УДК 621.3

О.Б. Полусин [1], аспірант, О.В. Тимченко [1, 2], д.т.н, професор

ДОСЛІДЖЕННЯ ПРОГРАМНИХ ПРОДУКТІВ ДЛЯ НАКЛАДЕННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ ТА ІНШИХ МЕТОДІВ ЗАХИСТУ МУЛЬТИМЕДІЙНИХ ДАНИХ ТА ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Анотація. Розглянуто ряд існуючих програмних засобів та методів за допомогою яких здійснюється стеганографічний захист мультимедійних даних, об'єктів авторського права та інтелектуальної власності. Досліджуються елементи методів захисту. Визначається необхідність застосування одиничного чи комплексного методів для здійснення більш надійнішого захисту інформації мультимедіа.

Ключові слова: цифровий водяний знак, програмне забезпечення, накладення ЦВЗ, об'єкт авторського права.

Abstract. A number of existing software tools and methods with which the steganographic protection of multimedia data, objects of copyright and intellectual property is carried out is considered. The elements of methods of protection are investigated. The necessity of using single or complex methods for more reliable protection of multimedia information is determined.

Keywords: digital watermark, software, overlaying of digital carriers, object of copyright.

Вступ. Сучасний стан інформаційного простору можна вважати нестабільним і таким, що в своєму розвитку за останні кілька років, перевершив досягнення останніх десятиліть в цілому. В процесі розвитку завжди існує два протилежні напрямки, що конкурують між собою. Першим можна вважати розвиток комп'ютерної техніки, програмних продуктів та й інформаційної технології в цілому для полегшення та покращення опрацювання інформаційних потоків. Протилежним напрямом вважається не гальмування у розвитку, а прогресивний розвиток у сфері інформаційної кіберзлочинності. Два протилежні напрями в сьогоденні не поступаються у розвитку один одному. У певних сферах один напрям переважає над іншим. На даний момент основним завданням залишається максимальний захист інформації, зокрема захист мультимедійних даних та інших об'єктів інтелектуальної власності.

Для захисту, в першу чергу даних мультимедія, використовується велика кількість програмних продуктів, що дозволяють накладати цифрові водяні знаки на об'єкти, які потребують захисту від несанкціонованого

[1], Українська академія друкарства
[2] Uniwersytet Warmińsko-Mazurski w Olsztynie

використання. Нажаль розробка великої кількості програмних продуктів, не збільшує ефективність і не забезпечує більш надійного захисту від зловмисників, а лише збільшує кількість цих самих програмних засобів. Часто навіть сама розробка програмного забезпечення не передбачає великої кількості можливих зовнішніх факторів впливу, що дозволяють використовувати програмне забезпечення з метою розробки методів змінення чи навіть знищення накладеного цифрового водяного знаку.

Аналіз. Дослідження методів стеганографії значно зростає, оскільки з розвитком персональних комп'ютерів, і розширенням Інтернету, інтерес до передачі захищеної конфіденційної інформації невпинно зростає. Причиною такого значного зацікавлення являється розвиток кіберзлочинності. Більшість сьогоднішніх теоретичних та практичних досліджень у сфері стенографії зосереджена на розробці нових та вдосконаленні існуючих методів захисту мультимедійних даних та об’єктів інтелектуальної власності в цілому. Переважна більшість досліджень сьогодення зосереджена лише на розвитку і покращенні єдиного методу, що на даний момент широко застосовується, а саме цифровий водяний знак.

Наприклад, в науковій роботі [1] розглядається метод вкладення ЦВЗ в аудіофайл зі стисненням; в роботі [2] – знову було запропоновано впровадження ЦВЗ, як для фізичних так і для електронних документів, але вже з можливістю вкладення певної ідентифікуючої інформації в ЦВЗ. Отже, дослідивши наукові роботи можна прийти до висновку, що більшість направлена на дослідження покращення якості та стійкості лише цифрового водяного знаку. При цьому підхід до комплексного захисту шляхом поєднання двох або більше методів залишається більш актуальним та менш дослідженим.

Постановка проблеми. Створення програмних засобів для захисту об’єктів інтелектуальної власності, до яких відносять мультимедійні дані набирають все більшої популярності. Поряд із цим якість надійності накладення та стійкості цифрових водяних знаків до зовнішнього впливу потребує значного покращення, яке можливе шляхом використання надійніших методів та вдосконалення елементів на які спрямовані зовнішні атаки з метою спотворення або знищення ЦВЗ.

Метою статті є дослідження існуючих програмних засобів та методів, що дозволяють здійснювати захист мультимедійних даних нанесенням цифрового водяного знаку та іншими шляхами.

Виклад основного матеріалу. Швидкий розвиток сучасних інформаційних технологій привів до того, що більшість продуктів інтелектуальної праці людей зберігається на цифрових носіях інформації. Вони не тільки зберігаються, але й розповсюджуються та продаються за допомогою глобальної мережі Інтернет, а також на цифрових носіях інформації. Це призвело до того, що виникла необхідність для захисту інтелектуальної власності, розміщеної у цифровому вигляді. Одним з

найбільш ефективних способів вирішення цієї проблеми є використання цифрових водяних знаків (ЦВЗ) [3].

На даний час, коли комп'ютерна стенографія отримала великий поштовх і широкий спектр розвитку, здійснювати захист мультимедійних даних та об'єктів інтелектуальної власності в цілому за допомогою комп'ютерних програмних засобів, що широко розповсюджені в глобальній мережі Інтернет, стало значно простіше. Найпоширеніші програмні засоби для захисту мультимедійних даних можна вважати такі, що дозволяють нанести ЦВЗ або підтвердити достовірність отриманої інформації, шляхом обрахунку хеш-сумми за різними алгоритмами. Тому, щоб отримати надійний захист даних від несанкціонованого використання, постає питання необхідності в досліджені програмних засобів.

В процесі дослідження виявилось, що в даний час окрім, програмних засобів існують онлайн сервіси, що дозволяють накласти цифровий водяний знак на зображення, але лише видимий, тобто такий, що можливо побачити при візуальному перегляді зображення. До популярних онлайн сервісів належать:

- https://www.watermarquee.com/;
- http://www.picmarkr.com/;
- http://www.watermarktool.com/ ;
- http://www.watermark.ws/.

В цілому даний підхід має право на існування, але нажаль не надає великих гарантій, що такий ЦВЗ буде стійким і надійним захистом від подальшого використання мультимедійних даних та об'єктів інтелектуальної власності в інших цілях. Для більш надійнішого захисту мультимедійних даних та об'єктів інтелектуальної власності необхідно застосовувати приховані цифрові водяні знаки, які будуть непомітними без застосування необхідних програмних засобів в поєднанні з іншими елементами захисту, наприклад хеш-сумм.

На сьогодні існує велика кількість програмних засобів, що дозволяють нанести цифровий водяний знак для захисту, більшість з яких не можна вважати досить універсальними, тобто такими, що дозволять поєднати кілька елементів в єдиний захищений об'єкт. Зазвичай в користувача повинні бути вже готові елементи, наприклад зображення яке необхідно захистити та елемент в якому міститься ідентифікаційна інформація про автора зображення. Програмний засіб лише здійснює накладання елемента на зображення, без можливості редагування елемента.

ImageSpyer (рис. 1) один із таких програмних засобів, який являється простим і зрозумілим у використанні. Ця програма не є професійним програмним забезпеченням, ти не менш вона забезпечує досить надійне вкладення цифрового водяного знаку методом LSB**.** Програма ImageSpyer підтримує такі формати JPG, TIF, GIF, PNG, BMP, однак збереження здійснюється лише в стислому форматі (BMP або PNG). Це пов'язано з тим, що при збережені зображення в стислому форматі не враховується значення

LSB, тому ЦВЗ неможливо буде витягти.

Перевагами даного програмного засобу являється зрозумілий інтерфейс, досить надійність в роботі та можливість шифрування інформації за допомогою різних криптографічних алгоритмів. Однак до головних недоліків можна віднести недопрацьованість, оскільки підтримує малу кількість форматів, а також вузький спектр застосування, тобто робота лише з зображеннями.

Рис. 1. Вікно програми ImageSpyer

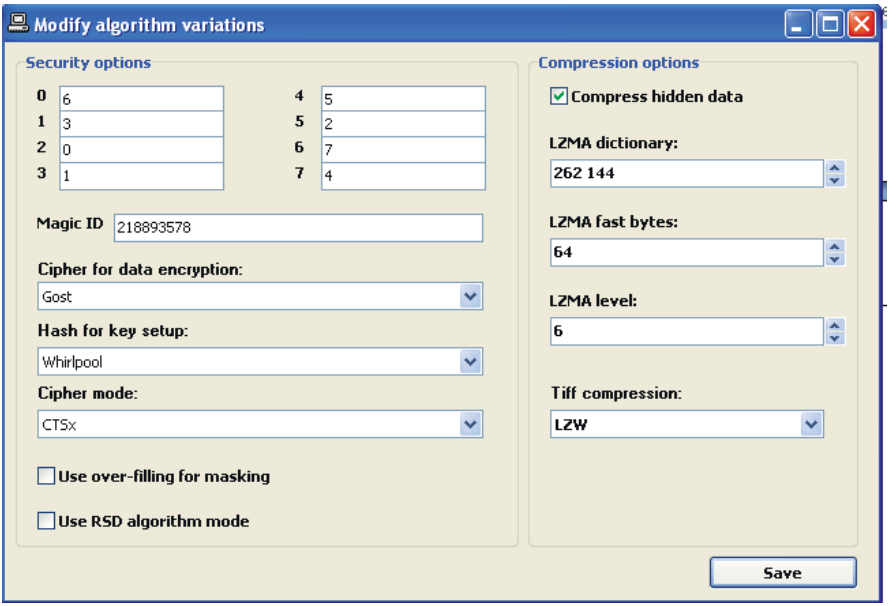

Рис. 2. Вікно налаштувань програми ImageSpyer

Програмний засіб TSR Watermark Image (рис.3), це ще одна можливість здійснювати захист зображень шляхом накладення цифрових водяних знаків.

На відміну від попередньої програми, з TSR Watermark Image користувач може здійснювати редагування цифрового водяного знаку який накладається. В даній програмі існує можливість обрати набір певних параметрів, які задають розташування, розмір, колір, коефіцієнт прозорості водяного знака. При цьому на відміну від ImageSpyer, в даній програмі підтримуються формати JPG, TIF, GIF, PNG, BMP, як для читання так і для збереження. Недоліком в даному програмному забезпеченні можна вважати відсутність будь-якого алгоритму шифрування.

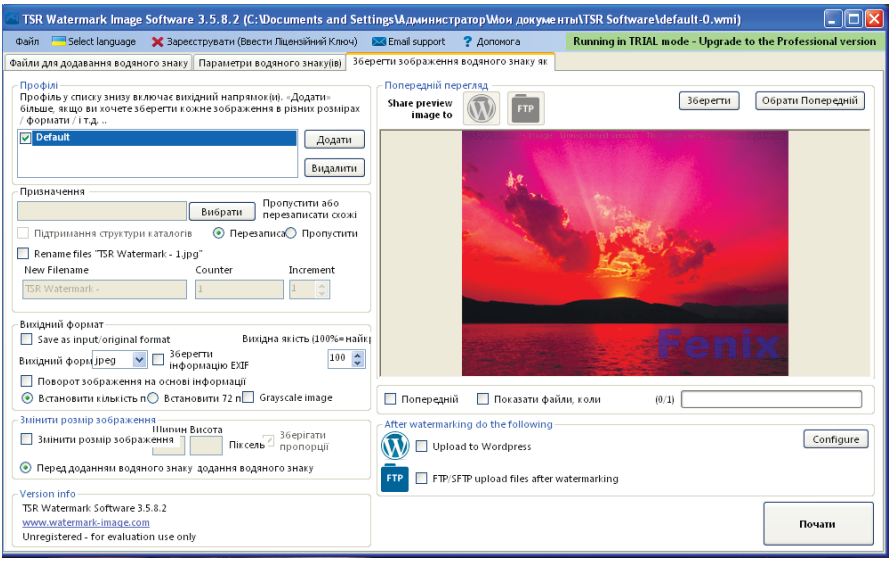

Рис. 3. Вікно програми TSR Watermark Image

Перелік програмних засобів існує досить великий, але нажаль немає вагомих відмінностей від наведених вище програмних засобів. Поряд із ними існують програмні засоби, що дозволяють якісно знищити цифровий водяний знак , тим самим дозволити використання мультимедійних та інших даних. Тому являється необхідним покращити цифровий водяний знак або ж здійснити перевірку на оригінальність.

В мережі Інтернет, щоб вберегтись від підробок, автори часто вказують хеш-сумму для порівняння отриманих даних з оригіналами, тим самим захищаючи свої авторські права.

Кількість програмних засобів, що допомагають в обрахунку хеш-функцій є досить велика. Зазвичай вони прості, малорозмірні і дозволяють обрахувати базові хеш-сумми, такі як MD5, SHA1, SHA256, SHA512, CRC32. Проте існують програмні засоби, що мають можливість обрахунку більшої кількості хеш-сумм. Однією із таких програм являється Easy Hash в якій наявний широкий перелік обрахунку хеш-сумм для різнотипних форматів.

Висновки

Дослідження в сфері комп'ютерної стенографії розвиваються швидко і невпинно. Однак швидкість не завжди дозволяє здійснювати якісних аналіз на якому в подальшому базується висновок. Захист цифровим водяним знаком на даному етапі розвитку вважається пріоритетним та надійним, однак дослідження показують, що велика кількість мультимедійних даних та об'єктів авторського права в цілому захищені не досить надійно,оскільки існують методи та засоби, що дозволяють обійти чи знищити захист. Необхідно здійснювати комплексних захист даних, з можливістю підтвердження чи відстеження мультимедійних даних, що використовуються з іншою метою.

1. *М. В. Калашніков, О. О. Яковенко, Н. І. Кушніренко*. Вбудовування цифрових водяних знаків у аудіо файли зі стисненням без втрат, електронний ресур [Lviv Polytechnic National University Institutional Repository http://ena.lp.edu.ua]

2. *Сагайдак Д.А., Файзуллин Р.Т.,* Способ формирования цифрового водяного знака для физических и электронных документов - - Компьютерная оптика, 2014, том 38, №1.

3 .*Грибунин В.Г*. Цифровая стеганография / Грибунин В.Г., Оков И.Н., Туринцев И.В. – Солон- Пресс, 2002. – 265 с.

Поступила 9.10.2017 р.

УДК 621.3

О.В. Тимченко [1, 2] , д.т.н, професор, О.В. Шевчук [2], ст. викл.

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ СТРІЧКОПРОВІДНИХ СИСТЕМ РУЛОННИХ РОТАЦІЙНИХ МАШИН

Анотація. Створено та проаналізовано поведінку натягу стрічкового матеріалу в рулонних ротаційних машинах на основі універсальної концепції створення багатополюсних елементів окремих вузлів.

Ключові слова: моделювання, рулонна ротаційна машина, багатополюсні елементи.

Abstract. Abstract. The behavior of the tape material tension in rolled rotary machines was created and analyzed on the basis of the universal concept of creating multipole elements of individual nodes.

Keywords: modeling, roll rotary machine, multipolar elements.

[1] Uniwersytet Warmińsko-Mazurski w Olsztynie

[2] Українська академія друкарства

