УДК 004.056.5

Д. О. Пінчук
В. В. Карпінець

ДОСЛІДЖЕННЯ ЗАВАДОСТІЙКОСТІ АЛГОРИТМІВ ЦИФРОВОГО ВОДЯНОГО МАРКУВАННЯ

Вінницький національний технічний університет

Анотація

У роботі представлено результати дослідження ефективності використання просторових і частотних доменів для приховування ідентифікаційних даних у графічних контейнерах. Проаналізовано ключові вразливості існуючих технологій маркування та запропоновано комплексне програмне рішення для проведення стегоаналітичного аудиту. На основі розробленого Full-Stack вебінструменту проведено стрес-тестування алгоритмів LSB, DCT та DWT за інженерними метриками PSNR та BER, що дозволило визначити межі їхньої робастності під дією навмисних і ненавмисних завад.

Ключові слова: цифрові водяні знаки, стегоаналіз, завадостійкість, просторові та частотні домени, коефіцієнт бітових помилок (BER).

Abstract

This paper presents the results of a study into the effectiveness of using spatial and frequency domains to conceal identifying data within image containers. It analyses the key vulnerabilities of existing watermarking technologies and proposes a comprehensive software solution for conducting a steganographic audit. Using the developed full-stack web tool, stress testing of the LSB, DCT and DWT algorithms was carried out against the engineering metrics PSNR and BER, which made it possible to determine the limits of their robustness under the influence of intentional and unintentional interference.

Keywords: digital watermarks, signal analysis, noise immunity, spatial and frequency domains, bit error rate (BER).

Вступ

Стрімке поширення мультимедійного контенту через незахищені мережеві канали актуалізує завдання контролю цілісності та підтвердження авторських прав на медіаоб'єкти. Традиційні криптографічні засоби забезпечують безпеку лише під час транспортування даних, проте повністю втрачають дію після розшифрування файлу на стороні легітимного користувача, виникає так званий «аналоговий пролом». Перспективним технологічним рішенням цієї проблеми є цифрове водяне маркування. Проте під час передавання через соціальні мережі чи вебсервіси файли зазнають автоматичного перекодування та стиснення. Метою роботи є комп'ютерне моделювання каскаду завад та експериментальне визначення меж стійкості просторових і частотних стегосистем за допомогою власного аналітичного вебінструменту.

Результати дослідження

У сучасну епоху масової діджиталізації та активного обміну інформацією через відкриті комп'ютерні мережі гостро постає проблема захисту авторських прав, автентифікації та контролю цілісності мультимедійних даних. Одним із найбільш прогресивних засобів проактивного захисту інформації є технологія цифрових водяних знаків (ЦВЗ), яка передбачає імплантацію прихованої ідентифікаційної мітки або стегоповідомлення безпосередньо у внутрішню структуру медіафайлу без помітного погіршення його вихідної якості. Даний підхід дозволяє усунути проблему «аналогового пролому», коли класичні криптографічні методи захисту каналів зв'язку втрачають свою ефективність одразу після розшифрування файлу кінцевим клієнтом, що вимагає розробки уніфікованих систем маркування контенту [1].

Процедура інтеграції стегоповідомлень у графічні файли-контейнери базується на використанні різноманітних математичних середовищ, серед яких фундаментальними є методи просторової та

частотної областей. Просторові алгоритми здійснюють пряму модифікацію безпосередньо числових значень яскравості колірних каналів растрової матриці, тоді як частотні методи передбачають попереднє ортогональне перетворення блоків зображення з подальшим коригуванням отриманих спектральних коефіцієнтів, що дозволяє гнучко адаптувати процес вбудовування під міжнародні стандарти компресії та обробки сигналів [2].

Оцінюючи функціональні можливості існуючих методів вбудовування ЦВЗ, слід виділити їхню чітку спеціалізацію залежно від обраного математичного домену. Просторові модифікації відрізняються мінімальною обчислювальною складністю та здатністю забезпечувати високу ємність стегоконтейнера, дозволяючи імплантувати значні масиви даних. У свою чергу, частотні трансформації, такі як дискретне косинусне перетворення (DCT) або дискретне вейвлет-перетворення (DWT) Хаара, мають унікальну властивість розподіляти енергію прихованого сигналу по суттєвих спектральних компонентах кадрів, що гарантує високу прихованість вкладення та базову стійкість до лінійних фільтрацій [3].

Попри значний технологічний потенціал, існуючі підходи до цифрового маркування мають певні недоліки та моменти, які потребують суттєвого вдосконалення та модернізації. Головною проблемою просторового кодування є його критично низька завадостійкість, оскільки будь-яке мінімальне перекодування або стиснення файлу з втратами повністю знищує інформацію у молодших бітах пікселів. Частотні ж методи вимагають складних каскадних обчислень, що при паралельній обробці великих потоків даних може спричинити високу латентність систем, а відсутність механізмів довготривалого структурування результатів досліджень ускладнює проведення комплексного порівняльного аудиту безпеки відкритих вебплатформ [4].

З метою розв’язання зазначених архітектурних та обчислювальних проблем у межах науково-дослідницької роботи було розроблено та практично впроваджено повнофункціональну аналітичну Full-Stack вебплатформу, яка об’єднала модулі просторового та частотного приховування з контуром імітаційного моделювання зовнішніх завад [5]. Головною перевагою створеного програмного комплексу є інтеграція оригінального диференціального підходу штучного зміщення енергетичного балансу спектральних коефіцієнтів, що дозволило досягти оптимального компромісу між критеріями візуальної невидимості мітки та її стійкості. У системі реалізовано ізольовану підсистему моделювання завад, яка з високою точністю відтворює вплив адитивного білого Гаусового шуму, лінійного розмиття (Blur) та JPEG-стиснення. Взаємодія між клієнтським інтерфейсом React та обчислювальним Express-сервером побудована за асинхронним REST API протоколом, а всі отримані інженерні коефіцієнти автоматично заносяться до реляційної бази даних SQLite через транзакційний журнал реєстрації операцій. У ході експериментів на платформі було проведено комплексне тестування, результати якого наочно продемонстрували, що частотний вейвлет-модуль (DWT) Хаара здатний безпомилково вилучати ЦВЗ із критично низьким рівнем помилок (BER = 0.80%) навіть в умовах агресивної фільтрації розмиттям у 5 пікселів, де просторовий метод LSB виявився абсолютно непрацездатним (BER = 50.00%).

Актуальність і практична цінність розробленого програмного комплексу полягає в його універсальності та можливості безпосередньої інтеграції у реальні контури інформаційної безпеки підприємств. Створену вебплатформу можна ефективно використовувати як автоматизовану систему наскрізного аудиту медіаконтенту, засіб верифікації автентичності цифрових документів, а також у видавничій та судовій експертизі для надійного підтвердження авторських прав і виявлення фактів несанкціонованого модифікування зображень. Окрім цього, інструмент є готовим рішенням для впровадження в освітній процес технічних університетів для наочної демонстрації принципів статистичного стегоаналізу.

Висновки

Проведені дослідження повністю підтвердили інженерну доцільність відходу від вразливих просторових методів стеганографії на користь частотних вейвлет-трансформацій. Програмна реалізація аналітичної вебплатформи дозволила автоматизувати процес стрес-тестування алгоритмів та накопичення інженерних метрик у реляційній базі даних. Експериментально доведено, що розроблений DWT-модуль на базі функцій Хаара забезпечує максимальний рівень завадостійкості цифрових водяних знаків під дією широкого спектра деструктивних впливів, що робить його надійним

інструментом для побудови сучасних комплексних систем захисту інтелектуальної власності в цифровому просторі.

Експериментально доведено, що розроблений DWT-модуль на базі функцій Хаара забезпечує максимальний рівень завадостійкості цифрових водяних знаків під дією широкого спектра агресивних деструктивних впливів. Шляхом порівняльного аналізу встановлено, що частотна декомпозиція блоків зображення локалізує корисний сигнал у середньочастотній області, мінімізуючи його спотворення при високочастотному зашумленні та спектральному квантуванні. Це робить розроблений підхід надійним інструментом для побудови сучасних комплексних систем захисту інтелектуальної власності в цифровому просторі, придатним для використання у реальних контурах кібербезпеки та корпоративного документообігу. Отримані аналітичні результати відкривають перспективи для подальшого вдосконалення стегосистем через інтеграцію інтелектуальних методів адаптивного вибору кроку квантування.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Graphics on the Web. World Wide Web Consortium (W3C). URL: https://www.w3.org/Standards/webdesign/graphics (дата звернення: 19.05.2026).
2. ISO/IEC 10918-1:1994. Digital Compression and Coding of Continuous-tone Still Images: JPEG. ISO. URL: https://www.iso.org/standard/18902.html (дата звернення: 19.05.2026).
3. Sharp Image Processing for Node.js / libvips Architecture. URL: https://sharp.pixelplumbing.com (дата звернення: 21.05.2026).
4. The JavaScript Object Notation (JSON) Data Interchange Format / Internet Engineering Task Force (IETF). RFC 8259. URL: https://datatracker.ietf.org/doc/html/rfc8259 (дата звернення: 21.05.2026).
5. Пінчук Д. О., Карпінець В. В. Дослідження стійкості цифрових водяних знаків у зображеннях із використанням стегоаналітичних методів. Матеріали LV Всеукраїнської науково-технічної конференції підрозділів ВНТУ, Вінниця, 24-27 березня 2026 р. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2026/paper/view/28682/23587 (дата звернення: 22.05.2026).

Пінчук Дар'я Олександрівна **–** студентка групи 1КІТС-22б, Факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: dashapinchukschool@gmail.com

Науковий керівник: ***Карпінець Василь Васильович*** **–** канд. техн. наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, e-mail: karpinets@gmail.com

Pinchuk Daria O. – student of group 1KITS-22b, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: dashapinchukschool@gmail.com

Supervisor: ***Karpinets Vasyl V.*** – Cand. Sc. (Eng.), Associated Professor, Head of the Chair of Management and Security of Information Systems, e-mail: karpinets@gmail.com