ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки

каф. ЕОМ

Система захисту інформації з використанням стеганографічних методів

Ст. групи КІУКІ-21-3
Полупан О.Р.

Керівник
ас. Романюк О.С.

2025

2

Мета роботи та завдання

- Мета роботи: створити систему захисту інформації з використанням стеганографічних методів. .

- Завдання:

- Провести аналіз використання стеганографії
- Проаналізувати методи використання стеганографії звукових файлів
- Провести порівняння методів стеганографії
- Розглянути методи шифрування
- Написання та тестування системи.

4

Використання стеганографії

- **Кібербезпека та кіберзлочинність**
- **Комунікації та конфіденційність**
- **Журналістика та анонімність**
- **Піратство та захист власності**
- **Судова медицина**
- **Криптовалюта та фінансова безпека**
- **Цифрові паспорти та біометричні дані**
- **Інтернет речей (IoT)**
- **Правозахист та поліція**

5

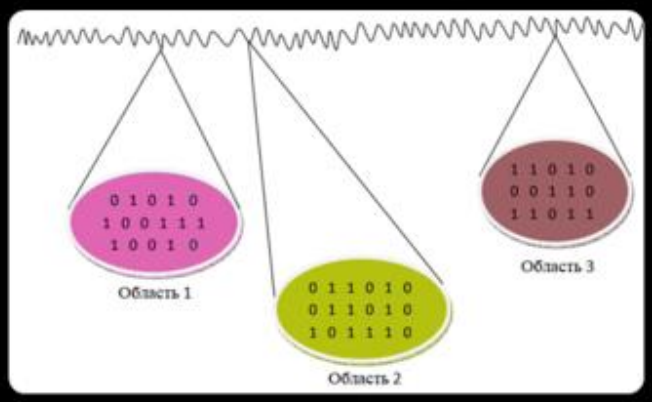
Використання LSB (Least Significant Bit)

- Метод LSB є особливо популярним у стеганографії звукових файлів. Він дозволяє вставляти інформацію в аудіо файл, зберігаючи високу якість звуку, при невдалому використанні цього методу може викликати виникнення шуму в аудіо файлі, який може бути помітним при великій кількості вбудовуваної інформації.

6

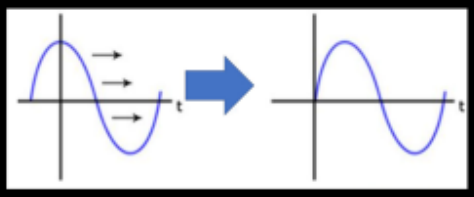
Паритетне кодування

- На відміну від традиційних підходів, де сигнал розбивається на окремі зразки, тут ми беремо кожен зразок і вкладаємо в нього біт парності замість того, щоб використовувати окремі біти для представлення інформації.



7

Фазове кодування



- Фазове кодування використовує фазові характеристики звукового сигналу для приховування інформації. Основні ідеї цього методу включають заміну фази початкового аудіосегменту еталонною фазою, яка представляє секретну інформацію, і корекцію решти фазових сегментів для збереження їхнього відносного фазового зв'язку.

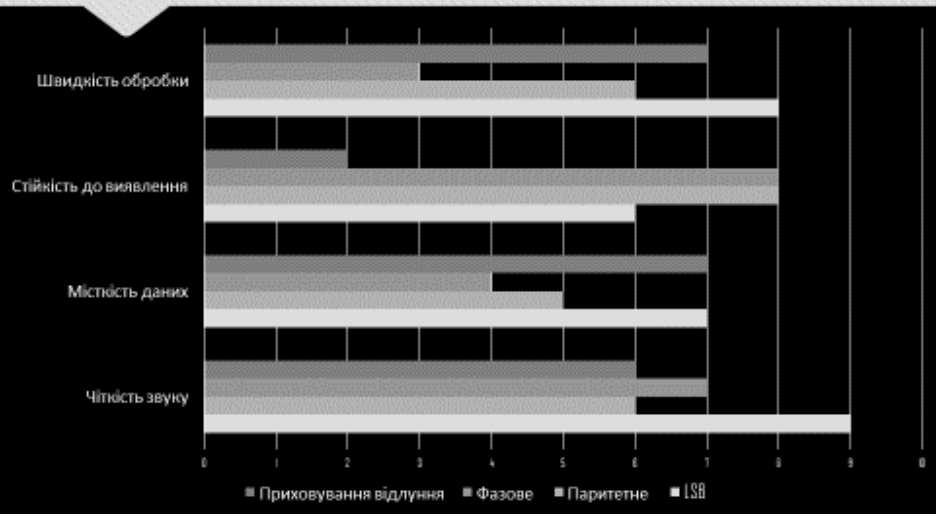
8

Приховування відлуння

- В сфері аудіостеганографії використання техніки відлуння відзначається вбудовуванням конфіденційної інформації у звуковий файл за допомогою внесення додаткових відлунь у дискретний сигнал. Підхід володіє вагомими перевагами, такими як висока швидкість передачі даних і надійність, роблячи його ефективним у порівнянні з іншими методами у деяких сферах застосування.

9

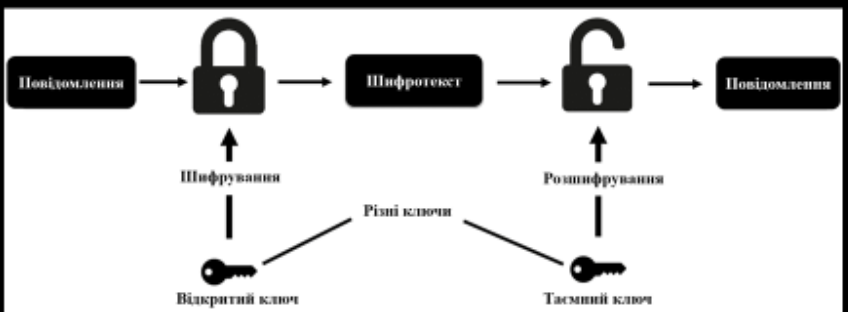
Порівняння методів стеганографії



10

Основні принципи роботи алгоритму RSA

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

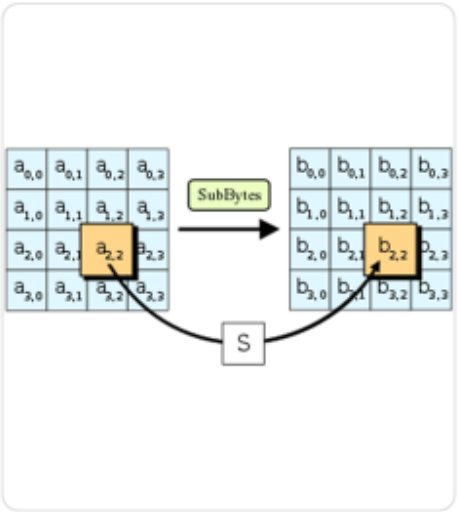


11

Алгоритм шифрування AES

Процес шифрування AES-256 складається з наступних етапів:

- розбиття вхідних даних на блоки по 128 біт;
- додавання раундового ключа до початкового стану;
- виконання 14 раундів перетворень, що включають операції заміни байтів, зсуву рядків, змішування стовпців та додавання раундового ключа;
- додавання фінального раундового ключа.



12

Комбінація AES та RSA

- Використання AES разом з RSA (Rivest-Shamir-Adleman) становить потужну комбінацію для забезпечення безпеки інформації у сучасних системах. RSA використовується для шифрування ключів, які потім використовуються AES для шифрування фактичних даних. RSA і AES доповнюють один одного, використовуючи кожен з них у своїй найбільш ефективній області. RSA ефективно шифрує невеликі обсяги даних (у нашому випадку, ключі), тоді як AES швидко і надійно шифрує великі обсяги інформації.

13

Вибір аудіоформату

- Основною причиною вибору не більш популярного MP3, а WAV є те, що другий є незгорнутим (uncompressed) аудіоформатом, який зберігає дані аудіо без втрат. Це означає, що вбудовування даних за допомогою методу LSB не призведе до втрати якості звуку, оскільки немає жодного стиснення чи втрати даних під час запису або читання файлу. Також до переваг формату WAV відносять відсутність стиснення та простоту структури даних, робота з форматом WAV є відносно простою та не потребує складних алгоритмів декодування чи стиснення.

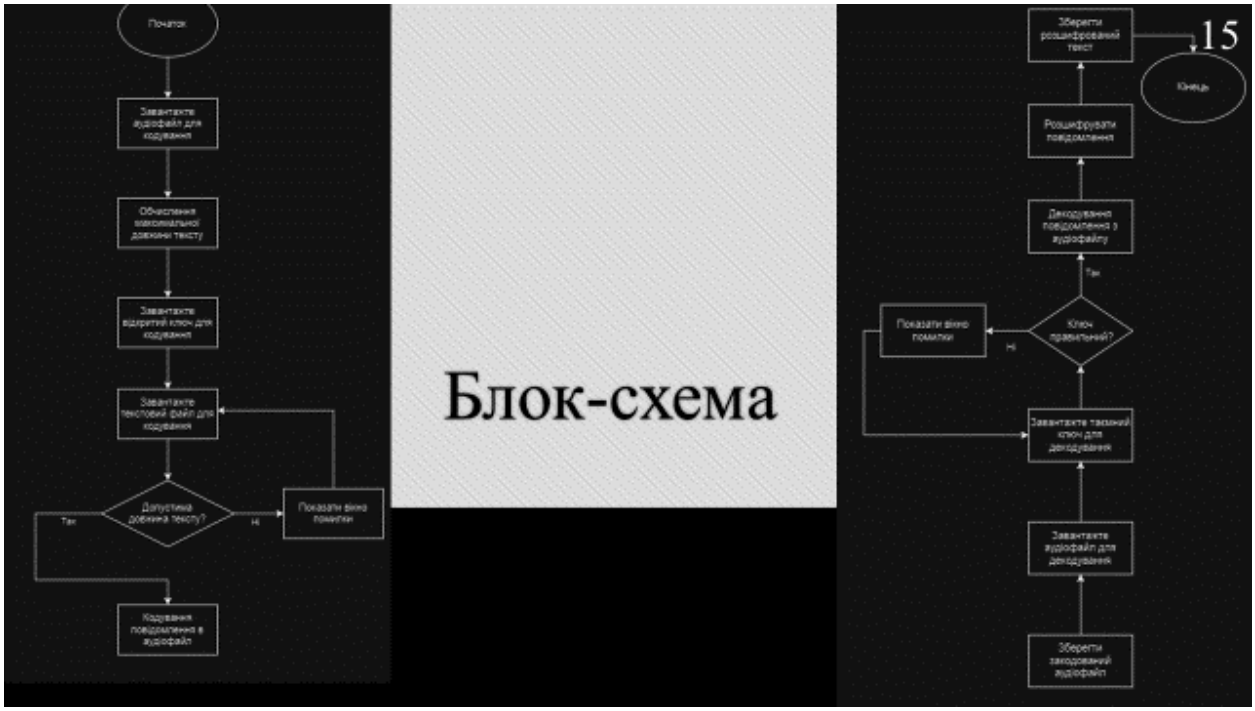
14

Логіка роботи програми

- Завантаження аудіофайлу для кодування;
- Обчислення максимальної довжини тексту;
- Завантаження публічного ключа для кодування;
- Завантаження текстового файлу для кодування;
- Перевірка довжини зашифрованого тексту;
- Кодування повідомлення в аудіофайл;
- Збереження закодованого аудіофайлу;
- Завантаження аудіофайлу для декодування;
- Завантаження приватного ключа для декодування;
- Декодування повідомлення з аудіофайлу;
- Розшифрування повідомлення;
- Збереження розшифрованого тексту.

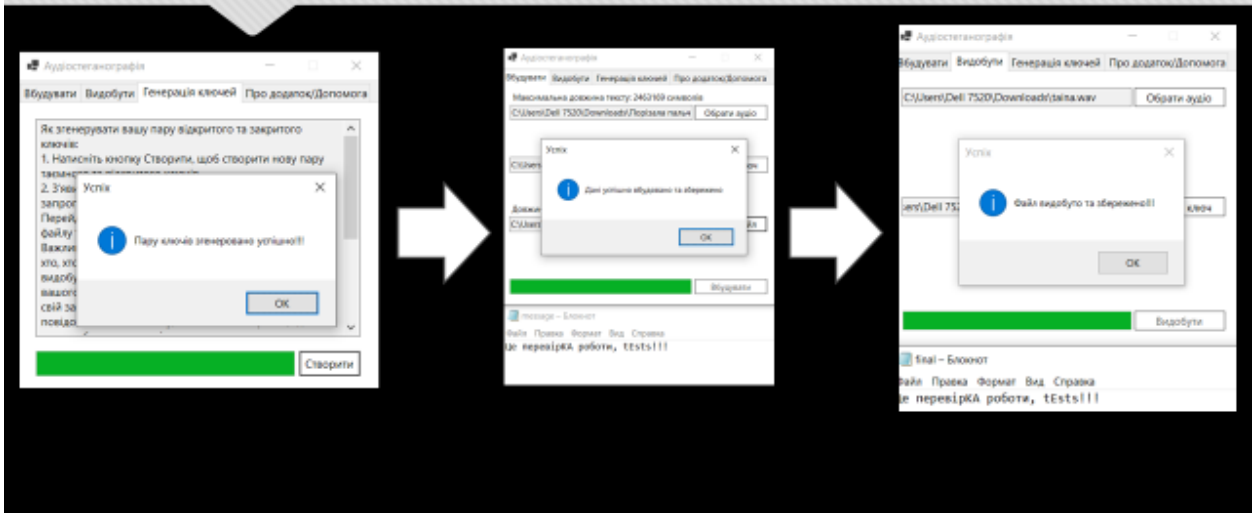
15

Блок-схема



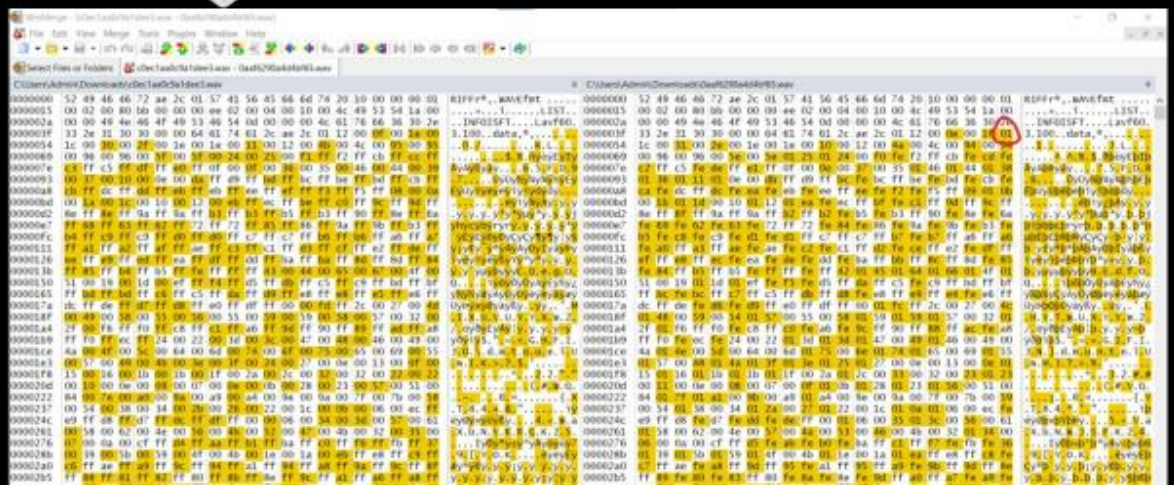
16

Тестування розробленого додатку



17

Аналіз перехопленого повідомлення з погляду криптоаналітика



18

ВИСНОВКИ

- В ході кваліфікаційної роботи було ретельно вивчено різноманітні методи стеганографії для приховування інформації у аудіофайлах.
- Метод LSB рекомендований як найбільш збалансований за параметрами ефективності та непомітності.
- Результатом роботи стало розроблення програмної реалізації методу приховування інформації у музичних файлах з використанням мови програмування C#.