

УДК 621.326

Макоїд О. – ст. гр. СП-42

Тернопільський національний технічний університет імені Івана Пулюя

ЗАСТОСУВАННЯ ПРИНЦИПІВ LSB ТА SPLIT SPECTER ДЛЯ ЗАХИСТУ АУДІО ТА ШИФРУВАННЯ ДАНИХ ВСЕРЕДИНИ НИХ

Науковий керівник: док.філософ. Мудрик І. Я.

Makoid O.

Ternopil Ivan Puluj National Technical University

APPLYING LSB AND SPLIT SPECTER PRINCIPLES FOR AUDIO PROTECTION AND DATA ENCRYPTION INSIDE AUDIO SIGNALS

Supervisor: Ph.D. Mudryk I.

Ключові слова: стеганографія, аудіозахист, спектральне кодування, приховування даних
Keywords: steganography, audio protection, spectral coding, data hiding

Аудіофайли є мало не найбільш вразливим видом цифрових даних, що часто піддається незаконному копіюванню, поширенню та дистрибуції. Одним з найбільш надійних варіантів захисту прав інтелектуальної власності для такого типу продуктів є застосування аудіостеганографії. Аудіостеганографія є процесом приховування інформації в аудіосигналі так, щоб її не можна було помітити неозброєним оком на спектрі чи почути, але можливо витягнути при наявності відповідного ключа або алгоритму [1].

Одним з таких методів є LSB (Least Significant Bit), що змінює найменш значущий біт у 16-бітному PCM-сигналі. Таке втручання настільки незначне, що не сприймається слухом. У стереотреці з частотою 44.1 кГц за секунду можна приховати кілька кілобайтів даних без втрати якості. Метод ефективний для вбудовування ID-треків, цифрових підписів та DRM-токенів. Щоправда, даний принцип має великий недолік — чутливість до обробки сигналу, наприклад, стиснення, фільтрації або перекодування (перетворення WAV аудіо в MP3 чи FLAC, наприклад), що може знищити приховану інформацію або сильно спотворити її [2].

З метою подолання таких обмежень застосовується принцип Split Specter (розщеплення спектра), що передбачає перехід аудіосигналу в частотну область через швидке перетворення Фур'є (FFT). На відміну від LSB тут дані вбудовуються у малочутливі діапазони спектра — зазвичай інфразвук (20–200 Гц) або ультразвук (понад 16 кГц) Це забезпечує вищу непомітність та стійкість до обробки — фільтрації, перекодування, нормалізації тощо.

Алгоритм охоплює: зчитування WAV-файлу, сегментацію на фрейми, застосування FFT, модифікацію амплітуд або фаз цільових частот згідно з бітами повідомлення (наприклад, з використанням псевдовипадкової послідовності), зворотне перетворення (IFFT) і збереження результату. Такий підхід дозволяє інтегрувати дані, що зберігаються навіть після агресивних перетворень сигналу [3].

Гібридний алгоритм застосування LSB та Split Spectrum може експотенційно збільшити захист, оскільки це не тільки збільшення можливого об'єму прихованої інформації, але й стійкості до спотворень. Принцип такого шифрування передбачає:

1. Попереднє шифрування повідомлення за допомогою алгоритму AES або

RC4;

2. Поділ за важливістю: службова інформація вбудовується в LSB, додаючи декілька біт між заголовком аудіо файлу та самим його наповненням;

3. Основне повідомлення (водяні знаки, ліцензії) у формі двійкового коду вставляється в спектр аудіо через спектральне кодування;

4. На завершення трек перевіряється на збереження прозорості звучання та стійкість до обробки.

Таке поєднання дозволяє ставити індивідуальні відбитки на кожен екземпляр файлу, легко ідентифіковувати та усунути джерело витоку, а також є надійним способом передавати конфіденційну інформацію, не привертаючи зайву увагу, тим самим гарантуючи ефективний первинний захист чутливим даним та інтелектуальній власності.

Однак варто врахувати, що накладання захисту на аудіо та його зчитування зазвичай займає деякий час для обробки, що, наприклад, для веб орієнтованих систем, є важливим фактором ефективності.

В такому разі варто розглянути варіанти його масштабування. Одним із таких є використання хмарних технологій для зберігання аудіо (Amazon S3) та розподіленої асинхронної обробки через Redis Queue. Дані інструменти ідеально підходять для масштабування задач такої складності, особливо, коли це стосується великої кількості відповідних даних для обробки.

Список використаних джерел:

1. Sumit Kumar A. Audio Steganography : The art of hiding secrets within earshot. *Medium*. 17.06.2018. URL: <https://sumit-arora.medium.com/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-2-of-2-c76b1be719b3> (дата звернення: 09.04.2025).
2. *International Journal of Computer Trends and Technology (IJCTT)*. 2014. Т. 13, вип. 2. С.
3. М. Petryk, М. Bachynskyi, V. Brevus, I. Mudryk, D. Mykhalyk. Analysis technology of neurological movements considering cognitive feedback influences of cerebral cortex signals. ITTAP CEUR Workshop Proceedings 3309 (2022): 45–54.
4. Nadiia, Y., Nadiia, M., Lesia, O., & Mudryk I., (2023). RADIAL-BASIS NEURAL NETWORKS FOR ENTERPRISES ACTIVITY PREDICTION. *European Science*, 3 (sge17-03), 42–48. <https://doi.org/10.30890/2709-2313.2023-17-03-012>