Овчинников Микола Юрійович, асистент кафедри кібербезпеки, Національний університет «Одеська юридична академія», м. Одеса, Україна, https://orcid.org/0009-0009-8221-7193

Ovchinnikov Mykola Yuriyovych, Assistant at the Department of Cybersecurity, National University "Odesa Law Academy", Odessa, Ukraine, https://orcid.org/0009-0009-8221-7193

ДОКАЗООРІЄНТОВАНИЙ ЗАХИСТ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА МУЛЬТИМЕДІЙНІ ДАНІ В ЕПОХУ КОНТЕНТУ, ЗГЕНЕРОВАНОГО ШІ

EVIDENCE-CENTRIC INTELLECTUAL PROPERTY PROTECTION FOR MULTIMEDIA DATA IN THE ERA OF AI-GENERATED CONTENT

Анотація. Стрімке поширення генеративного штучного інтелекту та безшовне розповсюдження контенту в соціальних мережах перетворили повторне використання мультимедіа на високошвидкісний, кросплатформний процес, у якому захищений твір може бути скопійований, відредагований, перекодований і повторно опублікований за лічені хвилини. За таких умов однофакторний захист (наприклад, лише водяні знаки або лише хешування) часто є недостатнім, оскільки зловмисники можуть скористатися відомими слабкими місцями будь-якого окремого сигналу. У статті запропоновано доказоорієнтований підхід до захисту прав інтелектуальної власності на мультимедійні дані, який трактує підтвердження авторства як об’єднання різнорідних доказів: робастних водяних знаків, контентних відбитків/перцептивних хешів,

криміналістичних слідів та незаперечного часового «якоря» в незмінному журналі (append-only) або блокчейні. Підхід узгоджується з програмами цифрової трансформації, де організаціям потрібні аудитовані, масштабовані й автоматизовані процеси, інтегровані в інформаційні системи, а не набір ізольованих алгоритмів. Формалізовано практичну модель загроз, релевантну платформним пайплайнам (стиснення, зміна розміру, кадрування, повторне кодування, накладання графіки та ШІ-редагування), і запропоновано конвеєр, що формує доказовий звіт із детекторами, метаданими походження та відтворюваними артефактами перевірки. Дві структуровані таблиці узагальнюють (I) механізми доказування та типові режими відмови, а також (II) поширені атаки й рекомендовані контрзаходи. Основний внесок полягає в системному дизайні, який можна реалізувати легкими компонентами та який підтримує як технічну оцінку, так і юридичне обґрунтування завдяки прозорим, повторюваним і простежуваним крокам верифікації. Запропонована модель може слугувати еталонною архітектурою для університетських і промислових впроваджень сервісів захисту мультимедійних прав та основою для міждисциплінарних досліджень у сфері ШІ, кібербезпеки й інформаційних систем.

Ключові слова: робастне водяне маркування, мультимедіа, мультимедійна криміналістика, перцептивне хешування, ШІ, виявлення копій, дипфейки, блокчейн, інтелектуальна власність.

Abstract

The rapid diffusion of generative artificial intelligence and the seamless distribution of content on social media have turned multimedia reuse into a high-velocity, cross-platform process in which a protected work can be copied, edited, re-encoded, and republished within minutes. Under such conditions, single-mechanism protection (e.g., only watermarking or only hashing) is often

insufficient, because adversaries can exploit the known weaknesses of any individual signal. This paper proposes an evidence-centric approach to protecting intellectual property rights in multimedia data, treating authorship verification as the fusion of heterogeneous proofs: robust watermarks, content fingerprints/perceptual hashes, forensic traces, and a tamper-evident time anchor in an append-only log or blockchain. The approach aligns with digital transformation programs, where organizations require auditable, scalable, and automated workflows integrated into information systems rather than isolated algorithms. We formalize a practical threat model relevant to platform pipelines (compression, resizing, cropping, re-encoding, graphic overlays, and AI-based editing) and propose a pipeline that produces an evidentiary report combining detector outputs, provenance metadata, and reproducible verification artifacts. Two structured tables summarize (I) evidence mechanisms and typical failure modes and (II) common attacks and recommended countermeasures. The main contribution is a system-level design implementable with lightweight components, supporting both technical assessment and legal reasoning through transparent, repeatable, and traceable verification steps. The proposed model can serve as a reference architecture for academic and industrial deployments of multimedia rights protection services and as a foundation for interdisciplinary research in AI, cybersecurity, and information systems.

Keywords: robust watermarking, multimedia, multimedia forensics, perceptual hashing, copy detection, AI, deepfake, blockchain, intellectual property, evidence fusion.

Постановка проблеми. Цифрова трансформація дедалі більше спирається на багаті медіадані – фотографії продуктів, навчальні відео, освітні матеріали та контент, створений користувачами – як на ключовий актив. Водночас онлайн-середовище підсилює несанкціоноване повторне

використання: перепублікація відбувається між платформами з автоматичним транскодуванням, адаптацією якості та агресивним стисненням. Традиційні підходи до реагування часто є повільними, платформозалежними й нерідко не забезпечують чітких технічних доказів, здатних витримати спір або судовий розгляд [1, с. 1673]. Проблема загострилася через робочі процеси генеративного ШІ. На практиці контент можна злегка модифікувати (перенесення стилю, інпейнтинг, заміна фону, маніпуляції з обличчям), щоб зменшити схожість з оригіналом, зберігаючи семантичну ідентичність. Генерація дипфейків і синтетичні правки ускладнюють традиційне «точне» виявлення збігів і роблять походження невизначеним, що підвищує потребу в робастних, пояснюваних і багатодоказових процесах верифікації [2, с. 6259]. За таких умов сучасна система захисту прав має задовольняти чотири системні вимоги: (I) робастність до типових платформних перетворень (стиснення, зміна розміру, повторне кодування), (II) пошук у масштабі (індексація та виявлення кандидатів-копій), (III) криміналістична пояснюваність, корисна для експертного аналізу, та (IV) аудитованість створення, зберігання і перевірки доказів. Огляди водяного маркування та приховування інформації підкреслюють, що жодна окрема техніка не є універсально стійкою, особливо за умов навмисної протидії; отже, практичні впровадження потребують комбінованого підходу [3, с. 1079].

Аналіз останніх досліджень і публікацій. Робастне водяне маркування залишається класичним механізмом доведення прав шляхом вбудовування секретного сигналу в носій. Моделі розширеного спектра формують основу, де детекція зводиться до кореляційного тесту за наявності спотворень [1, с. 1673]. У ширшому контексті література з приховування інформації відмежовує водяні знаки від стеганографії, описує моделі атак і акцентує компроміс між непомітністю, ємністю та робастністю. Показано, що безпека

може руйнуватися, коли атакувальник здатний адаптивно опитувати систему або оцінювати закономірності вбудовування [4, с. 474].

Комплементарний напрям – контентне виявлення копій і перцептивне хешування. Замість вбудовування система обчислює компактні дескриптори контенту та виконує пошук близьких дублікатів. Ранні підходи демонструють, що низьковимірні представлення з DCT-ознаками забезпечують практичну детекцію копій і доповнюють водяні знаки, коли попереднє вбудовування неможливе [5, с. 169]. Мультимедійна криміналістика додає ще один шар доказів, використовуючи сліди камери або кодека, шумові патерни та невідповідності, що виникають під час монтажу чи повторного кодування. Наприклад, підхід noiseprint формує відбиток моделі камери, придушуючи сценовий контент, і підтримує локалізацію маніпуляцій [6, с. 144].

Глибинне навчання стало центральним як для захисту, так і для атак. Огляди водяного маркування на основі deep learning вказують, що навчувані вбудовувачі та екстрактори можуть підвищувати робастність, але також створюють нові поверхні атаки (адверсаріальні приклади, викрадення моделі тощо) [7, с. 100662]. Нарешті, блокчейн і незмінні журнали розглядаються як механізм таймстемпінгу доказів і забезпечення незаперечності. У системах керування правами блокчейн застосовують для зберігання правових метаданих та «якоріння» відбитків або комітментів водяних знаків, що покращує аудитованість, але не замінює потреби в робастних сигналах ідентифікації [8, с. 9735].

Мета статті. Метою статті є запропонувати та описати доказоорієнтовану архітектуру захисту прав на мультимедійні дані в екосистемах, де контент швидко поширюється та модифікується за допомогою ШІ, а також сформулювати практичні контрзаходи, що поєднують робастні водяні знаки, виявлення на основі відбитків/хешів,

криміналістичну валідацію та незмінне часове «якоріння». Акцент зроблено на системному дизайні й придатності до впровадження в інформаційних системах, а не на розробці одного нового алгоритму вбудовування.

Виклад результатів. У цьому розділі представлено запропоновану доказоорієнтовану архітектуру захисту прав на мультимедійні дані: спочатку описано конвеєр верифікації та його ключові етапи, далі — сформульовано модель загроз для сучасних платформ і обґрунтовано роль робастних водяних знаків як первинного юридично значущого доказу. Також наведено узагальнення механізмів, типових атак і практичних контрзаходів, що забезпечують відтворюваність і простежуваність доказування.

Доказоорієнтований конвеєр (pipeline). Запропонований конвеєр трактує кожен випадок верифікації як відтворюваний експеримент, що формує структурований доказовий звіт. Ключове рішення — розділити: (а) пошук (виявлення кандидатів-копій), (б) перевірку (тестування гіпотез водяного знаку/схожості), (в) пояснення (криміналістичні перевірки та звітування). Таке розділення підтримує масштабування та робить генерування доказів повторюваним у часі й між інструментами (див. рис. 1) [9, с. 309].

Модель загроз для сучасних платформ. Платформні пайплайни застосовують перетворення, нейтральні для користувачів, але ворожі до крихких сигналів. Найпоширеніші: JPEG-рекомпресія, зміна роздільної здатності, кадрування та повторне кодування відео. До просунутих загроз належать накладання графіки (логотипи, субтитри), колюзійні атаки (усереднення кількох маркованих копій) і «оракульні» атаки, коли зловмисник може багаторазово опитувати публічний верифікатор [10, с. 1062].

Робастні водяні знаки як первинний юридично значущий доказ. Робастне маркування забезпечує доказ прав шляхом вбудовування

ключ-залежного сигналу в перцептивно незначущі компоненти носія. Класичні підходи моделюють екстракцію як кореляційний тест, де оцінений водяний знак порівнюють з оригінальною ключовою послідовністю.



Рисунок 1. Доказоорієнтований конвеєр захисту прав на мультимедіа (Джерело: розроблено автором).

Нормалізована кореляція (NC), визначена у формулі (1), широко використовується для детекції та звітування про впевненість у доказовому контексті [1, с. 1676].

$$NC = (\, sum_i\ w_i * w_hat_i \,) \,/\, sqrt(\, (sum_i\ w_i\text{^}2) * (sum_i\ w_hat_i\text{^}2) \,) \quad (1)$$

Нормалізована кореляція (NC) для детекції водяного знаку (Джерело:[1]).

Ємність, непомітність і обмеження за ROI. У багатьох промислових і медичних сценаріях важливо зберегти діагностично значущі області (ROI) без спотворень, вбудовуючи доказ у інші ділянки. Багато-ROI маркування дозволяє зберегти ROI практично незмінними, а інші області використати для вбудовування, що підвищує прийнятність у практиці [11, с. 648].

Відбитки/перцептивні хеші для пошуку в масштабі. Водяні знаки потребують попереднього вбудовування; отже, організаціям потрібні механізми виявлення для «історичного» контенту та для платформ, де вбудовування неможливе. Контентне виявлення копій формує компактні сигнатури й виконує приблизний пошук, працюючи як фронт-енд фільтр перед поглибленою верифікацією [5, с. 169].

Криміналістична валідація та протидія контркриміналістиці. Локалізація підробок і оцінка автентичності можуть спиратися на пристроєві відбитки та аналіз шумових залишків. Noiseprint-відбитки забезпечують відносно стабільний патерн, корисний для виявлення невідповідностей, які виникають через склеювання, повторний рендеринг або перекодування [6, с. 146].

ШІ-генеровані правки та дипфейки як фактор ризику. Огляди генерації й детекції дипфейків показують, що маніпуляції можуть зберігати семантичну ідентичність, змінюючи піксельні статистики; тому пошук схожості доцільно виконувати як на перцептивних, так і на глибинних ознаках, а верифікацію доповнювати пояснюваними криміналістичними індикаторами. Детекція дипфейків еволюціонує через зсуви датасетів і адверсаріальну адаптацію [12, с. 607].

Водяне маркування поза мультимедіа: захист моделей ШІ. Логіка доведення прав переноситься на глибинні нейронні мережі, що

використовуються в цифрових сервісах. Роботи з водяними знаками для DNN демонструють концепції black-box верифікації, коли право власності тестується через спеціально сформовані запити без доступу до параметрів [13, с. 1]. Оглядові праці пропонують таксономії водяних знаків DNN і пов'язують методи з класичною теорією, підкреслюючи робастність до fine-tuning, обрізання (pruning) та вилучення моделі [14, с. 171].

Часове «якоріння» та ланцюг збереження доказів (chain-of-custody). Практичний доказовий процес має фіксувати, що саме було перевірено, коли, з якими параметрами та які артефакти сформовано. Блокчейн або незмінні журнали можуть «якорити» відбитки/комітменти і метадані кейсу, забезпечуючи захист від підміни та незаперечність у часі. У контексті мультимедійної освіти блокчейн-DRM прототипи демонструють, як розподілено управляти правовими метаданими й записами перевірок [8, с. 9738]. Сучасні дослідження також пропонують надійний захист авторських прав для зображень із використанням блокчейна, підкреслюючи, що «якоріння» працює найкраще разом із сильними сигналами ідентифікації [15, с. 222].

Відеозахист і перцептивні хеші в незмінних журналах. Відеоспецифічні атаки (видалення кадрів, повторне кодування, часові деформації) вимагають стратегій ключових кадрів і синхронізації. Гібридні системи, що поєднують водяні знаки, перцептивні хеші та блокчейн-зберігання, підвищують верифікацію, зменшуючи обсяги даних завдяки «якорінню» компактних записів замість сирого відео [16, с. 8-11].

Порівняльний огляд механізмів доказування. Таблиця 1 узагальнює, як водяні знаки, хеші/відбитки, криміналістика та «якоріння» доповнюють одне одного. Це допомагає в системному проєктуванні та запобігає надмірній залежності від одного сигналу [17, с. 1064].

Таблиця 1

Механізми доказування для захисту прав на мультимедіа (Джерело: розроблено автором за [1, 3, 9]).

Механізм	Основна мета	Сильні сторони	Типові слабкі місця
Робастне водяне маркування	Доведення прав	Стійкість до багатьох перетворень; корисне для атрибуції	Може «зламатися» при сильних геометричних змінах; потрібне керування ключами
Крихке/напівкрихке маркування	Цілісність і виявлення підробок	Чутливе до змін; можливе локалізування маніпуляцій	Погано переносить рекомпресію; ризик хибних спрацювань
Відбитки/перцептивні хеші	Пошук і трекінг	Швидка індексація; працює без попереднього вбудовування	Потрібне налаштування порогів; ризик пропуску часткового використання
Мультимедійна криміналістика	Автентичність і пояснення	Не потребує вбудовування; може локалізувати підробку	Ймовірнісний характер; вразливість до контркриміналістики
Часове «якоріння» (ledger)	Таймстемп і аудитованість	Незаперечність; підтримка chain-of-custody	Самостійно не ідентифікує контент; питання приватності/управління

Відповідність «атака–контроль». Таблиця 2 відображає типові перетворення та їхній вплив на докази, а також пропонує контрзаходи. Важливо, що атакувальники часто експлуатують передбачувані платформні операції, а не «екзотичні» криптоатаки; тому інженерна реалістичність є критичною [10, с. 1066].

Таблиця 2

Поширені атаки та рекомендовані контрзаходи (Джерело: розроблено автором за [3, 7, 12]).

Атака/перетворення	Вплив на доказ	Рекомендовані контрзаходи
JPEG / платформна рекомпресія	Послаблює водяний знак; змінює дескриптори	Вбудовування в робастному домені; калібрування під пайплайн; об'єднання доказів
Зміна розміру / пропорцій	Десинхронізує водяний знак; зсуває ознаки	Шаблони синхронізації; багатомасштабні відбитки; ключові кадри (відео)
Кадрування / часткове використання	Вилучає частини з вбудовуванням; фрагментарне копіювання	Надлишкове вбудовування; регіональна індексація; локальні ознаки
Повторне кодування відео / зміна FPS	Часовий дрейф; зміна ключових кадрів	Виділення ключових кадрів; просторово-часові сигнатури; перевірка сегментів
Накладання графіки (лого/субтитри)	Оклюзія сигналів та ознак	Вбудовування в кількох смугах; оклюзійно-стійке зіставлення; криміналістика накладень
Генеративні правки / інпейнтинг	Може видаляти слабкі мітки; зберігає семантику	Пошук за глибинними ознаками; робастний водяний знак; криміналістичні перевірки
Колюзія / усереднення	Знижує детектованість	Персональні відбитки; колюзійно-стійкі коди; ротація ключів
Оракульні атаки на верифікатор	Адаптивне видалення через запити	Rate limiting; автентифікація розслідувань; журнали аудиту

Нотатки щодо реалізації в інформаційних системах. Легка реалізація може зберігати відбитки й метадані кейсів у реляційній БД, мати шар моніторингу для періодичних веб-сканувань і надавати API верифікації для

дослідників. Система повинна фіксувати параметри (ключі, пороги, версії ПЗ) для відтворюваності. Огляд інтелектуальної мультимедійної криміналістики для IoT підкреслює необхідність врахування адверсаріального середовища та довгострокової підтримуваності [18, с. 109451].

Управління та стандартизація. Генерування доказів має відповідати політикам організації та обмеженням приватності. Метадані прав повинні бути узгодженими й повними: погана якість метаданих робить «якоріння» малоефективним навіть за криптографічної коректності. Принципи проєктування blockchain-DRM наголошують на прозорих ліцензійних структурах і надійних метаданих прав як на практичній вимозі [19, с. 5].

Подальші напрями. Огляди фіксують зростання використання глибинних моделей у водяному маркуванні та стегоаналізі паралельно з ростом адверсаріальних атак. Комплексний огляд deep learning-стегоаналізу демонструє деградацію моделей при нових стратегіях вбудовування й адверсаріальних збуреннях, що підсилює аргумент на користь об'єднання доказів [20, с. 100353].

Міждоменне маркування: мультимедіа та моделі. У міру поширення водяних знаків для захисту моделей ШІ межа між «доказами контенту» та «доказами сервісу» розмивається. Методи зворотного приховування (reversible hiding) для DNN можуть підтримувати динамічні претензії на право власності за перетворень [21, с. 861].

Практичний порядок денний досліджень. Доцільно пріоритезувати: (I) бенчмарки робастності, узгоджені з реальними платформними пайплайнами, (II) шаблони доказових звітів, що містять пояснювані метрики, та (III) системні оцінки з урахуванням зберігання, затримок пошуку й часу прийняття рішень. Огляд водяних знаків у середовищах deep learning підкреслює необхідність комплексного тестування робастності під різними

атаками та прозорого звітування щодо умов і витрат експериментів [22, с. 031804-14].

Інституційний погляд. З позиції інформаційних систем описаний конвеєр доцільно реалізувати як модульний сервіс: інгест (ingestion), вбудовування (опційно), індексація, моніторинг, верифікація, звітування та аудит. Така декомпозиція підтримує поетапне впровадження і відповідає дорожнім картам цифрової трансформації в частині кібербезпеки та IP-комплаєнсу [17, с. 1070].

Висновки. У статті запропоновано доказоорієнтовану архітектуру захисту прав інтелектуальної власності на мультимедійні дані, придатну для контекстів цифрової трансформації. Ключова ідея полягає в трактуванні підтвердження прав як об'єднання різнорідних доказів: робастного водяного маркування для прямого сигналу належності, відбитків/перцептивних хешів для масштабованого пошуку, криміналістики для пояснення й аналізу підробок, а також «якоріння» в незмінному журналі для аудитованості та незаперечності.

Запропонований конвеєр є практичним: він розділяє пошук і перевірку, фіксує відтворювані параметри та формує структуровані доказові звіти. Діаграма, таблиці та зіставлення атак із контролями узагальнюють механізми й контрзаходи в реалістичній моделі загроз, включно з ШІ-редагуванням. Подальші дослідження доцільно спрямувати на стандартизоване тестування під реальні платформні пайплайни, уніфікацію шаблонів доказових звітів та приватність-збережне управління походженням із «якорінням» у реєстрах.

Список використаних джерел

1. Cox I. J., Kilian J., Leighton F. T., Shamoon T. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*. 1997. Vol. 6, No. 12. P. 1673–1687. DOI: https://doi.org/10.1109/83.650120.

2. Zhang T. Deepfake generation and detection, a survey. *Multimedia Tools and Applications*. 2022. Vol. 81, No. 5. P. 6259–6276. DOI: https://doi.org/10.1007/s11042-021-11733-y.

3. Hartung F., Kutter M. Multimedia watermarking techniques. *Proceedings of the IEEE*. 1999. Vol. 87, No. 7. P. 1079–1107.DOI: https://doi.org/10.1109/5.771066.

4. Anderson R. J., Petitcolas F. A. P. On the limits of steganography. *IEEE Journal on Selected Areas in Communications*. 1998. Vol. 16, No. 4. P. 474–481. DOI: https://doi.org/10.1109/49.668971.

5. Kim C. Content-based image copy detection. *Signal Processing: Image Communication*. 2003. Vol. 18, No. 3. P. 169–184. DOI: https://doi.org/10.1016/S0923-5965(02)00130-3.

6. Cozzolino D., Verdoliva L. Noiseprint: A CNN-Based Camera Model Fingerprint. *IEEE Transactions on Information Forensics and Security*. 2020. Vol. 15. P. 144–159. DOI: https://doi.org/10.1109/TIFS.2019.2916364.

7. Hosny K. M., Magdi A., ElKomy O., Hamza H. M. Digital image watermarking using deep learning: A survey. *Computer Science Review*. 2024. Vol. 53. Art. 100662. DOI: https://doi.org/10.1016/j.cosrev.2024.100662.

8. Guo J., Li C., Zhang G., Sun Y., Bie R. Blockchain-enabled digital rights management for multimedia resources of online education. *Multimedia Tools and Applications*. 2020. Vol. 79. P. 9735–9755. DOI: https://doi.org/10.1007/s11042-019-08059-1.

9. Amerini I., Anagnostopoulos A., Maiano L., Ricciardi Celsi L. Deep Learning for Multimedia Forensics. *Foundations and Trends in Computer*

Graphics and Vision. 2021. Vol. 12, No. 4. P. 309–457. DOI: https://doi.org/10.1561/0600000096.

10. Petitcolas F. A. P., Anderson R. J., Kuhn M. G. Information hiding - a survey. *Proceedings of the IEEE*. 1999. Vol. 87, No. 7. P. 1062–1078. DOI: https://doi.org/10.1109/5.771065.

11. Shih F. Y., Zhong X. High-capacity multiple regions of interest watermarking for medical images. *Information Sciences*. 2016. Vol. 367–368. P. 648–659. DOI: https://doi.org/10.1016/j.ins.2016.07.015.

12. Yu P., Xia Z., Fei J., Lu Y. A survey on deepfake video detection. *IET Biometrics*. 2021. Vol. 10, No. 6. P. 607–624. DOI: https://doi.org/10.1049/bme2.12031.

13. Zhang J., Gu Z., Jang J., Wu H. et al. Protecting Intellectual Property of Deep Neural Networks with Watermarking. *Proceedings of the 2018 on Asia Conference on Computer and Communications Security (ASIA CCS '18)*. 2018. DOI: https://doi.org/10.1145/3196494.3196550.

14. Li Y., Wang H., Barni M. A survey of Deep Neural Network watermarking techniques. *Neurocomputing*. 2021. Vol. 461. P. 171–193. DOI: https://doi.org/10.1016/j.neucom.2021.07.051.

15. Xiao X., He X., Zhang Y., Dong X. et al. Blockchain-based reliable image copyright protection. *IET Blockchain*. 2023. Vol. 3, No. 4. P. 222–237. DOI: https://doi.org/10.1049/blc2.12027.

16. Darwish S. M., Abu-Deif M. M., Elkaffas S. M. Blockchain for video watermarking: An enhanced copyright protection approach for video forensics based on perceptual hash function. *PLOS ONE*. 2024. Vol. 19, No. 10. Art. e0308451. DOI: https://doi.org/10.1371/journal.pone.0308451.

17. Swanson M. D., Kobayashi M., Tewfik A. H. Multimedia data-embedding and watermarking technologies. *Proceedings of the IEEE*. 1998. Vol. 86, No. 6. P. 1064–1087. DOI: https://doi.org/10.1109/5.687830.

18. Ding W., Abdel-Basset M., Ali A. M., Moustafa N. A survey of intelligent multimedia forensics for internet of things communications. *Engineering Applications of Artificial Intelligence*. 2024. Vol. 138. Art. 109451. DOI: https://doi.org/10.1016/j.engappai.2024.109451.

19. Ciriello R. F., Torbensen A. C. G., Hansen M. R. P., Muller-Bloch C. Blockchain-based digital rights management systems. *Electronic Markets*. 2023. Vol. 33. Art. 5. DOI: https://doi.org/10.1007/s12525-023-00628-5.

20. Ntivuguruzwa J. D. L. C., Ahmad T., Han F. Comprehensive survey on image steganalysis using deep learning. *Array*. 2024. Vol. 22. Art. 100353. DOI: https://doi.org/10.1016/j.array.2024.100353.

21. Wang L., Song Y., Xia D. Deep neural network watermarking based on a reversible image hiding network. *Pattern Analysis and Applications*. 2023. Vol. 26, No. 3. P. 861–874. DOI: https://doi.org/10.1007/s10044-023-01140-4.

22. Singh H. K., Singh A. K. Comprehensive review of watermarking techniques in deep-learning environments. *Journal of Electronic Imaging*. 2023. Vol. 32, No. 3. Art. 031804. DOI: https://doi.org/10.1117/1.JEI.32.3.031804.

References

1. Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6(12), 1673-1687. https://doi.org/10.1109/83.650120

2. Zhang, T. (2022). Deepfake generation and detection, a survey. Multimedia Tools and Applications, 81(5), 6259-6276. https://doi.org/10.1007/s11042-021-11733-y

3. Hartung, F., & Kutter, M. (1999). Multimedia watermarking techniques. Proceedings of the IEEE, 87(7), 1079-1107. https://doi.org/10.1109/5.771066

4. Anderson, R. J., & Petitcolas, F. A. P. (1998). On the limits of steganography. IEEE Journal on Selected Areas in Communications, 16(4), 474-481. https://doi.org/10.1109/49.668971

5. Kim, C. (2003). Content-based image copy detection. Signal Processing: Image Communication, 18(3), 169-184. https://doi.org/10.1016/S0923-5965(02)00130-3

6. Cozzolino, D., & Verdoliva, L. (2020). Noiseprint: A CNN-Based Camera Model Fingerprint. IEEE Transactions on Information Forensics and Security, 15, 144-159. https://doi.org/10.1109/TIFS.2019.2916364

7. Hosny, K. M., Magdi, A., ElKomy, O., & Hamza, H. M. (2024). Digital image watermarking using deep learning: A survey. Computer Science Review, 53, 100662. https://doi.org/10.1016/j.cosrev.2024.100662

8. Guo, J., Li, C., Zhang, G., Sun, Y., & Bie, R. (2020). Blockchain-enabled digital rights management for multimedia resources of online education. Multimedia Tools and Applications, 79, 9735-9755. https://doi.org/10.1007/s11042-019-08059-1

9. Amerini, I., Anagnostopoulos, A., Maiano, L., & Ricciardi Celsi, L. (2021). Deep Learning for Multimedia Forensics. Foundations and Trends in Computer Graphics and Vision, 12(4), 309-457. https://doi.org/10.1561/0600000096

10. Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding - a survey. Proceedings of the IEEE, 87(7), 1062-1078. https://doi.org/10.1109/5.771065

11. Shih, F. Y., & Zhong, X. (2016). High-capacity multiple regions of interest watermarking for medical images. Information Sciences, 367-368, 648-659. https://doi.org/10.1016/j.ins.2016.07.015

12. Yu, P., Xia, Z., Fei, J., & Lu, Y. (2021). A survey on deepfake video detection. IET Biometrics, 10(6), 607-624. https://doi.org/10.1049/bme2.12031

13. Zhang, J., Gu, Z., Jang, J., Wu, H., Stoecklin, M. P., Huang, H., & Molloy, I. (2018). Protecting Intellectual Property of Deep Neural Networks with Watermarking. Proceedings of the 2018 on Asia Conference on Computer and Communications Security (ASIA CCS '18). https://doi.org/10.1145/3196494.3196550

14. Li, Y., Wang, H., & Barni, M. (2021). A survey of Deep Neural Network watermarking techniques. Neurocomputing, 461, 171-193. https://doi.org/10.1016/j.neucom.2021.07.051

15. Xiao, X., He, X., Zhang, Y., Dong, X., Yang, L.-X., & Xiang, Y. (2023). Blockchain-based reliable image copyright protection. IET Blockchain, 3(4), 222-237. https://doi.org/10.1049/blc2.12027

16. Darwish, S. M., Abu-Deif, M. M., & Elkaffas, S. M. (2024). Blockchain for video watermarking: An enhanced copyright protection approach for video forensics based on perceptual hash function. PLOS ONE, 19(10), e0308451. https://doi.org/10.1371/journal.pone.0308451

17. Swanson, M. D., Kobayashi, M., & Tewfik, A. H. (1998). Multimedia data-embedding and watermarking technologies. Proceedings of the IEEE, 86(6), 1064-1087. https://doi.org/10.1109/5.687830

18. Ding, W., Abdel-Basset, M., Ali, A. M., & Moustafa, N. (2024). A survey of intelligent multimedia forensics for internet of things communications: Approaches, strategies, perspectives, and challenges for a sustainable future. Engineering Applications of Artificial Intelligence, 138, 109451. https://doi.org/10.1016/j.engappai.2024.109451

19. Ciriello, R. F., Torbensen, A. C. G., Hansen, M. R. P., & Muller-Bloch, C. (2023). Blockchain-based digital rights management systems: Design principles for the music industry. Electronic Markets, 33, Article 5. https://doi.org/10.1007/s12525-023-00628-5

20. Ntivuguruzwa, J. D. L. C., Ahmad, T., & Han, F. (2024). Comprehensive survey on image steganalysis using deep learning. Array, 22, 100353. https://doi.org/10.1016/j.array.2024.100353

21. Wang, L., Song, Y., & Xia, D. (2023). Deep neural network watermarking based on a reversible image hiding network. Pattern Analysis and Applications, 26(3), 861-874. https://doi.org/10.1007/s10044-023-01140-4

22. Singh, H. K., & Singh, A. K. (2023). Comprehensive review of watermarking techniques in deep-learning environments. Journal of Electronic Imaging, 32(3), 031804. https://doi.org/10.1117/1.JEI.32.3.031804