

СТЕГАНОФОНІЧНА СИСТЕМА ДЛЯ ІР-ТЕЛЕФОНІЇ

Ралець Д.Р.

Західноукраїнський національний університет
магістрант

I. Вступ

У сучасному цифровому світі, де зв'язок та обмін інформацією відіграють ключову роль, виникає необхідність удосконалення методів та засобів забезпечення безпеки та конфіденційності обміну даними. Із зростанням популярності голосових комунікацій та тенденцією до збільшення кількості онлайн-спілкувань, науковці та фахівці з безпеки зосереджують увагу на розробці ефективних засобів стеганофонії для захисту конфіденційної інформації в реальному часі. Стеганофонічні системи дозволяють приховати факт передачі конфіденційного повідомлення, інкапсулюючи його у стек мережевих протоколів.

II. Мета роботи

Метою роботи є розробка стеганофонічної системи, адаптованої до протоколів ІР-телефонії.

III. Особливості розробки стеганофонічної системи

Аналіз TCP/IP-протоколів таких як IP, UDP, TCP показує, що існують поля в пакетах, які не використовуються в процесі їх передачі по мережі. Це дає багато можливостей для того щоб конфіденційні повідомлення можна було приховати у таких полях пакетів та передати без втрати розміру самого повідомлення.

Опис процесу інкапсуляції конфіденційних повідомлень в трафік ІР-телефонії можна отримати представивши стеганофонічну систему, як систему зв'язку з передачею додаткової інформації (рисунок 1). Для цього потрібно об'єднати дві фази VoIP викликів: комутацію (маршрутизацію) викликів і передачу даних (кодованого голосу). Комутація викликів здійснюється передачею сигнальних повідомлень, а даний процес називається сигналізацією. Цей процес включає одночасну перевірку автентичності та цілісності захисту передачі звукових сигналів та повідомлень.



Рисунок 1 – Схема стеганофонічної системи

Задачу вбудовування і виділення повідомлень з іншої інформації виконує стеганофонічна система, яка складається з наступних основних елементів:

- прекодер - пристрій, призначений для перетворення прихованого повідомлення до виду, зручного для вбудовування в сигнал-контейнер. (Контейнером називається інформаційна послідовність, в якій ховається повідомлення);

- стегакодер - пристрій, призначений для здійснення вкладення прихованого повідомлення в інші дані з урахуванням їх моделі;
- пристрій виділення вбудованого повідомлення;
- стегадетектор - пристрій, призначений для визначення наявності стегаповідомлення;
- декодер - пристрій, що відновлює приховане повідомлення.

У роботі було розроблено стегафонічну систему, адаптовану до протоколів IP-телефонії (див.рис.2).

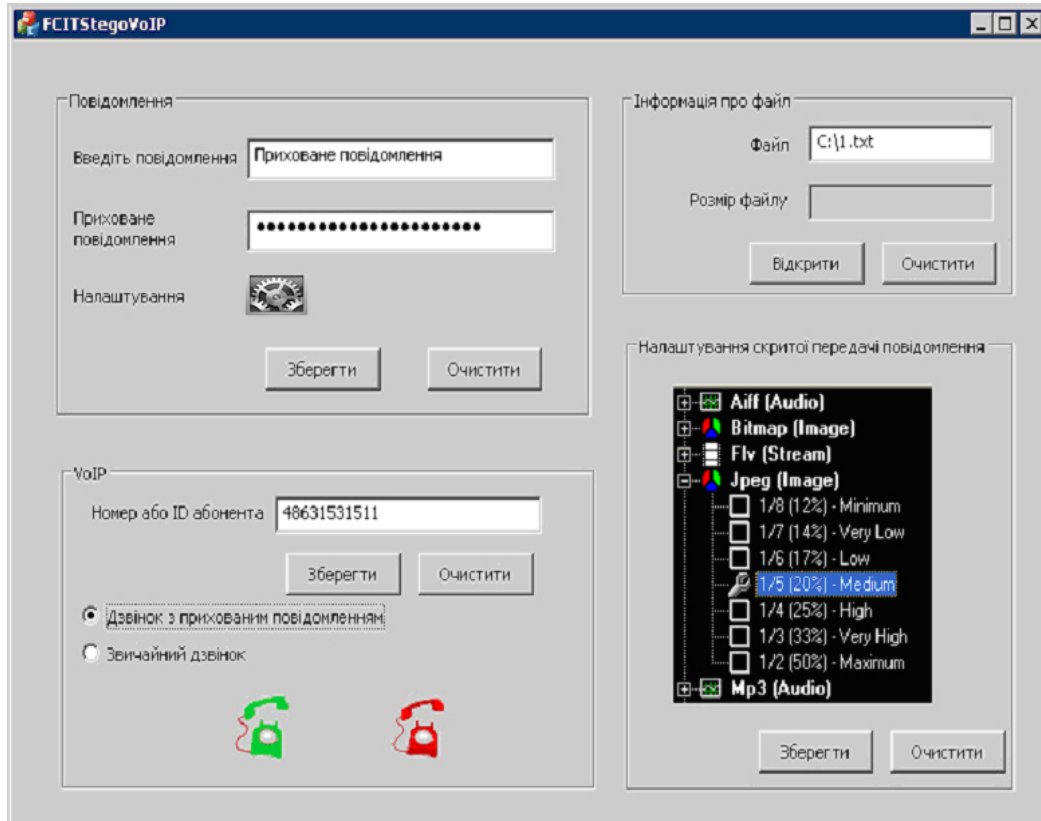


Рисунок 2 - Головне вікно стегафонічної системи FCITStegoVoIP

Для реалізації програмного забезпечення було використано VisualStudio 2022, мову програмування C++, з модуль OpenPuff v3.30 Steganography&Watermarking.

У головному вікні є можливість ввести текст прихованого повідомлення, або відкрити його з файлу, вибрати користувача для здійснення дзвінка, вибрати тип дзвінка – дзвінок з прихованим повідомленням, або реалізувати звичайний дзвінок, а також налаштувати основні характеристики передачі повідомлення – від вибору алгоритмів стиснення голосу, до вибору типових конфігурації для певних груп повідомлень.

Висновок

У даній роботі була запропонована стегафонічна система, адаптована до передачі конфіденційних повідомлень у трафіку IP-телефонії. Інкапсуляція повідомлень відбувається в мережеві протоколи, зберігаючи при цьому їхню цілісність та автентичність.

Результати дослідження підтверджують можливість використання запропонованої стегафонічної системи для забезпечення безпеки обміну голосовою інформацією в мережах IP-телефонії.

Список використаних джерел

1. Mazurczyk, W., Lubacz, J. and Szczypiorski, K. (2008) Hiding Data in VoIP. Proceedings of the 26th Army Science Conference (ASC 2008), Orlando, 1-4 December 2008.
2. Naidu, T.R.K.; Kumar, G.P.; Prasad, T.G. Overview of digital audiostream techniques. Int. J. Emerg. Technol. Eng. 2016, 3, 62–66.
3. Huang, Y.; Liu, C.; Tang, S.; Bai, S. Steganography integration into a low-bitrate speech codec. IEEE Trans. Inf. Forensics Secur. 2012, 7, 1865–1875.
4. Tian, H.; Wu, Y.; Chang, C.C.; Huang, Y.; Chen, Y.; Wang, T.; Cai, Y.; Liu, J. Steganalysis of adaptive multi-rate speech using statistical characteristics of pulse pairs. Signal Process. 2017, 134, 9–22.