УДК 004.056.5

Ю. Є. Яремчук

Є. М. Олексюк

Підвищення стійкості методу приховування даних в аудіосигналах до стиснення MP3 на основі QIM-квантування у частотній області та шифрування ключ-блоку

Вінницький національний технічний університет

Анотація. *У даній роботі представлено розробку гібридного методу приховування даних в аудіосигналах, спрямованого на забезпечення стійкості до стиснення з втратами (формат MP3). Запропоновано підхід, що базується на використанні квантування з індексною модуляцією (QIM) у частотній області модифікованого дискретного косинусного перетворення (MDCT). Особливістю методу є інтеграція криптографічного захисту параметрів вбудовування (ключ-блоку) за допомогою алгоритму AES-256. Обґрунтовано вибір частотної області для вбудовування інформації з урахуванням психоакустичної моделі MP3. Описано архітектуру методу, яка включає попередню обробку сигналу, адаптивне квантування та шифрування координат вбудовування, що дозволяє підвищити як надійність зберігання даних, так і захищеність від атак стеганалізу.*

Ключові слова: аудіостеганографія, QIM-квантування, MP3-компресія, MDCT, шифрування ключ-блоку, AES-256, кібербезпека, приховування даних.

Abstract*. This paper presents the development of a hybrid data hiding method in audio signals aimed at ensuring robustness against lossy compression (MP3 format). An approach based on Quantization Index Modulation (QIM) in the frequency domain of the Modified Discrete Cosine Transform (MDCT) is proposed. A distinctive feature of the method is the integration of cryptographic protection for embedding parameters (key-block) using the AES-256 algorithm. The choice of the frequency domain for information embedding is justified, taking into account the MP3 psychoacoustic model. The architecture of the method is described, which includes signal pre-processing, adaptive quantization, and encryption of embedding coordinates, allowing to increase both data reliability and protection against steganalysis attacks.*

Keywords: audio steganography, QIM quantization, MP3 compression, MDCT, key-block encryption, AES-256, cybersecurity, data hiding.

Вступ

Стрімкий розвиток цифрових технологій та мультимедійних комунікацій актуалізує проблему захисту авторських прав та забезпечення конфіденційності передачі даних. Аудіостеганографія, як метод приховування інформації в звукових сигналах, стикається з серйозним викликом — стійкістю до стиснення з втратами. Формат MP3, який є стандартом де-факто для зберігання аудіо, використовує складні психоакустичні моделі для видалення інформації, яку людське вухо не сприймає. Це робить традиційні методи, такі як LSB (Least Significant Bit), неефективними, оскільки вони модифікують саме ті компоненти сигналу, які першими знищуються при компресії. Тому метою дослідження є розробка методу, який би забезпечував надійне вбудовування даних у частотній області, сумісній з алгоритмами компресії, та гарантував криптографічну стійкість прихованого каналу.

Результати дослідження

У ході дослідження було проаналізовано вплив алгоритмів перцептивного кодування на цілісність стеганографічних даних. Встановлено, що основою формату MP3 є модифіковане дискретне косинусне перетворення (MDCT), яке переводить сигнал з часової області у частотну для подальшого квантування згідно з психоакустичною моделлю [1]. Ця модель визначає пороги маскування — рівні енергії, нижче яких звуки стають нечутними для людини в присутності гучніших сигналів. Класичні методи стеганографії, що працюють у часовій області, не враховують цих особливостей, що призводить до руйнування вбудованих бітів під час квантування коефіцієнтів у процесі стиснення [2].

Для вирішення цієї проблеми розроблено метод, що здійснює вбудовування безпосередньо у коефіцієнти MDCT. Це дозволяє синхронізувати процес приховування з внутрішньою структурою кодека MP3, мінімізуючи втрати при подальшому перекодуванні. В якості механізму модуляції обрано метод квантування з індексною модуляцією (QIM — Quantization Index Modulation), який, згідно з теорією інформації, забезпечує вищу ємність та стійкість порівняно з методами розширеного спектру [3].

Математична модель вбудовування описується наступним чином: для кожного біта повідомлення $m \in \{0, 1\}$ обирається відповідна решітка квантування. Модифікований коефіцієнт y обчислюється за формулою:

$$y = Q(x, \Delta, m) = \Delta \times round\left(\frac{x - d_m}{\Delta}\right) + d_m \quad (1)$$

де x — вихідний коефіцієнт MDCT, Δ — крок квантування, d_m — зміщення, що залежить від біта повідомлення.

Адаптивність методу досягається шляхом динамічного розрахунку кроку квантування Δ для кожного фрейму на основі локальної енергії сигналу. Це дозволяє збільшувати силу вбудовування в енергетично насичених ділянках спектру, де зміни менш помітні, та зменшувати її в "тихих" зонах, забезпечуючи виконання вимог щодо непомітності (Transparency).

Важливою складовою розробленої системи є забезпечення криптографічної безпеки. Більшість існуючих стеганографічних систем вразливі до атак, якщо зловмисник знає алгоритм вбудовування (принцип Керкгоффса). Для усунення цієї вразливості впроваджено концепцію «шифрованого ключ-блоку». Ключ-блок — це структура даних, що містить метаінформацію про процес вбудовування: індекси модифікованих коефіцієнтів MDCT, використані кроки квантування та параметри синхронізації.

Перед передачею або збереженням цей блок шифрується з використанням симетричного алгоритму блокового шифрування AES (Advanced Encryption Standard) з довжиною ключа 256 біт у режимі CBC (Cipher Block Chaining) [4].

Процес захисту описується виразом:

$$C_{KB} = AES - 256_{Key}(KB, IV) \quad (2)$$

де KB — відкритий ключ-блок, IV — вектор ініціалізації, Key — секретний ключ користувача. Такий підхід гарантує, що навіть за умови виявлення факту наявності прихованих даних (стеганаліз), зловмисник не зможе коректно вилучити інформацію без знання ключа розшифрування координат вбудовування.

Експериментальне дослідження проводилося на вибірці з 10 аудіофайлів різних жанрів (класика, рок, джаз, мовлення) загальною тривалістю понад 20 хвилин. Оцінювалися такі показники:

1. Стійкість до MP3-стиснення (Robustness). Вимірювався коефіцієнт бітових помилок (BER — Bit Error Rate) після стиснення стего-файлу з різними бітрейтами.

– При бітрейті 320 кбіт/с та 192 кбіт/с: BER ≈ 0.00. Дані відновлюються без помилок.

– При бітрейті 128 кбіт/с (стандартна якість): середній BER склав 0.022 (2.2%). Це критично важливий результат, оскільки традиційні методи (LSB) за таких умов демонструють BER на рівні 0.40–0.50 (втрата 40-50% даних). Використання кодів корекції помилок (наприклад, кодування Ріда-Соломона або мажоритарне дублювання) дозволяє повністю відновити повідомлення при BER < 0.05.

– При бітрейті 64 кбіт/с: BER зростає до 0.15, що свідчить про межу застосовності методу через значні спотворення сигналу кодеком.

2. Непомітність (Imperceptibility). Якість стего-сигналу оцінювалася за допомогою об'єктивної метрики SNR (Signal-to-Noise Ratio). Середнє значення SNR для тестової вибірки склало 30.56 дБ. Це значення перевищує поріг у 25 дБ, який вважається мінімально прийнятним для непомітності змін у аудіо. Суб'єктивний аналіз та візуальне порівняння спектрограм підтвердили відсутність чутних артефактів.

3. Пропускна здатність (Payload). Метод забезпечує швидкість передачі даних у межах 80–250 біт/с (залежно від спектральної насиченості файлу), що є достатнім для передачі текстових повідомлень, ключів шифрування або цифрових підписів.

Порівняльний аналіз показав переваги запропонованого методу над аналогами. Зокрема, методи часової області (LSB, Phase Coding) повністю втрачають працездатність після MP3-стиснення. Методи розширеного спектру (Spread Spectrum) є стійкими, але мають значно нижчу пропускну здатність. Гібридний метод демонструє найкращий баланс між стійкістю, ємністю та безпекою. Використання криптографічного захисту ключ-блоку додатково підвищує стійкість системи до статистичних атак, оскільки розподіл модифікованих коефіцієнтів стає псевдовипадковим і залежить від ключа шифрування, а не від структури самого повідомлення.

Висновки

Запропонований гібридний метод підвищення стійкості приховування даних в аудіосигналах поєднує переваги QIM-квантування у частотній області MDCT та сучасних криптографічних стандартів. Реалізація методу дозволяє нівелювати вплив MP3-компресії на цілісність прихованого повідомлення, забезпечуючи при цьому високу якість стего-сигналу. Шифрування ключ-блоку алгоритмом AES-256 унеможливлює відновлення даних без відповідного ключа доступу, що робить метод придатним для використання в захищених системах обміну інформацією.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Painter T., Spanias A. Perceptual coding of digital audio. *Proceedings of the IEEE*. 2000. Т. 88, № 4. P. 451–515.
2. Petitcolas F. A. P., Anderson R. J., Kuhn M. G. Information hiding-a survey. *Proceedings of the IEEE*. 1999. Т. 87, № 7. P. 1062–1078.
3. Chen B., Wornell G. W. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*. 2001. Т. 47, № 4. P. 1423–1443.
4. Daemen J., Rijmen V. *Design of Rijndael: AES - the Advanced Encryption Standard*. Springer London, Limited, 2013. 238 p.

Олексюк Євгеній Михайлович – студент групи 2КІТС-24м, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: zenaoleksuk@gmail.com

Науковий керівник: Яремчук Юрій Євгенович – д.т.н., професор каф. Менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: yurevyar@vntu.net

Oleksiuk Yevhenii M. – student of the 2KITS-24m group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: zenaoleksuk@gmail.com

Supervisor: Yaremchuk Yurii Yevhenovych – Doctor of Technical Sciences, Professor of the Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: yurevyar@vntu.net