ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ
ТА ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА ТЕХНІЧНИХ СИСТЕМ КІБЕРЗАХИСТУ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Підвищення ефективності захисту інформації що передається стеганографічними методами через мережеві канали об’єкту інформаційної діяльності»

на здобуття освітнього ступеня магістра
зі спеціальності __125 Кібербезпека та захист інформації»
(код, найменування спеціальності)
освітньо-професійної програми Технічні системи інформаційного та кібернетичного захисту

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Максим ОНИЩЕНКО

Виконав: здобувач вищої освіти групи СЗДМ 61
Максим ОНИЩЕНКО

Керівник: ТУРОВСЬКИЙ Олександр
д.т.н., професор (ПРІЗВИЩЕ, Ім’я)

Рецензент: _____
(ПРІЗВИЩЕ, Ім’я)

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кафедра ___Технічних систем кіберзахисту_____
Ступінь вищої освіти ____магістр_____
Спеціальність ___Кібербезпека та захист інформації_____
Освітньо-професійна програма _Технічні системи інформаційного та кібернетичного захисту__

ЗАТВЕРДЖУЮ
Завідувач кафедри ТСКБ
_____Олександр Туровський

«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Онищенку Максиму Вадимовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи:
«Підвищення ефективності захисту інформації що передається стеганографічними методами через мережеві канали об'єкту інформаційної діяльності»
керівник кваліфікаційної роботи __Олександр ТУРОВСЬКИЙ д.т.н., професор
(ПРІЗВИЩЕ Ім'я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» жовтня 2025 р. № 467

2. Строк подання кваліфікаційної роботи 15.12.2025 р.

3. Вихідні дані до кваліфікаційної роботи: графічні зображення, стеганографічні методи приховування інформації, структурна модель системи прихованої передачі інформації у зображенні, критерії оцінки системи передачі інформації у зображенні.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1.__ Огляд технології стеганографічного захисту даних в системі захисту інформації об'єкту інформаційної діяльності
2.__Дослідження можливостей застосування методів стеганографії та стеганоаналізу при забезпеченні захисту конфіденційних даних на об'єкті інформаційної діяльності.
3.__Розробка рекомендацій по комбінованому захисту конфіденційних даних з використанням методів стеганографії та криптографії
5. Перелік графічного матеріалу: ___Презентаційний матеріал на слайдах.

6. Дата видачі завдання 15.10.2025

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури		
2	Написання першого розділу роботи		
3	Написання другого розділу роботи		
4	Написання третього розділу роботи		
5	Написання висновків по роботі		
6	Підготовка демонстраційних матеріалів		
7	Підготовка доповіді		

Здобувач вищої освіти _____ Максим ОНИЩЕНКО

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник роботи _____ Олександр ТУРОВСЬКИЙ

(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина магістерської кваліфікаційної роботи: стор., рис., табл., джерел.

Об'єкт дослідження – Стеганографічні методи захисту інформації.

Предмет дослідження – Методи стеганографічного захисту конфіденційних даних при їх передачі.

Мета роботи – Удосконалення системи передачі конфіденційних даних стеганографічними методами.

Методи дослідження – системний аналіз, опрацювання літератури за даною темою.

У роботі проаналізовано методи стеганографічного захисту. Розглянуто можливість використання стеганографії для захисту конфіденційних даних.

Ґрунтуючись на проведеному досліджені було удосконалено стеганографічний метод захисту інформації та підвищено його надійність від витоку конфіденційних даних.

Галузь використання – захист конфіденційних даних на об'єкті інформаційної діяльності.

Апробація:

М.В. Онищенко, Д.П. Жуковський. Принципи побудови та основи функціонування системи кіберзахисту передачі конфіденційних даних мережевими каналами на основі стеганографічних технологій. *Всеукраїнської науково- практичної конференція: Актуальні проблеми безпеки інформаційно-телекомунікаційних систем*. м. Київ, 05 листопада 2025 року, Київ: РВЦ ДУІКТ. – 2025. С.41-42. https://duikt.edu.ua/uploads/p_2779_72486260.pdf

СТЕГАНОГРАФІЧНИЙ КАНАЛ, ЗАГРОЗИ ІНФОРМАЦІЇ, СТЕГОАНАЛІЗ, ЗАХИСТ КОНФІДЕНЦІЙНИХ ЗАХИСТ, ШИФРУВАННЯ, ІДЕНТИФІКАЦІЯ.

ABSTRACT

The text part of the master's qualification work: pages, figures, tables, sources.

The object of research is steganographic methods of information protection.

The subject of the research is methods of steganographic protection of confidential data during their transmission.

The purpose of the work is to improve systems for transmitting confidential data using steganographic methods.

Research methods – system analysis, numerical methods, literature review on this topic.

The work analyzes the methods of steganographic protection. The possibility of using steganography to protect confidential data is considered.

Based on the conducted research, the steganographic method of information protection was improved and its reliability against leakage of confidential data was increased.

Field of use – protection of confidential data at the object of information activity.

STEGANOGRAPHIC CHANNEL, INFORMATION THREATS, STEGOANALYSIS, PRIVACY PROTECTION, ENCRYPTION, IDENTIFICATION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ПЗ – програмне забезпечення.

SPIE (the international society for optics and photonics) – спільнота оптики та фотоніки

IEEE(ICIP) (international conference on image processing) - міжнародна конференція з обробки зображень.

LSB (Least Significant Bit) – найменш значущий біт.

SVG (Scalable Vector Graphics) – масштабована векторна графіка.

NIDS (network intrusion detection system) – система виявлення вторгнення.

NFT (non-fungible token) - незамінний токен.

RGB (Red, Green, Blue) – модель кольорів.

CMY (Cyan, Magenta, Yellow) – модель кольорів.

TIFF (Tagged Image File Format) – формат зображення.

JPEG (Joint Photographic Experts Group) - формат зображення.

MPEG (Moving Picture Experts Group) – формат рухомого зображення.

DKL (Kullback–Leibler divergence) - дивергенція Кульбака-Лейблера.

ROC (receiver operating characteristic) - отримувач операційної характеристики.

HTML (HyperText Markup Language) – мова гіпертекстової розмітки.

CSS (Cascading Style Sheets) – каскадні таблиці стилів.

SQL (Structured Query Language) – мова структурованих запросів.

AES (Advanced Encryption Standard) – симетричний алгоритм блочного шифрування.

ВСТУП

Важливість дослідження. Сьогодні інформація є одним із найважливіших ресурсів, а захист конфіденційних даних зараз є значним завданням для багатьох різних видів діяльності: від уряду до приватних компаній. Традиційні методи шифрування мають високий ступінь безпеки, але вони часто стають мішенню для хакерів через наявність зашифрованих даних. У цьому контексті стеганографія набуває значення в системах захисту інформації.

Стеганографія, як галузь науки та практичний метод, пропонує різноманітні підходи до приховування інформації в цифрових носіях, включаючи зображення, аудіо- та відеофайли, а також методи забезпечення їх передачі без наявності очевидних ознак втручання в структуру файлу. Однак швидкий розвиток технологій та збільшення обсягу цифрового трафіку призвели до нових проблем. Зокрема, існує необхідність підвищити стійкість стеганографічних методів до виявлення за допомогою стегоаналізу, а також удосконалити алгоритми приховування інформації для роботи з різними типами даних.

Важливість дослідження пояснюється необхідністю ефективних та надійних систем захисту конфіденційної інформації в контексті сучасного інформаційного простору. Існує зростаюча потреба в таких системах через зростання поширеності кіберзлочинності, промислового шпигунства та несанкціонованого доступу. Поєднання стеганографії з іншими методами захисту даних надає нові можливості для забезпечення інформаційної безпеки, зокрема в критично важливих сферах, таких як банківська система, оборона та медицина.

Метою цієї магістерської роботи є вдосконалення системи захисту конфіденційної інформації під час поширення інформації за допомогою стеганографічних методів шляхом розробки та вивчення нових підходів до приховування даних та підвищення їхньої стійкості до виявлення. У дослідженні будуть розглянуті сучасні методи стеганографії, оцінена їхня ефективність та

недоліки, а також запропоновано вдосконалення для підвищення ефективності захисту..

Об'єкт дослідження – Стеганографічні методи захисту інформації.

Предмет дослідження – Методи стеганографічного захисту конфіденційних даних при їх передачі.

Мета роботи – Удосконалити системи передачі конфіденційних даних стеганографічними методами.

Методи дослідження – системний аналіз, опрацювання літератури за даною темою.

Наукові завдання:

дослідити методи стеганографічного захисту на об'єкт інформаційної діяльності;

проаналізувати ймовірні загрози на об'єкти інформаційної діяльності;

удосконалити систему захисту конфіденційних даних з використанням стеганографії.

Практичне значення одержаних результатів полягає у удосконалені системи захисту конфіденційних даних с використанням комбінованого стеганографічно-криптографічного захисту.

РОЗДІЛ1.
ТЕОРЕТИЧНІ ОСНОВИ СТЕГАНОГРАФІЇ ТА ЇЇ РОЛЬ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ

1.1 Загальні поняття про стеганографію

Стеганографія – це метод таємного зв'язку. Він функціонує шляхом приховування повідомлень у нешкідливих об'єктах, призначених для цільових одержувачів. Найважливішим компонентом будь-якої стеганографічної системи є те, що стороння особа не повинна мати змоги розрізняти звичайні об'єкти від об'єктів, що містять секретну інформацію. Сучасна стеганографія все ще перебуває на початковій стадії. До початку 90-х років цей незвичайний метод непрямого зв'язку використовувався переважно шпигунами. У той час це неможливо було б назвати галуззю досліджень, оскільки методи були по суті простими ремеслами без теоретичної основи, яка дозволила б зрозуміти стеганографію такою, якою вона є сьогодні. Подальший спонтанний перехід комунікацій від аналогового до цифрового призвів до появи давньої галузі, яка зазнала вибухового зростання [1,2,3]. Приховування повідомлень в електронних документах для ведення таємного зв'язку здавалося простим для тих, хто мав мінімальні знання програмування. Стеганографічні технології швидко популяризувалися в Інтернеті, дозволяючи громадськості приховувати файли в цифрових зображеннях, аудіо чи тексті. Крім того, стеганографія викликала інтерес у вчених і швидко стала визнаною галуззю досліджень. Це вивело на перший план обговорення на професійних зустрічах, таких як щорічна конвенція SPIE з електронної обробки зображень у Сан-Хосе, Міжнародна конвенція IEEE з обробки зображень (ICIP) та конференція ACM з мультимедіа та безпеки [1,2,3]. У 1996 році в Кембриджі відбувся перший семінар з приховування інформації, і з того часу ця серія заходів стала найпопулярнішим щорічним зібранням новітніх теорій та методів приховування інформації.

Стеганографія має багато спільного з цифровим водяним знаком, але принципово відрізняється. Наприкінці 1990-х років цифровий водяний знак став найпопулярнішою формою приховування даних завдяки своїм численним корисним застосуванням, включаючи управління цифровими правами, безпечне розповсюдження медіа та автентифікацію. Зі зростанням розвитку водяних знаків інтерес до стеганографії та суміжних тем, таких як стеганааналіз, поступово зростав. Це було особливо актуально після побоювань, що злочинці скористаються стеганографією [1,2,3].

Тип носія	Кількість
Аудіо	445
Диск	416
Фото	1689
Мережа	39
Інше	81
Текст	255
Відео	86

Рис. 1.1 - Кількість стеганографічних програм, які можуть приховувати дані в електронних носіях станом на червень 2008 р.

1.2 Стегонаграфія через історію

Слово «стеганографія» походить від грецьких слів «steganos», що означає «прихований», та «graphia», що означає «письмо». Іншими словами, стеганографія — це наука про приховану комунікацію, існування якої невідоме. Термін «стеганографія» вперше вжив Йоганнес Трітеміус (1462-1516) у трилогії «Поліграфія» та «Стеганографія». Перші два томи описували стародавні методи приховування повідомлень (криптографію), тоді як третій том (1499), здавалося, зосереджувався на чаклунстві, чорній магії та методах спілкування зі світом духів. Том був опублікований у Франкфурті в 1606 році, а в 1609 році католицька церква

додала його до списку «libri prohibiti» (заборонених книг) [1,2,3]. Пізніше вчені почали вірити, що книга має код, і вони спробували розшифрувати її таємниці. Спроби розшифрувати таємне послання книги увінчалися успіхом у 1996 та 1998 роках, коли два різні дослідники незалежно один від одного вивели приховані повідомлення, закодовані в числах за допомогою кількох таблиць відповідностей у книзі. Повідомлення, очевидно, були досить поширеними. Першим було латинський аналог речення: «Швидка бура лисиця перемагає лінивого собаку», яке володіє всіма літерами алфавіту. Друге повідомлення звучало так: «Людина, яка надсилає цього листа, — шахрай і злодій». Стережіться його. «Він бажає щось для тебе зробити». Нарешті, третій був початком 21-го Псалма. Перший задокументований випадок стеганографії був використаний Геродотом для передачі повідомлення своєму господареві, розповідаючи про слугу, якого відправили до іонійського міста Мілет із прихованим повідомленням, написаним на його голові. Після татуювання чоловік збільшив довжину свого волосся, щоб приховати повідомлення. Він вирушив до Мілету, і, прибувши туди, поголив голову, щоб продемонструвати послання намісникy міста Арістагору [1,2,3]. Послання наказувало Арістагору розпочати повстання проти перського імператора. Також Геродот записав розповідь про Демарата, який використав стеганографію, щоб попередити Спарту про майбутнє вторгнення перського імператора Ксеркса до Греції. Щоб приховати своє послання, Демарат взяв віск з поверхні дерев'яної таблички, вирізав своє послання на дереві, а потім покрив табличку шаром воску, що зробило її схожою на типову чисту табличку, яку можна було безпечно передати до Спарти, не викликаючи підозр. Енею Тактику приписують створення численних винахідливих стеганографічні методи, включаючи приховування повідомлень у дизайні жіночих сережок або використання голубів для передачі секретної інформації. Він також описав кілька простих методів приховування повідомлень у тексті, спосіб, яким змінюються літери або використовуються маленькі отвори для позначення тексту. У 1966 році креативна та випадкова стеганографічна стратегія допомогла військовополоненому Джеремі Дентону передати одне слово своїм викрадачам у

В'єтнамі, коли вони змушували його брати участь у телевізійній дискусії. Зрозумівши, що він не може коментувати своїх викрадачів, він кліпнув очима азбукою Морзе під час розмови, вимовивши слово T-O-R-T-U-R-E (катування) [1,2,3]. Стеганографія стала предметом суперечки під час матчу між Віктором Корчним та Анатолієм Карповим, який завершився чемпіонатом світу з шахів у 1978 році. Під час одного матчу помічники Карпова дали йому піднос з йогуртом. Технічно це було порушенням правил, які забороняли фізичний контакт між гравцем та його командою під час гри. Голова делегації Петра Левверик одразу висловив свою стурбованість, стверджуючи, що команда Карпова надсилала... йому конфіденційну інформацію [1,2,3]. Наприклад, фіолетовий йогурт означатиме, що Карпов має запропонувати нічию, тоді як порція манго вказуватиме гравцеві відхилити пропозицію нічиєї. Частота появи їжі також могла бути використана для приховування додаткової інформації (часова стеганографія). Ця демонстрація, яка була викликана параноєю, поширеною в шахових іграх під час Холодної війни, розглядалася серйозно. Карпову дозволялося споживати лише один вид йогурту одночасно під час змагання (фіолетовий). Використовуючи термінологію книги, ми можемо вивести це вимірювання як активний нагляд керівника, який запобігає використанню стеганографії [1,2,3].

Нещодавнє зростання інтересу до стеганографії пояснюється швидким розвитком цифрових медіа, а також зростаючою поширеністю Інтернету (Рисунок 1.1 демонструє щорічну кількість дослідницьких робіт зі стеганографії, опублікованих IEEE) [4,5]. Сьогодні зображення, відео та звуки є звичайним явищем для обміну з родиною та друзями. Ці об'єкти сприяють приховуванню секретних повідомлень одним важливим способом: типові цифрові медіафайли складаються з багатьох окремих компонентів (таких як пікселі), які можна тонко змінити для кодування секретне повідомлення. Крім того, тим, хто хоче використовувати стеганографію, не потрібні технічні знання, Сам процес приховування є комп'ютеризованим і доступним онлайн безкоштовно. До кінця 2008 року, коли відбувалося написання цієї статті, в Інтернеті було доступно

кілька сотень різних стеганографічних продуктів [1,2,3]. На рисунку 1.2 показано кількість нових програм або переглянутої версії існуючого програмного забезпечення, які приховують дані в цифрових медіа або тексті. Деякі програмні додатки, що зосереджені на безпеці, конфіденційності та анонімності, мають можливість приховувати зашифровані повідомлення в зображеннях і музиці як засіб додаткового захисту [4,5].

1.3 Сучасна стеганографія

Оскільки електронні комунікації дуже вразливі до прослуховування та зловмисного вторгнення, безпека та конфіденційність людей зараз важливіші, ніж будь-коли раніше. Традиційні підходи базуються на криптографії, яка є зрілою галуззю, що має сувору математичну основу [4,5,6].

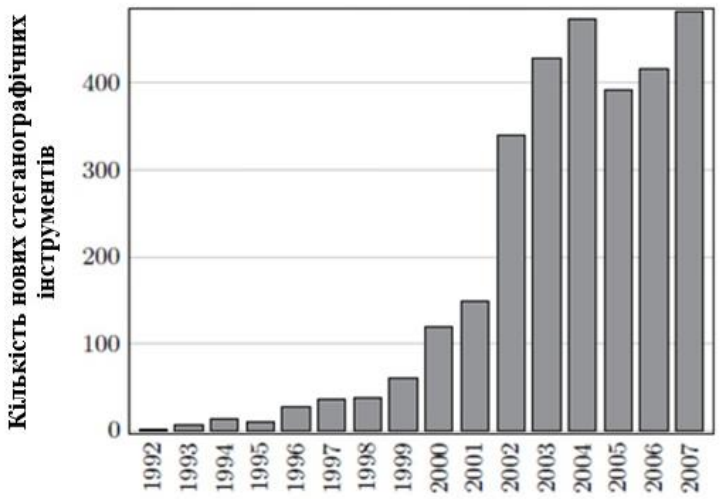


Рис 1.2 - Кількість нещодавно випущених програм стеганографічного програмного забезпечення або нових версій на рік.

Криптографічний метод конфіденційності полягає у тому, щоб зробити передачу інформації незрозумілою для тих, хто не має правильного ключа розшифрування. Коли зашифроване повідомлення підслуховується, навіть якщо його вміст захищено, той факт, що сторони спілкуються таємно, все одно

очевидний. У деяких випадках корисно уникати привертання уваги та натомість зберігати конфіденційні дані в інших об'єктах, щоб наявність секретної інформації не була очевидною. Саме цей метод використовується стеганографією [4,5,6].

Стеганографія є ефективною альтернативою шифруванню в тиранічних країнах, які забороняють використання криптографії, або в країнах, які хочуть уникнути уваги. Задокументований випадок стеганографії був представлений на 4-й Міжнародній конференції з приховування інформації. Два учасники розробили власну стеганографічну стратегію приховування повідомлень у цифрових зображеннях, які не були стиснуті, і вони успішно використовували цю стратегію понад десять років у країні, яка вороже ставилася до шифрування, цій країні було спеціально заборонено використовувати цю технологію [4,5,6]. Причиною їхніх марень стала розповідь друга, який уже жив у цьому районі. Ця людина намагалася надіслати електронного листа з прихованим паролем, але місцевий інтернет-провайдер повернув їй повідомлення: «Будь ласка, не надсилайте електронні листи з прихованими паролями – ми не можемо їх прочитати». На початку 80-х Сіммонс описав цікаві політичні наслідки можливості надсилати інформацію через прихований канал зв'язку. Згідно з Договором про ліквідацію ракет середньої та середньої дальності (РСМД), Радянський Союз і США погодилися поділитися своєю ядерною зброєю з іншими країнами, але не розголошувати місцезнаходження цієї зброї. Весь зв'язок мав бути гарантований стандартними цифровими підписами, які запобігали б зміні показань датчиків. Однак обидві сторони визнавали можливість приховування додаткової інформації через так звані підпорядковані канали, які були присутні в більшості схем цифрового підпису на той час. Це спонукало до досліджень щодо створення цифрових підписів, які не залежать від прихованих каналів [4,5,6].

1.4 Принцип роботи стеганографії

Концепція стеганографії базується на приховуванні інформації до моменту її розкриття. Одним з популярних методів є метод стеганографії з використанням

найменш значущого біта (LSB). Цей підхід використовується для поширення конфіденційної інформації в найменш значущих розрядах цифрового запису. Наприклад [6,7,8]:

Кожен піксель зображення складається з трьох байтів даних, що відповідають кольорам червоного, зеленого та синього. Однак деякі формати мають четвертий байт, призначений для прозорості, він називається "альфа". Стеганографія LSB - це зміна найменш значущого байта, яка приховує трохи особистої інформації, що є конфіденційною. Як результат, для приховування одного мегабайта інформації необхідно вісім мегабайт візуального контенту. Зміна останнього біта пікселя не призводить до видимої зміни зображення, тому при порівнянні оригінального та стеганографічно зміненого зображення різниця буде майже непомітною [6,7,8] Цей метод застосовується майже до всіх типів цифрових носіїв, включаючи аудіо- та відеофайли, дані розташовані в частинах, які найменше впливають на звук або зовнішній вигляд [6,7,8].

1.5 Типи стеганографії

Наразі існує п'ять основних типів стеганографії .

1.5.1 Дослівна стеганографія

Текстова стеганографія – це практика приховування конфіденційної інформації або особистих повідомлень у звичайному режимі. Цей підхід використовується в каналах комунікації, таких як електронні листи, дописи на форумах або дописи в соціальних мережах. Існує кілька методів для приховування прихованих повідомлень.

Можна використовувати прості методи, такі як зміна форматування тексту, наприклад, використання певних розділових знаків або пробілів. Більш складні методи, такі як використання стеганографічних методів для приховування інформації в тексті, також можуть бути використані для підвищення безпеки [8,9,10].

1.5.2 Криптоаналіз зображень

Стеганографія зображень – це метод приховування особистої інформації в цифрових зображеннях. Цей метод передбачає зміну представлення даних, які вже є на зображенні, без фактичної зміни візуального вигляду зображення для людського ока.

Один поширений метод – зміна найменш значущих цифр (LSD) значень пікселів, що дозволяє кодувати двійкові дані в зображеннях без значних спотворень. Інші методи, такі як приховування простору, також можуть бути використані для об'єднання зображень шляхом стратегічної зміни певних областей або кольорових компонентів одного зображення [8,9,10].

1.5.3 Відеостеганографія

Відеостеганографія – це практика приховування відеоконтенту в інших мультимедійних матеріалах. Цей підхід використовує переваги часового зв'язку між наступними відеокадрами, що дозволяє плавно інтегрувати приховану інформацію у відеопотік.

Один із використовуваних методів – перетворення окремих кадрів прихованого відео у відповідні додаткові відеокадри. Інші підходи включають використання векторів, що рухаються в одному напрямку, та зміну певних компонентів відеоданих [8,9,10].

1.5.4 Аудіостеганографія

Аудіостеганографія – це процес приховування секретної інформації в аудіозаписах, зберігаючи при цьому якість, прийнятну для слухачів. Цей підхід зосереджений на обмеженій чутливості слухової системи до невеликих змін звукових хвиль, що дозволяє вносити невеликі зміни до аудіозразків.

Деякі поширені методи аудіостеганографії включають зміну найменш значущих бітів (LSB) аудіосемплів для приховування даних або повідомлень, специфічних для певних діапазонів частот, з метою мінімізації чутних артефактів [8,9,10].

1.5.5 Стеганографія мережі

Мережева стеганографія – це процес приховування інформації в комунікаціях між учасниками мережі, щоб уникнути виявлення механізмами безпеки. Цей метод в основному використовується хакерами, оскільки він використовує переваги властивої надмірності та різноманітності протоколів у мережі, що дозволяє приховану передачу даних у заголовках пакетів, корисних навантаженнях або шаблонах передачі.

Методи, що використовуються в стеганографії мереж, включають розміщення даних у порожніх полях інформації, специфічної для протоколу, та зміну властивостей синхронізації мережевих пакетів [8,9,10].

1.6 Використання стеганографії

Сьогодні стеганографія використовується переважно в комп'ютерах, цифрових медіа та мережах швидкої доставки. Використовуючи стеганографію, передбачається:

Уникнення цензури: її можна використовувати для поширення нової інформації, уникаючи цензури та без страху відстеження повідомлення до відправника.

Цифрові водяні знаки: також використовуються для створення непомітних водяних знаків, які не впливають негативно на зображення та які все ще можна відстежити, щоб перевірити, чи було воно використано без дозволу.

Захист інформації: це використовується правоохоронними та урядовими установами для передачі дуже складної інформації іншим особам без необхідності ділитися нею далі [8,9,10].

1.7 Роль стеганографії в кібербезпеці

1.7.1 З точки зору кібербезпеки:

Захист даних та конфіденційність

ІТ-експерти та фахівці з безпеки використовують стеганографію як засіб захисту конфіденційної інформації та підвищення конфіденційності. Вони можуть використовувати стеганографічні методи для приховування секретної інформації, такої як ключі шифрування або докази автентичності, в цифрових активах. Приховуючи критичну інформацію в непомітних файлах або розмовах, організації можуть захистити себе від несанкціонованого доступу та недоліків даних [8,9,10].

Також стеганографія використовується експертами з кібербезпеки для захисту цифрових прав та створення водяних знаків. Вставляючи унікальні коди або інформацію щодо права власності в мультимедійний контент, такий як зображення чи відео, організації можуть запобігти несанкціонованому відтворенню або розповсюдженню прав власності. Інформація, прихована у файлах, може бути використана як доказ у випадках порушення авторських прав.

Протидія розвідці та криміналістика

Стеганографія використовується в контррозвідці та цифрових доказах для виявлення та аналізу прихованих даних у цифрових ресурсах. ІТ-експерти та фахівці з безпеки можуть використовувати спеціалізовані методи стеганографії для розпізнавання прихованих комунікацій, шкідливих завантажень або зашифрованих даних, прихованих за допомогою стеганографії [8,9,10].

Аналітики з кібербезпеки також можуть використовувати стеганографію для виявлення потенційних небезпек, пов'язаних з кібербезпекою, та запобігання ризику зараження даними чи шкідливим програмним забезпеченням. Це досягається шляхом ретельного вивчення підозрілих файлів або трафіку в мережі на предмет наявності ознак стеганографічного вторгнення. [8,9,10]

1.7.2 З боку кіберзлочинця:

Обман злочинців

Злочинці часто використовують стеганографію, щоб приховати свої дії та уникнути виявлення камерами безпеки. Наприклад, вони можуть розміщувати шкідливе програмне забезпечення, таке як віруси чи трояни, у, здавалося б,

нешкідливих файлах, таких як зображення чи документи, використовуючи стеганографічні методи. Це полегшує їм обхід традиційних заходів безпеки, таких як виявлення вірусів; це програмне забезпечення не призначене для розпізнавання прихованого шкідливого програмного забезпечення [8,9,10].

Також стеганографія використовується кіберзлочинцями для приховування викрадених даних, таких як фінансова інформація чи інтелектуальна власність, коли вони вилучають їх із несправних систем. Приховуючи важливі дані у файлах чи розмовах, які здаються нешкідливими, зловмисники можуть уникнути виявлення за допомогою інструментів моніторингу безпеки [8,9,10].

Прихований зв'язок

Стеганографія сприяє створенню непрямих каналів зв'язку, які дозволяють хакерам обмінюватися порадами, наказами або викраденою інформацією зі зламаними системами. Вставляючи повідомлення в, здавалося б, нешкідливі файли або трафік у мережі, зловмисники можуть спілкуватися із зараженими точками безпеки, не викликаючи підозр.

Злочинні організації також можуть використовувати стеганографію для планування незаконних дій, таких як публікація піратського контенту, скоєння фінансових злочинів або проведення кібератак. Приховуючи цифрові комунікації в незаконному контенті, вони можуть уникати спроб правоохоронних органів та спостереження виявити злочинну діяльність [8,9,10].

1.8 Використання стеганографії у кібератаках

З точки зору кібербезпеки, зловмисники можуть використовувати стеганографію для підривного розміщення шкідливих даних у файлах, які спочатку здаються безпечними. Оскільки стеганографія зазвичай використовується як засіб цілеспрямованого вторгнення, що вимагає значної підготовки та значного обсягу знань для досягнення бажаного ефекту, її використання зазвичай пов'язане зі вторгненнями, які плануються та виконуються

висококваліфікованими злочинцями. Ось список методів здійснення атак за допомогою стеганографії [8,9,10].

Викрадення або приховування шкідливого коду в цифрових носіях: зображення зазвичай стають жертвами атак через велику кількість додаткових даних, які додаються без зміни структури чи зовнішнього вигляду носія. Окрім зображень, відео, документів, аудіо та підписів електронних листів, також використовуються корисні навантаження, які є шкідливими та використовуються для їх розміщення [8,9,10].

Програми-вимагачі та крадіжка даних: кіберзлочинці, що займаються вимаганням, зазвичай використовують стеганографію для приховування даних під час атак. Цей метод сприяє приховуванню конфіденційної інформації в законних комунікаціях, що дозволяє отримувати дані без виявлення.

Приховування команд веб-сторінок: Зловмисники можуть використовувати веб-сторінки, щоб приховати команди, що керують їхніми імплантатами, використовуючи пробіли або файли журналів, розміщені на форумах. Цей метод дозволяє їм приховано передавати викрадені дані та підтримувати активність за допомогою криптографічного коду [8,9,10].

Шкідлива реклама: Зловмисники можуть використовувати стеганографію для реклами своїх продуктів або послуг, вони також можуть вбудовувати шкідливий код у банерну рекламу. Після заповнення цих банерів код витягується та перенаправляє користувачів на сторінки з експлойтами [8,9,10].

1.9 Приклади використання стеганографії в кібератаках.

Скімінг електронної комерції: У 2020 році платформа безпеки електронної комерції Sansec виявила, що хакери використовували стеганографію для розгортання шкідливого програмного забезпечення, яке збирає дані з вразливих сторінок. Шкідливе корисне навантаження було приховано в SVG-зображеннях, а декодер був розміщений на іншій веб-сторінці. Користувачі, які заповнювали свою інформацію на вразливих сторінках оформлення замовлення, не виявляли

жодної підозрілої поведінки, оскільки зображення виглядали як звичайні логотипи популярних корпорацій. Оскільки корисне навантаження виглядало як легітимне використання синтаксису SVG-елементів, стандартні монітори безпеки не змогли розпізнати небезпеку. SolarWinds: Також у 2020 році зловмисники приховали шкідливе програмне забезпечення в легітимних оновленнях для компанії з управління IT-інфраструктурою SolarWinds. Зловмисникам вдалося зламати Microsoft, Intel, Cisco та різні американські агентства. Вони використовували стеганографію, щоб приховати викрадені дані як невинно виглядаючі XML-файли, які надсилалися через HTTP із серверів управління. Інструкції в цих документах були представлені як звичайний текст [8,9,10].

У 2020 році компанії у Великій Британії, Німеччині, Італії та Японії стали жертвами кампанії стеганографії документів. Зловмисники уникли виявлення, приховуючи свою особу як зловмисників, щоб заразити легітимні документи програмою Excel. Шкідливе програмне забезпечення Mimikatz, яке має форму прихованого та замаскованого зображення, було встановлено за допомогою прихованого коду, вбудованого в зображення.

1.10 Захист від атак с використанням стеганографії

Стеганографія відносно проста у використанні, але від неї важко захиститися. Для зменшення ймовірності цього типу атаки можна вжити таких заходів [11,12,13]:

Підвищення обізнаності про кібербезпеку: Навчання співробітників небезпеці завантаження медіафайлів з невідомих джерел може значно зменшити ймовірність успішної атаки. Це навчання також повинно включати вміння розпізнавати шкідливі фішингові електронні листи, а також розуміння стеганографії як потенційної форми кібервторгнення. На фундаментальному рівні важливо навчити співробітників розпізнавати зображення з великими розмірами файлів, які можуть свідчити про наявність прихованих даних [11,12,13].

Впровадження веб-фільтрації та оновлень безпеки: Організації повинні використовувати веб-фільтрацію для запобігання безпечному перегляду Інтернету та завжди оновлювати програмне забезпечення найновішими доповненнями безпеки, щоб зменшити ймовірність вразливостей та атак [11,12,13].

Впровадження сучасних технологій захисту наприкінці: Компанії повинні використовувати технології, які перевершують просте сканування та базову перевірку. Ці рішення можуть розпізнавати код, прихований у зображеннях та інших формах маскування. Основні зусилля щодо розпізнавання шкідливих даних повинні бути спрямовані на кінцеві точки, розташування яких легше розпізнати [11,12,13].

Використовуйте інформацію про загрози: Компанії повинні активно шукати та використовувати інформацію про загрози, щоб бути в курсі останніх тенденцій, особливо щодо кібератак, які використовують стеганографію у своїх операціях.

Використовуйте комплексні антивірусні рішення: Сучасні антивірусні програми сприяють виявленню, ізоляції та видаленню шкідливого коду з комп'ютерів. Вони часто оновлюються, що забезпечує захист від найновіших вірусів та інших типів шкідливих програм [11,12,13].

1.11 Виявлення та протидія стеганографії

1.11.1 Візуальний огляд

Візуальний огляд включає спостереження за підозрілими файлами або повідомленнями на наявність аномальних закономірностей, які можуть свідчити про приховані дані. Цей ручний підхід може розпізнавати нерівності на зображеннях, такі як незвичайні закономірності або розбіжності в значеннях пікселів. Хоча цей підхід ефективний для розпізнавання очевидних ознак жорстокого поводження, він повільний через свою ручну природу. Він також неефективний для повного виявлення стеганографії через тонкість сучасних методів стеганографії [11,12,13].

1.11.2 Чисельний аналіз

Статистичні методи відіграють значну роль у виявленні стеганографії шляхом аналізу цифрових медіа на наявність аномальних закономірностей. Наприклад, аналіз розподілу значень пікселів на зображеннях або частотного спектру аудіо може виявити інформацію, яка прихована за допомогою стеганографічних методів. Цей метод вимагає спеціалізованого програмного забезпечення та алгоритмів, які використовуються для точного визначення аномальної статистики, що вказує на стеганографію [11,12,13].

1.11.3 Програмне забезпечення для стегананалізу

Програмне забезпечення для стегананалізу автоматично виявляє стеганографію, використовуючи алгоритми та статистичні моделі для аналізу файлів на наявність доказів стеганографії. Ці інструменти призначені для ефективного виявлення прихованих даних у цифрових носіях, що робить їх важливими компонентами стратегій кібербезпеки [11,12,13].

1.11.4 Перевірка цілісності файлів

Цілісність файлу перевіряється шляхом порівняння хеш-значення або контрольної суми файлу до та після передачі, щоб виявити будь-які зміни, спричинені стеганографією. Будь-які відмінності в цілісності файлу можуть свідчити про наявність прихованої інформації [11,12,13].

1.11.5 Аналіз мережевого трафіку

Атаки, засновані на стеганографічному методі роботи в мережі, можна розпізнати за допомогою комплексного аналізу трафіку в мережі. Моніторинг заголовків пакетів, їх корисного навантаження та часу передачі може виявити

аномальні закономірності або поведінку, що свідчать про стеганографію. Цього можна досягти за допомогою технологій NIDS та DPI [11,12,13].

1.11.6 Фільтри для контенту

Впровадження механізмів фільтрації на основі контенту може допомогти запобігти передачі підроблених даних шляхом сканування файлів та комунікацій на наявність закономірностей або підписів, які, як відомо, є стеганографічними. Інструменти фільтрації контенту можуть автоматично розпізнавати та запобігати потраплянню підозрілого контенту до мережі компанії, зменшуючи ймовірність стеганографічної атаки. Постійна зміна вмісту бази даних, яка зберігає контент, має вирішальне значення для того, щоб залишатися на крок попереду розвитку стеганографічних методів та векторів загроз [11,12,13].

1.11.7 Навчання та обізнаність користувачів

Навчання користувачів щодо небезпеки стеганографії та просування ефективних методів комунікації мають вирішальне значення для запобігання практиці стеганографії. Навчальні програми повинні зосереджуватися на важливості використання безпечних каналів зв'язку, уникненні використання незаконного програмного забезпечення або послуг та розпізнаванні потенційних індикаторів стеганографічної поведінки [11,12,13].

1.12 Стеганографія та водяні знаки

Хоча водяні знаки та стеганографія мають певну схожість у своєму призначенні, вони принципово відрізняються. У стеганографії зображення, що використовується як накладене зображення, є, по суті, приманкою, яка не має жодного зв'язку з секретним повідомленням. Натомість водяний знак зазвичай містить додаткову інформацію щодо накладеного зображення або іншу пов'язану

з ним відповідну інформацію, таку як теги, що ідентифікують відправника або одержувача. Наприклад, під час купівлі MP3-пісні онлайн інформація про продавця та покупця може бути включена до пісні як водяний знак, який є одночасно чутним та надійним. Водяний знак може бути використаний пізніше для пошуку копій пісні, які розповсюджуються незаконно. Також водяні знаки можуть бути використані для передачі інформації про саму пісню (наприклад, її унікальний хеш або дайджест), що дозволить пізніше визначити автентичність пісні шляхом порівняння пісні з водяним знаком [11,12,13].

Друга і, мабуть, найважливіша відмінність між стеганографією та водяним знаком полягає в запиті щодо існування секретного повідомлення на зображенні. Хоча стеганографія займається приховуванням даних, прихованих від спостерігача, наявність водяного знака часто рекомендується для запобігання незаконній поведінці, такій як несанкціоноване відтворення або розповсюдження. Крім того, стеганографія – це форма комунікації, яка вимагає передачі великих обсягів інформації. І навпаки, дуже короткий водяний знак у цифровому форматі може мати велике значення. Наприклад, наявність водяного знака (з корисним навантаженням 1 біт) може бути використана для позначення того, що зображення належить власнику. Ці різні вимоги до цих двох програм роблять їх дизайн та аналіз різними [11,12,13].

1.13 Різниця між стеганографією та криптографією.

Стеганографія та криптографія мають однакову мету – захистити повідомлення або секрет від доступу без дозволу, але вони досягають цього різними способами. Криптографія — це процес перетворення інформації в зашифрований текст, який можна розшифрувати лише за допомогою певного ключа. Однак той, хто отримає це повідомлення, розпізнає, що воно було зашифровано, оскільки з тексту одразу видно, що було використано шифрування.

З іншого боку, стеганографія не змінює саме повідомлення, а натомість приховує його існування. Замість шифрування даних, стеганографія приховує їх в інших файлах або повідомленнях, роблячи їх непомітними для зовнішнього світу.

Цей додатковий рівень секретності є корисним, оскільки приховане повідомлення все ще присутнє, що робить стеганографію ефективним інструментом для тих, хто хоче залишатися непоміченим під час спілкування [13,14].

1.14 Стеганографія та NFT

Існують деякі паралелі між стеганографією та NFT (нематеріальні токени, які не можуть бути взаємозамінними).

Під час створення NFT зазвичай можна додати додатковий контент, доступний лише власнику токена. Цей контент може включати різноманітні ресурси, такі як високоякісні зображення, повідомлення, відео, доступ до закритих спільнот, коди або навіть смарт-контракти. Подібно до стеганографії, NFT складаються з кількох окремих файлів або повідомлень, які приховані всередині них. Доступ до додаткового прихованого контенту мають лише вибрані користувачі [13,14].

1.15 Висновок до розділу

Стеганографія вважається одним із найдавніших методів приховування інформації. Її історія складна і почалася з фізичних методів, таких як приховане записування інструкцій або шифрів, і розвинулася до складних цифрових методів сьогодення. Її основна мета залишилася незмінною: забезпечити безшумну передачу інформації, непомітну для сторонніх спостерігачів. Сьогодні, завдяки розвитку інформаційних технологій, стеганографія стала потужним методом приховування даних у структурах цифрових носіїв, зокрема зображень, аудіо, відео та текстів. Ця технологія корисна для вас, оскільки дозволяє успішно приховувати дані в структурах цих файлів [13,14].

Сучасна стеганографія використовується для захисту даних у різних сферах, включаючи особисте спілкування, корпоративну безпеку, державне управління та фінансовий сектор. Зокрема, вона використовується в банківських організаціях для забезпечення секретності транзакцій, перевірки користувачів та запобігання витоку даних. Також важливою в кібербезпеці є стеганографія, яка забезпечує

додатковий рівень захисту в поєднанні з іншими методами, такими як шифрування [13,14].

Однак, стеганографія має і негативний бік: її можливості часто використовуються в кіберзлочинності для передачі таємної інформації, боротьби зі шкідливим програмним забезпеченням та уникнення виявлення. Це створює загрозу для експертів з безпеки, які повинні підвищувати свою кваліфікацію, щоб розпізнавати приховані дані [13,14].

Як результат, стеганографія продовжує бути як потужним методом приховування інформації, так і ключовим компонентом сучасної кібербезпеки. Її універсальність дозволяє вирішувати широкий спектр проблем захисту даних, проте вона також вимагає постійного вдосконалення, щоб впоратися із сучасними небезпеками цифрового світу. Вона успішно поєднує сучасні традиції та історичні досягнення, це поєднання забезпечує нові методи обміну інформацією [13,14].

РОЗДІЛ2.
КОМПЛЕКСНЕ ДОСЛІДЖЕННЯ МЕТОДІВ СТЕГАНОГРАФІЇ ТА СТЕГОАНАЛІЗУ.

2.1 Формати цифрового зображення

2.1.1 представлення кольору

Видиме світло – це суміш електромагнітного випромінювання з типовою довжиною хвилі приблизно від 380 нм до 750 нм. Кожен колір можна пов'язати з функцією спектральної щільності P(λ), яка описує кількість енергії, присутньої на будь-якій заданій довжині хвилі. Як результат, можна сказати, що існує нескінченна кількість різних кольорів, які відповідають певній функції розподілу ймовірностей P(λ), але людське око здатне сприймати лише невелику частину всіх можливих кольорів. У сітківці розташовані три різні типи рецепторів, які називаються колбочками, їхня найбільша чутливість – до червоного, зеленого та синього світла. Колбочки, які реагують на синє світло, мають найнижчий ступінь чутливості до інтенсивності світла, тоді як колбочки, які реагують на зелене світло, мають найвищий ступінь чутливості. Електричні сигнали, що надсилаються колбочками, передаються в мозок, що дозволяє нам сприймати колір. Це основа теорії сприйняття кольору, яка включає три компоненти [13,14].

Ця теорія призводить до адитивної кольорової моделі. Згідно з моделлю, будь-який колір можна отримати з лінійної комбінації трьох основних кольорів (або кольорових компонентів) – червоного, зеленого та синього. Вказуючи об'єм кожного кольору як R, G та B, де кожне число знаходиться в діапазоні [0,1] (починаючи від нуля до повної інтенсивності), кожен колір можна описати як тривимірний вектор у кольоровому кубі RGB (R, G, B) ∈[13,14] . Апаратні системи, що виробляють світло, зазвичай вважаються адитивними. Наприклад, старіші телевізори з електронно-променевою трубкою (CRT) використовують комбінацію трьох різних компонентів RGB на екрані. Рідкокристалічні дисплеї (РК) отримують світло від трьох сусідніх пікселів. Повний діапазон інтенсивності, який сприймається як білий, називається повною інтенсивністю, а низький

діапазон інтенсивності, який сприймається як темний або чорний, називається низькою інтенсивністю [15,16].

Субтрактивна кольорова модель використовується для апаратних пристроїв, які виробляють кольори, приймаючи певні довжини хвиль світла, а не вивільняючи їх. Корисним прикладом субтрактивного пристрою є принтер. Поширеними базовими кольорами субтрактивних систем є блакитний, пурпуровий та жовтий, що призводить до представлення кольору за допомогою вектора CMY. Ці три кольори отримують з білого шляхом віднімання від нього червоного, зеленого та синього. Система CMY доповнюється четвертим кольором, чорним (скорочено K), який використовується для посилення контрастності та економії кольорового тонера [15,16].

Адитивна система кольорів RGB та субтрактивна система кольорів CMY пов'язані між собою [15,16]:

$$C = 1-R, \quad (2.1)$$
$$M = 1-G \text{ або } (2.2).$$
$$Y = 1-B. \quad (2.3)$$

Незважаючи на те, що адитивна модель кольорів сімейства RGB описує кольори, які люди найімовірніше сприймають, вона є надмірно складною та надлишковою, оскільки три сигнали нерозривно пов'язані, що робить її передачу менш практичною. Популярною системою кольорів є модель YUV, яка була створена для передачі телевізійних кольорових сигналів. Необхідність зворотної сумісності з попередніми чорно-білими телевізорами призвела до того, що кольоровий телевізійний сигнал виводили з яскравості сигналу плюс кольоровість сигналу. Читач повинен розуміти, що відтепер літера Y завжди буде асоціюватися з яскравістю, а не з жовтим, на якому базується колірна система CMY(K) [15,16].

Яскравість Y розраховується як середньозважене значення трьох каналів RGB, ваги базуються на чутливості людини до трьох кольорів RGB [15,16].

$$Y = 0.299R + 0.587G + 0.114B. \quad (2.4)$$

Компоненти хромінансів – це різниці між кольоровими каналами та яскравістю [15,16].

$$U = R - Y, \quad (2.5)$$

$$V = B - Y \quad (2.6)$$

що передає інформацію про колір. Перетворення між системами RGB та YUV є лінійним [15,16]

$$\begin{pmatrix} Y \\ U \\ V \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ 0.701 & -0.587 & -0.114 \\ -0.299 & -0.587 & 0.886 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} \quad (2.7)$$

$$\begin{pmatrix} R \\ G \\ B \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & -0.509 & -0.194 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} Y \\ U \\ V \end{pmatrix} \quad (2.8)$$

Якщо кольори RGB представлені 8-бітними цілими числами в діапазоні {0, . . . , 255}, то яскравість Y поділяє цей же діапазон, тоді як U та V потрапляють у діапазон {-179,...,179}. Щоб привести всі три компоненти до одного діапазону, що може бути представлений 8 бітами, компоненти кольору далі лінійно перетворюють у C_r і C_b, отримуючи таким чином колірну модель Y $C_r C_b$. [15,16]

$$\begin{pmatrix} Y \\ C_r \\ C_b \end{pmatrix} = \begin{pmatrix} 0 \\ 128 \\ 128 \end{pmatrix} + \begin{pmatrix} 0.299 & 0.587 & 0.114 \\ 0.5 & -0.419 & -0.081 \\ -0.169 & -0.331 & 0.5 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} \quad (2.9)$$

Оскільки людське око менш чутливе до змін кольору, ніж до яскравості, кольорові сигнали часто представлені з меншою кількістю інформації, водночас забезпечуючи помітне спотворення зображення. Ця істина використовується у форматі стиснення JPEG, а також у телевізійних програмах, де менший відсоток смуги пропускання відводиться для сигналів кольоровості, а більший – для

яскравості. Цифрові зображення моделі Y є цифровими копіями аналогових зображень. Ці зображення створюються у форматах JFIF, TIFF та MPEG (Moving JPEG) [15,16].

2.1.2 Дискретизація кольору

Незважаючи на те, що деякі формати зображень здатні точно відображати значення інтенсивності кольору (IIF, PostScript), більшість форматів квантовані та представляють значення інтенсивності за допомогою фіксованої кількості бітів, що дозволяє захоплювати різні відтінки. Найефективніший режим дискретизації кольору залежить від мети. З одного боку, більшість факсимільних апаратів мають лише два режими кольору (чорний та білий), тоді як супутникові знімки високої роздільної здатності або фотореалістичні синтетичні зображення можуть мати до 16 бітів на колірний канал (48 бітів для кольору). Приклади типових колориметричних значень для вибраних цілей наведено в таблиці 2.1.

У таблиці 2.2 показано глибину кольору кожного формату. Для форматів палітри, які мають глибину кольору, значення представляє діапазон можливих кольорів [15,16].

Таблиця 2.1

Типова бітова глибина кольору для різних застосувань. Для $n_c \geq 8$ вибірка кольорових зображень здійснюється в бітах на колірний канал.

n_c	Кольори	Застосування
1	2	Факс, чорно-білі малюнки
2	4	
4	16	Малювання ліній, графіки, мультиплікація
8	256	Сірі зображення, повноцінні кольорові фото
12	4096	Сірі медичні зображення, сканування, цифровий вивід з датчиків
14	16384	Сканування, цифровий вивід з датчиків, зображення з якістю як з фільму
16	65536	Фото реалістичні синтетичні зображення, сканування, зображення зі спутників

Таблиця 2.2

Вибірка для популярних форматів зображень.

	Колір	Відтінки сірого	Палітра
BMP	24	8	1, 4, 8
TIFF	24, 30, 36, 42, 48	4-8	1-8
PNG	24, 48	1, 2, 4, 8, 16	1, 2, 4, 8
GIF	-	-	1-8
JPEG	24	8, 12	-

2.2 Стеганографічний канал

Основна мета стеганографії полягає в поширенні прихованих повідомлень без будь-яких прямих доказів того, що повідомлення передається. Цього можна досягти шляхом приховування повідомлень у спільних об'єктах, які потім передаються певним каналом зв'язку. У цій частині ми обговоримо окремі компоненти, що складають стеганографічний зв'язок [15,16].

Ми класифікуємо п'ять основних компонентів кожного стеганографічного каналу на такі категорії (див. Рисунок 2.1) [15,16]:

- Походження покриття,
- Методи кодування та декодування даних,
- Джерело підтримки, яке призводить до вбудовування або вилучення алгоритмів,
- Джерело інформації,
- Канал, призначений для обміну інформацією між відправником та одержувачем.

Сучасна стеганографія зазвичай робить деякі основні оцінки походження покриття, що дозволяє проводити формальний аналіз. Наприклад, розглядаючи джерело покриття як випадкову величину, можна оцінити стеганографію за допомогою теорії інформації. Як варіант, джерело покриття можна розглядати як оракул, який можна дослідити. Це призводить до дослідження складності стеганографії [15,16].

Рис 2.1 - Елементи стеганографічного каналу

Алгоритм вбудовування – це метод, за допомогою якого відправник створює зображення, що передає бажане секретне повідомлення. Процедура може вимагати обміну секретом між відправником і одержувачем, який називається стегоключем. Цей ключ важливий для забезпечення правильного вилучення секретного повідомлення зі стегозображення. Наприклад, відправник може включити свій секретний бітовий потік у найменш значущі пікселі на непересічній траєкторії, яка генерується псевдовипадково (визначається стегоключем) [15,16].

Протокол, якого дотримуються відправник і одержувач для вибору стегоключа, зазвичай представлений випадковою величиною, рівномірно розподіленою по простору всіх ключів. Наприклад, життєздатною стратегією є вибір стегоключа (з рівномірним розподілом) з множини всіх можливих стегоключів [15,16].

Походження повідомлення має значний вплив на безпеку стеганографічного зв'язку. Розглянемо дві крайнощі. З одного боку, відправник і одержувач завжди спілкуються з обмеженим повідомленням, зазвичай 16 бітами, у кожному наступному стеганографічному зображенні. І навпаки, їм потрібно спілкуватися за допомогою великих повідомлень і часто включати в зображення стільки деталей, скільки дозволяє алгоритм вбудовування. Інтуїтивно, учасники більше ризикують

у другому сценарії. Розподіл повідомлень можна розглядати як випадкову величину, розподілену по всіх можливих просторах повідомлень [15,16].

Фактичний канал зв'язку, який використовується для надсилання зображень, вважається основним каналом спостереження. Сторона, що захищається, може виконувати три різні функції. У пасивній позиції, яка спостерігає лише за трафіком, сторона, що спостерігає, не бере участі у фактичному спілкуванні між учасниками стеганографічного обміну. Це називається сценарієм пасивного варту. Як варіант, захист може вважати, що відправник і одержувач використовують стеганографію, вони намагатимуться запобігти обміну інформацією, навмисно змінюючи зображення, що передаються. Наприклад, ви можете зменшити розмір зображення за допомогою JPEG, ви можете обрізати або змінити розмір зображення, або ви можете застосувати невеликий обсяг обробки. Якщо ви не використовуєте стеганографію, стійку до цього типу маніпуляцій, стеганографічний канал буде негативно вплинути на захист. Це називається ситуацією активного варту. Зрештою, захист може спробувати визначити стеганографічний метод, який використовували відправник і одержувач, вони також можуть спробувати імітувати одну зі сторін або іншим чином спробувати ввести в оману сторони, що спілкуються. Різниця між зловмисним вартовим та активним вартовим полягає в тому, що перший займається моніторингом навколишнього середовища, тоді як другий — захистом навколишнього середовища. Дії активного вартового спрямовані на те, щоб зробити стеганографію неможливою для спілкування, тоді як зловмисний вартовий не обов'язково хоче повністю знищити канал для стеганографії, натомість він або вона використовує його для визначення, чи відбувається стеганографія. Пасивний випадок — це сценарій спілкування через стандартний інтернет-протокол, помилки виправляються та виконується автентифікація, що гарантує передачу безпомилкових даних [15,16].

Вищезазначене описує необхідність ширшого підходу до розгляду стеганографічного спілкування. Під час розробки стеганографічної схеми

учасники спілкування мають можливість вибору основних компонентів свого спілкування [15,16].

Алгоритми вбудовування та вилучення є критично важливими для будь-якої стегосистеми. Стеганографічні методи можуть використовувати три різні основні структури, що описують внутрішній механізм стеганографії та процесів вилучення. Відправник може досягти цього, вибравши зображення, в якому вже приховано бажане повідомлення. Це відомо як стеганографія вибору об'єктів. Або ж він може створити інструмент, який передає повідомлення. Ця стратегія називається стратегією стеганографії синтезу об'єктів. Третій варіант, який є найефективнішим для вміщення великих обсягів інформації, - це модифікація об'єктів за допомогою стеганографії. Це вважається найпопулярнішим методом приховування [15,16].

2.3 Стеганографія за вибором об'єкта

У стеганографії, яка включає вибір об'єктів, відправник має попередньо створену базу даних зображень, з якої він вибирає те, що передає бажане повідомлення. Наприклад, один байт даних може бути переданий, вибравши зображення в альбомному або портретному режимі. Як варіант, присутність тварини на зображенні може мати приховане повідомлення, таке як твердження «атака завтра». Алгоритм, який вбудовує зображення, може просто вибирати зображення випадковим чином з бази даних і знаходити зображення, яке легко передає бажане повідомлення. Мета стеганографічного ключа — встановити набір правил, які інтерпретують зображення. Одним із важливих прикладів стеганографії на основі об'єктів є хешування. Відправник вибирає зображення з бази даних і використовує до нього функцію хешування (ця функція може залежати від ключа і повинна бути надана одержувачу). Якщо хеш ідентичний бажаному бітовому шаблону повідомлення, зображення передається; в іншому випадку відправник вибирає інше зображення, доки не буде знайдено збіг. Орієнтовна кількість спроб, необхідних для успішного отримання збігу, залежить

від довжини хешу, який тому швидко стає неефективним. Після отримання зображення одержувач просто витягує хеш-функцію, щоб прочитати повідомлення. Перевага цього підходу полягає в тому, що об'єкт завжди на 100% натуральний, оскільки це справжнє зображення, яке жодним чином не було змінено. Найбільш очевидним недоліком є відсутність практичної ефективності [15,16].

Після подальшого дослідження можна виявити потенційний недолік вибіркової стеганографії, який би завадив людині стверджувати, що вона дійсно невиявлювана. Щоб прояснити це питання, ми використовуємо просту хеш-функцію, яка базується на найменш значущих бітах перших трьох пікселів зображення [15,16].

$$h(x) = \{x[1] \, mod \, 2, x[2] \, mod \, 2, x[3] mod 2\} \qquad (2.10)$$

Важливо розуміти, що дайджест має три складові біти. Проблема може виникнути, коли відправник вирішує використовувати цей метод для багаторазового зв'язку. Якщо кожна трійка бітів з усіх восьми можливих трійок має однакову ймовірність бути надісланою (що є поширеним припущенням, наприклад, під час надсилання частин зашифрованого документа), зображення, які надсилає відправник, з однаковою ймовірністю створять будь-яку з 8-бітових трійок, що й дайджест. Однак, як ми знаємо, що найменш значущі біти (LSB) перших трьох пікселів у верхньому лівому куті розподілені таким чином на природних зображеннях? Ймовірно, це не так, оскільки ці пікселі, ймовірно, є частиною неба, тому їхні значення навряд чи будуть незалежними. Важливо визнати, що ця проблема виникає лише тому, що ми враховуємо кілька способів використання стеганографічного каналу та дозволяємо злочинцю переглядати всі передачі від відправника, замість того, щоб розглядати одне зображення за раз [15,16].

2.3 Стеганографія за допомогою синтезу покриття

У стеганографії, яка приховує відправника, останній створює обкладинку, яка передає задумане повідомлення. Деякі ЗМІ повідомляли, що відео може містити приховані повідомлення, які виражаються через будь-який компонент відео, включаючи одяг, предмети або просто аудіо. Це був би приклад обкладинки, яка стеганографічно прихована [15,16].

Ще один цікавий приклад, який використовує текст як обкладинку замість цифрових зображень, – це кодування повідомлень, щоб вони нагадували спам. Тут стеганограф використовує той факт, що спам часто має незв'язні або своєрідні формулювання, які можна використовувати для приховування повідомлення. SpamMimic (www.spammimic.com) використовує мімікрію для приховування повідомлень у тексті, створеному спам-ботом, який нагадує спам [15,16].

Стеганографію комбінації обкладинок можна поєднувати зі стеганографією вибору обкладинок, щоб зменшити складність вбудованого повідомлення за допомогою хешування. Якщо ми можемо зробити кілька знімків однієї сцени однією цифровою камерою, то можна сказати, що сцена повторюється кілька разів. Наприклад, ми могли б розмістити камеру на штативі та зробити кілька знімків з постійним джерелом освітлення. Припустимо, що зображення мають 8-бітну градацію сірого, а інтенсивність i-го пікселя на j-му зображенні позначається як , де i = 1,…, n, j = 1, …, K. Тепер ми спостерігаємо важливий факт: значення інтенсивності світла на певному пікселі i, якщо їх спостерігати на всіх зображеннях j, залежать від наявності випадкового шуму на зображеннях, такого як читання книги, шум від вбудованої електроніки та вибух свічки [15,16].

Стеганограф використовує криптографічну хеш-функцію, яка змінюється таким чином, щоб повертати 4 біти при застосуванні до 16 пікселів. Наприклад, можна використовувати останні 4 біти хешу MD5. Значення 4 та 16 вибираються випадковим чином, можливі й інші значення. Щоб вбудувати своє повідомлення, відправник бере кожне зображення та розбиває його на окремі блоки розміром 4 ×

4 пікселі, потім створює нове зображення, об'єднуючи блоки, блоки 4 × 4 передадуть 4 біти повідомлення [15,16].

Щоб вбудувати перші чотири біти в перший блок пікселів розміром чотири × чотири, стеганограф шукатиме хеші, що відповідають хешу повідомлення, це відбуватиметься для кількості зображень. Після цього він переходить до наступного блоку та знаходить , що буде наступними 4 бітами повідомлення тощо. Остаточне зображення у буде мозаїкою, складеною з блоків, отриманих з різних зображень у = (, …, , , … ,). Ймовірність знаходження збігу в одному конкретному блоці всіх K зображень дорівнює $1-(1-1/16)^K$ [15,16].

Таким чином, ймовірність того, що можна буде включити все повідомлення, яке має n/16 груп по 4 біти, дорівнює $(1-(1-1/16)^k)^{n/16}$. Зі збільшенням кількості зображень ймовірність отримання правильної відповіді зменшується. Наприклад, ймовірність квадратного зображення розміром n = 512 × 512, яке має лише K = 400 зображень, дорівнює 0,99999998993… [15,16].

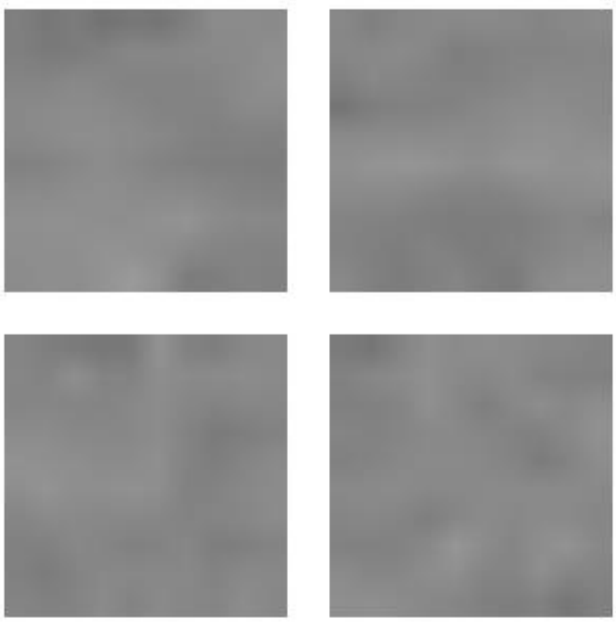


Рис 2.2 - 16 на 16 пікселів блок з чотирьох не стиснутих TIFF зображень синього неба знятого з однієї камери з коротким інтервалом.

Спочатку блоки здаються неоднорідними; незважаючи на вражаючу однорідність сцени, самі блоки не є однорідними. По-друге, блоки різні на кожному зображенні через генератори випадкового шуму [15,16].

Цей підхід має радше теоретичний, ніж практичний характер. Це пояснюється тим, що важко отримати кілька зразків одного й того ж сигналу (однакові фотографії однієї й тієї ж сцени, ідентичні лише на частку ширини пікселя). Невеликі відмінності у часі експозиції через механізм затвора та інші механічні коливання впливатимуть на вирівнювання різних зображень [15,16].

Схема робить умовне припущення, що пікселі на межах блоків незалежні, або, точніше, що випадкові компоненти зображень незалежні. Як ми вже зазначали в розділі 3, різні типи обробки в камері, такі як інтерполяція кольорів або фільтрація, призводять до залежності між сусідніми пікселями і, отже, між їхніми шумовими компонентами. Таким чином, захист може ініціювати атаку, вивчаючи зв'язки між пікселями, що перетинають межі блоків, і порівнюючи їх зі зв'язками між пікселями в сусідніх блоках [15,16].

Існує інша форма стеганографії, яка має якісний характер, і називається маскуванням даних. Концепція полягає в тому, що всі методи стеганографії зрештою автоматизовані та використовують набір числових значень із зображення, які потім оцінюються на сумісність з типовими характеристиками зображень обкладинки. Як результат, усі необхідні зусилля відправника полягають у тому, щоб уникнути виявлення, зробивши стегозображення схожим на обкладинку з точки зору простору ознак [17,18]. Саме «зображення» може не виглядати природним, якщо його характеристики схожі на характеристики природних зображень, воно буде виявлено детектором. Було розроблено практичний метод приховування даних за допомогою змінного в часі фільтра, який відображає кожне 1024-бітове повідомлення на відповідний аудіокадр, що відповідає певному опорному звуку [17,18].

2.4 Стеганографія через модифікацію контейнера

Відправник починає з зображення контейнера, яке змінюється, щоб включити конфіденційну інформацію. Комунікатори мають набір усіх можливих контейнерів, а також набір ключів та повідомлень, які, в найпростішому випадку, залежать від кожного контейнера [17,18]:

C . . . set of cover objects x ∈ C, (2.11)
K(x) . . . set of all stego keys for x, (2.12)
M(x) . . . set of all messages that can be communicated in x. (2.13)

На рисунку нижче стеганографічна стратегія ілюструється як пара функцій, що вбудовуються та вилучаються [17,18].

Emb : C ×K×M→C, (2.14)
Ext : C ×K→M, (2.15)
таких, що для всіх x ∈ C, усіх k ∈ K(x), m∈M(x),
Ext (Emb(x, k,m), k) = m. (2.16)

Іншими словами, відправник може покрити будь-яку область x ∈ C та приховати в ній будь-яке повідомлення m ∈ M(x), використовуючи будь-який секретний ключ k ∈ K(x), що призводить до стеганографічного зображення: y = Enc(x, k, m). Максимальна кількість повідомлень, які можна передати в певній області, обмежена стеганографічною стратегією, самою областю та кількістю повідомлень, які можна передати в цій області. Наприклад, якщо C — це множина всіх 512 × 512 градацій сірого, і стеганограф вставляє один біт повідомлення на піксель у кожне зображення, тоді середня кількість інформації на зображення дорівнює |M(x)| = для всіх x ∈ C [17,18].

І навпаки, якщо C — це множина всіх 512 × 512 градацій сірого JPEG з якістю = 75, і один біт вбудований у кожен ненульовий квантований коефіцієнт

DCT, тоді кількість повідомлень, які можна вбудувати в певну область, залежить від самої області, як кількість ненульових коефіцієнтів DCT у JPEG залежить від вмісту зображення [17,18].

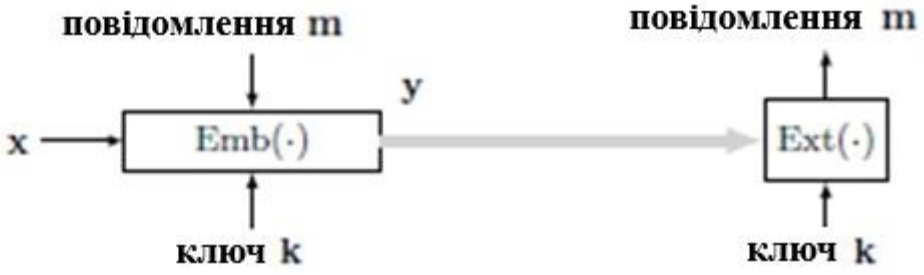


Рис 2.3 - Стеганографія модифікацією обгортки.

Таким чином, ми визначаємо ємність вбудовування (вантажопідйомність) покриття x у бітах як [17,18]

$$log_2|M(x)|, \qquad (2.17)$$

а відносна ємність вбудовування становить

$$\frac{log_2|M(x)|}{n}, \qquad (2.18)$$

де n — це кількість елементів у x, таких як кількість пікселів або ненульових коефіцієнтів DCT. Для растрових зображень відносну ємність часто виражають у bpp(біт на піксель) [17,18].

Для зображень JPEG одиницею вимірювання є bpnc (бітів на ненульовий коефіцієнт DCT). Беручи очікуване значення (4.8) та (4.9) стосовно розподілу покриттів, що дорівнює x, ми можемо обговорити середню ємність для вбудованості та відносну ємність для вбудованості [17,18].

Мабуть, найважливішим поняттям стеганографії є ємність для стеганографії, яка є максимальною кількістю бітів, які можна приховати без будь-яких виявлених статистичних ефектів. Як правило, стеганографічна ємність менша за ємність для вбудовання [17,18].

Процедури вбудовування стеганографії в покриття вимагають кодування зображень покриття та стеганографії як бітів або, загалом, символів певного алфавіту A відповідно до функції присвоєння символів π. [17,18]

$$\pi : X \rightarrow A, \quad (2.19)$$

де X — це набір окремих компонентів захисту, таких як пікселі або коефіцієнти DCT. Однією з поширених функцій, яка використовує найменш значущий біт, є функція парності [17,18].

$$LSB(x) = x \bmod 2. \quad (2.20)$$

Якщо вбудований алгоритм розроблений таким чином, щоб уникнути зміни певних областей зображення, зберігаючи при цьому оригінальне зображення, це називається адаптивною стеганографією. Наприклад, гладкі області зображення можна пропустити та зосередити в текстурованих областях. Частина зображення, яка змінюється, називається каналом вибору. Іншим прикладом каналу вибору є додавання бітів повідомлення до псевдовипадкового шляху, який проходить через зображення, отримане зі стего-ключа. Як правило, учасникам зв'язку вигідно зберігати свої таємниці або розкривати якомога менше інформації про канал вибору, цю інформацію може використовувати зловмисник. Якщо канал вибору є ексклюзивним для одного з учасників, це називається неспільним каналом вибору [17,18].

Стеганографія вносить помилки в накладання, змінюючи накладання.

Спотворення зазвичай вимірюється за допомогою відображення d(x, y), d : C × C → [0,∞). Одна з часто використовуваних сімей мір спотворення параметризується значенням γ ≥ 1, [17,18]

$$d_\gamma(x, y) = \sum_{i=1}^{n} |x[i] - y[i]|^\gamma. \quad (2.21)$$

Для γ = 1,

$$d_1(x,y) = \sum_{i=1}^{n} |x[i] - y[i]|. \qquad (2.22)$$

Для L_1норма між векторами x та y, поки

$$d_2(x,y) = \sum_{i=1}^{n} |x[i] - y[i]|^2. \qquad (2.23)$$

є енергією для внутрішніх змін.

Міра

$$v(x,y) = \sum_{i=1}^{n} 1 - \delta(x[i] - y[i]). \qquad (2.24)$$

це кількість змін під час вбудовування, де δ — дельта Кронекера (2.23). Зверніть увагу, що якщо амплітуда змін під час вбудовування становить $|x[i] - y[i]| = 1$, d_γ збігаються для всіх γ. [17,18]

Вищезазначена міра спотворення вважається абсолютною, оскільки вона обчислює загальний ступінь спотворення. Зазвичай спотворення виражають відносно загального об'єму контейнера (наприклад, для кожного пікселя це ступінь спотворення зображення порівняно з оригіналом, це називається відносним спотворенням) [17,18].

$$\frac{d(x,y)}{n} \qquad (2.25)$$

Кількість

$$\beta = \frac{v(x,y)}{n} \qquad (2.26)$$

називається частотою змін і зазвичай позначається як β.

Два популярних відносних показники — це середньоквадратична помилка (MSE) [17,18]

$$MSE = \frac{d_2(x,y)}{n} = \frac{1}{n}\sum_{i=1}^{n} |x[i] - y[i]|^2, \qquad (2.27)$$

та відношення пікової сигналу до шуму (PSNR).

$$PSNR = 10\log_{10}\frac{x_{max}^2}{MSE}, \qquad (2.28)$$

де x_{max}— це максимальне значення, яке може набрати x[i]. Наприклад, для 8-бітних градацій сірого x_{max} = 255. [17,18]

Середня величина спотворень, вбудованих у систему, – це очікуване значення E [d(x, y)], яке береться по всіх x ∈ C, k ∈ K, m ∈ M та вибирається з певним розподілом ймовірностей з відповідної множини [17,18].

Одним з найважливіших атрибутів стегосистеми є її ефективність вбудовування, цей атрибут має значний вплив на її безпеку. Ми визначаємо його тут, без формальних визначень, як середню кількість бітів на одиницю середнього спотворення [17,18].

$$e = \frac{E_x[\log_2 |M(x)|]}{E_{x,m}[d(x,y)]}, \qquad (2.29)$$

Складність розрахунку ефективності вбудованої схеми ґрунтується на стеганографічній стратегії, внутрішньому механізмі та джерелі приховування. Для найпростіших схем вбудовування, таких як схема LSB або ±1 у просторовій області, ефективність вбудовування можна легко розрахувати аналітичними засобами. І навпаки, для деяких стеганографічних методів максимальний обсяг даних, які можна приховати, а також спотворення, є складною функцією вмісту покриття або стего-ключа, що ускладнює розрахунок ефективності приховування з точки зору нашої нестачі знань про походження покриття. У цьому випадку ефективність вбудованого пристрою визначається експериментами. Зрештою, ми визнаємо, що ефективність вбудовування залежить від вимірювання спотворення d [17,18].

2.5 LSB-впровадження

```
// Ініціалізація PRNG використовуючи стего ключ
//Ввести: повідомлення m ∈ {0,1}^m,  зображення  x ∈ X^n
Path = Perm(n);
// Perm(n)  Псевдо-рандомна перестановка  {1,2,...,n}
y = x;
m = min(m,n);
// Якщо повідомлення більше за доступний об'єм, вкоротити його
for i = 1 to m {
  y[Path[i]] = x[Path[i]] + m[i] − x[Path[i]] mod 2;
}
// y це стего зображення з m вписані біти повідомлення
```

Алгоритм 2.1 - вбудоване повідомлення $m \in \{0,1\}^m$ прихована в зображені $x \in x^n$.

LSB-стеганографія вважається найпростішим з усіх стеганографічних методів. Її можна застосовувати до будь-якого набору даних, представленого числовими даними в цифровій формі. Припустимо, що x[i] – це ціла послідовність. Наприклад, x[i] може бути інтенсивністю світла в і-му пікселі 8-бітного кольорового зображення, індексом палітри у файлі GIF або квантованим коефіцієнтом DCT у файлі JPEG. Залежно від формату зображення та розрядності представлених значень, кожен x[i] можна виразити за допомогою бітів b[i, 1],…, b[i,], [17,18]

$$x[i] < \sum_{k=1}^{n_c} b[i,k]2^{n_c-k}, \qquad (2.30)$$

В результаті, ми можемо розглядати послідовність (b[i, 1],…, b[i,]) як представлення x[i] у порядку ведення записів (старший біт b[i, 1] – це перший біт). Найменший біт (LSB) – це останній біт байта[i,]. [17,18]

Процедура вставки LSB названа так, оскільки вона передбачає заміну значень LSB x[i] бітами повідомлення m[i], що призводить до отримання стего-зображення y[i]. Алгоритм 5.1 демонструє псевдокод для вставки цифрового підпису в зображення за допомогою секретного ключа, який є спільним для всіх учасників стеганографічного зв'язку [17,18].

Важливо зазначити, що в кольоровому зображенні кількість компонентів у накладенні в 3 рази більша, ніж у зображенні у градаціях сірого. В результаті використовується псевдовипадковий маршрут через усі пікселі та кольорові компоненти. Повідомлення, згенероване за допомогою алгоритму 2.1, можна відтворити за допомогою псевдокоду в алгоритмі 2.2. [17,18]

Величина змін у позиції молодшого біта (LSB) дорівнює 1, що є мінімально можливою зміною для будь-якої зміни позиції. У типових умовах перегляду зміни вставки в 8-бітному зображенні у градаціях сірого або кольоровому зображенні візуально не помітні. Крім того, оскільки природні зображення мають невелику кількість шуму через різні джерела шуму, присутні під час захоплення зображення, площина LSB необробленого, нестисненого природного зображення вже виглядає випадковою. На рисунку 2.4 показано оригінальне зображення та його площину LSB b[ri,] для червоного каналу [17,18].

```
// ініціалізація PRNG за допомогою стего ключа

Path = Perm(n);

for i = 1 to m {
  m[i] = y[Path[i]] mod 2;
}
// m це витягнуте секретне повідомлення
```

Алгоритм 2.2 вбудоване повідомлення m з стего зображення y.

Таблиця 2.3

Відносна кількість бітів, сусідніх пар і трійок бітів від площини LSB зображення

	Частота подій
іти	0.49942, 0.50058
ари	0.24958, 0.24984, 0.24984, 0.25073
ріо	0.1246, 0.1250, 0.1247, 0.1251, 0.1250, 0.1249, 0.1251, 0.1256

У таблиці 2.3 наведено частоту появи окремих бітів у b[i,], 1, …, n, парах суміжних бітів (b[i,], b[i + 1,]) та триплетах суміжних бітів (b[i,], b[i + 1,], b[i + 2,]) [17,18]. Ця інформація узгоджується з твердженням, що площина LSB розташована випадково. Незважаючи на те, що це не є доказом випадковості, аргумент все ще достатньо переконливий, щоб вважати, що будь-яка спроба розпізнати акт випадкового перевертання частини площини LSB буде невдалою. Це, здавалося б, очевидне твердження є неправильним, оскільки LSB легко розпізнати при вставці в зображення [17,18].

Навіть якби ймовірність площин LSB накладень була справді випадковою, все одно можна було б розпізнати зміни в розміщенні через механізм перевертання LSB, наприклад, якби друга площина LSB b[i, - 1] та площина LSB були залежними. У найекстремальнішому прикладі залежності, якщо b[i, - 1] = b[i,] для кожного і, розпізнавання змін молодшого біта було б простим. Все, що нам потрібно було б зробити, це порівняти площину молодшого біта з другою площиною молодшого біта [17,18].

Вставка молодшого біта є частиною класу стеганографічних методів, які беруть біти повідомлення та поміщають їх в один елемент накладання. Зрештою, кожен біт призначається певному компоненту. Процедура вставки нового

елемента виконується шляхом відвідування окремих компонентів, на які накладено повідомлення, та застосування процедури вставки нових компонентів (перегортання молодших бітів) за необхідності для вирівнювання молодших бітів з бітами повідомлення. Не всі стеганографічні схеми достатньо прості, щоб дотримуватися цієї простої парадигми вставки. Методи, що використовують синдромне кодування, мають кілька компонентів, які використовуються для вставки кожного біта, це тому, що алгоритм вилучення повинен знати про більше одного компонента, щоб вилучити один біт [17,18].

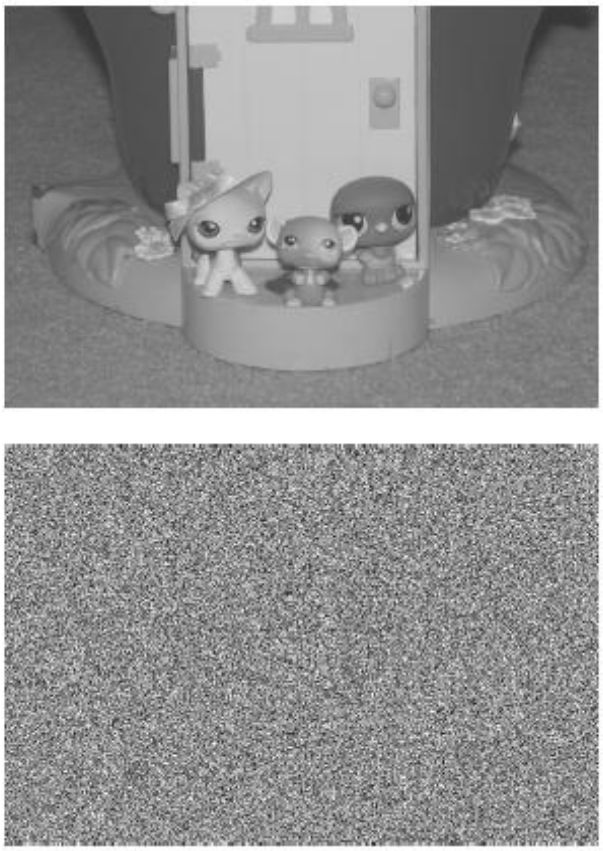


Рис. 2.4 - Справжній колір 800 x 548 фотографії та LSB площині його червоного каналу.

Операцію вставки, що полягає в перевертанні LSB, можна записати математично багатьма різними способами [17,18]:

$$LSBflip(x) = \begin{cases} x + 1 \text{ коли x парний} \\ x - 1 \text{ коли x не парний} \end{cases} \quad (2.31)$$

LSBflip – це обертання, яке досягає рівняння LSBflip(LSBflip(x)) = x. Це означає, що повторна вставка LSB частково змінює спотворення, внесені ним, тому існує обмеження на максимальне очікуване спотворення, яке може бути спричинене повторною вставкою LSB. Багато інших вставок не мають цієї властивості. Часткове руйнування механізму вставки може бути використано для атаки схем, що використовують вставку LSB [17].

Також, вставка LSB призводить до того, що несуміжні пари LSB індукуються у всьому наборі можливих значень {0, 1, ..., [17,18]

$$\{0,1\},\{2,3\},\dots,\{2^{n_c}-2,2^{n_c}-1\} \qquad (2.32)$$

Важливо зазначити, що якщо x[i] знаходиться в першій парі молодшого біту {2k, 2k + 1}, він повинен залишатися в цій позиції після вставки, оскільки елементи в парі мають різні молодші біти (2k ↔ 2k + 1). Це просте спостереження є основою для багатьох ефективних атак на метод LSB [17,18].

Для будь-якого стеганографічного методу часто корисно графічно продемонструвати вплив приховування на гістограму кольорів зображення. Багато стеганографічних методів додають особливі риси до гістограми, які можна використовувати для розпізнавання наявності прихованих повідомлень (атаки побудови). Нехай h[j], j = 0, ..., − 1, буде розподілом елементів на фотографії обкладинки [17,18].

$$h[j]=\sum_{i=1}^{n}\delta(x[i]-j), \qquad (2.33)$$

де δ — це дельта Кронекера (2.33).

Ми припустимо, що відправник додає до свого потоку послідовність з m випадкових байтів. Припущення про випадковість виправдане, оскільки відправник за своєю суттю зацікавлений у мінімізації впливу вбудовування, тому

він стискає повідомлення та, ймовірно, також шифрує його, щоб підвищити безпеку зв'язку. Нехай m - загальна кількість бітів, що передаються, включаючи початкове значення 0. Припускаючи, що біти розташовані вздовж псевдовипадкового шляху через зображення, ймовірність того, що піксель не змінюється, ідентична ймовірності того, що він не буде вибраний для включення, 1 − α, плюс ймовірність того, що він буде вибраний, α, помножена на ймовірність того, що зміна не потрібна, що відбувається з ймовірністю 1/2, оскільки ми використовуємо випадковий бітовий потік для вбудовування [17,18].

Таким чином, для будь-якого j,

$$\Pr\{y[i] = j | x[i] = j\} = 1 - a + \frac{a}{2} = 1 - \frac{a}{2}, \qquad (2.34)$$

$$\Pr\{y[i] \neq j | x[i]\} = \frac{a}{2} \qquad (2.35)$$

Оскільки під час вбудовування LSB значення пікселів у парі LSB {2k, 2k + 1}, k = 0, ... , −1, змінюються одне на одне, але ніколи на інші значення, загальна сума [2k] + [2k + 1] залишається однаковою для будь-якого значення α і тому не змінюється за методом LSB кодування. Це гістограма вмісту стегозображення. В результаті, очікуване значення [2k] дорівнює кількості пікселів зі значеннями 2k, які залишилися незмінними, плюс кількості пікселів зі значеннями 2k + 1 [17,18].

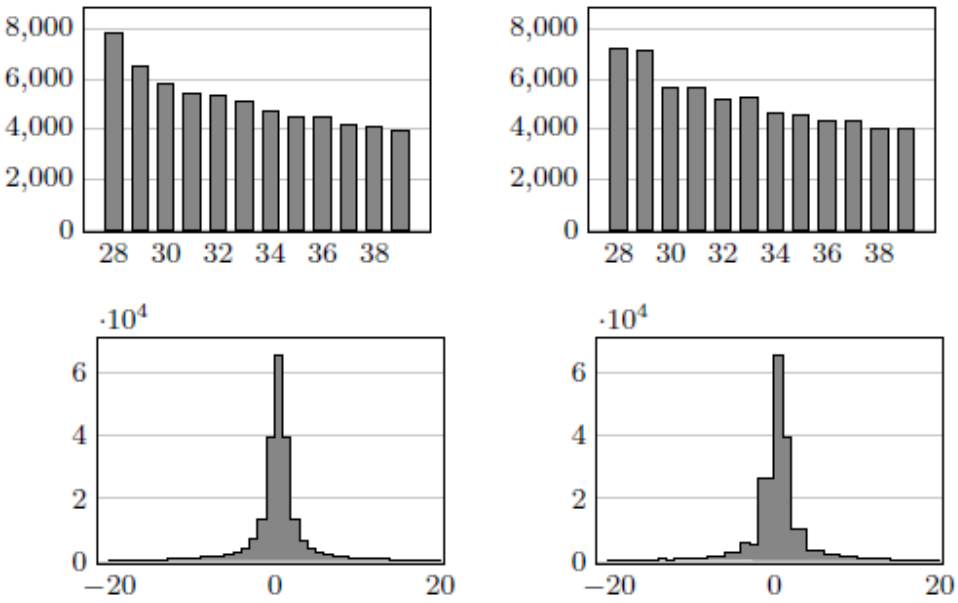


Рис. 2.5 - вплив вбудовування LSB на гістограму.

Вгорі: Збільшена частина гістограми показана на рисунку 2.5 після перетворення зображення у 8-бітну градацію сірого до та після кодування LSB. Внизу: Гістограма квантованих коефіцієнтів DCT того самого зображення до та після вбудовування за допомогою Jsteg. Ліві зображення представляють обкладинки, праві числа представляють стегограми [17,18].

які були змінені на 2k:

$$E\left[h_a[2k]\right] = \left(1 - \frac{a}{2}\right) h[2k] + \frac{a}{2} h[2k+1] \qquad (2.36)$$

$$E\left[h_a[2k+1]\right] = \frac{a}{2} h[2k] + \left(1 - \frac{a}{2}\right) h[2k+1] \qquad (2.37)$$

Зверніть увагу, що якщо повністю заповнити своє покривне зображення n бітами (α = 1), ми маємо [17,18]:

$$E\left[h_1[2k]\right] = E\left[h_1[2k+1]\right] = \frac{h[2k] + h[2k+1]}{2}, k = 0, \ldots, 2^{n_c - 1} - 1 \qquad (2.38)$$

Як наслідок, ми вважаємо, що розміщення LSB зазвичай знижує розподіл підрахунків у кожному інтервалі. Це призводить до сходоподібного візерунка в гістограмі стеганографічного зображення (рис. 2.5), який можна використовувати для розрізнення зображень, повністю вбудованих з LSB, від їх оригінальних зображень. Це спостереження представлено так званою атакою гістограми, яка описана нижче [17,18].

2.6 Стегоаналіз

Стеганологічний аналіз – це галузь наукового дослідження та практичний інструмент, що сприяє виявленню прихованої інформації в цифрових носіях, таких як зображення, аудіозаписи, відео чи текстові файли, що були вставлені за допомогою стеганографії. Його основна мета – визначити фактичне існування прихованих даних, і, якщо можливо, витягти або знищити ці дані. Сьогодні стеганографія зазвичай використовується для збереження інформації або приховування шкідливих дій, обидві ці функції набули особливого значення в кібербезпеці, цифрових доказах та інших галузях. Процедура стеганологічного аналізу включає спостереження за цифровими носіями на предмет змін, які можна віднести до прихованої інформації [19,20].

Наприклад, вбудовування даних у зображення може призвести до ледь помітних змін значень пікселів або статистичних властивостей файлу, таких як яскравість гістограм або розподіл кольорів. У випадку аудіо чи відео це можуть бути неправильне використання частотного спектру або аномалії в амплітудному спектрі. Основні інструменти стеганологічного аналізу включають статистичний аналіз, а також складні методи, такі як машинне навчання, яке передбачає використання алгоритмів для розпізнавання носіїв, що містять приховані дані, на основі великих наборів даних прикладів. Одним з основних завдань стеганалізу є розпізнавання методу приховування інформації. Якщо алгоритм відомий, це може значно спростити процес розпізнавання або отримання інформації. Однак більшість випадків пов'язані з ситуаціями з неоднозначністю, коли вихідний (або

оригінальний) носій невідомий, а алгоритм невідомий. Цей метод називається «сліпим» стеганалізом, і він особливо складний, оскільки вимагає створення універсальних детекторів, які не мають жодних попередніх знань про ціль [19,20].

Стеганаліз часто використовується в різних професіях. У кібербезпеці його метою є виявлення прихованих методів передачі даних, які можуть бути використані хакерами для обміну або передачі приватної інформації. У криміналістиці стеганаліз використовується для вивчення цифрових злочинів шляхом аналізу цифрових носіїв на наявність прихованої інформації, наприклад, у файлах підозрюваних. У військовій справі його метою є розпізнавання та розшифровка інформації, яка повинна зберігатися в таємниці, за допомогою підземних засобів [19,20].

Однак еволюція стеганографічних методів створила значну перешкоду для розвитку стеганалізу. З кожним роком складність алгоритмів приховування зростає, що призводить до складного завдання розпізнавання прихованої інформації. Крім того, велика кількість цифрових даних та обмежені ресурси змушують дослідників шукати компроміс між точністю виявлення та ефективністю алгоритму [19,20].

Як наслідок, стегааналіз має вирішальне значення для сучасної інформаційної безпеки, яка покликана протидіяти приховуванню інформації. Його розвиток вимагає міждисциплінарного підходу, що включає математику, інформатику, інформатику та теорію сигналів, а також модифікації існуючих методів та технічні вдосконалення стеганографії [19,20].

2.7 Типові сценарії

Будь-яке знання про стеганографічний канал, яке має відправник до атаки, може полегшити проведення атаки. Нагадаємо, що стеганографічний канал складається з п'яти основних компонентів [19,20,21]:

канал, що використовується для передачі інформації між учасниками комунікації,

створювач обкладинки,

походження повідомлень,

методи кодування та декодування даних,

джерело стегоключа, яке керує алгоритмами, що використовуються для вбудовування або вилучення даних.

Ми припускаємо, що спостерігач пасивний, що означає, що він просто спостерігає за розмовою, не беручи в ній безпосередньої участі. Як результат, фізичний канал, який використовується для комунікації, є без втрат і не впливає на аспекти секретності чи інтриги. Однак інші чотири елементи – алгоритм вбудовування та джерела обкладинок, повідомлень та стегоключів – є критично важливими. Загалом, чим більше знань отримано, тим успішніше розпізнати наявність таємно прихованих повідомлень. Хоча, безсумнівно, існують різні сценарії з різним рівнем деталізації, до яких спостерігач може отримати доступ щодо окремих компонентів стеганографічного каналу, два поширені сценарії - це моніторинг трафіку та аналіз викраденого комп'ютера [19,20,21].

Комп'ютеризований пристрій виявлення трафіку - це алгоритм, який вивчає кожну фотографію, що проходить через певний мережевий компонент. Прикладом може бути програма, яка перевіряє кожну фотографію, опубліковану в бінарній групі новин, або програма, яка контролює весь трафік за певною інтернет-адресою. У цьому випадку спостерігач обмежений інформацією щодо походження висвітлення, відправника повідомлень або стану системи. Це найскладніша ситуація, в якій принцип Керкгофа частково порушується. Як результат, спостерігач повинен мати стеганалітичні можливості, які можуть розпізнавати максимально можливу різноманітність стеганографічних методів [19,20,21].

Якщо спектр сторін, залучених до стеганографії, обмежений додатковою інформацією, різноманітність джерела висвітлення може бути зменшена, що призведе до кращого шансу спостерігача розпізнати будь-яку стеганографічну активність. Наприклад, коли керівник вже розпізнає, що хтось використовує стеганографію, можна отримати додаткову інформацію, яка допоможе зрозуміти

походження обкладинки або методу стеганографії. Якщо, наприклад, відправник використовує стеганографічний метод під час спостереження, керівник вже має інформацію про вбудовування методу, а також стегоключ простору. Або ж, якщо ми знаємо, що передається зображення, записане камерою, ми можемо придбати аналогічну камеру та змінити наш підхід на основі записаного зображення. Стеганографічну процедуру можна значно спростити, коли комп'ютер підозрюваного видалено, а завдання спостереження виконує керівник. У цьому випадку стеганографічний метод може залишатися на комп'ютері або його залишки можуть бути відновлені навіть після вилучення (наприклад, за допомогою веб-сайту Gargoyle's від Wetstone). Це надає важливі початкові дані про потенційний стегоканал. У деяких випадках спостерігач може розпізнати кілька версій одного й того ж зображення, які є по суті ідентичними. Спочатку можна оцінити, чи є ці різні версії результатом стеганографії чи іншого природного процесу, такого як стиснення одного й того ж зображення за допомогою двох різних компресорів JPEG. Порівнюючи зображення, можна зробити висновок про природу змін у просторі та їх конкретне розташування (канал зв'язку), і можна вважати, що зміни спричинені приховуванням секретного повідомлення. Як тільки спостерігач визнає, що відбувається стеганографія, процес завершено, і можна перейти до формального стеганологічного аналізу, метою якого є вилучення секретного повідомлення, або ж можна вирішити перервати канал зв'язку, якщо це є частиною експертизи [19,20,21].

2.11.1 Статистичний стегоаналіз

Інформаційно-теоретичне визначення стеганографічної безпеки починається з припущення, що джерело покриття розподілене по простору P_c всіх можливих покриттів C. Значення P_c (B) = $\int P_c(x)$ = — це ймовірність вибору покриття x ∈ B ⊂ C для приховування повідомлення. Припустимо, що певна стегасистема використовує покриття x ∈ C на вході, де x P_c подібний, але не такий самий, як

стегаключі та повідомлення (обидва з яких приймають значення у відповідних наборах згідно з розподілом), тоді розподіл стегазображень буде [19,20,21] .

2.11.2 Стеганоаналіз як проблема виявлення

Якщо спостерігач може зібрати достатню кількість прихованих зображень та обчислити ймовірність PDF-функції. Якщо ми можемо зрозуміти секретні закономірності, які дозволяють нам вивести PDF-функцію, або навчитися відрізняти її від стеганографії за допомогою інструментів машинного навчання, ми маємо проблему стеганалітичного аналізу, яка пов'язана з виявленням відомої стегосистеми, це проблема виявлення, яка призводить до простої перевірки гіпотез [19,20,21].

$$H_0 : x \sim P_c \qquad (2.86)$$

$$H_1 : x \sim P_s \qquad (2.87)$$

Оптимальним детектором для цієї задачі є детектор Неймана-Пірсона, який виводиться за допомогою тесту на відношення правдоподібності.

Якщо спостерігач не знає про стеганографічну систему, виникає проблема стеганоаналізу [19,20,21].

$$H : x \sim P_c \qquad (2.88)$$

що є складною проблемою перевірки гіпотез і зазвичай набагато складніша.

Очевидно, що існують інші підходи, розташовані між цими двома твердженнями, залежно від знання стеганографічного каналу, яким він володіє. Наприклад, якщо спостерігач знає про алгоритм, вбудований у повідомлення, але не про джерело повідомлення, то невідомий параметр β залежатиме від швидкості змін, і спостерігач повинен буде мати справу зі складною проблемою з одного боку, яка перевіряє гіпотезу одного боку [19,20,21].

Можна використовувати відповідні методи, такі як узагальнений тест правдоподібності, або перетворити це питання на просту проблему перевірки гіпотез, припустивши, що β є випадковою величиною, і розглядаючи її як таку (байєсівський підхід) [19,20,21].

2.11.3 Моделювання зображень за допомогою ознак

Практичний стеганографічний аналіз мультимедійних об'єктів, таких як зображення з цифрових сховищ, не може використовувати повне представлення зображень через їхню складність та розмір. Натомість потрібна простіша модель, яка полегшує задачу виявлення. Моделі, що використовуються в стеганографії, зазвичай отримують із зображень за допомогою набору числових атрибутів. Кожне зображення, x ∈ C, перетворюється на вектор ознак у d-вимірному просторі f = ((x), ... , де кожне : C → R. Випадкові величини, що представляють розташування покриття, повинні бути вибрані так, щоб мінімізувати відстань між кластерами f(x) та f(y). Далі, x ∼ , а стеганограми y ∈ перетворюються на випадкові величини f(x) ∼ та f(y) ∼ на . Для точного виявлення ознак ознака повинна бути вибрана таким чином, щоб кластери f(x) та f(y) були якомога несхожішими [19,20,21].

Налаштовані детектори

Будь-який алгоритм стеганалізу - це детектор, який описується функцією відображення F:→{0,1}, де F(x) = 0 означає, що x вважається покриттям, а F(x) = 1 означає, що x вважається стего. Множина = {x ∈ | F(x) = 1} називається критичною областю, оскільки детектор розглядатиме позицію лише як "стего". якщо x ∈ . Критична область є вичерпною в описі детектора [19,20,21].

Детектор може неправильно інтерпретувати два типи ситуацій: хибні тривоги та пропущені виявлення. Ймовірність хибної тривоги, або помилки виявлення, називається ймовірністю хибної тривоги, а ймовірність пропущеного виявлення називається ймовірністю пропущеного виявлення [19,20,21].

$$P_{FA} = \Pr\{F(x) = 1 | x \sim p_c\} = \int_{R_1} p_c(x)dx \qquad (2.89)$$

$$P_{MD} = \Pr\{F(x) = 0 | x \sim p_s\} = 1 - \int_{R_1} p_s(x)dx \qquad (2.90)$$

Ймовірності помилок будь-якого детектора повинні задовольняти таку нерівність [19,20,21]:

$$(1 - P_{FA}) \log \frac{1 - P_{FA}}{P_{MD}} + P_{FA} \frac{P_{FA}}{1 - P_{MD}} \leq D_{KL}(P_c || P_s) \qquad (2.91)$$

де DKL — це дивергенція Кульбака-Лейблера між двома ймовірнісними розподілами [19,20,21].

Для ефективної стеганографії значення (||) дорівнює 0, і єдиний детектор, який може створити спостерігач, – це випадкове припущення між обкладинкою та стего, це означає, що спостерігач не може створити вразливість. Для безпечних стегосистем, які мають рівень достовірності щонайменше є, ймовірність виявлення зменшується зі зниженням рівня достовірності. У стеганографії ефективні детектори повинні мати низький рівень хибних спрацьовувань. Це важливо, оскільки зображення, які вважаються такими, що можуть містити секретну інформацію, зазвичай піддаються додатковому аналізу, який ідентифікує стеганографічну програму, стего-ключ та секретне повідомлення. Це може вимагати використання словника методом перебору, що може бути як дорогим, так і трудомістким [19,20,21]. Як результат, детектор з низькою ймовірністю помилки, незважаючи на високу ймовірність промаху (наприклад, 0,5 або вище), є більш значущим. Оскільки стеганографічний зв'язок зазвичай повторюється, навіть детектор з a = 0,5 все ще відіграє значну роль, якщо його ймовірність хибного виявлення мала. Гіпотетична проблема в стеганалізі в першу чергу вирішується за допомогою парадигми Неймана-Пірсона [19,20,21]. Мета полягає у

створенні детектора з найвищою ймовірністю виявлення = 1 − , а також обмеженням на ймовірність хибнопозитивних результатів, ≤ . Незважаючи на потенційні витрати, пов'язані з обома типами помилок, байєсівські детектори зазвичай не використовуються в стеганалізі, оскільки ймовірність виявлення зображення покриття або стегозображення рідко оцінюється точно [19,20,21].

Через обмеження частоти хибнопозитивних результатів 0,05 оптимальним детектором Неймана-Пірсона є тест на відношення правдоподібності.

Навіть якщо спостерігач теоретично може створити оптимальні алгоритми стеганалізу, оцінюючи ймовірність зображень покриття та стегозображень, це буде можливо лише для низьковимірних моделей, які неадекватно описують покриття. Оскільки розмірність простору ознак часто висока, це особливо стосується сліпого стеганалізу, який часто неможливо точно оцінити. Натомість, проблема виявлення вважається проблемою класифікації (розпізнавання образів) і вирішується шляхом навчання класифікатора на великій базі даних зображень покриття та steg-зображень. Параметри класифікатора зазвичай змінюються для зниження рівня хибнопозитивних результатів [19,20,21].

2.9 Висновок до другого розділу

У цьому розділі розглянуто ключові принципи стеганографії в контексті цифрових зображень, які є основною формою носіїв, що використовуються для приховування інформації. Аналіз форматів цифрових зображень призвів до виявлення їхніх властивостей та обмежень, що впливають на вибір методів стеганографії. Зокрема, формати JPEG та BMP мають різні властивості, що впливають на здатність приховувати інформацію, яка вже була стиснута, що розглядається як функція колірної моделі, розміру файлу та методу стиснення.

Стеганографічний канал, як основа для прихованого обміну інформацією, був досліджений з точки зору його структури та функції. Цей канал передає дані непомітно, не привертаючи до них уваги спостерігачів, які знаходяться поза каналом. У цифровому контексті це передбачає використання як структурних

властивостей файлу, так і психологічних компонентів візуального сприйняття людини.

Методи стеганографії, розглянуті в цьому розділі, включають як прості методи, такі як зміна LSB, так і більш складні алгоритми, що використовують частотний аналіз та змінюють коефіцієнти DCT (дискретне косинусне перетворення). Кожен метод має переваги та недоліки, залежно від необхідного ступеня стабільності, рівня невідомості даних та типу носія. Увага була приділена процесу стеганалізу, який є протилежністю стеганографії. Були розглянуті його основні підходи, включаючи статистичну оцінку, аналіз сигнатур та використання машинного навчання. Важливо розрізняти стегааналіз на сліпий, який не має доступу до оригінального носія або знання методу приховування, та несліпий, який базується на порівнянні з відомим оригіналом. Як результат, розглянуті формати зображень, методи стеганографії та принципи стеганалізу сприяють всебічному розумінню принципів прихованої комунікації.

РОЗДІЛ 3.
ПРАКТИЧНА РЕАЛІЗАЦІЯ КОМБІНОВАНОГО ЗАХИСТУ КОНФІДЕНЦІЙНИХ ДАНИХ З ВИКОРИСТАННЯМ СТЕГАНОГРАФІЇ ТА КРИПТОГРАФІЇ

3.1 Використані інструменти та технології

3.1.1 Python

Python — це високоякісна мова програмування загального призначення, відома своєю зрозумілістю та легкістю навчання. Python підтримує кілька моделей програмування, включаючи об'єктно-орієнтоване, процедурне та функціональне програмування. Ключові переваги Python:

• Елегантність та складність: Ефективний синтаксис, який легко зрозуміти та написати.

• Стандартна багата бібліотека: Велика кількість бібліотек, багатих на засоби маніпулювання даними, веб-розробки, автоматизації, наукових обчислень тощо.

• Багатомовність: Може працювати на різних платформах, включаючи Windows, macOS та Linux.

• Велика спільнота: Багато ресурсів для навчання, документації та допомоги.

Python часто використовується у веб-розробці, автоматизації, аналізі даних, машинному навчанні та інших галузях [22,23,24].

3.1.2 Django

Django — це передова веб-платформа для створення веб-додатків на Python. Вона сприяє швидкому зростанню та гігієнічному, практичному дизайну, а також надає набір ресурсів та бібліотек для створення веб-сайтів. Основні атрибути Django [22,23,24]:

Швидкість розробки: Швидкість та ефективність Django у створенні веб-додатків пояснюються великою кількістю вбудованих функцій [22,23,24].

• Безпека: Включає захист від найпоширеніших веб-загроз, таких як SQL-ін'єкції, XSS, CSRF.

• Портативність: Чудово підходить для проектів, які мають велику кількість компонентів та потребують портативного виконання.

• Панель адміністратора: вбудована панель адміністратора для управління контентом, яка не потребує додаткових налаштувань.

• Відкритий код: Велика спільнота, яка просуває та вдосконалює платформу.

Django часто використовується для створення складних веб-додатків, таких як соціальні мережі, системи управління контентом (CMS), електронна комерція та інші платформи [22,23,24].

HTML та CSS в основному використовуються для створення та стилізації веб-сторінок.

HTML [22,23,24]:

• Структура веб-сторінки: HTML використовується для створення композиції веб-сторінок за допомогою тегів (наприклад, , <p>, <a>, img>).

• Текстовий вміст: Це те, що визначається заголовками, абзацами, списками, посиланнями та іншими текстовими компонентами.

• Багатомовність: Поєднання розмовної та писемної мови.

3.1.3 Комбінація HTML та CSS:

Разом HTML та CSS є фундаментальними компонентами веб-розробки, що дозволяє створювати красиві та функціональні веб-сторінки. Визначення структури та контенту в HTML відповідає за дизайн та макет, тоді як CSS в першу чергу відповідає за візуальний вигляд [22,23,24].

Ці технології зазвичай використовуються як для створення простих веб-сайтів, так і для складних веб-додатків [22,23,24].

3.1.4 SQL

SQL – це поширена мова для керування реляційними базами даних та доступу до них. Її метою є виконання різних дій з даними в базах даних,

включаючи зберігання, оновлення, видалення та отримання інформації. Основні цілі SQL [22,23,24]:

Запити до бази даних: Використовуйте оператор SELECT для збору інформації з таблиць.

Оновлення даних: Використовуйте INSERT, UPDATE та DELETE для додавання, зміни та видалення даних.

Керування структурами даних: Використовуйте CREATE, ALTER та DROP для створення, зміни та видалення таблиць та інших компонентів бази даних.

• Контроль доступу: Використовуйте GRANT та REVOKE для надання або заборони доступу до інформації.

SQL часто використовується в управлінні інформаційними системами баз даних (СУБД), такими як MySQL, PostgreSQL, SQLite та Oracle. Також використовуються інші програмні додатки, які використовуються для керування інформацією про базу даних. Його гнучкість та потужність роблять SQL фундаментальним інструментом для роботи з даними в різних дисциплінах, включаючи веб-розробку, аналіз даних, бізнес-аналітику та інш [22,23,24].

3.1.5 AES-256 Encryption

AES-256 – це симетричний криптографічний алгоритм, який використовується для захисту даних. AES-256 є частиною стандарту AES, який також включає AES-128 та AES-192, і має різну довжину ключа. Ключові аспекти AES-256: [22,23,24]

1. Симетричне шифрування [22,23,24]

• Симетричний ключ: Для шифрування та розшифрування інформації використовується один і той самий ключ, що означає, що і відправник, і одержувач повинні мати доступ до цього секретного ключа.

• Безпека ключа: Ключ довжиною 256 біт забезпечує високий ступінь захисту від цифрового криптоаналізу.

2. Склад алгоритму [22,23,24]

• Блочне шифрування: Використовує блок даних фіксованого розміру (128 бітів).

• Підпроцеси шифрування: AES-256 має 14 раундів шифрування, кожен з яких має кілька кроків (SubBytes, ShiftRows, MixColumns, AddRoundKey).

3. Застосування [22,23,24]

• Шифрування даних: Використовується для захисту конфіденційної інформації, такої як фінансові транзакції, дані користувачів та урядові документи.

• Надійні з'єднання: Використовується в протоколах безпеки, таких як TLS/SSL, які гарантують безпеку інтернет-з'єднань.

• Захист даних у стані спокою: Зазвичай використовується в системах зберігання даних, що використовують шифрування диска (наприклад, BitLocker).

4. Переваги AES-256 перелічені нижче [22,23,24].

Стійкість до атак: Висока стійкість до різних типів криптографічних атак, включаючи атаки методом грубої сили.

Продуктивність: Обробка даних ефективна завдяки оптимізованим алгоритмам.

3.1.6 Least Significant Bit (LSB) Steganography

Найменш значущий біт (LSB) – це метод стеганографії, який використовується для приховування інформації в мультимедійних файлах, таких як зображення, аудіо та відео. Фундаментальний принцип LSB-стеганографії полягає в приховуванні секретних повідомлень у найменш значущих бітах візуальних або слухових зразків, які майже непомітні для людського вуха чи ока [22,23,24].

1. Як функціонує LSB-стеганографія

У кольорових зображеннях кожен піксель складається з трьох байтів (RGB – червоний, зелений, синій). Найменш значущий біт (LSB) кожного байта перетворюється для зберігання секретного біта інформації [22,23,24].

• Зміни значень: Оскільки найменш значущий біт має незначний вплив на колір пікселя, ці зміни майже непомітні.

• Вторгнення даних: Секретне повідомлення перетворюється на байтовий рядок, який вбудований у найменш значущий біт кожного байта зображення чи аудіо.

2. Зразок за психологічною шкалою [22,23,24]

• Перший байт: 10101010

• Зворотний байт: 10101010 (останній біт замінюється першим бітом)

У цьому випадку останній біт змінюється, але це в першу чергу впливає на колірне відображення або звук, інформація все одно зберігається.

3. Застосування [22,23,24]

• Захист даних: Використовується для приховування конфіденційної інформації у візуальній або звуковій формі.

• Цифрові водяні знаки: Вони використовуються для захисту авторських прав за допомогою цифрових водяних знаків.

• Безпека зв'язку: Контроль за прихованою передачею інформації між користувачами.

5. Переваги та недоліки [22,23,24]

Переваги:

Легкість реалізації.

• Обман системи шляхом внесення невеликих змін до файлу без суттєвої зміни оригіналу.

Використання криптовалюти для захисту авторських прав та прихованого обміну інформацією.

Недоліки [22,23,24]:

• Обмежена кількість даних, які можна приховати.

Вразливість до атак, які змінюють файл.

Поєднання методу шифрування AES-256 та LSB-стеганографії – це потужний метод захисту даних, який пропонує два різні рівні захисту:

шифрування даних та приховування даних. Це забезпечує додатковий захист конфіденційної інформації, особливо під час передачі по незахищених каналах.

Чи можете ви повторити відповідь, розширити її, видалити код або, можливо, додати розрахунки, які демонструють переваги цієї комбінації?

Теоретичні комбінації AES-256 зі LSB-стеганографією [22,23,24]

Поєднання методу шифрування AES-256 та LSB-стеганографії – це потужний метод захисту даних, який пропонує два різні рівні захисту: шифрування даних та приховування даних. Це забезпечує додатковий захист конфіденційної інформації, особливо під час передачі по незахищених каналах [22,23,24].

1. Теоретичні основи AES-256 [22,23,24]

• AES-256 – це стандарт розширеного шифрування, який використовує 256-бітний ключ. Цей алгоритм є частиною стандартного протоколу AES, який також включає 128-бітну та 192-бітну версії. Унікальні особливості AES-256:

• Високий захист: 256-бітної довжини ключа достатньо для протистояння атакам методом перебору, оскільки кількість можливих комбінацій становить 22562^{256}, що практично неможливо передбачити.

• Блочне шифрування: AES базується на блоках даних по 128 бітів, що забезпечує ефективну обробку великих обсягів інформації.

Ефективність та швидкість: Алгоритми шифрування, оптимізовані для ефективності.

2. Теоретичні основи LSB-стеганографії [22,23,24]

LSB-стеганографія – це метод приховування даних у мультимедійних файлах, таких як зображення чи аудіо, шляхом зміни найменш значущих бітів кожного пікселя чи семплу. Ключові особливості LSB-стеганографії включають:

• Невеликі зміни: Незначна зміна у файлі, незначна для людського вуха чи ока, матиме мінімальний вплив на оригінальний файл.

• Виведення даних: Секретне повідомлення перетворюється на байт, який знаходиться або в найменш значущому бітах пікселя, або в байті аудіосемплу, після чого ця інформація приховується.

3. Переваги комбінованого методу [22,23,24].

Захист від проникнення насильницьких сил

• Шифрування AES-256 ефективне проти атак методом грубої сили завдяки великій кількості можливих комбінацій ключів. Кількість можливих комбінацій розраховується як 22562^{256}, що приблизно дорівнює 1,16×10771,16 \times 10^{77} варіантів. Для порівняння, з поточною обчислювальною потужністю, для дослідження всіх можливих ключів знадобляться мільйони років.

Прихованість та приховування [22,23,24]

• Стеганографія LSB дозволяє приховувати зашифроване повідомлення у звичайних файлах, таких як зображення, що зменшує ймовірність розпізнавання секретного повідомлення. Зміна лише найменш значущого біта має незначний вплив на оригінальний файл, який нелегко виявити без спеціальних інструментів.

4. Знижки та переваги розрахунку [22,23,24]

Обсяг даних

• AES-256 кодує дані в блоки по 128 бітів. Якщо взяти файл розміром 1 МБ (8 388 608 біт), після шифрування розмір файлу залишиться таким самим, але вміст буде повністю зашифрований.

Ефективність виведення

• LSB-стеганографія може приховати значну кількість інформації у файлах. Наприклад, зображення розміром 800x600 з 4-канальними пікселями має 480 000 пікселів або 1 440 000 байт (RGB). Використовуючи 1 байт на піксель, ми можемо приховати до 180 000 байт (приблизно 176 КБ). даних на цьому зображенні: цього достатньо, щоб приховати зашифроване повідомлення.

3.2 Демонстрація розробленого рішення.

Для вдосконалення програми було створено невеликий демонстраційний модуль онлайн-банкінгу, який зберігає інформацію про клієнтів. Цей модуль поєднаний з криптографічними та стеганографічними методами для збереження даних. Послідовність дій продемонстровано нижче [22,23,24].

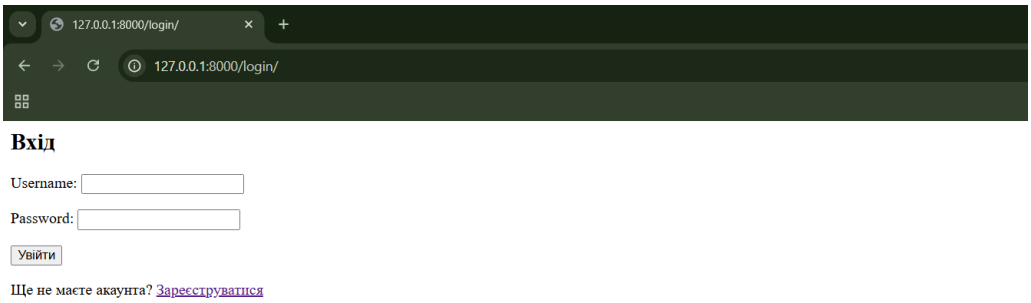


Рис. 3.1 – початкова форма авторизації

На початку роботи над модулем клієнту відображається екран авторизації (рис. 3.1), який він може використовувати як для її створення, так і для реалізації процесу реєстрації [22,23,24]

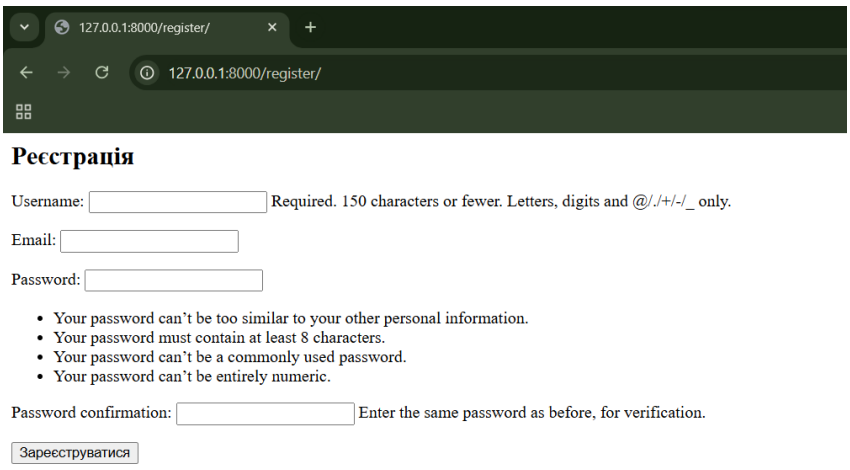


Рис. 3.2 – форма реєстрації

На початку роботи над модулем клієнту відображається екран авторизації (рис. 3.1), який він може використовувати як для її створення, так і для реалізації процесу реєстрації [22,23,24].

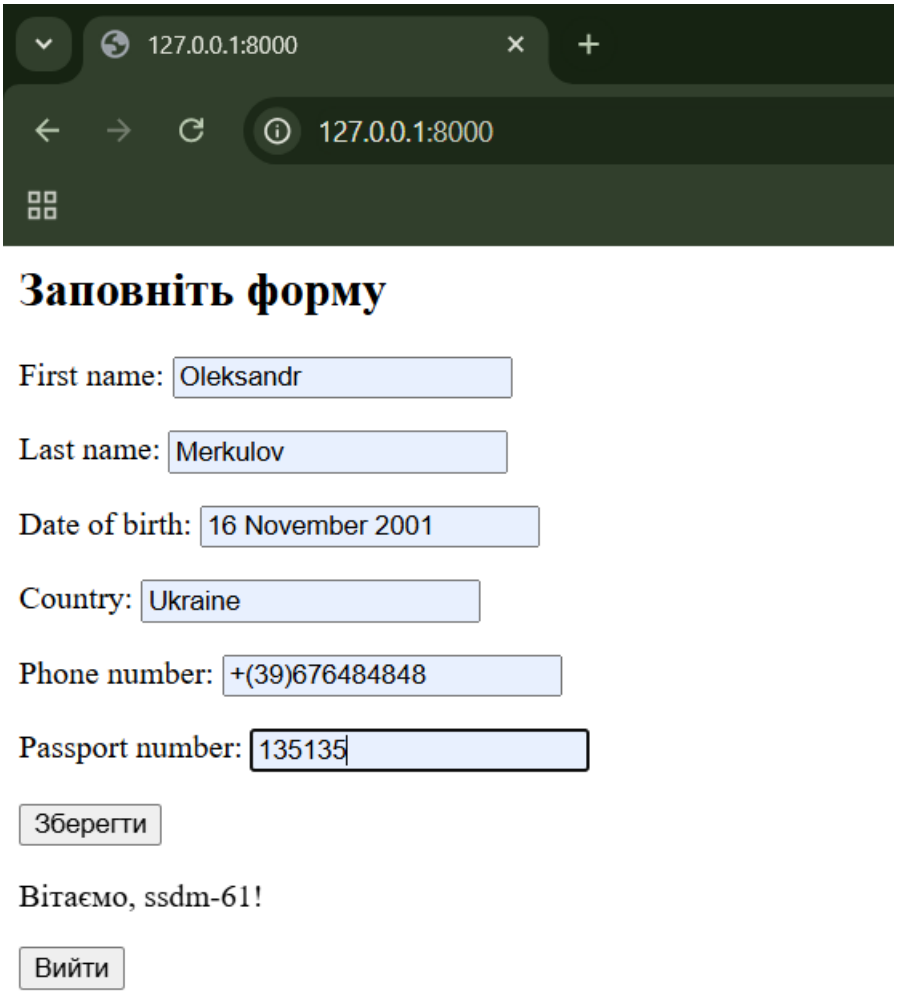


Рис. 3.3 - Форма з банківськими даними

На рисунку 3.3 показано інший підхід, який передбачає дані, спеціально додані до банківської системи. Теоретично, будь-яку інформацію можна включити до форми, але для цієї демонстрації включено основні дані, необхідні для отримання банківської картки [22,23,24].

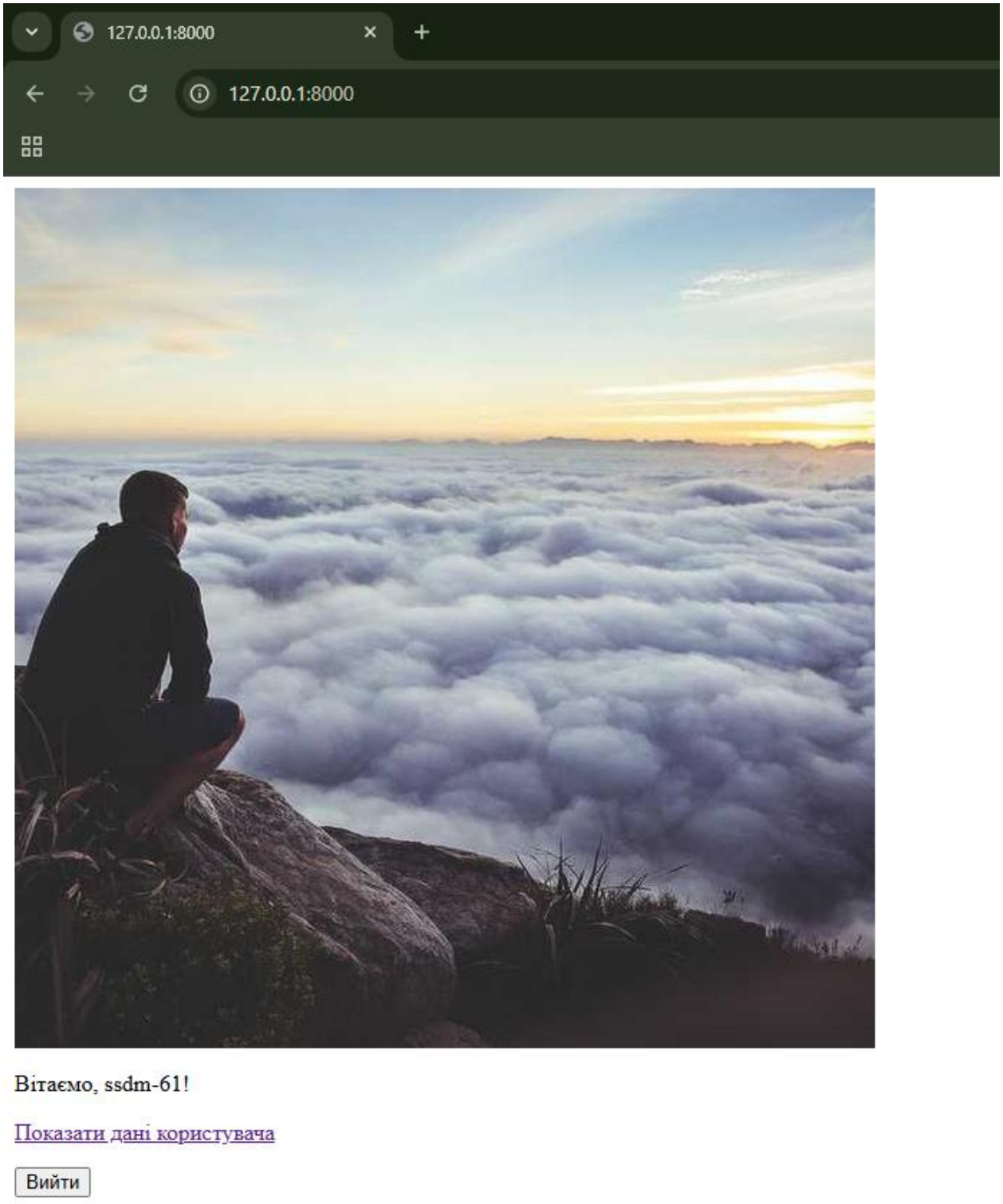


Рис. 3.4 – зображення з конфіденційними даними користувача

Спочатку Рисунок 3.4 може здатися дивним, але так воно і має бути. Після того, як користувач введе свої дані та натисне кнопку «Зберегти», система зашифрує їх за допомогою алгоритму AES-256. Після шифрування дані будуть

оброблені за допомогою методу LSB, який змінить біти фотографії та приховає повідомлення у випадково згенерованій фотографії, що показано на Рисунку 3.4 [22,23,24].

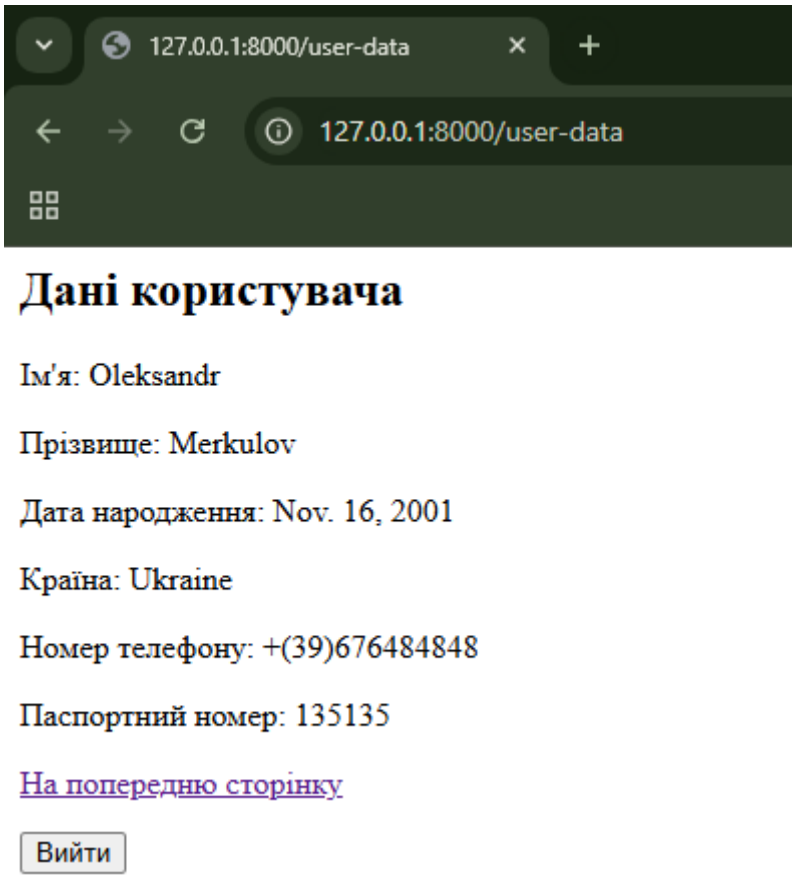


Рис. 3.5 - збережені дані користувача

На рисунку 3.5. показано збережені дані про користувача банку, загалом ця функціональність не є необхідною, але для демонстрації того, що конкретні дані зберігаються в цілому, можна отримати до них доступ на платформі. Процес їх відображення виглядає наступним чином: після запиту до системи вона знаходить раніше збережені фотографії з інформацією про користувача, витягує їх, потім виконується розшифрування та представлення на екрані [22,23,24].

3.3 Висновок до третього розділу.

У цьому розділі описано практичний проект, який демонструє метод зберігання клієнтських даних про банки за допомогою розробленого модуля Django.

Розроблений модуль складається з кількох частин. По-перше, персональні дані клієнта захищені AES-256, що є сучасним стандартом інформаційної безпеки, що використовує стійку до злому симетричну криптосистему. Далі, отримана зашифрована інформація приховується у випадково згенерованому зображенні за допомогою методу LSB. Цей метод робить інформацію повністю незрозумілою для тих, хто не має на це права. Цей метод виграє від поєднання криптографії, яка захищає вміст даних, та стеганографії, яка маскує сам факт їхньої наявності.

Поєднання AES-256 та LSB суттєво впливає на загальний ступінь захисту. Навіть якщо зображення отримано від неавторизованої особи, без відповідного ключа AES зловмисник не зможе розшифрувати приховану інформацію. Цей метод підвищує безпеку системи, створюючи багаторівневу систему безпеки, яка зменшує ймовірність доступу до конфіденційної інформації без авторизації.

Результати практичного застосування модуля демонструють цінність обраного методу. Використання Django сприяло легкій інтеграції модуля у веб-додаток, крім того, забезпечило підтримку для розвитку та простоту використання. Розроблений метод може бути застосований в інших сферах з високим ступенем конфіденційності.

В результаті, практичний міні-проект у цьому розділі демонструє, що поєднання шифрування AES-256 зі стеганографією на основі LSB є життєздатним рішенням для захисту конфіденційних даних, яке відповідає сучасним нормам інформаційної безпеки.

ВИСНОВКИ

Магістерська робота на подану тему досліджує актуальну проблему забезпечення конфіденційності даних у сучасному цифровому середовищі. У роботі розглянуто теоретичні аспекти стеганографії, історичний розвиток цієї галузі, сучасні технології приховування інформації, а також виконано практичну реалізацію удосконаленої системи захисту даних.

1. У першому розділі було детально проаналізовано основи стеганографії, її історію, сучасні підходи та типи, а також її значення для кібербезпеки. Показано, що стеганографія відіграє важливу роль у захисті інформації, забезпечуючи прихованість даних на додаток до традиційного шифрування. Водночас наголошено на необхідності розвитку стегоаналізу як інструменту протидії зловживанням стеганографією у злочинних цілях.

2. Другий розділ був присвячений аналізу технічних аспектів роботи стеганографічних систем, включаючи формати цифрових зображень, функціонування стеганографічного каналу та сучасні методи приховування даних. Також розглянуто стегоаналіз як процес виявлення прихованої інформації, зокрема його види: сліпий та не сліпий аналіз. Комплексний підхід до вивчення цих процесів дозволив сформувати розуміння ключових технологічних викликів у цій галузі.

3. У третьому розділі було розроблено практичний Django-модуль для захисту даних клієнтів банку. У ньому реалізовано поєднання двох ключових методів: шифрування AES-256 для захисту змісту даних і стеганографічного приховування за допомогою LSB у випадково згенерованих зображеннях. Це забезпечило багаторівневий підхід до захисту: навіть у разі компрометації стеганографічного носія без ключа AES розшифрувати дані неможливо. Експериментальні результати підтвердили ефективність такого підходу для забезпечення високого рівня конфіденційності.

4. Отримані результати підкреслюють, що стеганографія у поєднанні з криптографічними методами має великий потенціал для вдосконалення систем

захисту інформації. Розроблена система демонструє практичну цінність для застосування у банківському секторі, державних структурах та інших галузях, де безпека даних є критично важливою.

5. Таким чином, ця магістерська робота зробила внесок у розвиток теорії та практики стеганографії, запропонувавши сучасні підходи до захисту даних, що відповідають викликам сучасного інформаційного простору. Подальше дослідження цієї теми може зосередитися на підвищенні стійкості стеганографічних методів до новітніх технологій стегоаналізу, а також інтеграції їх у масштабовані інформаційні системи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конахович Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А. Ю. Пузиренко. - Київ: МК-Пресс, 2006. – 288с.

2. Кузнецов О. О. Стеганографія: навчальний посібник / О.О.Кузнецов, С. П. Євсеєв, О. Г. Король. - Х.: Вид. ХНЕУ, 2011. - 232с.

3. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. 2-е изд. / Рябко Б. Я., Фионов А. Н. // М.: Горячая линия - Телеком, 2013. 232 с.

4. Кінзерявий О.М. Стеганографічні методи приховування даних увекторні зображення, стійкі до активних атак на основі афінних перетворень / О.М. Кінзерявий // Київ – 2015, 324 с.

5. Вовк О.О. Методи підвищення стійкості та пропускної здатності систем прихованої передачі інформації / Вовк О.О. – Харків, 2016 – 177с.

6. Грибунин В. Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-Пресс, 2002. – 272 с.

7. Худьо В.Д., Моделювання стійкої стегофонічної системи із заданими характеристиками мережі / В.Д. Худьо // Тернопіль – 2017. – 98с.

8. Юдін О.К., Конахович Г.Ф., Корченко О.Г. Захист інформації в мережах передачі даних: Підручник. К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009, 716 с.

9. Fidrich J. Steganography in Digital Media: Principles, Algorithms, and Applications / J. Fidrich. – Cambridge: Cambride University Press, 2009. – 438 p.

10. 34. Kutter M. A fair benchmark for image watermarking systems / M. Kutter, F. Petitcolas // Proc. of SPIE: Security and Watermarking of Multimedia Contents. − San Jose, France, 1999. – vol. 3657 − P. 226 – 239.

11. Кінзерявий О.М. Стеганографічні методи приховування даних у векторні зображення, стійкі до активних атак на основі афінних перетворень / О.М. Кінзерявий // Київ – 2015, 324 с.

12. Лагун А. Використання вейвлет-перетворення для приховування інформації в нерухомих зображеннях / А. Лагун, І. Лагун // Захист інформації і безпека інформаційних систем. – Л., 2013. – С. 98 – 99.

13. Горніцька Д.А. Визначення коефіцієнтів важливості для експертного оцінювання у галузі інформаційної безпеки / Д.А. Горніцька, О.Г. Корченко, В.В. Волянська // Захист інформації. – 2012. – №1. – С. 108 – 121.

14. Ó Ruanaidh J. Rotation, scale and translation invariant digital image watermarking / J. Ó Ruanaidh, T. Pun // Proc. of the ICIP'97. – California, 1997. – vol. 1, P. 536–539.

15. Семенко К.О. Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / К.О. Семенко, наук. кер. О.О. Вовк // 20-й Міжнародний молодіжний форум «Радіоелектроніка і молодь у XXI столітті». – Х.: ХНУРЕ, 2016. – т.4. – С. 167 – 168.

16. Вовк О. О. Визначення коефіцієнтів важливості для експертного оцінювання стеганографічних методів / О. О. Вовк // Науковий журнал «Телекомунікаційні та інформаційні технології». – Київ, 2015. – №3. – С. 70 – 80.

17. Вовк О.О. Розроблення методики оцінювання важливості характеристик стеганографічних алгоритмів / О.О. Вовк, А.А. Астраханцев // Вісник національного університету «Львівська політехніка» «Інформаційні системи та мережі». – Львів, 2014. – № 805. – С. 52 – 60.

18. Вовк О.О. Синтез стеганографічного методу передачі даних, ефективного за критеріями надійності та захищеності / О.О. Вовк, А.А. Астраханцев // Електронне наукове фахове видання ХНУРЕ «Проблеми телекомунікацій». – Харків, 2015. – № 1 (16). – С. 103 – 115.

19. Vovk O. Synthesis of optimal steganographic method meeting given criteria / O. Vovk, A. Astrahantsev // Informatyka Automatyka Pomiary w Gospodarce i Ochronie Środowiska (technical and scientific journal). – Lublin, Poland, 2015. – P. 27-34

20. Сейеди С.А. Сравнение методов стеганографии в изображениях / С.А. Сейеди, Р.Х. Садыхов // Информатика. – БГУИР, 2013. – С. 66 – 75.

21. Вовк О.О. Анализ атак на цифровые водяные знаки в видеофайлах и изображениях / О.О. Вовк наук. кер. А.А. Астраханцев // V Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». – Запоріжжя, ЗНТУ, 2010. – С. 88 – 90.

22. Тігулев М. Стеганография в GIF [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/128327.

23. Основи комп'ютерної графіки: навч. посіб. / В.С. Березовський, В.О. Потієнко, І.О. Завадський; за заг. ред. А.М. Гуржія. − К.: BHV, 2009. − 400 с.

24. Грачева Ю.А. Несколько слов о стеганографии – методе защиты графической информации от нарушения авторских прав / Ю.А. Грачева // Московский государственный университет печати. – С. 76 – 81.

25. Adnan M. Watermark re-synchronization using log-polar mapping of image autocorrelation / M. Adnan, J. Meyer // Digim

ДОДАТОК А

Оформлення слайдів та роздаткового матеріалу

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Кваліфікаційна робота здобувача освітнього ступеня «Магістр»

ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ, ЩО ПЕРЕДАЄТЬСЯ СТЕГАНОГРАФІЧНИМИ МЕТОДАМИ ЧЕРЕЗ МЕРЕЖЕВІ КАНАЛИ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Спеціальність: 125 - Кібербезпека та захист інформації

Виконав: Максим ОНИЩЕНКО

Керівник: д.т.н., професор Олександр ТУРОВСЬКИЙ

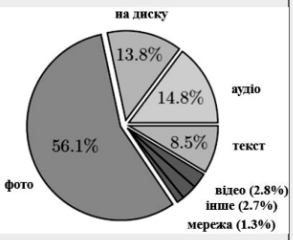
Київ - 2026

АКТУАЛЬНІСТЬ, МЕТА ТА НАУКОВІ ЗАВДАННЯ

- Актуальність визначається необхідністю захисту конфіденційних даних під час їх передавання мережевими каналами об'єкта інформаційної діяльності.
- Стеганографія дозволяє не лише захищати зміст повідомлення, а й приховувати сам факт його передавання.
- Мета роботи - удосконалити систему передачі конфіденційних даних стеганографічними методами.
- Завдання: дослідити методи стеганографічного захисту, проаналізувати загрози, розробити комбіноване стеганографічно-криптографічне рішення.

СТЕГАНОГРАФІЯ ЯК МЕТОД ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ

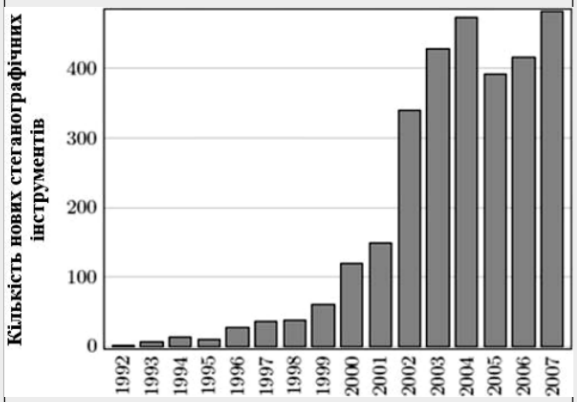
Тип носія	Кількість
Аудіо	445
Диск	416
Фото	1689
Мережа	39
Інше	81
Текст	255
Відео	86



- Стеганографія забезпечує приховану комунікацію шляхом вбудовування повідомлення у цифровий контейнер.
- Контейнерами можуть бути зображення, аудіо, відео, текстові документи або мережеві пакети.
- Ключова вимога - сторонній спостерігач не повинен відрізняти звичайний файл від файлу зі стеганографічним вкладенням.

РОЗВИТОК ІНСТРУМЕНТІВ СТЕГАНОГРАФІЇ ТА СУЧАСНІ РИЗИКИ

- Зростання кількості стеганографічних інструментів ускладнює контроль каналів передавання цифрових медіаданих.
- Стеганографія використовується як у легітимному захисті, так і у прихованих каналах кіберзлочинців.
- Для ОІД важливо поєднувати механізми стеганографії з криптографією та засобами виявлення прихованого трафіку.



ТИПИ СТЕГАНОГРАФІЇ ТА СФЕРИ ЇЇ ЗАСТОСУВАННЯ

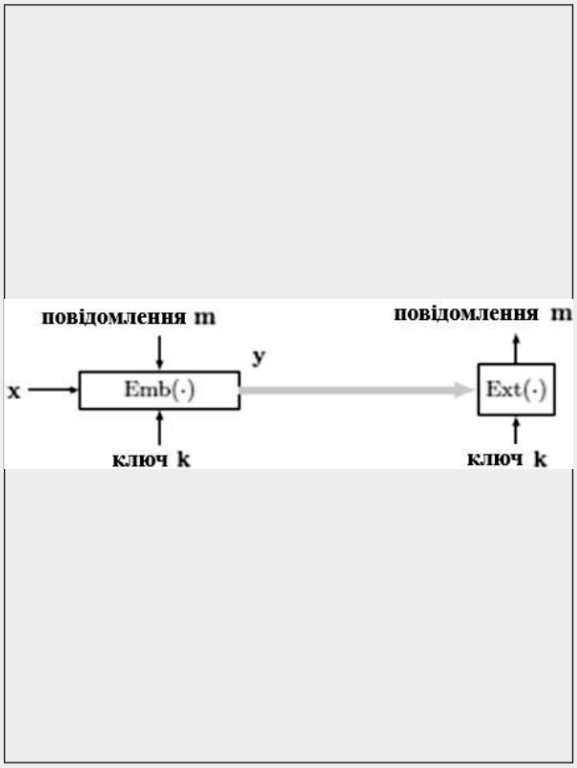
- Текстова стеганографія - приховування даних у структурі, форматуванні або символах тексту.
- Стеганографія в зображеннях - модифікація пікселів або частотних коефіцієнтів без видимих змін.
- Аудіо- та відеостеганографія - вбудовування повідомлень у малопомітні часові або частотні компоненти сигналу.
- Мережева стеганографія - приховане передавання даних у полях протоколів, синхронізації пакетів або службових ознаках трафіку.

СТЕГАНОГРАФІЧНИЙ КАНАЛ ПЕРЕДАЧІ ІНФОРМАЦІЇ

- Стеганографічний канал включає секретне повідомлення, контейнер, алгоритм вбудовування, ключ і канал передавання.
- Передавання має забезпечувати непомітність, достатню місткість і стійкість до спотворень або стискання.
- У роботі акцент зроблено на приховуванні інформації у цифрових зображеннях.

МЕТОДИ ПРИХОВУВАННЯ ДАНИХ У ЦИФРОВИХ ЗОБРАЖЕННЯХ

- У стеганографії зображень використовують модифікацію контейнера, синтез покриття та LSB-вбудовування.
- Метод LSB змінює найменш значущі біти пікселів, що майже не впливає на візуальне сприйняття.
- Недолік LSB - потенційна вразливість до статистичного стегоаналізу та повторного стискання.



LSB-ВБУДОВУВАННЯ ЯК БАЗОВИЙ МЕХАНІЗМ ЗАХИСТУ

Компонент захисту	Призначення
Контейнер	цифрове зображення, у якому змінюються молодші біти пікселів
Повідомлення	секретні дані, попередньо підготовлені до прихованого передавання
Молодший біт	розряд, зміна якого найменше впливає на візуальну якість зображення
Ключ/порядок	визначає послідовність розміщення бітів повідомлення в контейнері
Перевага	висока простота реалізації та непомітність для візуального контролю
Обмеження	потенційна вразливість до статистичного аналізу і повторного стискання

ПРИКЛАДИ КОНТЕЙНЕРІВ ТА ВІЗУАЛЬНА НЕПОМІТНІСТЬ ЗМІН

- У роботі наведено приклади контейнерів, у яких візуальна відмінність між оригіналом і стегооб’єктом є мінімальною.
- Наявність прихованої інформації не повинна змінювати семантику або зовнішній вигляд медіафайлу.
- Це створює додатковий рівень захисту під час передавання конфіденційної інформації мережею.

СТЕГОАНАЛІЗ ТА СТАТИСТИЧНЕ ВИЯВЛЕННЯ ПРИХОВАНИХ ДАНИХ

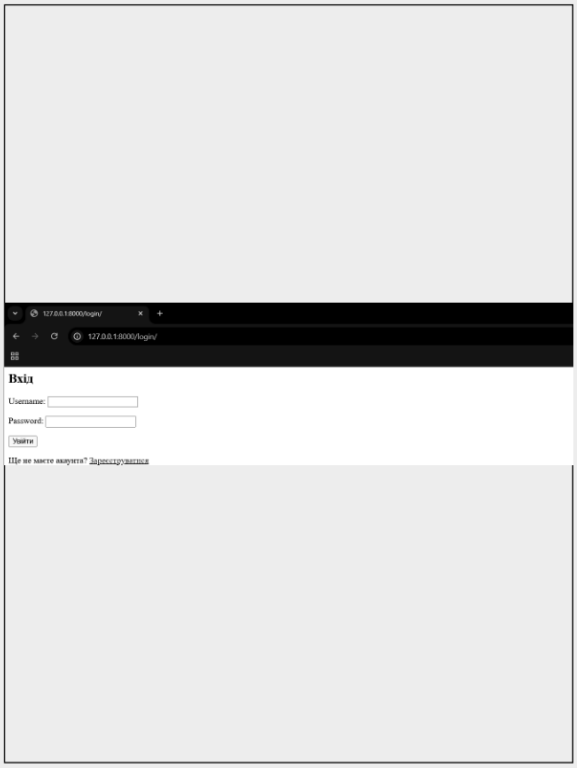
- Стегоаналіз спрямований на виявлення прихованої інформації за непрямими статистичними ознаками цифрового контейнера.
- Оцінюються гістограми, частотні характеристики, шумові компоненти, локальні артефакти та відхилення від природної структури зображення.
- Для LSB-методів характерними ознаками можуть бути зміни розподілу молодших бітів і статистичних залежностей між сусідніми пікселями.
- Практична стійкість методу визначається здатністю зберігати статистичну подібність до вихідного контейнера після вбудовування даних.

КОМБІНОВАНА МОДЕЛЬ СТЕГАНОГРАФІЧНО-КРИПТОГРАФІЧНОГО ЗАХИСТУ

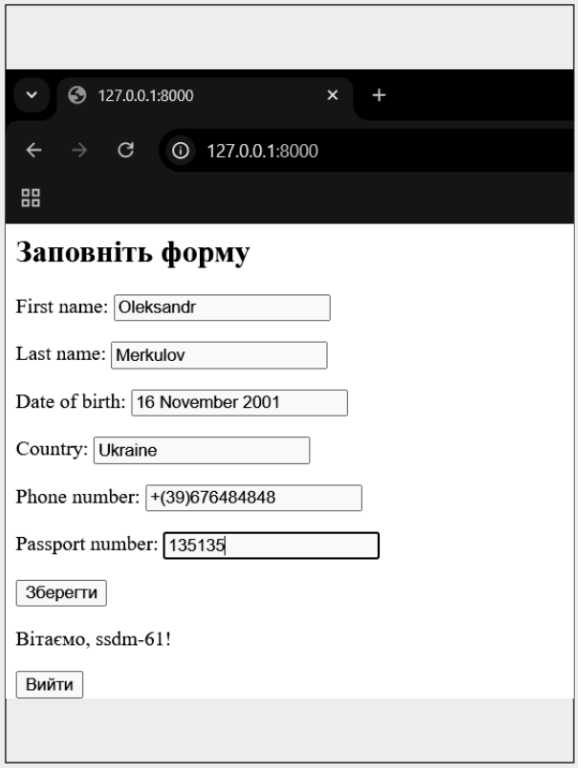
Компонент захисту	Призначення
Вхідне повідомлення	конфіденційні дані, що підлягають прихованому передаванню
AES-256	попереднє шифрування повідомлення перед стеганографічним вбудовуванням
LSB-вбудовування	приховування шифротексту у цифровому зображенні-контейнері
Ключі доступу	розділення криптографічного та стеганографічного рівнів захисту
Одержувач	витягування повідомлення зі стегооб’єкта і подальше розшифрування
Стегоаналіз	контроль ознак викривлення та виявлення прихованих даних

ВИКОРИСТАНІ ІНСТРУМЕНТИ ТА ТЕХНОЛОГІЇ РЕАЛІЗАЦІЇ

- Практична частина реалізована на основі Python, Django, HTML/CSS та SQL.
- Для криптографічного рівня використовується AES-256, для прихованого вбудовування - LSB-стеганографія.
- Веб-інтерфейс забезпечує авторизацію користувача та доступ до функцій прихованої передачі даних.



ПРОЦЕДУРА ФОРМУВАННЯ СТЕГОКОНТЕЙНЕРА



- Користувач обирає контейнер, вводить повідомлення та задає параметри приховування.
- Повідомлення шифрується, після чого шифротекст вбудовується у молодші біти зображення.
- Результатом є стегофайл, придатний для передавання мережевими каналами без очевидних ознак прихованого вмісту.

ДЕМОНСТРАЦІЯ РОБОТИ РОЗРОБЛЕНОГО РІШЕННЯ

- Розроблене рішення демонструє цикл приховування та подальшого отримання конфіденційного повідомлення.
- Після обробки контейнер зберігає візуальну якість і може бути використаний як звичайне цифрове зображення.
- Облікові та службові дані користувача підтримують контроль доступу до функцій системи.

ОЧІКУВАНИЙ ЕФЕКТ ВПРОВАДЖЕННЯ

- Підвищення прихованості передавання конфіденційних даних через мережеві канали ОІД.
- Зменшення ризику виявлення самого факту передавання захищеного повідомлення.
- Підвищення криптостійкості завдяки попередньому шифруванню AES-256 перед LSB-вбудовуванням.
- Можливість практичного застосування в системах захисту інформації, де потрібні конфіденційність і прихованість комунікації.

ВИСНОВКИ

- Проведено аналіз теоретичних основ стеганографії та її ролі у забезпеченні кібербезпеки.
- Досліджено методи стеганографії та стегоаналізу, зокрема LSB-вбудовування у цифрові зображення.
- Запропоновано комбінований підхід, що поєднує криптографічне шифрування AES-256 зі стеганографічним приховуванням.
- Практична реалізація підтверджує доцільність використання такого підходу для захисту конфіденційних даних на об’єкті інформаційної діяльності.