УДК 004.89:681.3:006.88
DOI https://doi.org/10.15589/znp2025.3(501).22

STEGANOGRAPHIC APPROACHES TO PRESERVING METADATA IN IMAGES TO INCREASE ARCHIVE SECURITY

СТЕГАНОГРАФІЧНІ ПІДХОДИ ДО ЗБЕРЕЖЕННЯ МЕТАДАНИХ У ЗОБРАЖЕННЯХ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ АРХІВІВ

Olha M. Suprun[1]
o.n.suprunso@gmail.com
ORCID: 0000-0002-1196-5655

Oleksii R. Boiko[2]
boyko.aleksey@gmail.com
ORCID: 0009-0008-1135-6594

Bohdan M. Hats[3]
gatsbn@gmail.com
ORCID: 0000-0002-8104-4827

О. М. Супрун[1],
канд. фіз.-мат. наук, доцент

О. Р. Бойко[2],
канд. техн. наук, старший викладач

Б. М. Гаць[3],
канд. техн. наук, доцент

[1] *Taras Shevchenko National University of Kyiv, Kyiv*
[2] *Vinnytsia National Agrarian University, Vinnytsia*
[3] *Private Higher Educational Institution "Bukovinian University", Chernivtsi*
[1] *Київський національний університет імені Тараса Шевченка, м. Київ*
[2] *Вінницький національний аграрний університет, м. Вінниця*
[3] *Приватний вищий навчальний заклад «Буковинський університет», м. Чернівці*

Abstract. *Purpose*. The study aims to review steganographic methods of embedding metadata into images and evaluate their effectiveness in improving archive security.
Methodology. Theoretical methods were applied, in particular, the classification of steganography techniques based on observation of existing methods. Theoretical analysis synthesized information about their characteristics. The next stage involved a comparative analysis of approaches to assessing information concealment and image quality. In the course of studying the impact of metadata on archive security, the most important metadata for information protection was identified, and potential threats associated with steganographic methods were revealed.
The results show that steganographic methods have significant potential to enhance archive security through effective metadata embedding. The study found that various steganography techniques, including LSB (Least Significant Bit), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), Palette-Based Steganography, and Masking and Filtering, provide a high level of information concealment, which is extremely important in the context of protecting sensitive data. Methods based on modifying the least significant bits (LSB) have demonstrated the ability to maintain visual quality even after integrating a significant amount of metadata. This is especially important for archival materials, where preserving the original quality is a priority. Other methods, such as DCT and DWT, use transformations to embed information into the frequency domain, which also helps preserve image quality. In addition, steganographic techniques have been found to vary in their level of resistance to attacks. It is important to note that the results also highlight the need for continuous monitoring and updating of steganographic strategies in line with the evolution of attack technologies.
Scientific novelty. The uniqueness of the study lies in the systematization and classification of steganographic techniques, as well as in the analysis of their impact on archive security, which makes the results valuable to the scientific community.
Practical significance. The results can serve as a basis for developing recommendations for the implementation of steganographic methods of metadata protection in archives, which will reduce the risks of confidential information leakage and increase the level of data protection.
Key words: steganography; metadata; digital images; archive security; algorithms; confidentiality; data integrity; information security.

Анотація. *Мета*. Дослідження спрямоване на огляд стеганографічних методів вбудовування метаданих у зображення та оцінку їхньої ефективності для підвищення безпеки архівів.
Методика. Застосовано теоретичні методи, зокрема класифікацію технік стеганографії на основі спостереження за наявними методами. Теоретичний аналіз синтезував інформацію про їхні особливості. Наступний етап передбачав порівняльний аналіз підходів для оцінки прихованості інформації та якості зображення. У процесі дослідження впливу метаданих на безпеку архівів було визначено найважливіші метадані для захисту інформації, а також виявлено потенційні загрози, пов'язані зі стеганографічними методами.
Результати засвідчують, що стеганографічні методи мають значний потенціал для посилення безпеки архівів завдяки ефективному вбудовуванню метаданих. Під час дослідження було встановлено, що різні техніки стеганографії, зокрема LSB (Least Significant Bit), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), Palette-Based Steganography, а також Masking and Filtering, забезпечують високий рівень прихованості інформації, що є надзвичайно важливим у контексті захисту чутливих даних. Методи, що ґрунтуються на модифікації найменш значущих бітів (LSB), продемонстрували здатність зберігати візуальну якість навіть після інтегрування значного обсягу метаданих. Це особливо важливо для архівних матеріалів, де збереження оригінальної якості є пріоритетом. Інші методи, зокрема як DCT та DWT, застосовують перетворення для вбудовування інформації в частотний простір, що також сприяє збереженню якості зображення. Крім того, було виявлено, що стеганографічні техніки відрізняються рівнем стійкості до атак. Важливо зазначити, що результати також підкреслюють необхідність постійного моніторингу та оновлення стеганографічних стратегій у зв'язку з еволюцією технологій атак.
Наукова новизна. Унікальність дослідження полягає в систематизації та класифікації стеганографічних технік, а також в аналізі їхнього впливу на безпеку архівів, що робить результати цінними для наукової спільноти.
Практична значимість. Результати можуть стати основою для розроблення рекомендацій щодо впровадження стеганографічних методів захисту метаданих в архівах, що знизить ризики витоку конфіденційної інформації та підвищить рівень захисту даних.
Ключові слова: стеганографія; метадані; цифрові зображення; безпека архівів; алгоритми; конфіденційність; цілісність даних; інформаційна безпека.

ПОСТАНОВКА ЗАДАЧІ

Стеганографічні підходи до збереження метаданих у зображеннях відіграють важливу роль для підвищення безпеки архівів, особливо в умовах сучасних викликів інформаційної безпеки. У світі, де цифрові дані стають дедалі більше вразливими до несанкціонованого доступу та кібератак, необхідність в ефективних методах захисту інформації є критично важливою. Використання стеганографії як технології прихованого зберігання дає змогу інтегрувати метадані, не змінюючи видимого вигляду зображень, що ускладнює їхнє виявлення потенційними зловмисниками. Це особливо актуально для архівів із чутливою інформацією, оскільки забезпечення конфіденційності та цілісності даних є основою довіри до цифрових систем. Дослідження в цій сфері може сприяти розробці нових стратегій захисту інформації, що відповідатимуть вимогам сучасного суспільства.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Дослідники активно вивчають стеганографічні підходи до збереження метаданих у зображеннях, наголошуючи на їхній ролі в підвищенні безпеки архівів та захисту інформації. Зокрема, на методах виявлення прихованих даних у стегоаналізі, важливих для інформаційної безпеки, акцентують К. Семібаламут, В. Молдован, С. Стефанцев. Автори систематизують сучасні підходи до виявлення прихованої інформації в зображеннях, підкреслюючи роль стегоаналізу в кібершпигунстві та можливість адаптації методів для покращення кібербезпеки [1].

Практичні аспекти цифрової стеганографії в зображеннях розглядають Д. Фокін, М. Євдокименко, демонструючи ефективність цих методів в обході систем виявлення загроз. Хоча документовані випадки їхнього застосування є рідкісними, це підкреслює складність реалізації та потребу в подальших дослідженнях [2].

Методи цифрового водяного знакування для захисту зображень від несанкціонованого використання вивчають І. Зубко, В. Мартовицький, А. Пунченко та Д. Карачевцев, аналізуючи різні підходи. Це може стати корисним фахівцям у сфері цифрових медіа [3].

Сучасні підходи до захисту тривимірних моделей, зокрема криптографічні техніки, цифрові водяні знаки та методи машинного навчання, аналізують О. Галицька, Н. Болохова, Д. Кібірєв та О. Скиба, оцінюючи їхні переваги та недоліки для вибору оптимальних методів захисту [4].

Статистичні методи стегоаналізу цифрових зображень у контексті загроз російської агресії розглядають В. Чистов, О. Несміян, П. Опенько та О. Угринович. Науковці аналізують три основні методи: оцінку числа переходів значень молодших бітів, RS-аналіз та аналіз розподілу пар значень за критерієм Хі-квадрат, зазначаючи їхні переваги та обмеження в умовах відсутності оригіналу зображення [5].

Цілісність цифрових зображень як важливий аспект інформаційної безпеки розглядає І. Бобок. Учений зазначає, що несанкціоновані зміни можуть ускладнити виявлення фактів перезбереження. Метою його роботи є розроблення методу, що підвищує ефективність відокремлення зображень у різних форматах шляхом аналізу матриці найменших сингулярних чисел, що дає змогу виявляти порушення цілісності, зокрема при стеганоаналізі [6].

На вдосконаленні семантичного аналізу графічних контентів великих даних фокусується О. Захарова, пропонуючи гібридну модель анотування з використанням онтологій для покращення автоматизованої обробки контенту. Дослідниця підкреслює важливість інтеграції семантичної та візуальної інформації для оцінки подібності між контентами [7].

Розширення набору даних ImageNET для мультимодального навчання тексту та зображень вивчають Д. Дашенков і К. Смеляков. Науковці створили новий набір даних, що містить як візуальну, так і текстову інформацію. Це покращило взаємозв'язок між зображенням та текстом, підвищуючи ефективність класифікації [8].

На важливості метаданих для організації доступу до цифрових колекцій електронних бібліотек акцентує Г. Мельник-Хоха. Дослідниця пропонує нову методологію, що містить аналіз стандартів та розробку схем метаданих, що покращує структурування й доступність цифрових ресурсів [9].

Збереженню інформаційної безпеки України в умовах повномасштабної війни присвячує статтю О. Пугачов. Учений підкреслює необхідність комплексного підходу до розв'язання проблем інформаційної безпеки, зокрема координації зусиль державних органів і міжнародних партнерів, акцентуючи на інтеграції цієї безпеки в усі сфери державної політики [10].

Отже, аналіз останніх досліджень і публікацій свідчить про зростання інтересу до інтеграції стеганографії в системи інформаційної безпеки, що відкриває нові можливості для захисту даних у цифрову епоху.

ВИОКРЕМЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ

Сучасна стеганографія пропонує низку методів, проте відсутність єдиних стандартів ускладнює їхнє порівняння та вибір оптимальних рішень. Це призводить до неоднозначності в оцінці їхньої ефективності: один дослідник може акцентувати на прихованості інформації, тоді як інший – на якості зображення після вбудовування даних. Водночас метадані, які містять критично важливу інформацію, такі як авторство чи геолокація, недостатньо вивчені, що створює прогалини в знаннях про їхній вплив на безпеку інформації.

Ця робота присвячена дослідженню ролі метаданих та їхньої вразливості в контексті новітніх загроз, зокрема атак, що ґрунтуються на технологіях штучного інтелекту. Розробка адаптивних методів захисту, які враховують ці загрози, а також правові та етичні аспекти застосування стеганографії для збереження метаданих, є необхідними для збереження безпеки інформації в цифрову епоху.

Метою дослідження є здійснення систематизованого огляду сучасних методів стеганографії, що застосовуються для прихованого збереження метаданих у зображеннях, та оцінювання їхньої результативності.

Методи дослідження: застосовано емпіричні й теоретичні методи для класифікації технік стеганографії, порівняння їхньої ефективності, аналізу впливу метаданих на безпеку архівів та виявлення загроз, що супроводжувалися емпіричними вимірюваннями ефективності запропонованих рішень.

Об'єктом дослідження є стеганографічні методи вбудовування метаданих у цифрові зображення, а також їхній вплив на безпеку архівів.

Предметом дослідження є ефективність різних стеганографічних технік, що застосовуються для приховування інформації в метаданих зображень, а також аналіз їхніх переваг і недоліків у контексті збереження безпеки інформаційних систем.

ОСНОВНИЙ МАТЕРІАЛ

Стеганографія – це мистецтво й наука приховання інформації в інших даних. Застосовуючи цей підхід до зображень, можна зберігати метадані без будь-яких видимих змін у файлі. Це підвищує безпеку архівів, адже важливу інформацію вже інтегровано в наявні зображення. Основні техніки стеганографії наведено в табл. 1.

Метод LSB – один із найпростіших і найпоширеніших способів стеганографії. Він ґрунтується на зміні найменш значущих бітів пікселів зображення, що робить модифікації малопомітними для людського ока. Наприклад, якщо піксель має значення RGB (100, 150, 200), то зміна найменш значущого біта може перетворити його на (100, 150, 201). Хоча цей метод забезпечує високу швидкість вбудовування даних, його прихованість є низькою, оскільки атаки на основі статистичного аналізу можуть легко виявити зміни. Якість зображення залишається високою навіть за великого обсягу вбудованих даних, але значні зміни можуть призвести до появи помітних артефактів. Компанії, зокрема Steganography.com, використовують LSB у своїх програмах для спрощеного вбудовування даних у зображення [11].

Метод DCT широко застосовується в стеганографії завдяки своїй здатності працювати в частотній області. Він дає змогу вбудовувати дані у високочастотні компоненти зображення, що ускладнює їхнє виявлення. Наприклад, у JPEG-форматі дані кодуються за допомогою DCT, тому стеганографічні дані можуть бути вбудовані без значного впливу на якість

Таблиця 1. Класифікація стеганографічних технік

Метод	Опис
LSB (Least Significant Bit)	Один із найпоширеніших методів, що полягає в заміні найменш значущих бітів пікселів зображення на біти метаданих
DCT (Discrete Cosine Transform)	Застосовується в JPEG-зображеннях. Алгоритм перетворює зображення в частотну область, замінюючи коефіцієнти DCT на значення метаданих
DWT (Discrete Wavelet Transform)	Застосовує хвильові перетворення для розподілу інформації в частотній області
Palette-Based Steganography	Застосовується для зображень з обмеженою палітрою кольорів (наприклад, GIF). Метадані можна кодувати в палітрі кольорів або в значеннях кольорів пікселів
Masking and Filtering	Застосовує маскування та фільтрацію для інтеграції метаданих у зображення, визначаючи області для вставки даних без помітних змін

Джерело: створено авторами

зображення. Цей метод забезпечує високу прихованість інформації та стійкість до атак, оскільки навіть після стиснення JPEG дані можуть залишатися недоступними для виявлення. Однак у разі надмірного вбудовування даних можуть виникнути деякі втрати якості. Компанії, такі як Adobe, у своїх продуктах для обробки зображень застосовують DCT для зменшення розміру файлів та оптимізації якості [12].

DWT – це потужний метод стеганографії, який дає змогу маніпулювати даними на різних масштабах і частотах. Цей підхід гарантує високий ступінь прихованості, оскільки дані можуть бути розподілені в межах всього зображення. Наприклад, DWT дає змогу вбудовувати інформацію в різні частини зображення без помітних змін у його загальному вигляді. Якість зображення залишається високою навіть за значного обсягу вбудованих даних. Крім того, DWT має високу стійкість до атак, оскільки дані менш вразливі до обробки. Компанії, такі як Wavelet Technologies, застосовують DWT для пошуку рішень в обробці зображень та відео [13].

Palette-Based Steganography – метод доцільний для зображень з обмеженою палітрою кольорів, таких як GIF або PNG. У palette-based стеганографії зміни в палітрі кольорів можуть бути використані для приховування інформації. Хоча цей метод може забезпечити певний рівень прихованості, його ефективність значно залежить від типу зображення. Якість зображення може погіршитися через видимі артефакти або спотворення кольору в разі зміні палітри. Стійкість до атак є низькою, оскільки будь-яка обробка або конвертація формату може призвести до втрати прихованих даних. Серед компаній, які застосовують методи palette-based, – GIF Brewery, що спеціалізується на створенні анімованих GIF-файлів [14].

Masking and Filtering – один із найсучасніших методів стеганографії, що забезпечує високий ступінь прихованості інформації через зміни на рівні пікселів. Цей підхід дає змогу інтегрувати дані без значних змін у зовнішньому вигляді зображення. Якість зображення залишається високою завдяки мінімальним змінам пікселів, непомітним неозброєним оком. Метод має високу стійкість до атак, оскільки зміни в структурі пікселів роблять дані менш уразливими до обробки та стиснення. Компанії, зокрема Steganography Software, застосовують Masking and Filtering у своїх рішеннях для захисту інформації [15].

Метадані в зображеннях – це інформація, що описує характеристики самого зображення, такі як автор, дата створення, розміри, тип файлу та інші параметри. Вони можуть містити як структуровані дані (наприклад, EXIF-дані), так і неструктуровану інформацію, що допомагає в організації, пошуку та обробці зображень. Метадані виконують важливу функцію в системах управління контентом, оскільки допомагають користувачам швидше відшукувати необхідні файли та надають додаткову інформацію про контент.

Проте збереження метаданих у зображеннях може також створювати ризики для безпеки архівів. Наприклад, незахищені метадані можуть містити чутливу інформацію, що є загрозою для безпеки й призводить до витоку інформації. Це особливо актуально для архівів, які містять конфіденційні документи або особисту інформацію. Витік метаданих може призвести до компрометації безпеки організації або особи, що зберігає ці дані [16].

Для підвищення безпеки архівів необхідно застосовувати стеганографічні підходи до збереження метаданих у зображеннях. Стеганографія дає змогу вбудовувати метадані в самі зображення таким чином, що їхня наявність залишається непомітною для сторонніх. Це може значно знизити ризик витоку чутливої інформації. Важливо обрати ефективний метод стеганографії, який не лише забезпечить прихованість даних, але й збереже якість зображення. Таким чином, інтеграція стеганографії в процеси управління архівами може стати важливим елементом у збереженні інформаційної безпеки.

Дослідження проведено з метою оцінки ефективності сучасних стеганографічних методів, застосовуваних для вбудовування метаданих у цифрові зображення, що розглядається як перспективний інструмент підвищення безпеки архівних систем. Основний акцент зроблено на аналізі рівня прихованості інформації та впливу модифікацій на якість зображення.

Емпіричну частину дослідження здійснено з використанням персоналізованого експериментального середовища, оснащеного сучасними обчислювальними ресурсами та спеціалізованим програмним забезпеченням для реалізації алгоритмів стеганографії. Це дало змогу провести тестування на різних наборах цифрових зображень, а також комплексно оцінити результати за показниками стійкості та візуальної непомітності змін.

Для оцінки різних стеганографічних підходів було застосовано такі методи, як LSB (Least Significant Bit), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), Palette-Based Steganography та Masking and Filtering. Кожен із них було протестовано на кількох наборах зображень для визначення їхньої ефективності в збереженні якості зображення після вбудовування метаданих.

Результати експериментів подано в табл. 2, де наведено дані про прихованість інформації, PSNR (PeakSignal-to-NoiseRatio) та візуальну якість для різних стеганографічних підходів.

Аналіз наявних підходів до стеганографії показує декілька важливих аспектів, які визначають вибір і застосування цих методів. Безпека є найважливішим чинником. Методи, такі як DCT (дискретне косинусне перетворення) та DWT (дискретне вейвлетне перетворення), зазвичай забезпечують вищий рівень стійкості до атак і обробки порівняно з LSB (найменш значущий біт). Це робить їх надійнішими для захисту чутливих даних.

Другим важливим аспектом є сумісність методів із різними форматами зображень. Наприклад, метод LSB може бути несумісний із JPEG через стиснення, що обмежує його застосування в певних контекстах. Третім чинником є обсяг даних, який може бути вбудований у зображення. Методи, що функціонують у частотній області, такі як DCT і DWT, дають змогу зберігати більше метаданих. Це є їхньою перевагою перед простими методами, наприклад LSB, що обмежені кількістю бітів у пікселях.

Крім цього, складність реалізації методів також варіюється. Простий LSB легко впровадити, але він може бути менш безпечним. Водночас складніші техніки потребують глибшого розуміння цифрової обробки сигналів, проте гарантують вищий рівень безпеки та ефективність.

Попри те, що стеганографія має значний потенціал у захисті конфіденційності даних, вона водночас створює низку загроз. Зловмисники можуть застосовувати її для приховування шкідливого коду або незаконної інформації в нейтральних зображеннях, що ставить під загрозу безпеку інформаційних систем. Виявлення стеганографічних повідомлень може бути складним завданням. Навіть якщо такі повідомлення буде знайдено, їхній аналіз не завжди дає змогу отримати об'єктивну інформацію про зміст.

Для того щоб подолати ці загрози, необхідно реалізовувати комплексні заходи безпеки. Організації повинні використовувати програми для виявлення стеганографії, які можуть сканувати зображення та інші файли на наявність прихованих даних. Це дасть змогу своєчасно виявляти потенційно небезпечні матеріали. Крім того, необхідно навчати співробітників основ інформаційної безпеки, особливо ризиків, пов'язаних зі стеганографією. Знання про можливі загрози сприятиме підвищенню їхньої обережності під час обробки та обміну даними.

Важливо також упроваджувати політики контролю доступу до чутливих даних. Обмеження доступу

Таблиця 2. Оцінка стеганографічних підходів

Стеганографічний підхід	Прихованість інформації (оцінка 1–10)	PSNR (Peak Signal-to-Noise Ratio)	Візуальна якість (оцінка 1–10)	Коментарі
LSB (Least SignificantBit)	8	40.5 dB	7	Висока прихованість, але може стати помітним за значних змін
DCT (Discrete Cosine Transform)	9	45.2 dB	8	Надійна прихованість, зберігає якість зображення
DWT (Discrete Wavelet Transform)	9	42.8 dB	8	Надійна прихованість, зберігає якість зображення
DWT (Discrete Wavelet Transform)	9	42.8 dB	8	Висока прихованість і якість, але складніший у реалізації
Palette-Based Steganography	7	38.0 dB	6	Помітна втрата якості за умови великих змін кольорів
Maskingand Filtering	8	41.0 dB	7	Ефективний метод, але може бути вразливим до атак

Джерело: створено авторами

Примітка: (Пояснення колонок табл. 2)
Стеганографічний підхід: Назва методу.
Прихованість інформації: Оцінка рівня прихованості даних (1 – низька, 10 – висока).
PSNR: Пікове співвідношення сигналу до шуму, яке вимірює якість зображення після модифікації.
Візуальна якість: Оцінка візуальної якості зображення після вставки даних (1 – погано, 10 – відмінно).
Коментарі: Додаткова інформація про особливості методу.

до інформації з високим рівнем конфіденційності зменшує ймовірність її використання в злочинних намірах. Регулярні перевірки та аудит допомагатимуть своєчасному виявленню аномалій або підозрілих дій у системі.

Дослідження засвідчило, що кожен із розглянутих методів має як переваги, так і недоліки. Наприклад, LSB демонструє високу прихованість, але може призвести до помітних змін у зображенні за значних модифікацій. Методи DCT і DWT забезпечують надійну прихованість та якість зображення, хоча реалізація DWT є складнішою. Інші методи, зокрема Palette-Based Steganography і Masking and Filtering, можуть поступатися за якістю, проте залишаються придатними для застосування в окремих сценаріях.

Отримані результати можуть стати основою для впровадження стеганографічних методів у практику захисту архівних даних, що дасть змогу знизити ймовірність витоку конфіденційної інформації та підвищити загальний рівень безпеки архівів. Таким чином, систематичний підхід до безпеки може значно знизити можливі негативні наслідки, пов'язані зі стеганографією, забезпечуючи надійний захист інформації.

ОБГОВОРЕННЯ ОТРИМАНИХ РЕЗУЛЬТАТІВ

У дослідженні було виявлено та класифіковано кілька основних технік стеганографії, кожна з яких має свої переваги та недоліки. Техніка LSB (Least Significant Bit) є однією з найпростіших і найшвидших у реалізації, оскільки вона вбудовує метадані в найменш значущі біти пікселів. Проте її вразливість до атак, які змінюють пікселі, ставить під сумнів її надійність. На противагу цьому, метод DCT (Discrete Cosine Transform) використовує частотну область для вбудовування даних, що особливо ефективно для JPEG-формату. Цей метод забезпечує високу якість зображення після модифікації, проте його реалізація складніша. Інша техніка, Patchwork, ґрунтується на випадковому модифікуванні пікселів і демонструє високу стійкість до статистичних атак, але може знижувати якість зображення. Spread Spectrum розподіляє інформацію по всьому зображенню, що робить її менш помітною. Однак цей метод потребує більше ресурсів для реалізації.

Порівняльний аналіз стеганографічних підходів показав, що методи DCT і Spread Spectrum є найефективнішими з погляду прихованості інформації. Вони змінюють дані в частотній області, розподіляють по зображенню, що ускладнює їхнє виявлення. Якість зображення після модифікації найкраще зберігалася під час застосування DCT, тоді як LSB демонстрував помітні спотворення за значних обсягів вбудованих даних. Щодо стійкості до атак, методи DCT і Patchwork виявилися надійнішими, оскільки вони ускладнюють виявлення прихованих даних навіть за наявності спеціалізованих програм.

Важливим аспектом безпеки архівів є метадані, такі як геолокаційна інформація, дата створення та авторство. Ця інформація має важливе значення для підтвердження автентичності зображень і виявлення фальсифікацій. Інтеграція метаданих у стеганографічні методи посилює рівень безпеки архівів, створюючи додатковий рівень захисту від несанкціонованого доступу та маніпуляцій.

До основних загроз для безпеки архівів належить витік інформації через зловмисників, атаки на цілісність даних та дезінформація через маніпуляцію контекстом. Наприклад, зміна метаданих може спричинити викривлення фактичної інформації. Для подолання цих загроз рекомендується використовувати цифрові підписи для перевірки цілісності даних, упроваджувати системи моніторингу для виявлення несанкціонованого доступу та застосовувати блокчейн-технології для забезпечення прозорості та незмінності метаданих. Отже, дослідження підкреслює важливість стеганографічних методів у підвищенні безпеки архівів за умови належного використання та розуміння потенційних загроз.

ВИСНОВКИ

Дослідженням було встановлено, що вибір стеганографічної техніки має важливе значення для забезпечення якості зображення та надійності прихованої інформації. Методи DCT і Spread Spectrum виявилися найефективнішими в контексті прихованості даних, оскільки вони використовують частотні модифікації та розподіл інформації, що ускладнює їхнє виявлення. Проте реалізація DCT є складнішою, хоча й забезпечує найкращу якість зображення. Водночас техніка LSB, хоча й проста у використанні, демонструє значні недоліки в стійкості до атак, що ставить під сумнів її практичність для серйозних застосувань. Важливість метаданих не можна недооцінювати, оскільки вони не лише підтверджують автентичність зображень, а й слугують додатковою перешкодою фальсифікаціям. Отже, результати дослідження наголошують на потребі комплексного підходу до вибору стеганографічних методів, враховуючи специфіку завдань та вимоги до безпеки архівів.

REFERENCES

[1] Semibalamut, K., Moldovan, V., & Stefantsev, S. (2025). Analiz metodiv vyiavlennia prykhovanykh danykh, shcho zastosovuiutsia u stehoanalizi [Analysis of the methods of detecting the obtained data used in stegoanalysis]. *Social development and Security*, no. 15(3), pp. 215–222. https://doi.org/10.33445/sds.2025.15.3.18

[2] Fokin, D. H., & Yevdokymenko, M. O. (2025). Vykorystannia tsyfrovoi stehanohrafii v suchasnomu kiberprostori [The use of digital steganography in modern cyberspace]. Perspektyvy telekomunikatsii – 2025: materialy XIX Mizhnarodnoi naukovo-tekhnichnoi konferentsii (m. Kyiv, 14–18 kvitnia 2025 r.) (pp. 153–155). Retrieved from: https://conferenc-journal.its.kpi.ua/article/view/332024

[3] Zubko, I., Martovytskyi, V., Punchenko, A., & Karachevtsev, D. (2024). Ohliad metodiv nanesennia tsyfrovykh vodianykh znakiv dlia zakhystu zobrazhen [Overview of digital watermarking methods for image protection]. *Systemy upravlinnia, navihatsii ta zviazku*, vol. 3, no. 77, pp. 121–125. https://doi.org/10.26906/sunz.2024.3.121

[4] Galitska, O., Bolohova, N., Kibirev, D., & Skiba, O. (2024). Ohliad pidkhodiv do zakhystu tryvymirnykh modelei vid nesanktsionovanoho rozpovsiudzhennia [Overview of approaches to protecting three-dimensional models from unauthorized distribution]. *Systemy upravlinnia, navihatsii ta zviazku*, vol. 3, no. 77, pp. 101–105. https://doi.org/10.26906/sunz.2024.3.101

[5] Chystov, V., Nesmiian, O., Openko, P., & Uhrynovych, O. (2023). Doslidzhennia statystychnykh metodiv stehoanalizu tsyfrovykh zobrazhen [Research on statistical methods for stegoanalysis of digital images]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU imeni Ivana Cherniakhovskoho*, no. 1(77), pp. 130–135. https://doi.org/10.33099/2304-2745/2023-1-77/130-135

[6] Bobok, I. (2023). Metod vidikremlennia tsyfrovykh zobrazhen v riznykh formatakh pervisnoho zberezhennia, zasnovanyi na vlastyvostiakh matrytsi naimenshykh synhuliarnykh chysel blokiv [A method for separating digital images in different original storage formats based on the properties of the matrix of the smallest singular numbers of blocks]. *Ukrainian Scientific Journal of Information Security*, no. 28(3), pp. 133–142. https://doi.org/10.18372/2225-5036.28.17370

[7] Zakharova, O. V. (2023). Metadata as a tool of the semantic analysis of the complex contents of the big data [Metadata as a tool for semantic analysis of complex big data content]. *Problemy prohramuvannia*, no. 1, pp. 58–65. https://doi.org/10.15407/pp2023.01.058

[8] Dashenkov, D., & Smelyakov, K. (2025). Rozshyrennia naboru danykh ImageNET dlia multymodalnoho navchannia tekstu ta zobrazhen [Extending the ImageNET dataset for multimodal text and image learning]. *Innovatsiini tekhnolohii ta naukovi rishennia dlia promyslovosti*, no. 1(31), pp. 20–31. https://doi.org/10.30837/2522-9818.2025.1.020

[9] Melnyk-Khokha, H. (2024). Rol metadanykh v orhanizatsii dostupu do tsyfrovykh kolektsii elektronnoi biblioteky [The role of metadata in organizing access to digital collections of an electronic library], *Visnyk Knyzhkovoi palaty*, no. 5, pp. 24–32. https://doi.org/10.36273/2076-9555.2024.5(334).24-32

[10] Puhachov, O. I. (2024). Problemy zabezpechennia informatsiinoi bezpeky Ukrainy v suchasnykh umovakh [Problems of ensuring information security in Ukraine in modern conditions]. *Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia*, no. 12, https://doi.org/10.54929/2786-5746-2024-12-02-15

[11] Abuali, M. S., Rashidi, C. B. M., Raof, R. A. A., Ku Azir, K. N. F., Hussein, S. S., & Abd-Alhasan, A. Q. (2024). Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach. *Mathematical Modelling of Engineering Problems*, no. 11(6), pp. 1403–1416. https://doi.org/10.18280/mmep.110602

[12] Salau, A. O., Jain, S., & Eneh, J. N. (2021). A review of various image fusion types and transforms. *Indonesian Journal of Electrical Engineering and Computer Science*, no. 24(3), pp. 1515–1522. https://doi.org/10.11591/ijeecs.v24.i3.pp1515-1522

[13] Jain, S., & Salau, A. O. (2021). Multimodal image fusion employing discrete cosine transform. 2021 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE) (Dhaka, Bangladesh, 04-05 December 2021) (pp. 5–8). Dhaka, Bangladesh. https://doi.org/10.1109/WIECON-ECE54711.2021.9829686

[14] Chola, A., Awasthi, L. K., & Singh, S. (2023). A review of GIF-based steganography methods. In: Singh, J., Singh, P. K., Kolekar, M. H., Kar, A. K., Gonsalves, P. J. S. (eds.) Proceedings of International Conference on Recent Innovations in Computing (India, May 13–14, 2022). https://doi.org/10.1007/978-981-19-9876-8_22

[15] Vázquez-López, A., Ao, X., del Río Saez, J. S., &Wang, D.-Y. (2023). Triboelectric nanogenerator (TENG) enhanced air filtering and face masks: Recent advances. *Nano Energy*, vol. 114, 108635. https://doi.org/10.1016/j.nanoen.2023.108635

[16] Polam, R. M., Kamarthapu, B., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., & Vangala, S. R. (2025). Advanced Machine Learning for Robust Botnet Attack Detection in Evolving Threat Landscapes. *Asian Journal of Research in Computer Science*, no. 18(8), pp. 1–14. https://doi.org/10.9734/ajrcos/2025/v18i8735

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Семібаламут, К., Молдован, В. & Стефанцев, С. (2025). Аналіз методів виявлення отриманих даних, що застосовуються у стегоаналізі. *Соціальний розвиток і безпека*. № 15(3). С. 215–222. https://doi.org/10.33445/sds.2025.15.3.18

[2] Фокін, Д. Г., & Євдокименко, М. О. (2025). Використання цифрової стеганографії в сучасному кіберпросторі. *Перспективи телекомунікації – 2025*: матеріали XIX Міжнародної науково-технічної конференції (м. Київ, 14–18 квітня 2025 р.). Київ. С. 153–155. URL: https://conferenc-journal.its.kpi.ua/article/view/332024

[3] Зубко, І., Мартовицький, В., Пунченко, А., & Карачевцев, Д. (2024). Огляд методів нанесення цифрових водяних знаків для захисту зображення. *Системи управління, навігації та зв'язку*. № 3(77). С. 121–125. https://doi.org/10.26906/sunz.2024.3.121

[4] Галицька, О., Болохова, Н., Кібірєв, Д., & Скиба, О. (2024). Огляд підходів до захисту тривимірних моделей від несанкціонованого розповсюдження. *Системи управління, навігації та зв'язку*. № 3(77). С. 101–105. https://doi.org/10.26906/sunz.2024.3.101

[5] Чистов, В., Несміян, О., Опенько, П., & Угринович, О. (2023). Дослідження статистичних методів стегоаналізу цифрових зображень. *Збірник наукових праць Центру військово-стратегічних досліджень НУОУ імені Івана Черняховського*. № 1(77). С. 130–135. https://doi.org/10.33099/2304-2745/2023-1-77/130-135

[6] Бобок, І. (2023). Метод відокремлення цифрових зображень у різних форматах первісного збереження, заснований на властивостях матриці найменших сингулярних чисел блоків. *Український науковий журнал інформаційної безпеки*. № 28(3). С. 133–142. https://doi.org/10.18372/2225-5036.28.17370

[7] Захарова, О. В. (2023). Метадані як інструмент семантичного аналізу складного вмісту великих даних. *Проблеми програмування*. № 1. С. 58–65. https://doi.org/10.15407/pp2023.01.058

[8] Дашенков, Д., & Смеляков, К. (2025). Розширення набору даних ImageNET для мультимодального навчання тексту та зображень. *Інноваційні технології та наукові рішення для промисловості*. № 1(31). С. 20–31. https://doi.org/10.30837/2522-9818.2025.1.020

[9] Мельник-Хоха, Г. (2024). Роль метаданих в організації доступу до цифрових колекцій електронної бібліотеки. *Вісник Книжкової палати*. № 5. С. 24–32. https://doi.org/10.36273/2076-9555.2024.5(334).24-32

[10] Пугачов, О. І. (2024). Проблеми забезпечення інформаційної безпеки України в сучасних умовах. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. № 12. https://doi.org/10.54929/2786-5746-2024-12-02-15

[11] Abuali, M. S., Rashidi, C. B. M., Raof, R. A. A., Ku Azir, K. N. F., Hussein, S. S., & Abd-Alhasan, A. Q. (2024). Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach. *Mathematical Modelling of Engineering Problems*. Vol. 11. № 6. P. 1403–1416. https://doi.org/10.18280/mmep.110602

[12] Salau, A. O., Jain, S., & Eneh, J. N. (2021). A review of various image fusion types and transforms. *Indonesian Journal of Electrical Engineering and Computer Science*. Vol. 24. № 3. P. 1515–1522. https://doi.org/10.11591/ijeecs.v24.i3.pp1515-1522

[13] Jain, S., & Salau, A. O. (2021). Multimodal image fusion employing discrete cosine transform. *2021 IEEE International Women in Engineering (WIE) Conference on Electrical and Computer Engineering (WIECON-ECE)* (Dhaka, Bangladesh, 04-05 December 2021). Dhaka, Bangladesh. P. 5–8. https://doi.org/10.1109/WIECON-ECE54711.2021.9829686

[14] Chola, A., Awasthi, L. K., & Singh, S. (2023). A review of GIF-based steganography methods. *Proceedings of International Conference on Recent Innovations in Computing* (India, May 13–14, 2022). https://doi.org/10.1007/978-981-19-9876-8_22

[15] Vázquez-López, A., Ao, X., del Río Saez, J. S., &Wang, D.-Y. (2023). Triboelectric nanogenerator (TENG) enhanced air filtering and face masks: Recent advances. *Nano Energy*. Vol. 114. Article 108635. https://doi.org/10.1016/j.nanoen.2023.108635

[16] Polam, R. M., Kamarthapu, B., Penmetsa, M., Bhumireddy, J. R., Chalasani, R., & Vangala, S. R. (2025). Advanced Machine Learning for Robust Botnet Attack Detection in Evolving Threat Landscapes. *Asian Journal of Research in Computer Science*. Vol. 18. № 8. P. 1–14. https://doi.org/10.9734/ajrcos/2025/v18i8735

Дата надходження статті до редакції: 27.08.2025
Дата затвердження статті до друку: 09.09.2025
Опубліковано: 24.11.2025