Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 «Кібербезпека»
(код і назва спеціальності)
освітня програма Кібербезпека
(назва освітньої програми)
на тему: Засоби захисту інформації з використанням стеганотехнологій

Виконавець: студент 4 курсу, групи КБ-42

_____ **Владислав БОДРУНОВ**
(підпис) (ім'я прізвище)

	Прізвище, ініціали	**Підпис**
Керівник роботи	Яніна ШЕСТАК	

Нормоконтроль	Сергій ДАКОВ	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Владислав Бодрунов**
(група) (прізвище ім'я по-батькові)

Тема кваліфікаційної роботи Засоби захисту інформації з використанням стеганотехнологій

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №5 від 17.11.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Стеганографія, Стего-об'єкт, Криптографія, Приховування інформації, Секретний ключ, Алгоритми стеганографії, Візуальний аналіз

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Загальні положення стеганографії, принципи та застосування стеганографії для захисту інформації, різниця між стеганографією і криптографією, базова модель стеганографії, метод дослідження максимальної стійкості стеганографічної системи, методи застосування стеганографії в якості приховування ключа, дослідження методів приховування інформації в різних типах даних.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Стеганографія дозволяє захистити конфіденційну інформацію від зловмисників шляхом приховування даних в інших носіях, що забезпечує ефективний захист від зовнішніх загроз.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Владислав БОДРУНОВ (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.11.2022 – 4.12.2022	*виконано*
2	Аналіз літератури	28.01.2023 –20.02.2023	*виконано*
3	Розгляд загальних положень стеганографії	24.02.2023 – 04.03.2023	*виконано*
4	Дослідження відмінностей стеганографії і криптографії.	05.03. 2023– 24.03.2023	*виконано*
5	Огляд існуючих методів приховування інформації за допомогою стеганографії	25.03. 2023– 07.04.2023	*виконано*
6	Дослідження формулу оцінки міцності стенографічної системи.	07.04. 2023– 12.04.2023	*виконано*
7	Дослідження методів приховуванні інформації в зображенні	12.04. 2023– 16.04.2023	*виконано*
8	Дослідження методів приховуванні інформації в аудіо	17.04. 2023– 20.04.2023	*виконано*
9	Дослідження методів приховуванні інформації в тексті	21.04. 2023– 09.05.2023	*виконано*
10	Аналіз відмінностей між оригінальним файлом та з прихованою інформацією	10.05. 2023– 04.06.2023	*виконано*
11	Оформлення пояснювальної записки	05.06.2023 – 08.06.2023	*виконано*

Завдання видав _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Владислав БОДРУНОВ (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 06 червня 2023 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 60 сторінок, включає в себе зміст, вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці дипломної роботи міститься 20 рисунків, 1 таблиця та 21 літературне джерело.

Метою роботи є дослідження методів та засобів стеганографії для приховування інформації в зображеннях, аудіо та текстових файлах і надання практичних рекомендацій щодо їх використання.

Об'єктом дослідження є процес приховування інформації.

Предметом дослідження є методи захисту інформації з використанням стеганографії.

Методи дослідження:

- аналіз відкритих джерел;
- порівняння методів захисту інформації за допомогою стеганографії;
- Візуальне порівняння оригінального файлу та файлу з прихованим повідомленням;

Практичною цінністю опис та порівняння способів та методів приховування інформації та ключів в різних інформаційних файлах.

Практична новизна: надання рекомендацій для вибору метода приховування інформації в різних типах файлів.

Ключові слова*:* стеганографія, стегосистема, стегаиаліз, стеганографічний контейнер, стеганографічне перетворення, захист інформації, стего-об'єкт.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕННЬ

LSB	Least significant bit
DWT	Discrete wavelet transform
ROI	Region of Interest
JPEG	Joint photographic experts group
PNG	Portable network graphics
BMP	Bitmap
STEGO	Graphics interchange format
LSBM	Least significant bit matching
WAV	Waveform audio file
MIDI	Musical instrument digital interface
AVI	Audio video interleave
MPEG	Moving picture experts group
MPI	Message passing interface
VOC	Creative voice file
SHA	Secure hash algorithm
RGB	Red green blue
TCP	Transmission control protocol
UDP	User datagram protocol
IP	Internet protocol
HTML	Hypertext Markup Language
DCT	Discrete cosine transform
SHA 256	Secure hash algorithm 256
RGB	Red green blue
ПЗ	Програмне забезпечення

ВСТУП

Захист інформації від несанкціонованого доступу є важливою, але не повністю вирішеною проблемою. Один з перспективних методів захисту інформації є стеганографія, яка є сукупністю методів та засобів, що дозволяють приховувати сам факт існування секретної інформації в тому або іншому середовищі. Існують два основних підходи до гарантованого захисту вмісту повідомлень: перший - шифрування повідомлень для блокування несанкціонованого доступу за допомогою криптографічних методів захисту, другий - застосування стеганографічних методів захисту для приховування факту існування інформації в невинних посланнях, знижуючи ймовірність її виявлення. Незважаючи на те, що криптографічний захист може бути легко розшифрований, стеганографічні методи захисту є більш ефективними, оскільки вони дають змогу вмонтувати інформацію в невинні повідомлення без підозри. Оскільки сьогодні маємо невирішені проблеми захисту авторських прав, захисту прав на особисту таємницю, організації електронної торгівлі, протиправної діяльності хакерів і терористів, інтерес до стеганографії очікується зростати в найближчі роки. Тож ***актуальність роботи*** полягає в дослідженні методів приховування інформації за допомогою стеганотехнологій.

Метою роботи є дослідження та аналіз методів приховування інформації з використанням стеганотехнологій.

Для досягнення зазначеної мети дипломної роботи поставлено наступні **завдання**:

- дослідити методи приховування інформації в різних типах даних
- провести аналіз кожного методу та визначити алгоритм їх роботи
- надати практичні рекомендації щодо вибору та використання різних методів приховування інформації та визначити недоліки методів.

Об’єктом дослідження є процес приховування інформації в різних типах даних, таких як зображення, аудіо та текст.

Предметом дослідження є механізми та засоби, реалізації методів приховування інформації

Методи дослідження:

- аналіз відкритих джерел;
- аналіз методів приховування інформації в різних типах даних;
- порівняння оригінального файлу і файлу з прихованим повідомленням.

Практична цінність роботи полягає в наступному:

- дослідження методів приховування інформації в зображеннях, аудіо та тексті з метою забезпечення конфіденційності та безпеки цінної інформації;
- реалізація порівняльного аналізу та визначення розбіжностей між оригінальним файлом та файлом з прихованим повідомленням

РОЗДІЛ 1
ОПИС ЗАГАЛЬНИХ АСПЕКТІВ СТЕГАНОГРАФІЇ ТА ЇЇ ВІДМІННОСТІ ВІД КРИПТОГРАФІЇ

1.1 Загальні положення стеганографії

Перші прояви стеганографії сягають далеко назад в історію людства і відомі з часів Стародавнього Риму та Греції. В давні часи, люди використовували різні методи стеганографії для передачі та отримання таємної інформації. Один з таких методів полягав у прихованому записі повідомлення на папері, який після цього був згорнутий та захований у середині фрукту, наприклад, в лимоні. При отриманні повідомлення, отримувач повинен був зробити деякі маніпуляції з фруктом, щоб отримати приховане повідомлення.

У середньовіччі, стеганографія була широко використовувана в політичних відносинах, і була дуже популярна серед розвідників. Один з найвідоміших методів, використаних у цей час, полягав у написанні таємного повідомлення на пергаменті, який після цього був згорнутий та захований у середині скорлупи яйця. Інші методи включали використання інкрустації таємного повідомлення у керамічних чи металевих предметах, які можна було передавати як звичайний подарунок.

З появою комп'ютерів, стеганографія зазнала змін та стала більш складною та надійною. Сучасні методи стеганографії використовуються для передачі прихованої інформації через мережі Інтернет та інші електронні засоби зв'язку.

Хоча перші згадки про стеганографію датуються давньогрецькою історією, сучасні методи стеганографії почали розвиватися з появою електронних пристроїв. Один з перших методів стеганографії був використаний у 1985 році, коли компанія Digital Equipment Corporation розробила програму для приховування повідомлень в зображеннях [1].

Протягом 1990-х років стеганографія стала все популярнішою в світі комп'ютерних технологій. У 1995 році Нільс Бергстром з компанії DigiMark створив

перший комерційний продукт з використанням стеганографії для захисту авторських прав на зображеннях.

Протягом наступних років було розроблено багато нових методів стеганографії, що дозволило захистити повідомлення від виявлення спеціальними програмами. Однак, стеганографія також може бути використана для зловживань та кримінальної діяльності, тому захист від неї стає все важливішим у світі, де захист приватності стає дедалі більш складним завданням.

Отже, історія стеганографії свідчить про постійний розвиток методів приховування та витягнення інформації, а також про важливість захисту від неправомірного використання цих методів [2].

Сучасні методи комп'ютерної стеганографії є самостійним науковим напрямком інформаційної безпеки, який досліджує проблеми створення компонентів приховуваної інформації у відкритому інформаційному середовищі, що може бути сформоване обчислювальними системами та мережами. Особливістю стеганографії є те, що вона дозволяє вирішувати деякі важливі задачі захисту інформації в рамках традиційно існуючих інформаційних потоків або інформаційного середовища, не оголошуючи прямого факту існування захищуваної інформації. На сьогоднішній день, стеганографія є сукупністю методів та технічних рішень для захисту інформації, що базуються на різних принципах. Однак, зі стрімким зростанням інформаційно-телекомунікаційних технологій, комп'ютерні методи стеганографії та їх застосування в кібернетичному просторі є найбільш активно розвиваючимися. Методична та інструментальна база багатьох підходів до стеганографії має спільність з криптографією, яку встановив Шенон при створенні загальної теорії секретного зв'язку. Це пояснюється тим, що стеганографія та криптографія розвивалися як єдиний науковий напрямок - тайнопис. Лише в кінці XIX століття після формулювання Кирхгофом основних законів криптографії, включаючи умову, що стійкість криптографічного перетворення залежить від таємниці ключа, криптографія стала окремою наукою від стеганографії. Одним з ключових моментів у стеганографії є збереження в таємниці алгоритму застосування стеганографічного перетворення [1].

Завдяки швидкому розвитку обчислювальної техніки великі об'єми медіа постійно завантажуються та передаються по інтернету. Різноманіття цих медіа викликає труднощі при аналізі звичайного та аномального контенту в них. Оскільки більшість процесів в Інтернеті керуються людьми, передбачення поведінки та аналіз аномалій є складним процесом, який може вимагати високої обчислювальної потужності та складних алгоритмів.

Стеганографія ґрунтується на цій непередбачуваності, щоб здійснювати приховування інформації внутрішньо в невинні пакети даних. Якщо в криптографії головний акцент зроблений на тому, що зловмисник не може отримати інформацію про пакет даних з його зашифрованого вмісту, то стеганографія має на меті створення комунікаційного каналу між двома сторонами без посередника, який б міг здогадатись про існування цього каналу. Можна легко зробити висновок, що припущення, запропоновані стеганографією, є сильнішими, ніж ті, які запропоновані криптографією. [2]

Особливий випадок приховування інформації - це цифрове водяне знакування. Цифрове водяне знакування - це процес вбудовування інформації в цифровий мультимедійний контент, так що цю інформацію (водяний знак) можна в подальшому видобути або виявити для різних цілей, включаючи запобігання копіюванню та контролю. Цифрове водяне знакування стало активною та важливою областю досліджень, а розробка та комерціалізація технік водяного знакування вважається необхідним для вирішення деяких проблем, пов'язаних із швидким поширенням цифрового контенту. Основна різниця між приховуванням інформації та водяним знакуванням полягає в відсутності активного противника. У водяному знакуванні, такому як захист авторських прав та аутентифікація, існує активний противник, який намагається видалити, недійснувати або підробити водяні знаки. У приховуванні інформації немає такого активного противника, оскільки немає жодної цінності, пов'язаної з вилученням інформації, прихованої в контенті. Тим не менше, техніки приховування інформації повинні бути стійкими до випадкових спотворень [3].

1.2 Основні принципи стеганографії та її застосування для захисту інформації

Загальні положення стеганографії передбачають використання різних методів та технік для приховування інформації в мультимедійних даних. Одним з найбільш важливих аспектів стеганографії є те, що приховане повідомлення має бути непомітним для людей та залишатися в тому ж самому форматі, що і оригінальний файл [4].

Іншим важливим аспектом стеганографії є забезпечення безпеки та конфіденційності прихованого повідомлення, тобто забезпечення того, що лише авторизовані користувачі можуть отримати доступ до цієї інформації.

Для забезпечення безпеки і конфіденційності стеганографічні методи можуть використовувати шифрування або інші методи захисту даних [5].

Застосування стеганографії для захисту інформації полягає в тому, що повідомлення може бути приховане в образах, аудіо- та відеофайлах, тим самим захищаючи конфіденційні дані від небажаних осіб.

Одним з прикладів застосування стеганографії є захист авторських прав на мультимедійні файли, які можуть бути підроблені або скопійовані. Шляхом приховування інформації в оригінальному файлі можна забезпечити доказову базу про походження файлу та зменшити ризик його підробки.

Крім того, стеганографія може бути використана для передачі конфіденційних даних через небезпечні зони, такі як Інтернет. Зашифроване повідомлення може бути приховане в невинному зображенні або звуковому файлі і передане без залучення додаткових засобів шифрування, що збільшує рівень безпеки та надійності комунікації.

Проте, варто пам'ятати, що застосування стеганографії не забезпечує повної захисту інформації, тому важливо дотримуватися всіх стандартних заходів безпеки, включаючи сильне шифрування та захист від шкідливих програм [6].

1.3 Різниця між криптографією і стеганографією

В сучасному житті інформація є надзвичайно цінним ресурсом, доступ до якого став значно простішим завдяки глобальним комп'ютерним мережам. Однак, це також призвело до підвищення загрози порушення безпеки даних, зокрема несанкціонованого доступу до конфіденційної інформації, яка часто знаходиться у цифровому форматі. Завдання надійного захисту цих даних є давньою і до цього часу невирішеною проблемою.

З огляду на розвиток мультимедійних технологій, які дозволяють обробляти та відтворювати різні типи сигналів у цифровому форматі, захист інформації є особливо актуальною темою. Легкість відновлення та висока потенційна завадостійкість цифрових даних мають свої переваги, проте загроза викрадення та модифікації їх також значно збільшилась.

Для захисту конфіденційних даних в інформаційних системах використовуються різні методи, серед яких криптографія та стеганографія. Криптографія - це метод захисту інформації шляхом зміни її зрозумілості для неповідомлених шляхом шифрування. Однак, цей метод не є повністю ефективним, оскільки наявність шифрованого повідомлення може привернути увагу зловмисників.

Щоб уникнути такої уваги, використовують стеганографію - науку, яка досліджує методи та способи приховування конфіденційної інформації при передачі, зберіганні та обробці. Цей метод дозволяє приховати сам факт існування секретної інформації, що робить її непомітною для зловмисників.

Загалом, криптографія та стеганографія є важливими інструментами для захисту даних, і вони можуть бути використані як окремо, так і разом, для забезпечення максимального захисту від несанкціонованого доступу до конфіденційної інформації. Однак, ні один метод захисту не є ідеальним, і захист даних може бути порушений при наявності достатньої мотивації та ресурсів зловмисників. Тому, крім захисту даних за допомогою криптографії та стеганографії, також важливо дотримуватися загальних правил безпеки даних, таких як

використання сильних паролів, оновлення програмного забезпечення та застосування заходів захисту мережі та систем [7].

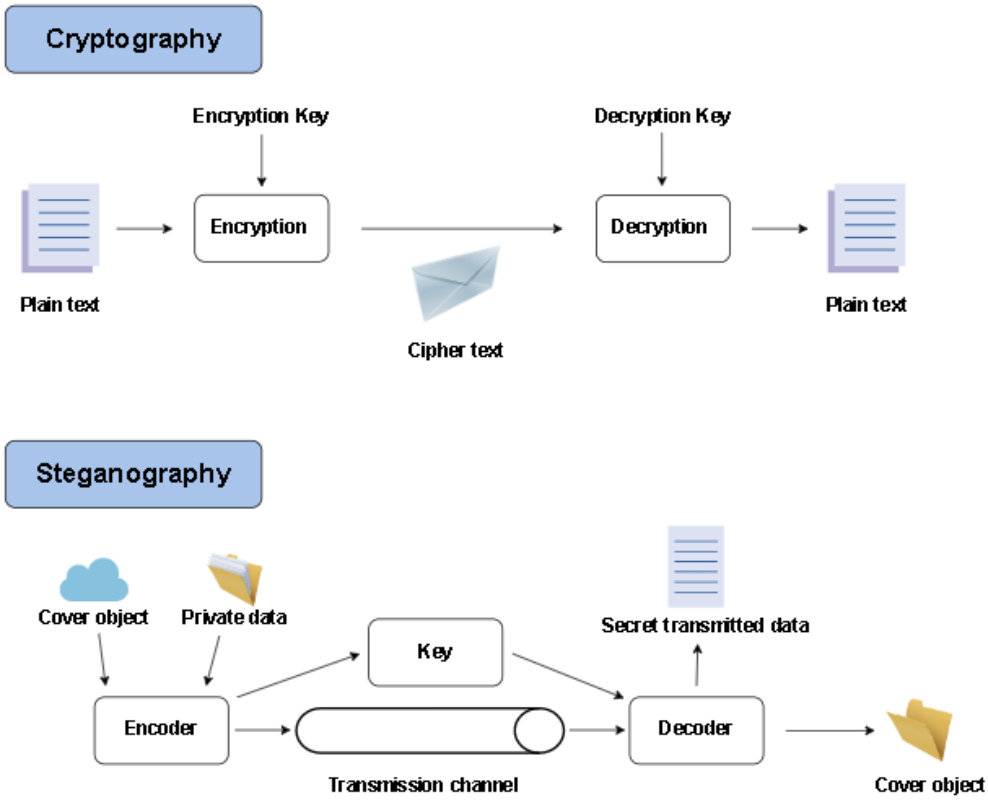

Рисунок 1.1 Послідовність роботи стеганографії і криптографії

Щоб приховати секретну інформацію в зображенні, можна використовувати комбінацію методів шифрування та стеганографії. Спочатку зашифрувавши повідомлення, а потім вставивши його в зображення, можна передавати інформацію без виявлення. Крім того, якби зловмиснику вдалося розкрити приховане повідомлення за допомогою стеганографічних засобів, йому все одно знадобився б ключ криптографічного декодування для розшифровки зашифрованого вмісту [8]. У таблиці 1.1 наведено короткий перелік переваг і недоліків обох методів .

Таблиця 1.1

Порівння стеганографії і криптографії

Поняття	Криптографія	Стеганографія
1	cryptos graphein – секретне письмо	steganos graphein – приховане письмо

Продовження таблиця 1.1

2	Приховується лише саме повідомлення	Приховується факт таємного спілкування
3	Інформація перетворюється	Інформація приховується
4	Перетворена інформація не схована і відома користувачу	Прихована інформація схована від користувача
5	Основна мета криптографії полягає в тому, щоб зберегти вміст повідомлення в секреті від несанкціонованого доступу	Суть стеганографії полягає в тому, щоб зробити інформацію невидимою для будь-кого, хто не знає, де шукати або що шукати

Стеганографія та криптографія є дві різні галузі, пов'язані з безпекою та захистом комунікації.

Стеганографія - це наука, що досліджує методи та техніки приховування інформації в інших даних (наприклад, в зображеннях, звукових файлів) без привертання уваги спостерігачів. В основі стеганографії лежить ідея про збереження структури даних, тобто прихована інформація інтегрується в наявні дані, не змінюючи їх суттєво. Стеганографія не вимагає складних математичних перетворень, а зосереджується на методах приховування інформації таким чином, щоб здавалося, ніби вона відсутня.

З іншого боку, криптографія - це наука, що займається захистом комунікації шляхом зміни змісту даних таким чином, щоб вони стали незрозумілими для неавторизованих осіб. Криптографія використовує математичні методи, теорію чисел та інші підходи для шифрування та розшифрування інформації. У криптографії інформація перетворюється за допомогою алгоритмів шифрування, що забезпечує конфіденційність та цілісність даних.

Таким чином, найсуттєвіша відмінність між стеганографією та криптографією полягає в тому, що стеганографія забезпечує приховування інформації, не змінюючи структуру даних, тоді як криптографія змінює дані за допомогою математичних методів [9].

Висновок за 1 розділом

У даному розділі було розглянуто загальні положення стеганографії, основні принципи її функціонування та можливості застосування для захисту інформації. Загальні положення стеганографії включають поняття приховання інформації в недивних або непомітних носіях, таких як зображення, аудіофайли або текстові документи. Основні принципи стеганографії полягають у вбудовуванні прихованої інформації у носії та витягуванні її на приймачі.

Використання стеганографії для захисту інформації має декілька переваг. По-перше, вона дозволяє зберігати конфіденційну інформацію прихованою, надійно захищаючи її від несанкціонованого доступу. По-друге, стеганографія дозволяє обходити механізми виявлення та блокування шифрованої інформації, оскільки прихована інформація не викликає підозр. По-третє, використання стеганографії може знизити ризик виявлення самого факту передачі конфіденційної інформації.

Різниця між криптографією і стеганографією полягає у підходах до захисту інформації. Криптографія займається шифруванням даних з метою забезпечення їх конфіденційності, цілісності та аутентичності. Вона використовує математичні алгоритми для перетворення повідомлень у незрозумілий вигляд, що забезпечує захист інформації під час передачі. Стеганографія, з іншого боку, не шифрує самі дані, а приховує їх існування. Вона використовує методи вбудовування додаткової інформації у носії, таким чином, що зовнішній спостерігач не може виявити наявність прихованої інформації. Стеганографія спирається на принцип "приховання в очевидному", що робить її менш підозрілою в порівнянні з криптографією. Висновок

полягає в тому, що як криптографія, так і стеганографія є важливими інструментами для захисту інформації, проте вони використовують різні підходи. Криптографія забезпечує захист даних шляхом їх шифрування, тоді як стеганографія приховує інформацію в недивних носіях. Враховуючи ці різниці, важливо обирати належний підхід до захисту конфіденційної інформації залежно від конкретних потреб та обставин.

РОЗДІЛ 2
ПРОЦЕС НАДАННЯ ДОСТУПУ ДО WEB-ЗАСТОСУНКІВ. ВРАЗЛИВОСТІ ТА МЕТОДИ ЗАХИСТУ

2.1 Базована модель стеганографії

На Рисунок 2.1, можна побачити модель стеганографії. Повідомлення - це дані, які відправник бажає зберегти в таємниці. Це може бути звичайний текст, шифротекст, інший зображення або будь-що інше, що може бути вбудоване в бітовий потік, таке як маркування авторського права, таємне спілкування або серійний номер. Пароль відомий як стегоключ, який забезпечує те, що лише одержувач, який знає відповідний ключ декодування, зможе видобути повідомлення з прихованого об'єкту. Прихований об'єкт з вбудованим таємним повідомленням називається стего-об'єктом.

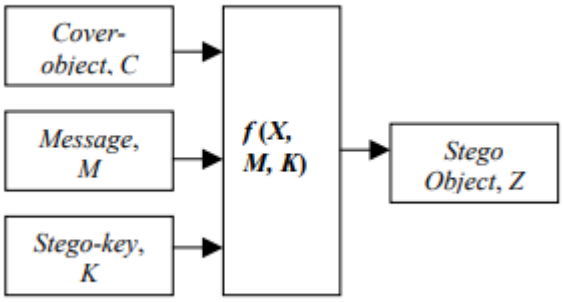

Рисунок.2.1 Базова модель стеганографії

Для відновлення повідомлення зі стего-об’єкта потрібен сам об’єкт-обкладинка та відповідний ключ декодування, якщо під час процесу кодування використовувався стего-ключ.

Нижче наведено кілька варіантів приховувальних об'єктів, які можуть використовуватися в якості покривного об'єкту [9]:

- Мережеві протоколи, такі як TCP, IP та UDP, можуть використовуватися для приховування і передачі додаткової інформації. Це може включати вбудовання даних у заголовки або використання не використовуваних полів протоколів.
- Звук, що використовує цифрові аудіоформати, такі як WAV, MIDI, AVI, MPEG, MPI та VOC, може бути використаний для приховування інформації. Це може бути досягнуто шляхом вбудовування додаткових даних в аудіофайли, наприклад, в непомітні зміни амплітуди або частоти звуку.
- Файли та диски можуть приховувати та додавати файли за допомогою "slack space" - прихованого простору. Це означає, що вільний простір на диску може бути використаний для збереження прихованої інформації, або додавання додаткових файлів в існуючі файли.
- Текст може бути використаний як покривний об'єкт за допомогою різних методів. Наприклад, можна використовувати нульові символи, аналогічно мові Морзе, для приховування додаткової інформації у текстових документах. Також, HTML та Java можуть бути використані для створення покривних об'єктів шляхом вбудовування прихованої інформації у веб-сторінки або програмний код.
- Файли зображень, такі як BMP, GIF та JPG, можуть також бути використані як покривні об'єкти. Додаткова інформація може бути прихована у структурі файлу або в непомітних змінах пікселів. Крім того, кольорові зображення та зображення в градаціях сірого кольору можуть слугувати покривними об'єктами для приховування додаткової інформації.

Процес складається з двох етапів:

1. Ідентифікація зайвих бітів у ковер-об'єкта. Зайві біти - це ті біти, які можуть бути змінені без порушення якості або цілісності ковер-об'єкта.

2. Процес вбудовування вибирає підмножину зайвих бітів, які будуть замінені даними з секретного повідомлення. Стего-об'єкт створюється шляхом заміни обраних зайвих бітів бітами повідомлення.

Протягом останніх декількох років було запропоновано безліч технік стеганографії, які дозволяють вбудовувати приховані повідомлення у мультимедійні

об'єкти [10]. Існує багато методів для того, щоб приховати інформацію або повідомлення у зображеннях таким чином, щоб зміни, внесені до зображення, були непомітними для сприйняття. Розповсюдженими підходами є [10]:

- Вставлення менш значущих бітів (LSB): Цей метод полягає в заміні найменш значущих бітів пікселів зображення на біти прихованого повідомлення. Через те, що найменш значущі біти мають менший вплив на вигляд зображення, зміни є малопомітними. Цей підхід особливо ефективний для зображень з великою кількістю пікселів, де дрібні зміни в бітах мало помітні.
- Маскування та фільтрування: Цей підхід використовує методи маскування, щоб приховати повідомлення у зображенні. Маскування полягає у використанні областей зображення, які змінюються незначно або не змінюються взагалі, для приховування інформації. Фільтрування використовується для згладжування змін і робить їх менш помітними.
- Трансформаційні методи: Цей підхід використовує різні математичні трансформації для приховування повідомлення у зображенні. Наприклад, методи на основі перетворення Фур'є можуть використовувати високочастотні компоненти для приховування інформації. Інші методи можуть використовувати перетворення кольорових просторів або вейвлет-аналіз для приховування повідомлення у зображенні.

Вставлення менш значущих бітів (LSB) - простий підхід до вбудовування інформації у зображення. Найпростіші техніки стеганографії вбудовують біти повідомлення безпосередньо в найменш значущі бітові площини оригінального зображення в детермінованій послідовності. Модулювання менш значущих бітів не призводить до помітних змін, оскільки амплітуда змін дуже мала.

Техніки маскування та фільтрування, які зазвичай застосовуються до зображень 24-бітного та відтінків сірого кольору, приховують інформацію, позначаючи зображення подібно до водяних знаків на папері. Техніки проводять аналіз зображення, щоб вбудувати інформацію в значущі області, так що приховане повідомлення стає більш інтегральною частиною оригінального зображення, ніж просте приховування його на рівні шуму.

Техніки перетворення вбудовують повідомлення, модулюючи коефіцієнти в області перетворення, такі як дискретне косинусне перетворення (DCT), яке використовується при стисненні JPEG, дискретне перетворення Фур'є або хвильове перетворення. Ці методи приховують повідомлення в значущих областях оригінального зображення, що робить їх більш стійкими до атак. Перетворення можуть бути застосовані на всьому зображенні, в окремих блоках або інших варіантах.

Метод LSB полягає в заміні останніх значущих бітів у контейнері (наприклад, зображенні, аудіо або відеозапису) на біти прихованого повідомлення, щоб різниця між оригінальним та зміненим контейнером була непомітною для людського сприйняття.

Існує також метод розширення палітри, який діє лише для формату GIF. Цей метод дозволяє збільшити розмір палітри зображення-контейнера, що дає додатковий простір для запису байтів прихованого повідомлення в місці байтів кольорів. Якщо розглядати мінімальний розмір палітри, який становить 2 кольори (6 байтів), то максимальний розмір прихованого повідомлення може досягати 762 байти (256×3-6). Однак недолік цього методу полягає у низькій криптозахищеності, оскільки приховане повідомлення може бути прочитане будь-яким текстовим редактором, якщо воно не додатково зашифроване [10].

У більшості мультимедійних файлів після області даних міститься прапор і службова інформація. Якщо вмістити приховане повідомлення після цього прапора, його буде неможливо помітити під час перегляду або прослуховування. Оскільки для неущільнених форматів файлів параметри (розподільна спроможність зображень, частота дискретизації, розрядність, тривалість для звуку) дозволяють легко встановити розмір, краще приховувати повідомлення в ущільнених форматах (MP3, AVI тощо). Існує багато методів стеганографії, які можна застосовувати до практично всіх типів мультимедіа-файлів, і вони є стійкими та мають високу пропускну здатність. Однак їх легко помітити і видалити.

2.2 Метод дослідження максимальної стійкості стенографічної системи

Для досягнення максимальної стійкості стеганографічної системи важливо правильно вибрати елементи контейнера, які будуть модифіковані під час вбудовування інформації**.** Елемент контейнера - це найменша частина цифрового об'єкту, яка може бути змінена. Оптимальний вибір елементів дозволяє максимізувати стійкість стеганографічної системи при заданому розмірі прихованого повідомлення або забезпечити високу перепускну здатність при заданій швидкості. Таким чином, задача полягає у розробці ефективного методу вибору елементів контейнера для вбудовування інформації. Контейнер може бути розділений на групи, які не перетинаються, і складатися з елементів з подібними властивостями та розподілом.

Ми розглядаємо контейнер як множину з m груп елементів, де кожна група характеризується кількістю елементів, що містяться в ній згідно з певним розподілом – k_i. C_i - діапазон значень елементів контейнера, які можуть бути включені до і-ої групи. Зміна елементу в і-й групі дає можливість вбудувати q_i біт. Зміна елементу в певній підгрупі дозволяє вбудувати q_i бітів, де q_i визначається логарифмом числа C_i за основою 2.

Отже, цифровий об'єкт (контейнер або стего) розглядається у вигляді векторів, що складаються з елементів контейнера.

Розглянемо випадок коли x_i – це кількість модифікованих елементів і-ї групи, в якій x_i лежить на проміжку від 0 до k_i ($0 \leq x_i \leq k_i$) та сума $x_i + q_i = n$

Функція $f_i(c)$ відображає щільність розподілу елементів у і-й групі стеганографічного контейнера. Інформація, яка прихована в контейнері, має високу ентропію, оскільки часто є зашифрованою або стисненою.

Завдяки цій властивості можна визначити функцію щільності розподілу елементів і-ої групи контейнеру, у якій приховано повідомлення $\overline{f_i}(c_i, x_{i0})$, де x_i - кількість незмінних елементів:

$$\overline{f_l}(c_i, x_i) = \frac{k_i - x_i}{k_i} f_i(c) + \frac{x_i}{k_i} * \frac{1}{|c_i|} \qquad (1)$$

Позначимо за P(S) ймовірність вибору цифрового об'єкту S як стегано-контейнера:

$$P(S) = \prod_{i=1}^{m} \prod_{j=1}^{ki} \overline{f_l}\left(c_j^i\right) \quad (2)$$

Аналогічно обчислюється імовірність $\overline{P}$(S), що після вбудовування інформації отримаємо стегано-контейнер S:

$$\overline{P}(S) = \prod_{i=1}^{m} \prod_{j=1}^{ki} \overline{f_l}\left(c_j^i, x_i\right) \quad (3)$$

Представлені формули дозволяють оцінити міцність стеганографічної системи з використанням інформаційно-технічного підходу та розрахувати відносну ентропію (відстань Кульбака-Лейблера), що відображає відмінність між двома ймовірнісними розподілами.

$$D\left(P \parallel \overline{P}\right) = \sum_S P(S) \log_2 \frac{P(S)}{\overline{P}(S)} \quad (4)$$

Міра того, наскільки відмінні між собою два ймовірнісних розподіли визначається відстанню Кульбака-Лейблера, що використовується для оцінки стійкості стеганографічної системи за допомогою інформаційно-технічного підходу. Чим менша ця відстань, тим вище стійкість системи. Для задачі оптимального розподілу приховуваного повідомлення в стеганографічному контейнері потрібно знайти вектор $\{x_i\}$, $0 \le x_i \le k_i$, для якого величина $D\left(P \parallel \overline{P}\right)$ буде мінімальною [11].

2.3 Методи зстосування стегонографії в якості приховування ключа

Більшість застосувань стеганографії ґрунтуються на одному загальному принципі, який проілюстровано на Рисунку 2.2. Аліса, яка бажає передати таємне повідомлення m Бобу, випадковим чином обирає (з використанням приватного джерела випадкових чисел r) безпечне повідомлення c, яке може бути передано Бобу без підозри, та вбирає таємне повідомлення в c, ймовірно, використовуючи ключ k, який називається стегоключем. Таким чином, Аліса змінює обкладинку c на стегооб'єкт s. Це повинно бути зроблено дуже обережно, щоб стороння особа, яка знає тільки видимо безпечне повідомлення s, не могла виявити наявності таємного повідомлення. У "ідеальній" системі нормальна обкладинка не повинна відрізнятися

від стегооб'єкта, або людина, або комп'ютер, який шукає статистичні закономірності. Теоретично, обкладинки можуть бути будь-якими данними, які може прочитати комп'ютер, такими як файли зображень, цифровий звук або письмовий текст.

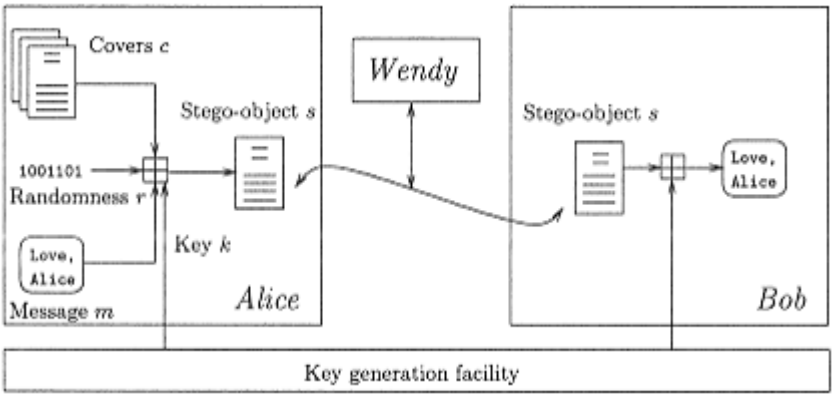

Рисунок 2.2 Схематичний образ стеганографії

Після цього Аліса передає s по ненадійному каналу Бобу і сподівається, що Венді не помітить вбудованого повідомлення. Боб може відновити m, оскільки він знає метод вбудовування, який використовувала Аліса, та має доступ до ключа k, використаного в процесі вбудовування. Цей процес вилучення повинен бути можливим без початкової обкладинки c. Якщо спостерігач має доступ до набору $\{c_1, ..., c_n\}$ обкладинок, переданих між обома сторонами комунікації, він не повинен бути здатний визначити, які обкладинки c_i містять таємну інформацію. Таким чином, безпека невидимої комунікації в основному полягає у нездатності розрізнити обкладинки від стегооб'єктів.

У практиці не всі дані можуть бути використані як обкладинка для секретної комунікації, оскільки модифікації, що застосовуються в процесі вбудовування, не повинні бути видимі жодній сторонній особі, яка не бере участі в комунікаційному процесі. Цей факт вимагає, щоб обкладинка містила достатньо зайвих даних, які можуть бути замінені секретною інформацією. Наприклад, через похибки вимірювання будь-які дані, які є результатом якогось фізичного сканування, містять стохастичний компонент, який називається шумом. Такі випадкові артефакти можуть бути використані для передачі секретної інформації. Насправді виявляється, що шумні дані мають більш переваги в більшості стеганографічних застосувань.

2.3.1 Чиста стеганографія

Чиста стеганографія - це система, яка не потребує попереднього обміну таємною інформацією, такою як стего-ключ. Для вбудовування секретної інформації в оболонку використовується відображення E: C×M → C, де C - множина можливих оболонок, а M - множина можливих повідомлень. Для видобування секретного повідомлення з оболонки використовується відображення D: C → M. Алгоритми вбудовування та видобування повинні бути доступними відправникові та отримувачеві, але не повинні бути доступні публічно. Необхідно, щоб кількість можливих оболонок була не меншою за кількість можливих повідомлень.

Згідно визначення:

Четвірка = <C, M, D, E>, де C — множина можливих покриттів, M набір секретних повідомлень з |C| ≥ |M|, E : C×M → C функція вкладення та D : C → M вилучення функція з властивістю D(E(c,m)) = m для всіх m ∈ M і c ∈ C називається чистою стеганографічною системою.

Більшість практичних стеганографічних систем використовують набір C, який містить значущі та безпечні повідомлення, такі як значущі цифрові зображення або тексти, що були створені за допомогою таблиць Тритеміуса зображену на Рис.2.3. Це дозволяє двом спілкуючимся сторонам обмінюватися повідомленнями, не викликаючи підозри. Процес вбудовування зазвичай здійснюється таким чином, щоб обкладинка та стегооб’єкт були перцептуально подібні. Формально, перцептивна подібність може бути визначена за допомогою функції подібності [7].

TRITHEMIUS-TABELLE

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Рисунок.2.3 Таблиця Trithemius

Функція sim : C2 → (-∞, 1] називається функцією подібності на множині C, якщо для будь-яких двох елементів x, y ∈ C, вона повертає значення від -∞ до 1, де значення ближче до 1 вказує на більшу подібність між x та y.

$$sim(x, y) \Leftrightarrow x = y \qquad (5)$$

При x ≠ y, sim(x,y) < 1

У випадку цифрових зображень або цифрового аудіо кореляцію між двома сигналами можна використовувати як функцію подібності. Тому більшість практичних стеганографічних систем намагаються виконати умову, що подібність між оригінальним повідомленням та повідомленням, закодованим у зображенні (звуку), максимальна. Цю умову можна формально виразити як $sim(c, E(c, m)) \approx 1$ для всіх $m \in M$ і $c \in C$.

Щоб забезпечити таємність спілкування, необхідно використовувати приватні обкладинки, які не доступні зловмисникам. Відправник може створити обкладинки шляхом запису або сканування. Для кожного процесу спілкування випадковим чином вибирається обкладинка. Однак перед вибором обкладинки випадковим чином, відправник може переглянути базу даних придатних для використання обкладинок та вибрати ту, яка зміниться найменше в процесі вбудовування. Функція подібності sim може бути використана для визначення подібності обкладинок [7].

Під час кодування, відправник обирає покриття (елемент) c, яке максимально наближене до елементів множини C, з урахуванням наступної умови: він вибирає той елемент c з множини C, який має найвищу ступінь схожості (виміряну за допомогою функції sim) з його шифрованою версією E(x, m), де x належить до множини C. Таким чином, відправник вибирає елемент c, який найкраще підходить для приховування повідомлення m у контексті множини C.

2.3.2 Стеганографія відкритого ключа

Так само як і у криптографії з відкритим ключем, стеганографія з відкритим ключем не потребує обміну секретним ключем. Системи стеганографії з відкритим ключем використовують два ключі: один закритий і один відкритий. Відкритий ключ зберігається в публічній базі даних. Під час вбудовування використовується відкритий ключ, а для реконструкції секретного повідомлення використовується закритий ключ.

Одним зі способів побудувати систему стеганографії з відкритим ключем є використання криптографії з відкритим ключем. Будемо припускати, що Аліса та Боб

можуть обмінятися відкритими ключами якогось алгоритму криптографії з відкритим ключем . У системі стеганографії з відкритим ключем використовується той факт, що функцію декодування D (де D є функцією на всьому наборі C) в стеганографічній системі можна застосовувати до будь-якого покриву c, чи містить він таємне повідомлення, чи ні. У останньому випадку результатом буде випадковий елемент M, який ми назвемо "природною випадковістю" покриву. Якщо припустити, що ця природна випадковість статистично не відрізняється від криптотексту, створеного деякою системою криптографії з відкритим ключем, можна побудувати безпечну систему стеганографії, вбудувавши криптотекст замість незашифрованого таємного повідомлення.

Андерсон в своїх роботах запропонував протокол стеганографії з відкритим ключем, який базується на тому, що зашифрована інформація має достатньо випадковий вигляд, щоб бути прихованою. Аліса шифрує секретне повідомлення відкритим ключем Боба, отримує випадково виглядаюче повідомлення та вставляє його в канал спілкування, що є відомим Бобу та Венді. Це замінює частину "природної випадковості", яка супроводжує кожен процес спілкування. Ми припускаємо, що як криптографічні алгоритми, так і функції вбудовування є відомі публіці. Боб не може передбачити, чи передається в обкладинці секретна інформація, тому він просто намагається витягти і розшифрувати повідомлення за допомогою свого закритого ключа, якщо запідозрює надходження повідомлення. Якщо обкладинка насправді містить секретну інформацію, то розшифрована інформація є повідомленням від Аліси. Важливим аспектом є те, що Боб має підозрювати використання стеганографічної техніки і спробувати розшифрувати кожну обкладинку, яку він отримує від Аліси [12].

Якщо ми припустимо, що Венді знає про використаний метод вбудовування, вона може спробувати вилучити секретне повідомлення, яке було надіслане Алісою до Боба. Але якщо метод шифрування створює випадково виглядаючий зашифрований текст, то Венді не матиме доказів того, що вилучена інформація є більшою, ніж кілька випадкових бітів. Вона не зможе вирішити, чи вилучена

інформація є значущою, чи це лише частина природної випадковості, якщо не зможе зламати криптосистему.

Кравер розширив цей протокол, щоб імітувати чисту стеганографію, використовуючи як відкритий, так і закритий ключі. Чиста стеганографія зазвичай більш популярна в більшості додатків, оскільки партнерам по комунікації не потрібно використовувати спільний стеганографічний ключ. Проте, чистий протокол стеганографії не забезпечує жодної безпеки, якщо метод вбудовування відомий зловмиснику. Але, якщо Аліса та Боб реалізують протокол обміну ключами з використанням стеганографії з відкритим ключем, вони зможуть обмінюватися секретним ключем k, який потім вони можуть використовувати в системі стеганографії зі секретним ключем. Оскільки ніякий стего-ключ (крім їх відкритого ключа шифрування) не повинен бути відомий заздалегідь, ми можемо називати процес комунікації чистою стеганографією.

У цьому протоколі Аліса спочатку створює пару випадкових ключів - відкритий та приватний, що можуть бути використані з будь-якою криптосистемою з відкритим ключем. Потім вона надсилає відкритий ключ по відкритому каналу, який може слухать Бобу (і Венді також). А ні Боб, а ні Венді не можуть знати, скільки випадкових бітів містить канал. Однак Боб підозрює, що стего-об'єкт, надісланий Алісою, містить відкритий ключ, і намагається його витягти. Він використовує цей ключ, щоб вставити випадково обраний ключ k разом із коротким підтверджувальним повідомленням, обидва зашифровані відкритим ключем Аліси, у обкладинку та надсилає її Алісі. Венді може спробувати витягнути секретну інформацію, надіслану Бобом, але вона ймовірно побачить лише випадковий зашифрований текст. Аліса підозрює, що повідомлення надійшло від Боба, витягує секретну інформацію та розшифровує її за допомогою свого закритого ключа. Тепер Аліса та Боб можуть використовувати спільний стего-ключ k. Цей протокол показаний на Рис 2.4.

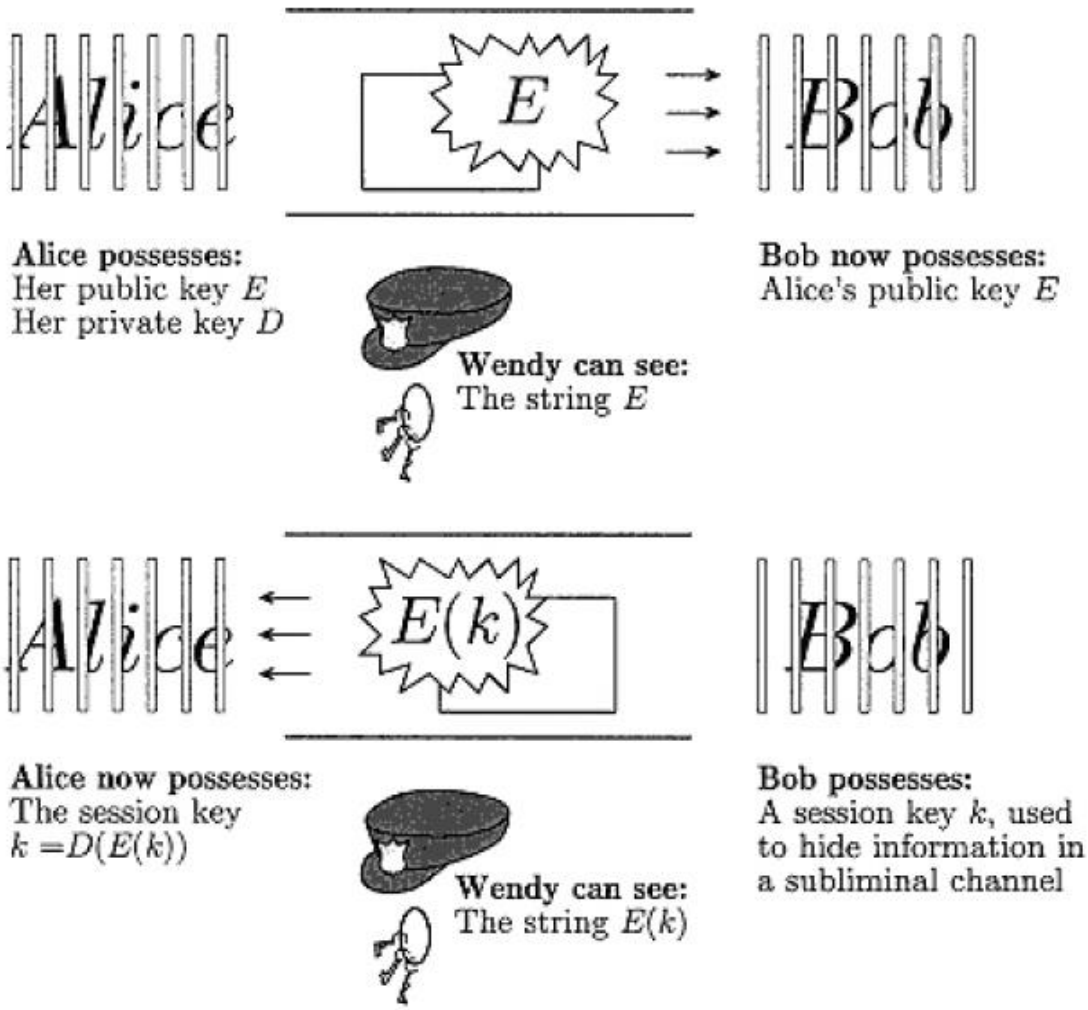

Рисунок. 2.4 Ілюстрація протоколу стенографічного обміну ключів

2.4 Визначення наявної відмівнності між зображенням без прихованого тексту з зображенням з прихованим текстом

Для вбудовування даних у зображення нам потрібні два важливі файли. Перше — оригінальне зображення, так зване зображення обкладинки. Зображення (рис. 4), яке у форматі JPEG буде містити приховану інформацію, використав зображення з інтернету. Другий файл — це саме повідомлення, тобто інформація, яку потрібно приховати в зображенні. Текст який я приховую зображено на Рис. 2.5 Для цього використав онлайн застосунок з Github [14].

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Vivamus tempus nibh sit amet metus lobortis ultricies. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Nulla in feugiat turpis. Mauris eu arcu egestas, feugiat odio vitae, consequat metus. Phasellus iaculis, dolor a commodo bibendum, quam massa rutrum orci, sed laoreet nisl mi nec ipsum. Nunc vel pharetra sem, et sodales est. Nullam eget turpis ut nulla pellentesque viverra sit amet sed enim. Sed ac turpis mi. Quisque sed nisi vel tellus ornare pharetra. Nulla dapibus commodo est a semper. Morbi fermentum est facilisis lorem egestas volutpat. Morbi iaculis, sapien sit amet posuere tempor, justo lectus mattis sapien, in viverra libero justo quis orci. Vivamus fringilla erat blandit pellentesque vehicula.

Рисунок.2.5 Текст

Рисунок.2.6 Зображення

Далі за допомогою онлайн застосунку закодував у Зображення (Рис.2.6) свій текст (Рис.2.5). В результаті отримав таке зображення (Рис.2.7)

Рисунок.2.7 Зображення з закодованим текстом

Отже переглянувши два зображення: Рис.2.6 – без закодованого тексту і Рис.2.7 – з закодованим текстом. При порівнянні різниця між ними майже не помітна, а якщо нема оригіналу то дуже складно зрозуміти що переді мною зображення з закодованим текстом.

Між ними я помітив таку різницю:

Колір на зображенні з закодованим текстом (Рис.2.7) трохи відрізняється ніж на оригіналі (Рис.2.6)

На Рис.2.8 навів порівняння кольорів зображення для цього використав ПЗ Adobe Photoshop. Самі кольори брав з фрагменту зображення на якому зображено корпус комп’ютера, попередньо перевірив що там однотонна заливка.

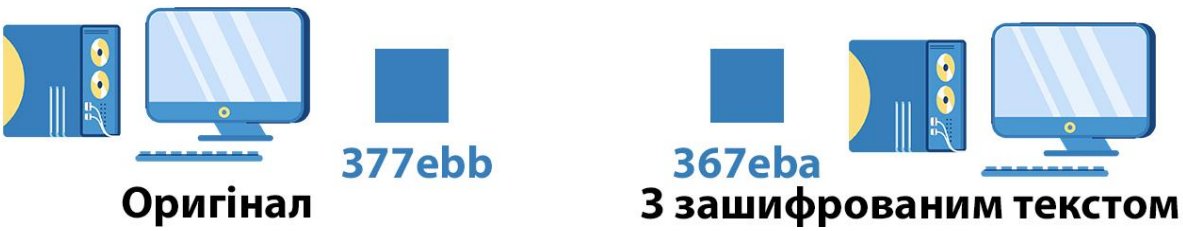

Рисунок.2.8 Порівняння кольорів

Також при порівняв хеш двох зображень, і отримав такі результати:

Оригінал: SHA256
7133D662C58A2BEC07D80AD985649094C8756528541DDE96F51D540E10F03AB3

З зашифрованим текстом: SHA256
1E57E158D259345E04356FFA585C1F3F8132CD00BAA2880BB220DD160AE99AA3

З цих досліджень можна зробити висновок що якщо в зловмисника є оригінал і він може порівняти візуально або порівняти хеш зображень. То він зможе визначити що в одному зображень щось приховане.

Висновок за 2 розділом

У даному розділі було розглянуто базову модель стеганографії, метод дослідження максимальної стійкості стеганографічних систем, методи використання стеганографії для приховування ключа та визначення наявної відмінності між зображенням без прихованого тексту та зображенням з прихованим текстом.

Базова модель стеганографії представляє собою концептуальну схему, яка включає приховування інформації в носії та її витягування на приймачі. Ця модель описує загальний процес стеганографії та визначає основні компоненти системи.

Метод дослідження максимальної стійкості стеганографічної системи є важливим аспектом в процесі проектування та оцінки ефективності стеганографічних методів. Він включає в себе аналіз стійкості прихованої інформації до різних атак, таких як стеганаліз, що дозволяє виявити приховану інформацію. Цей метод допомагає встановити межу між стійкістю та виявленістю прихованої інформації.

Методи застосування стеганографії для приховування ключа є цікавим аспектом, де стеганографія використовується для забезпечення безпеки криптографічних ключів. Це може включати вбудовування ключа в носії або використання стеганографії для передачі ключа в прихованому вигляді, що забезпечує конфіденційність ключової інформації та унеможливлює його виявлення.

Визначення наявної відмінності між зображенням без прихованого тексту та зображенням з прихованим текстом є важливою задачею в стеганографії. Воно

включає порівняння пікселів, статистичний аналіз та визначення різниці візуального враження між цими зображеннями. Це дозволяє виявити наявність прихованої інформації та оцінити її відмінність від оригінального зображення.

Загалом, в розділі було визначено, що базова модель стеганографії, методи дослідження стійкості, використання стеганографії для приховування ключа та визначення відмінності між зображеннями є важливими аспектами стеганографії. Вони допомагають зрозуміти та покращити ефективність стеганографічних систем, забезпечуючи безпеку та надійність приховання інформації.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ МЕТОДІВ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В РІЗНИХ ТИПАХ ДАННИХ

3.1 Метод найменш значущого біта (LSB)

Сучасна стеганографія найчастіше використовує метод LSB (молодший значущий біт) зображення для приховування піксельної інформації. Цей метод найбільш ефективний, коли розмір файлу, який приховується, перевищує розмір вихідного файлу, а також якщо зображення має градації сірого кольору. При використанні методу LSB можна закодувати три біти піксельної інформації в кожному пікселі 24-бітного зображення.

Для кращого розуміння, розглянемо цифрове зображення як двовимірний масив пікселів. Кожен піксель містить значення, залежно від його типу та глибини. Ми розглянемо найбільш поширені режими - RGB (3x8-бітних пікселів, справжній колір) та RGBA (4x8-бітних пікселів, справжній колір з маскою прозорості). Ці значення належать діапазону від 0 до 255 (8-бітні значення) [15]. На Рис.3.1 можна побачити приклад, в якому обрали випадковий піксель з зображення^

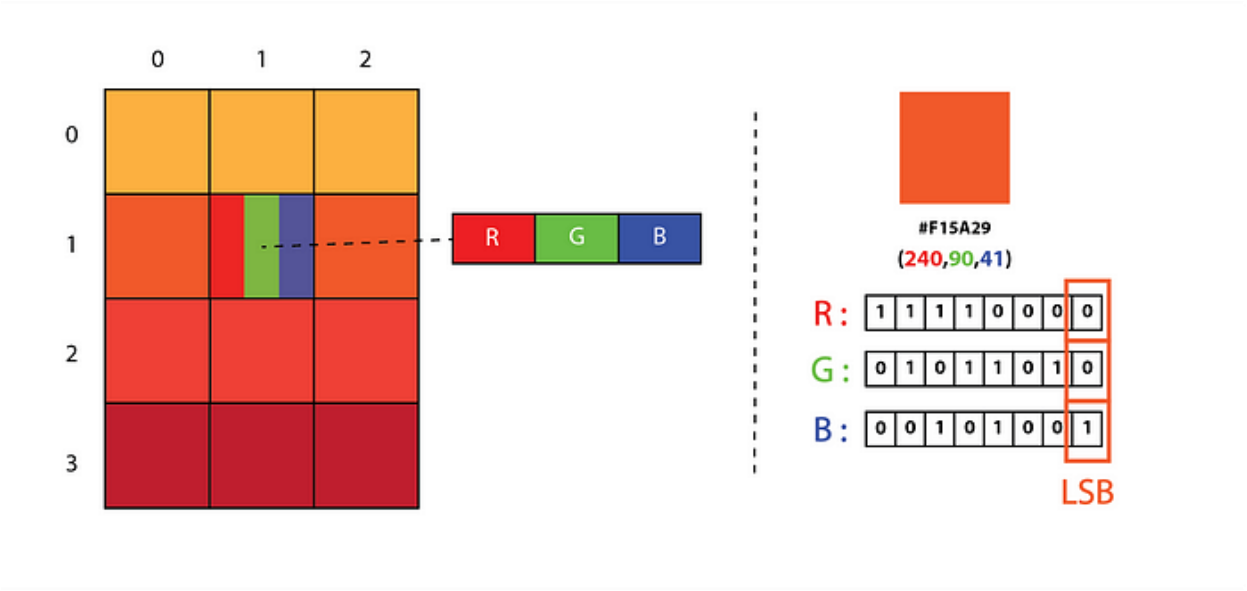

Рисунок.3.1 Визначення найменшого значущого біта

Для прикладу візьмемо такі пікселі:

Піксель №1 (00100111; 11101001; 11001000) – HEX #27e9c8

Піксель №2 (00100111; 11001000; 11101001)

Піксель №3 (11001000; 00100111; 11101001)

а значення нашого повідомлення А:

01000001

Результат буде наступним:

(00100110 11101001 11001000) – HEX #26e9c8

(00100110 11001000 11101000)

(11001000 00100110 11101001)

Алгоритм для методу LSB

Користувач повинен ввести stego-ключ як пароль (stego-ключ використовується для вбудови секретного повідомлення в файл-обкладинку). Після вставки секретного повідомлення в файл-обкладинку, отриманий стего-зображення надсилається отримувачеві через бажаний канал зв'язку. При визначенні точки початку вбудови LSB спочатку збирається stego-ключ від користувача. Обчислюється сума ASCII-значення кожного символу stego-ключа, а потім обчислюється середнє значення цих символів. Під час заміни секретного повідомлення у LSB файлу-обкладинки, перша позиція LSB вибирається відповідно до обчисленого середнього значення символів введеного stego-ключа. Потім процес заміни буде продовжуватися до кінця секретного повідомлення.

На стороні відправника, для вбудовування секретного повідомлення в обкладинку зображення, застосовується алгоритм з такими кроками:

1. Отримання вхідного зображення обкладинки і секретного повідомлення, яке потрібно приховати.

2. Приймання стего-ключа від користувача та обчислення середнього значення символів ключа.

3. Застосування перетворення до кожного символу секретного повідомлення та кожного біту молодшого значущого біту (LSB) червоного каналу зображення обкладинки згідно з положенням середнього значення стего-ключа.

4. Заміна молодших значущих бітів (LSB) червоного каналу зображення обкладинки бінарними значеннями секретного повідомлення, починаючи з початкової точки і закінчуючи кінцем повідомлення.

5. Вставлення спеціального кінцевого символу в кінці секретного повідомлення для позначення його завершення.

6. Обчислення показників якості, таких як PSNR (Пікове співвідношення сигналу до шуму) і SNR (Співвідношення сигналу до шуму), між вихідним зображенням та отриманим стего-зображенням.

7. Відправка стего-зображення одержувачу для подальшого відновлення секретного повідомлення.

Також можна використовувати метод LSB та симетричний ключ:

LSB має переваги у простоті вбудовування бітів повідомлення безпосередньо в площину LSB обкладинки, і багато методів використовують ці методи [16]. Застосування модуляції LSB не призводить до помітної відмінності для людини, оскільки зміна амплітуди є невеликою. Таким чином, тегове зображення, отримане за допомогою LSB, майже не відрізняється від зображення обкладинки, що забезпечує високу прозорість відображення LSB.

Однак, використання LSB має деякі недоліки. Він дуже чутливий до будь-якого виду фільтрації або маніпуляції зі стего-зображенням. Наприклад, масштабування, обертання, кадрування, додавання шуму або стиснення з втратами до стего-зображення може призвести до втрати повідомлення.

Розмір інформації, яку можна приховати, залежить від розміру зображення обкладинки. Щоб зберегти високу пропускну здатність, розмір повідомлення має бути меншим за розмір зображення обкладинки. Користування зображення обкладинки з великою ємністю дозволяє приховувати більше інформації в меншому зображенні обкладинки, що зменшує пропускну здатність, яка необхідна для передачі стего-зображення.

Ще одним недоліком є те, що зловмисник може легко знищити приховане повідомлення, видаливши або обнуливши всю площину LSB. При цьому якість сприйняття модифікованого стегозображення змінюється мінімально. Тому, якщо

цей метод викликає підозри у когось, що щось приховується в стего-зображенні, то він вже не є ефективним.

Також LSB є найпростішим способом вставлення інформації в цифровий аудіофайл. Цей метод полягає в заміні молодшого значущого біта кожної точки вибірки двійковим повідомленням, що дозволяє закодувати велику кількість даних. У кодуванні LSB ідеальна швидкість передачі даних становить 1 кбіт/с на 1 кГц. Але деякі реалізації кодування LSB замінюють два молодших біта вибірки двома бітами повідомлення, що збільшує кількість даних, які можна закодувати, але також збільшує кількість шуму в аудіофайлі.

Для збільшення ліміту до чотирьох бітів розроблений новий метод, який створений Недєлко Цвеїч, Тапіо Сеппбен і mediaTeam Oulu з лабораторії обробки інформації Університету Оулу у Фінляндії. Щоб отримати секретне повідомлення з LSB-закодованого звукового файлу, приймачу потрібен доступ до послідовності вибіркових індексів, які використовуються в процесі вбудовування.

Зазвичай довжина секретного повідомлення, яке потрібно закодувати, менша за загальну кількість зразків у звуковому файлі. Після цього потрібно вирішити, як вибрати підмножину зразків, які міститимуть секретне повідомлення, і повідомити це рішення одержувачу. Один із простих способів полягає в тому, щоб почати з початку звукового файлу і виконувати кодування LSB, доки повідомлення не буде повністю вбудовано, залишаючи решту зразків без змін.

Крім того, в кодуванні LSB є ще одна проблема, пов'язана зі стійкістю до атак. Якщо зловмисник володіє оригінальним файлом, він може порівняти його з LSB-закодованим файлом і виявити, де відбулися зміни. Щоб уникнути цього, можна використовувати метод, який забезпечує випадковість вбудовування даних. Наприклад, можна вибирати випадковий підмінний біт замість молодшого значущого біта. Це знижує ймовірність виявлення стеганографічної вбудовки, оскільки зловмиснику доведеться вибрати правильний біт для заміни. Однак цей метод збільшує обчислювальну складність процесу вбудовування, оскільки потрібно генерувати випадкові числа.

Існує також ризик втрати даних при передачі LSB-закодованих файлів через мережу. Якщо аудіофайл буде сильно стиснутий або буде переданий через шумну мережу, може статися так, що підмінні біти будуть пошкоджені, і це призведе до втрати даних. Щоб уникнути цього, можна використовувати методи корекції помилок, такі як кодування з помилковою корекцією, які дозволяють виявляти та виправляти помилки при передачі даних.

Незважаючи на ці обмеження, вбудовування інформації в аудіофайли за допомогою кодування LSB є досить простим і ефективним методом. Цей метод може бути застосований в багатьох сферах, включаючи криміналістику, наукові дослідження, охорону авторських прав та інші.

Існують дві основні недоліки, пов'язані з використанням методів, таких як кодування LSB:

Перший недолік полягає в тому, що людське вухо є надзвичайно чутливим і може легко виявляти навіть найменші звуки, що вводяться в звуковий файл. Другий недолік полягає в тому, що такий метод не є надійним. Якщо звуковий файл з вбудованою секретною інформацією, закодованою методом LSB, буде підданий перекодуванню, то вбудована інформація буде втрачена. Щоб покращити надійність, можна застосовувати техніку надмірності під час кодування секретного повідомлення. Проте, використання методів надмірності призводить до значного зниження швидкості передачі даних.

3.1.1 Метод Pixel Value Differencing

Метод стеганографії, в якому використовуються біти молодшого значущого біта (LSB) пікселів для приховування секретних даних, є відомим та давнім. Однак, метод LSB є вразливим до аналізу розподілу значень RGB . Дослідники Ву та Цай [17] виявили, що крайові області зображення можуть надавати більше простору для приховування даних порівняно з гладкими областями. Вони розробили метод стеганографії, відомий як Pixel Value Differencing (PVD), який базується на цьому принципі.

Метод стеганографії Pixel Value Differencing (PVD) є одним із способів приховування інформації у цифрових зображеннях. Він базується на аналізі відмінностей між піксельними значеннями сусідніх пікселів у зображенні. Принцип роботи PVD полягає у використанні незначних змін в піксельних значеннях для кодування прихованого повідомлення. Зображення, в якому буде приховуватися інформація, називається покривальним зображенням, а повідомлення - прихованим повідомленням [18].

Основні кроки методу PVD:

Крок 1. Вибирається піксель у покривальному зображенні, який буде використовуватися для приховування бітової інформації.

Крок 2. Вибирається сусідній піксель, зазвичай ліворуч або вище, відносно пікселя-господаря.

Крок 3. Обчислюється різниця між піксельними значеннями пікселя-господаря та пікселя-сусіда.

Крок 4. Приховане повідомлення біт за бітом кодується у найменш значущих бітах різниці піксельних значень. Це змінює незначну кількість піксельних значень, що візуально малопомітна.

Крок 5. Кроки 2-4 повторюються для всіх пікселів, у які приховується інформація.

У даному методі обкладинка зображення використовується для приховування секретного повідомлення у вигляді довгого потоку бітів. Цей метод, використовується для захисту конфіденційної інформації у зображеннях, які мають 256 градацій сірого кольору, був запропонований у 2004 році. В даному методі використовується різниця між сусідніми пікселями для визначення можливої кількості вставлених бітів у зображення. Чим більша різниця між пікселями, тим більше фрагментів секретного повідомлення може бути приховано. Це означає, що при наявності великої різниці між пікселями, можна вставити більше бітів секретного повідомлення. Зображення сканується зигзагоподібно, починаючи з верхнього лівого кута, і поділяється на блоки, кожний з яких містить два послідовних неперекриваються пікселі. У блоках різниця між пікселями використовується для визначення властивостей гладкості зображення обкладинки. Це допомагає визначити

місцезнаходження пікселів. Значення різниці менше вказує на гладку область, тоді як більші значення вказують на крайові області. Секретні біти даних зберігаються саме у крайових областях, оскільки їх важко помітити для людського ока, ніж якщо зберігати їх у гладких областях.

Для проведення порівняльного аналізу було використано зображення, отримане з наукової статті:

Оригінал

З закодованим повідомленням

3.2 Фазове кодування

Фазове кодування зменшує недоліки методів аудіо стеганографії, які стикаються з проблемами шуму. Основу фазового кодування складає той факт, що людське вухо менш чутливе до фазових компонентів звуку, ніж до шуму. Замість введення додаткового шуму, ця техніка кодує біти повідомлення у вигляді змін фазового спектру цифрового сигналу, що дозволяє досягти непомітного кодування з точки зору співвідношення сигнал/шум. На Рис 3.2 показано оригінальний та закодований сигнали.

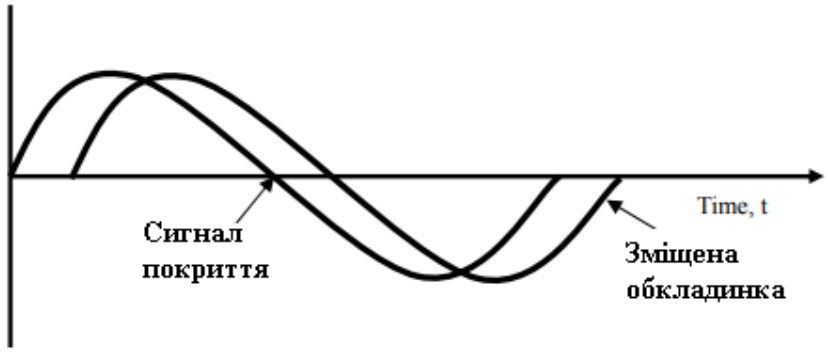

Рисунок.3.2 Вихідний сигнал покриття та сигнал, отриманий шляхом зміщення і фазового кодування.

Пояснення процедури кодування фаз включає наступні кроки:

- Початковий звуковий сигнал $s[i], (0 \leq i \leq I-1)$ розбивається на серію коротких сегментів $s_n[i], (0 \leq n \leq N-1)$, довжина кожного з них відповідає розміру повідомлення , яке має бути закодоване.
- До n-го сегмента сигнала $s_n[i]$ застосовується k-точкове дискретне перетворення Фур'є (ДПФ), де $\phi = I/N$ і створюються матриці фаз $\phi_n(w_k)$ і амплітуда $A_n(w_k)$, для $(0 \leq k \leq K-1)$
- Обчислюються різниці фаз між сусідніми сегментами, $(0 \leq n \leq N-1)$:

$$\Delta\phi_{n+1}(w_k) = \phi_{n+1}(w_k) - \phi_n(w_k) \qquad (6)$$

- Фазові зсуви між послідовними сегментами можуть бути легко виявлені. Іншими словами, абсолютні фази сегментів можуть змінюватись, але відносні різниці фаз між сусідніми сегментами повинні бути збережені. Тому секретне повідомлення вставляється лише у вектор фази першого сегмента сигналу наступним способом:

$$Phas\_new = \begin{cases} Phase\_old + \frac{\pi}{2}, \text{якщо біт повідомлення} = 1 \\ Phase\_old + \frac{\pi}{2}, \text{якщо біт повідомлення} = 0 \end{cases} \qquad (7)$$

- Створення нової фазової матриці відбувається шляхом поєднання нової фази першого сегмента та початкової різниці фаз.

- Шляхом використання цієї нової фазової матриці разом з оригінальною матрицею амплітуд, звуковий сигнал відновлюється за допомогою оберненого ДПФ, а потім звукові сегменти об'єднуються разом.

Для отримання секретного повідомлення з звукового файлу одержувач повинен знати довжину сегмента. Потім він може використовувати ДПФ для отримання фаз та вилучення інформації. Однак, одним недоліком фазового кодування є низька швидкість передачі даних, оскільки секретне повідомлення кодується лише у першому сегменті сигналу. Цю проблему можна вирішити, збільшивши довжину сегмента сигналу. Однак, це призводить до більш раптових змін у співвідношенні фаз між кожною частотною складовою сегмента, що полегшує виявлення кодування. В результаті фазове кодування використовується, коли потрібно приховати лише невеликий обсяг даних, наприклад, для водяного знаку.

Один з недоліків методу фазового кодування полягає в тому, що корисне навантаження значно обмежене, оскільки лише перший блок використовується для вбудовування секретного повідомлення (M). Крім того, повідомлення M не розподіляється по всій стегоконтейнеру C, що означає, що дані є локалізованими, і їх можна легко видалити за допомогою атаки обрізання. [19]

3.2 Метод Echo Hiding

Метод стеганографії "Echo hiding" є одним з підходів до приховування секретної інформації в аудіофайлах. Його основна ідея полягає в використанні особливостей звукових хвиль, що несприйнятні для людського вуха, для вбудовування конфіденційних даних.

У процесі застосування методу "Echo hiding", аудіофайл розбивається на невеликі сегменти, в які вбудовуються фрагменти секретного повідомлення. Ці фрагменти впроваджуються в області звукових хвиль, що зазвичай відповідають за ехо або відлуння, і мають мінімальну амплітуду, непомітну для сприйняття людиною.

Після вбудовування секретних даних, аудіофайл може бути програваним без помітних змін, і лише при використанні відповідної процедури демаскуючого аналізу

можливе виявлення прихованої інформації. Демаскування базується на знанні алгоритму вбудовування, який допомагає відновити приховані дані з аудіофайлу. Необхідно відзначити, що цей метод має свої обмеження та недоліки. Він обмежується обсягом інформації, яку можна вбудувати в аудіофайл, існує ризик втрати даних під час стиснення аудіофайлу та можливість помітної зміни якості звуку. Тому при використанні даного методу важливо ретельно враховувати значимість прихованої інформації та її вплив на якість аудіофайлу [20].

Для вбудовування інформації в аудіо файл використовується така формула:

$$x_{\text{сг}}(n) = x(n) + \alpha * m(n) * h(n) \quad (8)$$

Де:

$x_{\text{сг}}(n)$ - стегосигнал (звуковий сигнал після вбудовування),

$x(n)$ - оригінальний звуковий сигнал,

α - параметр вбудовування, який визначає величину впливу секретного повідомлення на звуковий сигнал

$m(n)$ - бінарне повідомлення (0 або 1),

$h(n)$ - функція ехо, яка визначає області звукових хвиль, в які можна вбудовувати секретну інформацію.

n - відповідає дискретному часу аудіофайлу, тобто позиції в часовому ряді звукового сигналу [22].

Розглянемо переваги та недоліки цього методу

До переваг можна віднести:

- Забезпечує прихованість секретної інформації в звуковому сигналі. При правильному вбудовуванні, стегосигнал виглядає майже ідентичним до оригінального сигналу, що робить його важким для виявлення звичайними методами.
- Використовує ехо-зони в звуковому сигналі для вбудовування секретної інформації. Це дозволяє використовувати наявні резерви в сигналі без необхідності введення додаткових даних або створення нових структур.
- При правильному вбудовуванні секретного повідомлення методом Echo hiding несправні зміни в якості звуку практично непомітні. Стегосигнал звучить майже так само, як і оригінальний сигнал [21].

Недоліки методу "Echo hiding":

- Метод може бути вразливим до атак, зокрема до атак на стиснення аудіофайлів або до атак на видалення даних. Під час стиснення аудіофайлу може втрачатись деяка інформація, що може призвести до втрати секретних даних. Крім того, атака на видалення даних може призвести до видалення ехо-зон, де вбудовується інформація, і знищити секретне повідомлення.
- Обмежена пропускна здатність для вбудовування секретної інформації. Це пов'язано з тим, що вбудовування відбувається лише в областях з ехо-зонами, які можуть бути обмеженими в звуковому сигналі.
- Можуть відбутись незначні зміни в якості звуку через вбудовування секретного повідомлення. Деякі люди можуть помітити ці зміни або вплив на відтворення звуку [21].

3.3 Текстова стеганографія

Залежно від носія, який використовується для введення секретних даних, стеганографія може бути класифікована на зображення, текст, аудіо та відео стеганографію. У стеганографії тексту можуть застосовуватися різноманітні методи, включаючи зміну форматування існуючого тексту, зміну слів у тексті, генерацію випадкових послідовностей символів або використання контекстно-вільних граматик для створення читабельних текстів. В порівнянні з іншими типами документів, такими як зображення, аудіо- або відеофайли, текстова стеганографія вважається найскладнішою через відсутність надлишкової інформації в тексті, яку можна використати для приховування. В стеганографії зображень або аудіофайлів можуть вноситися непомітні зміни, тоді як в текстових файлах навіть додаткова літера або розділовий знак можуть бути помітними для випадкового читача . Завдяки меншому обсягу пам'яті, необхідного для зберігання текстового файлу, а також швидкій та простій передачі даних, стеганографія тексту вважається більш практичним методом порівняно з іншими типами стеганографії. Загалом, стеганографію тексту можна

класифікувати на три типи: випадкову та статистичну генерацію на основі формату, лінгвістичні методи.

Рисунок 3.3 Різновиди текстової стеганографії

3.3.1 Format-based steganography

У даній формі стеганографії використовуються фізичні особливості текстових символів, що змінюються таким чином, що їх не сприймає людське око. Наприклад, рядки тексту переміщуються вертикально, приховуючи фрагменти секретних даних, а слова переміщуються горизонтально або вертикально. Деякі пробіли між словами, абзацами або рядками також можуть використовуватися для приховування даних. Використання особливостей фізичного формату тексту дозволяє змінювати фізичні характеристики слів, щоб заховати інформацію, залежно від символів і мови. Численні дослідження в цій галузі розширюють можливості стеганографії тексту шляхом зміни фізичних властивостей текстового формату.

Зміщення рядка

У цьому методі секретне повідомлення заховане шляхом вертикального зсуву рядків тексту на певну відстань . Позначена лінія має дві невидимі контрольні лінії по обидва боки для визначення напрямку зсуву. Для захування біту 0 рядок зсувається вгору, а для захування біту 1 рядок зсувається вниз. Визначення напрямку зсуву виконується шляхом вимірювання відстані між центроїдом позначеної лінії та її контрольними лініями [23]. Однак, якщо текст буде перенабраний або використовується програма оптичного розпізнавання символів (OCR), прихована

інформація може бути втрачена. Також можна спостерігати відстані за допомогою спеціальних пристроїв для оцінки відстаней [24].

Процес вбудовування секретного повідомлення за допомогою методу зміщення рядка передбачає внесення змін у відстані між рядками або висоту рядків у текстовому документі. Це може включати збільшення або зменшення відстані між рядками, що незначно змінює вид тексту, але залишає його читабельним для людини.

Приховане повідомлення вставляється шляхом регулювання розміщення рядків у документі залежно від бітової послідовності секретної інформації. Наприклад, зміщення рядка може бути виконане, додавши додатковий проміжок після кожного n-го рядка, де n - це певне число, що відповідає бітовій послідовності. Іншим варіантом може бути встановлення різних висот рядків у відповідності до значень бітів повідомлення. Процес виявлення і витягування прихованої інформації з текстового документа, отриманого за допомогою методу зміщення рядка, виконується шляхом аналізу відстаней між рядками або висот рядків. При належному розумінні правил вбудовування, отримувач може виявити та відновити секретне повідомлення з тексту. Метод зміщення рядка має свої переваги і обмеження. Він є візуально непомітним, оскільки зміни розміщення рядків зазвичай не привертають увагу читача. Однак, використання цього методу може бути обмежене в ситуаціях, де документи проходять обробку або піддаються автоматичному аналізу, який може розкрити приховану інформацію.

Зміщення слів

У цьому методі секретне повідомлення приховується шляхом зсуву слів горизонтально, тобто вліво або вправо, для представлення біту 0 або 1 відповідно. Зміщення слів виявляється за допомогою кореляційного методу, який порівнює профіль як форму хвилі та вирішує, чи походить він від сигналу, середній блок якого був зміщений вліво або вправо. Цей метод може бути менш очевидним, оскільки зміна відстані між словами для заповнення рядка є відносно поширеною. Однак, якщо хтось знає алгоритм визначення відстаней, він може порівняти стеготекст з алгоритмом і отримати приховану інформацію, використовуючи відхилення. Крім того, повторне введення або використання програм оптичного розпізнавання символів (OCR) може

призвести до втрати прихованої інформації [25]. На зображенні Рис.3.4 зображено приклад приховування інформації шляхом зміщення слів

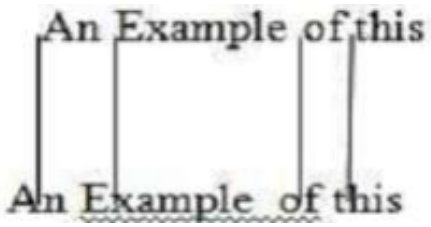

Рисунок.3.4 Приховування інформації за допомогою зміщення слів

Метод зміщення слів має свої переваги та обмеження. З одного боку, він є візуально непомітним та здатним внести значну кількість інформації у текстовий документ, а також проявляє високу стійкість до виявлення з боку неавторизованих осіб. З іншого боку, метод може бути вразливим до аналізу тексту, автоматичного розпізнавання та обробки, що може привести до розкриття прихованого повідомлення.

Кодування ознак

У даному методі кодування ознак відбуваються зміни деяких функцій тексту. Наприклад, кінцева частина певних символів, таких як "h", "d", "b" і т.д., може бути подовжена або трохи скорочена, змінюючи тим самим текст і приховуючи інформацію. Цей метод дозволяє приховати великий обсяг інформації в тексті, не розкриваючи читачеві наявність такої інформації. Зафіксована форма розміщення символів призводить до втрати інформації. Повторне форматування тексту або використання програм оптичного розпізнавання символів (OCR) може призвести до втрати прихованої інформації .

3.3.2 Метод випадкової та статистичної генерації

Випадкова та статистична генерація використовується для створення обкладинки, яка відповідає статистичним властивостям. Цей метод заснований на послідовності символів і слів.

Відображення слів

Ця техніка включає шифрування секретного повідомлення за допомогою генетичного перехресного оператора, а потім вставку отриманого шифрованого тексту у файл обкладинки. Для цього використовуються два біти одночасно, які вставляються у файл обкладинки за допомогою пробілів між словами парної або непарної довжини. Для досягнення цього використовується певна техніка відображення. Позиції вставки зберігаються в окремому файлі і передаються разом із стегооб'єктом до отримувача.

Документ MS Word

У цій техніці сегменти тексту в документі піддаються деградації, щоб імітувати низьку письмову майстерність автора. При цьому секретне повідомлення вбудовується у вибрані деградовані елементи, які потім відстежуються з метою виявлення змін. Процес вкладання даних здійснюється таким чином, що стегодокумент маскується як звичайний текст, що виглядає як результат спільного написання [26].

3.3.3 Лінгвістичний метод

Лінгвістичний метод - це підхід до стеганографії, який комбінує методи синтаксису та семантики для приховування секретної інформації в текстових документах. Цей метод базується на використанні особливостей мови та мовних конструкцій для вбудовування інформації, що робить його візуально непомітним для неповідомленого спостерігача.

Одним з ключових аспектів лінгвістичного методу є використання синтаксичних правил мови. Синтаксис описує правила, які визначають правильну структуру речень та фраз в мові. В стеганографії цей принцип використовується для гарантії, що вбудована інформація не порушує синтаксичну правильність тексту. Таким чином, приховане повідомлення вписується в межі допустимих синтаксичних конструкцій, що дозволяє зберегти натуральний вигляд тексту. Крім синтаксису, лінгвістичний метод також використовує семантику - вивчення значень слів і їх

зв'язків. В цьому контексті стеганографія використовує синоніми - слова, які мають подібне або близьке значення, але відрізняються в своїй лексичній формі. Синонімна заміна слів дозволяє приховувати бітову інформацію в тексті, замінюючи одне слово на його синонім, що не суттєво змінює семантику речення або тексту загалом. Це дозволяє зберегти зміст повідомлення, одночасно приховуючи його існування в тексті.

Семантичний метод

У даному методі використовуються синоніми для певних слів з метою заховати інформацію в тексті. Заміна слів синонімами може відображати одну або кілька бітових комбінацій, що відносяться до секретної інформації. Однак, важливо зауважити, що цей метод може змінити смисл тексту.

Інтервали між словами та інтервали між абзацами

У методі інтервалів між словами, секретне повідомлення вбудовується за допомогою пробілів, які розміщуються між словами. Цей метод використовує один пробіл для кодування біта "0" та два пробіли для кодування біта "1". У методі Манчестер використовуються проміжки між словами для визначення прихованих бітів секретного повідомлення. Наприклад, "01" і "10" кодуються як "1" біт і "0" біт відповідно, тоді як "00" і "11" не використовуються для приховування даних. На Рис.3.5 зображено як виглядає текст при приховуванні в ньому інформації шляхом інтервалів

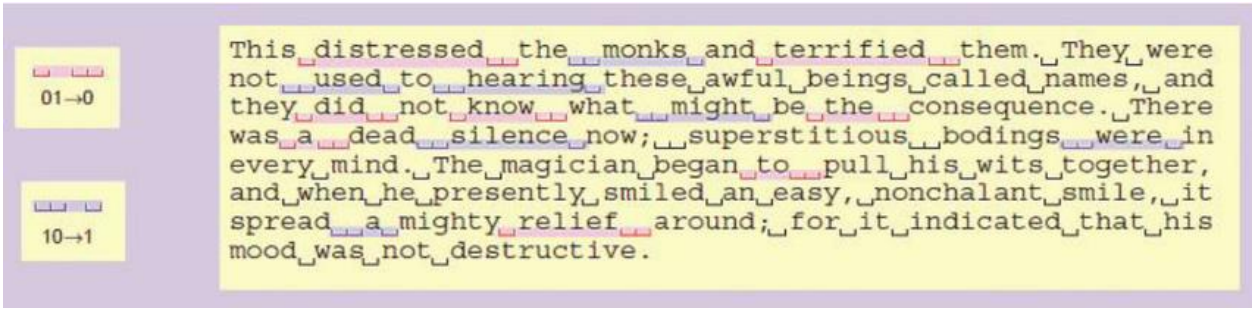

Рисунок.3.5 Приховування інформації за допомогою інтервалів

У методі кінцевих пробілів, секретне повідомлення заховане в кінці кожного рядка шляхом вставки додаткових пробілів. За допомогою кінцевих інтервалів між рядками можна приховати різну кількість бітів секретного повідомлення. Наприклад,

використовуючи два пробіли можна приховати 1 біт, використовуючи чотири пробіли можна приховати 2 біти, а з восьми пробілів можна приховати 3 біти секретного повідомлення і так далі. На Рис.3.6 зображено приклад використання цього методу

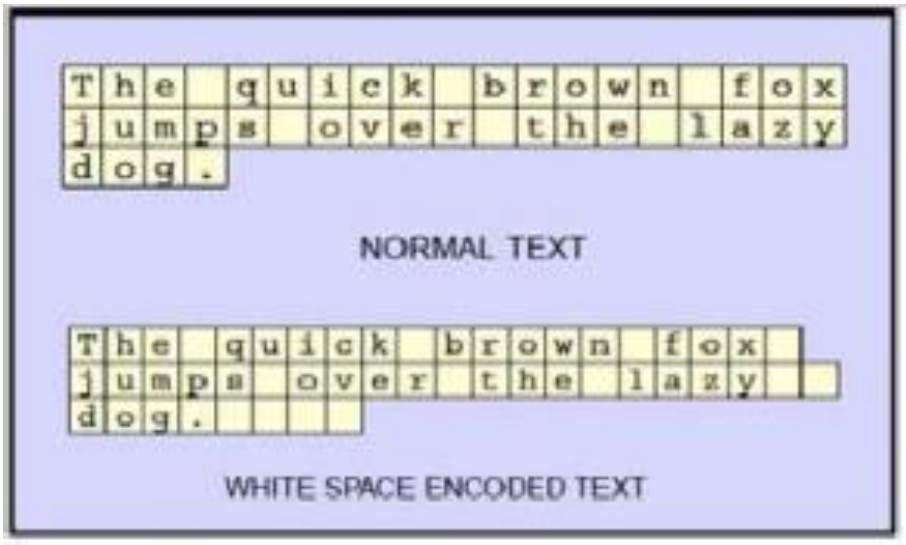

Рисунок.3.6 Метод кінцевих пробілів

У методі інтервалу між абзацами, секретне повідомлення приховується шляхом вставки пробілу між двома рядками або порожнього рядка між абзацами. Цей пробіл або порожній рядок використовується для передачі бітової інформації, а кількість вставлених пробілів визначає кількість прихованих бітів. Наприклад, один пробіл може представляти 1 біт, а порожній рядок - 0 бітів [27]. Приклад цього методу зображено на Рис.3.7

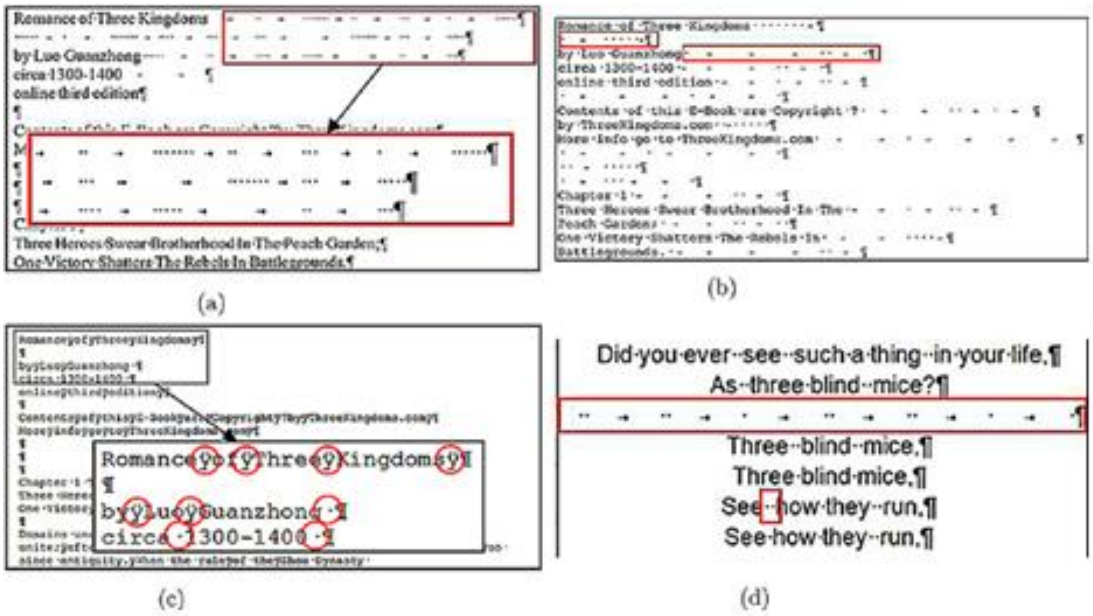

Рисунок.3.7 Приклад приховування в інтервалі між абзацами

3.4 Розгляд використання методу зміни інтервалів

Розберемо послідовність дій для приховування тексту або ключа в тексті за допомогою пробілів між словами. Для цього візьмемо такі позначення, де «0» - це один пробіл, а «1» це відповідно два пробіли. Візьмемо якийсь текст як на Рис.3.8

Україна завжди асоціюється з безкраїми золотими ланами під чистим блакитним небом. Повний дозрілий колос пшениці символізує багатство та родючість, він важкий і хилиться до самої землі, ніби дякуючи за силу, якою вона його наповнила. Над ланами легко кружляють птахи, і далеко навкруги розноситься їхній спів.

Рисунок.3.8 Текст для приховування

Також візьмемо слово яке будемо приховувати, я обрав слово «key».

Далі переводимо це слово в бінарний вигляд:

«01101011 01100101 01111001»

Тепер за описаними позначеннями розставляємо пробіли в тексті. В мене вийшов такий результат який зорбражено на Рис.3.9

Україна завжди асоціюється з безкраїми золотими ланами під чистим блакитним небом. Повний дозрілий колос пшениці символізує багатство та родючість, він важкий і хилиться до самої землі, ніби дякуючи за силу, якою вона його наповнила. Над ланами легко кружляють птахи, і далеко навкруги розноситься їхній спів.

Рисунок.3.9 Результат приховування слова

Для більш помітного розгляду ввімкну відображення всіх знаків в програмі Word. Та позначу відповідні значення. Результат зображено на Рис.3.10

Україна[0]завжди[1]·асоціюється[1]·з[0]безкраїми[1]·золотими[0]ланами[1]·під[1]·чистим[0]·блакитним[1]·небом.[1]·Повний[0]·дозрілий[0]колос[1]·пшениці·[0]символізує[1]·багатство[0]та[1]·родючість,[1]·він[1]·важкий[1]·і[0]хилиться[0]до[1]·самої·землі,·ніби·дякуючи·за·силу,·якою·вона·його·наповнила.·Над·ланами·легко·кружляють·птахи,·і·далеко·навкруги·розноситься·їхній·спів.¶

Рисунок.3.10 Дослідження тексту

Відповідно написавши послідовність отриманих «0» та «1» та розбивши її по групах з 8 символів отримаємо наше зашифроване слово.

Провівши це дослідження можна зазначити що воно є доволі непомітним для ока людини і тому може бути використано як метод приховування інформації, але він комп'ютера таке приховати не можливо. Також сам процес приховування є не зручним і щоб приховати великий обсяг тексту, потрібно щоб в нас обсяг тексту в який ми хочемо приховати моє бути більшим в n-разів.

Висновок за 3 розділом

В даному розділі було розглянуто кілька методів стеганографії, що дозволяють приховувати інформацію в непомітний спосіб. Кожен з цих методів має свої особливості та переваги.

Метод найменш значущого біта (LSB) є одним з найпоширеніших методів стеганографії. Він полягає у заміні найменш значущих бітів покривального контейнера на біти прихованого повідомлення. Цей метод відносно простий у реалізації і може бути застосований до різних типів медіа, таких як зображення, звук і відео. Однак, його недоліком є відносно низька стійкість до атак і можливість виявлення змін у стегоконтейнері.

Фазове кодування є методом стеганографії, який використовує зміни у фазі сигналу для приховування інформації. Цей метод досить складний у реалізації, але він забезпечує високу стійкість до атак і невиявлення змін у стегоконтейнері. Він широко застосовується в аудіостеганографії та відеостеганографії, де приховування інформації проводиться на рівні аудіосигналу чи відеопотоку.

Метод Echo Hiding (приховування ехо) використовує властивості аудіопотоку та його ехо для приховування інформації. Він базується на затримці та накладанні ехо-сигналу на оригінальний аудіопотік. Цей метод може бути використаний для стійкого приховування повідомлення в аудіофайлах. Він відносно надійний і має високу стійкість до атак, оскільки ехо-зміни зазвичай непомітні для слухача.

Текстова стеганографія, як назва вказує, використовує текстові повідомлення для приховування інформації. Цей метод може використовувати різні техніки, такі як внесення змін у форматування тексту, використання резервованих символів або заміна певних слів. Він забезпечує високу стійкість до виявлення, оскільки текстові повідомлення зазвичай мають великий обсяг і непомітні зміни можуть легко затонути у текстовому контенті.

В цьому розділі ми розглянули різні методи стеганографії, кожен з яких має свої переваги та обмеження. Вибір методу залежить від конкретного застосування та вимог щодо стійкості до атак. Незалежно від обраного методу, стеганографія є потужним інструментом для приховування інформації та забезпечення конфіденційності комунікацій.

ВИСНОВКИ

У дипломній роботі було розглянуто методи та засоби стеганографії для приховування інформації в зображеннях, аудіо та текстових файлах.

У першій частині дипломної роботи були розглянуті перші прояви стеганографії та як вона розвивалась до теперішнього часу. В роботі проаналізовано різницю між криптографією і стеганографією. Криптографія в основному займається шифруванням повідомлення з метою забезпечення конфіденційності та цілісності даних. З іншого боку, стеганографія спрямована на таємне приховування самого факту існування повідомлення. Її ціль полягає в тому, щоб зробити саме існування прихованого повідомлення якомога менш помітним.

В другій частині дипломної роботи було розглянуто базову модель стеганографії, яка є основою для приховування інформації в різних типах медіа, таких як зображення, аудіо та текст. Метод дослідження максимальної стійкості стеганографічної системи був обговорений з метою забезпечення надійності та непомітності прихованої інформації.

Досліджено різні методи застосування стеганографії в якості приховування ключа, що дозволяє забезпечити безпеку комунікації та захист від несанкціонованого доступу до конфіденційної інформації. Використання стеганографії для приховування ключа дозволяє зберегти конфіденційність інформації навіть у випадку перехоплення або атаки на саму систему шифрування.

Також було проведено визначення наявної відмінності між зображенням без прихованого тексту та зображенням з прихованим текстом. Це дослідження дозволило оцінити рівень помітності змін, внесених стеганографічним алгоритмом.

У третій частині дипломної роботи були розглянуті методи стеганографії та наведені рекомендації по їх використанню:

- Зображення: Використовуйте метод LSB для невеликих обсягів інформації, оберіть формат зображення відповідно до потреб, враховуйте розмір зображення.

- Аудіо: Використовуйте некомпресовані формати, наприклад, WAV, уникайте стиснутих форматів, приховуйте інформацію у менш помітних частотних діапазонах, збалансуйте кількість інформації та помітність змін.
- Текст: Використовуйте менш очевидні місця для приховування тексту, такі як інтервали між словами або прогалини в документі.

Виходячи із поставленої мети дипломної роботи були виконані наступні завдання:

- досліджено різні методи приховування інформації в зображенні, аудіо та текстовому файлах.
- проведено аналіз методів приховування інформації в зображенні, тексті та визначено алгоритм роботи цих методів та було визначена відмінність між оригінальним файлом і з прихованою інформацією.
- надані практичні рекомендації для приховування інформації в різних типах даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A. Siper, R. Farley, C. Lombardo “The Rise of Steganography”, Pace University, 2005, 7с.

2. "Steganography: A Brief History" - [Електронний ресурс]. – Режим доступу: https://www.techopedia.com/

3. “Image Steganography: Concepts and Practice” - [Електронний ресурс]. – Режим доступу: http://sharif.edu/~kharrazi/pubs/ims04.pdf

4. K. Schmeh, P. Horster "Steganography: The Art of Hiding Information", Paperback, 2005, 118с.

5. P. Stavroulakis, M. Stamp "Handbook of Information and Communication Security"

6. H. Taha Sencar, Ali Naci Yildiz та Ahmet Sabit Aktas "Steganography Techniques: A Review and Comparative Study"

7. О. Кузнецов, С. Євсеєв, О. Король “СТЕГАНОГРАФІЯ” : навчальний посібник, Харків. Вид. ХНЕУ, 2011, 232с.

8. “Difference between Steganography and Cryptography” - [Електронний ресурс]. – Режим доступу: https://www.geeksforgeeks.org/difference-between-steganography-and-cryptography/

9. Haripriya Rout, B. K. Mishra “Pros and Cons of Cryptography , Steganography and Perturbation techniques”

10. Y. Frank "Digital Watermarking and Steganography: Fundamentals and Techniques"

11. Стеганографічний алгоритм захисту даних з використанням файлів зображень - [Електронний ресурс]. – Режим доступу: http://www.economy.nayka.com.ua/?op=1&z=5584].

12. Anderson, R. J., "Stretching the Limits of Steganography," in Information Hiding: First International Workshop, Proceedings, vol. 1174 of Lecture Notes in Computer Science, Springer, 1996, 10с.

13. S. Craver, "On Public-Key Steganography in the Presence of an Active Warden" Technical Report RC 20931, IBM, 1997, 368c.

14. “Steganography Online” - [Електронний ресурс]. – Режим доступу: https://stylesuxx.github.io/steganography/

15. “LSB Image Steganography Using Python” - [Електронний ресурс]. – Режим доступу: https://medium.com/swlh/lsb-image-steganography-using-python-2bbbee2c69a2

16. R. Chandramouli, N. Memon, “Analysis of LSB Based Image Steganography Techniques”, IEEE, 2001, с 1019.

17. D.-C. Wu and W.-H. Tsai, “ A Steganographic Method by Pixel-Value Differencing and Exploiting Modification Direction” Journal of Computers Vol. 28, No. 1, 2017, с 29.

18. Fridrich, J., Goljan, M., & Du, R. (2001). “Reliable detection of LSB steganography in color and grayscale images. In Proceedings of the 2001 workshop on Multimedia and security” Magazine of IEEE Multimedia, Special Issue on Security, October-November issue, 2001, с 30.

19. B. Dunbar, “A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment” SANS Institute InfoSec Reading Room, 2002, с 9.

20. Johnson, N. F., & Jajodia, S. « Exploring steganography: seeing the unseen» IEEE Computer, 1998, с 34.

21. Cox, I., Miller, M., & Bloom, J. « Digital Watermarking and Steganography» (2nd ed.). Morgan Kaufmann., 2007, с 624.

22. J. Fridrich, «Steganography in digital media: Principles, algorithms, and applications», Cambridge University Press, 2014, с 466.

23. J. Cummins, P. Diskin, S. Lau, and R. Parlett, “Steganography and digital watermarking” School of Computer Science, 2004, с 593.

24. M. H. S. Shahreza, and M. S. Shahreza, «A new synonym text steganography» Int. Conf. on Intelligent Information Hiding and Multimedia Signal Processing, 2008.

25. L. Y. Por, T. F. Ang, and B. Delina, “WhiteSteg- a new scheme in information hiding using text steganography”, WSEAS Transactions on Computers, 2008, с 10.

26. S. H. Low, N. F. Maxemchuk, J. T. Brassil, and L. O. Gorman, “Document marking and identificationusing both line and word shifting”, Institute of Electrical and Electronics Engineers, c 853.

27. W. Bender, D. Gruhl, N. Morimoto, and A. Lu, “Techniques for data hiding”, Ibm Systems Journal, 1996, c 336.