КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (31), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.31.963
УДК 004.056.53

Радівілова Тамара Анатоліївна
д.т.н., професор. професор кафедри інфокомунікаційної інженерії ім. В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID 0000-0001-5975-0269
tamara.radivilova@nure.ua

Чакрян Вадим Хазарович
к.т.н. старший викладач кафедри інфокомунікаційної інженерії ім. В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID 0000-0003-4827-9779
vadym.chakrian@nure.ua

Снігуров Аркадій Владиславович
к.т.н., доцент, декан факультету інфокомунікацій, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID 0000-0003-1355-7978
arkadii.snihurov@nure.ua

Добринін Ігор Станіславович
к.т.н., доцент, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID 0000-0001-8910-2609
ihor.dobrynin@nure.ua

Агеєв Дмитро Володимирович
д.т.н., професор. професор кафедри інфокомунікаційної інженерії ім. В.В. Поповського
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID 0000-0002-2686-3854
dmytro.aheiev@nure.ua

Пшеничних Сергій Васильович
к.т.н., доцент, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID 0000-0003-0533-2306
serhii.pshenychnykh@nure.ua

Штангей Світлана Вікторівна
к.т.н., доцент, доцент кафедри інфокомунікаційної інженерії ім. В.В. Поповського,
Харківський національний університет радіоелектроніки, Харків, Україна
ORCID ID 0000-0002-9200-3959
svitlana.shtanhei@nure.ua

МЕТОД ПРИХОВУВАННЯ ІНФОРМАЦІЇ ЗА ДОПОМОГОЮ АЛГОРИТМУ ШИФРУВАННЯ AES ТА СТЕГАНОГРАФІЧНОГО МЕТОДУ LSB ІЗ ЗАХИСТОМ ВІД ОБРІЗАННЯ ТА СТЕГОАНАЛІЗУ

Анотація. В епоху стрімкого зростання обсягів цифрової інформації, забезпечення її захищеної передачі є критичним завданням. Поєднання стенографії та шифрування створює потужний дворівневий механізм безпеки, який одночасно шифрує дані та приховує їх передачу. В роботі запропоновано метод, який реалізує дворівневий захист. Секретне повідомлення спочатку шифрується за допомогою надійного алгоритму AES з ключем 256 біт. Це перетворює вихідний текст на псевдовипадкову послідовність бітів, що ускладнює статистичний аналіз. Далі зашифровані дані вбудовуються у 24-бітне кольорове зображення-

© Т.А. Радівілова, В.Х. Чакрян, А.В. Снігуров, І.С. Добринін, Д.В. Агеєв, С.В. Пшеничних, С.В. Штангей, 2025

контейнер з використанням модифікованого методу LSB. Новизна підходу полягає в таких вдосконаленнях: в один піксель зображення вбудовується один повний байт повідомлення, біти якого розподіляються по RGB каналах, що забезпечує ємність; . пікселі, обираються у псевдовипадковому порядку за допомогою генератора псевдовипадкових чисел (PRNG), для додаткового маскування застосовується другий PRNG, що надає додатковий захист від стегоаналізу; Початок вбудовування повідомлення зміщується від початку файлу на основі розмірів зображення, що захищає дані при частковому обрізанні стегоконтейнера. Для оцінки ефективності роботи розробленого методу були обрані стандартні метрики: пікове відношення сигнал-шум (PSNR), індекс структурної подібності (SSIM) та нормалізована взаємна кореляція (NCC). Експериментальний аналіз показав, що запропонований метод забезпечує високу якість стегозображень. Навіть при максимальному заповненні контейнера (262 144 байти) показник PSNR залишався на високому рівні (56.67–56.76 дБ), а метрики SSIM та NCC були дуже близькі до 1, що свідчить про мінімальні візуальні спотворення. Візуально відрізнити оригінальне зображення від стегоконтейнера неможливо. Порівняльний аналіз з іншими відомими методами (для 100 000 байтів) показав, що запропонований алгоритм має вищі показники PSNR (70.01–70.07 дБ), що підтверджує його ефективність. Використання подвійного PRNG та вбудовування по одному байту на піксель забезпечує як високу безпеку, так і значну пропускну здатність. Розроблений гібридний метод, що поєднує шифрування AES-256 та модифіковану LSB-стеганографію з псевдовипадковим вибором пікселів і бітів, є ефективним рішенням для прихованої передачі великих обсягів даних. Метод забезпечує високий рівень безпеки, стійкість до стегоаналізу та візуальну непомітність вбудованих даних, що підтверджується високими значеннями метрик PSNR, SSIM та NCC.

Ключові слова: стеганографія, криптографія, AES, LSB, приховування, дані, контейнер, зображення, безпека, шифрування.

ВСТУП

Зі зростанням обсягів цифрової інформації та необхідністю її захисту, методи криптографії та стеганографії набувають ключового значення. Криптографія (шифрування) забезпечує конфіденційність даних, роблячи їх незрозумілими для сторонніх осіб. Стеганографія забезпечує прихованість самого факту передачі повідомлення, вбудовуючи його у нешкідливий на вигляд об'єкт-контейнер (наприклад, зображення, аудіо- чи відеофайл). Комбінація цих двох підходів створює потужний інструмент, завдяки якому зашифровані дані приховуються, що ускладнює їх виявлення та дешифрування [1, 2].

В криптографії для забезпечення конфіденційності даних використовують математичні перетворення, завдяки яким дані приймають заплутану форму [1]. В стеганографії секретні повідомлення вбудовуються в зображення або в мультимедійні файли при їх невидимої передачі відкритими каналами зв’язку [3]. Стеганографія приховує як конфіденційні дані, так і зв'язок між відправником та одержувачем, тоді як криптографія приховує конфіденційні дані і використовується для ідентифікації відправника та одержувача [4, 5]. Ефективним та одним із найпопулярніших підходів є поєднання криптографічних та стеганографічних методів захисту інформації від несанкціонованого доступу [6, 7].

Останні дослідження свідчать про значний інтерес до поєднанні стеганографії та криптографії [8]. Багато наукових робіт присвячено поєднанню криптографічного методу AES та стеганографічного методу LSB [9, 10], так як вони є найшвидшими та мають низький рівень спотворення. Для максимізації ємності вбудовування при збереженні непомітності автори робіт [11, 12] пропонують підхід, в якому шифрований на основі AES текст розподіляється і вбудовується за допомогою методу LSB у всі три

канали кольорів RGB (червоний, зелений і синій) зображення обкладинки. А у дослідженні [13] для максимізації ємності застосовується метод адаптивної заміни LSB, де аналізується значення пікселів і складність різних областей зображення. Потім визначається оптимальна кількість LSB, які слід використовувати для вбудовування.

Однак подальші дослідження послідовно впроваджували додаткові рівні складності та техніки доповнення. В роботі [14] автори запропонували гібридну схему, яка складається з AES, обміну ключами на основі еліптичної кривої Діффі Хеллмана, LSB. Інші підходи передбачають динамічну заміну LSB, наприклад вбудовування в 2-й або 3-й LSB на додаток до 1-го, на основі певних критеріїв пікселів зображення-покриття, як наприклад в роботі [15]. Тут замість використання фіксованого 1-бітного LSB, цей адаптивний метод вбудовує різну кількість бітів (наприклад, від 1 до 4) у різні пікселі. Цей підхід базується на характеристиках зображення-покриття, що дозволяє збалансувати високу ємність вбудовування з мінімальним візуальним спотворенням.

Дослідники пішли далі простої заміни LSB, запропонувавши модифікації для підвищення безпеки. Наприклад, деякі моделі впроваджують випадковий або не послідовний шаблон вбудовування LSB. Автори роботи [16] удосконалили криптографічні процедури та рандомізовані солі, щоб зробити дані більш прихованими та захищеними від третіх осіб, та використовували блоки еліптичних кривиз з відповідною прокладкою, щоб захистити дані під час передачі та унеможливити їхню втрату. У статті [17] запропоновано алгоритм, що базується на гібридній одномірній хаотичній карті в поєднанні з двомірною композитною хаотичною картою для створення початкового вектора позиції вбедовування, в парі з методами оптимізації, для оптимізації випадкових місць вбудовування, та найменш значущих бітів (LSB). В роботі [18] автори пропонують на основі генератора псевдовипадкових чисел (PRNG) для вибору випадкових пікселів та для вибору випадкового бітового положення в значеннях R, G і B пікселя для вбудовування одного байта інформації. У статті [19] пропонується нова гібридна техніка приховування даних, яка використовує мозаїчні зображення як шум. Секретні дані спочатку шифруються за допомогою AES, потім цей шифрований текст приховується за допомогою заміни LSB, але в межах численних невеликих плиток, що складають мозаїку. Використання мозаїчних зображень забезпечує природно складний і «шумний» носій, що підвищує безпеку прихованих даних і потенційно може забезпечити вищу ємність вбудовування порівняно зі стандартними зображеннями. В роботі [20] запропоновано алгоритм стеганографії на основі зображень, який поєднує заміну LSB з магічною матрицею, багаторівневим алгоритмом шифрування (MLEA), секретним ключем (SK) та транспозицією, перевертанням для зашумлення даних.

Також дослідники для захисту від підміни вбудованого повідомлення запровадили моделі, які орієнтовані на цілісність. У роботі [21] побудовано модель, яка після шифруваання інтегрує коди виправлення помилок (ECC) перед вбудовуванням даних за допомогою LSB. У статті [22] генерується хеш-код автентифікації повідомлення (HMAC), у роботі [23] дані шифруються на основі AES, а ключ AES шифрується RSA, у роботі [24] використовувати шифрування на основі AES і Blowfish, у роботі [25] шифрований текст алгоритмічно кодується в синтетичну послідовність ДНК і після цього вбудовується в зображення на основі LSB.

Незважаючи на популярність комбінування алгоритмів AES (для шифрування) та LSB (для вбудовування) , залишається актуальною проблема підвищення стійкості таких систем до стегоаналізу та атак, як-от обрізання зображення, а також оптимізації балансу між обсягом прихованих даних та візуальною якістю контейнера.

Мета дослідження: розробка та аналіз вдосконаленого методу приховування даних, що базується на інтеграції криптографічного алгоритму AES та стеганографічного методу LSB, для забезпечення високого рівня конфіденційності, цілісності та непомітності передачі інформації. Для досягнення поставленої мети потрібно вирішити наступні задачі:

- розробити рішення для шифрування прихованого повідомлення за допомогою Advanced Encryption Standard (AES), інтегрувати його зі стеганографією на основі Least Significant Bits (LSB), з метою захисту вмісту секретного повідомлення від розкриття;
- забезпечити захист від обрізання зображення, щоб не втратити вбудоване повідомлення;
- модифікувати алгоритм для зашумлення простору, який не використовується у зображенні, у спектрі невидимому для зору задля складності виявлення стегоконтейнера;
- зробити метод стійким до стеганографічних та візуальниз атак, які можуть призвести до виявлення прихованого повідомлення;
- мінімізувати візуальні спотворення в стеганозображенні при максимізації довжини повідомлення.

Ці завдання спрямовані на створення методу стеганографічного захисту інформації, в якому повідомлення буде надійно приховане маючи щирокий діапазон довжини, захищене від обрізання, від стеганографічних та візуальних атак.

МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ

Алгоритм шифрування AES та стеганографічний метод заміни найменш значущого біта LSB.

Advanced Encryption Standard (AES) – це стандарт симетричного блочного шифрування, затверджений NIST, в основі якого лежить алгоритм Rijndael – симетричний алгоритм блочного шифрування. Він використовує ключі довжиною 128, 192 або 256 біт і оперує блоками даних розміром 128 біт. Завдяки високій швидкості та доведеній криптостійкості, AES є світовим стандартом для захисту даних. Використання AES гарантує, що навіть у разі виявлення прихованого повідомлення, його розшифрування без відповідного ключа буде практично неможливим.

Стеганографічний метод заміни найменш значущого біта LSB. Метод Least Significant Bit (LSB, найменш значущий біт) є одним з найпоширеніших методів стеганографії. Він полягає у заміні найменш значущих бітів пікселів зображення-контейнера на біти повідомлення, яке необхідно приховати.

У кольоровому 24-бітному зображенні, де кожен піксель представлений трьома байтами (R, G, B), заміна останнього біта в кожному байті призводить до мінімальних, візуально непомітних змін кольору пікселя. Це забезпечує високу непомітність вбудовування.

Для аналізу стеганографічних алгоритмів використовують набір характеристик [25], зокрема:

- пропускна здатність – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в зображенні фіксованого розміру;
- стійкість – здатність вилучити приховану інформацію після загальних операцій з обробки зображень;

- невидимість – прозорість на рівні сприйняття людиною;
- захищеність – вбудована інформація не може бути видалена цілеспрямованими атаками, основаними на відомому алгоритмі вбудовування та вилучення, і знанні принаймні одного носія з прихованим повідомленням;
- кількість вбудовуваної інформації – кількість інформації, яку можна вбудувати в контейнер;
- складність вбудовування і виявлення – кількість стандартних операцій, які будуть виконані для вбудовування і виявлення прихованого повідомлення.

За більшістю вищенаведених характеристик метод LSB є найпоширенішим серед методів заміни в просторовій області. Застосування стеганографічного методу LSB в середньому вимагає, щоб тільки половина біт зображення-контейнера були змінені.

Пропускна здатність методу дорівнює 1/8 розміру контейнера або ж розміром в 1/4 контейнера (відповідно при використанні 2 останніх бітів в байтах), якщо відкинути в розрахунках службову інформацію на початку файлу, яка є незначною щодо розміру зображення.

Інтегрований метод приховування інформації шляхом поєднання алгоритму шифрування AES та стеганографічного методу LSB.

Інтегрований метод, що поєднує AES і LSB, виконується в три основні етапи:

1. Шифрування повідомлення.

Перед вбудовуванням, вихідне повідомлення (текст, файл) шифрується за допомогою алгоритму AES з використанням обраного секретного ключа.

Результатом є потік псевдовипадкових бітів, який має вигляд шуму і не має статистичних ознак вихідного повідомлення. Це ускладнює не лише дешифрування, але й стеганоаналіз (аналіз на наявність прихованого повідомлення), оскільки властивості зашифрованих даних краще відповідають шуму, що є бажаним для LSB.

2. Вибір та підготовка контейнера.

Як контейнер зазвичай обирається некомпресоване або безвтратно стиснене зображення (наприклад, PNG), оскільки стиснення із втратами (наприклад, JPEG) може порушити вбудовані LSB біти. Визначається максимально можливий обсяг даних для вбудовування, який залежить від розміру контейнера. Наприклад, у 24-бітному зображенні 1/8 загального розміру файлу може бути використана для приховування, якщо замінюється один LSB на кожен колірний канал.

3. Вбудовування (стеганографічний процес).

Зашифроване повідомлення (біт за бітом) вбудовується в найменш значущі біти обраних пікселів зображення-контейнера, починаючи з певної початкової позиції, відомої тільки відправнику та отримувачу. До зашифрованого повідомлення зазвичай додається заголовок (метадані), що містить інформацію про довжину повідомлення, що дозволяє отримувачу коректно витягнути дані.

Отримане зображення називається стего-зображенням і візуально не відрізняється від оригіналу.

В роботі [12] для покращення показників характеристик стеганографічного алгоритму LSB було вбудовано модуль симетричного шифрування інформації AES для захищеності; розроблено алгоритм з подвійною та потрійною місткістю відносно стандартних показників, що поліпшує показник пропускної здатності.

І цій роботі стоїть задача модифікувати алгоритм для зашумлення простору, який не використовується у зображенні, у спектрі невидимому для зору задля складності виявлення стегоконтейнера.

Модифікований алгоритм включає в себе окрім вищезазначених етапів ще додаткові етапи:

– шифрування повідомлення (в роботі використовується алгоритм шифрування з довжиною ключа 256 біт);
– зміну алгоритму пошуку кінця повідомлення (замість пошуку в циклі побітового декодування): виділяються останні біти кожного каналу усього зображення та довжина повідомлення за допомогою бінарного пошуку по всій строчці входження маркеру;
– здвиг повідомлення від початку стеганоконтейнера заснований на визначенні широти та довжини зображення для захисту від атаки обрізання (алгоритм сам визначає початок і кінець зашифрованого повідомлення, а приймаючій стороні невідомо про відсоток здвигу);
– вибір молодших бітів для приховування є псевдовипадковим і проводиться розсіювання повідомлення по всій довжині контейнера, що унеможливлює стеганографічний аналіз.

Загальна схема роботи модифікованого алгоритму показана на рисунку 1.

У цьому розділі приводяться концепції, підходи, принципи, методи та інші положення, на яких безпосередньо базується дослідження. Зазначаються основні терміни, поняття та категорії, що лежать в основі дослідження.

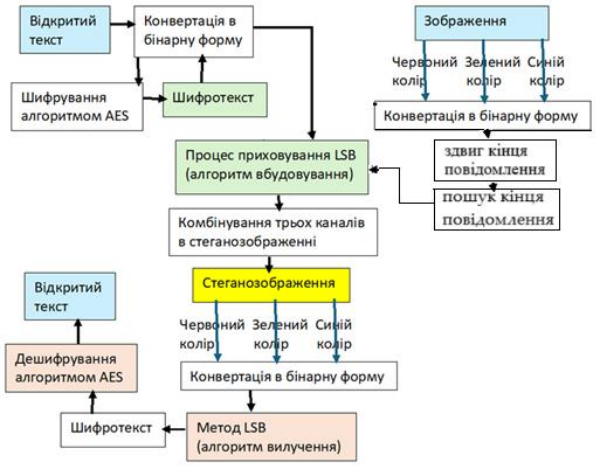

Рис. 1. Загальна схема роботи стеганографічного алгоритму LSB поєднаного із алгоритмом шифрування AES

В даній роботі використовується модифікація алгоритму з кодуванням інформації в молодші біти, які обираються псевдовипадковим чином і проводиться розсіювання повідомлення по всій довжині контейнера [12, 18] для надійного приховування великого обсягу даних у 24-бітовому кольоровому зображенні. Це досягається шляхом вбудовування одного байта секретного повідомлення в кожен піксель «обкладинки» зображення, використовуючи комбінацію випадкового вибору пікселів і маніпуляцій на рівні бітів для забезпечення безпеки.

Алгоритм побудований на двох основних підходах:

1. **Висока ємність:** вбудовування одного повного 8-бітного байту повідомлення в один піксель RGB каналів, розділяючи байт повідомлення на три групи і приховуючи їх у відповідних колірних каналах: 3 біти надходять у червоний канал, 3 біти надходять у

зелений канал, 2 біти потрапляють у синій канал. Це дозволяє розміру повідомлення досягати 33,33% від розміру зображення-покриття (наприклад, зображення розміром 512x512 пікселів може приховати 262 144 байти).

2. **Безпека (подвійний Pseudo Random Number Generator PRNG):** Безпека досягається за допомогою генератора псевдовипадкових чисел (PRNG) на двох різних етапах. PRNG генерує послідовність чисел, яка здається випадковою, але визначається початковим значенням. Щоб декодувати повідомлення, необхідно мати те саме початкове значення.

–**PRNG 1 (вибір пікселів):** Вибирає пікселі у випадковому, неповторному порядку для вбудовування байтів повідомлення. Це запобігає послідовному зберіганню повідомлення, що ускладнює його виявлення.

–**PRNG 2 (заплутування бітів):** додає рівень шифрування, використовуючи випадковий біт з самого пікселя, щоб замаскувати біт повідомлення перед вбудовуванням.

Покроковий алгоритм вбудовування одного байту секретного повідомлення у випадково обраний піксель. Цей процес повторюється для кожного байта в повідомленні.

1. **Обирається піксель:** Використовується не повторюваний PRNG, щоб вибрати випадковий піксель з «обкладинки»-зображення, який ще не використовувався.

2. **Розділяється байт повідомлення:** береться 8-бітний байт повідомлення і роздяється на три групи: b_1, b_2, b_3 (для червоного), b_4, b_5, b_6 (для зеленого) і b_7, b_8 (для синього).

3. **Вбудується в червоний канал (3 біти):**

–Щоб вбудувати перший біт повідомлення (b_1):

- Використовується PRNG, щоб випадково вибрати один з 5 найважливіших бітів оригінального червоного значення пікселя.
- Виконується операція XOR: результат = (вибраний найважливіший біт) XOR
- Замінюється 3-й найменш значущий біт (LSB) значення червоного кольору цим результатом.

–Повтор цього процесу для другого біта повідомлення (b_2), розмістивши результат у 2-му LSB, і для третього біта повідомлення (b_3), розмістивши результат у 1-му LSB.

4. **Вбудовування в зелений канал (3 біти):**

–Виконується та сама процедура, що й у кроці 3, але використовуються біти зеленого каналу та друга група бітів повідомлення (b_4, b_5, b_6).

5. **Вбудвування в синій канал (2 біти):**

–Те ж саме, але тільки для двох бітів.

–Щоб вбудувати сьомий біт повідомлення (b_7):

- Використовується PRNG, щоб випадково вибрати один з 5 найважливіших бітів синього значення.
- Обчислюється результат = (вибраний найважливіший біт) XOR (b_7).
- Замінюється 2-й LSB синього значення цим результатом.

–Повторюється для останнього біта повідомлення (b_8), розмістивши результат у 1-му LSB.

Після цих кроків один байт повідомлення надійно прихований в одному пікселі. Потім алгоритм переходить до наступного байта повідомлення і процес повторюється, поки не буде вбудовано все повідомлення, створюючи остаточне стего-зображення.

ОЦІНКА ЯКОСТІ СТЕГАНОСИСТЕМИ

Для проведення порівняльного аналізу стеганографічних алгоритмів було обрано такі основні та найчастіше використовувані показники якості: Peak Signal-to-Noise Ratio

Формула для розрахунку **Peak Signal-to-Noise Ratio (PSNR)**, або пікового відношення сигнал-шум:

$$PSNR = 10 * log_{10}\left(\frac{MAX_I^2}{MSE}\right), \quad (1)$$

де *MSE* – це **Mean Squared Error** (середньоквадратична похибка) між оригінальним і зміненим зображеннями (stegoimage).

MAX_I – це максимальне можливе значення яскравості (інтенсивності) пікселя (для 8-бітових зображень MAX_I=255, а для 10-бітових – MAX_I=1023.

$$MSE = \frac{1}{m \cdot n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[C(x,y) - S(x,y)]^2, \quad (2)$$

де m – кількість рядків (висота) зображення; n – кількість стовпців (ширина) зображення; *C(x,y)* – значення пікселя в оригінальному зображенні за координатами *(x,y);*

Високе значення PSNR вказує на те, що змінене зображення дуже схоже на оригінальне, тобто рівень "шуму" (змін) низький.

або індекс структурної подібності, є більш складним порівняно з PSNR, оскільки він враховує три ключові компоненти, що відповідають особливостям людського зору: яскравість, контраст і структуру.

SSIM-індекс для двох зображень (або вікон) x та y обчислюється як добуток трьох компонентів:

$$SSIM(c,s) = [l(o,p)]^{\alpha} \cdot [c(o,p)]^{\beta} \cdot [s(o,p)]^{\gamma}, \quad (3)$$

де $l(o,p) = \frac{2\mu_o\mu_p + const_1}{\mu_o^2 + \mu_p^2 + const_1}$ – компонент яскравості (luminance), μ_o та μ_p – середні значення інтенсивності пікселів у вікнах o та p; $c(o,p) = \frac{2\sigma_o\sigma_p + const_2}{\sigma_o^2 + \sigma_p^2 + const_2}$ – компонент контрасту (contrast), σ_o та σ_p – стандартні відхилення інтенсивності пікселів (вимірювання контрасту) у вікнах o та p; $s(o,p) = \frac{\sigma_{op} + const_3}{\sigma_o\sigma_p + const_3}$ – компонент структури σ_{op} – коваріація між пікселями вікон *o* та *p* (вимірювання структурної подібності); α,β,γ – коефіцієнти, що визначають важливість кожного компонента (зазвичай їх значення дорівнюють 1); *const₁, const₂, const₃* – невеликі константи, які додаються для уникнення ділення на нуль, коли знаменники близькі до нуля. Їх значення розраховуються за формулами *t1=(K1,MAXI)2, const2=(K2,MAXI)2*, де K – константи (зазвичай K_1=0.01, K_2=0.03).

або нормалізована взаємна кореляція, – це метрика, яка використовується в стеганографії для оцінки подібності між двома зображеннями. У контексті стеганографії, NCC допомагає визначити, наскільки стеганозображення (зображення з прихованими даними) схоже на оригінальне зображення-контейнер. На відміну від метрик, таких як PSNR або MSE, які фокусуються на різниці на рівні пікселів, NCC вимірює ступінь лінійної залежності між двома зображеннями.

Формула для NCC виглядає так:

$$NCC = \frac{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}(C(x,y)-\overline{C})(S(x,y)-\overline{S})}{\sqrt{\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}(C(x,y)-\overline{C})^2 \sum_{x=0}^{m-1}\sum_{y=0}^{n-1}(S(x,y)-\overline{S})^2}}, \quad (3)$$

де *C(x,y)* – значення пікселя в оригінальному зображенні; *S(x,y)* – значення пікселя в стеганозображенні; $\overline{C}$ та $\overline{S}$ – середні значення інтенсивності пікселів в оригінальному та стеганозображенні відповідно; m і n – розміри зображення (висота і ширина).

Значення NCC знаходиться в діапазоні від -1 до 1. Значення NCC, близьке до 1, свідчить про дуже високу схожість між зображеннями. Це означає, що стеганозображення має майже ідентичну структуру та розподіл інтенсивності пікселів, що і оригінальне. Високе значення NCC (наприклад, понад 0,99) є позитивним показником для стеганографічного алгоритму, оскільки він демонструє, що вбудовування даних не суттєво змінило загальну структуру зображення, що робить приховані дані важкими для виявлення.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Мета експериментів полягала в аналізі ефективності запропонованого методу стеганографії . Набір даних для передачі секретного повідомлення складався з текстового файлу (.txt). Експеримент проводився на комп'ютері, оснащеному процесором Intel(R) Core(TM) i9-13900HX з тактовою частотою 5,40 GHz, 32,0 ГБ оперативної пам'яті та 64-розрядною операційною системою Windows 11.

В роботі реалізовано та проведено аналіз стеганографічного алгоритму LSB з шифруванням AES з довжиною ключа 256 бітів, який включає в себе модифікацію алгоритму з кодуванням інформації в молодші біти, які обираються псевдовипадковим чином і проводиться розсіювання повідомлення по всій довжині контейнера.

Для цього було взято два зображення розміром 512*512 = 262144 пікселів, які наведено на рисунку 2 та проведено аналіз роботи стеганографічних методів. Було обрано різну довжину вбудовуваних даних: від 1000 до 262144 байтів. Кожен байта секретного повідомлення вбудовувався в кожен піксель «обкладинки» зображення, використовуючи комбінацію випадкового вибору пікселів і маніпуляцій на рівні бітів для забезпечення безпеки модифікованого алгоритму, який описано вище.

Рис. 2. Зображення використовувані в експерименті для аналізу стеганографічних алгоритмів

Для розуміння обсягу викривлень, які вносяться в зображення, необхідно порівняти метрики для різних обсягів вбудованих даних. Дослідження проведено на двох зображеннях розміром 512*512 пікселів. В якості типових розмірів даних для

вбудовування були взяті різні значення вбудовуваних даних від 1000 до 262144 байтів. місткості символів

Значення показників спотворення стегоконтейнера для двох зображень і різної довжини даних наведено в таблиці 1.

Таблиця 1

Значення показників спотворення стегоконтейнера для двох зображень і різної довжини даних

	Показники спотворення	Довжина вбудовуваного повідомлення					
кіт							
зелень							

Очевидно, що збільшення обсягу даних для вбудовування в контейнер негативно впливає на статистику відображення, але даний вплив не знижує метрику нормальних показників, які є достатніми для стеганографії.

Через випадковість у виборі пікселів та бітів, неавторизований користувач не може отримати повідомлення, навіть якщо він виявив наявність секретного повідомлення на зображенні. Крім того, для підвищення безпеки в запропонованому методі застосовується шифрування повідомлення алгоритмом AES та вбудовування одного байта секретного повідомлення в кожен піксель «обкладинки» зображення, використовуючи комбінацію випадкового вибору пікселів і маніпуляцій на рівні бітів для забезпечення безпеки.

У таблиці 2 наведено порівняльну характеристику показника спотворення стеганоконтейнера PSNR запропонованого методу та існуючих методів стеганографії в комбінації із шифруванням повідомлення.

Таблиця 2

Значення показника спотворення стеганоконтейнера PSNR для існуючих алгоритмів та запропонованого для вбудовування 100000 байтів

	[17]	[11]	[20]	[18]	Запропонований алгоритм
Кіт					
зелень					

Результати аналізу демонструють вищу якість запропонованого алгоритму в порівнянні з існуючими стратегіями. Важливим аспектом, який слід враховувати, є визначення оптимального розміру бітів повідомлення, вбудованих в зображення певного розміру, для забезпечення ефективної стеганографії. Отже, перед вбудовуванням секретного повідомлення в зображення важливо обчислити пікселі повідомлення та зображення, щоб визначити найкращий розмір і формат зображень для даного розміру текста.

Результати запропонованого нами методу були кращими, ніж результати методів, описаних у [11, 17, 18, 20]. Згідно з таблицею 2, запропонований метод має відносно

високу здатність до приховування порівняно з існуючими методами, з нормальним PSNR. Це досягається за рахунок вбудовування одного байта секретного повідомлення в кожен піксель «обкладинки» зображення, використовуючи комбінацію випадкового вибору пікселів і маніпуляцій на рівні бітів для забезпечення безпеки.

Спираючись на отримані результати, можна прийти до висновку, що найкращі значення показників якості мають алгоритми, де кодування інформації відбувалося в бітах каналів стеганоконтейнера, які обирались псевдовипадковим чином.

Нормована середня абсолютна різниця, яка вказує ступінь відмінності між вихідним контейнером і контейнером з вбудованим секретним файлом передбачувано росте зі збільшенням довжини повідомлення, проте зростання не є істотним. Якість зображення відхиляється від 1 в середньому на 0,025%. Візуально зміни в контейнерах неможливо помітити ні в запропонованій реалізації ні в реалізаціяї інщих авторів,, які були проаналізовані.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В роботі надано варіант вирішення актуальної проблеми підвищення стійкості стегосистем до стегоаналізу та атак, а також показники ефективності стеганографії, щодо обсягу прихованих даних та візуальною якістю контейнера. В роботі запропоновано вдосконалений метод приховування даних, що базується на інтеграції криптографічного алгоритму AES з ключем 256 біт та стеганографічного методу LSB, для забезпечення високого рівня конфіденційності, цілісності та непомітності передачі інформації. На основі алгоритма LSB зашифровані дані вбудовуються у 24-бітне кольорове зображення-контейнер: в один піксель зображення вбудовується 8 біт повідомлення. Біти розподіляються по каналах: 3 біти в червоний, 3 біти в зелений та 2 біти в синій. Для вбудовування використовуються не послідовні пікселі, а пікселі, обрані у псевдовипадковому порядку за допомогою генератора псевдовипадкових чисел (PRNG). Це розподіляє повідомлення по всьому контейнеру, унеможливлюючи просте виявлення. Для додаткового маскування та заплутування застосовується другий PRNG. Перед вбудовуванням біти повідомлення проходять операцію XOR з псевдовипадково обраними старшими бітами самого пікселя-контейнера. Для забезпечення захисту від обрізання початок вбудовування повідомлення зміщується від початку файлу на основі розмірів зображення, що захищає дані при частковому обрізанні стегоконтейнера.

Для оцінки ефективності роботи запропонованого методу обрані стандартні метрики: пікове відношення сигнал-шум (PSNR), індекс структурної подібності (SSIM) та нормалізована взаємна кореляція (NCC). Експерименти проводились на зображеннях розміром 512x512 пікселів, в які вбудовувалися дані обсягом від 1000 до 262144 байтів (максимальна ємність). Експерименти показали, що запропонований метод забезпечує високу якість стегозображень. Навіть при максимальному заповненні контейнера (262144 байти) показник PSNR залишався на високому рівні (56.67–56.76 дБ), а метрики SSIM та NCC були дуже близькі до 1, що свідчить про мінімальні візуальні спотворення. Візуально відрізнити оригінальне зображення від стегоконтейнера неможливо. Порівняльний аналіз з іншими відомими методами (для 100 000 байтів) показав, що запропонований алгоритм має вищі показники PSNR (70,01–70,07 дБ), що підтверджує його ефективність. Використання подвійного PRNG та вбудовування по одному байту на піксель забезпечує як високу безпеку, так і значну пропускну здатність. Таким чином запропонований гібридний метод, що поєднує шифрування AES-256 та модифіковану

LSB-стеганографію з псевдовипадковим вибором пікселів і бітів, є ефективним рішенням для прихованої передачі великих обсягів даних. Метод забезпечує високий рівень безпеки, стійкість до стегоаналізу та візуальну непомітність вбудованих даних, що підтверджується високими значеннями метрик PSNR, SSIM та NCC.

В подальшому перспективним напрямом дослідження є проведення стегоаналізу запропонованого методу, включаючи R/S аналіз. Також необхідно створити програмну реалізацію стегосистеми, яка автоматично конвертує зображення в необхідний формат та необхідного розміру в залежності від довжини секретного повідомлення. Також необхідно зробити аналіз

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018, May). Decrypting SSL/TLS traffic for hidden threats detection. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 143-146). IEEE. doi: 10.1109/DESSERT.2018.8409116.
2. Радівілова, Т., Добринін, І., Пантєлєєв, В., Фісенко, Д., Мазепа, А., & Білодід, В. (2025). Аналіз методів прогнозування внутрішніх загроз на основі аналізу даних соціальної мережі twitter. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, *4*(28), 478–489. https://doi.org/10.28925/2663-4023.2025.28.818
3. Ivanisenko, I., Kirichenko, L., & Radivilova, T. (2016, August). Investigation of multifractal properties of additive data stream. In *2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP)* (pp. 305-308). IEEE. doi: 10.1109/DSMP.2016.7583564.
4. Радівілова, Т., Кіріченко, Л., Пантєлєєв, В., Мазепа, А., & Білодід, В. (2024). Аналіз методів автентифікації для вебзастосунків та реалізація вебзастосунку з інтегрованою системою автентифікації. *Сучасний стан наукових досліджень та технологій в промисловості*, (3 (29)), 76-90. doi: https://doi.org/10.30837/2522-9818.2024.3.076
5. Alghawli, A. S. A., & Radivilova, T. (2024). Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation. *Alexandria Engineering Journal*, *107*, 136-149. doi:10.1016/j.aej.2024.07.036
6. Nasution, R. I. H., Fauzi, A., & Khair, H. (2023). Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image. *Journal of Artificial Intelligence and Engineering Applications (JAIEA)*, *2*(3), 89-98. doi: 10.59934/jaiea.v2i3.201
7. Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. *Applied Sciences*, *13*(21), 11771. doi: 10.3390/app132111771
8. Talasila, S., Vijaya Kumar, G., Vijaya Babu, E., Nainika, K., Veda Sahithi, M., & Mohan, P. (2023, June). The hybrid model of lsb—technique in image steganography using aes and rsa algorithms. In *International Conference on Soft Computing and Signal Processing* (pp. 403-413). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-99-8451-0_34
9. Gupta, A., Ali, A., Pandey, A. K., Gupta, A. K., & Tripathi, A. (2022, November). Metamorphic cryptography using AES and LSB method. In *2022 International Conference on Advances in Computing, Communication and Materials (ICACCM)* (pp. 1-8). IEEE. doi: 10.1109/ICACCM56405.2022.10009381.
10. Gopika, R., A., Ganesh, R. S. (2025). Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: A robust data security framework. *Expert Systems with Applications*, 279, 127403. doi: 10.1016/j.eswa.2025.127403.
11. Raiyan, S. R., & Kabir, M. H. (2025). SCReedSolo: A Secure and Robust LSB Image Steganography Framework with Randomized Symmetric Encryption and Reed-Solomon Coding. *arXiv preprint arXiv:2503.12368*.
12. Radivilova, T., Dobrynin, I., Snihurov, A., Stanhei, S., & Bulba, S. (2025). Image Steganography Method using LSB and AES Encryption Algorithm. In 2025 Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography 2025 (CQPC 2025), 4016, (pp.32-44). Ceur.
13. Apau, R., Twum, F., Asante, M., & Hayfron-Acquah, J. B. (2024, February). A Secure and High Embedding Capacity Image Steganography Scheme Using Image Enhancement Technique, Compression,

and Genetic Algorithm. In *International Congress on Information and Communication Technology* (pp. 307-325). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-97-5441-0_27

14. Malik, C., Jha, M., Jha, M., & Bansal, A. (2024, June). A Novel Approach for Image Steganography and Cryptography Using Genetic Algorithm. In *International Conference on Data Analytics & Management* (pp. 77-90). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-96-3372-2_6.
15. Reddy, K. K., Kumar, N. V., Sajan, L., Teja, M. P., & Kumar, V. P. (2023, December). Enhancing Steganography Security: A Dual Layer Approach with LSB and AES Algorithm. In International Conference on Advances in Computational Intelligence and Informatics (pp. 321-327). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-97-4727-6_32.
16. Kumar, N., Soni, M. (2025). Randomized salt LSB: a novel approach to steganography with improved concealment and robustness. *Int. j. inf. tecnol.*, **17**, 4401–4414. doi: 10.1007/s41870-025-02501-4.
17. Khalil, N., Sarhan, A., Alshewimy, M. A.M. (2024) A secure image steganography based on LSB technique and 2D chaotic maps. *Computers and Electrical Engineering*, 119(B), 109566. doi: 10.1016/j.compeleceng.2024.109566.
18. Ehsan Ali, U. A., Ali, E., Sohrawordi, M., & Sultan, M. N. (2021). A LSB based image steganography u
19. Roy, S., Islam, M.M. (2022). A Hybrid Secured Approach Combining LSB Steganography and AES Using Mosaic Images for Ensuring Data Security. *SN COMPUT. SCI.* **3**, 153. doi: 10.1007/s42979-022-01046-8.
20. Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., Díez, I.T., Vargas, D. L. R., & Espinosa, J. C. M. (2025). A novel and efficient digital image steganography technique using least
21. Padmaja, S., & Basha, S. M. (2025). A Novel Hybrid Steganography Approach for Securing Text, Images, and Audio with Robust Encryption in Audio Steganography. *ITEGAM-JETIA*, *11*(52), 136-147. doi: 10.5935/jetia.v11i52.1235.
22. Abood, M. H., & Abdulmajeed, S. W. (2022). High Security Image Cryptographic Algorithm Using Chaotic Encryption Algorithm with Hash-LSB Steganography. *Al-Iraqia Journal for Scientific Engineering Research*, *1*(2), 65-74. doi: doi.org/10.58564/IJSER.1.2.2022.53.
23. Durge, R. S., & Deshmukh, V. M. (2025). Securing Cloud Data: A hybrid encryption approach with RSA and AES for enhanced security and performance. Journal of Integrated Science and Technology, 13(3), 1060-1060. doi: 10.62110/sciencein.jist.2025.v13.1060.
24. Sabeen, S. (2024, December). Securing Cloud Data: A Comprehensive Review of Hybrid Cryptography and Analysis of AES, Blowfish, and Twofish Algorithms. In *2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS)* (pp. 568-575). IEEE. doi: 10.1109/ICACRS62842.2024.10841570
25. Sahu, A., & Pradhan, C. (2023, January). A novel image steganography technique using AES encryption in DCT domain. In *International Conference on Distributed Computing and Intelligent Technology* (pp. 349-354). Cham: Springer Nature Switzerland. doi: 10.1007/978-3-031-24848-1_26.

Tamara Radivilova
Dr. eng. sc., prof., professor of V.V. Popovskyy department of infocommunication engineering,
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID 0000-0001-5975-0269
tamara.radivilova@nure.ua

Vadym Chakrian
PhD, Senior lecturer of the V.V. Popovsky Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID 0000-0003-4827-9779
vadym.chakrian@nure.ua

Arkadii Snihurov
PhD, Assoc. Prof., Dean of the Faculty of Information and Communication, Assoc. Prof. of the V.V. Popovsky Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID 0000-0003-1355-7978
arkadii.snihurov@nure.ua

Ihor Dobrynin
PhD, Assoc. Prof., Assoc. Prof. of the V.V. Popovsky Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID 0000-0001-8910-2609
ihor.dobrynin@nure.ua

Dmytro Ageyev
Dr. eng. sc., prof., professor of V.V. Popovskyy department of infocommunication engineering,
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID 0000-0002-2686-3854
dmytro.aheiev@nure.ua

Serhii Pshenychnykh
PhD, Assoc. Prof., Assoc. Prof. of the V.V. Popovsky Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID 0000-0003-0533-2306
serhii.pshenychnykh@nure.ua

Svitlana Shtangei
PhD, Assoc. Prof., Assoc. Prof. of the V.V. Popovsky Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics, Kharkiv, Ukraine
ORCID ID 0000-0002-9200-3959
svitlana.shtanhei@nure.ua

METHOD OF HIDING INFORMATION USING THE AES ENCRYPTION ALGORITHM AND THE LSB STEGANOGRAPHIC METHOD WITH PROTECTION AGAINST CROPPING AND STEGANALYSIS

Abstract. In an evolving era of rapidly increasing digital information volumes, ensuring its secure transmission is a critical task. The combination of steganography and encryption creates a powerful two-level security mechanism that simultaneously encrypts data and conceals its transmission. This paper proposes a method that implements two-level protection. The secret message is first encrypted using a reliable AES algorithm with a 256-bit key. This converts the source text into a pseudo-random sequence of bits, which complicates statistical analysis. Next, the encrypted data is embedded into a 24-bit color container image using a modified LSB method. The novelty of the approach lies in the following improvements: one full byte of the message is embedded into one pixel of the image, with its bits distributed across the RGB channels, which provides capacity; pixels are selected in a pseudo-random order using a pseudo-random number generator (PRNG), and a second PRNG is used for additional masking, providing additional protection against steganography

analysis; The start of message embedding is shifted from the beginning of the file based on the image size, which protects the data when the steganographic container is partially cropped. Standard metrics were selected to evaluate the effectiveness of the developed method: peak signal-to-noise ratio (PSNR), structural similarity index (SSIM), and normalized cross-correlation (NCC). Experimental analysis showed that the proposed method provides high-quality steganographic images. Even with maximum container filling (262,144 bytes), the PSNR remained high (56.67–56.76 dB), and the SSIM and NCC metrics were very close to 1, indicating minimal visual distortion. It is impossible to visually distinguish the original image from the stego container. A comparative analysis with other known methods (for 100,000 bytes) showed that the proposed algorithm has higher PSNR values (70.01–70.07 dB), confirming its effectiveness. The use of a double PRNG and embedding one byte per pixel ensures both high security and significant throughput. The developed hybrid method, which combines AES-256 encryption and modified LSB steganography with pseudo-random selection of pixels and bits, is an effective solution for the covert transmission of large amounts of data. The method provides a high level of security, resistance to steganography analysis, and visual invisibility of embedded data, as confirmed by high PSNR, SSIM, and NCC metrics.

Key words: steganography, cryptography, AES, LSB, concealment, data, container, image, security, encryption.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Radivilova, T., Kirichenko, L., Ageyev, D., Tawalbeh, M., & Bulakh, V. (2018, May). Decrypting SSL/TLS traffic for hidden threats detection. In 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (pp. 143-146). IEEE. doi: 10.1109/DESSERT.2018.8409116.
2. Radivilova, T., Dobrynin, I., Panteleev, V., Fisenko, D., Mazepa, A., & Bilodid, V. (2025). Analysis of methods for predicting internal threats based on analysis of data from the social network Twitter. Electronic professional scientific publication “Cybersecurity: Education, Science, Technology,” 4(28), 478–489. doi: 10.28925/2663-4023.2025.28.818
3. Ivanisenko, I., Kirichenko, L., & Radivilova, T. (2016, August). Investigation of multifractal properties of additive data stream. In 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP) (pp. 305-308). IEEE. doi: 10.1109/DSMP.2016.7583564.
4. Radivilova, T., Kirichenko, L., Panteleev, V., Mazepa, A., & Bilodid, V. (2024). Analysis of authentication methods for web applications and implementation of a web application with an integrated authentication system. Current state of scientific research and technology in industry, (3 (29)), 76-90. doi: 10.30837/2522-9818.2024.3.076
5. Alghawli, A. S. A., & Radivilova, T. (2024). Resilient cloud cluster with DevSecOps security model, automates a data analysis, vulnerability search and risk calculation. Alexandria Engineering Journal, 107, 136-149. doi:10.1016/j.aej.2024.07.036
6. Nasution, R. I. H., Fauzi, A., & Khair, H. (2023). Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image. Journal of Artificial Intelligence and Engineering Applications (JAIEA), 2(3), 89-98. doi: 10.59934/jaiea.v2i3.201
7. Alanzy, M., Alomrani, R., Alqarni, B., & Almutairi, S. (2023). Image steganography using LSB and hybrid encryption algorithms. Applied Sciences, 13(21), 11771. doi: 10.3390/app132111771
8. Talasila, S., Vijaya Kumar, G., Vijaya Babu, E., Nainika, K., Veda Sahithi, M., & Mohan, P. (2023, June). The hybrid model of lsb—technique in image steganography using aes and rsa algorithms. In International Conference on Soft Computing and Signal Processing (pp. 403-413). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-99-8451-0_34
9. Gupta, A., Ali, A., Pandey, A. K., Gupta, A. K., & Tripathi, A. (2022, November). Metamorphic cryptography using AES and LSB method. In 2022 International Conference on Advances in Computing, Communication and Materials (ICACCM) (pp. 1-8). IEEE. doi: 10.1109/ICACCM56405.2022.10009381.
10. Gopika, R., A., Ganesh, R. S. (2025). Dynamic pixel shuffling and hash LSB steganography with RC4 encryption: A robust data security framework. Expert Systems with Applications, 279, 127403. doi: 10.1016/j.eswa.2025.127403.

11. Raiyan, S. R., & Kabir, M. H. (2025). SCReedSolo: A Secure and Robust LSB Image Steganography Framework with Randomized Symmetric Encryption and Reed-Solomon Coding. arXiv preprint arXiv:2503.12368.
12. Radivilova, T., Dobrynin, I., Snihurov, A., Stanhei, S., & Bulba, S. (2025). Image Steganography Method using LSB and AES Encryption Algorithm. In 2025 Proceedings of the Workshop Classic, Quantum, and Post-Quantum Cryptography 2025 (CQPC 2025), 4016, (pp.32-44). Ceur.
13. Apau, R., Twum, F., Asante, M., & Hayfron-Acquah, J. B. (2024, February). A Secure and High Embedding Capacity Image Steganography Scheme Using Image Enhancement Technique, Compression, and Genetic Algorithm. In International Congress on Information and Communication Technology (pp. 307-325). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-97-5441-0_27
14. Malik, C., Jha, M., Jha, M., & Bansal, A. (2024, June). A Novel Approach for Image Steganography and Cryptography Using Genetic Algorithm. In International Conference on Data Analytics & Management (pp. 77-90). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-96-3372-2_6.
15. Reddy, K. K., Kumar, N. V., Sajan, L., Teja, M. P., & Kumar, V. P. (2023, December). Enhancing Steganography Security: A Dual Layer Approach with LSB and AES Algorithm. In International Conference on Advances in Computational Intelligence and Informatics (pp. 321-327). Singapore: Springer Nature Singapore. doi: 10.1007/978-981-97-4727-6_32.
16. Kumar, N., Soni, M. (2025). Randomized salt LSB: a novel approach to steganography with improved concealment and robustness. Int. j. inf. tecnol., 17, 4401–4414. doi: 10.1007/s41870-025-02501-4.
17. Khalil, N., Sarhan, A., Alshewimy, M. A.M. (2024) A secure image steganography based on LSB technique and 2D chaotic maps. Computers and Electrical Engineering, 119(B), 109566. doi: 10.1016/j.compeleceng.2024.109566.
18. Ehsan Ali, U. A., Ali, E., Sohrawordi, M., & Sultan, M. N. (2021). A LSB based image steganography using random pixel and bit selection for high payload. doi: 10.5815/ijmsc.2021.03.03
19. Roy, S., Islam, M.M. (2022). A Hybrid Secured Approach Combining LSB Steganography and AES Using Mosaic Images for Ensuring Data Security. SN COMPUT. SCI. 3, 153. doi: 10.1007/s42979-022-01046-8.
20. Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., Díez, I.T., Vargas, D. L. R., & Espinosa, J. C. M. (2025). A novel and efficient digital image steganography technique using least significant bit substitution. Scientific Reports, 15(1), 107. doi: 10.1038/s41598-024-83147-3.
21. Padmaja, S., & Basha, S. M. (2025). A Novel Hybrid Steganography Approach for Securing Text, Images, and Audio with Robust Encryption in Audio Steganography. ITEGAM-JETIA, 11(52), 136-147. doi: 10.5935/jetia.v11i52.1235.
22. Abood, M. H., & Abdulmajeed, S. W. (2022). High Security Image Cryptographic Algorithm Using Chaotic Encryption Algorithm with Hash-LSB Steganography. Al-Iraqia Journal for Scientific Engineering Research, 1(2), 65-74. doi: doi.org/10.58564/IJSER.1.2.2022.53.
23. Durge, R. S., & Deshmukh, V. M. (2025). Securing Cloud Data: A hybrid encryption approach with RSA and AES for enhanced security and performance. Journal of Integrated Science and Technology, 13(3), 1060-1060. doi: 10.62110/sciencein.jist.2025.v13.1060.
24. Sabeen, S. (2024, December). Securing Cloud Data: A Comprehensive Review of Hybrid Cryptography and Analysis of AES, Blowfish, and Twofish Algorithms. In 2024 3rd International Conference on Automation, Computing and Renewable Systems (ICACRS) (pp. 568-575). IEEE. doi: 10.1109/ICACRS62842.2024.10841570
25. Sahu, A., & Pradhan, C. (2023, January). A novel image steganography technique using AES encryption in DCT domain. In International Conference on Distributed Computing and Intelligent Technology (pp. 349-354). Cham: Springer Nature Switzerland. doi: 10.1007/978-3-031-24848-1_26.

(cc) BY-NC-SA
This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.