УДК 004.056.5

В. В. Торохтій
В. В. Карпінець

ВДОСКОНАЛЕНИЙ МЕТОД ГІБРИДНОЇ LSB-СТЕГАНОГРАФІЇ ДЛЯ ПІДВИЩЕННЯ СТІЙКОСТІ ДО ПАСИВНОГО СТЕГОАНАЛІЗУ

Вінницький національний технічний університет

Анотація

У роботі розглянуто науково-методичний підхід до підвищення стійкості LSB-стеганографії до пасивного стегоаналізу. Основну увагу приділено не програмній реалізації, а формалізації моделі прихованої передачі даних, структурі вдосконаленого алгоритму, ролі адаптивного симетричного шифрування, псевдовипадкового вибору позицій вбудовування та динамічного корекційного кодування на основі кодів Ріда-Соломона. Запропонований підхід зменшує передбачуваність бітової структури прихованого повідомлення, знижує ризик статистичного виявлення та підвищує ймовірність коректного відновлення даних після часткового пошкодження стегоконтейнера.

Ключові слова: LSB-стеганографія, пасивний стегоаналіз, прихована передача даних, симетричне шифрування, псевдовипадкове вбудовування, коди Ріда-Соломона, стегоконтейнер.

Abstract

The paper considers a scientific and methodological approach to increasing the resistance of LSB steganography to passive steganalysis. The main focus is placed not on software implementation but on the formalization of the covert data transmission model, the structure of the improved algorithm, the role of adaptive symmetric encryption, pseudorandom embedding position selection, and dynamic Reed-Solomon error correction coding. The proposed approach reduces the predictability of the hidden bit sequence, decreases the risk of statistical detection, and improves the probability of correct data recovery after partial stego-container distortion.

Keywords: LSB steganography, passive steganalysis, covert data transmission, symmetric encryption, pseudorandom embedding, Reed-Solomon codes, stego-container.

Вступ

Прихована передача даних у цифрових зображеннях є важливим напрямом інформаційної безпеки, оскільки вона спрямована не тільки на захист змісту повідомлення, а й на маскування самого факту інформаційного обміну. У відкритих або потенційно контрольованих каналах зв'язку така властивість є принциповою, адже виявлення факту приховування вже може бути достатнім для блокування, фільтрації або подальшої активної атаки на контейнер.

Одним із найпоширеніших підходів у цифровій стеганографії є LSB-метод, у якому повідомлення вбудовується в найменш значущі біти пікселів. Його перевагами є простота, висока місткість і незначний візуальний вплив на зображення. Водночас класичне послідовне LSB-вбудовування є вразливим до пасивного аналізу, оскільки воно може змінювати статистичну структуру молодших бітів, гістограмні характеристики та кореляційні зв'язки між елементами зображення [1], [2].

Пасивний стегоаналіз відрізняється від активних атак тим, що зловмисник не змінює контейнер, а лише аналізує його властивості. Тому захист від такого типу атак повинен бути спрямований на зменшення статистичної помітності прихованого повідомлення, розсіювання бітів у контейнері та усунення повторюваних закономірностей у вбудованій послідовності.

Метою роботи є обґрунтування вдосконаленого методу гібридної LSB-стеганографії для підвищення стійкості до пасивного стегоаналізу шляхом поєднання адаптивного симетричного шифрування, псевдовипадкового розміщення даних і динамічного корекційного кодування.

Результати дослідження

Формалізація запропонованого підходу починається з визначення множини основних об’єктів стеганографічного перетворення. Нехай C - цифрове зображення-контейнер, M - приховуване повідомлення, K - секретний ключ, E_K - функція симетричного шифрування, R - процедура корекційного кодування, P_K - псевдовипадкова перестановка позицій вбудовування, а S - сформований стегоконтейнер. У загальному вигляді процес можна подати як S = Embed(C, R(E_K(M)), P_K).

Науковий зміст такого подання полягає в тому, що захист забезпечується не окремою операцією вбудовування, а послідовним перетворенням повідомлення перед внесенням у контейнер. Шифрування усуває семантичні та статистичні ознаки відкритого тексту, корекційне кодування додає надлишковість для відновлення, а псевдовипадковий розподіл позицій зменшує передбачуваність розміщення бітів.

Модель пасивного порушника у запропонованому підході передбачає, що зловмисник має доступ до стегоконтейнера S і може виконувати візуальний, гістограмний, ентропійний, кореляційний та LSB-аналіз. При цьому він не володіє секретним ключем K і не знає конкретної перестановки P_K. Отже, задача захисту зводиться до мінімізації відмінностей між C і S за візуальними та статистичними показниками, а також до унеможливлення відновлення послідовного шаблону вбудовування.

Адаптивне симетричне шифрування в межах методу виконує дві функції. По-перше, воно захищає зміст повідомлення у випадку часткового вилучення бітової послідовності. По-друге, воно перетворює відкриті дані на псевдовипадкову послідовність, що не містить очевидних повторів. Для LSB-стеганографії це важливо, оскільки текстові або структуровані файли без попереднього шифрування можуть утворювати регулярні бітові патерни, помітні під час аналізу молодших бітів.

Псевдовипадковий вибір позицій вбудовування є другим ключовим елементом методу. На відміну від послідовного LSB-вбудовування, де бітова послідовність розміщується в пікселях у фіксованому порядку, запропонований підхід використовує ключову перестановку позицій. Це дозволяє розподілити зміни по контейнеру більш рівномірно та зменшити локальні статистичні аномалії, які можуть виникати при концентрації прихованих даних у певній ділянці зображення.

Динамічне корекційне кодування на основі кодів Ріда-Соломона застосовується для підвищення надійності відновлення повідомлення. Наукове значення цього елемента полягає у виборі кількості перевірочних символів не як сталої величини, а як параметра, що залежить від розміру зашифрованих даних і доступної місткості контейнера. Це дає змогу підтримувати баланс між непомітністю та стійкістю до пошкоджень.

Нехай |D| - розмір зашифрованих даних, Cap(C) - доступна місткість контейнера, e_min і e_max - мінімальна та максимальна кількість перевірочних символів. Тоді кількість корекційних символів може визначатися як e = min(e_max, max(e_min, floor(|D|/10), Cap(C) - |D|)). Така залежність дозволяє збільшувати надлишковість для більших повідомлень, але не перевищувати допустиму місткість контейнера.

У межах запропонованої моделі важливим є критерій збереження природних властивостей контейнера. Для оцінювання якості стегоконтейнера доцільно використовувати MSE, PSNR, SSIM, ентропію та аналіз гістограм. Проте ці показники необхідно розглядати комплексно: низьке значення MSE або високе значення PSNR підтверджує візуальну непомітність, але не гарантує відсутність статистичних ознак в LSB-площині.

Загальний алгоритм вдосконаленого методу можна подати як послідовність науково обґрунтованих етапів: нормалізація повідомлення, генерація випадкового вектора ініціалізації, симетричне шифрування, додавання корекційної надлишковості, генерація ключової перестановки позицій, LSB-вбудовування та формування стегоконтейнера. Зворотний процес передбачає вилучення бітів за тією самою перестановкою, корекційне декодування, розшифрування та перевірку цілісності отриманих даних.

Авторське значення запропонованого підходу полягає не у створенні нового криптографічного примітива, а в поєднанні відомих механізмів у єдину модель стеганографічного захисту, орієнтовану саме на протидію пасивному аналізу. Така постановка є більш науковою, оскільки акцент переноситься з опису інтерфейсу або програмних модулів на формалізацію процесу приховування, модель загроз і критерії стійкості.

Таблиця 1 - Узагальнення елементів вдосконаленого методу гібридної LSB-стеганографії

Елемент методу	Наукове призначення	Очікуваний ефект
Модель пасивного порушника	Врахування аналізу гістограм, LSB-площини, ентропії та кореляції	Формування вимог до статистичної непомітності стегоконтейнера
Адаптивне симетричне шифрування	Перетворення повідомлення на псевдовипадкову бітову послідовність	Зменшення регулярних патернів і захист змісту повідомлення
Псевдовипадкова перестановка позицій	Ключове розсіювання бітів по контейнеру	Зниження передбачуваності та локальних статистичних аномалій
Динамічне корекційне кодування	Адаптація надлишковості до обсягу даних і місткості контейнера	Підвищення ймовірності відновлення без надмірного збільшення помітності
Комплексне оцінювання	Використання MSE, PSNR, SSIM, ентропії та гістограм	Баланс між візуальною якістю, місткістю та стійкістю до пасивного аналізу

Отже, результати дослідження показують, що підвищення стійкості LSB-стеганографії до пасивних атак доцільно розглядати як багатокомпонентну задачу. Вона включає не лише зміну способу вбудовування, а й попередню криптографічну трансформацію повідомлення, адаптивне додавання надлишковості та контроль статистичної подібності між контейнером і стегоконтейнером. Саме таке поєднання дозволяє зменшити ймовірність виявлення прихованого каналу без повної відмови від переваг просторового LSB-підходу.

Висновки

У результаті дослідження обґрунтовано вдосконалений метод гібридної LSB-стеганографії, орієнтований на підвищення стійкості прихованої передачі даних до пасивного стегоаналізу. Запропонований підхід поєднує адаптивне симетричне шифрування, псевдовипадковий вибір позицій вбудовування та динамічне корекційне кодування.

Формалізована модель показує, що основна перевага методу полягає у зменшенні передбачуваності прихованої бітової послідовності та її розміщення в контейнері. Це ускладнює аналіз LSB-площини, гістограмний аналіз і пошук локальних статистичних відхилень.

Динамічне використання кодів Ріда-Соломона дозволяє підвищити надійність відновлення повідомлення після часткового пошкодження або обробки стегоконтейнера. При цьому кількість перевірочних символів має визначатися з урахуванням місткості контейнера, щоб не створювати надмірної статистичної помітності.

Запропонована модель не замінює базовий LSB-метод, а розвиває його шляхом додавання криптографічного, стохастичного та корекційного рівнів. Це робить підхід придатним для подальшого дослідження, експериментального порівняння з класичною LSB-стеганографією та використання в системах прихованого передавання конфіденційних даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Subramanian N., Elharrouss O., Al-Maadeed S., Bouridane A. Image Steganography: A Review of the Recent Advances. IEEE Access. 2021. Vol. 9. P. 23409-23423. DOI: 10.1109/ACCESS.2021.3053998.
2. Rustad S., Yudistira N., Sari Y. A., et al. Digital image steganography survey and investigation. Signal Processing. 2023. Vol. 206. Article 108908.
3. Apau R., Agyemang J. O., et al. Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. PLOS ONE. 2024. Vol. 19, No. 9. Article e0308807. DOI: 10.1371/journal.pone.0308807.
4. Kombrink M. H., Galli J. Image Steganography Approaches and Their Detection Strategies. ACM Computing Surveys. 2024. DOI: 10.1145/3694965.
5. Alanzy M. Image Steganography Using LSB and Hybrid Encryption Algorithms. Applied Sciences. 2023. Vol. 13, No. 21. Article 11771. DOI: 10.3390/app132111771.
6. Rahman S., Ahmad J., et al. A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image. Scientific Reports. 2023. Vol. 13. Article 14596. DOI: 10.1038/s41598-023-41303-1.
7. Radivilova T., Hassan H., et al. Image Steganography Method using LSB and AES Encryption. CEUR Workshop Proceedings. 2025. Vol. 4016.
8. Aljughaiman A., et al. Content-adaptive LSB steganography with saliency fusion, RS coding, and hybrid embedding. Scientific Reports. 2025. DOI: 10.1038/s41598-025-33920-9.
9. AFM Z. A., et al. Randomization Strategies in Image Steganography: Security Techniques and Comparative Analysis. Computers, Materials & Continua. 2024. DOI: 10.32604/cmc.2024.050834.

10. Raiyan S. R., Kabir M. H. SCReedSolo: A Secure and Robust LSB Image Steganography Framework with Randomized Symmetric Encryption and Reed-Solomon Coding. arXiv. 2025. DOI: 10.48550/arXiv.2503.12368.
11. Chi H., et al. A Simple and Efficient Data Hiding Method with Error Correction Based on Hamming Code. Electronics. 2024. Vol. 13, No. 11. Article 2018. DOI: 10.3390/electronics13112018.
12. National Institute of Standards and Technology. Advanced Encryption Standard (AES). FIPS 197, Update 1. Gaithersburg: NIST, 2023. DOI: 10.6028/NIST.FIPS.197-upd1.

Торохтій Віктор В. **-** студент групи 2КІТС-22б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, email: torohtijv3@gmail.com

Карпінець Василь Васильович **-** завідувач кафедри менеджменту та безпеки інформаційних систем, кандидат технічних наук, доцент, Вінницький національний технічний університет, м. Вінниця, email: karpinets@vntu.edu.ua

Torokhtii Viktor V. **-** student of group 2KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, email: torohtijv3@gmail.com

Karpinets Vasyl V. **-** Head of the Department of Management and Security of Information Systems, Candidate of Technical Sciences, Associate Professor, Vinnytsia National Technical University, Vinnytsia, email: karpinets@vntu.edu.ua