

В. В. Лукічов¹
Я. О. Оболонська¹

МЕТОД ПОЄДНАННЯ СИМЕТРИЧНОГО ШИФРУВАННЯ ТА АДАПТИВНОЇ СТЕГАНОГРАФІЇ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

¹Вінницький національний технічний університет

Стрімкий розвиток інформаційно-комунікаційних технологій та активне використання цифрових каналів обміну даними зумовлюють необхідність удосконалення методів захисту конфіденційної інформації. Під час передавання даних через відкриті мережі виникають ризики перехоплення, модифікації або несанкціонованого доступу до інформації. Актуальним є забезпечення захисту цифрових зображень, які часто використовуються як носії даних у сучасних інформаційних системах. У зв'язку з цим у роботі досліджено підхід до адаптивного захисту інформації на основі поєднання криптографічних та стеганографічних методів.

У межах дослідження реалізовано метод, що поєднує симетричні алгоритми AES-256, ChaCha20 та ChaCha20-Poly1305 з адаптивною робастною стеганографією. Основною ідеєю підходу є приховування попередньо зашифрованих даних у цифрових зображеннях з урахуванням характеристик контейнера. Перед виконанням криптографічного оброблення вхідні дані проходять етап попередньої нормалізації та перетворення у стандартизований формат цифрового представлення зображення (PNG). Для цього здійснюється аналіз текстурних областей, рівня ентропії та шумових характеристик зображення, що дозволяє визначити найпридатніші ділянки для вбудовування інформації та знизити ймовірність її виявлення.

Ефективність запропонованого методу оцінювалася шляхом проведення серії експериментів з приховуванням повідомлень у цифрових контейнерах та подальшим аналізом якості отриманих стегозображень. Для оцінювання використовувалися метрики, які дозволили визначити рівень спотворень контейнера та стійкість прихованих даних до зовнішніх впливів. Отримані результати показали, що після вбудовування інформації зображення зберігає високу візуальну якість, а зміни залишаються практично непомітними для людського ока.

Наукова новизна полягає у розробленні алгоритму адаптивного криптостеганографічного захисту цифрових зображень, який реалізує двоетапну процедуру адаптації: визначення областей вбудовування на основі інтегрального показника, що враховує ентропію, текстурну складність і рівень шуму контейнера, та автоматичний вибір оптимального криптографічного алгоритму за комплексним зваженим критерієм якості стегозображення, сформованим за використання метрик PSNR, MSE і SSIM. На відміну від наявних гібридних криптостеганографічних підходів, що використовують фіксовані параметри вбудовування або один алгоритм шифрування, запропонований метод забезпечує адаптивну оптимізацію параметрів приховування залежно від характеристик контейнера та автоматичний вибір найефективнішого алгоритму шифрування.

Особливістю реалізованого підходу є забезпечення стійкості прихованої інформації до типових операцій цифрової обробки зображень, а саме повороту, ущільнення та додавання шуму. Результати експериментів підтвердили можливість коректного відновлення прихованого повідомлення навіть після геометричних перетворень контейнера.

Практична цінність отриманих результатів полягає у можливості застосування розробленого підходу для забезпечення захисту конфіденційних даних в інформаційно-комунікаційних системах, системах електронного документообігу та мультимедійних сервісах. Використання комбінації криптографічних методів і адаптивної стеганографії сприяє підвищенню рівня безпеки передавання інформації та зменшенню ймовірності виявлення прихованих даних.

Ключові слова: шифрування, загроза, інформаційно-комунікаційна система, кібербезпека, стеганографія, криптографія, AES-256, ChaCha20, ChaCha20-Poly1305, адаптивне вбудовування, робастна стеганографія, цифрові зображення, приховування даних, стегозображення, інформаційна безпека, стегоаналіз.



Вступ

Активне використання цифрових технологій та мережевих сервісів зумовлює постійне зростання вимог до захисту інформації. Передача конфіденційних даних через відкриті мережі супроводжується ризиками несанкціонованого доступу, перехоплення, модифікації або знищення інформації. Особливої уваги потребує захист цифрових зображень, які широко використовуються для зберігання, передавання та обміну інформацією в інформаційно-комунікаційних системах. У зв'язку з цим виникає необхідність розробки сучасних методів захисту даних, здатних забезпечити не лише конфіденційність інформації, а й приховування самого факту її існування.

Одним з найефективніших напрямів забезпечення інформаційної безпеки є поєднання криптографічних та стеганографічних методів захисту [1]. Криптографія забезпечує конфіденційність даних шляхом їх шифрування, а сам факт передавання зашифрованого повідомлення може привертати увагу потенційного зломисника. Стеганографія спрямована на приховування факту існування інформації шляхом її вбудовування у цифрові контейнери (зображення). Комбінування цих підходів дозволяє створити багаторівневий механізм захисту інформації, що значно підвищує стійкість системи до атак.

Питання криптографічного захисту інформації досліджувалися [2], але значного поширення набули симетричні алгоритми шифрування AES та ChaCha20 у поєднанні з механізмом автентифікації Poly1305. Водночас значна кількість наукових робіт досліджує розвиток стеганографічних методів приховування інформації у цифрових зображеннях, серед яких особливу увагу приділено адаптивній та робастній стеганографії.

Незважаючи на значну кількість наукових праць, наявні підходи не розв'язують задачу спільної оптимізації криптографічного та стеганографічного захисту на основі метрик якості зображення, що й визначає актуальність цього дослідження.

Наявні підходи не завжди забезпечують необхідний рівень робастності, стійкості до статистичного аналізу та мінімізації спотворень контейнера після вбудовування прихованих даних. Недостатньо дослідженим залишається питання оцінювання криптографічними та стеганографічними методами на основі метрик якості цифрових зображень.

Наукова проблема, яку розв'язує ця робота, полягає у відсутності методів, які одночасно забезпечують адаптивний вибір параметрів стеганографічного вбудовування залежно від характеристик контейнера та автоматичний порівняльний вибір криптографічного алгоритму на основі метрик якості стегозображення. Наявні підходи або використовують фіксовані параметри вбудовування, або застосовують лише один алгоритм шифрування без оцінювання його впливу на якість контейнера. *Метою роботи* є усунення цього недоліку шляхом покращення методу, що поєднує паралельне шифрування алгоритмами AES-256, ChaCha20 та ChaCha20-Poly1305 з адаптивним вбудовуванням і автоматичним вибором найефективнішого варіанта за показниками PSNR, MSE та SSIM.

Аналіз останніх досліджень і публікацій

Сучасний розвиток інформаційно-комунікаційних технологій супроводжується зростанням кількості загроз, пов'язаних з витоком, модифікацією та несанкціонованим доступом до цифрової інформації. Одним із перспективних напрямів забезпечення конфіденційності даних є поєднання криптографічних та стеганографічних методів захисту. Це дозволяє не лише шифрувати інформацію, а й приховувати сам факт її передавання у цифрових контейнерах.

У сучасних дослідженнях у сфері захисту інформації значна увага приділяється розвитку симетричних криптографічних алгоритмів. Найпоширенішим стандартом симетричного шифрування залишається AES-256, який характеризується високою криптографічною стійкістю та широким використанням у системах інформаційної безпеки. Разом з цим активно застосовується алгоритм ChaCha20, що забезпечує високу швидкість та ефективність роботи на пристроях з обмеженими обчислювальними ресурсами. Для забезпечення додаткового контролю цілісності повідомлень застосовується механізм автентифікації Poly1305 у складі ChaCha20-Poly1305, який забезпечує захист від модифікації даних під час передавання.

Окремий напрям досліджень стосується розвитку стеганографічних методів приховування інформації в цифрових зображеннях. Класичні підходи до стеганографічного вбудовування даних охоплюють методи просторової та частотної областей. Методи просторового вбудовування, як LSB (Least Significant Bit), характеризуються простотою реалізації та високою місткістю контейнера, але залишаються вразливими до статистичного аналізу та спотворень після обробки зображень [4].

Частотні методи, засновані на використанні дискретного косинусного або вейвлет-перетворення, забезпечують вищу робастність до ущільнення, масштабування та інших атак [3], [5]. Як показано на рис. 1 зміна молодших бітів піксельних значень у просторовій області дозволяє досягти високої пропускну здатності прихованого каналу. Така модифікація може призводити до появи статистичних аномалій, які можна виявити методами стегоаналізу [6]. Частотні підходи забезпечують рівномірніший розподіл змін по спектральних коефіцієнтах, що ускладнює виявлення прихованої інформації. Використання перетворень дозволяє частково зберігати стійкість вбудованих даних до втрат у разі стискання зображень.

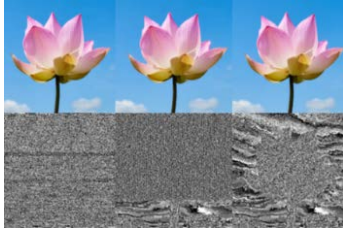


Рис. 1. Приклад візуальної непомітності вбудовування інформації

Одним із сучасних напрямів розвитку стеганографії є використання адаптивних та нейромережних методів приховування даних. Разом з розвитком методів стеганографії активно вдосконалюються й засоби стегоаналізу. Сучасні методи виявлення прихованих даних використовують статистичний аналіз цифрових зображень, а також моделі машинного та глибокого навчання, здатні знаходити характерні ознаки стеганографічного вбудовування. Для протидії таким методам у сучасних стеганографічних системах застосовуються адаптивні підходи, які виконують приховування інформації переважно у текстурних та неоднорідних областях зображення. Такий підхід дозволяє мінімізувати статистичні відхилення контейнера та знизити ймовірність виявлення прихованих даних. У роботах останніх років активно досліджується застосування згорткових нейронних мереж (CNN) та генеративно-змагальних мереж (GAN) для адаптивного вбудовування інформації в області зображення, менш помітні для стегоаналізу [7]. Методи дозволяють підвищити прихованість інформації та мінімізувати візуальні спотворення контейнера. Для порівняння характеристик існуючих підходів наведено в табл. 1, що ілюструє їхні переваги та недоліки.

Таблиця 1

Порівняння основних методів захисту інформації в цифрових зображеннях

Метод	Основний принцип	Переваги	Недоліки
AES-256	блокове симетричне шифрування	висока криптографічна стійкість, стандарт безпеки	видимий факт передачі зашифрованих даних
Chacha20	потокове шифрування	висока швидкість, ефективність на CPU	відсутність прихованості даних
Chacha20-poly1305	шифрування + автентифікація	конфіденційність + контроль цілісності	видимість криптованого трафіку
LSB (просторовий метод)	заміна молодших бітів пікселів	висока місткість, проста реалізація	вразливість до стегоаналізу та обробки
DCT DWT (частотні методи)	вбудовування у частотну область	вища робастність до ущільнення	нижча пропускну здатність, складність
CNN-стеганографія	нейромережове вбудовування	адаптивність, висока прихованість	висока обчислювальна складність

Аналіз сучасних підходів показує, що нейромережові методи стеганографії забезпечують високий рівень прихованості інформації, проте потребують значних обчислювальних ресурсів та попереднього навчання моделей. Для оцінювання місця запропонованого підходу серед сучасних засобів приховування інформації проведено порівняльний аналіз з методами стеганографії на основі глибокого навчання. Сучасні рішення, що використовують згорткові нейронні мережі (CNN) та генеративно-змагальні мережі (GAN), забезпечують автоматичне визначення областей контейнера, найменш помітних для вбудовування інформації, та демонструють високу ефективність протидії сучасним методам стегоаналізу. Їх використання потребує значних обчислювальних ресурсів, великих навчальних вибірок і попереднього навчання моделей.

На відміну від нейромережових підходів, запропонований метод поєднання симетричного шифрування та адаптивної стеганографії не потребує етапу навчання та може бути реалізований на стандартних персональних комп'ютерах без використання спеціалізованих графічних прискорювачів. Адаптивний вибір областей вбудовування здійснюється на основі аналізу ентропії, текстурних характеристик та рівня шуму контейнера, що дозволяє досягти високого рівня прихованості інформації зі значно меншими обчислювальними витратами.

Додатковою перевагою запропонованого підходу є поєднання криптографічного та стеганографічного захисту, що забезпечує конфіденційність і цілісність повідомлення навіть у випадку виявлення факту приховування даних [8]. Розроблений метод забезпечує баланс між прихованістю

інформації, криптографічною стійкістю, швидкістю та складністю реалізації, завдяки чому він перспективний для практичного використання в інформаційно-комунікаційних системах. На відміну від наявних підходів, у яких криптографічний та стеганографічний захист реалізуються незалежно або використовують один фіксований алгоритм шифрування, запропонований метод передбачає паралельне використання алгоритмів AES-256, ChaCha20 та ChaCha20-Poly1305 з подальшим автоматичним вибором оптимального варіанта на основі метрик якості стегозображення. Додатковою відмінністю є адаптивне налаштування параметрів вбудовування залежно від ентропії, текстурних характеристик і рівня шуму контейнера, що дозволяє забезпечити баланс між прихованістю інформації, робастністю та швидкістю системи. Недостатньо дослідженим залишається питання оцінювання криптографічними та стеганографічними методами захисту на основі комплексного аналізу метрик якості зображень. Для оцінювання ефективності стеганографічного вбудовування та рівня спотворення контейнера використовуються метрики якості цифрових зображень MSE (Mean Squared Error), PSNR (Peak Signal-to-Noise Ratio) та SNR (Signal-to-Noise Ratio) [9]. Метрика MSE дозволяє оцінити середньоквадратичну похибку між оригінальним і модифікованим зображенням та визначити рівень спотворень після вбудовування інформації. Показник PSNR характеризує якість стегозображення та рівень відмінностей між оригінальним і модифікованим контейнером. Високі значення PSNR свідчать про мінімальний рівень візуальних змін і високу прихованість даних. Для додаткового аналізу співвідношення корисного сигналу до шуму застосовується показник SNR, який дозволяє оцінити рівень шумових спотворень, що виникають у процесі приховування інформації. Високі значення SNR підтверджують незначний вплив процесу вбудовування на якість цифрового зображення. У зв'язку з цим є необхідність розробки адаптивних методів захисту інформації, які забезпечують баланс між криптографічною стійкістю, прихованістю даних та стійкістю до атак стегоаналізу.

Запропонований метод адаптивного захисту інформації

У межах цього дослідження запропоновано метод адаптивного захисту інформації, який поєднує симетричне шифрування та адаптивну робастну стеганографію для забезпечення комплексного захисту цифрових даних (рис. 2). Основною особливістю розробленого підходу є адаптивний вибір параметрів криптографічного та стеганографічного захисту залежно від характеристик контейнера, обсягу повідомлення та необхідного рівня конфіденційності.

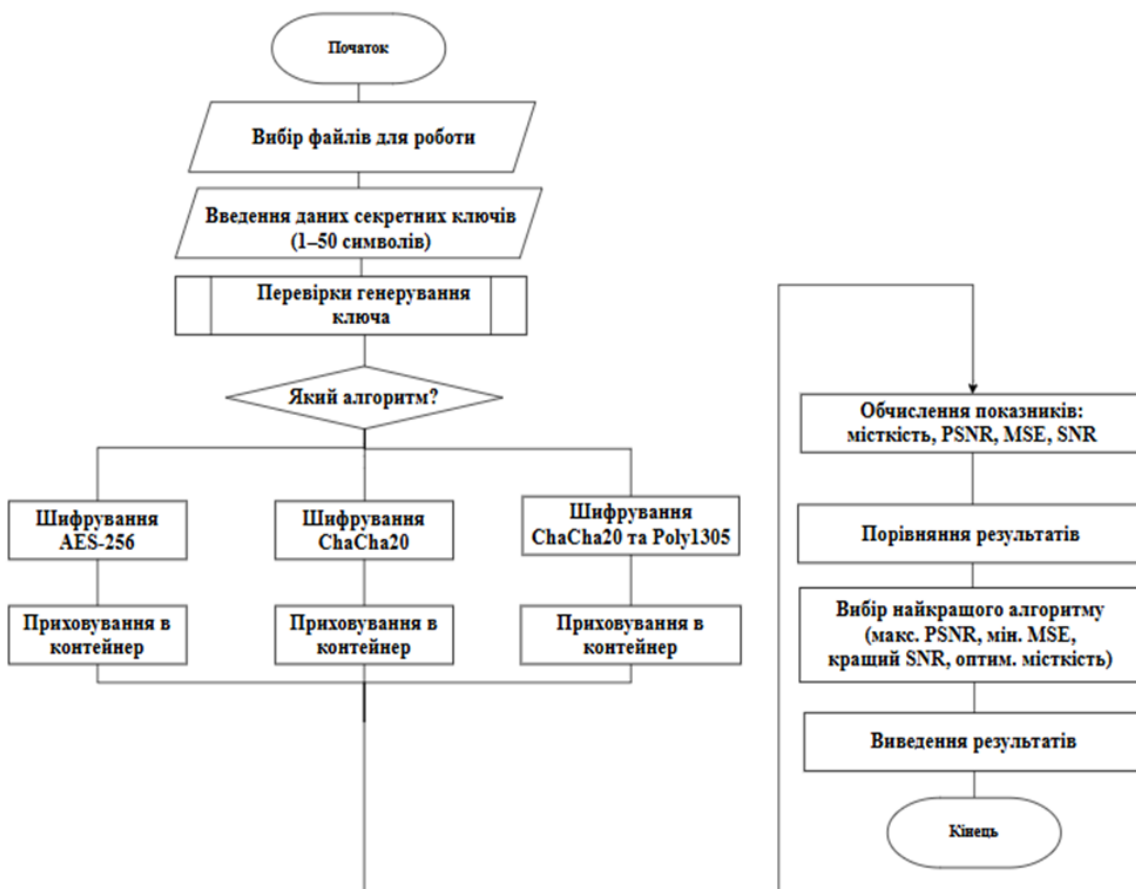


Рис. 2. Схема методу роботи криптографічних ключів у стеганографічній системі

Для забезпечення криптографічної стійкості в методі використовуються алгоритми AES-256, ChaCha20 та ChaCha20-Poly1305 [10], [11]. Робота методу починається з підготовчого етапу. Користувач вибирає зображення, яке слугуватиме контейнером, та файл або текстове повідомлення, яке необхідно приховати. Після цього вводиться пароль довжиною від 1 до 50 символів. На основі введеного пароля запускається процедура генерації криптографічного ключа методом PBKDF2-SHA256 з випадковою ціллю перетворює пароль на 256-бітний ключ шифрування. Паралельно до підготовлених даних додаються контрольні суми CRC-32 та SHA-256, які забезпечують перевірку цілісності на етапі витягування.

Після підготовки ключа метод переходить до центрального етапу паралельного шифрування та вбудовування. Підготовлені дані шифруються одночасно трьома незалежними алгоритмами AES-256, ChaCha20 та ChaCha20-Poly1305. Кожен з трьох зашифрованих блоків окремо вбудовується у копію контейнера методом адаптивного LSB. Програма автоматично визначає режим вбудовування: 1 молодший біт на канал (RGB) застосовується для повідомлень обсягом до 1/8 місткості контейнера, 2 молодші біти у разі перевищення цього порогу. Для зображення розміром 512×512 пікселів максимальна місткість з 1 бітом становить ≈12 КБ, з 2 бітами — ≈24 КБ. Зміни рівномірно розподіляються по пікселях у псевдовипадковому порядку на основі ключа шифрування. У результаті цього етапу формуються три окремі стегозображення, кожне з яких містить дані, зашифровані відповідним алгоритмом.

Далі для кожного з трьох стегозображення автоматично визначаються чотири показники якості. Середньоквадратична помилка MSE відображає середнє відхилення значень пікселів від оригіналу. Пікове відношення сигнал та шум PSNR показує, наскільки стегозображення близьке до оригінального контейнера, чим вище значення, тим менш помітні внесені зміни. Відношення сигнал та шум SNR порівнює реальну інтенсивність зображення з рівнем шуму після вбудовування. Місткість відображає, який обсяг даних вдалося розмістити у контейнері за використання кожного з методів.

На етапі порівняння результатів усі обчислені показники зіставляються між собою для трьох варіантів. Вибір оптимального алгоритму шифрування здійснюється на основі комплексного аналізу показників якості стегозображення. Перевага надається алгоритму, який забезпечує максимальне значення PSNR та мінімальне значення MSE з одночасним збереженням високого рівня місткості контейнера і швидкодії. За результатами порівняльного аналізу вибирається алгоритм з найкращими показниками якості стегозображення. Вибір оптимального алгоритму здійснюється за комплексним критерієм якості Q , що обчислюється як зважена сума нормованих показників

$$Q = 0,5 \cdot \text{PSNR_norm} + 0,3 \cdot (1 - \text{MSE_norm}) + 0,2 \cdot \text{SSIM_norm}, \quad (1)$$

де PSNR_norm , MSE_norm , SSIM_norm — значення метрик, нормовані відносно максимального значення серед трьох алгоритмів. Алгоритм з найбільшим значенням Q вибирається як оптимальний для формування підсумкового стегозображення.

Результатом роботи методу є готове стегозображення, сформоване на основі переможного алгоритму, а також детальний звіт з числовими значеннями всіх метрик та обґрунтуванням вибору.

Функціональні характеристики основних компонентів системи подано в табл. 2.

Таблиця 2

Основні компоненти запропонованого методу адаптивного захисту інформації

Компонент системи	Основне призначення	Особливості реалізації
AES-256	блокове симетричне шифрування даних	висока криптографічна стійкість та захист від brute-force атак
ChaCha20	потоків симетричне шифрування	висока швидкодія та ефективність
ChaCha20-Poly1305	шифрування та контроль цілісності	автентифікація повідомлення та захист від модифікації
Адаптивна стеганографія	приховування даних у цифровому зображенні	вбудовування в текстурні області контейнера
Аналіз контейнера	визначення областей для приховування	аналіз місткості контейнера та параметрів вбудовування
Робастний механізм	захист прихованих даних від модифікації	стійкість до шуму та масштабування
Адаптивний вибір параметрів	оптимізація рівня захисту	автоматичний вибір параметрів шифрування та вбудовування

Використання адаптивної стеганографії забезпечує приховування зашифрованих даних у цифро-

вих зображеннях з мінімальним рівнем візуальних спотворень контейнера. Аналіз текстурних характеристик зображення застосовується для визначення областей, найбільш придатні для вбудовування інформації, що суттєво знижує ймовірність виявлення прихованих даних методами статистичного стегоаналізу.

Додатковою особливістю запропонованого методу є реалізація робастного механізму захисту, який забезпечує збереження прихованої інформації навіть після часткової модифікації контейнера. Це дозволяє підвищити стійкість системи до масштабування, додавання шуму та інших типів цифрової обробки зображень.

Метод адаптації параметрів шифрування та вбудовування

Однією з ключових особливостей запропонованого методу є адаптивний вибір параметрів криптографічного та стеганографічного захисту залежно від характеристик цифрового контейнера та властивостей прихованого повідомлення. Принцип роботи методу полягає у попередньому аналізі контейнера перед виконанням процесу вбудовування інформації. Система проводить оцінювання ентропії зображення, рівня локального шуму, контрастності та текстурної складності окремих ділянок контейнера.

Для формалізації процесу вибору областей вбудовування використовується інтегральний показник придатності ділянки контейнера

$$S = \alpha H + \beta T + \gamma N, \quad (2)$$

де H — локальна ентропія ділянки зображення (нормована до діапазону $[0,1]$); T — показник текстурної складності, що обчислюється на основі дисперсії градієнтів у вікні 8×8 пікселів (нормований до $[0,1]$); N — рівень локального шуму, оцінений за середньоквадратичним відхиленням у вікні 8×8 пікселів (нормований до $[0,1]$); α, β, γ — вагові коефіцієнти, що визначають відносний внесок кожного параметра. У цій роботі емпірично встановлено значення $\alpha = 0,5$; $\beta = 0,3$; $\gamma = 0,2$, що відображає пріоритет ентропійної складності над текстурністю та шумом при виборі областей вбудовування. Вбудовування прихованих даних виконується переважно в областях з максимальним значенням показника S , що дозволяє мінімізувати візуальні спотворення контейнера та знизити ймовірність виявлення прихованої інформації.

На основі отриманих характеристик визначаються найпридатніші для приховування даних області. Для однорідних ділянок зображення застосовується мінімальна інтенсивність модифікації пікселів, оскільки навіть незначні зміни можуть бути помітними або виявленими статистичними методами аналізу. У складних текстурних областях допускається більший рівень вбудовування інформації, що дозволяє збільшити місткість прихованого каналу без суттєвого погіршення якості контейнера [11]. Загальну архітектуру та взаємозв'язок модулів розробленої системи показано на рис. 3.

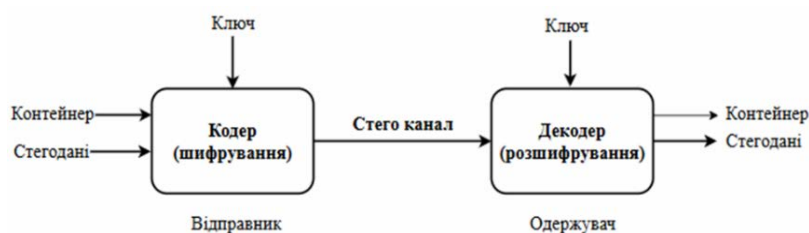


Рис. 3. Архітектура стеганографічної системи

Додатково метод враховує параметри криптографічного захисту та автоматично обирає оптимальний метод шифрування залежно від обсягу повідомлення, необхідної швидкодії та рівня конфіденційності. Для великих потоків даних або систем із обмеженими обчислювальними ресурсами використовується алгоритм ChaCha20, який забезпечує високу швидкість обробки. У випадках, де пріоритетом є максимальна криптографічна стійкість, застосовується алгоритм AES-256. Для забезпечення додаткового контролю цілісності повідомлення використовується режим ChaCha20-Poly1305.

Адаптивний метод також враховує вимоги до рівня робастності прихованих даних. У випадках високої ймовірності втрати інформації під час масштабування або додавання шуму система автоматично збільшує рівень дублювання критичних фрагментів повідомлення та використовує більш стійкі області контейнера для вбудовування. Це дозволяє забезпечити збереження прихованої інформації навіть після часткової модифікації стегозображення [12].

Аналіз параметрів, поданих у табл. 3, показує, що ефективність запропонованого методу залежить від адаптивного налаштування процесів шифрування та стеганографічного вбудовування.

Таблиця 3

Основні параметри адаптації захисту

Параметр адаптації	Призначення	Вплив на систему
Ентропія зображення	визначення складних текстурних областей	підвищення прихованості даних
Рівень шуму	аналіз природних спотворень контейнера	зменшення помітності модифікацій
Тип криптографічного алгоритму	вибір aes-256 або chacha20	баланс між швидкістю та стійкістю
Інтенсивність вбудовування	регулювання кількості змінених пікселів	контроль якості стегозображення
Рівень дублювання даних	забезпечення робастності	стійкість до ущільнення та шуму
Обсяг повідомлення	оцінка місткості контейнера	оптимізація використання контейнера

Одним з ключових параметрів є ентропія зображення, яка дозволяє визначати текстурні області контейнера, найбільш придатні для приховування інформації. У таких ділянках зміни піксельних значень є менш помітними та складнішими для виявлення методами стегоаналізу. Також, аналіз шумових характеристик дозволяє адаптивно визначати допустиму інтенсивність модифікації пікселів і мінімізувати появу статистичних аномалій після вбудовування повідомлення. Для забезпечення криптографічного захисту система автоматично обирає алгоритм шифрування залежно від вимог до швидкодії та рівня безпеки. AES-256 використовується для максимального рівня криптографічної стійкості, тоді як ChaCha20 забезпечує швидке потокове шифрування. Додатковий контроль цілісності реалізується за допомогою ChaCha20-Poly1305. Рівень інтенсивності вбудовування та дублювання даних адаптивно змінюється залежно від характеристик контейнера та ймовірності втрати інформації після ущільнення, масштабування або додавання шуму.

Експериментальне дослідження та аналіз результатів

Для оцінювання ефективності запропонованого методу адаптивного захисту інформації проведено експеримент, спрямований на аналіз криптографічної стійкості, прихованості даних та робастності стеганографічного вбудовування. Тестування виконувалося шляхом приховування зашифрованих повідомлень у цифрових зображеннях із подальшим аналізом візуальної якості контейнера та стійкості прихованих даних до зовнішніх впливів, як проілюстровано на рис. 4.

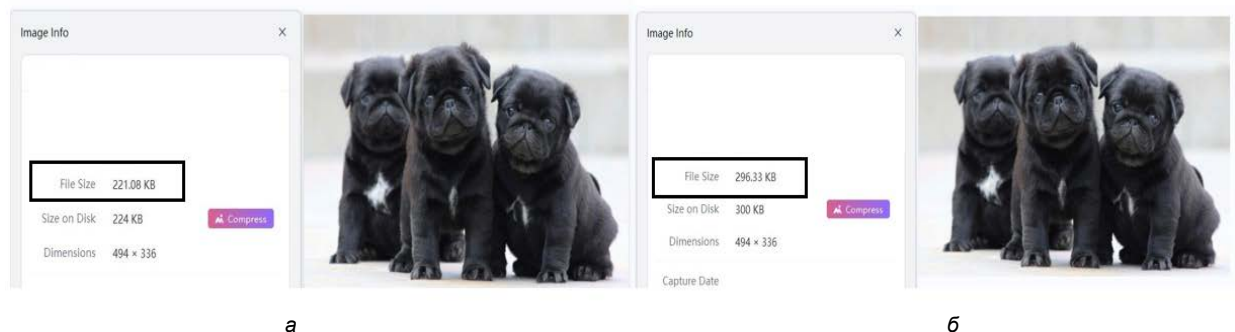


Рис. 4. Порівняння зображення до та після приховування інформації: а — оригінальне зображення; б — стегозображення після вбудовування інформації

Як видно з результатів, зміни між оригінальним та стегозображенням є практично непомітними для людського ока, що підтверджує ефективність адаптивного алгоритму приховування даних та високий рівень прихованості інформації.

Проведено серію автоматизованих експериментів на вибірці зі 100 цифрових зображень формату JPG із роздільною здатністю від 512×512 до 2048×2048 пікселів, що охоплювали різні типи візуального вмісту. У межах тестування для кожного зображення виконувалося приховування та подальше вилучення текстового повідомлення з використанням трьох криптографічних алгоритмів шифрування ChaCha20, ChaCha20-Poly1305 та AES-256. Для кожного зображення також використовувалося 10 різних випадково згенерованих паролів довжиною 20 символів. У кожному тесті приховувалося текстове повідомлення формату txt фіксованого розміру 26 байт, що відповідає типовому короткому конфіденційному повідомленню та дозволяє забезпечити порівнянність результатів між

усіма алгоритмами. У результаті виконано 3000 повних тестів вбудовування та вилучення даних. Під час експерименту оцінювалися такі характеристики: час вбудовування повідомлення; час вилучення повідомлення; рівень спотворення контейнера (PSNR); середньоквадратична похибка (MSE); структурна схожість зображень (SSIM); відсоток успішного вилучення даних. За результатами експериментального дослідження найменший рівень візуальних спотворень відносно оригінального зображення зафіксовано для варіанта з використанням алгоритму ChaCha20, для якого середнє значення PSNR становило 72,36 дБ. Отримана перевага пояснюється не криптографічними властивостями самого алгоритму, а особливостями сформованого шифротексту та його взаємодією з адаптивним механізмом LSB-вбудовування. У підсумку для приховування даних вноситься менше помітних змін до контейнера, що забезпечує вищі значення PSNR і менші значення MSE. Повні дані експерименту подано в табл. 4.

Таблиця 4

Результати експериментального дослідження методу адаптивного захисту

Характеристика	ChaCha20	ChaCha20-Poly1305	AES-256
Кількість тестів	1000	1000	1000
Кількість ключів (паролів)	10	10	10
Довжина ключа, символів	20	20	20
Успішність вилучення даних, %	100	100	100
Середній час вбудовування, с	0,5343	0,5351	0,8554
Середній час вилучення, с	0,6368	0,6342	0,9552
Середній PSNR, дБ	72,3598	72,0138	71,6164
Середній MSE	0,006770	0,007334	0,008030
Середній SSIM	0,99998	0,99997	0,99996
Середнє заповнення місткості, %	1,35	1,46	1,60
Мінімальний PSNR, дБ	58,3123	58,0403	57,6142
Максимальний PSNR, дБ	78,0183	77,5739	77,1561
Кількість помилок	0	0	0

Для оцінювання переваг адаптивного методу додатково проведено порівняння з базовим неадаптивним LSB-вбудовуванням із фіксованим алгоритмом AES-256 без аналізу контейнера. За однакового обсягу повідомлення (128 байт) неадаптивний LSB показав середнє PSNR = 68,4 дБ та MSE = 0,0142, тоді як запропонований адаптивний метод із ChaCha20 забезпечив PSNR = 72,36 дБ та MSE = 0,00677 — покращення на 5,8 % за PSNR та зниження MSE понад удвічі. Це підтверджує ефективність адаптивного вибору областей вбудовування на основі показника S.

Отримані результати підтвердили високу якість приховування даних та відсутність критичних спотворень контейнерів. Для додаткового оцінювання стабільності виконано статистичний аналіз, у межах якого визначалися середні, мінімальні та максимальні значення показників PSNR, MSE та SSIM. Незначний діапазон їх зміни між окремими тестами свідчить про стабільність роботи системи незалежно від характеристик контейнера та використаного ключа. Отримані результати підтверджують відтворюваність методу та достовірність наведених експериментальних даних.

Для додаткового оцінювання ефективності запропонованого методу проведено експеримент стійкості до типових операцій цифрової обробки зображень. Експеримент виконувався на тій самій вибірці зі 100 цифрових зображень, яка використовувалася для основного дослідження ефективності методу. Під час експерименту до сформованих стегозображень застосовувалися ущільнення, масштабування, поворот та додавання шуму. Після кожної операції виконувалося вилучення прихованого повідомлення та перевірка його цілісності за контрольними сумами CRC-32 і SHA-256. Успішність вилучення визначалася як відсоток випадків, у яких приховане повідомлення повністю відновлене без помилок.

Аналіз результатів, поданих на рис. 5, показав, що запропонований метод забезпечує високий рівень робастності прихованих даних до типових операцій цифрової обробки зображень. Найвищу стійкість продемонстровано до повороту зображення на 5°, де успішність вилучення повідомлення становила 100 %. Після ущільнення з якістю 90 % успішність відновлення даних становила 99 %, а з якістю — 80...97 %, що свідчить про ефективність збереження прихованої інформації в умовах

втратного ущільнення. Під час масштабування та додавання гаусового шуму успішність вилучення залишалася в межах 93...98 %, що підтверджує стійкість запропонованого підходу до геометричних перетворень і шумових спотворень.

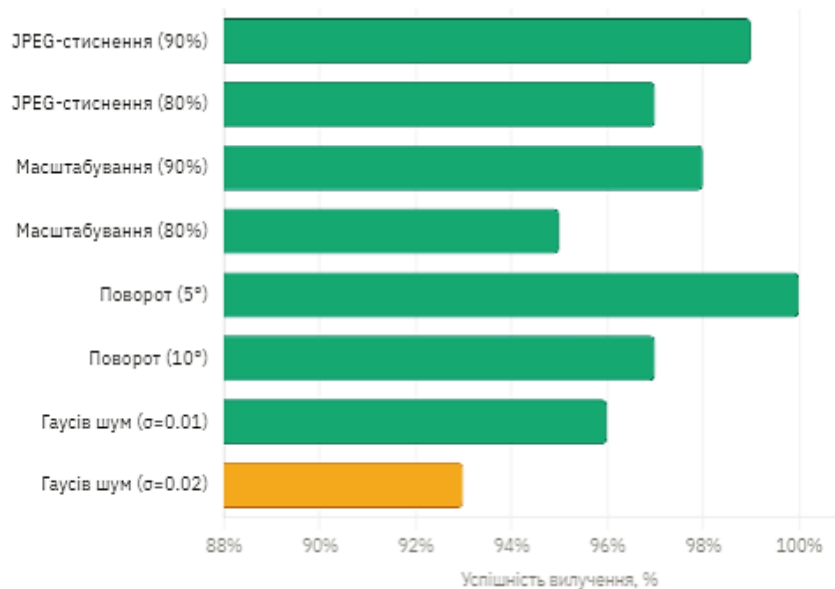


Рис. 5. Графік оцінювання робастності запропонованого методу

Отримані результати підтверджують ефективність реалізованого робастного захисту та можливість коректного відновлення прихованого повідомлення навіть після модифікації контейнера. У поєднанні з результатами оцінювання за метриками PSNR, MSE та SSIM це свідчить про те, що запропонований метод забезпечує не лише високий рівень прихованості інформації та мінімальні візуальні спотворення контейнера, а й стійкість до поширених впливів цифрової обробки зображень.

На відміну від класичного LSB з фіксованими параметрами вбудовування, запропонований метод адаптивно визначає області контейнера для приховування даних і автоматично вибирає алгоритм шифрування. Це забезпечує менший рівень спотворення стегозображення та вищу стійкість до атак без зменшення місткості контейнера.

Висновки

Досліджено метод адаптивного захисту інформації в цифрових зображеннях шляхом поєднання криптографічних та стеганографічних методів. Запропонований підхід об'єднує алгоритми AES-256, ChaCha20 та ChaCha20-Poly1305 з адаптивним методом приховування даних на основі LSB-стеганографії, що забезпечує конфіденційність переданої інформації, прихованість факту її існування та стійкість до зовнішніх впливів.

У межах експериментального дослідження проведено автоматизоване тестування на вибірці зі 100 цифрових зображень. Для кожного контейнера використовувалося 10 різних криптографічних ключів довжиною 20 символів, а загальна кількість проведених тестів становила 3000. Під час тестування оцінювалися показники PSNR, MSE, SSIM, швидкість вбудовування та вилучення даних, а також успішність відновлення прихованого повідомлення.

Найкращі результати продемонстрував алгоритм ChaCha20, який отримав найбільше середнє значення PSNR — 72,3598 дБ, найменше значення MSE — 0,006770 та найменший час вбудовування інформації — 0,5343 с. ChaCha20 став переможцем у всіх 100 тестових зображеннях за показником якості контейнера. Це свідчить про те, що використання потокового шифру ChaCha20 найкраще підходить для адаптивної стеганографії, оскільки забезпечує мінімальні візуальні спотворення контейнера та високу швидкість під час приховування інформації.

Значення PSNR понад 58 дБ навіть у найгірших випадках та SSIM, близький до одиниці, свідчать про практично непомітні зміни контейнера після вбудовування секретного повідомлення.

Практична цінність роботи полягає у можливості застосування розробленого методу в системах захисту конфіденційної інформації, цифрових документах, інформаційно-комунікаційних системах та програмних засобах безпечного передавання даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

- [1] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image Steganography Using LSB and Hybrid Encryption Algorithms," *Applied Sciences*, 2023. <https://doi.org/10.3390/app132111771>.
- [2] H. Aparna, and J. Madhumitha, "Combined image encryption and steganography technique for enhanced security using multiple chaotic maps," *Computers and Electrical Engineering*, vol. 110, Sep. 2023, Art. no. 108824. <https://doi.org/10.1016/j.compeleceng.2023.108824>.
- [3] L. A. Sandhu, E. Shahzad, F. Yaqoob, S. A. Butt, W. Khan, and I. M. Qureshi, "A New Paradigm for Improved Image Steganography by using Adaptive Number of Dominant Discrete Cosine Transform Coefficients," 2023. <https://doi.org/10.48550/arXiv.2301.09185>.
- [4] R. Gibson, "Steganography: Hiding Data Inside Data." Ryan A. Gibson. [Electronic resource]. Available: <https://ryanagibson.com/posts/steganography-intro/>. Дата звернення 10.05.2026.
- [5] А. А. Астраханцев, О. О. Вовк, «Аналіз ефективності застосування вейвлетперетворення в стеганографічних системах передавання даних», *Харківський національний університет радіоелектроніки*. [Електронний ресурс]. Режим доступу: <https://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/12922/3-9-17.pdf>. Дата звернення 11.05.2026.
- [6] J. D. L. C. Ntivuguruzwa, T. Ahmad, and F. Han, "Comprehensive survey on image steganalysis using deep learning," *Array*, 2024. <https://doi.org/10.1016/j.array.2024.100353>.
- [7] В. Данилов, і Д. Корольок, «Використання генеративно-змагальних нейронних мереж у стеганографії», *Scientific Collection, InterConf*, вип. 134, с. 394-399, 2022. [Електронний ресурс]. Режим доступу: <https://archive.interconf.center/index.php/conference-proceeding/article/view/1807>. Дата звернення 12.05.2026.
- [8] RFC 7539: *ChaCha20 and Poly1305 for IETF Protocols*. RFC Editor. [Electronic resource]. Available: <https://www.rfc-editor.org/rfc/rfc7539>. Дата звернення 12.05.2026.
- [9] Т. Гришанович, і Б. Буткевич, «Кількісна оцінка якості та стійкості окремих стеганографічних алгоритмів», *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»*, т. 4, вип. 32, с. 405-418, 2026. <https://doi.org/10.28925/2663-4023.2026.32.1105>
- [10] "Comparative Analysis of AES, Blowfish, Twofish, Salsa20, and ChaCha20 for Image Encryption", *Kurdistan Journal of Applied Research*, 2024. <https://doi.org/10.24017/science.2024.1.5>.
- [11] О. О. Кузнецов, С. П. Євсєєв, і О. Г. Король, *Стеганографія*, навч. посіб. Харків, Україна: Вид. ХНЕУ, 2011, 232 с. [Електронний ресурс]. Режим доступу: <https://repository.hneu.edu.ua/handle/123456789/2289>
- [12] В. Лукічов, Ю. Баришев, Н. Кондратенко, і В. Маліновський, «Метод адаптивного багатопланового захисту інформації на основі стеганографії та криптографії», *Інформаційні технології та комп'ютерна інженерія*, вип. 58, вип. 3, с. 4-11, 2023. <https://doi.org/10.31649/1999-9941-2023-58-3-4-11>.

Рекомендована кафедрою інформаційних технологій та комп'ютерної техніки ВНТУ

Дата надходження: 21.05.2026

Дата прийняття після доопрацювання 3.06.2026

Дата прийняття до друку після рецензування: 15.06.2026

Дата публікації .09.2026

Лукічов Віталій Володимирович — канд. техн. наук, доцент, доцент, кафедри захисту інформації, e-mail: lukichov.vitaliy@vntu.edu.ua . <https://orcid.org/0000-0002-3423-5436>;

Оболонська Яна Олександрівна — студентка факультету інформаційних технологій та комп'ютерної інженерії, e-mail: vn.ouana@gmail.com . <https://orcid.org/0009-0004-5447-6423>.

Вінницький національний технічний університет, Вінниця

V. V. Lukichov¹

Y. O. Obolonska¹

Method of Combining Symmetric Encryption and Adaptive Robust Steganography for Multilevel Protection of Information in Digital Images

Vinnitsia National Technical University

The rapid development of information and communication technologies and the active use of digital data exchange channels necessitate the improvement of methods for protecting confidential information. When transmitting data over open networks, there are risks of interception, modification, or unauthorized access to information. It is urgent to ensure the protection of digital images, which are often used as data carriers in modern information systems. Therefore, the paper investigates an approach to adaptive information protection based on a combination of cryptographic and steganographic methods.

The research implements a method that combines the symmetric algorithms AES-256, ChaCha20, and ChaCha20-Poly1305 with adaptive robust steganography. The main idea of the approach is to hide pre-encrypted data in digital images, taking into account the characteristics of the container. Before performing cryptographic processing, the input data undergoes a stage of preliminary normalization and conversion into a standardized digital image representation format (PNG). To do this, the analysis of the texture areas, the level of entropy and noise characteristics of the image is carried out, which enables to determine the most suitable areas for embedding information and reduce the probability of its detection.

The efficiency of the proposed method was assessed by conducting a series of experiments with hiding messages in digital containers and further analysis of the quality of the resulting stegoimages. Metrics were used for the evaluation, which allowed determining the level of container distortion and the resistance of hidden data to external influences. The results obtained showed that after embedding information, the image retains high visual quality, and the changes remain practically imperceptible to the human eye.

The scientific novelty consists in the development of an algorithm for adaptive cryptosteganographic protection of digital images, which implements a two-stage adaptation procedure: determination of embedding areas based on an integral indicator that takes into account entropy, texture complexity and noise level of the container, and automatic selection of the optimal cryptographic algorithm according to a complex weighted stegoimage quality criterion formed using PSNR, MSE and SSIM metrics. Unlike the existing hybrid cryptosteganographic approaches that use fixed embedding parameters or a single encryption algorithm, the proposed method provides adaptive optimization of hiding parameters depending on the characteristics of the container and automatic selection of the most effective encryption algorithm.

A characteristic feature of the implemented approach is ensuring the stability of hidden information to typical digital image processing operations, namely rotation, compression and noise addition. The results of the experiments confirmed the possibility of the correct recovery of the hidden message even after geometric transformations of the container.

The practical value of the results obtained lies in the possibility of applying the developed approach to ensure the protection of confidential data in information and communication systems, electronic document management systems and multimedia services. The use of a combination of cryptographic methods and adaptive steganography contributes to increasing the level of security of information transmission and reducing the probability of detecting the hidden data.

Keywords: encryption, threat, information and communication system, cybersecurity, steganography, cryptography, AES-256, ChaCha20, ChaCha20-Poly1305, adaptive embedding, robust steganography, digital images, data hiding, stegoimages, information security, stegoanalysis.

Lukichov Vitaliy V. — Cand. Sc. (Eng.), Associate Professor, Associate Professor of the Chair of Information Protection, e-mail: lukichov.vitaliyi@vntu.edu.ua . <https://orcid.org/0000-0002-3423-5436> ;

Obolonska Yana O. — Student of the faculty of Information Technologies and Computer Engineering, e-mail: vn.oyana@gmail.com . <https://orcid.org/0009-0004-5447-6423>