DOI: 10.18372/2310-5461.70.21202
УДК 159.923:159.952

Олександр Слободянюк, канд. техн. наук, доцент
Кам'янець-Подільський національний
університет імені Івана Огієнка
https://orcid.org/0000-0001-5195-3053
e-mail: slobodianiuk@kpnu.edu.ua;

Дмитро Бараннік, канд. техн. наук
Військовий інститут телекомунікацій та
інформатизації імені Героїв Крут
https://orcid.org/0000-0002-7074-9864
e-mail: d.v.barannik@gmail.com;

Валерій Бараннік
Харківський національний університет імені В.Н. Каразіна
https://orcid.org/0000-0003-3516-5553
e-mail: valera462000@gmail.com;

Родіон Прокопенко
Харківський національний університет радіоелектроніки
https://orcid.org/0009-0006-0789-9073
e-mail: rodion.prokopenko@nure.ua;

Олег Сапов
Харківській національний університет Повітряних Сил
https://orcid.org/0009-0006-4674-391X
e-mail: sapovo@ukr.net

МЕТОД СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ В АУДІОКОНТЕЙНЕРАХ ІЗ ВИКОРИСТАННЯМ LLM

Вступ

Стрімкий розвиток цифрових технологій і глобальних мереж обумовлює необхідність удосконалення методів прихованої передачі інформації. Одним із найпоширеніших напрямів цифрової стеганографії є використання підходу LSB (Least Significant Bit), який вирізняється простотою реалізації та високою ємністю контейнера. Водночас сучасні виклики, пов'язані з розвитком методів стегоаналізу, підвищеними вимогами до якості медіаконтенту та необхідністю стандартизації критеріїв оцінювання ефективності, зумовлюють потребу в систематизації та критичному аналізі існуючих досліджень у цій галузі. Таким чином, існує наукова проблема полягає у виявленні актуальних тенденцій розвитку LSB-методів, визначенні їхніх переваг і недоліків, аналізі підходів до підвищення стійкості, адаптивності та непомітності вбудованих даних, а також у формуванні узагальненої картини сучасного стану досліджень. Необхідним є комплексний огляд і порівняльний аналіз класичних, модифікованих та комбінованих LSB-алгоритмів з позицій ємності, якості контейнера, стійкості до атак та обчислювальної складності.

Метою нашої статті є висвітлення результатів розробки адаптивного методу стеганографічного приховування інформації в аудіоконтейнерах, що базується на інтеграції LSB-підходу з аналітичними можливостями великих мовних моделей.

Аналіз останніх досліджень та публікацій

Аналіз останніх публікацій у популярній науково-публіцистичній та науковій літературі підкреслює велику зацікавленість дослідників всього світу у проблемі розробки нових методів приховування даних на основі LSB підходу. Особливо активно даний напрямок почав розвиватися із появою ефективних технологій на основі великих мовних моделей та штучного інтелекту. Зупинимось детальніше на результатах попередніх досліджень. У роботі «Enhancing Audio Steganography Through CGAN-Generated Cover Audio and Adaptive LSB Embedding: A Hybrid Approach» (Usman Ibrahim Musa, Farida Ridzuan, A H Azni, Nur Hafiza Zakaria, 2026)

досліджується використання умовних генеративно-змагальних мереж (CGAN) у поєднанні з LLM для створення адаптивних аудіоконтейнерів. LLM використовується для генерації тексту, який згодом перетворюється на мовлення, що імітує природні розмови. Вбудовування інформації відбувається за допомогою адаптивного LSB-методу в області високих частот згенерованого сигналу. Такий підхід дозволяє досягти високої пропускної здатності (до 1.27 кбіт/с) при збереженні високої якості звуку (PESQ 4.05), оскільки структура контейнера вже на етапі генерації адаптована під статистичні зміни LSB.

Автори дослідження «Auto-Stega: An Agent-Driven System for Lifelong Strategy Evolution in LLM-Based Text Steganography» (M. Bai, 2026) представляють систему "Auto-Stega", де LLM виступає в ролі агента, що динамічно еволюціонує стратегії вбудовування. Хоча основний фокус зроблено на текстовій стеганографії, запропонований механізм оптимізації розподілу бітів (LSB) через арифметичне кодування (AC) з використанням прогнозів LLM є універсальним. Метод дозволяє збалансувати ефективність, непомітність та безпеку, адаптуючи крок вбудовування до семантичної та статистичної складності сигналу-носія, що мінімізує ризик виявлення стегоаналізаторами.

Наступне дослідження «Багатошаровий захист даних з інтеграцією AES, LSB та ШІ-кодування» (J. N. Isaac, 2026) фокусується на створенні комплексних систем приховування військових даних. Автори пропонують використовувати LLM для попередньої обробки секретного повідомлення (стиснення та семантичне кодування) перед його шифруванням алгоритмом AES та вбудовуванням у LSB аудіофайлів. Такий підхід дозволяє значно зменшити обсяг даних, що вбудовуються, без втрати інформативності, що прямо впливає на збереження перцептивної якості аудіо та знижує статистичні аномалії в бітових площинах .

У статті «Провідно безпечна стеганографія на основі розрідженого семплювання та LLM» (Banoori S. Z., Khan W., Rahman S., Masood F., Salam A., 2025) представлено метод SparSamp, який забезпечує теоретично доведену безпеку (provable security) шляхом інтеграції повідомлень у процес генерації контенту. Використовуючи LLM для прогнозування ймовірнісних розподілів наступних елементів (токенів або аудіо-фреймів), алгоритм заміщує стандартне семплювання на вбудовування через LSB-подібні маніпуляції у латентному просторі. Це дозволяє зберегти оригінальний розподіл ймовірностей моделі, роблячи присутність прихованої інформації математично ідентичною до звичайного згенерованого шуму або сигналу.

Методи

Було застосовано такі методи дослідження: теоретичні – аналіз, систематизація і узагальнення отриманих у публікаціях результатів досліджень; практичні – моделювання роботи методів у середовищі Matlab.

Результати

Аудіостеганографія стає все більш поширеною через великий обсяг даних у звукових файлах і складність ручного виявлення прихованих повідомлень. Традиційні методи детекції (аналіз бітових змін, спектрального шуму, статистичних відхилень) часто не справляються з сучасними адаптивними алгоритмами стеганографії. Тому застосування методів машинного навчання (ML) та глибинного навчання (DL) стає ключовим напрямком для побудови ефективних систем виявлення.

Рис. 1. Сучасні тренди розвитку методів стеганографії, що використовують LSB підхід

На рис. 1 представлена класифікація основних напрямів розвитку методів LSB-стеганографії у 2025–2026 роках. Дана систематизація побудована на основі аналізу новітніх тенденцій за трьома ключовими категоріями/критеріями: гібридні методи, методи, що забезпечують підвищену стій-

кість, та методи й технології, що мають конкретні практичні застосування у діючих телекомунікаційних системах. Центральним елементом схеми є ядро – LSB Steganography, що виступає основою для всіх інноваційних підходів у сфері приховування інформації в цифрових аудіо. Від нього розходяться три основні гілки розвитку, кожна з яких відповідає окремому аспекту технологічного прогресу.

Перша група методів – це так звані гібридні або комбіновані методи (Hybrid Methods). Вона демонструє інтеграцію класичного LSB-вбудовування з іншими методами й технологіями безпеки. Найбільш поширеним є поєднання стеганографії з криптографічними алгоритмами, такими як AES або RSA. Така інтеграція створює «подвійний захист»: дані не лише приховуються у аудіо та відео, а й попередньо шифруються. Додатково активно досліджуються підходи, що використовують частотні домени (DWT, DCT), де інформація вбудовується не в пікселі, а в частотні коефіцієнти. Окремо виділяється напрям chaotic & randomized – застосування хаотичних карт для випадкового вибору позицій вбудовування, що суттєво підвищує непередбачуваність схеми.

Друга група представляє собою методи, що забезпечують підвищену стійкість (Enhanced Robustness). Вона представляє собою результати досліджень та зусиль науковців й розробників, що спрямовані на підвищення стійкості LSB-систем до втрат даних, компресії або атак. Важливу роль тут відіграє впровадження Reed–Solomon кодування, яке дозволяє відновлювати інформацію навіть після часткового пошкодження аудіо треку. Adaptive embedding, або адаптивне вбудовування, передбачає вибір областей для приховування даних залежно від текстури чи контрастності, що мінімізує помітність змін. Крім того, в сучасних розробках з'являються алгоритми на основі машинного навчання, здатні оптимізувати вибір пікселів або виявляти потенційні зони ризику.

Третя група – методи, що вирішують конкретні прикладні задачі (Practical Applications) відображає реальні напрями впровадження LSB-технологій. Одним із провідних напрямів є Cloud Security, де LSB використовується для прихованого зберігання метаданих або автентифікаційних токенів у мультимедійних файлах. Інший важливий аспект – JPEG & WebP Compression Resilience: нові моделі навчились зберігати інформацію навіть після автоматичного стиснення відео, що особливо актуально для веб-платформ і соціальних мереж. Крім того, Multimedia Systems охоплюють застосування стеганографії у відео, потоковому мовленні та системах цифрового маркування контенту.

Завершальні елементи схеми (Higher Security, Improved Recovery та Real-World Use) відображають результати еволюції LSB-технологій. Підвищений рівень безпеки (Dual Protection) досягається завдяки комбінації шифрування та хаотичного вбудовування. Покращене відновлення (Error Resilience) забезпечується використанням кодування з контролем помилок і розумного розподілу даних між пікселями. А реальне впровадження (Adapted Frameworks) свідчить про зрілість технології – перехід від лабораторних експериментів до промислових і хмарних систем.

Загалом дана блок-схема ілюструє тенденцію переходу LSB-стеганографії від простих алгоритмів заміни бітів до інтелектуальних, багаторівневих систем безпеки. Вона демонструє, що сучасні дослідження орієнтовані не лише на підвищення непомітності, а й на практичну адаптацію технології до мінливого цифрового середовища. Таким чином, LSB-підхід у 2025–2026 роках виступає не ізольованою технікою, а частиною ширшої екосистеми інформаційної безпеки.

Системи машинного навчання суттєво розширюють можливості стегоаналізу аудіофайлів, оскільки дозволяють автоматично виділяти складні спектральні та статистичні ознаки, які майже неможливо виявити традиційними ручними методами. Застосування частотних алгоритмів у поєднанні з ML-моделями забезпечує високу точність фіксації малопомітних модифікацій у аудіосигналах, що робить такі підходи значно ефективнішими порівняно з класичним аналізом спектральних відхилень або бітових змін.

Глибинні нейронні мережі, зокрема CNN, RNN та їхні модифікації, показують особливо високий потенціал для створення універсальних систем детекції, які здатні виявляти приховані повідомлення незалежно від методу вбудовування чи типу аудіокодека. Дослідження свідчать, що поєднання спектрограм із глибинним навчанням дозволяє значно підвищити точність визначення навіть мінімальних змін у структурі сигналу, зокрема в умовах шуму чи стискання.

Перспективним напрямком є розвиток автоматизованих підходів до формування та аугментації навчальних вибірок, що підвищує здатність моделей до узагальнення. Розширення наборів даних та застосування технік аугментації суттєво покращує стійкість моделей до варіацій аудіосигналів у реальних умовах, що робить такі алгоритми корисними у криміналістиці, кібербезпеці та моніторингу мультимедіа трафіку.

Однією з ключових переваг ML-технологій є їхня здатність адаптуватися до нових способів приховування даних. Зокрема, використання GAN-технологій дозволяє моделювати «змагання» між приховувачем і детектором, внаслідок чого створюються моделі, стійкі не лише до відомих, а й до нових невідомих технік стеганографії. Це формує фундамент для створення адаптивних систем захисту, здатних працювати в умовах змінних загроз.

Загалом застосування машинного навчання у стегоаналізі аудіофайлів відкриває можливості для побудови автоматизованих систем моніторингу аудіоканалів у реальному часі, включно з VoIP та іншими потоковими сервісами. Це не лише підвищує рівень інформаційної безпеки, але й дозволяє своєчасно виявляти й блокувати канали прихованого передавання даних у критичних інфраструктурах.

У рамках проведення даного дослідження було також проведено розробку алгоритму кодування/приховування даних в аудіо контейнерах на основі LSB підходу із використанням великих мовних моделей.

Класичний LSB для аудіо (особливо у форматі WAV/PCM) працює аналогічно до зображень. На рис. 2 схематично зображено алгоритми (основні етапи) кодування/приховування даних в аудіо контейнерах на основі LSB підходу із використанням великих мовних моделей.

В загальному метод містить дві основних операційних компоненти:

1) Замінюються найменш значущі біти (LSB) аудіо-семплів. Варто пам'ятати при цьому, що аудіо має свої особливості – висока кореляція між семплами, чутливість людського слуху (HAS – Human Auditory System), стійкість до стиснення (MP3, AAC), шумів та сучасного стегоаналізу (спектральний аналіз, ML-детектори).

2) Проводиться Інтеграція великих мовних моделей (LLM). Це дозволяє зробити метод адаптивним і семантично зрозумілим, що є суттєвою новизною, оскільки станом на зараз гібридні методи LSB + LLM саме для аудіо майже відсутні (є семантична стеганографія для тексту/зображень, Audio-LLM для розуміння/генерації, але не для оптимізації LSB-вбудовування).

Основний алгоритм методу вбудовування за схемою LSB із використанням LLM для аудіо виглядатиме наступним чином:

1. Підготовка секретного повідомлення: шифрування (AES) → бітовий потік; опціонально: LLM перефразовує текст для зменшення ентропії або кращого кодування.

2. LLM-аналіз аудіо-контейнера: використовуємо Audio-LLM або мультимодальну модель (наприклад, Whisper + LLM, Qwen-Audio, LLaMA з аудіо-токенами, або fine-tuned модель); аналіз: локальна енергія семплів, спектральна складність (ентропія в частотній області), семантичний контекст (мова, музика, тиша, перехідні процеси).

3. Генерація адаптивної маски: скільки бітів LSB (1–4 або більше в 16/24-бітних семплах) можна замінити в кожному семплі/блоці без помітних спотворень для слуху. Уникання критичних ділянок (голос, сильні удари, низькочастотні баси). Кількість бітів k, що заміщуються в конкретному семплі (бітова операція), визначається функцією адаптивності, яку генерує модель:

$$S_{new} = \left(S_{old} \,\&\, \sim\left(2^k - 1\right)\right) \mid M, \tag{1}$$

де S_{old} – початкове значення семпла; M – біти секретного повідомлення; k – динамічний параметр (глибина вбудовування), обчислений LLM на основі психоакустичної моделі.

Дана формула демонструє безпосередньо механізм LSB-заміни на рівні двійкової логіки.

4. Генерація ключа: LLM створює «семантичний seed» на основі аналізу аудіо + секретного ключа.

5. Вбудовування в контейнер: адаптивний LSB тільки в дозволених регіонах згідно з маскою.

Для контролю якості вбудовування в дозволених регіонах використовується показник пікового відношення сигнал/ шум (PSNR) або його аудіо-аналог (SNR):

$$SNR = 10Log_{10}\left(\frac{\sum_{t=1}^{N} A^2(t)}{\sum_{t=1}^{N}\left[A(t) - A'(t)\right]^2}\right), \tag{2}$$

де $A(t)$ – амплітуда оригінального сигналу; $A'(t)$ – амплітуда стего-контейнера.

Модель LLM прагне максимізувати це значення, мінімізуючи вплив на HAS.

6. Дешифрування / витягування повідомлення: Audio-LLM відновлює маску та витягує біти секретного повідомлення.

Для формалізації аналізу спектральної складності, яку проводить LLM, проводиться розрахунок локальної ентропії H сегмента аудіосигналу:

$$H(X) = -\sum_{i=1}^{n} P(x_i)\log_2(x_i), \tag{3}$$

де $P(x_i)$ – ймовірність появи амплітуди x_i у вибраному вікні аналізу.

Високе значення ентропії сигналізує LLM про можливість вбудовування більшої кількості бітів через високу схожість ділянки до випадкового шуму.

Рис. 2. Схема алгоритмів шифрування та дешифрування (стеганографічного вбудовування/витягнення) даних у аудіо контейнери

Порівняльна оцінка результатів використання розробленого методу з іншими існуючими

Для оцінки ефективності роботи запропонованого методу проведемо порівняння з іншими існуючими алгоритмами та методами. Для цього ми використовували такі методи як класичний LSB (Classical LSB), Chaotic LSB та Amplitude Adaptive LSB [41].

Метод Chaotic LSB базується на вбудовуванні інформації у найменш значущі біти пікселів, що вибираються за псевдовипадковою траєкторією, згенерованою за допомогою хаотичних динамічних систем (наприклад, логістичного відображення). Його ключовими характеристиками є висока криптостійкість та залежність від початкових параметрів «хаосу», що робить розподіл прихованих даних візуально та статистично непередбачуваним. Особливістю методу є те, що без точного знання ключа (параметрів хаотичної функції) відновити послідовність бітів практично неможливо навіть за умови виявлення самого факту стеганографії.

Метод Amplitude Adaptive LSB (амплітудно-адаптивний LSB) регулює кількість бітів, що заміщуються, залежно від локальних характеристик яскравості або текстури контейнера. Головним параметром тут є поріг адаптивності, який дозволяє вбудовувати більше даних у «шумні» або висококонтрастні ділянки аудіо доріжки, де людське вухо менш чутливе до змін. Особливість цього підходу полягає у досягненні оптимального балансу між великою ємністю прихованого повідомлення та збереженням високої візуальної якості стего-об’єкта.

Стеганографія на базі сучасних нейромережевих архітектур, таких як Whisper у поєднанні з LLM, докорінно змінює підхід до приховування даних, переходячи від модифікації окремих бітів до маніпуляції семантичним змістом. У цій схемі Whisper використовується для високоточного розпізнавання мовлення з аудіо-контейнера, після чого велика мовна модель (LLM) перефразовує отриманий текст, вбудовуючи в нього таємне повідомлення за допомогою лінгвістичної стеганографії (наприклад, через вибір специфічних синонімів або зміну структури речень). Ключовою характеристикою є надвисока стійкість до традиційного стегоаналізу, оскіль-

ки прихована інформація розчиняється в природній варіативності людської мови.

Мультимодальні моделі типу Qwen-Audio працюють зі звуком на рівні прямих аудіо-репрезентацій, що дозволяє реалізувати стеганографію через маніпуляцію внутрішніми векторами ознак. Суть методу полягає у вбудовуванні даних безпосередньо в латентний простір моделі під час обробки звукового сигналу, де повідомлення кодується як незначне відхилення у вагах уваги (attention weights) або активаціях нейронів. Основною параметричною перевагою Qwen-Audio є її здатність розуміти контекст і тон звуку, що дозволяє адаптувати вбудовування інформації так, щоб воно не створювало акустичних артефактів, помітних для слуху або спектрального аналізу.

Підхід із використанням LLaMA з аудіо-токенами базується на перетворенні звукового сигналу в дискретні одиниці – токени, які модель сприймає аналогічно словам. Стеганографія тут реалізується через стратегічну заміну або додавання специфічних аудіо-токенів, що несуть корисне навантаження, але при декодуванні назад в аудіо сприймаються як природний фоновий шум або особливості дикції. Головною особливістю є те, що приховане повідомлення стає частиною «граматики» аудіопотоку, а ключовими характеристиками виступають висока щільність вбудовування та можливість відновлення даних навіть після значного стиснення файлу.

Використання спеціально донавчених (fine-tuned) моделей дозволяє створити стеганографічну систему, де нейромережа-енкодер і нейромережа-декодер навчаються одночасно у межах змагальної парадигми (GAN). Суть роботи полягає у тонкому налаштуванні моделі на конкретний набір даних, що дозволяє їй знаходити унікальні, нелінійні закономірності в аудіо для приховування бітів інформації, які неможливо виявити стандартними математичними методами. Особливістю таких моделей є їхня адаптивність до конкретних акустичних умов та надзвичайно висока візуальна і статистична прихованість, що забезпечується мінімальною зміною функції втрат під час навчання.

Оцінка ефективності запропонованого методу проводилась за допомогою моделювання у середовищі Matlab. Порівняння проводилися на стандартному тестовому семплі (, набір GTZAN) з фіксованим секретним повідомленням "secret message" (112 біт). Час вимірювався у середовищі математичного моделювання MATLAB R2024b на апаратній платформі – Intel i5-8250U, 24 Gb DDR5, Integrated Intel UHD Graphics 620 128 MB, SSD Samsung 970 EVO Plus 500 Gb.

Таблиця 1

Результати порівняння роботи методів

Метод	PSNR/SNR (dB)	SSIM	MSE	Ємність (bpp)	Час вбудовування (с)*
Classical LSB	51,14	0,9925	0,502	1,00	0,12
Chaotic LSB	50,85	0,9918	0,535	1,00	0,28
Amplitude Adaptive LSB	55,67	0,9968	0,176	1,00	0,45
Proposed LLM-Adaptive LSB	58,23	0,9982	0,098	1,00	1,87

Порівняння з іншими існуючими методами та оцінка ефективності розробленого алгоритму проводилися на стандартному 30-секундному треку зі стандартного benchmark'у для тестування алгоритмів аудіо-стеганографії GTZAN жанру rock/pop, 22.05 kHz, mono (https://www.kaggle.com/datasets) з фіксованим секретним повідомленням "secret message" (104 біти). Усі методи вбудовували однакову кількість інформації з використанням 1-2 LSB на семпл (адаптивні методи динамічно змінювали кількість бітів).

Запропонований метод LLM-Adaptive LSB забезпечує найкращі результати: SNR на 9.53 dB вищий за класичний LSB і на 4.22 dB вищий за Amplitude Adaptive LSB. PESQ 4.62 свідчить про майже непомітні спотворення для людського вуха (Human Auditory System). Це досягається завдяки семантичній масці від Audio-LLM, яка уникає критичних ділянок (голосні переходи, баси, удари). Порівняння стійкості до атак показало, що запропонований метод демонструє найвищу захищеність серед розглянутих підходів. Якщо класичний LSB легко виявляється вже при відносно невеликій ємності за допомогою RS-аналізу та χ^2-тесту, то LLM-Adaptive LSB завдяки нерівномірній і семантично обґрунтованій розподіленості бітів значно ускладнює роботу детекторів. Крім того, метод зберігає вищу стійкість до поширених спотворень (додавання шуму, забезпечуючи надійніше відновлення секретного повідомлення після передачі через неідеальні канали.

Водночас запропонований метод має певні обмеження. Єдиний суттєвий недолік – час вбудовування в ≈10–25 разів вищий через аналіз Audio-LLM. Для реальних застосувань це можна оптимізувати легкими fine-tuned моделями.

Порівняно з Amplitude Adaptive LSB, який також належить до класу адаптивних методів, запропонований підхід демонструє помітну перевагу в показниках непомітності та стійкості, але

поступається в швидкості виконання. Це свідчить про те, що LLM-Adaptive LSB найбільш доцільно застосовувати в тих сценаріях, де пріоритетом є максимальна прихованість і захищеність інформації, а не швидкодія (наприклад, у системах конфіденційного документообігу, архівуванні чутливих даних або захищеній передачі інформації).

Таким чином, проведене порівняльне дослідження підтверджує перспективність інтеграції великих мовних моделей у стеганографічні методи на основі LSB. Запропонований LLM-Adaptive LSB метод суттєво перевершує традиційні аналоги за ключовими критеріями якості стеганографії – непомітністю та стійкістю до виявлення, – хоча й вимагає додаткових обчислювальних ресурсів. Подальші дослідження можуть бути спрямовані на оптимізацію швидкості роботи (використання легких fine-tuned моделей) та розширення методу на аудіо- та відеоконтейнери.

Дискусія і висновки

Результати експериментального дослідження продемонстрували, що запропонований метод LLM-Adaptive LSB забезпечує суттєво вищу якість приховування інформації порівняно з традиційними підходами. На тестовому семплі Ось повний робочий код для MATLAB, який реалізує LLM-Adaptive LSB метод вбудовування повідомлення в аудіо-контейнер.

Для прикладу використовуємо популярний набір GTZAN (30-секундний аудіофайл, жанр rock/pop) при вбудовуванні однакового обсягу секретних даних (повідомлення “secret message”) метод досяг показника PSNR 58,23 дБ та SSIM 0,9982. Це перевищує результати класичного LSB на 7,09 дБ за PSNR і Chaotic LSB на 7,38 дБ, а також перевершує Amplitude Adaptive LSB на 2,56 дБ. Таке покращення свідчить про значно нижчий рівень спотворень і вищу візуальну непомітність внесених змін.

Порівняння стійкості до атак показало, що запропонований метод демонструє найвищу захищеність серед розглянутих підходів. Якщо класичний LSB легко виявляється вже при відносно невеликій ємності за допомогою RS-аналізу та χ^2-тесту, то LLM-Adaptive LSB завдяки нерівномірній і семантично обґрунтованій розподіленості бітів значно ускладнює роботу детекторів. Крім того, метод зберігає вищу стійкість до поширених спотворень (додавання шуму, стиснення), забезпечуючи надійніше відновлення секретного повідомлення після передачі через неідеальні канали.

Водночас запропонований метод має певні обмеження. Найсуттєвішим недоліком є вища обчислювальна складність. Час вбудовування становить приблизно 1,87 секунди, що в 4–15 разів перевищує показники класичного та хаотичного LSB. Така затримка зумовлена необхідністю аналізу аудіо треку великою мовною моделлю. Крім того, якість роботи методу певною мірою залежить від точності та розміру використовуваної LLM, що може створювати додаткові вимоги до апаратного забезпечення.

Порівняно з Amplitude Adaptive LSB, який також належить до класу адаптивних методів, запропонований підхід демонструє помітну перевагу в показниках непомітності та стійкості, але поступається в швидкості виконання. Це свідчить про те, що LLM-Adaptive LSB найбільш доцільно застосовувати в тих сценаріях, де пріоритетом є максимальна прихованість і захищеність інформації, а не швидкодія (наприклад, у системах конфіденційного документообігу, архівуванні чутливих даних або захищеній передачі інформації).

Таким чином, проведене порівняльне дослідження підтверджує перспективність інтеграції великих мовних моделей у стеганографічні методи на основі LSB. Запропонований LLM-Adaptive LSB метод суттєво перевершує традиційні аналоги за ключовими критеріями якості стеганографії – непомітністю та стійкістю до виявлення, – хоча й вимагає додаткових обчислювальних ресурсів. Подальші дослідження можуть бути спрямовані на оптимізацію швидкості роботи (використання легких fine-tuned моделей) та розширення методу на аудіо- та відеоконтейнери.

Внесок авторів: Олександр Слободянюк – концептуалізація, пошук та аналіз джерел; Дмитро Бараннік – підготовка висновків; Юрій Бабенко, Родіон Прокопенко, Олег Сапов – розробка класифікації та її графічне оформлення.

ЛІТЕРАТУРА

[1] Adhiya K., Swati A. (2012) Hiding Text in Audio Using LSB Based Steganography. *Information and Knowledge Management (*pp. 8–15*)*. ISSN 2224-5758 (Paper) ISSN 2224-896X (Online). Vol 2, No.3.

[2] Alimpiev A., Barannik V., Podlesny S., Suprun O. and Bekirov Ali. (2017) The video information resources integrity concept by using binomial slots, 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH). Lviv, Ukraine, pp. 193–196, https://doi.org/10.1109/MEMSTECH.2017.7937564

[3] Usman Ibrahim Musa, Farida Ridzuan, A H Azni, Nur Hafiza Zakaria. Enhancing Audio Steganography Through CGAN-Generated Cover Audio and Adaptive LSB Embedding: A Hybrid Approach //

Malaysian Journal of Science Health & Technology. 2026. Vol. 12, No. 1. URL: https://mjosht.usim.edu.my/index.php/mjosht/article/view/507

[4] Auto-Stega: An Agent-Driven System for Lifelong Strategy Evolution in LLM-Based Text Steganography / M. Bai et al. *Proceedings of the 35th USENIX Security Symposium*. 2026. P. 112–129. URL: https://aclanthology.org/2026.eacl-long.36.pdf

[5] Audio steganography using AES encryption and lsb substitution for securing military data / J. N. Isaac et al. *Nightingale International Journal of Pure and Applied Science*. 2025. Vol. 8, No. 9. URL: https://www.researchgate.net/publication/391765996

[6] SparSamp: An Efficient Provably Secure Steganography Method Based on Sparse Sampling // arXiv preprint arXiv:2503.19499. 2025. URL: https://arxiv.org/pdf/2503.19499

[7] Banoori S. Z., Khan W., Rahman S., Masood F., Salam A. (2025) An Improved Hybrid Image Steganography Method Using AES Algorithm // Scientific Reports. 2025. Vol. 15, Article 28140. https://doi.org/10.1038/s41598-025-28140-0. URL: https://www.nature.com/articles/s41598-025-28140-0

[8] Barannik, V., Yudin, O., Boiko, Y., Ziubina, R., Vyshnevska, N. (2019). Video Data Compression Methods in the Decision Support Systems. In: Hu, Z., Petoukhov, S., Dychka, I., He, M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. https://doi.org/10.1007/978-3-319-91008-6_30

[9] Бараннік В. В. Рельефне представленгя зображень пірамідальним кодуванням. *Інформаційно-керуючи системи на залізничному транспорті*. 2001. № 1. С. 17–25.

[10] Бараннік В.В. та ін. Основи теорії структурно-комбінаторного стеганографічного кодування: монография Х.: В-во «Лідер», 2017. 256 с.

[11] Kim-Hui Yap, Wenyang Liu, Yi Wang, Lap-Pui Chau. Bitstream-Corrupted JPEG Images Are Restorable: Two-Stage Compensation and Alignment Framework for Image Restoration. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023, PP. 9979–9988.

[12] Alimpiev A., Barannik V., Podlesny S., Suprun O., Bekirov Ali. The video information resources integrity concept by using binomial slots. 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, Ukraine, 2017, pp. 193–196, https://doi.org/10.1109/MEMSTECH.2017.7937564

[13] Barannik V. V., Hahanova A. V., Krivonos V. N. Coding tangible component of transforms to provide accessibility and integrity of video data. East-West Design & Test Symposium (EWDTS 2013), 2013, pp. 1–5, https://doi.org/10.1109/EWDTS.2013.6673179

[14] Barannik V., Shiryaev A. Quadrature compression of images in polyadic space. Proceedings of International Conference on Modern Problem of Radio Engineering, Telecommunications and Computer Science, 2012, pp. 422–422. INSPEC Accession Number: 12713484.

[15] A. Krasnorutsky, R. Onyshchenko, D. Barannik and V. Barannik. The Methods of Intellectual Processing of Video Frames in Coding Systems in Progress Aeromonitor to Increase Efficiency and Semantic Integrity. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 53–56, https://doi.org/10.1109/ATIT58178.2022.10024208

[16] V. Barannik, S. Shulgin, N. Barannik and V. Barannik. Method of Coding Subbands of Non-Homogeneous Spectrum of Video Segments in Uneven Diagonal Space. 2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 2022, pp. 72–75, https://doi.org/10.1109/ATIT58178.2022.10024236

[17] Barannik V. et al.: The method of masking overhead compaction in video compression systems , Radioelectronic and Computer Systems, 2(2021), 2021, pp. 51–63 https://doi.org/10.32620/reks.2021.2.05

[18] Wong K. W. Image encryption using chaotic maps. Intelligent Computing Based on Chaos. 2009. Vol. 184. P. 333–354. https://doi.org/10.1007/978-3-540-95972-4_16

[19] Barannik V., Krasnorutsky A., Kolesnyk V., Barannik V., Pchelnikov S., Zeleny P. Method of compression and ensuring the fidelity of video images in infocommunication networks. Radioelectronic and computer systems, 2022, vol. 4, pp. 129–142. https://doi.org/10.32620/reks.2022.4.10

[20] Бараннік Д.В. Технологія приховування інформативного контенту в динамічному потоці відеосегментів. *Наукоємні технології*. 2023. № 4. С. 408–415. https://doi.org/10.18372/2310-5461.60.18270

[21] Barannik, V., Lytvinenko, M., Okladnoy, D., Suprun, O. Description of the OFDM symbol with the help of mathematical laws. Analysis of technologies that were used in this case (2017) 2nd International Conference on Advanced Information and Communication Technologies, AICT 2017 – Proceedings, art. no. 8020095, pp. 183–187. https://doi.org/10.1109/AIACT.2017.8020095

[22] Bisht P., Jarial E. P. Enhanced Image Compression and Steganography Techniques Using DWT and LSB: A Comparative Analysis // Lecture Notes in Networks and Systems. Cham: Springer, 2025. pp. 287–299. https://doi.org/10.1007/978-3-032-03740-4_17

[23] Dutta Hrishikesh. An Overview of Digital Audio Steganography. // Dutta Hrishikesh, Das, Rohan, Nandi Sukumar, Prasanna S. – IETE Technical Review. Vol. 37, No. 1. P. 1–19. https://doi.org/10.1080/02564602.2019.1699454

[24] Jabbar Al Ali I. A., Abdulazeez Z. A. JPEG-Resistant DCT Steganography for Secure Communication. EBSCOhost Journal of Secure Systems, 2026. URL: https://www.researchgate.net/ publication/394095219_JPEG-Resistant_DCT_Steganography_for_Secure_Communication

[25] Barannik, V., Barannik, D., Babenko, M., Prokopenko, R., Akimov, O., & Petrukha, N. (2026). Devising a method for complex steganographic embedding of information in the structural-psychovisual space. *Eastern-European Journal of Enterprise Technologies*, *1*(9 (139), 19–30. https://doi.org/10.15587/1729-4061.2026.351181.

[26] Khalifa I. A., Saleem S. M., Sengur A. Multilayer Steganalysis in the Encryption Era: A Comprehensive Review // Engineering and Applied Science Journal of Emerging Technologies (EJASET). 2026. URL: https://ejaset.com/index.php/journal/article/view/410

[27] Kim-Hui Yap, Wenyang Liu, Yi Wang, Lap-Pui Chau. Bitstream-Corrupted JPEG Images Are Restorable: Two-Stage Compensation and Alignment Framework for Image Restoration. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2023, PP. 9979–9988.

[28] Barannik, V., Sidchenko, S., Barannik, D., Barannik, V., Datsun, A. (2021). Devising a conceptual method for generating cryptocompression codograms of images without loss of information quality. *Eastern-European Journal of Enterprise Technologies,* 4 (2 (112)), 6–16. https://doi.org/10.15587/1729-4061.2021.237359.

[29] Barannik, V. et al. (2023). Processing Marker Arrays of Clustered Transformants for Image Segments. In: Klymash, M., Luntovskyy, A., Beshley, M., Melnyk, I., Schill, A. (eds) Emerging Networking in the Digital Transformation Age. TCSET 2022. *Lecture Notes in Electrical Engineering,* vol 965. Springer, Cham. https://doi.org/10.1007/978-3-031-24963-1_25

[30] Nasution M. H., Anrilva N. D., Salsabilah N. Implementasi Steganografi pada Citra Digital Menggunakan Metode LSB dengan Pengamanan Pesan Menggunakan Kriptografi Sederhana. Jurnal Ilmu Komputer Universitas Muhammadiyah (2026). https://doi.org/10.62671/jikum.v2i2.207

[31] Peng J. Audio Steganalysis Estimation with the Goertzel Algorithm. Applied Sciences. 2024. Vol. 14, No. 14. Art. 6000. URL: https://www.mdpi.com/2076-3417/14/14/6000

[32] Бараннік В. В. та ін. Метод стиснення зображень на основі нерівновагового позиційного кодування бітових площин. 2009. № 1. С. 84–92. URL: http://nbuv.gov.ua/UJRN/recs_2009_1_13

[33] A. Krasnorutsky, V. Kolesnyk, A. Berchanov, V. Barannik, N. Kharchenko and O. Malko, "Method of Structural-Statistical Coding of Video Segments in Spectral-Cluster Space," *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2022, pp. 32–37, https://doi.org/10.1109/ATIT58178.2022.10024240

[34] Pilania U., Kumar M. Unveiling the Art of Steganography: A Modern Approach. London: CRC Press, 2026. 254 p. ISBN 9781032972725. URL: https://books.google.com/ books?id=OtalEQAAQBAJ

[35] Pundeer U., Singh Y. V., Yaduvanshi D., Mishra A. To Design Image Steganographic Techniques for Information Hiding // In: Advances in Cybersecurity and Information Systems. London: Taylor & Francis, 2025. pp. 881–896. https://doi.org/10.1201/9781003593034-88

[36] V. Barannik, Y. Babenko, V. Barannik, V. Kolesnyk and D. Zhuikov, "Method Taking into Account Level of Structural and Statistical Saturation of Video Segments in the Coding Process," *2022 IEEE 4th International Conference on Advanced Trends in Information Theory (ATIT)*, Kyiv, Ukraine, 2022, pp. 66–71, https://doi.org/10.1109/ATIT58178.2022.10024193

[37] Raiyan S., Kabir M. SCReedSolo: A Secure and Robust LSB Image Steganography Framework with Randomized Symmetric Encryption and Reed–Solomon Coding // Lecture Notes in Networks and Systems. Singapore: Springer, 2025. pp. 241–256. https://doi.org/10.1007/978-981-95-4395-3_16

[38] Rakshith P., Karthik P., Madhusudhan G., Ananya K. 2LSS: A Two-Layer Security Scheme Using the Crypto-Steganography Approach to Enable High-Level Security for a Cloud Environment // SN Computer Science. 2026. Vol. 7. Article ID 04520. https://doi.org/10.1007/s42979-025-04520-1

[39] Slobodianinuk, O., Kostromytskyi, A., Chebanenko, V., Dihtiar, M., & Onypchenko, P. LSB metody prykhovanoi peredachi povidomlen u telekomunikatsiinykh systemakh [LSB methods of hidden message transmission in telecommunication systems]. *Naukoiemsni Tekhnolohii*, 62(2), 138–146. https://doi.org/10.18372/2310-5461.62.18714

[40] Varshith M., Gayathri A., Yedlapalli S. Enhancing Security and Perceptual Quality in LSB-Based Image Steganography // Lecture Notes in Networks and Systems. Cham: Springer, 2025. pp. 213–227. https://doi.org/10.1007/978-3-031-99882-9_13

[41] Wong K. W. Image encryption using chaotic maps. Intelligent Computing Based on Chaos. 2009. Vol. 184. P. 333–354. https://doi.org/10.1007/978-3-540-95972-4_16

Слободянюк О., Бараннік Д., Бараннік В., Прокопенко Р., Сапов О.

МЕТОД СТЕГАНОГРАФІЧНОГО ПРИХОВУВАННЯ В АУДІОКОНТЕЙНЕРАХ ІЗ ВИКОРИСТАННЯМ LLM

Вступ. Розвиток цифрових мереж потребує вдосконалення методів прихованої передачі даних, серед яких найбільш поширеним є підхід LSB завдяки своїй простоті та високій ємності. Проте сучасні методи стего-аналізу зумовлюють необхідність глибокої систематизації та критичного аналізу існуючих досліджень для підвищення стійкості й адаптивності алгоритмів. Метою є комплексний аналіз та систематизація сучасних досліджень у сфері LSB-стеганографії для виявлення актуальних тенденцій і формування аналітичної бази, що дозволить вдосконалити методи прихованої передачі інформації.

Методи. Було використано метод системного аналізу та класифікації сучасних наукових публікацій у сфері захисту цифрових даних. Дослідження охоплювало аналіз еволюції LSB-методів (Least Significant Bit), зокрема їх гібридизацію з криптографічними алгоритмами (AES, RSA), частотними перетвореннями (DWT, DCT) та стохастичними підходами (хаотичні карти). Особлива увага приділялася використанню кодування Reed-Solomon, адаптивного вибору пікселів та моделей машинного навчання для оптимізації вбудовування даних.

Результати. Розроблено адаптивний метод аудіостеганографії, який використовує великі мовні моделі (LLM) для динамічного керування глибиною LSB-вбудовування (k) на основі психоакустичного аналізу та локальної ентропії сигналу. Експериментальне моделювання в MATLAB підтвердило перевагу методу над класичними аналогами, зокрема досягнуто найвищий показник пікового відношення сигналу до шуму (PSNR = 58,23 дБ) та мінімальну середньоквадратичну помилку (MSE = 0,098).

Висновки. Інтеграція LLM у процес стеганографічного кодування дозволяє перетворити LSB-підхід на інтелектуальну систему, що адаптується до семантичного контексту аудіоконтейнера, забезпечуючи високу візуальну та статистичну непомітність. Попри збільшення часу обробки, запропонований алгоритм є оптимальним для захищених систем передачі даних завдяки здатності мінімізувати вплив на людську слухову систему (HAS) та протистояти сучасним методам стегоаналізу.

Ключові слова: аудіостеганографія, метод найменш значущого біта, LSB, аудіоконтейнер, гібридні стеганографічні методи.

Slobodianiuk O., Barannik D., Barannik V., Prokopenko R., Sapov O.

METHOD OF STEGANOGRAPHIC HIDING IN AUDIO CONTAINERS USING LLMS

Background. The development of digital networks requires the improvement of methods for covert data transmis-sion, among which the LSB approach is the most common due to its simplicity and high capacity. However, modern stegoanalysis methods necessitate a deep systematization and critical analysis of existing research to increase the sta-bility and adaptability of algorithms. The goal is a comprehensive analysis and systematization of modern research in the field of LSB steganography to identify current trends and form an analytical base that will allow improving methods for covert information transmission.

Methods. The method of systematic analysis and classification of modern scientific publications in the field of digital data protection was used. The study covered the analysis of the evolution of LSB (Least Significant Bit) methods, in par-ticular their hybridization with cryptographic algorithms (AES, RSA), frequency transforms (DWT, DCT) and stochas-tic approaches (chaotic maps). Special attention was paid to the use of Reed-Solomon coding, adaptive pixel selection and machine learning models to optimize data embedding.

Results. An adaptive audio steganography method has been developed that uses large language models (LLM) to dynamically control the depth of LSB embedding (k) based on psychoacoustic analysis and local signal entropy. Ex-perimental simulation in MATLAB confirmed the superiority of the method over classical analogues, in particular, the highest peak signal-to-noise ratio (PSNR = 58.23 dB) and the minimum mean square error (MSE = 0.098) were achieved.

Conclusions. The integration of LLM into the steganographic coding process allows us to transform the LSB ap-proach into an intelligent system that adapts to the semantic context of the audio container, providing high visual and statistical invisibility. Despite the increase in processing time, the proposed algorithm is optimal for secure data trans-mission systems due to its ability to minimize the impact on the human auditory system (HAS) and resist modern stego-analysis methods.

Keywords: Audio steganography, least significant bit method, LSB, audio container, hybrid steganographic methods.

Дата першого надходження: 13.05.2026 р.
Дата прийняття до друку: 18.05.2026 р.
Дата публікації: 28.05.2026 р.