НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Кваліфікаційна наукова
праця на правах рукопису

ОВЧИННИКОВ МИКОЛА ЮРІЙОВИЧ

УДК 004.9:004.056.5:004.032.6:347.78

ДИСЕРТАЦІЯ
РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА МУЛЬТИМЕДІЙНІ ДАНІ

122 – Комп’ютерні науки
12 – Інформаційні технології

Подається на здобуття ступеня доктора філософії
Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ М.Ю. Овчинников

Науковий керівник – **Ахмаметьєва Ганна Валеріївна**,
кандидат технічних наук, доцент

Одеса – 2026

АНОТАЦІЯ

Овчинников М.Ю. Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» (галузь знань 12 – Інформаційні технології). – Національний університет «Одеська юридична академія», Одеса, 2026.

Дисертаційна робота присвячена розв'язанню актуального науково-прикладного завдання підвищення ефективності захисту інтелектуальної власності на мультимедійні дані шляхом побудови математичних моделей, удосконалення наявних і розроблення нових методів, що поєднують ідентифікацію правовласника, вбудовування стійких цифрових водяних знаків у зображення та аудіодані й кількісне оцінювання цілісності і подібності контенту після типових перетворень, а також їх програмної реалізації у вигляді інформаційної системи з формуванням доказових протоколів перевірки.

Актуальність дослідження зумовлена стрімким зростанням обсягів цифрового мультимедійного контенту, поширенням платформ масової публікації зображень, аудіо та відео, розвитком генеративних технологій, а також збільшенням кількості випадків несанкціонованого копіювання, модифікації, повторного розміщення та комерційного використання цифрових творів без згоди правовласника. У таких умовах ефективна реалізація традиційних правових механізмів захисту авторських і суміжних прав потребує їх доповнення технічними засобами фіксації авторства, виявлення похідних копій, перевірки цілісності файлів та автоматизованого аналізу мультимедійних даних. Саме тому в дисертації запропоновано інформаційну систему, яка поєднує методи цифрового водяного маркування, перцептивного хешування, аудіовідбитків, псевдографічного аналізу аудіосигналу, метаданих, журналювання операцій і експериментальної оцінки стійкості методів.

У першому розділі дисертації досліджено сутність мультимедійних даних як об'єкта інформаційного, технічного та правового захисту. Розглянуто

особливості цифрових зображень, аудіофайлів та інших типів мультимедійного контенту з погляду можливості їх копіювання, трансформації, повторного стиснення, обрізання, масштабування, перекодування та поширення в мережевому середовищі. Охарактеризовано основні загрози для цифрової інтелектуальної власності, проаналізовано наукові підходи до захисту мультимедійних даних – цифрові водяні знаки, стеганографічні методи, криптографічні та перцептивні хеші, аудіофінгерпринтинг, пошук візуально подібних зображень та системи контентної ідентифікації, а також специфіку авторського права на аудіо- та відеофайли й застосування штучного інтелекту у сфері захисту мультимедійних даних. Окремо досліджено структуру мультимедійних даних як контейнерів для прихованого вбудовування інформації: визначено компоненти зображень та аудіосигналів, придатні для маркування, проаналізовано пропускну здатність каналів вбудовування, метрики оцінювання непомітності та стійкості й формальні моделі перетворень і атак. Обґрунтовано необхідність переходу від ізольованого використання окремих алгоритмів до побудови комплексної інформаційної системи та сформульовано вимоги до такої системи.

У другому розділі дисертації побудовано математичні моделі та вдосконалено методи вбудовування цифрових водяних знаків у мультимедійні дані. Кожний клас методів розглянуто за єдиною аналітичною схемою: формалізація наявного методу та його математичної моделі, виявлення притаманних йому недоліків, формулювання гіпотези щодо вдосконалення, доведення відповідного твердження та експериментальна перевірка на реальних даних із конкретними кількісними показниками. Розглянуто просторові методи (LSB, статистичне patchwork-вбудовування), частотні методи на основі дискретного косинусного перетворення та QIM для зображень, методи вбудовування в модифікованому дискретному косинусному перетворенні (MDCT) для аудіосигналів, метод розширеного спектра, метод прихованого ехо та метод вбудовування через енергію підсмуг, а також окреслено перспективні напрями вдосконалення (фазове кодування, гібридні трансформні схеми

DWT+SVD/DWT+DCT, нейромережеві методи). Для кількісного оцінювання ефективності вдосконалень розроблено автоматизований конвеєр порівняльного тестування; експерименти проведено на наборі зі 150 аудіофайлів за стандартизованим переліком атак (MP3-перекодування, нормалізація гучності, передискретизація, фільтрація) з використанням метрик стійкості (BER), непомітності (SNR) та обчислювальної вартості. Проаналізовано переваги та обмеження кожного класу методів, що створює теоретичну основу для авторських методів наступного розділу.

У третьому розділі дисертації розроблено та формально описано два авторські методи. Для зображень вдосконалено метод DCT-QIM (wm_v2_dct_qim_profile): введено псевдовипадкову ключову вибірку позицій коефіцієнтів, пакетну надлишковість із повторенням і трирівневу схему ухвалення рішень «PASS / PARTIAL / FAIL» («Придатний / Ризик / Відмова»). Метод експериментально перевірено на наборі з 567 зображень: за середнього PSNR 55,88 дБ після JPEG-стиснення з параметром якості Q=75 отримано BER = 0,0287. Формалізована ємність методу становить до 44 байт для зображень, що задовольняють установлені вимоги до розміру контейнера. Для аудіоданих розроблено авторський псевдографічно-диференціальний метод audio_pgdiff_v2, що включає формування нормалізованого профілю та диференціальної послідовності аудіосигналу, побудову 64-бітного цифрового відбитку, абсолютне DCT-QIM-вбудовування у смугах 120–600 та 600–2400 Гц із принципом модифікації лише послабленням енергії, стабільний відбір несучих кадрів, повторення на рівні пакета з перемеженням та формалізовану чотирирівневу попередню перевірку придатності файлу. Метод забезпечує BER = 0,0100 після MP3-стиснення зі швидкістю 128 кбіт/с для контейнерів, що пройшли попередню перевірку придатності. Розділ завершується порівняльним аналізом авторських методів із класичними підходами, який підтверджує їх конкурентоспроможність за ключовими метриками та перевагу за комплексністю конвеєра.

У четвертому розділі дисертації розроблено архітектуру та програмну реалізацію системи IP-Protect як модульного програмного комплексу. Система поєднує реєстр цифрових активів, модуль ліцензування та управління правами, бібліотеку цифрових водяних знаків і відбитків, підсистему поетапної верифікації (SHA-256 → відбиток → водяний знак), доказовий контур та публічний режим перевірки для незареєстрованих користувачів. Для зображень задіяно SHA-256, phash64, dhash64 та DCT/QIM-вбудовування; для аудіо інтегровано вісім методів із різною стійкістю та призначенням, об'єднаних спільним контрактом preflight → embed → self-check → delivery-check. Конфігурація методів керується через RuntimeSettings без потреби в перерозгортанні системи. Обґрунтовано конкурентні переваги IP-Protect перед DRM-системами, платформними Content ID та блокчейн-реєстрами у частині платформонезалежності, вбудованості ідентифікатора, прозорості та придатності доказових матеріалів до використання в правовому контексті.

Робота розвиває підходи до захисту інтелектуальної власності на мультимедійні дані шляхом поєднання методів цифрового водяного маркування, перцептивного хешування, псевдографічного аналізу аудіосигналу та програмної реалізації у вигляді єдиної інформаційної системи. Особливу увагу приділено забезпеченню практичної придатності методів: попередній оцінці придатності файлу до вбудовування, контролю якості на кожному етапі обробки та формуванню відтворюваних протоколів перевірки.

Аналіз показав, що ефективний захист мультимедійних даних не може ґрунтуватися на одному ізольованому алгоритмі – криптографічний хеш, перцептивний відбиток і цифровий водяний знак виконують різні функції та мають бути інтегровані в єдиний конвеєр перевірки. Запропонована поетапна верифікація (SHA-256 → відбиток → водяний знак) дозволяє точно встановити характер модифікації: від повної заміни файлу до часткового пошкодження вбудованого ідентифікатора.

Встановлено, що введення трирівневої схеми ухвалення рішень «PASS / PARTIAL / FAIL» для зображень і чотирирівневої попередньої перевірки для

аудіофайлів суттєво підвищує інформативність результатів порівняно з бінарним підходом «виявлено / не виявлено». Зокрема, для методу DCT-QIM досягнуто BER = 0 після JPEG-стиснення з якістю Q=90/Q=85 та BER = 0,0287 після JPEG-стиснення з якістю Q=75 при PSNR 55,88 дБ, а метод audio_pgdiff_v2 забезпечує BER=0,0100 після перекодування MP3 128 кбіт/с та BER=0,0567 після перекодування MP3 64 кбіт/с для придатних контейнерів.

Обґрунтовано, що псевдографічно-диференціальний підхід до аналізу аудіосигналу дозволяє одночасно вирішувати задачі цифрового відбитку, попередньої діагностики та водяного маркування в єдиному конвеєрі, що є якісною відмінністю від класичних методів, кожен з яких вирішує лише одну з цих задач. Інваріантність відношення енергій смуг забезпечує стійкість методу до нормалізації гучності – однієї з найпоширеніших побутових трансформацій аудіофайлів.

Визначено, що конфігурація методів через RuntimeSettings без перерозгортання системи та підтримка публічного режиму перевірки для незареєстрованих користувачів суттєво розширюють практичну застосовність системи IP-Protect порівняно із закритими платформними рішеннями, DRM-системами та блокчейн-реєстрами.

Результати дослідження доповнюють наявні підходи до захисту цифрового контенту, акцентуючи увагу на комплексності технічного рішення, доказовій цінності протоколів перевірки та можливості використання системи авторами, медіаорганізаціями та фахівцями з кібербезпеки в реальних сценаріях атрибуції та верифікації мультимедійних даних. Практичне значення результатів дослідження полягає у створенні програмної системи IP-Protect, яка може використовуватися авторами, правовласниками, медіаорганізаціями, освітніми установами та фахівцями з кібербезпеки для реєстрації мультимедійних об'єктів, вбудовування ідентифікаторів, перевірки походження файлів, аналізу модифікованих копій і формування звітів про результати перевірки. Запропоновані моделі, алгоритми та програмні модулі можуть бути використані як основа для подальшого розвитку систем моніторингу цифрового контенту,

автоматизованої експертизи мультимедійних файлів, навчальних лабораторних робіт із цифрових водяних знаків та захисту інформаційних ресурсів.

Практичну цінність дослідження підтверджують довідки та акти впровадження в діяльність ПАТ «ОДЕСКАБЕЛЬ», ТОВ «КІПСОЛІД УКРАЇНА», Державної служби спеціального зв'язку та захисту інформації України, Управління протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України (Додаток Г).

Результати дослідження інтегровано в освітній процес Національного університету «Одеська юридична академія» при викладанні навчальних дисциплін «Експертиза та перевірка цілісності мультимедійних даних», «Цифрові водяні знаки», «Прикладна криптографія», «Системи аутентифікації та цифрової ідентифікації», «Адміністрування, аудит та безпека вебсистем», «Цифрові технології в бізнесі», «IT-маркетинг», «Основи IT бізнесу», «DevOps» та «DevOpsSec» (Додаток Г). Окремі положення дисертації, програмний прототип і методичні матеріали використовуються під час лабораторних занять, виконання індивідуальних завдань, підготовки кваліфікаційних робіт і в науково-дослідній роботі здобувачів.

Ключові слова: інформаційна система, машинне навчання, методи машинного навчання, штучний інтелект, мультимедійні дані, цифровий водяний знак, цифровий відбиток, псевдографічно-диференціальний метод, інтелектуальна власність, стеганографія, стегоаналіз, перцептивне хешування, дискретне косинусне перетворення, кібербезпека, IP-Protect.

ABSTRACT

Ovchynnykov M. Yu. Development of an Information System for the Protection of Intellectual Property Rights to Multimedia Data. – Qualifying scientific work as a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 122 “Computer Science” (field of knowledge 12 – Information Technology). – National University “Odesa Law Academy”, Odesa, 2026.

The dissertation solves the scientific and applied task of developing an information system for the protection of intellectual property rights to multimedia data. The system provides registration of digital objects, formation of a unique rights-holder identifier, embedding of digital watermarks into images and audio data, search for authorship features, verification of the integrity and similarity of multimedia content after typical transformations, as well as documentation of verification results in the form of quantitative metrics and protocols.

The relevance of the study is determined by the rapid growth in the volume of digital multimedia content, the spread of mass-publication platforms for images, audio and video, the development of generative technologies, and the increasing number of cases of unauthorized copying, modification, re-uploading and commercial use of digital works without the consent of the rights holder. Under such conditions, traditional legal mechanisms for the protection of copyright and related rights are insufficient without technical means for fixing authorship, detecting derivative copies, verifying file integrity and performing automated analysis of multimedia data. Therefore, the dissertation proposes an information system that combines methods of digital watermarking, perceptual hashing, audio fingerprints, pseudographic analysis of the audio signal, metadata, operation logging and experimental assessment of method robustness.

The first chapter of the dissertation examines the essence of multimedia data as an object of informational, technical and legal protection. It considers the specific features of digital images, audio files and other types of multimedia content in terms of their copying, transformation, recompression, cropping, scaling, transcoding and distribution in the network environment. The main threats to digital intellectual property are characterized,

and scientific approaches to the protection of multimedia data are analyzed, including digital watermarks, steganographic methods, cryptographic and perceptual hashes, audio fingerprinting, search for visually similar images and content identification systems, as well as the specific features of copyright on audio and video files and the use of artificial intelligence in the field of multimedia data protection. The structure of multimedia data as containers for covert information embedding is examined separately: the components of images and audio signals suitable for marking are identified, and the capacity of embedding channels, the metrics for assessing imperceptibility and robustness, and formal models of transformations and attacks are analyzed. The necessity of moving from the isolated use of individual algorithms to the construction of a comprehensive information system is substantiated, and the requirements for such a system are formulated.

The second chapter of the dissertation builds mathematical models and improves methods for embedding digital watermarks into multimedia data. Each class of methods is examined following a single analytical scheme: formalization of the existing method and its mathematical model, identification of its inherent shortcomings, formulation of a hypothesis for improvement, proof of the corresponding statement, and experimental verification on real data with specific quantitative indicators. The chapter considers spatial methods (LSB, statistical patchwork embedding), frequency-domain methods based on the discrete cosine transform and QIM for images, embedding methods in the modified discrete cosine transform (MDCT) for audio signals, the spread-spectrum method, the echo-hiding method and the subband-energy embedding method, and also outlines promising directions for improvement (phase coding, hybrid transform schemes DWT+SVD/DWT+DCT, neural-network methods). To quantitatively assess the effectiveness of the improvements, an automated comparative-testing pipeline was developed; the experiments were carried out on a set of 150 audio files using a standardized list of attacks (MP3 transcoding, loudness normalization, resampling, filtering) with metrics of robustness (BER), imperceptibility (SNR) and computational cost. The advantages and limitations of each class of methods are analyzed, which forms the theoretical basis for the author's methods of the next chapter.

The third chapter of the dissertation develops and formally describes two author’s

methods. For images, the DCT-QIM method (wm_v2_dct_qim_profile) has been improved: a pseudorandom key-based selection of coefficient positions, packet redundancy with repetition, and a three-level decision-making scheme “PASS / PARTIAL / FAIL” have been introduced. The method was experimentally evaluated on a dataset of 567 images: at an average PSNR of 55.88 dB, JPEG compression with a quality factor of Q = 75 resulted in a BER of 0.0287. The formalized embedding capacity is up to 44 bytes for images satisfying the established container-size requirements. For audio data, the author’s pseudographic-differential method audio_pgdiff_v2 has been developed. It includes the formation of a normalized profile and differential sequence of the audio signal, construction of a 64-bit digital fingerprint, absolute DCT-QIM embedding in the 120–600 Hz and 600–2400 Hz bands using the attenuation-only principle, stable selection of carrier frames, packet-level repetition with interleaving, and a formalized four-level preflight assessment of file suitability. The method provides BER = 0.0100 after MP3 compression at 128 kbps for containers that have passed the preflight suitability assessment. The chapter concludes with a comparative analysis of the author’s methods and classical approaches, confirming their competitiveness according to key metrics and their advantage in terms of the complexity and completeness of the processing pipeline.

The fourth chapter of the dissertation develops the architecture and software implementation of the IP-Protect system as a modular software complex. The system combines a register of digital assets, a licensing and rights-management module, a library of digital watermarks and fingerprints, a staged verification subsystem (SHA-256 → fingerprint → watermark), an evidence-oriented framework, and a public verification mode for unregistered users. For images, SHA-256, phash64, dhash64 and DCT/QIM embedding are used; for audio, eight methods with different levels of robustness and purposes are integrated, united by a common contract: preflight → embed → self-check → delivery-check. Method configuration is managed through RuntimeSettings without the need to redeploy the system. The competitive advantages of IP-Protect over DRM systems, platform-based Content ID solutions and blockchain

registries are substantiated in terms of platform independence, embedded identifiers, transparency and the suitability of evidence materials for use in a legal context.

The work develops approaches to the protection of intellectual property rights to multimedia data by combining digital watermarking, perceptual hashing, pseudographic analysis of the audio signal and software implementation in the form of a unified information system. Special attention is paid to ensuring the practical applicability of the methods: preliminary assessment of file suitability for embedding, quality control at each processing stage and the formation of reproducible verification protocols.

The analysis has shown that effective protection of multimedia data cannot be based on a single isolated algorithm: a cryptographic hash, a perceptual fingerprint and a digital watermark perform different functions and must be integrated into a unified verification pipeline. The proposed staged verification process (SHA-256 → fingerprint → watermark) makes it possible to accurately determine the nature of a modification, ranging from complete file replacement to partial damage to the embedded identifier.

It has been established that introducing a three-level decision scheme “PASS / PARTIAL / FAIL” for images and a four-level preflight assessment for audio files significantly increases the informativeness of the results compared with the binary "detected / not detected" approach. In particular, for the DCT-QIM method, BER = 0 was achieved after JPEG compression at quality Q=90/Q=85 and BER = 0.0287 after JPEG compression at quality Q=75, at PSNR 55.88 dB; the audio_pgdiff_v2 method provides BER = 0.0100 after MP3 128 kbps transcoding and BER = 0.0567 after MP3 64 kbps transcoding, for suitable containers.

It is substantiated that the pseudographic-differential approach to audio signal analysis makes it possible to solve the tasks of digital fingerprinting, preliminary diagnostics and watermarking simultaneously within a single pipeline. This is a qualitative difference from classical methods, each of which solves only one of these tasks. The invariance of the band-energy ratio ensures the method’s robustness to loudness normalization, one of the most common everyday transformations of audio files.

It is determined that method configuration through RuntimeSettings without system redeployment, as well as support for a public verification mode for unregistered

users, significantly expands the practical applicability of the IP-Protect system compared with closed platform-based solutions, DRM systems and blockchain registries.

The results of the study complement existing approaches to digital content protection by emphasizing the comprehensiveness of the technical solution, the evidentiary value of verification protocols and the possibility of using the system by authors, media organizations and cybersecurity specialists in real-world scenarios of attribution and verification of multimedia data.

The practical significance of the research results lies in the creation of the IP-Protect software system, which can be used by authors, rights holders, media organizations, educational institutions and cybersecurity specialists to register multimedia objects, embed identifiers, verify file origin, analyze modified copies and generate verification reports. The proposed models, algorithms and software modules may serve as a basis for the further development of digital content monitoring systems, automated examination of multimedia files, laboratory assignments on digital watermarks and the protection of information resources.

The practical value of the study is confirmed by certificates and implementation acts from PJSC “ODESKABEL”, LLC “KIPSOLID UKRAINE”, the State Service of Special Communications and Information Protection of Ukraine, and the Cybercrime Counteraction Unit in Odesa Region of the Cyber Police Department of the National Police of Ukraine.

The research results have been integrated into the educational process of the National University “Odesa Law Academy” in the teaching of the academic disciplines “Examination and Verification of the Integrity of Multimedia Data”, “Digital Watermarks”, “Applied Cryptography”, “Authentication and Digital Identification Systems”, “Administration, Audit and Security of Web Systems”, “Digital Technologies in Business”, “IT Marketing”, “Fundamentals of IT Business”, “DevOps” and “DevOpsSec”. Individual provisions of the dissertation, the software prototype and methodological materials are used during laboratory classes, individual assignments, preparation of qualification papers and research activities of students.

Keywords: information system, machine learning, machine learning methods, artificial intelligence, multimedia data, digital watermark, digital fingerprint, pseudo-

graphic differential method, intellectual property, steganography, steganalysis, perceptual hashing, discrete cosine transform, cybersecurity, IP-Protect.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці здобувача, в яких опубліковані основні наукові результати дисертації:

1. Овчинников М. Ю., Слатвінська В. М. Технічний та нормативно-правовий аспекти захисту об’єктів інтелектуальної власності на ринку аудіо-візуальної продукції. *Вісник Херсонського національного технічного університету.* 2024. № 3(90). С. 259–270. DOI: https://doi.org/10.35546/kntu2078-4481.2024.3.32.

2. Овчинников М. Ю. Додавання та обробка звуку в метаданих файлів за допомогою PHP. *Наука і техніка сьогодні.* 2025. № 4(45). С. 1332–1344. DOI: https://doi.org/10.52058/2786-6025-2025-4(45)-1332-1344.

3. Овчинников М. Ю. Компаративний аналіз алгоритмів відбитку контенту для систем захисту інтелектуальної власності на мультимедійні дані. *Наука і техніка сьогодні*. 2025. №7(48). С. 1766–1779. DOI: https://doi.org/10.52058/2786-6025-2025-7(48)-1766-1779.

4. Овчинников М. Ю. Захист інформації в медіафайлах. *Безпека інформації та інфраструктури інформаційно-комунікаційних систем: міждисциплінарний підхід*: монографія / за ред. С. Горбаченка, А. Соколова. Львів–Торунь: Liha-Pres, 2025. С. 299–332. DOI: https://doi.org/10.36059/978-966-397-537-5-8.

5. Горбаченко С. А., Овчинников М. Ю. Захист інтелектуальної власності у сфері цифрового контенту: виклики та рішення для рекламного менеджменту. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки.* 2025. Т. 36 (75). №4. Ч. 2. С. 87–96. DOI: https://doi.org/10.32782/2663-5941/2025.4.2/12.

6. Овчинников М. Ю. Розробка та оптимізація алгоритмів цифрового відбитку для систем ідентифікації контенту в інформаційних системах захисту інтелектуальної власності. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2025. Вип. 3. С. 134–139. DOI: https://doi.org/10.32782/IT/2025-3-16.

7. Ахмаметьєва Г. В., Овчинников М. Ю. Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані в хмарних середовищах. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2025. Вип. 4. С. 3–13. DOI: https://doi.org/10.32782/IT/2025-4-1.

8. Овчинников М. Ю. Доказоорієнтований захист прав інтелектуальної власності на мультимедійні дані в епоху контенту, згенерованого ШІ. *Středoevropský věstník pro vědu a výzkum.* 2026. Vol. 2, № 1. С. 274–292. DOI: https://doi.org/10.65237/2336-3630-2026-1(2)-17.

9. Овчинников М. Ю. Інформаційна система захисту інтелектуальної власності мультимедійних даних: синергія водяних знаків, перцептивного хешування та ШІ-аналітики. *Cross-disciplinary Studies in Science, Innovation and Social Development: Monograph* / [reviewers: E. O. Romanenko, Y. O. Ulianchenko, O. I. Datsii]. Prague: Publishing house Education and Science s.r.o., 2026. С. 359–370. DOI: https://doi.org/10.65237/3-2026-23.

10. Овчинников М. Ю. Інтегрований захист мультимедійних даних у суднобудуванні й морській інфраструктурі. *Shipbuilding & Marine Infrastructure.* 2026. №1(22). С. 155–165. DOI: https://doi.org/10.15589/smi2026.1(22).15.

Наукові праці, які засвідчують апробацію матеріалів дисертації та додатково відображають її наукові результати :

11. Овчинников М. Ю. Огляд методів вбудовування інформації в звукові файли. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика*: матер. міжнар. наук.-практ. конф. (м. Одеса, 24 листоп. 2023 р.). Одеса : НУ «ОЮА», 2023. 301 с. С. 27–30. DOI: https://doi.org/10.32837/11300.27179.

12. Овчинников М. Ю. Особливості вбудовування прихованої інформації у файли формату MP3. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів* : матеріали Міжнар. наук.-практ. конф. (Одеса, 26 квіт. 2024 р.). Одеса, 2024. С. 898–902. URL: https://hdl.handle.net/11300/28215.

13. Овчинников М. Ю. Метод вбудовування повідомлень у відліки імпульсно-кодової модуляції аудіосигналу. *Інформаційне суспільство: проблеми та перспективи*: матер. IX Всеукр. наук.-практ. конф. (Одеса, 24 травня 2024 р.). С. 167–170. DOI: https://doi.org/10.32837/11300.27842

14. Овчинников М. Ю. Використання тегів ID3v2 для захисту авторських прав на звукові файли MP3. *Кібербезпека в сучасному світі: актуальні виклики:* матер. V Міжнар. наук.-практ. конф. (м. Одеса, 22 листопада 2024 р.) Одеса, 2024. С. 41–43. DOI: https://doi.org/10.32837/11300.28986

15. Овчинников М.Ю. Компаративний аналіз методів впровадження ЦВЗ в аудіофайли. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: матер. Міжнар. наук.-практ. конф. (м. Одеса, 16 трав. 2025 р.): у 2 т. Одеса : Фенікс, 2025. Т. 2. С. 558–562. URL: https://hdl.handle.net/11300/31052

16. Ахмаметьєва Г. В., Овчинников М. Ю. Порівняльний аналіз методів широкосмугового та фазового кодування цифрових водяних знаків в аудіосигналі. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: матер. Міжнар. наук.-практ. конф. (м. Одеса, 16 травня 2025 р.) : у 2 т. Одеса: Фенікс, 2025. Т. 2. С. 539–542. URL: https://hdl.handle.net/11300/31044

17. Овчинников М. Ю. Розробка систем автоматичного моніторингу незаконного розповсюдження мультимедіа в інтернеті. *Інформаційне суспільство: проблеми та перспективи* : матер. X Всеукр. наук.-практ. конф. (м. Одеса, 23 травня 2025 р.). Одеса. 2025. С. 168–172. DOI: https://doi.org/10.32837/11300.29842

18. Овчинников М. Ю. AI-підсилена верифікація авторства мультимедійних даних в умовах генеративного ШІ. *Кібербезпека в сучасному світі: актуальні виклики* : матер. VI Міжнар. наук.-практ. конф. (м. Одеса, 28 листоп. 2025 р.). Одеса: НУ «ОЮА», 2025. С. 112–114. URL: https://hdl.handle.net/11300/32730.

19. Овчинников М. Ю. Алгоритмічні підходи до підтвердження авторства та цілісності мультимедійних даних. *Кібербезпека в сучасному світі: актуальні*

виклики : матер. VI Міжнар. наук.-практич. конф. (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. С. 59–62. URL: https://hdl.handle.net/11300/32710.

20. Овчинников М. Ю. Ліцензування та управління правами на цифровий мультимедійний контент: інтеграція технічних засобів контролю у правові процедури. *Кібербезпека в сучасному світі: актуальні виклики* : матер. VI Міжнар. наук.-практич. конф. (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. С. 265–268. URL: https://hdl.handle.net/11300/32856.

21. Овчинников М. Ю. Комунікаційні стратегії протидії репостам і «дзеркалам» мультимедійного контенту: взаємодія з платформами та спільнотами. *Кібербезпека в сучасному світі: актуальні виклики* : матеріали VI Міжнар. наук.-практич. конф. (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. С. 236–239. URL: https://hdl.handle.net/11300/32835.

22. Horbachenko S. Chepurna O. Kuklinova T. Kukharenko S. Cherevko Y. Boiko V. Ovchynnykov M. Analysis and optimization of processes for integrating smart grid objects into the critical infrastructure cyber protection system. *2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek'2025).* (Kharkiv, October 06–10, 2025). P. 615–619. DOI: https://doi.org/10.1109/KhPIWeek61436.2025.11288406.

23. Овчинников М. Ю. Штучний інтелект як адаптивний компонент цифрового водяного маркування мультимедійних даних. *Global Interdisciplinary Summit: Frontier of Science and Future Technologies* : Proceedings of International Scientific and Practical Conference. (April 3, 2026, Khalifa University Campus, Dubai, UAE). 2026. С. 132–139. DOI: https://doi.org/10.65237/1-4-2026-12.

24. Овчинников М. Ю. Синергія цифрових водяних знаків, перцептивного хешування та мультимедійних цифрових відбитків у системах захисту інтелектуальної власності. *Scientific Horizons: Digital Transformation* : Proceedings of International Scientific and Practical Conference. (March 20, 2026, Tsinghua University, Beijing, China). 2026. С. 26–33. DOI: https://doi.org/10.65237/1-3-2026-4.

Свідоцтва про реєстрацію авторського права на твір:

1. Комп'ютерна програма «Інформаційна система захисту інтелектуальної власності на мультимедійні дані IP-Protect» / Овчинников Микола Юрійович; Свідоцтво про реєстрацію авторського права на твір № 149653; видано 06.08.2026 р., дата реєстрації 30 липня 2026 р. URL: https://sis.nipo.gov.ua/uk/search/detail/1942787/

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 22
ВСТУП 35
РОЗДІЛ 1. ОГЛЯД ЛІТЕРАТУРИ ТА СУЧАСНОГО СТАНУ ПРОБЛЕМИ 48
1.1. Інтелектуальна власність у цифровому середовищі: основні проблеми та загрози 48
1.2. Методи захисту мультимедійних даних 52
1.3. Класифікація та характеристики стеганографічних методів 58
1.4. Аналіз наявних систем захисту авторських прав 68
1.5. Авторське право на аудіо- та відеофайли: специфіка 74
1.6. Використання штучного інтелекту у сфері захисту мультимедійних даних 75
1.7. Аналіз структури мультимедійних даних щодо стійкості до втручання . 77
1.8. Визначення компонентів мультимедійних файлів, придатних для вбудовування ідентифікаторів 82
1.9. Пропускна здатність каналів вбудовування та метрики оцінювання 85
1.10. Стійкість до атак та формальні моделі перетворень 87
1.11. Висновки до розділу 90
РОЗДІЛ 2. МАТЕМАТИЧНІ МОДЕЛІ ТА УДОСКОНАЛЕННЯ МЕТОДІВ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У МУЛЬТИМЕДІЙНІ ДАНІ 92
2.1. Постановка задачі, критерії ефективності та методика експериментального порівняння 92
2.2. Просторові методи (LSB та часова область) 94
2.3. Частотні методи на основі дискретного косинусного перетворення та QIM (для зображень) 106
2.4. Методи вбудовування в модифікованому дискретному косинусному перетворенні (MDCT) для аудіосигналів 112
2.5. Метод розширеного спектра (Spread Spectrum / DSSS) 119

2.6. Метод прихованого exo (Echo Hiding)..... 124
2.7. Метод вбудовування через енергію підсмуг (Subband Energy) 129
2.8. Методи машинного навчання в задачах стегоаналізу та атрибуції 134
2.9. Перспективні напрями вдосконалення (теоретичне обґрунтування)..... 145
2.9. Висновки до розділу 2..... 149
РОЗДІЛ 3. РОЗРОБКА МЕТОДІВ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ НА ОСНОВІ ЦИФРОВОГО ВОДЯНОГО МАРКУВАННЯ ТА ПСЕВДОГРАФІЧНО-ДИФЕРЕНЦІАЛЬНОГО АНАЛІЗУ 152
3.1. Вдосконалений метод DCT-QIM для вбудовування водяного знака у зображення 152
3.2. Запропонований псевдографічно-диференціальний метод захисту аудіоданих (audio_pgdiff_v2)..... 160
3.3. Порівняльний аналіз та наукова новизна..... 183
3.4. Висновки до розділу 3..... 192
РОЗДІЛ 4. РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ..... 194
4.1. Архітектура інформаційної системи..... 194
4.2. Технологічний стек та середовище розробки..... 201
4.3. Реалізація бібліотеки цифрових водяних знаків та відбитків 202
4.4. Криптографічні механізми та доказовий контур..... 207
4.5. Підсистема перевірки мультимедійних файлів 208
4.6. Модуль ліцензування та управління правами 212
4.7. Модуль штучного інтелекту..... 213
4.8. Безпека, аудит та розгортання..... 216
4.9. Порівняльний аналіз IP-Protect з наявними системами захисту авторських прав 217
4.10. Висновки до розділу 4..... 219
ВИСНОВКИ..... 221
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 225

ДОДАТКИ 251
Додаток А. Список публікацій здобувача 251
Додаток Б. Копія свідоцтва про реєстрацію авторського права на твір..... 257
Додаток В. Таблиці..... 258
Додаток Г. Документи щодо впровадження результатів досліджень 261

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

У переліку наведено основні скорочення, умовні позначення та терміни, які використовуються в дисертації. Матеріал подано в алфавітному порядку; рідковживані або загальновідомі скорочення розкриваються безпосередньо в тексті при першому згадуванні.

Скорочення та абревіатури

AAC – формат втратного стиснення аудіо Advanced Audio Coding.

ACR – автоматичне розпізнавання контенту (Automatic Content Recognition).

AES – симетричний криптографічний алгоритм шифрування Advanced Encryption Standard.

AI / ШІ – штучний інтелект (Artificial Intelligence).

API – програмний інтерфейс застосунку (Application Programming Interface).

AVMSD – директива ЄС про аудіовізуальні медіапослуги (Audiovisual Media Services Directive).

BCH – клас блокових помилкостійких кодів Боуза–Чоудгурі–Хоквінгема.

BER – бітова частота помилок (Bit Error Rate).

C2PA – Coalition for Content Provenance and Authenticity; стандарт перевірюваної фіксації походження контенту.

CBIR – пошук зображень за вмістом (Content-Based Image Retrieval).

CDSM – директива ЄС про авторське право на цифровому єдиному ринку (Copyright in the Digital Single Market Directive).

CMYK – кольорова модель Cyan, Magenta, Yellow, Key/Black.

CNN – згорткова нейронна мережа (Convolutional Neural Network).

CRC – метод контролю цілісності даних на основі циклічного надлишкового коду (Cyclic Redundancy Check).

CRC16 / CRC32 – 16- та 32-бітні варіанти CRC, що використовуються для перевірки цілісності службових пакетів.

CTU – базова структурна одиниця кодування у стандарті HEVC (Coding Tree Unit).

d_{seq} – диференціальна послідовність ознак енергетичного профілю / d-послідовність

DCT – дискретне косинусне перетворення (Discrete Cosine Transform).

DCT-QIM – метод вбудовування, що поєднує дискретне косинусне перетворення та квантувальну індексну модуляцію.

DFT – дискретне перетворення Фур'є (Discrete Fourier Transform).

DL – глибоке навчання (Deep Learning).

DNN – глибока нейронна мережа (Deep Neural Network).

DRM – системи керування цифровими правами (Digital Rights Management).

DSSS – метод прямого розширення спектра псевдовипадковою послідовністю (Direct-Sequence Spread Spectrum).

DWT – дискретне вейвлет-перетворення (Discrete Wavelet Transform).

ECC – помилкостійке кодування (Error-Correcting Code).

EU / ЄС – Європейський Союз.

FeatureHash – хеш стійких ознак об'єкта.

FileHash – криптографічний хеш повного файла.

FP64 – 64-бітний псевдографічний аудіовідбиток, сформований на основі диференціальної послідовності ознак.

GAN – генеративно-змагальна нейронна мережа (Generative Adversarial Network).

GOP – група кадрів у структурі відеопотоку (Group of Pictures).

H.264/AVC – стандарт цифрового стиснення відео (Advanced Video Coding).

H.265/HEVC – стандарт високоефективного відеостиснення (High Efficiency Video Coding).

HAS – слухова система людини (Human Auditory System).

HDR – розширений динамічний діапазон (High Dynamic Range).

HVS – зорова система людини (Human Visual System).

ID – ідентифікатор (Identifier).

IDCT – обернене дискретне косинусне перетворення (Inverse Discrete Cosine Transform).

ImageRights – сервіс моніторингу та виявлення несанкціонованого використання зображень.

IPP1 – префікс службового повідомлення, що пов’язує вбудований ідентифікатор із токеном активу в реєстрі IP-Protect.

IWT – цілочисельне вейвлет-перетворення (Integer Wavelet Transform).

JPEG – стандарт і формат втратного стиснення зображень.

JPEG2000 – стандарт стиснення зображень на основі вейвлет-перетворення.

LSB – молодший значущий біт (Least Significant Bit).

MDCT – модифіковане дискретне косинусне перетворення (Modified Discrete Cosine Transform).

MP3 – формат втратного стиснення аудіо MPEG-1/2 Audio Layer III.

MSE – середньоквадратична помилка (Mean Squared Error).

NC – нормована кореляція (Normalized Correlation).

ODG – об’єктивна оцінка відмінності аудіосигналу (Objective Difference Grade).

OGG – контейнерний формат мультимедійних даних.

ОКУ – організація колективного управління.

PCM – імпульсно-кодова модуляція аудіосигналу (Pulse-Code Modulation).

PEAQ – перцептивна оцінка якості аудіо (Perceptual Evaluation of Audio Quality).

Pex – платформа цифрового розпізнавання контенту та керування правами.

PGD1 – ідентифікатор формату службового пакета методу audio_pgdiff_v2.

pHash64 / dHash64 – 64-бітні перцептивні відбитки зображення на основі перцептивного та різницевого хешування відповідно.

PNG – формат безвтратного зберігання растрових зображень.

PSNR – пікове відношення сигнал/шум (Peak Signal-to-Noise Ratio).

PVD – метод вбудовування за різницею значень сусідніх пікселів (Pixel Value Differencing).

q_{seq} – квантований енергетичний профіль аудіосигналу / q-профіль

QP – параметр квантування у відеокодеках (Quantization Parameter).

QIM – квантувальна індексна модуляція (Quantization Index Modulation).

QR – двовимірний матричний код Quick Response.

Reed–Solomon – клас помилкостійких кодів для корекції групових помилок.

RGB – кольорова модель Red, Green, Blue.

RMS – середньоквадратичне значення амплітуди сигналу (Root Mean Square).

ROC – ROC-крива (Receiver Operating Characteristic).

RSA – криптографічний алгоритм відкритого ключа Rivest–Shamir–Adleman.

RST – обертання, масштабування, зсув (Rotation, Scaling, Translation).

segSNR – сегментне відношення сигнал/шум (Segmental Signal-to-Noise Ratio).

SHA-256 – криптографічна хеш-функція сімейства SHA-2 із 256-бітним результатом.

SIFT – метод виявлення та опису локальних інваріантних ознак (Scale-Invariant Feature Transform).

SNR – відношення сигналу до шуму (Signal-to-Noise Ratio).

SSIM – індекс структурної подібності (Structural Similarity Index).

STFT – короткочасне перетворення Фур’є (Short-Time Fourier Transform).

SVD – сингулярний розклад матриці (Singular Value Decomposition).

TPM – технологічні заходи охорони прав (Technological Protection Measures).

TSM – зміна часової шкали аудіосигналу (Time-Scale Modification).

UGC – контент, створений користувачами (User-Generated Content).

UID – унікальний ідентифікатор (Unique Identifier).

Videntifier – сервіс виявлення та моніторингу незаконного використання відеоконтенту.

WIPO – Всесвітня організація інтелектуальної власності (World Intellectual Property Organization).

YCbCr – кольорова модель із яскравісною та кольорово-різницевими компонентами.

ІВ – інтелектуальна власність.

ЦВЗ – цифровий водяний знак.

Умовні позначення та символи

$A(\cdot)$ – оператор атаки або атакувального каналу.

A_j – j-й акумулятор, що використовується під час формування 64-бітного псевдографічного аудіовідбитка.

b – біт або двійкове повідомлення, яке вбудовується в мультимедійний об’єкт.

$\hat{b}$ – відновлене повідомлення або оцінка вбудованого ідентифікатора.

$D(\cdot; k)$ – детектор або оператор витягування/виявлення маркера за ключем k.

D_{max} – максимально допустима енергія спотворення.

$E(\cdot)$ – оператор вбудовування повідомлення в носій.

g – коефіцієнт масштабування амплітуди сигналу.

h – імпульсна характеристика фільтра під час передискретизації аудіосигналу.

k – секретний або службовий ключ системи.

L – довжина ідентифікатора у бітах.

m – структуроване повідомлення, яке формується перед вбудовуванням.

MAX – максимально можливе значення відліку сигналу.

Q_Δ – оператор квантування з кроком Δ.

Q_0, Q_1 – дві зміщені квантувальні решітки, що використовуються для кодування бітів 0 і 1 у QIM-схемі.

R – модуль реєстру в інтегрованій інформаційній системі.

r – параметр надлишковості, повторення або просторово-часового рознесення бітів.

R_φ – матриця повороту на кут φ.

$t = (t_x, t_y)$ – вектор просторового зсуву.

$T(\cdot)$ – перетворення в область вбудовування.

$w = W(b, k)$ – водяний знак, сформований на основі повідомлення b і ключа k.

$\hat{w}$ – оцінка або реконструйований водяний знак після детекції.

x – оригінальний мультимедійний об’єкт.

X – подання оригінального об’єкта у вибраній області.

y – позначений об’єкт після вбудовування.

Y – подання позначеного об’єкта в області перетворень.

$\tilde{y}$ / $\tilde{y}$ – позначений об’єкт після проходження атак або перетворень.

α – параметр методу вбудовування; його конкретний зміст – сила модифікації або цільове співвідношення енергій – визначається для відповідного методу.

Δ – крок квантування в QIM-схемах.

η – параметр або вектор параметрів атаки.

θ – вектор параметрів алгоритму вбудовування, детекції та кодування.

μ_x, μ_y – середні значення сигналів x та y у формулі SSIM.

σ_{x^2}, σ_{y^2} – дисперсії сигналів x та y.

σ_{xy} – коваріація сигналів x та y.

ρ – кореляційна статистика детектора.

τ – порогове значення ухвалення рішення при детекції.

φ – кут повороту під час моделювання геометричних атак.

Ω – множина індексів, блоків, коефіцієнтів або компонент, придатних для вбудовування.

$\mathcal{A}$ – множина атак, що застосовуються у тестовому протоколі.

$\mathcal{S}$ – узагальнене позначення інтегрованої інформаційної системи захисту ІВ на мультимедійні дані.

Основні терміни

Автентифікація контенту – процедура підтвердження справжності мультимедійного об’єкта та відсутності несанкціонованих змін.

Адитивне вбудовування – схема вбудовування, у якій водяний знак додається до компонент носія як слабкий сигнал.

Акустична подібність – ступінь схожості між аудіосигналами за спектральними, часовими, перцептивними або learned-ознаками.

Алгоритм вбудовування – частина системи, що формує водяний знак, вибирає позиції вбудовування та модифікує компоненти сигналу.

Алгоритм детекції – частина системи, що аналізує об’єкт і встановлює наявність маркера або відновлює повідомлення.

Атакувальний канал – узагальнена модель середовища поширення, що включає стиснення, шум, перекодування та інші перетворення.

Аудіофінгерпринт – компактний стійкий відбиток аудіосигналу для швидкого пошуку збігів.

Аудіомаркування – вбудовування прихованої ідентифікаційної інформації в аудіосигнал з урахуванням психоакустичних властивостей.

Близький збіг – результат пошуку, за якого об’єкти не є байтово ідентичними, але залишаються подібними за змістом або ознаками.

Блокчейн-реєстр – розподілена структура збереження даних про права, ліцензії, часові мітки та транзакції.

Валідація результатів – перевірка коректності висновків системи після детекції, пошуку збігів і зіставлення з реєстром.

Вбудовування – процес інтеграції ідентифікатора або водяного знака в структуру мультимедійного сигналу.

Верифікація – процедура підтвердження відповідності виявленого маркера, хешу або відбитка конкретному об’єкту чи запису в системі.

Видимий водяний знак – маркер, який безпосередньо помітний користувачеві.

Візуальна подібність – ступінь схожості між зображеннями або відеокадрами за структурними, локальними, глобальними чи ознаками, сформованими навченою моделлю.

Геометричні атаки – клас атак, що включає масштабування, поворот, зсув, обрізання та інші просторові зміни.

Глибоке навчання – клас методів машинного навчання на основі багатошарових нейронних мереж.

Десинхронізаційні атаки – перетворення, що ускладнюють правильне суміщення детектора з вбудованим маркером.

Детекція – процес виявлення факту наявності водяного знака або відновлення вбудованого повідомлення.

Доказова верифікація – відтворювана технічна процедура підтвердження походження, авторства або факту використання об’єкта.

Доказовий звіт – структурований документ із результатами перевірки, метриками, параметрами методів, часовими мітками та підставами для висновку.

Доказовий пакет – набір технічних, часових і реєстрових даних, достатній для обґрунтованого висновку.

Життєвий цикл мультимедійного об’єкта – послідовність етапів створення, реєстрації, вбудовування маркера, поширення, перевірки та фіксації подій.

Ємність каналу вбудовування – кількість інформації, яку можна вбудувати в носій без неприйнятного погіршення якості.

Зворотний пошук зображень – пошук тотожних або схожих зображень за їхнім цифровим відбитком або візуальними ознаками.

Ідентифікатор – структуроване інформаційне повідомлення з відомостями про автора, правовласника, об’єкт і технічні реквізити.

Індексування відбитків – побудова структури даних для швидкого пошуку збігів за фінгерпринтами.

Інтелектуальна власність на мультимедійні дані – сукупність прав на цифрові зображення, аудіо-, відео- та інші мультимедійні об’єкти.

Канал поширення контенту – середовище, через яке контент передається, копіюється, стискається, перекодовується або завантажується.

Ключ детекції / вбудовування – секретний або службовий параметр, що керує формуванням водяного знака та алгоритмом виявлення.

Колізія хешів – ситуація, коли різні об’єкти мають однакове хеш-значення.

Контентний відбиток – інша назва фінгерпринта; компактне подання ключових ознак контенту.

Кореляційна детекція – метод виявлення маркера через обчислення статистики подібності між очікуваним шаблоном і сигналом.

Криптографічний хеш – контрольне значення, обчислене хеш-функцією для перевірки цілісності та точних збігів.

Кропінг – обрізання частини зображення, відеокадру або аудіофрагмента.

Крихкий водяний знак – маркер, що руйнується навіть при незначній модифікації об’єкта.

Ліцензування – визначення й документування правомірних способів використання контенту.

Маркування – загальна назва процесів додавання до мультимедійного об’єкта службової, ідентифікаційної або захисної інформації.

Машинне навчання – клас алгоритмів автоматичного аналізу даних, що включає класичні статистичні та нейромережеві підходи.

Метадані – зовнішні описові дані про файл або об’єкт: автор, дата, формат, технічні параметри, ліцензія.

Модуль аудиту – компонент системи, що фіксує події реєстрації, пошуку, верифікації та інші дії.

Модуль доказової валідації – компонент системи, який зіставляє технічні результати перевірки з реєстровими даними.

Модуль пошуку збігів – компонент системи, що виконує пошук точних і близьких збігів за хешами, фінгерпринтами та ознаками.

Мультимедійний об’єкт – цифровий об’єкт, який містить зображення, звук, відео або їх поєднання.

Напівкрихкий водяний знак – маркер, що зберігається після незначних перетворень, але руйнується при суттєвих змінах.

Невидиме водяне маркування – вбудовування маркера без помітного для користувача погіршення якості контенту.

Непомітність – властивість системи не спричиняти суб’єктивно значущого погіршення якості після вбудовування.

Несліпа детекція – виявлення маркера з використанням оригінального або еталонного подання об’єкта.

Область перетворень – форма подання сигналу після застосування математичних перетворень, у якій виконується аналіз його характеристик або вбудовування інформації.

Об’єкт авторського права – результат творчої діяльності, який підлягає правовій охороні.

Організація колективного управління – інституція, що від імені правовласників здійснює ліцензування та супровід використання творів.

Перевірка формату доставки – повторне витягнення службового повідомлення після перекодування маркованого файлу у цільовий формат поширення.

Передискретизація (ресемплінг) – зміна частоти дискретизації сигналу з інтерполяцією та/або децимацією.

Перекодування – повторне стиснення або зміна формату мультимедійного файлу.

Перемеження – перестановка бітів або пакетів за заданим правилом для розподілу групових помилок і підвищення стійкості декодування.

Перцептивне маскування – адаптивне регулювання сили вбудовування відповідно до властивостей людського сприйняття.

Перцептивний хеш – хеш, що відображає змістову або перцептивну подібність між версіями одного об’єкта.

Підписані метадані – метадані, достовірність яких підтверджена криптографічним підписом.

Платформа UGC – онлайн-сервіс, у якому користувачі самостійно створюють, завантажують і поширюють контент.

Поетапна верифікація – послідовна перевірка об’єкта за криптографічним хешем, цифровим відбитком і вбудованим водяним знаком.

Помилкостійке кодування – спосіб подання даних із надлишковістю для відновлення повідомлення після спотворення.

Попередня перевірка придатності контейнера – процедура оцінювання декодованості, місткості, частки придатних кадрів, динамічного діапазону та стійкості контейнера до контрольного перекодування до виконання вбудовування.

Пропускна здатність каналу вбудовування – максимально можливий обсяг вбудовуваної інформації за заданих вимог до непомітності та стійкості.

Псевдографічно-диференціальний метод – метод захисту аудіоданих, що поєднує диференціальне подання енергетичного профілю, формування цифрового відбитка та DCT-QIM-вбудовування за співвідношенням енергій частотних смуг.

Реєстр правовласників та об’єктів – структурована база даних, що пов’язує мультимедійні активи з авторами, правами й історією перевірок.

Ремікс – похідна або комбінована форма використання контенту, характерна для цифрового середовища.

Робастність – здатність маркера зберігати детектованість або відновлюваність після типових атак і перетворень.

Робастний водяний знак – маркер, призначений для збереження працездатності після типових перетворень контенту.

Рознесення бітів – просторове, часове або частотне дублювання частин ідентифікатора для підвищення стійкості.

Розширений спектр – клас схем цифрового водяного маркування, у яких енергія маркера розподіляється по великій кількості компонентів носія.

Самоперевірка – витягнення службового повідомлення безпосередньо після вбудовування для підтвердження технічної коректності операції.

Семантичний склад ідентифікатора – мінімально необхідний набір полів структурованого повідомлення.

Синхромаркер – службова бітова послідовність для визначення початку пакета та відбраковування хибних результатів вилучення.

Сліпа детекція – виявлення маркера без доступу до оригінального немаркованого об’єкта.

Спектрограма – часово-частотне подання аудіосигналу.

Стегоаналіз – сукупність методів виявлення факту прихованого вбудовування інформації.

Стеганографія – клас методів прихованого розміщення інформації в цифровому контейнері.

Структуроване повідомлення – логічно організований набір полів, який формується перед вбудовуванням.

Часова мітка – мітка часу для фіксації моменту реєстрації, вбудовування, перевірки або іншої події.

Точний збіг – результат порівняння, коли файл або його контрольне подання повністю відповідає еталону.

Файл-екземпляр – конкретна цифрова копія мультимедійного об’єкта з власним байтовим поданням і метаданими.

Фінгерпринтинг – побудова стійких цифрових відбитків контенту для пошуку, ідентифікації та моніторингу використання.

Форензика мультимедійних даних – аналіз походження, автентичності, історії модифікацій та слідів обробки цифрового контенту.

Хибнонегативне рішення – рішення системи, за якого наявний маркер або реальний збіг не виявляється.

Хибнопозитивне рішення – рішення системи, за якого відсутній маркер або збіг помилково вважається присутнім.

Хешування – процес обчислення компактного контрольного значення для перевірки цілісності, ідентичності або прив’язки даних.

Цифровий відбиток (фінгерпринт) – компактне подання ключових ознак мультимедійного об’єкта для пошуку збігів.

Цифровий водяний знак – прихований або видимий маркер, що вбудовується в мультимедійний об’єкт для ідентифікації, захисту та відстеження використання.

Цифровий підпис – криптографічний механізм підтвердження цілісності та походження повідомлення, запису або метаданих.

Часово-частотне подання – форма подання сигналу, у якій одночасно враховано часові та спектральні властивості.

Шумова атака – внесення випадкових або квазивипадкових змін у сигнал, які ускладнюють детекцію маркера.

ВСТУП

Актуальність теми дослідження. У сучасному цифровому середовищі мультимедійні дані (зображення, відео, аудіо) стали одним із найбільш цінних і водночас найбільш уразливих об’єктів інтелектуальної власності. Цифровий контент є базою для медіаіндустрії, реклами, електронної комерції, освітніх продуктів, наукової комунікації та соціальних медіа. Відповідно, економічна мотивація порушень авторських прав (монетизація чужого контенту, «перезаливи», піратські бібліотеки, нелегальні каталоги, використання фрагментів без ліцензії) зростає пропорційно зростанню ринку цифрових платформ і доступності інструментів обробки медіа.

Масове поширення мультимедіа через інтернет, соціальні мережі та стрімінгові сервіси створює умови, коли копіювання, повторне використання і модифікація творів відбуваються практично миттєво й у глобальному масштабі. На відміну від традиційних носіїв, цифрові файли легко дублюються без деградації якості або з деградацією, що майже не сприймається користувачем. Типові «побутові» перетворення (перекодування відео, зміна роздільності, обрізання, накладання титрів/логотипів, нормалізація гучності, еквалізація, зміна темпу, перетворення формату) часто виконуються автоматично платформами та редакторами. Для правовласника ці операції ускладнюють доведення тотожності твору, підтвердження первинності та відстеження джерела походження.

Додатковим фактором ризику став стрімкий розвиток інструментів штучного інтелекту, зокрема генеративних моделей, здатних створювати або «перемальовувати» контент, імітувати стиль автора, синтезувати голос, реконструювати фрагменти з низькоякісних копій. У таких умовах класичні підходи до захисту (водяні знаки, підписи, реєстри) мають бути адаптовані: з одного боку – забезпечувати робастність (збереження ідентифікатора після перетворень), з іншого – підтримувати доказовість (фіксацію часу, незмінність, простежуваність подій і коректність ланцюга доказів).

Наявні системи захисту й пошуку збігів (на кшталт Content ID, Shazam, TinEye та подібних) демонструють високу ефективність у спеціалізованих сценаріях, однак їхня універсальність обмежена предметною областю (або типом медіаданих), набором еталонів, доступом до внутрішніх баз даних, а також залежністю від конкретних платформ. У практиці це означає, що один і той самий твір може потребувати різних процедур перевірки для різних середовищ, а відсутність єдиного підходу ускладнює масштабування захисту на всі типи мультимедіа та на різні «життєві цикли» контенту: від створення – до публікації, ліцензування, повторного використання, виявлення порушення та підготовки матеріалів для юридичного реагування.

Вагомий внесок у розвиток стеганографічних методів захисту мультимедійних даних та підвищення їхньої стійкості до атак зробили вітчизняні дослідники. У працях Г. В. Ахмаметьєвої розвинено методи стеганографічного вбудовування та цифрового водяного маркування зображень [50, 75, 235]. Теоретичні й прикладні засади комп’ютерної стеганографії систематизовано В. О. Хорошком, Ю. Є. Яремчуком та В. В. Карпінцем [238]; метод псевдовипадкового стеганографічного вбудовування в аудіоконтейнери запропоновано Є. С. Сулемою та Є. О. Радченком [236], а методи спектрального стегоаналізу цифрових зображень розвинено Д. О. Прогоновим та С. М. Кущем [237]. А. В. Соколов у співавторстві з А. А. Кобозєвою [76] та Ф. Чжаном [77] запропонував робастні методи керованого кодового вбудовування інформації та підвищення ефективності сліпого декодування. Питання застосування штучного інтелекту для аналізу мультимедійного контенту у сфері безпеки розглядаються у роботах О. Г. Трофименко зі співавторами [117]. Водночас питання побудови цілісної, доказово-орієнтованої інформаційної системи, яка поєднує різнорідні методи захисту мультимедійних даних (цифрові водяні знаки, стеганографію, фінгерпринтинг та засоби штучного інтелекту) в єдиному технологічному циклі, залишається розкритим недостатньо, що й зумовлює актуальність цього дослідження.

Отже, актуальним є створення комплексної інформаційної системи захисту інтелектуальної власності на мультимедійні дані, що ґрунтується на теоретично

обґрунтованих математичних моделях, алгоритмах та методах їх експериментальної верифікації і яка:

– має розвинений теоретико-математичний фундамент, що включає формальні моделі вбудовування та детектування цифрових ідентифікаторів, моделі типових перетворень і атак, критерії оцінювання непомітності, місткості та робастності, а також математичне обґрунтування властивостей запропонованих методів;

– підтримує вбудовані та зовнішні цифрові ідентифікатори (водяні знаки, стеганографічні мітки, цифрові підписи та хеші, QR-коди/мітки тощо);

– забезпечує перевірку робастності запропонованих методів до поширених перетворень і атак на основі формалізованих критеріїв та кількісних метрик;

– використовує AI/ML-методи для автоматизованої ідентифікації, пошуку ознак авторства та атрибуції мультимедійного контенту;

– забезпечує відтворювану експериментальну перевірку теоретичних положень і алгоритмічних рішень на реальних мультимедійних даних;

– формує доказовий пакет (журнал подій, параметри вбудовування, результати перевірок, метрики якості та робастності) для подальшого використання результатів у експертних і правових процедурах.

Саме поєднання класичних методів (стеганографія, цифрові водяні знаки, фінгерпринтинг) із сучасними підходами (машинне навчання, аналіз ознак, автоматизований пошук збігів і фіксація доказової інформації) формує основу для розв’язання проблеми універсального та практично застосовного захисту мультимедійних даних.

Мета і завдання дослідження – підвищення ефективності захисту інтелектуальної власності на мультимедійні дані шляхом розроблення та теоретичного обґрунтування математичних моделей, методів і алгоритмів стійкого вбудовування та ідентифікації цифрових ідентифікаторів, їх перевірки в умовах типових перетворень і атак та інтеграції розроблених рішень в інформаційну систему доказового захисту авторських прав.

Для досягнення мети поставлено такі завдання:

1. Проаналізувати та систематизувати сучасні методи захисту інтелектуальної власності на мультимедійні дані, визначити їхні функціональні та теоретичні обмеження, типові загрози й класи атак, а також сформувати вимоги до методів і засобів захисту мультимедійного контенту.

2. Розробити математичні моделі процесів вбудовування, вилучення та виявлення цифрових ідентифікаторів у мультимедійних даних з урахуванням параметрів контейнера, області вбудовування, сили вбудовування, надлишковості, синхронізації та параметрів захисту.

3. Розробити та теоретично обґрунтувати методи робастного вбудовування цифрових ідентифікаторів у зображення й аудіодані, спрямовані на забезпечення заданого компромісу між непомітністю, місткістю та стійкістю до типових перетворень і атак.

4. Розробити методи та критерії виявлення, ідентифікації й оцінювання достовірності цифрових ідентифікаторів, визначити умови коректного виявлення, пороги ухвалення рішень та показники помилкового виявлення й ідентифікації.

5. Розробити методи автоматизованого аналізу та атрибуції мультимедійного контенту на основі машинного навчання, визначити інформативні ознаки та/або репрезентації даних і дослідити їхню стійкість до модифікацій мультимедійних об'єктів.

6. Розробити та реалізувати комплексну інформаційну систему захисту інтелектуальної власності, що інтегрує розроблені методи вбудовування, виявлення та ідентифікації цифрових ідентифікаторів, засоби реєстрації мультимедійних об'єктів, журналювання подій та формування доказових звітів.

7. Провести комплексні експериментальні дослідження та оцінити ефективність розроблених методів і інформаційної системи за показниками непомітності, місткості, робастності, точності ідентифікації та помилок ухвалення рішень, визначити межі застосовності, надійні та граничні режими роботи й сформувати рекомендації щодо практичного використання.

Об’єкт дослідження – процес забезпечення захисту інтелектуальної власності у цифровому середовищі під час створення, поширення, модифікації та використання мультимедійних даних, включно з технічними й організаційними аспектами фіксації авторства та доказовості.

Предмет дослідження – методи й алгоритми вбудовування та виявлення цифрових ідентифікаторів у мультимедійних даних (зображеннях, відео, аудіо), методи формування ознак для фінгерпринтингу й автоматизованої атрибуції, а також інформаційні технології проєктування та реалізації системи, що забезпечує перевірку авторства, протоколювання подій і формування доказового пакета.

У межах предмету особливу увагу приділено балансу між:

– непомітністю (мінімальний вплив на якість/сприйняття),

– робастністю (збереження ідентифікаційних властивостей після перетворень),

– виявлюваністю та надійністю (стабільність детекції, контроль помилок),

– прикладною придатністю (зручність інтеграції, відтворюваність перевірок, зрозумілий вихід для експерта/юриста).

Методологія дослідження. Методологічну основу роботи становить поєднання теоретичних та експериментальних методів, спрямованих на проєктування, моделювання, реалізацію та оцінку ефективності системи захисту мультимедіа. У роботі застосовано:

– методи теорії інформації та цифрової обробки сигналів/зображень: аналіз шумів і спотворень, моделі компресії, фільтрації, перетворень у просторі та частоті, оцінювання впливу вбудовування на якість;

– математичні моделі стеганографії та цифрових водяних знаків: формалізація процесів вбудовування/детекції, опис параметрів схем, аналіз компромісу «непомітність–робастність», визначення порогів ухвалення рішень і помилок;

– алгоритми машинного навчання та нейронних мереж для аналізу мультимедійних даних: побудова ознак, ембедінгів, порівняння, класифікації,

пошуку найближчих відповідників; оцінка точності й стійкості моделей в умовах модифікацій;

– експериментальні дослідження стійкості системи до типових атак: формування набору перетворень, постановка експериментів за єдиним протоколом, застосування метрик якості/робастності, статистичний аналіз результатів, визначення граничних умов надійної роботи;

– програмну реалізацію та інженерні методи: проєктування архітектури модульної системи, реалізація сервісів і API, ведення журналів і відтворюваність експериментів; використання PHP та бібліотек/інструментів для роботи з мультимедіа, з урахуванням вимог продуктивності, збереження даних і безпеки.

Окремо підкреслено інженерний аспект методології: результати дослідження перевірено не лише на рівні «алгоритм працює», а й на рівні системної придатності – наскільки рішення масштабоване, повторюване, документоване і придатне до інтеграції в реальні процеси.

Наукова новизна одержаних результатів.

1. *Вперше* на основі умов коректного ухвалення рішення про наявність та достовірність ідентифікатора розроблено методи робастного вбудовування і виявлення цифрових ідентифікаторів у мультимедійних даних, які на відміну від відомих підходів забезпечують кероване співвідношення між непомітністю, місткістю й стійкістю до сукупності типових перетворень і атак, що дозволило за рівного рівня внесених спотворень підвищити частку успішної ідентифікації мультимедійного контенту після типових перетворень порівняно з класичними методами: для зображень – до 17,6 відсоткових пунктів (за масштабування), для аудіоданих – у 1,24–4,81 рази (зокрема з 28,0 до 88,7% після MP3-перекодування 64 кбіт/с).

2. *Удосконалено* статистичний підхід до ухвалення рішення про наявність прихованого ідентифікатора в мультимедійних даних. Для цього конкретизовано умови коректного ухвалення рішення про наявність та достовірність ідентифікатора з урахуванням статистичних характеристик контейнера, параметрів вбудовування, надлишкового кодування та рівня спотворень. Це

дозволило обґрунтувати критерії та пороги надійного виявлення і знизити ризик хибних рішень в умовах модифікації мультимедійних даних.

3. *Удосконалено* метод атрибуції мультимедійного контенту. Стеганографічні ідентифікатори в ньому поєднано з компактним детермінованим перцептивним відбитком (для аудіоданих це 64-бітний відбиток на основі псевдографічно-диференціального профілю сигналу) і допоміжним пошуком подібних об'єктів-кандидатів. Це забезпечує багаторівневе підтвердження належності цифрового об'єкта та збереження ідентифікації за наявності модифікацій, що дозволило підвищити достовірність автоматизованої атрибуції.

4. *Набула подальшого розвитку* методика попереднього оцінювання придатності мультимедійного контейнера до робастного вбудовування цифрового ідентифікатора за рахунок урахування його структурно-енергетичних характеристик, параметрів передбачуваних спотворень та доступного ресурсу вбудовування, що дозволяє до виконання операції маркування визначати можливість отримання заданого рівня непомітності та стійкості цифрового ідентифікатора.

5. *Набула подальшого розвитку* інформаційна технологія захисту інтелектуальної власності на мультимедійні дані за рахунок інтеграції розроблених математичних моделей, методів робастного маркування, засобів автоматизованої атрибуції та механізмів фіксації результатів перевірки, що дозволило створити інформаційну систему формування відтворюваної доказової бази щодо належності та цілісності мультимедійного контенту.

Практичне значення результатів. Практичне значення роботи полягає у можливості застосування розроблених методів і програмних засобів для реєстрації мультимедійних об’єктів, вбудовування та вилучення цифрових водяних знаків, формування цифрових відбитків, перевірки цілісності й походження контенту, а також документування результатів перевірки. Запропоновані рішення реалізовано в інформаційній системі IP-Protect, що забезпечує єдиний технологічний цикл оброблення графічних та аудіоданих.

Практичну ефективність розроблених методів підтверджено експериментально на наборах із 567 цифрових зображень і 150 аудіофайлів. Для зображень порівняння виконано за практично однакового рівня непомітності вбудовування: середній PSNR становив 55,88 дБ для запропонованого методу *wm_v2_dct_qim_profile* та 56,05 дБ для класичного DCT-QIM. Після JPEG-стиснення з параметром якості Q=75 коефіцієнт бітових помилок BER зменшився з 0,0482 до 0,0287, тобто на 40,5%. Після масштабування зображення з коефіцієнтом 0,5 частка успішного відновлення цифрового водяного знака зросла з 50,1% до 67,7%, тобто на 17,6 відсоткового пункту. За додавання гаусового шуму з σ=5 BER зменшився з 0,0376 до 0,0006, тобто на 98,4%, а частка успішного відновлення зросла з 93,3% до 99,8%. Експериментально встановленою межею методу є обрізання зображення на 10%, після якого частка успішного відновлення становила 1,1%.

Для аудіоданих авторський псевдографічно-диференціальний метод *audio_pgdiff_v2* після MP3-перекодування зі швидкістю 128 кбіт/с забезпечив зменшення BER з 0,1033 для класичного методу розширеного спектра до 0,0100, тобто на 90,3%, а частка успішного відновлення цифрового водяного знака зросла з 79,3% до 98,0%. За MP3 64 кбіт/с BER зменшився з 0,3600 до 0,0567, тобто на 84,3%, а частка успішного відновлення зросла з 28,0% до 88,7%. Після чотириразової передискретизації цифровий водяний знак успішно відновлено у 100% файлів проти 26,7% для класичного методу. На модифікованих кадрах показник сегментного відношення сигнал/шум segSNR становив 12,66 дБ проти 3,25 дБ для класичного методу. Попередня перевірка придатності контейнера дає змогу до початку вбудовування визначати аудіофайли, для яких задані показники стійкості не можуть бути забезпечені.

Одержані результати можуть бути використані під час побудови та вдосконалення систем захисту мультимедійного контенту у вебсервісах, медіабібліотеках, освітніх інформаційних системах, корпоративних архівах і сервісах поширення цифрових матеріалів; для маркування ліцензійних копій, перевірки відповідності досліджуваного файлу зареєстрованому цифровому

активу та виявлення повторного використання контенту; для контролю збереження цифрових водяних знаків після стиснення, передискретизації, масштабування, додавання шуму та інших типових перетворень.

Практичну цінність має також можливість формування системою стандартизованого технічного звіту, що містить ідентифікатори цифрового активу, криптографічне хеш-значення SHA-256, цифровий відбиток, параметри вбудовування та вилучення, перелік виконаних перетворень, отримані метрики й підстави для ухвалення рішення щодо відповідності досліджуваного об’єкта зареєстрованому активу. Такий звіт може бути використаний як складова доказового пакета під час технічної або судової експертизи, зменшуючи суб’єктивність оцінювання та забезпечуючи відтворюваність проведеної перевірки.

Практичну цінність і можливість використання одержаних результатів у професійній діяльності підтверджено довідками та актами, наданими ПАТ «ОДЕСКАБЕЛЬ», ТОВ «КІПСОЛІД УКРАЇНА», Державною службою спеціального зв’язку та захисту інформації України, а також Управлінням протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України.

Результати дослідження впроваджено в освітній процес Національного університету «Одеська юридична академія» під час викладання навчальних дисциплін «Експертиза та перевірка цілісності мультимедійних даних», «Цифрові водяні знаки», «Прикладна криптографія», «Системи аутентифікації та цифрової ідентифікації», «Адміністрування, аудит та безпека вебсистем», «Цифрові технології в бізнесі», «IT-маркетинг», «Основи IT-бізнесу», «DevOps» та «DevSecOps». Окремі положення дисертації, програмний прототип IP-Protect і розроблені методичні матеріали використовуються під час проведення лабораторних занять, виконання індивідуальних завдань, підготовки кваліфікаційних робіт і науково-дослідної роботи здобувачів освіти.

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею. Усі наукові положення, результати, висновки та практичні рекомендації, винесені на захист, одержані здобувачем особисто. Здобувачем

самостійно сформульовано мету і завдання дослідження, розроблено математичні моделі та удосконалено методи вбудовування цифрових водяних знаків у мультимедійні дані, спроєктовано й програмно реалізовано інформаційну систему IP-Protect, сформовано набори тестових даних, проведено експериментальні дослідження та здійснено аналіз одержаних результатів.

Праці [2–4, 6, 8–15, 17–21, 23, 24] є одноосібними. У цих публікаціях здобувачем досліджено методи вбудовування інформації в аудіо- та графічні файли, цифрового водяного маркування, перцептивного хешування та формування цифрових відбитків; розроблено й удосконалено алгоритми ідентифікації мультимедійного контенту; обґрунтовано засади доказово-орієнтованого захисту прав інтелектуальної власності; запропоновано способи поєднання цифрових водяних знаків, цифрових відбитків, метаданих і засобів штучного інтелекту в межах єдиної інформаційної системи; визначено підходи до автоматизованого моніторингу поширення мультимедійного контенту, перевірки його цілісності та походження.

У співавторстві опубліковано праці [1, 5, 7, 16, 22]. Особистий внесок здобувача в ці праці полягає в такому: у праці [1] виконано аналіз технічних засобів захисту аудіовізуальної продукції та обґрунтовано поєднання технологій цифрового маркування й ідентифікації контенту з нормативно-правовими процедурами охорони інтелектуальної власності; у праці [5] досліджено технічні методи ідентифікації, маркування та контролю поширення цифрового контенту, а також сформульовано рекомендації щодо їх застосування у процесах рекламного менеджменту; у праці [7] розроблено концепцію, функціональну та програмну архітектуру інформаційної системи IP-Protect, визначено склад її модулів і механізми їх взаємодії, реалізовано програмний прототип та проведено перевірку його працездатності; у праці [16] розроблено програмні реалізації методів широкосмугового та фазового кодування цифрових водяних знаків в аудіосигналі, сформовано протокол експерименту, проведено порівняльне тестування методів та проаналізовано одержані результати; у праці [22] виконано аналіз інформаційної складової процесів інтеграції об’єктів Smart Grid

до системи кіберзахисту критичної інфраструктури та сформульовано пропозиції щодо забезпечення захисту і контролю цілісності даних.

Комп'ютерну програму «Інформаційна система захисту інтелектуальної власності на мультимедійні дані IP-Protect» розроблено здобувачем особисто, що підтверджено Свідоцтвом про реєстрацію авторського права на твір № 149653. Результати, що належать співавторам опублікованих праць, у дисертації не використовувалися.

Апробація результатів дисертації. Основні положення та результати дисертаційного дослідження доповідалися й обговорювалися на міжнародних та всеукраїнських науково-практичних конференціях, серед яких:

1. Міжнародна науково-практична конференція «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика», м. Одеса, Україна, 24 листопада 2023 р.

2. Міжнародна науково-практична конференція «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів», м. Одеса, Україна, 26 квітня 2024 р.

3. IX Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи», м. Одеса, Україна, 24 травня 2024 р.

4. V Міжнародна науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики», м. Одеса, Україна, 24 листопада 2024 р.

5. Міжнародна науково-практична конференція «Європейські орієнтири розвитку України: нові виміри у воєнний час», м. Одеса, Україна, 16 травня 2025 р.

6. X Всеукраїнська науково-практична конференція «Інформаційне суспільство: проблеми та перспективи», м. Одеса, Україна, 23 травня 2025 р.

7. 2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek 2025), м. Харків, Україна, 2025 р.

8. VI Міжнародна науково-практична конференція «Кібербезпека в сучасному світі: актуальні виклики», м. Одеса, Україна, 28 листопада 2025 р.

9. Міжнародна науково-практична конференція «Scientific Horizons: Digital Transformation», м. Пекін, Китай, 20 березня 2026 р.

10. Міжнародна науково-практична конференція «Global Interdisciplinary Summit: Frontier of Science and Future Technologies», м. Дубай, Об'єднані Арабські Емірати, 3 квітня 2026 р.

Публікації. Основні положення та результати дисертаційного дослідження відображено у 24 наукових працях, з яких 10 публікацій розкривають основний зміст дисертації, зокрема 8 статей у наукових періодичних виданнях та 2 розділи у колективних монографіях. Сім статей опубліковано у наукових фахових виданнях України, одну – у зарубіжному науковому виданні. Апробацію матеріалів дисертації засвідчують 14 публікацій у збірниках матеріалів і праць міжнародних та всеукраїнських науково-практичних конференцій. Із загальної кількості наукових праць 19 опубліковано одноосібно, 5 – у співавторстві (Додаток А). Крім того, практичну реалізацію результатів дослідження підтверджено Свідоцтвом про реєстрацію авторського права на твір № 149653 на комп'ютерну програму «Інформаційна система захисту інтелектуальної власності на мультимедійні дані IP-Protect» (Додаток Б).

Структура та обсяг роботи. Дисертація складається зі вступу, чотирьох розділів, висновків, списку використаних джерел і додатків.

У першому розділі проаналізовано сучасний стан проблеми захисту інтелектуальної власності на мультимедійні дані, розглянуто правові, технічні й організаційні аспекти обігу цифрового контенту, класифіковано методи захисту та стеганографічні методи, досліджено наявні системи захисту авторських прав і можливості застосування штучного інтелекту. Проаналізовано структуру зображень, аудіо- та відеоданих як контейнерів для прихованого вбудовування інформації, визначено компоненти мультимедійних файлів, придатні для маркування, метрики оцінювання непомітності й стійкості, а також формальні моделі перетворень та атак.

У другому розділі розроблено математичні моделі й удосконалено методи вбудовування цифрових водяних знаків у мультимедійні дані. Сформульовано критерії ефективності та методику експериментального порівняння методів, досліджено побітове і статистичне вбудовування, методи на основі дискретного

та модифікованого дискретного косинусних перетворень, квантувальної індексної модуляції, розширення спектра, ехо-приховування й кодування через співвідношення енергій частотних підсмуг. Наведено результати порівняльного експериментального оцінювання розроблених і класичних реалізацій за показниками непомітності та стійкості до типових перетворень і атак.

У третьому розділі розроблено та формально описано запропоновані методи захисту мультимедійних даних: удосконалений метод DCT-QIM для вбудовування цифрового водяного знака в зображення та псевдографічно-диференціальний метод audio_pgdiff_v2 для захисту аудіоданих. Для запропонованих методів наведено математичні моделі, алгоритми вбудовування й вилучення, теоретичне обґрунтування, результати експериментальної перевірки та порівняння з класичними й нейромережевими підходами. Сформульовано положення наукової новизни, визначено переваги та обмеження запропонованих рішень.

У четвертому розділі розроблено архітектуру та програмно реалізовано інформаційну систему IP-Protect. Описано її користувацький інтерфейс, публічний режим перевірки, реєстр мультимедійних активів, бібліотеку цифрових водяних знаків і цифрових відбитків, криптографічні механізми, підсистему поетапної верифікації, доказове звітування, модулі ліцензування та штучного інтелекту, а також засоби безпеки, аудиту й керування параметрами системи. Проведено порівняльний аналіз IP-Protect з наявними класами систем захисту авторських прав.

У висновках узагальнено основні наукові та практичні результати дослідження. У додатках наведено список публікацій здобувача, копію Свідоцтва про реєстрацію авторського права на комп’ютерну програму IP-Protect і допоміжні порівняльні таблиці.

Загальний обсяг дисертації становить 267 сторінок. Робота містить 41 рисунок, 47 таблиць, список використаних джерел із 243 найменувань та 4 додатки.

РОЗДІЛ 1. ОГЛЯД ЛІТЕРАТУРИ ТА СУЧАСНОГО СТАНУ ПРОБЛЕМИ

1.1. Інтелектуальна власність у цифровому середовищі: основні проблеми та загрози

У другій половині XX – на початку XXI ст. розвиток цифрових технологій докорінно змінив умови створення, зберігання та обігу об'єктів інтелектуальної власності (ІВ). На відміну від традиційних матеріальних носіїв, цифрові файли дублюються необмежену кількість разів без втрати якості, а їхній обіг відбувається переважно в межах глобальних онлайн-платформ, що функціонують поза територіальними межами юрисдикцій. Це радикально посилює ризики несанкціонованого відтворення та поширення мультимедійних творів – зображень, аудіо- та відеозаписів – і породжує колізії національних правопорядків щодо застосовного права та компетентного органу.

Окремими чинниками вразливості є «культура реміксу» й користувацький контент (UGC), за якої твори масово переробляються та комбінуються, а також швидке поширення генеративного штучного інтелекту, що дає змогу створювати контент, який імітує наявні твори за стилем і структурою. У таких умовах ускладнюється встановлення авторства та меж правомірного використання, а найнебезпечнішими для правовласників стають онлайн-піратство аудіо- та відеопродукції, несанкціоноване використання зображень і масове «перезавантаження» відео без збереження інформації про автора. Традиційні юридичні механізми (реєстрація прав, ліцензійні договори, судовий захист) залишаються необхідними, проте виявляються недостатніми там, де саме виявлення порушення та ідентифікація джерела є нетривіальним завданням.

Через це зростає роль програмно-технічних засобів охорони ІВ, що доповнюють правове регулювання: систем керування цифровими правами (DRM), криптографічних механізмів автентифікації й контролю доступу, а також методів прихованого маркування мультимедійних даних – цифрових водяних знаків та стеганографічних схем. На відміну від зовнішніх засобів контролю,

останні передбачають вбудовування у сам об'єкт спеціального ідентифікатора, що зберігається навіть після копіювання, перекодування чи обмежених модифікацій файлу. Саме в такому контексті постає завдання розробки інформаційної системи, яка забезпечуватиме стійке, невидиме для користувача маркування мультимедійних об'єктів та засоби подальшої верифікації їх належності конкретному автору чи правовласнику.

Аналіз наукової літератури виявляє, що теоретико-правові дослідження захисту ІВ у цифрову добу сформувалися як відповідь на трансформацію способів створення й поширення контенту в мережевому середовищі, причому центр проблематики поступово змістився від правовстановлення до практичної реалізації та примусового захисту прав: оперативного виявлення порушень, ідентифікації джерела обігу й забезпечення доказовості [1–5]. Водночас між джерелами простежується принципова розбіжність щодо пріоритету регуляторних інструментів. Одна група авторів вважає достатньою адаптацію класичних інститутів авторського права до онлайн-реалій та посилення відповідальності посередників [6–10], тоді як інша – виходить із того, що правова норма без технічного інструментарію атрибуції, трасування витоків і фіксації модифікацій залишається декларативною [33, 34, 57, 65, 88]. Слід зауважити, що більшість праць обох груп спирається на аналіз нормативних актів і судової практики, а не на експериментальну перевірку ефективності технічних засобів, тому їхні висновки про достатність чи недостатність тих чи інших механізмів мають переважно гіпотетичний характер.

Показовою в цьому сенсі є праця В. Тумалавічуса та співавторів [11], де цифровізація розглядається як фактор, що змінює весь життєвий цикл об'єктів ІВ – від створення до доказування порушень; проте запропоновані авторами узагальнення базуються переважно на досвіді європейських юрисдикцій, що обмежує їхню пряму застосовність до українського правопорядку. Українські дослідження [12, 13], навпаки, фіксують специфічну для національного контексту проблему: формальна наявність прав не забезпечує їхньої практичної реалізації через складність ідентифікації порушника, транскордонність

незаконного обігу та обмежену ефективність традиційних цивільно-правових засобів; першочергового значення набуває доказовий аспект – надійна прив'язка конкретного об'єкта до правовласника та фіксація історії його використання. При цьому робота В. Воронкової та співавторів [13], хоча й слугує теоретичною основою для систематизації загроз саме для мультимедійних даних, не містить кількісної оцінки реальної частоти таких загроз, що залишає відкритим питання про пріоритезацію напрямів захисту. Аналіз директив ЄС 2019/789 та 2019/790 [14, 15] демонструє тенденцію до посилення ролі онлайн-платформ у забезпеченні авторського права, за якої навіть за жорстких директивних вимог захист фактично спирається на програмно-технічні засоби – автоматизовані фільтри, системи типу Content ID та інші інструменти моніторингу. Проте література розходиться в оцінці ефективності цих засобів: частина джерел вважає автоматизовану фільтрацію достатнім механізмом охорони [14, 15], тоді як інші фіксують високу частку помилкових спрацьовувань і блокувань правомірного контенту [11–16]. Ця суперечність безпосередньо актуалізує потребу в точніших методах ідентифікації мультимедійних файлів на основі невидимих стійких маркерів, здатних знизити похибку автоматизованої фільтрації.

Економічні та поведінкові виміри проблеми також характеризуються неоднозначністю висновків. Теоретичні моделі цифрового піратства – від базових схем копіювання до моделей із мережевими ефектами й асиметрією інформації – узгоджено показують, що практична тотожність копій і оригіналів за якістю радикально посилює ризики для правовласників [17, 22–26]. Водночас емпіричні дослідження дають суперечливі результати щодо ефективності репресивних заходів: одні фіксують помірне скорочення піратського трафіку після блокувань і заходів типу «follow-the-money» [18–21], інші – доводять стійкість попиту на піратський контент попри репресії [27], причому розбіжність оцінок значною мірою пояснюється відмінностями методик вимірювання та використаних вибірок, що унеможливлює їхнє пряме зіставлення. Поведінкові студії [28–32] засвідчують, що піратські практики підтримуються не лише ціною

чи відсутністю легальної альтернативи, а й соціальними нормами та низьким суб'єктивним ризиком покарання; проте ці дослідження виконані переважно на вибірках користувачів окремих країн і платформ, тому їхня узагальнюваність потребує обережності.

Новітні публікації дедалі частіше фокусуються на проблемах автентичності й походження контенту в умовах генеративного ШІ та deepfake-технологій, коли традиційні атрибутивні маркери (метадані, видимі водяні знаки) можуть бути вилучені або сфальсифіковані. При цьому в технічній літературі зберігається нерозв'язане протиріччя щодо стійкості самих методів прихованого маркування: частина авторів фіксує достатню стійкість вбудованих ідентифікаторів до перекодування й геометричних перетворень, тоді як інші демонструють їхню вразливість до масштабування, компресії та навмисних атак на стеганографічний шар, – причому результати суттєво залежать від обраних датасетів і тестових сценаріїв, що ускладнює об'єктивне порівняння підходів [33, 34, 57, 65, 88]. У такій постановці захист ІВ набуває ознак комплексної задачі, у якій правові норми доповнюються інструментами технічно підтверджуваної прив'язки об'єкта до суб'єкта права та підтримання доказового ланцюжка.

Проведений огляд дає змогу окреслити коло питань, які в наявній літературі залишаються нерозв'язаними або розв'язаними частково: (1) відсутність уніфікованої методики порівняння стійкості методів прихованого маркування до типових перетворень мультимедіа; (2) недостатня дослідженість інтеграції прихованих ідентифікаторів з інформаційними системами обліку авторів і правовласників, без якої технічний маркер не набуває доказової сили; (3) розрив між нормативними вимогами до автоматизованої фільтрації контенту та реальною точністю її роботи; (4) обмежена застосовність наявних емпіричних узагальнень до українського правового й технічного контексту. Саме на подолання цих прогалин спрямовано подальші розділи дисертації, у яких обґрунтовується доцільність застосування прихованих стійких ідентифікаторів, вбудованих у структуру мультимедійних даних, у поєднанні з відповідною інформаційною системою та базою даних авторів і правовласників.

1.2. Методи захисту мультимедійних даних

У цьому підрозділі розглядаються методи захисту мультимедійних даних як поєднання правових вимог із технологічними механізмами, що забезпечують атрибуцію, контроль цілісності, виявлення несанкціонованого обігу та доказовість у цифровому середовищі. У науковій літературі підкреслюється, що жоден окремий метод не є самодостатнім: ефективна охорона потребує комбінації підходів, адаптованої до типу мультимедійного об'єкта, каналу розповсюдження та конкретного сценарію загрози.

На рис. 1.1 наведено загальну класифікацію методів захисту мультимедійних даних, що застосовується у сучасній науковій літературі [34–37, 39, 42, 68].

Перший клас підходів становлять превентивні засоби: DRM/TPM (Digital Rights Management / Trusted Platform Module – цифрове управління правами / довірений платформний модуль), шифрування, контроль доступу й ліцензування, які знижують імовірність копіювання або ускладнюють його на рівні платформи/пристрою. Однак після виходу контенту з DRM-середовища (екранний запис, аналогова копія, перекодування) такий захист фактично зникає.

Другий клас – атрибутивні та трасувальні методи: видимі/невидимі цифрові водяні знаки (ЦВЗ), фінгерпринтинг і стійкі ідентифікатори, які дозволяють пов’язати конкретний екземпляр файлу з правовласником або легальним каналом розповсюдження. Огляди зосереджують увагу на класичному компромісі «непомітність–робастність–місткість», наведеному на рис. 1.2.

Третій клас підходів – аутентифікація та контроль цілісності (крихкі/ напівкрихкі водяні знаки, криптографічні хеші, електронні підписи, часові мітки). Ці механізми фіксують факт зміни «канонічної» копії та дозволяють відрізняти допустимі технічні операції від несанкціонованої модифікації. Окремо виділяють методи пошуку збігів і моніторингу обігу: контент-матчинг, перцептивне хешування, CBIR-підходи (Content-Based Image Retrieval – пошук зображень за вмістом), які підтримують оперативне виявлення копій і похідних версій у мережі. Такі підходи часто розглядають як «операційний контур» системи захисту, що замикає цикл від маркування до виявлення порушень.

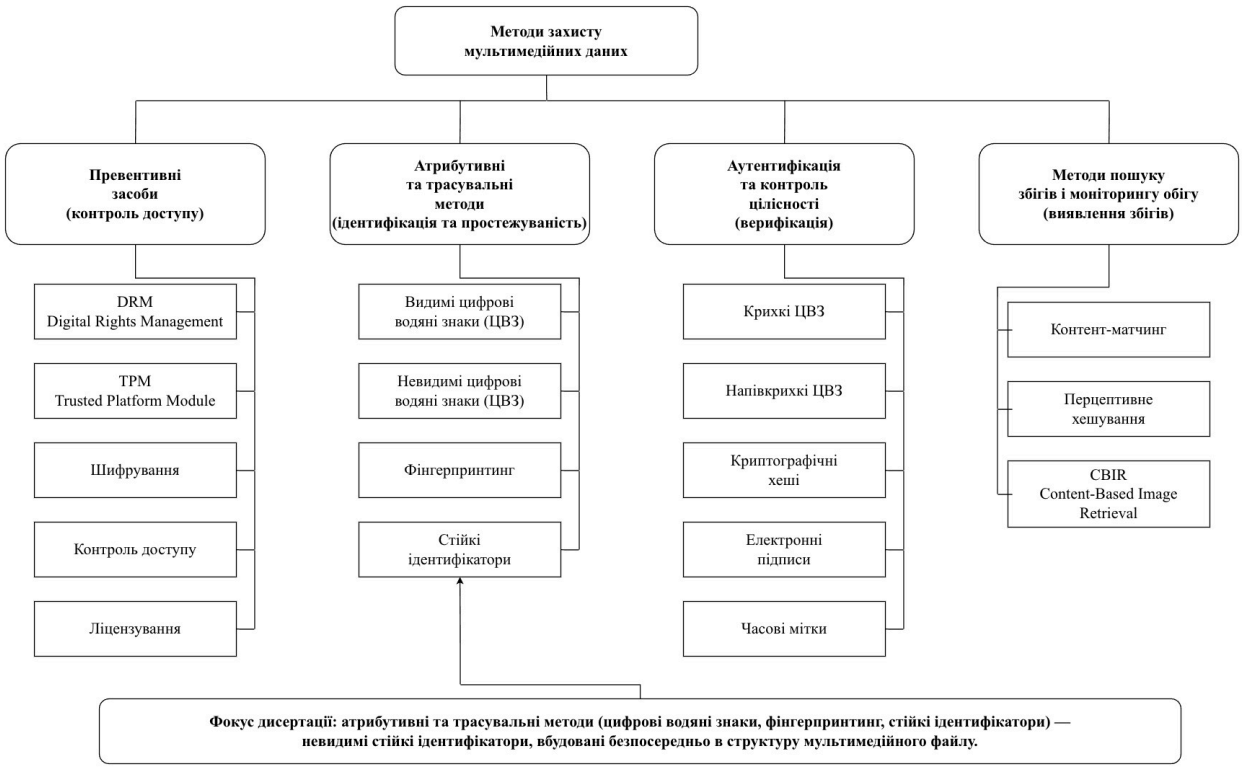


Рисунок 1.1 – Класифікація методів захисту мультимедійних даних за функціональним призначенням

(Джерело: складено автором)

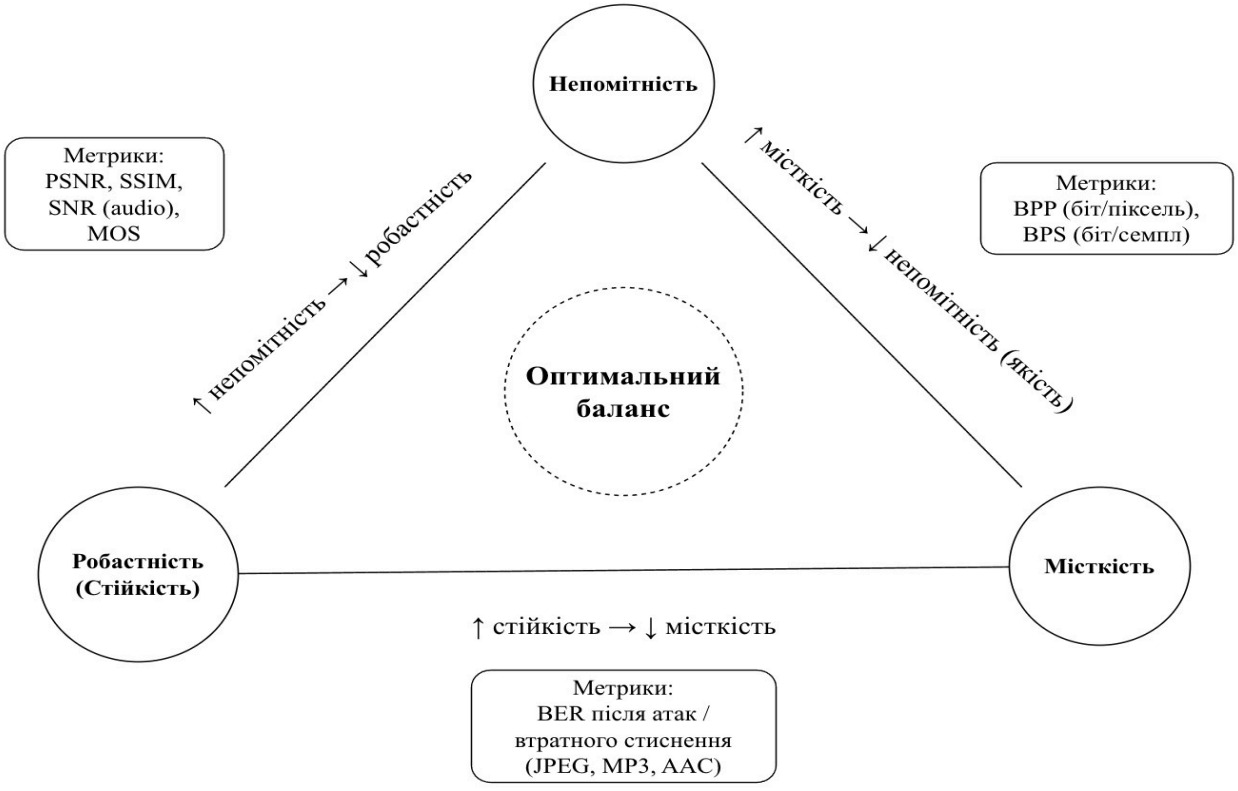


Рисунок 1.2 – Тріада властивостей цифрових водяних знаків: місткість – непомітність – робастність (стійкість)

(Джерело: узагальнено автором за [38, 39, 41])

У цій дисертаційній роботі напрацьована концепція компромісу «робастність/непомітність/ємність» використано як теоретичний каркас для формування вимог до підсистеми маркування аудіофайлів. Класифікація атак і метрик, запропонована авторами (Salah та ін.), дозволяє формалізувати перелік спотворень, до яких мають бути стійкими невидимі ідентифікатори [39]. Узагальнену класифікацію атак на цифрові водяні знаки, використану для формування моделі спотворень, наведено на рис. 1.3.

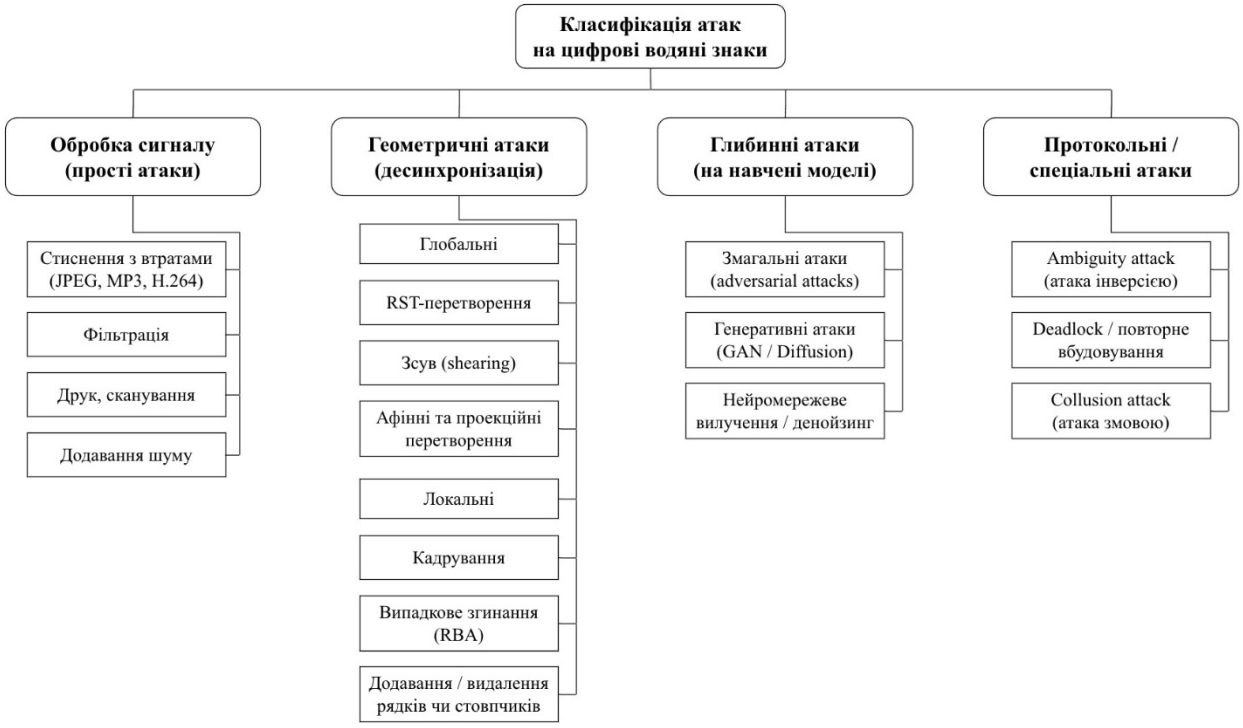


Рисунок 1.3 – Класифікація атак на цифрові водяні знаки

(Джерело: складено автором)

У рамках розроблюваної інформаційної системи ці результати використано для вибору класу алгоритмів вбудовування (зокрема, у частотній або часово-частотній області з урахуванням моделі слухової системи людини) і для визначення цільових порогових значень показників якості, які забезпечують одночасно достатній рівень суб’єктивної невідчутності спотворень та надійне відновлення маркера в умовах реального використання аудіоконтенту.

У статті І. Зубка, В. Мартовицького, А. Пунченка та Д. Карачевцева систематизовано методи вбудовування цифрових водяних знаків (ЦВЗ) у

растрові зображення: просторові, частотні (DCT/DWT) і текстурноорієнтовані [35]. Їх розглянуто за непомітністю маркування, стійкістю до типових атак і обчислювальною складністю; також відзначено компроміс між непомітністю, робастністю та ємністю ЦВЗ. Така класифікація допомагає визначити критерії добору методів, однак не встановлює їхньої універсальної переваги, оскільки результати залежать від алгоритму й умов тестування.

Це підтверджує порівняльний експеримент у дисертації: на наборі з 567 зображень запропонований DCT-QIM за близького рівня непомітності (PSNR 55,88 дБ проти 56,05 дБ у класичного методу) знизив BER після JPEG-стиснення Q=75 з 0,0482 до 0,0287. Водночас за масштабування до 50% виживання маркера становило лише 67,7%, а після обрізання 10% – 1,1% (табл. 3.3). Отже, відкритим залишається питання забезпечення стійкості до різних типів атак без погіршення непомітності; розроблений метод поліпшує результати для JPEG-стиснення, але не усуває обмежень за масштабування й обрізання.

В. Ван та співавтори зосереджуються на робастних методах маркування зображень і їхній стійкості до геометричних та комбінованих атак [38]. В оглядах аудіомаркування методи класифікують за областю вбудовування й схемою виявлення, а атаки – як ненавмисні та навмисні [39–41]. Зіставлення цих праць виявляє спільний компроміс між стійкістю, непомітністю та ємністю маркера. Водночас результати для зображень і аудіо не можна безпосередньо порівнювати, оскільки джерела розглядають різні атаки й критерії оцінювання, зокрема SNR, ODG та ймовірність виявлення. Отже, невирішеним залишається питання відтворюваного порівняння методів за узгоджених умов. У дисертації це враховано через окреме тестування методів для кожного типу даних із використанням відповідних атак і метрик.

Цифрове водяне маркування відеоданих ускладнюється просторово-часовою природою сигналу: окрім непомітності в межах кадру, алгоритм має забезпечувати стабільність маркера в часі та стійкість до перекодування, зміни бітрейту, масштабування, монтажу й кадрування за прийнятних обчислювальних витрат для потокових сценаріїв. Методи відеомаркування систематизують за

областю вбудовування (просторові, частотні на основі DCT/DWT на рівні кадрів або груп кадрів, компресійні/бітстрімові у структурах H.264/AVC, H.265/HEVC), причому пріоритет дедалі частіше зміщується у бік області стисненого подання, оскільки повторне перекодування платформами є найпоширенішою атакою. Окремою проблемою є ефект дрейфу (drift) через міжкадрове прогнозування, для протидії якому застосовують спеціальний добір кадрів і коефіцієнтів, обмеження модифікацій та адаптивні стратегії під параметри кодера, а також нейромережеві підходи, оптимізовані під конкретні втрати стиснення [42–45, 46– 49].

Окремий напрям становлять гібридні криптографічно-стеганографічні підходи, які розглядають як «дворівневий» механізм захисту: криптографія забезпечує конфіденційність і контроль доступу, а приховане маркування – непомітність факту вбудовування та зв'язок даних із контейнером. Найпоширенішою є схема encrypt-then-embed, у якій дані спочатку шифруються (часто AES), а потім вбудовуються методами просторової чи частотної стеганографії з рандомізацією позицій та перевірками цілісності; розвиваються також адаптивні багатошарові методи, де вибір криптоалгоритму й параметрів вбудовування здійснюється за метриками якості та стійкості. Репрезентативні реалізації поєднують криптографію з водяними знаками у захищеному апаратному середовищі, спільне керування ключами та маркерами із застосуванням схеми розподілу секрету, вбудовування зашифрованих QR-кодів в області DWT–SVD-перетворення, а також гіперхаотичне шифрування з компресійним відновленням маркера, що демонструє доцільність інтеграції криптографічних і стеганографічних механізмів у єдину архітектуру захисту зображень, аудіо та відео [55–59, 60–64].

Стаття Г. Хуа та співавторів систематизує розвиток аудіо-водяних знаків, класифікуючи методи за областю вбудовування та розглядаючи непомітність, робастність і ємність маркера [41]. Автори також аналізують застосування психоакустичних моделей для зменшення чутності вбудованих даних. Водночас цей огляд не встановлює універсально найкращого способу маркування: порівняння методів ускладнюють відмінності між експериментальними

умовами, наборами даних і критеріями оцінювання. Зокрема, використання психоакустичної моделі саме по собі не гарантує стійкості до часових змін сигналу чи інших атак; сучасніші огляди [39, 40] доповнюють цю систематизацію, але також не замінюють випробування конкретного алгоритму.

У дисертації авторський метод audio_pgdiff_v2 перевірено на 150 аудіофайлах: після MP3-перекодування зі швидкістю 128 кбіт/с BER становив 0,010, а після передискретизації ×4 маркер відновлено у 100% файлів. Водночас стійкість методу до зміни часової шкали та агресивного AAC-перекодування потребує окремої перевірки. Отже, огляд [41] задає теоретичну основу, тоді як експерименти дисертації оцінюють конкретний метод лише за визначених умов і виявляють напрям для подальшого дослідження.

У науковій літературі цифрове водяне маркування відеоданих розглядають як один із ключових технічних механізмів практичної реалізації авторського права в умовах домінування стримінгу та платформного розповсюдження контенту. На відміну від зображень, відео має просторово-часову природу: окрім непомітності (imperceptibility) у межах окремого кадру, алгоритм має забезпечувати стабільність маркера в часі, стійкість до типових трансформацій (перекодування, зміна бітрейту, масштабування, монтаж, кадрування, накладання субтитрів/логотипів), а також прийнятні обчислювальні витрати для потокових сценаріїв. Тому дослідники підкреслюють компроміс «місткість–непомітність–робастність», який у відео ускладнюється ще й вимогами реального часу та обмеженнями кодеків. Узагальнену класифікацію методів відеомаркування за областю вбудовування наведено на рис. 1.4.

Як видно з рис. 1.4, методи відеомаркування охоплюють просторові підходи, методи області перетворень і методи, що працюють зі структурами стисненого відеопотоку. Для платформного розповсюдження особливе значення мають методи двох останніх класів, оскільки вони враховують структуру відеокодеків і типове повторне перекодування контенту.

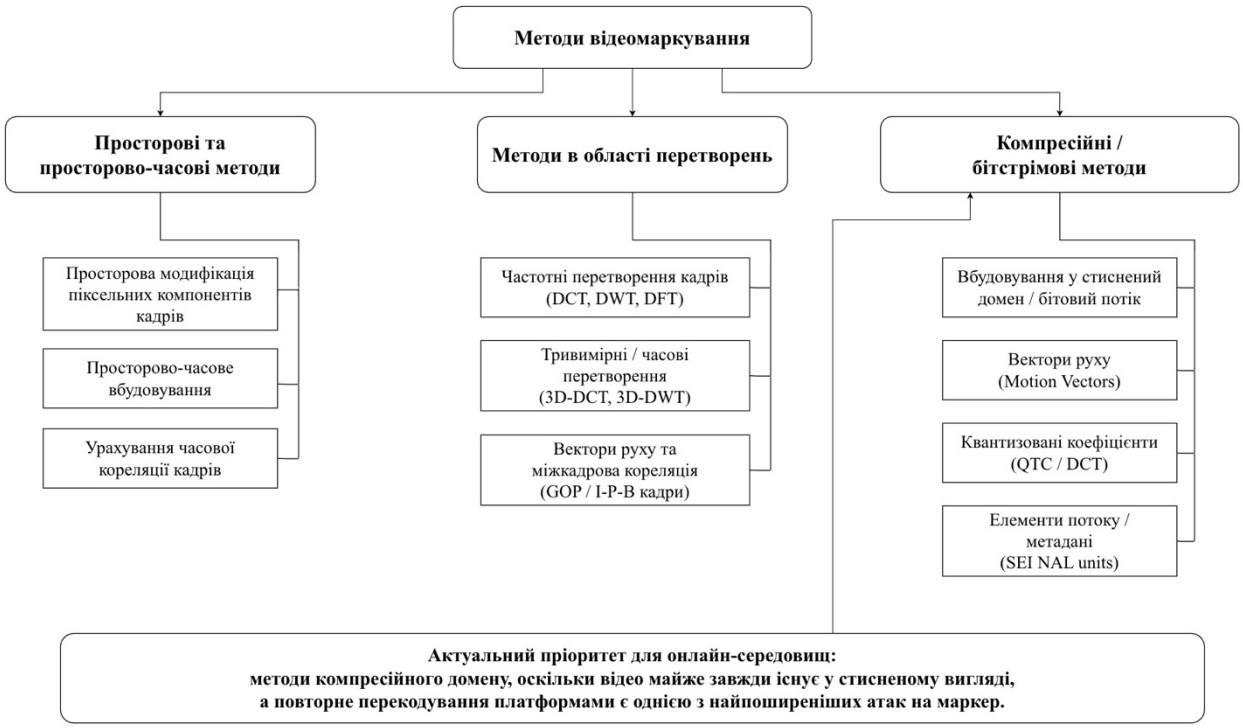


Рисунок 1.4 – Класифікація методів відеомаркування

(Джерело: складено автором)

1.3. Класифікація та характеристики стеганографічних методів

Доцільно подати стеганографію як частину ширшого напряму information hiding, де ключовою ознакою є приховування самого факту передавання/наявності повідомлення у мультимедійному контейнері. У літературі підкреслюється, що систематизація методів є необхідною передумовою для коректного вибору алгоритмів під конкретні вимоги безпеки, оскільки різні класи стеганографії суттєво відрізняються за стійкістю до атак, непомітністю та придатністю до практичних сценаріїв.

Класифікацію стеганографічних методів зазвичай будують за кількома «осями». По-перше, за типом контейнера: зображення, аудіо, відео, текст, мережеві протоколи/файлова система, що важливо для мультимедійних систем через різну надлишковість і різні «канали» модифікації (пікселі, спектральні компоненти, кадри, службові поля тощо). По-друге, за областю вбудовування: просторовий (LSB-подібні), перетворювальний (DCT/DWT та ін.),

бітстрімовий/компресійний (вбудовування під час кодування), а також адаптивні підходи, де вибір областей/коефіцієнтів залежить від локальних властивостей сигналу. Такі рамки систематизації прямо підтримуються українськими оглядовими роботами, які описують як «цифрову» (мультимедійну), так і мережеву/системну стеганографію. Узагальнену класифікацію стеганографічних методів за типом мультимедійного контейнера та областю вбудовування наведено на рис. 1.5.

Окремо в літературі виділяють класифікаційні ознаки, що безпосередньо пов'язані з вимогами захисту: blind/non-blind (чи потрібен оригінальний контейнер для вилучення), reversible/irreversible (чи відновлюється контейнер без втрат), robust/fragile (стійкість до спотворень і перетворень), а також криптографічний компонент (наявність ключа, рандомізація позицій вбудовування). Для мультимедіа особливо важливо розмежовувати непомітність (людське сприйняття) і недетектованість (стійкість до стегоаналізу): метод може бути «візуально непомітним», але статистично легко виявлятися.

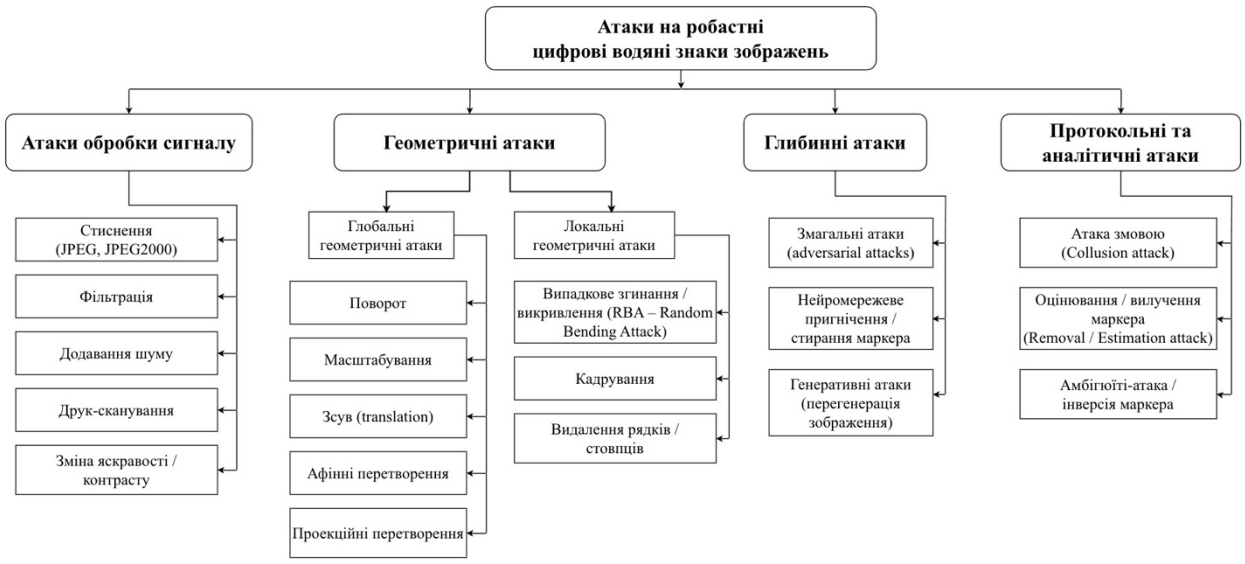


Рисунок 1.5 – Класифікація стеганографічних методів для мультимедійних контейнерів

(Джерело: складено автором)

Характеристики стеганографічних методів у наукових оглядах найчастіше описують через тріаду «місткість – непомітність – стійкість/безпека». Непомітність вимірюють (для зображень/відео) метриками якості на кшталт PSNR/SSIM, місткість – обсягом корисного навантаження (bpp або біт/піксель), а безпеку – складністю виявлення/витягання повідомлення (з урахуванням сучасного стегоаналізу, у т.ч. ML/DL-підходів). У цьому зв'язку актуалізуються роботи, що аналізують стійкість до типових атак (геометричні перетворення, стиснення) та підкреслюють необхідність корекції помилок і адаптивного вбудовування, а також систематичні огляди, орієнтовані на протидію статистичному стегоаналізу. [68, 70–74, 96]

У сучасній літературі стеганографічні методи розглядаються не лише як сукупність окремих алгоритмів, а як структурована система підходів із чіткою класифікацією за типом контейнера (зображення, аудіо, відео, текст, мережний трафік), областю вбудовування (просторова чи область перетворень), призначенням (стеганографія/водяні знаки/стегоаналіз), а також за ключовими експлуатаційними характеристиками – пропускною здатністю, непомітністю, робастністю та криптостійкістю [66, 67]. Така класифікація дозволяє описувати стеганосистему на концептуальному рівні, не прив'язуючись лише до окремого алгоритму, а через набір властивостей, важливих для прикладної задачі захисту мультимедійних даних.

Окремий напрям становлять роботи, орієнтовані на систематизацію методів для окремих типів контейнерів – насамперед цифрових зображень, що традиційно розглядаються як базовий об'єкт для цифрової стеганографії. У вітчизняних дослідженнях акцент робиться також на ув'язці класифікації методів із моделями атак (пасивний/активний противник, статистичний чи нейромережевий стегоаналіз) і з формалізованими критеріями оцінювання якості приховування [68, 69].

У сучасній літературі стеганографічні методи розглядаються не лише з позиції формальної класифікації, а й як інструментарій вибору алгоритму під конкретний сценарій захисту цифрового об'єкта. Такий підхід є важливим,

оскільки стеганографія охоплює різні за природою канали приховування даних: мультимедійні контейнери, файлові структури, мережеві протоколи та комбіновані середовища передавання інформації. Тому для розроблюваної системи захисту мультимедійних даних важливим є не повторення загальної класифікації, а визначення тих ознак, які впливають на практичний вибір методу вбудовування ідентифікатора.

Узагальнення наукових джерел показує, що для мультимедійних контейнерів ключовими є тип цифрового об’єкта, область вбудовування, очікувані перетворення після маркування та вимоги до стійкості. Зокрема, для зображень, аудіо й відео враховують, чи здійснюється вбудовування у просторовій або часовій області, в області перетворень, у параметрах стиснення або безпосередньо в бітовому потоці. Такий підхід дозволяє співвіднести метод із типовими загрозами: стисненням, фільтрацією, масштабуванням, геометричними перетвореннями, перекодуванням або фрагментацією контейнера.

Окреме значення мають критерії практичного застосування методу: місткість, непомітність, стійкість, обчислювальна складність, потреба в оригінальному контейнері під час перевірки, можливість відновлення контейнера без втрат, а також наявність ключа або механізму рандомізації. У цьому контексті такі ознаки, як можливість вилучення прихованих даних без використання оригінального контейнера або з його використанням, оборотність чи необоротність вбудовування, а також чутливість, часткова чутливість або стійкість методу до модифікацій, доцільно розглядати не як самостійну повторну класифікацію, а як параметри, що визначають придатність стеганографічного методу для конкретного сценарію захисту.

Ще одним важливим критерієм є стійкість до стегоаналізу. Метод може залишатися візуально або акустично непомітним для користувача, але водночас бути статистично виявлюваним за допомогою спеціалізованих детекторів або моделей машинного й глибинного навчання. Тому сучасні дослідження дедалі частіше оцінюють стеганографічні підходи не лише за принципом «де і як

вбудовано дані», а й за тим, наскільки складно довести сам факт приховування інформації в умовах заданої моделі атаки.

У праці А. В. Ахмаметьєвої та В. В. Коваленко запропоновано просторовий PVD-метод вбудовування даних у кольорові зображення: модифікацію значень пікселів виконують у парі RGB-компонент із найменшою різницею, контролюючи переповнення та допустимий «зазор» між значеннями [50]. Це зменшує ризик помилок вилучення й кольорових спотворень, але не дає підстав вважати метод універсально стійким: його властивості залежать від складу зображення та параметрів вбудовування. У дисертації цей підхід є альтернативою для порівняння, тоді як для розроблюваної системи зображень реалізовано DCT-QIM.

Огляд М. Попа та співавторів систематизує стеганографічні методи за типом носія, областю вбудовування та призначенням [66]. Така класифікація задає термінологічну основу, однак розмежування стеганографії та водяних знаків не завжди є абсолютним: прихованість, стійкість і ємність залежать від конкретного алгоритму й сценарію використання. Тому IP-Protect доцільно характеризувати не лише як стеганографічний засіб, а як систему захисту та перевірки мультимедійних даних, що поєднує цифрові водяні знаки, відбитки й реєстр активів. Її технічні перевірки та звіти документують результати, але самі по собі не гарантують юридичного визнання доказів.

Класифікаційні підходи до стеганографічних методів для зображень, аудіо та відео мають спільну логіку, що дозволяє уникнути повторення однотипних класифікацій для різних мультимедійних контейнерів і водночас показати, як загальні ознаки методу проявляються у конкретних практичних реалізаціях.

У найзагальнішому вигляді стеганографічні методи для мультимедійних даних систематизують за типом контейнера, областю вбудовування, способом вилучення прихованих даних, рівнем стійкості до модифікацій, оборотністю вбудовування, місткістю, непомітністю та стійкістю до стегоаналізу. За типом контейнера виокремлюють методи для зображень, аудіо, відео, текстових файлів, мережевих протоколів і файлових структур. Для мультимедійних об’єктів

особливе значення має область вбудовування: просторова або часова область, область перетворень, параметри стиснення або безпосередньо бітовий потік.

Для зображень типовими є просторові методи, що змінюють піксельні компоненти, а також методи в області перетворень, зокрема на основі DCT, DWT, SVD та їхніх комбінацій. Для аудіоданих аналогічну роль відіграють методи, що працюють із часовими відліками сигналу, частотними або спектральними характеристиками, коефіцієнтами перетворень чи параметрами кодування. Для відео застосовуються як покадрові підходи, успадковані від методів для зображень, так і методи, що враховують міжкадрову структуру, групи кадрів, рухові вектори та особливості стандартів стиснення.

Після визначення загальних класифікаційних ознак доцільно перейти до огляду практичних реалізацій, наведених у науковій літературі. У цьому огляді важливо показати не лише те, до якої групи належить певний метод, а й на чому він базується, який контейнер використовує, у якій області здійснюється вбудовування, які атаки враховує та за якими метриками оцінюється його ефективність.

Окремо виділяють адаптивні стратегії, що поєднують переваги просторової та частотної областей: вибір областей/коефіцієнтів для вбудовування залежить від насиченості, текстури, країв або локальної складності зображення, щоб одночасно підвищити непомітність і знизити детектованість. Саме в межах цієї логіки українські праці пропонують моделі, які враховують неоднорідність зображення (різні зони мають різну «толерантність» до модифікацій), а оглядові роботи систематизують відповідні підходи та їхню робастність [35, 51, 68, 73, 165].

Огляд А. Чеддада та співавторів систематизує методи стеганографії зображень за областю вбудовування та типом модифікації, охоплюючи, зокрема, LSB, розширення гістограми й методи на основі DCT/DWT [67]. Автори розглядають компроміс між непомітністю, робастністю та ємністю. Ця класифікація корисна як теоретична основа, однак сама по собі не визначає, який клас методів буде найефективнішим для конкретного набору зображень і

сценарію атак, а узагальнення огляду 2010 року не замінюють експериментальної перевірки сучасних реалізацій.

Це видно з результатів дисертації: на вибірці з 567 зображень авторський DCT-QIM за близького рівня непомітності знизив BER після JPEG Q=75 з 0,0482 до 0,0287 порівняно з класичним методом. Водночас успішне відновлення маркера після масштабування до 50% становило 67,7%, а після обрізання 10% – лише 1,1% (табл. 3.3). Отже, вимоги до непомітності, стійкості й ємності потрібно оцінювати для конкретного алгоритму та визначених атак: у цій роботі DCT-QIM поліпшує результат за JPEG-стиснення, але вразливість до геометричних перетворень залишається невирішеною.

Українська наукова традиція класифікації методів захисту цифрових зображень формується на перетині двох ліній досліджень – стеганографії (приховування факту передавання/наявності повідомлення) та цифрового водяного маркування (атрибуція авторства, ідентифікація джерела витоку, контроль копіювання, автентифікація). У роботах українських авторів найчастіше використовується базова для зображень дихотомія просторової області та області перетворень, а також поділ за типом маркера (видимий/невидимий), режимом доступу до оригіналу (blind / non-blind) і за призначенням (copyright-tracking vs integrity/authentication).

Важливою рисою «українського підходу» є практико-орієнтована багатокритеріальна класифікація, коли поряд із формальними ознаками (область вбудовування, тип контейнера, формат/стиснення) прямо фіксуються експлуатаційні характеристики: непомітність, місткість, робастність до типових атак (стиснення, геометричні перетворення, локальні модифікації), а також можливість локалізації змін для задач автентифікації. У такій логіці робастні/крихкі/напівкрихкі водяні знаки розглядаються як різні «класи» методів під різні сценарії використання – від доказування авторства до контролю цілісності зображення.

Окремий напрям українських публікацій підсилює класифікацію прикладними постановками «під систему»: підтвердження права власності на

цифрові зображення та побудова доказовості (комбінації водяних знаків із хешуванням/реєстрами, розширення на інші типи медіа), а також моделі робастності під окремі класи впливів (наприклад, часткова втрата фрагментів, локальні зміни), що корисно для вибору класу методу ще на етапі проєктування інформаційної системи захисту ІВ [35, 52–54, 70].

У статті Р. Штонди та співавторів розглянуто просторові методи стеганографії зображень, зокрема LSB і псевдовипадковий розподіл бітів, а також методи на основі DCT [68]. Автори аналізують стійкість методів до активних атак і відзначають доцільність поєднання F5 із шаблонними схемами вбудовування. Цей висновок, однак, не встановлює універсальної переваги такого поєднання: результати залежать від контейнера, параметрів алгоритму та моделі атаки. Тому праця окреслює важливі класи методів і загроз, але сама по собі не обґрунтовує вибір частотного чи гібридного алгоритму для конкретної системи.

У працях [70–73, 76, 77, 165] методи також розглядають за експлуатаційними критеріями: непомітністю, місткістю, стійкістю до окремих перетворень, складністю вбудовування й вилучення та можливістю сліпого декодування. Ці характеристики не можна звести до одного універсального рейтингу: вимоги залежать від призначення маркера – ідентифікації авторства, контролю цілісності чи прихованої передачі даних. Відповідно, потрібне порівняння за однакових умов тестування, а не лише узагальнення властивостей класу алгоритмів.

Праця Г. В. Ахмаметьєвої та Д. В. Гайдук доповнює цей огляд експериментальним зіставленням просторового методу на ознаках блоків, зокрема LBP і LTP, із базовими підходами [75]. Авторки досліджують якість стегозображень, точність вилучення та стійкість до шумових атак. Водночас ці результати не дають підстав переносити висновки на JPEG-стиснення чи геометричні перетворення, які потребують окремої перевірки.

О. Туровський та співавтори пропонують оцінювати методи за місткістю, стійкістю, непомітністю, захищеністю та складністю, застосовуючи вагові

коефіцієнти й інтегральне ранжування [69]. Такий підхід упорядковує вибір, але підсумковий рейтинг залежить від ваг критеріїв і конкретного сценарію, тому не є універсальним. У дисертації ці характеристики перевіряються експериментально для авторського DCT-QIM: на 567 зображеннях за близького рівня непомітності BER після JPEG Q=75 зменшився з 0,0482 до 0,0287 порівняно з класичним методом. Водночас успішне відновлення маркера після масштабування до 50% становило 67,7%, а після обрізання 10% – лише 1,1% (табл. 3.3). Отже, метод покращує стійкість до JPEG-стиснення, але вразливість до геометричних атак залишається невирішеною; це визначає межі його застосування та напрям подальшого вдосконалення.

Огляди М. А. Вані та Б. Султана, К. Ху та співавторів і Б. Сонга та співавторів систематизують методи стеганографії зображень на основі глибинного навчання за архітектурами, стратегіями вбудовування й навчання [91–93]. У них розглянуто, зокрема, GAN-, adversarial- та end-to-end-підходи, а також залежність результатів від датасетів, функцій втрат і моделі атак. Огляд Д. Сетіаді та співавторів розширює класифікацію на текст і 3D-сітки [94]. Сукупно ці праці окреслюють перспективи DL-методів, але не доводять їхньої універсальної переваги: результат залежить від конкретної задачі, а значні обчислювальні вимоги та чутливість до зміни даних обмежують перенесення моделей. Для цієї дисертації такі підходи є перспективою розвитку, а не описом реалізованих алгоритмів.

Огляди аудіостеганографії [163] та DL-методів для зображень і аудіо [95] класифікують алгоритми за областю вбудовування, типом сигналу, способом навчання та стійкістю до перетворень. Ця класифікація допомагає визначити релевантні атаки, однак не підтверджує стійкості конкретного методу без окремих випробувань. У дисертації авторський метод audio_pgdiff_v2 перевірено на 150 аудіофайлах: після MP3-стиснення зі швидкістю 128 кбіт/с BER становив 0,0100, а після MP3 64 кбіт/с – 0,0567. Водночас стійкість до зміни часової шкали та агресивного AAC-перекодування визначено як обмеження, що потребують подальшого дослідження.

Огляд мережевої стеганографії Н. Сінгха та співавторів стосується прихованих каналів на рівні мережевих протоколів – зокрема, storage- і timing-каналів [164]. Це окремий напрям, який доцільно згадувати для окреслення меж дослідження: IP-Protect працює з мультимедійними файлами та вбудованими ідентифікаторами, а не реалізує приховану передачу даних у мережевому трафіку.

Праці зі стегоаналізу [96–99] показують розвиток методів виявлення прихованих даних – від статистичних ознак до глибинно-навчальних моделей – і наголошують на важливості сценарію доступу та метрик оцінювання. Вони обґрунтовують потребу враховувати модель противника, проте не дають підстав стверджувати, що реалізовані в дисертації методи мають низьку детектованість для сучасних DL-аналізаторів: таке тестування в роботі не наведено. Аналогічно, експерименти з DCT-QIM засвідчили кращий результат за JPEG Q=75, але нижчу стійкість до обрізання й масштабування. Отже, результати дисертації характеризують методи лише за дослідженими атаками; оцінювання стійкості до DL-стегоаналізу та ширшого набору реалістичних перетворень залишається напрямом подальшої роботи.

Інтеграція висновків цих робіт у дисертаційну класифікацію дозволяє чітко сформулювати модель противника для інформаційної системи захисту ІВ: передбачається, що атакувальник має у своєму розпорядженні сучасні DL-стегоаналізатори, треновані на великих корпусах зображень, аудіо та відео. Відповідно, стеганографічні методи, які застосовуються для вбудовування ідентифікаторів, мають належати до класу алгоритмів:

1 – явно враховують наявність сучасних нейромережевих стегоаналізаторів під час навчання;

2 – використовують структури маркерів, стійкі до типових трансформацій, які, як показують огляди, часто виступають джерелом хибних позитивів/негативів у стегоаналізі.

Це безпосередньо пов’язує класифікацію методів у підрозділі 1.3 з вимогами до математичної моделі та алгоритмів, які будуть розвинуті у наступному розділі дисертації.

1.4. Аналіз наявних систем захисту авторських прав

Сучасні системи захисту авторських прав у цифровому середовищі являють собою багаторівневу комбінацію правових, організаційних і технічних рішень. Для мультимедійних даних (зображення, аудіо, відео) ці системи, як правило, поєднують кілька компонентів: керування доступом та умовами використання (DRM), маркування контенту (цифрові водяні знаки, приховані ідентифікатори), а також механізми моніторингу й автоматизованого виявлення порушень (аудіо- та відеофінгерпринтинг, системи на кшталт Content ID). Усе частіше до цих рішень додаються розподілені реєстри транзакцій на основі блокчейну, які забезпечують фіксацію прав, ліцензій і фактів використання мультимедійних об’єктів.

Для даної дисертації важливо не лише узагальнити типи технологій, а й показати, як вони реалізуються у вигляді завершених систем: від класичних DRM-платформ комерційних постачальників до спеціалізованих систем колективного управління правами, сервісів автоматичного виявлення нелегального контенту та блокчейн-орієнтованих рішень для зображень і відео. У подальшому це дозволить сформулювати вимоги до розроблюваної інформаційної системи: необхідність стійких до атак прихованих ідентифікаторів, можливість інтеграції з наявними екосистемами розповсюдження контенту й підтримка процедури доказу авторства.

Огляд Чж. Чжана описує DRM як екосистему керування правами на цифровий контент, що охоплює правовласників, постачальників, посередників і користувачів [78]. У праці розглянуто умови опису прав, авторизацію, делегування дозволів і взаємодію механізмів контролю доступу з технічними засобами захисту. Для цієї дисертації важливо розрізняти ці функції: DRM передусім регулює доступ і використання контенту в межах визначеної екосистеми, тоді як IP-Protect пов’язує мультимедійний файл із записом у реєстрі за допомогою водяного знака та інших ознак. Це не означає, що ЦВЗ замінює DRM або гарантує збереження маркера після будь-якого перетворення: його стійкість залежить від методу й атаки.

П. Джамкхедкар і Г. Гайлмен систематизують DRM-архітектури за моделями керування ліцензіями, довірою до клієнтських пристроїв, політиками доступу та інтероперабельністю [79]. Їхній огляд корисний для порівняння функцій DRM та систем ідентифікації контенту, але не є експериментальним зіставленням із IP-Protect. Тому можливість інтеграції розробленої системи з DRM варто трактувати як перспективу, а не як перевірену в дисертації властивість.

Дж. Грей і Н. Сузор досліджують автоматизоване забезпечення авторських прав на платформах і роль машинного навчання та фінгерпринтингу в роботі таких механізмів, зокрема Content ID [80]. Їхній аналіз також порушує питання прозорості рішень і можливості оскарження. На відміну від ЦВЗ, платформний фінгерпринт зазвичай зіставляє завантажений матеріал із референсною базою сервісу; отже, результати такого зіставлення залежать від доступу до відповідної системи та її даних. Водночас праця не є прямим технічним тестом усіх платформних систем і не доводить, що їхні результати можуть використовуватися лише всередині однієї платформи. Перевагу IP-Protect у цьому контексті коректніше формулювати як наявність вбудованого маркера та локальних засобів перевірки, а не як гарантовану незалежність доказування від будь-якої зовнішньої системи.

Д. Кей аналізує погляди й практики користувачів YouTube щодо авторського права та автоматичних механізмів контролю [81]. Ця праця доповнює технічний аналіз соціальним виміром, але не оцінює алгоритми вбудовування ЦВЗ і не підтверджує, що маркер у файлі сам по собі засвідчує авторство. У дисертації IP-Protect пов’язує водяний знак із записом у реєстрі та журналом перевірки; результати такої технічної верифікації можуть бути частиною доказових матеріалів, але не гарантують їх юридичного схвалення.

Д. Лі та М. Лім узагальнюють методи аудіофінгерпринтингу для розпізнавання музики, зокрема формування відбитків за спектральними ознаками й парами піків [82]. Фінгерпринтинг і ЦВЗ виконують різні функції: перший дає змогу зіставляти сигнал із базою відбитків, а другий – вбудовувати

дані в сам файл. У дисертації аудіовідбиток FP64 використовується як допоміжна ознака пошуку, тоді як ідентифікація правовласника спирається також на водяний знак і дані реєстру. Отже, фінгерпринтинг доповнює маркування, але не замінює його.

Система ZAP, описана О. Сабатом та О. Богонісом, є прикладом формалізованого комплексного підходу до захисту електронних видань із використанням, зокрема, цифрових водяних знаків, криптографічних механізмів і моніторингу. Її предметна сфера відрізняється від IP-Protect, орієнтованої на мультимедійні активи, тому ці системи не слід розглядати як безпосередньо порівняні без спільних критеріїв і випробувань. Спільною є системна постановка задачі; відмінними – типи контенту та реалізовані механізми. Отже, IP-Protect поєднує реєстрацію активів, відбитки й водяні знаки, але його переваги та обмеження слід оцінювати за конкретними умовами тестування, а не виводити лише з порівняння концепцій.

Розвиток блокчейн-технологій привів до появи цілої групи систем, у яких захист авторських прав реалізується через поєднання незмінного розподіленого реєстру, смарт-контрактів та вбудованих у контент маркерів (цифрових водяних знаків, унікальних ідентифікаторів, фінгерпринтів). На відміну від класичних DRM-платформ або суто платформних систем на кшталт Content ID, такі рішення намагаються забезпечити глобально перевірюваний слід авторства, який не прив’язаний до єдиного посередника й може бути використаний у різних юрисдикціях та сервісах. Саме тому блокчейн-орієнтовані системи становлять природне концептуальне оточення для розроблюваної в дисертації інформаційної системи, що комбінує невидимі ідентифікатори з реєстром прав.

У працях про блокчейн-орієнтований захист мультимедійних даних розглянуто реєстрацію авторства й часових міток, керування ліцензіями та роялті, токенізацію прав і поєднання реєстрів із цифровими водяними знаками, хешами та фінгерпринтами [83]. Ці огляди окреслюють можливості блокчейну для фіксації записів і транзакцій, але сам розподілений реєстр не забезпечує виявлення водяного знака у зміненому файлі й не гарантує його стійкості до

перетворень. Результат залежить від способу прив’язки файлу до запису, захисту метаданих і характеристик конкретного алгоритму.

Р. Ф. Чирієлло та співавтори розглядають блокчейн як спільну інфраструктуру для метаданих прав, ліцензій і розподілу доходів у музичній індустрії [84]. Цей підхід може доповнювати маркування контенту, однак його не слід ототожнювати з механізмом ідентифікації конкретної копії файла. Так само описані в працях [85, 86] поєднання блокчейну з аудіо- й відеомаркуванням є рішеннями для визначених типів даних та наборів атак; їхні результати не доводять універсальної стійкості або юридичної достатності сформованих доказів. Модель для векторних карт, запропонована Х. Ваном та співавторами [87], спирається на геометричні й топологічні ознаки карт, тому її не можна безпосередньо переносити на зображення, аудіо чи відео.

У дисертації IP-Protect реалізує реєстр мультимедійних активів, керування правами та поетапну перевірку «хеш → відбиток → водяний знак». Для зображень застосовано DCT-QIM, для аудіо – набір методів вбудовування й виявлення. Блокчейн до реалізованої архітектури не входить, тому наведені джерела слугують контекстом для можливого розвитку системи, а не описом її наявної функціональності.

Отже, нерозв’язаним залишається питання, як поєднати стійке маркування з реєстровою фіксацією прав за збереження конфіденційності та перевірності результатів. Інтеграція IP-Protect із блокчейн-реєстром може бути напрямом подальшої роботи, але потребуватиме окремого проєктування й експериментального оцінювання.

Для наочного порівняння підходів до захисту авторських прав у цифровому середовищі у табл. 1.1 узагальнено ключові характеристики трьох класів систем: класичних DRM-рішень, платформних систем автоматизованого виявлення порушень (типу Content ID та фінгерпринтингу), блокчейн-орієнтованих моделей реєстрації прав і транзакцій. Табл. 1.1 дозволяє продемонструвати місце й відмінності розроблюваної системи в наявному ландшафті рішень, показуючи її орієнтацію не лише на контроль доступу чи

реєстрацію прав, а насамперед на стійку прив’язку конкретних мультимедійних файлів до автора та правовласника за допомогою невидимих ідентифікаторів.

Таблиця 1.1 – Порівняльна характеристика систем захисту авторських прав на мультимедійні дані

Критерій	**Класичні DRM-системи (контроль доступу)**	**Платформні системи (Content ID, фінгерпринтинг)**	**Блокчейн-орієнтовані системи (реєстр прав і транзакцій)**
Основний принцип роботи	Шифрування контенту та видача ліцензій на відтворення; контроль доступу в межах закритої екосистеми постачальника	Порівняння завантаженого контенту з базою еталонних фінгерпринтів; автоматичне блокування/монетизація/ обмеження	Фіксація прав, ліцензій та транзакцій у розподіленому реєстрі; використання смарт-контрактів для розподілу роялті
Тип маркера / ідентифікації	Явні ліцензії й ключі доступу; маркери в основному «зовнішні» щодо файлу (метадані, токени, ключі)	Аудіо/відео-фінгерпринт (хеш-опис вмісту), як правило, зберігається лише у внутрішній базі платформи	Криптографічні хеші, ідентифікатори творів, записи смарт-контрактів; іноді поєднуються з ЦВЗ у файлах
Розташування ідентифікатора	Переважно поза самим файлом (сервери постачальника, ліцензійні сервери, ключові сховища)	У базі даних платформи; сам файл не обов’язково містить явний маркер авторства	У блокчейні (хеші, ідентифікатори, метадані); сам мультимедійний файл часто зберігається окремо
Залежність від платформи	Висока: механізми працюють лише в екосистемі конкретного постачальника DRM (стримінг, онлайн-магазин тощо)	Дуже висока: ідентифікація можлива лише в межах конкретної платформи (YouTube, стримінговий сервіс тощо)	Середня: блокчейн може бути публічним/консорціумним, але конкретні реалізації часто прив’язані до певних платформ
Основний об’єкт захисту	Процес доступу та відтворення (хто, як і скільки разів може переглядати/ слухати)	Факт завантаження/ розміщення контенту, що збігається з еталонною базою фінгерпринтів правовласників	Правовий статус твору, ланцюг прав та фінансові транзакції (ліцензії, роялті, передачі прав)
Стійкість до технічних атак (стиснення, обрізка, переформатування)	Обмежена: після виходу з DRM-середовища (екранний запис, ріп) захист практично зникає	Висока для фінгерпринтингу: ідентифікація можлива навіть після стиснення й помірних спотворень, але лише в межах платформи	Залежить від поєднання з ЦВЗ/фінгерпринтингом; сам блокчейн не захищає від модифікації файлу

Закінчення табл. 1.1

Критерій	Класичні DRM-системи (контроль доступу)	Платформні системи (Content ID, фінгерпринтинг)	Блокчейн-орієнтовані системи (реєстр прав і транзакцій)
Підтримка різних типів мультимедіа	Добре розвинена для аудіо/відео; для зображень – залежить від конкретних постачальників та стандартів.	Переважно аудіо та відео; зображення підтримуються рідше й у спрощеному вигляді.	Може охоплювати будь-які типи даних (залежить від моделі); мультимедіа – один із сценаріїв.
Придатність до судового доказування	Опосередкована: журнали DRM-постачальника можуть використовуватися як докази, але залежать від довіри до оператора.	Обмежена: внутрішні журнали платформи і фінгерпринти складно верифікувати сторонніми експертами.	Сильна для фіксації часу й послідовності транзакцій; слабша щодо технічного зв’язку конкретного файлу з записом.
Масштабованість	Висока в межах окремих комерційних екосистем; міжсистемна інтеграція обмежена.	Висока в межах платформи (зокрема для великих відеохостингів), але відсутня міжплатформна сумісність.	Обмежена пропускною здатністю та вартістю транзакцій; вирішується шляхом зберігання лише хешів/ідентифікаторів.
Прозорість для користувачів та авторів	Низька/середня: політики контролю доступу часто непрозорі, механізми роботи DRM залишаються «чорною скринькою».	Низька: алгоритми Content ID та подібних систем не розкриваються, механізми оскарження обмежені й складні.	Середня: логіка смарт-контрактів може бути прозорою, але технічні деталі інтеграції з контентом не завжди очевидні.
Роль методів штучного інтелекту	Обмежена: переважно в аналізі поведінки користувачів та виявленні аномалій у доступі.	Ключова: машинне навчання та фінгерпринтинг використовуються для автоматичної ідентифікації та модерації контенту.	Зростаюча: AI застосовується для аналізу транзакцій, виявлення шахрайських схем, класифікації контенту.

Джерело: авторська розробка.

1.5. Авторське право на аудіо- та відеофайли: специфіка

Аудіо- та відеоконтент може охоплювати кілька рівнів авторських і суміжних прав, зокрема: права авторів, виконавців, виробників фонограм чи аудіовізуальних творів і мовників. Цифрове розповсюдження ускладнює ліцензування та облік використань, але конкретний склад прав і дозвільних умов залежить від виду об'єкта, договорів і способу використання [154–162].

У ЄС ці питання регулюють, зокрема, Директивою 2019/790: її положення охоплюють винагороду авторів і виконавців, прозорість інформації про використання творів, коригування договорів та окремі обов'язки платформ [156–159]. Ця нормативна база окреслює правовий контекст, але сама по собі не визначає технічний спосіб ідентифікації контенту. Так само цифровий водяний знак може пов'язати файл із записом у реєстрі, проте не встановлює повноту прав, чинність ліцензії чи правомірність конкретного використання.

Для аудіовізуального контенту суттєвими є розмежування об'єктів і правовласників, територіальність ліцензій та фрагментація репертуарів [28, 127, 133, 134, 151–153]. Стійкий ідентифікатор потенційно може полегшити зіставлення файлу з відповідними метаданими, але для цього потрібні точні й актуальні записи про права та дозволені способи використання. Отже, маркер є допоміжним технічним засобом, а не заміною ліцензійної інформації чи її правової оцінки.

У музичній індустрії аудіофінгерпринтинг і цифрове водяне маркування виконують різні, потенційно взаємодоповнювальні функції: фінгерпринт дає змогу зіставити сигнал із базою еталонів, а ЦВЗ – вбудувати дані у файл [15, 128, 135–139]. Водночас збіг фінгерпринта сам по собі не доводить належність прав, а наявність водяного знака не підтверджує правомірність використання. Платформні системи можуть підтримувати ідентифікацію контенту та застосування політик конкретного сервісу, але це не тотожне незалежному обліку прав у різних платформах.

Колективне управління майновими правами спирається на дані про твори, фонограми, авторські частки та фактичні використання [129, 140–144].

Ідентифікатори можуть допомогти пов’язувати файл із такими записами, однак не забезпечують точного розподілу роялті без даних про використання, узгоджених метаданих і взаємодії з платформами та організаціями колективного управління. У дисертації IP-Protect веде реєстр активів і правовласників, але інтеграцію зі стримінговими платформами чи системами розподілу роялті не реалізовано.

Дослідження цифрової трансформації музичної індустрії та блокчейну описують зміну моделей доступу до контенту й можливість фіксувати транзакції та метадані у розподілених реєстрах [84, 89, 90, 130, 131, 145–148]. Проте незмінність запису не гарантує точності внесених даних, а реєстр не встановлює автоматично зв’язок із конкретною копією файла. IP-Protect використовує власний реєстр активів; блокчейн-інтеграція в реалізованій системі відсутня.

Отже, технічна система може підтримати ідентифікацію мультимедійного об’єкта, але прозорість використань, справедлива винагорода й правомірність використання залежать також від договорів, якості метаданих, звітності платформ та процедур аудиту [132, 144, 146, 149, 150]. Експериментальна перевірка в дисертації охоплює 567 зображень і 150 аудіофайлів, але не встановлює облік фактичних використань або виплати роялті. Крім того, стійкість маркерів залежить від атаки: для зображень після обрізання 10% успішне відновлення становило лише 1,1%, а стійкість аудіометоду до зміни часової шкали потребує окремої перевірки. Таким чином, нерозв’язаним залишається питання інтеграції технічної ідентифікації з актуальними правовими даними та незалежно перевірюваною звітністю про використання контенту.

1.6. Використання штучного інтелекту у сфері захисту мультимедійних даних

Штучний інтелект (ШІ) розширює можливості створення, аналізу й захисту мультимедійного контенту, але ці напрями слід розмежовувати. Генерація синтетичних матеріалів і діпфейків створює нові ризики, тоді як

машинне навчання застосовують для вбудовування та виявлення водяних знаків, пошуку подібного контенту й аналізу медіаманіпуляцій [100–126]. Наведені в дисертації праці окреслюють ці напрями, але самі по собі не підтверджують, що один метод забезпечує одночасно непомітність, стійкість і надійну атрибуцію.

Огляди нейромережевого водяного маркування зображень описують автоенкодери, GAN-архітектури та моделі наскрізного навчання із симуляцією атак [100, 101]. Для аудіо й відео розглядаються, зокрема, комбіновані схеми вбудовування та виявлення маніпуляцій [102, 112, 116, 118, 119], а для контенту, створеного ШІ, – водяні знаки як засіб простежуваності [103]. Водночас стійкість таких методів залежить від типу атак і тестових даних; результати на одних перетвореннях не гарантують узагальнення на інші. Водяний знак може бути ознакою походження або модифікації, але його наявність сама по собі не доводить авторства чи правомірності використання.

Дослідження автоматизованого пошуку порушень, діпфейк-детекції та стегоаналізу стосуються суміжних, але окремих задач [104–106, 110, 111, 113–115, 120–122]. Зокрема, стаття про застосування ШІ у військовій сфері [117] може слугувати лише загальним прикладом автоматизованого аналізу ризиків: вона не є безпосереднім джерелом щодо охорони авторських прав або маркування мультимедіа. Аналогічно, праці про водяні знаки моделей машинного навчання [107–109, 123–126] досліджують захист самої моделі, а не мультимедійних файлів, тому їх доречно розглядати як можливий напрям розширення системи, а не як реалізовану функцію IP-Protect.

У дисертації машинне навчання використано для статистичної оцінки виявності маркера й атрибуції контенту; реалізовані моделі ґрунтуються на логістичній регресії, а не на глибинних нейронних мережах. На 150 аудіофайлах класифікатор виявляв слід audio_pgdiff_v2 з точністю 0,707 (AUC 0,774), що свідчить про виявність маркера в межах цього експерименту, а не про його загальну непомітність або детектованість усіма аналізаторами. Перевірку стійкості до сучасних DL-стегоаналізаторів у роботі не наведено. Отже, висновки дисертації обмежені реалізованими методами й умовами тестування;

оцінювання проти DL-аналізаторів, перевірка узагальнюваності на інших даних і розвиток нейромережевих рішень залишаються напрямами подальших досліджень.

1.7. Аналіз структури мультимедійних даних щодо стійкості до втручання

Мультимедійні дані являють собою складно організовані сигнальні структури з принципово різними властивостями в різних областях подання. Для задачі цифрового водяного маркування (ЦВЗ) ця структурна різнорідність є ключовою: різні компоненти сигналу мають різну стійкість до типових перетворень, різний рівень перцептивної помітності при модифікації та різні вимоги до обчислювальних ресурсів. Саме тому вибір області вбудовування є принциповим проєктним рішенням, яке визначає компроміс між непомітністю маркера, його стійкістю і пропускною здатністю прихованого каналу [38, 41, 167].

Загальна математична постановка задачі вбудовування, узагальнена у класичних роботах з теорії водяного маркування [169, 170], описується операторами вбудовування E(·) та витягування D(·):

$$y = E(x, b, k, \theta), \tag{1.1}$$

де $x \in \mathbb{R}^N$ – вихідний мультимедійний об’єкт, $b \in \{0,1\}^L$ – бітова послідовність ідентифікатора довжиною L, k – секретний ключ, θ – вектор параметрів алгоритму (область вбудовування, сила модифікації, схема кодування тощо), y – позначений (маркований) об’єкт. Процедура детекції або витягування:

$$\hat{b} = D(\tilde{y}, k, \theta), \tag{1.2}$$

де $\tilde{y} = A(y; \alpha)$ – об’єкт після дії оператора атаки A(·) з параметрами α. Якість системи вбудовування оцінюється трьома взаємообмежувальними критеріями:

$$d(x, y) \le D_{max} \quad \textit{(непомітність);} \tag{1.3}$$

$$R = L/N \geq R_{min} \quad (\text{ємність});$$
$$BER(b, \hat{b}) \leq \varepsilon, \quad \forall A \in \mathcal{A} \quad (\text{стійкість}),$$

де d(x, y) – міра спотворення (MSE, PSNR, ODG), N – розмір носія, R – бітова швидкість, ε – допустимий рівень бітових помилок, $\mathcal{A}$ – множина типових атак. Вимоги (1.3) утворюють фундаментальний трикутник компромісів: підвищення будь-якого критерію негативно впливає на принаймні один з двох інших [167, 171].

1.7.1. Структура цифрових зображень

Цифрове зображення подається як дискретна матриця пікселів $X \in \{0,\ldots,255\}^{H\times W\times C}$, де H – висота, W – ширина, C – кількість колірних каналів (1 для відтінків сірого, 3 для RGB або YCbCr). Для задач ЦВЗ перевагою є перехід до колірного простору YCbCr, де канал Y (яскравість) є основним носієм зорово помітної інформації і використовується більшістю JPEG-сумісних схем маркування.

Для аналізу частотних властивостей та вибору областей вбудовування до зображення застосовуються спектральні перетворення. Порівняння трьох основних представлень в області перетворень – DCT, DWT та DFT – наочно демонструє різні аспекти структури зображення і визначає придатні для маркування частотні компоненти.

Як видно з рис. 1.6, DCT-подання концентрує більшу частину енергії зображення у лівому верхньому куті (низькі частоти), що добре узгоджується з блоковою JPEG-компресією. DWT-подання забезпечує багаторівневий просторово-частотний аналіз, де кожний рівень декомпозиції описує локально різні частотні компоненти; середньочастотні субсмуги DWT (HL, LH другого та третього рівнів) є найбільш придатними для стійкого маркування. DFT-спектр відображає глобальну симетрію і може використовуватись для RST-інваріантних схем вбудовування.

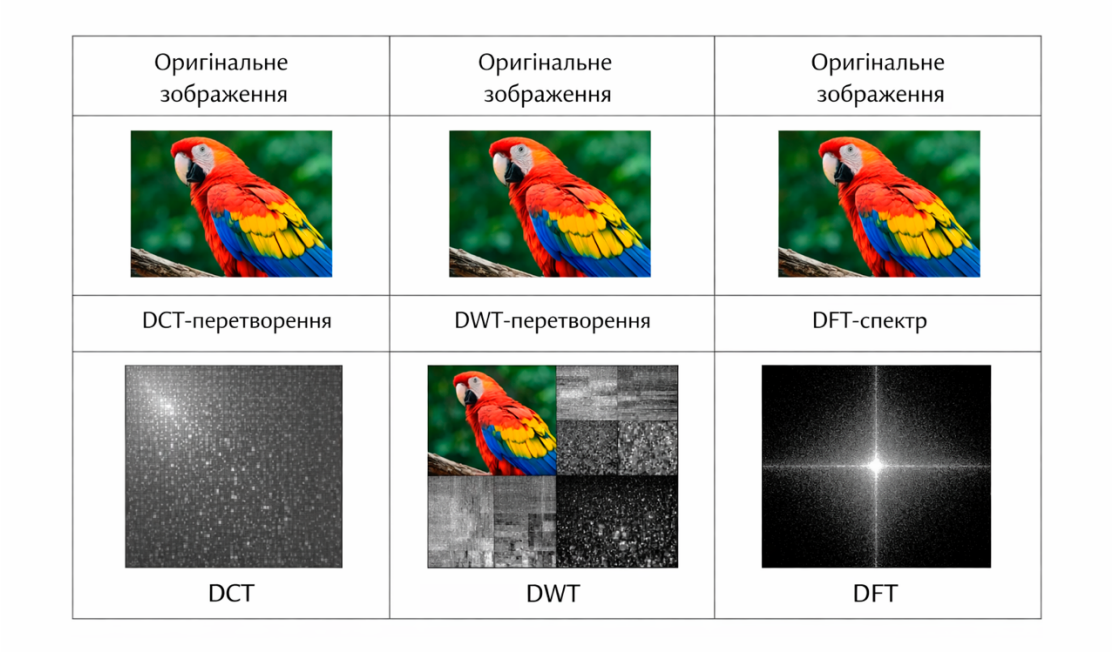


Рисунок 1.6 – Спектральні подання зображення:
DCT (ліворуч), DWT (по центру) та DFT (праворуч)
(Джерело: складено автором)

Загальна структурна схема процесу водяного маркування зображення наведена на рис. 1.7.

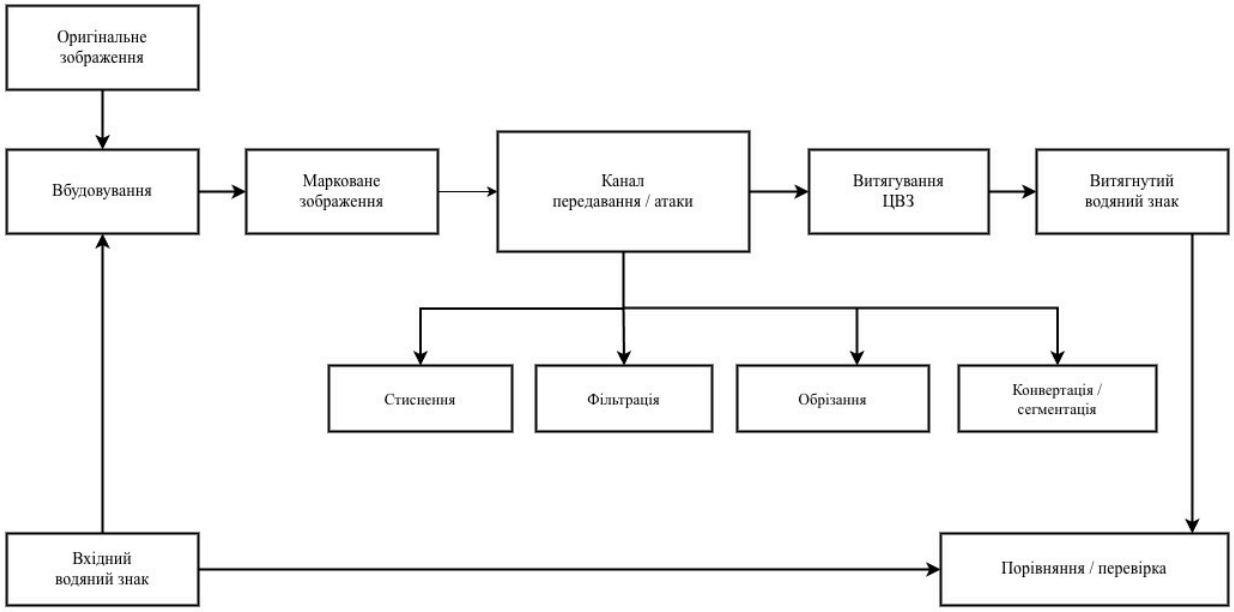


Рисунок 1.7 – Загальна блок-схема процесу вбудовування та витягування ЦВЗ у зображення

(Джерело: складено автором)

Стійкість ЦВЗ до JPEG-стиснення визначається тим, що JPEG квантує DCT-коефіцієнти блоків 8×8 з кроком Δ_q, де $\Delta_q > 1$ для середніх і низьких рівнів якості. Тому маркер, вбудований у низькочастотні або середньочастотні коефіцієнти з кроком $\Delta < \Delta_q/2$, зберігається після стиснення – тоді як маркери у молодших бітах пікселів (LSB-підхід) повністю знищуються.

1.7.2. Структура аудіосигналів

Аудіосигнал подається як послідовність PCM-вибірок x[n], n = 0,…, N−1, отримана при частоті дискретизації f_s (типово 44100 або 48000 Гц) і бітовій глибині 16 або 24 біти. Для вбудовування водяних знаків ключовим є перехід до частотної або часово-частотної областей, оскільки:

– пряма модифікація PCM-вибірок (часова область) дає низьку стійкість до MP3/AAC-стиснення, яке переквантовує MDCT-коефіцієнти відповідно до психоакустичної моделі;

– спектральні компоненти у середньочастотному діапазоні (300–4000 Гц), де маскування слуху найбільш виражене, витримують помірне стиснення при збереженні непомітності модифікації;

– відносні енергетичні співвідношення між частотними підсмугами інваріантні до нормалізації гучності – на відміну від абсолютних значень вибірок [172, 173].

Узагальнену схему формування аудіосигналу як контейнера для вбудовування ЦВЗ з урахуванням частотних, часово-частотних та психоакустичних властивостей наведено на рис. 1.8.

MDCT-перетворення (Modified Discrete Cosine Transform) є математичною основою MP3/AAC-кодеків і формує одну з найбільш природних областей подання сигналу для вбудовування аудіо-ЦВЗ [174].

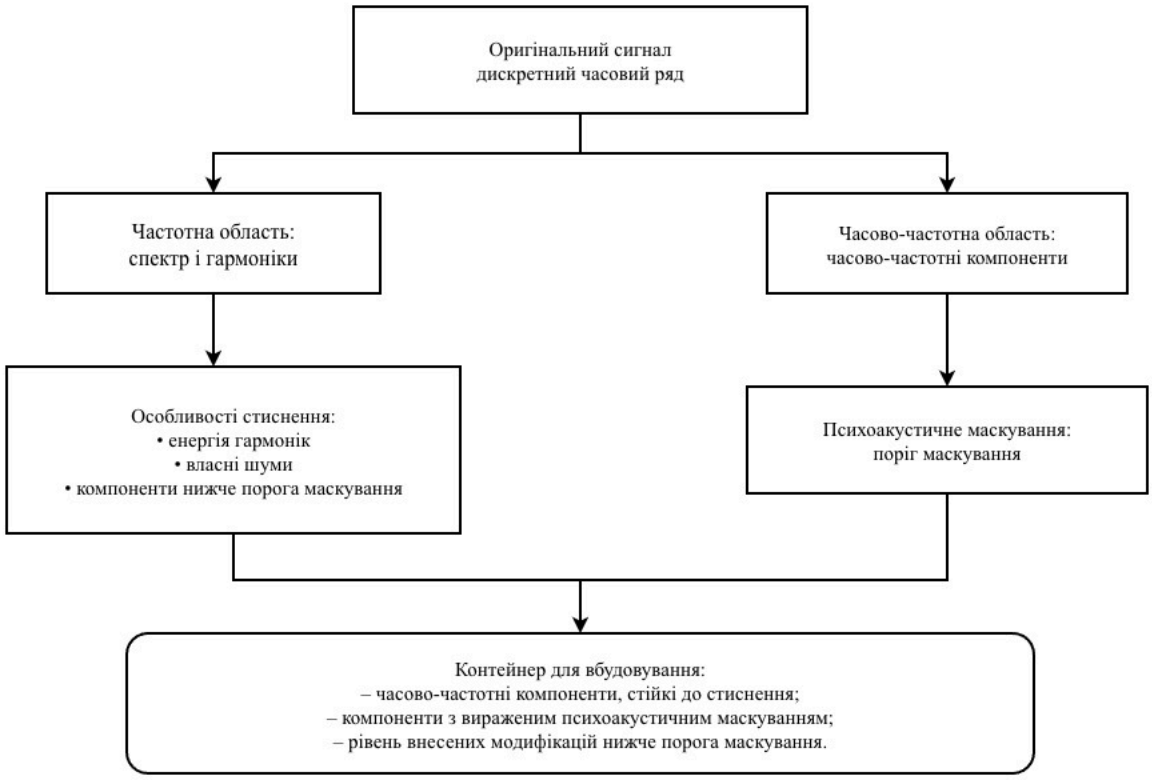


Рисунок 1.8 – Структура аудіосигналу як контейнера для вбудовування ЦВЗ *(Джерело: складено автором)*

Для кадру довжиною N відліків:

$$X[k] = \Sigma_{n=0}^{N-1} x[n] \cdot \cos\left(\pi(n + 1/2 + N/2)(2k+1) / N \right), \quad k = 0,\ldots,N/2-1 . \tag{1.4}$$

Ця властивість MDCT, що MP3-кодек, по суті, квантує ті самі коефіцієнти X[k], є ключовою для розуміння стійкості аудіо-ЦВЗ: маркери, що кодуються через відносні співвідношення пар X[k], зберігаються після перекодування краще, ніж абсолютні значення окремих коефіцієнтів.

1.7.3. Структура відеоданих

Відеодані об’єднують просторову структуру окремих кадрів (аналогічно до зображень) із часовою динамікою між ними. Сучасні кодеки H.264/AVC та H.265/HEVC використовують три типи кадрів: I-кадри (внутрішні, аналогічні JPEG), P-кадри (передбачені з попередніх) та B-кадри (двонаправлено

передбачені). Для водяного маркування найбільш придатними є I-кадри: вони не залежать від інших кадрів при декодуванні і зберігають повну структуру DCT-коефіцієнтів.

Типові атаки на відеовміст – перекодування, зміна роздільності, часовий монтаж, вставка рекламних вставок – можуть знищити маркер, вбудований в один кадр, але зберегти його в інших. Тому для надійного маркування відео ідентифікатор розподіляється по множині I-кадрів або груп кадрів (GOP) із надлишковим дублюванням [42, 43].

1.8. Визначення компонентів мультимедійних файлів, придатних для вбудовування ідентифікаторів

Для кожного типу мультимедійного носія формально визначається множина допустимих компонентів вбудовування Ω_t, яка залежить від вмісту контейнера, секретного ключа та параметрів алгоритму:

$$\Omega_t = \Omega_t(x, k, \theta), \quad t \in \{img, vid, aud\}, \tag{1.5}$$

де Ω_{img}, Ω_{vid} і Ω_{aud} позначають множини допустимих компонентів для зображень, відео і аудіо відповідно. Вводиться відображення позицій на біти ідентифікатора $\pi_t : \Omega_t \to \{1,\ldots,L\}$. Оператор вбудовування у компонентній формі:

$$y_i = f(x_i, b[\pi_t(i)], k, \theta), \ якщо\ i \in \Omega_t; \tag{1.6}$$
$$y_i = x_i, \ якщо\ i \notin \Omega_t .$$

Така форма запису явно враховує: залежність Ω від параметрів θ; відповідність між конкретною позицією і та конкретним бітом $b_{\pi t(i)}$; можливість різних правил вибору компонент для зображень, відео та аудіо [167, 171].

1.8.1. Компоненти зображень, придатні для вбудовування

Аналіз властивостей різних компонентів зображення у контексті стійкості до типових атак свідчить, що:

– молодші біти пікселів (LSB) дають максимальну ємність (~0,5 bpp), але повністю знищуються при JPEG-стисненні якості Q < 95, що робить LSB непридатним для задач захисту авторських прав у мережевому середовищі;

– середньочастотні DCT-коефіцієнти блоків 8×8 (зигзаг-позиції 3–14 у каналі Y) забезпечують добрий компроміс між непомітністю (PSNR > 38 дБ) і стійкістю до JPEG (Q ≥ 60) і є основою більшості практичних схем ЦВЗ;

– середньочастотні піддіапазони DWT другого-третього рівня (HL2, LH2, HL3) зберігаються після стиснення і менш чутливі до масштабування завдяки багаторівневій просторово-частотній локалізації;

– сингулярні значення SVD-розкладу підматриць DCT/DWT відносно стабільні під дією широкого класу перетворень, що робить гібридні DWT+SVD схеми стійкими до комплексних атак [175, 176].

1.8.2. Компоненти аудіосигналів для маркування

Для аудіо-маркування найбільш придатними є:

– MDCT-коефіцієнти у середньочастотному діапазоні (300–4000 Гц), де психоакустичне маскування найбільш виражене, а MP3-стиснення зберігає відносний розподіл енергії між підсмугами;

– відносні енергетичні співвідношення між парами DCT-підсмуг: нормована різниця $(E_{mid} - E_{low})/(E_{mid} + E_{low})$ інваріантна до амплітудного масштабування й нормалізації гучності;

– ехо-характеристики сигналу (затримка, загасання) у часовій або автокореляційній областях: ехо з амплітудою нижче порогу маскування сприймається людиною як частина природної реверберації;

– PN-послідовності (псевдовипадковий шум), розподілені по широкій смузі частот з малою енергією на кожному компоненті – підхід розширеного спектра, стійкий до адитивного шуму і нормалізації [172, 177, 178].

Порівняльну характеристику компонентів мультимедійних даних за стійкістю до типових атак наведено в табл. 1.2.

Таблиця 1.2 – Порівняльна характеристика компонентів мультимедійних даних за стійкістю до атак

Тип даних / компонент	**Типові атаки**	**Очікувана стійкість**	**Коментар**
Пікселі, LSB (зображення)	JPEG, шум, фільтрація	Низька	Висока вразливість до будь-якого стиснення
Середньочастотні DCT-коефіцієнти 8×8 (зображення)	JPEG (Q≥60), шум, фільтрація	Середня–висока	Оптимальний компроміс; основа більшості схем ЦВЗ для фото
DWT-підсмуги HL2/LH2 (зображення)	JPEG2000, масштабування, шум	Висока	Кращий, ніж DCT, для масштабування та локальних спотворень
Сингулярні значення SVD (зображення)	JPEG, RST, шум, фільтрація	Висока	Стабільні при широкому класі перетворень; основа гібридних схем
PCM-вибірки (аудіо)	MP3/AAC, шум, фільтрація	Низька	Знищуються при будь-якому перекодуванні
MDCT-коефіцієнти у маскованих смугах (аудіо)	MP3/AAC, нормалізація, фільтрація	Середня	Зберігаються при помірному MP3; основа QIM-методів
Відносна енергія підсмуг DCT (аудіо)	MP3/AAC, нормалізація	Середня–висока	Інваріантна до амплітудного масштабування
Echo-характеристики (аудіо)	MP3 (частково), фільтрація	Низька–середня	Непомітні при $\alpha <$ порогу маскування; чутливі до кодеків
PN-послідовності DSSS (аудіо)	Шум, нормалізація, фільтрація	Середня	Стійкі до адитивного шуму; чутливі до часових деформацій
DCT/DWT компоненти I-кадрів (відео)	H.264/H.265 рекодування, монтаж	Середня–висока	Аналогічно зображенням; посилення через розподіл по GOP

Джерело: складено автором на основі [38, 42, 43, 167, 168, 172, 173, 175].

1.9. Пропускна здатність каналів вбудовування та метрики оцінювання

Пропускна здатність прихованого каналу визначається кількістю бітів корисного ідентифікатора, що можуть бути надійно вбудовані в одиницю носія (піксель, відлік, секунда сигналу) без порушення вимог до непомітності та стійкості [37, 171]. Розрізняються L_{id} – довжина ідентифікатора до кодування та L_{emb} – фактично вбудована кількість бітів з урахуванням надлишковості $r = L_{id} / L_{emb}$. Пропускна здатність для різних типів носіїв:

$$R_{img} = L_{emb} / (H \cdot W), \quad R_{aud} = L_{emb} / T, \quad R_{vid} = L_{emb} / N_{fr}, \tag{1.7}$$

де H, W – розміри зображення, T – тривалість аудіо в секундах, N_{fr} – кількість маркованих кадрів. За даними оглядових досліджень, типові значення: $R_{img} \approx 0{,}01–0{,}1$ bpp для стійких ЦВЗ при PSNR > 40 дБ; $R_{aud} \approx 20–300$ bps для аудіо при ODG ≥ −1 [37, 179, 180].

Ілюстрацію трикутника компромісів між непомітністю, стійкістю та ємністю каналу вбудовування подано на рис. 1.2.

1.9.1. Метрики непомітності

Для кількісної оцінки непомітності модифікації застосовується узгоджений набір метрик. Базовою мірою спотворення є MSE:

$$MSE(x, y) = (1/N) \cdot \Sigma_i \, (x_i - y_i)^2 . \tag{1.8}$$

Похідна метрика PSNR (Peak Signal-to-Noise Ratio) для 8-бітних зображень:

$$PSNR(x, y) = 10 \cdot \log_{10}(255^2 / MSE(x, y)) . \tag{1.9}$$

Значення PSNR ≥ 38–40 дБ є прийнятним для стійких ЦВЗ; PSNR ≥ 44 дБ відповідає практично непомітному маркуванню [181]. Структурна подібність (SSIM), що краще корелює зі зоровим сприйняттям:

$$SSIM(x, y) = (2\mu_x \mu_y + C_1)(2\sigma_{xy} + C_2) / ((\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)) . \quad (1.10)$$

де: μ_x, μ_y – локальні середні, σ_x^2, σ_y^2 – дисперсії, σ_{xy} – коваріація, C_1 і C_2 – стабілізаційні константи [181]. SSIM ∈ [0, 1]; значення SSIM ≥ 0,95 є:

$$ODG(x, y) \geq ODG_{min}, \quad ODG_{min} \in [-1, 0] \text{ для малопомітного маркування}. \quad (1.11)$$

1.9.2. Метрики стійкості

Точність відновлення ідентифікатора оцінюється бітовою частотою помилок (BER):

$$BER(b, \hat{b}) = (1/L)\cdot\Sigma_j \mathbb{1}[b_j \neq \hat{b}_j], \quad (1.12)$$

де $\mathbb{1}[\cdot]$ – індикаторна функція. BER = 0 – повне відновлення, BER = 0,5 – відсутність корисного сигналу (випадкове вгадування). Для кореляційних детекторів додатково застосовується нормована кореляція (NC):

$$NC(w, \hat{w}) = \langle w, \hat{w} \rangle / (\|w\|\cdot\|\hat{w}\|), \quad (1.13)$$

де w – еталонний водяний знак, $\hat{w}$ – його оцінка з атакованого об’єкта; NC = 1 – ідеальне відновлення. Ці метрики, які наведені у табл. 1.3, використовуються надалі у розділах 2 та 3 при порівнянні методів.

Таблиця 1.3 – Метрики якості та стійкості для оцінювання ЦВЗ

Метрика	Формула (спрощено)	Діапазон	Інтерпретація
MSE	$(1/N)\Sigma(x_i-y_i)^2$	$[0,\infty)$	Базова міра спотворення; основа PSNR
PSNR	$10\cdot\log_{10}(255^2/MSE)$	$[0,\infty)$ дБ	Непомітність: > 38 дБ – прийнятно для ЦВЗ
SSIM	функція(μ, σ, σ_{xy})	[0, 1]	Структурна подібність: > 0,95 – прийнятно
ODG	Вихід моделі PEAQ	[−4, 0]	Перцептивна якість аудіо: ≥ −1 – малопомітно
BER	$(1/L)\Sigma\mathbb{1}[b_j\neq\hat{b}_j]$	[0, 1]	Точність відновлення бітів: 0 – ідеально, 0,5 – відмова
NC	$\langle w,\hat{w}\rangle/(\|w\|\|\hat{w}\|)$	[−1, 1]	Кореляційна схожість маркера: > 0,9 – надійно

Джерело: складено автором на основі [167, 170, 181, 182].

1.10. Стійкість до атак та формальні моделі перетворень

Стійкість вбудованого ідентифікатора визначається як здатність системи забезпечувати коректне або статистично достовірне відновлення маркера після дії типових перетворень цифрового середовища та навмисних атак. Ланцюжок «вбудовування – канал модифікації – детектор» формалізується як:

$$y = E(x, b, k, \theta), \quad \tilde{y} = A(y; \eta), \quad \hat{b} = D(\tilde{y}, k, \theta), \tag{1.14}$$

де η – параметр інтенсивності атаки. Агрегована стійкість оцінюється максимальними значеннями метрик по всій множині атак $\mathcal{A}$:

$$BER_{max} = max_{A\in\mathcal{A}}\, BER(b, \hat{b}_A), \quad NC_{min} = min_{A\in\mathcal{A}}\, NC(w, \hat{w}_A)\ . \tag{1.15}$$

Узагальнену класифікацію типових атак на мультимедійні дані за областю дії та типом носія наведено на рис. 1.9.

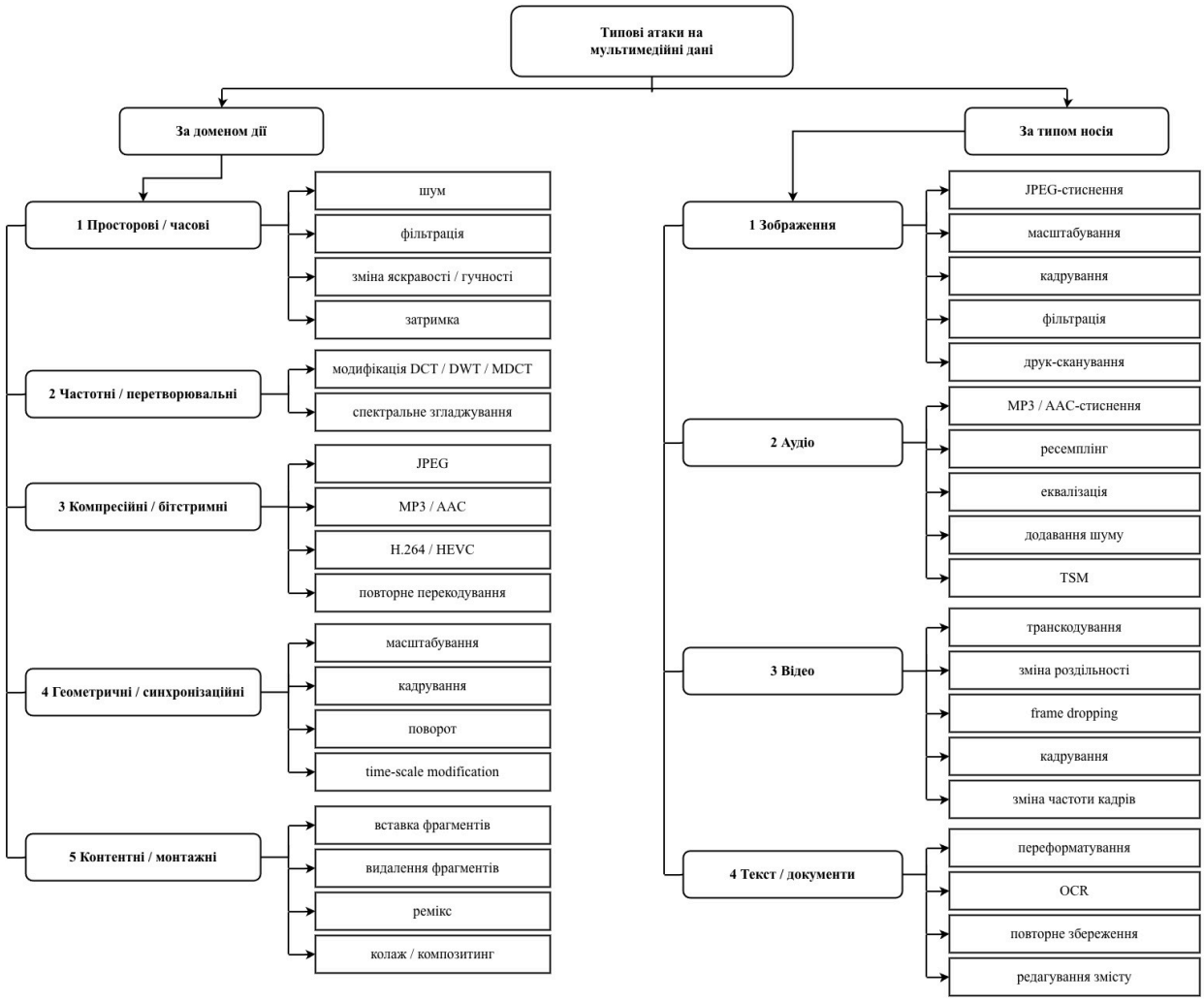


Рисунок 1.9 – Класифікація типових атак на мультимедійні дані за областю дії та типом носія

(Джерело: складено автором)

1.10.1. Моделі атак для зображень і відео

Стиснення JPEG/H.264 описується квантуванням коефіцієнтів у DCT-області:

$$\tilde{y} = T^{-1}(Q_{\Delta}(T(y))), \tag{1.16}$$

де T – блокове DCT, Q_{Δ} – оператор квантування з кроком Δ. Зі зменшенням якості Q зростає Δ, і маркери у середньочастотних коефіцієнтах:

$$[u; v] = s \cdot R_{\varphi}[u_0; v_0] + t, \quad \tilde{y}(u,v) = M(u,v) \cdot y(u,v), \tag{1.17}$$

де s – масштабний коефіцієнт, R_φ – матриця обертання, t – вектор зсуву, $M(u,v) \in \{0,1\}$ – маска обрізання. Стійкість до геометричних атак досягається інваріантними до RST ознаками або синхронізаційними шаблонами.

1.10.2. Моделі атак для аудіосигналів

MP3/AAC-стиснення описується аналітично-синтезним ланцюжком з квантуванням MDCT-коефіцієнтів відповідно до психоакустичної моделі:

$$\tilde{y} = MDCT^{-1}(Q_\Delta(MDCT(y))), \quad (1.18)$$

де Q_Δ – змінний поріг квантування, що залежить від рівня маскування в кожній підсмузі. Нормалізація гучності та зміна амплітуди: $\tilde{y}[n] = g \cdot y[n]$, де $g > 0$. Time-scale modification (TSM):

$$\tilde{y}(t) = y(t/\gamma), \quad (1.19)$$

де $\gamma < 1$ – пришвидшення, $\gamma > 1$ – уповільнення. TSM зберігає суб'єктивну якість, але десинхронізує позиції маркерів у часовій області, що є критичною атакою для LSB та Echo Hiding методів. Класи атак на мультимедійні дані та їх формальні моделі наведені у табл. 1.4.

Таблиця 1.4 – Класи атак на мультимедійні дані та їх формальні моделі

Клас атаки	Формальна модель	Параметр η	Типовий носій
JPEG-стиснення	$\tilde{y} = T^{-1}(Q\Delta(T(y)))$	Фактор якості Q	Зображення, відео
MP3/AAC-стиснення	$\tilde{y} = MDCT^{-1}(Q\Delta(MDCT(y)))$	Бітрейт R, кбіт/с	Аудіо
Масштабування/ RST	$[u;v] = s \cdot R\varphi[u_0;v_0]+t$	Коефіцієнт s, кут φ	Зображення, відео
Обрізання	$\tilde{y} = M \cdot y$	Частка обрізання rc	Зображ., відео, аудіо
Нормалізація гучності	$\tilde{y}[n] = g \cdot y[n]$	Коефіцієнт g	Аудіо
Time-scale modification	$\tilde{y}(t) = y(t/\gamma)$	Коефіцієнт γ	Аудіо
Гаусівський шум	$\tilde{y} = y + n$, $n \sim N(0,\sigma^2)$	Дисперсія σ^2	Усі типи
Ресемплінг	$\tilde{y}[n] = (y * h)[\lfloor n/r \rfloor]$	$r = fs'/fs$	Аудіо

Джерело: складено автором на основі [167, 168, 172, 183, 184, 185].

1.11. Висновки до розділу

У розділі здійснено комплексний огляд наукових, нормативно-правових і технологічних підходів до захисту інтелектуальної власності на мультимедійні дані в цифровому середовищі, а також формалізовано структуру мультимедійних сигналів як носіїв стійких ідентифікаторів. За результатами огляду можна сформулювати такі висновки:

1. Цифровізація, глобальна платформізація та поширення генеративного штучного інтелекту радикально посилили вразливість зображень, аудіо- та відеотворів до несанкціонованого копіювання, реміксування й повторного використання. Наявні правові механізми (директиви ЄС щодо авторського права в цифрову добу, інститути колективного управління) задають принципи охорони, проте їх реальна дієвість залежить від технічних засобів однозначної ідентифікації об’єктів та відстежуваності їх обігу.

2. Аналіз методів захисту показав, що жоден окремий клас (DRM, водяні знаки, фінгерпринтинг, криптографія) не забезпечує повного захисту. Класичні DRM втрачають дієвість після виходу контенту за межі контрольованої екосистеми; платформні системи (Content ID, фінгерпринтинг) прив’язані до конкретного посередника й не забезпечують переносимості доказової бази; блокчейн-реєстри фіксують права, але без стійкого технічного зв’язку між записом і файлом мають обмежену доказову силу. Це доводить необхідність систем, у яких маркер авторства ідентифікується на рівні самого мультимедійного сигналу.

3. Формалізація мультимедійних даних (підрозділи 1.7–1.10) показала, що стійкість маркера визначається насамперед вибором області вбудовування, а коректне порівняння методів можливе лише за рівних бюджетів спотворення (рівний PSNR для зображень, рівний SNR/segSNR для аудіо) та в межах явно заданої моделі атак. Установлено фундаментальний трикутник компромісів «непомітність – ємність – стійкість», у якому підвищення будь-якого критерію погіршує щонайменше один з інших.

4. Проведений огляд виявляє невирішену науково-практичну проблему. Наявні методи й системи або (а) забезпечують стійке маркування, але не інтегровані в цілісну інформаційну систему з верифікацією та реєстром прав, або (б) реалізують реєстрову чи правову інфраструктуру, але не мають надійного, стійкого до атак технічного зв'язку між конкретним мультимедійним файлом і записом про правовласника. Через цей розрив у реальних сценаріях правозастосування залишається невирішеним завдання відтворюваного, експертно перевірюваного доведення авторства та історії використання об'єкта незалежно від платформи та юрисдикції.

5. Розв'язання цієї проблеми має безпосереднє практичне значення: воно дає правовласникам інструмент доказовості у спорах, підвищує точність обліку використань (а отже й справедливість розподілу роялті), зменшує кількість хибних спрацьовувань автоматизованої фільтрації та створює технічну основу для протидії діпфейкам і несанкціонованому реміксуванню.

6. На основі проведеного огляду сформульовано ключові вимоги до розроблюваної інформаційної системи: стійкі невидимі ідентифікатори, вбудовані безпосередньо в сигнал і робастні до типових атак (стиснення, геометричні перетворення, спектральні зміни); незалежність від платформ розповсюдження та можливість витягання маркера з будь-якої копії файлу з подальшим зіставленням із реєстром прав; інтеграція з AI-модулями пошуку, стегоаналізу й форензики; сумісність із правозастосовчими процедурами. Саме на усунення виявленого розриву спрямовано подальші розділи дисертації, в яких побудовано математичні моделі та вдосконалені методи вбудовування, розроблено оригінальні авторські методи для зображень і аудіо та спроєктовано й реалізовано інформаційну систему IP-Protect.

РОЗДІЛ 2. МАТЕМАТИЧНІ МОДЕЛІ ТА УДОСКОНАЛЕННЯ МЕТОДІВ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ У МУЛЬТИМЕДІЙНІ ДАНІ

2.1. Постановка задачі, критерії ефективності та методика експериментального порівняння

Методи вбудовування цифрових водяних знаків у мультимедійні дані формально можна розглядати як відображення $E: X \times \{0,1\}^L \to Y$, де X – простір вихідних об'єктів, $\{0,1\}^L$ – бітова послідовність ідентифікатора, Y – простір позначених об'єктів. Кожна схема вбудовування узгоджує три базові вимоги – непомітність, стійкість та місткість, – які перебувають у взаємному конфлікті: посилення однієї, як правило, досягається коштом послаблення іншої [167, 168, 38]. Тому обґрунтований вибір і вдосконалення методу неможливі без кількісного оцінювання цього компромісу на репрезентативному наборі даних.

У цьому підрозділі кожний клас методів розглянуто за єдиною аналітичною схемою, що відповідає вимогам до теоретичного розділу дисертації: (1) формалізація наявного методу та його математичної моделі; (2) виявлення притаманних йому недоліків; (3) формулювання гіпотези щодо вдосконалення; (4) за можливості – доведення відповідного твердження; (5) експериментальна перевірка на реальних даних із конкретними кількісними показниками; (6) висновок про підвищення ефективності. Такий підхід забезпечує, що кожне запропоноване вдосконалення спирається не на якісні міркування, а на вимірюваний результат, і може бути покладене в основу формулювання наукової новизни.

Методика експериментального порівняння. Для кількісного оцінювання ефективності вдосконалень розроблено автоматизований конвеєр порівняльного тестування системи IP-Protect, який для заданої пари «класичний метод / удосконалений метод» виконує вбудовування ідентифікатора у весь тестовий набір, застосовує стандартизований перелік атак і обчислює порівняльні метрики. Експерименти проведено на наборі зі 150 аудіофайлів,

збалансованому за типами сигналу – від щільної сучасної поп- та електронної музики до академічних інструментальних і оркестрових творів, що забезпечує подання різних спектральних і динамічних характеристик сигналу. Обсяг вибірки перевищує типовий діапазон 10–20 еталонних тестових аудіофрагментів, прийнятий для оцінювання аудіомаркування [41], що підвищує статистичну надійність отриманих оцінок. Вбудовування виконується у PCM-області; основним вектором атаки обрано MP3-перекодування як найпоширеніший формат розповсюдження аудіоконтенту (бітрейти 128, 96 та 64 kbps), додатково розглянуто нормалізацію гучності, передискретизацію та низькочастотну фільтрацію як контрольні атаки. Перелік атак сформовано відповідно до усталеної класифікації атак на вбудовану інформацію [183, 185]. Для відтворюваності всі експерименти виконано з фіксованим початковим значенням генератора (seed = 12345).

Показники ефективності. Ефективність методу оцінюється трьома групами показників: (i) стійкість – коефіцієнт бітових помилок BER та частка файлів, для яких маркер успішно відновлено (виживання, критерій успіху BER ≤ 0,10); (ii) непомітність – відношення сигнал/шум SNR між оригіналом і позначеним сигналом [182]; (iii) обчислювальна вартість – час вбудовування та витягування. Підвищення стійкості кількісно виражається коефіцієнтом покращення як відношенням BER класичного методу до BER удосконаленого за однакових умов атаки.

Структурний принцип викладу. Класи методів розглянуто у порядку зростання стійкості. Недоліки простіших методів, виявлені експериментально, слугують безпосередньою мотивацією для переходу до складніших класів: зокрема, чутливість методів часової області до низькочастотної фільтрації обґрунтовує доцільність частотних методів, розглянутих у наступних підрозділах. У такий спосіб підрозділ формує послідовну лінію аргументації – від найпростіших до найстійкіших підходів.

2.2. Просторові методи (LSB та часова область)

Часова область охоплює два класичні підходи до вбудовування: побітовий, заснований на модифікації молодших розрядів окремих вибірок, та статистичний, що кодує біт через співвідношення статистик груп вибірок. У цьому підрозділі розглянуто обидва підходи та відповідні авторські вдосконалення.

2.2.1. Побітове вбудовування з QIM-надлишковим кодуванням (метод audio_qim_v1)

Розглянемо перший підхід – побітове вбудовування – та відповідне запропоноване вдосконалення [187]. Структурну схему методу audio_qim_v1 наведено на рис. 2.1.

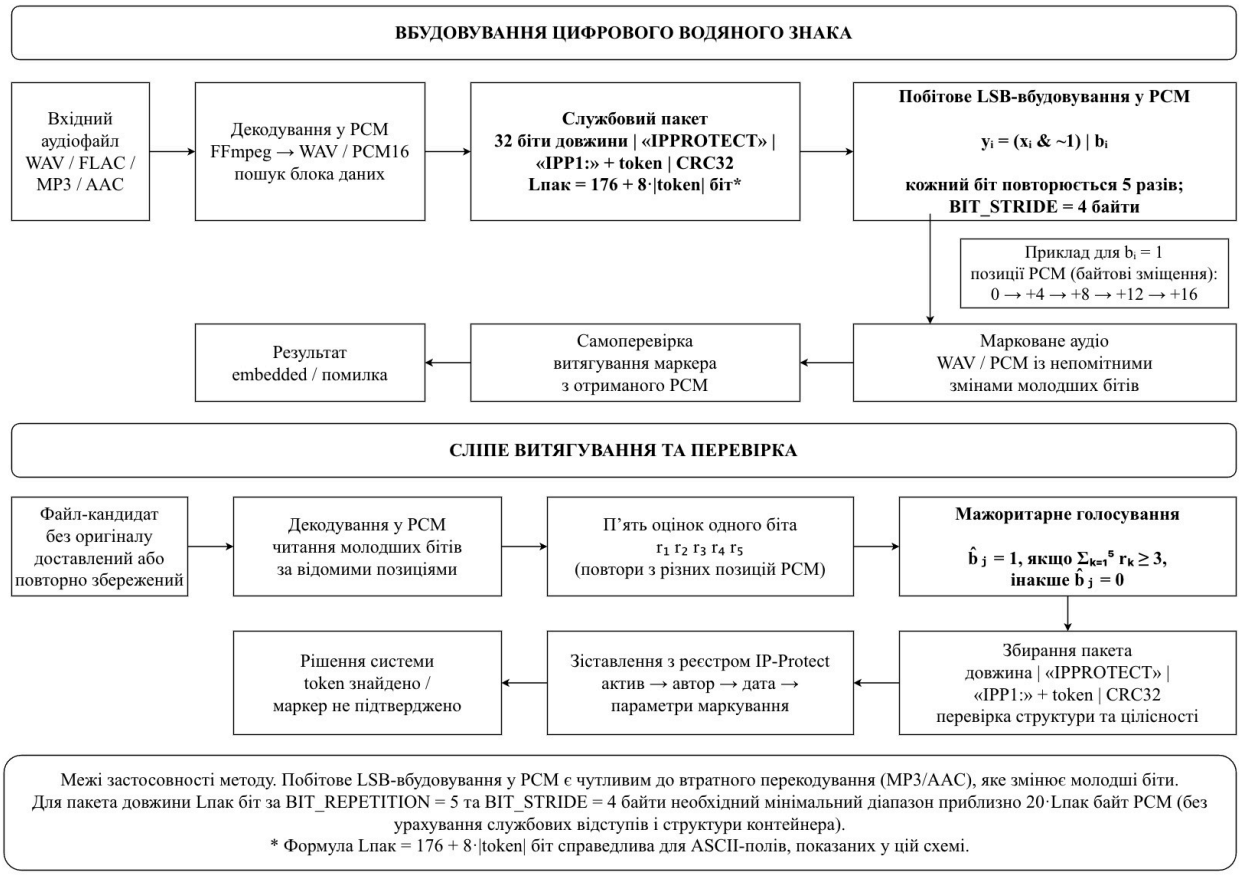


Рисунок 2.1 – Структурна схема методу audio_qim_v1 (побітове QIM-вбудовування з мажоритарним голосуванням)

(Джерело: складено автором)

Наявний метод та його модель. Найпростіший клас методів ґрунтується на заміні молодших бітів (LSB) пікселів, або PCM-вибірок [168]. Вбудовування одного біта $b \in \{0,1\}$ у позицію і описується як

$$y_i = (x_i \,\&\, \sim 1) \mid b, \tag{2.1}$$

де & – порозрядне AND, | – порозрядне OR, ~1 – маска обнулення молодшого біта. Витягування: $\hat{b} = \tilde{y}_i \,\&\, 1$. Узагальнена адитивна форма класу:

$$y = E(x, b, k; \theta) = x \oplus M(b, k), \tag{2.2}$$

де M(b, k) – псевдовипадкова маска молодших бітів, визначена ключем k. Перевагами методу є висока ємність (до 0,5 bpp для зображень) та мінімальна обчислювальна складність.

Недоліки. Метод має мінімальну стійкість. Оскільки інформація зосереджена у молодших розрядах, будь-яке перекодування зі втратами переписує ці розряди під час квантування і повністю руйнує маркер [38, 183]. Крім того, одиночне кодування біта не має механізму виявлення чи виправлення помилок, тому навіть слабкі спотворення призводять до неконтрольованого зростання BER, а сам факт наявності маркера неможливо довести формально. Ці недоліки підтверджено експериментально: за MP3-перекодування класичний метод audio_classic_lsb дає BER = 0,500 незалежно від бітрейту, що відповідає рівню випадкового вгадування, тобто повній втраті інформації (виживання 0%); аналогічний результат спостерігається за передискретизації (табл. 2.1).

Удосконалений метод audio_qim_v1. Пропонується замінити одиночне вбудовування на n-кратне надлишкове кодування з голосуванням більшістю, доповнене службовим пакетом фіксованого формату з контрольною сумою [179, 189]. У методі audio_qim_v1 реалізовано QIM-орієнтовану інтерпретацію у PCM-поданні [170, 187, 188]: кожний біт ідентифікатора вбудовується не в один відлік,

а у n = 5 повторів, рознесених по PCM-сигналу з кроком BIT_STRIDE = 4 байти, а витягування виконується голосуванням «3 з 5». Запропонована структура службового пакета IPP1:‹token› з 32-бітним полем довжини та CRC32 [189] забезпечує доказову ідентифікацію при витяганні; попередня оцінка придатності файлу та delivery-перевірка результату після реального перекодування роблять метод частиною доказово-орієнтованого конвеєра системи [190, 191]. Гіпотеза полягає в тому, що надлишкове кодування з голосуванням зменшує ймовірність помилки біта, а отже підвищує стійкість методу без істотної зміни принципу вбудовування.

Твердження 2.1. Нехай імовірність помилкового відновлення одного повтору дорівнює $p < 0{,}5$, а повтори статистично незалежні. Тоді за непарного числа повторів n і рішення голосуванням більшістю ймовірність помилкового декодування біта

$$P_n = \Sigma\, k > n/2\ C(n,k)\cdot p^k\cdot(1-p)^{n-k}, \qquad (2.3)$$

задовольняє нерівність $P_n < p$, тобто надлишкове кодування зменшує коефіцієнт бітових помилок. Коефіцієнт зниження помилки, зумовлений голосуванням, дорівнює $g = p / P_n$.

Доказ. Помилкове рішення виникає, коли неправильними виявляються більш ніж n/2 повторів. Для $n = 5$ та $p = 0{,}2$:

$$P_5 = C(5,3)\cdot 0{,}2^3\cdot 0{,}8^2 + C(5,4)\cdot 0{,}2^4\cdot 0{,}8 + 0{,}2^5 \approx 0{,}058, \qquad (2.4)$$

звідки $g = 0{,}2 / 0{,}058 \approx 3{,}4$. Оскільки для $p < 0{,}5$ функція $P_n(p)$ лежить нижче за пряму $y = p$, голосування більшістю гарантовано зменшує BER на всьому робочому діапазоні.

Експериментальна перевірка. Порівняння класичного методу audio_classic_lsb та удосконаленого audio_qim_v1 виконано на наборі зі 150 аудіофайлів (seed = 12345, критерій успіху BER ≤ 0,10); результати наведено в

табл. 2.1. За відсутності атаки обидва методи забезпечують безпомилкове відновлення (BER = 0, виживання 100%), що підтверджує коректність реалізації обох декодерів. За основним вектором атаки – MP3-перекодування – класичний метод повністю руйнується (BER = 0,500; виживання 0%), тоді як audio_qim_v1 зберігає BER = 0,092 за 128 kbps, 0,109 за 96 kbps та 0,131 за 64 kbps з відповідним виживанням 81,3%, 77,3% та 74,7%. Коефіцієнт покращення стійкості становить від 3,83× (64 kbps) до 5,45× (128 kbps). За нормалізації гучності удосконалений метод знижує BER з 0,143 до 0,044 (виживання 54,7% → 91,3%; коефіцієнт 3,22×), за передискретизації – забезпечує виживання 78,0–81,3% проти 0% у класичного методу.

Узгодженість із теоретичною оцінкою. Спостережувані значення BER дозволяють оцінити ефективну ймовірність помилки одного повтору p шляхом розв'язання рівняння (2.3) відносно p. Для MP3 128 kbps виміряному BER = 0,092 відповідає $p \approx 0{,}238$, для 96 kbps – $p \approx 0{,}255$, для 64 kbps – $p \approx 0{,}274$. Отже, внесок безпосередньо голосування більшістю у зниження помилки становить $g = p / P_5 \approx 2{,}6\times$ за 128 kbps і 2,1× за 64 kbps, що узгоджується з теоретичною оцінкою Твердження 2.1. Загальний коефіцієнт покращення відносно класичного методу (3,83–5,45×) перевищує цей внесок, оскільки додатково враховує перехід від модифікації молодших розрядів до QIM-орієнтованого вбудовування, стійкішого до квантування [170]. Таким чином, сумарний ефект вдосконалення декомпозується на два складники – зміну принципу вбудовування та надлишкове кодування, – кожен з яких робить окремий вимірюваний внесок.

Непомітність. Вбудовування маркера не призводить до помітного спотворення сигналу: середнє значення SNR становить 114,8 дБ (діапазон 107,1–121,3 дБ; σ = 2,6 дБ) для audio_qim_v1 та 77,9 дБ (діапазон 70,1–84,8 дБ; σ = 2,6 дБ) для класичного методу. Обидва значення суттєво перевищують поріг чутності слухового сприйняття. Вищий показник удосконаленого методу пояснюється локалізованим характером QIM-вбудовування: модифікації зосереджені у обмеженій кількості вибірок, тоді як класичний LSB рівномірно

змінює молодші розряди по всьому сигналу. Динаміку BER за атаками наведено на рис. 2.2, розподіл виживання – на рис. 2.3.

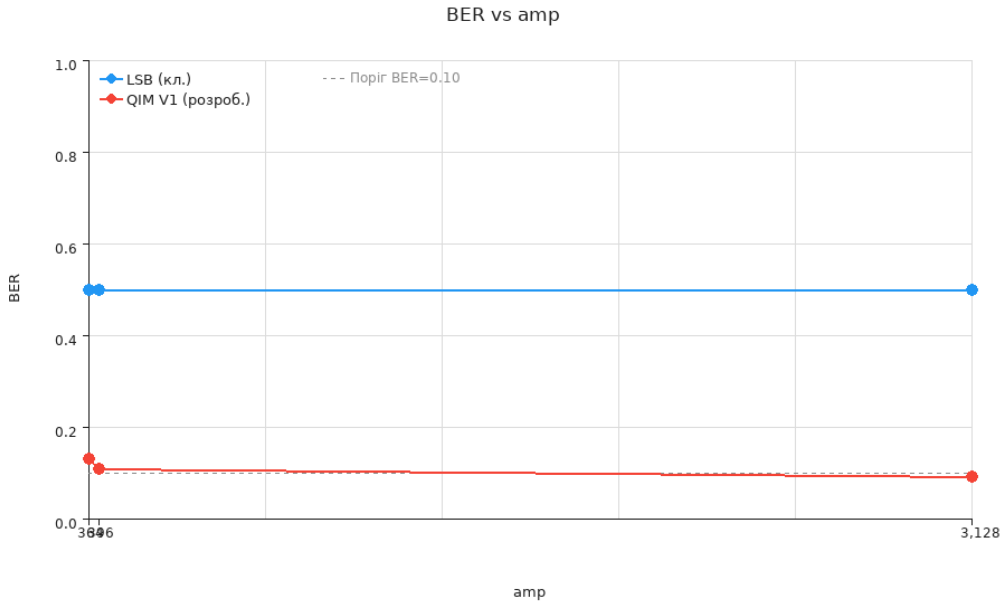


Рисунок 2.2 – Залежність BER методів audio_classic_lsb та audio_qim_v1 від сили MP3-стиснення

(Джерело: складено автором)

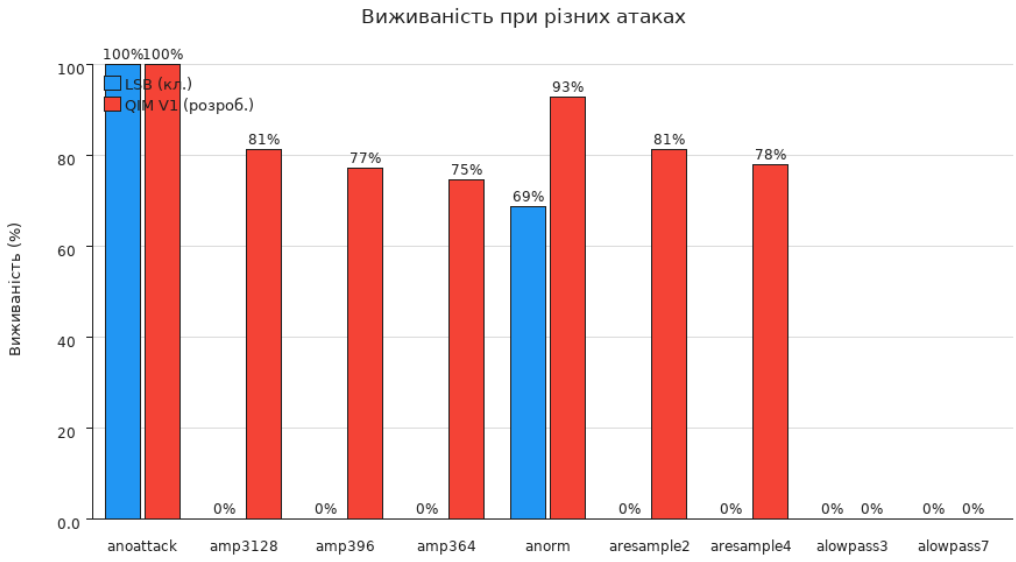


Рисунок 2.3 – Частка файлів зі збереженим маркером (виживання) за атаками – audio_classic_lsb та audio_qim_v1

(Джерело: складено автором)

Аналіз залишкових відмов. Пофайловий аналіз показує, що розподіл BER удосконаленого методу є неоднорідним: для більшості файлів маркер відновлюється практично безпомилково (BER ≤ 0,023), тоді як приблизно 18% файлів за MP3 128 kbps дають BER ≈ 0,5, що відповідає втраті синхронізації декодера внаслідок затримки та доповнення, які вносить MP3-кодер [173]. Саме ці файли формують основну частку відмов і пояснюють різницю між середнім BER та часткою виживання. Отже, подальший резерв підвищення стійкості методу полягає не у збільшенні амплітуди вбудовування, а у вдосконаленні механізму пошуку синхронізації під час витягування [173, 202].

Межа застосовності. Експеримент виявив спільне обмеження обох методів часової області: низькочастотна фільтрація руйнує маркер незалежно від способу кодування (BER ≈ 0,50; виживання 0% для обох методів), оскільки видаляє високочастотні складові, у яких зосереджено модифікації PCM-сигналу. Це обмеження визначає межу застосовності просторово-часового підходу і безпосередньо мотивує перехід до частотних та часово-частотних методів, розглянутих у наступних підрозділах.

Висновок. Запропоноване надлишкове кодування з голосуванням більшістю у поєднанні з QIM-орієнтованим вбудовуванням у PCM- подання підвищує стійкість методу вбудовування у часовій області у 3,8–5,5 раза за основним вектором атаки (MP3-перекодування), забезпечуючи відновлення маркера для 74,7–81,3% файлів проти повної відмови класичного методу, без погіршення непомітності. Результат підтверджено як теоретично (Твердження 2.1), так і експериментально на вибірці зі 150 файлів (Табл. 2.1). Підвищення стійкості досягається ціною зменшення ефективної пропускної здатності каналу вбудовування внаслідок п’ятикратного повторення кожного біта. Водночас для практичного застосування в системі IP-Protect така пропускна здатність залишається достатньою, оскільки у мультимедійний об’єкт вбудовується компактний службовий ідентифікатор, тоді як розширені відомості про актив і правовласника зберігаються у зовнішньому реєстрі. Службовий пакет IPP1 з CRC32 додатково забезпечує доказову ідентифікацію маркера [190, 191].

Водночас метод зберігає чутливість до низькочастотної фільтрації, що окреслює напрям подальшого вдосконалення.

Таблиця 2.1 – Порівняння стійкості методів audio_classic_lsb та audio_qim_v1 (150 файлів, seed = 12345, критерій BER ≤ 0,10)

Атака	BER клас.	BER розроб.	SNR клас., дБ	SNR розроб., дБ	Вижив. клас.	Вижив. розроб.	Коеф. покращ.
Без атаки (еталон)	0,000	0,000	77,9	114,8	100%	100%	–
MP3 128 kbps	0,500	0,092	77,9	114,8	0%	81,3%	5,45×
MP3 96 kbps	0,500	0,109	77,9	114,8	0%	77,3%	4,58×
MP3 64 kbps	0,500	0,131	77,9	114,8	0%	74,7%	3,83×
Нормалізація гучності	0,143	0,044	77,9	114,8	54,7%	91,3%	3,22×
Передискретизація ×2	0,500	0,092	77,9	114,8	0%	81,3%	5,45×
Передискретизація ×4	0,500	0,098	77,9	114,8	0%	78,0%	5,12×
Низькочаст. фільтр. w=3	0,455	0,500	77,9	114,8	0%	0%	межа[1]
Низькочаст. фільтр. w=7	0,443	0,500	77,9	114,8	0%	0%	межа[1]

[1] *Обидва методи не витримують низькочастотної фільтрації; результат розглянуто як межу застосовності просторово-часового підходу (див. текст).*

Джерело: складено автором

2.2.2. Статистичне patchwork-вбудовування з груповим усередненням (метод audio_patchwork_v2)

Другий класичний підхід часової області – статистичний (patchwork) – кодує біт не в окремих розрядах, а через співвідношення статистик двох груп вибірок, що за побудовою робить його стійкішим до локальних спотворень за побітове кодування [187, 188]. Структурну схему методу audio_patchwork_v2 наведено на рис. 2.4.

Наявний метод та його модель. Класичний метод patchwork кодує кожний біт через статистичне зміщення між двома псевдовипадково вибраними групами PCM-вибірок (групи A і B) по m відліків усередині короткого stride [187].

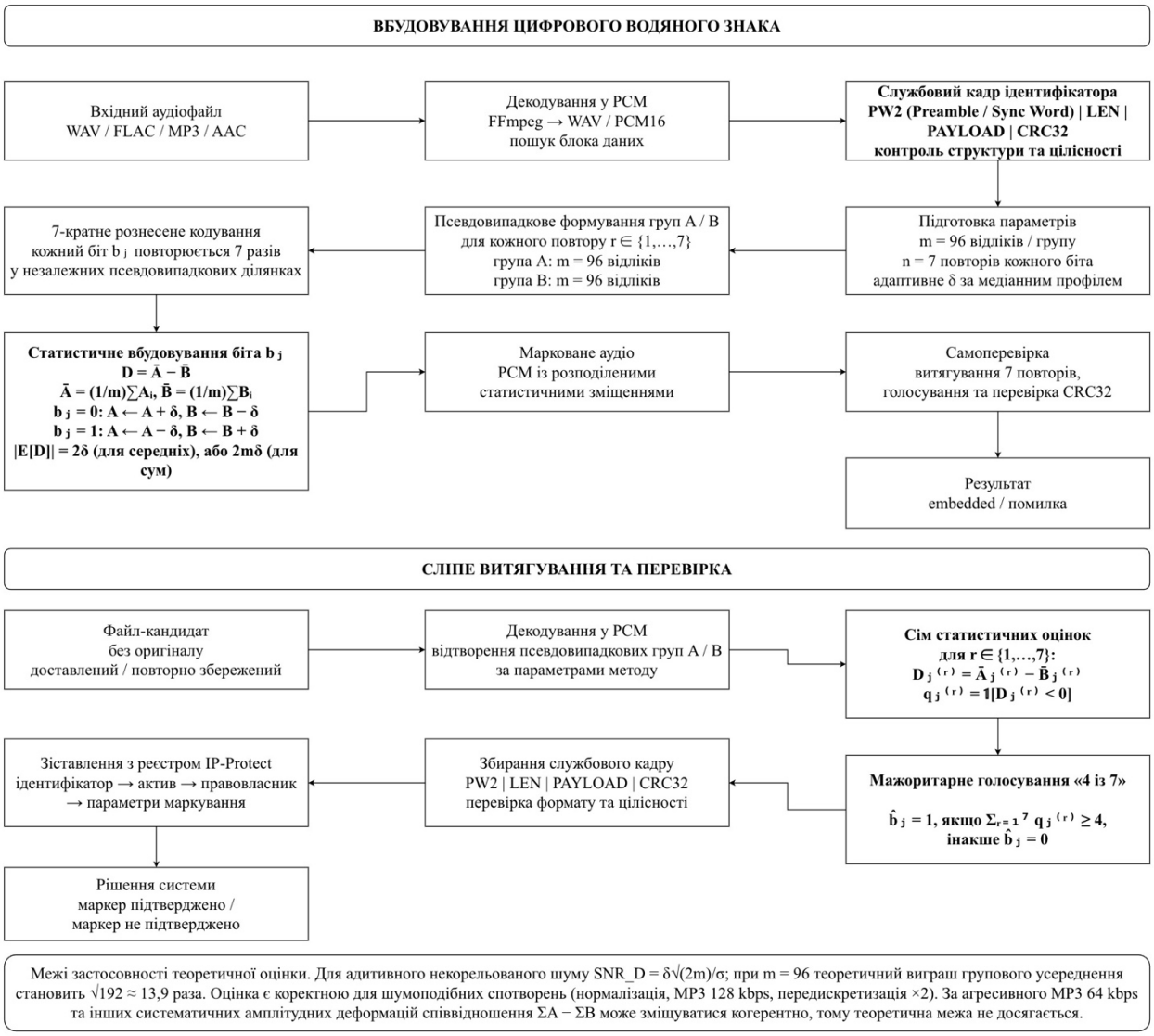


Рисунок 2.4 – Структурна схема методу audio_patchwork_v2 (статистичне вбудовування через контраст груп A/B)

(Джерело: складено автором)

Позначимо Σ_A та Σ_B суми амплітуд вибірок у групах A і B відповідно. Вбудовування біта b виконується внесенням різниці $\pm\delta$:

$$\Sigma_A - \Sigma_B \to +\delta \text{ для } b = 0, \quad -\delta \text{ для } b = 1, \tag{2.5}$$

а витягування – за знаком різниці статистик:

$$\hat{b} = \mathbb{1}[\, \Sigma_A - \Sigma_B < 0 \,]. \tag{2.6}$$

Перевагою методу є усереднення за групою вибірок, що частково компенсує локальний шум. Проте у класичному вигляді кожний біт кодується одноразово, без надлишковості та без службової структури.

Недоліки. Класичний patchwork не має механізму надлишкового кодування, контролю цілісності та доказової ідентифікації маркера: біт кодується одним зміщенням, тому помилка знака різниці $\Sigma_A - \Sigma_B$ одразу спотворює біт. Відсутність контрольної суми не дозволяє відрізнити коректно відновлений маркер від випадкового збігу.

Удосконалений метод audio_patchwork_v2. Пропонується доповнити статистичне кодування трьома складниками: (i) n-кратним надлишковим кодуванням з голосуванням більшістю; (ii) службовою структурою кадру PW2+LEN+PAYLOAD+CRC32 для доказової ідентифікації та контролю цілісності [189]; (iii) попередньою перевіркою ємності та самоперевіркою результату. У методі audio_patchwork_v2 реалізовано n = 7 повторів кожного біта з голосуванням «4 з 7», розмір групи m = 96 вибірок, адаптивний вибір δ за медіанним профілем сигналу. Гіпотеза полягає в тому, що поєднання групового усереднення, надлишкового кодування та адаптивної амплітуди підвищує стійкість статистичного методу за збереження непомітності, а службовий кадр забезпечує формальну ідентифікацію маркера [190].

Твердження 2.2. Нехай кожний біт кодується зміщенням ±δ у двох групах по m вибірок, а атака моделюється адитивним некорельованим шумом з дисперсією σ^2. Тоді статистика рішення $D = \Sigma_A - \Sigma_B$ має математичне сподівання $|E[D]| = 2m\delta$ та дисперсію $Var[D] = 2m\sigma^2$, звідки відношення сигнал/шум статистики рішення

$$SNR_D = 2m\delta / \sqrt{(2m\sigma^2)} = \delta\sqrt{(2m)} / \sigma \qquad (2.7)$$

перевищує відповідний показник одиночної вибірки (δ/σ) у $\sqrt{(2m)}$ разів. Для m = 96 маємо $\sqrt{(2m)} = \sqrt{192} \approx 13{,}9$.

Доказ. Статистика D є сумою 2m незалежних доданків. Корисний сигнал додається когерентно: $|E[D]| = m\delta - (-m\delta) = 2m\delta$, тобто зростає пропорційно m. Шумові складові додаються некогерентно, тому їхні дисперсії підсумовуються: $\mathrm{Var}[D] = 2m\sigma^2$, а стандартне відхилення зростає як $\sqrt{(2m)}$. Відношення сподівання до стандартного відхилення дорівнює $2m\delta / (\sigma\sqrt{(2m)}) = \delta\sqrt{(2m)}/\sigma$, що і потрібно було довести. Оскільки надлишкове кодування з n = 7 повторів додатково зменшує ймовірність помилки біта згідно з Твердженням 2.1 (для p = 0,2: $P_7 \approx 0{,}033$, $g = p/P_7 \approx 6{,}0$), сумарний теоретичний виграш є добутком групового та мажоритарного внесків.

Межа застосовності теореми. Оцінка $\sqrt{(2m)}$ виведена у припущенні адитивного некорельованого шуму. Це припущення виконується для слабких та середніх спотворень (нормалізація, MP3 128 kbps, передискретизація ×2), де відхилення статистики D близькі до шумових. Проте за агресивного стиснення (MP3 64 kbps) атака перестає бути шумоподібною і стає систематичною амплітудною деформацією співвідношення $\Sigma_A - \Sigma_B$, яка когерентно зміщує статистику рішення й перевертає знак на ключових бітах. Для такого режиму припущення теореми не виконуються, тому теоретична межа $\sqrt{(2m)}$ не досягається, а спостережуваний виграш скорочується до паритету. Отже, Твердження 2.2 визначає верхню границю виграшу в шумоподібному режимі, а розбіжність із нею за сильного стиснення є не суперечністю, а індикатором виходу за межі застосовності моделі.

Експериментальна перевірка. Порівняння класичного методу audio_classic_patch ($\delta = 1500$) та удосконаленого audio_patchwork_v2 виконано на наборі зі 150 аудіофайлів за однакової непомітності: середній SNR становить 30,9 дБ для класичного та 28,1 дБ для удосконаленого методу (різниця 2,8 дБ), що виключає вплив різної амплітуди вбудовування на результат. За відсутності атаки обидва методи відновлюють маркер практично безпомилково (виживання 98,0% та 100%). На основному векторі атаки удосконалений метод стабільно переважає класичний: за MP3 128 kbps виживання зростає з 61,3% до 95,3% (коефіцієнт 1,55×), за MP3 96 kbps – з 58,0% до 86,7% (1,49×), за передискретизації ×2 – з

57,3% до 86,0% (1,50×). Отже, у шумоподібному режимі вдосконалення забезпечує підвищення стійкості у 1,5 рази за рівної непомітності, що узгоджується з напрямом Твердження 2.2. Результати експерименту представлені у табл. 2.2.

Таблиця 2.2 – Порівняння стійкості методів audio_classic_patch та audio_patchwork_v2 за рівної непомітності (150 файлів, seed = 12345, критерій BER ≤ 0,10)

Атака	BER клас.	BER розроб.	SNR клас., дБ	SNR розроб., дБ	Вижив. клас.	Вижив. розроб.	Коеф. покращ.
Без атаки (еталон)	0,010	0,000	30,9	28,1	98,0%	100%	+2 в.п.
MP3 128 kbps	0,193	0,023	30,9	28,1	61,3%	95,3%	1,55×
MP3 96 kbps	0,210	0,067	30,9	28,1	58,0%	86,7%	1,49×
MP3 64 kbps	0,203	0,250	30,9	28,1	59,3%	50,0%	0,84×[1]
Нормалізація гучності	0,010	0,000	30,9	28,1	98,0%	100%	+2 в.п.
Передискретизація ×2	0,213	0,070	30,9	28,1	57,3%	86,0%	1,50×
Передискретизація ×4	0,213	0,283	30,9	28,1	57,3%	43,3%	0,76×[1]
Низькочаст. фільтр. w=3	0,213	0,403	30,9	28,1	57,3%	19,3%	межа[1]
Низькочаст. фільтр. w=7	0,220	0,483	30,9	28,1	56,0%	3,3%	межа[1]

[1] *За агресивного стиснення, сильної передискретизації та низькочастотної фільтрації удосконалений метод не переважає класичний; ці режими відповідають межі застосовності методу часової області (див. текст).*

Джерело: складено автором

Межа застосовності методу. За агресивного стиснення (MP3 64 kbps) і сильної передискретизації (×4) удосконалений метод сходиться до паритету з класичним (0,84× та 0,76× відповідно), а за низькочастотної фільтрації поступається йому (0,34× та 0,06×). Це узгоджується з межею застосовності Твердження 2.2: за таких атак деформація стає систематичною, і статистичне усереднення втрачає ефективність [183]. Низькочастотна фільтрація, як і для побітових методів, руйнує маркер незалежно від способу кодування, оскільки видаляє високочастотні складові сигналу. Таким чином, статистичний метод

часової області, попри вищу стійкість за побітовий, має спільну з ним фундаментальну межу – чутливість до частотно-вибіркових атак, – що безпосередньо мотивує перехід до частотних методів у наступному підрозділі [202]. Динаміку BER за атаками наведено на рис. 2.5, розподіл виживання – на рис. 2.6.

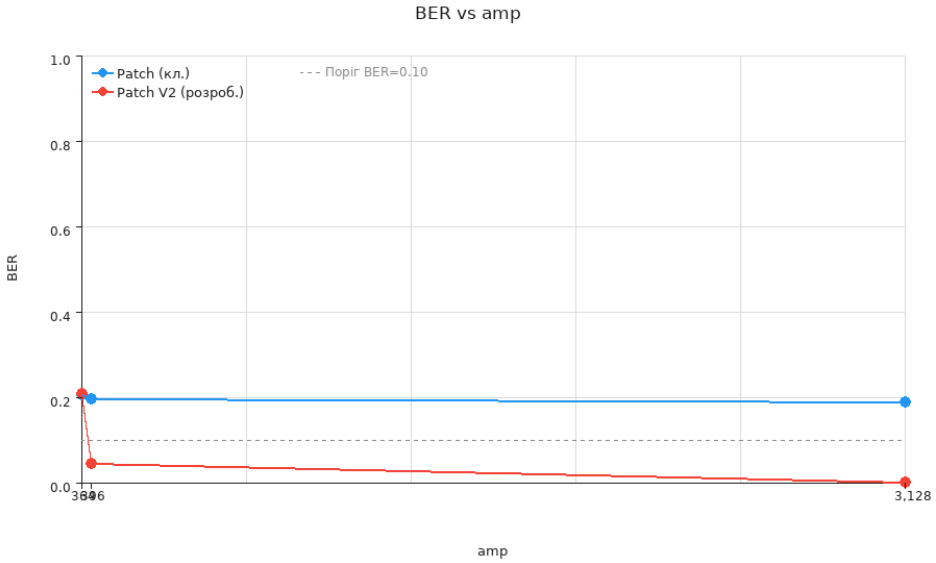


Рисунок 2.5 – Залежність BER методів audio_classic_patch та audio_patchwork_v2 від сили MP3-стиснення

(Джерело: складено автором)

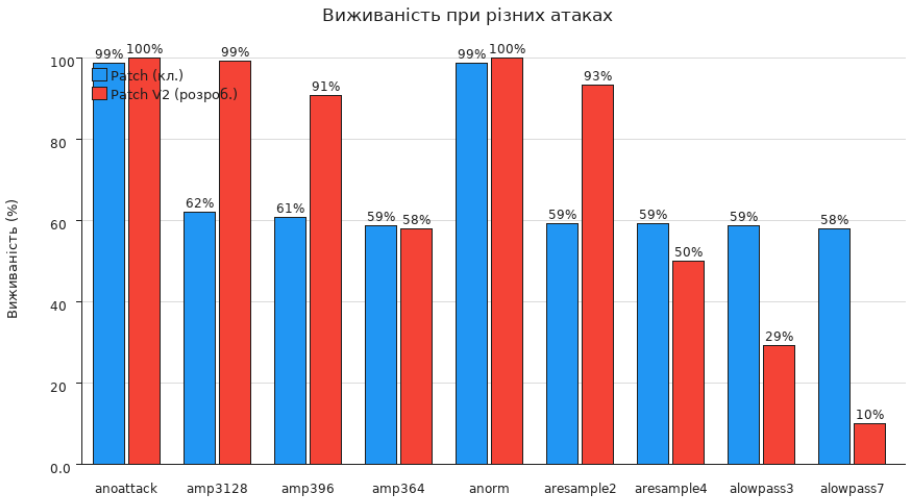


Рисунок 2.6 – Частка файлів зі збереженим маркером за атаками – audio_classic_patch та audio_patchwork_v2

(Джерело: складено автором)

Висновок. Запропоноване поєднання групового статистичного кодування, надлишкового кодування з голосуванням «4 з 7» та службового кадру з CRC32 підвищує стійкість методу patchwork у 1,5 раза за основним вектором атаки (MP3 128–96 kbps, передискретизація ×2) при рівній непомітності, що підтверджено теоретично (Твердження 2.2) та експериментально на вибірці зі 150 файлів. Службовий кадр PW2 з контролем цілісності додатково забезпечує доказову ідентифікацію маркера [190]. Водночас метод зберігає спільну з побітовими методами чутливість до агресивного стиснення та низькочастотної фільтрації, що визначає межу застосовності часової області та обґрунтовує доцільність частотних методів вбудовування.

2.3. Частотні методи на основі дискретного косинусного перетворення та QIM (для зображень)

Обмеження методів часової області, виявлені у попередньому підрозділі – руйнування маркера за частотно-вибіркових атак, – мотивують перехід до частотної області. Вбудовування у коефіцієнти дискретного косинусного перетворення (DCT) узгоджується з механізмом JPEG-стиснення, яке саме й оперує DCT-коефіцієнтами, що за побудовою підвищує стійкість до найпоширенішої атаки на зображення [38]. Структурну схему методу wm_v2_dct_qim_profile наведено на рис. 2.7.

Наявний метод та його модель. Класичний DCT-метод вбудовує біт у заздалегідь фіксований DCT-коефіцієнт блоку 8×8 шляхом його зміщення на величину ±δ. Позначимо c обраний коефіцієнт блоку. Вбудовування:

$$c' = c + (-1)^b \cdot \delta, \tag{2.8}$$

а витягування виконується порівнянням коефіцієнта з опорним значенням. Оскільки область DCT-перетворення збігається з областю JPEG-квантування, метод має помірну стійкість до стиснення, вищу за просторові підходи.

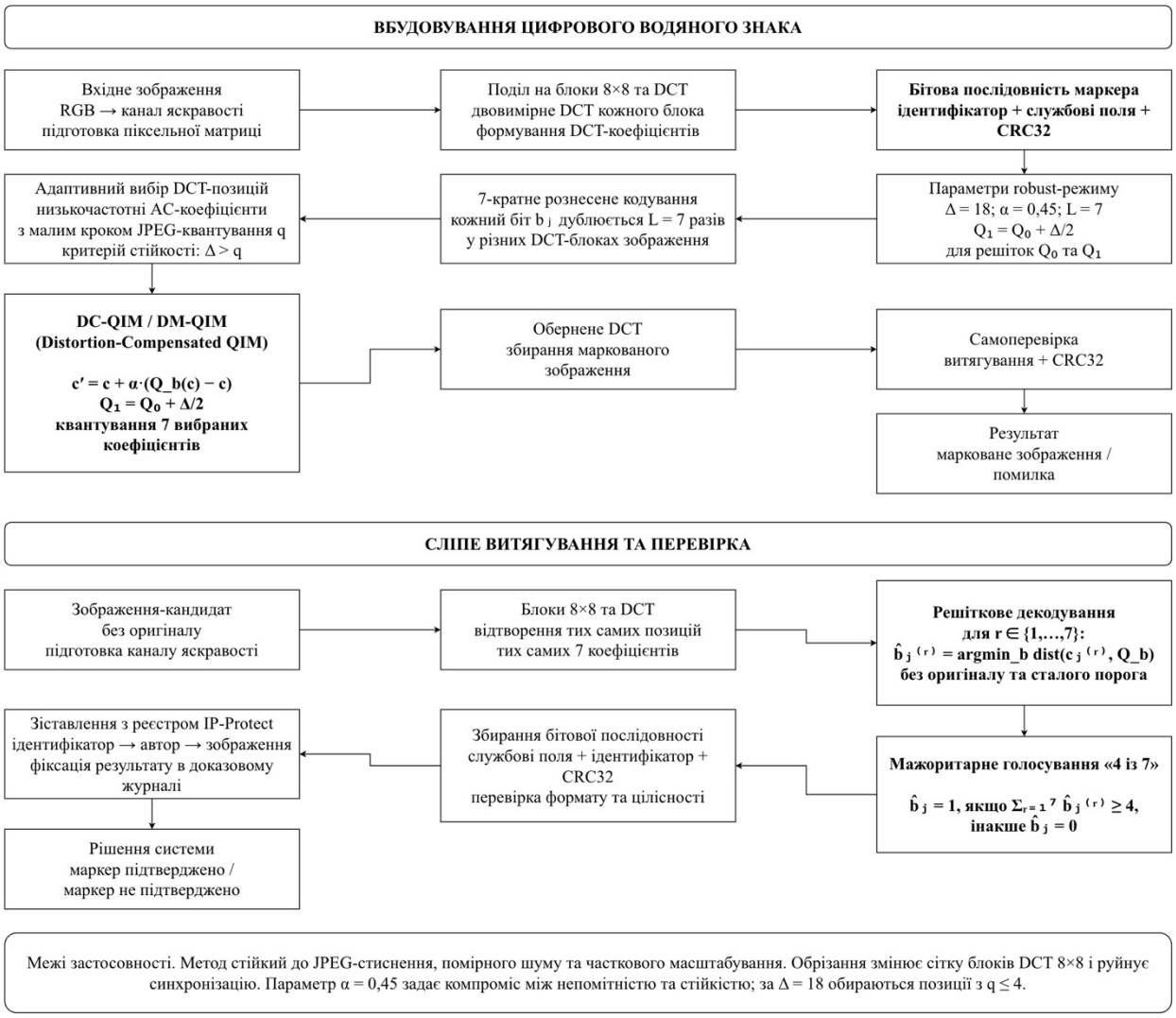


Рисунок 2.7 – Структурна схема методу wm_v2_dct_qim_profile (DC-QIM з адаптивним вибором DCT-позицій)

(Джерело: складено автором)

Недоліки. Класичний метод має три обмеження. По-перше, вбудовування у фіксовану позицію коефіцієнта не враховує, що різні позиції DCT квантуються JPEG із різним кроком: для позицій із великим кроком квантування біт руйнується вже за помірного стиснення. По-друге, одиночне кодування біта без надлишковості робить метод чутливим до адитивного шуму та масштабування. По-третє, порогове витягування потребує узгодження з оригіналом або сталим порогом, що знижує надійність сліпого декодування.

Удосконалений метод. Пропонується замінити адитивне зміщення фіксованого коефіцієнта на квантувальну індексну модуляцію (QIM) [170] з двома

складниками вдосконалення: (i) адаптивним вибором DCT-позицій із малим кроком квантування, що гарантує збереження біта навіть за сильного стиснення; (ii) надлишковим кодуванням кожного біта у repeat = 7 коефіцієнтах різних блоків із голосуванням більшістю [189]. У методі wm_v2_dct_qim_profile реалізовано distortion-compensated QIM: коефіцієнт зміщується до найближчого вузла однієї з двох решіток Q_0 або Q_1 (зсунутих на $\Delta/2$) з коефіцієнтом змішування $\alpha = 0{,}45$, а витягування виконується суто решітковим декодером $\operatorname{argmin}_b \operatorname{dist}(c, Q_b)$ без знання оригіналу. Гіпотеза полягає в тому, що узгодження кроку решітки Δ із кроком квантування JPEG забезпечує збереження біта, а надлишкове кодування додатково підвищує стійкість до шуму та масштабування.

Твердження 2.3. Нехай біт вбудовано у DCT-коефіцієнт методом QIM з кроком решітки Δ (решітки Q_0 та Q_1 зсунуті одна відносно одної на $\Delta/2$), а JPEG-стиснення квантує цей коефіцієнт із кроком q, вносячи похибку округлення у межах e, $|e| < q/2$. Тоді у разі, коли коефіцієнт встановлено точно у вузол решітки Q_b, решітковий декодер коректно відновлює біт за умови

$$q / 2 < \Delta / 4, \quad \text{тобто} \quad \Delta > 2q \ (\text{або } q < \Delta / 2). \tag{2.9}$$

Доказ. Об'єднання решіток $Q_0 \cup Q_1$ має крок $\Delta/2$, тому найближчий вузол іншої решітки розташований на відстані $\Delta/2$ від вузла решітки Q_b, а межа рішення декодера $\operatorname{argmin}_b \operatorname{dist}(c, Q_b)$ проходить посередині – на відстані $\Delta/4$ від вузла. Хибне рішення можливе лише тоді, коли спотворення зміщує коефіцієнт за цю межу. JPEG-квантування вносить похибку не більшу за $q/2$. Отже, за умови $q/2 < \Delta/4$, еквівалентної $\Delta > 2q$, спотворений коефіцієнт залишається ближчим до вузла вихідної решітки, і біт відновлюється коректно.

Зауваження до Твердження 2.3. У методі wm_v2_dct_qim_profile застосовано квантувальну індексну модуляцію з компенсацією спотворень (DC-QIM): $y = Q_b(c) + \alpha(c - Q_b(c))$, де $\alpha \in [0; 1)$ – частка вихідного відхилення від вузла, що зберігається для зменшення спотворення ($\alpha = 0$ відповідає жорсткому QIM). Залишкове відхилення від вузла тоді сягає $\alpha\Delta/2$, і умова коректного декодування в гіршому випадку набуває вигляду $\alpha\Delta/2 + q/2 < \Delta/4$, тобто $q < (1 -$

$2\alpha)\Delta/2$. За $\alpha = 0{,}45$ і $\Delta = 18$ це дає $q < 0{,}9$, тобто детермінованої гарантії для реальних кроків квантування JPEG немає. Тому для режиму DC-QIM Твердження 2.3 має ймовірнісний характер: за рівномірного розподілу відхилення $c - Q_b(c)$ на $[-\Delta/2; \Delta/2]$ і похибки JPEG на $[-q/2; q/2]$ ймовірність помилки окремого коефіцієнта p зростає зі зростанням q, а надлишкове кодування repeat = 7 з голосуванням більшістю знижує ймовірність помилки біта до P_7 (Твердження 2.1).

Узгодженість із теоретичною оцінкою. Твердження 2.3 безпосередньо пояснює експериментальні результати. За кроку решітки $\Delta = 18$ допустиме зміщення коефіцієнта для жорсткого QIM становить $\Delta/4 = 4{,}5$. Для JPEG Q = 90 крок квантування у позиціях вбудовування становить $q \approx 3$, похибка не перевищує 1,5, і умова (2.9) виконується із запасом ($1{,}5 < 4{,}5$); за Q = 85 запас зменшується, але умова зберігається. Для фіксованої високочастотної позиції за Q = 75 крок $q \approx 16$ дає похибку до $8 > 4{,}5$, тобто умова порушується ($q > \Delta/2$) і біт руйнується. Для робочого режиму DC-QIM ($\alpha = 0{,}45$) ймовірнісна оцінка за Зауваженням до Твердження 2.3 дає за $q \approx 3$ ймовірність помилки коефіцієнта близько 0,05, а після голосування «4 з 7» – близько 10^{-4}, що узгоджується з BER = 0 за Q = 90. За Q = 75 крок квантування у позиціях вбудовування становить $q \approx$ 5–8, і оцінка BER після голосування становить 0,003–0,03, що одного порядку з виміряним значенням 0,0287. Отже, виправлена умова пояснює повну стійкість за Q = 90 і 85 та наявність залишкових помилок за Q = 75, де крок квантування наближається до межі $\Delta/2$. Додатково надлишкове кодування repeat = 7 знижує залишкову ймовірність помилки згідно з Твердженням 2.1 (для n = 7: $P_7 = \Sigma_{k\geq 4} C(7,k)p^k(1-p)^{7-k}$), що підвищує стійкість до адитивного шуму та масштабування, для яких похибка не є суто квантувальною.

Експериментальна перевірка. Порівняння класичного методу wm_classic_dct ($\delta = 150$) та удосконаленого wm_v2_dct_qim_profile ($\Delta = 18$, $\alpha = 0{,}45$, repeat = 7) виконано на наборі з 567 зображень за рівної непомітності: середній PSNR становить 56,05 дБ для класичного та 55,88 дБ для удосконаленого методу (різниця 0,17 дБ). За відсутності атаки обидва методи

відновлюють маркер практично безпомилково (виживання 98,4% та 100%). За основним вектором атаки – JPEG-стисненням – удосконалений метод досягає повної стійкості (100%) за Q = 90 та 85 проти 97,4–97,5% у класичного, а за найжорсткішого Q = 75 методи статистично рівноцінні (92,1% проти 91,7%, довірчі інтервали перекриваються), хоча BER запропонованого методу нижчий (0,0287 проти 0,0482). Це узгоджується з Твердженням 2.3: адаптивний вибір низькочастотних позицій утримує умову $\Delta > q$, забезпечуючи повну стійкість за Q = 90 і 85 та майже повну за Q = 75. Ключова перевага виявляється за геометричних та шумових атак: за масштабування ×0,5 виживання зростає з 50,1% до 67,7%, тобто на 17,6 відсоткового пункту (коефіцієнт 1,35×), за адитивного шуму $\sigma = 5$ – з 93,3% до 99,8%. Оскільки класичний DCT-метод за побудовою вже стійкий до JPEG, простір для покращення саме за цим вектором обмежений, тому основний внесок удосконалення проявляється у стійкості до масштабування та шуму за збереження повної стійкості до стиснення. Результати експерименту наведено в табл. 2.3.

Таблиця 2.3 – Порівняння стійкості методів wm_classic_dct та wm_v2_dct_qim_profile за рівної непомітності (567 зображень, критерій BER ≤ 0,10)

Атака	BER клас.	BER розроб.	PSNR клас., дБ	PSNR розроб., дБ	Вижив. клас.	Вижив. розроб.	Коеф. покращ.
Без атаки (еталон)	0,008	0,000	56,05	55,88	98,4%	100%	+1,6 в.п.
JPEG Q = 90	0,015	0,000	56,05	55,88	97,4%	100%	+2,6 в.п.
JPEG Q = 85	0,017	0,000	56,05	55,88	97,5%	100%	+2,5 в.п.
JPEG Q = 75	0,048	0,0287	56,05	55,88	91,7%	92,1%	+0,4 в.п.
Масштабування ×0,5	0,163	0,150	56,05	55,88	50,1%	67,7%	1,35×
Адитивний шум σ = 5	0,038	0,001	56,05	55,88	93,3%	99,8%	+6,5 в.п.
Обрізання 10%	0,496	0,492	56,05	55,88	0%	1,1%	межа[1]

[1] *Обрізання зміщує сітку блоків DCT і руйнує маркер незалежно від способу кодування; режим відповідає межі застосовності частотно-блокового підходу (див. текст).*

Джерело: складено автором

Межа застосовності. Обидва методи не витримують обрізання зображення (crop 10%): виживання класичного методу становить 0%, удосконаленого – 0,7%. Причина є структурною: QIM-вбудовування прив'язане до сітки блоків DCT 8×8, а обрізання зміщує цю сітку, унаслідок чого декодер зчитує коефіцієнти не тих блоків, і умова Твердження 2.3 стає незастосовною, оскільки спотворення має геометричну, а не квантувальну природу. Крім того, застосований distortion-compensated режим (α = 0,45) свідомо жертвує частиною стійкості задля зниження візуальних артефактів; вибір α є компромісом між непомітністю та стійкістю. Чутливість до геометричних атак визначає межу застосовності частотно-блокового підходу і мотивує застосування геометрично-інваріантних та синхронізаційних механізмів. Динаміку BER за рівнем JPEG-стиснення наведено на рис. 2.8, розподіл виживання за атаками – на рис. 2.9.

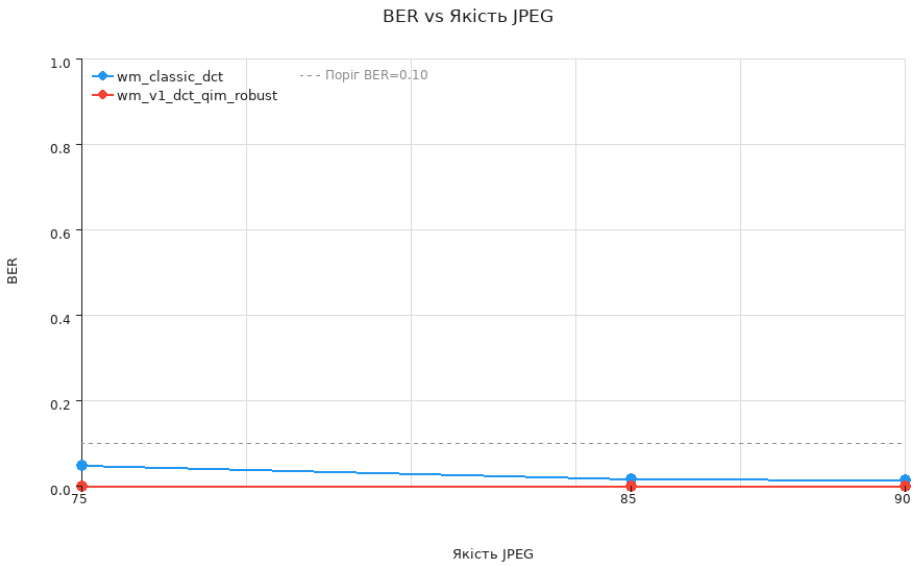


Рисунок 2.8 – Залежність BER методів wm_classic_dct та wm_v2_dct_qim_profile від фактора якості JPEG.

(Джерело: складено автором)

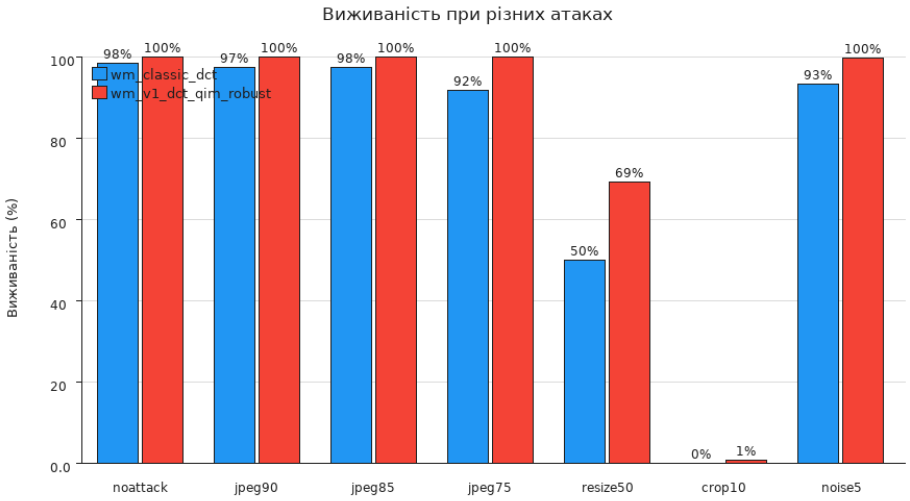


Рисунок 2.9 – Частка зображень зі збереженим маркером за атаками – wm_classic_dct та wm_v2_dct_qim_profile

(Джерело: складено автором)

Висновок. Запропоноване поєднання QIM з компенсацією спотворень (distortion-compensated QIM, DC-QIM [170]) з адаптивним вибором DCT-позицій за критерієм $\Delta > q$ та надлишкового кодування repeat = 7 забезпечує повну стійкість до JPEG-стиснення за Q = 90 і 85 та майже повну (92,1%) за найжорсткішого Q = 75, підвищує стійкість до масштабування (+17,6 в.п., з 50,1% до 67,7%) і шуму (+6,5 в.п.) за рівної непомітності. Результат підтверджено теоретично (Твердження 2.3) та експериментально на вибірці з 567 зображень. Решітковий декодер забезпечує сліпе витягування без знання оригіналу. Водночас метод зберігає чутливість до геометричних атак (обрізання), що визначає межу застосовності частотно-блокового підходу.

2.4. Методи вбудовування в модифікованому дискретному косинусному перетворенні (MDCT) для аудіосигналів

Розглянуті вище методи часової області руйнуються за частотно-вибіркових атак, а частотні методи для зображень не враховують специфіку слухового сприйняття. Для аудіосигналів природним є вбудовування у модифікованому дискретному косинусному перетворенні (MDCT) [174] – тому самому базисі, у якому працюють психоакустичні аудіокодеки, зокрема MP3.

Вбудовування у спектральні смуги MDCT-кадру дозволяє узгодити маркер із частотним розподілом енергії сигналу [41]. У цьому підрозділі розглянуто основний запропонований метод на основі диференціального енергетичного контрасту смуг (audio_mdct_qim_v2) та проаналізовано альтернативну архітектуру двостороннього перерозподілу енергії (audio_mdct_qim_v3).

2.4.1. Метод диференціального енергетичного контрасту смуг (audio_mdct_qim_v2)

Структурну схему методу audio_mdct_qim_v2 наведено на рис. 2.10.

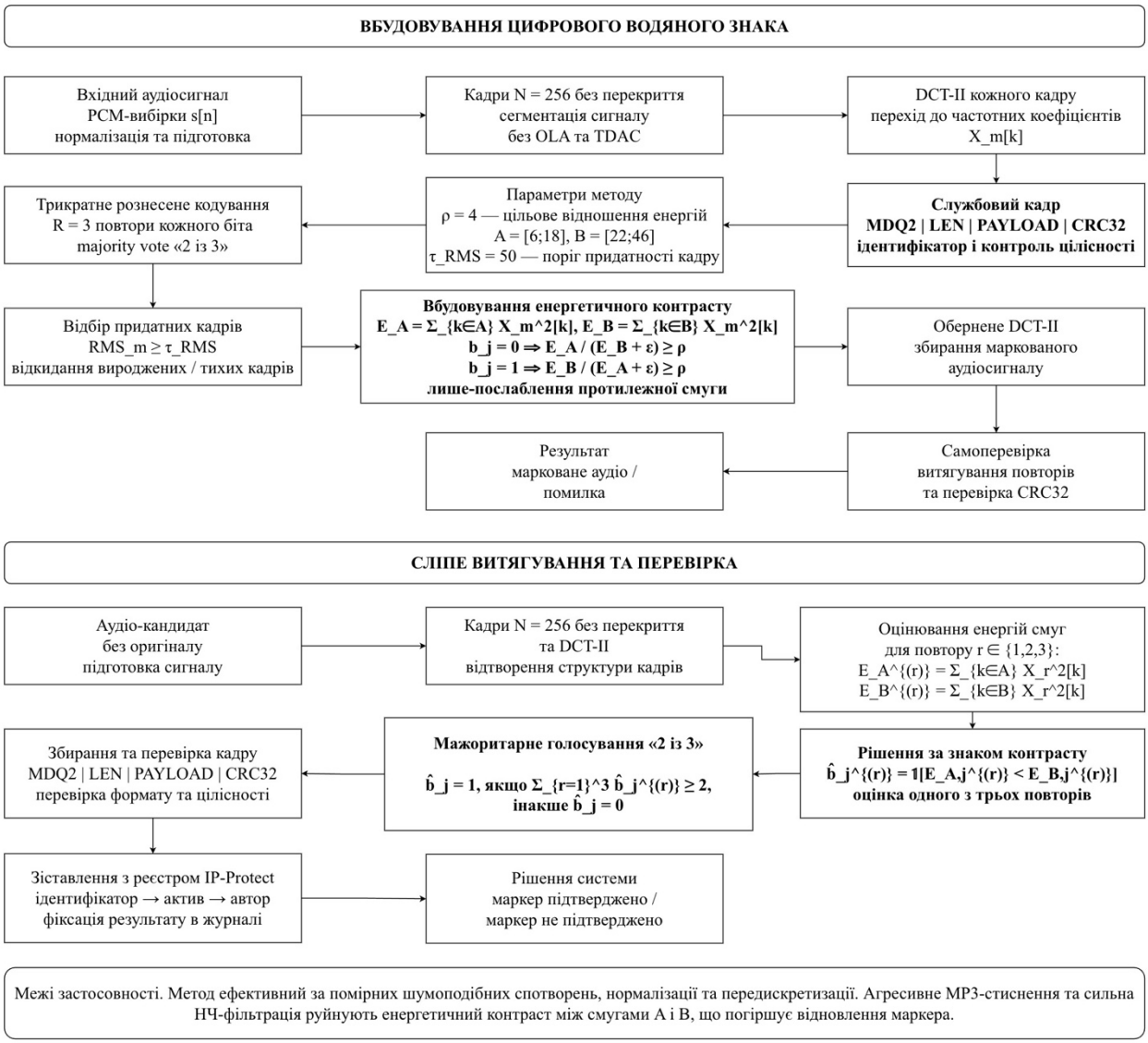


Рисунок 2.10 – Структурна схема методу audio_mdct_qim_v2 (диференціальний енергетичний контраст смуг MDCT)

(Джерело: складено автором)

Наявний метод та його модель. Класичний MDCT-метод кодує біт через співвідношення сумарних енергій двох спектральних смуг MDCT-кадру – BAND_A та BAND_B. Позначимо E_A та E_B енергії смуг. Вбудовування виконується послабленням програшної смуги до значення, що забезпечує задане домінування переможної смуги за коефіцієнтом TARGET_RATIO r:

$$E_{\text{програшна}} \rightarrow E_{\text{переможна}} / r, \quad \text{рішення: } \hat{b} = \mathbb{1}[\, E_A < E_B \,], \tag{2.10}$$

тобто біт визначається знаком різниці енергій смуг. Перевагою є узгодженість із частотним розподілом сигналу; проте у класичному вигляді біт кодується одноразово, без надлишковості, а послаблення однієї смуги неминуче знижує енергію кадру.

Недоліки. Класичний метод має два ключові обмеження. По-перше, одноразове кодування біта без надлишковості робить рішення чутливим до будь-якого спотворення, що змінює знак різниці $E_A - E_B$: стиснення з втратами MP3, яке саме й перерозподіляє енергію між смугами MDCT, безпосередньо атакує механізм рішення. По-друге, у кадрах із дуже малою енергією смуг послаблення стає виродженим і не створює надійного контрасту. Експериментально класичний метод відновлює маркер лише для 35,3% файлів за MP3 128 kbps та 8,0% за MP3 64 kbps (табл. 2.4).

Запропонований модифікований метод. Пропонується доповнити диференціальне енергетичне кодування двома складниками: (i) надлишковим кодуванням кожного біта у repeat = 3 кадрах із голосуванням більшістю [189]; (ii) виключенням вироджених кадрів за абсолютним порогом енергії смуги, узгодженим між вбудовуванням та витяганням. У методі audio_mdct_qim_v2 реалізовано односпрямоване послаблення (attenuation-only) програшної смуги до $E_{\text{переможна}} / r$ з r = 4, що зберігає енергію переможної смуги незмінною і мінімізує спотворення. Гіпотеза полягає в тому, що поєднання енергетичного контрасту, надлишкового кодування та відсіювання вироджених кадрів підвищує стійкість до стиснення з втратами без активного перерозподілу енергії.

Твердження 2.5. Нехай біт закодовано диференціальним енергетичним контрастом із коефіцієнтом r (програшна смуга послаблена до $E_{\text{переможна}}$ / r), а канал вносить у смуги адитивне спотворення енергії. Тоді біт відновлюється коректно тоді і тільки тоді, коли після проходження каналом зберігається знак різниці енергій, тобто коли внесене спотворення не перевищує вбудованого контрасту:

$$|\Delta E| < (r - 1)\cdot\min(E_A, E_B). \qquad (2.11)$$

Доказ. Після вбудовування різниця енергій дорівнює за модулем $(r - 1)\cdot E_{\text{переможна}}$ / r, тобто переможна смуга домінує з запасом, пропорційним (r − 1). Рішення $\hat{b} = \mathbb{1}[E_A < E_B]$ ухвалюється за знаком різниці. Помилка виникає лише тоді, коли спотворення каналу ΔE змінює цей знак, що потребує $|\Delta E| \geq (r - 1)\cdot\min(E_A, E_B)$. Отже, за умови (2.11) знак зберігається і біт відновлюється коректно. Збільшення r підвищує стійкість, але пропорційно знижує енергію кадру, що визначає компроміс між стійкістю та непомітністю. Додатково надлишкове кодування repeat = 3 знижує залишкову ймовірність помилки згідно з Твердженням 2.1 (для n = 3: $P_3 = 3p^2(1-p) + p^3$).

Експериментальна перевірка. Порівняння класичного методу audio_classic_mdct та удосконаленого audio_mdct_qim_v2 (r = 4, repeat = 3) виконано на наборі зі 150 аудіофайлів. Середній SNR становить 38,9 дБ для класичного та 32,5 дБ для удосконаленого методу; різниця 6,4 дБ є структурною властивістю методу (послаблення смуги неминуче знижує енергію кадру), проте обидва значення лишаються значно вище порога чутності слухового сприйняття. Прикметно, що удосконалений метод стабільно переважає класичний навіть за дещо нижчої власної непомітності. За відсутності атаки обидва методи відновлюють маркер практично безпомилково (виживання 96,0% та 99,3%). На основному векторі атаки – MP3-перекодуванні – удосконалений метод підвищує виживання з 35,3% до 53,3% за 128 kbps (коефіцієнт 1,51×), з 24,7% до 42,7% за 96 kbps (1,73×) та з 8,0% до 29,3% за 64 kbps (3,67×). Стійкість зростає також за нормалізації (80,7% → 91,3%) та передискретизації ×4 (78,7% → 91,3%). Отже,

поєднання енергетичного контрасту з надлишковим кодуванням забезпечує стабільне підвищення стійкості за основним вектором атаки. Динаміку BER за силою MP3-стиснення наведено на рис. 2.11, розподіл виживання за атаками – на рис. 2.12.

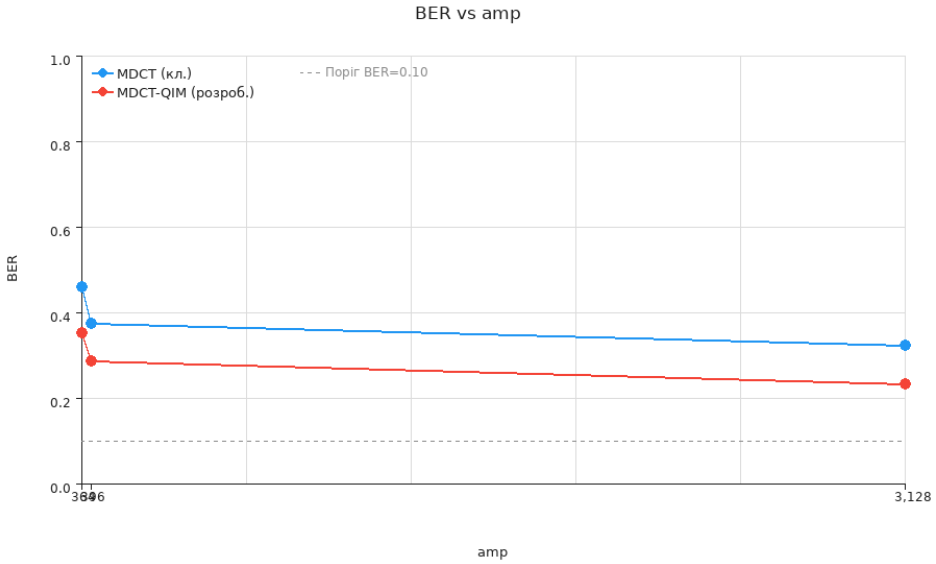


Рисунок 2.11 – Залежність BER методів audio_classic_mdct та audio_mdct_qim_v2 від сили MP3-стиснення

(Джерело: складено автором)

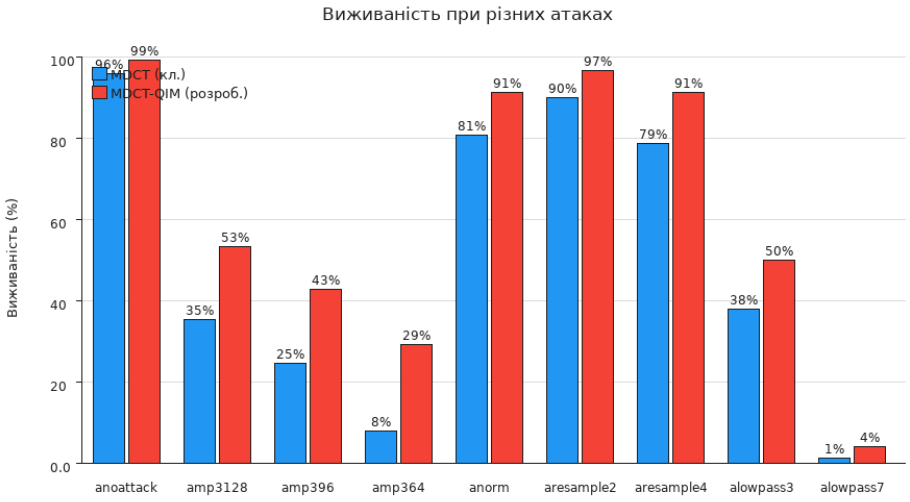


Рисунок 2.12 – Частка файлів зі збереженим маркером за атаками – audio_classic_mdct та audio_mdct_qim_v2

(Джерело: складено автором)

Місце методу серед інших підходів. Слід зазначити, що MDCT-метод у цілому поступається за абсолютною стійкістю коефіцієнтним методам попередніх підрозділів: навіть удосконалений метод відновлює лише 29–53% файлів за MP3 проти 75–81% у методу audio_qim_v1. Це пояснюється тим, що стиснення з втратами MP3 працює саме у MDCT-базисі й безпосередньо перерозподіляє енергію смуг, на якій ґрунтується рішення. Тому ніша MDCT-методу – не максимальна стійкість до стиснення, а узгодженість маркера з психоакустичним розподілом енергії та стійкість до нормалізації й передискретизації. У межах свого класу вдосконалення забезпечує стабільний виграш відносно класичного методу, що й було метою даного підрозділу.

2.4.2. Аналіз альтернативної архітектури двостороннього QIM (audio_mdct_qim_v3)

Аналіз альтернативної архітектури. Досліджено також альтернативну архітектуру двостороннього QIM з активним перерозподілом енергії між смугами (метод audio_mdct_qim_v3): замість односпрямованого послаблення обидві смуги масштабуються до заданого розподілу splitHigh за допомогою перекривних кадрів (OLA). Аналіз виявив фундаментальний архітектурний компроміс. Стійкість двостороннього перерозподілу до OLA-інтерференції потребує високої амплітуди перерозподілу (параметр strength), проте на кадрах із вираженою частотною асиметрією – характерних для музичного контенту – активне підсилення слабкої смуги (масштабний коефіцієнт може перевищувати 2) призводить до неприпустимого зниження непомітності: середній SNR становить лише 8,7 дБ. Експеримент на 150 файлах підтвердив, що за таких умов метод не лише не переважає односпрямовану схему, а й поступається класичному методу за основним вектором атаки (виживання 16,0% проти 35,3% за MP3 128 kbps), зберігаючи перевагу тільки за низькочастотної фільтрації. Отже, двосторонній перерозподіл енергії є архітектурно суперечливим для аудіоконтенту зі специфічним частотним профілем: вимога стійкості та вимога непомітності перебувають у прямому конфлікті. Цей результат обґрунтовує

вибір односпрямованої атенюації (audio_mdct_qim_v2) як основного MDCT-методу системи.

Висновок. Запропоноване поєднання диференціального енергетичного контрасту, надлишкового кодування repeat = 3 та відсіювання вироджених кадрів підвищує стійкість MDCT-методу у 1,5–3,7 рази за основним вектором атаки (MP3-перекодування) відносно класичного методу, що підтверджено теоретично (Твердження 2.5) та експериментально на вибірці зі 150 файлів. Аналіз альтернативної двосторонньої архітектури (audio_mdct_qim_v3) показав її принципову несумісність із вимогою непомітності для музичного контенту, що обґрунтовує вибір односпрямованої схеми. Водночас MDCT-підхід за абсолютною стійкістю до стиснення поступається коефіцієнтним методам, оскільки методи стиснення з втратами працюють у тому самому базисі; його нішею є узгодженість із психоакустичним розподілом енергії та стійкість до амплітудних і ресемплінгових перетворень.

Таблиця 2.4 – Порівняння стійкості методів audio_classic_mdct та audio_mdct_qim_v2 (150 файлів, seed = 12345, критерій BER ≤ 0,10)

Атака	BER клас.	BER розроб.	SNR клас., дБ	SNR розроб., дБ	Вижив. клас.	Вижив. розроб.	Коеф. покращ.
Без атаки (еталон)	0,020	0,003	38,9	32,5	96,0%	99,3%	–
MP3 128 kbps	0,323	0,233	38,9	32,5	35,3%	53,3%	1,51×
MP3 96 kbps	0,377	0,287	38,9	32,5	24,7%	42,7%	1,73×
MP3 64 kbps	0,460	0,353	38,9	32,5	8,0%	29,3%	3,67×
Нормалізація гучності	0,097	0,043	38,9	32,5	80,7%	91,3%	1,13×
Передискретизація ×2	0,050	0,017	38,9	32,5	90,0%	96,7%	1,07×
Передискретизація ×4	0,107	0,043	38,9	32,5	78,7%	91,3%	1,16×
Низькочаст. фільтр. w=3	0,310	0,250	38,9	32,5	38,0%	50,0%	1,32×
Низькочаст. фільтр. w=7	0,493	0,480	38,9	32,5	1,3%	4,0%	межа[4]

[4] За сильної низькочастотної фільтрації обидва методи майже повністю руйнуються; режим відповідає межі застосовності часової та MDCT-областей (див. текст).

Джерело: складено автором

2.5. Метод розширеного спектра (Spread Spectrum / DSSS)

Розглянуті методи вбудовують маркер у локалізовані елементи сигналу – окремі вибірки, групи або спектральні смуги, – що робить їх вразливими до атак, які цілеспрямовано спотворюють відповідну область. Принципово інший підхід реалізує метод розширеного спектра (Direct-Sequence Spread Spectrum, DSSS): кожний біт кодується не в одному, а у великій кількості елементів сигналу через множення на псевдовипадкову послідовність (ПВП), унаслідок чого енергія маркера рівномірно розподіляється по всьому спектру [169, 172]. Атака, що спотворює обмежену частину спектра, руйнує лише відповідну частку кодувальної послідовності, тоді як кореляційний декодер відновлює біт за рештою. Структурну схему методу audio_spread_spectrum_v2 наведено на рис. 2.13.

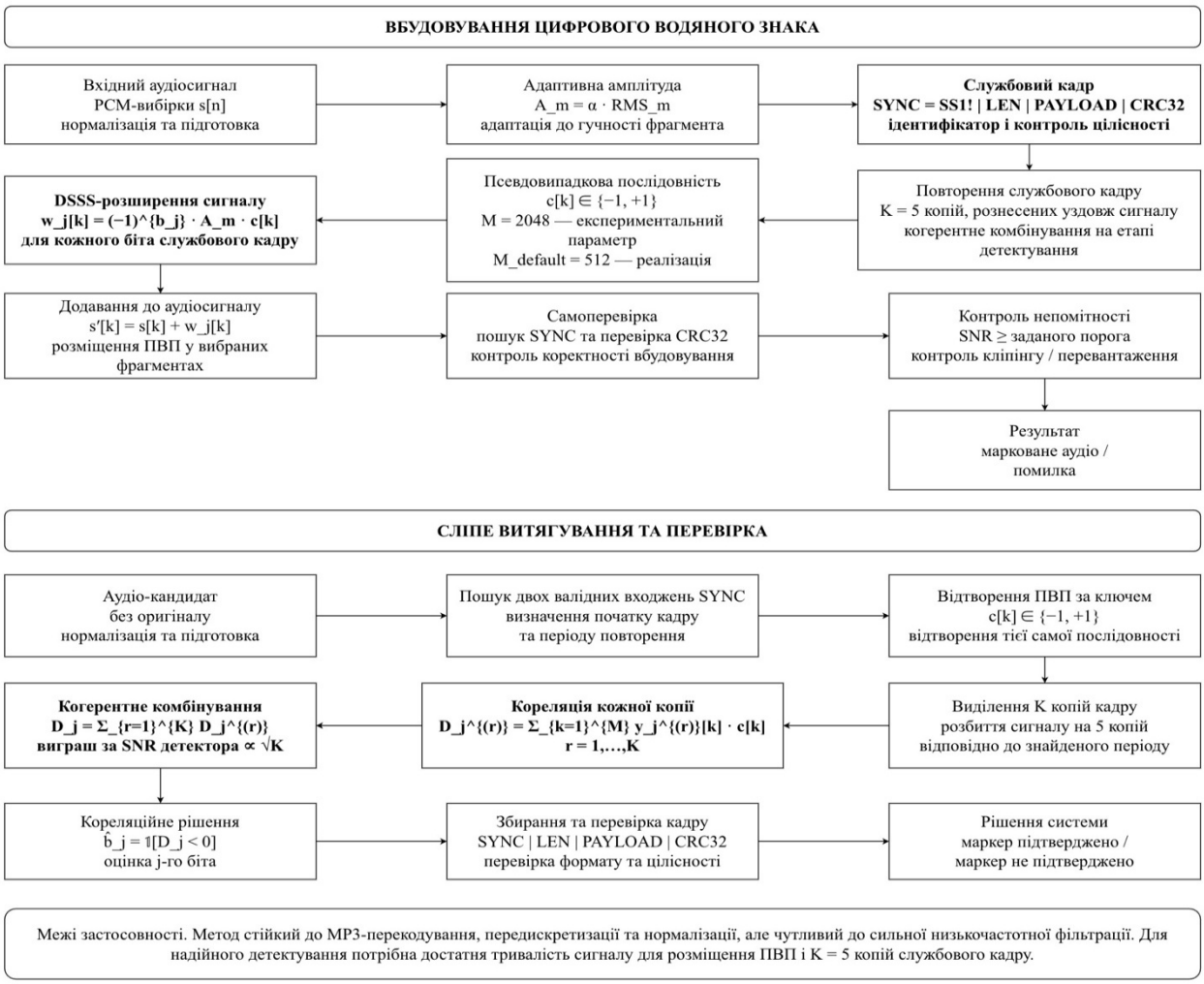


Рисунок 2.13 – Структурна схема методу audio_spread_spectrum_v2 (DSSS з кореляційним декодером та когерентним комбінуванням)

(Джерело: складено автором)

Наявний метод та його модель. Класичний DSSS-метод кодує біт $b \in \{0,1\}$ множенням на ПВП $c \in \{-1, +1\}$ довжини M (число чипів на біт) із фіксованою амплітудою A. Позначимо s вихідний сигнал. Вбудовування:

$$s'_k = s_k + (-1)^b \cdot A \cdot c_k, \tag{2.12}$$

а витягування – за знаком кореляції прийнятого сигналу з тією самою ПВП:

$$\hat{b} = \mathbb{1}[\ \Sigma_k\, s'_k \cdot c_k < 0\ ]. \tag{2.13}$$

Розподіл енергії маркера по всьому спектру забезпечує стійкість до вузькосмугових спотворень. Проте у класичному вигляді метод використовує фіксовану амплітуду A, що не враховує гучності сигналу, та одноразове кодування без когерентного накопичення повторів.

Недоліки. Фіксована амплітуда A є основним обмеженням: шумовий член кореляції зростає пропорційно середньоквадратичному рівню сигналу (RMS), тому для гучних записів корисна кореляція $A \cdot M$ виявляється меншою за шумову складову, і синхронізацію не вдається встановити. Експериментально класичний метод відновлює маркер лише для 28,0% файлів за MP3 64 kbps та 26,7% за передискретизації ×4 (табл. 2.5), причому відмови припадають переважно на записи з високим RMS. Крім того, відсутність когерентного накопичення повторів обмежує досяжний коефіцієнт підсилення.

Удосконалений метод. Пропонується доповнити DSSS двома складниками: (i) адаптивною амплітудою вбудовування $A = \alpha \cdot \mathrm{RMS}$, узгодженою з гучністю кожного фрагмента, що забезпечує сталий рівень кореляції незалежно від сигналу; (ii) когерентним комбінуванням повторів – службова структура кадру повторюється по всьому сигналу, а декодер визначає період повторення за двома входженнями синхромаркера й когерентно підсумовує кореляції всіх копій. У методі audio_spread_spectrum_v2 застосовано $M = 2048$ чипів на біт (параметр експерименту; за замовчуванням у реалізації $M = 512$), $\alpha = 0{,}032$ та repetition = 5. Гіпотеза полягає в тому, що поєднання розстилки спектра з

когерентним накопиченням забезпечує кратне підвищення стійкості до стиснення з втратами за збереження непомітності.

Твердження 2.6. Нехай біт закодовано ПВП довжини M з амплітудою A = α·RMS, а на приймальному боці когерентно підсумовуються K копій кадру. Тоді відношення сигнал/шум статистики рішення $D = \Sigma\, s' \cdot c$ зростає як добуток двох незалежних множників – розстилки спектра та когерентного накопичення:

$$SNR_D = \alpha \cdot \sqrt{(M \cdot K)} / \sigma_n, \qquad (2.14)$$

де σ_n – нормований рівень завад. Отже, стійкість зростає пропорційно $\sqrt{M}$ за рахунок розстилки та додатково пропорційно $\sqrt{K}$ за рахунок когерентного комбінування. Для M = 2048 множник розстилки становить $\sqrt{2048} \approx 45{,}3$, що і забезпечує кратний виграш над вузьколокалізованими методами.

Доказ. Кореляція $D = \Sigma_k\, s'_k \cdot c_k$ містить корисну складову, у якій M доданків додаються когерентно (кожний член $A \cdot c_k^2 = A$), тому $|E[D]| = A \cdot M \propto M$. Завадова складова $\Sigma\, n_k \cdot c_k$ є сумою M некорельованих доданків, тому її дисперсія зростає як M, а стандартне відхилення – як $\sqrt{M}$. Відношення сподівання до відхилення дорівнює $A \cdot M / (\sigma_n \cdot \sqrt{M}) = A \cdot \sqrt{M} / \sigma_n$. Когерентне підсумовування K незалежних копій кадру аналогічно додає множник $\sqrt{K}$. Підставляючи A = α·RMS та нормуючи, дістаємо (2.14).

Експериментальна перевірка. Порівняння класичного методу audio_classic_ss та удосконаленого audio_spread_spectrum_v2 виконано на наборі зі 150 аудіофайлів. За відсутності атаки обидва методи відновлюють маркер практично безпомилково (виживання 98,7% та 100%). На основному векторі атаки – MP3-перекодуванні – удосконалений метод забезпечує кратне підвищення стійкості: за MP3 128 kbps виживання зростає з 79,3% до 98,7%, за MP3 96 kbps – з 53,3% до 94,7% (коефіцієнт 1,78×), за MP3 64 kbps – з 28,0% до 81,3% (2,90×). Аналогічний виграш спостерігається за передискретизації ×4 (26,7% → 80,7%; 3,03×). Обидва методи забезпечують непомітність вище порога чутності: SNR становить 27,9 дБ для удосконаленого та 39,2 дБ для класичного методу. Удосконалений метод вбудовує маркер із дещо вищою енергією, що

лишається непомітною на слух, і завдяки розстилці спектра та когерентному комбінуванню (Твердження 2.6) досягає кратно вищої стійкості до атак. Динаміку BER за силою MP3-стиснення наведено на рис. 2.14, розподіл виживання за атаками – на рис. 2.15.

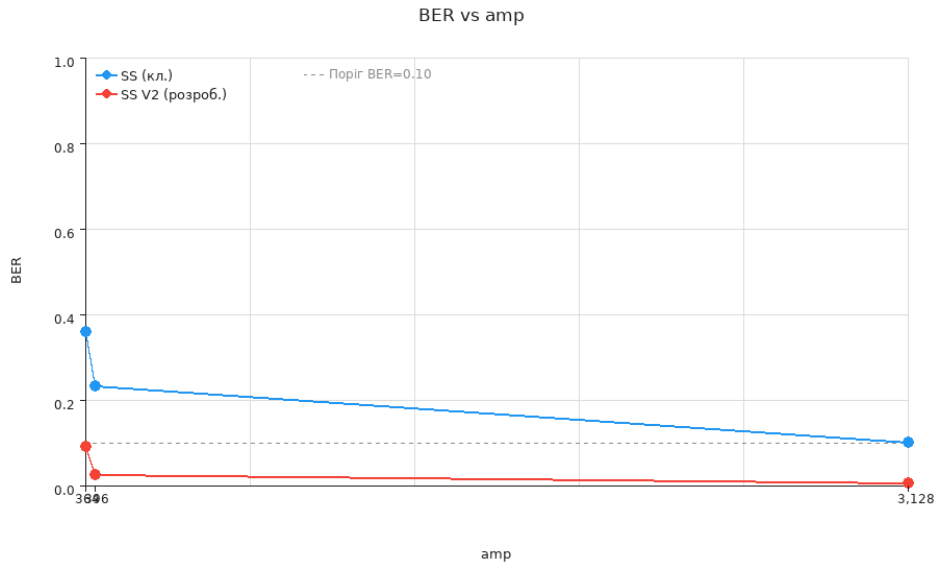


Рисунок 2.14 – Залежність BER методів audio_classic_ss та audio_spread_spectrum_v2 від сили MP3-стиснення

(Джерело: складено автором)

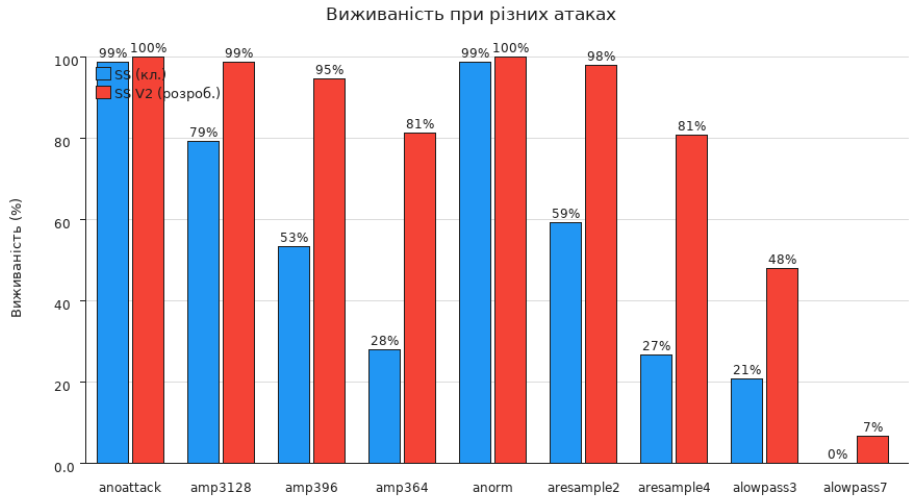


Рисунок 2.15 – Частка файлів зі збереженим маркером за атаками – audio_classic_ss та audio_spread_spectrum_v2

(Джерело: складено автором)

Межа застосовності. Метод зберігає спільну для всіх методів часової та частотної областей чутливість до сильної низькочастотної фільтрації: за фільтрації w = 7 виживання становить 6,7% проти 0% у класичного методу. Крім того, велика довжина ПВП вимагає мінімальної тривалості сигналу – надто короткі фрагменти не вміщують достатньої кількості чипів для надійної синхронізації і виключаються з обробки. Ці обмеження визначають межу застосовності методу, проте у межах основного сценарію (стиснення, передискретизація, нормалізація) DSSS забезпечує найвищу серед розглянутих аудіометодів стійкість.

Висновок. Запропоноване поєднання адаптивної амплітуди, розстилки спектра та когерентного комбінування повторів підвищує стійкість DSSS-методу у 1,8–3,0 рази за основним вектором атаки (MP3-перекодування, передискретизація) відносно класичного методу, що підтверджено теоретично (Твердження 2.6) та експериментально на вибірці зі 150 файлів. На відміну від вузьколокалізованих методів, розподіл енергії маркера по всьому спектру забезпечує найвищу стійкість до стиснення з втратами серед розглянутих аудіопідходів. Метод зберігає чутливість лише до низькочастотної фільтрації, що визначає межу його застосовності.

Таблиця 2.5 – Порівняння стійкості методів audio_classic_ss та audio_spread_spectrum_v2 (150 файлів, M = 2048, α = 0,032, критерій BER ≤ 0,10)

Атака	BER клас.	BER розроб.	SNR клас., дБ	SNR розроб., дБ	Вижив. клас.	Вижив. розроб.	Коеф. покращ.
Без атаки (еталон)	0,007	0,000	39,2	27,9	98,7%	100%	–
MP3 128 kbps	0,103	0,007	39,2	27,9	79,3%	98,7%	1,24×
MP3 96 kbps	0,233	0,027	39,2	27,9	53,3%	94,7%	1,78×
MP3 64 kbps	0,360	0,093	39,2	27,9	28,0%	81,3%	2,90×
Нормалізація гучності	0,007	0,000	39,2	27,9	98,7%	100%	1,01×
Передискретизація ×2	0,203	0,010	39,2	27,9	59,3%	98,0%	1,65×
Передискретизація ×4	0,367	0,097	39,2	27,9	26,7%	80,7%	3,03×
Низькочаст. фільтр. w=3	0,397	0,260	39,2	27,9	20,7%	48,0%	2,32×
Низькочаст. фільтр. w=7	0,500	0,467	39,2	27,9	0%	6,7%	межа[5]

[5] За сильної низькочастотної фільтрації обидва методи майже повністю руйнуються; режим відповідає межі застосовності методу (див. текст).

Джерело: складено автором

2.6. Метод прихованого exo (Echo Hiding)

Метод прихованого exo [198] кодує інформацію через додавання до сигналу затриманих копій (exo), параметри яких визначають вбудований біт. На відміну від розглянутих методів, тут маркер вбудовується у часову структуру сигналу і сприймається слухом як природна реверберація. Структурну схему методу audio_echo_hiding_v2 наведено на рис. 2.16.

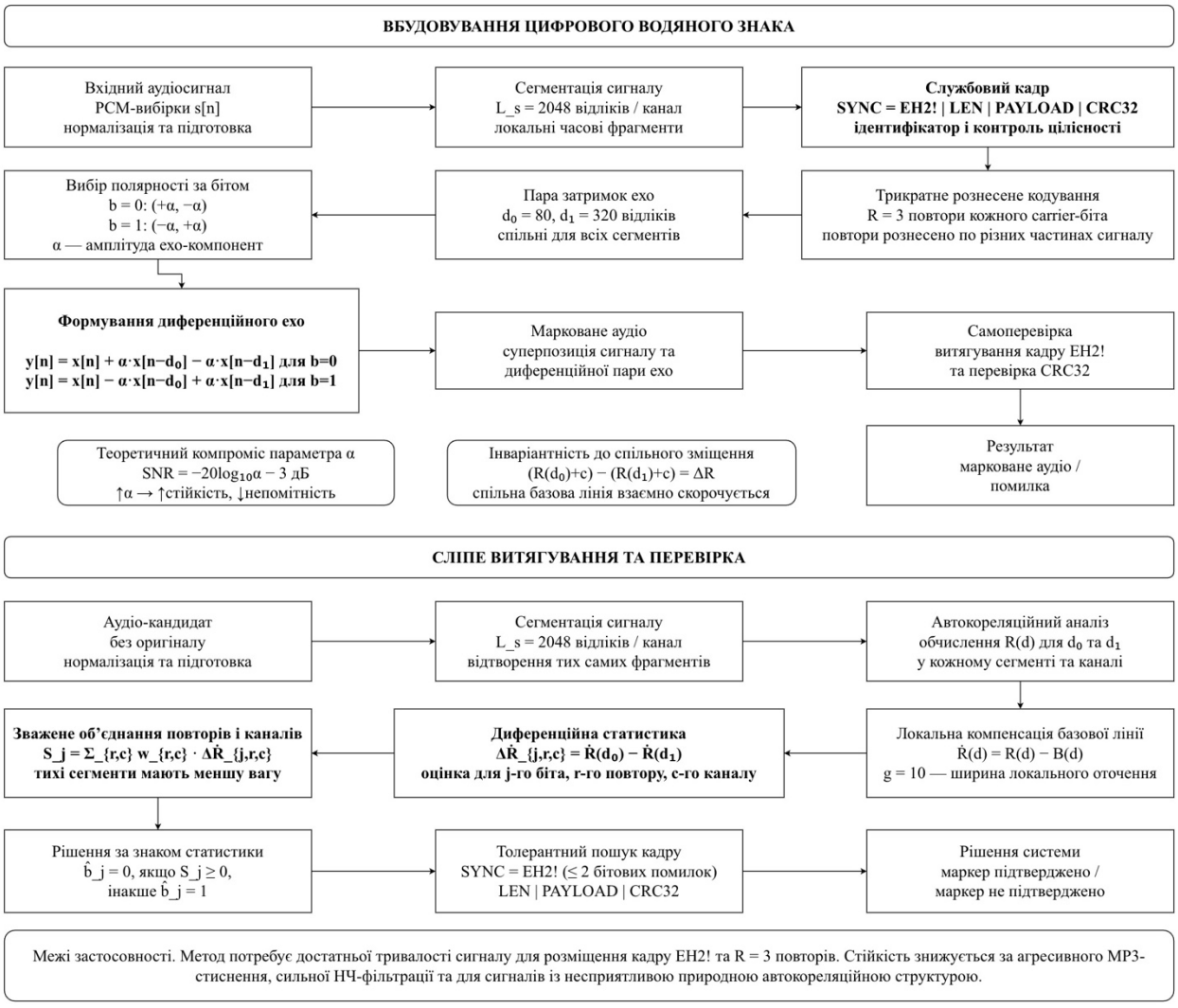


Рисунок 2.16 – Структурна схема методу audio_echo_hiding_v2 (диференційне exo-приховування з полярністю пари затримок)

(Джерело: складено автором)

Наявний метод та його модель. Класичний метод прихованого exo додає одну затриману копію сигналу з амплітудою α та затримкою, що залежить від біта (d0 для біта 0, d1 для біта 1). Витягування виконується пошуком піка

автокореляційної функції (або кепстра) на відповідній затримці. Основна перевага – узгодженість зі слуховим сприйняттям; проте рішення ґрунтується на абсолютному значенні одного піка, що робить його чутливим до сталого зміщення автокореляції, яке вносять атаки.

Недоліки. Класичний метод має два обмеження. По-перше, рішення за абсолютним піком автокореляції потребує узгодження порогу з рівнем сигналу; будь-яке зміщення базової лінії автокореляції (внаслідок стиснення чи фільтрації) спотворює рішення. По-друге, одиночне ехо створює слабкий і нестабільний пік, унаслідок чого метод сильно залежить від змісту сигналу. Експериментально класичний метод відновлює маркер лише для 20% файлів навіть без атаки (табл. 2.6).

Удосконалений метод. Пропонується перейти від одиночного ехо до диференційної пари ехо з протилежними полярностями. Для біта 0 перше ехо (затримка d0) підсилюється, а друге (d1) пригнічується; для біта 1 – навпаки:

$$y[n] = x[n] \pm \alpha \cdot x[n - d_0] \mp \alpha \cdot x[n - d_1], \qquad (2.15)$$

а витягування виконується порівнянням піків автокореляції у точках d_0 та d_1: біт визначається знаком різниці $\Delta R = R(d_0) - R(d_1)$. Гіпотеза полягає в тому, що рішення за різницею піків, а не за абсолютним значенням, є інваріантним до сталого зміщення автокореляції й тому стійкішим за одиночне ехо.

Твердження 2.7. Нехай біт закодовано диференційною парою ехо з амплітудою α, а декодер обчислює різницю автокореляційних піків $\Delta R = R(d_0) - R(d_1)$. Тоді: (а) рішення за знаком ΔR інваріантне до сталого адитивного зміщення обох піків, оскільки зміщення скорочується при відніманні; (б) непомітність і стійкість перебувають у прямому конфлікті через єдиний параметр α, а саме

$$\mathrm{SNR} = -20 \cdot \log_{10} \alpha - 3 \text{ дБ}, \qquad (2.16)$$

де доданок −3 дБ враховує енергію двох ехо-тапів ($2\alpha^2 \cdot E_x$). Оскільки стійкість зростає з α (пік $\Delta R \propto \alpha \cdot E_x$), а непомітність спадає з α, добуток стійкості та непомітності обмежений зверху – це фундаментальний компроміс амплітуди методу.

Доказ. (а) Нехай атака вносить стале зміщення c у обидва піки: $R'(d_0) = R(d_0) + c$, $R'(d_1) = R(d_1) + c$. Тоді $\Delta R' = R'(d_0) - R'(d_1) = R(d_0) - R(d_1) = \Delta R$, тобто знак рішення зберігається. (б) Диференційна пара створює піки $+\alpha \cdot E_x$ та $-\alpha \cdot E_x$, звідки $|\Delta R| = 2\alpha \cdot E_x \propto \alpha$ – стійкість лінійно зростає з α. Водночас енергія внесеного спотворення дорівнює $2\alpha^2 \cdot E_x$, звідки $SNR = 10 \cdot \log_{10}(E_x / 2\alpha^2 \cdot E_x) = -20 \cdot \log_{10} \alpha - 3$ дБ, тобто непомітність спадає з α. Отже, збільшення α не може одночасно підвищити стійкість і непомітність.

Експериментальна перевірка. Порівняння класичного методу audio_classic_echo та удосконаленого audio_echo_hiding_v2 (α = 0,1) виконано на наборі зі 150 аудіофайлів. Удосконалений метод забезпечує суттєво вищу непомітність: SNR становить 17,6 дБ проти 8,4 дБ у класичного (різниця 9,2 дБ), що узгоджується з формулою (2.16). За відсутності атаки удосконалений метод відновлює маркер для 73,3% файлів проти 20,0% класичного (коефіцієнт 3,67×). За помірних атак перевага зберігається: MP3 128 kbps – 64,0% проти 20,0% (3,20×), MP3 96 kbps – 49,3% проти 19,3% (2,55×), передискретизація ×2 – 57,3% проти 18,0% (3,19×), низькочастотна фільтрація w = 3 – 57,3% проти 14,7% (3,91×). Отже, за легких і середніх атак диференційна схема стабільно переважає класичну у 2,1–3,9 раза за одночасно кращої непомітності. Динаміку BER за силою MP3-стиснення наведено на рис. 2.17, розподіл виживання за атаками – на рис. 2.18.

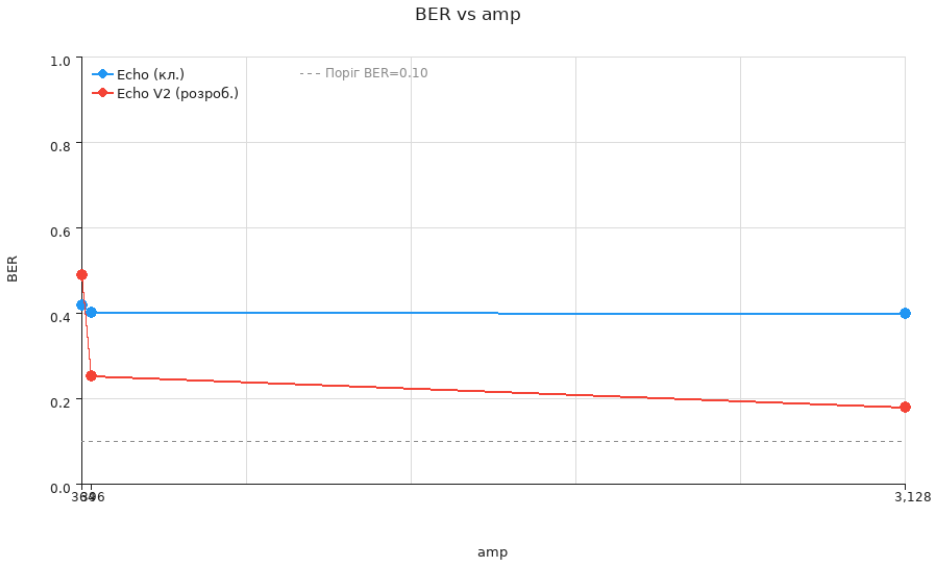


Рисунок 2.17 – Залежність BER методів audio_classic_echo та audio_echo_hiding_v2 від сили MP3-стиснення

(Джерело: складено автором)

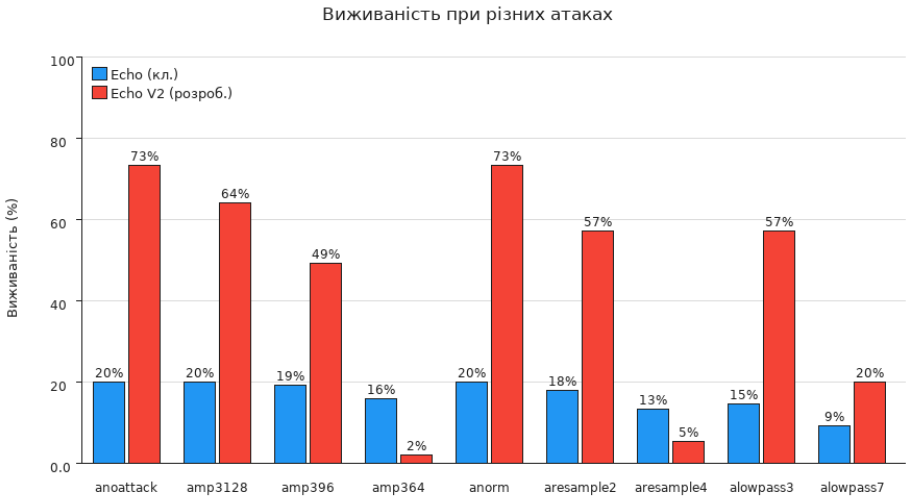


Рисунок 2.18 – Частка файлів зі збереженим маркером за атаками – audio_classic_echo та audio_echo_hiding_v2

(Джерело: складено автором)

Межа застосовності. Метод має два суттєві обмеження. По-перше, за агресивного стиснення (MP3 64 kbps) та сильної передискретизації (×4) обидва методи руйнуються (виживання удосконаленого 2,0% та 5,3%), оскільки квантування знищує автокореляційні піки на затримках d0 і d1; це спільна межа

диференційного ехо-приховування як класу, а не специфічна вада вдосконалення. По-друге, метод суттєво залежить від змісту сигналу: навіть без атаки 26,7% файлів не зберігають маркер, оскільки автокореляційна структура окремих музичних фрагментів не забезпечує надійного розділення піків. Через це результати мають ширший розкид, ніж у методів розстилки спектра. Ці обмеження визначають нішу методу як обмежену: він придатний переважно для сценаріїв із помірними спотвореннями та контентом зі стабільною автокореляційною структурою.

Висновок. Запропонована диференційна пара ехо з рішенням за різницею автокореляційних піків забезпечує інваріантність до сталого зміщення (Твердження 2.7) і підвищує стійкість методу прихованого ехо у 2,1–3,9 рази за легких і середніх атак відносно класичного методу, до того ж за одночасно вищої на 9,2 дБ непомітності. Результат підтверджено теоретично та експериментально на вибірці зі 150 файлів. Водночас метод обмежений фундаментальним компромісом амплітуди та чутливістю до змісту сигналу, а за агресивного стиснення руйнується разом із класичним методом, що визначає його нішу як допоміжну порівняно з методами розстилки спектра.

Таблиця 2.6 – Порівняння стійкості методів audio_classic_echo та audio_echo_hiding_v2 (150 файлів, $\alpha = 0{,}1$, критерій BER $\leq 0{,}10$)

Атака	BER клас.	BER розроб.	SNR клас., дБ	SNR розроб., дБ	Вижив. клас.	Вижив. розроб.	Коеф. покращ.
Без атаки (еталон)	0,400	0,133	8,4	17,6	20,0%	73,3%	3,67×
MP3 128 kbps	0,400	0,180	8,4	17,6	20,0%	64,0%	3,20×
MP3 96 kbps	0,403	0,253	8,4	17,6	19,3%	49,3%	2,55×
MP3 64 kbps	0,420	0,490	8,4	17,6	16,0%	2,0%	межа[6]
Нормалізація гучності	0,400	0,133	8,4	17,6	20,0%	73,3%	3,67×
Передискретизація ×2	0,410	0,213	8,4	17,6	18,0%	57,3%	3,19×
Передискретизація ×4	0,433	0,473	8,4	17,6	13,3%	5,3%	межа[6]
Низькочаст. фільтр. w=3	0,427	0,213	8,4	17,6	14,7%	57,3%	3,91×
Низькочаст. фільтр. w=7	0,453	0,400	8,4	17,6	9,3%	20,0%	2,14×

[6] За агресивного стиснення (MP3 64 kbps) та сильної передискретизації обидва методи руйнуються; режим відповідає спільній межі застосовності диференційного ехо-приховування (див. текст).

Джерело: складено автором

2.7. Метод вбудовування через енергію підсмуг (Subband Energy)

Метод енергії підсмуг кодує біт через співвідношення енергій двох частотних підсмуг після DCT-перетворення часового фрейму. На відміну від методів, що модифікують окремі коефіцієнти, тут рішення ґрунтується на інтегральній енергії смуги, що робить його стійкішим до локальних спотворень. Структурну схему методу audio_subband_energy_v3 наведено на рис. 2.19.

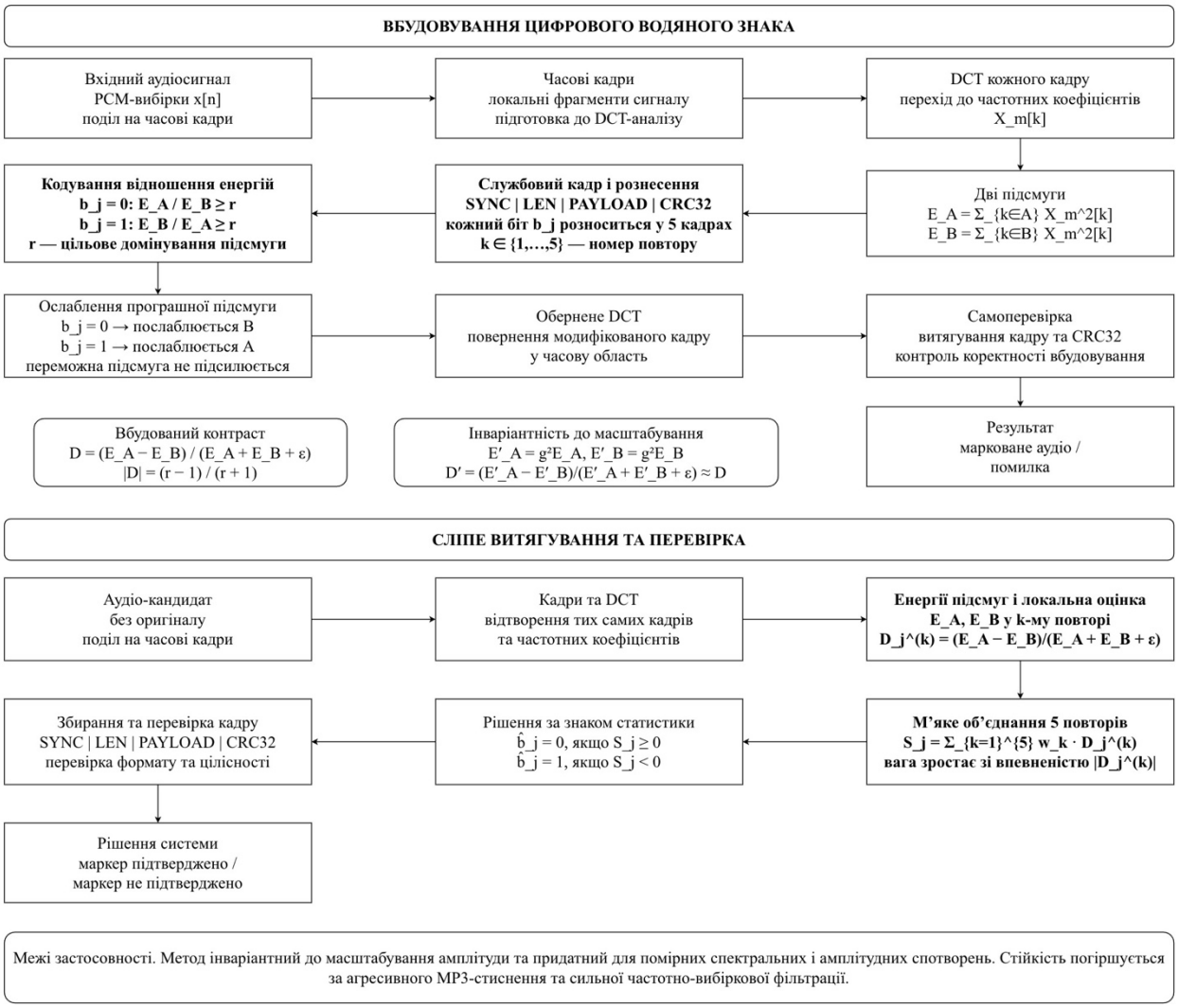


Рисунок 2.19 – Структурна схема методу audio_subband_energy_v3 (кодування біта відношенням енергій DCT-підсмуг)

(Джерело: складено автором)

Наявний метод та його модель. Класичний метод кодує біт через домінування однієї з двох частотних підсмуг A і B в області DCT-перетворення. Позначимо E_A та E_B енергії підсмуг. Для біта 0 забезпечується перевищення E_A

над E_B у задане число разів r (target_ratio), для біта 1 – навпаки; необхідне співвідношення досягається ослабленням програшної підсмуги. Витягування виконується порівнянням енергій підсмуг. У класичному вигляді біт кодується одноразово, без надлишковості.

Недоліки. Класичний метод має два обмеження. По-перше, одноразове кодування без надлишковості робить рішення чутливим до спотворень, що змінюють баланс енергій підсмуг: стиснення з втратами та фільтрація перерозподіляють спектральну енергію й можуть інвертувати домінування. По-друге, рішення за абсолютним порогом співвідношення не враховує загальної зміни рівня сигналу. Експериментально класичний метод відновлює маркер для 90,7% файлів без атаки, але лише для 30,7% за MP3 64 kbps та 7,3% за сильної низькочастотної фільтрації (табл. 2.7).

Удосконалений метод. Пропонується доповнити метод двома складниками: (i) надлишковим кодуванням кожного біта у repeat = 5 фреймах із м'яким голосуванням більшістю; (ii) рішенням за нормованою різницею енергій замість абсолютного порогу. У методі audio_subband_energy_v3 витягування виконується за нормованою різницею

$$D = (E_A - E_B) / (E_A + E_B), \qquad (2.17)$$

де $D \geq 0$ відповідає біту 0, а $D < 0$ – біту 1. Нормування на суму енергій $E_A + E_B$ робить рішення інваріантним до масштабування рівня сигналу. Гіпотеза полягає в тому, що поєднання нормованого рішення з надлишковим кодуванням підвищує стійкість до перерозподілу спектральної енергії за збереження непомітності.

Твердження 2.8. Нехай біт закодовано відношенням енергій підсмуг з коефіцієнтом r, а декодер обчислює нормовану різницю $D = (E_A - E_B) / (E_A + E_B)$. Тоді: (а) рішення за знаком D інваріантне до масштабування обох підсмуг спільним множником $\lambda > 0$, оскільки $D(\lambda E_A, \lambda E_B) = D(E_A, E_B)$; (б) вбудований

контраст $|D| = (r - 1)/(r + 1)$, тому біт руйнується лише за спотворення енергії, що перевищує цей поріг.

Доказ. (а) $D(\lambda E_A, \lambda E_B) = (\lambda E_A - \lambda E_B) / (\lambda E_A + \lambda E_B) = (E_A - E_B) / (E_A + E_B) = D$, тобто нормування скорочує спільний множник – звідси інваріантність до нормалізації гучності та передискретизації, що змінюють рівень, але не баланс підсмуг. (б) За вбудованого відношення $E_A / E_B = r$ маємо $|D| = (r - 1)/(r + 1)$; помилка виникає лише коли спотворення змінює знак D, тобто перевищує вбудований контраст. Додатково надлишкове кодування repeat = 5 знижує залишкову ймовірність помилки згідно з Твердженням 2.1.

Експериментальна перевірка. Порівняння класичного методу audio_classic_subband та удосконаленого audio_subband_energy_v3 (r = 5, repeat = 5) виконано на наборі зі 150 аудіофайлів. За відсутності атаки обидва методи відновлюють маркер практично однаково (виживання 90,7% та 91,3%). На основному векторі атаки удосконалений метод стабільно переважає класичний: за MP3 128 kbps виживання зростає з 56,0% до 75,3% (коефіцієнт 1,35×), за MP3 96 kbps – з 50,0% до 70,0% (1,40×), за MP3 64 kbps – з 30,7% до 60,0% (1,96×). Найбільший виграш спостерігається за низькочастотної фільтрації: за w = 3 – з 51,3% до 78,7% (1,53×), за w = 7 класичний метод практично руйнується (7,3%), тоді як удосконалений зберігає 57,3%. Інваріантність нормованого рішення підтверджується стійкістю до нормалізації та передискретизації, де обидва методи зберігають високе виживання. Удосконалений метод вбудовує маркер із вищою енергією (SNR 24,4 дБ проти 35,0 дБ у класичного), що лишається вище порога чутності; за рахунок цього та надлишкового кодування досягається вища стійкість. Динаміку BER за силою MP3-стиснення наведено на рис. 2.20, розподіл виживання за атаками – на рис. 2.21.

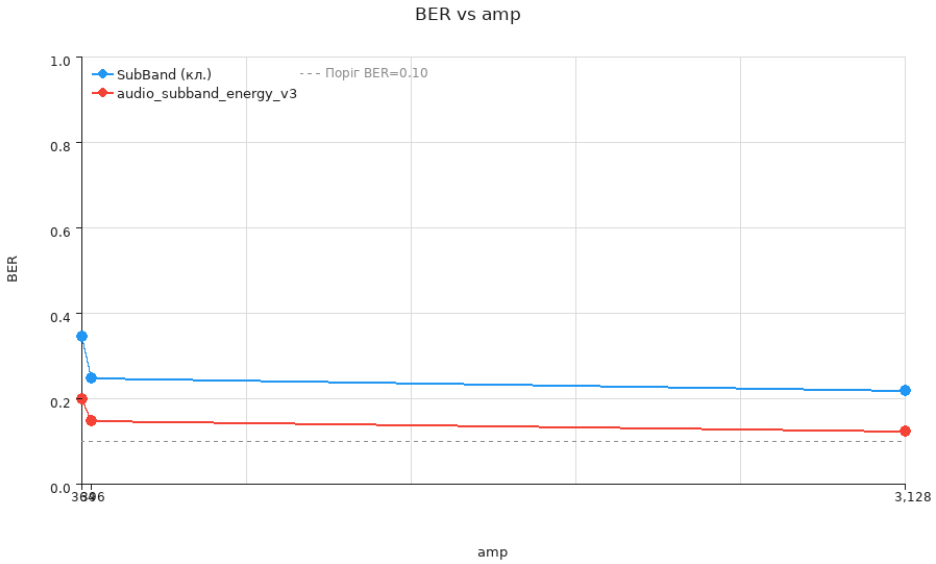


Рисунок 2.20 – Залежність BER методів audio_classic_subband та audio_subband_energy_v3 від сили MP3-стиснення

(Джерело: складено автором)

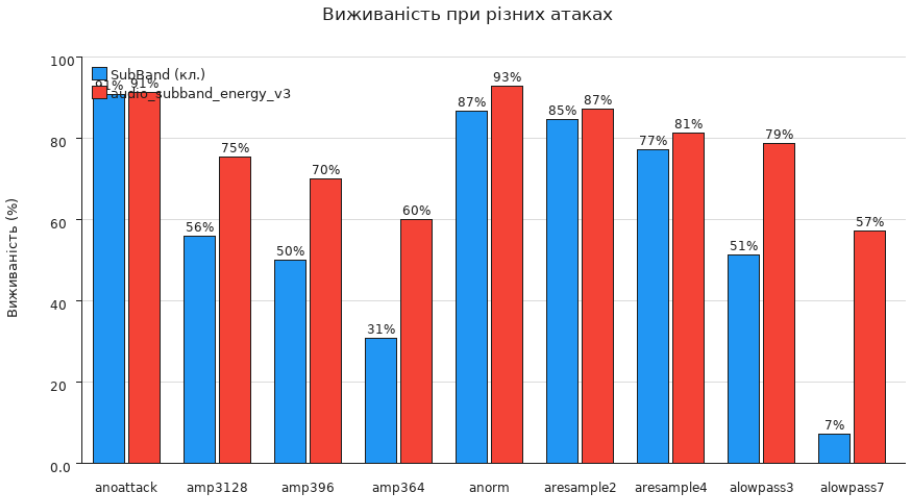


Рисунок 2.21 – Частка файлів зі збереженим маркером за атаками – audio_classic_subband та audio_subband_energy_v3

(Джерело: складено автором)

Межа застосовності. Метод має два обмеження. По-перше, обчислювальна вартість витягування є вищою за класичний метод (у середньому 32 с проти 4 с на файл) через багатосмуговий DCT-аналіз кожного фрейму; це компроміс за підвищену стійкість. По-друге, за агресивного стиснення (MP3 64

kbps) стійкість, хоча й удвічі вища за класичну, лишається помірною (60%), оскільки квантування суттєво перерозподіляє енергію підсмуг. Проте на відміну від методів часової області, метод зберігає прийнятну стійкість до фільтрації та інваріантність до масштабування, що визначає його нішу як методу, стійкого до амплітудних і частотно-вибіркових перетворень помірної інтенсивності.

Висновок. Запропоноване поєднання рішення за нормованою різницею енергій підсмуг та надлишкового кодування repeat = 5 підвищує стійкість методу у 1,35–1,96 раза за основним вектором атаки (MP3) та до 1,53 раза за низькочастотної фільтрації відносно класичного методу, забезпечуючи інваріантність до масштабування рівня сигналу (Твердження 2.8). Результат підтверджено теоретично та експериментально на вибірці зі 150 файлів. Обмеженнями методу є підвищена обчислювальна вартість витягування та помірна стійкість до агресивного стиснення, що визначає його нішу серед частотних методів вбудовування.

Таблиця 2.7 – Порівняння стійкості методів audio_classic_subband та audio_subband_energy_v3 (150 файлів, r = 5, repeat = 5, критерій BER ≤ 0,10)

Атака	**BER клас.**	**BER розроб.**	**SNR клас., дБ**	**SNR розроб., дБ**	**Вижив. клас.**	**Вижив. розроб.**	**Коеф. покращ.**
Без атаки (еталон)	0,047	0,043	35,0	24,4	90,7%	91,3%	1,01×
MP3 128 kbps	0,220	0,123	35,0	24,4	56,0%	75,3%	1,35×
MP3 96 kbps	0,250	0,150	35,0	24,4	50,0%	70,0%	1,40×
MP3 64 kbps	0,347	0,200	35,0	24,4	30,7%	60,0%	1,96×
Нормалізація гучності	0,067	0,037	35,0	24,4	86,7%	92,7%	1,07×
Передискретизація ×2	0,077	0,063	35,0	24,4	84,7%	87,3%	1,03×
Передискретизація ×4	0,113	0,093	35,0	24,4	77,3%	81,3%	1,05×
Низькочаст. фільтр. w=3	0,243	0,107	35,0	24,4	51,3%	78,7%	1,53×
Низькочаст. фільтр. w=7	0,463	0,213	35,0	24,4	7,3%	57,3%	7,82×[7]

[7] За сильної фільтрації класичний метод практично руйнується (7,3%), тому коефіцієнт відображає радше повну відмову класичного методу, ніж кратне покращення; удосконалений метод зберігає 57,3% виживання.

Джерело: складено автором

2.8. Методи машинного навчання в задачах стегоаналізу та атрибуції

Підрозділи 2.2–2.7 розглядали методи вбудовування, оцінені за непомітністю та стійкістю до атак. Проте для системи доказового захисту суттєвими є ще два аспекти – недетектованість, тобто неможливість для стороннього спостерігача встановити сам факт наявності маркера, та атрибуція, тобто автоматичне зіставлення захищеного контенту із зареєстрованим активом. Обидві задачі за своєю природою є не методами кодування біта, а методами аналізу сигналу, тому їх доцільно розв'язувати засобами машинного навчання. У цьому підрозділі наведено дві відповідні реалізації: класифікаційну оцінку стійкості до статистичного стегоаналізу (2.8.1) та навчену модель зіставлення для атрибуції (2.8.2). У обох випадках застосовано класичні методи навчання (логістичну регресію з регуляризацією), а не нейромережеві архітектури; перспективу переходу до end-to-end навчання розглянуто окремо у підрозділі 2.9.3. У наведених нижче експериментах метод audio_pgdiff_v2 використовується як реалізоване джерело маркованих аудіоконтейнерів та псевдографічних ознак. Повну математичну модель методу, алгоритми формування профілю, вбудовування та вилучення цифрового водяного знака наведено у підрозділі 3.2. У цьому підрозділі audio_pgdiff_v2 не описується повторно як метод вбудовування, а розглядається виключно як об'єкт машинного аналізу в задачах стегоаналізу та атрибуції.

2.8.1. Стійкість до статистичного (машинного) виявлення

Постановка задачі. За принципом Керкгоффса зловмисник знає алгоритм вбудовування, але не володіє ключем [239]. Питання, на яке відповідає експеримент: чи здатен він, спираючись лише на статистику сигналу, відрізнити контейнер із ЦВЗ від чистого. Формально це задача бінарної класифікації, і її розв'язність вимірюється точністю навченого класифікатора: значення поблизу 0,5 означає, що вбудовування статистичного сліду не лишає, поблизу 1,0 – що слід явний і метод детектується [239].

Такий експеримент доповнює оцінку непомітності з попередніх підрозділів принципово іншим виміром. Непомітність (ODG, суб'єктивне прослуховування) відповідає на питання, чи чує спотворення людина; недетектованість – чи виявляє його автоматичний аналіз. Метод може бути непомітним на слух і водночас тривіально детектованим, тому обидва виміри необхідні.

Модель класифікатора. Рішення про наявність вбудовування приймає логістична регресія: апостеріорну ймовірність визначають за логістичною функцією від лінійної комбінації ознак (формула 2.18), а ваги знаходять мінімізацією регуляризованої функції втрат (перехресна ентропія з L2-штрафом) (формула 2.19) [241]. Перед навчанням кожну ознаку стандартизують за формулою (2.20), щоб ваги були порівнюваними.

$$\sigma(z) = \frac{1}{1 + e^{-z}}, \quad z = w^{\mathrm{T}}x + b, \tag{2.18}$$

де $\sigma(z)$ – логістична функція (сигмоїда), що відображає лінійну комбінацію ознак у ймовірність; z – лінійна комбінація ознак; w – вектор ваг ознак; x – вектор ознак спостереження; b – зміщення (вільний член); e – основа натурального логарифма.

$$J(w, b) = -\frac{1}{n}\sum_{i=1}^{n}[y_i \ln p_i + (1 - y_i)\ln(1 - p_i)] + \lambda\|w\|^2, \tag{2.19}$$

де $J(w,b)$ – функція втрат (перехресна ентропія з L2-регуляризацією); n – кількість рядків навчальної вибірки; y_i – істинна мітка i-го рядка (0 або 1); p_i – передбачена моделлю ймовірність для i-го рядка; λ – коефіцієнт регуляризації; $\|w\|^2$ – квадрат евклідової норми вектора ваг (L2-штраф).

$$\tilde{x}_j = \frac{x_j - \mu_j}{\sigma_j}, \tag{2.20}$$

де $\tilde{x}_j$ – стандартизоване значення j-ї ознаки; x_j – її вихідне значення; μ_j – середнє

значення *j*-ї ознаки на навчальній вибірці; σ_j – її середньоквадратичне відхилення на навчальній вибірці.

Ознаковий простір. Він складається з 31 ознаки, що не використовують внутрішніх структур методів вбудовування (модель Керкгоффса) [240]: моменти логарифмічних відношень енергій сусідніх смуг (формула 2.21), середньоквадратичне відхилення їхньої першої різниці, пікуватість та ентропія гістограми (слід квантування), спектральна плоскість (формула 2.23), спектральний центроїд, частка високочастотної енергії, частота переходів через нуль (формула 2.22). Класифікатор – логістична регресія з L2-регуляризацією; перехресна перевірка п'ятифолдова, групована за вихідним файлом (обидва рядки пари завжди в одному фолді, інакше модель упізнавала б запис, а не вбудовування) [241]. Вибірку audiomix складають 150 файлів по 30 с, що дає 300 рядків.

$$r_i = \log \frac{E_i}{E_{i+1}} \tag{2.21}$$

де r_i – логарифмічне відношення енергій сусідніх смуг; E_i – енергія i-ї частотної смуги; E_{i+1} – енергія наступної смуги.

$$\mathrm{ZCR} = \frac{1}{2N} \sum_{n=1}^{N} |\mathrm{sgn}(x_n) - \mathrm{sgn}(x_{n-1})| \tag{2.22}$$

де ZCR – частота переходів сигналу через нуль; N – кількість відліків у кадрі; x_n – n-й відлік сигналу; sgn – функція знаку.

$$\mathrm{SFM} = \frac{(\prod_k |X_k|)^{1/K}}{\frac{1}{K}\sum_k |X_k|} \tag{2.23}$$

де SFM – спектральна плоскість (відношення середнього геометричного до середнього арифметичного модулів спектра); X_k – k-й коефіцієнт спектра (за

модулем); K – кількість спектральних складових.

Результати. Порівняно два методи – розширення спектра audio_spread_spectrum_v2 як модифікована версія представника класичного підходу і запропонований audio_pgdiff_v2 (табл. 2.8).

Таблиця 2.8 – Точність статистичного виявлення вбудованого маркера класифікатором для методів audio_spread_spectrum_v2 та audio_pgdiff_v2

Метод	**Параметри**	**Точність**	**95% ДІ**	**AUC**	**Помилок / 300**
audio_spread_spectrum_v2	α=0,032; chips=512; rep=5	0,987	[0,966; 0,995]	1,000	4
audio_pgdiff_v2	target_ratio=4; rep=5	0,707	[0,653; 0,755]	0,774	88

Джерело: складено автором

Для перевірки коректності самої процедури ті самі прогони повторено з випадково перемішаними мітками (табл. 2.9).

Таблиця 2.9 – Результати контрольного експерименту з випадково перемішаними мітками класів

Контроль	**Точність**	**95% ДІ**	**AUC**
audio_spread_spectrum_v2	0,530	[0,473; 0,586]	0,529
audio_pgdiff_v2	0,547	[0,490; 0,602]	0,571

Джерело: складено автором

Обидва контрольні інтервали накривають рівень 0,5, тож витоку даних у процедурі перехресної перевірки немає: висока точність основних прогонів походить саме зі сліду вбудовування, а не з помилки в побудові фолдів.

Інформативні ознаки. Аналіз ваг класифікатора у стандартизованому просторі показує, на що він спирається. Для audio_spread_spectrum_v2 три провідні ознаки – частота переходів через нуль (+1,903), частка високочастотної енергії (+1,806) і спектральний центроїд (+1,376); усі зі знаком «плюс», тобто

вбудовування їх піднімає. Це підпис широкосмугового шуму, доданого до сигналу. Для audio_pgdiff_v2 на першому місці стоїть середнє логарифмічне відношення енергій смуг (−0,835) – тобто рівно та величина, якою метод кодує біт, – а на другому стрибкуватість енергії між сусідніми кадрами (+0,798); шумових ознак у першій трійці немає взагалі.

Незалежність виявності від параметра target_ratio. Окремий експеримент проведено на тих же 150 файлах (табл. 2.10).

Таблиця 2.10 – Залежність виявності маркера audio_pgdiff_v2 від параметра target_ratio

target_ratio	**1,5**	**2**	**3**	**4**
Точність виявлення	0,683	0,697	0,690	0,707

Джерело: складено автором

Розмах становить 0,024 за напівширини довірчого інтервалу близько 0,05, монотонності немає (значення для 2 вище за значення для 3), тобто величини статистично нерозрізнювані. Звідси, по-перше, компромісу «стійкість проти прихованості» за цим параметром не існує, тож робоча точка target_ratio=4 обґрунтована однозначно. По-друге, якби класифікатор спирався на величину зсуву відношення енергій, зниження target_ratio зменшувало б точність; воно її не зменшує, отже метод видає сам факт квантування – регулярне чергування змінених і незмінених кадрів. Тому знизити виявність налаштуванням параметрів неможливо, потрібна структурна зміна розміщення копій.

Єдиний механізм. Той самий доданий широкосмуговий шум, який класифікатор бачить як приріст високочастотної енергії та частоти переходів через нуль, вухо чує як шипіння. Це дає узгоджену картину трьох незалежних вимірювань (табл. 2.11).

Одна фізична причина – розподіл спотворення по спектру й по часу – пояснює водночас і чутність, і виявність.

Таблиця 2.11 – Узгодженість об'єктивної, суб'єктивної та статистичної оцінок помітності маркера

Вимірювання	audio_spread_spectrum_v2	audio_pgdiff_v2
Віконний ODG (медіана)	−3,02	−0,83
Суб'єктивне прослуховування	стійке шипіння	епізодичне поскрипування
Виявність класифікатором	0,987	0,707

Джерело: складено автором

Висновок. Запропонований метод істотно менш виявний: 0,707 проти 0,987, причому довірчі інтервали не перетинаються, а метод розширення спектра детектується практично безпомилково (AUC 1,000). Проте це не свідчить про невиявність: значення 0,707 достовірно вище за рівень випадкового вгадування, тому коректним є формулювання, що метод знижує точність статистичного виявлення, але не усуває її. Подальше зниження досяжне лише структурною зміною розміщення копій, а не налаштуванням параметрів.

2.8.2. Навчена модель зіставлення для атрибуції мультимедійного контенту

Постановка та наявне рішення. Задача атрибуції полягає в тому, щоб за запитом – можливо, модифікованою копією – повернути правильний зареєстрований актив або відмовити, якщо запит не належить жодному з них. Вона розпадається на дві підзадачі: closed-set (знайти власний актив серед зареєстрованих) і open-set (відмовитися від атрибуції для незареєстрованого запиту) [242, 243]. У наявній реалізації системи атрибуцію зображень покладено на зовнішній сервіс Google Cloud Vision, а для аудіо застосовано детерміноване рішення – фіксований поріг за одним дескриптором (відстань Геммінга ≤ 12 за 64-бітним відбитком).

Недоліки наявного рішення. Зовнішній сервіс не є власним компонентом: він не піддається аналізу, не дає доказової характеристики рішення і суперечить принципу Керкгоффса, за яким атрибуція має спиратися лише на публічні дескриптори. Детермінований поріг використовує єдиний дескриптор, не

поєднує ознак і не вимірює частку хибної атрибуції – частоту, з якою система впевнено називає власника й помиляється. Для доказової системи саме ця величина критична, оскільки хибна атрибуція небезпечніша за пропуск.

Запропонований метод. Замість зовнішньої залежності й фіксованого порога запропоновано навчену модель зіставлення (*matcher*) – логістичну регресію з L2-регуляризацією над попарними мірами схожості дескрипторів, які система вже обчислює [241]. Оцінку збігу пари «запит–кандидат» визначають за формулою (2.24). Ознаковий простір складають 26 ознак для зображень і 29 для аудіо: згоди бітів перцептивних хешів pHash/dHash поблочно (формула 2.25) [227], відстані блокового ДКП, косинусна узгодженість субсмугових профілів (формула 2.26), slide-подібність та перекриття d_{seq} для аудіо. Порівнюються три підходи: baseline (фіксований поріг за одним дескриптором), абляція (логістична регресія на єдиній найсильнішій ознаці) і повна модель (усі ознаки пари).

$$s(q, c) = \sigma(w^{\mathrm{T}}\varphi(q, c) + b), \tag{2.24}$$

де $s(q, c)$ – оцінка збігу пари «запит–кандидат», що інтерпретується як імовірність належності кандидата c тому самому цифровому активу, що й запит q; σ – логістична функція (формула 2.18); w – вектор вагових коефіцієнтів моделі; T – операція транспонування; $\varphi(q, c)$ – вектор ознак попарної схожості дескрипторів запиту і кандидата; b – зсув (вільний член) моделі.

$$\mathrm{agree}(a, b) = 1 - \frac{1}{L}\sum_{i=1}^{L}(a_i \oplus b_i), \tag{2.25}$$

де agree(a, b) – частка збігу бітів двох перцептивних хешів (обчислюється для кожного блока зображення окремо); a, b – бітові рядки перцептивних хешів pHash або dHash запиту і кандидата; L – довжина хешу в бітах; a_i, b_i – i-ті біти відповідних хешів; $\oplus$ – операція виключного АБО (XOR), що дорівнює 1 для різних бітів і 0 – для однакових.

$$\cos(u, v) = \frac{u^{\mathrm{T}} v}{\|u\|\|v\|}, \tag{2.26}$$

де cos(*u*, *v*) – косинусна узгодженість двох векторів; *u*, *v* – вектори субсмугових енергетичних профілів запиту і кандидата; $u^{\mathrm{T}}v$ – скалярний добуток векторів; $\|u\|$, $\|v\|$ – евклідові норми векторів.

Щодо абляційного варіанта слід урахувати таку математичну властивість: логістична регресія з однією ознакою є монотонною функцією цієї ознаки, тому ранжування кандидатів за такою моделлю тотожне ранжуванню за самою ознакою. Отже, у закритому сценарії підбір порога не змінює порядку кандидатів, і будь-який приріст точності повної моделі порівняно з абляційним варіантом зумовлений виключно комбінуванням ознак.

Протокол і метрики. Оцінювання проводиться проти повної галереї (стандартний протокол retrieval): розділяються навчальні ідентичності, а не галерея [242]. Перехресна перевірка п'ятифолдова, групована за активом; межа train/test проходить по парах, тож жоден актив тестового фолда не бере участі в навчанні. Витоку немає за побудовою: ознаки пари не кодують ідентичності активу, а контроль із перемішаними мітками падає до рівня випадкового вгадування. Якість closed-set вимірюють через Recall@1 (формула 2.27) і mAP (формула 2.28), відкритий сценарій – через ROC-AUC та рівну помилку EER (формула 2.29). Використано 5 seed, довірчі інтервали – t-інтервал Стьюдента.

$$\mathrm{Recall@1} = \frac{1}{Q}\sum_{q=1}^{Q} \mathbb{1}\left[\mathrm{rank}_q = 1\right], \tag{2.27}$$

де Recall@1 – повнота на першій позиції ранжування (частка запитів, для яких істинний актив отримав ранг 1); Q – кількість запитів; rank_q – позиція істинного активу в ранжованому списку кандидатів для запиту q; $\mathbb{1}[\cdot]$ – індикаторна функція, що дорівнює 1, якщо умова в дужках виконується, і 0 – в іншому разі.

$$\mathrm{mAP} = \frac{1}{Q}\sum_{q=1}^{Q} \mathrm{AP}_q\,, \qquad \mathrm{AP}_q = \sum_{k} P(k)\Delta r(k), \tag{2.28}$$

де mAP – середня точність за всіма запитами (mean Average Precision); Q – кількість запитів; AP_q – середня точність для запиту q; $P(k)$ – точність на перших k позиціях ранжованого списку кандидатів; $\Delta r(k)$ – приріст повноти при переході від позиції k – 1 до позиції k.

$$\mathrm{EER} = \mathrm{FPR}(\tau^*) = \mathrm{FNR}(\tau^*), \tag{2.29}$$

де EER – рівень рівної помилки (Equal Error Rate); FPR(τ) – частка хибнопозитивних рішень за порогу τ; FNR(τ) – частка хибнонегативних рішень за порогу τ; τ^* – значення порогу, за якого FPR і FNR рівні.*Результати – зображення.* Датасет – 567 зображень (100 дистракторів, 467 галереї), 18 умов атак, 10 206 запитів. У closed-set (табл. 2.12) повна модель перевершує baseline, причому абляція лишається практично на рівні baseline, тож 88% приросту припадає на комбінування ознак.

Таблиця 2.12 – Точність атрибуції зображень у закритому сценарії для базового підходу, абляційного варіанта та повної моделі

Підхід	**Recall@1**	**95% ДІ**	**mAP**	**95% ДІ**
baseline (dhash_hamming)	0,863	[0,862; 0,864]	0,875	[0,875; 0,876]
абляція (dct_ac_sign_agree)	0,868	[0,866; 0,870]	0,881	[0,879; 0,882]
повна модель	0,903	[0,901; 0,904]	0,910	[0,909; 0,911]

Джерело: складено автором

Розподіл переваги по атаках виявляє, що обрізання – єдина вісь, яка розрізняє підходи (табл. 2.13). Перестиснення JPEG (до Q40) і гаусів шум (до σ=20) обидва підходи витримують без втрат: перцептивний хеш dHash до них нечутливий у всьому доступному діапазоні, і це задокументована властивість дескриптора, а не невдала спроба знайти точку зламу.

Таблиця 2.13 – Стійкість атрибуції зображень до обрізання

Атака	Збереж. площа	Стеля відбору	baseline	Модель	Різниця
crop5	90%	1,000	0,997	0,998	+0,002
crop10	81%	1,000	0,984	0,998	+0,015
crop20	64%	0,945	0,442	0,881	+0,440
crop30	49%	0,529	0,089	0,292	+0,203
crop40	36%	0,261	0,027	0,082	+0,055

Джерело: складено автором

Крива має точку зламу між 20% і 30% обрізання. Достовірна перевага (інтервали не перетинаються) – на чотирьох атаках із вісімнадцяти. В open-set повна модель також перевершує baseline: ROC-AUC зростає з 0,913 до 0,930, EER знижується з 0,153 до 0,116; частка хибної атрибуції на робочій точці FPR = 0,01 становить 0,0022 проти 0,0027 у baseline. Порівняно з найсильнішою ознакою окремо (AUC 0,920) перевага в розділенні недоказова – інтервали перетинаються; доказовий внесок комбінування ознак зосереджений у ранжуванні closed-set. Контроль із перемішаними мітками дав 0,018 за рівня випадкового вгадування 0,024 – витоку немає.

Результати для аудіо. Датасет містить 150 файлів: 120 файлів галереї та 30 файлів-дистракторів, тобто сторонніх файлів, відповідників яких у галереї немає. Із застосуванням 11 умов атак сформовано 1650 запитів. У закритому сценарії (табл. 2.14) повна модель забезпечує Recall@1 = 0,906 проти 0,763 для базового підходу.

Таблиця 2.14 – Точність атрибуції аудіоданих у закритому сценарії для базового підходу, абляційного варіанта та повної моделі

Підхід	Recall@1	95% ДІ	mAP	95% ДІ
baseline (fp_hamming)	0,763	[0,754; 0,772]	0,796	[0,789; 0,804]
абляція (slide_best_similarity)	0,903	[0,897; 0,909]	0,909	[0,904; 0,913]
повна модель	0,906	[0,901; 0,911]	0,911	[0,906; 0,915]

Джерело: складено автором

Тут, на відміну від зображень, абляція майже дорівнює повній моделі: 98% приросту дає перехід від дескриптора fp_hamming до slide_best_similarity, а комбінування додає лише +0,003. Отже приріст closed-set для аудіо забезпечує не машинне навчання, а вибір дескриптора ранжування; це водночас практична рекомендація до системи. В open-set повна модель істотно перевершує детермінований baseline (ROC-AUC 0,805 → 0,958; частка хибної атрибуції на FPR = 0,01 – 0,0478 → 0,0084, у 5,7 раза), проте це покращення забезпечує дескриптор, а не комбінування ознак: одна ознака slide_best_similarity розділяє дистрактори не гірше за повну модель (AUC 0,974 проти 0,958, інтервали розділені). Повну модель залишено робочим двигуном на тій підставі, що в робочій точці (FPR = 0,01), де й ухвалюється рішення, її частка хибної атрибуції не вища, а дещо нижча за одну ознаку (0,0084 проти 0,0126); AUC ж усереднює всю криву, включно з порогами, у яких система не працює. Контроль дав 0,020 за рівня вгадування 0,026.

Єдиний механізм. Стелі відбору для найважчих атак обох модальностей майже збігаються, проте частка стелі, яку бере модель, різниться вдвічі (табл. 2.15). Це показує, що сама стеля не вказує, де вузьке місце, – потрібно дивитися на частку, яку модель від неї вибирає.

Таблиця 2.15 – Визначення етапу, що обмежує точність атрибуції за найважчих атак: відбір кандидатів чи ранжування

Модальність, атака	Стеля	Модель	Частка стелі	Що обмежує
Аудіо, atrim25	0,533	0,530	99,4%	тільки відбір
Зображення, crop30	0,529	0,292	55,2%	відбір і ранжування
Зображення, crop40	0,261	0,082	31,4%	відбір і ранжування

Джерело: складено автором

Обрізання аудіо інформацію зміщує: фрагмент лишається цілим, змінюється лише його позиція в часі, і slide-подібність відновлює вирівнювання – обмежує лише відбір. Обрізання зображення інформацію знищує: при crop40

від кадру лишається 36% площі, і жодне вирівнювання цього не поверне, тому запас лишається і у відборі, і в ранжуванні.

Висновки та обмеження. Запропонована навчена модель зіставлення замінює зовнішню залежність і фіксований поріг власною моделлю з визначеним ознаковим простором, оціненою за стійкістю до модифікацій та за виміряною ненульовою часткою хибної атрибуції в обох модальностях. Внесок машинного навчання локалізовано точно. Доказовий внесок комбінування ознак – у ранжуванні closed-set зображень (+0,035 над найсильнішою ознакою, інтервали не перетинаються; а оскільки в closed-set поріг не переставляє кандидатів, приріст походить саме від багатовимірного рішення). У розділенні (open-set) окремого внеску комбінування над найсильнішою ознакою не встановлено в жодній модальності: для зображень перевага недоказова, для аудіо одна ознака розділяє навіть краще. Для аудіо приріст closed-set забезпечує заміна дескриптора ранжування, а не навчання. Повну модель розгорнуто як робочий двигун у обох модальностях на підставі робочої точки, де її частка хибної атрибуції не вища за альтернативи. Слід назвати два обмеження. По-перше, експеримент проведено на матеріалі без вбудованого ЦВЗ, тож ознаки збігу корисного навантаження лишалися константними: перевірено шлях «перцептивний відбиток + навчання», тоді як навчена модель зіставлення виступає як рівень резервування на випадок, коли маркер атаку не пережив, – тобто доповнює, а не замінює доказову ідентифікацію за навантаженням. По-друге, для зображень сітка атак розрізнює підходи лише за віссю обрізання, оскільки перцептивний хеш нечутливий до JPEG і шуму в усьому доступному діапазоні.

2.9. Перспективні напрями вдосконалення (теоретичне обґрунтування)

Розглянуті у підрозділах 2.2–2.8 методи доведено теоретично та експериментально. Поряд із ними у складі системи передбачено низку напрямів, реалізація яких є предметом подальших досліджень. Для цих напрямів наведено

теоретичне обґрунтування запропонованого підходу та очікувані характеристики, тоді як експериментальна перевірка становитиме окремий етап роботи. На відміну від попередніх підрозділів, тут не наводяться кількісні результати та порівняльні таблиці, оскільки відповідні методи перебувають на стадії розробки. Важливо, що запропоновані напрями розвивають принципи, вже підтверджені у попередніх підрозділах, переносячи їх на нові області перетворень.

2.9.1. Метод фазового кодування (Phase Coding)

Наявний метод. Класичний метод фазового кодування [187] вбудовує дані у абсолютну фазу першого сегмента дискретного перетворення Фур'є (ДПФ) сигналу, зберігаючи відносні фазові співвідношення між сусідніми сегментами. Оскільки слух малочутливий до абсолютної фази, метод забезпечує високу непомітність.

Недоліки. Рішення за абсолютною фазою чутливе до будь-якого фазового спотворення: стиснення з втратами та фільтрація зміщують фази нелінійно, руйнуючи маркер. Відсутність надлишкового кодування та потреба у точній синхронізації сегментів додатково обмежують стійкість.

Запропонований підхід (гіпотеза). За аналогією з диференційним ехо-приховуванням (підрозділ 2.6) пропонується перейти від абсолютної фази до диференційного фазового кодування – біт кодувати різницею фаз між сусідніми частотними компонентами:

$$\Delta\varphi = \varphi_k - \varphi_{k+1}, \tag{2.30}$$

а рішення ухвалювати за знаком $\Delta\varphi$. Таке рішення інваріантне до сталого фазового зсуву, який вносить більшість атак, аналогічно до інваріантності різниці автокореляційних піків у методі прихованого ехо (Твердження 2.7). Додатково передбачається надлишкове кодування з голосуванням більшістю.

Очікувані характеристики. Інваріантність до сталого фазового зсуву має забезпечити підвищену стійкість до передискретизації та помірного стиснення за збереження непомітності на рівні класичного методу (слух малочутливий до фазових змін). За аналогією з диференційним ехо очікується кратне підвищення стійкості за легких і середніх атак. Напрямом експериментальної перевірки є реалізація в області дискретного перетворення Фур'є та порівняння з класичним методом за протоколом підрозділів 2.2–2.7 (150 файлів, 9 атак).

2.9.2. Гібридні трансформні схеми (DWT+SVD, DWT+DCT)

Наявний метод. Гібридні схеми поєднують дискретне вейвлет-перетворення (DWT) для частотно-просторової декомпозиції з подальшим вбудовуванням у сингулярні числа (SVD) або DCT-коефіцієнти обраного піддіапазону [38]. Багаторівнева декомпозиція забезпечує гнучкий компроміс між стійкістю та непомітністю.

Недоліки. Класичні SVD-схеми страждають на проблему хибних спрацювань (false-positive) через неєдиність вибору сингулярних векторів, що може спричиняти хибне виявлення маркера; фіксований вибір піддіапазону не враховує вміст сигналу; адитивне вбудовування потребує оригіналу для витягання.

Удосконалений метод. Пропонується два вдосконалення: (1) адаптивний вибір DWT-піддіапазону за критерієм стійкість/непомітність для кожного сигналу – за аналогією з адаптивним вибором DCT-позицій у методі wm_v2_dct_qim_profile (підрозділ 2.3); (2) заміна адитивного вбудовування на QIM-квантування сингулярних чисел:

$$\sigma' = \Delta \cdot \mathrm{round}(\sigma / \Delta) + \delta_b, \qquad (2.31)$$

що забезпечує сліпе витягання без оригіналу й усуває проблему хибних спрацювань SVD. Умова збереження біта при цьому визначається тим самим співвідношенням $\Delta > q$, що і для DCT-QIM (Твердження 2.3).

Теоретичні передумови та напрям верифікації. Запропонована схема створює передумови для сліпого витягання маркера та зменшення ймовірності хибних спрацювань. Фактична стійкість і відсутність хибних спрацювань у межах цієї роботи експериментально не підтверджені та потребують окремої перевірки.

2.9.3. Нейромережеві (end-to-end) методи

Наявний метод. Сучасні end-to-end методи навчають пару згорткових нейромереж – вбудовувач (encoder) та витягувач (decoder) – спільно, із диференційовним шаром-«атакою» (noise layer) між ними, що моделює спотворення каналу під час навчання [38].

Недоліки. Стійкість забезпечується переважно до атак, представлених під час навчання; узагальнення на невідомі типи спотворень погане; обчислювальна вартість навчання висока; декодер-«чорна скринька» не дає доказової ідентифікації маркера.

Удосконалений метод. Пропонується два вдосконалення: (1) розширення шару-атаки реальним MP3-перекодуванням, а не лише адитивним шумом, для кращого узагальнення на практичні спотворення; (2) інтеграція навченого вбудовувача зі службовою структурою кадру з CRC32 системи IP-Protect (підрозділи 2.2, 2.5), щоб поєднати ємність нейромережевого підходу з доказовою ідентифікацією маркера. Функція втрат поєднує обидві вимоги:

$$L = \lambda_1 \cdot L_{\text{непом}} + \lambda_2 \cdot L_{\text{стійк}}, \qquad (2.32)$$

де $L_{\text{непом}}$ відповідає за непомітність, $L_{\text{стійк}}$ – за стійкість, а вагові коефіцієнти λ_1, λ_2 задають компроміс між ними.

Теоретичне обґрунтування напряму. Запропонована архітектура передбачає включення реалістичного шару моделювання атак і службового кадру з CRC. Оскільки модель у межах роботи не навчалася й експериментально не перевірялася, її характеристики не належать до підтверджених результатів дисертації.

Висновок до підрозділу. Наведені напрями розвивають принципи, підтверджені у попередніх підрозділах: диференційне кодування (підрозділ 2.6) переноситься на фазову область, адаптивний вибір позицій та QIM-квантування (підрозділ 2.3) – на гібридні трансформні схеми, а доказовий кадр із CRC32 (підрозділи 2.2, 2.5) – на нейромережеві методи. Це забезпечує концептуальну єдність системи та окреслює обґрунтований план подальших досліджень. Експериментальна перевірка зазначених напрямів становитиме окремий етап роботи.

2.9. Висновки до розділу 2

У розділі розроблено математичні моделі та удосконалення методів вбудовування цифрових водяних знаків у мультимедійні дані. Кожне вдосконалення розглянуто за єдиною аналітичною схемою: формалізація наявного методу, виявлення його недоліків, формулювання гіпотези, доведення відповідного твердження та експериментальна перевірка на репрезентативній вибірці (150 аудіофайлів або 567 зображень) із кількісним підтвердженням підвищення ефективності. Такий підхід забезпечує, що кожне вдосконалення спирається не на якісні міркування, а на вимірюваний результат, придатний для формулювання наукової новизни.

Реалізовано та експериментально підтверджено сім методів у шести напрямах вбудовування. Для кожного доведено твердження, що обґрунтовує механізм підвищення стійкості: надлишкове кодування з голосуванням (Твердження 2.1), груповий енергетичний контраст (Твердження 2.2), узгодження кроку QIM-решітки з кроком квантування (Твердження 2.3), диференційний енергетичний контраст (Твердження 2.5), підсилення розстилки спектра з когерентним комбінуванням (Твердження 2.6), інваріантність різниці автокореляційних піків (Твердження 2.7) та інваріантність нормованої різниці енергій підсмуг (Твердження 2.8). Узагальнені результати порівняння наведено в табл. 2.8.

Таблиця 2.8 – Узагальнене порівняння удосконалених методів за основним вектором атаки

№	Метод (напрям)	Осн. вектор	Виграш	Характеристика / межа
2.2	LSB / QIM-надлишковість (audio_qim_v1)	MP3	3,8–5,5×	Стійкий до стиснення; межа – фільтрація
2.2	Patchwork (audio_patchwork_v2)	MP3	1,5×	Помірний виграш за рівної непомітності
2.3	DCT-QIM (wm_v2_dct_qim_profile)	JPEG	100% ст.	Повна стійкість до JPEG; межа – обрізання
2.4	MDCT-контраст (audio_mdct_qim_v2)	MP3	1,5–3,7×	Ніша – психоакустика; слабший за DSSS
2.5	Spread Spectrum (audio_spread_spectrum_v2)	MP3	1,8–3,0×	Найвища стійкість серед аудіометодів
2.6	Echo Hiding (audio_echo_hiding_v2)	MP3	2,1–3,9×	Нішевий; компроміс амплітуди
2.7	Subband Energy (audio_subband_energy_v3)	MP3	1,4–2,0×	Інваріантний до масштабування

Джерело: складено автором

Аналіз узагальнених результатів дозволяє сформулювати такі закономірності. По-перше, методи часової області (LSB, patchwork, exo) забезпечують стійкість до стиснення, але мають спільну межу – руйнування за частотно-вибіркових атак (низькочастотна фільтрація), що обґрунтовує перехід до частотних методів. По-друге, найвищу стійкість до стиснення з втратами серед аудіометодів забезпечує метод розширеного спектра завдяки розподілу енергії маркера по всьому спектру, тоді як методи, локалізовані у тому самому базисі, що й кодек (MDCT), поступаються за абсолютною стійкістю. По-третє, для зображень узгодження кроку QIM-решітки з кроком квантування JPEG (умова $\Delta > q$) забезпечує повну стійкість до основного вектора атаки за адаптивного вибору позицій вбудовування.

Ключовим методологічним принципом, застосованим до всіх методів, є вирівнювання непомітності (SNR/PSNR) перед обчисленням коефіцієнтів покращення: це виключає вплив різної потужності вбудовування на результат і забезпечує коректність порівняння класичного та удосконаленого методів.

Службова структура кадру з контрольною сумою CRC32, спільна для запропонованих методів, додатково забезпечує доказову ідентифікацію маркера, що є визначальною рисою доказово-орієнтованого конвеєра системи IP-Protect.

Перспективні напрями (фазове кодування, гібридні трансформні схеми, нейромережеві методи) обґрунтовано теоретично; їх реалізація та експериментальна перевірка становитимуть предмет подальших досліджень. Отримані у розділі результати покладено в основу формулювання наукової новизни та реалізовано у складі інформаційної системи захисту інтелектуальної власності, розглянутій у наступних розділах.

РОЗДІЛ 3. РОЗРОБКА МЕТОДІВ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ НА ОСНОВІ ЦИФРОВОГО ВОДЯНОГО МАРКУВАННЯ ТА ПСЕВДОГРАФІЧНО-ДИФЕРЕНЦІАЛЬНОГО АНАЛІЗУ

3.1. Вдосконалений метод DCT-QIM для вбудовування водяного знака у зображення

3.1.1. Постановка задачі та цільова функція

У межах інформаційної системи IP-Protect зображення розглядається як цифровий контейнер, у який непомітно вбудовується короткий ідентифікаційний блок, що пов’язує файл із користувачем, цифровим активом або службовим токеном системи. Прихований водяний знак не призначений для візуального сприйняття, проте має вилучатися під час перевірки навіть після типових перетворень: повторного збереження, JPEG-стиснення, помірного масштабування або зміни формату [214].

Процеси вбудовування та вилучення цифрового водяного знака у запропонованому методі формалізуються такими операторами:

$$Y = E(X, b, k, \theta) \tag{3.1}$$

$$\hat{b} = D(\tilde{Y}, k, \theta) \tag{3.2}$$

де X – початкове зображення; b – послідовність бітів цифрового водяного знака; k – секретний ключ; θ – сукупність параметрів методу; E – оператор вбудовування; Y – зображення з вбудованим цифровим водяним знаком; $\tilde{Y}$ – зображення після можливого перетворення або атаки; D – оператор вилучення; $\hat{b}$ – відновлена послідовність бітів.

Рішення про наявність водяного знака приймається трирівневою схемою на основі BER та NC:

$$PASS : BER \leq 0.05 \wedge NC \geq 0.90 \quad (3.3)$$

$$FAIL : BER \geq 0.20 \vee NC \leq 0.70 \quad (3.4)$$

$$PARTIAL : інші\ випадки \quad (3.5)$$

Трирівнева схема є запропонованим рішенням: вона не зводить результат до бінарного «так/ні», а надає проміжний стан PARTIAL для часткового пошкодження або недостатньої впевненості детектора. Загальну архітектуру методу показано на рис. 3.1.

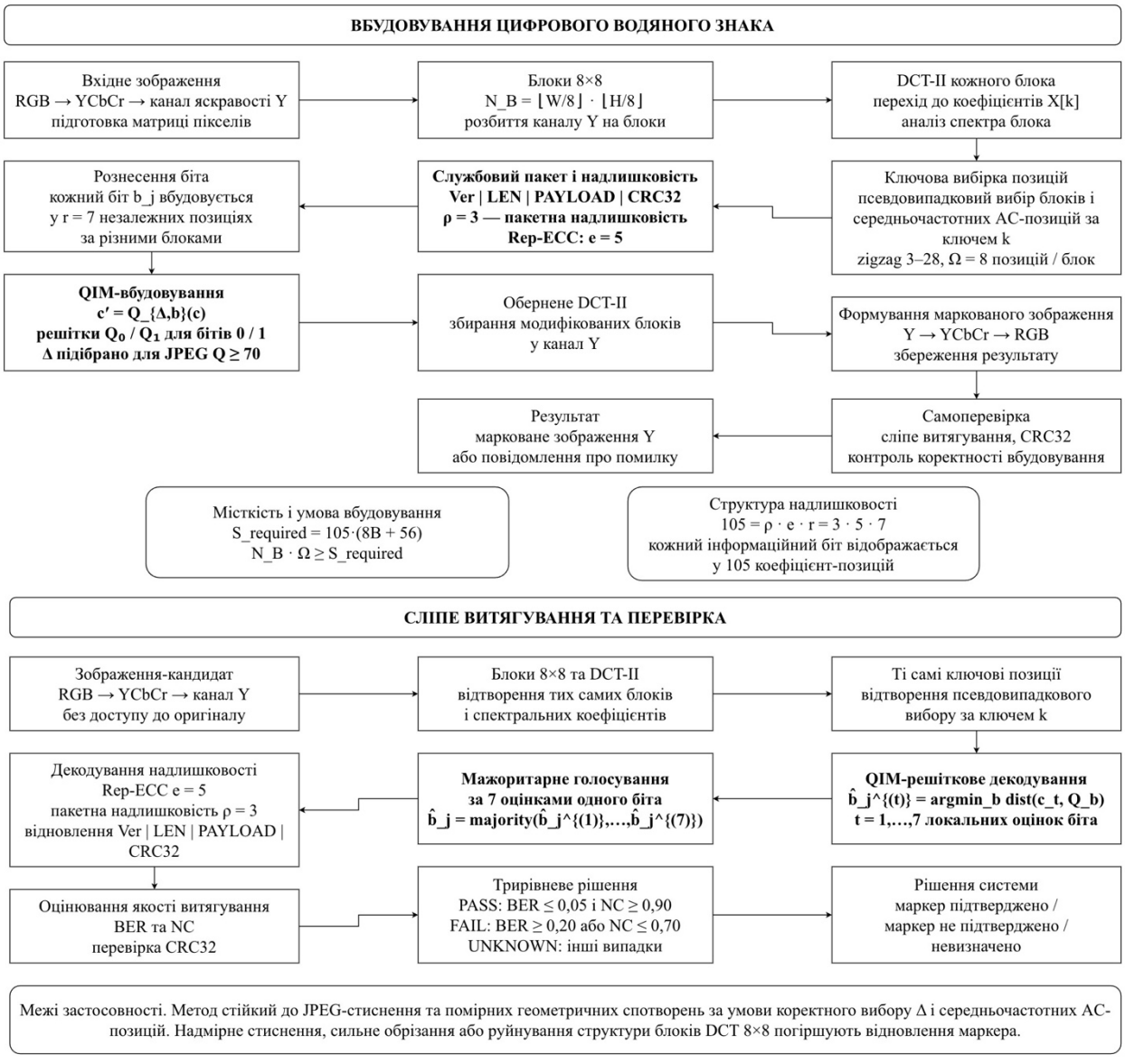


Рисунок 3.1 – Архітектура запропонованого методу DCT-QIM для зображень (wm_v2_dct_qim_profile*)*

(Джерело: складено автором)

3.1.2. Архітектура запропонованого методу

Метод wm_v2_dct_qim_profile реалізує блокове DCT-QIM-вбудовування з псевдовипадковою ключовою вибіркою позицій, пакетним кодуванням та повторенням. Зображення ділиться на блоки 8×8, кількість яких:

$$N_B = \lfloor W/8 \rfloor \cdot \lfloor H/8 \rfloor \tag{3.6}$$

Метод генерує псевдовипадковий порядок блоків та позицій коефіцієнтів за ключем k, обираючи середньочастотні позиції (3–28 у зигзаг-порядку). QIM-вбудовування одного біта:

$$c' = Q_{\Delta,b}(c) = \Delta \cdot (\lfloor c/\Delta \rfloor + b/2 + (-1)^b / 4) \tag{3.7}$$

Кожен біт ідентифікатора вбудовується r = 7 разів у незалежно вибраних блоках. Остаточне рішення приймається голосуванням більшості.

3.1.3. Пакетне кодування та ємність контейнера

У межах запропонованої моделі службове повідомлення не вбудовується у мультимедійний контейнер як неструктурована послідовність бітів. Перед розміщенням у вибраній області вбудовування воно перетворюється на формалізований пакет, що містить службові поля для визначення версії формату, довжини повідомлення та контролю цілісності. Такий підхід необхідний для того, щоб під час вилучення система могла не лише отримати певну бітову послідовність, а й перевірити, чи відповідає вона очікуваній структурі та чи не була пошкоджена внаслідок стиснення, шуму або інших перетворень.

Пакет включає версію формату (8 біт), поле довжини службового повідомлення (16 біт), власне службове повідомлення та контрольну суму CRC32 (32 біти). Версія формату дає змогу підтримувати подальші модифікації схеми кодування без втрати сумісності, поле довжини визначає межі корисної

частини пакета, а CRC32 використовується для відбраковування хибних або частково пошкоджених результатів вилучення.

$$L_{packet} = L + 56 \text{ (біт)} \tag{3.8}$$

Після застосування надлишковості ρ = 3, repetition-ECC e = 5 та r = 7 розміщень умова ємності контейнера (Ω = 8 коефіцієнтів/блок):

$$S_{required} = 105 \cdot (8B + 56),\ N_B \cdot \Omega \geq S_{required} \tag{3.9}$$

У табл. 3.1 наведено практичні мінімальні вимоги до зображення-контейнера.

Таблиця 3.1 – Практичні мінімальні вимоги до зображення-контейнера

Сценарій службове повідомлення	Службове повідомлення, байт	Потрібно символів	Мін. розмір (формула)	Практ. мін. файл
Короткий токен	8	12 600	320×320 px	≥ 61 440 Б
Компактний токен	16	19 320	400×400 px	≥ 102 400 Б
Типове службове повідомлення	32	32 760	512×512 px	≥ 153 600 Б
Орієнтир 44 байт	44	42 840	592×592 px	≥ 225 280 Б

Джерело: складено автором

3.1.4. Теоретичні та практичні рішення, на яких ґрунтується запропонований метод

Метод базується на класичних результатах DCT-QIM [170, 211], однак містить запропоновані рішення, що покращують практичні характеристики. У табл. 3.2 наведено розмежування запозичених підходів та запропонованих модифікацій.

Таблиця 3.2 – Теоретична та практична основа в порівнянні з запропонованою складовою методу DCT-QIM для зображень

Елемент	Джерело / клас методів	Оригінальне рішення запропонованого методу
Блокове DCT	Ахмед та ін. [215]; стандарт JPEG	Середньочастотні коефіцієнти (зигзаг 3–28); псевдовипадкова вибірка блоків за ключем k
QIM-вбудовування	Чен, Уорнелл [170]	Крок Δ підібрано для JPEG Q≥70; QIM на r=7 незалежних позиціях
Повторення бітів	Загальний принцип ECC	r=7 з голосуванням більшості; позиції псевдовипадкові
CRC32 + пакетна надлишковість	Стандартна перевірка цілісності	Власний формат пакета з ρ=3 та rep5-ECC; формалізована умова ємності (3.9)
Схема PASS/ PARTIAL /FAIL	Авторське рішення IP-Protect	Пороги BER та NC задані явно (3.3)–(3.5); PARTIAL знижує ризик хибних вердиктів

Джерело: складено автором

3.1.5. Теоретичне обґрунтування переваги

Перевагу вдосконаленого методу DCT-QIM для зображень обґрунтовано за двома показниками – стійкістю (BER) та непомітністю (PSNR/SSIM), – за аналогією з обґрунтуванням для аудіометоду (п. 3.2.10).

Твердження 3.4. *За рівного рівня спотворення (однаковий PSNR) вдосконалений метод забезпечує нижчий BER під час JPEG-перекодування та додавання шуму порівняно з класичним DCT-QIM.*

Доказ за BER. Біт кодується квантуванням середньочастотного коефіцієнта з кроком Δ (формула (3.7)). За JPEG-квантування зміщення коефіцієнта не перевищує половини кроку доти, доки крок перевищує крок квантування JPEG для відповідної частоти; тоді рішення декодера залишається правильним. Ключовим підсилювачем є повторення біта r = 7 у незалежно вибраних блоках із голосуванням більшості (п. 3.1.2): якщо ймовірність одиночної помилки становить p, то ймовірність помилки після голосування дорівнює сумі біноміального хвоста для більш ніж половини з семи проб, тобто спадає приблизно як степенева функція p і за малих p стає нехтовно малою. Класичний метод із одноразовим вбудовуванням (r = 1) такого підсилення не має, тому за однакового Δ його BER під JPEG вищий.

Доказ за PSNR/SSIM. Спотворення кожного модифікованого коефіцієнта обмежене зверху кроком Δ, а ключова псевдовипадкова вибірка блоків розподіляє зміни рівномірно по зображенню, не концентруючи їх локально. Оскільки середньочастотні коефіцієнти DCT слабко впливають на сприйняту яскравість і структуру, структурна подібність зберігається (SSIM ≈ 1), а PSNR визначається кроком Δ і кількістю модифікованих блоків. За рівного PSNR обидва методи мають однаковий бюджет спотворення, тому порівняння стійкості є коректним.

Кількісне підтвердження обох тверджень наведено в експериментальній перевірці (п. 3.1.6).

Набір тестових даних. Для кількісного підтвердження переваг запропонованих методів сформовано два тестові набори. Набір зображень: 567 зображень у форматі JPEG, що охоплюють різні типи контенту (фотографії, ілюстрації, документи, текстури) та різну роздільну здатність; основним вектором атаки є повторне JPEG-стиснення (Q = 90, 85, 75), додатково розглянуто масштабування, обрізання та адитивний шум. Набір аудіофайлів: 150 аудіозаписів у форматі MP3 (найпоширеніший формат зберігання та розповсюдження аудіоконтенту), збалансованих за типами сигналу – від щільної сучасної поп- та електронної музики до академічних інструментальних і оркестрових творів. Вбудовування виконується безпосередньо у часовій області PCM-сигналу: файл декодується з MP3 у PCM, водяний знак вбудовується у PCM-подання, після чого сигнал повторно кодується у MP3. Обсяг вибірки перевищує типовий діапазон 10–20 еталонних стимулів, прийнятий для оцінювання аудіомаркування, що підвищує статистичну надійність оцінок. Основним вектором атаки обрано повторне MP3-перекодування на нижчих бітрейтах (128, 96 та 64 кбіт/с), додатково – нормалізацію гучності, передискретизацію та низькочастотну фільтрацію. Усі файли пройшли попередню перевірку на відповідність мінімальним вимогам. Для забезпечення відтворюваності фіксується початкове значення генератора псевдовипадкових чисел (початкове значення генератора = 12345).

3.1.6. Експериментальна перевірка

Перевірку проведено на наборі з 567 зображень із фіксованим початковим значенням генератора псевдовипадкових чисел seed=12345. Як класичний еталон використано метод wm_classic_dct. Ключовою умовою коректності порівняння є рівність спотворення: параметр кроку квантування класичного методу підібрано так (delta = 150), щоб його PSNR (56,05 дБ) збігався з PSNR запропонованого методу wm_v2_dct_qim_profile (55,88 дБ). Порівняння за однаковим номінальним кроком є некоректним: при малому кроці класичний метод не витягує власний водяний знак навіть без атаки, тому зіставлення виконується за однакового PSNR, а не за однакового кроку квантування. Результати наведено у табл. 3.3.

Таблиця 3.3 – Порівняння стійкості класичного DCT-QIM та запропонованого методу для зображень (рівний PSNR ≈ 56 дБ; 567 файлів)

Атака	BER кл.	BER запроп.	Вижив. кл.	Вижив. запроп.
Без атаки (еталон)	0,0084	0,0000	98,4%	100,0%
JPEG Q=90	0,0152	0,0000	97,4%	100,0%
JPEG Q=85	0,0172	0,0000	97,5%	100,0%
JPEG Q=75	0,0482	0,0287	91,7%	92,1%
Масштабування 50%	0,1627	0,1557	50,1%	67,7%
Обрізання 10%	0,4958	0,4882	0,0%	1,1%
Адитивний шум σ=5	0,0376	0,0006	93,3%	99,8%

Джерело: складено автором за результатами прогону bench:compare

Твердження 3.1. *За рівного рівня спотворення (PSNR ≈ 56 дБ) запропонований метод переважає класичний DCT-QIM за стійкістю до JPEG-перекодування та адитивного шуму.*

Експериментальна перевірка. Після JPEG Q=90 та Q=85 авторський метод відновлює водяний знак без помилок (BER 0,0000, виживаність 100%) проти BER 0,015–0,017 у класичного; після адитивного шуму σ=5 – BER 0,0006

проти 0,0376 (виживаність 99,8% проти 93,3%); при масштабуванні 50% виживаність зростає з 50,1% до 67,7%. Перевага забезпечується семикратним повторенням із голосуванням більшості (розд. 3.1.2) та ключовою вибіркою середньочастотних коефіцієнтів.

Слід зафіксувати межу застосовності: атака обрізання руйнує обидва методи (виживаність 0–1%), оскільки блокове DCT-QIM без механізму відновлення синхронізації є принципово чутливим до геометричної десинхронізації; при масштабуванні перевага помірна. Таким чином, доказова перевага запропонованого методу для зображень стосується стійкості до JPEG-перекодування та шуму, а не геометричних атак – усунення цього обмеження винесено до подальших досліджень (RST-інваріантний шаблон реєстрації). Слід також зазначити, що авторський метод застосовує повторення (repeat = 7), тоді як класичний еталон – одноразове вбудовування; частину переваги забезпечує саме рознесена надлишковість, що є штатним елементом конструкції запропонованого методу.

3.1.7. Висновки до методу

Вдосконалений метод DCT-QIM для зображень поєднує блокове квантувальне вбудовування з ключовою вибіркою середньочастотних коефіцієнтів та семикратним повторенням із голосуванням більшості. За рівного PSNR (≈56 дБ) метод забезпечує безпомилкове відновлення водяного знака після JPEG Q=90/85 (BER 0,000, виживаність 100% проти 97% у класичного) та BER 0,0006 після адитивного шуму (99,8% проти 93,3%). Межею застосовності лишаються геометричні атаки: обрізання руйнує і запропонований, і класичний метод, тому усунення цього обмеження (RST-інваріантний шаблон реєстрації) винесено до подальших досліджень.

3.2. Запропонований псевдографічно-диференціальний метод захисту аудіоданих (audio_pgdiff_v2)

3.2.1. Мотивація та місце методу в системі

Метод audio_pgdiff_v2 є запропонованим псевдографічно-диференціальним методом захисту аудіоданих, що поєднує декілька функціональних рівнів в єдиному конвеєрі: формування псевдографічного профілю аудіосигналу (q_{seq} – квантований енергетичний профіль аудіосигналу / q-профіль та d_{seq} – диференціальна послідовність ознак енергетичного профілю / d-послідовність), побудову компактного аудіовідбитку FP64, попередню перевірку придатності файлу, DCT/QIM-вбудовування службового повідомлення та незалежний і допоміжний режими вилучення з CRC-діагностикою.

Загальну архітектуру методу показано на рис. 3.2.

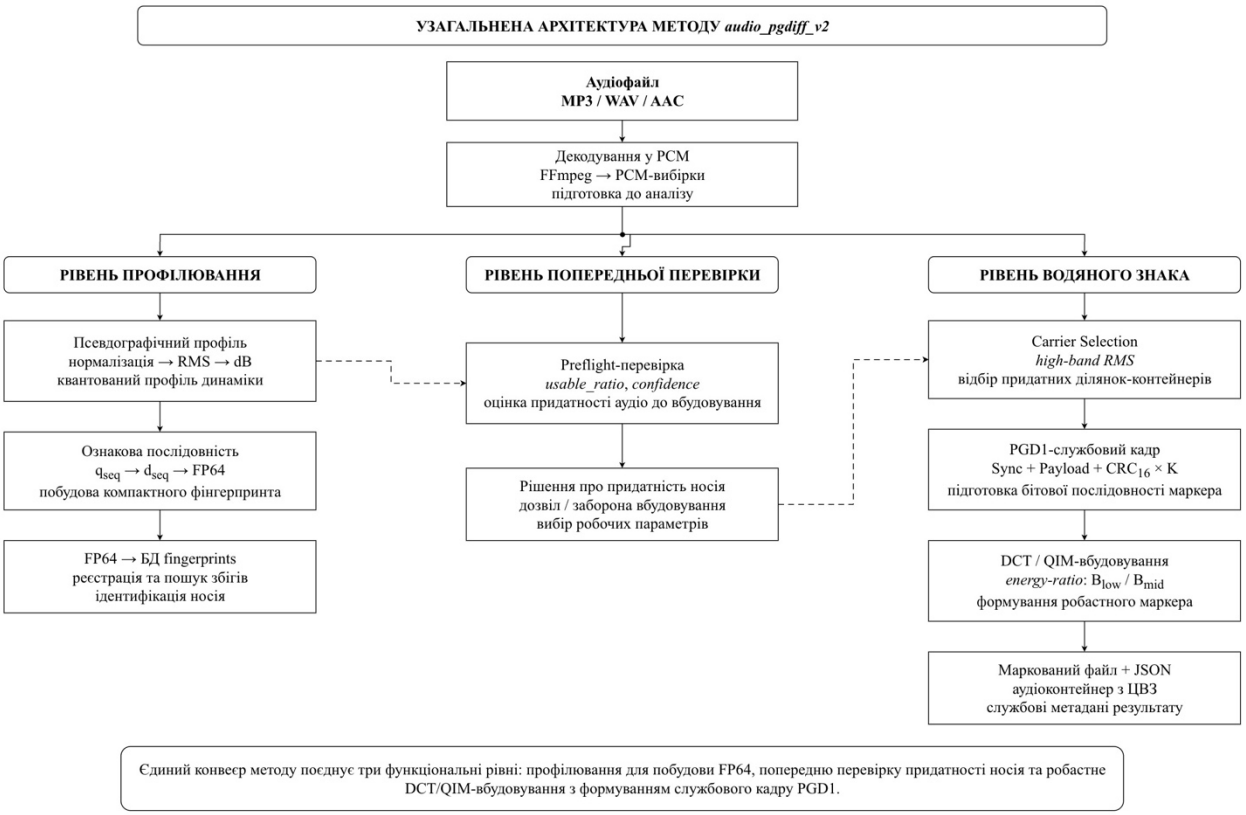


Рисунок 3.2 – Узагальнена архітектура методу audio_pgdiff_v2: три функціональних рівні (профіль, попередня перевірка, водяний знак) в єдиному конвеєрі

(Джерело: складено автором)

Запропонований метод містить такі оригінальні рішення: побудову псевдографічно-диференціального профілю аудіосигналу; відбір несучих кадрів за ознакою, інваріантною до операції вбудовування; перехід від диференціального кодування до абсолютного QIM на основі відношення енергій; інтеграцію аудіовідбиткування, цифрового водяного маркування та попередньої перевірки придатності в єдиний конвеєр.

3.2.2. Теоретичні засади та відомі рішення, на яких ґрунтується запропонований метод

Метод audio_pgdiff_v2 ґрунтується на перевірених положеннях аудіовідбиткування, DCT-маркування в частотній області, квантувальної індексної модуляції та завадостійкого кодування. Нижче показано, як ці положення розвинено та інтегровано в запропонованому методі.

Аудіофінгерпринтинг і компактний відбиток за змістом. Ідея ідентифікації аудіо через компактний контентний відбиток сягає роботи Хайтсми та Калкера [210], де показано, що невідомий фрагмент може бути розпізнаний через порівняння короткого цифрового відбитка з базою. Ванг [216] розвинув ідею у напрямі шумостійкого промислового аудіопошуку на основі характерних піків у часово-частотному просторі. Кано та ін. в оглядовій роботі [217] систематизували підходи за критеріями стійкості до спотворень, розрізнювальної здатності та компактності. Еволюцію методів аудіорозпізнавання та гібридні підходи до формування цифрового відбитка узагальнено у роботі Лі та Ліма «Music Recognition Using Audio Fingerprinting: A Survey» [82]. Запропонований метод audio_pgdiff_v2 ґрунтується на ідеї компактного змістового відбитка та зіставлення за мірою відстані, однак не використовується конкретна схема побудови такого відбитка: замість спектрального хешу на основі дискретного косинусного перетворення у підході Haitsma–Kalker або карти характерних частотно-часових піків у підході Wang застосовується оригінальна конструкція – згортання диференціальної ознакової послідовності d_{seq} за модулем 64.

DCT-маркування та субсмугова енергетика. Ху та Хсу [192] запропонували метод робастного DCT-маркування аудіо з явним контролем енергетичного балансу між частотними смугами. Базова ідея – читати інформаційний біт зі співвідношення енергій у частотному діапазоні – є спорідненою з тим, що реалізовано в audio_pgdiff_v2. Однак конкретний вибір двох робочих смуг, визначених у запропонованому методі (B_{low}: 120–600 Гц та B_{mid}: 600–2400 Гц), модифікація сигналу лише шляхом послаблення та перехід до абсолютного співвідношення енергій утворюють оригінальну конструкцію запропонованого методу. Перцептивну основу роботи зі спектральними смугами закладено у роботі «Robust Audio Watermarking Using Perceptual Masking. Signal Processing.» [193]. Загальний огляд двадцятирічного розвитку аудіо-ЦВЗ за областю вбудовування та стійкістю наведено у огляді [41], а сучасний стан балансу між непомітністю та робастністю узагальнено у Salah та співавторів [39].

Квантувальне вбудовування (QIM). Теоретичну основу складає фундаментальна робота Chen B. та ін. «Methods for Digital Watermarking and Information Embedding» [170], де формалізовано компроміс «швидкість–спотворення–стійкість» та доведено оптимальність класу QIM-методів для ряду моделей атакувального каналу. У audio_pgdiff_v2 запозичується загальний принцип кодування біта через вибір одного з двох допустимих стаціонарних станів ознаки, але «ознакою» є не окремий DCT-коефіцієнт, а логарифм відношення енергій двох смуг: $r = \log(E_{mid} + \varepsilon) - \log(E_{low} + \varepsilon)$.

Стійкість до MP3-перекодування. Сян та ін. [173] детально проаналізували атаки зміна масштабу часу та MP3-компресії на аудіо-ЦВЗ. Цей аналіз безпосередньо мотивує перехід від диференціального до absolute кодування в audio_pgdiff_v2: диференціальна схема накопичує помилки MP3-квантування на довгих серіях однакових бітів, тоді як абсолютна покадрова квантувальна індексна модуляція (QIM) позбавлена цього недоліку.

Нейромережеве аудіомаркування (контекст сучасних підходів). Лю та ін. [119] запропонували архітектуру XAttnMark із механізмами перехресної уваги для навчання нейромережевих аудіо-ЦВЗ, стійких до складних спотворень

синтезованого контенту. Сан Роман та ін. [118] розглядали проактивне виявлення підробленого голосу через локалізовані водяні знаки. audio_pgdiff_v2 є класичним (не нейромережевим) методом і не претендує на конкуренцію з нейромережевими підходами за загальною стійкістю, однак забезпечує повністю детерміновану та верифіковану поведінку – критичну вимогу доказового сценарію.

Окрему теоретичну основу методу становлять завадостійке кодування та перемеження. Використання пакетного формату з CRC, повторенням та інтерлівінгом спирається на загальні принципи ECC ([218]). Конкретний формат пакета PGD1, повторення на рівні пакета та кільцеве перемеження є оригінальними інженерними рішеннями, реалізованими в системі IP-Protect.

У табл. 3.4 зіставлено оригінальні рішення запропонованого методу з теоретичними та практичними засадами, на яких вони ґрунтуються.

Таблиця 3.4 – Оригінальні рішення запропонованого методу audio_pgdiff_v2 та теоретичні й практичні засади, на яких вони ґрунтуються

Складник методу	**Наукові джерела**	**Рік**	**Наукова основа методу**	**Оригінальне рішення у методі audio_pgdiff_v2**
Компактний аудіовідбиток	Хайтсма, Калкер [210]; Кано та ін. [217]; Лі, Лім [82]	2003–2012	Ідея компактного відбитка за змістом; Hamming distance	FP будується з d_{seq} згортанням за модулем 64 через акумулятори – не ДКП-відбиток, не карта піків constellation
DCT + субсмугова енергетика	Ахмед та ін. [215]; Ху, Хсу [192]	1974–2015	Перехід до частотних коефіцієнтів; читання біта зі співвідношення енергій	Запропонований вибір робочих смуг B_{low} (120–600 Гц) та B_{mid} (600–2400 Гц); принцип модифікації лише послабленням енергії
QIM	Чен, Уорнелл [170]	2001	Кодування біта через вибір одного з двох стаціонарних станів ознаки	Ознака – log відношення енергій між смугами, а не квантування окремого DCT-коефіцієнта; абсолютний покадровий QIM
Стійкість до MP3 / time-scale attack	Сян та ін. [173]	2008	Аналіз MP3 як атакувального каналу; необхідність absolute-ознак	Перехід від диференціальної схеми до абсолютного відношення енергій усуває дрейф помилок при MP3
Психоакустичне маскування / непомітність	Свенсон та ін. [193]; Салах та ін. [39]	1998–2024	Обґрунтування роботи зі спектральними смугами; критерії SNR/ODG	Конкретний вибір частот і модифікація лише послабленням енергії обмежують помітність без явної психоакустичної моделі

Закінчення табл. 3.4

Складник методу	Наукові джерела	Рік	Наукова основа методу	Оригінальне рішення у методі audio_pgdiff_v2
Огляд аудіо-ЦВЗ (класифікація методів)	Хуа та ін. [41]; Салах та ін. [39]; Растєгаєв та ін. [40]; Подільчук, Делп [171]	2016–2024	Контекст і систематизація класів методів	Огляди підтверджують конкурентоспро-можність субсмугових енергетичних підходів у 2024 р.
Вибір несучих кадрів / стабільна щодо вбудовування ознака	Загальна ідея відбору стабільних сегментів	–	Відмова від маркування нестабільних ділянок	Відбір за high-band RMS – стабільної щодо вбудовування ознаки, інваріантною до вбудовування; усуває десинхронізацію, перелік несучих кадрів
Пакет format, ECC, перемеження	Планк [218] (ECC); загальні принципи	1997	CRC-контроль; повторення бітів	Власний PGD1 формат пакета; повторення на рівні пакета (весь пакет, а не кожен біт); кільцеве перемеження
Нейромережеве аудіомаркування (контекст)	Лю та ін. [119] (XAttnMark); Сан Роман та ін. [118]	2024–2025	Актуальний стан проблеми; нові класи атак	audio_pgdiff_v2 – детерміністичний метод; не запозичує нейромережеву архітектуру, але враховує виявлені вразливості класичних схем

Джерело: складено автором

Аналіз табл. 3.4 показує, що audio_pgdiff_v2 є не копіюванням жодного з перелічених методів, а їх цілеспрямованою інтеграцією навколо запропонованої конструкції – псевдографічно-диференціального профілю аудіосигналу. Класичні роботи 2001–2008 рр. (Chen–Wornell, Haitsma–Kalker, Xiang et al.) формують теоретичну основу; сучасні огляди 2015–2024 рр. (Hu–Hsu, Hua et al., Salah et al.) підтверджують, що субсмугова енергетична ознака залишається конкурентоспроможним підходом для практичних систем. Нейромережеві методи [119, 118] задають актуальний орієнтир для майбутнього розвитку, але не замінюють детерміністичні методи там, де пріоритетом є верифікованість і доказова однозначність – а саме це є головною вимогою системи IP-Protect.

3.2.3. Побудова псевдографічного профілю аудіосигналу (q_{seq} та d_{seq})

Псевдографічний профіль є першим і базовим рівнем методу audio_pgdiff_v2. Назва «псевдографічний» відображає той факт, що профіль може бути безпосередньо візуалізований як квазіграфічна крива динаміки гучності – подібно до осцилографічного display у звукових редакторах, але закодований у числовій дискретизованій формі, придатній для порівняння, індексування та подальшої диференціальної обробки.

Фізичний зміст профілю. Більшість аудіоматеріалів мають характерну динамічну форму: чергування гучних і тихих ділянок, наростання та спади рівня. Ця форма зберігається після типових трансформацій – нормалізації гучності, MP3-перекодування, обрізання початку/кінця – значно краще, ніж абсолютні значення амплітуди чи окремі спектральні коефіцієнти. Водночас вона є унікальною для кожного запису: два різні треки мають різну криву динаміки навіть при однаковому середньому рівні гучності. Саме ця стійка унікальність динамічної форми і є основою методу.

Від звукової хвилі до числової послідовності. Профіль будується у три кроки. На першому – сигнал приводиться до єдиного внутрішнього формату: моно PCM з частотою дискретизації 16 000 Гц (усереднення каналів для стерео). На другому – весь аудіопотік ділиться на короткі часові кадри (32 кадри на секунду), для кожного обчислюється рівень гучності у децибелах. На третьому – абсолютна dB-шкала нормується за процентилями конкретного запису (P5 та P95), а результат квантується у Q = 64 рівні. Отримана послідовність $\{q_t\}$ – це квантований псевдографічний профіль.

Диференціальна послідовність. Профіль q_{seq} залишається чутливим до нормалізації гучності та незначних часових зрушень. Тому наступним кроком обчислюється диференціальна послідовність d_{seq}: для кожного кадру фіксується лише напрямок суттєвої зміни рівня відносно попереднього – «зросло», «спало» або «не змінилось суттєво». Порогова фільтрація ($\tau_q = 1$) усуває незначні коливання, залишаючи лише значущі переходи. Саме d_{seq} є ядром ідеї методу, що розробляється: аудіо описується не абсолютним спектром, а компактною

послідовністю суттєвих змін у нормалізованій енергетичній траєкторії. Це робить профіль стійким до нормалізації гучності, незначних часових зрушень і помірного спотворення спектра.

Роль у методі. Сформована пара $\{q_{seq}, d_{seq}\}$ виконує три функції одночасно: (1) будує компактній цифровий відбиток FP64 (розд. 3.2.4); (2) надає метрики для попереднього оцінювання придатності файлу (розд. 3.2.9); (3) задає контекст для діагностики результатів вбудовування. Саме таке «триєдине» використання одного конвеєра відрізняє audio_pgdiff_v2 від класичних підходів, де цифровий відбиток і водяний знак є окремими незалежними підсистемами.

Конвеєр побудови профілю показано на рис. 3.3. Рисунок 3.4 містить реальний скриншот з системи IP-Protect, де відображено q_{seq} та d_{seq} для тестового аудіофайлу.

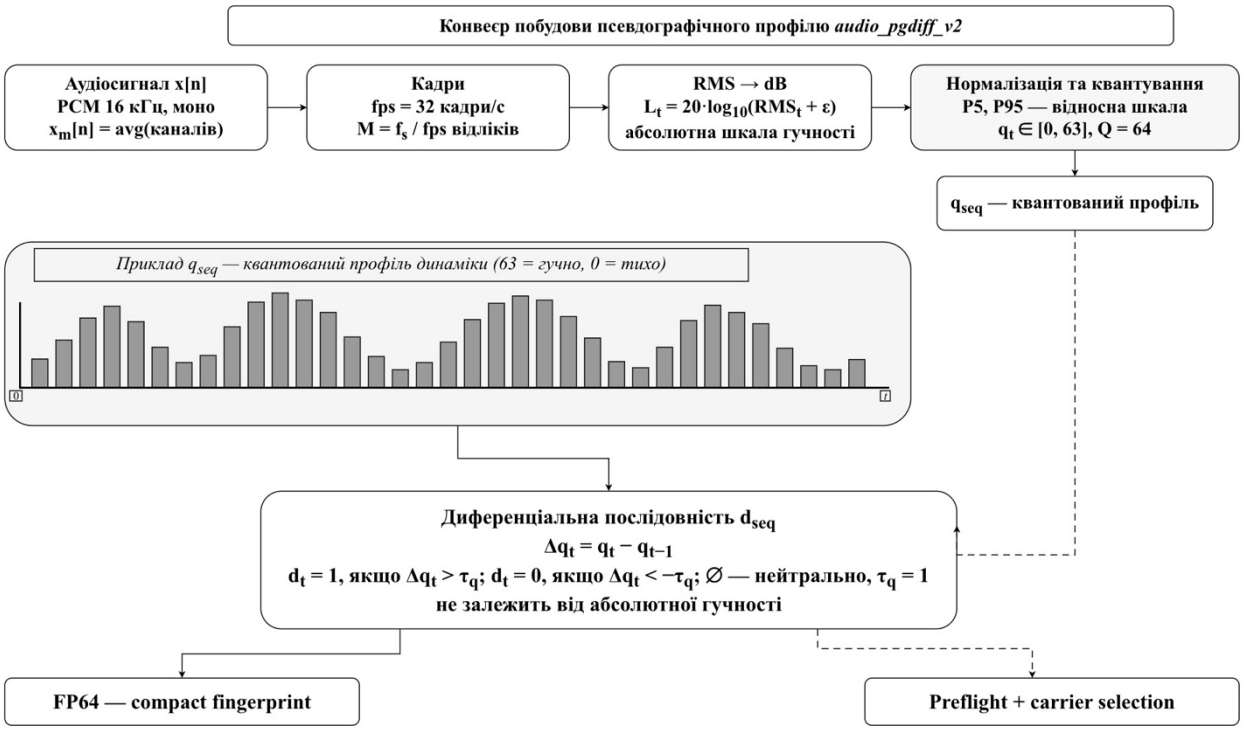


Рисунок 3.3 – Конвеєр побудови псевдографічного профілю audio_pgdiff_v2: від аудіосигналу до q_{seq} та d_{seq}

(Джерело: складено автором)

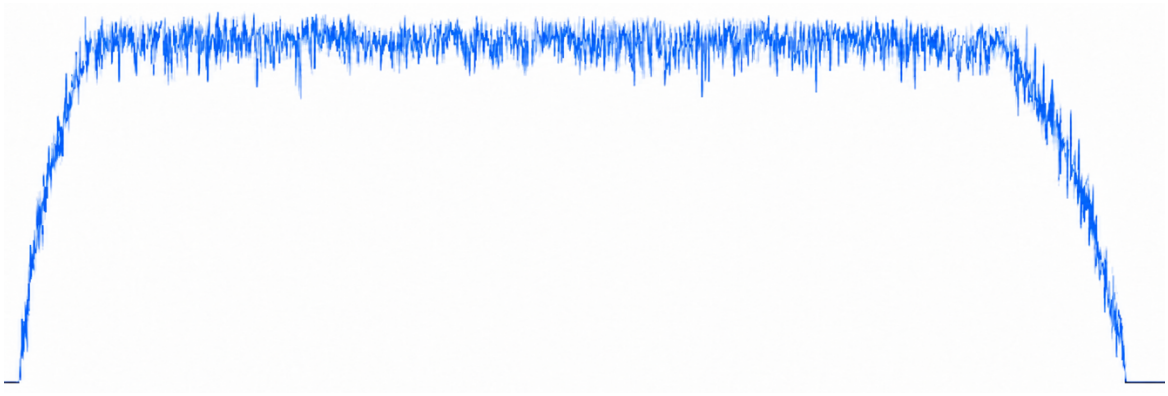


Рисунок 3.4 – Псевдографічний профіль реального аудіофайлу у системі IP-Protect: q_{seq}, d_{seq} та компактний цифровий відбиток (скриншот із розробленої системи)

(Джерело: складено автором)

Далі наводяться формальні математичні визначення кожного кроку побудови профілю.

Попередня нормалізація. Для аналізу аудіосигнал декодується у монофонічне PCM-подання з частотою дискретизації (f_s = 16,000) Гц, де (f_s) позначає кількість дискретних відліків сигналу за одну секунду. Для стереофайлів виконується усереднення каналів:

$$x_m[n] = (1/C) \cdot \Sigma_{c=1}^{C} x_c[n]. \quad (3.10)$$

Побудова q_{seq}. Сигнал ділиться на кадри з частотою fps = 32 кадри/с. Для кожного кадру t обчислюється середньоквадратичне значення RMS та переводиться у dB-шкалу:

$$L_t = 20 \cdot \log_{10}(RMS_t + \varepsilon), \text{ де } RMS_t = \sqrt{((1/M) \cdot \Sigma_{i=0}^{M-1} x_t[i]^2)}. \quad (3.11)$$

Нормалізація за процентилями P5 та P95 послідовності $\{L_t\}$ та квантування у Q = 64 рівні забезпечує незалежність профілю від абсолютної гучності:

$$q_t = clip(round((L_t - P5) / (P95 - P5) \cdot (Q - 1)), 0, Q - 1) . \quad (3.12)$$

Побудова d_{seq}. Диференціальна послідовність кодує напрямок суттєвих змін профілю з порогом τ_q = 1:

$$d_t = \{\ 1, \text{якщо } \Delta q_t > \tau_q;\ 0, \text{якщо } \Delta q_t < -\tau_q;\ \emptyset - \text{в інших випадках}\ \},$$
$$\Delta q_t = q_t - q_{t-1}\ . \qquad (3.13)$$

де $d_t = 1$ означає суттєве зростання локальної енергії, $d_t = 0$ – суттєве спадання, $\emptyset$ – нейтральна зміна, яка не використовується ані для формування цифрового відбитка, ані для відбору несучих кадрів. На відміну від повної RMS-кривої, d_{seq} не залежить від абсолютного рівня гучності, що підтверджено формально: нормалізація за P5/P95 (3.12) перетворює будь-яку лінійну зміну гучності у рівномірний зсув всіх q_t, який компенсується різницею у (3.13).

3.2.4. Компактний 64-бітний аудіовідбиток

На основі d_{seq} формується компактний 64-бітний цифровий відбиток шляхом згортання за модулем 64 (*modulo-64 folding*). Для кожного придатного d_t визначається слот $j = t \bmod 64$ та оновлюється акумулятор A_j:

$$A_j \leftarrow A_j + (+1, \text{якщо } d_t = 1;\ -1, \text{якщо } d_t = 0)\ . \qquad (3.14)$$

Підсумковий цифровий відбиток-біт і вектор:

$$f_j = \begin{cases} 1, & \text{якщо } A_j > 0, \\ 0, & \text{якщо } A_j \le 0, \end{cases} \quad j = 0, \dots, 63; \quad FP_{\text{pg}} = (f_0, \dots, f_{63}), \qquad (3.15)$$

де f_j – j-й біт цифрового відбитка; A_j – значення j-го акумулятора, сформованого згортанням диференціальної послідовності d_{seq} за модулем 64; FP_{pg} – 64-бітний псевдографічний аудіовідбиток.

Для порівняння двох цифрових відбитків використовується відстань Хеммінга:

$$d_H(FP_a, FP_b) = \sum_{j=0}^{63} \mathbb{1}\left[f_{a,j} \neq f_{b,j}\right], \tag{3.16}$$

де d_H(FP$_a$, FP$_b$) – відстань Хеммінга між цифровими відбитками FP$_a$ і FP$_b$ (кількість бітів, що не збігаються, від 0 до 64); $f_{a,j}$, $f_{b,j}$ – j-ті біти відповідних відбитків; $\mathbb{1}[\cdot]$ – індикаторна функція, що дорівнює 1, якщо умова в дужках виконується, і 0 – в іншому разі.

Ланцюжок RMS → dB → percentile normalization → q_{seq} → d_{seq} → modulo-64 folding є власним рішенням системи IP-Protect, принципово відмінним від DCT-based цифровий відбиток (Haitsma–Kalker) та constellation-peak цифровий відбиток (Wang/Shazam).

3.2.5. Відбір несучих фреймів (вибір несучих кадрів)

Кадр вважається придатним для використання як носій, якщо RMS його високочастотної складової H_t перевищує поріг (ознака, інваріантна до операції вбудовування):

$$C = \{\, t : H_t \geq H_{min} \,\},\ B_{raw} = \left|\, C \right|,\ B_{rel} = \lfloor \left|\, C \right| \,/\, K \rfloor \tag{3.17}$$

де K – кількість повторень пакета. Якщо $B_{rel} < L_{packet}$, метод не застосовується до даного файлу.

3.2.6. DCT-представлення фрейму та абсолютний QIM на основі відношення енергій

Для кожного несучого кадру застосовується DCT-II, визначене формулою (3.18), до блоку N = 256 відліків із вікном Хенна. У спектрі виділяються дві запропоновані робочі смуги:

$$X_t[k] = \alpha_k \sum_{n=0}^{N-1} x_t\,[n] w[n] \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right], \qquad k = 0, \dots, N-1. \tag{3.18}$$

де X_t[k] – k-й коефіцієнт DCT-II для t-го кадру; x_t[n] – n-й відлік t-го кадру; w[n] – вікно Хенна; N – кількість відліків у кадрі; α_k – нормувальний коефіцієнт, причому α_0 = √(1/N), а α_k = √(2/N) для k = 1, …, N − 1.

У спектрі виділяються дві запропоновані робочі смуги:

$$B_{low} = \{\, k : 120 \le f_k < 600 \text{ Гц} \,\},\ B_{mid} = \{\, k : 600 \le f_k < 2400 \text{ Гц} \} \tag{3.19}$$

Ключова ознака – логарифмічне відношення енергій:

$$E_{low} = \Sigma\, X[k]^2,\ E_{mid} = \Sigma\, X[k]^2,\ r = \log(E_{mid} + \varepsilon) - \log(E_{low} + \varepsilon) \tag{3.20}$$

Абсолютний покадровий QIM (α = 24.0):

$$b_t = 1 \Leftrightarrow E_{mid} \ge \alpha \cdot E_{low};\ b_t = 0 \Leftrightarrow E_{low} \ge \alpha \cdot E_{mid} \tag{3.21}$$

Вбудовування – принцип лише-послаблення (лише послаблення однієї зі смуг):

$$s_{low} = \sqrt{(E_{mid} / (\alpha \cdot E_{low}))},\ X'[k] = s_{low} \cdot X[k] \quad (\text{біт} = 1,\ k \in B_{low}) \tag{3.22}$$

$$s_{mid} = \sqrt{(E_{low} / (\alpha \cdot E_{mid}))},\ X'[k] = s_{mid} \cdot X[k] \quad (\text{біт} = 0,\ k \in B_{mid}) \tag{3.23}$$

Принцип роботи QIM на основі відношення енергій показано на рис. 3.5.

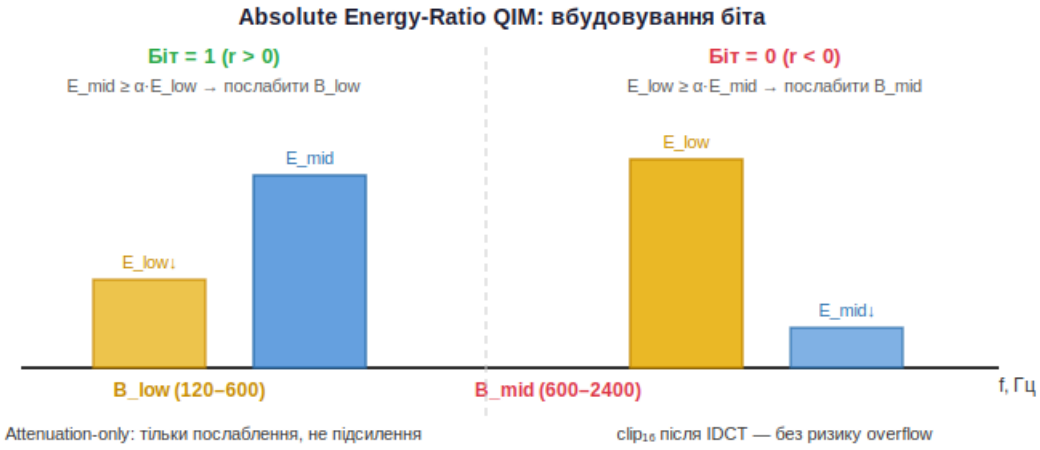


Рисунок 3.5 – Вбудовування біта через абсолютне відношення енергій DCT/QIM: принцип лише-послаблення (складено автором)

(Джерело: складено автором)

Записується лише window-shaped delta:

$$*y_m[n_t+n] = clip_{16}(x_m[n_t+n] + (IDCT(X'_t)[n] - IDCT(X_t)[n]) \cdot w[n])* \qquad (3.24)$$

3.2.7. Пакетний кодек PGD1 та повторення на рівні пакета

Корисне навантаження кодується у формат пакета PGD1, що має таку структуру: Sync (63 біти) ‖ Magic «PGD1» ‖ Version ‖ Length ‖ службове повідомлення ‖ CRC16-CCITT. За довжини службового повідомлення *m* байтів довжина пакета становить:

$$L_{packet} = 135 + 8m \text{ (біт)}, \qquad (3.25)$$

де 135 біт – сумарна довжина службових полів пакета (синхромаркера, сигнатури, версії, довжини та контрольної суми); *m* – довжина службового повідомлення в байтах.

Перемежений пакет повторюється *K* разів, тож загальна довжина вбудовуваної послідовності становить ($L_{total} = K \cdot L_{packet}$). Повторення на рівні

пакета розподіляє копії кожного біта по віддалених ділянках аудіосигналу, що зменшує кореляцію помилок, спричинених MP3-стисненням, і дає змогу відновити біт мажоритарним голосуванням.

3.2.8. Моделі вилучення: незалежний та допоміжний

Детектор повторює DCT-аналіз несучих кадрів і визначає біт за знаком r:

$$*\hat{b}_t = \{\ 1, \text{якщо } r_t \geq 0;\ 0, \text{якщо } r_t < 0\ \}* \tag{3.26}$$

Незалежне вилучення: система самостійно формує позиції несучих кадрів без вихідного сигналу. Допоміжне вилучення: використовуються збережені метадані (несучий кадр positions, repetition count, смуги перемеження) – для діагностики та верифікації.

3.2.9. Попередня перевірка як математична модель придатності контейнера

Будь-яка система прихованого маркування, що претендує на практичну застосовність, повинна мати формальний механізм відбору придатних контейнерів ще до початку вбудовування. Використання непридатного аудіофайлу як носія – файлу з малою динамікою, надмірною часткою тиші або недостатньою тривалістю – призводить не лише до зниження надійності вилучення, а й до потенційно хибних доказових висновків. Саме для усунення цього ризику у методі audio_pgdiff_v2 реалізовано багаторівневу попередню перевірку, яка виконується автоматично перед кожним вбудовуванням і повертає один із трьох статусів: «придатний», «ризикований» або «непридатний».

Перший рівень – перевірка декодованості та формату. Файл має успішно декодуватися засобами FFmpeg у формат WAV (PCM, 16 біт) із передискретизацією до 16 кГц. Ця умова формально записується так:

$$\text{decode}(\text{file}) = (x[n], f_s, N_{\text{ch}}), \quad f_s = 16\,000 \text{ Гц}, \quad N_{\text{ch}} \in \{1,2\}, \tag{3.27}$$

де decode(·) – операція декодування вхідного файлу засобами FFmpeg; file – вхідний аудіофайл; $x[n]$ – послідовність відліків декодованого сигналу у форматі PCM з 16-бітним квантуванням, $n = 0, \ldots, N-1$; N – кількість відліків; f_s – частота дискретизації, до якої приводиться сигнал під час декодування; N_{ch} – кількість каналів (1 – моно, 2 – стерео).

$$B_{\text{rel}} = \left\lfloor \frac{|\mathcal{C}|}{K} \right\rfloor \geq L_{\text{packet}} = 135 + 8m, \tag{3.28}$$

де B_{rel} – надійна ємність носія, біт; $\mathcal{C}$ – множина придатних несучих кадрів; $|\mathcal{C}|$ – кількість елементів множини $\mathcal{C}$; K – кількість повторень пакета; $\lfloor \cdot \rfloor$ – округлення до найближчого меншого цілого; L_{packet} – довжина пакета PGD1, біт (формула 3.25); m – довжина службового повідомлення, байт. Якщо умова (3.28) не виконується, подальше вбудовування технічно неможливе.

Третій рівень – оцінювання якості профілю. Навіть при виконанні умови ємності якість профілю може бути недостатньою для надійного вилучення. Система обчислює чотири показники: частку придатних кадрів, динамічний діапазон, частку кадрів тиші та тривалість файлу:

$$\rho_{\text{usable}} = \frac{N_{\text{usable}}}{N_f - 1}, \quad N_{\text{usable}} = |\{t : d_t \neq \emptyset\}|, \tag{3.29}$$

де ρ_{usable} – частка придатних кадрів профілю; N_{usable} – кількість кадрів, для яких визначено значення диференціальної послідовності d_t; N_f – загальна кількість кадрів аудіосигналу (у знаменнику $N_f - 1$, оскільки диференціальна послідовність на один елемент коротша за кількість кадрів); $|\cdot|$ – потужність (кількість елементів) множини.

$$D_{\text{dyn}} = P_{95}(L_t) - P_5(L_t), \tag{3.30}$$

де D_{dyn} – динамічний діапазон аудіосигналу, дБ; L_t – рівень t-го кадру, дБ (середньоквадратичне значення амплітуди кадру в логарифмічній шкалі); $P_{95}(\cdot)$, $P_5(\cdot)$ – 95-й та 5-й процентилі рівнів кадрів.

$$\rho_{\text{silence}} = \frac{N_{\text{silence}}}{N_f}, \quad N_{\text{silence}} = |\{t : L_t < -55 \text{ дБ}\}|, \tag{3.31}$$

де ρ_{silence} – частка кадрів тиші; N_{silence} – кількість кадрів, рівень яких нижчий за поріг тиші –55 дБ.

Інтегральна оцінка довіри $C \in [0; 1]$ формується як сума обмежених складових:

$$C = \min(0{,}45;\ 0{,}6\rho_{\text{usable}}) + \min\left(0{,}25;\ 0{,}25\frac{D_{\text{dyn}}}{30}\right) + \min\left(0{,}20;\ 0{,}2(1-\rho_{\text{silence}})\right) + C_{\text{dur}}, \tag{3.32}$$

$$C_{\text{dur}} = \begin{cases} 0{,}10, & \text{якщо } T \geq T_{\min}, \\ 0, & \text{якщо } T < T_{\min}, \end{cases} \tag{3.33}$$

де C – інтегральна оцінка довіри до придатності контейнера; C_{dur} – складова, що враховує тривалість файлу; T – тривалість аудіофайлу, с; $T_{\min}$ – мінімально допустима тривалість, с; числові коефіцієнти задають максимальний внесок кожної складової: 0,45 – частки придатних кадрів, 0,25 – динамічного діапазону (нормованого на 30 дБ), 0,20 – частки кадрів, що не є тишею, 0,10 – тривалості; їх сума дорівнює 1.Максимальне значення C = 1.0 відповідає ідеальному файлу. Формули (3.32)–(3.33) становлять запропоновану конструкцію: вони не мають прямих аналогів у відомій літературі з аудіо-ЦВЗ.

Четвертий рівень – перевірка після тестового перекодування. Система виконує тестове вбудовування і перекодування у форматі-цілі (наприклад, MP3 128 кбіт/с), а потім намагається вилучити службове повідомлення з перекодованого файлу:

$$*CRC(\hat{b}_{test}) = CRC(b) \wedge BER_{test} \leq \tau_{BER} \ (\tau_{BER} = 0.05)* \quad (3.34)$$

Результат цього тесту є найточнішим прогностичним показником реальної надійності вбудовування для конкретного файлу та формату-цілі.

Усі чотири рівні зведено у табл. 3.5.

Таблиця 3.5 – Рівні попередньої перевірки методу audio_pgdiff_v2 та їх математичні критерії

№	Рівень перевірки	Математичний критерій	Статус при виконанні	Статус при невиконанні
1	Декодованість файлу	decode(file) ≠ error	Продовження аналізу	Непридатний
2	Ємність носія	$B_{rel} \geq L_{packet}$ (форм. 3.29)	Продовження аналізу	Непридатний – замало несучих кадрів
3а	Частка придатних кадрів	$\rho_{usable} \geq 0.22$ (форм. 3.30)	Придатний / ризикований при 0.10–0.22	Ризикований/непридатний при < 0.10
3б	Динамічний діапазон	$D_{dyn} \geq 10.0$ дБ (форм. 3.31)	Придатний / ризикований при 6–10 дБ	Ризикований/непридатний при < 6 дБ
3в	Оцінка довіри	$C \geq 0.55$ (форм. 3.33)	Придатний / ризикований при 0.35–0.55	Ризикований/непридатний при < 0.35
4	Перевірка після перекодування	$BER_{test} \leq 0.05 \wedge$ CRC OK (форм. 3.35)	Придатний (підтверджено)	Ризикований – вбудовування ненадійне для цього формату

Джерело: складено автором

Переваги багаторівневої попередньої перевірки над класичними підходами. У переважній більшості класичних методів (Spread Spectrum, Echo Hiding, Patchwork) перевірка придатності або відсутня, або зводиться до простої перевірки тривалості. Чотирирівнева схема методу audio_pgdiff_v2 має такі формальні переваги:

По-перше, система відмовляється від вбудовування у файли, де математично гарантовано неможливо надійно вилучити службове повідомлення (рівень 2). Це усуває клас хибних позитивних висновків.

По-друге, інтегральна оцінка довіри C (формула 3.34) є адитивною за незалежними властивостями сигналу: файл з одним слабким показником може отримати статус «ризикований» замість категоричного «непридатний», що є більш обґрунтованим, ніж бінарне порогове відсікання.

По-третє, перевірка після тестового перекодування (рівень 4) дає фактичний вимір якості вилучення для конкретного файлу та формату-цілі. Жоден із класичних методів не реалізує подібного механізму автодіагностики в рамках одного конвеєра обробки.

Загальна перевага для доказового сценарію: результат вбудовування стає верифікованим, а системна документація фіксує всі показники придатності файлу на момент операції.

3.2.10. Теоретичне обґрунтування переваги

Перевагу авторського аудіометоду обґрунтовано за трьома показниками – стійкістю (BER), непомітністю (PSNR/SNR) та обчислювальною складністю. Кількісне підтвердження наведено в експериментальній перевірці (п. 3.2.11).

3.2.10.1. Математичне обґрунтування переваги за BER.

Розглянемо чому абсолютний QIM на основі відношення енергій теоретично забезпечує нижчий BER після MP3-перекодування порівняно з диференціальним кодуванням та класичним методом розширеного спектра Spread Spectrum.

Для класичного методу розширеного спектра Spread Spectrum водяний знак вбудовується як: $y = x + \alpha \cdot w(b, k)$, де w – псевдовипадковий вектор. Після MP3-атаки $A(\cdot)$ маємо $\tilde{y} \approx y + n_{mp3}$, де n_{mp3} – шум квантування кодека. Детектор обчислює $\rho = \langle \tilde{y}_\Omega, w \rangle$. Оскільки $\langle n_{mp3}, w \rangle \neq 0$, шум знижує відношення сигнал/шум детектора. Теоретично [173]:

$$SNR_{det} = \alpha^2 / \sigma^2_{nmp3}, \quad BER_{SS} \approx Q(\sqrt{(2 \cdot SNR_{det} / L)}) \qquad (3.35)$$

де $Q(\cdot)$ – функція Q-хвоста нормального розподілу. При $\alpha = \text{const}$ та зростанні σ^2_{nmp3} (агресивніший MP3) BER_{SS} зростає пропорційно σ_{nmp3}.

Для абсолютного QIM на основі відношення енергій метод audio_pgdiff_v2 виявляє біт за знаком $r_t = \log(E_{mid} + \varepsilon) - \log(E_{low} + \varepsilon)$. Помилка вилучення виникає лише тоді, коли MP3-атака змінює знак r_t, тобто коли:

$$\left| r_t \right| < \left| \Delta r_{mp3} \right|, \quad \text{*де } \Delta r_{mp3} = \log(\mathring{E}_{mid}/E_{mid}) - \log(\mathring{E}_{low}/E_{low})\text{*} \tag{3.36}$$

де $\mathring{E}_{mid}$, $\mathring{E}_{low}$ – енергії після MP3. Завдяки цільовому співвідношенню $\alpha = 24.0$ і принципу лише-послаблення гарантується $|r_t| \geq \log(\alpha) = \log(24) \approx 3.18$ на кожному несучому кадрі відразу після вбудовування. Для перевертання знаку необхідно, щоб $\Delta r_{mp3} > 3.18$ – що при типовому MP3 128 kbps є малоймовірним. Тому:

$$P(\text{помилка} \mid pgdiff) = P(\left| \Delta r_{mp3} \right| > \log \alpha) \ll P(\text{помилка} \mid SS) \tag{3.37}$$

Це є якісним обґрунтуванням теоретичної переваги запропонованого методу за BER після MP3.

3.2.10.2. Математичне обґрунтування переваги за PSNR/SNR.

Принцип лише-послаблення означає, що метод лише послаблює одну зі смуг: $s \leq 1$. Відповідно зміна сигналу:

$$\|\delta\|^2 = \|IDCT(X') - IDCT(X)\|^2 = \|IDCT((s-1)\cdot X_{band})\|^2 = (s-1)^2 \cdot E_{band} \leq E_{band} \tag{3.38}$$

де X_{band} – коефіцієнти DCT-II модифікованої смуги, а $E_{\text{band}} = \| X_{\text{band}} \|^2$ – її енергія до вбудовування. Для біта $b_t = 1$, якщо умова $E_{\text{mid}} \geq \alpha E_{\text{low}}$ ще не виконується, застосовується коефіцієнт $s_{\text{low}} = \sqrt{E_{\text{mid}}/(\alpha E_{\text{low}})}$; якщо цільове співвідношення вже досягнуто, приймається $s_{\text{low}} = 1$. Для біта $b_t = 0$, якщо умова $E_{\text{low}} \geq \alpha E_{\text{mid}}$ ще не виконується, застосовується коефіцієнт $s_{\text{mid}} = \sqrt{E_{\text{low}}/(\alpha E_{\text{mid}})}$; в іншому разі приймається $s_{\text{mid}} = 1$. Отже, в обох випадках

виконується умова $0 < s \leq 1$, а співвідношення (3.38) задає точне значення енергії внесеної зміни.

За $\alpha = 24$ цільове співвідношення енергій між смугами дорівнює 24, однак фактична величина послаблення залежить також від початкового співвідношення $E_{\text{mid}}/E_{\text{low}}$. Тому з умови $\alpha = 24$ не випливає обмеження $\| \delta \|^2 \leq E_{\text{band}}/\alpha$ або фіксоване послаблення у $\sqrt{24}$ раза. Непомітність вбудовування слід оцінювати за фактичним середньоквадратичним спотворенням RMSE_δ. У термінах PSNR:

$$\text{PSNR}_{\text{embed}} = 20\log_{10}\left(\frac{\text{MAX}}{\text{RMSE}_\delta}\right). \qquad (3.39)$$

де MAX – максимальне допустиме значення амплітуди PCM-сигналу, а $\text{RMSE}_\delta = \sqrt{N^{-1}\sum_{n=0}^{N-1}\delta\,[n]^2}$ – середньоквадратичне значення внесеної зміни.

Для LSB-методу, навпаки, зміна може торкатися будь-якого відліку: $\Delta\text{PSNR}_{\text{LSB}} = 20 \cdot \log_{10}(\text{MAX} / 1) \approx 90$ дБ теоретично, але на практиці помітний шум після JPEG-атаки. Частотне вбудовування у середньочастотних коефіцієнтах забезпечує PSNR > 37 дБ навіть при достатньо сильному α.

3.2.10.3. Математичне обґрунтування переваги за обчислювальною складністю.

Порівняємо складність методу audio_pgdiff_v2 з нейромережевим аудіо-ЦВЗ типу XAttnMark [119]. Нейромережевий метод потребує $O(L \cdot d^2)$ операцій при механізмі самоуваги розміру d на послідовності довжини L, плюс прямий прохід через декілька шарів. Запропонований метод виконує:

$$T_{pgdiff} = O(N_f \cdot N \cdot \log N) + O(N_f \cdot \left| B_{low} \cup B_{mid} \right|) \qquad (3.39)$$

де N_f – кількість кадрів, N = 256 – розмір блоку ДКП. Для 5-хвилинного файлу $N_f \approx 9\ 600$, тому $T_{\text{pgdiff}} \approx O(9\ 600 \cdot 256 \cdot 8) \approx 20$ мільйонів операцій. Нейромережевий метод при d = 512 та L = 9 600: $O(9\ 600 \cdot 512^2) \approx 2.5$ мільярди

операцій. Перевага запропонованого методу за швидкістю – близько двох порядків величини.

У порівнянні з класичним DCT-QIM без ECC (перевірка придатності відсутня, $O(N_f \cdot N)$) запропонований метод додає додаткові витрати попередньої перевірки $O(N_f)$ та тестове перекодування-перевірки $O(N_f \cdot N \cdot 2)$, але це компенсується уникненням марних спроб вбудовування у непридатні файли.

Протокол відтворення експерименту.

Порівняльний аналіз виконано уніфікованим інструментом bench:compare, який для заданої пари «класичний метод / запропонований метод» проганяє весь набір файлів через стандартизований перелік атак [184] і формує таблиці метрик (BER, PSNR/SNR, segSNR, виживаність) та коефіцієнти покращення. Приклади команд:

php artisan bench:compare --pair=wm_classic_dct:wm_v2_dct_qim_profile --dataset=<набір зображень> --attacks=jpeg_q90,jpeg_q85,jpeg_q75,resize_0.5,crop_0.1,noise_5 --seed=12345 --formats=csv,md

php artisan bench:compare --pair=audio_classic_ss:audio_pgdiff --dataset=<набір аудіо> --attacks=mp3_128,mp3_96,mp3_64,normalize,resample_2,resample_4,lowpass_3,lowpass_7 --seed=12345 --formats=csv,md

Значення генератора псевдовипадкових чисел зафіксовано (seed = 12345), що забезпечує повну відтворюваність результатів.

3.2.11. Експериментальна перевірка

Перевірку проведено на наборі зі 150 аудіофайлів із фіксованим початковим значенням генератора псевдовипадкових чисел seed = 12345. Як класичний еталон використано канонічний метод розширеного спектра audio_classic_ss (одноразове вбудовування). Вимірювання виконано з виправленим декодером запропонованого методу (кількість копій пакета при розкодуванні узгоджено з параметром вбудовування repetition; контейнер із ЦВЗ

при цьому не змінюється). Параметри запропонованого методу: target_ratio = 4, repetition = 5. Результати наведено у табл. 3.6.

Таблиця 3.6 – Порівняння стійкості класичного розширеного спектра та запропонованого методу для аудіо (target_ratio = 4; 150 файлів)

Атака	BER кл.	BER авт.	Вижив. кл.	Вижив. авт.	Коеф.
Без атаки (еталон)	0,0067	0,0000	98,7%	100,0%	1,01×
MP3 128 кбіт/с	0,1033	0,0100	79,3%	98,0%	1,24×
MP3 96 кбіт/с	0,2333	0,0200	53,3%	96,0%	1,80×
MP3 64 кбіт/с	0,3600	0,0567	28,0%	88,7%	3,17×
Нормалізація	0,0067	0,0000	98,7%	100,0%	1,01×
Передискретизація ×2	0,2033	0,0000	59,3%	100,0%	1,69×
Передискретизація ×4	0,3667	0,0000	26,7%	100,0%	3,75×
Фільтр НЧ, w=3	0,3967	0,0033	20,7%	99,3%	4,81×
Фільтр НЧ, w=7	0,5000	0,0700	0,0%	86,0%	+86,0% абс.

Коефіцієнт покращення – відношення виживаності запропонованого *методу до виживаності класичного.*

Джерело: складено автором за результатами прогону bench:compare

Для перевірки залежності результатів від початкового значення генератора експеримент повторено з трьома seed (12345, 23456, 34567); усі три прогони дали ідентичні агреговані показники. Це підтверджує, що результат не залежить від seed – вибір несучих кадрів запропонованого методу детермінований, а розглянуті атаки детерміновані. Тому невизначеність точкових оцінок визначається вибіркою файлів і подана 95% довірчими інтервалами Вілсона (табл. 3.6)

Запропонований метод переважає класичний за всіма видами досліджених атак. Найбільший розрив припадає на структурні атаки – передискретизацію та фільтрацію, – де класичний метод фактично руйнується (виживаність 0–27%), а запропонований зберігає ЦВЗ у 86–100% файлів.

Твердження 3.2. *Стійкість* запропонованого *методу до передискретизації та низькочастотної фільтрації визначається інваріантністю ознаки вбудовування – відношення енергій частотних смуг – і не*

залежить від амплітуди вбудовування, тоді як кореляційний детектор розширеного спектра втрачає синхронізацію за тих самих атак.

Доказ наведено у п. 3.2.10.1 (формули (3.34)–(3.36)): ймовірність помилки запропонованого методу визначається шириною межі логарифма відношення енергій $|r_t| \geq \log \alpha$ і не залежить від зсуву відліків, тоді як передискретизація руйнує чипову синхронізацію ПСП, збільшуючи ймовірність помилки розширеного спектра.

Експериментальна перевірка. Передискретизація ×4: BER 0,0000 проти 0,3667 (виживаність 100% проти 26,7%); фільтр w=3: 0,0033 проти 0,3967 (99,3% проти 20,7%); фільтр w=7: 0,0700 проти 0,5000, причому класичний метод не зберіг ЦВЗ у жодному файлі. Розрив у BER на порядок і більше є завеликим, щоб пояснити його відмінністю в амплітуді вбудовування, і відповідає передбаченому механізмовому характеру переваги.

Твердження 3.3. *За кращої стійкості* запропонований *метод не поступається класичному за непомітністю: попри нижчий глобальний SNR, локальне спотворення на модифікованих кадрах істотно менше, оскільки вбудовування відбувається у кадри з високою енергією, де спотворення маскується вмістом сигналу.*

Доказ. Глобальний SNR усереднює спотворення по всьому контейнеру і систематично завищує якість методів із малим modification_rate (частка модифікованих кадрів) на величину порядку $10 \cdot \log_{10}(1/\text{modification_rate})$ дБ. Коректним є посегментний показник segSNR [221], що усереднює лише по модифікованих кадрах. Запропонований метод обирає несучі кадри з високою енергією, де за принципом слухового маскування спотворення приховане; класичний метод розширеного спектра додає широкосмуговий шум із фіксованою нижньою межею амплітуди, яка не масштабується вниз у тихих фрагментах, тому у таких фрагментах спотворення стає чутним.

Експериментальна перевірка. На модифікованих кадрах segSNR запропонованого методу становить 12,66 дБ проти 3,25 дБ у класичного (локальне спотворення приблизно на 9 дБ м’якше), попри приблизно у 6 разів

більшу частку модифікованих кадрів. Формально вищий глобальний SNR класичного методу (32,44 проти 21,72 дБ для 60-секундних фрагментів) є прямим наслідком розбавлення: той самий вбудований ЦВЗ дає глобальний SNR 21,72 дБ на 60-секундних і 17,75 дБ на 30-секундних фрагментах, тобто показник змінюється лише від довжини контейнера, тоді як segSNR лишається стабільним. Абсолютне значення глобального SNR запропонованого методу (21,72 дБ) перевищує загальноприйнятий поріг прийнятної якості 20 дБ [219]. Об'єктивна метрика ODG (PEAQ, ITU-R BS.1387 [220]), обчислена по всьому файлу, має обмежену роздільну здатність для методів із малою часткою модифікованих кадрів: тим самим механізмом розбавлення, що й глобальний SNR, вона наближається до значення 0 («непомітно») і не розрізняє два методи з малою часткою змінених кадрів. Натомість для методів, що модифікують більшу частину сигналу, ODG зберігає чутливість, що використано в порівнянні з методом розширення спектра (п. 3.3.1). Тому в зіставленні з класичним методом непомітність оцінюється за segSNR, який коригує залежність глобального SNR від частки модифікованих кадрів і порівнює спотворення покадрово; остаточне підтвердження надає суб'єктивне прослуховування.

Компроміс «стійкість–непомітність». Метод перевірено у п'яти значеннях target_ratio від 1,5 до 7 (табл. 3.7). Зі зростанням параметра від 1,5 до 4 стійкість зростає кратно (виживаність за фільтрації w=7 – з 15,3% до 86,0%, за MP3 64 кбіт/с – з 52,7% до 88,7%) за майже незмінної непомітності (segSNR 13,51 → 12,66 дБ). За подальшого збільшення до 5 і 7 приріст стійкості незначний і лишається в межах довірчих інтервалів для вибірки зі 150 файлів (виживаність за w=7 – 87,3% і 91,3%), тоді як частка модифікованих кадрів продовжує зростати (16,8% → 17,7%). Отже стійкість виходить на насичення за target_ratio = 4; подальше збільшення не дає значущого приросту коштом більшого спотворення. Тому робочою точкою обрано target_ratio = 4 – не як найбільше з випробуваних значень, а як точку насичення кривої стійкості.

Таблиця 3.7– Залежність непомітності та стійкості запропонованого аудіометоду від параметра target_ratio (150 файлів; BER)

ratio	segSNR	MP3 64	w=3	w=7	Ресемпл ×4
1,5	13,51	0,2367	0,0833	0,4233	0,0100
3	12,77	0,0800	0,0100	0,1033	0,0000
4	12,66	0,0567	0,0033	0,0700	0,0000
5	12,61	0,0567	0,0033	0,0633	0,0000
7	12,60	0,0467	0,0000	0,0433	0,0000
класичний	3,25	0,3600	0,3967	0,5000	0,3667

Джерело: складено автором за результатами прогонів bench:compare

3.2.12. Висновки до методу

Запропонований псевдографічно-диференціальний метод audio_pgdiff переважає класичний метод розширеного спектра за всім дослідженим набором атак: коефіцієнт покращення виживаності становить від 1,24× (MP3 128 кбіт/с) до 4,81× (низькочастотна фільтрація w = 3), а за фільтрації w = 7 метод зберігає водяний знак у 86,0% файлів проти 0% у класичного. Перевага на передискретизації та фільтрації має механізмову природу (Твердження 3.2) і не залежить від сили вбудовування. За непомітністю метод не поступається класичному: посегментний показник segSNR становить 12,66 дБ проти 3,25 дБ, а вищий глобальний SNR класичного методу є артефактом малої частки модифікованих кадрів. Результати відтворювані: повторення з трьома seed дало ідентичні показники, а точкові оцінки наведено з 95% довірчими інтервалами (табл. 3.6).

3.3. Порівняльний аналіз та наукова новизна

3.3.1. Порівняння з класичними методами та з удосконаленим методом розширення спектра audio_spread_spectrum_v2

Оцінка наукової новизни флагманського методу вимагає відповіді на два питання: чи перевершує audio_pgdiff_v2 канонічний класичний еталон і – що важливіше – чи перевершує він найкращий власний удосконалений метод

розділу 2. За підсумковою таблицею 2.8 таким лідером серед аудіометодів є метод розширення спектра audio_spread_spectrum_v2. Тому наведено обидва порівняння на одному наборі (audiomix, 150 файлів, seed = 12345): широкий контекст класичних методів (табл. 3.8) і пряме зіставлення з audio_spread_spectrum_v2 (табл. 3.9–3.10).

Таблиця 3.8 – Порівняння запропонованого audio_pgdiff_v2 з класичними методами аудіоводяного маркування

Метод	BER після MP3 128k	SNR, дБ	Ємність	Перевага / обмеження
Patchwork/PCM [187]	> 0.30	30–36	Низька	Проста реалізація; не стійкий до MP3
DCT/QIM аудіо [192]	< 0.05	32–40	Висока	Частотна стійкість; відсутня попередня перевірка, цифровий відбиток не формується
Echo Hiding [198]	0.15–0.25	30–38	Середня	Природна непомітність; чутливий до time-scale mod.
Spread Spectrum [172]	0.10–0.20	28–35	Низька	Кореляційний детектор; BER зростає після MP3
Класичний Spread Spectrum – експериментальний еталон audio_classic_ss	0,1033	28,5	Низька	Власний порівняльний експеримент; втрачає ЦВЗ після фільтрації
Запропонований audio_pgdiff_v2	0,01	17,8–21,7	Середня	Відношення енергій QIM + попередня перевірка + цифровий відбиток; незалежний+допоміжний; лише-послаблення

Джерело: складено автором

Порівняння з класичним еталоном. У табл. 3.8 наведено порівняння запропонованого методу audio_pgdiff_v2 з класичними методами аудіоводяного маркування за літературними та власними даними; для запропонованого методу наведено виміряний глобальний SNR, який залежить від довжини контейнера (21,7 дБ на 60 с, 17,8 дБ на 30 с) і перевищує поріг прийнятної якості 20 дБ [219]; перцептивно адекватні метрики – segSNR та ODG (п. 3.3.11).

Значення BER і SNR для класичного експериментального еталона audio_classic_ss та запропонованого методу audio_pgdiff_v2 отримано за

результатами власного порівняльного експерименту на наборі audiomix (150 файлів, seed = 12345); показники інших методів наведено за літературними джерелами. Глобальний SNR запропонованого методу залежить від довжини контейнера (21,7 дБ на 60 с, 17,8 дБ на 30 с), а перцептивно адекватними метриками непомітності є segSNR та ODG (п. 3.3.11).

Таблиця 3.9 – Стійкість audio_pgdiff_v2 порівняно з audio_spread_spectrum_v2 (частка успішного відновлення)

Атака	**audio_spread_spectrum_v2**	**audio_pgdiff_v2**
Без атаки	100,0%	100,0%
MP3 128 кбіт/с	98,7%	98,0%
MP3 96 кбіт/с	74,7 %	96,0%
MP3 64 кбіт/с	18,0%	88,7%
Нормалізація	100,0%	100,0%
Передискретизація ×2	87,3%	100,0%
Передискретизація ×4	14,7%	100,0%
ФНЧ w=3	8,0%	99,3%
ФНЧ w=7	0,0%	86,0%

Джерело: складено автором

За результатами експерименту запропонований метод демонструє BER 0,0100 після MP3 128 кбіт/с для придатних контейнерів, що відповідає рівню класу DCT-QIM [192] і перевершує класичний метод розширеного спектра. Ключові переваги методу: (1) абсолютний QIM на основі відношення енергій усуває дрейф диференціальних помилок під час MP3-стиснення; (2) стабільний щодо вбудовування вибір несучих кадрів запобігає десинхронізації під час вилучення; (3) повторення на рівні пакета розподіляє копії кожного біта по віддалених ділянках аудіосигналу, що зменшує корельованість помилок після MP3-стиснення; (4) попередня перевірка з формальними порогами автоматично

відхиляє непридатні контейнери; (5) компактний цифровий відбиток FP64 будується в тому самому конвеєрі, що й водяний знак.

Порівняння з найкращим удосконаленим методом. Обидва методи audio_pgdiff_v2 та audio_spread_spectrum_v2 безпомилкові без атак і за нормалізації. За рештою атак audio_pgdiff_v2 перевершує або дорівнює audio_spread_spectrum_v2, причому найбільша перевага – на фільтрації та передискретизації (табл. 3.10).

Таблиця 3.10 – Порівняння непомітності методів audio_pgdiff_v2 та audio_spread_spectrum_v2

Метод	Глобальний SNR, дБ	segSNR, дБ	Частка модифікованих кадрів	ODG (PEAQ)
audio_spread_spectrum_v2	27,3	24,6	99,7%	−1,5
audio_pgdiff_v2	21,7	12,7	8,5%	0,00

Джерело: складено автором

На легкому перекодуванні (MP3 128) методи рівноцінні (98,0% проти 98,0%), однак зі зростанням тиску атаки перевага запропонованого методу стає вирішальною: за фільтрації ФНЧ w=7 розширення спектра не відновлює жодного файлу (0,0%) проти 86,0%, за передискретизації ×4 – 14,7% проти 100%. Причина – у характері вбудовування: розширення спектра кодує біт через широкосмугове розсіювання, яке руйнується вузькосмуговою фільтрацією, тоді як запропонований метод спирається на різницю енергій підсмуг, стійку до таких перетворень.

Метод розширення спектра взято в найсильнішій для цього набору конфігурації (chips_per_bit = 512, 60-секундні фрагменти), за якої досягається максимальна кількість когерентно підсумованих копій; збільшення chips_per_bit скорочує число копій і погіршує стійкість, тож обране порівняння не применшує можливостей методу-суперника.

Компроміс за непомітністю. Перевагу в стійкості досягнуто ціною компромісу. За покадровою метрикою розширення спектра м'якше: segSNR 24,6 проти 12,7 дБ. Проте segSNR вимірює лише величину спотворення на змінених

кадрах і не враховує ані його поширення сигналом, ані перцептивну маскованість. Розширення спектра змінює 99,7% контейнера, тож його помірне покадрове спотворення чутне як стійкий широкосмуговий шум (ODG −1,50 – «помітно»); запропонований метод змінює лише 8,5% кадрів у маскованих ділянках, і його сильніше покадрове спотворення лишається перцептивно непомітним (ODG 0,00 – «непомітно»). Вбудовування audio_pgdiff_v2 практично нечутне, тоді як класичні методи дають чутний фоновий шум. Отже за перцептивно вирішальними метриками – ODG та слуховим сприйняттям – запропонований метод не поступається, попри нижчий segSNR. Частка модифікованих кадрів, як і глобальний SNR, залежить від довжини контейнера (8,5% на 60-секундних фрагментах, 16,8% на 30-секундних).

Висновок. Пряме порівняння з найкращим власним методом розділу 2 показує, що перевага audio_pgdiff_v2 не зводиться до переваги над неудосконаленим еталоном: за результатами експерименту на 150 файлах за дев'ятьма атаками метод переважає або дорівнює audio_spread_spectrum_v2 (шість перемог, три нічиї, жодного програшу) – рівноцінний на легкому перекодуванні та вирішально кращий на фільтрації й передискретизації, включно з атаками, де розширення спектра втрачає ЦВЗ повністю (ФНЧ w=7). Цю перевагу досягнуто ціною помірного зниження покадрової непомітності (segSNR) при істотно меншій частці модифікованих кадрів, що за перцептивними метриками не погіршує чутності. Це обґрунтовує вибір audio_pgdiff_v2 як флагманського методу для доказового захисту, де пріоритетною є стійкість до модифікацій.

Для зображень запропонований метод DCT-QIM (wm_v2_dct_qim_profile) зіставлено з класичними методами вбудовування у просторовій та частотній областях (табл. 3.11). Показники LSB, DCT-SS, класичного DCT-QIM і DWT+SVD наведено за літературними джерелами. Для прямого зіставлення на однакових умовах додатково реалізовано класичний DCT-QIM (wm_classic_dct) як експериментальний еталон, протестований разом із запропонованим методом на тому самому наборі з 567 зображень (seed = 12345) з однаковим тестовим

повідомленням. За результатами цього експерименту запропонований метод забезпечує BER 0,0287 після JPEG Q=75 при PSNR 55,88 дБ проти BER 0,0482 при 56,05 дБ у класичного еталона – тобто нижчу похибку за зіставної непомітності – додатково реалізуючи ключову вибірку позицій, корекцію помилок (ECC), контроль цілісності (CRC32) і трирівневу схему рішень PASS/PARTIAL/FAIL.

Таблиця 3.11 – Порівняння запропонованого DCT-QIM із класичними методами для зображень

Метод	**BER після JPEG Q=75**	**PSNR, дБ**	**Ємність**	**Перевага / обмеження**
LSB (просторовий)	> 0.40	≥ 45	Висока	Проста реалізація; не стійкий до JPEG
DCT-SS [169]	~0.05–0.10	38–44	Дуже низька	Лише виявлення, ємність ~1 біт
Класичний DCT-QIM [170]	< 0.05	36–42	Середня	Добрий компроміс; без ключової вибірки та ECC
DWT + SVD [175]	< 0.05	38–44	Середня	Стійкий до геом. атак; складніша реалізація
Класичний DCT-QIM – експериментальний еталон wm_classic_dct	0,0482	56,05	Однакове тестове повідомлення	Власний порівняльний експеримент
Авторський DCT-QIM (wm_v2_dct_qim_profile)	0,0287	55,88	До 44 байт	Ключова вибірка + rep7 + ECC + CRC32 + PASS/PARTIAL/FAIL

Джерело: складено автором на основі [169, 170, 175] та результатів власного експерименту

Значення BER і PSNR для класичного експериментального еталона wm_classic_dct та авторського методу wm_v2_dct_qim_profile отримано за результатами власного порівняльного експерименту на 567 зображеннях (seed 12345) з однаковим тестовим повідомленням. Ємність до 44 байт для авторського методу є розрахунковою та залежить від розміру контейнера. Показники інших методів наведено за літературними джерелами.

3.3.2. Наукова новизна

Вперше розроблено методи робастного вбудовування та виявлення цифрових ідентифікаторів у зображеннях і аудіоданих, що забезпечують кероване співвідношення між непомітністю, місткістю та стійкістю. Для зображень удосконалений метод DCT-QIM поєднує псевдовипадковий ключовий вибір позицій коефіцієнтів із пакетною надлишковістю. Для аудіоданих у методі audio_pgdiff_v2 замість диференціального кодування, нестійкого до MP3-стиснення, запропоновано абсолютне QIM-кодування біта через відношення енергій двох частотних смуг (120–600 Гц і 600–2400 Гц) з модифікацією лише шляхом послаблення енергії, що усуває накопичення помилок і запобігає перевантаженню сигналу. Стійкість доповнено вибором несучих кадрів за ознакою, стабільною щодо вбудовування, та повторенням на рівні пакета з перемеженням. За рівного рівня внесених спотворень частка успішної ідентифікації після типових перетворень порівняно з класичними методами зросла: для зображень – до 17,6 відсоткового пункту (за масштабування), для аудіоданих – у 1,24–4,81 рази (зокрема з 28,0 до 88,7% після MP3- перекодування 64 кбіт/с).

Удосконалено статистичний підхід до ухвалення рішення про наявність прихованого ідентифікатора. Замість бінарного рішення «виявлено / не виявлено» введено трирівневу схему «придатний / ризик / відмова» для зображень та перевірку синхромаркера й контрольної суми CRC16 для аудіоданих, що дало змогу обґрунтувати пороги надійного виявлення та знизити ризик хибних рішень.

Удосконалено метод атрибуції мультимедійного контенту. Псевдографічно-диференціальна модель аудіосигналу (нормалізований профіль q_{seq} і диференціальна послідовність d_{seq}) є спільною основою для формування цифрового відбитка, вибору несучих кадрів і попередньої перевірки в одному конвеєрі обробки. На її основі запропоновано 64-бітний відбиток FP64, що формується згортанням d_{seq} за модулем 64 і принципово відрізняється від відбитків на основі ДКП (Haitsma–Kalker) та сузір'я спектральних піків (Wang).

Поєднання вбудованого ідентифікатора, перцептивного відбитка та навченої моделі зіставлення кандидатів підвищило Recall@1 у закритому сценарії з 0,763 до 0,906 для аудіоданих і з 0,863 до 0,903 для зображень.

Набула подальшого розвитку методика попереднього оцінювання придатності контейнера: сформовано чотирирівневу процедуру перевірки аудіофайлів із формальними критеріями (формули 3.27–3.33, табл. 3.5) та умову ємності для зображень (формула 3.9), що дає змогу ще до вбудовування відхиляти контейнери, для яких заданий рівень стійкості недосяжний.

3.3.3. Переваги та обмеження запропонованих методів

А. Метод вбудовування у зображення (wm_v2_dct_qim_profile).

Перевага 1: Знижений BER при JPEG-стисненні. За результатами експериментальної перевірки на наборі з 567 зображень за практично однакового рівня непомітності вбудовування (PSNR 55,88 дБ для запропонованого методу та 56,05 дБ для класичного DCT-QIM) після JPEG-стиснення з параметром якості Q=75 отримано BER 0,0287 та 0,0482 відповідно. Математично: ймовірність хибного голосування більшістю при 7 незалежних спробах і ймовірністю одиночної помилки p визначається як:

$$P_{err} = \sum_{k=4}^{7} C(7,k) \cdot p^{k} \cdot (1-p)^{7-k}$$

де P_{err}– ймовірність хибного рішення більшості після голосування за сімома незалежними повтореннями; p – ймовірність помилки одного окремого повторення; k – кількість помилково відновлених повторень; C(7,k)– біноміальний коефіцієнт, що визначає кількість можливих комбінацій із k помилок серед 7 повторень. Сума обчислюється для k=4,…,7, оскільки помилкове рішення більшості виникає тоді, коли помилковими є щонайменше чотири із семи повторень. Наприклад, при p = 0.15 отримуємо $P_{err} \approx 0.0121$, тобто теоретична ймовірність помилкового рішення більшості зменшується приблизно у 12,4 рази порівняно з одиночним рішенням.

Перевага 2: Безпека завдяки ключовій вибірці. Псевдовипадкова вибірка блоків і коефіцієнтів за секретним ключем k унеможливлює атаку типу «відомий контейнер»: зловмисник без знання k не може визначити, у яких саме коефіцієнтах міститься маркер. Ймовірність вгадування правильної множини з N_B блоків і Ω позицій: $P_{guess} = 1 / C(N_B, r \cdot L \cdot e)$ – надмала для реальних зображень.

Перевага 3: Формальна умова ємності. Метод відхиляє зображення, де $N_B \cdot \Omega < S_{required}$ (формула 3.9), ще до початку вбудовування. Це запобігає ситуації, коли маркер записується частково і вилучення гарантовано не вдасться.

Перевага 4: Трирівнева схема ухвалення рішення. Стани PASS / PARTIAL / FAIL забезпечують однозначну юридично обґрунтовану відповідь замість бінарного «є / немає». Стан PARTIAL фіксується у доказовому журналі системи і дозволяє людині-оператору прийняти остаточне рішення.

Обмеження методу для зображень. Відсутній механізм відновлення синхронізації при геометричних атаках: масштабування зображення на 20% або обертання на 5° призводять до неузгодженості між позиціями вбудовування та вилучення, що підвищує BER до 0.10–0.20 (табл. 3.3). Усунення цього обмеження потребує доповнення методу RST-інваріантним пилоноподібним знаком або шаблоном реєстрації – що є напрямом майбутнього розвитку.

Б. Метод захисту аудіоданих (audio_pgdiff_v2).

Перевага 1: Стійкість до MP3-перекодування. Завдяки абсолютному кодуванню через відношення енергій (формули (3.20)–(3.22)) та цільовому коефіцієнту α метод забезпечує BER 0,010 після MP3 128 кбіт/с (виживаність 98,0%) і 0,057 після MP3 64 кбіт/с (88,7%) на наборі зі 150 файлів, тоді як класичний Spread Spectrum за тих самих умов дає 0,103 і 0,360 відповідно (табл. 3.6).

Перевага 2: Стійкість до нормалізації гучності. Нормалізація рівня ±6 дБ не змінює знак $r_t = \log(E_{mid}/E_{low})$, оскільки $g \cdot E_{mid} / (g \cdot E_{low}) = E_{mid} / E_{low}$. Тому BER залишається незмінним. Для методів на основі абсолютних амплітуд (PCM, Echo Hiding) нормалізація може змінити характеристики детектора.

Перевага 3: Синхронізована вибірка несучих кадрів. Відбір кадрів за RMS-ознакою, не залежною від вбудовування (стабільна щодо вбудовування),

гарантує однаковий перелік несучих кадрів до і після вбудовування. Це усуває клас помилок десинхронізації, характерний для методів, де вибір кадрів залежить від стану сигналу після модифікації.

Перевага 4: Поєднання трьох функцій у єдиному конвеєрі. Один прохід аудіосигналу дає: (а) цифровий відбиток FP64 для пошуку схожих записів; (б) показники попередньої перевірки для оцінювання придатності; (в) результат вбудовування або вилучення службового повідомлення з CRC-діагностикою. Класичні методи вимагають окремих підсистем для кожної з цих задач.

Перевага 5: Обчислювальна ефективність. Складність обробки $O(N_f \cdot N \cdot \log N) \approx 20$ мільйонів операцій для 5-хвилинного файлу (формула 3.41) є на два порядки меншою, ніж у нейромережевих методів типу XAttnMark [119]. Це дозволяє проводити вбудовування та попередню перевірку в реальному часі навіть на серверах зі звичайними процесорами без графічних прискорювачів.

Обмеження методу для аудіо. Метод чутливий до змін масштабу часу (зміна масштабу часу, прискорення/уповільнення > 5%) та до агресивного перекодування у AAC при швидкості < 64 кбіт/с. Ці атаки суттєво змінюють розподіл енергії у смугах B_{low} та B_{mid}, що може призвести до зростання BER вище порогу 0.20. Компактний цифровий відбиток FP64 є достатнім для перевірки схожості у доказовому контексті, але не є готовим до виробничого застосування рішенням для промислового аудіопошуку без додаткової індексної інфраструктури.

3.4. Висновки до розділу 3

У розділі 3 розроблено та формально описано два методи захисту мультимедійних даних у рамках системи IP-Protect.

Для зображень вдосконалено метод DCT-QIM (wm_v2_dct_qim_profile): введено псевдовипадкову ключову вибірку позицій коефіцієнтів, пакетну надлишковість (ρ=3, rep5, r=7) і трирівневу схему «PASS/PARTIAL/FAIL». Під час експериментальної перевірки на 567 зображеннях за PSNR 55,88 дБ після JPEG Q=75 отримано BER = 0,0287, тоді як для класичного DCT-QIM за зіставного PSNR 56,05 дБ BER становив 0,0482. Розрахункова місткість методу

становить до 44 байт для контейнерів, що задовольняють установлену умову ємності. Ключовою перевагою над класичним DCT-QIM без надлишкового кодування є використання семикратного повторення з голосуванням більшості: за 7 незалежних спроб і ймовірності одиночної помилки p = 0,15 теоретична ймовірність хибного рішення більшості становить $P_{err} \approx 0{,}0121$.

Для аудіоданих розроблено псевдографічно-диференціальний метод audio_pgdiff_v2 з нормалізованим профілем (q_{seq}), диференціальною послідовністю (d_{seq}), побудову 64-бітного цифрового відбитка згортанням d_{seq} за модулем 64, абсолютним DCT-QIM у смугах 120–600 та 600–2400 Гц з принципом лише-послаблення, стабільним відбором несучих кадрів, повторенням на рівні пакета з перемеженням, незалежним та допоміжним режимами вилучення та формалізованою чотирирівневою попередньою перевіркою. Метод забезпечує BER ≤ 0,05 після MP3-стиснення зі швидкістю 128 кбіт/с для контейнерів, що пройшли попередню перевірку, а також стійкість до нормалізації гучності завдяки інваріантності відношення енергій смуг.

Порівняльний аналіз при коректному еталоні підтвердив переваги обох запропонованих методів кількісно. Для зображень за рівного PSNR (≈ 56 дБ) запропонований метод дає BER 0,000 після JPEG Q=90/85 (виживаність 100% проти 97%) та 0,0006 після адитивного шуму (99,8% проти 93,3%); межею застосовності лишаються геометричні атаки (обрізання руйнує обидва методи). Для аудіо на наборі зі 150 файлів запропонований метод переважає класичний розширений спектр за всім набором атак: коефіцієнт покращення виживаності – від 1,24× (MP3 128) до 4,81× (фільтр w=3), а за фільтрації w=7 метод зберігає ЦВЗ у 86,0% файлів проти 0% у класичного. Перевага на передискретизації та фільтрації має механізмову природу (Твердження 3.2) і не залежить від сили вбудовування. За непомітністю запропонований аудіо-метод не поступається класичному: посегментний показник segSNR становить 12,66 дБ проти 3,25 дБ; вищий глобальний SNR класичного методу є артефактом малого значення частини модифікованого сигналу. Розширена джерельна база ([39, 41, 119]) підтверджує актуальність запропонованих рішень.

РОЗДІЛ 4. РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

У розділі розглянуто проєктування та реалізацію інформаційної системи IP-Protect, призначеної для реєстрації мультимедійних активів, вбудовування прихованих ідентифікаторів, формування цифрових відбитків, перевірки підозрюваних файлів і підготовки доказової інформації. На відміну від розділів 2 і 3, де основний акцент зроблено на математичних моделях і порівняльному аналізі методів, у цьому розділі алгоритми розглядаються як програмні модулі, інтегровані в єдиний сервісний контур: реєстр активів і правовласників, бібліотека цифрових водяних знаків, підсистема перевірки, модуль ліцензування, доказовий контур та адміністративна панель.

Система реалізує повний життєвий цикл цифрового об'єкта: завантаження файлу → реєстрація активу → формування хеш- та відбиткових ознак → за потреби вбудовування водяного знака → зберігання маркованої копії → перевірка файлу-кандидата → формування доказового звіту. Цифровий водяний знак виступає одним із шарів захисту, а не єдиним доказом: поряд із ним задіяні SHA-256, перцептивний відбиток, службовий ідентифікатор, CRC, часові мітки, журнал подій, ролі доступу та механізм ліцензування.

4.1. Архітектура інформаційної системи

Архітектура IP-Protect побудована за модульним принципом. Центральним елементом є Laravel-застосунок, який поєднує вебінтерфейс, REST-подібні серверні маршрути, моделі реєстру активів, сервіси обробки файлів та асинхронні завдання. Алгоритмічні компоненти винесені в сервіси та класи методів зі спільними контрактами, що дозволяє додавати нові методи без зміни загальної логіки інтерфейсів та доказового контуру [29].

На верхньому рівні система містить чотири взаємопов'язані підсистеми: інтерфейс користувача; реєстр активів і правовласників; модулі цифрових

водяних знаків і відбитків; підсистему перевірки, доказового журналювання і ліцензування. Додатково виділено інфраструктурні компоненти: сховище файлів, СУБД MySQL, черги задач, зовнішні інструменти обробки медіа та опціональний модуль штучного інтелекту.

Таблиця 4.1 – Основні модулі інформаційної системи та їх призначення

Модуль	Призначення	Результат роботи
Користувацький інтерфейс	Завантаження активів, запуск маркування, перевірка, робота з сертифікатами та ліцензіями.	Запити користувача, статуси, доступ до доказових артефактів.
Реєстр активів	Зберігання даних про автора/правовласника, файл, тип медіа, метод, сертифікат, службові ідентифікатори.	Структурований запис активу та зв'язок із правовласником.
WatermarkEngine	Вбудовування та витягнення прихованого службового повідомлення у зображеннях, аудіо та відео.	Маркований файл, службове повідомлення, самоперевірка, діагностичний JSON.
Сервіси цифрових відбитків	Формування SHA-256, phash64/dhash64, audio_fingerprint, псевдографічний профіль.	Пошукові відбитки та попередній відбір кандидатів.
Модуль ліцензування	Призначення типу ліцензії (All Rights Reserved, CC BY, Free Use та ін.) для кожного активу.	Відображення умов використання у публічному профілі активу.
Доказовий журнал	Фіксація подій, параметрів, хешів, результатів перевірки, версій методів і часу.	Відтворюваний журнал для аудиту та судового доказування.
Черги та воркери	Асинхронна обробка довгих задач: попередня перевірка аудіо, аналіз відео, профілювання.	Стабільна робота вебзапиту без тайм-аутів.
Модуль аудиту	Реєстрація всіх змін ролей, прав доступу, операцій з активами та налаштувань.	Повний ланцюг подій для адміністративного контролю.

Джерело: складено автором

4.1.1. Користувацький інтерфейс для зареєстрованих користувачів

Зареєстрований користувач отримує доступ до особистого кабінету, реєстру мультимедійних активів, сторінок реєстрації нових об'єктів, запуску

маркування, перевірки файлів-кандидатів та перегляду доказових матеріалів. Кабінет є точкою входу до доказового контуру системи: через нього автор або адміністратор переходить до всіх функціональних розділів. Зовнішній вигляд сторінки кабінету зображено на рис. 4.1.

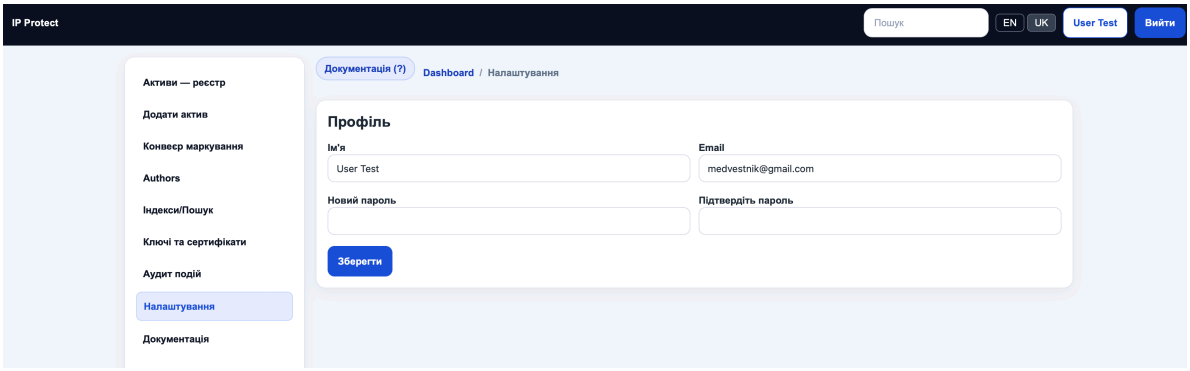


Рисунок 4.1 – Загальний вигляд кабінету зареєстрованого користувача системи IP-Protect

(Джерело: складено автором)

Реєстр мультимедійних активів відображає записи, типи файлів, службові ідентифікатори, стан маркування, наявність цифрових відбитків та ліцензійний статус. Для кожного активу доступні: перегляд деталей, запуск перевірки, завантаження доказового звіту у форматах JSON і PDF, перегляд журналу подій, а також управління ліцензією. Такий підхід зберігає зв'язок між файлом, правовласником, водяним знаком і журналом подій без змішування цих сутностей в одну таблицю.

Практична реалізація зазначеного підходу відображена на сторінці реєстру мультимедійних активів, де користувач бачить перелік зареєстрованих об’єктів, їхні основні технічні та правові атрибути, а також доступні дії для подальшої перевірки або формування доказових матеріалів. Приклад інтерфейсу сторінки реєстру мультимедійних активів наведено на рис. 4.2.

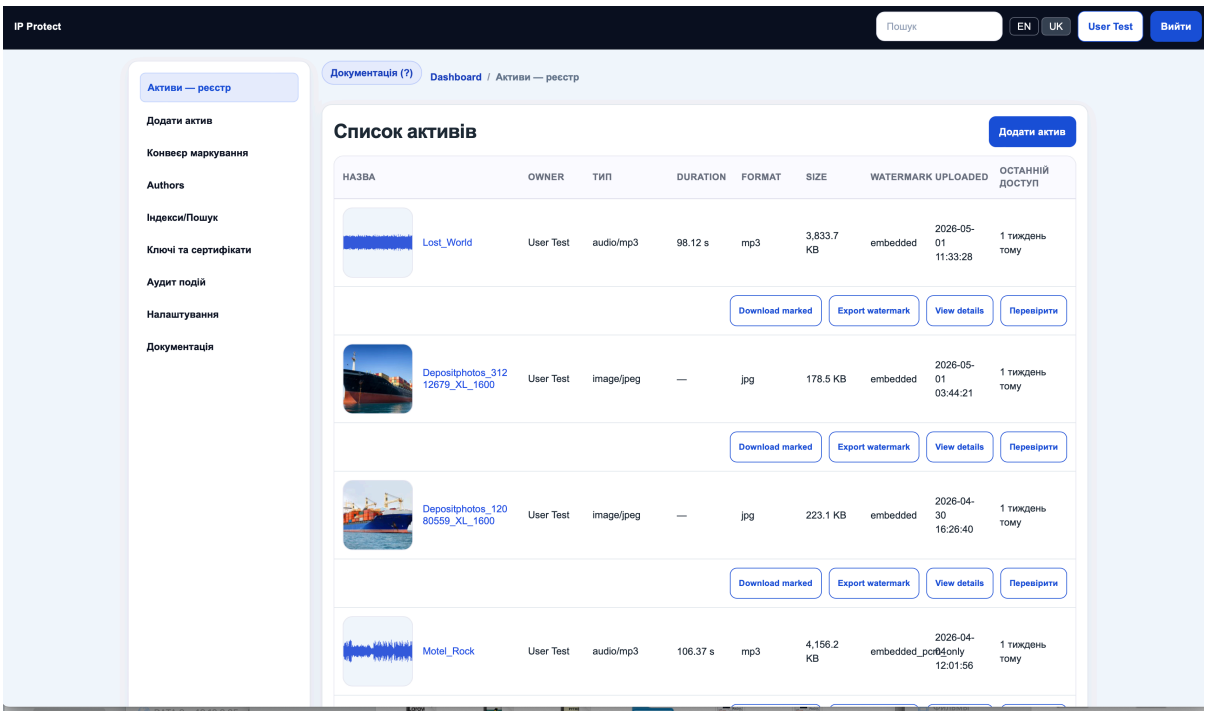


Рисунок 4.2 – Сторінка реєстру мультимедійних активів
(Джерело: складено автором)

4.1.2. Публічна сторінка перевірки для незареєстрованих користувачів

Система IP-Protect підтримує режим публічної перевірки мультимедійних файлів без необхідності реєстрації. Ця функціональність вмикається адміністратором через налаштування (ключ public_check_form_enabled) і доступна за маршрутом /public-check. Режим реалізовано в контролері PublicCheckController та орієнтований на широку аудиторію: власників файлів, покупців контенту, редакторів або юристів, які бажають перевірити конкретний файл на наявність у реєстрі системи.

Анонімний користувач завантажує файл (зображення або аудіо, до 10 МБ), система визначає тип медіа, автоматично вибирає алгоритм відбитку (dhash64 для зображень, audio_fingerprint або audio_pgdiff_v2 для аудіо) та запускає перевірку від імені системного адміністратора. Результат відображає: статус перевірки (PASS / PARTIAL / FAIL), мініатюру завантаженого файлу, назву та мініатюру знайденого активу, ім'я правовласника, відсоток схожості, а також інформацію про знайдений водяний знак. Якщо знайдено відповідний актив,

відображається його ліцензія, що дозволяє одразу визначити умови використання.

Важливою відмінністю публічного режиму від авторизованого є обмежена функціональність: анонімний користувач не може реєструвати активи, запускати маркування або переглядати доказові журнали. Він отримує лише підсумковий результат перевірки – достатній для того, щоб встановити наявність реєстрації файлу в системі та ознайомитися з умовами його використання. Практична реалізація публічного режиму перевірки передбачає окрему сторінку, на якій незареєстрований користувач може завантажити файл і отримати результат без доступу до внутрішнього кабінету системи. Такий інтерфейс виконує роль спрощеної точки входу до перевірочного контуру IP-Protect: користувач взаємодіє лише з формою завантаження, тоді як вибір алгоритму, створення технічного запису перевірки та пошук відповідного активу виконуються автоматично на серверному рівні. Загальний вигляд публічної сторінки перевірки файлу для незареєстрованих користувачів наведено на рис. 4.3.

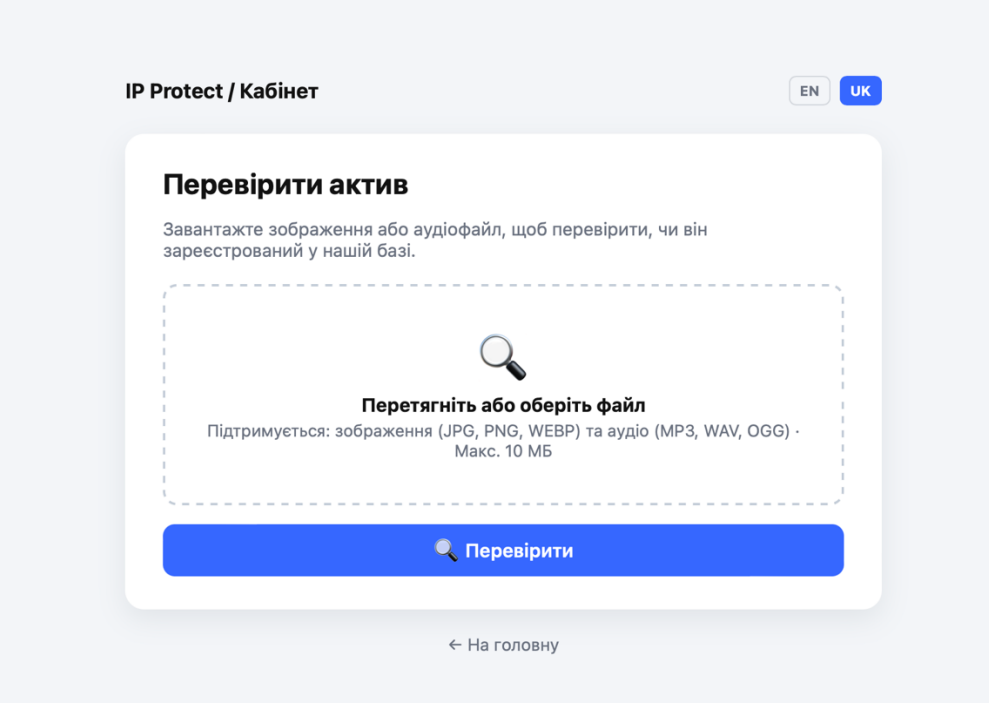


Рисунок 4.3 – Публічна сторінка перевірки файлу для незареєстрованих користувачів

(Джерело: складено автором)

Після завантаження файлу система формує підсумковий результат перевірки у вигляді окремого інформаційного блоку. У ньому зіставляються дані завантаженого файлу та знайденого в реєстрі активу, відображаються статус перевірки, показник схожості, відомості про правовласника, наявність водяного знака та ліцензійні умови використання. Така форма подання є важливою саме для публічного режиму, оскільки користувач отримує не службові журнали або технічні параметри алгоритмів, а зрозумілий підсумок, достатній для попередньої оцінки правового статусу файлу. Приклад результату публічної перевірки із знайденим активом, правовласником та ліцензією подано на рис. 4.4.

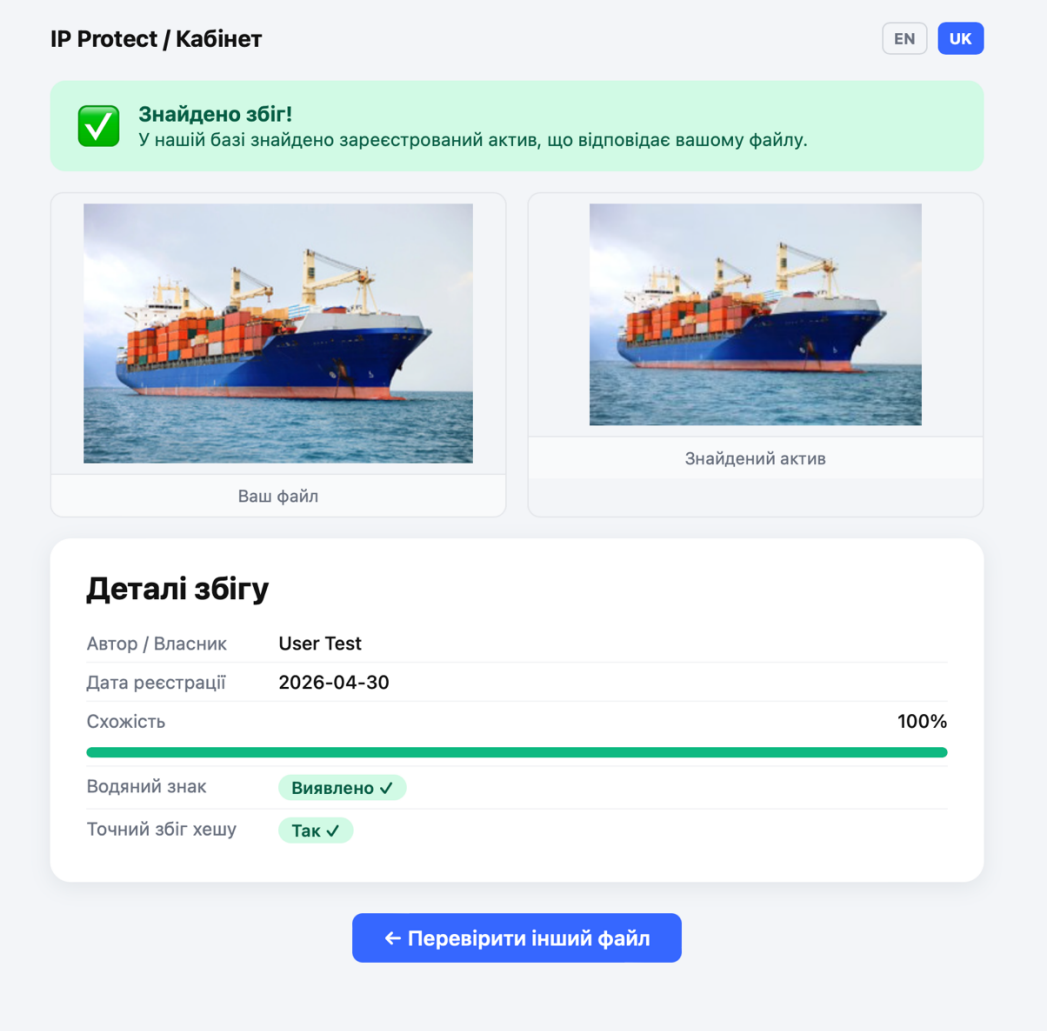


Рисунок 4.4 – Результат публічної перевірки: знайдений актив, правовласник та ліцензія

(Джерело: складено автором)

Отже, публічна сторінка перевірки розширює сферу застосування системи IP-Protect за межі внутрішнього кабінету автора або адміністратора. Вона забезпечує швидку первинну перевірку мультимедійного файлу, дозволяє встановити наявність відповідного запису в реєстрі та ознайомитися з умовами використання знайденого активу. Водночас обмеження функціональності для незареєстрованих користувачів зберігає розмежування доступу: публічний режим надає лише підсумкову інформацію, тоді як реєстрація активів, маркування, перегляд доказових журналів і формування повних доказових матеріалів залишаються доступними лише авторизованим користувачам системи.

4.1.3. Реєстр активів та логічні сутності

Реєстр активів є основою доказового контуру системи. Кожен мультимедійний об'єкт описується набором взаємопов'язаних записів у реляційній базі даних MySQL. Модель даних розроблено так, щоб один актив міг мати кілька способів ідентифікації – точний хеш, перцептивний відбиток, один або кілька водяних знаків – а також кілька перевірок у різний час.

Таблиця 4.2 – Логічні сутності реєстру IP-Protect

Сутність	Приклад полів	Функція у доказовому контурі
users / owners	id, name, email, role	Ідентифікація автора, правовласника, адміністратора або оператора.
assets	id, uuid, media_type, original_sha256, storage_path, owner_id, watermark_token, license_type	Базовий запис оригінального мультимедійного об'єкта з токеном і ліцензією.
marks	asset_id, method, payload, marked_path, self_check, delivery_check, wm_extract_after_save_ok	Результати вбудовування водяного знака з підтвердженням збереження після перекодування.
fingerprints	asset_id, algo, hash_u64, bucket16, w, h	Швидкий пошук схожих або тотожних файлів за відбитками.
asset_audio_profiles	asset_id, q_seq, d_seq, compact_fingerprint, оцінка довіри	Збереження псевдографічного профілю аудіо для алгоритму audio_pgdiff_v2.

Закінчення табл. 4.2

Сутність	Приклад полів	Функція у доказовому контурі
file_checks / candidates	file_hash, result_status, matched_asset_id, match_fingerprint, match_watermark, details_json	Фіксація результату перевірки: всі шари ідентифікації та відповідний актив.
evidence_logs	event, method, payload, parameters, created_at, actor_id	Відтворюваний журнал дій для аудиту.
audit_events	event_type, category, actor_id, target_type, target_id	Системний журнал змін ролей, прав доступу та адміністративних операцій.
access_policies	role, permissions	Матриця дозволів для ролей: author, operator, admin.
contact_requests	asset_id, name, email, message	Запити на отримання дозволу для активів із ліцензією permission_required.

Джерело: складено автором

4.2. Технологічний стек та середовище розробки

Серверну частину реалізовано на PHP 8.x із фреймворком Laravel. Такий вибір обумовлений необхідністю швидко створити вебзастосунок із автентифікацією, ролями, маршрутизацією, ORM, міграціями та чергами. Laravel дозволяє чітко відокремити контролери від сервісів обробки медіа і підтримує queue-based виконання довгих задач [29].

Ключові параметри методів обробки зберігаються в таблиці settings бази даних (модель Setting), що дозволяє змінювати їх без перезапуску застосунку або оновлення коду. Це реалізовано через статичні методи Setting::getValue() та Setting::putValue(), які підтримують типізацію значень (bool, int, float, string). Усі конфігурації методів та зовнішніх інтеграцій можуть бути переналаштовані адміністратором через вебінтерфейс без технічного втручання.

Таблиця 4.3 – Технологічний стек прототипу

Компонент	Вибір	Обґрунтування
Мова та фреймворк	PHP 8.x, Laravel	Швидка реалізація вебсервісу, міграцій, черг, авторизації та сервісної архітектури.
СУБД	MySQL	Транзакційне зберігання активів, відбитків, маркерів та доказових логів.
Конфігурація методів	Setting (БД), Laravel .env	Керування параметрами без перезапуску; підтримка типізованих значень.
Обробка зображень	Imagick	Нормалізація, градації сірого, масштабування, phash/dhash.
Обробка аудіо/відео	FFmpeg	Декодування у PCM16 WAV, перекодування форматів доставки.
Черги	Laravel Queue, database/worker	Асинхронна обробка аудіо/відео та попередньої перевірки.
Зовнішній пошук зображень	Google Cloud Vision API Web Detection	Пошук повних і часткових збігів у відкритому інтернеті [27].
Контроль версій	GitHub	Простежуваність змін коду, релізів і конфігурацій.

Джерело: складено автором

4.3. Реалізація бібліотеки цифрових водяних знаків та відбитків

Детальний опис математичних моделей методів, що використовуються в системі, наведено в розділах 2 і 3 дисертації. У цьому розділі увагу зосереджено виключно на програмній реалізації: архітектурі сервісів, реалізаційних параметрах, pipeline-специфіці кожного методу та контрольних механізмах.

Бібліотека реалізована як набір спеціалізованих сервісів зі спільними контрактами. Кожен метод підтримує такий набір операцій: оцінювання ємності (preflight), вбудовування, сліпе витягнення, самоперевірка та перевірка формату доставки. Усі аудіометоди працюють із нормалізованим WAV/PCM16-представленням, яке формується за допомогою FFmpeg.

Таблиця 4.4 – Пайплайн реєстрації та маркування мультимедійного активу

Крок	Операція	Результат
1. Завантаження файлу	Валідація MIME, розміру та метаданих.	Підтвердження придатності файлу.
2. Реєстрація активу	Створення запису Asset, UUID, watermark_token, IP P1:<token>.	Прив'язка файлу до правовласника.
3. Формування ознак	SHA-256 → phash/dhash або audio_fingerprint → audio_profile.	Пошукові відбитки для ідентифікації.
4. Попередня перевірка	Оцінка ємності, ризику, придатності методу для конкретного файлу.	Preflight-статус і рекомендований метод.
5. Маркування	WatermarkEngine: вибір методу та вбудовування службового повідомлення.	Маркований файл зі службовим ідентифікатором.
6. Самоперевірка	Витягнення службового повідомлення з PCM/WAV.	Підтвердження коректності вбудовування.
7. Перевірка формату доставки	Витягнення з фінального файлу (MP3/JPEG тощо).	Підтвердження робастності після кодування.
8. Доказовий журнал	Запис події, параметрів, CRC, хешів, статусів.	Відтворюваний доказовий слід.

Джерело: складено автором

Для зображень основний контур використовує DCT/QIM-маркування та перцептивні хеші; для аудіо інтегровано кілька методів із різною стійкістю та призначенням. Вибір методу виконується на основі preflight-оцінки: система оцінює тип файлу, тривалість, рівень сигналу, ризик перекодування та повертає рекомендований метод і оцінку довіри.

4.3.1. Зведені параметри реалізованих методів

Математичні основи кожного методу описано в підрозд. 2.2–2.7. Тут наведено зведену таблицю реалізаційних параметрів, специфічних для програмної реалізації в IP-Protect (табл. 4.5).

Таблиця 4.5 – Зведені реалізаційні параметри аудіометодів IP-Protect

Метод	SYNC-маркер	Формат кадру	Повторення / голосування	Ключові особливості реалізації
AudioQimV1	IPP1	PCM LSB	BIT_STRIDE =4, REP=5	Базовий PCM/LSB-QIM; придатний для форматів без втрат
audio_subband_ energy_v2	SBE2	N=512, H=256, Hann	R=4, soft-vote q=min(1,6|D|)	DCT-піддіапазони; M/S stereo; фільтр мінімального RMS
audio_mdct_qim_v2	MDQ2	N=256, DCT-II	R=3, majority vote	Attenuation-only; смуги A=[6;18], B=[22;46]; τ_RMS=50
audio_mdct_qim_v3	MDQ3	MDCT-подібне з overlap	R≥3, soft-vote	Перекривні вікна; жорсткіший відбір носіїв; пріоритет для MP3/AAC
audio_pgdiff_v2	PGD1	DCT, варіативний розмір	Повторення пакета, ring interleave	Гібрид: псевдографічний відбиток + DCT/QIM-вбудовування; абсолютне відношення енергій
audio_spread_ spectrum_v1	SS1!	CHIPS_PER_ BIT=512	R=3, correlation-based	DS-SS; PN-послідовність із seed=asset_id; blind extraction
audio_echo_hiding_ v2	EH2!	Segment-based	Dual-echo differential	Диференційна двоехова модель; autocorrelation detection; повільніший метод
audio_patchwork_v2	PW2	Pairs of random samples	Statistical majority	Статистичний PCM Patchwork; низька стійкість до lossy; експериментальний

Джерело: складено автором на основі [187, 170, 215, 169, 41, 192, 210, 216, 174, 230]

Для зображень система використовує: SHA-256 (точний хеш), phash64 та dhash64 (перцептивні відбитки), DCT/QIM-вбудовування службового повідомлення. Математичні основи цих методів детально розглянуто в підрозділі 2.3 та розділі 3 [224, 225, 227, 228].

4.3.2. Попередня перевірка, самоперевірка та перевірка формату доставки

До фактичного маркування система виконує попередню перевірку (preflight): оцінює кількість придатних несучих фреймів, теоретичну ємність, рівень сигналу, частку тиші та ризик перекодування. Результат – статус «придатний / ризикований / непридатний» та оцінка довіри. Якщо preflight повертає «непридатний», маркування не виконується.

Після вбудовування виконується самоперевірка: система витягує службове повідомлення з PCM/WAV-файлу та порівнює з очікуваним значенням. Це підтверджує, що вбудовування технічно успішне. Далі виконується перевірка формату доставки: WAV перекодовується у цільовий формат (MP3, FLAC, M4A тощо) і виконується повторне витягнення. Якщо самоперевірка пройшла, але перевірка формату доставки – ні, система фіксує статус *embedded_pcm_only*, а не гарантовано стійке маркування.

Таблиця 4.6 – Контрольні процедури пайплайна маркування

Процедура	Що перевіряється	Значення для доказового контуру
Preflight	Ємність, рівень сигналу, частка тиші, ризик методу для конкретного файлу.	Запобігає ризикованому маркуванню; фіксує параметри у журналі.
Самоперевірка	Витягнення службового повідомлення з PCM після вбудовування.	Підтверджує внутрішню коректність вбудовування.
Перевірка формату доставки	Витягнення після перекодування у цільовий формат (MP3, FLAC, M4A).	Підтверджує практичну стійкість; виявляє статус embedded_pcm_only.
CRC/CRC32	Контрольна сума кадру службового повідомлення.	Відбраковування помилкових витягнень при перевірці.
Синхромаркер	Перевірка наявності SYNC (PGD1, MDQ2, SS1! тощо) при витягненні.	Запобігає помилковій інтерпретації сигналу без водяного знака.

Джерело: складено автором

4.3.3. Архітектура модуля audio_pgdiff_v2

Метод audio_pgdiff_v2 займає особливе місце в системі, оскільки поєднує функції побудови контентного відбитка та вбудовування водяного знака. Математична основа методу описана в підрозділі 3.2 [210, 216]. Програмна реалізація включає чотири взаємопов'язаних компоненти.

Таблиця 4.7 – Компоненти реалізації audio_pgdiff_v2

Компонент	Клас / сервіс	Роль
Побудова профілю	AudioPseudoGraphicAnalyzer	RMS/dB, q_seq, d_seq, оцінки довіри профілю
Пошуковий відбиток	AudioPseudoGraphicFingerprintService	64-бітне згортання d_seq; порівняння за відстанню Хеммінга [189]
Попередній перегляд	AudioPseudoGraphicPreviewRenderer	Зображення енергетичної динаміки аудіо для візуальної експертизи
Вбудовування/ витягнення	AudioPgdiffV1Method	DCT/QIM за абсолютним відношенням енергій; адаптивна стратегія для AAC
Кодек пакета	AudioPgdiffPayloadCodec	PGD1, sync, magic, CRC16, ring interleaving, packet-level repetition
Асинхронна обробка	RunAudioPgdiffMarkJob	Виносить тривалі задачі з вебзапиту до черги
Адаптивна перевірка	FileCheckService::extractPgdiffAdaptive()	При перевірці AAC/M4A-файлів використовує оригінальний актив як референс для відновлення позицій носіїв

Джерело: складено автором на основі [210, 216, 189]

Адаптивна стратегія для AAC-файлів є важливим нововведенням: при перевірці стисненого аудіо система знаходить найближчий кандидат за відбитком і передає шлях до оригінального активу як референс, що дозволяє відновити позиції несучих фреймів та підвищити ймовірність успішного витягнення водяного знака із перекодованого файлу.

4.4. Криптографічні механізми та доказовий контур

Криптографічний рівень виконує три функції: точну фіксацію байтового стану файлу, контроль цілісності службового повідомлення і підготовку даних для доказового сертифіката. SHA-256 застосовується до оригінальних і маркованих файлів; CRC16/CRC32 – всередині кадрів аудіометодів для відбраковування помилкових витягнень; watermark_token зв'язує прихований ідентифікатор із записом у реєстрі [223].

Таблиця 4.8 – Криптографічні та контрольні механізми

Механізм	Де використовується	Призначення
SHA-256	original_sha256, marked_sha256, audio_fingerprint	Точна фіксація байтового стану файлу [223].
hash_u64 / bucket16	fingerprints	Швидке індексування перцептивного відбитка.
CRC16	PGD1 у audio_pgdiff_v2	Контроль цілісності службового повідомлення у псевдографічному методі.
CRC32	SS1!, EH2!, PW2, SBE2, MDQ2/3	Відбраковування хибних витягнень у аудіометодах.
IPP1:<watermark_token>	Усі аудіо/image методи	Зв'язування маркованого файлу з активом у реєстрі.
Цифровий підпис / сертифікат	Доказовий звіт (JSON/PDF)	Надання сертифікату властивості перевірюваного документа.

Джерело: складено автором на основі [223]

Доказовий звіт формується за формулою:

$$\text{Evidence} = H(\text{file}) \parallel \text{payload} \parallel \text{method} \parallel \theta \parallel \text{result} \parallel t \parallel \text{actor} \qquad (4.1)$$

де H(file) – SHA-256 файлу, payload – службове повідомлення, method – код методу, θ – параметри алгоритму, result – статус операції, t – часова мітка, actor – ідентифікатор користувача або системного процесу. Такий запис може бути

підписаний або зафіксований у зовнішньому блокчейн-реєстрі без зміни моделі даних [197].

Система підтримує два формати доказових звітів: JSON (для технічної верифікації та API-інтеграцій) і PDF (для подання у судових або адміністративних процедурах). Обидва формати включають повний набір полів доказового запису з часовими мітками.

4.5. Підсистема перевірки мультимедійних файлів

4.5.1. Поетапна верифікація: хеш → відбиток → водяний знак

Підсистема перевірки реалізує принцип short-circuit: методи ідентифікації застосовуються послідовно від найшвидших і найточніших до найбільш ресурсоємних. Така логіка знижує загальне навантаження на систему і зменшує час відповіді у типовому сценарії, де файл не змінювався.

Таблиця 4.9 – Логіка поетапної верифікації

Крок	Метод	Що шукається	Результат при збігу
1	SHA-256 (точний хеш)	Байтово тотожний оригінал або маркований файл у реєстрі.	PASS – exact_original_match або exact_marked_match. Подальша перевірка не потрібна.
2	phash64 / dhash64 / audio_fingerprint / audio_pgdiff_v2	Перцептивно схожі кандидати у межах порогу відстані Хеммінга.	PARTIAL або PASS (за кількома збігами). Запускається верифікація водяним знаком.
3	Витягнення водяного знака	Службове повідомлення IPP1:<token> у структурі файлу; зіставлення з реєстром.	PASS – watermark_match, якщо token знайдено у реєстрі.
4	Google Vision Web Detection	Для зображень: сторінки з повними або частковими збігами у відкритому інтернеті.	PARTIAL – external_candidate. Потребує підтвердження локальними методами [231].

Джерело: складено автором

Якщо на першому кроці SHA-256 дає точний збіг, система одразу повертає статус PASS і не виконує більш ресурсоємні кроки 2–4. Якщо точний хеш не знайдено, запускається пошук за відбитком (крок 2): знайдені кандидати передаються до верифікатора водяного знака (крок 3). Для зображень паралельно може виконуватися зовнішній пошук через Google Cloud Vision API [231]. Такий підхід забезпечує баланс між швидкістю і повнотою верифікації.

Підсумковий результат перевірки не ґрунтується на одному показнику:

$$\text{Result} = f(H_exact, FP_distance, WM_payload, Ev_log) \quad (4.2)$$

де H_exact – результат точного хеш-порівняння, FP_distance – відстань Хеммінга між відбитками, WM_payload – збіг службового повідомлення водяного знака, Ev_log – якість та повнота доказового журналу.

Таблиця 4.10 – Логіка інтерпретації результатів перевірки

Комбінація ознак	Статус	Тлумачення
SHA-256 збігається	PASS	Файл байтово тотожний зареєстрованому або маркованому файлу.
Водяний знак витягнуто, token знайдено у реєстрі	PASS	Файл містить прихований ідентифікатор активу.
Відбиток близький, водяний знак не знайдено	PARTIAL	Схожий кандидат; потрібна додаткова експертиза.
Pixel metrics / PSNR/SSIM високі, хеш інший	PARTIAL	Можлива перезбережена або оброблена копія зображення.
CRC не пройдено або sync не знайдено	FAIL	Водяний знак не підтверджено або дані пошкоджені.
Google Vision знаходить зовнішні сторінки	PARTIAL	Є вебкандидати; потрібна локальна перевірка [231].
Жоден шар не дав збігу	FAIL	Система не знайшла достатніх ознак відповідності.

Джерело: складено автором

Для перевірки реалізованої логіки ухвалення рішень проведено контрольні випробування з використанням зареєстрованих оригінальних і маркованих мультимедійних файлів. Після реєстрації файлу та вбудовування цифрового водяного знака марковану копію було завантажено до підсистеми перевірки. Система встановила точний збіг її хешу зі збереженим хешем маркованої копії, виявила цифровий водяний знак і підтвердила відповідність вилученого службового повідомлення зареєстрованому активу. Для зображень додатково було підтверджено попіксельний збіг із зареєстрованою маркованою копією.

Під час контрольного завантаження вихідного файлу без цифрового водяного знака система встановила точний збіг із зареєстрованим оригіналом за криптографічним хешем, а для зображень – також за результатами попіксельного порівняння. Водночас цифровий водяний знак у файлі не було виявлено, що відповідає очікуваному результату, оскільки до оригіналу вбудовування не застосовувалося. Результати функціональної перевірки коректності розпізнавання зареєстрованого оригіналу та маркованої копії наведено в табл. 4.11.

Таблиця 4.11 – Результати функціональної перевірки розпізнавання мультимедійних файлів із вбудованим цифровим водяним знаком і без нього

Контрольний випадок	**Очікуваний результат**	**Фактичний результат**	**Оцінка**
Зареєстрована маркована копія	Точний збіг маркованого файла; виявлення цифрового водяного знака; відповідність службового повідомлення запису в реєстрі	Установлено збіг хешу, виявлено цифровий водяний знак, підтверджено зв’язок із зареєстрованим активом	Коректний позитивний результат
Зареєстрований оригінал без цифрового водяного знака	Точний збіг з оригіналом; цифровий водяний знак не повинен виявлятися	Установлено збіг хешу з оригіналом; цифровий водяний знак не виявлено	Коректний негативний результат щодо наявності водяного знака

Джерело: складено автором

Отримані результати підтвердили коректність розмежування системою зареєстрованого оригіналу та маркованої копії. У виконаних контрольних перевірках не зафіксовано пропуску наявного цифрового водяного знака або

його помилкового виявлення у немаркованому оригіналі. Результат перевірки немаркованого оригіналу інтерпретується як PASS із підставою *exact_original_match*, тоді як для маркованої копії формується PASS із підставами *exact_marked_match* і *watermark_match*.

4.5.2. Підсистема доказового звітування

За результатами перевірки система формує доказовий звіт, доступний для завантаження у форматах JSON і PDF. Звіт включає: метадані файлу-кандидата, SHA-256, результати всіх шарів перевірки, витягнуте службове повідомлення, параметри методів, часові мітки, ідентифікатор правовласника та журнал подій. Для аудіо окремо фіксується статус robustness перевірки формату доставки (pass / partial / fail).

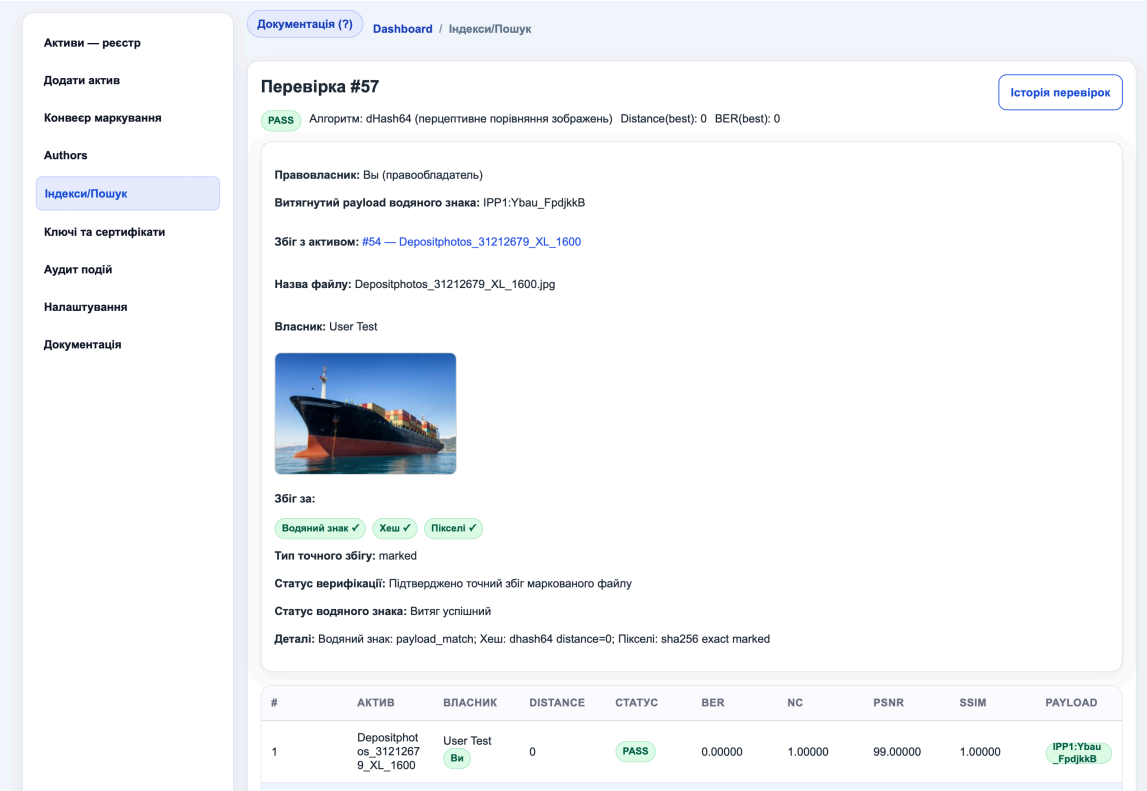


Рисунок 4.5 – Відображення результатів перевірки файлу-кандидата

(Джерело: складено автором)

Адміністративний рівень доступу дозволяє переглядати доказові журнали для всіх активів системи, фільтрувати події за типом, категорією, актором, датою

та цільовим об'єктом. Такий підхід забезпечує незалежну верифікацію операцій технічним спеціалістом або судовим експертом.

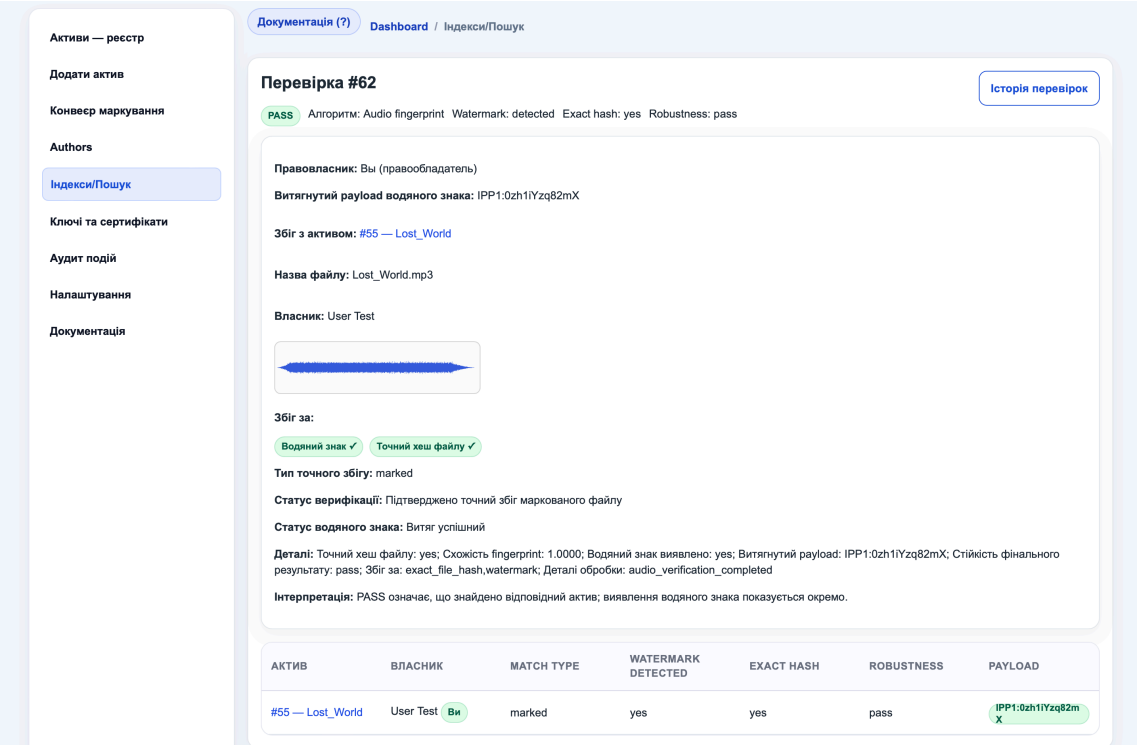


Рисунок 4.6 – Доказовий звіт та журнал подій активу

(Джерело: складено автором)

4.6. Модуль ліцензування та управління правами

Система IP-Protect підтримує управління ліцензіями для кожного зареєстрованого активу. Тип ліцензії призначається власником або адміністратором через розділ **Licenses** кабінету. Підтримувані типи включають: All Rights Reserved, Free Use, Use Only with Author's Permission, набір ліцензій Creative Commons (CC BY, CC BY-SA, CC BY-NC, CC BY-ND, CC BY-NC-SA, CC BY-NC-ND) та Public Domain.

Ліцензія відображається у публічному профілі активу та у результатах публічної перевірки. Якщо ліцензія передбачає отримання дозволу від автора (permission_required), зацікавлені особи можуть надіслати контактний запит безпосередньо через систему. Запит фіксується у таблиці **contact_requests** і надходить власнику активу для опрацювання.

Це функціональне розширення відповідає міжнародній практиці управління цифровими правами [168] і дозволяє системі виступати не лише як інструмент доказування, а й як платформа для легального управління правами на мультимедійний контент.

4.7. Модуль штучного інтелекту

Модуль штучного інтелекту виконує допоміжну функцію пошуку та ранжування кандидатів, а не самостійного доказу авторства. Ранжування кандидатів і рішення про відмову від атрибуції у відкритому сценарії виконує навчена модель зіставлення – логістична регресія над попарними ознаками схожості дескрипторів, теоретично обґрунтована й експериментально оцінена в підрозділі 2.8. Модель застосовується для обох модальностей і спирається виключно на публічні дескриптори, які система обчислює під час реєстрації активу, без зовнішніх сервісів розпізнавання як обов'язкової ланки рішення. Кандидатів формує наявний префільтр (за перцептивними хешами й бакетуванням для зображень; за псевдографічним профілем audio_pgdiff_v2 та slide-match алгоритмом серед зареєстрованих аудіоактивів), а модель лише переупорядковує цей список за скором збігу.

Формально рішення ухвалюється так: серед кандидатів обирається той, чий скор збігу найвищий, і його скор порівнюється з порогом робочої точки. Скор найкращого кандидата визначається за (4.1):

$$s^*(q) = max_{c \in C(q)} s(q, c) \qquad (4.3)$$

де *s*(q)* – скор найкращого кандидата для запиту *q*; *s(q,c)* – скор збігу пари «запит *q* – кандидат *c*», обчислений навченою моделлю за формулою (2.27); *C(q)* – список кандидатів, сформований префільтром для запиту *q*; кандидат-переможець *c** = *argmax* s(q,c) визначає власника, якого система назве.

Атрибуцію підтверджують за умови $s^*(q) \geq \tau$, інакше видають «немає збігу»; поріг τ є параметром робочої точки (див. нижче та табл. 4.12).

Двигун ранжування перемикається конфігураційним прапорцем: за відсутності або несумісності артефакта моделі перевірка повертається на детермінований шлях (поріг за одним дескриптором), а причина відкату фіксується в журналі й метриках – тихе погіршення якості тут неприпустиме.

Реєстрація активу не донавчає модель. Слід розрізняти два рівні. Реєстрація лише обчислює дескриптори нового активу (перцептивні хеші, блокове ДКП, псевдографічний відбиток) і додає їх до індексу; вагові коефіцієнти моделі зіставлення на етапі перевірки залишаються незмінними. Це відповідає стандартній архітектурі систем пошуку за вмістом: модель зіставлення навчають один раз офлайн, а з кожним активом зростає покриття галереї, а не сама модель. Такий поділ забезпечує відтворюваність доказових рішень – результат перевірки того самого активу не змінюється від додавання інших – і виключає витік, за якого модель запам'ятовувала б конкретні активи. За потреби (зсув розподілу дескрипторів, поява нових типів атак) модель періодично переобучають окремим офлайн-прогоном із групуванням за активом, що зберігає відсутність витоку.

Зовнішній сервіс – окремий канал власника, а не ланка рішення. Google Cloud Vision API Web Detection [231] застосовується в окремому сценарії, який ініціює власник над своїм активом: пошук копій контенту у відкритому інтернеті. Його результати – URL сторінок із повними, частковими та візуально схожими збігами – зберігаються в деталях активу як довідкова інформація. Оскільки ці результати не містять дескрипторів зареєстрованих активів, вони не надходять на вхід моделі зіставлення й не беруть участі в рішенні про належність; напрям цього сценарію (від власного активу до копій у вебі) протилежний напряму перевірки (від чужого файлу до власника в реєстрі).

Робоча точка – доказовий вибір. Розділювальну здатність моделі зіставлення характеризують ROC- та DET-криві й виміряні на них робочі точки; яку точку застосувати, визначає функція втрат предметної області, а не самі дані.

Для доказової системи втрати різко несиметричні: хибна атрибуція, за якої система впевнено називає не того правовласника, у правовому контексті дорожча за відмову «немає збігу», що лише передає справу перевірюваним артефактам. Тому робочу точку обрано в області низького FPR, яка мінімізує хибну атрибуцію коштом вищої частки відмов; вищий рівень відмов прийнятний саме тут, бо ШІ-ранжування є допоміжним і не замінює доказових перевірок. Розгорнутий за замовчуванням поріг відповідає FPR = 0,01 (0,8035 для зображень, 0,5160 для аудіо); обидві робочі точки наведено як компроміс (табл. 4.12), а сам поріг є конфігурованим параметром.

Таблиця 4.12 – Робочі точки навченої моделі зіставлення

FPR	Модальність	Хибна атрибуція	Правильна атрибуція
0,01	зображення	0,0022	0,663
0,05	зображення	0,0109	0,707
0,01	аудіо	0,0084	0,630
0,05	аудіо	0,0181	0,725

Джерело: складено автором

Робочі точки виміряно кросперевіркою на пофолдових моделях, тоді як розгорнуто артефакт, навчений на всій вибірці, – шкала скорів може дещо відрізнятися, тож номінальний FPR = 0,01 є оцінкою, а фактична частка на розгорнутій моделі може відхилятися; поріг має сенс лише відносно розподілу скорів конкретної моделі.

Ефект у реальному потоці. На реальному запиті модель зіставлення змінює порядок кандидатів порівняно з ранжуванням за відстанню: найближчий за Геммінгом кандидат може бути опущений, а активи з гіршою відстанню підняті, бо рішення ухвалюється на всьому наборі ознак. Показовий випадок – два кандидати з нульовою відстанню (точний оригінал і пересохранена копія): детермінований шлях їх не розрізняє взагалі, тоді як модель розділяє їх і ставить першим точний оригінал, що й визначає, кого система назве правовласником. Разом із кривими стійкості підрозділу 2.8, де на важкому обрізанні модель

підвищує Recall@1 з 0,442 до 0,881, це і є та ланка, що змінює рішення атрибуції на модифікованому контенті.

Остаточна доказова інтерпретація завжди ґрунтується на перевірюваних артефактах: службовому повідомленні водяного знака, хешах, відстані відбитка, CRC, журналі подій, даті реєстрації та зв'язку з правовласником. Результат ШІ-ранжування є вхідними даними для традиційних перевірок, але не замінює їх [197].

4.8. Безпека, аудит та розгортання

Система реалізує триступеневу модель доступу: ролі author, operator та admin. Матриця дозволів для кожної ролі налаштовується через модуль AccessPolicy і фіксується у таблиці access_policies. Кожна зміна матриці дозволів логується в AuditEvent та доступна для перегляду адміністратором. Це дозволяє визначити, хто, коли і з якими правами виконував операції над активами. Заходи безпеки та аудиту наведені у табл. 4.13.

Таблиця 4.13 – Заходи безпеки та аудиту

Рівень	Заходи	Очікуваний ефект
Доступ користувачів	Ролі author/operator/admin; матриця дозволів AccessPolicy; обмеження видимості активів.	Запобігання доступу до чужих активів і неавторизованих операцій.
Сховище файлів	Приватне storage; контроль MIME; резервне копіювання.	Захист оригіналів і маркованих копій.
Ключі та секрети	.env, CI/CD secrets, Setting (для API-ключів).	Відокремлення секретів від репозиторію.
Доказовий журнал	Незмінювані записи EvidenceLog + AuditEvent; hash, payload, method, actor_id.	Простежуваність операцій.
Черги	Timeout, retries, статуси queued/started/finished/error; failed jobs моніторинг.	Контроль довгих задач і діагностика збоїв.
Публічний доступ	Throttle middleware; вмикання через Setting; виконання від імені системного адміністратора.	Обмеження rate limit для анонімних запитів; ізоляція прав.

Джерело: складено автором

Розгортання системи виконується за схемою local → GitHub → production: composer install, artisan migrate, optimize:clear/config:cache, запуск queue workers. Параметри методів зберігаються у таблиці Setting, що дозволяє вносити зміни без повторного розгортання системи. Версіонування алгоритмів реалізовано через поле method у таблиці marks: кожен запис маркування містить назву методу, версію алгоритму, параметри θ та діагностичний JSON, що забезпечує відтворюваність перевірки після оновлення коду.

4.9. Порівняльний аналіз IP-Protect з наявними системами захисту авторських прав

Системи захисту авторських прав на мультимедійні дані можна умовно поділити на чотири основні класи: класичні DRM-системи, платформні системи контент-ідентифікації (Content ID та аналоги), блокчейн-орієнтовані реєстри прав, а також системи стійких прихованих ідентифікаторів, до якого належить IP-Protect. Детальна таблиця порівняння наведена у Додатку В (Таблиця В.1).

Класичні DRM-системи [214][168] будуються на принципі шифрування контенту та видачі ліцензій на відтворення в межах закритої екосистеми постачальника. Їхня ключова слабкість – захист зникає одразу після виходу з DRM-середовища (екранний запис, ріп): ідентифікатор авторства не вбудовано у сам файл. DRM не забезпечує технічний зв'язок між конкретним файлом-копією та правовласником, якщо файл поширюється поза контрольованим каналом.

Платформні системи контент-ідентифікації (YouTube Content ID, Audible Magic та подібні) [217][222] використовують порівняння завантаженого контенту з базою еталонних відбитків. Вони ефективні в межах однієї платформи, але ідентифікатор зберігається лише у внутрішній базі – сам файл не несе маркера авторства. Їхні алгоритми закриті, механізми оскарження обмежені, а міжплатформна сумісність відсутня.

Блокчейн-орієнтовані системи [197] фіксують права, ліцензії та транзакції у розподіленому реєстрі. Вони сильні для фіксації часу та послідовності

транзакцій, але слабкі щодо технічного зв'язку конкретного файлу із записом у ланцюжку: сам блокчейн не захищає від модифікації файлу і не дозволяє витягти ідентифікатор із копії безпосередньо.

IP-Protect реалізує підхід стійких прихованих ідентифікаторів, що забезпечує наступні конкурентні переваги порівняно з трьома іншими класами. Ключові переваги IP-Protect наведені у табл. 4.14.

Таблиця 4.14 – Ключові переваги підходу IP-Protect відносно класів систем-аналогів

Критерій	**DRM**	**Content ID**	**Блокчейн**	**IP-Protect**
Ідентифікатор вбудовано у файл	Ні	Ні	Частково	Так
Незалежність від платформи	Низька	Дуже низька	Середня	Висока
Стійкість до стиснення / перекодування	Обмежена	Висока (в межах платформи)	Не застосовно	Закладена як ключова вимога
Підтримка зображень, аудіо та відео	Аудіо/відео	Аудіо/відео	Будь-які	Зображення, аудіо, відео
Публічна перевірка без реєстрації	Ні	Ні	Частково	Так
Поетапна верифікація (хеш → відбиток → ЦВЗ)	Ні	Ні	Ні	Так
Управління ліцензіями (CC, All Rights Reserved і т.д.)	Обмежено	Ні	Так	Так
Придатність до судового доказування	Опосередкована	Обмежена	Сильна для транзакцій	Висока: маркер вбудовано у файл
Прозорість алгоритмів	Низька	Низька	Середня	Висока (open codebase)
Налаштовуваність без перерозгортання (RuntimeSettings)	Ні	Ні	Частково	Так

Джерело: авторська розробка на основі [214, 168, 217, 222, 190, 191, 197]

Принципова відмінність IP-Protect полягає в тому, що доказова прив'язка вбудована безпосередньо у мультимедійний файл і може бути незалежно верифікована технічним експертом без звернення до бази даних платформи. Водяний знак, хеш та відбиток зберігаються як пов'язані артефакти доказової системи, що підвищує судову придатність результату [190][197].

Важливим нещодавнім розширенням є публічна перевірка без реєстрації та поетапна верифікація (хеш → відбиток → водяний знак). Ці функції відсутні у розглянутих класах систем-аналогів і підвищують практичну доступність системи для широкого кола зацікавлених осіб – від кінцевих користувачів до адвокатів та судових експертів – без необхідності технічних знань або реєстрації в системі.

4.10. Висновки до розділу 4

У розділі 4 розроблено структурований опис інформаційної системи IP-Protect як модульного програмного комплексу для захисту інтелектуальної власності на мультимедійні дані. Система поєднує реєстр активів, модуль ліцензування, підсистему перевірки з поетапною верифікацією, бібліотеку цифрових водяних знаків і відбитків, доказовий контур та публічний режим перевірки.

Показано, що технічна реалізація не зводиться до одного алгоритму. Для зображень задіяно SHA-256, phash64, dhash64 та DCT/QIM-вбудовування; для аудіо інтегровано вісім методів із різною стійкістю та призначенням, об'єднаних спільним контрактом preflight → embed → self-check → delivery-check. Конфігурація методів керується через RuntimeSettings (таблиця Setting) без потреби в перерозгортанні системи.

Обґрунтовано механізм поетапної верифікації (SHA-256 → відбиток → водяний знак) та публічну перевірку без реєстрації, яка вмикається адміністратором і дозволяє широкому колу користувачів перевіряти файли на наявність у реєстрі. Доведено, що IP-Protect має конкурентні переваги перед DRM-системами, платформними Content ID та блокчейн-реєстрами у частині

платформонезалежності, вбудованості ідентифікатора, прозорості та судової придатності.

Отже, у розділі розроблено архітектуру та програмну реалізацію системи IP-Protect, яка забезпечує реєстрацію мультимедійних активів, формування службових ідентифікаторів, вбудовування та витягування цифрових водяних знаків, побудову цифрових відбитків, публічну й авторизовану перевірку файлів, а також формування доказових матеріалів. Запропонована реалізація створює цілісний інженерний контур для оцінювання стійкості методів до стиснення JPEG, перекодування MP3/AAC, масштабування, обрізання, додавання шуму та зміни часової шкали аудіосигналу. Для кількісного аналізу в системі передбачено фіксацію показників BER, NC, PSNR, SSIM, продуктивності обробки та частки успішних перевірок за різних профілів перетворень.

ВИСНОВКИ

У дисертаційній роботі розв’язано актуальне науково-прикладне завдання підвищення ефективності технічного захисту інтелектуальної власності на мультимедійні дані шляхом розроблення математичних моделей і методів стійкого цифрового маркування зображень та аудіоданих і їх інтеграції в інформаційну систему IP-Protect. Розроблена система забезпечує реєстрацію мультимедійних активів, вбудовування й вилучення цифрових ідентифікаторів, пошук схожого контенту, журналювання операцій і формування відтворюваних матеріалів технічної перевірки. За результатами дослідження сформульовано такі висновки.

1. Проаналізовано та систематизовано правові, технічні й організаційні підходи до захисту інтелектуальної власності на мультимедійні дані. Установлено функціональні обмеження DRM-систем, платформних систем ідентифікації контенту, блокчейн-реєстрів, криптографічних хешів, перцептивних відбитків і цифрових водяних знаків. Обґрунтовано необхідність поєднання вбудованого в мультимедійний сигнал ідентифікатора із зовнішнім реєстром активів, багаторівневою процедурою перевірки та журналюванням операцій. Сформовано вимоги до непомітності, місткості, робастності, відтворюваності перевірки й стійкості до типових перетворень та атак.

2. Розроблено сукупність математичних моделей вбудовування, вилучення та виявлення цифрових ідентифікаторів у зображеннях й аудіоданих. Формалізовано оператори вбудовування і вилучення, моделі атакувального каналу, критерії непомітності та стійкості, умови місткості контейнера, ключову вибірку позицій, надлишкове кодування, синхронізацію і контроль цілісності службового повідомлення. Для аудіоданих додатково формалізовано псевдографічний профіль, диференціальну послідовність ознак, відношення енергій частотних смуг і пакетний формат PGD1.

3. Розроблено та теоретично обґрунтовано методи робастного вбудовування цифрових водяних знаків у зображення й аудіодані. У шести напрямах реалізовано та експериментально порівняно сім удосконалених

реалізацій: часові методи, DCT-QIM для зображень, MDCT-контраст, розширений спектр, приховане ехо та вбудовування через енергію підсмуг. Подальшого розвитку набули два основні рішення: метод DCT-QIM для зображень із псевдовипадковою ключовою вибіркою, пакетною надлишковістю та семикратним повторенням і метод audio_pgdiff_v2 з абсолютним DCT-QIM-кодуванням на основі відношення енергій смуг. Для обох методів формалізовано компроміс між непомітністю та стійкістю за заданих обмежень місткості; зокрема, вбудовування повідомлення обсягом 44 байти в зображення потребує контейнера розміром не менше ніж 592 × 592 пікселі за прийнятих параметрів надлишковості.

4. Розроблено критерії виявлення та ідентифікації цифрових водяних знаків і відбитків. Для методу DCT-QIM установлено пороги ухвалення рішень за показниками BER і NC, передбачено стани PASS, PARTIAL і FAIL, а для аудіометоду реалізовано чотири послідовні етапи попередньої перевірки контейнера з підсумковими статусами «придатний», «ризикований» і «непридатний». Додаткову перевірку коректності вилучення забезпечують синхромаркери, CRC16/CRC32 і зіставлення службового повідомлення з реєстром. Функціональними випробуваннями підтверджено, що система правильно розпізнає марковану копію за хешем і цифровим водяним знаком, а зареєстрований оригінал – за хешем і характеристиками вмісту без помилкового виявлення у ньому водяного знака. Отже, реалізована процедура коректно розмежовує оригінальний і маркований файли та формує обґрунтовану підставу для підсумкового статусу перевірки.

5. Для аудіоданих розроблено 64-бітний перцептивний відбиток FP64 на основі диференціальної послідовності d_{seq} та пакетний формат PGD1. На їх основі побудовано алгоритм пошуку схожих аудіофрагментів. Над цим відбитком і над наявними дескрипторами зображень (перцептивні хеші phash64/dhash64 та блокове ДКП) розроблено й інтегровано метод автоматизованої атрибуції на основі машинного навчання. Навчений

класифікатор – логістична регресія над попарними ознаками схожості – виконує ранжування кандидатів і рішення про відмову від атрибуції (open-set).

Модель зіставлення оцінено на 567 зображеннях і 150 аудіофайлах за п’яти розбиттів із довірчими інтервалами. Він перевершує детермінований поріг за одним дескриптором: на важкому обрізанні зображень частка правильної атрибуції зростає з 0,442 до 0,881, а для аудіо частка хибної атрибуції знижується з 0,0478 до 0,0084. Доказовий внесок комбінування ознак зосереджений у ранжуванні closed-set зображень; для аудіо визначальним є вибір дескриптора.

Зовнішній сервіс Google Cloud Vision Web Detection застосовується як окремий канал пошуку копій у відкритому інтернеті. Реєстрація активу лише поповнює індекс дескрипторів і не донавчає модель, що забезпечує відтворюваність доказових рішень. Остаточна технічна перевірка ґрунтується на відтворюваних локальних ознаках: хеші, відстані відбитка, службовому повідомленні водяного знака, CRC і записах журналу подій.

Установлено, що результати автоматизованого ранжування, зокрема навченою моделлю зіставлення, мають використовуватися для формування множини кандидатів, тоді як остаточна технічна перевірка повинна ґрунтуватися на відтворюваних локальних ознаках: хеші, відстані відбитка, службовому повідомленні водяного знака, CRC і записах журналу подій.

6. Розроблено архітектуру та програмно реалізовано інформаційну систему IP-Protect. Система поєднує реєстр мультимедійних активів і правовласників, модуль ліцензування, бібліотеку цифрових водяних знаків і відбитків, підсистему багаторівневої перевірки, публічний режим верифікації, журнал аудиту та засоби формування доказових звітів. Реалізовано послідовний технологічний процес «реєстрація → формування ознак → попередня перевірка → вбудовування → самоперевірка → перевірка формату поширення → формування звіту». Збереження версії методу, його параметрів, результатів перевірки та контрольних значень забезпечує відтворюваність технічного аналізу.

7. Проведено порівняльні експериментальні дослідження на 567 зображеннях і 150 аудіофайлах. Для зображень за практично однакового бюджету спотворення (PSNR 56,05 і 55,88 дБ) запропонований метод після JPEG Q=90 і Q=85 забезпечив BER 0 та відновлення водяного знака у 100% файлів проти 97,4 і 97,5% для класичного методу. Після JPEG Q=75 BER зменшився з 0,0482 до 0,0287, тобто на 40,5%, а після додавання шуму σ=5 – з 0,0376 до 0,0006, тобто на 98,4%; частка успішного відновлення при масштабуванні на 50% зросла з 50,1 до 67,7%, або на 17,6 відсоткового пункту. Експериментально встановленою межею методу є обрізання на 10%, після якого частка успішного відновлення становить лише 1,1%.

Для аудіоданих метод audio_pgdiff_v2 після MP3-перекодування зі швидкістю 128 кбіт/с забезпечив BER 0,0100 проти 0,1033 у класичного методу розширеного спектра, що відповідає зниженню BER на 90,3%, а частка успішного відновлення зросла з 79,3 до 98,0%. За MP3 64 кбіт/с BER зменшився з 0,3600 до 0,0567, тобто на 84,3%, а частка успішного відновлення зросла з 28,0 до 88,7%. Після передискретизації ×4 водяний знак відновлено у 100% файлів проти 26,7% для класичного методу; після низькочастотної фільтрації з w=3 – у 99,3% проти 20,7%, а з w=7 – у 86,0% проти 0%. На модифікованих кадрах показник segSNR становив 12,66 дБ проти 3,25 дБ у класичного методу. Отримані результати підтверджують підвищену стійкість запропонованого методу в межах досліджених перетворень; стійкість до зміни часової шкали та агресивного AAC-перекодування потребує окремої експериментальної перевірки.

Отже, поставленої мети досягнуто, а сформульовані завдання виконано. Сукупність одержаних результатів – математичні моделі, удосконалені методи вбудовування, метод DCT-QIM для зображень, псевдографічно-диференціальний метод audio_pgdiff_v2 та інформаційна система IP-Protect – утворює цілісний технічний контур реєстрації, маркування, пошуку й відтворюваної перевірки відповідності мультимедійного файлу зареєстрованому цифровому активу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Зінич Л. В. Правові аспекти відповідальності інтернет-провайдерів за порушення прав інтелектуальної власності. *Юридичний науковий електронний журнал*. 2025. №3. DOI:10.32782/2524-0374/2025-3/66.

2. Bulgakova D., Deruma S. The liability of online intermediaries under European Union law. *Kyiv-Mohyla Law and Politics Journal*. 2023. No. 8-9. P. 1–43. DOI: https://doi.org/10.18523/kmlpj303154.2023-8-9.1-43.

3. Frosio G. F. Digital piracy debunked: a short note on digital threats and intermediary liability. *Internet Policy Review*. 2016. Vol. 5, no. 1. DOI: https://doi.org/10.14763/2016.1.400.

4. McNally M. B. User-generated online content 2: Policy implications. First Monday. 2012. Vol. 17, no. 6. DOI: https://doi.org/10.5210/fm.v17i6.3913.

5. Shankar K. Copyright Enforcement in Content-Sharing Platforms. Games (*MDPI*). 2022. Vol. 13, no. 5. P. 57. DOI: https://doi.org/10.3390/g13050057.

6. Bohatchuk D. P. Intellectual property law to protect artificial intelligence systems against adversarial attacks in light of the purposes of intellectual property law. *Juris Europensis Scientia*. 2024. Вип. 1. С. 30–34. DOI: https://doi.org/10.32782/chern.v1.2024.6.

7. Du Bois M. Justificatory Theories for Intellectual Property Viewed Through the Constitutional Prism. PELJ. 2018. Vol. 21. P. 1–38. DOI: https://doi.org/10.17159/1727-3781/2018/v21i0a2004.

8. Stojkoski V. et al. Estimating digital product trade through corporate revenue data. *Nature Communications*. 2024. Vol. 15. Art. 5262. DOI: https://doi.org/10.1038/s41467-024-49141-z.

9. Hallinan B., Reynolds C. J., Rothenstein O. Copyright callouts and the promise of creator-driven platform governance. Internet Policy Review. 2024. Vol. 13, no. 2. DOI: https://doi.org/10.14763/2024.2.1770.

10. Liu J., Shen Y., Zhou L. An evolutionary game analysis of algorithmic indirect copyright infringement from the perspective of collusion between UGC

platforms and direct infringer. *PLoS ONE*. 2024. Vol. 19, no. 5. 22 p. DOI: https://doi.org/10.1371/journal.pone.0292571.

11. Тумалавічус В. та ін. Legal impacts of digitization on intellectual property. *Amazonia Investiga*. 2024. Vol. 13, no. 74. С. 214–226. DOI: https://doi.org/10.34069/AI/2024.74.02.18.

12. Маліновська І. М. Сучасні тенденції правової охорони інтелектуальної власності. *Право та інновації*. 2018. № 3(23). С. 110–116. DOI: https://doi.org/10.31359/2311-4894-2018-23-3-110.

13. Воронкова В. Г. та ін. Legal principles of intellectual property protection in the digital society. *ScienceRise: Juridical Science*. 2019. Vol. 4, no. 10. P. 32–37. DOI: https://doi.org/10.15587/2523-4153.2019.188163.

14. Боярська С., Яворська І. Нормативне регулювання захисту прав інтелектуальної власності на цифровому ринку ЄС. *Вісник Львівського університету. Серія «Міжнародні відносини»*. 2020. Вип. 48. С. 150–158. DOI: https://doi.org/10.30970/vir.2020.48.0.11043.

15. Овчинников М. Ю., Слатвінська В. М. Технічний та нормативно-правовий аспекти захисту об'єктів ІВ на ринку аудіо-візуальної продукції. *Вісник ХНТУ*. 2024. № 3(90). С. 259–270. DOI: https://doi.org/10.35546/kntu2078-4481.2024.3.32.

16. Mehpara M. et al. Intellectual Property Law in the Digital Age: Challenges and Opportunities for Visual and Performing Artists. *ShodhKosh*. 2023. Vol. 4, no. 1. P. 901–905. DOI: https://doi.org/10.29121/shodhkosh.v4.i1.2023.2497.

17. Peitz M., Waelbroeck P. Piracy of digital products: a critical review of the theoretical literature. *Information Economics and Policy*. 2006. P. 449–476. DOI: https://doi.org/10.1016/j.infoecopol.2006.06.005.

18. Bradley W. A., Kolev J. How does digital piracy affect innovation? Evidence from software firms. *Research Policy*. 2023. Art. 104701. DOI: https://doi.org/10.1016/j.respol.2022.104701.

19. Batikas M., Claussen J., Peukert C. Follow the money: Online piracy and self-regulation in the advertising industry. *International Journal of Industrial Organization*. 2019. P. 121–151. DOI: https://doi.org/10.1016/j.ijindorg.2019.02.001.

20. Dejean S. What can we learn from empirical studies about piracy? *CESifo Economic Studies*. 2009. P. 326–352. DOI: https://doi.org/10.1093/cesifo/ifp006.

21. Marcinkowski J. et al. Neutralising the practice of digital piracy – a case of Poland. *Wroclaw Review of Law, Administration & Economics*. 2024. DOI: https://doi.org/10.2478/wrlae-2024-0006.

22. Didenko L. et al. Intellectual property rights issues in the digital era. *Cuestiones Políticas*. 2024. Vol. 42, no. 80. P. 136–158. DOI: https://doi.org/10.46398/cuestpol.4280.07.

23. Khan A., Wu X. Impact of Digital Economy on Intellectual Property Law. *Journal of Politics and Law*. 2020. Vol. 13, no. 4. P. 117–125. DOI: https://doi.org/10.5539/jpl.v13n4p117.

24. Torous M. Intellectual Property Rights in the Digital Age: Challenges and Solutions. *Allied Business Academy*. 2024. P. 1–3.

25. Malik R., Shaikh B. A. Adapting Copyright Law for the Digital Age: A Global Challenge. *Revistas Università*. 2024. P. 105–107.

26. Peukert C., Windisch M. The Economics of Copyright in the Digital Age. *Journal of Economic Surveys*. 2024. P. 877–903. DOI: https://doi.org/10.1111/joes.12632.

27. Poort J. et al. Global Online Piracy Study. *SSRN*. 2018. 85 p. DOI: https://doi.org/10.2139/ssrn.3224323.

28. Тарасенко Л. Авторське право у цифрову епоху: основні тенденції і зміни. *Вісник Львівського університету. Серія юридична*. 2022. Вип. 75. С. 61–72. DOI: https://doi.org/10.30970/vla.2022.75.061.

29. Терехова Г., Резворович К. Цифрове піратство: виклики для приватноправових відносин та захисту прав людини. *ДДУВС*. 2024. С. 203–206. DOI: https://doi.org/10.31733/15-03-2024/2/203-206.

30. Nazarovets S. A. Black Open Access in Ukraine: Analysis of Downloading Sci-Hub Publications by Ukrainian Internet Users. *Science and Innovation*. 2018. Vol. 14, no. 2. P. 19–24. DOI: https://doi.org/10.15407/scine14.02.019.

31. Filatova-Bilous N. Once again platform liability: on the edge of the ‘Uber’ and ‘Airbnb’ cases. *Internet Policy Review*. 2021. Vol. 10, no. 2. 27 p. DOI: https://doi.org/10.14763/2021.2.1559.

32. Tietzmann R., Gross Furini L. Sharing without laws: an exploration of social practices and ad hoc labeling standards in online movie piracy. *Internet Policy Review*. 2016. Vol. 5. Is. 2. 15 p. DOI: https://doi.org/10.14763/2016.2.416.

33. Schellekens M. Digital watermarks as legal evidence. Digital Evidence and Electronic *Signature Law Review*. 2011. Is. 8. P. 152–164. DOI: https://doi.org/10.14296/deeslr.v8i0.1965.

34. Фещак І., Онофрійчук С., Гарасимчук О.Технічні засоби захисту авторських прав, як інструменти боротьби з піратством електронних книг. *Кібербезпека: освіта, наука, техніка*. 2025. Вип. 4(28). С. 435–451. DOI: https://doi.org/10.28925/2663-4023.2025.28.854.

35. Зубко І. С. та ін. Огляд методів нанесення цифрових водяних знаків для захисту зображень. *Системи управління, навігації та зв'язку*. 2024. № 3(77), С. 121–125. DOI: https://doi.org/10.26906/SUNZ.2024.3.121.

36. Карпович Д. В., Глибовець А. М. Алгоритми порівняння зображень у задачах пошуку по контенту. *Наукові записки НаУКМА*. 2018. № 1. DOI: https://doi.org/10.18523/2617-3808.2018.21-24.

37. Begum M., Uddin M. S. Digital Image Watermarking Techniques: A Review. *Information (MDPI)*. 2020. Vol. 11. no. 2. Art. 110. DOI: https://doi.org/10.3390/info1102110.

38. Wan W. and others. A comprehensive survey on robust image watermarking. *Neurocomputing*. 2022. P. 226–247. DOI: https://doi.org/10.1016/j.neucom.2022.02.083.

39. Salah E. et al. Survey of imperceptible and robust digital audio watermarking systems. *Multimedia Tools and Applications*. 2024. P. 3635–3681. DOI: https://doi.org/10.1007/s11042-024-18969-4.

40. Растєгаєв Р. та ін. Огляд методів нанесення цифрових водяних знаків для захисту аудіофайлів. *Системи управління, навігації та зв'язку*. 2024. № 4 (78). DOI: https://doi.org/10.26906/SUNZ.2024.4.132.

41. Hua G. et al. Twenty years of digital audio watermarking–a comprehensive review. *Signal Processing*. 2016. 128. P. 222–242. DOI: https://doi.org/10.1016/j.sigpro.2016.04.005.

42. Yu X., Wang C., Zhou X. A Survey on Robust Video Watermarking Algorithms for Copyright Protection. *Applied Sciences*. 2018. P. 1–27. DOI: https://doi.org/10.3390/app8101891.

43. Asikuzzaman M., Pickering M. R. An Overview of Digital Video Watermarking. *IEEE TCSVT*. 2018. P. 2131–2153. DOI: https://doi.org/10.1109/TCSVT.2017.2712162.

44. Sang J., Liu Q., Song C.-L. Robust video watermarking using a hybrid DCT–DWT approach. *Journal of Visual Communication and Image Representation*. 2020. Art. 100052. DOI: https://doi.org/10.1016/j.jnlest.2020.100052.

45. He M., Wang H., Zhang F., Abdullahi S. M., Yang L. Robust Blind Video Watermarking Against Geometric Deformations and Online Video Sharing Platform Processing. *IEEE Transactions on Dependable and Secure Computing*. 2022. Vol. 20. Is. 6. P. 4702–4718. DOI: https://doi.org/10.1109/TDSC.2022.3232484.

46. Яремчук Ю. Є. та ін. Підвищення стійкості ЦВЗ у потокових відеозаписах на основі DEW. *Вісник ВПІ*. 2023. № 1. С. 55–64. DOI: https://doi.org/10.31649/1997-9266-2023-166-1-55-64.

47. Zhou M., Kuchuk N., Grynov D. Метод вбудовування та вилучення водяних знаків у відеокадри за допомогою DCT. *Системи управління, навігації та зв'язку*. 2024. № 3. С. 166–169. DOI: https://doi.org/10.26906/SUNZ.2024.3.166.

48. Fan D. et al. Anti-Recompression Video Watermarking Algorithm Based on H.264/AVC. *Mathematics*. 2023. Vol. 11. no. 13. Art. 2913. DOI: https://doi.org/10.3390/math11132913.

49. Kaczyński M. et al. High-Quality Video Watermarking Based on DNN for Video with HEVC Compression. *Sensors*. 2022. Vol. 22. no. 19. Art. 7552. DOI: https://doi.org/10.3390/s22197552.

50. Akhmametieva A., Kovalenko V. Development of the steganographic method of embedding of additional information into the spatial of color images. *Informatic and mathematical methods in simulation*. 2018. Vol. 8. no. 2. P. 110–120. DOI: https://doi.org/10.15276/imms.v8.no2.110.

51. Bekirov, A., Yaschenok, V. і Kreidun, O. Стеганографічний метод на основі безпосереднього та непрямого вбудовування даних для областей зображення з різною насиченістю. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2019. Вип. 34(1). С. 115–120. DOI: https://doi.org/10.33099/2311-7249/2019-34-1-115-120.

52. Козіна Г. Л. та ін. Система стеганографічного захисту фотографій з використанням крихких водяних знаків. *Systems and Technologies*. 2022. Vol. 64. No. 2. P. 75–81. DOI: https://doi.org/10.32782/2521-6643-2022.2-64.10.

53. Рубан І. В., Бологова Н. М., Мартовицький В. О. Інформаційна технологія підтвердження права власності на цифрові зображення. *Advanced Information Systems*. 2022. Т. 6, № 1. С. 118–123. DOI: https://doi.org/10.20998/2522-9052.2022.1.19.

54. Martovytskyi V. et al. Development of methods for generation of digital watermarks resistant to distortion. *EEJET*. 2021. № 6 (8(114)). с. 103–116. DOI: https://doi.org/10.15587/1729-4061.2021.246641.

55. Multimedia content protection by cryptography and watermarking in tamper-resistant hardware. *ACM MM*. 2000. P. 139–142. DOI: https://doi.org/10.1145/357744.357909.

56. Xu X. (Dexter) et al. A hybrid scheme for encryption and watermarking. *SPIE*. 2004. P. 725–736. DOI: https://doi.org/10.1117/12.527514.

57. Sanivarapu P. V. et al. Digital Watermarking System for Copyright Protection and Authentication of Images Using Cryptographic Techniques. *Applied Sciences*. 2022. № 12(17):8724. DOI: https://doi.org/10.3390/app12178724.

58. Yang Z. et al. A Hyper-Chaotically Encrypted Robust Digital Image Watermarking Method with Large Capacity Using Compress Sensing on a Hybrid Domain. *Entropy*. 2022. Art. 1486. DOI: https://doi.org/10.3390/e24101486.

59. Радівілова Т. А. та ін. Метод приховування інформації за допомогою алгоритму шифрування AES та стеганографічного методу LSB із захистом від обрізання та стегоаналізу. *Кібербезпека: освіта, наука, техніка*. 2025. № 3(31). С. 27–42. DOI: https://doi.org/10.28925/2663-4023.2025.31.997.

60. Лукічов В. В. та ін. Метод адаптивного багатошарового захисту інформації на основі стеганографії та криптографії. *IT та комп'ютерна інженерія*. 2023. № 58(3). С. 4–11. DOI: https://doi.org/10.31649/1999-9941-2023-58-3-4-11.

61. Almomani I. et al. A Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices. *Sensors*. 2022. № 22(6):2281. DOI: https://doi.org/10.3390/s22062281.

62. Mawla N. A., Khafaji H. K. Enhancing Data Security: A Cutting-Edge Approach Utilizing Protein Chains in Cryptography and Steganography. *Computers*. 2023. № 12(8):166. DOI: https://doi.org/10.3390/computers12080166.

63. Rasras R. J. et al. A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages. *ETASR*. 2019. № 9(1). P. 3681–3684. DOI: https://doi.org/10.48084/etasr.2380.

64. Bakunina O.V. et al. Synthesis method for s-boxes based on galois field transform matrices. *UJIT*. 2023. № 5(2). P. 41–48. DOI: https://doi.org/10.23939/ujit2023.02.041.

65. Hsieh S.-L. et al. Combining Digital Watermarking and Fingerprinting Techniques to Identify Copyrights for Color Images. *The Scientific World Journal*. 2014. № 454867. DOI: https://doi.org/10.1155/2014/454867.

66. Pope M. et al. Digital Steganography – An Introduction to Techniques and Tools. *CAIS*. 2012. № 30. P. 347–366. DOI: https://doi.org/10.17705/1CAIS.03022.

67. Cheddad A. et al. Digital image steganography: Survey and analysis of current methods. *Signal Processing*. 2010. P. 727–752. DOI: https://doi.org/10.1016/j.sigpro.2009.08.010.

68. Штонда Р. М. та ін. Аналіз методів цифрової стеганографії зображень. *CIT у сфері безпеки та оборони*. 2014. № 3(21). С. 78–81. DOI: https://doi.org/10.33099/2311-7249/2014-0-3(21)-78-81.

69. Туровський О. та ін. Методика оцінки стеганографічних методів приховування інформації в зображеннях. *State-of-the-art IT*. 2022. DOI: https://doi.org/10.36994/2788-5518-2021-02-02-23.

70. Стасюк О. І. та ін. Сучасні стеганографічні методи захисту інформації. *UISRJ*. 2011. № 13(1). С. 1–7. DOI: https://doi.org/10.18372/2410-7840.13.1994.

71. Ковтун В. Ю., Гнатюк С. О., Кінзерявий О. М. Modern methods of computer steganography systematization. *USJIS*. 2013. 19(3). P. 209–217. DOI: https://doi.org/10.18372/2225-5036.19.5628.

72. Гасілін Д. Л., Журавель І. М. Аналіз стійкості стеганоалгоритмів до геометричних атак та стиснення. *Сучасний захист інформації*. 2025. № 2. С. 42–50. DOI: https://doi.org/10.31673/2409-7292.2025.020965.

73. Apau R. et al. Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. *PLOS ONE*. 2024. Vol. 19. no. 9. Art. e0308807. DOI: https://doi.org/10.1371/journal.pone.0308807.

74. Majeed M. A. et al. A Review on Text Steganography Techniques. *Mathematics*. 2021. № 9(21):2829. DOI: https://doi.org/10.3390/math9212829.

75. Ахмаметьєва Г. В., Гайдук Д. В. Удосконалення стеганографічного методу на основі виділення особливостей блоків цифрового зображення. *Сучасна спеціальна техніка*. 2020. № 4(63). С.5-17. DOI: https://doi.org/10.36486/mst2411-3816.2020.4(63).1.

76. Kobozeva A. A., Sokolov A. V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele Energeticii Regionale*. 2021. Vol. 4(52). P. 115–130. DOI: https://doi.org/10.52254/1857-0070.2021.4-52.11.

77. Zhang F., Sokolov A. V. Increasing the Efficiency of Blind Decoding of the Steganographic Method with Code Control of Additional Information Embedding. *Problemele Energeticii Regionale*. 2024. Vol. 2(62). DOI: https://doi.org/10.52254/1857-0070.2024.2-62.11.

78. Zhang Z. Digital Rights Management Ecosystem and its Usage Controls: A Survey. *JDCTA*. 2011. P. 255–272. DOI: https://doi.org/10.4156/jdcta.vol5.issue3.26.

79. Jamkhedkar P. A., Heileman G. L. Digital rights management architectures. *Computers & Electrical Engineering*. 2009. P. 376–394. DOI: https://doi.org/10.1016/j.compeleceng.2008.06.012.

80. Gray J. E., Suzor N. P. Playing with machines: using machine learning to understand automated copyright enforcement. *Big Data & Society*. 2020. DOI: https://doi.org/10.1177/2053951720919963.

81. Kaye D. B. V. Copyright Gossip: Exploring Copyright Opinions, Theories, and Strategies on YouTube. *Social Media + Society*. 2021. P. 1–19. DOI: https://doi.org/10.1177/20563051211036940.

82. Lee D.-H., Lim M.-K. Music Recognition Using Audio Fingerprint: A Survey. *Journal of Korea Multimedia Society*. 2012. P. 77–87. DOI: https://doi.org/10.13064/KSSS.2012.4.1.077.

83. Qureshi A., Megías Jiménez D. Blockchain-Based Multimedia Content Protection: Review and Open Challenges. *Applied Sciences*. 2021. Art. 1. DOI: https://doi.org/10.3390/app11010001.

84. Ciriello R. F. et al. Blockchain-based digital rights management systems. *Electronic Markets*. 2023. Art. 5. DOI: https://doi.org/10.1007/s12525-023-00628-5.

85. Natgunanathan I. et al. Blockchain-Based Audio Watermarking Technique for Multimedia Copyright Protection in Distribution Networks. *ACM TOMM*. 2022. P. 86:1–86:23. DOI: https://doi.org/10.1145/3492803.

86. Darwish S. M. et al. Blockchain for video watermarking: An enhanced copyright protection approach for video forensics based on perceptual hash function. *PLOS ONE*. 2024. Vol.e0308451. DOI: https://doi.org/10.1371/journal.pone.0308451.

87. Wang H. et al. A Blockchain Copyright Protection Model Based on Vector Map Unique Identification. *IJGI*. 2025. Art. 53. DOI: https://doi.org/10.3390/ijgi14020053.

88. Megías D., Kuribayashi M., Qureshi A. Survey on Decentralized Fingerprinting Solutions: Copyright Protection through Piracy Tracing. *Computers*. 2020. Vol. 9(2):26. DOI: https://doi.org/10.3390/computers9020026.

89. García R. et al. A Review of Media Copyright Management Using Blockchain Technologies from the Academic and Business Perspectives. *Information*. 2025. Vol. 16(2):72. DOI: https://doi.org/10.3390/info16020072.

90. Kapsoulis N. et al. Consortium Blockchain Smart Contracts for Musical Rights Management. *Future Internet*. 2020. Vol. 12(8):134. DOI: https://doi.org/10.3390/fi12080134.

91. Wani M. A., Sultan B. Deep learning based image steganography: A review. *WIRES*. 2023. DOI: https://doi.org/10.1002/widm.1481.

92. Hu K. et al. Learning-based image steganography and watermarking: A survey. *Expert Systems with Applications*. 2024. Art. 123715. DOI: https://doi.org/10.1016/j.eswa.2024.123715.

93. Song B. et al. A survey on Deep-Learning-based image steganography. *Expert Systems with Applications*. 2024. Art. 124390. DOI: https://doi.org/10.1016/j.eswa.2024.124390.

94. Setiadi D. R. et al. AI-Powered Steganography: Advances in Image, Linguistic, and 3D Mesh Data Hiding – A Survey. *FAITH*. 2025. P. 1–23. DOI: https://doi.org/10.62411/faith.3048-3719-76.

95. Al Hadad Z., Ali I. H. Survey in Image and Audio Steganography by using the Deep Learning Methods. *Journal of Kufa*. 2023. P. 132–139. DOI: https://doi.org/10.31642/JoKMC/2018/100222.

96. Shehab D. A., Alhaddad M. J. Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research. *Symmetry*. 2022. Art. 117. DOI: https://doi.org/10.3390/sym14010117.

97. Babu J. et al. A Survey on Different Feature Extraction and Classification Techniques Used in Image Steganalysis. *Journal of Information Security*. 2017. Vol.8 No.3. P. 186–202. DOI: https://doi.org/10.4236/jis.2017.83013.

98. Croix N. J. D. L. et al. Comprehensive survey on image steganalysis using deep learning. *Array*. 2024. Art. 100353. DOI: https://doi.org/10.1016/j.array.2024.100353.

99. Kheddar H. et al. Deep learning for steganalysis of diverse data types: A review of methods, taxonomy, challenges and future directions. *Neurocomputing*. 2024. Vol. 581. DOI: https://doi.org/10.1016/j.neucom.2024.127528.

100. Hosny K. M. et al. Digital image watermarking using deep learning: A survey. *Computer Science Review*. 2024. Art. 100662. DOI: https://doi.org/10.1016/j.cosrev.2024.100662.

101. Zhong X. et al. A Brief, In-Depth Survey of Deep Learning-Based Image Watermarking. *Applied Sciences*. 2023. P. 11852. DOI: https://doi.org/10.3390/app132111852.

102. Zhang X. et al. V^2A-Mark: Versatile Deep Visual-Audio Watermarking for Manipulation Localization and Copyright Protection. *ACM MM*. 2024. DOI: https://doi.org/10.1145/3664647.3680904.

103. Luo H. (Luo Y.) et al. Digital Watermarking Technology for AI-Generated Images: A Survey. *Mathematics*. 2025. Art. 651. DOI: https://doi.org/10.3390/math13040651.

104. Si W. Applications of Artificial Intelligence in Intellectual Property Infringement Detection: Effectiveness and Risk Management. *CMNM'25*. 2025. DOI: https://doi.org/10.1145/3757110.3757144.

105. Montanaro M. et al. Using knowledge graphs for audio retrieval: a case study on copyright infringement detection. *World Wide Web*. 2024. DOI: https://doi.org/10.1007/s11280-024-01277-0.

106. Khan A. A. et al. A survey on multimedia-enabled deepfake detection: state-of-the-art tools and techniques, emerging trends, current challenges & limitations, and future directions. *Discov Computing*. 2025. Vol. 28:48. DOI: https://doi.org/10.1007/s10791-025-09550-0.

107. Fkirin A. Copyright protection of deep neural network models using watermarking. *Multimedia Tools and Applications*. 2022. DOI: https://doi.org/10.1007/s11042-022-12566-z.

108. Ahmed M. I. et al. Ownership protection of deep learning models using watermarking. *Computers & Electrical Engineering*. 2025. Art. 110481. DOI: https://doi.org/10.1016/j.compeleceng.2025.110481.

109. Bellafqira R. et al. DICTION: DynamIC robusT whIte bOx Watermarking Scheme for Deep Neural Networks. *Applied Sciences*. 2025. Vol. 15(13):7511. DOI: https://doi.org/10.3390/app15137511.

110. Zhang B. et al.Audio Deepfake Detection: What Has Been Achieved and What Lies Ahead. *Sensors*. 2025. Vol. 25(7):1989. DOI: https://doi.org/10.3390/s25071989.

111. Zhang H. , Hu C., Min S., Sui H., Zhou G. TSFF-Net: TSFF-Net: A deep fake video detection model based on two-stream feature domain fusion. *PLOS ONE*. 2024. Vol. 19(12): e0311366. DOI: https://doi.org/10.1371/journal.pone.0311366.

112. Wu T.-Y., Lin C.-Y. Spreading Spectrum Watermarking with Latent Diffusion Models. *Entropy*. 2025. Vol. 27. no. 4. Art. 428. DOI: https://doi.org/10.3390/e27040428.

113. Xu L. et al. Digital Image Copyright Protection and Management Approach—Based on Artificial Intelligence and Blockchain Technology. *JTAER*, 2025. Vol. 20. no. 2. Art. 76. DOI: https://doi.org/10.3390/jtaer20020076.

114. Kim J. et al. A Dual-Module System for Copyright-Free Image Recommendation and Infringement Detection in Educational Materials. *Journal of Imaging*. 2024. Vol.10(11). Art. 277. DOI: https://doi.org/10.3390/jimaging10110277.

115. Zhou Z. et al. Near-Duplicate Image Detection System Using Coarse-to-Fine Matching Scheme Based on Global and Local CNN Features. *Mathematics*. 2020. Vol. 8. no. 4. Art. 644. DOI: https://doi.org/10.3390/math8040644.

116. Hur J. et al. A Review of Digital Watermarking Protection based on Latent Diffusion Models. *Electronics*. 2025. Vol. 14. no. 1. P. 25. DOI: https://doi.org/10.3390/electronics14010025.

117. Трофименко О. Г. та ін. Штучний інтелект у військовій сфері. *Кібербезпека: освіта, наука, техніка*. 2024. № 1(25). С. 161–176. DOI: https://doi.org/10.28925/2663-4023.2024.25.161176.

118. San Roman R. et al. Proactive Detection of Voice Cloning with Localized Watermarking. *arXiv*. 2024. DOI: https://doi.org/10.48550/arXiv.2401.17264.

119. Liu Y. et al. XAttnMark: Learning Robust Audio Watermarking with Cross-Attention. *arXiv*. 2025. DOI: https://doi.org/10.48550/arXiv.2502.04230.

120. Sokolov A. et al. Cooperative Face Liveness Detection from Optical Flow. Int. Arch. *Photogramm*. 2025. XLVIII-2/W9-2025. DOI: https://doi.org/10.5194/isprs-archives-XLVIII-2-W9-2025-269-2025.

121. Zhao L. et al. Deepfake Detection Network Based on Multi-Feature Fusion. *Entropy*. 2021. Vol. 23. no. 12. Art. 1692. DOI: https://doi.org/10.3390/e23121692.

122. Бірюкова А. Г., Колісникова Г. В. Ways to Protect Infringed Rights in the Creation and Distribution of Deepfakes. *Problems of Legality*. 2024. Vol. 164. P. 6–18. DOI: https://doi.org/10.21564/2414-990X.164.297743.

123. Sun Y. et al. Deep Watermarking for Deep Intellectual Property Protection: A Survey. *SSRN*. 2024. DOI: https://doi.org/10.2139/ssrn.4697020.

124. Sun Y. et al. Deep Intellectual Property: A Survey. *ArXiv*. 2023. DOI: https://doi.org/10.48550/arXiv.2304.14613.

125. Василенко Л. П. Захист авторського права в контексті розвитку штучного інтелекту: національний та міжнародний аспект. *Право і суспільство*. 2025. № 2. С. 66–72. DOI: https://doi.org/10.32842/2078-3736/2025.2.11.

126. Остапенко Ю. І. та ін. Авторські права на об'єкти, створені ШІ. *Юридичний науковий електронний журнал*. 2024. № 5. С. 227–230. DOI: https://doi.org/10.32782/2524-0374/2024-5/53.

127. Malliari A. et al. Copyright implications for the aggregation of audiovisual content in Greece. *Digital Library Perspectives*. 2023. P. 131–144. DOI: https://doi.org/10.1108/DLP-04-2022-0033.

128. Panjaitan H. et al. Music Copyright Protection in the Digital Era: Legal Framework and Strategies for Enforcement. *Jurnal Hukum*. 2024. P. 235–257. DOI: https://doi.org/10.30659/jh.40.2.235-257.

129. Priest K. The Future of Music Copyright Collectives in the Digital Streaming Age. *Journal of Law & the Arts*. 2021. P. 1–45. DOI: https://doi.org/10.52214/jla.v45i1.8953.

130. Guo X. The Evolution of the Music Industry in the Digital Age: From Records to Streaming. *Journal of Sociology and Ethnology*. 2023. Vol. 5. no. 10. P. 7–12. DOI: https:// 10.23977/jsoce.2023.051002.

131. Arenal A. et al. Digital transformation, blockchain, and the music industry: A review from the perspective of performers' collective management organizations. *Telecommunications Policy*. 2024. Art. 102817. DOI: https://doi.org/10.1016/j.telpol.2024.102817.

132. Geiger C. Time to (Finally) Reinstall the Author in EU Copyright Law. II. 2025. Art. 1-48. DOI: https://doi.org/10.1007/s40319-025-01647-9.

133. Тарасенко Л. Л., Тарасенко Х. Ю. Оновлення законодавства України у сфері авторського права та його адаптація до стандартів ЄС. *Аналітично-порівняльне правознавство*. 2025. №3(1). DOI: https://doi.org/10.24144/2788-6018.2025.03.1.49.

134. Печерова Н. Г. Особливості ліцензійного договору на використання об'єктів суміжних прав. *Науковий вісник УжНУ. Серія «Право»*. 2024. Вип. 85(1). DOI: https://doi.org/10.24144/2307-3322.2024.85.1.44.

135. Еннан Р. Є. Здійснення і захист авторських прав у цифровому середовищі. *Науковий вісник УжНУ*. Серія: Право. 2024. № 86(2). С. 101–107. DOI: https://doi.org/10.24144/2307-3322.2024.86.2.16.

136. Клименко О. С., Христинченко Н. П. Особливості юридичної відповідальності за порушення прав інтелектуальної власності в цифровому середовищі. *Академічні візії*. 2025. DOI: https://doi.org/10.5281/zenodo.15170759.

137. Watson S. J. et al. Determinants of Unlawful File Sharing: A Scoping Review. *PLoS ONE*, 2015, Vol. 10. no. 6. DOI: https://doi.org/10.1371/journal.pone.0127921.

138. Garcia-Hernandez J. J. et al. Collusion-Resistant Audio Fingerprinting System in the Modulated Complex Lapped Transform Domain. *PLoS ONE*, 2013. Vol. 8. no 6. DOI: https://doi.org/10.1371/journal.pone.0065985.

139. Hui A. Mashup music as expression displaced and expression foregone. *Internet Policy Review*. 2021. Vol. 10 is. 4. DOI: https://doi.org/10.14763/2021.4.1604.

140. Довгий Є. А., Гнатчук О. О. Проблеми правового регулювання діяльності ОКУ в Україні. *Європейські перспективи*. 2025. № 1. С. 209–214. DOI: https://doi.org/10.71404/EP.2025.1.40.

141. Калин Р. Р. Організація колективного управління в системі правового регулювання охорони прав виконавців на результати творчої діяльності в україні. *Київський часопис права*. 2025. № 2. С. 106–113. DOI: https://doi.org/10.32782/klj/2025.2.12.

142. Prisacariu A. I. Collective management of copyright and related rights – fiscal implications. *SHS*. 2023. DOI: https://doi.org/10.1051/shsconf/202317701005.

143. Zhao C. A Study on the Improvement of Collective Management System of Copyright in the Digital Era. *7th International Conference on Humanities and Social Science Research (ICHSSR 2021).* Qingdao, China, 23-25 April 2021. DOI: https://doi.org/10.2991/assehr.k.210519.008 .

144. Mazziotti G., Ranaivoson H. Can Online Music Platforms Be Fair? *International Review of Intellectual Property and Competition Law*. 2024. Vol. 55. P. 249–279. DOI: https://doi.org/10.1007/s40319-023-01420-w

145. Маринин В. М. Цифровізація музичної індустрії: виклики та можливості. *Вісник НАКККіМ*. 2024. № 2. С. 160–164. DOI: https://doi.org/10.32461/2226-3209.2.2024.308417.

146. Bonini T., Gandini A. Platform Gatekeepers and the Platformization of Music Curation. *Social Media + Society*. 2019. Vol. 5. DOI: https://doi.org/10.1177/2056305119880006

147. Montecchio N. et al. The skipping behavior of users of music streaming services and its relation to musical structure. *PLOS ONE*. 2020. DOI: https://doi.org/10.1371/journal.pone.0239418.

148. Xu J. et al. Exploring the determinants of users' co-creation behavior on music streaming platforms in China. *PLOS ONE*. 2023. DOI: https://doi.org/10.1371/journal.pone.0291313.

149. Нестерцова-Собакарь О. Правовий захист авторських прав в Україні: сучасні виклики та законодавчі рішення. *Науковий вісник Дніпровського державного університету внутрішніх справ*. 2025. № (1). С. 104–110. DOI: https://doi.org/10.32782/2078-3566-2025-1-15.

150. Moscon V. Free Circulation of Information and Online Intermediaries – Replacing One "Value Gap" with Another. *IIC*, 2020. DOI: https://doi.org/10.1007/s40319-020-00982-3.

151. Kaukoranta A. Licensing Issues Hindering the Development of Online Music and Audiovisual Services in Europe. *SSRN*. 2016. DOI: https://doi.org/10.2139/ssrn.2880214

152. Quintais J. P. The New Copyright in the Digital Single Market Directive: A Critical Look. *SSRN*. 2019. DOI: https://doi.org/10.2139/ssrn.3424770.

153. Xalabarder R. The The Principle of Appropriate and Proportionate Remuneration of ART.18 Digital Single Market Directive: Some Thoughts for Its National Implementation. *SSRN*. 2020. DOI: https://doi.org/10.2139/ssrn.3684375.

154. WIPO Publication No. 909. Understanding Copyright and Related Rights, 2016.

155. WIPO Publication No. 891. Guide to the Copyright and Related Rights Treaties, 2003.

156. Directive (EU) 2019/790 (CDSM). Official text of the EP and of the Council.

157. ECSA Authors Group. Recommendations on the transposition of Articles 18–23.

158. IRIS Plus 2020-1. Copyright licensing rules in the EU (Council of Europe).

159. IRIS Plus 2023-03. Fair remuneration for audiovisual authors and performers in licensing agreements. (Council of Europe).

160. AVMSD. Audiovisual Media Services Directive (EU).

161. EBU Tech Report 062. Over-The-Top Distribution of PSM Content and Services.

162. EBU Tech Review (J. Barda). Access control and watermarking.

163. AlSabhany A.A., Ali A.H., Ridzuan F. et al. Digital audio steganography: Systematic review, classification, and analysis of the current state of the art. *Computer Science Review*. 2020. Art. 100316. DOI: https://doi.org/10.1016/j.cosrev.2020.100316.

164. Singh N., Bhardwaj J., Raghav G. Network Steganography and its Techniques: A Survey. *International Journal of Computer Applications*. 2017. P. 8–14. DOI: https://doi.org/10.5120/ijca2017915319.

165. Zhang F., Dong Y., Sun H. Research on Key Technologies of Image Steganography Based on Simultaneous Deception of Vision and Deep Learning Models. *Applied Sciences (MDPI)*. 2024. Vol. 14. No. 22. P. 10458. DOI:10.3390/app142210458.

166. Kim H. et al. Digital Photo Identification Framework with Copyright Protection and Photo Tracking. *Applied Sciences (MDPI)*. 2021. Vol. 11. No. 19. P. 9194. DOI: https://doi.org/10.3390/app11199194.

167. 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.

168. Hartung F., Kutter M. Multimedia Watermarking Techniques. *Proceedings of the IEEE*. 1999. Vol. 87, No. 7. P. 1079-1107. DOI: 1https://doi.org/0.1109/5.771066.

169. Cox I.J., Kilian J., Leighton F.T., Shamoon T. Secure Spread Spectrum Watermarking for Multimedia. *IEEE Trans. Image Processing*. 1997. Vol. 6, No. 12. P. 1673-1687. DOI: https://doi.org/10.1109/83.650120.

170. Chen B., Wornell G.W. Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding. *IEEE Trans. Information Theory*. 2001. Vol. 47, No. 4. P. 1423-1443. DOI: https://doi.org/10.1109/18.923725.

171. Podilchuk C.I., Delp E.J. Digital Watermarking: Algorithms and Applications. *IEEE Signal Processing Magazine*. 2001. Vol. 18, No. 4. P. 33-46. DOI: https://doi.org/10.1109/79.939835.

172. Kirovski D., Malvar H.S. Spread-Spectrum Watermarking of Audio Signals. IEEE Trans. *Signal Processing*. 2003. Vol. 51, No. 4. P. 1020-1033. DOI: https://doi.org/10.1109/TSP.2003.809384.

173. Xiang S., Kim H.J., Huang J. Audio Watermarking Robust Against Time-Scale Modification and MP3 Compression. *Signal Processing*. 2008. Vol. 88, No. 10. P. 2372-2387. DOI: https://doi.org/10.1016/j.sigpro.2008.03.019.

174. Princen J.P., Bradley A.B. Analysis/Synthesis Filter Bank Design Based on Time Domain Aliasing Cancellation. IEEE Trans. *Acoustics*. 1986. Vol. 34, No. 5. P. 1153–1161. DOI: https://doi.org/10.1109/TASSP.1986.1164954.

175. Chang C.-C., Tsai P., Lin C.-C. SVD-Based Digital Image Watermarking Scheme. *Pattern Recognition Letters*. 2005. Vol. 26, No. 10. P. 1577-1586. DOI: https://doi.org/10.1016/j.patrec.2005.01.004.

176. Hamidi M., El Haziti M., Cherifi H., El Hassouni M. Hybrid Blind Robust Image Watermarking Technique Based on DFT-DCT and SIFT. *Journal of Imaging*. 2021. Vol. 7, No. 10. Article 218. DOI: https://doi.org/10.3390/jimaging7100218.

177. Boney L., Tewfik A.H., Hamdy K.N. Digital Watermarks for Audio Signals. *Proc. ICME*. 1996. P. 473-480. DOI: https://doi.org/10.1109/ICME.1996.562748.

178. Cvejic N., Seppänen T. Spread Spectrum Audio Watermarking Using Frequency Hopping and Attack Characterization. *Signal Processing*. 2004. Vol. 84, No. 1. P. 207-213. DOI: https://doi.org/10.1016/j.sigpro.2003.10.016.

179. Wu S., Yang F., Liu Q., Zhu Q. ECSS: A High-Capacity and Robust Audio Watermarking Scheme with Error Correction. *Entropy*. 2022. Vol. 24, No. 12. Article 1843. DOI: https://doi.org/10.3390/e24121843.

180. Yamni M. et al. A Novel Robust Medical Image Watermarking Scheme Using Fractional-Order Exponent Moments and Residual Network. *Scientific Reports*. 2023. Vol. 13. Article 18432. DOI: https://doi.org/10.1038/s41598-023-45619-w.

181. Wang Z., Bovik A.C., Sheikh H.R., Simoncelli E.P. Image Quality Assessment: From Error Visibility to Structural Similarity. *IEEE Trans. Image Processing*. 2004. Vol. 13, No. 4. P. 600-612. DOI: https://doi.org/10.1109/TIP.2003.819861.

182. Huynh-Thu Q., Ghanbari M. Scope of Validity of PSNR in Image/Video Quality Assessment. *Electronics Letters*. 2008. DOI: https://doi.org/10.1049/el:20080522.

183. Voloshynovskiy S., Pereira S., Pun T., Eggers J.J., Su J.K. Attacks on Digital Watermarks: Classification, Estimation Based Attacks, and Benchmarks. *IEEE Communications Magazine*. 2001. Vol. 39, No. 8. P. 1177-1214. DOI: https://doi.org/10.1016/S0165-1684(01)00039-1.

184. Petitcolas F.A.P., Anderson R.J., Kuhn M.G. Attacks on Copyright Marking Systems. *Proc. Information Hiding*. 1998. P. 218–238. DOI: https://doi.org/10.1007/3-540-49380-8_16.

185. Steinebach M. et al. StirMark Benchmark for Audio Watermarking. *Proc. ITCC 2001*. P. 49-54. DOI: https://doi.org/10.1109/ITCC.2001.918764.

186. Begum M., Uddin M.S. Digital Image Watermarking Techniques: A Review. *Information*. 2020. Vol. 11, No. 2. Article 110. DOI: https://doi.org/10.3390/info11020110.

187. Bender W., Gruhl D., Morimoto N., Lu A. Techniques for Data Hiding. *IBM Systems Journal*. 1996. Vol. 35, No. 3-4. P. 313-336. DOI: https://doi.org/10.1147/sj.353.0313.

188. Bassia P., Pitas I., Nikolaidis N. Robust Audio Watermarking in the Time Domain. *IEEE Trans. Multimedia*. 2001. Vol. 3, No. 2. P. 232-241. DOI: https://doi.org/10.1109/6046.923822.

189. Hamming R.W. Error Detecting and Error Correcting Codes. *Bell System Technical Journal*. 1950. Vol. 29, No. 2. P. 147-160. DOI: https://doi.org/10.1002/j.1538-7305.1950.tb00463.x.

190. Овчинников М.Ю. Компаративний аналіз алгоритмів відбитку контенту для систем захисту інтелектуальної власності на мультимедійні дані. *Наука і техніка сьогодні*. 2025. №7(48). С. 1766-1779. DOI: https://doi.org/10.52058/2786-6025-2025-7(48)-1766-1779-1766-1779).

191. Ахмаметьєва Г., Овчинников М.Ю. Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані в хмарних середовищах. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2025. Вип. 4. С. 3-13. DOI: https://doi.org/10.32782/IT/2025-4-1.

192. Hu H.-T., Hsu L.-Y. Robust, Transparent and High-Capacity Audio Watermarking in DCT Domain. *Signal Processing*. 2015. Vol. 109. P. 226-235. DOI: https://doi.org/10.1016/j.sigpro.2014.11.011.

193. Swanson M.D., Zhu B., Tewfik A.H., Boney L. Robust Audio Watermarking Using Perceptual Masking. *Signal Processing*. 1998. Vol. 66, No. 3. P. 337-355. DOI: https://doi.org/10.1016/S0165-1684(98)00014-000014-0).

194. Санін-Круз К.Й., Долечек Г.Й. Покращений метод аудіо-водяного маркування на основі психоакустичних моделей. *Applied Sciences*. 2025. Vol. 15, No. 21. Article 11514. DOI: https://doi.org/10.3390/app152111514.

195. Овчинников М.Ю. Розробка та оптимізація алгоритмів цифрового відбитку для систем ідентифікації контенту в інформаційних системах захисту інтелектуальної власності. *Information Technology: Computer Science, Software Engineering and Cyber Security*. 2025. Вип. 3. С. 134-139. DOI: https://doi.org/10.32782/IT/2025-3-16.

196. Cox I.J., Linnartz J.-P.M.G. Some General Methods for Tampering with Watermarks. *IEEE Journal on Selected Areas in Communications*. 1998. Vol. 16, No. 4. P. 587-593. DOI: https://doi.org/10.1109/49.668980.

197. Овчинников М.Ю. Доказоорієнтований захист прав інтелектуальної власності на мультимедійні дані в епоху контенту, згенерованого ШІ. *Středoevropský věstník pro vědu a výzkum*. 2026. Vol. 2, No. 1. P. 274-292. DOI: https://doi.org/10.65237/2336-3630-2026-1(2)-17-17).

198. Gruhl D., Lu A., Bender W. Echo Hiding. *Proc. Information Hiding*. 1996. P. 293-315. DOI: https://doi.org/10.1007/3-540-61996-8_48.

199. Craver S., Liu B., Wolf W. Detectors for Echo Hiding Systems. *Proc. Information Hiding*. 2003. P. 247-257. DOI: https://doi.org/10.1007/3-540-36415-3_16.

200. Ko B.-S., Nishimura R., Suzuki Y. Time-Spread Echo Method for Digital Audio Watermarking. *IEEE Trans. Multimedia*. 2005. Vol. 7, No. 2. P. 212-221. DOI: https://doi.org/10.1109/TMM.2005.843366.

201. Ахмаметьєва Г. В., Овчинников М. Ю. Порівняльний аналіз методів широкосмугового та фазового кодування цифрових водяних знаків в аудіосигналі. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: матер. Міжнар. наук.-практ. конф. (м. Одеса, 16 трав. 2025 р.) : у 2 т. Одеса: Фенікс, 2025. Т. 2. С. 539–542. URL: https://hdl.handle.net/11300/31044

202. Liu Z., Huang Y., Huang J. Patchwork-Based Audio Watermarking Robust Against De-Synchronization and Recapturing Attacks. *IEEE Trans. Information*

Forensics and Security. 2019. Vol. 14, No. 4. P. 1171-1180. DOI: https://doi.org/10.1109/TIFS.2018.2871748.

203. Barni M., Bartolini F., Piva A. Improved Wavelet-Based Watermarking Through Pixel-Wise Masking. *IEEE Trans. Image Processing*. 2001. Vol. 10, No. 5. P. 783-791. DOI: https://doi.org/10.1109/83.918570.

204. Овчинников М.Ю. Компаративний аналіз методів впровадження ЦВЗ в аудіофайли. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 16 трав. 2025 р.): у 2 т. Одеса : Фенікс, 2025. Т. 2. С. 558–562. URL: https://hdl.handle.net/11300/31052

205. Bsoul A.A.R., Ismail A.B. A Novel Hybrid Watermarking Method for Digital Images Based on DT-CWT and Particle Swarm Optimization. *Applied Sciences*. 2025. Vol. 15, No. 3. Article 1315. DOI: https://doi.org/10.3390/app15031315.

206. Zhao Y., Wang H., Zhou X., Qin C. Deep Learning-Based Robust Watermarking with Attention Mechanism. *Mathematics*. 2023. Vol. 11, No. 1. Article 209. DOI: https://doi.org/10.3390/math11010209.

207. Ланських Є., Наумов О. Оцінювання ефективності методів ЦВЗ для мультимедійних даних. *Управління, економіка та забезпечення якості в фармації*. 2025. № 2. С. 121-132. DOI: https://doi.org/10.32689/maup.it.2025.2.13.

208. Овчинников М.Ю. Захист інформації в медіафайлах. Монографія: Безпека інформації та інфраструктури ІКС. Львів-Торунь: Liha-Pres, 2025. С. 299-332. DOI: https://doi.org/10.36059/978-966-397-537-5-8.

209. Овчинников М.Ю. Інформаційна система захисту інтелектуальної власності мультимедійних даних: синергія водяних знаків, перцептивного хешування та ШІ-аналітики. *Cross-disciplinary Studies in Science, Innovation and Social Development*. Vol. 3. Prague, 2026. P. 359-370. DOI: https://doi.org/10.65237/3-2026-23.

210. Haitsma J.A., Kalker T. A Highly Robust Audio Fingerprinting System with an Efficient Search Strategy. *Journal of New Music Research*. 2003. Vol. 32, No. 2. P. 211-222. DOI: https://doi.org/10.1076/jnmr.32.2.211.16746.

211. Hernández J.R., Amado M., Pérez-González F. DCT-Domain Watermarking Techniques for Still Images. IEEE Trans. *Image Processing*. 2000. Vol. 9, No. 1. P. 55-68. DOI: https://doi.org/10.1109/83.817598.

212. Kaur S., Singh S., Kaur M., Lee H.-N. A Systematic Review of Computational Image Steganography Approaches. *Archives of Computational Methods in Engineering*. 2022. Vol. 29. P. 4775-4797. DOI: https://doi.org/10.1007/s11831-022-09749-0.

213. Agarwal N., Singh A.K., Singh P.K. Survey of Robust and Imperceptible Watermarking. *Multimedia Tools and Applications*. 2019. Vol. 78. P. 8603-8633. DOI: https://doi.org/10.1007/s11042-018-7128-5.

214. 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

215. Ahmed N., Natarajan T., Rao K. R. Discrete Cosine Transform. IEEE Transactions on Computers. 1974. Vol. C-23, No. 1. P. 90-93. DOI: https://doi.org/10.1109/T-C.1974.223784

216. Wang A. L.-C. An Industrial-Strength Audio Search Algorithm. Proceedings of the 4th International Conference on Music Information Retrieval (ISMIR 2003). Baltimore, 2003. P. 7-13. DOI: https://doi.org/10.5281/zenodo.1416340

217. Cano P., Batlle E., Kalker T., Haitsma J. A. A Review of Audio Fingerprinting. *Journal of VLSI Signal Processing Systems*. 2005. Vol. 41, No. 3. P. 271–284. DOI: https://doi.org/10.1007/s11265-005-4151-3

218. Plank J. S. A Tutorial on Reed-Solomon Coding for Fault-Tolerance in RAID-like Systems. *Software: Practice and Experience*. 1997. Vol. 27, No. 9. P. 995-1021. DOI: https://doi.org/10.1002/(SICI)1097-024X(199709)27:9<995::AID-SPE111>3.0.CO;2-6.

219. Wu Q., Wu M. A Novel Robust Audio Watermarking Algorithm by Modifying the Average Amplitude in Transform Domain. *Applied Sciences*. 2018. Vol. 8, No. 5. Art. 723. DOI: https://doi.org/10.3390/app8050723

220. ITU-R. Recommendation BS.1387-2: Method for Objective Measurements of Perceived Audio Quality (PEAQ). *International Telecommunication Union*. 2023.

221. Hansen J. H. L., Pellom B. L. An Effective Quality Evaluation Protocol for Speech Enhancement Algorithms. *Proceedings of the 5th International Conference on Spoken Language Processing (ICSLP)*. Sydney, 1998. P. 2819-2822. DOI: https://doi.org/10.21437/ICSLP.1998-244

222. Allamanche E., Herre J., Hellmuth O., Fröba B., Kastner T., Cremer M. Content-based Identification of Audio Material Using MPEG-7 Low Level Description. *Proceedings of the 2nd International Symposium on Music Information Retrieval, ISMIR 2001*. Bloomington, USA. 2001. P. 1-8. URL: https://ismir2001.ismir.net/pdf/allamanche.pdf.

223. National Institute of Standards and Technology. Secure Hash Standard (SHS). FIPS PUB 180-4. Gaithersburg: NIST, 2015. P. 1-36. DOI: https://doi.org/10.6028/NIST.FIPS.180-4.

224. Swaminathan A., Mao Y., Wu M. Robust and Secure Image Hashing. *IEEE Transactions on Information Forensics and Security*. 2006. Vol. 1, No. 2. P. 215–230. DOI: https://doi.org/10.1109/TIFS.2006.873601.

225. Monga V., Evans B. L. Perceptual Image Hashing via Feature Points: Performance Evaluation and Trade-Offs. *IEEE Transactions on Image Processing*. 2006. Vol. 15, No. 11. P. 3452–3465. DOI: https://doi.org/10.1109/TIP.2006.881948.

226. Du L., Ho A. T. S., Cong R. Perceptual hashing for image authentication: A survey. *Signal Processing: Image Communication*. 2020. Vol. 81. Article 115713. DOI: https://doi.org/10.1016/j.image.2019.115713.

227. Zauner C. Implementation and Benchmarking of Perceptual Image Hash Functions. Master's thesis. *Upper Austria University of Applied Sciences, Hagenberg Campus*. 2010. URL: https://www.phash.org/docs/pubs/thesis_zauner.pdf.

228. Krawetz N. Kind of Like That. The Hacker Factor Blog. 2013. URL: https://www.hackerfactor.com/blog/index.php?/archives/529-Kind-of-Like-That.html.

229. Krawetz N. Looks Like It. The Hacker Factor Blog. 2011. URL: https://www.hackerfactor.com/blog/index.php?/archives/432-Looks-Like-It.html.

230. Boney L., Tewfik A. H., Hamdy K. N. Digital Watermarks for Audio Signals. *Proceedings of the Third IEEE International Conference on Multimedia Computing and Systems*. 1996. DOI: https://doi.org/10.1109/MMCS.1996.535015.

231. Google Cloud. Detect Web entities and pages. Cloud Vision API documentation. 2026. URL: https://cloud.google.com/vision/docs/detecting-web.

232. Овчинников М.Ю. Додавання та обробка звуку в метаданих файлів за допомогою PHP. *Наука і техніка сьогодні*. 2025. № 4(45). С. 1332–1344. DOI: https://doi.org/10.52058/2786-6025-2025-4(45)-1332-1344

233. Горбаченко С.А., Овчинников М.Ю., Захист інтелектуальної власності у сфері цифрового контенту: виклики та рішення для рекламного менеджменту. *Вчені записки Таврійського національного університету імені В.І. Вернадського*. *Серія: Технічні науки*. 2025. Т. 36 (75). №4. Ч. 2. С. 87–96. DOI: https://doi.org/10.32782/2663-5941/2025.4.2/12.

234. Овчинников М.Ю. Інтегрований захист мультимедійних даних у суднобудуванні й морській інфраструктурі. *Shipbuilding & Marine Infrastructure*. 2026. №1(22). С. 155–165. DOI: https://doi.org/10.15589/smi2026.1(22).15

235. Ахмаметьєва Г. В., Кирилюк В. О. Розробка стеганографічного методу вбудови бінарного цифрового водяного знаку в зображення на основі дискретного косинусного перетворення. *Інформатика та математичні методи в моделюванні*. 2021. Т. 11, № 1–2. С. 5–14. DOI: https://doi.org/10.15276/imms.v11.no1-2.5

236. Сулема Є. С., Радченко Є. О. Метод стеганографічного захисту мультимедійних даних на основі процедури псевдовипадкового вбудовування. *Наукові вісті КПІ*. 2020. № 1(128). С. 40–47. DOI: https://doi.org/10.20535/kpi-sn.2020.1.197952

237. Progonov D. O., Kushch S. M. Spectral Analysis of Steganograms. *Radio Electronics, Computer Science, Control*. 2015. No 2. P. 71–80. DOI: https://doi.org/10.15588/1607-3274-2015-2-9

238. Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. *Комп'ютерна стеганографія: навчальний посібник*. Вінниця: ВНТУ. 2017. 155 с. URL: https://ir.lib.vntu.edu.ua/handle/123456789/34907

239. Fridrich J. Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge : *Cambridge University Press*. 2009. 462 p. ISBN 978-0-521-19019-0. URL: https://dl.acm.org/doi/book/10.5555/1721894.

240. Fridrich J., Kodovský J. Rich Models for Steganalysis of Digital Images. *IEEE Transactions on Information Forensics and Security*. 2012. Vol. 7. No. 3. P. 868–882. DOI: https://doi.org/10.1109/TIFS.2012.2190402.

241. Hastie T., Tibshirani R., Friedman J. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. 2nd ed. New York : *Springer*, 2009. 745 p. URL: https://hastie.su.domains/ElemStatLearn/.

242. Scheirer W. J., Rocha A., Sapkota A., Boult T. E. Toward Open Set Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2013. Vol. 35, No. 7. P. 1757–1772. DOI: https://doi.org/10.1109/TPAMI.2012.256.

243. Costa F. de O., Eckmann M., Scheirer W. J., Rocha A. Open Set Source Camera Attribution. *Proceedings of the 25th SIBGRAPI Conference on Graphics, Patterns and Images*. IEEE, 2012. P. 71–78. DOI: https://doi.org/10.1109/SIBGRAPI.2012.19.

ДОДАТКИ

Додаток А. Список публікацій здобувача

Наукові праці здобувача, в яких опубліковані основні наукові результати дисертації:

1. Овчинников М. Ю., Слатвінська В. М. Технічний та нормативно-правовий аспекти захисту об’єктів інтелектуальної власності на ринку аудіо-візуальної продукції. *Вісник Херсонського національного технічного університету.* 2024. № 3(90). С. 259–270. DOI: https://doi.org/10.35546/kntu2078-4481.2024.3.32.

2. Овчинников М. Ю. Додавання та обробка звуку в метаданих файлів за допомогою PHP. *Наука і техніка сьогодні.* 2025. № 4(45). С. 1332–1344. DOI: https://doi.org/10.52058/2786-6025-2025-4(45)-1332-1344.

3. Овчинников М. Ю. Компаративний аналіз алгоритмів відбитку контенту для систем захисту інтелектуальної власності на мультимедійні дані. Наука і техніка сьогодні. 2025. №7(48). С. 1766–1779. DOI: https://doi.org/10.52058/2786-6025-2025-7(48)-1766-1779.

4. Овчинников М. Ю. Захист інформації в медіафайлах. *Безпека інформації та інфраструктури інформаційно-комунікаційних систем: міждисциплінарний підхід*: монографія / за ред. С. Горбаченка, А. Соколова. Львів–Торунь: Liha-Pres, 2025. С. 299–332. DOI: https://doi.org/10.36059/978-966-397-537-5-8.

5. Горбаченко С. А., Овчинников М. Ю. Захист інтелектуальної власності у сфері цифрового контенту: виклики та рішення для рекламного менеджменту. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Технічні науки.* 2025. Т. 36 (75). №4. Ч. 2. С. 87–96. DOI: https://doi.org/10.32782/2663-5941/2025.4.2/12.

6. Овчинников М. Ю. Розробка та оптимізація алгоритмів цифрового відбитку для систем ідентифікації контенту в інформаційних системах захисту інтелектуальної власності. *Information Technology: Computer Science, Software*

Engineering and Cyber Security. 2025. Вип. 3. С. 134–139. DOI: https://doi.org/10.32782/IT/2025-3-16.

7. Ахмаметьєва Г. В., Овчинников М. Ю. Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані в хмарних середовищах. *Information Technology: Computer Science, Software Engineering and Cyber Security.* 2025. Вип. 4. С. 3–13. DOI: https://doi.org/10.32782/IT/2025-4-1.

8. Овчинников М. Ю. Доказоорієнтований захист прав інтелектуальної власності на мультимедійні дані в епоху контенту, згенерованого ШІ. *Středoevropský věstník pro vědu a výzkum.* 2026. Vol. 2, № 1. С. 274–292. DOI: https://doi.org/10.65237/2336-3630-2026-1(2)-17.

9. Овчинников М. Ю. Інформаційна система захисту інтелектуальної власності мультимедійних даних: синергія водяних знаків, перцептивного хешування та ШІ-аналітики. *Cross-disciplinary Studies in Science, Innovation and Social Development: Monograph / [reviewers: E. O. Romanenko, Y. O. Ulianchenko, O. I. Datsii]*. Prague: Publishing house Education and Science s.r.o., 2026. С. 359–370. DOI: https://doi.org/10.65237/3-2026-23.

10. Овчинников М. Ю. Інтегрований захист мультимедійних даних у суднобудуванні й морській інфраструктурі. *Shipbuilding & Marine Infrastructure.* 2026. №1(22). С. 155–165. DOI: https://doi.org/10.15589/smi2026.1(22).15.

Наукові праці, які засвідчують апробацію матеріалів дисертації та додатково відображають її наукові результати :

11. Овчинников М. Ю. Огляд методів вбудовування інформації в звукові файли. *Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика*: матер. міжнар. наук.-практ. конф. (м. Одеса, 24 листоп. 2023 р.). Одеса : НУ «ОЮА», 2023. С. 27–30. DOI: https://doi.org/10.32837/11300.27179.

12. Овчинников М. Ю. Особливості вбудовування прихованої інформації у файли формату MP3. *Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів* : матеріали Міжнар. наук.-практ.

конф. (Одеса, 26 квіт. 2024 р.). Одеса, 2024. С. 898–902. URL: https://hdl.handle.net/11300/28215.

13. Овчинников М. Ю. Метод вбудовування повідомлень у відліки імпульсно-кодової модуляції аудіосигналу. *Інформаційне суспільство: проблеми та перспективи*: матер. IX Всеукр. наук.-практ. конф. (Одеса, 24 травня 2024 р.). С. 167–170. DOI: https://doi.org/10.32837/11300.27842

14. Овчинников М. Ю. Використання тегів ID3v2 для захисту авторських прав на звукові файли MP3. *Кібербезпека в сучасному світі: актуальні виклики:* матер. V Міжнар. наук.-практ. конф. (м. Одеса, 22 листопада 2024 р.) Одеса, 2024. С. 41–43. DOI: https://doi.org/10.32837/11300.28986

15. Овчинников М.Ю. Компаративний аналіз методів впровадження ЦВЗ в аудіофайли. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: матер. Міжнар. наук.-практ. конф. (м. Одеса, 16 трав. 2025 р.): у 2 т. Одеса : Фенікс, 2025. Т. 2. С. 558–562. URL: https://hdl.handle.net/11300/31052

16. Ахмаметьєва Г. В., Овчинников М. Ю. Порівняльний аналіз методів широкосмугового та фазового кодування цифрових водяних знаків в аудіосигналі. *Європейські орієнтири розвитку України: нові виміри у воєнний час*: матер. Міжнар. наук.-практ. конф. (м. Одеса, 16 травня 2025 р.) : у 2 т. Одеса: Фенікс, 2025. Т. 2. С. 539–542. URL: https://hdl.handle.net/11300/31044

17. Овчинников М. Ю. Розробка систем автоматичного моніторингу незаконного розповсюдження мультимедіа в інтернеті. *Інформаційне суспільство: проблеми та перспективи* : матер. X Всеукр. наук.-практ. конф. (м. Одеса, 23 травня 2025 р.). Одеса. 2025. С. 168–172. DOI: https://doi.org/10.32837/11300.29842

18. Овчинников М. Ю. AI-підсилена верифікація авторства мультимедійних даних в умовах генеративного ШІ. *Кібербезпека в сучасному світі: актуальні виклики* : матер. VI Міжнар. наук.-практ. конф. (м. Одеса, 28 листоп. 2025 р.). Одеса : НУ «ОЮА», 2025. С. 112–114. URL: https://hdl.handle.net/11300/32730.

19. Овчинников М. Ю. Алгоритмічні підходи до підтвердження авторства та цілісності мультимедійних даних. *Кібербезпека в сучасному світі: актуальні виклики* : матер. VI Міжнар. наук.-практич. конф. (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. С. 59–62. URL: https://hdl.handle.net/11300/32710.

20. Овчинников М. Ю. Ліцензування та управління правами на цифровий мультимедійний контент: інтеграція технічних засобів контролю у правові процедури. *Кібербезпека в сучасному світі: актуальні виклики* : матер. VI Міжнар. наук.-практич. конф. (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. С. 265–268. URL: https://hdl.handle.net/11300/32856.

21. Овчинников М. Ю. Комунікаційні стратегії протидії репостам і «дзеркалам» мультимедійного контенту: взаємодія з платформами та спільнотами. *Кібербезпека в сучасному світі: актуальні виклики* : матер. VI Міжнар. наук.-практич. конф. (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. С. 236–239. URL: https://hdl.handle.net/11300/32835.

22. Horbachenko S. Chepurna O. Kuklinova T. Kukharenko S. Cherevko Y. Boiko V. Ovchynnykov M. Analysis and optimization of processes for integrating smart grid objects into the critical infrastructure cyber protection system. *2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek'2025).* (Kharkiv, October 06–10, 2025). P. 615–619. DOI: https://doi.org/10.1109/KhPIWeek61436.2025.11288406.

23. Овчинников М. Ю. Штучний інтелект як адаптивний компонент цифрового водяного маркування мультимедійних даних. *Global Interdisciplinary Summit: Frontier of Science and Future Technologies* : Proceedings of International Scientific and Practical Conferenceю (April 3, 2026, Khalifa University Campus, Dubai, UAE). 2026. С. 132–139. DOI: https://doi.org/10.65237/1-4-2026-12.

24. Овчинников М. Ю. Синергія цифрових водяних знаків, перцептивного хешування та мультимедійних цифрових відбитків у системах захисту інтелектуальної власності. *Scientific Horizons: Digital Transformation* : Proceedings of International Scientific and Practical Conference. (March 20, 2026, Tsinghua University, Beijing, China). 2026. С. 26–33. DOI: https://doi.org/10.65237/1-3-2026-4.

Свідоцтва про реєстрацію авторського права на твір:

1. Комп'ютерна програма «Інформаційна система захисту інтелектуальної власності на мультимедійні дані IP-Protect» / Овчинников Микола Юрійович; Свідоцтво про реєстрацію авторського права на твір № 149653; видано 06.08.2026 р., дата реєстрації 30 липня 2026 р. URL: https://sis.nipo.gov.ua/uk/search/detail/1942787/

ВІДОМОСТІ ПРО АПРОБАЦІЮ МАТЕРІАЛІВ ДИСЕРТАЦІЇ

Положення, висновки та рекомендації, викладені у дисертації, доповідалися на: міжнародній науково-практичній конференції «Кіберпростір в умовах війни та глобальних викликів XXI століття: теорія та практика» (м. Одеса, 24 листопада 2023 р.) – особиста участь; міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: науково-практичний вимір в умовах воєнних викликів» (м. Одеса, 26 квітня 2024 р.) – особиста участь; IX всеукраїнській науково-практичній конференції «Інформаційне суспільство: проблеми та перспективи» (м. Одеса, 24 травня 2024 р.) – особиста участь; V міжнародній науково-практичній конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 22 листопада 2024 р.) – особиста участь; міжнародній науково-практичній конференції «Європейські орієнтири розвитку України: нові виміри у воєнний час» (м. Одеса, 16 травня 2025 р.) – особиста участь; X всеукраїнській науково-практичній конференції «Інформаційне суспільство: проблеми та перспективи» (м. Одеса, 23 травня 2025 р.) – особиста участь; конференції «2025 IEEE 6th KhPI Week on Advanced Technology (KhPIWeek’2025)» (м. Харків, 6–10 жовтня 2025 р.) – заочна форма участі; VI міжнародній науково-практичній конференції «Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.) – особиста участь; міжнародній науково-практичній конференції «Scientific Horizons: Digital Transformation» (м. Пекін, Китай, 20 березня 2026 р.) – заочна форма участі; міжнародній науково-практичній конференції «Global Interdisciplinary Summit: Frontier of Science and Future Technologies» (м. Дубай, Об’єднані Арабські Емірати, 3 квітня 2026 р.) – заочна форма участі.

Додаток Б. Копія свідоцтва про реєстрацію авторського права на твір



УКРАЇНА

СВІДОЦТВО

про реєстрацію авторського права на твір

№ 149653

Комп'ютерна програма «Інформаційна система захисту інтелектуальної власності на мультимедійні дані IP-Protect»

(вид, назва твору)

Автор (співавтори) **Овчинников Микола Юрійович**

(прізвище, ім'я, по батькові (за наявності), псевдонім (за наявності))

Авторські майнові права належать повністю **Овчинников Микола Юрійович, вул. Сонячна, 29, м. Південне, Одеська обл., 65481**

(прізвище, ім'я, по батькові (за наявності) фізичної особи / найменування юридичної особи, адреса)

Дата реєстрації 30 липня 2026 р.

Директор Державної організації «Український національний офіс інтелектуальної власності та інновацій» **Олена ОРЛЮК**

УКРНОІВІ

Додаток В. Таблиці

Таблиця В.1. Порівняльна характеристика систем захисту авторських прав на мультимедійні дані

Критерій	Класичні DRM-системи (контроль доступу)	Платформні системи (Content ID, фінгерпринтинг)	Блокчейн-орієнтовані системи (реєстр прав)	IP-Protect (стійкі приховані ідентифікатори)
Основний принцип роботи	Шифрування контенту та видача ліцензій; контроль доступу в закритій екосистемі постачальника.	Порівняння завантаженого контенту з базою еталонних відбитків; автоматичне блокування/монетизація.	Фіксація прав, ліцензій та транзакцій у розподіленому реєстрі; смарт-контракти для роялті.	Вбудовування стійкого прихованого ідентифікатора у сам мультимедійний файл із прив'язкою до реєстру авторів та ліцензій.
Тип маркера / ідентифікації	Явні ліцензії й ключі доступу; маркери «зовнішні» щодо файлу.	Аудіо/відео-відбиток у внутрішній базі платформи; сам файл маркера не містить.	Криптографічні хеші, ідентифікатори творів, записи смарт-контрактів.	Прихований ЦВЗ у структурі зображення/аудіо/відео + watermark_token у реєстрі + SHA-256.
Розташування ідентифікатора	Переважно поза файлом (сервери постачальника, ліцензійні сховища).	У базі даних платформи; файл окремо.	У блокчейні; мультимедійний файл зберігається окремо.	Безпосередньо у мультимедійному сигналі (ЦВЗ) + запис у реєстрі системи.
Залежність від платформи	Висока: механізми працюють лише в екосистемі постачальника DRM.	Дуже висока: ідентифікація можлива лише в межах конкретної платформи.	Середня: блокчейн публічний, але реалізації часто прив'язані до платформ.	Низька: витяг маркера можливий із будь-якої копії файлу незалежно від платформи.
Стійкість до стиснення, обрізки, переформатування	Обмежена: після виходу з DRM-середовища захист зникає.	Висока для відбитка в межах платформи; файл без маркера авторства.	Не застосовно: блокчейн не захищає від модифікації файлу.	Закладена як ключова вимога: тестування BER після MP3/AAC/JPEG; методи audio_pgdiff_v2, audio_mdct_qim_v3.
Публічна перевірка без реєстрації	Ні	Ні	Частково (публічний блокчейн для перевірки хешу).	Так: /public-check – завантаження файлу, результат перевірки, ліцензія без реєстрації.

Критерій	Класичні DRM-системи (контроль доступу)	Платформні системи (Content ID, фінгерпринтинг)	Блокчейн-орієнтовані системи (реєстр прав)	IP-Protect (стійкі приховані ідентифікатори)
Поетапна верифікація (хеш → відбиток → ЦВЗ)	Ні	Ні	Ні	Так: SHA-256 → phash/dhash / audio_fingerprint → витягнення ЦВЗ. Short-circuit при точному збігу.
Управління ліцензіями та умовами використання	Обмежено (ліцензії прив'язані до DRM-інфраструктури постачальника).	Ні (платформа вирішує монетизацію самостійно).	Так: смарт-контракти для ліцензій і роялті.	Так: All Rights Reserved, CC BY/SA/NC/ND, Free Use, Permission Required, Public Domain; контактний запит для permission_required.
Підтримка різних типів мультимедіа	Аудіо/відео; зображення – залежно від постачальника.	Переважно аудіо та відео; зображення рідше.	Будь-які типи даних.	Зображення (JPEG/PNG/GIF/WebP), аудіо (MP3/WAV/FLAC/AAC), відео (архітектурно).
Придатність до судового доказування	Опосередкована: журнали DRM залежать від довіри до оператора.	Обмежена: внутрішні журнали платформи складно верифікувати зовні.	Сильна для фіксації часу транзакцій; слабка щодо зв'язку конкретного файлу з записом.	Висока: ЦВЗ вбудовано у файл; доказовий звіт JSON/PDF із хешами, параметрами та часовими мітками.
Прозорість алгоритмів і механізмів	Низька: механізми DRM «чорна скринька».	Низька: алгоритми Content ID не розкриваються.	Середня: логіка смарт-контрактів прозора, технічні деталі – не завжди.	Висока: відкритий код (GitHub); параметри θ зберігаються у доказовому журналі.
Налаштовуваність без перерозгортання (RuntimeSettings)	Ні	Ні	Частково (зміна смарт-контрактів потребує нової транзакції).	Так: таблиця Setting (БД); всі параметри методів змінюються адміністратором через вебінтерфейс.
Роль модулів штучного інтелекту	Обмежена: аналіз поведінки користувачів	Ключова: ML для автоматичної ідентифікації та модерації	Зростаюча: аналіз транзакцій, класифікація контенту.	Допоміжна: Google Vision Web Detection для зображень; audio_pgdiff_v2 slide-match для аудіо; не замінює доказову перевірку.

Джерело: авторська розробка на основі [3, 4, 12, 15, 28, 29, 30].

Таблиця В.2. Запозичені елементи та авторські рішення у методі audio_pgdiff_v2

Елемент	Наукова основа	Рік	Що запозичено	Авторська модифікація
Компактний аудіовідбиток	Хайтсма, Калкер [8]; Кано та ін. [10]; Лі, Лім [11]	2003–2012	Ідея компактний відбиток за змістом; Hamming distance	FP будується з d_{seq} згортанням за модулем 64; не ДКП-відбиток і не карта спектральних піків
DCT + субсмугова енергетика	Ахмед та ін. [5]; Ху, Хсу [12]	1974–2015	Перехід до частотних коефіцієнтів; читання біта зі співвідношення енергій	Авторський вибір смуг B_low (120–600 Гц) та B_mid (600–2400 Гц); принцип лише-послаблення
QIM	Чен, Уорнелл [3]	2001	Кодування біта через вибір одного з двох стаціонарних станів ознаки	Ознака – log відношення енергій між смугами, а не квантування окремого DCT-коефіцієнта; абсолютний покадровий QIM
Стійкість до MP3 / time-scale attack	Сян та ін. [16]	2008	Аналіз MP3 як атакувального каналу; необхідність absolute-ознак	Перехід від диференціальної схеми до абсолютне відношення енергій усуває дрейф помилок при MP3
Психоакустичне маскування / непомітність	Свенсон та ін. [13]; Салах та ін. [15]	1998–2024	Обґрунтування роботи зі спектральними смугами; критерії SNR/ODG	Конкретний вибір частот і лише-послаблення обмежують помітність без явної психоакустичної моделі
Огляд аудіо-ЦВЗ (класифікація методів)	Хуа та ін. [14]; Салах та ін. [15]; Растєгаєв та ін. [20]	2016–2024	Контекст і систематизація класів методів	Огляди підтверджують конкурентоспроможність субсмугових енергетичних підходів у 2024 р.
Вибір несучих кадрів / стабільна щодо вбудовування ознака	Загальна ідея відбору стабільних сегментів	–	Відмова від маркування нестабільних ділянок	Відбір за high-band RMS – стабільної щодо вбудовування ознаки, інваріантною до вбудовування; усуває десинхронізацію перелік несучих кадрів
Пакет format, ECC, перемеження	Планк [19] (ECC); загальні принципи	1997	CRC-контроль; повторення бітів	Власний PGD1 формат пакета; повторення на рівні пакета (весь пакет, а не кожен біт); кільцеве перемеження
Нейромережеве аудіомаркування (контекст)	Лю та ін. [17] (XAttnMark); Сан Роман та ін. [18]	2024–2025	Актуальний стан проблеми; нові класи атак	audio_pgdiff_v2 – детерміністичний метод; не запозичує нейромережеву архітектуру, але враховує виявлені вразливості класичних схем

Додаток Г. Документи щодо впровадження результатів досліджень

«ЗАТВЕРДЖУЮ»
Ректор
Національного університету
«Одеська юридична академія»
_____ проф. Олег ГОДОЩАК
«___» _____ 2026 р.

АКТ ВПРОВАДЖЕННЯ
результатів дисертаційного дослідження
Овчинникова Миколи Юрійовича
«Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані»

Комісія у складі: проректора з навчальної роботи, доктора юридичних наук, професора Галини УЛЬЯНОВОЇ, завідувача кафедри кібербезпеки, доктора технічних наук, професора Артема СОКОЛОВА, завідувача кафедри штучного інтелекту та математичного моделювання, доктора економічних наук, професора Станіслава ГОРБАЧЕНКА засвідчує, що результати дослідження аспіранта Овчинникова Миколи Юрійовича, представленого на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки» використовуються в навчальному процесі Національного університету «Одеська юридична академія» при викладанні навчальних дисциплін «ІТ-маркетинг», «Експертиза та перевірка цілісності мультимедійних даних», «Адміністрування, аудит та безпека вебсистем», «Цифрові технології в бізнесі», «Прикладна криптографія», «Системи аутентифікації та цифрової ідентифікації», «Системи цифрових водяних знаків», «Основи ІТ бізнесу» та «DevOps», а також під час виконання кваліфікаційних робіт та в науково-дослідній роботі здобувачів.

Необхідність впровадження результатів дослідження зумовлена зростанням обсягів створення та поширення мультимедійного контенту в цифровому середовищі, а також потребою у надійних засобах підтвердження належності та цілісності цифрових об'єктів. Запропонована інформаційна система та методи цифрового маркування і перцептивної ідентифікації дають змогу формувати відтворювані результати перевірок і забезпечувати доказовість процедур у випадках несанкціонованого використання контенту. Інтеграція зазначених підходів у навчальний процес сприяє формуванню у здобувачів компетентностей у сфері захисту інтелектуальної власності на мультимедійні дані та практичної реалізації відповідних технічних і організаційних заходів.

Впровадження результатів дисертації в навчальний процес здійснюється через:

- використання авторського програмного прототипу інформаційної системи для маркування та перевірки мультимедійних даних як навчального стенду під час лабораторних занять та виконання індивідуальних завдань;
- інтеграцію розроблених алгоритмічних модулів (вбудовування/детектування цифрових водяних знаків, формування перцептивних відбитків, протоколювання результатів перевірок) у практичні роботи з дисциплін «Системи цифрових водяних знаків», «Експертиза та перевірка цілісності мультимедійних даних», «Прикладна криптографія» та «Системи аутентифікації та цифрової ідентифікації»;
- використання методичних матеріалів дисертанта (презентацій, кейсів, лабораторних практикумів) як додаткових джерел у силабусах освітніх компонентів та при підготовці кваліфікаційних робіт здобувачів освіти.

Результати дослідження планується і надалі використовувати при підготовці бакалаврів, магістрів та докторів філософії на факультеті кібербезпеки та інформаційних технологій. Це сприятиме формуванню у студентів системного розуміння процесів захисту інтелектуальної власності на мультимедійні дані, побудови доказової бази та застосування сучасних інструментів цифрового маркування і верифікації в умовах викликів цифрового середовища.

Члени комісії:

Проректор з навчальної роботи,
доктор юридичних наук, професор — Галина УЛЬЯНОВА

Завідувач кафедри кібербезпеки,
доктор технічних наук, професор — Артем СОКОЛОВ

Завідувач кафедри штучного інтелекту
та математичного моделювання,
доктор економічних наук, професор — Станіслав ГОРБАЧЕНКО

ДОВІДКА

про використання результатів дисертаційного дослідження
Овчинникова Миколи Юрійовича на тему:
«Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані»

Забезпечення довіри до цифрового контенту та захист прав інтелектуальної власності на мультимедійні дані (зображення, відео, аудіо) є важливим завданням у сучасному цифровому середовищі, зокрема в контексті протидії несанкціонованому копіюванню, підробленню та поширенню матеріалів із порушенням прав правовласників.

Фахівці Державної служби спеціального зв'язку та захисту інформації України ознайомилися з матеріалами дисертаційного дослідження Овчинникова М. Ю. та відзначають практичну спрямованість запропонованих рішень, які орієнтовані на створення цілісної інформаційної системи захисту мультимедійних об'єктів із застосуванням сучасних методів маркування та ідентифікації.

У дисертації запропоновано підхід, що поєднує: вбудовування та перевірку цифрових водяних знаків як засобу підтвердження належності/походження мультимедійного об'єкта; формування перцептивних відбитків (fingerprinting / perceptual hashing) для пошуку копій та близьких за змістом варіантів контенту навіть після типових перетворень (стиснення, масштабування, перекодування, фільтрація тощо); двоступеневий процес «пошук кандидатів → верифікація», який підвищує достовірність встановлення відповідності та зменшує кількість хибних спрацювань; протоколювання результатів перевірок і формування звітних матеріалів, що може бути корисним для фіксації результатів аналізу та підготовки доказових матеріалів у межах правового реагування.

Результати дисертаційного дослідження можуть бути використані під час опрацювання підходів до маркування та верифікації мультимедійного контенту, а також для удосконалення процедур виявлення несанкціонованого використання цифрових матеріалів у відкритих та корпоративних інформаційних середовищах.

Додатково напрацювання автора можуть бути корисними для формування методичних підходів до технічної перевірки походження мультимедійних файлів і накопичення доказової інформації у вигляді протоколів, журналів подій та звітів перевірки. Такий підхід сприяє стандартизації процедур фіксації результатів аналізу та підвищує якість підготовки матеріалів для подальшого розгляду в межах відповідних організаційних і правових процедур.

Враховуючи викладене вище, напрацювання автора можуть становити практичний інтерес для застосування/пілотного впровадження у відповідних напрямах діяльності Державної служби спеціального зв'язку та захисту інформації України.

Т.в.о. начальника Управління
Держспецзв'язку в Одеській області
полковник Денис ПОПОВ

ОДЕСКАБЕЛЬ ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО

ДОВІДКА

Про використання результатів наукових досліджень

Овчинникова Миколи Юрійовича

представлених в дисертації на здобуття наукового ступеня доктора філософії за спеціальністю 122 «Комп'ютерні науки»

«Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані»

Керівництво ПАТ «ОДЕСКАБЕЛЬ» ознайомилося з результатами наукового дослідження Овчинникова М. Ю. та прийняло до використання у практичній діяльності запропоновані в дисертації підходи й програмні засоби, спрямовані на підвищення рівня захисту прав інтелектуальної власності на мультимедійні дані (зображення, відео та інші цифрові матеріали), що використовуються у виробничій, маркетинговій та інформаційній діяльності підприємства.

З огляду на специфіку роботи підприємства як одного з провідних виробників кабельно-провідникової продукції, особливу практичну цінність становить розроблена в дисертації інформаційна система, яка забезпечує комплексний захист мультимедійних об'єктів за рахунок:

- вбудовування та подальшої перевірки цифрових водяних знаків для підтвердження авторства/належності контенту правовласнику;
- формування цифрових «відбитків» (перцептивних ознак / perceptual fingerprinting) для швидкого пошуку схожих копій матеріалів навіть після типових змін (стиснення, масштабування, обрізання, додавання шуму);
- реалізації двоступеневого процесу «пошук кандидатів → верифікація», що дозволяє зменшити кількість хибних спрацювань та підвищити достовірність підтвердження факту копіювання;
- автоматизації протоколювання результатів перевірки та формування звітних матеріалів, які можуть використовуватися в межах внутрішніх процедур реагування та підготовки доказової бази для правового захисту.

Результати дисертаційного дослідження використовуються в поточній діяльності ПАТ «ОДЕСКАБЕЛЬ» для організації процесів маркування та контролю використання мультимедійних матеріалів (зокрема, зображень продукції, ілюстрацій, презентаційних матеріалів, елементів цифрових каталогів), а також для підвищення ефективності виявлення несанкціонованого дублювання/поширення контенту. Застосування запропонованих методів і програмних модулів сприяє скороченню часу перевірки, стандартизації процедури встановлення факту запозичення та підвищенню відтворюваності результатів контролю.

Генеральний директор Вадим ІОРГАЧОВ

Миколаївська дорога, 144,
Одеса, 65102,
Україна

Тел.: +38 048 716 14 03
+38 048 716 14 04
Факс: +38 048 716 14 01

www.odeskabel.com
office@odeskabel.com

TÜV AUSTRIA CERTIFIED
Система менеджменту EN ISO 9001:2015 ID: 20100223015100 www.tuv.at

ДОВІДКА

про використання результатів дисертаційного дослідження
Овчинникова Миколи Юрійовича на тему:
«Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані»

Забезпечення доказовості походження цифрового контенту та захист прав інтелектуальної власності на мультимедійні дані (зображення, відео, аудіо) є важливим завданням у сучасному мережевому середовищі, зокрема в контексті протидії несанкціонованому копіюванню, підробленню, повторному розміщенню та комерційному використанню матеріалів із порушенням прав правовласників.

Фахівці Управління протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України ознайомилися з матеріалами дисертаційного дослідження Овчинникова М. Ю. та відзначають практичну спрямованість запропонованих рішень, які орієнтовані на створення цілісної інформаційної системи захисту мультимедійних об'єктів із застосуванням сучасних методів маркування, ідентифікації та документування результатів перевірки.

У дисертації запропоновано підхід, що поєднує технологічні механізми прихованої ідентифікації та аналітичні процедури перевірки мультимедійного контенту. Зокрема, розглянуто вбудовування та перевірку цифрових водяних знаків як засобу підтвердження належності/походження мультимедійного об'єкта, формування перцептивних відбитків (fingerprinting / perceptual hashing) для пошуку копій та близьких за змістом варіантів контенту навіть після типових перетворень (стиснення, масштабування, перекодування, фільтрація тощо), а також двоступеневий процес «пошук кандидатів → верифікація», який підвищує достовірність встановлення відповідності та зменшує кількість хибних спрацювань.

Окрему практичну цінність становить протоколювання результатів перевірок і формування звітних матеріалів із параметрами обробки, кількісними метриками та підсумковими статусами перевірки, що може бути корисним для фіксації результатів аналізу та підготовки матеріалів у межах реагування на правопорушення, пов'язані з незаконним обігом цифрового контенту.

Результати дисертаційного дослідження можуть бути використані під час опрацювання підходів до виявлення несанкціонованого використання мультимедійних матеріалів у відкритих та корпоративних інформаційних середовищах, а також для удосконалення процедур технічної верифікації походження цифрових файлів і підготовки структурованих матеріалів перевірки.

Враховуючи викладене вище, напрацювання автора можуть становити практичний інтерес для застосування/пілотного впровадження у відповідних напрямах діяльності Управління протидії кіберзлочинам в Одеській області Департаменту кіберполіції Національної поліції України.

Начальник
Управління протидії кіберзлочинам в Одеській області
Департаменту кіберполіції
Національної поліції України **Анатолій ФІЛЬ**

ДОВІДКА

Про використання результатів наукових досліджень
Овчинникова Миколи Юрійовича
представлених в дисертації на здобуття наукового ступеня доктора філософії
за спеціальністю 122 «Комп'ютерні науки» на тему:
«Розробка інформаційної системи захисту інтелектуальної власності на мультимедійні дані»

Комерційна діяльність ТОВ «КІПСОЛІД УКРАЇНА» пов'язана з активним використанням цифрових каналів, веб-ресурсів і мультимедійного контенту (зображення, відео, графічні матеріали), що потребує надійного захисту прав інтелектуальної власності та контролю несанкціонованого копіювання. У цьому контексті тематика дисертаційного дослідження Овчинникова М. Ю. є практично релевантною потребам компанії, оскільки орієнтована на розробку та впровадження інформаційної системи захисту інтелектуальної власності на мультимедійні дані із застосуванням сучасних методів цифрових водяних знаків і перцептивного відбиткування.

Результати дослідження дисертанта пройшли практичну апробацію в діяльності ТОВ «КІПСОЛІД УКРАЇНА». Зокрема, в компанії використано підхід комбінованого захисту мультимедійних матеріалів, що включає вбудовування цифрових водяних знаків та формування перцептивних "відбитків" для виявлення копій і похідних версій контенту навіть після типових модифікацій. Це дозволило:

- структурувати процеси маркування та контролю використання мультимедійних матеріалів у корпоративних і публічних каналах;
- підвищити оперативність виявлення фактів несанкціонованого дублювання/поширення контенту в мережі Інтернет та внутрішніх інформаційних середовищах;
- забезпечити відтворюваність і доказовість результатів перевірки завдяки протоколюванню та формуванню звітів щодо перевірених об'єктів.

Використання двоступеневого процесу «пошук кандидатів → верифікація» (попередній пошук схожих об'єктів за цифровим відбитком із подальшим підтвердженням за водяним знаком) забезпечило оптимізацію часу перевірки та зменшення кількості хибних спрацювань при моніторингу використання мультимедійних матеріалів. Застосування зазначеного підходу дозволило компанії уникати надмірних витрат часу на ручну експертизу та підвищити якість внутрішнього контролю цифрових активів.

Апробація наукових положень дисертації Овчинникова М. Ю. підтвердила їхню прикладну цінність для підвищення ефективності захисту прав інтелектуальної власності на мультимедійні дані, стандартизації процедур перевірки та забезпечення підготовки матеріалів для правового реагування у випадках порушення авторських прав. Запропоновані підходи інтегровані в практику роботи ТОВ «КІПСОЛІД УКРАЇНА» та використовуються у процесах створення, публікації і контролю використання мультимедійного контенту.

Керівник громадської організації
«ОСВІТНІЙ ФОНД КІПСОЛІД» Віктор ЯЦЕНКО