УДК 004.056

Д.О. Козак
О.В. Салієва

ЗАХИСТ АВТОРСЬКОГО ПРАВА НА ВІДЕОФАЙЛИ З ВИКОРИСТАННЯМ ЦИФРОВОГО ВОДЯНОГО ЗНАКА

Вінницький національний технічний університет

Анотація

В роботі розглянуто існуючі методи захисту авторського права на інтелектуальну власність, зокрема медіа файли. Досліджено найбільш доступні та розповсюджені методи захисту відео на онлайн сервісах, визначено їх переваги та недоліки. Проаналізовано метод захисту авторського права на відео з використанням цифрового водяного знаку та розглянуто найбільш актуальні методи вбудовування ЦВЗ у файли.

Ключові слова: *мультимедійні файли, захист авторського права, цифрові водяні знаки, онлайн-сервіси, алгоритми вбудовування ЦВЗ.*

Abstract

In this article considers the existing methods of copyright protection of intellectual property, in particular media files. The most available and widespread methods of video protection on online services are researched, their advantages and disadvantages are defined. The method of protection of copyright on video with the use of digital watermark is analyzed and the most actual methods of embedding CEV in files are considered.

Keywords: *multimedia files, copyright protection, digital watermarks, online services, CEV embedding algorithms.*

Вступ

Стрімкий розвиток інформаційних технологій став вагомим поштовхом до широкого використання цифрових фотографій, DVD фільмів, музики у форматі mp3. На жаль, більшість створених мультимедіа, що є результатами інтелектуальної діяльності використовуються в мережі з грубими порушеннями діючого законодавства.

Особливе значення застосування технічних засобів захисту авторського права для мультимедіа набувають при відтворенні та розповсюдженні його в Інтернеті. Коли автор викладає результат своєї творчої діяльності в мережу, файли стають доступними для всіх користувачів. В таких ситуаціях варто якнайбільше уваги приділяти захисту свого авторства на той чи інший створений об’єкт.

В даній роботі запропоновано більш детальніше розглянути методи захисту відео на онлайн-сервісі та дослідити засіб захисту авторського права за допомогою цифрового водяного знаку (ЦВЗ).

Методи захисту відео на онлайн - сервісі

Розглянемо три варіанти захисту онлайн – відео та проаналізуємо докладніше кожен варіант.

1. Шифрування посилання на відео, вставленого в плеєр [1]. Існує думка, що долучення в плеєр відео не у вигляді файлу mp4, а у вигляді зашифрованого набору символів в base64, наддасть відео захищеності. Як виявляється на практиці, дістати зашифроване посилання через HTML код не складе ніяких труднощів. Потім можна вставити посилання в будь-який онлайн-сервіс, що перекодує з base64 і пряме посилання на відеофайл готове, доступне для завантаження. Отже, будь-який користувач може завантажити відео з зашифрованим посиланням. В результаті це не є захистом.

2. Створення відео потоку [1]. Перш ніж розглядати відеопотік розберемо як завантажується відео.

Звичайний відеофайл (mp4). Припустимо файл має об’єм 1Гб і його тривалість 30 хвилин. Після натискання на кнопку програвання файл відразу починає підтягуватися на комп'ютер користувача.

Відеопотік. Суть відеопотоку в тому, що один великий mp4 файл розрізається на безліч дрібних файлів тривалістю від 1 сек. до 60 сек. Всі ці файли об'єднуються в плейлист. Замість одного великого mp4 файлу в плеєр вставляється плейлист. Тому замість одного великого mp4 файлу в 1Гб, який вантажиться послідовно, отримуємо безліч дрібних, які можуть довантажувати паралельно.

Отже, відеопотік спрощує перегляд відео, знижує навантаження на сервер як по потужності так і по трафіку і не дозволяє швидко завантажити відео. Тому завдяки використанню потоку виграють всі і

користувачі і автори. Звичайно, це не 100% захист, але сильно ускладнює процес скачування і відкладає час початку викладання відео в інтернеті.

3. Інфопротектор [1]. Відеопотік складно висмикнути з сайту, але можна зняти з екрану за допомогою інших програм. Тому якщо необхідно вжити тотального захисту від програм, які знімають, то доцільним є застосування Інфопротектору. Він захищає файли, відкриваються вони за допомогою персонального ліцензійного ключа, який перетворюється в водні знаки. І навіть якщо відео знімуть з екрану, то буде відомо хто це зробив. Єдина проблема – немає можливості переглядати відео на мобільних пристроях.

Для правового захисту інтелектуальної власності доцільним є застосування більш професійніших засобів. В роботі розглянемо захист медіа за допомогою цифрового водяного знаку.

Поняття цифрового водяного знаку

Цифровий водяний знак (ЦВЗ) – це спеціальна мітка, вбудована в цифровий контент з метою захисту авторських прав і підтвердження цілісності самого документа [2]. ЦВЗ можна вбудовувати в електронні документи будь-якого типу і активно використовуються при розміщенні унікальних фотографій, відео, аудіо треків в електронному вигляді в глобальній мережі Інтернет. Щоб комп'ютерний файл, який представляє собою твір мультимедіа, не міг бути змінений без відома автора, застосовуються ЦВЗ. Якщо твір піддається певним змінам, то разом з ним змінюється і ЦВЗ.

Цифрові водяні знаки діляться на видимі і невидимі [3]. Як правило, усі системи цифрових водяних знаків мають два типових блоки (рис. 1): схему внесення водяного знака і схему пошуку/витягання.

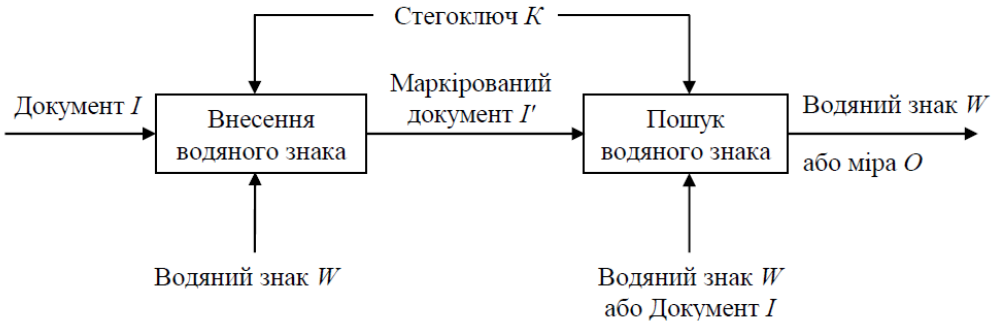

Рисунок 1 – Узагальнена схема системи ЦВЗ [4]

Вхідною інформацією для схеми внесення водяного знака є цифровий об’єкт I, водяний знак W і стегоключ K (необов’язковий параметр). Водяний знак W може мати будь-який вигляд: число, текст, зображення та ін. Практично в усіх системах ЦВЗ передбачена наявність одного або навіть декількох стегоключів, які необхідні для захисту водяних знаків від несанкціонованих змін. Виходом системи є цифровий об’єкт з вбудованим водяним знаком [4].

Вихідними даними для процесу пошуку і/або видалення водяного знака є: цифровий об’єкт $\bar{I}'$ з водяним знаком, стегоключ К і, в залежності від реалізованого методу, оригінальні копії даних I та/або водяного знака W.

Результатом роботи схеми є витягнений водяний знак W або деяка оцінка O, за якою можна судити про ймовірне існування знака W в об’єкті $\bar{I}'$. Подібна структура систем водяних знаків характерна для усіх видів цифрових даних: аудіо, зображень, відео, форматованих текстів, тривимірних моделей, параметрів мультиплікаційних моделей та ін.

При використанні ЦВЗ повинні виконуватись наступні вимоги до них: непомітність для користувачів, індивідуальність алгоритму нанесення, можливість для автора виявити несанкціоноване використання файлу, неможливість видалення неуповноваженими особами, стійкість до різних змін носія-контейнера.

Крім цього, у системах цифрових водяних знаків повинні враховуватися, принаймні, такі аспекти: завадостійкість водяного знака до випадкових перекручувань і навмисних атак – найважливіша характеристика, від якої залежать споживчі властивості системи, обов’язкове використання стегоключів для гарантованого захисту водяних знаків від навмисних перекручувань і видалень; оптимальний поріг «видимості» водяного знака – параметр, який характеризує припустимий рівень

внесених водяним знаком перекручувань, відносний об’єм вносимої інформації – параметр, який залежить від характеру приховуваних даних і від природи цифрового об’єкта.

Під час внесення водяного знака великого об’єму знижується його завадостійкість до атак.

Відповідно до принципу Кірхгофса, алгоритм внесення і витягання водяних знаків не повинен бути секретним, а доступ до водяного знака повинен бути обмежений. Цю умову можна виконати під час вибору місця розташування водяного знака, яке буде залежати від стегоключа. Від правильного вибору місця розташування водяного знака залежать також видимі перекручування в зображенні. Це обумовлено особливостями органів зору людини, чутливість яких змінюється відповідно до характеру текстури зображення [4].

Враховуючи усі наведені вимоги до використання цифрового водяного знаку, далі розглянемо деякі найбільш доцільні алгоритми вбудовування ЦВЗ у відео, що планується використати у майбутніх дослідженнях.

Алгоритми вбудовування ЦВЗ у відео

У вітчизняній і зарубіжній літературі описано безліч різних методів і алгоритмів впровадження цифрового водяного знаку у медіафайли. Такі методи діляться на просторові, частотні та стиснені за стандартом MPEG (рис. 2) [5]. Наприклад, до просторових методів відноситься метод LSB. До частотних – нанесення ЦВЗ шляхом розширення спектру.

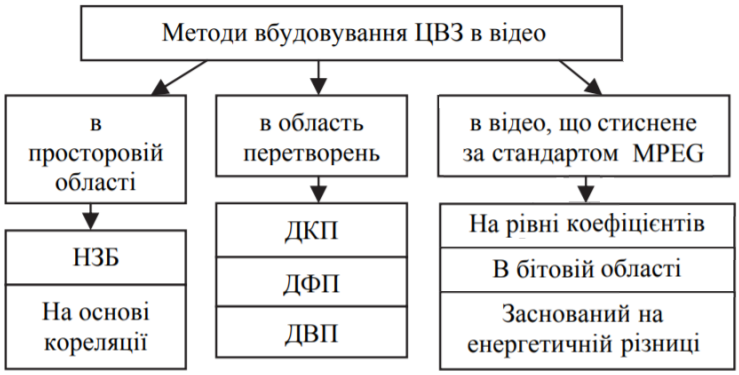

Рисунок 2 – Класифікація методів вбудовування в відео [5]

Розглянемо існуючі алгоритми вбудовування ЦВЗ у відео, а саме адитивні алгоритми, алгоритми на основі злиття ЦВЗ і контейнера, алгоритми з використанням фрактальних перетворень.

В адитивних методах впровадження ЦВЗ є послідовність чисел w_i довжини N, яка впроваджується в вибрану підмножину відліків вихідного зображення f. Основний і найбільш часто використовуваний вираз для вбудовування інформації в цьому випадку має вигляд:

$$f(m,n) = f(m,n)(1 + aw_i).$$

Для збільшення стійкості до видалення ЦВЗ в багатьох алгоритмах застосовуються широкосмугові сигнали. При цьому інформаційні біти можуть бути багаторазово повторені, закодовані із застосуванням коригуючого коду, або до них може бути застосовано будь-яке інше перетворення, після чого вони модулюють за допомогою псевдовипадкової гаусівської послідовності. Така послідовність є гарною моделлю шуму, присутнього в реальних зображеннях. У той же час синтетичні зображення (створені на комп'ютері) не містять шумів, і в них важче непомітно вмонтувати таку послідовність. Зазвичай легше спочатку згенерувати рівномірно розподілену послідовність. Відомий алгоритм перетворення такої послідовності в гаусову (алгоритм Боксу-Мюллера).

Якщо замість послідовності псевдовипадкових чисел в зображення вбудовується інше зображення (наприклад, логотип фірми), то відповідні алгоритми впровадження називаються алгоритмами злиття. Розмір впроваджуваного повідомлення набагато менше розміру вихідного файлу. Перед вбудовуванням воно може бути зашифровано або перетворено якимось іншим чином [6 – 7].

У таких алгоритмів є такі переваги: можна припустити певне перекручення прихованого повідомлення, так як людина все одно зможе розпізнати його та наявність впровадженого логотипу є більш переконливим доказом прав власності, ніж наявність деякого псевдовипадкового числа. Таким чином, алгоритм використовує досить складну модель людського зору.

Особливістю методу з використанням фрактальних перетворень стеганографічного вбудовування інформації в стегоконтейнер є використання в якості ключа двовимірного фрактального зображення, в якості якого використаний двовимірний фрактал алгебраїчного типу. З цією метою можна використовувати, наприклад, фрактальне зображення алгебраїчного типу у вигляді множини Жюліа в якості секретного ключа [8].

В результаті зловмисник не зможе згенерувати ідентичне фрактальне зображення без точного значення деякого комплексного числа, яке заздалегідь погоджується між відправником і отримувачем, а також ряду інших параметрів, що робить запропонований метод стійким до атак. Перевагою запропонованого алгоритму є можливість вилучення ЦВЗ без знання оригінального контейнера, оскільки проміжним контейнером для водяного знака є фрактал. Використання фракталів як ключа для вилучення ЦВЗ, дозволяє забезпечувати витяг ЦВЗ практично без втрат, при цьому стегоконтейнер візуально нічим не відрізняється від контейнера, що містить секретну інформацію.

Висновки

Отже, завдання надійного захисту авторських прав, прав інтелектуальної власності або конфіденціальних даних (які в більшості випадків мають цифровий формат) від несанкціонованого доступу є однією з найпоширеніших і майже невирішених сьогодні проблем.

Загалом, розглянуті три варіанти захисту онлайн-відео, а саме: шифрування посилання на відео, відео потік та інфопротектор є лише частково дієвими на практиці, орієнтуються на звичайного користувача та не дають високу ймовірність захисту інтелектуальної власності.

Саме тому в даній роботі увага наділялась дослідженню методів захисту мультимедійних файлів та онлайн сервісу не лише загальнодоступними методами, але й більш професійнішими, наприклад, таких як застосування цифрового водяного знаку. Даний метод дозволяє приховувати додаткову інформацію в різних цифрових об'єктах. Досліджено існуючі алгоритми вбудовування ЦВЗ у відео, а саме адитивні алгоритми, алгоритми на основі злиття ЦВЗ і контейнера, алгоритми з використанням фрактальних перетворень та визначено їх основні переваги та недоліки.

Оскільки в Україні питання ефективного захисту авторського права в Інтернеті є невирішеним, відповідному правовому регулюванню має передувати дослідження та узагальнення міжнародного досвіду.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Захист відео онлайн сервісів. *JOOMLA центр*: веб-сайт. URL: https://joomla.center/blog-kurteev/kak-zashchitit-onlajn-video (дата звернення 01.03.2021).
2. Пономарев К. И., Путилов Г. П. Стеганография: учеб. пос. Москва: МИЭМ, 2009. 70 с.
3. Конахович Г.Ф. Компьютерная стеганография. Теория и практика: учеб. пос. Киев: МК-Пресс, 2006. 288 с.
4. Хорошко В.О., Яремчук Ю.Є., Карпінець В.В. Комп'ютерна стеганографія: навч. посіб. Вінниця: ВНТУ, 2017. 155 с.
5. Грибунин В.Г., Оков И. Н., Туринцев И. В. Цифровая стеганография: учеб. пос. Москва: СОЛОН-Пресс, 2002. 272 с.
6. Шостак Н.В., Астраханцев А.А. Дослідження стійкості алгоритмів захисту авторських прав на відеопродукцію. *Системи обробки інформації.* 2017. № 2 (148). С. 138-143.
7. Григорьян А. К. Аветисова Н. Г. Методы внедрения цифровых водяных знаков в потоковое видео. Обзор. *Информационно-управляющие системы.* 2010. №2. С. 38-45.
8. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стегоанализ: монография. Москва: Вузовская книга, 2009. 220 с.

Козак Діана Олегівна – студентка групи УБ-17б, факультет менеджменту і інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: fm.ub17b.kozak@gmail.com.

Салієва Ольга Володимирівна – асистент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця

Науковий керівник: ***Карпінець Василь Васильович*** – кандидат технічних наук, доцент, завідувач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця

Kozak Diana O. – student of UB-17b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail: fm.ub17b.kozak@gmail.com

Salieva Olga V. – Assistant Professor, Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia

Supervisor: ***Karpinets Vasyl V.*** – Ph. D., assistant professor, Head of the Department of Management and Security of Information Systems, Vinnytsa National Technical University, Vinnytsia