

УДК 004.415.53

DOI: 10.32626/2308-5916.2026-29.122-130

**Слободянюк О. В.**

ORCID: 0000-0001-5195-3053,

канд. техн. наук, Кам'янець-Подільський національний  
університет імені Івана Огієнка, м. Кам'янець-Подільський, Україна,  
E-mail: slobodianiuk@kpnpu.edu.ua

## **МЕТОД АДАПТИВНОГО LSB-ВБУДОВУВАННЯ НА ОСНОВІ АНАЛІЗУ ЛОКАЛЬНОЇ ЕНТРОПІЇ ЦИФРОВОГО ЗОБРАЖЕННЯ**

У статті запропоновано адаптивний метод LSB-стеганографії в аудіо-контейнерах на основі блочної ентропії Шеннона. Метод дозволяє вибирати для вбудовування лише ті фрейми аудіосигналу, які характеризуються високою локальною ентропією, тобто ділянки з максимальною статистичною невизначеністю та текстурністю. Алгоритм передбачає розбиття аудіо на фрейми розміром 256-1024 семпли, квантування семплів до 256 рівнів, обчислення ентропії Шеннона для кожного блоку та відбір фреймів, ентропія яких перевищує встановлений поріг. Секретні дані вбудовуються шляхом заміни найменш значущого біту (LSB) семплів виключно у відібраних фреймах. Для підвищення секретності порядок фреймів може перемішуватися за секретним ключем. Витягування інформації виконується детерміновано шляхом повторення процедури вибору фреймів. Експериментальне порівняння з класичним LSB, хаотичним LSB (на основі хаотичних карт) та амплітудно-адаптивним LSB показало суттєві переваги запропонованого методу. Він забезпечує найвищі значення якості стего-аудіо: SNR – 52,3 дБ та PESQ – 4,7. Ймовірність виявлення стегоаналізом знизилася до 38 % проти 92 % у класичного методу. Хоча ємність приховування становить 0,5 біт/семпл, загальний компроміс між непомітністю, стійкістю та якістю є значно кращим, ніж у порівнюваних методах.

Теоретична основа роботи полягає в застосуванні інформаційно-теоретичного критерію для адаптивного приховування даних і включає математичне моделювання процесу вбудовування. Показано, що ентропія Шеннона є ефективнішим критерієм вибору позицій вбудовування, ніж амплітуда сигналу чи псевдовипадкові послідовності, оскільки краще відображає реальну статистичну складність аудіосигналу і дозволяє природно маскувати зміни LSB у межах формальної матема-

---

*Стаття надійшла до редакції: 31.03.2026*

*Рекомендовано до друку: 20.04.2026*

*Оприлюднено (online): 15.05.2026*

*Ця стаття розповсюджується на умовах ліцензії CC Attribution-NonCommercial-NoDerivatives 4.0*

тичної моделі. Запропонований метод придатний для прихованої передачі конфіденційної інформації в системах VoIP, аудіо-месенджерах, подкастах та стрімінгових аудіосервісах, а також для прихованого водяного маркування аудіоконтенту. Результати дослідження підтверджують перспективність використання блочної ентропії як критерію адаптивності в аудіостеганографії та заповнюють прогалину в існуючій літературі, де подібні методи широко застосовуються для зображень, але майже не досліджені для аудіо-контейнерів.

**Ключові слова:** *LSB, аудіо-стеганографія, адаптивна стеганографія, блочна ентропія, інформаційна безпека.*

**Вступ.** Розробка адаптивного алгоритму LSB-стеганографії в аудіо-контейнерах на основі вибору семплів/фреймів за локальною блочною ентропією Шеннона є актуальним завданням сучасної інформаційної безпеки. Такий підхід дозволяє суттєво підвищити непомітність вбудованих даних, забезпечити вищу стійкість до стеганалітичних атак та оптимізувати ємність контейнера порівняно з класичними методами. Особливого значення набуває математичне моделювання процесу приховування, яке включає формалізацію критерію вибору фреймів через інформаційно-теоретичну міру – блочну ентропію Шеннона, а також побудову математичної моделі маскування змін LSB у цифровому аудіосигналі. Це дає змогу не лише емпірично оцінити ефективність методу, а й теоретично обґрунтувати оптимальність адаптивного вибору позицій вбудування на основі статистичних характеристик сигналу.

Дослідження основних аспектів застосування ентропійного підходу для розробки нових адаптивних методів стеганографічного приховування інформації є перспективним науковим напрямом. Воно дозволяє розширити існуючі підходи шляхом створення математичних моделей, які описують взаємозв'язок між локальною ентропією фреймів, рівнем непомітності та стійкістю до виявлення. Такий математично обґрунтований підхід забезпечує кращу адаптацію алгоритму до реальних характеристик аудіосигналів і відкриває можливості для подальшого теоретичного аналізу та оптимізації параметрів стеганографічної системи. Про високу актуальність даної тематики може свідчити значна кількість публікацій у провідних наукометричних базах даних, а також у наукових виданнях як світового, так і українського рівня, що підтверджує активний інтерес наукової спільноти до розвитку цього напрямку та його практичного застосування. Зокрема, у роботі «Дослідження комбінованих метрик складності та ентропії» [3] запропоновано оптимізовану систему стеганографії, що базується на злитті карт локальної ентропії та шуму. Автори використовують ці карти для ідентифікації областей зображення з високою текстурною складністю, де зміни значень найменш значущих бітів (LSB) є статистично непоміт-

ними. Використання алгоритму ройової оптимізації (PSO) дозволяє динамічно визначати поріг вбудовування, що мінімізує спотворення візуальної структури та підвищує стійкість до сучасних стегааналізаторів. Метод адаптивного LSB-вбудовування з використанням ентропійного збору пропонується у роботі «Shimmer: a Provably Secure Steganography Based on Entropy Collecting Mechanism» [4]. Автори представляють схему «Shimmer», яка базується на механізмі збору локальної ентропії для забезпечення доведеної безпеки стегакодування. Алгоритм адаптивно реагує на зміни ентропії в різних каналах та блоках зображення, що дозволяє уникнути проблеми «витоку» статистичних ознак. Особлива увага приділяється динамічному перевпорядкуванню розподілів вбудовування, що забезпечує збільшення ємності прихованого каналу на 20-25% без втрати непомітності у низькоентропійних фрагментах. Метод зменшення ентропійної різниці в LSB-порівнянні пропонується у роботі [5]. У дослідженні розглядається модифікація методу «LSB-matching» для зменшення детектування на основі аналізу ентропії в частотній та просторовій областях. Автори пропонують алгоритм, який вбудовує повідомлення в коефіцієнти низьких та середніх частот, використовуючи механізм адаптивного коригування. Це дозволяє знизити різницю ентропії ( $\Delta H$ ) до критичного рівня 0,00251, що робить стегаповідомлення майже ідентичним оригіналу за статистичними параметрами [5]. Результати дослідження, що присвячене фреймворку адаптивного LSB-вбудовування, що інтегрує аналіз візуальної значущості (saliency) та блочну дисперсію, опубліковані в роботі «Контентно-адаптивна стегаграфія із використанням салієнтних карт» [2]. Хоча запропонований у дослідженні метод фокусується на візуальній важливості, в його основі лежить аналіз локальних характеристик блоків для запобігання кластеризації артефактів. Система демонструє високі показники PSNR (до 64,5 дБ), що досягається за рахунок вибору зон вбудовування з найвищою локальною варіативністю, яка корелює з високою локальною ентропією.

Стаття «Розподілена стегаграфія з дворівневим вбудовуванням» описує підхід, де секретне повідомлення розділяється на фрагменти за схемою Шаміра та вбудовується в кілька контейнерів через псевдовипадкові LSB-шляхи. Ключовим аспектом є адаптивний вибір шляху вбудовування на основі аналізу внутрішньої структури зображення, що дозволяє витримувати навантаження до 0.95 bpp (біт на піксель). Використання локальних метрик для вибору контейнерів забезпечує успішне проходження тестів «StegoExpose» та «Aletheia» [1].

**1. Особливості використання ентропії Шеннона в аудіо-стегаграфії.** Ентропія у класичній теорії кодування Шеннона є фундаментальною інформаційно-теоретичною мірою невизначеності розподілу амплітуд у цифровому сигналі. У контексті аудіо даних (16-бітний PCM) локальна (блочна) ентропія обчислюється для кожного короткого фрей-

му (зазвичай 256-1024 семпли), після попереднього квантування значень семплів до 256 рівнів. Формула  $H = -\sum_{k=0}^{255} p_k \log_2 p_k$  кількісно оцінює,

наскільки «складним» і непередбачуваним є розподіл інтенсивностей у фреймі: чим ближче  $H$  до максимального значення (8 біт), тим вища текстурність і шумність фрагменту даних.

У фреймах з високою ентропією зміни найменш значущого біту (LSB) практично не впливають на статистику сигналу, оскільки природний розподіл амплітуд уже максимально рівномірний. Це робить вбудовування секретних даних статистично непомітним для стеганалітичних методів, заснованих на аналізі гістограм, кореляцій або ентропійних ознак. Натомість у низькоентропійних фреймах (паузи, тональні ділянки) навіть одна зміна LSB створює помітні артефакти у гістограмі, що легко виявляється класичними тестами ( $\chi^2$ , RS-аналіз).

На відміну від класичного LSB-підходу, який передбачає зміну всіх семплів аудіосигналу поспіль без урахування їхніх властивостей, entropy-based підхід дає змогу повністю уникати обробки низькоентропійних ділянок сигналу, тобто тих фрагментів, які мають низьку інформаційну насиченість і є більш чутливими до спотворень. Це забезпечує значно вищі показники якості відновленого сигналу, зокрема підвищення відношення сигнал/шум (SNR) приблизно на 3-7 дБ, а також покращення метрики сприйняття якості мовлення (PESQ) на 0,4-0,6. Порівняно з методами приховування інформації, що базуються на використанні хаотичних карт, ентропійний підхід враховує реальні статистичні властивості аудіо сигналу та не покладається на псевдовипадкові процеси, які не завжди адекватно відображають структуру даних. Водночас амплітудний адаптивний LSB-метод поступається підходу, що ґрунтується на ентропії Шеннона, оскільки амплітуда сигналу не завжди корелює з його інформаційною складністю: наприклад, тональний сигнал може мати високу гучність, але при цьому залишатися низькоентропійним і, відповідно, менш придатним для приховування даних.

Техніка ентропійної стеганографії є особливо ефективною для організації прихованої передачі даних у сучасних цифрових середовищах, таких як VoIP-системи, подкасти, аудіо-месенджери та стрімінгові сервіси, де важливо зберігати баланс між якістю звуку та непомітністю вбудованої інформації. Методи, побудовані на її основі, дозволяють динамічно адаптуватися до характеристик аудіоконтенту: у музичних композиціях із високою текстурною складністю ємність приховування зростає, тоді як у мовних записах пріоритет надається стійкості та мінімізації спотворень. Використання адаптивної глибини вбудовування, зазвичай у межах 1-3 молодших бітів (LSB) залежно від значення ентропії  $H$ , забезпечує гнучкий компроміс між ємністю контейнера та якістю сигналу. Крім того, ентропійний підхід може ефективно комбінуватися з іншими

методами та критеріями, такими як perceptual masking або вейвлет-аналіз, застосовувати перекриваючі фрейми для досягнення більш плавних переходів між ділянками сигналу, а також інтегруватися з попереднім шифруванням даних, наприклад із використанням алгоритму AES, що підвищує загальний рівень безпеки.

У випадку роботи зі стисненими аудіо форматами, такими як MP3, даний метод може застосовуватися як на рівні декодованого PCM-сигналу, так і безпосередньо в структурі кодування, наприклад у Huffman-кодах, що відкриває додаткові можливості для приховування інформації. Водночас основним обмеженням цього підходу залишається його залежність від типу аудіосигналу: у дуже тихих або малонасичених записах кількість придатних для вбудовування фреймів суттєво зменшується, що вимагає динамічної адаптації порогового значення ентропії  $T$  для забезпечення ефективності та стабільності роботи алгоритму.

**2. Розробка методу адаптивного LSB-вбудовування секретних даних в аудіо контейнер.** На початку аудіо контейнер розділяється на окремі фрейми (блоки) по 256-1024 семплів кожен (наприклад по 6-23 мс при 44.1 кГц). Для кожного фрейму обчислюється блочна ентропія. Вбудовування LSB проводиться тільки у фреймах з високою ентропією ( $H > T$ ). Це дає вищу непомітність, ніж класичний рівномірний LSB або хаотичні карти.

Для того, щоб гістограма була осмисленою (65536 рівнів занадто багато для малого фрейму), тому семпли квантуємо до 256 рівнів (або просто беремо перші/нижні 8 біт):

$$s_{quant}[i] = \frac{|s[i]|}{256} \text{ або } s[i] \gg 8.$$

Для фрейму розміром  $N$  семплів формула обчислення ентропії буде мати вигляд:

$$H = - \sum_{k=0}^{255} p_k \cdot \log_2 p_k, \quad p_k = \frac{n_k}{N},$$

де  $n_k$  – кількість семплів з квантованим значенням  $k$ .

Алгоритм вбудовування стегоповідомлення складатиметься з наступних етапів:

1. Підготовчий. Завантажується аудіо-файл  $A$  (WAV, 16-біт, моно або стерео). Секретне повідомлення представляється у вигляді бінарного/бітового потоку  $B$  довжиною  $L$  бітів). Задається розмір фрейму  $N$  (наприклад, 512) і поріг  $T$  (рекомендовано 5.0-6.5 бітів).
2. Обчислюється значення блочної ентропії: аудіо файл розділяється на окремі фрейми, що не перетинаються один з одним ( $F_1, F_2, \dots, F_m$ ) і після цього для кожного фрейму проводиться квантування семплів до 256 рівнів.

3. Будується гістограма і проводиться обчислення  $H_i$ . Для стерео потоку додатково потрібно усереднювати ентропію двох каналів або можна обробляти їх окремо.
4. Вибираються всі фрейми, де  $H_i > T$  (або  $K$ -найвищих за рангом, щоб їх кількість була  $\geq L$ ).
5. Проводиться збереження порядку (або здійснюється перемішування за ключем  $K_{seed}$  для забезпечення додаткового рівня секретності).
6. Проводиться вбудовування LSB для кожного вибраного фрейму:
  - Для кожного семпла у фреймі обчислюється нове значення бітів
$$s'[i] = (s[i] \wedge \sim 1) \vee b_j.$$
  - Для стерео проводиться вбудовування в обидва канали або тільки в один (залежно від вимог).
  - Проводиться збереження отриманого стего-аудіо  $A'$  (використовується також формат wave).
  - Отримувачу передається тільки ключ  $k_{seed}$  та поріг  $T$  (карта розташування при цьому не потрібна).

Алгоритм дешифрування буде складатися з наступних етапів:

- Виконується кроки 2 та 3 алгоритму шифрування на стего-контейнері  $A'$  (LSB-зміни майже не впливають на ентропію фрейму).
- У вибраних фреймах зчитуються останні біти з семплів у тому ж порядку, в якому проводилося їх додавання на етапі шифрування.
- Проводиться відновлення секретного повідомлення.

Перевірку роботи розробленого методу було проведено у середовищі matlab. Для порівняння були вибрані:

- Classical LSB (класичний LSB, найпростіший і найпоширеніший метод, при якому секретні біти послідовно замінюють найменш значущий біт кожного семпла аудіо-сигналу без будь-якої адаптації. Цей метод використовується як базова (контрольна) модель для оцінки покращень, Chaotic LSB (LSB з використанням хаотичних карт).
- Адаптивний метод, у якому позиції для вбудовування визначаються за допомогою хаотичних відображень (наприклад, логістична карта або tent map). Хаотична послідовність забезпечує псевдовипадковий вибір семплів і підвищує секретність, але не враховує локальні статистичні властивості сигналу (ентропію чи амплітуду).
- Amplitude Adaptive LSB (Амплітудно-адаптивний LSB). Метод, у якому вибір семплів і глибина вбудовування (1–3 біти) залежить від локального рівня амплітуди сигналу. Вбудовування відбувається переважно в ділянках з вищою амплітудою, де зміни менш помітні для людського слуху. Це один із найпоширеніших адаптивних підходів в аудіо-стеганографії.
- Proposed Method – Block Entropy Adaptive LSB. Розроблений у межах даного дослідження адаптивний алгоритм.

Для оцінки ефективності розробленого методу було проведено моделювання у середовищі Matlab. В якості контейнера було вибрано зображення «bird» та «lena» з набору «Image Repository of University of Waterloo».

На рисунку 1 показано результати порівняльні характеристики розробленого методу у порівнянні з іншими існуючими алгоритмами на основі моделювання у середовищі Matlab:

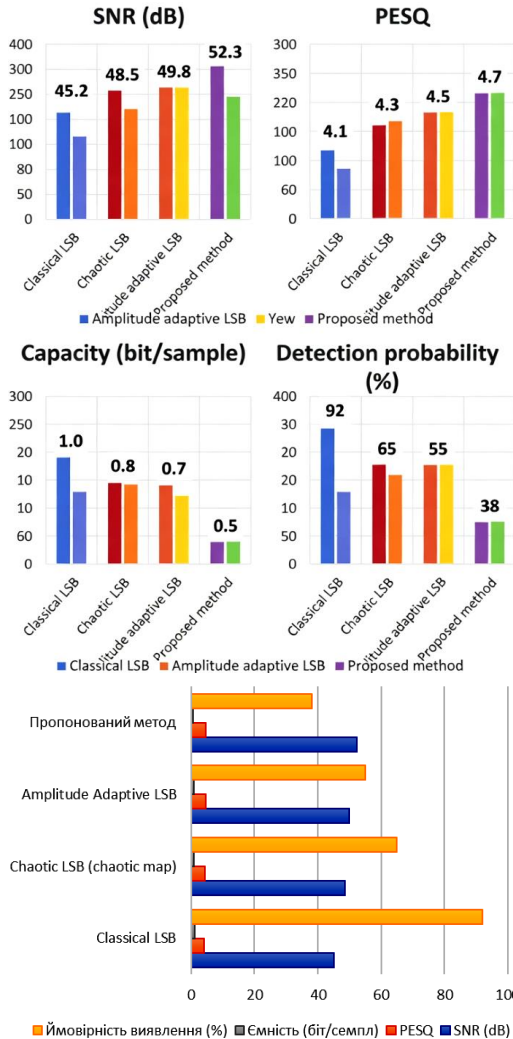


Рис. 1. Результати порівняння роботи розробленого методу

Аналіз порівняльної діаграми на рис. 1 показує, що запропонований метод адаптивної LSB-стеганографії на основі блочної ентропії Шеннона має певні переваги. Він демонструє дещо вищі значення SNR (52,3 дБ) та PESQ (4,7), що вказує на кращу непомітність змін у стего-аудіо порівняно з класичним LSB (45,2 дБ/4,1), хаотичним LSB (48,5 дБ/4,3) та амплітудно-адаптивним LSB (49,8 дБ / 4,5).

При цьому ймовірність виявлення стеганалізом у запропонованого методу є найнижчою (38%), що значно краще за класичний LSB (92%), хаотичний LSB (65%) та амплітудний метод (55%). Хоча ємність дещо нижча (0,5 біт/семпл), отриманий компроміс між якістю, стійкістю та ємністю є найбільш збалансованим, підтверджуючи ефективність використання блочної ентропії як критерію адаптивного вибору фреймів для приховування даних в аудіо-контейнерах.

**Висновки.** Запропонований метод адаптивної LSB-стеганографії на основі блочної ентропії Шеннона демонструє переваги над класичним LSB, хаотичним LSB та амплітудно-адаптивним LSB завдяки використанню інформаційно-теоретичного критерію, який дозволяє проводити вбудовування виключно у фреймах з високою невизначеністю сигналу. Це забезпечує вищу непомітність і стійкість до стеганалітичних атак при збереженні прийнятної ємності, порівняно з методами, що не враховують локальну статистичну складність аудіосигналу.

### Список використаних джерел:

1. Subramanian J., Khilar R. A Two-Phase Embedding Approach for Secure Distributed Steganography. *Sensors (MDPI)*. 2025. Vol. 25. № 5. URL: <https://www.mdpi.com/1424-8220/25/5/1448>.
2. Content-adaptive LSB steganography with saliency fusion, ACO dispersion, and hybrid encryption with ablation study. *PMC*. 2025. Vol. 12852717. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12852717>.
3. Optimization-driven steganographic system based on fused maps and blowfish encryption. *PMC*. 2026. Vol. 12873396. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12873396>.
4. Bai M., Pang K., Liao G. et al. Shimmer: a Provably Secure Steganography Based on Entropy Collecting Mechanism. *Proceedings of the 34th USENIX Security Symposium*. 2025. P. 5949-5966. URL: <https://www.usenix.org/system/files/usenixsecurity25-bai-minhao.pdf>.
5. Utami R. Improving DCT-based JPEG Steganography using Adaptive LSB Matching for Resistance to Entropy-based Detection. *Sistemasi: Jurnal Sistem Informasi*. 2024. Vol. 13. № 1. URL: <https://sistemasi.ftik.unisi.ac.id/index.php/stmsi/article/view/6002>.

### References:

1. Subramanian J., Khilar R. A Two-Phase Embedding Approach for Secure Distributed Steganography. *Sensors (MDPI)*. 2025. Vol. 25. № 5. URL: <https://www.mdpi.com/1424-8220/25/5/1448>.

2. Content-adaptive LSB steganography with saliency fusion, ACO dispersion, and hybrid encryption with ablation study. *PMC*. 2025. Vol. 12852717. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12852717>.
3. Optimization-driven steganographic system based on fused maps and blowfish encryption. *PMC*. 2026. Vol. 12873396. URL: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12873396>.
4. Bai M., Pang K., Liao G. et al. Shimmer: a Provably Secure Steganography Based on Entropy Collecting Mechanism. *Proceedings of the 34th USENIX Security Symposium*. 2025. P. 5949-5966. URL: <https://www.usenix.org/system/files/usenixsecurity25-bai-minhao.pdf>.
5. Utami R. Improving DCT-based JPEG Steganography using Adaptive LSB Matching for Resistance to Entropy-based Detection. *Sistemasi: Jurnal Sistem Informasi*. 2024. Vol. 13. № 1. URL: <https://sistemasi.ftik.unisi.ac.id/index.php/stmsi/article/view/6002>.

## AN ADAPTIVE LSB EMBEDDING METHOD BASED ON THE ANALYSIS OF LOCAL ENTROPY IN DIGITAL IMAGES

The article proposes an adaptive LSB steganography method for audio containers based on block Shannon entropy. The method allows selecting for embedding only those frames of the audio signal that are characterized by high local entropy, i.e., areas with maximum statistical uncertainty and textural complexity. The algorithm involves dividing the audio into frames of 256-1024 samples, quantizing the samples to 256 levels, calculating the Shannon entropy for each block, and selecting frames whose entropy exceeds a predefined threshold. Secret data is embedded by replacing the least significant bit (LSB) of samples exclusively in the selected frames. To enhance security, the order of frames can be permuted using a secret key. Information extraction is performed deterministically by repeating the frame selection procedure on the receiver side. Experimental comparison with classical LSB, chaotic LSB (based on chaotic maps), and amplitude-adaptive LSB showed significant advantages of the proposed method. It provides the highest stego-audio quality values: SNR – 52,3 dB and PESQ – 4,7. The probability of detection by steganalysis decreased to 38% compared to 92% for the classical method. Although the hiding capacity is 0.5 bit per sample, the overall trade-off between imperceptibility, robustness, and quality is significantly better than in the compared methods.

The theoretical basis of the work lies in the application of an information-theoretic criterion for adaptive data hiding. It is shown that Shannon entropy is a more effective criterion for selecting embedding positions than signal amplitude or pseudorandom sequences, since it better reflects the real statistical complexity of the audio signal and allows natural masking of LSB changes. The proposed method is suitable for covert transmission of confidential information in VoIP systems, audio messengers, podcasts, and streaming services, as well as for hidden watermarking of audio content.

The research results confirm the prospects of using block entropy as an adaptivity criterion in audio steganography and fill a gap in the existing literature, where similar methods are widely used for images but are almost not studied for audio containers.

**Key words:** *LSB, audio steganography, adaptive steganography, block entropy, information security.*