УДК 004.056.5 DOI https://doi.org/10.35546/kntu2078-4481.2024.3.32

М. Ю. ОВЧИННИКОВ
асистент кафедри кібербезпеки
Національний університет «Одеська юридична академія»
ORCID: 0009-0009-8221-7193

В. М. СЛАТВІНСЬКА
доктор філософії, асистент кафедри кібербезпеки
Національний університет «Одеська юридична академія»
ORCID: 0000-0002-6082-981X

ТЕХНІЧНИЙ ТА НОРМАТИВНО-ПРАВОВИЙ АСПЕКТИ ЗАХИСТУ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ НА РИНКУ АУДІО-ВІЗУАЛЬНОЇ ПРОДУКЦІЇ

У статті детально досліджуються виклики та потенційні рішення у сфері захисту інтелектуальної власності на аудіовізуальні продукти. Мета цієї статті – дослідити різні аспекти захисту прав інтелектуальної власності на ринку аудіовізуальної продукції України, зосередившись на її технічних та юридичних аспектах. Автори прагнуть надати повний огляд наявних методів та інструментів, які використовуються для захисту авторських прав на аудіовізуальні твори, а також розглянути їхню ефективність на практиці.

Дослідження виявило, що Україна має відповідні правові норми, які регулюють захист інтелектуальної власності на аудіовізуальну продукцію, зокрема Закон України «Про авторське право і суміжні права». Однак, на практиці існують значні проблеми, пов'язані з відсутністю сучасної інфраструктури, недостатньою інформованістю громадян, слабкими інститутами контролю та виконання права. Автори статті надають детальний опис відомих існуючих методів стеганографії, які використовуються для захисту цифрових аудіо та відеофайлів, таких як використання цифрового водяного знака (ЦВЗ) та інших стеганографічних технік. Вони також розглядають можливості використання глибинного навчання та нейронних мереж, які надають нові перспективи щодо стійкості ЦВЗ до різних атак.

Стаття дійшла висновку, що ефективний захист інтелектуальної власності на ринку аудіовізуальної продукції України вимагає комплексного підходу, який включатиме як технічні, так і юридичні заходи. Необхідним є розвиток інформаційних систем, які дозволять відстежувати та припиняти піратство, а також підвищення рівня обізнаності населення щодо прав інтелектуальної власності. Автори також акцентують на значенні міжнародної співпраці та імплементації міжнародних стандартів у національне законодавство, щоб створити єдиний, взаємовигідний та конкурентоспроможний ринок.

Під час дослідження було виявлено, що деякі методи стеганографії, такі як використання ЦВЗ на основі реверберації, можуть бути досить вразливими до атак, які націлені на придушення цієї техніки. Тому важливо розробляти більш надійні та універсальні підходи, які були б стійкими до різного роду атак.

Ключові слова: *аудіовізуальні твори, авторське право, стеганографія, цифровий водяний знак, нейронні мережі, захист інформації, комп'ютерні науки, методика реверберації.*

M. YU. OVCHINNIKOV
Assistant at the Department of the Cybersecurity
National University "Odesa Law Academy"
ORCID: 0009-0009-8221-7193

V. M. SLATVINSKA
PhD, at the Department of the Cybersecurity
National University "Odesa Law Academy"
ORCID: 0000-0002-6082-981X

TECHNICAL AND REGULATORY ASPECTS PROTECTION OF INTELLECTUAL PROPERTY IN THE AUDIO-VISUAL MARKET

The article underscores the significance of a robust legal framework capable of adapting to the unique challenges posed by the digital age. Despite some progress, substantial gaps and inconsistencies persist in the legal landscape, hindering the effective defense of intellectual property rights in the audio-visual sector. This domain is paramount as the industry contributes significantly to Ukraine's economy, creating employment opportunities and generating substantial revenue.

The study delves into the intricacies of protecting multimedia data, focusing on digital watermarking technology, which embeds hidden information within audio and video files. The relevance of such technology is highlighted by the prevalence of piracy and unauthorized distribution that threaten the financial stability of content creators and distributors.

The article explores the intersection of law and technology, emphasizing the need for a comprehensive approach to preserve the rights of authors and producers in the digital era.

The legal dimension of the issue is outlined, highlighting the rights of authors and producers under Ukrainian copyright law. The exclusive rights to reproduce, distribute, and communicate audio-visual works to the public are emphasized, as well as the personal non-property rights, such as the right to be recognized as the author and the right to protect the work from distortion. Protecting intellectual property rights involves several key stages and stakeholders, encompassing civil, administrative, and criminal legal measures.

The article presents a technical analysis of digital signal processing, specifically the discretization and quantization of analogue signals to produce digital ones. This is essential for understanding the mechanisms of digital watermarking, which rely on the subtle alteration of the digital signal to incorporate hidden data.

A notable steganographic technique discussed is the use of reverberation. This phenomenon is a natural byproduct of sound waves reflecting off enclosed surfaces, creating an echo effect. The article suggests modulating the time delay between the original signal and the reverberation to encode data. However, the authors concede that this approach is susceptible to deliberate attempts to suppress reverberation, such as noise reduction algorithms, which can inadvertently erase the embedded watermark.

Another method explored is the Gaussian model, which, while theoretically promising for embedding and extracting one bit of information, faces practical limitations due to the complexity of real-world audio signals. The article acknowledges the challenges inherent in creating a universally applicable solution for digital watermarking and the necessity of continual research to improve the resilience of these methods against intentional attacks and unauthorized alterations.

In conclusion, the article underscores the critical nature of protecting intellectual property in the audio-visual market, emphasizing the interplay between legal frameworks and technological advancements. It calls for a multidisciplinary approach to tackle the evolving challenges of digital piracy and ensure a thriving and innovative industry that can attract foreign investment and contribute positively to Ukraine's international reputation.

Key words: *audiovisual works, copyright, steganography, digital watermark, neural networks, information security, computer science, reverberation technique.*

Постановка проблеми

Сутність проблеми захисту прав інтелектуальної власності на ринку аудіовізуальної продукції в Україні полягає у відсутності комплексної та ефективної правової бази, яка б адекватно реагувала на унікальні виклики, що постають перед цим сектором. Зі стрімким розвитком технологій та легкістю доступу до цифрового контенту захист аудіовізуальної продукції від піратства, несанкціонованого розповсюдження та неправомірного використання стає дедалі складнішим. Незважаючи на певний прогрес, досягнутий за останні роки, все ще існують значні прогалини та неузгодженості в нормативно-правовому полі, які перешкоджають ефективному захисту прав інтелектуальної власності на аудіовізуальному ринку. Тому вивчення цього питання є вкрай важливим, оскільки аудіовізуальна індустрія робить значний внесок в економіку України, працевлаштовуючи тисячі людей та генеруючи мільярди доларів доходу. Захист прав інтелектуальної власності в цьому секторі не лише забезпечує фінансову стабільність авторів, виробників та дистриб'юторів, але й сприяє створенню здорового та конкурентного ринкового середовища, яке заохочує інновації та інвестиції. Більше того, оскільки Україна продовжує інтегруватися у світову економіку, ефективний захист прав інтелектуальної власності на аудіовізуальному ринку стає все більш важливим для створення репутації надійного партнера та залучення іноземних інвестицій.

Аналіз останніх досліджень і публікацій

Тема захисту мультимедійних даних обговорюється у наукових колах досить давно. Публікації присвячені питанням та методам захисту авторських прав на аудіо та відео продукцію постійно оновлюються й автори цих публікацій пропонують різноманітні вдосконалення вже наявних методів або принципово нові. В основному все зводиться до застосування методів стеганографії для розміщення цифрового водяного знака (ЦВЗ) в мультимедійних даних.

Інтерес викликає стаття, присвячена сталій системі водяних знаків для перезапису звуку з урахуванням глибокого навчання [8]. Дослідники вивчають проблему вбудовування стійких цифрових водяних знаків під час перезапису звуку. ЦВЗ на аудіо широко використовуються для відстеження джерела витоку даних. Наприклад, один і той же аудіофайл, який використовують різні відділи однієї організації або різні люди позначається різними ЦВЗ. Це дає змогу звузити коло при пошуку джерела витоку даних. Надійність водяного знака визначає можливість відстеження алгоритму приховування інформації. З розвитком цифрових технологій перезапис звуку (Audio Recording, AR) став ефективним та потайним способом крадіжки секретів. Процес AR може значно зруйнувати сигнал водяного знака, зберігаючи вихідний зміст. Це ставить нову вимогу до звукових водяних знаків бути стійкими до спотворень AR. На жаль, жоден з існуючих алгоритмів не здатний ефективно протистояти атакам AR через складність цього процесу. Щоб вирішити цю проблему, у цій статті пропонується DeAR (A Deep-Learning-Based Audio Re-recording Resilient Watermarking), система водяних знаків, стійка до перезапису звуку, що базується на глибокому навчанні. Розвиток нейромереж привів до виявлення DNN Watermarking (deep neural network

watermarking) – технологія влаштування ЦВЗ в медіафайли з використанням глибокої нейронної мережі. Автори спробували застосувати дану технологію для аудіофайлів. Вони розробили систему глибокого навчання для аудіо, яка дозволяє ефективно впроваджувати та отримувати сигнал водяного знака. Крім того, щоб протистояти атакам AR, автори ретельно проаналізували спотворення, що виникають у процесі AR, та розробили відповідний шар спотворень для взаємодії з запропонованою структурою водяних знаків. Великі експерименти показують, що запропонований алгоритм здатний протистояти як звичайним спотворенням електронного каналу, а й спотворенням AR. При високій якості впровадження (SNR=25,86 дБ) та відстані перезапису 20 см алгоритм досягає середньої точності відновлення бітів 98,55% [8].

Автор іншої статті Світловський О.В. [9] провів систематизацію моделей та алгоритмів створення ЦВЗ для аудіофайлів. Автором розроблено моделі та алгоритми створення цифрових водяних знаків у звукових форматах. Проведено дослідження для різних форматів представлення даних, а також досліджено можливості їх застосування в аудіофайлах. Розглянуто методики та результати аналізу статистичної непомітності та можливості відновлення вбудованої послідовності ЦВЗ стороннім спостерігачем для оцінки якості ЦВЗ в об'єктах звукових форматів. Також досліджено побудову та використання універсальних перетворень стиснення для стеганографічного вбудовування ЦВЗ в об'єкти-контейнери різних типів з мінімальним рівнем дисперсії спотворень на основі штучних двошарових нейронних мереж прямого поширення, що дозволяє підвищити ефективність та захищеність передачі прихованих даних каналами. Обґрунтовано доцільність такого методу. Автором розроблено спеціальне математичне та програмне забезпечення для створення цифрових водяних знаків для аудіоданих.

Також можна згадати роботи, які присвячені дослідженню стійкості різних алгоритмів стеганографії: Voloshynovskiy S. [10], Popa R. [11], Johnson N. F. [12].

Формулювання мети дослідження

Мета статті – визначити способи захисту об'єктів інтелектуальної власності на аудіовізуальну продукцію з технічної та юридичної точок зору.

Викладення основного матеріалу дослідження

Стаття 6 Закону України «Про обов'язковий примірник документів» вказує: «Аудіовізуальною продукцією є кіно-, відео-, фото-, фонодокументи» [1]. Натомість звужуємо розгляд зазначених об'єктів авторського права до аудіо-. Тобто музичні твори (з текстом або без тексту), аудіовізуальні твори є об'єктами авторського права згідно зі ст. 430 Глави 36 Цивільного кодексу України [2].

Як правило, згідно зі статтею 41 Конституції України: «Кожен має право володіти, користуватися і розпоряджатися своїм майном, що є результатом інтелектуальної і творчої діяльності» [3].

Водночас виключний перелік суб'єктів-авторів аудіовізуальних творів визначено у частині 16 статті 1 Закону України «Про авторське право і суміжні права» [4]. Тобто йдеться про власників майнових та особистих немайнових прав на аудіовізуальні твори.

Зокрема майновими правами на аудіовізуальний твір є: «Право на виготовлення примірників аудіовізуального твору, право на продаж, здавання в оренду, дарування примірників аудіовізуального твору, право на показ аудіовізуального твору публіці, право на передачу аудіовізуального твору в ефір або по кабелю, право на доведення аудіовізуального твору до загалу таким чином, що кожен користувач може мати доступ до нього в будь-який час і в будь-якому місці за власним вибором, право на створення нового твору на основі існуючого, право на субтитрування, озвучення (дублювання), переклад» [4]. При цьому майнові права на аудіовізуальний твір зазвичай переходять до продюсера з моменту створення твору або можуть залишатися у авторів за договором відповідно до ч. 2 тієї ж статті.

Особистими немайновими правами авторів є: «Право визнаватися автором твору, право на використання твору під своїм справжнім ім'ям або псевдонімом, право на захист твору від будь-якого викривлення, скорочення або іншої зміни, право на оприлюднення твору, право на отримання винагороди за використання твору» [4]. Особисті немайнові права залишаються у авторів і не можуть бути передані згідно ч. 2 тієї ж статті.

Стосовно використання аудіовізуального твору то обов'язково потрібна згода автора або правовласника. Натомість можливі і винятки, передбачені законом [4].

Під захистом авторських прав на аудіовізуальні твори слід розуміти комплекс заходів, спрямованих на охорону прав авторів та інших суб'єктів авторського права на аудіовізуальні твори.

При цьому захист авторських прав на аудіовізуальні твори відбувається 3 способами. Зокрема цивільно-правовими, адміністративно-правовими та кримінально-правовими. Цивільно-правові способи захисту включають в себе визнання права, відшкодування шкоди, зупинення порушення, вилучення контрафактної продукції [5, с. 115]. Адміністративно-правові способи захисту – це: накладення штрафу, конфіскація контрафактної продукції. До кримінально-правових способів захисту належать: позбавлення волі, штраф, обмеження волі.

Серед відомих юридичних методів захисту авторських прав на аудіовізуальні твори можна назвати державну реєстрацію авторських прав, яка не є обов'язковою, але з офіційним підтвердженням автора і дати створення твору, використання знака авторського права, укладення договору і судовий захист.

Тобто процес захисту об'єктів інтелектуальної власності на ринку аудіовізуальної продукції в Україні включає кілька ключових етапів та зацікавлених сторін, що зображено на Рис. 1:

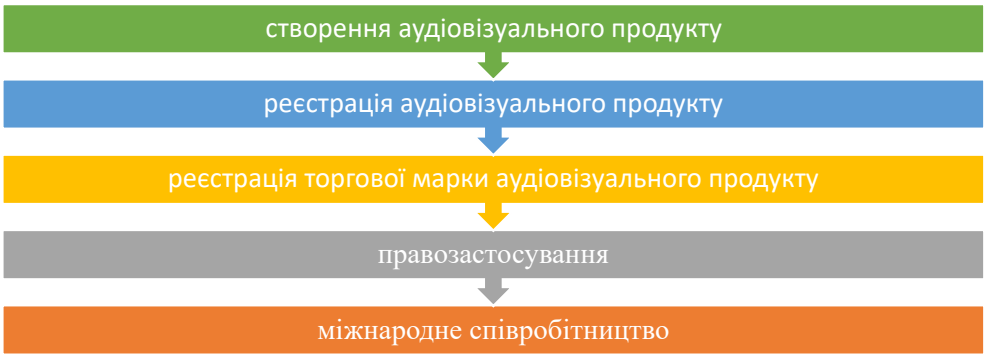

Рис. 1. Процес захисту інтелектуальної власності аудіовізуального продукту

Джерело: авторська розробка

Звернемо увагу, як видно з рис. 1 процес захисту інтелектуальної власності аудіовізуального продукту складається із 5 взаємопов'язаних кроків.

Зокрема, спочатку творець контенту або продюсер має на меті розробити аудіовізуальний продукт, як фільм, телевізійне шоу або рекламний ролик. А вже після того, як продукт завершено, творець повинен зареєструвати його у відповідних органах, щоб встановити право власності та захистити права інтелектуальної власності.

Загальновідомо, що в Україні захист авторських прав автоматично поширюється на оригінальні твори, включаючи аудіовізуальну продукцію. Проте реєстрація авторського права забезпечує додатковий правовий захист і полегшує реалізацію прав. Реєстрацією авторських прав на аудіовізуальні твори займається Державне підприємство «Український інститут інтелектуальної власності» (УКРПАТЕНТ). Згідно з пунктом 4 Постанови Кабінету міністрів України від 18.07.1995 № 532 «Про державну реєстрацію прав автора на твори науки, літератури і мистецтва»: «Міністерство культури забезпечує на базі Державного фонду фільмів Національного центру Олександра Довженка опрацювання матеріалів, поданих у зв'язку з державною реєстрацією прав автора на аудіовізуальні твори, та окреме, недоступне для запозичення, зберігання позитивних кінокопій і вихідних матеріалів аудіовізуальних творів» [6].

Якщо аудіовізуальний продукт містить будь-які відмітні елементи, такі як логотип або брендинг, творець може також захотіти зареєструвати торгову марку, щоб захистити інтелектуальну власність, пов'язану з цими елементами. Реєстрацією торгових марок займається Державна організація «Український національний офіс інтелектуальної власності та інновацій» (УКРНОІВІ).

Відповідно до пункту 33 статті 1 Закону «Про медіа» [7] український аудіовізуальний ринок також має власний орган саморегулювання – Національну раду з питань телебачення і радіомовлення. Він розробляє та впроваджує галузеві стандарти, розглядає скарги та суперечки, а також здійснює моніторинг ефіру на предмет несанкціонованого використання об'єктів інтелектуальної власності.

Після того, як права інтелектуальної власності були створені та зареєстровані, творці та виробники повинні забезпечити дотримання цих прав, щоб запобігти їх порушенню. Це включає моніторинг ринку на предмет несанкціонованого використання, видачу листів з вимогою припинити порушення, подання судових позовів проти порушників та співпрацю з правоохоронними органами з метою вилучення контрафактної продукції.

Варто підкреслити, що Україна є членом кількох міжнародних організацій, що займаються питаннями захисту прав інтелектуальної власності, включаючи Всесвітню організацію інтелектуальної власності та Європейську патентну конвенцію. Це членство дозволяє Україні співпрацювати з іншими країнами з метою обміну передовим досвідом, координації зусиль у сфері правозастосування та захисту прав інтелектуальної власності на глобальному рівні.

У цьому процесі зацікавлені сторони, такі як творці контенту, продюсери, дистриб'ютори, мовники та юристи у сфері інтелектуальної власності, відіграють вирішальну роль у забезпеченні захисту та дотримання прав інтелектуальної власності на українському аудіовізуальному ринку.

Технічний захист авторських прав на аудіовізуальні твори – це комплекс заходів щодо захисту творів від несанкціонованого доступу, копіювання, розповсюдження та використання.

Питання юридичного захисту авторських прав тісно пов'язані з технічним захистом аудіовізуальної продукції. У цілому нині технічний захист об'єктів аудіовізуальної продукції полягає в розміщенні міток всередині файлу для ідентифікації правовласника. Такі мітки повинні бути непомітними, стійкими до випадкової або навмисної зміни або видалення, а також легко розпізнаватись при необхідності ідентифікації. Крім того, враховуючи, що

більшість форматів зберігання аудіо та відео інформації піддаються стиску за допомогою різних алгоритмів, які використовують надмірність такого типу даних, обов'язково має дотримуватися цілісність авторських міток при компресії файлів.

Такі мітки повинні зберігатися й у разі копіювання звукового або відео файлу навіть у випадку, коли об'єкт копіювання знаходиться на відстані від запису і на копію додатково накладаються перешкоди, спотворення, шуми.

Стеганографія дозволяє розміщувати об'єкти з конфіденційною інформацією всередині якогось контейнера з даними таким чином, що сам факт присутності всередині контейнера якихось даних теж прихований. У нашому випадку контейнером виступає аудіо або відеофайл, а в якості прихованої інформації виступають дані про правовласника.

Таку приховану інформацію прийнято називати цифровим водяним знаком (ЦВЗ). Принцип вбудовування ЦВЗ у файл, що містить мультимедійні дані та виділення ЦВЗ з нього показано на Рис. 2:

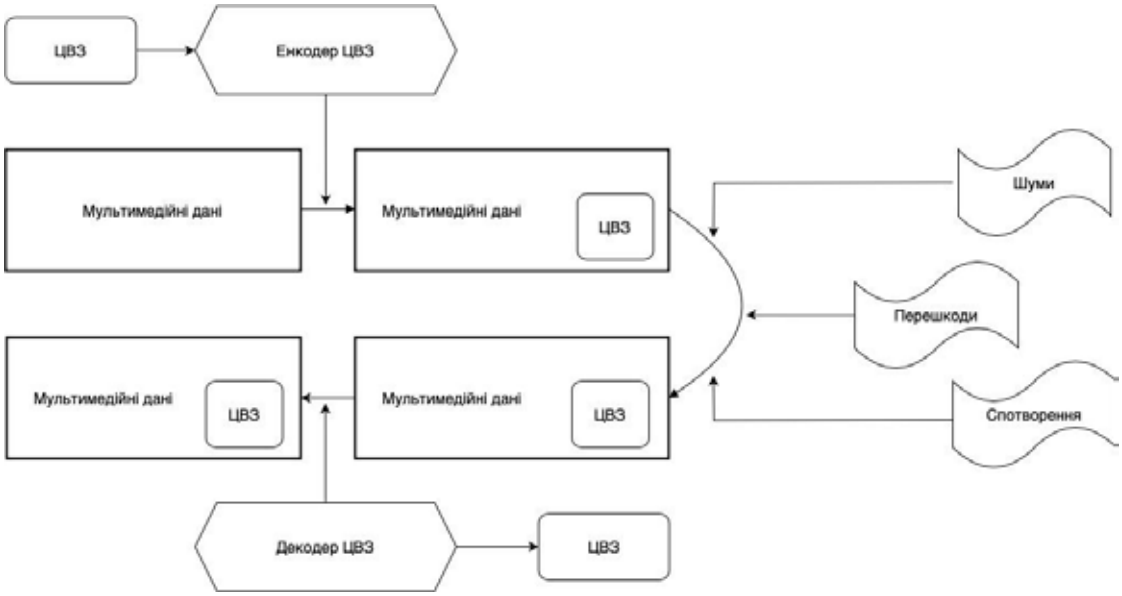

Рис. 2. Структурна схема роботи з ЦВЗ для мультимедійного файлу

Джерело: авторська розробка

YouTube Content ID. У деяких випадках підтвердити авторські права на аудіо або відео можна простим порівнянням. Саме так реалізовано захист авторських прав на майданчику найбільшого відео хостингу YouTube, який було створено у 2005 році та придбано компанією Google у 2006 році. І вже у 2007 році було розроблено та впроваджено систему цифрової ідентифікації контенту Content ID для захисту авторських прав на відео платформі YouTube [13, 14, 19]. Суть цієї системи полягає в порівнянні нових відео файлів, які завантажуються на платформу YouTube із завантаженими раніше. Порівняння відбувається за візуальною та аудіо складовою завантажуваного файлу. Якщо коефіцієнт схожості вище заданих системою параметрів, система вважає відео таким, що порушує авторські права користувача, відео якого вже є в системі. Збіг може бути повним або частковим. Звичайно, можлива ситуація, коли відео завантажене на платформу раніше за правовласника, але система налаштована так, що не всі, хто завантажує відео є учасниками системи Content ID. Для того щоб користуватися її можливостями, необхідно відповідати низці вимог. Варто зважити і на те, що не всі правовласники користуються цією системою. Також, якщо користуватися послугами дистриб'юторів цифрового контенту, автори мають можливість включати або вимикати Content ID, а також робити винятки для деяких користувачів при включеному Content ID.

Загалом різних комбінацій умов може бути чимало. Система не ідеальна, крім того, порівняння вимагає від платформи багато обчислювальних ресурсів. Для оптимізації роботи Content ID в систему потрапляють лише відео, тривалість яких перевищує 30 секунд. Незважаючи на недоліки, система Content ID дозволяє в більшості випадків захистити особливо популярних авторів від копіювання їх творів усередині відео платформи.

Використання такого методу є допустимим в рамках окремо взятого сервісу, але не вирішує глобального завдання, якщо врахувати те, що тільки на YouTube щодня завантажується близько 4 мільйонів нових відео.

Для надійного захисту ЦВЗ у мультимедійних даних можна використовувати цифрові, криптографічні і стеганографічні методи та його комбінації.

Теги ID3v2 для звукових файлів MP3. Найпростіший спосіб розміщення ЦВЗ в мультимедійних даних має на увазі розміщення мітки безпосередньо в коді файлу або в його мета даних. Файли формату MP3 (скор. від

MPEG-1 Audio Layer III або MPEG-2 Audio Layer III) містять різні аудіодані, такі як звуки, звукові ефекти, музику та голосові записи. Згодом структура цих файлів змінювалася. В даний час можна виділити два основні компоненти MP3 файлу: ID3-тег і послідовність кадрів (фреймів). Структура формату чимось нагадує кіноплівку.

ID3-тег другої версії розміщується на початку файлу (у версії ID3v2.3, яка є найбільш поширеною на сьогоднішній день) або наприкінці файлу (у версії ID3v2.4) та містить різноманітну довідкову інформацію. Наприклад, для музичних композицій ID3 тег включає ім'я треку, альбому, виконавця та інші дані.

ID3 (від англ. IDentify MP3) – надзвичайно популярний формат тегів даних аудіофайлів. Теги ID3 підтримуються в iTunes, Windows Media Player, Winamp, YME, MusicMatch та апаратних програвачах, таких як iPod, Creative Zen, Toshiba Gigabeat та Sony Walkman. Тег ID3 є контейнером метаданих, який найчастіше використовується в поєднанні з форматом аудіофайлів MP3. Теги ID3 дозволяють передавати таку інформацію, як назва, виконавець, альбом, трек, рік, обкладинка або іншу інформацію про файл [15].

Таблиця 1

Структура вмісту файлу MP3

Область тега ID3v2	**Фрейм тега ID3v2**	**Область заголовка тега ID3v2**	**Заголовок фрейму містить поля: Ідентифікатор, Розмір, Прапори**
		Вміст фрейму тега	Метадані
	…	…	…
	Фрейм тега ID3v2	Область заголовка тега ID3v2	Заголовок фрейму містить поля: Ідентифікатор, Розмір, Прапори
		Вміст фрейму тега	Метадані
Область аудіо даних	Область фреймів (один або більше фреймів)	Фрейм MP3	Заголовок фрейма
			Аудіо дані
		…	…
		Фрейм MP3	Заголовок фрейма
			Аудіо дані

Джерело: авторська розробка.

Як показано у таблиці 1, файл MP3 може містити область тега ID3 з областю аудіоданих [15]. Тег ID3 складається з таких компонентів: заголовка, та одного або кількох кадрів різного змісту [16]. ID3v2 має змінну довжину і може розміщуватися як на початку файлу [v2.3], так і в кінці [v2.4]. Тег складається з кількох «фреймів», кожен з яких містить певні метадані. Наприклад, фрейм «TIT2» зберігає назву композиції. Максимальний розмір одного фрейма обмежений 16 МБ, а загальний розмір тега не може перевищувати 256 МБ. Текст у фреймах може бути закодований у форматах UTF-16 або UTF-8, а біт кодування вказує на тип текстового фрейма. Стандарт ID3v2 визначає 84 типи фреймів, але також допускає створення користувацьких фреймів програмами. Серед стандартних фреймів є ті, що використовуються для зберігання обкладинок альбомів, кількості ударів на хвилину, інформації про авторські права і ліцензії, текстів пісень, посилань та інших даних. Файл із тегом у форматі ID3v2 починається з символів ID3, які є частиною заголовка (Header) тега. Заголовок складається з 10 байт і містить поля, описані нижче. Порядок байтів у ID3v2 – big endian, а розмір записується у 7-бітових байтах, де старший біт завжди дорівнює 0.

Метадані, які містяться у файлі, можуть у явному вигляді містити інформацію про авторські права, але цього не достатньо, тому що такі дані легко змінити або видалити, використовуючи спеціальне програмне забезпечення. Варто враховувати і той факт, що з 23 квітня 2017 року, коли минув термін дії пов'язаних з MP3 патентів, цей формат став фактично форматом з відкритим вихідним кодом. Тобто технічно немає перешкод для зміни вмісту файлу. Але можна розмістити дані про правовласника потай, використовуючи популярні стеганографічні методи. Наприклад, у зображенні, яке розміщується в метаданих як обкладинка музичного альбому або фото автора твору, можна за допомогою LSB (Least Significant Bit) методу [17] розмістити приховану інформацію про автора. У тегу ID3v2 обкладинка альбому або фотографія автора зберігається у форматі двійкових даних усередині спеціального фрейму під назвою APIC (Attached Picture). Цей фрейм може містити зображення в різних графічних форматах, таких як: JPEG (image/jpeg), PNG (image/png), GIF (image/gif), хоча цей формат використовується рідше. Фрейм APIC включає кілька полів, серед яких: MIME-тип зображення (наприклад, image/jpeg чи image/png), який вказує на формат файлу зображення; тип зображення – байт, що означає, що саме зображено (наприклад, обкладинка переднього плану, обкладинка заднього плану, іконка, логотип і т.д.); опис – текстове поле, що містить опис зображення (опціонально); власне дані зображення – двійкові дані, що представляють зображення у вибраному форматі (JPEG, PNG і т.д.). Така інформація буде непомітною. Враховуючи, що обмеження на розмір файлу, що завантажується в тегах ID3v2 не накладаються, то розміщення повної інформації про автора виглядає цілком реально.

Даний метод застосовується для зображень формату PNG, GIF, BMP. Формати PNG і BMP не використовують стиснення, а формат GIF використовує стиснення без втрат. Варто зазначити, що формат BMP останнім часом майже не використовується, тому наявність такого файлу може викликати підозру. На жаль, метод LSB не застосовується до найбільш популярного графічного формату JPG через те, що цей формат використовує стиснення з втратами і при стисненні файлу будуть втрачені найменш значущі біти, що містять нашу приховану інформацію.

Метод LSB. Принцип роботи цього методу можна розглянути з прикладу 24-бітного растрового RGB-зображення. Одна точка зображення в цьому форматі кодується трьома байтами, кожен з яких відповідає за інтенсивність одного із трьох складових кольорів (рисунок 3).

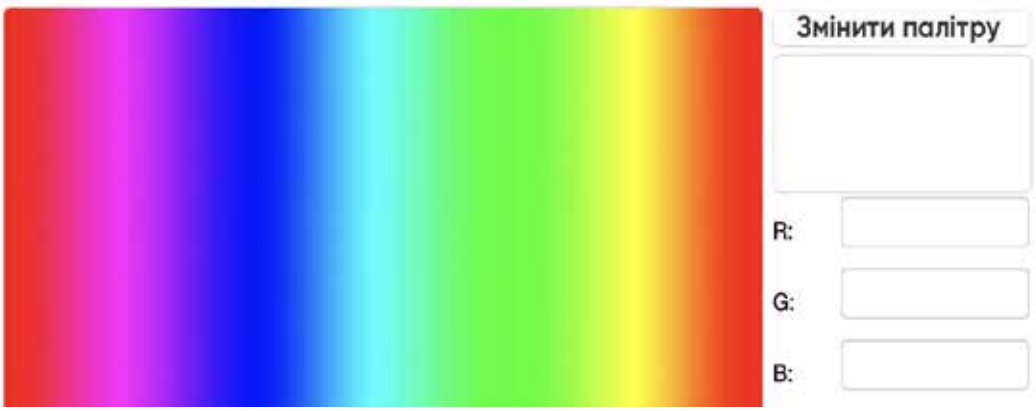

Рис. 3. Палітра RGB

COLORREF – стандартний тип для представлення кольорів у Windows API. Використовується для визначення кольору RGB, та її значення зберігається у вигляді 32-бітного (4-байтного) числа. У форматі RGB використовується три канали: червоний (Red), зелений (Green) та синій (Blue), але у зворотному порядку, кожен з яких займає 1 байт (8 біт), що в сумі становить 3 байти (24 біти) на піксель. Старший байт (крайній зліва) зарезервований і зазвичай не використовується, він дорівнює нулю, тому формат виглядає як 0x00BBGGRR. У деяких графічних форматах файлу, наприклад.png, четвертий байт – це альфа-канал (Alpha), який відповідає за прозорість. У цьому випадку колірна схема записується як RGBA.

При визначенні будь-якого RGB кольору, значення змінної типу COLORREF можна записати у шістнадцятковому вигляді так:

$$0x00bbggrr \tag{1}$$

де:

rr, gg, bb – значення інтенсивності відповідно до червоної, зеленої та синьої складових кольору. Максимальне їхнє значення – 0xFF.

Визначити змінну типу COLORREF можна так:

$$COLORREF\ C = RGB\ (\ r, g, b\ ); \tag{2}$$

де:

COLORREF C – змінна типу COLORREF, яка буде містити значення кольору.

RGB – макрос, який використовується для створення значення COLORREF з трьох компонентів: червоного, зеленого та синього.

r, g, b – інтенсивність (в діапазоні від 0 до 255) відповідно червоної, зеленої та синьої складових визначається кольору C. Тобто яскраво-синій колір може бути визначений як (0,0,255), червоний як (255,0,0), яскраво-фіолетовий – (255,0,255), чорний – (0,0,0), а білий – (255,255,255).

В результаті ми отримаємо вже інший відтінок, що мало відрізняється від вихідного. Такі схожі кольори важко розрізнити навіть на великих ділянках заливки, хоча різниця буде помітна при детальному аналізі за окремими точками. Заміна двох молодших біт практично не вловлюється людським оком. При необхідності можна використовувати три розряди, що незначно вплине на якість зображення. Можна визначити корисний об'єм RGB-контейнера. Якщо використовуються два біти з восьми на кожен канал, то можна заховати три байти корисної інформації на кожні чотири пікселі зображення, що становить 25% від загального обсягу зображення. Таким чином, маючи файл зображення розміром 160 Кбайт (при такому обсязі це буде картинка досить гарної якості), можна приховати в ньому до 40 Кбайт довільних даних, так що неозброєним оком ці зміни будуть непомітні,

а це досить великий обсяг інформації, якщо врахувати, що один символ займає 1–2 байти (залежить від мови та кодування).

Також за допомогою методу LSB можна закодувати секретне повідомлення в аудіофрагменті. Тобто повідомлення конвертується в бінарний формат і далі відбувається ітерація елементів аудіофайлу, де для кожного елемента в масці нижніх бітів встановлюється відповідне бінарне значення повідомлення.

Аналізуючи отримані результати після застосування методу стеганографії LSB, можна відзначити, що закодоване повідомлення майже не вплинуло на частотні і спектральні характеристики аудіосигналу. Також під час прослуховування не було помічено спотворень [21].

У прикладі із зображенням у метатегах аудіофайлу формату MP3 поєднані два основні напрямки, якими розвивається сучасна стеганографія. Перше – використання особливостей файлових форматів та розміщення інформації безпосередньо у файловому коді, в даному випадку це тег ID3v2, який не чути при прослуховуванні музичного файлу. Хоча ці дані не є прихованими з точки зору стеганографії та їх існування не є секретом, але щоб відобразити картинку, додану в метатеги, потрібне спеціальне програмне забезпечення. Другий популярний напрям стеганографії – використання надмірностей, які мають мультимедійні формати даних, такі, як зображення, аудіо або відео.

Цифрове оброблення сигналу. Другий напрямок стеганографії для мультимедійних даних, що активно розвивається, вивчає цифрову обробку сигналу. Сигнал – це зміна будь-якої фізичної величини, яка використовується для пересилання даних. Якщо він є безперервним у часі, це аналоговий сигнал. Можна відобразити аналоговий сигнал на графіку, де на горизонтальній осі буде відраховуватись час, а на вертикальній рівні сигналу. Поділ горизонтальної осі на рівні одиниці часу називається дискретизацією. Надання кожному такому відліку значення рівня сигналу називається квантуванням. Якщо ми застосуємо до аналогового сигналу дискретизацію та квантування, ми отримаємо цифровий сигнал [22]. Цифровий сигнал – це сигнал, який можна представити у вигляді дискретних (цифрових) значень. Приклад відображення цифрового сигналу показано на рис. 4. Надмірність аудіовізуальних даних дозволяє «сховати» секретну інформацію [18] усередині контейнера з аудіовізуальними даними. Крім того, особливість аудіо та відео файлів полягає в тому, що їх можна почути або побачити відповідно, а людське вухо та око мають дуже обмежені можливості в частині сприйняття звукових або колірних відтінків. Це дозволяє «заховати» приховану інформацію у невеликих спотвореннях сигналу, непомітних для людського ока чи вуха.

До прихованої, всередині звукового або відео контейнера, інформації (стеганоповідомлення, у нашому випадку це ЦВЗ) пред'являється ряд вимог: надійність сприйняття, стійкість до руйнівних атак, стійкість до стеганоаналізу, а також невелика обчислювальна складність в умовах використання в режимі реального часу [20].

Звертаємо увагу ще й на те, що присутність ЦВЗ у файлі повинна зберігатися і при зміні тривалості самого файлу, щоб при поділі нашого ЦВЗ не залишився у відрізаній частині.

Цифрова обробка сигналу – це способи обробки сигналу на основі чисельних методів з використанням цифрових обчислювальних засобів. В основі лежить дискретне перетворення Фур'є, яке дозволяє аналоговий сигнал зазнати дискретизації та квантування.

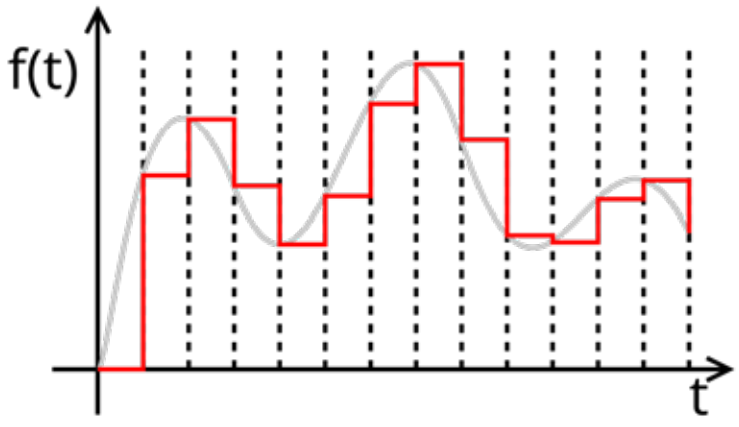

Рис. 4. Цифровий сигнал

Це дозволяє розглядати будь-який цифровий сигнал як деяку матрицю (приклад на рис. 5), а до неї, відповідно, застосовні всі математичні методи для матриць.

Для цифрового звукового файлу тут рядки – це тимчасові відліки (зазначені у дужках, $0<t<T$), а $S_i(t)$ у стовпці визначають рівень сигналу різної частоти. Такою матрицею можна описати і відео, стовпці описуватимуть колірні та світлові характеристики для кожної точки зображення.

$$\boldsymbol{S}_{(TxM)}=\begin{vmatrix} s_1(1) & s_2(1) & \dots & s_i(1) & \dots & s_M(1) \\ s_1(2) & s_2(2) & \dots & s_i(2) & \dots & s_M(2) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_1(t) & s_2(t) & \dots & s_i(t) & \dots & s_M(t) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_1(T) & s_2(T) & \dots & s_i(T) & \dots. & s_M(T) \end{vmatrix}$$

Рис. 5. Цифровий сигнал у вигляді матриці [23]

Найбільш популярними методами стеганографії, які використовуються для цифрових сигналів, що представляють собою цифрове аудіо або відео, є методи засновані на незначних спотвореннях цифрового сигналу, таких як реверберація, частотно-фазова модуляція [24, 25].

Метод, що ґрунтується на явищі реверберації. Розглянемо, як працює метод реверберації. Метод ґрунтується на властивості людського слуху не розрізняти присутність ехосигналу, якщо затримка між основним сигналом та ехосигналом не перевищує певного часу.

Реверберація є результатом багатьох відображень звуку, які виникають у реальному приміщенні. Насправді ми чуємо реверберацію щодня і настільки звикли чути реверберацію без будь-якого особливого відчуття.

Реверберація, ймовірно, є одним із найбільш часто використовуваних ефектів у музиці. Було розроблено різноманітні способи синтетичного додавання реверберації до записів. Практично додавання реверберації означає взяти лінійну згортку імпульсної характеристики приміщення (IR, impulse response) і джерела звуку.

Існують різні схеми розрахунку імпульсної характеристики приміщення, яке визначається формою, розміром і коефіцієнтом матеріалів його поверхні, а також положенням джерела та слухача в приміщенні. Це одновимірна дискретна функція часу, яку можна описати рівнянням:

$$h(n) = a_1 * \delta(n - n_1) + a_2 * \delta(n - n_2) + \dots + a_L * \delta(n - n_L) \quad (3)$$

де L – довжина імпульсної характеристики приміщення h(n), a_i – величина і-го відбитого звуку, n_i – час затримки і-го відбитого звуку. Це дозволить нам використовувати його як IR – імпульсну характеристику для імітації реверберації. Експерименти демонструють, що імпульсні характеристики h(t) явно відрізняються в однакових параметрах кімнати, але положення джерела та слухача різне. Ми просто використовуємо різницю, щоб вставити ЦВЗ. Прихована інформація кодується в параметрах реверберації, таких як час затримки, коефіцієнт загасання, частотні характеристики або амплітуда відлуння. Наприклад, невеликі зміни часу затримки реверберації можуть бути бітами даних.

Цей метод вразливий до навмисних атак, спрямованих на придушення луни. Алгоритми для придушення луни відносно прості в реалізації та доступні. Зловмисники можуть легко застосувати такі алгоритми до підозрілого аудіофайлу, щоб нейтралізувати можливе приховане повідомлення, навіть якщо вони не знають, чи використовується реверберація для стеганографії. Це робить метод уразливим перед навіть нецільовими атаками на аудіофайл.

Використання явища реверберації створення системи цифрових водяних знаків також часто розглядається у науковій літературі [24]. Розглянемо застосування ефекту реверберації для розміщення ЦВЗ всередині звукового файлу з використанням одного кімнатного імпульсу, незначно модулюючи час затримки між основним сигналом і часом початку реверберації. В цьому випадку схема занурення виглядає так, як показано на рис. 6.

На рисунку 6 v(1) – v(M) – імпульсні відгуки фільтрів, що застосовуються для імітації реверберації. Відмінність між фільтрами v(1) – v(M) полягає у різному часі затримки між вихідним сигналом та реверберацією. Так як можливе використання кількох величин затримки, то проміжок часу, протягом якого діє один фільтр, можна вкласти M біт, де M – число використовуваних варіантів затримки.

Якщо позначити вихідний сигнал S(t) і перейти до безперервного часу t, з'являється можливість апроксимувати гауссівським процесом з відомою кореляційною функцією, яка описує залежність між значеннями процесу в різних точках часу або простору. Можна припустити, що це дозволяє побудувати оптимальний приймач для виділення одного біта вкладеної інформації (при використанні двох фільтрів). Схема оптимального прийому сигналів Гауса відображена на рис. 7.

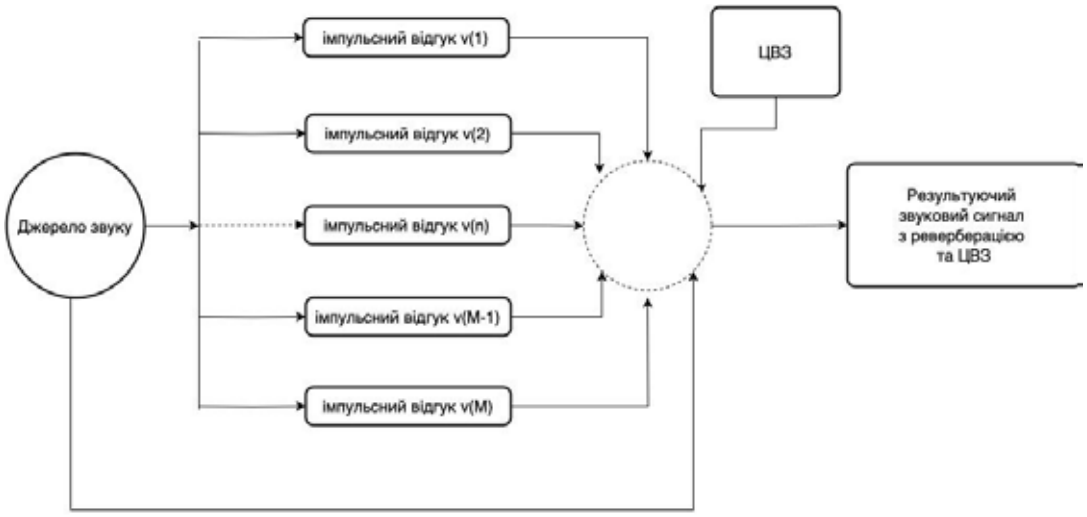

Рис. 6. Метод додавання ЦВЗ, заснований на реверберації

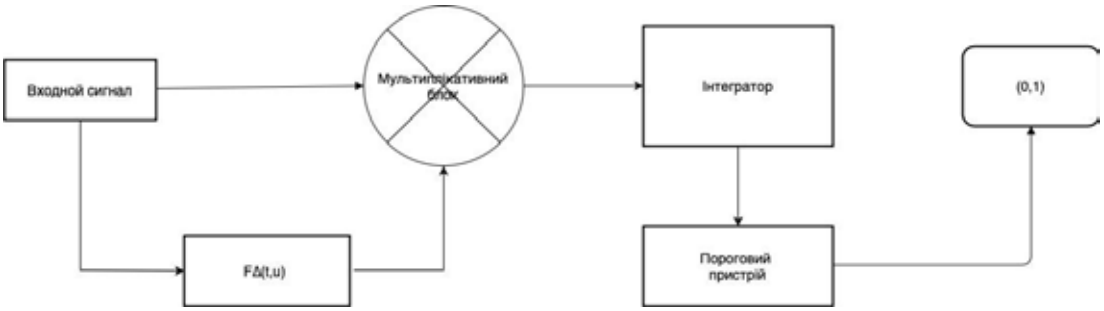

Рис. 7. Оптимальний прийом сигналів Гауса

На рисунку 7 $F_{\Delta}(t,u)$ – розв'язання інтегрального рівняння:

$$\int_0^T\int_0^T P_0(t,x)F_{\cdot}(x,y)P_1(y,u)\,dx\,dy = P_1(t,u) - P_0(t,u) \tag{4}$$

де $P_{0(1)}(t,x)$ – кореляційні функції сигналів на виході першого та другого фільтра відповідно; T – часовий інтервал, у якому вбудовується один біт.

Однак, модель з гауссівською апроксимацією вхідного сигналу S(t), яка призводить до оптимальної вирішальної схеми, показаної на рис. 7, суттєво відрізняється від нашої вихідної моделі тим, що звуковий сигнал досить погано апроксимується гауссівським процесом. Також точно не відома кореляційна функція вхідного звукового сигналу, та не можна вважати взаємонезалежними сигнали на входах першого та другого фільтрів. Все це вказує на те, що ми не зможемо побудувати оптимальний приймач для отримання одного біта вкладеної інформації, спираючись на викладену на рис. 7 схему при доказі її оптимальності.

Висновки

Проблема вбудовування ЦВЗ в аудіовізуальній продукції поки що не має чіткого рішення, яке б задовольняло всі необхідні умови, які повинні виконуватися. Методи запропоновані різними вченими досить ефективні за певних умов і в конкретній ситуації. Однак жоден з них не є достатньо універсальним, щоб він міг бути застосовним для будь-якого типу аудіовізуальних даних.

Найбільш перспективними здаються стеганографічні методи, які стосуються змін безпосередньо самого звуку або зображення, в даному випадку більш актуальним є питання стійкості таких методів до навмисних атак або стегоаналізу. Але не можна скидати з рахунків методи, пов'язані з файловими змінами. Сучасні технології та пристрої все більше видаляють користувача від того, що лежить в основі споживаної ними інформаційної продукції, обмежуючи його можливості щодо втручання в сам інформаційний продукт.

Аналіз опублікованих робіт щодо цифрової стеганографії показує величезний інтерес, який викликає ця тема у дослідників. Захист авторського права на аудіовізуальний контент має не лише юридичні та технічні аспекти. Якщо взяти до уваги, що йдеться про величезний потік цифрового контенту, який щодня з'являється на просторах інтернет і фактично є частиною нашого життя, стає зрозуміло, що актуальність проблеми з кожним днем збільшується.

Список використаної літератури

1. Про обов'язковий примірник документів: Закон України від 09.04.1999 № 595-XIV. Відомості Верховної Ради України, 1999, № 22-23, Ст. 199.

2. Цивільний кодекс України від 16.01.2003 № 435-IV. Відомості Верховної Ради України, 2003, № 40-44, Ст. 356.

3. Конституція України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України, 1996, № 30, Ст. 141.

4. Про авторське право і суміжні права: Закон України від 15.04.2023, підстава – 2974-IX URL: https://zakon.rada.gov.ua/laws/show/2811-20#Text (дата звернення: 18.06.2024).

5. Сусліков Л.М., Студеняк І.П. Створення об'єктів інтелектуальної власності: Навчальний посібник. Ужгород: Видавництво УжНУ «Говерла», 2020. 407 с. URL: https://dspace.uzhnu.edu.ua/jspui/handle/lib/45071 (дата звернення: 18.06.2024).

6. Про державну реєстрацію прав автора на твори науки, літератури і мистецтва: Постанова Кабінету міністрів України від 18.07.1995 № 532 URL: https://zakon.rada.gov.ua/laws/show/532-95-%D0%BF#Text (дата звернення: 18.06.2024).

7. Про медіа: Закон України від 13.12.2022 № 2849-IX. Відомості Верховної Ради України, 2023, № 47-50, Ст.120.

8. Liu C. et al. Dear: A deep-learning-based audio re-recording resilient watermarking. Proceedings of the AAAI Conference on Artificial Intelligence. 2023. Vol. 37. Is. 11. P. 13201-13209.

9. Світловський Є. В. Моделі і алгоритми створення цифрових водяних знаків для аудіо-файлів. Перспективні технології та прилади. 2024. Т. 1. №. 24. С. 99-106.

10. Voloshynovskiy S. et al. Attacks on digital watermarks: classification, estimation based attacks, and benchmarks. IEEE communications Magazine. 2001. Т. 39. №. 8. P. 118-126.

11. Popa R. An analysis of steganographic techniques. The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering. 1998. Vol. 65. 59 pp.

12. Johnson N. F. et al. Information Hiding: Steganography and Watermarking-Attacks and Countermeasures, Journal of Electronic Imaging. 2001, 10. 825. 10.1117/1.1388610.

13. Boroughf B. The next great YouTube: improving content ID to Foster creativity, cooperation, and fair compensation. Alb. LJ Sci. & Tech. 2015. Vol. 25. P. 95.

14. Як працює система Content ID. Довідка Youtube https://support.google.com/youtube/answer/2797370?hl=uk

15. Yatigammana K., Wijayarathna G. Integrating Micro-lesson Metadata in ID3V2 of MP3. 2021 From Innovation To Impact (FITI). IEEE, 2021. Vol. 1. P. 1-6.

16. Nilsson M., „ID3 tag version 2.4.0 – Main Structure," 01 November 2000. [Online]. Available: https://id3.org/id3v2.4.0-structure. [Accessed 07 December 2020].

17. Samborskyi I., Tolstova A. Сучасний стан та перспективи розвитку стеганографії у телекомунікаційних системах. Collection" Information Technology and Security". 2022. Т. 10. №. 1. С. 27-38.

18. Іванов В. Г. та ін. Захист авторських прав мультимедійних даних. Theory and practice of jurisprudence. 2011. Т. 1. №. 1. С. 18-18.

19. Олещенко Л. М. Програмне забезпечення для аналізу даних платформи YouTube. Вчені записки. 2024. С. 22024111.

20. Світловський Є., Трапезон К. Стеганографічні підходи до оброблення аудіосигналів. Вісник КрНУ імені Михайла Остроградського. 2023. Вип. 3. С. 185-192.

21. Лавер В. О., Левчук О. М. Обробка зображень: навч.-метод. посіб. 2021. С. 11.

22. Lin Y. et al. Audio watermark. Audio Watermark A Comprehensive Foundation Using MATLAB. Springer International Publishing; Cham, Switzerland, 2015. 213 pp.

23. Ngo N. M., Unoki M. Method of audio watermarking based on adaptive phase modulation. IEICE transactions on information and systems. 2016. Vol. 99. №. 1. P. 92-101.

24. Hua G. et al. Twenty years of digital audio watermarking–a comprehensive review. Signal processing. 2016. Vol. 128. P. 222-242.

25. Nian G., Wang S., Ge Y. Research of improved echo data hiding: audio watermarking based on reverberation. 2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07. IEEE, 2007. Vol. 2. P. II-177-II-180.

References

1. Pro oboviazkovyi prymirnyk dokumentiv: Zakon Ukrainy vid 09.04.1999 № 595-XIV [Law of Ukraine on the Mandatory Copy of Documents, No. 595-XIV] (1999). *Vidomosti Verkhovnoi Rady Ukrainy – The Bulletin of the Verkhovna Rada of Ukraine*, (22-23), 199 [in Ukrainian].

2. Tsyvilnyi kodeks Ukrainy vid 16.01.2003 № 435-IV [The Civil Code of Ukraine, No. 435-IV] (2003). *Vidomosti Verkhovnoi Rady Ukrainy – The Bulletin of the Verkhovna Rada of Ukraine*, (40-44), Art. 356 [in Ukrainian].

3. Konstytutsiia Ukrainy vid 28.06.1996 № 254k/96-VR [The Constitution of Ukraine, No. 254к/96-ВР] (1996). *Vidomosti Verkhovnoi Rady Ukrainy – Vidomosti Verkhovnoi Rady Ukrayiny*, (30), 141 [in Ukrainian].

4. Pro avtorske pravo i sumizhni prava: Zakon Ukrainy vid 15.04.2023, pidstava – 2974-IX [Law of Ukraine on Copyright and Related Rights, No. 2974-IX] (2023). Retrieved from https://zakon.rada.gov.ua/laws/show/2811-20#Text [in Ukrainian].

5. Suslikov, L. M., & Studeniak, I. P. (2020). Stvorennia obiektiv intelektualnoi vlasnosti: Navchalnyi posibnyk [Creation of Intellectual Property Objects: Study guide]. *Uzhhorod: Vydavnytstvo UzhNU «Hoverla» – Uzhhorod: UzhNU Publishing House 'Hoverla'*. Retrieved from https://dspace.uzhnu.edu.ua/jspui/handle/lib/4507[in Ukrainian].

6. Pro derzhavnu reiestratsiiu prav avtora na tvory nauky, literatury i mystetstva: Postanova Kabinetu ministriv Ukrainy vid 18.07.1995 № 532 [Resolution of the Cabinet of Ministers of Ukraine on State Registration of Author's Rights to Works of Science, Literature, and Art, No. 532] (1995). Retrieved from https://zakon.rada.gov.ua/laws/show/532-95-%D0%BF#Text [in Ukrainian].

7. Pro media: Zakon Ukrainy vid 13.12.2022 № 2849-IX [Law of Ukraine on Media, No. 2849-IX] (2022). *Vidomosti Verkhovnoi Rady Ukrainy – Bulletin of the Verkhovna Rada of Ukraine*, (47-50), 120 [in Ukrainian].

8. Liu, C., et al. (2023). Dear: A deep-learning-based audio re-recording resilient watermarking. *Proceedings of the AAAI Conference on Artificial Intelligence*, 37 (11), 13201-13209 [in English].

9. Svitlovskyi Ye. V. (2024). Modeli i alhorytmy stvorennia tsyfrovykh vodianykh znakiv dlia audio-failiv [Models and algorithms for creating digital watermarks for audio files]. *Perspektyvni tekhnolohii ta prylady – Perspective technologies and devices*, 1 (24), 99-106 [in Ukrainian].

10. Voloshynovskiy, S., et al. (2001). Attacks on digital watermarks: Classification, estimation-based attacks, and benchmarks. *IEEE Communications Magazine*, 39(8), 118-126 [in English].

11. Popa, R. (1998). An analysis of steganographic techniques. The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, 65 [in English].

12. Johnson, Neil & Duric, Zoran & Jajodia, Sushil & Memon, Nasir. (2001). Information Hiding: Steganography and Watermarking–Attacks and Countermeasures. *Journal of Electronic Imaging*. 10. 825. 10.1117/1.1388610 [in English].

13. Boroughf, B. (2015). The next great YouTube: Improving content ID to foster creativity, cooperation, and fair compensation. *Albany Law Journal of Science & Technology*, 25, 95 [in English].

14. Yak pratsiuie systema Content ID. Dovidka Youtube [YouTube Help. How the Content ID system works]. Retrieved from https://support.google.com/youtube/answer/2797370?hl=uk[in Ukrainian].

15. Yatigammana, K., & Wijayarathna, G. (2021). Integrating micro-lesson metadata in ID3V2 of MP3. From Innovation to Impact (FITI). IEEE. 1, 1-6 [in English].

16. Nilsson, M. (2000). ID3 tag version 2.4.0 – Main structure. Retrieved from https://id3.org/id3v2.4.0-structure [in English].

17. Samborskyi, I., & Tolstova, A. (2022). Suchasnyi stan ta perspektyvy rozvytku stehanohrafii u telekomunikatsiinykh systemakh [Current state and prospects of steganography development in telecommunication systems]. Collection» Information Technology and Security»- *Collection 'Information Technology and Security*, 10 (1), 27-38 [in Ukrainian].

18. Ivanov, V. G., et al. (2011). Zakhyst avtorskykh prav multymediinykh danykh [Copyright protection of multimedia data]. *Theory and practice of jurisprudence – Theory and Practice of Jurisprudence*, 1 (1), 18-18 [in Ukrainian].

19. Oleshchenko, L. M. (2024). Prohramne zabezpechennia dlia analizu danykh platformy YouTube [Software for analyzing YouTube platform data]. *Vcheni zapysky – Scientific Notes*, 22024111 [in Ukrainian].

20. Svitlovsky E., Trapezon K. (2023). Stehanohrafichni pidkhody do obroblennia audiosyhnaliv [Steganographic approaches to audio signal processing]. (2023). *Visnyk KrNU imeni Mykhaylа Ostrohradskoho – Bulletin of the Mykhailo Ostrohradskyi Kyiv National University*, Issue 3, 185-192 [in Ukrainian].

21. Laver, V. O., & Levchuk, O. M. (2021). Obrobka zobrazhen: navch.-metod. posib [Image processing: Study guide]. 11. [in Ukrainian].

22. Lin, Y., et al. (2015). Audio Watermark: A Comprehensive Foundation Using MATLAB. Springer International Publishing; Cham, Switzerland, 213 [in English].

23. Ngo, N. M., & Unoki, M. (2016). Method of audio watermarking based on adaptive phase modulation. *IEICE Transactions on Information and Systems*, 99 (1), 92-101 [in English].

24. Hua, G., et al. (2016). Twenty years of digital audio watermarking–a comprehensive review. *Signal Processing*, 128, 222-242 [in English].

25. Nian, G., Wang, S., & Ge, Y. (2007). Research of improved echo data hiding: Audio watermarking based on reverberation. *IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07*, 2, II-177-II-180 [in English].