може приховати існування секретної інформації, що викличе увагу та підозру у сторонніх зловмисників. Навіть якщо зловмисники не зможуть розшифрувати секретну інформацію за короткий час, вони можуть перехопити процес передачі та знайти термінали передачі даних, щоб здійснити атаку, що становить велику загрозу для передачі інформації. За останні кілька років новий метод безпеки, який називається цифровою стеганографією [4], привернув широку увагу та інтерес як в академічній спільноті, так і в промисловій сфері. На відміну від

методу шифрування, який робить секретну інформацію нечитабельною та незрозумілою, метод стеганографії спрямований на те, щоб зробити секретну інформацію непомітною шляхом приховування її на загальному носії. Цифрові носії, що використовуються для стеганографії, включають двійковий текст, аудіо та зображення тощо; Серед них зображення використовується найчастіше, оскільки воно має велику здатність приховувати більше секретної інформації та багату текстуру для підвищення непомітності. Стеганографія, що використовує зображення як носій, зазвичай називається стеганографією зображень [5], і для досягнення приховування інформації було запропоновано багато схем стеганографії зображень. Ми можемо розділити ці схеми на дві категорії, а саме: традиційну стеганографію зображень та стеганографію зображень на основі глибокого навчання.

У традиційній стеганографії зображень найтиповішим репрезентативним методом є метод найменш значущого біта (LSB) [6]. Як усім відомо, візуальний вигляд зображення визначається його пікселями, і кожен піксель містить три значення R, G та B. Ці значення пікселів представлені 8-бітним двійковим числом, візуальний вигляд зображення в основному визначається старшими бітами, а молодші біти мають найменший вплив на візуальний вигляд. Тому метод LSB реалізується шляхом вбудовування секретної інформації в молодші біти зображення обкладинки, щоб зберегти візуальний вигляд зображення обкладинки незмінним. Метод LSB широко використовується, оскільки він може приховувати різні форми секретних даних, включаючи звичайний текст та дані зображень; однак, секретні дані, вбудовані методом LSB, легко виявити завдяки фіксованій маніпуляції та статистичній властивості. Згодом був запропонований інший метод, який називається високоневиявлювана стеганографія (HUGO) [7], де вперше було запропоновано концепцію функції спотворення для моделювання та керівництва стеганографією. В [8] запропонували метод, який називається вейвлет-отриманими вагами (WOW), який може адаптивно

вбудовувати секретну інформацію в різні області зображення відповідно до їхньої текстурної складності. У роботі [9] далі обговорили універсальну функцію спотворення, незалежну від вбудованої області, а функція спотворення визначається як сума відносних змін коефіцієнтів багатонаправленого фільтра, що змушує модифікації зосереджуватися на областях з багатою текстурою або високочастотним шумом, тим самим уникаючи вбудовування секретних даних у гладкі області. Для розширення застосування методу було запропоновано метод стеганографії, спеціально розроблений для зображень JPEG [10], який перетворює зображення в частотну область за допомогою дискретного косинусного перетворення. Функція спотворення визначається частотними коефіцієнтами, доступними для гнучкого розподілу вбудованих даних.

Хоча вищезгадані традиційні методи значно сприяли розвитку стеганографії зображень, вони все ще стикаються з наступними проблемами.

Вони завжди призначені для приховування невеликої кількості повідомлень на бітовому рівні (<0,4 біт/піксель), де ємність корисного навантаження вимірюється в бітах на піксель (біт/піксель), тому вони не можуть задовольнити вимогу приховування даних зображення.

Вони завжди розробляються на основі знань предметної області та ручно створених ознак з низькою розмірністю, які не можуть точно відобразити статистичні характеристики високого порядку цілі [11], що значно обмежує стеганографічну продуктивність. Крім того, штучне проектування, що спирається на знання предметної області, є не тільки дорогим, але й трудомістким та тривалим.

З огляду на вищезазначені обмеження традиційних методів стеганографії, останніми роками деякі вчені досліджували впровадження глибокого навчання в стеганографічну техніку, прагнучи досягти прориву в порівнянні з традиційними методами, спираючись на потужну здатність глибокого навчання до представлення ознак. Зокрема, в [12] розробили систему автоматичного навчання, що базується на генеративно-змагальних

мережах (GAN), яка створює карту ймовірності спотворення шляхом навчання дискримінатора за допомогою генератора. Для генерації зображень обкладинки вищої якості в [13] розробили стеганографічну мережу під назвою SSGAN, замінивши традиційну GAN на нову WGAN [13], а потім вони застосували традиційні алгоритми вбудовування, щоб вбудувати секретні дані у згенероване зображення обкладинки. Хоча різні методи [12, 13] досягли прогресу в своїй стеганографічній продуктивності, вони не повністю позбулися залежності від традиційних алгоритмів вбудовування. З цією метою в [14] запропонували наскрізну стеганографічну структуру під назвою HiDDeN, яка може бути застосована як у стеганографії, так і в водяних знаках. Для подальшого збільшення ємності корисного навантаження було запропоновано новий метод стеганографії під назвою SteganoGAN [15], і експерименти показують, що цей метод досяг сучасного корисного навантаження 4,4 біт/пікс. Однак усі вищезгадані методи на основі глибокого навчання все ще призначені для приховування невеликої кількості повідомлень на бітовому рівні. Для досягнення мети приховування даних зображення була розроблена нова мережа кодер-декодер [16] на основі згорткових нейронних мереж (CNN), які можуть приховати ціле секретне зображення в інше зображення-обкладинку. Однак цей метод генерує приховані зображення з видимими спотвореннями через грубу розробку моделі. Для подальшого покращення стеганографічної продуктивності цього методу [17] запропонували глибоку оборотну мережу та отримали приємну для сприйняття продуктивність. Однак, залишкова інформація між прихованим зображенням та оригінальним зображенням обкладинки, яка значною мірою визначає безпеку стеганографії, не була продемонстрована в їхньому дослідженні. В [18] показав карту залишків, отриману шляхом фіксації піксельних відмінностей між прихованим зображенням та зображенням обкладинки, та вказав на напрямок дослідження щодо покращення безпеки стеганографії; однак, якість прихованого зображення суттєво не покращилася. Для подальшого покращення якості прихованого

зображення та підвищення стеганографічної продуктивності джерела, в [19] спробували поглибити та розширити мережу, використовуючи різні передові стратегії об'єднання ознак, і в результаті було досягнуто значного прогресу.

Хоча вищезгадані методи на основі глибокого навчання [20] успішно досягли мети приховування даних зображень, проблеми безпеки, особливо візуальної безпеки, не були належним чином вирішені. Крім того, останні дослідження зазвичай розробляють складні моделі для покращення продуктивності, але вони ігнорують обчислювальну складність моделі на практиці.

2 МЕТОДИ

2.1 Загальна архітектура

У попередніх методах стеганографії зображень дослідники зазвичай прагнули покращити стеганографічну продуктивність, покладаючись на складне проектування моделей, що значно збільшувало споживання пам'яті методом. Враховуючи обмежені ресурси пам'яті та обчислювальних ресурсів у практичних пристроях, таких як смартфони, дуже важливо розробити стеганографічну модель з низькою складністю. Для цього ми побудували мережу зі структурою «вниз-вгору», щоб зменшити роздільну здатність проміжних карт ознак, тим самим зменшуючи складність моделі та накладні витрати пам'яті. Загальна архітектура запропонованого нами методу показана на рисунку 2.1

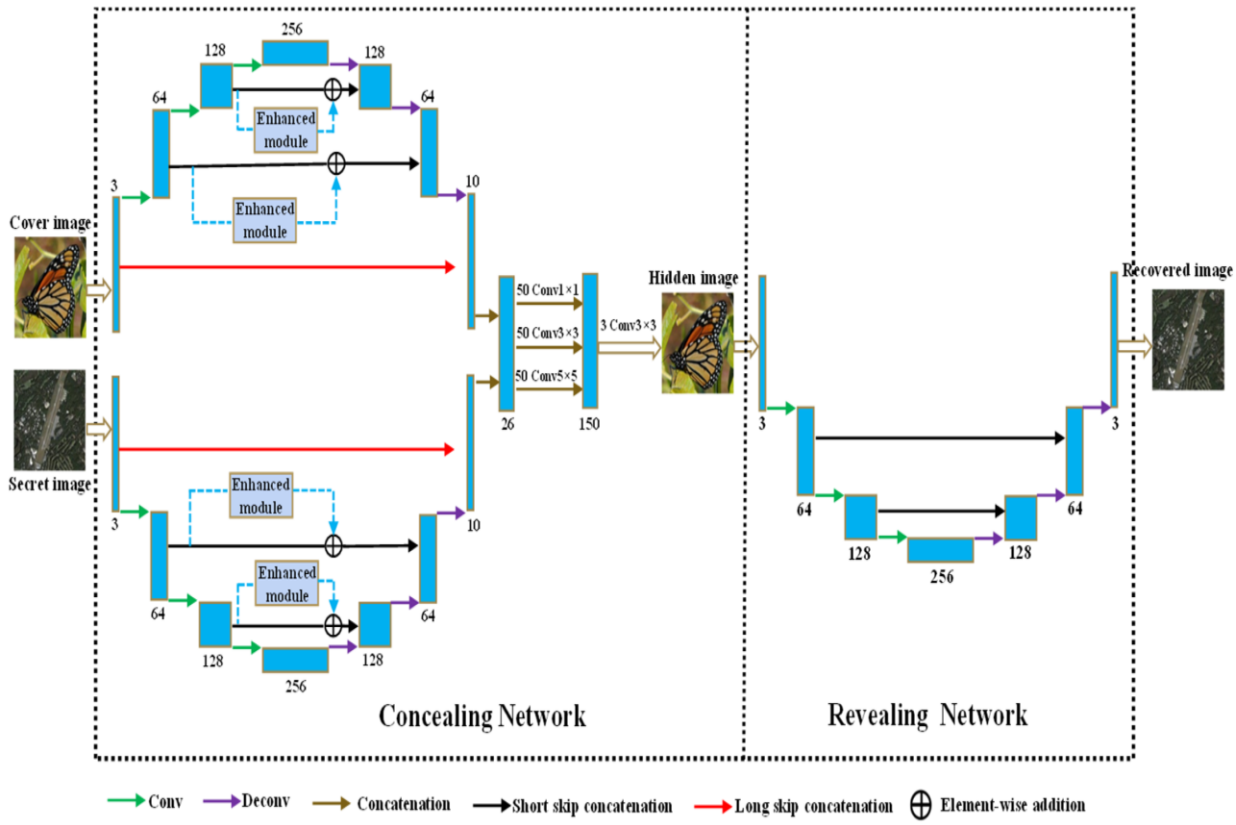

Рисунок 2.1 – Загальна архітектура запропонованого методу.

Як показано на рисунку 2.1, запропонована мережа містить дві підмережі, які називаються мережею приховування та мережею розкриття. Спочатку відправник вбудовує секретне зображення в загальне зображення обкладинки за допомогою мережі приховування та синтезує зображення, яке називається прихованим зображенням (вбудованим із секретним контентом). Приховане зображення передається через публічний Інтернет, не викликаючи підозр у зловмисників. Потім приймач отримує приховане зображення та витягує секретну інформацію з прихованого зображення за допомогою мережі розкриття, щоб отримати відновлене зображення. У процесі приховування зображення обкладинки та секретне зображення окремо подаються до двох гілок мережі приховування. За допомогою серії операцій дискретизації (які досягаються за допомогою шарів безперервної згортки) вхідні зображення поступово стискаються в дрібномасштабні карти ознак. Операція дискретизації має такі переваги: вона може ефективно захоплювати семантичну інформацію високого рівня та довгострокові кореляції з попіксельної інформації зображення обкладинки та секретного зображення; вона може зменшити роздільну здатність проміжних карт ознак, тим самим зменшуючи складність моделі та споживання пам'яті. Згодом, роздільна здатність карти ознак поступово розширюється до роздільної здатності оригінального зображення за допомогою серії операцій підвищення роздільної здатності (які досягаються шляхом реалізації шарів безперервної деконволюції). Потім, високорівневі абстрактні ознаки, витягнуті з гілки обкладинки та секретної гілки, об'єднуються у верхньому шарі за допомогою операції конкатенації. За допомогою багатомасштабних операцій згортки Conv 1×1, Conv 3×3 та Conv 5×5, багаті ознаки різних масштабів додатково повністю витягуються та високо об'єднуються. Нарешті, номер каналу карти ознак зменшується до 3 за допомогою операції Conv 3×3, щоб отримати приховане зображення, візуально схоже на зображення обкладинки. Аналогічно, для мережі виявлення, її вхід - це приховане зображення, вбудоване в секретну інформацію. За допомогою серії операцій зниження

роздільної здатності, роздільна здатність прихованого зображення поступово зменшується, а цінна семантична інформація для реконструкції секретного зображення витягується та зберігається. Потім, дрібні деталі секретного зображення поступово реконструюються за допомогою серії операцій підвищення роздільної здатності. Симетричні шари згортки та деконволюції з'єднані коротким пропуском конкатенації для покращення об'єднання ознак низькорівневих та високорівневих ознак, крім того, ця операція може добре боротися з проблемою зникнення градієнта. Числа, такі як 3, 26 та 50, представляють номери каналів карт ознак.

У цій роботі кожен шар згортки та деконволюції супроводжується операцією пакетної нормалізації (BN) для пришвидшення навчання, за винятком останнього шару цих двох підмереж. У процесі зниження частоти дискретизації використовується функція активації LeakyReLU з нахилом 0,2, а функція активації Relu використовується в процесі підвищення частоти дискретизації. Розмір ядра в процесах зниження та підвищення частоти дискретизації встановлено як 4×4 з кроком 2. На відміну від інших досліджень, які зазвичай використовують операцію об'єднання для зниження частоти дискретизації, у нашій роботі операція об'єднання відкидається для зниження частоти дискретизації, оскільки це призведе до серйозної втрати деталей зображення та збільшення складності обчислень.

2.2 Конкатенація довгих пропусків

У нашому завданні, щоб забезпечити непомітність, синтетичне приховане зображення має бути схожим на зображення обкладинки. Крім того, для гарантії якості відновлення очікується, що відновлене зображення буде схожим на секретне зображення. Однак, після серії шарів згортки та деконволюції, вхідні зображення, такі як зображення обкладинки та секретне зображення, неминуче втрачають певну інформацію, що надзвичайно негативно впливає на ефективність приховування та виявлення. Щоб

вирішити цю проблему, ми також пропонуємо пропускну конкатенацію, показану на рисунку 2.1, яка може безпосередньо передавати інформацію про необроблене зображення верхньому шару та допомагати синтезувати деталі країв та текстури, тим самим покращуючи ефективність приховування та виявлення.

Конкатенація довгих пропусків досягається за допомогою конкатенації каналів карт ознак, враховуючи вхідне зображення якI_iIi, конкатенацію довгих пропусків можна описати як

$$I_o = F_P[I_i] * I_i$$

Де I_o представляє результат операції конкатенації, F_P[ ] вказує на процес вилучення ознак, реалізований серією шарів згортки-деконволюції, та * представляє операцію конкатенації каналів. Припустимо, що вхідне зображення I_i маєc_1c1канали та $F_P[Ii]$ має $c2$ канали. Після операції об'єднання вихід I_o має c1+c2 канали. Можна помітити, що конкатенація з довгим пропуском може безпосередньо передавати інформацію про необроблене зображення на верхній шар і створювати вихідний I_o містити вихідну вхідну інформацію I_i, таким чином ефективно зменшуючи втрату інформації з початкових вхідних даних.

Як показано на рисунку 2.1, зображення обкладинки або секретне зображення має лише 3 канали: R, G та B, тому конкатенація з довгим пропуском не призведе до суттєвого збільшення кількості каналів вихідних карт ознак. В результаті складність обчислень збільшується лише незначно.

2.3 Стратегія NAFF

У попередніх завданнях комп'ютерного зору, таких як виявлення об'єктів, розпізнавання цілей та семантична сегментація, функція активації

зазвичай відіграє значну роль у вищезгаданих завданнях, оскільки активовані ознаки представляють ознаки та атрибути вищого рівня, які більше сприяють розрізненню високорівневих категорій цілі. Однак стеганографія зображення до зображення належить до змішаного режиму завдань високого та низького рівнів, оскільки вона вимагає не лише семантичної інформації високого рівня для проведення процесу приховування та розкриття, але й низькорівневих ознак для реконструкції дрібних деталей зображення. Однак операція активації може змінити детальну інформацію зображення та погіршити точність деяких низькорівневих ознак, таких як інформація про текстуру та краї. З цієї причини ми пропонуємо нову стратегію під назвою NAFF для об'єднання неактивованих ознак замість традиційних активованих ознак, які широко використовуються в більшості досліджень комп'ютерного зору. Запропонована NAFF може зберегти більше низькорівневих ознак зображення обкладинки та прихованого зображення та забезпечити кращий нагляд за синтезом текстури та деталей країв, тим самим покращуючи якість синтезу прихованого зображення та якість відновлення прихованого зображення.

2.4 Розширений модуль

Механізм уваги відіграє важливу роль у сприйнятті людським мозком та системою зору, і він може спонукати систему сприйняття зосередитися на помітній області цільового об'єкта. Протягом останніх кількох років механізм уваги широко застосовується в різних інтелектуальних завданнях, таких як виявлення об'єктів [21], підписування зображень [22] тощо, і досяг видатної продуктивності. Нещодавно деякі вчені спробували впровадити механізм уваги в завдання стеганографії зображень для подальшого покращення продуктивності стеганографії. Зокрема, в [23] впровадили механізм уваги в стеганографію на основі GAN без вбудовування та розробили модуль уваги для зосередження на просторовій інформації та захоплення кореляції між

пікселями. Потім в [24] запропонували наскрізну стеганографічну мережу з модулем уваги каналу для зосередження на інформації каналу та захоплення взаємозалежностей каналів. Однак обидва методи в [21, 22] все ще призначені для приховування невеликої кількості повідомлень на бітовому рівні. Натхненні вищезазначеними роботами, ми досліджуємо інтеграцію механізму уваги в наше завдання стеганографії зображень для приховування даних зображення, і сподіваємося, що механізм уваги відіграватиме дві ролі. Перша роль полягає у вилученні помітних ознак з обкладинки зображення та синтезі помітної цілі прихованого зображення для маскування та затьмарення вбудованого секретного вмісту, тим самим підвищуючи візуальну безпеку та непомітність. Друга роль полягає у вилученні важливої інформації з прихованого зображення та збереженні важливих підказок у прихованому зображенні для відновлення важливого секретного вмісту у відновленому зображенні. Тому розроблено вдосконалений модуль, який допоможе мережі адаптивно зосередитися на помітній області зі значними ознаками, що показано на рисунку 2.2

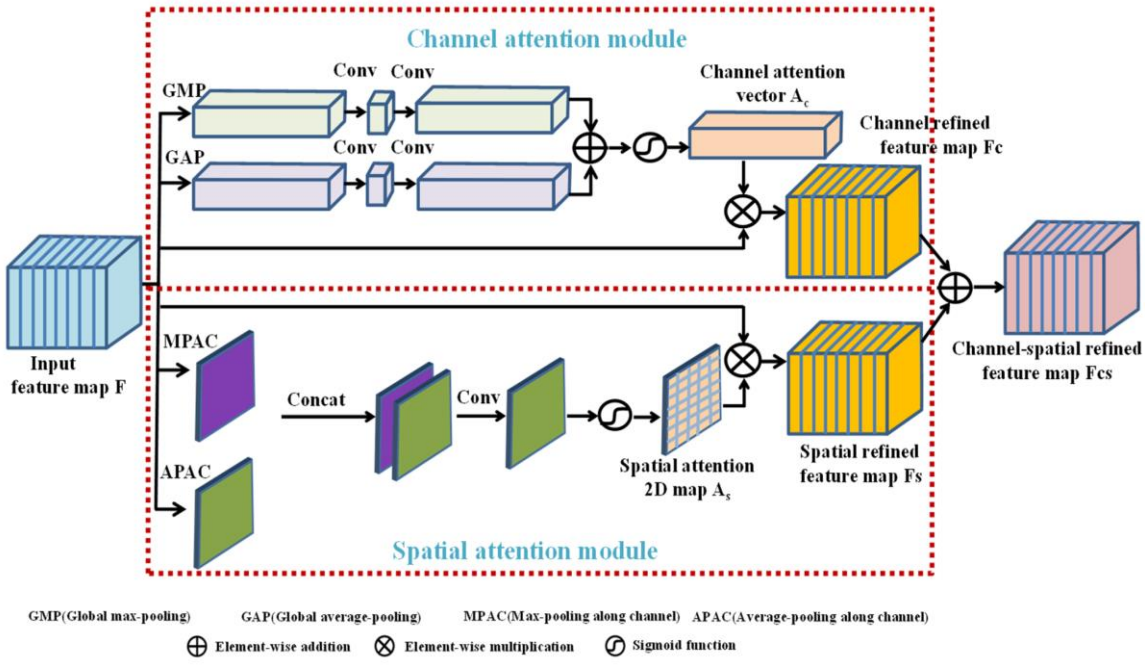

Рисунок 2.2 – Архітектура вдосконаленого модуля.

Зокрема, вдосконалений модуль, розроблений у цій роботі, складається з двох підмодулів, а саме модуля уваги до каналу та модуля просторової уваги. Ці два підмодулі паралельно виявляють визначальні ознаки та зосереджуються на визначальних ознаках з двох різних точок зору: вимірів каналу та просторових вимірів; таким чином, вони доповнюють один одного. Порівняно з модулем уваги, який зосереджується лише на просторовій інформації, та модулем уваги, який зосереджується лише на інформації каналу, розроблений нами вдосконалений модуль фіксує значну інформацію як у вимірах каналу, так і в просторових вимірах. Крім того, розроблений вдосконалений модуль є надзвичайно легким та значно підвищує можливості представлення ознак, майже не збільшуючи складність моделі. Наводимо детальний опис його модулів.

Модуль уваги до каналу: щоб забезпечити візуальну схожість прихованого зображення та відновленого зображення з оригінальним зображенням обкладинки та прихованим зображенням, слід приділити більше уваги виразним областям, таким як високочастотна текстура, контур та краї, які відіграють вирішальну роль у візуальному вигляді. Тому глобальне об'єднання максимумів (GMP) та глобальне об'єднання середніх значень (GAP), показані на рисунку 2.2, одночасно застосовуються для стиснення та агрегування інформації з кожного каналу вхідної карти ознак. GMP може зберегти найважливішу ознаку з усіх каналів, тоді як GAP може використовуватися як допоміжний засіб для збору іншої цінної інформації та збереження глобальної інформації з усіх каналів. Припустимо, що вхідна карта ознак $F \in R^{C \times H \times W}$ подається в модуль уваги до каналу; після операцій стискання GMP та GAP, два вектори каналу розміром $R^{C \times 1 \times 1}$ можна отримати (зазвичай, номер каналу, представлений як C є великим значенням, але складність модуля можна ще більше зменшити, використовуючи два безперервні шари Conv 1×1. Номер каналу першої операції Conv 1×1 дорівнює C/r, де r – коефіцієнт зменшення номера каналу, а номер каналу

другої операції Conv 1×1 дорівнює C Функція активації Relu використовується між цими двома операціями Conv 1×1 для подальшого покращення можливостей вилучення нелінійних ознак. Для спрощення вищезазначені операції можна представити символом, який називаєтьсяC_rCCrC). Два канальні вектори, що утворюютьсяC_rCCrCдодаються, а потім активуються функцією активації сигмоподібної форми для генерації вектора уваги каналу як$\mathbf{A}_c \in \mathbf{R}^{C \times 1 \times 1}$AC∈RC×1×1Зрештою, ми можемо отримати уточнену карту ознак каналу $\mathbf{F}_c$ наступним чином.

Стійкість заданого алгоритму вилучення та декодування стеганографічних даних оцінюється на основі його стійкості до атак, точності відновлення, обчислювальної складності та толерантності до помилок.

Алгоритм забезпечує надійний захист завдяки XOR-шифруванню з ключем, згенерованим на основі логістичної карти, що підвищує стійкість до атак методом перебору. Кодування ДНК вводить додатковий рівень трансформації, що ускладнює прямий аналіз.

Кодування на основі QR-кодів покращує надійність завдяки вбудованій корекції помилок, що дозволяє часткове відновлення, навіть якщо виникають незначні спотворення. Етапи вилучення та дешифрування є обчислювально ефективними. Вилучення LSB, декодування ДНК та дешифрування XOR працюють в$O(n)$ часова складність. Метод дозволяє точно відновити повідомлення з неушкодженого стегозображення. Кілька етапів кодування та шифрування підвищують конфіденційність даних. Це ускладнює для будь-яких зловмисників доступ до прихованої інформації без правильного ключа розшифрування.

Запропонований метод є безпечним, ефективним та здатним забезпечити високу точність відновлення даних. Це досягається завдяки використанню хаотичного шифрування, стійкості QR-кодів та ДНК-кодування, що разом підвищує конфіденційність. Його обчислювальна ефективність робить його практичним рішенням для стеганографічних застосувань, де цілісність повідомлень є критично важливою.

2.5 Збільшення розміру медіафайлів

Збільшення розміру медіафайлів у нашій системі головним чином зумовлене багаторівневим процесом кодування, який включає AES-шифрування, кодування послідовностей ДНК, генерацію QR-кодів та LSB-стеганографію. Кожен шар вводить додаткові дані для підвищення безпеки та стійкості. AES-шифрування розширює повідомлення за допомогою доповнення блоків та перетворень, тоді як ДНК-кодування додатково збільшує розмір, перетворюючи двійкові послідовності на нуклеотиди. Генерація QR-кодів додає надмірність для виправлення помилок, а LSB-стеганографія змінює значення пікселів у зображенні, що потенційно впливає на стиснення та розмір файлу. На відміну від традиційних одношарових методів, які спрямовані на мінімізацію змін розміру, наш підхід надає пріоритет надійній безпеці там, де збільшення розміру медіафайлів виправдане, гарантуючи, що приховані дані залишаються безпечними та непомітними.

2.6 Порівняльне обговорення з традиційними стеганографічними методами

Традиційні стеганографічні методи, такі як вбудовування найменш значущих бітів (LSB), покращене зіставлення найменш значущих бітів (ELSB), зіставлення найменш значущих бітів (LSBM) та методи на основі DCT, спрямовані на мінімізацію збільшення розміру файлу під час вбудовування секретних даних. Наприклад, базове вбудовування LSB замінює найменш значущі біти значень пікселів бітами секретного повідомлення, що призводить до незначних змін у розмірі файлу. Однак такі підходи дуже вразливі до атак на основі статистичного стегоаналізу та кореляції пікселів, що робить їх непридатними для застосувань з високим рівнем безпеки. На противагу цьому, наш багаторівневий підхід, який

інтегрує шифрування AES, кодування послідовностей ДНК, перетворення QR-коду та вбудовування LSB, вводить додаткові рівні безпеки за рахунок збільшення розміру файлу. Етапи шифрування та кодування додають надмірність та накладні витрати на перетворення, що сприяє збільшенню розміру носія, але значно підвищує стійкість до стегоаналізу, криптоаналізу та атак методом перебору. Хоча методи на основі DCT розподіляють дані за частотними компонентами для покращення непомітності, вони часто страждають від артефактів стиснення та втрати прихованих даних у форматах стиснення з втратами, таких як JPEG. Для порівняння, наш метод забезпечує надійне шифрування, цілісність даних та прихований зв'язок, що робить його більш придатним для високозахищених застосувань, де надійність має пріоритет над мінімальним розширенням файлу.

3 ТЕСТУВАННЯ СИСТЕМИ

У цьому розділі ми спочатку представимо експериментальну платформу та установку. Потім ми проведемо масштабні експерименти, щоб ретельно перевірити ефективність наших варіантів проектування та продемонструвати перевагу нашого методу.

3.1 Методи стеганографії для аудіофайлів

3.1.1 Метод найменш значущого біта (LSB)

Цей метод є одним із найпопулярніших завдяки простоті реалізації. Дані приховуються шляхом заміни найменш значущих бітів у вибірках аудіофайлу. При цьому зміни у звуці залишаються непомітними для людського вуха. Основні переваги методу це великий обсяг прихованих даних та незмінність розміру аудіофайлу після приховування [24].

Однак для підвищення стійкості рекомендується використовувати «зашумлені» файли-контейнери, оскільки у «чистих» контейнерах зміни в молодших бітах легко виявити [24].

Зручніше за все відобразити метод найменш значущого біту у вигляді зображення:

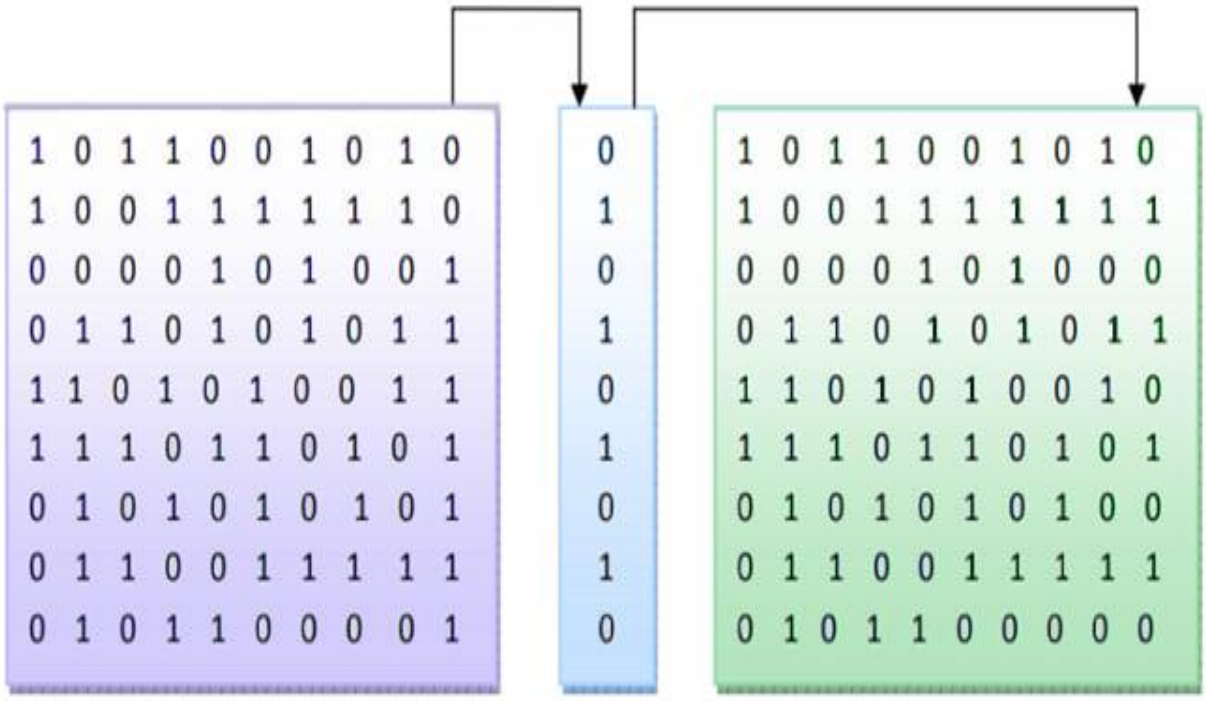

Рисунок 3.1 – Метод LSB для аудіо-стеганографії

3.1.2 Паритетне кодування

Ще одним із цікавих і ефективних методів звукової стеганографії є використання паритетного кодування. На відміну від традиційних підходів, де сигнал розбивається на окремі зразки, тут ми беремо кожен зразок і вкладаємо в нього біт парності замість того, щоб використовувати окремі біти для представлення інформації, що підвищує стійкість до атак. У цьому методі, якщо біт парності не відповідає секретному біту, який ми хочемо закодувати, ми можемо інвертувати найменш значущий біт (LSB) у зразку в цьому регіоні. Це дає відправнику більше гнучкості при кодуванні секретної інформації. Розглянемо схему методу паритетного кодування, де перші три біти закодовані на наступному зображенні:

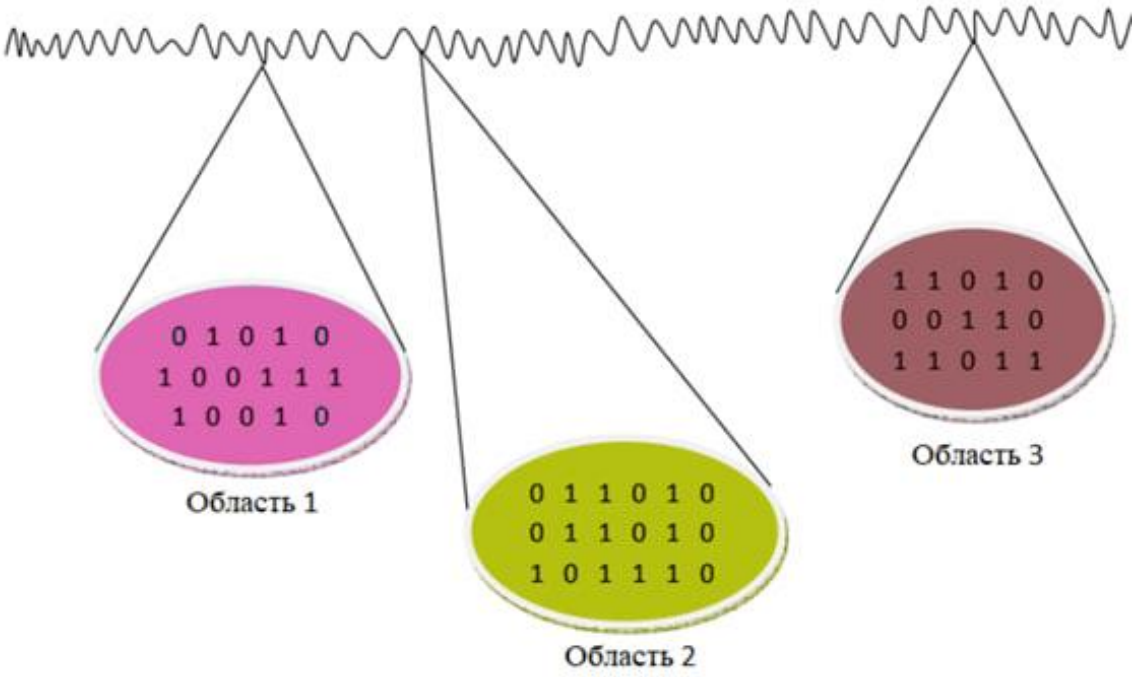

Рисунок 3.2 – Метод паритетного кодування

3.1.3 Фазове кодування

Колись це був інноваційний метод, оскільки він використовує фазові характеристики звукового сигналу для приховування інформації. Основні ідеї цього методу включають заміну фази початкового аудіосегменту еталонною фазою, яка представляє секретну інформацію, і корекцію решти фазових сегментів для збереження їхнього відносного фазового зв'язку. Такий підхід використовується для забезпечення безшумного кодування інформації. Представимо логіку метода графічно.

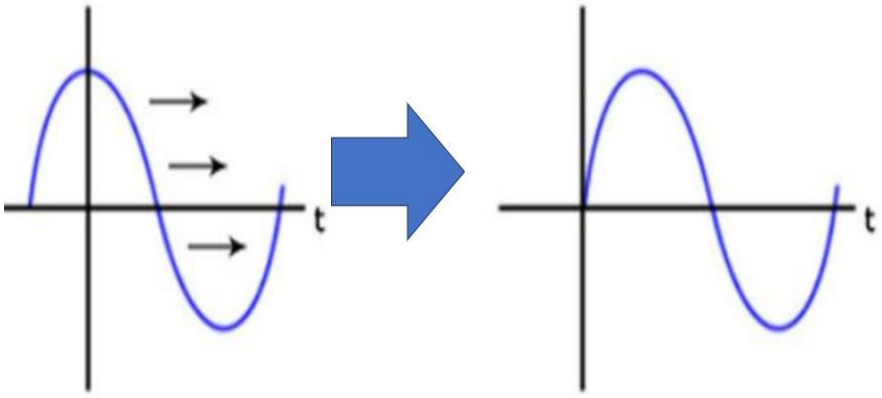

Рисунок 3.3 – Метод фазового кодування

3.1.4 Приховування відлуння

В сфері аудіостеганографії використання техніки відлуння відзначається вбудовуванням конфіденційної інформації у звуковий файл за допомогою внесення додаткових відлунь у дискретний сигнал. Цей підхід володіє вагомими перевагами, такими як висока швидкість передачі даних і надійність, роблячи його ефективним у порівнянні з іншими методами, з недоліків - можна закодувати лише один біт конфіденційної інформації, якщо маємо лише одне відлуння вихідного сигналу. Для успішного приховування даних важливо, щоб три параметри відлуння різнилися: амплітуда, швидкість розпаду та зміщення (час затримки) від вихідного сигналу. Всі ці параметри повинні залишатися нижче порогу слухової чутливості людини, щоб відлуння не виявлялося легко. Візуально цей процес можна представити у наступний спосіб.

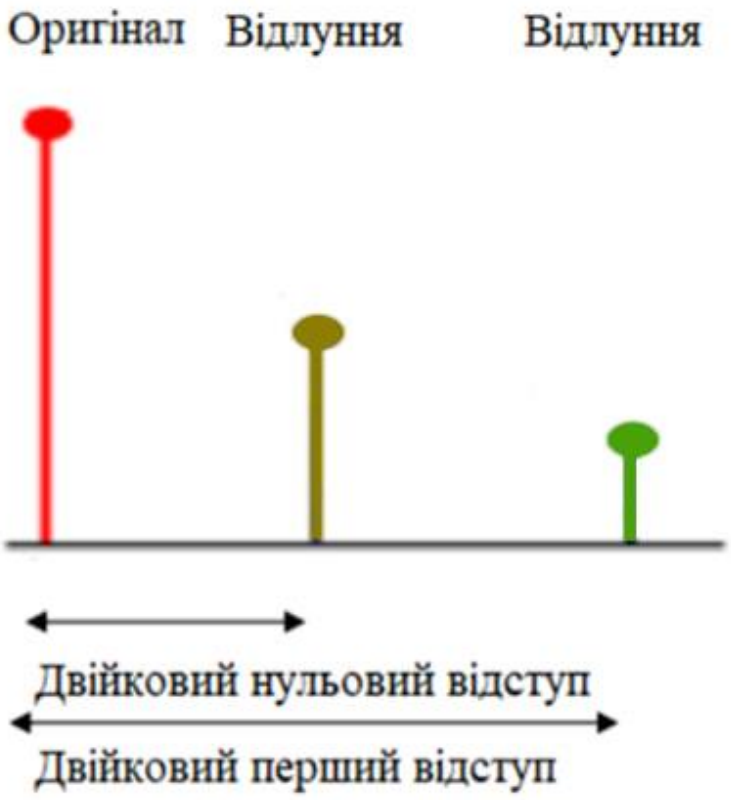

Рисунок 3.4 – Метод приховування відлуння

3.1.5 Порівняння методів приховування інформації

Зробимо програмну реалізацію кожного розглянутого методу стеганографії, та відобразимо результат тестування у діаграмі (Рисунок 3.5).

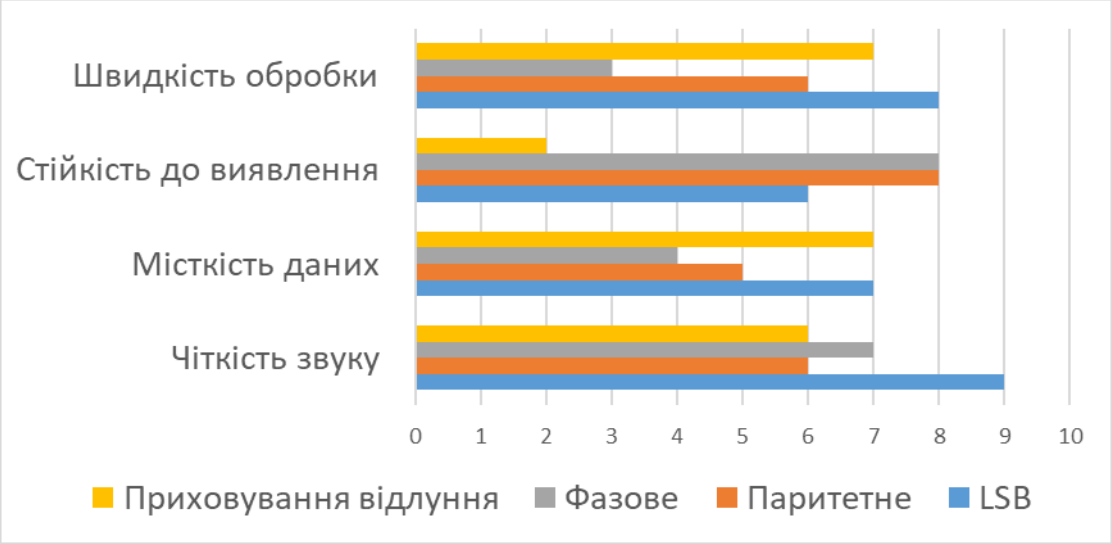

Рисунок 3.5 – Порівняння методів стеганографії за кількома критеріями

Представлені методи були порівняні за кількома критеріями.

Швидкість обробки: кожен метод вбудовував однакове текстове повідомлення у однаковий аудіофайл, за оцінку 10 був прийнятий результат у 1 секунду, так від результату була сформована шкала оцінення.

Стійкість до виявлення: можливість виявити данні за допомогою спеціалізованого програмного забезпечення, дослідник знаходив оригінальну аудіокомпозицію та порівнював її з зміненою на наявність вбудованого повідомлення, на зображенні виявлений вбудований біт зазначений червоним кольором (Рисунок 3.6).

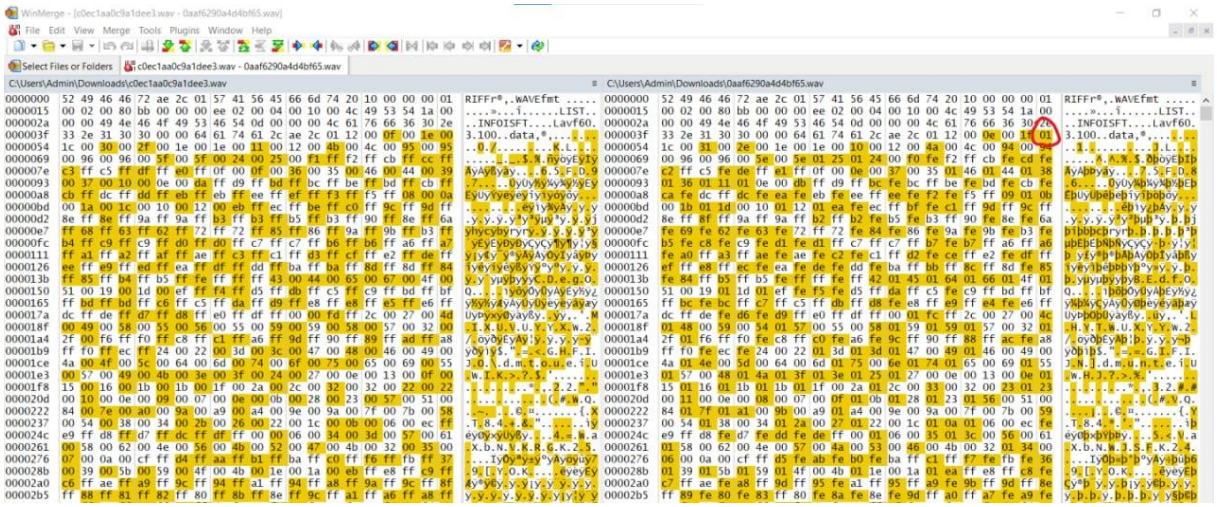

Рисунок 3.6 – Порівняння оригінального та зміненого аудіофайлу у хексовому редакторі

Місткість даних: за ідеальне значення максимально вбудованого текстового повідомлення було прийняте 0,1% від маси музичного файла, згідно цього методи стеганографії отримали оцінки.

Чіткість звуку: виявлення на слух змін у аудіофайлах, порівняння знайденого оригіналу та аудіофайлу з вбудованим повідомленням.

3.1.6 Обґрунтування вибору методу LSB

Для моделі гібридної стеганографії обрано метод LSB з кількох причин:

- простота реалізації, метод не потребує складних обчислень і легко інтегрується у програмне забезпечення;
- висока ефективність, LSB дозволяє приховувати великі обсяги даних без значного впливу на якість звуку;
- незмінність розміру файлу, на відміну від інших методів, таких як фазове кодування чи приховування відлунь, LSB не змінює сильно розмір аудіофайлу після приховування даних.

Проте метод має певні обмеження, зокрема вразливість до атак. Для мінімізації ризиків у дослідженні використано файли-контейнери з шумом, що ускладнює визначення змін у бітових структурах [24].

3.2 Аналіз криптографічних методів захисту

3.2.1 Основні принципи роботи алгоритму RSA

Криптосистема RSA (абревіатура від Rivest, Shamir та Adleman) є алгоритмом шифрування відкритого ключа, що базується на складній задачі факторизації довгих чисел.

Основні принципи роботи алгоритму RSA полягають в обранні двох простих чисел p і q, і обчисленні їх добутку $n = p \times q$ (де n є модулем). Після цього вибирається показник e, який задовольняє умову $1 < \mathrm{e} < (p-1) \times (q-1)$ та є взаємно простим з числом $(p-1) \times (q-1)$. Потім обчислюється d так, щоб $(e \times d - 1)$ ділилося на $(p-1) \times (q-1)$, створюючи пару ключів (n,e) - відкритий ключ та (n,d) - закритий ключ. Представимо принципи роботи алгоритму RSA схематично, на рисунку 3.7.

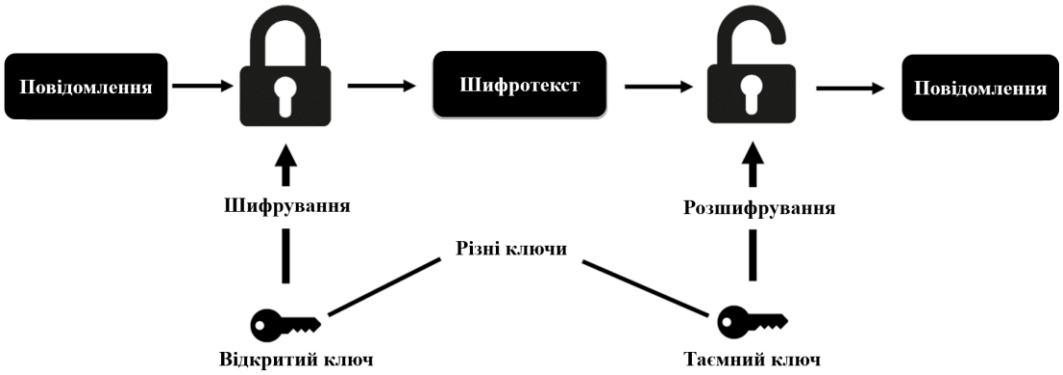

Рисунок 3.7 – Принцип роботи RSA

3.2.2 Алгоритм шифрування AES

Алгоритм шифрування AES використовує складний набір математичних концепцій для забезпечення безпеки обробки даних. Одним із ключових елементів є поле Галуа, яке є основою для виконання арифметичних операцій у шифруванні. Поле Галуа можна уявити як скінченну множину, в якій визначені операції додавання, віднімання,

множення та ділення, проте з певними відмінностями.

AES-256 широко використовується для захисту конфіденційної інформації в урядових, військових та комерційних організаціях в усьому світі. Він застосовується для шифрування даних на жорстких дисках, в мережевих протоколах, системах електронної пошти та інших додатках, де потрібен надійний захист інформації.

Процес шифрування AES-256 складається з наступних етапів: розбиття вхідних даних на блоки по 128 біт, додавання раундового ключа до початкового стану, виконання 14 раундів перетворень, що включають операції заміни байтів, зсуву рядків, а на прикінці відбувається змішування стовпців та додавання раундового ключа та фінального раундового ключа.

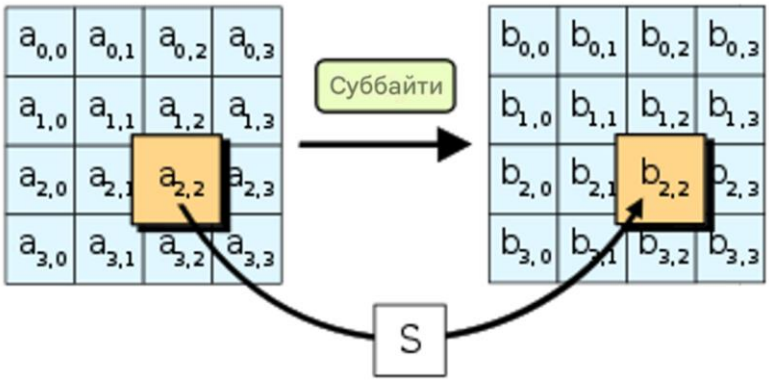

Рисунок 3.8 – Логіка роботи шифрування AES

Використання AES разом з RSA (Rivest-Shamir-Adleman) становить потужну комбінацію для забезпечення безпеки інформації у сучасних системах. RSA використовується для шифрування ключів, які потім використовуються AES для шифрування фактичних даних.

3.3 Модель гібридної стеганографічної системи

Розроблене програмне забезпечення реалізовано мовою програмування C#. Воно виконує такі етапи:

- завантаження аудіофайлу у форматі WAV;

- шифрування текстового повідомлення алгоритмом AES;
- шифрування ключа AES за допомогою RSA;
- приховування зашифрованого повідомлення та зашифрованого ключа AES за допомогою LSB.
- Збереження результату у новий аудіофайл.

Робота програми базується на наступних принципах:

- мінімізація змін у контейнері. Використання LSB дозволяє вносити мінімальні зміни до аудіосигналу, що зберігає якість звуку;
- шифрування повідомлення. Шифрування гарантує захист прихованих даних навіть у випадку виявлення їх у контейнері.

Розглянемо схеми прямого та обратного рішення, на рисунах 3.9 та 3.10

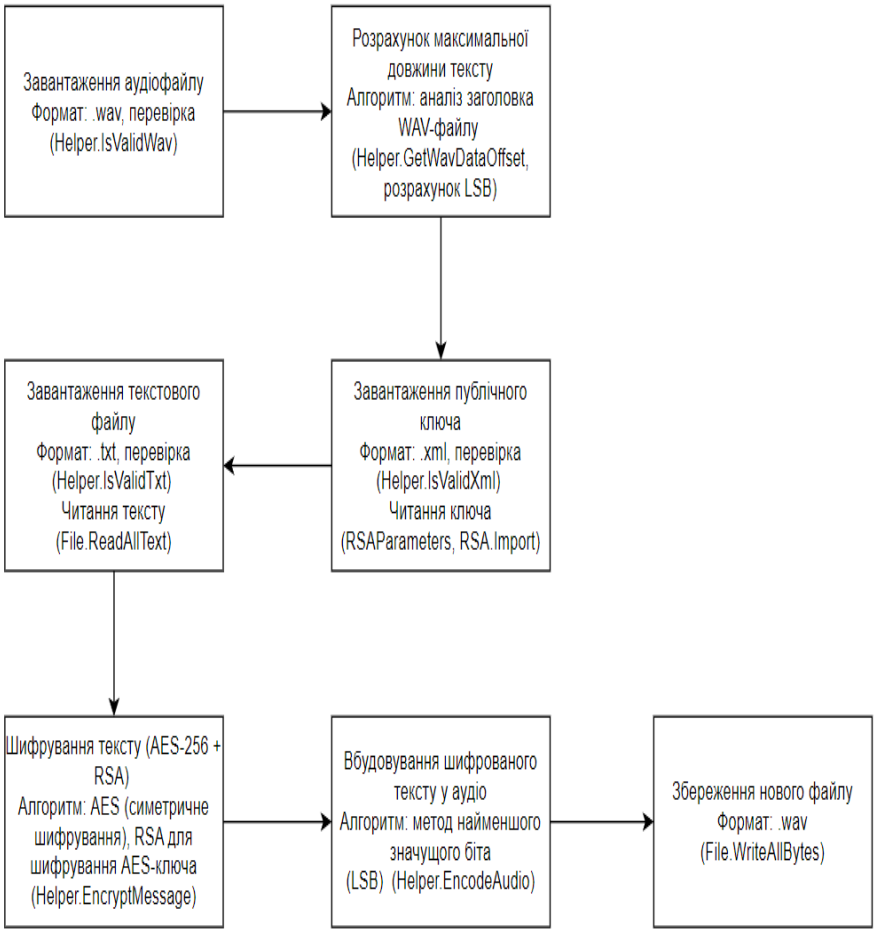

Рисунок 3.9 – Схема вбудовування повідомлення

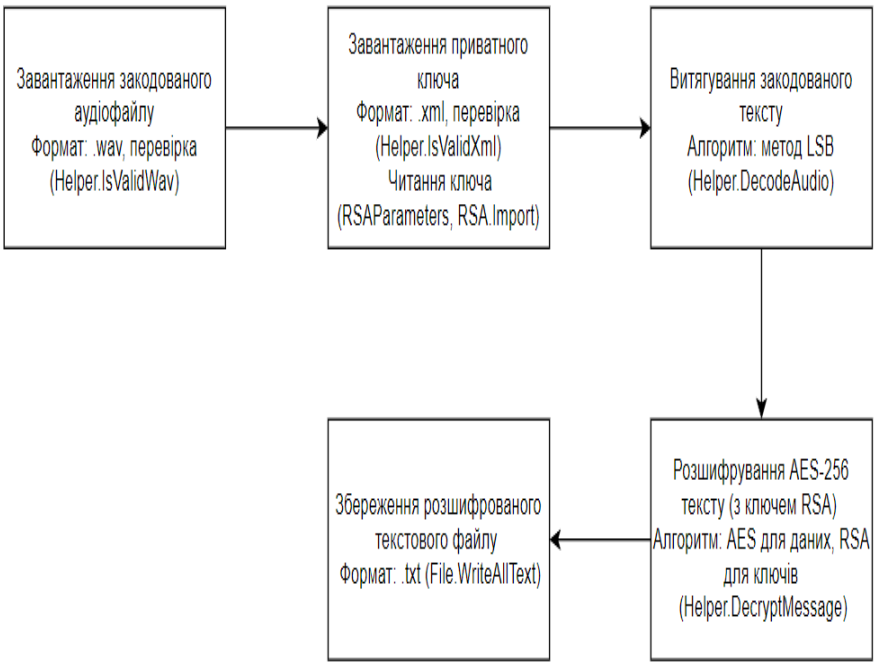

Рисунок 3.10 – Схема видобування повідомлення

Дослыдження підтверджує ефективність методу LSB для приховування великих обсягів даних в аудіофайлах. Поєднання стеганографії з криптографічними методами (AES, RSA) дозволяє підвищити стійкість до атак. У результаті проведеного дослідження було розроблено та проаналізовано модель гібридної стеганографії для приховування інформації у цифрових аудіофайлах. На основі порівняльного аналізу різних методів стеганографії підтверджено ефективність методу LSB для приховування великих обсягів даних в аудіофайлах, зокрема через його простоту реалізації та мінімальний вплив на якість звуку.

Поєднання стеганографії з криптографічними методами (AES, RSA) дозволяє суттєво підвищити стійкість до атак завдяки багаторівневому захисту даних. Застосування AES забезпечує надійне шифрування повідомлення, а RSA гарантує безпечну передачу ключів шифрування. Розроблене програмне забезпечення демонструє можливості гібридної стеганографії на практиці. Подальші дослідження передбачають вдосконалення стеганографічних методів для підвищення рівня захисту даних.

ВИСНОВКИ

Інтеграція стеганографії та криптографії в багаторівневу систему безпеки пропонує надійний метод для прихованого зв'язку, значно покращуючи захист даних від несанкціонованого доступу. Це дослідження представляє вдосконалену криптостегонографічну модель, яка використовує AES-шифрування, кодування послідовностей ДНК, QR-коди та LSB-стеганографію для безпечного вбудовування тексту в зображення. Завдяки використанню цього комплексного підходу посилюється безпека даних, забезпечуючи конфіденційність, цілісність та стійкість до виявлення. Експериментальні результати показують, що запропонована система ефективно захищає конфіденційні дані, зберігаючи при цьому невидимість та цілісність даних за допомогою складних стеганографічних методів. Аналіз ентропії та стандартного відхилення додатково розкриває вплив різних стеганографічних методів на інформаційний вміст та текстуру, причому LSB та адаптивні LSB-методи пропонують оптимальний баланс між безпекою та виявлюваністю. Крім того, алгоритм продемонстрував високу стійкість до диференціального криптоаналізу, досягнувши високих значень (99,5784%, 99,4292% та 99,5784%) та значень UACI (33,5873%, 33,5149% та 33,3745%), що підтверджує його стійкі властивості дифузії та плутанини.

Хоча ця модель безпеки значно покращує безпечну передачу даних, ми визнаємо, що криптографічні та стеганографічні методи можуть бути використані для незаконної діяльності, такої як приховування несанкціонованого зв'язку. Щоб зменшити ці ризики, впровадження передових методів судово-медичного аналізу, включаючи стеганоаналіз на основі машинного навчання та моніторинг мережевого трафіку, є важливим для виявлення аномалій. Крім того, слід запровадити суворі механізми контролю доступу та регуляторні рамки для сприяння дотриманню етичних та правових норм. З іншого боку, законне застосування нашої системи є

широким і охоплює безпечні бізнес-комунікації, конфіденційну передачу медичних даних, захист інтелектуальної власності та безпечний зв'язок у середовищах з високим рівнем ризику. Завдяки відповідальному впровадженню цих технологій організації та окремі особи можуть підвищити безпеку даних, дотримуючись етичних міркувань. Подальша робота буде зосереджена на вдосконаленні обчислювальної ефективності багаторівневих методів безпеки та розробці передових механізмів виявлення для балансування безпеки з судово-медичним аналізом. Постійно адаптуючи ці методи, розвиток ландшафту кібербезпеки може гарантувати, що криптографічні та стеганографічні досягнення служитимуть як безпеці, так і етичним імперативам у цифрову епоху.

Під час кваліфікаційної роботи ми пропонуємо вдосконалену стеганографічну мережу з низькою складністю обчислень для автоматичного захисту приватних або секретних даних зображень без використання традиційних алгоритмів вбудовування. Ми використовуємо структуру «знизу вгору» для побудови загальної архітектури, тим самим зменшуючи складність обчислень моделі. Ми пропонуємо конкатенацію з довгим пропуском для збереження більшої кількості необробленої інформації та стратегію NAFF для збереження більшої кількості низькорівневих ознак, що ефективно покращує продуктивність приховування. Крім того, ми додатково розробляємо вдосконалений модуль на основі уваги для вилучення важливих ознак з оригінальних зображень, реконструюючи та покращуючи важливу ціль, щоб приховати та замаскувати вбудований секретний вміст, що ефективно підвищує непомітність. Для втрат стеганографії ми розробляємо гібридну функцію втрат, щоб комплексно покращити якість прихованого зображення, тим самим значно покращуючи візуальну безпеку. Що ще важливіше, на відміну від інших проектів, які спираються на складні модулі, наші проекти прості та легкі в реалізації, що ефективно підвищує продуктивність стеганографії, майже без збільшення складності обчислень.

На практиці приховане зображення може постраждати від шуму та атак

стиснення JPEG, і як забезпечити цілісність відновлення прихованого зображення в таких екстремальних випадках є напрямком наших майбутніх досліджень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Aazam, M.; Zeadally, S.; Harras, K.A. Deploying Fog Computing in Industrial Internet of Things and Industry 4.0. IEEE Trans. Ind. Inf. 2018, 14, 4674–4682.

2. Howe, J.; Khalid, A.; Rafferty, C.; Regazzoni, F.; O'Neill, M. On Practical Discrete Gaussian Samplers for Lattice-Based Cryptography. IEEE Trans. Comput. 2018, 67, 322–334.

3. Yan, B.; Xiang, Y.; Hua, G. Improving the Visual Quality of Size-Invariant Visual Cryptography for Grayscale Images: An Analysis-by-Synthesis (AbS) Approach. IEEE Trans. Image Process 2019, 28, 896–911.

4. Wang, J.; Cheng, L.M.; Su, T. Multivariate Cryptography Based on Clipped Hopfield Neural Network. IEEE Trans. Neural Netw. Learn. Syst. 2018, 29, 353–363.

5. Li, W.; Zhou, W.; Zhang, W.; Qin, C.; Hu, H.; Yu, N. Shortening the Cover for Fast JPEG Steganography. IEEE Trans. Circuits Syst. Video Technol. 2020, 30, 1745–1757.

6. Wang, Y.; Zhang, W.; Li, W.; Yu, X.; Yu, N. Non-Additive Cost Functions for Color Image Steganography Based on Inter-Channel Correlations and Differences. IEEE Trans. Inf. Forensics Secur. 2020, 15, 2081–2095.

7. Pevný, T.; Filler, T.; Bas, P. Using High-Dimensional Image Models to Perform Highly Undetectable Steganography. In Proceedings of the International Workshop on Information Hiding, Calgary, AB, Canada, 28–30 June 2010; Springer: Berlin/Heidelberg, Germany, 2010; pp. 161–177.

8. Holub, V.; Fridrich, J. Designing steganographic distortion using directional filters. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Tenerife, Spain, 2–5 December 2012; pp. 234–239.

9. Holub, V.; Fridrich, J.; Denemark, T. Universal distortion function for

steganography in an arbitrary domain. EURASIP J. Inf. Secur. 2014, 1, 1–13.

10. Su, W.; Ni, J.; Li, X.; Shi, Y.Q. A New Distortion Function Design for JPEG Steganography Using the Generalized Uniform Embedding Strategy. IEEE Trans. Circuits Syst. Video Technol. 2018, 28, 3545–3549.

11. Zhao, W.; Du, S. Spectral–Spatial Feature Extraction for Hyperspectral Image Classification: A Dimension Reduction and Deep Learning Approach. IEEE Trans. Geosci. Remote Sens. 2016, 54, 4544–4554.

12. Tang, W.; Tan, S.; Li, B.; Huang, J. Automatic Steganographic Distortion Learning Using a Generative Adversarial Network. IEEE Signal Process. Lett. 2017, 24, 1547–1551.

13. Shi, H.; Dong, J.; Wang, W.; Qian, Y.; Zhang, X. SSGAN: Secure steganography based on generative adversarial networks. In Proceedings of the Pacific Rim Conference on Multimedia, Harbin, China, 28–29 September 2017; Springer: Cham, Switzerland, 2017; pp. 534–544.

14. Arjovsky, M.; Chintala, S.; Bottou, L. Wasserstein GAN. Available online: http://arxiv.org/abs/1701.07875.

15. Zhu, J.; Kaplan, R.; Johnson, J.; Fei-Fei, L. HiDDeN: Hiding data with deep networks. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 8–14 September 2018; pp. 657–672. [Google Scholar]

16. Zhang, K.A.; Cuesta, A.; Infante, L.X.; Veeramachaneni, K. SteganoGAN: High Capacity Image Steganography with GANs. Available online: http://arxiv.org/abs/1901.03892 (accessed on 30 January 2019).

17. Rahim, R.; Nadeem, S. End-to-end trained CNN encode-decoder networks for image steganography. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 8–14 September 2018; pp. 723–729.

18. Duan, X.; Jia, K.; Li, B.; Guo, D.; Zhang, E.; Qin, C. Reversible Image Steganography Scheme Based on a U-Net Structure. IEEE Access 2019, 7, 9314–9323.

19. Baluja, S. Hiding Images within Images. IEEE Trans. Pattern Anal. Mach. Intell. 2020, 42, 1685–1697.

20. Chen, F.; Xing, Q.; Liu, F. Technology of Hiding and Protecting the Secret Image Based on Two-Channel Deep Hiding Network. IEEE Access 2020, 8, 21966–21979.

21. Zhu, Y.; Zhao, C.; Guo, H.; Wang, J.; Zhao, X.; Lu, H. Attention CoupleNet: Fully Convolutional Attention Coupling Network for Object Detection. IEEE Trans. Image Process 2019, 288, 113–126.

22. Ji, J.; Xu, C.; Zhang, X.; Wang, B.; Song, X. Spatio-Temporal Memory Attention for Image Captioning. IEEE Trans. Image Process 2020, 29, 7615–7628.

23. Yu, C.; Hu, D.; Zheng, S.; Jiang, W.; Li, M.; Zhao, Z.Q. An improved steganography without embedding based on attention GAN. Peer--Peer Netw. Appl. 2021, 14, 1446–1457.

24. Tan, J.; Liao, X.; Liu, J.; Cao, Y.; Jiang, H. Channel Attention Image Steganography with Generative Adversarial Networks. IEEE Trans. Netw. Sci. Eng. 2022, 9, 888–903.

25. He, K.; Zhang, X.; Ren, S.; Sun, J. Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Las Vegas, NV, USA, 26 June–1 July 2016; pp. 770–778.