УДК 004.932.2:004.056.55
DOI https://doi.org/10.32689/maup.it.2025.2.13

Євген ЛАНСЬКИХ
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій проектування,
Черкаський державний технологічний університет,
y.lanskykh@chdtu.edu.ua
***ORCID:** 0000-0003-3389-5720*

Олексій НАУМОВ
аспірант кафедри інформаційних технологій проектування,
Черкаський державний технологічний університет,
o.m.naumov.asp23@chdtu.edu.ua
***ORCID:** 0009-0004-7573-3871*

СУЧАСНІ МЕТОДИ ЦИФРОВОГО ВОДЯНОГО МАРКУВАННЯ ЗОБРАЖЕНЬ: КЛАСИФІКАЦІЯ, АНАЛІЗ І ТЕНДЕНЦІЇ РОЗВИТКУ

Анотація. *У статті представлено комплексний огляд сучасних методів цифрового водяного маркування зображень, що використовуються для забезпечення авторських прав, перевірки автентичності та відстеження джерел розповсюдження цифрового контенту.*

Мета роботи *полягає в систематизації підходів до цифрового маркування зображень, зокрема традиційних, гібридних і заснованих на глибокому навчанні, а також у виявленні їх технічних характеристик, сильних і слабких сторін, практичної ефективності та науково-технологічних викликів у контексті цифрової безпеки.*

Методологія *дослідження базується на системному аналізі актуальних наукових джерел, включаючи рецензовані публікації, оглядові статті, експериментальні дослідження та прикладні реалізації алгоритмів цифрового водяного маркування. Для класифікації методів використано низку ключових технічних і функціональних критеріїв, зокрема: стійкість до атак, прозорість маркування, складність реалізації, обчислювальна ефективність, можливість сліпого виявлення (blind detection), адаптивність до типу зображень, а також широта сфер застосування. Порівняння методів здійснювалося з урахуванням їх здатності забезпечувати баланс між цими характеристиками, що дозволяє визначити оптимальні підходи для практичного застосування в умовах зростаючих вимог до цифрової безпеки, приватності та захисту інтелектуальної власності.*

Наукова новизна *роботи полягає у цілісному узагальненні еволюції методів водяного маркування із фокусом на сучасні технологічні тенденції, серед яких виокремлюються: інтеграція глибокого навчання для підвищення автономності алгоритмів; поєднання водяного маркування з криптографією та блокчейном; розробка адаптивних рішень, здатних масштабуватися під різні формати зображень і умови використання.*

Висновки. *Цифрове водяне маркування залишається стратегічно важливим інструментом захисту цифрового контенту. Проаналізовані методи демонструють широкий спектр рішень із різним ступенем прозорості, стійкості до атак та обчислювальної ефективності. Традиційні підходи, засновані на обробці у просторі або частотній області, є добре вивченими, але мають обмежену адаптивність. Гібридні методи поєднують переваги класичних рішень, проте потребують оптимізації для протидії сучасним атакам. Методології на основі глибокого навчання забезпечують новий рівень функціональності, зокрема можливість маркування без доступу до оригіналу (blind watermarking), однак стикаються з викликами, пов'язаними з високими ресурсними витратами та браком стандартів. У контексті цифрової трансформації суспільства актуальними стають дослідження, спрямовані на розробку надійних, масштабованих і нормативно врегульованих систем водяного маркування, здатних ефективно функціонувати в умовах зростаючих вимог до безпеки, приватності та інтероперабельності цифрових платформ.*

Ключові слова: *цифрове водяне маркування, захист авторських прав, стійкість до атак, гібридні методи, глибоке навчання, сліпе маркування, цифрові зображення.*

Yevhen LANSKYKH, Oleksii NAUMOV. MODERN METHODS OF DIGITAL IMAGE WATERMARKING: CLASSIFICATION, ANALYSIS AND DEVELOPMENT TRENDS

Abstract. *This article presents a comprehensive review of contemporary digital image watermarking methods used to ensure copyright protection, verify authenticity, and trace the sources of digital content distribution.*

The purpose *of the study is to systematize approaches to digital image watermarking, including traditional, hybrid, and deep learning-based methods, and to identify their technical characteristics, strengths and weaknesses, practical efficiency, and scientific and technological challenges in the context of digital security.*

The methodology *is based on a systematic analysis of current scientific sources, including peer-reviewed publications, review articles, experimental studies, and applied implementations of digital watermarking algorithms. The classification of methods was conducted using a set of key technical and functional criteria, including: robustness against attacks, watermark*

transparency, implementation complexity, computational efficiency, the possibility of blind detection, adaptability to image types, and the breadth of application areas. The comparative analysis focused on assessing the balance between these characteristics, which enables the identification of optimal approaches for practical application in conditions of increasing demands for digital security, privacy, and intellectual property protection.

***The scientific novelty** of the study lies in the integrated generalization of the evolution of watermarking methods, with a particular focus on current technological trends. These include the integration of deep learning to increase the autonomy of algorithms; combining watermarking with cryptographic and blockchain technologies; and the development of adaptive solutions capable of scaling across different image formats and application scenarios.*

***Conclusions.** Digital watermarking remains a strategically important tool for protecting digital content. The analyzed methods demonstrate a wide range of solutions with varying degrees of transparency, robustness against attacks, and computational performance. Traditional approaches, based on spatial or frequency domain processing, are well-studied but have limited adaptability. Hybrid methods combine the advantages of classical techniques but require further optimization to withstand sophisticated attacks. Deep learning-based methodologies offer a new level of functionality, including blind watermarking (embedding and extraction without access to the original image), yet face challenges such as high computational costs and the lack of standardized evaluation protocols. In the context of the ongoing digital transformation of society, it is crucial to develop reliable, scalable, and legally regulated watermarking systems capable of functioning effectively under growing requirements for security, privacy, and interoperability across digital platforms.*

***Key words:** digital watermarking, copyright protection, attack robustness, hybrid methods, deep learning, blind watermarking, digital images.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Захист авторських прав, автентичність цифрових зображень та протидія несанкціонованому розповсюдженню мультимедійного контенту є критично важливими завданнями в умовах сучасного інформаційного середовища. Поширення цифрових технологій у поєднанні з легкістю копіювання даних значно ускладнило захист інтелектуальної власності, що актуалізувало потребу в надійних і універсальних засобах цифрового маркування.

Цифрові водяні знаки (ЦВЗ) виступають ключовим інструментом для забезпечення захисту зображень, оскільки дають змогу вбудовувати приховану інформацію без істотного впливу на візуальну якість. Серед найважливіших наукових та практичних завдань, які розв'язуються через використання ЦВЗ, варто виділити:

- ідентифікацію та підтвердження авторства зображень;
- виявлення несанкціонованих змін або редагування;
- простежування джерела поширення контенту;
- використання в цифрових архівах, судово-експертній практиці та блокчейн-системах.

Однак впровадження таких технологій супроводжується низкою технічних проблем: забезпечення стійкості до атак (обрізання, фільтрація, масштабування), збереження якості зображення, швидкість обробки та адаптивність до різних умов.

Аналіз останніх досліджень і публікацій. Аналіз сучасних публікацій дозволяє виокремити кілька провідних напрямів розвитку методів цифрового водяного знакування (ЦВЗ). Одним із таких напрямів є оглядові та узагальнюючі праці, в яких проаналізовано десятки підходів до ЦВЗ. Зокрема, в оглядах [1], [2], [7] розглянуто методи, що базуються на дискретному вейвлет-перетворенні (DWT), косинусному перетворенні (DCT), найменш значущому біті (LSB) та застосуванні хаотичних карт.

Ряд публікацій [6; 13; 15] зосереджується на комплексному аналізі сучасних технологій цифрового маркування. Так, Hind M. Al-Dabbas та співавтори систематизують наявні рішення та можливі атаки на ЦВЗ. У дослідженні Shweta Wadhera і колег представлено напрями застосування ЦВЗ у сфері охорони здоров'я, освіти та інформаційної безпеки. У свою чергу, Wang та співавтори пропонують інтеграцію цифрового маркування зі стеганографією на основі глибокого навчання, що відображає міждисциплінарний підхід до вирішення проблем захисту цифрового контенту.

Інший напрям досліджень охоплює традиційні та гібридні підходи. У роботах [3] і [4] розглядаються як класичні, так і хаотичні алгоритми маркування, зокрема із використанням відображення Хенона та карти кота Арнольда. Такі рішення спрямовані на підвищення стійкості до атак, зберігаючи водяний знак у зміненому середовищі. Дослідження [5] підтверджує ефективність гібридних схем, у яких поєднуються методи сингулярного розкладання (SVD) із блочними перетвореннями, що дозволяє досягти стійкості без суттєвого зниження прозорості. У статті [16] описано чотириступеневий алгоритм, який комбінує DWT, DCT, SVD та скремблювання, демонструючи високу надійність навіть у випадках зниження роздільності зображення.

Окремий напрям становлять методи, засновані на глибокому навчанні. У роботі Zhong та ін. [17] представлено архітектуру, здатну здійснювати вбудовування водяного знаку в режимі «blind», тобто без доступу до оригінального зображення. Запропоноване рішення забезпечує стійкість до широкого спектру атак, включаючи навіть фотозйомку екрана. Схожий підхід описано в [10], де акцент зроблено

на підвищення геометричної стійкості маркування. Тренована нейромережева модель демонструє здатність зберігати водяний знак після трансформацій, таких як зміна кута, масштабування чи обертання.

Таким чином, наведені джерела демонструють як широту наукових підходів до цифрового водяного маркування, так і нагальну потребу в уніфікованих, ефективних і універсальних рішеннях, здатних функціонувати в умовах складного й змінного цифрового середовища.

Мета статті – систематизація сучасних методів цифрового маркування зображень; аналіз технічних та алгоритмічних підходів (традиційних, гібридних і на базі глибокого навчання); виявлення сильних і слабких сторін кожної групи методів; а також виявлення наукових і технологічних викликів, пов'язаних із захистом контенту в умовах швидкого розвитку цифрових платформ. Особлива увага приділяється стійкості алгоритмів до атак, збереженню візуальної якості зображення, обчислювальній ефективності методів та можливостям застосування у практичних галузях – кібербезпека, цифрова ідентифікація, захист контенту.

Виклад основного матеріалу. Методи цифрового водяного маркування класифікують за різними критеріями, зокрема за способом вбудовування, рівнем перетворення, способом отримання інформації, типом носія, а також за використанням інтелектуальних технологій. З метою систематизації сучасних підходів до цифрового водяного маркування (ЦВМ) зображень доцільно виділити три основні категорії: традиційні, гібридні та методи на основі глибокого навчання (deep learning, DL). Такий поділ базується як на історії розвитку методів, так і на технічних особливостях реалізації алгоритмів, що дозволяє більш об'єктивно провести їх порівняльний аналіз та оцінити перспективи практичного застосування. В оглядовій літературі [1; 2; 6; 7; 13; 15] і практичних реалізаціях можна виокремити три основні категорії методів.

Перша група методів – це традиційні методи цифрового водяного маркування, які ґрунтуються переважно на використанні класичних математичних перетворень або маніпуляціях на рівні пікселів. До них належать просторові методи, що передбачають модифікацію бітів зображення (наприклад, LSB-вставка) [7], частотні методи, що використовують дискретні перетворення (DCT, DWT, FFT), де водяний знак вбудовується у спектральні компоненти [1; 2], а також хаотичні системи, що застосовують детермінований хаос для шифрування або позиціонування водяного знака [3; 4]. Традиційні методи відзначаються відносною простотою реалізації та низькими обчислювальними витратами, що робить їх придатними для пристроїв із обмеженими ресурсами [1; 2; 4; 6]. Зокрема, метод на основі логістичного хаотичного відображення продемонстрував ефективність у забезпеченні початкового рівня стійкості та безпеки вбудованого маркування [4]. Ці підходи залишаються актуальними для задач, де потрібна швидка і легка реалізація без високих вимог до безпеки, зокрема в захисті авторських прав у відкритих базах даних. Однак основним недоліком цієї групи методів є їх низька адаптивність до складних атак, зокрема геометричних спотворень, обтинання та втрат стиснення JPEG.

Друга група – це гібридні методи, які поєднують переваги кількох трансформаційних доменів і додаткових механізмів, що дозволяє підвищити як стійкість, так і візуальну якість [3; 5; 16]. Також гібридні підходи інтегрують додаткові техніки – хаотичні перетворення, криптографічні алгоритми, статистичні моделі, алгоритми оптимізації (генетичні, рої частинок) [3; 15; 16]. Наприклад, комбінація перетворень (DWT+DCT+SVD) дозволяє балансувати між прозорістю та стійкістю [5; 16], а комбінування хаотичних карт і частотних алгоритмів підвищує стійкість і ускладнює несанкціоноване вилучення знака. Так, у роботі [3] запропоновано комбіноване використання хаотичних перетворень для генерації стійкого водяного знака, що ускладнює зворотну інженерію та підвищує криптостійкість. Гібридні методи часто мають вищу продуктивність, їх перевагами є можливість налаштування під конкретні потреби користувача та досягнення балансу між прозорістю, стійкістю та продуктивністю. Ці методи ефективно застосовуються у сфері цифрової ідентифікації, медичних зображень, судової експертизи. Проте складність реалізації таких систем значно вища, як і обчислювальна складність, особливо у випадках використання багаторівневих перетворень, адже вони потребують ретельного налаштування.

Третя група – це методи цифрового маркування, що базуються на глибокому навчанні, яке останнім часом активно розвивається. Цей напрям є найновішим і передбачає використання нейронних мереж, таких як автоенкодери, згорткові нейронні мережі (CNN), GAN-архітектури та трансформери для навчання вбудовування та виявлення водяного знака [8; 10; 11; 13; 14; 15; 17]. Перевагою цих методів є автоматична адаптація до контенту зображення, висока ємність маркування та стійкість до складних атак, зокрема до геометричних трансформацій, шуму та перекодування [8; 10; 14]. Також вони використовуються для вбудовування та видобування знака у «blind» режимі. Наприклад, у роботі [10] запропоновано сліпу схему маркування зображень на основі глибокого навчання, яка демонструє стійкість до змін масштабу, обертання та інших геометричних деформацій. Разом з тим, такі методи

є ресурсоємними, потребують великих обсягів даних для навчання, а також характеризуються низькою інтерпретованістю, що може ускладнювати їх використання в критично важливих додатках (наприклад, цифрова судова експертиза). Також існують мережі, стійкі до геометричних викривлень, що дозволяють зберегти водяний знак після атак типу обертання, масштабування, обрізання [10]. Загалом ці підходи демонструють високу адаптивність до різних форматів зображень і атак, відкривають нові можливості для інтеграції ЦВМ у розумні системи, захист AI-контенту, deepfake-детекцію, NFT тощо, але потребують великих обсягів даних і ресурсів для навчання.

Класифікація методів цифрового водяного маркування на традиційні, гібридні та засновані на глибокому навчанні дозволяє систематизувати сучасні підходи відповідно до їхніх технічних характеристик, ефективності та застосовності в умовах динамічного цифрового середовища. Такий поділ також сприяє кращому розумінню сильних і слабких сторін кожної групи методів, що є необхідним для обґрунтованого вибору рішень у практичних задачах – від захисту авторських прав до протидії нелегальному тиражуванню цифрового контенту. Така класифікація дозволяє ефективно орієнтуватися в поточному стані досліджень, порівнювати алгоритми за релевантними критеріями та прогнозувати вектори подальшого розвитку технологій цифрового захисту зображень.

З урахуванням швидкого розвитку алгоритмів та зростання вимог до захисту мультимедійного контенту, порівняльний аналіз основних підходів до цифрового водяного маркування є ключовим для виявлення їх сильних і слабких сторін. Для забезпечення всебічної та об'єктивної оцінки сучасних методів було обрано сім ключових критеріїв, які охоплюють як технічні характеристики, так і здатність адаптуватися до прикладних потреб цифрового середовища.

Одним із базових параметрів є стійкість до атак. Вона передбачає здатність водяного знака зберігатися після типових спотворень, таких як стиснення JPEG і JPEG2000, фільтрація, обертання, масштабування, обтинання або додавання шуму. Цей критерій є критично важливим для захисту авторських прав та довготривалого збереження маркування у змінному цифровому середовищі [6; 7, 14].

Не менш важливою є прозорість, яка визначає ступінь впливу водяного знака на візуальну якість зображення. Ідеальним вважається маркування, яке є повністю невидимим для людського ока, що особливо актуально для використання у високоякісних зображеннях, наприклад у медицині, поліграфії чи цифровому мистецтві [16; 17].

Складність реалізації також є суттєвим фактором, оскільки вона впливає на можливість впровадження методу у реальні системи. Вона охоплює як програмну реалізацію, так і алгоритмічну складність, потребу в зовнішніх модулях, а також можливість роботи у розподілених або апаратно обмежених середовищах [4; 13].

Обчислювальна ефективність відіграє ключову роль у застосуваннях, де потрібна обробка великої кількості зображень або функціонування в реальному часі. Вона враховує час, необхідний для вбудовування та виявлення знака, використання пам’яті та можливість реалізації на мобільних чи вбудованих пристроях [8; 15].

Окремо розглядається можливість сліпого виявлення, тобто здатність алгоритму розпізнавати водяний знак без необхідності у збереженні або доступі до оригінального зображення. Такий підхід є особливо важливим для відкритих або розподілених систем, де автентифікація має здійснюватися без зайвих залежностей [3; 5].

Ще одним критичним аспектом є адаптивність до типу зображень. Висока гнучкість у роботі з текстурованими, рівномірними, контрастними чи кольоровими зображеннями дозволяє значно розширити сферу застосування цифрового маркування в різних галузях [2; 10].

Останнім критерієм виступає широта сфер застосування. До них належать захист авторських прав, цифрова ідентифікація, інформаційна безпека, автентифікація контенту, використання в NFT або в цифрових паспортах об'єктів тощо [11; 18].

Таким чином, зазначені критерії забезпечують комплексне уявлення про потенціал кожної категорії методів – традиційних, гібридних та заснованих на глибокому навчанні. Вони дозволяють оцінити не лише технічні характеристики, але й практичну доцільність впровадження відповідних рішень у конкретних умовах.

У таблиці нижче узагальнено характеристики традиційних, гібридних та методів на основі глибокого навчання за критичними параметрами, що визначають їхню практичну цінність.

Аналіз показує, що хоча традиційні методи залишаються актуальними завдяки простоті, високій якості зображень після маркування та невеликим обчислювальним витратам, вони поступаються іншим за стійкістю до складних атак та адаптивністю. Гібридні методи демонструють найкращий баланс між прозорістю, стійкістю та універсальністю. Вони добре масштабуються та часто забезпечують підтримку сліпого виявлення, проте їх реалізація є більш складною. Методи на основі глибокого навчання

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

мають найвищий потенціал, особливо в контексті автоматизації, адаптивного вбудовування та стійкості до складних атак. Вони демонструють найвищу стійкість та гнучкість, проте вимагають значних ресурсів для навчання і розгортання. Їхні обмеження – висока обчислювальна складність та потреба в навчальних даних. Таким чином, вибір оптимального підходу залежить від конкретних вимог до захисту зображень, доступних обчислювальних ресурсів та умов використання.

Таблиця 1

Порівняльний аналіз методів цифрового водяного маркування

Критерій	Традиційні методи	Гібридні методи	Методи на основі глибокого навчання
Стійкість до атак	Середня. Добре працюють проти простих атак, вразливі до геометричних трансформацій	Висока. Забезпечують надійність до широкого спектра атак, включаючи фільтрацію, стиснення, масштабування	Дуже висока. Навчені мережі можуть зберігати знак навіть після фотозйомки або перекодування
Прозорість (якість зображення)	Висока (особливо в частотних методах)	Висока або середня (залежно від схеми комбінування)	Висока, але може залежати від архітектури моделі
Складність реалізації	Низька або середня. Реалізація не потребує значних обчислювальних ресурсів	Середня або висока. Потребують ретельного налаштування та комбінування алгоритмів	Висока. Необхідне навчання моделей, підбір гіперпараметрів та використання GPU
Обчислювальна ефективність	Висока. Швидка обробка навіть на слабкому обладнанні	Середня. Залежить від кількості етапів та складності перетворень	Залежить від моделі: може бути швидким, але навчання – ресурсоємне
Можливість сліпого виявлення (blind detection)	Часткова підтримка	Так, реалізується в багатьох схемах	Так. Один з основних плюсів DL-підходів
Адаптивність до типу зображень	Обмежена. Потребують ручного налаштування під кожний тип зображення	Краща адаптивність завдяки комбінуванню підходів	Висока. DL-моделі можуть навчатися на різних типах даних
Сфери застосування	Захист авторських прав, цифрові архіви	Судово-експертні системи, стійке маркування медіа, блокчейн	Кібербезпека, маркування в соцмережах, протидія фейкам, цифрова ідентифікація

Сфера цифрового водяного маркування динамічно розвивається під впливом новітніх технологій, зокрема штучного інтелекту, блокчейну та генеративних моделей. Попри значний прогрес, низка наукових і прикладних проблем залишається актуальною, а нові виклики постають у зв'язку з ускладненням цифрового середовища. Сучасні тенденції розвитку цифрового водяного маркування (ЦВМ) відкривають нові можливості, але водночас потребують переосмислення підходів, методів і архітектур.

Одним із ключових напрямів є застосування глибокого навчання як рушійної сили інтелектуального маркування. Алгоритми на основі DL забезпечують високий рівень стійкості до складних атак і здатні зберігати вбудований водяний знак навіть після суттєвих спотворень зображення [8; 14]. Проте висока ефективність таких методів супроводжується значними обчислювальними витратами, що ускладнює їх використання на мобільних або вбудованих пристроях. Окрім того, моделі DL мають високу складність, ризик переадаптації до специфічних даних і потребують ретельного навчання [8].

Іншою важливою проблемою стало протистояння генеративним моделям, зокрема diffusion-based генераторам і deepfake-контенту. Сучасні генератори здатні перегенерувати зображення настільки глибоко, що традиційні водяні знаки зникають. У відповідь на це досліджується маркування у латентному просторі моделей, яке дозволяє впроваджувати знаки, що зберігаються навіть після генеративних атак. Також розробляються підходи до модифікації самих генераторів з метою вбудованої автентифікації [10; 11].

У контексті децентралізованих технологій ЦВМ знаходить нове застосування в екосистемі Web3 та NFT. Тут цифрові знаки працюють разом із криптографічними сертифікатами для підтвердження авторства, права власності та валідації об'єктів через блокчейн [18]. Поєднання ЦВМ і NFT підвищує прозорість походження зображень, але водночас створює нові виклики, зокрема щодо масштабованості, сумісності з платформами та стійкості до повторного кодування або републікації.

Окрему увагу дослідників привертає етичний аспект цифрового маркування, особливо в чутливих сферах – медицині, юриспруденції, соціальних мережах. Виникає потреба у балансі між захистом і приватністю. Одним із інноваційних рішень у цьому напрямі є концепція revocable watermarking – маркування, яке можна відкликати, деактивувати або редагувати за ініціативою правовласника [9].

Цифрове водяне маркування дедалі ширше застосовується для автоматизованого виявлення порушень авторських прав. Сучасні гібридні системи, що поєднують традиційні методи з компонентами глибокого навчання, здатні виявляти маркування навіть у потоковому відео або на платформах з масовим обміном контентом (YouTube, Facebook, Instagram) [6]. Перспективним напрямом стає розвиток watermark-as-a-service (WaaS) – хмарних сервісів, інтегрованих із системами керування цифровим контентом.

Зростання роздільної здатності зображень і потреба в обробці в реальному часі висувають нові вимоги до обчислювальної ефективності. Традиційні складні DL-архітектури замінюються спрощеними моделями, wavelet-перетвореннями, хаотичними функціями та методами енергоефективного аналізу. Технології TinyML та Edge AI дозволяють реалізовувати ЦВМ на пристроях із обмеженими ресурсами, зберігаючи належну якість та стійкість [12].

Таким чином, подальший розвиток цифрового водяного маркування відбуватиметься у напрямі збалансованої інтеграції новітніх технологій, таких як DL, blockchain, генеративні моделі та edge-computing.

Підсумовуючи викладене, можна виокремити низку ключових викликів, що наразі стоять перед дослідницькою спільнотою у сфері ЦВМ. Однією з найбільш гострих проблем залишається відсутність уніфікованих стандартів. Недостатня узгодженість форматів, метрик якості та процедур верифікації ускладнює інтеграцію маркування в міжплатформенні системи та юридичні середовища.

Крім того, зростає потреба у забезпеченні стійкості до новітніх типів атак, зокрема до deepfake, адаптивних фільтрів та AI-реставрації. Незважаючи на досягнення гібридних та DL-підходів, ці загрози становлять серйозну перешкоду для гарантування автентичності цифрового контенту. Ще одним невирішеним питанням залишається баланс між прозорістю та стійкістю. Досягнення високих показників обох характеристик без втрати візуальної якості зображення є технічно складним завданням, особливо у випадку високодинамічного або деталізованого контенту.

Значною проблемою також є обмеження обчислювальних ресурсів. Сучасні методи на основі глибокого навчання демонструють високу ефективність, проте вимагають значних обчислювальних потужностей для тренування і розгортання, що обмежує їх використання в енергоефективних або вбудованих системах. Крім того, нові моделі штучного інтелекту вже здатні виконувати «очищення» зображень від водяних знаків, включаючи навіть складні маркування. Це формує нагальну потребу в розробці рішень, здатних протистояти нейромережевим методам фільтрації.

На тлі вказаних викликів можна окреслити перспективні напрями подальшого розвитку. По-перше, інтеграція цифрового маркування з криптографічними протоколами та блокчейн-технологіями дозволяє забезпечити трасованість авторства і фіксацію змін контенту. По-друге, перспективними є адаптивні системи, засновані на самонавчанні, здатні реагувати на зміну типів атак та умов функціонування в режимі реального часу.

Ще один важливий вектор розвитку пов'язаний із поширенням ЦВМ на мультимодальні дані. Сучасні дослідження поступово виходять за межі маркування лише зображень, зосереджуючись також на відео, аудіо та 3D-контенті, що потребує універсальних алгоритмів. У правовому аспекті зростає значення цифрових водяних знаків як доказового інструмента, що актуалізує потребу в їх формальній валідації, експертній оцінці та правовому визнанні.

Нарешті, розвиток концепції explainable AI (XAI) у сфері DL-маркування сприяє підвищенню прозорості роботи глибоких моделей. Це, у свою чергу, дозволяє краще оцінювати ризики, пояснювати процеси вбудовування та виявлення маркування, а також формувати довіру до таких технологій з боку користувачів і регуляторів.

Висновки. У цій статті було проведено систематизацію сучасних методів цифрового водяного маркування зображень, здійснено їх порівняльний аналіз та окреслено актуальні тенденції розвитку. На основі вивчених джерел можна зробити такі узагальнення.

Цифрове водяне маркування є ключовим інструментом захисту цифрових зображень, оскільки забезпечує ідентифікацію авторства, верифікацію автентичності та простеження джерел поширення контенту. Методи цифрового водяного маркування за своїми характеристиками та підходами поділяються на традиційні, гібридні та засновані на глибокому навчанні.

Традиційні методи працюють у просторі або частотній області, тоді як гібридні поєднують переваги різних підходів, демонструючи баланс між прозорістю, стійкістю та обчислювальною ефективністю,

ISSN 2786-5460 (Print), ISSN 2786-5479 (Online)

хоча й залишаються чутливими до складних атак. У свою чергу, методи на базі глибокого навчання відкривають нові можливості, зокрема для маркування в умовах відсутності оригіналу зображення (blind watermarking), проте вимагають значних ресурсів і поки що не мають загальноприйнятих стандартів.

У зв'язку з цим подальші дослідження доцільно спрямовувати на розробку адаптивних, масштабованих і стійких рішень, зокрема із використанням блокчейн- та криптографічних технологій, а також на правову стандартизацію застосування цифрових водяних знаків у доказових процесах.

Таким чином, цифрове водяне маркування продовжує залишатися активною та стратегічно важливою сферою наукових досліджень, із суттєвим потенціалом до практичного застосування в умовах цифрової трансформації суспільства.

Список використаних джерел:

1. Гавриленко В. О. Дослідження методів побудови цифрових водяних знаків для захисту зображень. 2016. URL: https://dglib.nubip.edu.ua/handle/123456789/1868.

2. Лозинський С. С. Формування цифрового водяного знаку для захисту авторських прав на графічні об'єкти. *Наукові праці НУХТ*, 2020. URL: https://openarchive.nure.ua/handle/document/30248.

3. Сімонов С. О., Іванов С. М., Романенко О. В. Побудова цифрового водяного знака з використанням хаотичних перетворень. *Східно-Європейський журнал передових технологій*. 2021. № 6/9 (114), с. 6–16. DOI: 10.15587/1729-4061.2021.246641.

4. Чекан І. І., Піскорський В. В. Метод вбудовування водяного знака у зображення на основі логістичного хаотичного відображення. *Інформація і керування*. 2021. № 3, с. 121–127. DOI: 10.20998/2522-9052.2021.3.15.

5. A. F. Eldaoushy et al. Efficient Hybrid Digital Image Watermarking. Journal of Optics, 2023. DOI: 10.1007/s12596-023-01144-7.

6. Al-Dabbas H. M., Azeez R. A., Ali A. E. Digital Watermarking, Methodology, Techniques, and Attacks: A Review. *Iraqi Journal of Science*. 2023. Vol. 64, No. 8, pp. 4146–4160. DOI: 10.24996/ijs.2023.64.8.37.

7. Al-khafaji H., Al-Himyari B. A., Hussain N. F. Techniques for Digital Watermarking in Images: A Review. *Journal of University of Babylon for Pure and Applied Sciences*. 2024. DOI: 10.29196/ycdrt588.

8. Ben Jabra, S., Ben Farah, M. Deep Learning-Based Watermarking Techniques Challenges: A Review of Current and Future Trends. *Circuits, Systems, and Signal Processing*. 2024. 43, 4339–4368. DOI: 10.1007/s00034-024-02651-z.

9. Gaur S., Barthwal V. An Extensive Analysis of Digital Image Watermarking Techniques International. *Journal of Intelligent Systems and Applications in Engineering*. 2024. 12(1), 121–145. DOI: 10.31201/ijisae.2024.12145.

10. Mareen H., Antchougov L., Delvaux J., et al. Blind Deep-Learning-Based Image Watermarking Robust Against Geometric Transformations. arXiv preprint, 2024. 12 c. URL: https://arxiv.org/abs/2402.09062.

11. Padhi S. K., Ali S. S. DLOVE: A New Security Evaluation Tool for Deep Learning Based Watermarking TechniquesarXiv preprint, 2024. DOI: 10.48550/arXiv.2407.06552.

12. Rani S., Kaur P. Optimized and Secure Digital Image Watermarking Technique Using Henon Mapping in Redundant Domain. *Multimedia Tools and Applications*. 2024. 83, 81151–81166. DOI: 10.1007/s11042-024-18643-9.

13. Wadhera S., Kamra D., Bedi P., et al. A Comprehensive Review on Digital Image Watermarking. arXiv preprint, 2022. URL: https://arxiv.org/abs/2207.06909.

14. Wang X., Zhang Y., Li H., et al. A Brief, In-Depth Survey of Deep Learning-Based Image Watermarking. *Applied Sciences*, 2023, 13(21), 11852. DOI: 10.3390/app132111852.

15. Wang Z., Byrnes O., Bansal R., et al. Data Hiding with Deep Learning: A Survey Unifying Digital Watermarking and Steganography. arXiv preprint, 2021. URL: https://arxiv.org/abs/2107.09287.

16. Xie Y., Wang Y., Ma M. Design of a Hybrid Digital Watermarking Algorithm with High Robustness. *Journal of Web Engineering*. 2023. DOI: 10.13052/jwe1540-9589.19567.

17. Zhang J., Yu J., Ma J., Wang Y., Jiang H., Wu Z. A Robust Image Watermarking Method Based on Deep Neural Networks. arXiv preprint, 2020. 10 c. URL: https://arxiv.org/abs/2007.02460.

18. Zhao, L., Gui, X., Shao, Y., Dai, H. Survey on Multipurpose Digital Image Watermarking. *Journal of Computer-Aided Design & Computer Graphics*, 2024, 36(2), 195–222. DOI: 10.3724/SP.J.1089.2024.20078.

Дата надходження статті: 17.06.2025
Дата прийняття статті: 23.06.2025
Опубліковано: 23.09.2025