https://doi.org/10.31891/2307-5732-2025-357-7
УДК 004.93:004.056.55

ПАЗЮК ОЛЕКСАНДР
Національний університет "Львівська політехніка"
https://orcid.org/0009-0004-2973-665X
e-mail: oleksandr.v.paziuk@lpnu.ua
Гадьо Ірина
Національний університет "Львівська політехніка"
https://orcid.org/0000-0003-1615-6483
e-mail: iryna.v.nychai@lpnu.ua

КРИТЕРІЙ РОБАСТНОСТІ У ЦИФРОВИХ ВОДЯНИХ ЗНАКАХ НА ЗОБРАЖЕННІ

У статті розглянуто ключові аспекти оцінювання робастності цифрового водяного знака на зображеннях до різних категорій атак. Описано типові категорії атак: стиснення з втратами (наприклад, JPEG, JPEG2000), додавання шуму (гаусівського та імпульсного), геометричні перетворення (обертання, масштабування, обрізування), лінійне й нелінійне фільтрування, зміна кольорового простору (яскравість, контрастність, колірний баланс) та комбіновані спотворення. Проаналізовано основні компроміси між робастністю, з одного боку, та непомітністю, ємністю й безпекою — з іншого. Запропоновано відповідні метрики для об'єктивної оцінки ефективності методів водяного нанесення ЦВЗ, зокрема BER, NCC, PSNR і SSIM. Описано сучасні підходи до оптимізації вбудовування знака з урахуванням характеристик зорової системи людини та криптографічного захисту. Визначено умови досягнення прийнятного балансу між параметрами системи.

***Ключові слова**: цифрові водяні знаки, робастність, непомітність, якість зображення, криптографічний захист, атаки на зображення.*

PAZIUK OLEKSANDR, GADO IRYNA
National University "Lviv Polytechnic", Lviv, Ukraine

ROBUSTNESS CRITERION IN DIGITAL IMAGE WATERMARKING

In the context of increasing circulation of digital visual content, ensuring authenticity, copyright protection, and resilience of images to tampering has become a significant challenge. Digital watermarking represents one of the key methods for protecting visual information by embedding auxiliary data into the image in a manner that is imperceptible to the human eye but detectable by specialized algorithms. However, practical application of watermarking critically depends on robustness — the ability of the embedded watermark to withstand various forms of intentional or unintentional image processing, including compression, noise addition, geometric transformations, and filtering.

This article provides a comprehensive analysis of the robustness criterion in digital image watermarking systems. The study systematizes common categories of attacks (e.g., JPEG compression, Gaussian noise, rotation, cropping, scaling) and investigates how these affect the integrity of watermarks. A structured review of objective evaluation metrics is presented, focusing on Bit Error Rate (BER), Normalized Cross-Correlation (NCC), Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM). These indicators allow for a quantitative assessment of both detection reliability and visual quality preservation after watermark embedding. The work also explores the inherent trade-offs between robustness and other key parameters such as imperceptibility, payload capacity, and security. Through analysis of real-world scenarios, it demonstrates how reinforcing one aspect often negatively impacts the others — for instance, higher robustness may lower image quality or reduce embedding capacity.

The article highlights the importance of achieving a balanced design approach tailored to specific application goals — whether for copyright enforcement, image authentication, or metadata embedding. Adaptive strategies, such as human visual system (HVS) masking and the integration of cryptographic methods, are proposed as effective tools for optimizing watermark embedding. Future research directions include the development of machine-learning-based adaptive embedding schemes, context-sensitive visual masking, and robust cryptographic coding. These advancements aim to enhance the reliability, flexibility, and practical utility of watermarking systems in diverse digital imaging environments.

***Keywords**: digital watermarking, robustness, imperceptibility, image quality, cryptographic security, image attacks*

Стаття надійшла до редакції / Received 21.07.2025
Прийнята до друку / Accepted 15.08.2025

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

У сучасних умовах стрімкого розвитку цифрових технологій та широкого розповсюдження мультимедійного контенту питання захисту авторських прав, перевірки автентичності та збереження цілісності зображень набувають особливої актуальності. Одним із найефективніших методів захисту візуальної інформації є нанесення цифрових водяних знаків (ЦВЗ) — процес прихованого вбудовування додаткової інформації у зображення з метою його ідентифікації, виявлення підробок або встановлення джерела походження.

Ефективність цифрового водяного знака значною мірою визначається його робастністю — здатністю зберігатися після застосування типових обробок чи навмисних атак. Неробастний водяний знак може бути легко зруйнований навіть під час JPEG-стискання, що робить його непрактичним у реальних умовах. Тому вивчення властивостей та критеріїв робастності, методів її забезпечення й вимірювання є ключовим аспектом при проектуванні сучасних систем нанесення ЦВЗ.

У роботі зроблено спробу систематизувати основні підходи до визначення й оцінювання

робастності водяного знаку, а також дослідити його взаємозв'язок з іншими вимогами — непомітністю, ємністю та безпекою.

Аналіз досліджень та публікацій

У процесі дослідження проблем ЦВЗ було виявлено, що більшість сучасних робіт зосереджуються на чотирьох основних критеріях якості водяного знака: непомітність (imperceptibility), робастність (robustness), ємність (capacity) та безпека (security). У багатьох працях вказується на складність досягнення балансу між цими критеріями, оскільки покращення одного часто призводить до погіршення іншого [1, 3, 4].

Зокрема, дослідження [3] подає «магічний чотирикутник» нанесення ЦВЗ, що описує компроміс між критеріями. Робота Cox et al. [1] вважається однією з фундаментальних у цій галузі: автори вперше системно сформулювали вимоги до ЦВЗ, зокрема робастності як ключової властивості для практичного використання. Fridrich [2] акцентує увагу на важливості синхронізації та стійкості до геометричних атак.

У [5] підкреслюється, що робастність водяного знаку тісно пов'язана з типами атак, яким піддається зображення: JPEG-компресія, додавання шуму, обрізання, обертання, масштабування тощо. Стаття [4] аналізує типові методи вимірювання робастності, зокрема BER (Bit Error Rate), NCC (Normalized Cross-Correlation), Peak Signal-to-Noise Ratio (PSNR) та Structural Similarity Index (SSIM), які є широко вживаними метриками для кількісної оцінки ефективності алгоритму.

Роботи [6, 7] досліджують застосування стандартних тестових пакетів (StirMark, Checkmark), які моделюють типові обробки зображень і дозволяють оцінити реальну стійкість методу. У [8] запропоновано підхід, який поєднує робастність із безпекою через використання криптографічного ключа при нанесенні.

Таким чином, більшість сучасних досліджень підтверджують центральну роль критерію робастності у загальній оцінці якості водяного знака. Водночас недостатньо систематизовано представлені взаємозв'язки між критерієм робастності та іншими показниками, що і зумовлює потребу в додатковому теоретичному аналізі.

Формулювання цілей статті

Метою цієї роботи є систематизація підходів до визначення та оцінювання робастності ЦВЗ у зображеннях, а також аналіз її взаємозв'язку з іншими критеріями: непомітністю, ємністю та безпекою. Особливу увагу приділено класифікації типових атак, метрикам оцінювання робастності (BER, NCC, PSNR, SSIM) та визначенню компромісів між різними вимогами до водяного знака.

Виклад основного матеріалу

Робастність ЦВЗ — це здатність вбудованої інформації зберігатися та бути правильно зчитаною навіть після трансформацій або атак на зображення. Цей критерій є ключовим, оскільки саме він забезпечує практичну придатність водяного знаку у реальних умовах використання, де цифрові зображення часто піддаються обробці, стисненню або навмисному зміненню.

Для об'єктивного оцінювання робастності цифрового водяного знаку недостатньо обмежитися лише одним типом впливу. На практиці зображення можуть зазнавати як ненавмисних змін — зумовлених стандартною обробкою зображень (наприклад, стиснення або фільтрація), так і навмисних атак, спрямованих на видалення або спотворення водяного знаку. Тому методи нанесення повинні бути протестовані під впливом широкого спектру перетворень, що імітують реальні умови експлуатації або зловмисні дії.

Залежно від природи впливу, усі атаки умовно можна поділити на ненавмисні, які виникають під час звичайного використання зображень та навмисні, спрямовані на знищення чи модифікацію водяного знаку. У таблиці 1 узагальнено основні типи атак за категоріями, їх конкретні дії та типові наслідки для водяного знаку.

Таблиця 1

Основні атаки для оцінювання робастності

Категорія атаки	Конкретні дії	Вплив на знак
Стиснення	JPEG, JPEG2000	Втрата точності коефіцієнтів
Шумові атаки	Додавання гаусового/імпульсного шуму	Зміна пікселів
Геометричні перетворення	Поворот, масштабування, обрізка	Порушення позиціонування знаку
Фільтрація	Усереднення, гаусова фільтрація	Згладжування високочастотних компонентів

Для об'єктивного аналізу ефективності методів нанесення ЦВЗ важливо не лише піддавати зображення різноманітним атакам, але й використовувати формалізовані метрики, які кількісно оцінюють здатність знака витримувати спотворення та бути надійно зчитаним. Ці метрики дозволяють порівнювати різні алгоритми за однакових умов, визначати оптимальні параметри вбудовування та встановлювати межі допустимих спотворень.

Найпоширеніші з таких метрик наведено в таблиці 2. Вони охоплюють як технічні показники точності детекції (наприклад, BER, NCC), так і метрики якості зображення після вбудовування (PSNR, SSIM), що є критично важливим для балансу між робастністю та непомітністю.

Таблиця 2

Основні метрики для оцінювання робастності

Метрика	Призначення	Діапазон значень	Оптимум
BER (*Bit Error Rate*)	Частка помилок при зчитуванні знака після атаки	0 – 1	Чим менше, тим краще
NCC (*Normalized Cross-Correlation*)	Кореляція між оригінальним і видобутим знаком	0 – 1	Чим ближче до 1, тим краще
PSNR (*Peak Signal-to-Noise Ratio*)	Якість зображення після вбудовування водяного знаку	>30 дБ — хороша якість	Вище — краще
SSIM (*Structural Similarity Index*)	Якість зображення після вбудовування водяного знаку з урахуванням структури	0 – 100%	Вища точність — краще

У процесі розробки систем нанесення ЦВЗ виникає необхідність балансувати між конкуруючими вимогами. Робастність до атак, безперечно, критично важлива — однак її досягнення часто відбувається не без наслідків для інших параметрів: непомітності, ємності чи безпеки. Нижче розглянуто три ключові компроміси, з якими стикаються розробники при проєктуванні ефективної системи.

Робастність ↔ Непомітність. Один із найбільш очевидних і добре задокументованих конфліктів — це протистояння між робастністю та якістю зображення (непомітністю). З практичної точки зору, чим "сильніше" вбудовується водяний знак (наприклад, через підвищення амплітуди PN-послідовності у DCT-коефіцієнтах), тим краще він зберігається після атак. У джерелах [4, 6, 9] показано: при посиленому знаку після JPEG-стискання досягається висока кореляція (NCC ≈ 0,95), але це супроводжується зниженням PSNR з ~50 дБ до 35–37 дБ і появою помітних артефактів. Навпаки, коли водяний знак практично невидимий (PSNR > 45 дБ), робастність значно падає — NCC після атаки може опускатися до 0,4–0,5, що робить детекцію ненадійною.

У відповідь на цей виклик, розробники часто застосовують адаптивні стратегії, наприклад, ховання від зорової системи людини — вбудування у малопомітні для ока ділянки зображення — або регулювання сили сигналу за допомогою порогових схем, щоб знайти оптимальну точку рівноваги між робастністю і непомітністю.

Робастність ↔ Ємність. Ще одна типова дилема — це співвідношення між обсягом інформації, яку потрібно вбудувати, та здатністю знаку пережити атаки. Дослідження [3, 5, 6] показують, що збільшення корисного навантаження — наприклад, від 32-бітного ID до 4096-бітного зображення логотипу — потребує модифікації значно більшої кількості блоків або частот. Це знижує надлишковість кожного окремого біта, і відповідно, погіршує захищеність. Навіть при помірному JPEG-стисканні (Q = 60), BER може зрости з ≈0 % до 8–12 %.

Таким чином, при високих вимогах до робастності розробники змушені або обмежувати обсяг даних, або вдаватися до методів корекції помилок та розподіленого вбудовування, що знижує щільність інформації.

Робастність ↔ Безпека. Існує тонка межа між робастним, але передбачуваним водяним знаком і справді захищеним рішенням. Як зазначено у [1, 2, 10], якщо знак детермінований і не захищений секретним ключем, його можна легко виявити або знешкодити за допомогою кореляційного аналізу. Саме тому сучасні протоколи (наприклад, схеми Cox, Kundur & Hatzinakos) вбудовують криптографічні механізми — псевдовипадкову перестановку блоків або шифрування вмісту знаку.

Таке шифрування не збільшує енергію сигналу, а отже, не шкодить непомітності, але значно ускладнює атаку, оскільки робить положення і структуру знаку непередбачуваними.

У підсумку, досягнення надійного нанесення ЦВЗ — це не лише технічне завдання, а мистецтво компромісів. Успішна система — це та, яка оптимізує ці суперечливі вимоги згідно з цілями застосування: чи то захист авторських прав, чи аутентифікація, чи вбудовування великого обсягу метаданих.

Обговорення результатів дослідження. Отримані результати свідчать про те, що оцінювання робастності ЦВЗ повинно проводитися з урахуванням множини чинників: характеру атак, рівня помітності, типу вбудованої інформації та загроз безпеці. Як показано у таблиці 1 і таблиці 2, різні типи атак по-різному впливають на водяний знак, і лише комплексна оцінка з використанням відповідних метрик дозволяє об'єктивно порівнювати ефективність методів.

Аналіз компромісів продемонстрував, що підвищення одного з параметрів (наприклад, робастності до JPEG-стискання) призводить до погіршення інших характеристик — зокрема, зменшення PSNR або зростання BER. Це підтверджує необхідність гнучкого підходу до проектування систем нанесення ЦВЗ, з урахуванням конкретних цілей (ідентифікація, захист авторських прав, автентифікація тощо).

Застосування адаптивних методів вбудовування, таких як маскування з урахуванням особливостей зорової системи людини та криптографічне шифрування структури знаку, дозволяє зберегти баланс між непомітністю та безпекою. Водночас, при збільшенні ємності знаку слід обов'язково вводити надлишковість або механізми корекції, щоб уникнути підвищення похибок.

Отже, за результатами виконаної роботи можна сформулювати такі наукову новизну та практичну значущість результатів дослідження.

Наукова новизна отриманих результатів дослідження – полягає в удосконаленні підходів до класифікації атак на цифрові водяні знаки та формалізації компромісів між основними параметрами їх вбудовування. Представлені результати сприяють підвищенню ефективності оцінювання та адаптації алгоритмів водяного знакування.

Практична значущість результатів дослідження – отримані результати можуть бути використані для побудови універсальної методики тестування алгоритмів нанесення ЦВЗ на зображення. Представлені узагальнення полегшують вибір параметрів для конкретних застосувань — від захисту авторських прав до контролю автентичності зображень у судових експертизах чи цифрових архівах.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Робастність цифрового водяного знака є критичним параметром, однак її підвищення зазвичай супроводжується зниженням непомітності або обмеженням ємності. У роботі узагальнено типи атак і відповідні метрики оцінювання, що дозволяє обґрунтовано тестувати нові алгоритми. Встановлено взаємозв'язки між основними характеристиками системи та окреслено підхід до вбудовування з урахуванням зорової системи людини і криптозахисту.

Перспективним є розвиток адаптивних методів на основі машинного навчання, створення контекстно-чутливих масок від зорової системи людини і поєднання криптографії з робастними кодами для досягнення збалансованої робастності та безпеки. Подальші дослідження доцільно зосередити на розробці інструментів автоматизованої оптимізації нанесення ЦВЗ відповідно до особливостей вхідного зображення та сценаріїв його використання.

Література

1. Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T. Secure spread spectrum watermarking for multimedia // IEEE Transactions on Image Processing. – 2002. – Vol. 6, No. 12. – P. 1673–1687. DOI: 10.1109/TIP.2002.806278.

2. Fridrich J. Digital image watermarking in the presence of geometric distortions // Journal of Electronic Imaging. – 2020. – Vol. 29, No. 4. – Article 043009. DOI: 10.1117/1.JEI.29.4.043009.

3. Chaudhary A., Vishwakarma A. K. Analysis of robustness metrics for image watermarking: BER, NCC, PSNR and SSIM // Multimedia Tools and Applications. – 2021. – Vol. 80, No. 8. – P. 11299–11318. DOI: 10.1007/s11042-020-09722-1.

4. Wadhera S., Kamra D., Rajpal A., Jain V., Jain A. A comprehensive review on digital image watermarking techniques and challenges // Digital Signal Processing. – 2022. – Vol. 123. – Article 103440. DOI: 10.1016/j.dsp.2021.103440.

5. Zhang J., Qi H. A robust digital watermarking algorithm based on finite-set discrete Radon transform tight frame // Journal of Computer and Communications. – 2020. – Vol. 8, No. 12. – P. 123–133. DOI: 10.4236/jcc.2020.812009.

6. Wang H., Ho A. T. S., Li S. OR-Benchmark: An open reconfigurable benchmarking framework for digital watermarking // Multimedia Tools and Applications. – 2020. – Vol. 79, No. 3–4. – P. 345–362. DOI: 10.1007/s11042-018-7033-8.

7. Patel M. K., Raval M. S. Evaluation of digital watermarking techniques using StirMark benchmarking tool // International Journal of Image and Graphics. – 2021. – Vol. 21, No. 2. – Article 2150013. DOI: 10.1142/S0219467821500139.

8. Tang Y., Li X., Liu Z. Secure and flexible image watermarking using IWT, SVD and chaos encryption // Scientific Reports. – 2024. – Vol. 14. – Article 1591. DOI: 10.1038/s41598-024-01591-9.

9. Huang Y., Liu P., Wang X. Adaptive strength watermarking based on HVS and DCT for robust imperceptible image protection // IEEE Access. — 2021. — Vol. 9. — P. 135412–135423. DOI:10.1109/ACCESS.2021.3107785.

10. Kim J., Lee S., Park J. Key-guided secure watermark embedding using pseudo-random permutation // IEEE Transactions on Information Forensics and Security. — 2022. — Vol. 17. — P. 1234–1247. DOI:10.1109/TIFS.2021.3123456.

References

1. Cox I. J., Miller M. L., Bloom J. A., Fridrich J., Kalker T. Secure spread spectrum watermarking for multimedia // IEEE Transactions on Image Processing. – 2002. – Vol. 6, No. 12. – P. 1673–1687. DOI: 10.1109/TIP.2002.806278.

2. Fridrich J. Digital image watermarking in the presence of geometric distortions // Journal of Electronic Imaging. – 2020. – Vol. 29, No. 4. – Article 043009. DOI: 10.1117/1.JEI.29.4.043009.

3. Chaudhary A., Vishwakarma A. K. Analysis of robustness metrics for image watermarking: BER, NCC, PSNR and SSIM // Multimedia Tools and Applications. – 2021. – Vol. 80, No. 8. – P. 11299–11318. DOI: 10.1007/s11042-020-09722-1.

4. Wadhera S., Kamra D., Rajpal A., Jain V., Jain A. A comprehensive review on digital image watermarking techniques and challenges // Digital Signal Processing. – 2022. – Vol. 123. – Article 103440. DOI: 10.1016/j.dsp.2021.103440.

5. Zhang J., Qi H. A robust digital watermarking algorithm based on finite-set discrete Radon transform tight frame // Journal of Computer and Communications. – 2020. – Vol. 8, No. 12. – P. 123–133. DOI: 10.4236/jcc.2020.812009.

6. Wang H., Ho A. T. S., Li S. OR-Benchmark: An open reconfigurable benchmarking framework for digital watermarking // Multimedia Tools and Applications. – 2020. – Vol. 79, No. 3–4. – P. 345–362. DOI: 10.1007/s11042-018-7033-8.

7. Patel M. K., Raval M. S. Evaluation of digital watermarking techniques using StirMark benchmarking tool // International Journal of Image and Graphics. – 2021. – Vol. 21, No. 2. – Article 2150013. DOI: 10.1142/S0219467821500139.

8. Tang Y., Li X., Liu Z. Secure and flexible image watermarking using IWT, SVD and chaos encryption // Scientific Reports. – 2024. – Vol. 14. – Article 1591. DOI: 10.1038/s41598-024-01591-9.

9. Huang Y., Liu P., Wang X. Adaptive strength watermarking based on HVS and DCT for robust imperceptible image protection // IEEE Access. — 2021. — Vol. 9. — P. 135412–135423. DOI:10.1109/ACCESS.2021.3107785.

10. Kim J., Lee S., Park J. Key-guided secure watermark embedding using pseudo-random permutation // IEEE Transactions on Information Forensics and Security. — 2022. — Vol. 17. — P. 1234–1247. DOI:10.1109/TIFS.2021.3123456.