Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
завідувач кафедри кібербезпеки
та захисту інформації
_____Н.В. Лукова-Чуйко
« » червня 2021р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

дипломної роботи
***бакалавра*.**
(назва освітнього рівня)

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітня програма Кібербезпека
(назва освітньої програми)

на тему: «Методи та моделі захисту авторського права аудіо об'єктів»

Виконавець: студентка IV курсу, групи КБ-42

_____ **Бурбела Катерина Русланівна**
(підпис) (прізвище ім'я по-батькові)

	Прізвище, ініціали	**Підпис**
Керівник	Зюбіна Р.В.	

Нормоконтроль	Зюбіна Р. В.	

Київ 2021

Міністерство освіти і науки України
«Київський національний університет імені Тараса Шевченка»

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри кібербезпеки
та захисту інформації
_____Н.В. Лукова-Чуйко
«10» жовтня 2020 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-42** **Бурбела Катерина Русланівна**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи Методи та моделі захисту авторського права аудіо об'єктів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема дипломної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №2 від 08.10.2020 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Стеганографія, авторське право

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно ознайомитися з нормативно правовою базою сфери авторського права, стеганографічними засобами захисту авторського права, обрати метод приховування даних та ознайомитися з його алгоритмом, розробити програмне забезпечення спрямоване на захист авторського права стеганографічними методами.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено програмний продукт, спрямований на вбудовування цифрового водяного знаку в аудіо об’єкти.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання:12 жовтня 2020 року

Завдання видав _____ (підпис) Р.В. Зюбіна (ініціали, прізвище)

Завдання прийняла до виконання _____ (підпис) К.Р. Бурбела (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	25.01.2021 – 30.01.2021	*виконано*
2	Аналіз літератури	31.01.2021 – 12.02.2021	*виконано*
3	Обґрунтування вибору рішення	13.02.2021 – 18.02.2021	*виконано*
4	Вивчення нормативно правової бази у сфері авторського права	19.02.2021 – 07.03.2021	*виконано*
5	Аналіз проблем інформаційної безпеки у сфері авторського права	08.03.2021 – 25.03.2021	*виконано*
6	Дослідження методів та алгоритмів стеганографії	26.03.2021 – 10.04.2021	*виконано*
7	Вироблення програмного забезпечення для вбудовування цифрового водяного знаку в аудіо об’єкт	11.04.2021 – 17.05.2021	*виконано*
8	Оформлення пояснювальної записки	18.05.2021 – 08.06.2021	*виконано*
9	Підготовка до захисту дипломної роботи	09.06.2020 – 21.06.2021	*виконано*

Завдання видав _____ (підпис) Р.В. Зюбіна (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) К.Р. Бурбела (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 08 червня 2021 року

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 57 сторінок основного тексту, 17 рисунків та 1 формулу. Список використаних джерел містить 29 найменувань і займає 3 сторінки.

Метою даної роботи є дослідження методів захисту авторського права з використанням стеганографічних алгоритмів, спрямованих на вбудовування цифрового водяного знаку в аудіо об’єкти.

У роботі проаналізована існуюча література з питання захисту авторського права, стеганографії, її використання з метою захисту інформації та література про стеганографічні засоби та методи.

Розроблено програмний продукт для захисту авторських прав у аудіо об’єктах. Представлено процес роботи розробленого програмного додатку та проведено аналіз його ефективності.

Ключові слова: авторське право, захист авторського права, стеганографія, стеганографічні методи, комп’ютерна стеганографія, цифрова стеганографія, аудіо стеганографія, фазове кодування.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, СИМВОЛІВ

DRM – англ. Digital rights management – технічні засоби захисту авторського права.

LSB – англ. Least Significant Bit – найменш значущий біт.

WAV – WAVE – формат файлу-контейнера для зберігання записів оцифрованого аудіо потоку.

КС – комп’ютерна стеганографія.

ЦВЗ – цифровий водяний знак.

ЦОС – цифрова обробка сигналів.

ЗМІСТ

РЕФЕРАТ 4

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, СИМВОЛІВ 5

ЗМІСТ 6

ВСТУП 8

РОЗДІЛ 1 СТЕГАНОГРАФІЯ ТА ЇЇ ВИКОРИСТАННЯ У СФЕРІ АВТОРСЬКОГО ПРАВА 11

1.1 Авторське право. Основні терміни, актуальні аспекти його забезпечення . 11

1.2 Стеганографія, терміни та визначення 14

1.3 Практичні аспекти використання стеганографічних методів захисту інформації 21

Висновки за розділом 1 25

РОЗДІЛ 2 МЕТОДИ АУДІО СТЕГАНОГРАФІЇ, ЯК ВИРІШЕННЯ ПОСТАВЛЕНОЇ ПРОБЛЕМИ 27

2.1 Способи забезпечення авторського права з використанням стеганографічних методів 27

2.2 Методи стеганографії файлів 28

2.3 Порівняння методів аудіо стеганографії 37

Висновки за розділом 2 38

РОЗДІЛ 3 ЗАХИСТ АВТОРСЬКОГО ПРАВА В АУДІО ОБ’ЄКТАХ 41

3.1 Порівняльна характеристика різних мов програмування 41

3.2 Вимоги до розробленого програмного забезпечення 43

3.3 Результат виконання прописаного алгоритму 45

Висновки за розділом 3 48

ВИСНОВКИ 51

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 55
ДОДАТКИ 58

ВСТУП

Актуальність. Досить стрімкий розвиток інформаційних технологій спричиняє актуалізацію питання інформаційної безпеки. Питання отримання вільного доступу до інформації з кожним днем вирішується все швидше і швидше, а те з яким обсягом інформація публікується у мережі Інтернет ставить перед нами важливу задачу захисту авторського права на інтелектуальну власність.

Кількість мультимедійних даних, опублікованих чи розповсюджених у мережі Інтернет перевів проблему захисту авторства на новий рівень. Що власне і призвело до стрімкого розвитку та розробки систем захисту мультимедійної інформації від несанкціонованого копіювання та розповсюдження.

До того моменту, як з'явилася необхідність захисту авторського права для цифрових технологій, популярним методом затвердження власника, автора інформації були водяні мітки та методи надання власних ідентифікаційних номерів. Для мультимедійних даних було створено аналоги цих методів, які дають змогу не просто встановлювати мітки, які вкажуть на того кому належать авторські права на цей об'єкт, а й за допомогою цих міток відслідковувати використання, копіювання та опублікованих даних.

Цифрові водяні знаки є одним з найбільш ефективних технічних засобів захисту. Його сутність полягає у тому, що в об'єкт, який потребує захисту, вибудовується невидима (інколи видима) мітка, яка дозволяє контролювати використання мультимедійного продукту, який було марковано.

Першим типом мультимедійних даних, для якого практикувалося так зване маркування були цифрові зображення. Це пояснюється великою інформаційною ємністю подібних об'єктів. Проте, у сьогодення, метод маркування об'єктів зустрічається не тільки для зображень, а й для аудіо та відео файлів. Є безліч методів, які сприяють вбудовуванню даних у будь-який мультимедійний об'єкт.

Якщо узагальнити питання маркування даних, то можна дійти висновку, що ця проблема розглядається як проблема передачі або вбудовування слабкого сигналу,

яким буде цифровий водяний знак, у широкосмуговий сигнал, який є стеганоконтейнером. Цей сигнал має бути вбудований таким чином, щоб людські органи сприйняття не могли відчути різницю між оригінальним файлом без маркування і файлом, в який вже вбудовано цифровий водяний знак. Також важливим аспектом є унеможливлення внесення спотворень до вже маркованого файлу, щоб унікальну мітку не можна було виправити чи взагалі видалити з об'єкту.

Взагалі, вимоги до створеного та вбудованого в мультимедійні дані водяного ключа є досить неоднозначними. З одного боку необхідно забезпечити найменш помітне, відчутне спотворення у порівнянні з оригінальним файлом, а з іншого боку необхідно забезпечити високо стійкість цифрового водяного знаку до видалення чи коригування, для чого частіше за все використовують метод повторного вбудовування цифрового водяного знаку, а це створює велику кількість спотворень у маркованому об'єкті. Також системи вбудовування цифрового водяного знаку мають враховувати особливості сучасних стандартів стиснення, як JPEG, WAV або MPEG для успішної передачі або зберігання цифрових об'єктів.

Аналіз останніх досліджень та літератури. До іноземних вчених, які зробили вклад у вивчення методів стеганографії можна віднести: Gopalan, K., Wenndt, S., Haddad, D. До вітчизняних науковців, які вивчали цю тематику можна віднести Г. Ф. Конахович, Д. О. Прогонов, В. Г. Грибунин, Гончаров Н. О.

Усе вищесказане призводить до того, що *завдання* розробки програмного забезпечення, яке буде використовувати оптимальний алгоритм впровадження цифрового водяного знаку для захисту аудіо об'єктів від несанкціонованого видалення чи копіювання, є актуальними.

Тому *метою роботи* є дослідження методів захисту авторського права з використанням стеганографічних алгоритмів, спрямованих на вбудовування цифрового водяного знаку в аудіо об'єкти.

Для досягнення поставленої мети необхідно вирішити наступні *завдання:*

- розглянути існуючу нормативно-правову базу створену з метою регулювати захист авторського права в Україні та процес використання стеганографічних алгоритмів;

- дослідити проблематику питання захисту авторського права та використання стеганографічних методів та алгоритмів;
- дослідити існуючі стеганографічні алгоритми на предмет найбільш відповідного всім вимогам для вирішення головного завдання роботи;
- розробити програмний продукт спрямований на вирішення проблеми вбудовування цифрового водяного знаку з метою захисту авторських прав в аудіо об’єктах.

Об'єктом дослідження в даній роботі є процес захисту авторського права методами стеганографії.

Предметом дослідження в даній роботі є методи, засоби і алгоритми захисту авторського права стеганографічними методами.

До *методів дослідження* дипломної роботи можна віднести:

- аналіз літератури, пов’язаної зі стеганографічними методами та авторським правом;
- аналіз нормативно-правових документів, спрямованих на регулювання питань захисту авторського права та використання стеганографічних методів;
- порівняння існуючих стеганографічних алгоритмів;
- вивчення та узагальнення існуючих практик з метою вирішення поставленої задачі.

РОЗДІЛ 1
СТЕГАНОГРАФІЯ ТА ЇЇ ВИКОРИСТАННЯ У СФЕРІ АВТОРСЬКОГО ПРАВА

1.1 Авторське право. Основні терміни, актуальні аспекти його забезпечення

Питання авторського права на даний момент є чи не одним з найактуальніших, переважна кількість інформації зараз публікується в мережі Інтернет, де у кожного є вільний доступ до цих даних і безмежна кількість можливостей порушити їхню цілісність, конфіденційність і, при бажанні доступність. Якщо взяти за приклад типовий веб-сайт, то можна побачити там безліч мультимедійних цифрових об'єктів, які потребують захисту. Такими об'єктами можуть виступати текстові об'єкти, відео або фотозображення. Зазвичай ці об'єкти захищаються авторським правом.

В Україні сфера діяльності авторського права регулюється Законом України про авторське право та суміжні права. згідно цього закону авторське право — це особисті немайнові права і майнові права авторів та їх правонаступників, пов'язані із створенням та використанням творів науки, літератури і мистецтва.

Авторське право поширюється на об'єкти як оприлюднені, так і не оприлюднені, ці об'єкти можуть існувати в будь-якій формі, як усній так і письмовій чи друкованій. Враховуючи проблематику даної роботи необхідно розглянути об'єкти, опубліковані у мережі Інтернет чи ті, що містяться на будь-якій обчислювальній машині, тобто мультимедійні об'єкти. Проте майже всі об'єкти авторського права можна перекласти у цифровий мультимедійний об'єкт. Тому існує окремий термін — керування цифровими правами.

Digital rights management (далі DRM) — це термін, яким визначається сукупність технологій авторизації, які використовують виробники програмних

забезпечень, приватні особи та узагалі власники авторського права з метою обмежити несанкціоноване використання цифрової інформації та носіїв. Також це термін використовується для опису обмежень, пов'язаних безпосередньо з використанням пристроїв або творів у цифровій формі. На даний момент DRM використовується багатьма провідними компаніями, такими як Apple Inc., Microsoft та BBC.

Головною проблемою процесу доведення реальних авторських прав в мережі Інтернет є занадто швидка модифікація інформації, її постійне оновлення, редагування та будь-які видозміни. Тобто головною задачею є оперативне закріплення прав власності і надання певної доказової бази щодо їх закріплення відповідним органам. До способів закріплення факту наявності авторського права на веб сторінках можна віднести наступне:

– нотаріальне посвідчення для веб сайту;

– акт огляду веб сайту з додатком у вигляді фотографії (скріншоту) власне сайту, який здійснюється безпосередньо адвокатом, працюючим на власника об'єкту;

– фактично сама роздруківка сторінки веб сайту засвідчена власником з підтвердженням достовірності у вигляді встановлення відповідних печаток та дат.

В Україні існує необхідність закріпити нормативну базу, яка регулює можливість встановлення юридичного факту наявності авторського права і його допустимості у використанні в якості доказу отриманого в мережі Інтернет. На даний момент документом, який займається регуляцією цього процесу є "Рекомендації щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет". [2]

Відповідно до згаданого вище документу існують наступні технічні засоби, які сприяють закріпленню авторського права на об'єктах розміщених в мережі Інтернет:

– Ідентифікація об'єктів авторського права і суміжних прав. Даний засіб розуміє собою надання певних рис, котрі будуть відрізняти об'єкти між собою

(наприклад: ідентифікаційних код, короткі власні назви чи певні нумерації в реєстрах)

До методів ідентифікації відносяться ідентифікаційний код ISBN, тобто міжнародний стандартний книжковий номер та ідентифікаційний код ISAN, котрий відповідає за досить ефективний захист фільмів та будь-яких інших аудіовізуальних творів. [3]

Якщо конкретніше, то код ISBN є універсальним ідентифікаційним кодом, його проставляють на всіх книгах та брошурах незалежно від їх обсягу та виготовлення. Цей код дає змогу зібрати в одну єдину систему видання та розповсюдження книжок, замінюючи собою довгі бібліографічні описи. Код ISAN або міжнародний стандартний аудіовізуальний номер є одним зі способів систематизації будь-яких унікальних аудіовізуальних об'єктів (наприклад: фільмів, телевізійних програм чи, навіть, реклам). Цей код дозволяє не просто зібрати в одну систематизовану так би мовити базу даних усі ці об'єкти, а й ідентифікувати усі пов'язані між собою версії і їх особливості (наприклад, різні ліцензійні озвучки одного й того ж фільму) [4]

– Електронний цифровий підпис (далі ЕЦП)

ЕЦП – це такий вид підпису, який отримується внаслідок шифрування певного набору електронних даних, і надає можливість ідентифікувати підписувача. Накладається ЕЦП з використанням особистого ключа, а перевіряється за допомогою відкритого. Проте є суттєвий недолік даного методу, він є ефективним виключно за використання вже існуючої інфраструктури відкритих ключів. [5]

– Цифрові водяні знаки (далі ЦВЗ)

Даний засіб відноситься до технологій DRM, і в принципі саме він і цікавить нас у нашій роботі. ЦВЗ — це технологія, створена для захисту мультимедійних даних методом впровадження в них міток з інформацією. Зазвичай це текст або логотип, який ідентифікує автора та\або власника даних.

ЦВЗ можуть бути видимими або невидимими. Переважно ЦВЗ впроваджуються в цифрові дані невидимо. Вони відрізняються тим, що інформація

буквально “зашивається” прямо в сигнал, а об’єкти мультимедіа таким чином являють собою контейнери даних.

Взагалі ЦВЗ не є механізмом DRM, проте є частиною системи DRM, яка використовується для надання так званої візуальної інформації про легальність використання контенту і включає в себе дані про особливості цього контенту наприклад, про продавця або покупця.

1.2 Стеганографія, терміни та визначення

З кожним днем людство робить все більше кроків на зустріч новим технологіям, що призводить до змінення пріоритетів щодо захисту таких об’єктів, як інформація. Законі України “Про інформацію” визначає інформацію як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Наразі хіба що не найбільшу цінність має саме інформаційний ресурс, отримання доступу до якого, унаслідок появи глобальних комп’ютерних мереж, тепер є надзвичайно простим. Одразу зі спрощенням способів використання інформаційних технологій прогресує і кількість загроз порушення безпеки даних. Даний прогрес також викликає зростання способів та методів захисту інформації, конфіденційних даних, прав інтелектуальної власності, а також авторських прав.

Завдання надійного захисту інформації (котра наразі має переважно цифровий формат) від несанкціонованого доступу є однією з невирішених на сьогодні проблем. Згідно до Закону України “Про інформацію”, захист інформації визначається як сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Інтенсивний розвиток технологій, за допомогою яких можна отримати можливість обробки та відтворення різних типів сигналів (або текстових та мультимедійних об’єктів) спричиняє актуалізацію питання захисту інформаційного ресурсу представленому в цифровому вигляді.

Звичайно є переваги подання та передачі даних у цифровому форматі, наприклад

– зручність використання;
– зручність зберігання;
– швидкість передачі;
– легкість відновлення;
– перспективи їх використання за допомогою різних програмних рішень.

Проте всі переваги, за невдалого використання, можуть бути перекреслені через таку саму легкість і швидкість з якою вони можуть бути викрадені, модифіковані чи знищені.

Дуже складно сказати, що існує спосіб захистити будь-що так, щоб ніхто не мав до цього доступ, саме тому кількість загроз довкола інформаційних об’єктів призводить до розвитку їх захисних систем. Що також спричинило появу питання розробки методів захисту інформації до яких належать криптографічні та стеганографічні методи. [6]

Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” зазначає, що криптографічний захист інформації — це вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо. [7]

Якщо спростити, то мета криптографічного захисту інформації — це зробити дані незрозумілими для непосвячених, приховати зміст повідомлень та файлів методом їх шифрування. [6]

Даний метод захисту розв’язує встановлену вище проблему тільки частково, адже зашифрована інформація своєю незрозумілістю досить сильно привертає увагу і, якщо зловмисник заволодіє файлом захищеним з використанням цього методу – відразу зрозуміє, що в ньому розміщено секретну інформацію і впродовж певного часу зможе її дешифрувати.

Стеганографія — тайнопис, при якому повідомлення, закодоване таким чином, що не виглядає як повідомлення — на відміну від криптографії. Таким

чином непосвячена людина принципово не може розшифрувати повідомлення — бо не знає про факт його існування.

Спрощено – завданням стеганографії є приховання факту наявності секретних даних при їх передачі, обробці або зберіганні, адже стеганографія вивчає способи та методи приховування конфіденційних відомостей.

При використанні цього методу ще однією важливою задачею є унеможливлення виявлення в перехопленому повідомленні наявності іншого (прихованого) повідомлення і взагалі мінімізація можливості виникнення будь-яких підозр.

Очевидно, що передача зашифрованої (незрозумілої) інформації викликає певні підозри, тому переважно ці дві науки використовуються разом, а саме:

- криптографія – для шифрування;
- стеганографія – для приховування факту передачі зашифрованої інформації.

Таким чином, ці два методи стають не взаємозамінними, а взаємодоповнюючими.

Стеганографія є менш популярним методом захисту. Вона здійснюється різними способами. Проте загальною рисою є вбудовування повідомлення в об'єкт, який при відкритому пересиланні адресатові не буде привертати значну увагу.

До основних визначень, якими оперує стеганографія, належать:

- повідомлення — це будь-які дані, що призначені для передачі;
- стеганоконтейнер — це оригінальний варіант файлу, який призначений для приховування даних або повідомлень;
- стеганоповідомлення — це власне інформація, яка вбудовується у стеганоконтейнер;
- порожній контейнер — це початковий файл, до того як в ньому розмістили повідомлення;
- заповнений контейнер — файл з вже вбудованим у нього секретним повідомленням;

- об’єм контейнеру — це найбільш можлива частина файлу, у яку є змога помістити повідомлення;
- процент заповнення контейнеру — та частина стеганоконтейнеру, яка є заповненою вбудованим повідомленням.

Історично напрям стеганографічного приховування інформації був першим, проте згодом був витиснутий криптографією через особливості її стійкості та швидкий розвиток. Приховування інформації виключно базуючись на факті невідомості зловмисникам методу, покладеного в основі приховування, є досить малоефективним.

Перший опис використання стеганографії датується греками. Геродот розповідає, як грекам було передано повідомлення про ворожі наміри Ксерсеса під воском письмової таблички, і описує техніку нанесення послідовних букв у титульний текст секретним чорнилом вигадану завдяки Енею.

Піратські легенди розповідають про практику татуювання секретної інформації, наприклад карти, на голові когось з команди так, щоб можна було волоссям її приховувати.

Кан розповідає про хитрість, яка застосовувалася в Китаї з вбудовуванням ідеограми коду в заздалегідь встановлену позицію в диспетчері. Подібна ідея призвела до системи решіток, що застосовувалася в середньовічній Європі, де дерев'яний шаблон розміщували над, здавалося б, нешкідливим текстом, висвітлюючи вбудоване таємне повідомлення.

Під час Другої світової війни шпигунами застосовувався решітчастий метод або деякі його варіації. У той же період німці розробили технологію мікро точок, яка друкує чітку, якісну фотографію, зменшуючи її до розміру крапки.

Ходять чутки, що в 1980-ті роки Маргарет Тетчер, тодішній прем'єр-міністр Великобританії, настільки роздратувалась через витоки документів кабінету міністрів у пресі, що вона запрограмувала текстові процесори для кодування ідентичності письменника в інтервалі слів, таким чином маючи можливість простежити нелояльних міністрів.

Під час "холодної війни" США та СРСР хотіли сховати свої датчики в об'єктах ворога. Ці пристрої повинні були непомітно надсилати дані своїм країнам.

У 1985 р. персональні комп'ютери почали використовувати для класичної стеганографії. Подальший розвиток відбувався досить повільно, але сьогодні існує велика кількість програм для стеганографії. Будучи формою захисту, яка покладається на секретність, алгоритм стеганографії, на відміну від криптографічного, повинен враховувати правдоподібну форму, яку повинні мати сформовані дані, щоб вони не викликали підозр.

У цифровій стеганографії електронні комунікації можуть включати стеганографічне кодування в транспортному рівні, наприклад файл документа, файл зображення, програма або протокол. Мультимедійні файли ідеально підходять для стеганографічної передачі через їх великий розмір. Наприклад, відправник може надіслати нешкідливий файл зображення та відкоригувати колір одного пікселя в сотні відповідно до алфавітного символу. Зміни настільки тонкі, що навряд чи хтось їх помітить, якщо вони спеціально не шукають їх.

Тому стеганографія представляється ідеальним інструментом для створення секретних каналів зв'язку, які можуть бути використані в складних сценаріях шпигунства, комп'ютерних злочинів та порушення конфіденційності як державних, так і приватних суб'єктів.

Сьогодні стеганографія досліджується як з законних, так і з незаконних причин.

Серед перших є військові телекомунікації, які використовують розширений спектр, щоб приховати як повідомлення, так і його джерело.

Іншим важливим використанням є вбудовування даних про медичні зображення, щоб не виникало проблем зі збігом записів та зображень пацієнта.

На промисловому ринку, з появою цифрових комунікацій та зберігання, однією з найважливіших проблем є захист авторських прав, тому розробляються методи цифрових водяних знаків, щоб обмежити використання захищених авторським правом даних.

Серед незаконних причин – практика приховування сильно зашифрованих даних, щоб уникнути контролю, передбаченого законами про експорт криптографії.

Невидиме чорнило – є одним з прикладів класичної стеганографії, не пов'язаної з комп'ютерами. Людина може написати повідомлення прозорими або «невидимими» чорнилом, яке можна побачити лише тоді, коли на папір нанесено інше чорнило або рідина. Подібним чином, у цифровій стеганографії мета полягає в тому, щоб приховати інформацію від користувачів, за винятком тих, хто призначений бачити або чути її. [10]

Комп'ютерна стеганографія — це напрям класичної стеганографії, заснований на особливостях комп'ютерної платформи. Нижче наведено кілька прикладів комп'ютерної стеганографії:

- відтворення звукової доріжки назад для розкриття секретного повідомлення;
- відтворення відео з більш високою частотою кадрів (FPS), щоб виявити приховане зображення;
- вбудовування повідомлення в червоний, зелений або синій канал зображення RGB;
- приховування інформації в заголовку файлу або метаданих;
- вбудовування зображення чи повідомлення у фотографію за допомогою додавання цифрових шумів.

Якщо детальніше розглядати стеганографічну файлову систему StegFS для UNIX подібних систем, суть якої полягає у приховуванні даних в невикористовуваних форматах файлів, підміну символів у назвах файлів чи текстову стеганографію, можна навести більш конкретні приклади:

– використання зарезервованих полів комп'ютерних форматів файлів;

Суть цього методу полягає у використанні поля розширення. Не заповнена актуальною інформацією частина цього поля, за замовчуванням заповнюється нулями. Що, відповідно, дає змогу використати цю "нульову" частину для запису своїх даних. Проте, цей метод має недолік, який полягає у малому обсягу переданої інформації.

– метод приховування інформації в невикористовуваних місцях гнучких дисків;

При використанні зазначеного алгоритму повідомлення розміщується у невживані частини гнучкого диску, наприклад, на нульову доріжку. Однак цей метод, як і попередній має недолік у передачі невеликих за розміром даних.

– Використання особливостей файлових систем

При зберіганні на жорсткому диску файл завжди займає певну кількість кластерів. Наприклад, у раніше широко використовуваної файлової системи FAT32 (використовуваної в Windows 98/Me/2000) стандартний розмір кластера — 4 Кб. Відповідно для зберігання 1 Кб інформації на диску виділяється 4 Кб інформації, з яких тільки 1 Кб реально потрібен для зберігання файлу, інші ж 3 Кб ні на що не використовуються. Ці 3 Кб вільного місця можна з легкістю застосувати з метою зберігання інформації. Проте до недоліків можна віднести, що подібне зберігання/передача даних має дуже велику ймовірність виявлення.

Розвиток засобів цифрової обчислювальної техніки дав поштовх для розвитку комп'ютерної стеганографії, яка базується на поміщені секретного повідомлення в цифрові дані з аналоговою природою, наприклад в фотозображення, відео чи аудіозаписи.

Визначається цифрова стеганографія, як напрям класичної стеганографії, заснований на захованні або впровадженні додаткової інформації в цифрові об'єкти, викликаючи при цьому деякі спотворення, які знаходяться нижче межі чутливості середньостатистичної людини та не призводять до помітних змін цих об'єктів.

Методи за яких прихована інформація передається з використанням особливостей роботі протоколів передачі даних набувають великої популярності. Подібні методи мають назву «мережева стеганографія». Для реалізації подібного протоколу можуть використовуватися як зміна властивостей одного протоколу так і два або більше взаємопов'язаних протоколів з метою більш надійно приховати факт передачі секретного повідомлення.

1.3 Практичні аспекти використання стеганографічних методів захисту інформації

До основних задач стеганографії відносяться не тільки сам факт секретної передачі файлу, а й вбудовування цифрових водяних знаків та вбудовування ідентифікаційних номерів.

Згідно до основних задач, основним завданням будь-якої стеганографічної системи (далі СС) є розміщення повідомлення в контейнері таким чином, щоб сторонні спостерігачі не помічали різниці між оригінальним об'єктом та модифікованим. До базових характеристик СС відносяться:

- невідчутність;
- стійкість;
- безпека;
- пропускна здатність (для створюваного стеганографічного каналу).

Під невідчутністю мається на увазі, що повідомлення має бути вкраплене так, щоб для людських органів відчуття це було непомітно. Наприклад, для зображень повідомлення має бути непомітним для людського зору, а в аудіо файлах — повідомлення має бути нечутно. Такого допомагають досягти або незначні зміни внесені до стеганоконтейнеру або врахування особливостей людських органів почуттів, наприклад використання тих частот, що людина не чує для аудіо стеганографії або внесення модифікацій, які лежать нижче абсолютного порогу чутності.

Суть поняття стійкості залежить по-перше від типу стеганосистеми а по-друге від типу атак, які є для неї характерними. Одним з прикладів вирахування стійкості стеганосистеми можна вважати оцінку кількості помилок, що виникли при вилученні інформації зі стеганоконтейнеру після можливого спотворення не навмисними або активними атаками. Якщо говорити про системи, в яких здійснюються пасивні атаки, то СС вважається стійкою, коли несанкціонований користувач не матиме змогу відрізнити пусті і заповнені контейнери між собою без використання особливих методів, наприклад, візуального аналізу.

Поняття ємності визначається кількістю даних повідомлення, що потенційно можуть бути вкраплені в один елемент контейнера і не порушити умови невідчутності та стійкості. Способи визначення кількості приховуваної інформації існують різні через різні види порушників, можливості та типи контейнерів і самих повідомлень. Проте незмінним є те, що ємність визначає саме об'єм інформації, яку є можливість приховати і цей об'єм називається наповненістю контейнера. Очевидно, що з метою правильного функціонування СС коефіцієнт наповненості не може перевищувати пропускну здатність створюваного стегоканалу. Вимірюється наповненість переважно у відсотках, тому максимально наповнений контейнер матиме наповненість 100%, а пустий — 0%.

Основними галузями застосування стеганографії є:

- захист від копіювання;
- прихована анотація документів;
- автентифікація;
- прихований зв'язок.

До захисту від копіювання можна віднести сферу електронної комерції, контроль за копіювання (наприклад в DVD дисках, чи фільмах на піратських сайтах) та питання несанкціонованого розповсюдження мультимедійної інформації загалом.

До прихованої анотації документів можна віднести приховування даних про пацієнтів на медичних знімках або про власників в мультимедійних базах даних.

Системи відеоспостереження, голосова пошта та конфіденційне діловиробництво можна віднести до галузі автентифікації.

В галузі прихованого зв'язку стеганографія може використовуватися в якості військових та розвідувальних додатків.

Секретна передача даних є класичною задачею стеганографії, проте напрямки, які орієнтовані переважно для захисту інтелектуальної власності є більш актуальними для даної роботи. І переважно цей напрям вважається напрямком розвитку комп'ютерної стеганографії, яка також має два основні напрями використання:

- пов’язаний із цифровою обробкою сигналів (далі ЦОС)
- непов’язаний з ЦОС

Той, що непов’язаний з ЦОС має собою на увазі розміщення конфіденційної інформації в заголовках даних, на жаль він не знайшов широкого застосування через малу стійкість до атак, через легке виявлення та модифікацію або видалення прихованого повідомлення.

Перший же напрямок, який є пов’язаним з ЦОС розуміється як метод, в якому секретне повідомлення вбудовується в цифрові або мультимедійні дані. І наразі переважна кількість досліджені здійснюється саме в цьому напрямку, що спричинило виникнення поняття цифрової стеганографії (далі ЦС). [11]

З зазначеного вище можна зробити висновок, що цифрова стеганографія — це напрямок стеганографії, який заснований на використанні цифрових об’єктів у якості стеганоконтейнера.

ЦС містить у собі наступні напрямки:

- вбудовування інформації з метою її прихованої передачі;
- вбудовування цифрових водяних знаків або watermarking (далі ЦВЗ);
- вбудовування ідентифікаційних номерів або fingerprinting;
- вбудовування заголовків або captioning.

Перший варіант несе за собою досить очевидний посил, а саме приховування факту передачі інформації у об’єкті. Другий напрям, ЦВЗ, як зазначено вище, слугує більше для захисту авторських прав. Його відмінність від першого напряму полягає у тому, що при прихованій передачі даних зловмисник не здогадується про факт наявності інформації, а в випадку з ЦВЗ факт наявності навпаки відомий.

Цифрові водяні знаки переважно використовуються для захисту від копіювання або несанкціонованого використання, наприклад в мультимедійних файлах, фотографіях буде стояти мітка, яка засвідчує факт належності об’єкту певному юридичному або фізичному обличчю. На відміну від звичайних водяних знаків, ЦВЗ можуть бути як видимі, так і невидимі. Невидимі зазвичай аналізуються спеціальним декодером, який може засвідчити факт коректності та належності цього

цифрового знаку. Зазвичай він містить якісь дані про власника, наприклад його автентичний код.

Напрямок вбудовування ідентифікаційних номерів відрізняється від ЦВЗ тим, що, при використанні першого напрямку, ми розміщуємо в об'єкт не "якусь" інформацію про власника, а конкретний унікальний вбудований номер (який також називають відбитком). Таким чином власник або виробник мультимедійних даних може не просто помітити усі копії свого об'єкту, а й відслідковувати його подальшу долю на предмет порушень прав інтелектуальної власності, і, якщо порушення буде виявлено, можна буде з легкістю відслідкувати зловмисника.

Метод вбудовування заголовків застосовується у медицині, наприклад для підпису медичних знімків (рентгенівських знімків) Його метою є зберігання різнорідної інформації в єдиному цілому. Цей напрям відзначається тим, що він єдиний, в якому немає явного потенційного зловмисника.

Щодо актуальності зазначеного вище напрямку захисту інформації, можна зазначити, що стеганографія розвивається досить інтенсивно застосовується у найрізноманітніших науках.

З боку виконання задач стеганографії, можна відзначити той факт, що з точки зору першої і основної задачі, а саме приховання передачі викраденої інформації, стеганографічні методи дають змогу та ресурси, котрі можна використати з метою виконання поставленої задачі.

Якщо говорити про наступну задачу стеганографії, захист авторського права від піратства, винайдено безліч методів встановлення певних міток, які допоможуть досягти виконання поставленої задачі. Дані методи настільки розповсюджені, що вже використовуються у багатьох електронних версіях журналів.

Розрізняють два методи впровадження стеганографії в якості засобів програмно-технічного захисту:

- додатковий захист;
- вбудований захист.

У випадку додаткового захисту, стеганографія є лише доповненням до основних засобів захист в комп'ютерній системі. А у випадку вбудованого захисту,

стеганографічні засоби виступають у якості окремих компонентів інформаційної системи. [12]

При порівнянні даних методів стає зрозуміло, що перший спосіб є більш гнучким для використання, але більш проблематичним у разі виникнення несумісностей різних засобів захисту між собою. В той час як другий спосіб є більше надійним але критичним до внесення будь-яких змін.

Висновки за розділом 1

У першому розділі було розглянуто основні терміни і положення сфери авторського права та стеганографічного захисту. Переважна кількість визначень, які стосуються авторського права є зазначеними у Законі Україні “Про авторське право та суміжні права”. Щодо документів, які регулюють діяльність у сфері стеганографічного захисту інформації, було використано Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”, проте також можна зазначити, що вони потребують досконалого доопрацювання.

Згідно до наведених вищу досліджень можна стверджувати, що авторське право – це особисті немайнові права і майнові права авторів та їх правонаступників, пов’язані із створенням та використанням творів науки, літератури і мистецтва, а стеганографічний захист інформації – це спосіб захисту даних методом приховання їх наявності в об’єкті.

У ході дослідження вказано, що сферою використання авторського права є захист об’єктів як оприлюднених, так і не оприлюднених, ці об’єкти можуть існувати в будь-якій формі, як усній так і письмовій, друкованій чи електронній.

Встановлено головну проблему процесу доведення реальних авторських прав в мережі Інтернет, а саме: факт занадто швидкої модифікація інформації, її постійне оновлення, редагування та будь-які її видозміни.

У даному розділі було також визначено основні сфери застосування стеганографії (наприклад для факту приховування передачі військових

даних/таємниць), а також було зазначено, що на теперішній час сфера авторського права є основною галуззю використання та розвитку стеганографічних методів.

Також було наведено історичні приклади використання стеганосистем. Також було наведено приклади сучасного їх застосування у різних галузях. було зазначено, що стеганографічні методи використовуються не тільки з метою захистити авторське право у мультимедійних даних, а й у різних сферах життя людини, наприклад у медицині для розміщення інформації про пацієнта на рентгенівських знімках.

У цьому розділі було встановлено основні характеристики стеганографічних систем, до яких відносяться:

- невідчутність;
- стійкість;
- безпека;
- пропускна здатність (для створюваного стеганографічного каналу).

З точки зору дотримання вказаних параметрів (характеристик), стеганографічні методи дають змогу та ресурси, котрі можна використати з метою виконання поставленої задачі.

Проведений аналіз та порівняння дають можливість визначити наступні кроки проведення дослідження:

1. визначити методи стеганографії направлені на захист авторського права;
2. навести загальну характеристику методів стеганографії файлів;
3. запропонувати приклади використання обраного методу кодування (стеганографії).

РОЗДІЛ 2
МЕТОДИ АУДІО СТЕГАНОГРАФІЇ, ЯК ВИРІШЕННЯ ПОСТАВЛЕНОЇ ПРОБЛЕМИ

2.1 Способи забезпечення авторського права з використанням стеганографічних методів

Основною галуззю застосування цифрової стеганографії є захист авторського права. З плином часу ця сфера розвивається все більше і більше, створюється все більше методик встановлення факту власності над інформаційним об’єктом у мультимедійній сфері.

Проте все ж визначається два основних напрямки вбудовування інформації, яка засвідчує факт належності даних власникові. До першого напрямку відносяться цифрові водяні знаки, до другого вшиття певного ідентифікаційного коду в файл.

До спільних властивостей обох методів відноситься факт того, що вшиття цієї інформації не має бути прихованим, та те, що обидва методи базуються на додані до файлу особливої інформації, яка повідомляє нам, хто є власником об’єкту.

Щодо відмінностей можна зазначити, що метод вбудовування коду в файл, водночас з забезпеченням інформування про наявність в об’єкту власника, також дає змогу залучити інтелектуальну власність до бази даних. Ця база даних дасть змогу не просто швидко ідентифікувати будь-яку копію об’єкту, а й дасть змогу ефективно відслідковувати шляхи копій, їхню долю та можливі правопорушення в їх бік. Якщо проводити зрозумілу аналогію, та такий ідентифікаційний код можна порівняти з індивідуальним номером кожної книги у бібліотеці. Навіть за відсутності книги у самій бібліотеці, завжди є можливість з’ясувати, де вона знаходиться, хто нею користується. Приблизно те саме можуть зробити власники об’єктів, котрі забезпечують захист авторського права саме цим методом.

Проте більш простим у досягненні та не проблематичним у підтверджені є методика використання ЦВЗ. Хоча й сутність не особливо відрізняється від

вбудовування ідентифікаційного номеру, проте через відсутність необхідності отримувати той самий код у певного уповноваженого органу, метод ЦВЗ є більш доступним.

Проте у нього є й недоліки, а саме можливість вилучення цифрового водяного знаку з об’єкту методом стиснення файлу.

Для захисту авторського права об’єкт може мати будь-яку мультимедійну форму, починаючи з текстових файлів та закінчуючи аудіо й відео файлами.

2.2 Методи стеганографії файлів

Методи, призначені для приховування даних класифікують також за принципами, які лежать в їх основі, таким чином визначають так звані форматні методи стеганографії та неформатні.

До форматних належать ті стеганографічні системи, які базуються на використанні особливостей форматів файлу. Фактично такий метод полягає у аналізі формату файлу з метою пошуку службових полів, зміна яких ніяк не відзначиться на стані стеганоконтейнеру. Перевагою такого методу є те, що, під час його використання, ми вносимо зміну в службові поля, що ніяк не відображається на самому файлі.

Неформатні методи не залежать від формату файлу, а використовує безпосередньо дані, завдяки яким ми отримаємо файл таким, який він представлений, тобто, у випадку графічних зображень, це будуть, наприклад, біти, а в випадку аудіо файлів це можуть бути фази чи коливання. [13]

Використання таких методів, на відміну від форматних методів, призводить до появи спотворень в нашому початковому файлі, проте все одно даний метод є більш стійким до будь-якого виду атак.

Розглянемо детальніше найбільш відомі алгоритми стеганографії та наведемо їх плюси і мінуси. До методів, які ми розглянемо відносяться:

- алгоритми з використанням особливостей формату файлу;
- LSB кодування;

- ехо кодування;
- фазове кодування.

2.2.1 Алгоритми з використанням особливостей формату файлу

До найпростіших алгоритмів приховування повідомлень відноситься використання особливостей формату файлів. Цей метод є простим у реалізації та не потребує особливого програмного забезпечення.

До прикладів застосування даного методу відноситься запис інформації у метадані та використання службових полів формату, які завжди присутні у файлах, проте в даний момент часу не використовуються. [14]

До переваг даного методу відносять:

- метод є простим у використанні;
- простота реалізації методу;
- можливість прихованої передачі значного об’єму даних.

Проте, як і будь-який інший метод, так званий “форматний” метод має й свої недоліки:

- можливість побудови повністю автоматичного алгоритму для виявлення факту приховування повідомлення;
- низька стійкість до пасивних атак. [15]

Одним з найвідоміших методів приховування даних за допомогою особливостей формату файлів є метод приховування в палітрі.

Цей метод базується на тому, що всі елементи палітри складаються з чотирьох байт, проте зазвичай лише перші три з них використовуються для кодування кольору. Останній же байт дорівнює нулю і не використовується. Що дає змогу приховати до 256 байтів повідомлення без внесення змін до розміру вихідного BMP-файлу.

2.2.2 LSB кодування

Метод LSB (Least Significant Bit, найменший значущий біт) кодування використовує надмірність файлів, якщо точніше, то він використовує молодші (останні) значущі біти, в яких практично немає корисної інформації) для розміщення в них повідомлення. Така заміна бітів майже не впливає на сам файл і не створює спотворень, які будуть помітними для людини.

До переваг даного методу можна віднести:

- великий обсяг даних, які можна передати;
- можливість використання з метою забезпечення авторського права.

Одним з недоліків методу LSB кодування є те, що при заміні бітів відбувається спотворення статичних характеристик цифрового потоку, що при використанні певних методів стеганографічного аналізу призводить до стрімкого виявлення факту приховування інформації. [16]

Для більшого розуміння наведемо приклад використання даного методу. В якості стеганоконтейнеру виступатиме зображення у форматі BMP. До особливостей файлів цього формату відноситься те, що умовно його можна розбити на чотири частини, а саме:

- заголовок файлу;
- заголовок зображення;
- палітру зображення;
- зображення.

Для реалізації методу заміни найменш значущого біта використовується тільки запис, який міститься у заголовку зображення.

Перші два байти такого заголовку є сигнатурою BM, далі записано розмір файлу в байтах. Наступні чотири байти є зарезервованими, вони містять нулі. І наступним записано відстань зміщення від початку файлу до байтів власне самого зображення. А пікселі кодуються трьома байтами RGB.

Суть методу полягає у заміні молодших бітів в байтах, які відповідають за кодування кольору. візьмемо за приклад наступний байт секретного повідомлення:

11001001,

а байти зображення будуть наступними:

11011001 01000110 00110100 10010110 ...

Для того, щоб закодувати повідомлення необхідно розділити його на чотири двох бітові частини наступним чином:

11 00 10 01

А далі здійснити заміну молодших бітів зображення:

11011011 01000100 00110110 10010101 ...

Така заміна не буде помітною для людського ока, а старі пристрої навіть не зможуть відобразити подібні редакції цифрового потоку. В даному прикладі я замінювала тільки два молодших біти, взагалі кількість потенційно замінюваних бітів є необмеженою, проте варто зважати увагу на те, що при захованні більшого об'єму інформації здійснюється більша кількість замін бітів, внаслідок чого створюється більше спотворень в оригінальному файлі. [17]

2.2.3 Ехо кодування

Даний метод реалізується за допомогою вбудовування в аудіо сигнал (тобто використовуваний стеганоконтейнер) даних способом додавання в нього ехо сигналу. Для кодування послідовності значень використовують нерівномірні проміжки між вже наявними в контейнері ехо сигналами. Якщо при накладені повідомлення дотримуватися ряду обмежень, то умова непомітності для людського ока буде збережена.

Ехо кодування відбувається за допомогою заміни значень трьох характерних для даного методу параметрів:

- початкової амплітуди;
- ступеню загасання;
- затримки.

Дані параметри змінюються при досягненні певного порогу між сигналом і ехо, і в утвореній точці людина вже не зможе їх розрізнити. Факт наявності даної

точки визначити складно, адже вона залежить не тільки від самого слухача, а й від якості вихідного файлу.

При ехо кодуванні зазвичай використовується затримка, яка приблизно дорівнює одній тисячній секунди, що є цілком нормальним для переважної кількості записів та слухачів. Для кодування нуля та одиниці використовуються два різних значення затримки і головною умовою для вибору цих значень є те, що вони мають бути на більшими за поріг чутливості слухача.

Окрім заміни значень часу затримки, встановлюються рівні початкової амплітуди і часу загасання, так щоб вони не перевищували поріг чутливості слухових систем людини.

Процес витягу прихованої інформації потребує виявлення інтервалу між ехо сигналами. Щоб це зробити необхідно провести певні дослідження:

- порівняти амплітуду автокореляційної функції в двох позиціях;
- дослідити косинус перетворення Фур'є натурального логарифму спектра потужності кодованого сигналу.

Дані обчислення дадуть змогу виявити інтервал між ехо сигналом та вихідним сигналом.

Проте метод використання ехо кодування має ряд недоліків:

- цей метод є досить складним для розуміння людини, яка не вміє робити певні математичні та фізичні обчислення;
- реалізація цього методу потребує певного обладнання й особливо обережного виконання процесу;
- при використанні даного способу висока ймовірність внесення у стеганоконтейнер спотворень, які будуть помітними;
- не завжди є можливість точно визначити, що було передано: нуль чи одиниця;
- даний метод складно використовувати у якості каналу передачі повідомлень через його низьку пропускну здатність.

Через значну кількість недоліків використання ехо кодування як методу стеганографії є дуже рідким та складним при реалізації. [18]

2.2.4 Фазове кодування

Метод фазового кодування базується на використанні особливостей сприйняття людського вуха, якщо точніше то на тому, що воно сприймає не значення самої фази, а відмінності між різними фазами. Для чіткого розуміння наведу визначення фази. Повна фаза коливання ─ це аргумент періодичної функції, який описує коливальний процес. [19]

При використанні цього методу сигнал розбивають на ділянки $S_0, S_1, \ldots, S_{n-1}$ таким чином, щоб значення фази першої ділянки передавало закодоване повідомлення, а значення фаз на інших ділянках було таким, щоб відрізнити фази між собою було як мінімум складно, а краще неможливо. [16]

Для того, щоб закодувати значення фаз, береться множина вже наявних фаз та вираховується набір рівномірно розподілених значень, які відповідають нулю та одиниці. Значення фази, яка кодується замінюється найближчим значенням, яке відповідатиме необхідному біту. Для того, щоб закодувати один біт повідомлення використовується певна послідовність змін фаз, яка, звичайно, відрізняється для нуля і одиниці. Якщо зобразити процес фазового кодування, то виглядатиме він наступним чином (Рис.2.1-2.9):

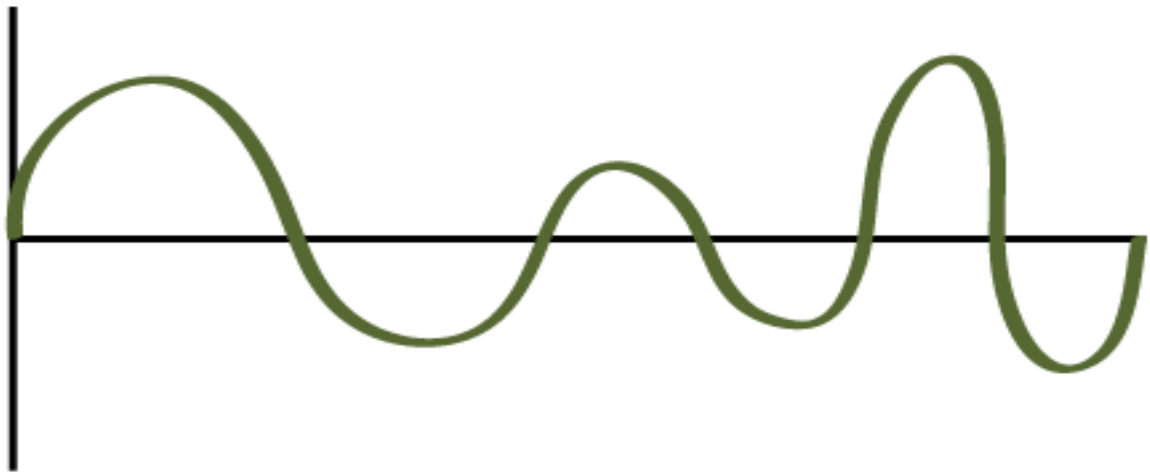

Рисунок 2.1 – Початковий сигнал

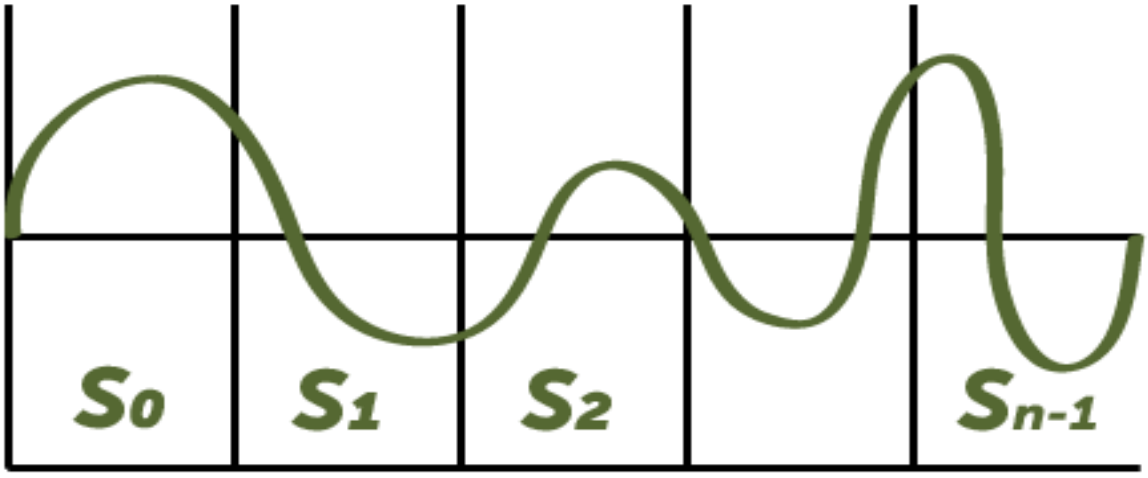

Рисунок 2.2 – Початковий сигнал розбивається на n сегментів

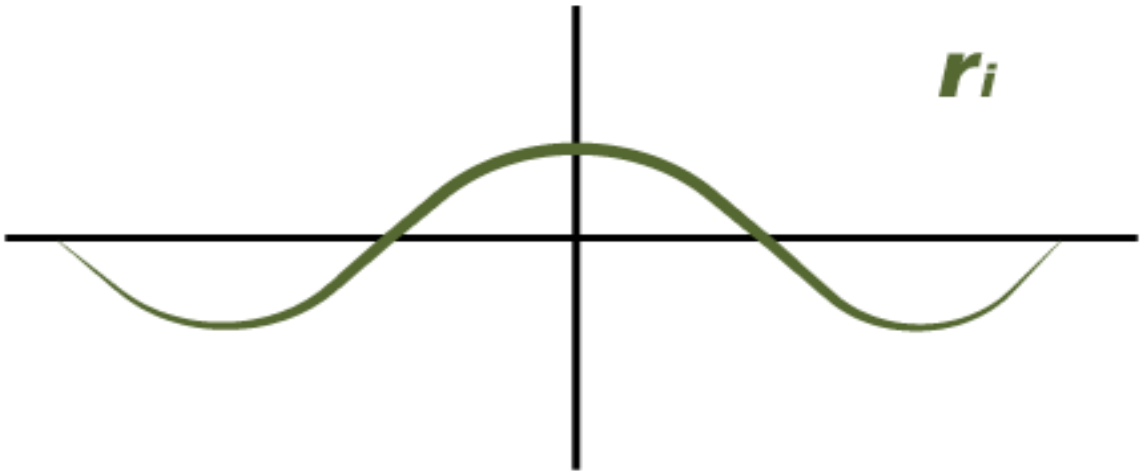

Рисунок 2.3 – Виділення амплітуди кожного сегменту

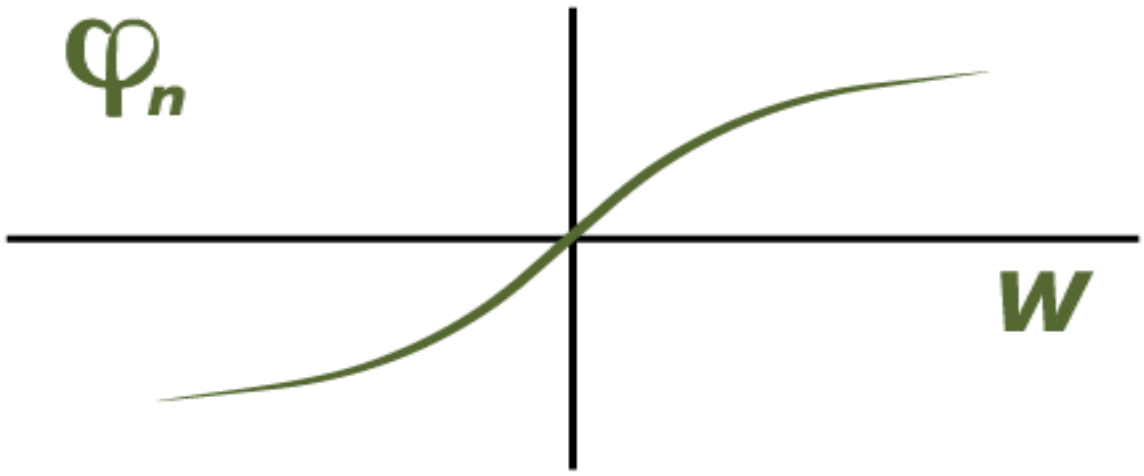

Рисунок 2.4 – Виділення фази кожного сегменту

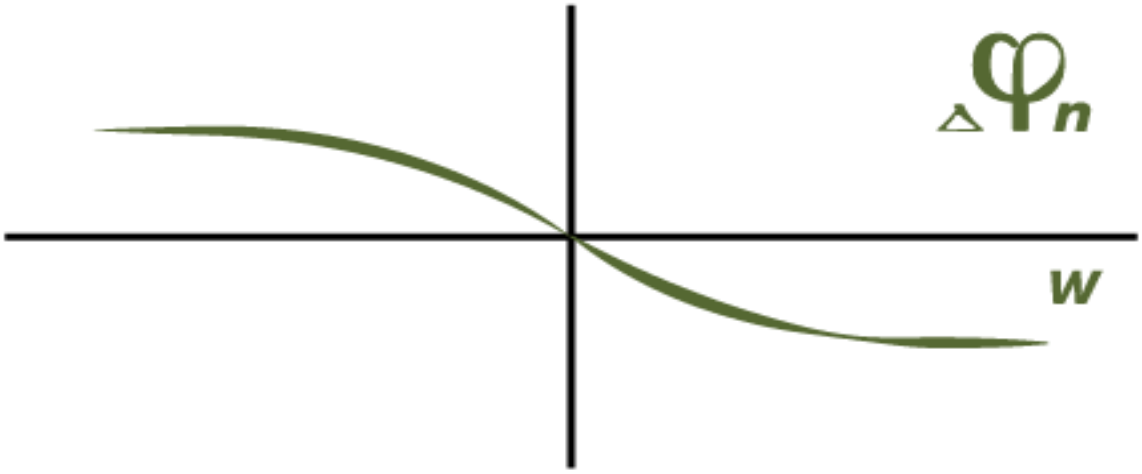

Рисунок 2.5 – Різниця фаз між сусідніми елементами

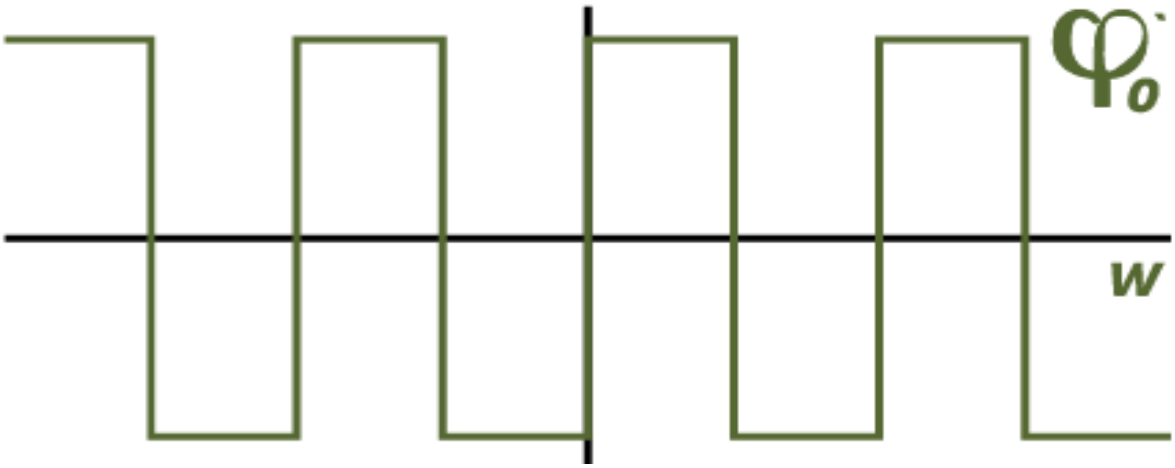

Рисунок 2.6 – Створення нової фази для сегменту S_0

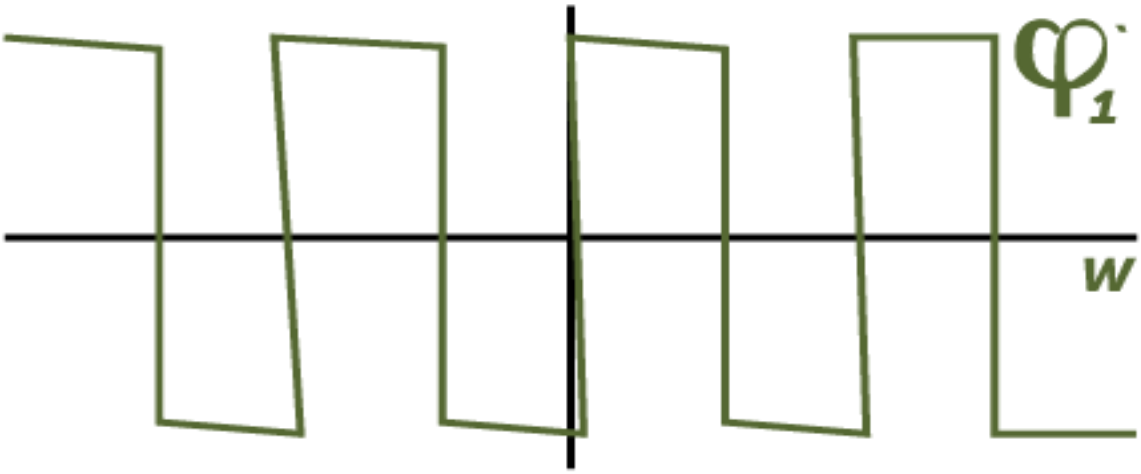

Рисунок 2.7 – Створення нової фази для інших сегментів

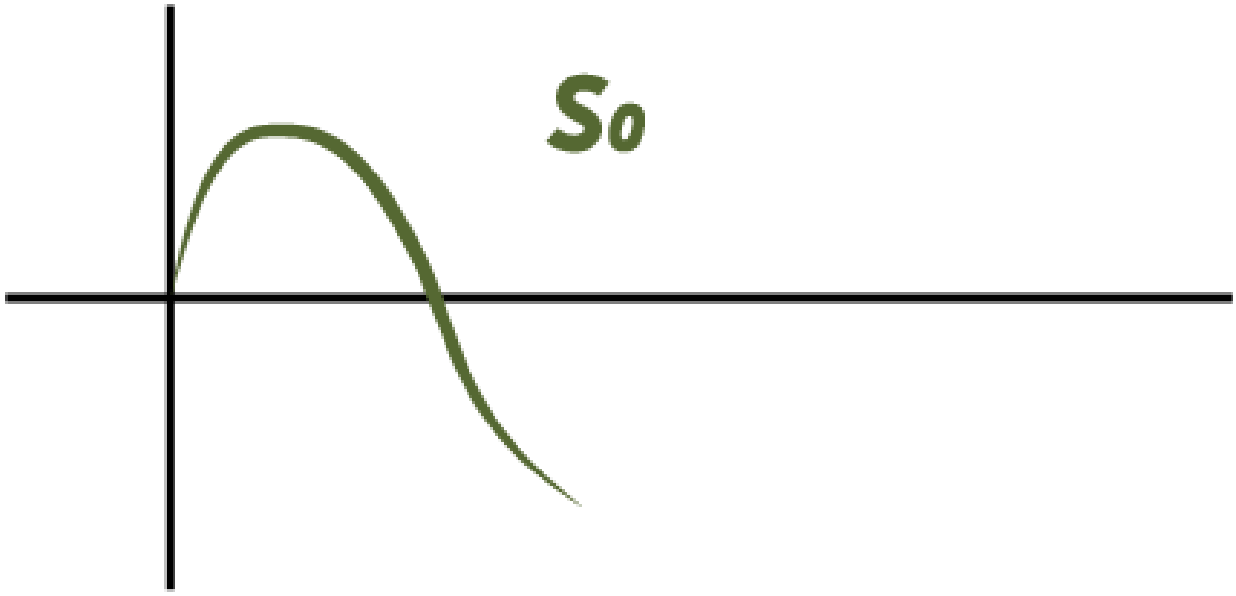

Рисунок 2.8 – Об’єднання нової фази та початкової амплітуди, щоб отримати новий сегмент S_0

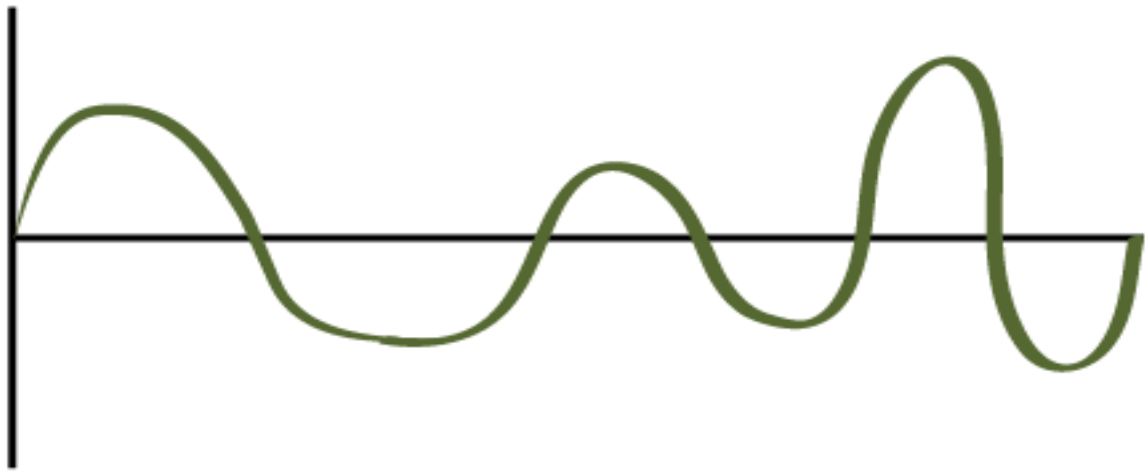

Рисунок 2.9 – Сигнал з вбудованим ЦВЗ, отриманий внаслідок об’єднання отриманих сегментів

Для того, щоб вилучити приховане повідомлення з файлу використовується спеціальна функція виявлення:

$$q = \Sigma\, r_i\,(v_i - \varphi_i)^2 - r_i\,(u_i - \varphi_i)^2 \qquad (2.1)$$

Позначення, використанні у даній формулі мають наступні значення:

- $u = \{\alpha_0, \beta_1, \alpha_2, \beta_3\}$— отриманий сигнал;
- r_i — амплітуда і-го отриманого сигналу;
- φ_i— фаза і-го отриманого сигналу.

- $u = \{\alpha_0, \beta_1, \alpha_2, \beta_3\}$ — очікувана/передбачувана послідовність фаз у разі кодування одиниці;
- $v = \{\alpha_0, \beta_1, \alpha_2, \beta_3\}$ — очікувана/передбачувана послідовність фаз у разі кодування нуля;
- α_i, β_i — найближчі значення фаз, які відповідають нулю та одиниці.

Після проведення підрахунків за допомогою наведеної формули отримуємо значення q. Якщо дане значення більше нуля, то біт переданого повідомлення дорівнює одиниці, якщо він менший за нуль, то біт відповідно дорівнює нулю. [20]

До недоліків методу фазового кодування належить:

- низька швидкість передачі даних, адже таємне повідомлення можна закодувати виключно у першому сегменті заданого сигналу;
- для вирішення першого недоліку дуже часто збільшують довжину першого сегменту сигналу, що призводить до виникнення другого недоліку, а саме високій ймовірності виявлення повідомлення у разі його великих розмірів.

Виходячи з недоліків запропонованого методу, можна зробити висновок, що він ідеально підходить для приховування невеликих фрагментів даних, таких як цифровий водяний знак. [21]

2.3 Порівняння методів аудіо стеганографії

Серед розглянутих методів, а саме: алгоритмів з використанням особливостей формату файлу, LSB та ехо кодування й фазового кодування; було проведено аналіз з метою виявлення найбільш вигідного для реалізації.

Метод використання форматів файлу, хоч і є простим у реалізації та використанні, має дуже низьку стійкість до пасивних атак та має дуже високу ймовірність виявлення прихованих даних. Що робить його ненадійним у разі використання даного алгоритму з метою забезпечення авторського права.

Метод LSB дає нам змогу використовувати його для підтвердження факту наявності авторського права, а також надає змогу передавати великі об’єми даних.

Проте він має досить високу ймовірність спотворення початкового сигналу, що робить його для нас не досить надійним.

Метод ехо кодування має низку недоліків, таких як:

- складність у реалізації;
- висока ймовірність внесення у стеганоконтейнер спотворень, які будуть помітними;
- складності при відтворенні переданого повідомлення після отримання закодованого сигналу;

Що робить його ненадійним у використанні з метою забезпечення авторського права аудіо об’єктів.

Останнім розглянутим методом є метод фазового кодування, серед недоліків якого було виявлено те, що він не придатний для передачі великих об’ємів даних. Проте через те, що цифровий водяний знак має невеликі розміри, цей метод найбільш ефективним для вирішення проблеми, поставленої у цій роботі.

Висновки за розділом 2

У другому розділі було розглянуто основні методи забезпечення авторського права з використанням стеганографічних методів.

Визначається два основних напрямки вбудовування інформації, яка засвідчує факт належності даних власникові. До першого напрямку відносяться цифрові водяні знаки, до другого вшиття певного ідентифікаційного коду в файл.

Якщо надання файлу власного індивідуального коду розуміє під собою отримання об’єктом певного ідентифікатору, то вбудовування водяних знаків має дуже широку кількість алгоритмів, які виконають поставлену задачу. Ці методи та алгоритми можна поділити на форматні та неформатні. Перевагою форматного методу є те, що, під час його використання, зміна вноситься в службові поля, що ніяк не відображається на самому файлі. А використання неформатних методів, призводить до появи спотворень в нашому початковому файлі, проте все одно даний метод є більш стійким до будь-якого виду атак.

Згідно до наведеної вище інформації можна стверджувати, що до найпопулярніших методів відносяться:

- алгоритми з використанням формату файлу;
- LSB кодування;
- ехо кодування;
- фазове кодування.

У даному розділі було проведено порівняння зазначених методів та виявлено переваги і недоліки кожного з них. Проведений аналіз дав змогу обрати метод, який буде найбільш вдачним та найбільш простим у реалізації одночасно.

Метод найменшого значущого біта використовує надмірність файлів, якщо точніше, то він використовує молодші (останні) значущі біти, в яких практично немає корисної інформації) для розміщення в них повідомлення. Переважно цей метод використовується для розміщення цифрових водяних знаків у графічних об’єктах.

Метод ехо кодування реалізується за допомогою вбудовування в аудіо сигнал цифрового водяного знаку способом додавання в нього ехо сигналу. Для кодування послідовності значень використовують нерівномірні проміжки між вже наявними в контейнері ехо сигналами. Проте через високу ймовірність внесення у стеганоконтейнер спотворень, які будуть помітним, цей метод майже не використовується.

Метод фазового кодування полягає у заміні вихідного звукового елемента на відносну фазу, яка і є секретним повідомленням. До недоліків цього методу відноситься той факт, що він не придатний для передачі великих об’ємів даних. Це робить його більш актуальним для використання у якості алгоритму для вбудовування цифрового водяного знаку. Оскільки ймовірність спотворення секретного повідомлення в даному методі є значно меншою, ніж в інших досліджених, він є найбільш ефективним для побудови власного програмного забезпечення спрямованого на захист авторського права у аудіо об’єктах.

Проведений аналіз та порівняння дають можливість визначити наступні кроки проведення дослідження та реалізації програмного забезпечення:

1. визначити мову програмування, за допомогою якої можна буде написати програмне забезпечення з найменшою можливістю виникнення неполадків;

2. визначити загальні характеристики програмного забезпечення, яке реалізується;

3. навести приклад результату виконання прописаного алгоритму.

РОЗДІЛ 3
ЗАХИСТ АВТОРСЬКОГО ПРАВА В АУДІО ОБ'ЄКТАХ

3.1 Порівняльна характеристика різних мов програмування

Для написання програмного забезпечення, яке, за допомогою обраного стеганографічного алгоритму, буде приховувати у обраному аудіо файлі цифровий водяний знак, спочатку необхідно вибрати мову програмування, для реалізації скрипта.

Серед усіх існуючих мов програмування, базуючись на вже отриманих раніше знаннях, вибір постає між мовами Java, C# та Python. Для подальшого вибору, проведемо аналіз та порівняльну характеристику обраних мов. Трьома основними параметрами для порівняння будуть:

- простота написання;
- можливості та обмеження при написанні скриптів;
- кількість бібліотек для використання.

За першим параметром мова програмування Python явно перемагає, через простоту свого синтаксису. Синтаксис даної мови легко читається, немає ніяких синтаксичних дужок, складних конструкцій та модифікаторів, на відміну від мов програмування C# та Java. Синтаксис C# потребує від розробника чіткого дотримання певних правил при створенні методів або при спадкуванні класів. У той час як код написаний на Python є простим для читання та у разі виявлення помилок у процесі розробки не викликає ніяких складностей через великі кількості конструкцій. Щодо складності вивчення Java у порівнянні з Python, то вона також є набагато складнішою мовою програмування. Що призводить до того, що вивчити цю мову, не маючи ніякого технічного бекграунду або досвіду якоїсь роботи з мовами програмування, буде непросто.

Щодо другого параметру для порівняння можна сказати, що мова C# є обмеженою, адже її написання можна здійснювати тільки у IDE, у той час як Python

є сумісним з різними платформами. Ця інтегрованість та кроссплатформенність позбавляють розробників необхідності вибору середовища для написання скриптів. Говорячи про Java, можна взяти до уваги, що ця мова програмування дає можливість розробляти кросплатформенні додатки, але і Python є сумісним з багатьма операційними системами.

Якщо порівнювати кількість бібліотек, котрі кожна з мов програмування пропонує для використання, то навіть велика кількість стандартних бібліотек C# програє у порівнянні з кількістю бібліотек з відкритим кодом, запропонованих Python, що спрощує використання даної мови програмування. [21]

Варто зазначити, що на даний момент Python постійно розвивається, як мова програмування, що призводить до росту кількості IT спеціалістів, які користуються саме цією мовою програмування. На даний момент часу Python масово використовується для розвитку фінансових технологій та машинного навчання. І у якості прикладу можна навести такі організації, котрі використовують Python для створення досить великих проектів, як Google, Yandex та інші.

Складно сказати, що саме ця мова програмування є кращою за інші запропоновані, адже з точки зору розвитку інформаційних технологій, можна зазначити, що кожна мова програмування має свої особливості, переваги та недоліки, які можна використовувати для розвитку тієї чи іншої сфери.

Проте хотілося б зазначити, що саме Python зараз переважно використовується для веб-розробки, автоматизації різних задач та для написання ігор. Варто зауважити, що через свою простоту у написанні, розробка з використанням мови програмування Python може зайняти приблизно у 3-4 рази менше часу ніж розробка додатків з використанням, наприклад, Java. Що і спричиняє велику популярність цієї мови програмування у порівнянні з іншим, особливо для новачків у сфері написання скриптів. [22]

Якщо підсумувати, то до переваг Python відносяться наступні:

- кросплатформеність, що під собою розуміє наявність інтерпретаторів для багатьох платформ, що дає змогу для його використання на будь-якій операційній системі;

- наявність великої кількості сервісі, середовищ розробки та фреймворків;
- можливість використання великої кількості бібліотек, у тому числі можливість підключення бібліотек написаних мовами C, що дозволяє підвищити ефективність проектів;
- велика кількість літератури, в якій описані процеси написання скриптів чи розробки веб додатків, що значно спрощує процес навчання чи взагалі роботу з даною мовою програмування.

Виходячи з перерахованого вище, для написання програмного забезпечення, націленого на приховування цифрового водяного знаку, мова програмування Python буде більш оптимальною через свою кроссплатформенність, простоту та велику кількість запропонованих для використання бібліотек.

3.2 Вимоги до розробленого програмного забезпечення

Попередньо проведені дослідження дозволяють повністю сформувати технічне завдання на виготовлення програмного забезпечення, яке буде вирішувати проблему захисту авторського права у аудіо об’єктах.

Поставимо декілька основних питань до програмного забезпечення, яке необхідно реалізувати, а саме:

- які початкові дані ми маємо;
- що ми маємо отримати по завершенні роботи програми;
- що ми маємо для успішного написання та виконання програми;
- що необхідно для виконання програми;
- яким є алгоритм роботи програмного забезпечення, яке необхідно написати;
- які вимоги є до програмного забезпечення, яке розробляється.

До особливостей початкового стеганоконтейнеру з назвою beat.wav відноситься те, що це сигнал, тривалість якого складає вісім секунд, частота дискретизації дорівнює 44100 Гц, має один канал, розширенням файлу з сигналом є WAV та за розміром файл складає 1,43 Мб.

Як уточнення варто зазначити, що частотою дискретизації є частота взяття відліків неперервного за часом сигналу при його дискретизації.

До особливостей стеганоповідомлення з назвою msg.txt, яке необхідно розмістити у встановлений стеганоконтейнер відноситься його вміст: “Kateryna Burbela is now an owner”, формат файлу — TXT і розмір самого повідомлення — 264 бітів.

По завершенні виконання роботи програми отримано заповнений стеганоконтейнер, який залишається незмінним відносно людських органів сприйняття, а саме з тим самим розширенням файлу з сигналом — WAV та розміром файлу — 1,43 Мб.

Для виконання поставленої задачі використовується операційна система Linux Kali з встановленим на неї Python 3 для написання скриптів, перший з яких буде вбудовувати у заданий сигнал обране повідомлення, а другий буде вилучати з заповненого стеганоконтейнеру розміщене у ньому стеганоповідомлення.

Для перевірки результату необхідно застосовувати програмне забезпечення, яке допоможе побудувати спектральну і часову діаграми оригінального сигналу та сигналу з вбудованим цифровим водяним знаком. Провівши дослідження з метою з’ясування, яке програмне забезпечення буде задовольняти дану потребу було вирішено використовувати програму Izotope Rx.

Алгоритмом роботи, тобто здійснення фазового кодування виконується за наступними етапами:

- спочатку необхідно розділити звуковий сигнал на серію Nкоротких сегментів;
- наступним кроком буде застосування k-точкового дискретного перетворення Фур’є, у якому $k = I/N$, де I — довжина дискретних значень сигналу;
- створюються масиви фаз і амплітуд;
- наступним кроком необхідно запам’ятати різницю фаз між усіма сусідніми сегментами;
- визначаємо значення, які будуть відображати двійкову послідовність, а саме $\pi/2$та $-\pi/2$будуть відображати один та нуль відповідно;

- враховуючи встановлену різницю фаз необхідно відтворити масив фаз;

Процес відновлення звукового сигналу здійснюється за допомогою застосування операції зворотного дискретного перетворення Фур'є [24].

Під час реалізації програмного забезпечення, яке буде працювати за вказаним алгоритмом необхідно вжити певних заходів, спрямованих на зниження рівня спотворень, а саме:

- крайні сегменти мають залишатися незмінними;
- під час формування нових фаз додавання стеганоповідомлення починається з високочастотних складових.

Отже головними вимогами до програмного забезпечення є:

- незмінність стеганоконтейнеру для органів чуття людини;
- незмінність розміру та основних властивостей стеганоконтейнеру;
- створення скрипту, спрямованого як на вбудовування цифрового водяного знаку, так і на його вилучення.

3.3 Результат виконання прописаного алгоритму

До вхідних даних, які ми маємо відноситься стеганоконтейнер з назвою beat.wav до його властивостей відноситься те, що це сигнал, тривалість якого складає вісім секунд, частота дискретизації дорівнює 44100 Гц, він має один канал, розширенням файлу з сигналом є WAV та за розміром файл складає 1,43 Мб.

Використовуючи програмне забезпечення Izotope Rx, побудуємо спектральну діаграму початкового сигналу:

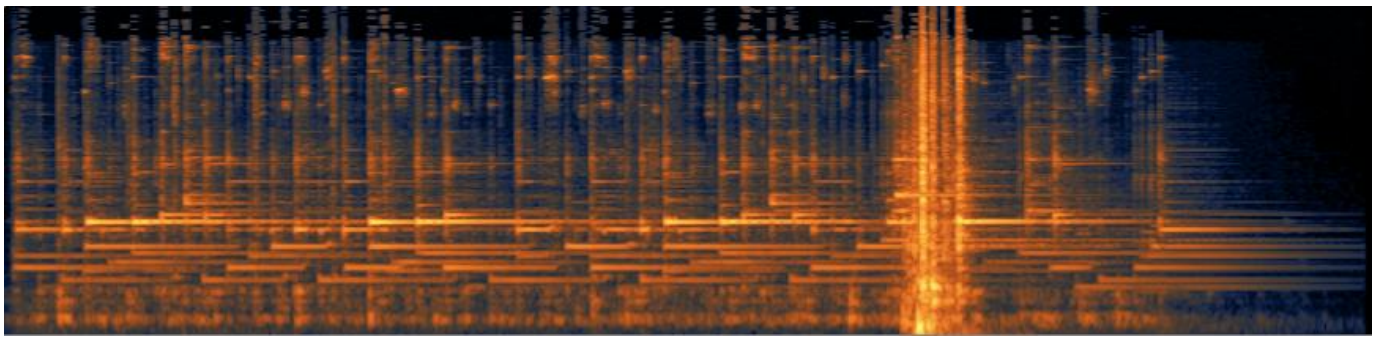

Рисунок 3.1 – Спектральна діаграма для порожнього стеганоконтейнеру.

Та будуємо часову діаграму оригінального сигналу:

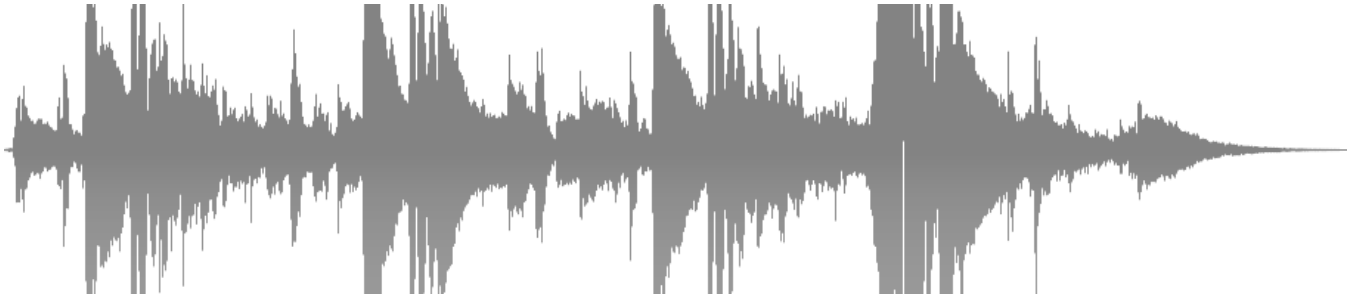

Рисунок 3.2 – Часова діаграма для порожнього стеганоконтейнеру

Згідно до поставленої задачі наступним кроком буде приховування обраного о стеганоповідомлення, розміщеного у файлі формату TXT з назвою msg.txt, з розміром 264 бітів, у нашому стеганоконтейнері, а саме:

“Kateryna Burbela is now an owner”

Для виконання скрипту необхідно відкрити термінал Linux Kali та перейти до папки у якій розміщено файл зі скриптом, файл з стеганоконтейнером та файл з стеганоповідомленням. Для цього виконуємо наступні команди і отримаємо відповідний результат:

cd Desktop/py-stego-phase-master

python stego_phase.py -i “wav/beat.wav” -m “msg.txt” -o “wav/stego.wav”

```
katerina@kkali:~/Desktop/py-stego-phase-master$ python stego_phase.py -i "wav/beat.wav" -m "msg/msg.txt" -o "wav/stego.wav"
reading wave container ...
preparing container ...
performing fft transform ...
msg integration ...
saving stego container ...
Done.
Remember segment width to recover message: 1024
katerina@kkali:~/Desktop/py-stego-phase-master$
```

Рисунок 3.3 – Виконання скрипту, який розміщує цифровий водяний знак у стеганоконтейнері

Розглянемо, як змінилися спектральна і часова діаграми заданого стеганоконтейнеру після вбудовування в нього стеганоповідомлення.

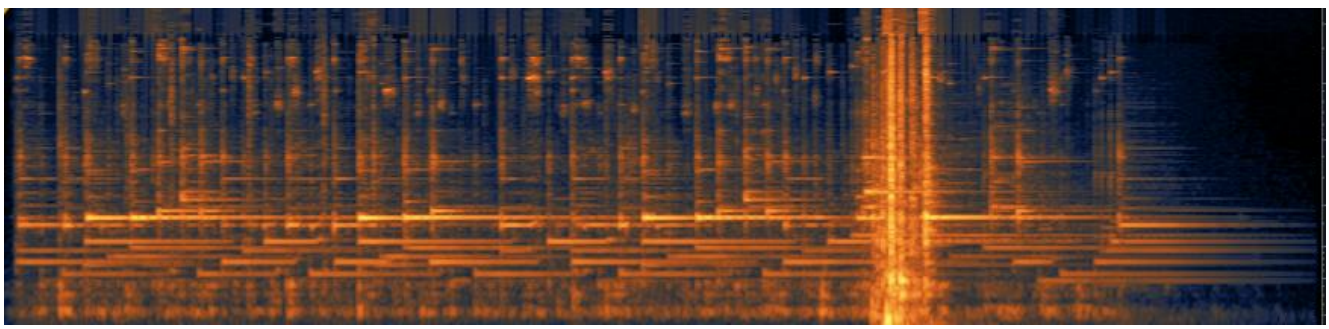

Рисунок 3.4 – Спектральна діаграма для заповненого стеганоконтейнеру

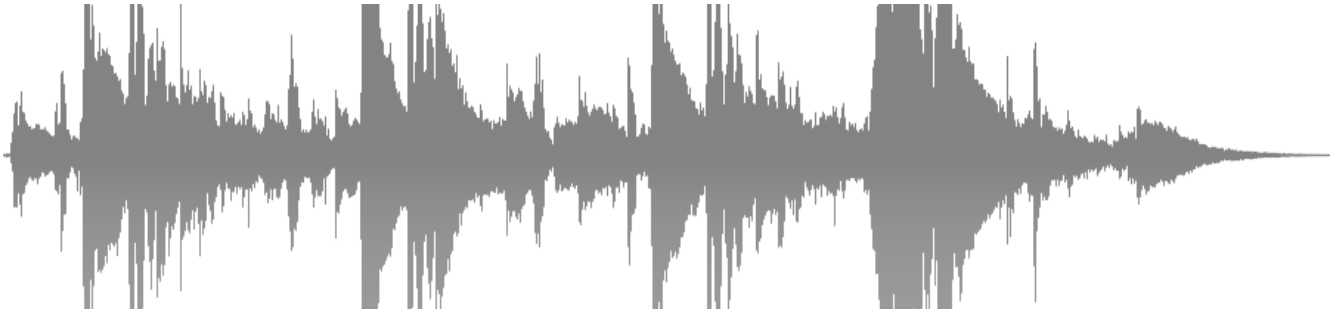

Рисунок 3.5 – Часова діаграма для заповненого стеганоконтейнеру

Модифікація фази була здійснена для вбудовування повідомлення довжиною 264 біт за незмінної довжини сегменту, яка дорівнює 1024 біти. У разі збільшення довжини повідомлення, який хочуть розмістити на сегменті такої самої довжини, при прослуховуванні аудіо файлу буде чутно легке потріскування, характерне для недопустимої зміни фази.

Наведемо приклад такого аудіо об’єкту використавши цифрового водяного знаку msg2.txt розміром 3872 біта. Одразу наведемо порівняльний приклад часової та спектральної діаграм:

Рисунок 3.6 – Спектральна діаграма порожнього та наповнених стеганоконтейнерів

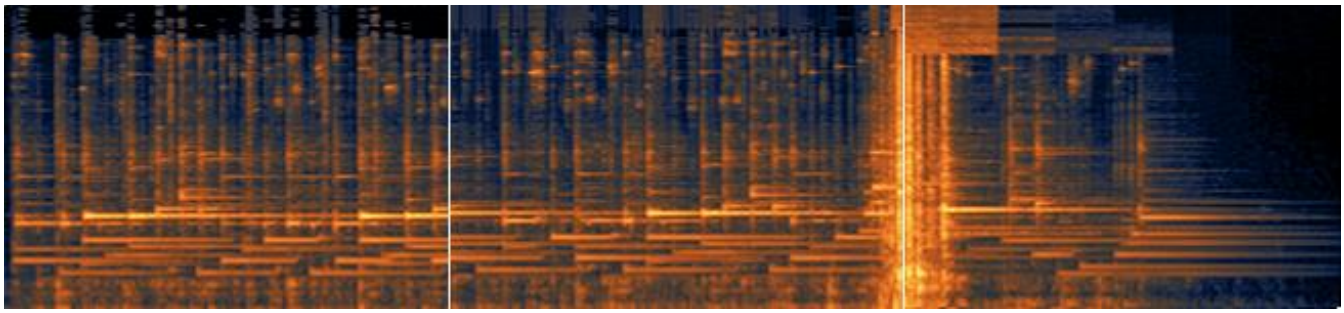

Рисунок 3.7 – Часова діаграма порожнього та наповнених стеганоконтейнерів

З лівого боку наведено часову та спектральну діаграми порожнього стеганоконтейнеру, а з правого — наповненого.

По центру наведено часову і спектральну діаграми наповненого стеганоконтейнеру з цифровим водяним знаком розміром, який задовольняє вимоги алгоритму. А з лівого боку можна побачити діаграми наповненого стеганоконтейнеру з міткою занадто великого розміру накладену поверх діаграми порожнього.

Виходячи з наведених графіків можна зазначити, що аудіо контейнер з розміщеним у ньому цифровим водяним знаком, відповідним до норм даного методу, є не відмінним від оригінального контейнеру.

Для виконання скрипту спрямованого на вилучення повідомлення або цифрового водяного знаку зі стеганоконтейнеру необхідно перейти у ту саму папку, в якій розміщено файл зі скриптом, файл зі стеганоконтейнером та файл зі стеганоповідомленням, для цього виконуємо наступні команди:

cd Desktop/py-stego-phase-master

python stego_phase.py -i "wav/stego.wav" -m "msg/msg_recovered.txt" -- karg 1024

Після виконання скрипту з зазначеними параметрами побачимо наступний результат:

```
katerina@kkali:~/Desktop/py-stego-phase-master$ python stego_phase.py -i "wav/stego.wav" -m "ms
1024
reading wave container ...
preparing container ...
performing fft transform ...
recovering message ...

Done.
```

Рисунок 3.8 – Виконання скрипту, який вилучає цифровий водяний знак із стеганоконтейнеру

Наведений вище приклад виконання скрипта з використанням методу фазового кодування дає змогу діти висновку, що використання цього або подібних програмних продуктів є ефективним.

Висновки за розділом 3

У третьому розділі було розглянуто застосування методу фазового кодування з метою захисту авторського право у аудіо файлах.

Було проведено порівняльну характеристику мов програмування C#, Java та Python. Трьома основними параметрами для порівняння цих мов програмування обрано:

- простоту написання;
- можливості та обмеження при написанні скриптів;
- кількість бібліотек для використання;

Внаслідок проведеного аналізу з'ясовано, що для написання програмного забезпечення, націленого на приховування цифрового водяного знаку, мова програмування Python буде більш оптимальною через свою кроссплатформенність, простоту та велику кількість запропонованих для використання бібліотек.

Також у третьому розділі було визначень загальні характеристики реалізованого програмного забезпечення та вхідних даних. Було визначено особливості порожнього стеганоконтейнеру, а саме те що це аудіо сигнал, тривалість якого складає вісім секунд, частота дискретизації дорівнює 44100 Гц, було визначено розширення файлу (WAV) та його розмір (1,43 Мб).

Також у цьому розділі вказано особливості стеганоповідомлення, яке було розміщено у встановлений стеганоконтейнер. До цих особливостей належить вміст стеганоповідомлення: "Kateryna Burbela is now an owner", формат файлу — TXT і розмір самого повідомлення — 264 бітів.

Також було зазначено головні вимоги до створеного програмного забезпечення, а саме:

- невідчутність змін у стеганоконтейнері для органів чуття людини;
- однаковий розмір та основні властивості порожнього та наповненого стеганоконтейнерів;

У даному розділі наведено приклад виконання створеного скрипту, який розміщує цифровий водяний знак в обраному аудіо файлі або стеганоконтейнері.

По завершенні виконання написаної програми було отримано заповнений стеганоконтейнер, з незмінними даними по відношенню до людських органів сприйняття, з тим самим розширенням файлу — WAV та незмінним розміром файлу — 1,43 Мб.

І як висновок можна зазначити, що застосування даного скрипта є ефективним і перспективним для захисту авторського права в аудіо об’єктах.

ВИСНОВКИ

У даній дипломній роботі було досліджено методи захисту авторського права з використанням стеганографічних алгоритмів, спрямованих на вбудовування цифрового водяного знаку в аудіо об’єкти.

На початку проведення дослідження було наведено основні терміни та визначення та було з’ясовано, що переважна кількість визначень, які стосуються авторського права є зазначеними у Законі Україні “Про авторське право та суміжні права”. А до документів, які регулюють діяльність у сфері стеганографічного захисту інформації, можна віднести Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. Також було зазначено, що сфера стеганографічного захисту інформації потребує досконалого доопрацювання у плані нормативно правової бази.

Згідно до наведених вище нормативно-правових джерел було визначено, що авторське право — це особисті немайнові права і майнові права авторів та їх правонаступників, пов’язані із створенням та використанням творів науки, літератури і мистецтва, а стеганографія — це спосіб приховування секретного повідомлення всередині (або навіть поверх) об’єкту, що не є секретним. Наприклад, у наші дні багато прикладів стеганографії передбачають вбудовування секретного фрагмента тексту всередину малюнка. Або приховування секретного повідомлення чи сценарію всередині документа Word або Excel.

Також було зазначено мету захисту авторського права, яка полягає у захисті інформаційної власності від несанкціонованого копіювання, розповсюдження та/або редагування. Метою ж стеганографії було визначено приховування секретних об’єктів. Це як одна з форм прихованого спілкування і вона може передбачати використання будь-якого засобу для приховування повідомлень. Було зазначено, що стеганографія не є різновидом криптографії, оскільки вона не передбачає шифрування даних або використання ключа.

У ході дослідження було наведено велику кількість історичних аспектів використання методів стеганографії, таких як невидимі чорнила. Проте в наші дні ця наука все більше набуває так званого діджиталізованого поняття, впроваджуючи нові технології захисту, які вже відносять до поняття цифрової стеганографії. [24]

У цифровій сфері стеганографія передбачає приховування даних або повідомлень у цифрових файлах та інших цифрових структурах. Методи забезпечення авторського права за використання методів цифрової стеганографії визначають два основних напрямки вбудовування інформації, яка засвідчує факт належності даних власникові. До першого напрямку відносяться цифрові водяні знаки, до другого вшиття певного ідентифікаційного коду в файл.

Надання файлу власного індивідуального коду розуміє під собою отримання об’єктом певного ідентифікатору, а вбудовування водяних знаків має більшу кількість алгоритмів, які можуть помістити цифровий водяний знак в об’єкт. Ці методи та алгоритми можна поділити на форматні та неформатні, перші з яких використовують під час вбудовування даних у об’єкт особливості формату файлів, а другі відповідно не використовують. Перевагою форматного методу є те, що, під час його використання, зміна вноситься в службові поля, що ніяк не відображається на самому файлі. А використання неформатних методів, призводить до появи спотворень в нашому початковому файлі, проте все одно даний метод є більш стійким до будь-якого виду атак.

Переважно у цій роботі було вивчено особливості та проведено аналіз і порівняння наступних методів цифрової стеганографії:

- алгоритми з використанням формату файлу;
- LSB кодування;
- ехо кодування;
- фазове кодування.

Для вирішення завдання даної дипломної більш детального дослідження потребували методи аудіо стеганографії. І під час проведених досліджень було з’ясовано, що ефективна аудіо стеганографічна схема повинна мати такі

характеристики, як не чутність спотворень (або перцептивна прозорість) та надійність.

Серед вивчених методів найбільш актуальним став метод фазового кодування, який полягає у заміні вихідного звукового елемента на відносну фазу, яка і є секретним повідомленням. До недоліків цього методу відноситься той факт, що він не придатний для передачі великих об'ємів даних через те, що секретне повідомлення кодується лише в першому сегменті сигналу і для вилучення секретного повідомлення із звукового файлу, одержувач повинен знати довжину сегменту в якому ці дані закодовані. Це робить даний метод більш актуальним для використання у якості алгоритму для вбудовування цифрового водяного знаку. Оскільки ймовірність спотворення секретного повідомлення в даному методі є значно меншою, ніж в інших досліджених, він є найбільш ефект. [26]

Наступним кроком було вирішення практичної частини завдання даної роботи, а саме розробки програмного забезпечення, яке буде використовувати оптимальний алгоритм впровадження цифрового водяного знаку для захисту аудіо об'єктів від несанкціонованого видалення чи копіювання, є актуальними.

Для досягнення поставленої мети було вирішено наступні завдання наступним чином відповідно:

- досліджено різні мови програмування, які можна було б використати для написання скрипту, який би розміщував цифровий водяний знак в аудіо об'єкт;
- було наведено та досліджено алгоритм фазового кодування, та адаптовано його для написання програмного забезпечення;
- і як наслідок було розроблено власний програмний продукт спрямований на вирішення проблеми вбудовування цифрового водяного знаку з метою захисту авторських прав в аудіо об'єктах.

Задля перевірки роботи створеного скрипту було проведено його дослідження на аудіо файлі, було обрано невеликий стеганоконтейнер у вигляді аудіо запису формату WAV та водяний знак у форматі TXT. Також за допомогою створеного скрипта було досліджено якість відтворення розміщеного у стеганоконтейнері секретного повідомлення.

В рамках опису розробленого скрипта було наведено схему його роботи та інструкції з використання застосунку. До результатів дослідження було додано графічні ілюстрації з графіками, які дали змогу провести порівняльний аналіз файлу до внесення модифікацій та після.

З огляду на все вищесказане можна дійти висновку, що в результаті проведених досліджень та розробок було досягнуто поставлену мету.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України “Про авторське право та суміжні права” від 23.12.1993 № 3792-XII

2. Рекомендації щодо вдосконалення механізму регулювання цифрового використання об’єктів авторського права і суміжних прав через мережу Інтернет, від 20 грудня 1996 року

3. Іващенко Віктор Анатолійович // Технічні способи захисту авторських прав у всесвітній мережі Інтернет на етапі до порушення [Електронний ресурс]. — Режим доступу до документа https://cutt.ly/Nnd9F5v

4. Школа авторів БукРі // Що таке ISBN? [Електронний ресурс]. — Режим доступу до документа http://bookri.com.ua/bookri-school/what_is_isbn.html

5. Редакція ПБО // Електронна звітність — основні поняття та перші кроки [Електронний ресурс]. — Режим доступу до документа https://i.factor.ua/ukr/journals/nibu/2013/september/issue-70/article-63890.html

6. К 338 Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних : підручник. / Г. Ф. Конахович, Д. О. Прогонов, О. Ю. Пузиренко. — К. : «Центр учбової літератури», 2018. — 558 с., іл.

7. Закон України Про захист інформації в інформаційно-телекомунікаційних системах (Відомості Верховної Ради України (ВВР), 1994, № 31, ст.286)

8. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-Пресс, 2002. – 272 с.

9. Зимцов Андрей Методы цифровой стеганографии для защиты авторских прав // ISBN: 9783659105630 Год издания: 2012 Язык: Русский 148стр.

10. Стеганография [Електронний ресурс]. — Режим доступу до документа: https://cryptowiki.net/index.php?title=Стеганография

11. Артёхин Б. В. Стеганография // Журнал «Защита информации. Конфидент». — 1996. — № 4. — С. 47–50.

12. D. Kahn, The Codebreakers: The Story of Secret Writing. Macmillan Publishing Company, New York, USA, 1996. — 1200 p.

13. Материал из Национальной библиотеки им. Н. Э. Баумана // Методы сокрытия информации в графических изображениях [Електронний ресурс]. — Режим доступу до документа https://cutt.ly/End9X5J

14. Статическая стеганография [Електронний ресурс]. — Режим доступу до документа http://inmad.vntu.edu.ua/portal/static/016825C2-B242-4775-BE41-9A5E5FA4A24F.pdf

15. Хорошко В. О., Азаров О. Д., Шелест М. Є., Яремчук Ю. Є. Основи комп'ютерної стеганографії : Навч. посіб. для студентів і аспірантів. — Вінниця : ВДТУ, 2003. — 143 с.

16. Стеганография и стегоанализ в аудіо файлах [Електронний ресурс]. — Режим доступу до документа http://elib.sfu-kras.ru/bitstream/handle/2311/29251/vkr_strelnikov_final.pdf?sequence

17. LSB стеганография [Електронний ресурс]. — Режим доступу до документа https://habr.com/ru/post/112976/

18. Молодежный научно-технический вестник # 01, январь 2013 УДК: 003.26.004.056.57 авторы: Гончаров Н. О., Заикин М. А

19. Внедрение информации модификацией фазы аудиосигнала [Електронний ресурс]. — Режим доступу до документа https://tech.wikireading.ru/13291

20. Барсуков В. С., Романцов А. П. Компьютерная стеганография: вчера, сегодня, завтра. Технологии информационной безопасности XXI века. — матеріали İnternet-ресурсу «Специальная техника» (http://st.ess.ru/).

21. ISSN : 2278 – 1021 International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 4, June 2012 1 LSB Modification and Phase Encoding Technique of Audio Steganography Revisited Prof. Samir Kumar, BandyopadhyayBarnali, Gupta Banik

22. Харрисон Мэтт Как устроен Python. Гид для разработчиков, программистов и интересующихся. —СПб.: Питер, 2019. — 272 с.: ил. — (Серия “Библиотека программиста”). ISBN 978-5-4461-0906-7

23. Гэддис Т. Начинаем программировать на Python. - 4-е изд.: Пер. с англ. - СПб.: БХВ-Петербург, 2019. - 768 с.: ил. ISBN 978-5-9775-4002-5

24. The Ancient Practice of Steganography: What Is It, How Is It Used and Why Do Cybersecurity Pros Need to Understand It // By James Stanger [Електронний ресурс]. — Режим доступу до документа https://www.comptia.org/blog/what-is-steganography

25. Gopalan, K., Wenndt, S., Haddad, D.: Steganographic method for covert audio communications. U.S. Patent 7 231 271 (2007)

26. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. — М. : «Солон-Пресс», 2009. — 272 с.

27. Auguste Kerckhoffs, La Cryptographie Militaire. Journal des sciences militaires, pp: 5–83, Jan. 1883, pp: 161–191, Feb. 1883.

28. K. Burbela, Толюпа С.В. STEGANOGRAPHY IN DAILY LIFE // матеріали III Міжнар. Наук.-практ. Конф. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” 2019 (PCSITS)

29. К. Бурбела, Р. Зюбіна Алгоритми використання стеганографії // матеріали IV Міжнар. Наук.-практ. Конф. “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” 15-16 квітня 2021 року (PCSITS)

ДОДАТКИ

ДОДАТОК А

```
# -*- coding: utf-8 -*-
#!/usr/bin/env python
# to capture console args
import sys, getopt
# math functions
from math import *
import cmath
# use numpy
import numpy as np
# wav io wrapper module
import wav_io
# helper methods for stego operations
from stego_helpers import *
# run some tests
from tests import run_tests

def hide(source, destination, message):
    # read wav file
    print 'reading wave container...'
    (nchannels, sampwidth, framerate, nframes, comptype, compname),\
    (left, right) = wav_io.wav_load(source)
    # select channel to hide message in
    container = left
    container_len = len(container)
    # ------------------------------------
```

```
    # prepare container
    # ----------------------------------
    print 'preparing container...'
    message_len = 8 * len(message)          # msg len in bits
    v = int(ceil(log(message_len,  2)+1))    # get v from equation: 2^v >= 2 * message_len
    segment_width = 2**(v+1)               # + 1 to reduce container distortion after msg
integration
    segment_count = int(ceil(container_len  / segment_width))    # number of segments to
split container in
    # add silence if needed
    if segment_count > container_len / segment_width:
        container = [(container[i] if i < container_len else 0) for i in range(0,
segment_count*segment_width)]
    container_len = len(container)          # new container length
    # split signal in 'segment_count' segments with 'segment_width' width
    segments = chunks(container, segment_width)
    # ----------------------------------
    # apply FFT
    # ----------------------------------
    print 'performing fft transform...'
    delta = [np.fft.rfft(segments[n]) for n in range(0, segment_count)]  # -> segment_width /
2 + 1
    # extract amplitudes
    vabs = np.vectorize(abs)    # apply vectorization
    amps = [vabs(delta[n]) for n in range(0,  segment_count)]
    # extract phases
    varg = np.vectorize(arg)    # apply vectorization
    phases = [varg(delta[n])  for n in range(0, segment_count)]
    # ----------------------------------
    # save phase subtraction
```

```
    delta_phases = segment_count*[None]
    delta_phases[0] = 0 * phases[0]
    def sub (a, b): return a - b
    vsub = np.vectorize(sub)
    for n in range(1, segment_count):
        delta_phases[n] = vsub(phases[n], phases[n-1])
    # ------------------------------------
    # integrate msg, modify phase
    print 'msg integration...'
    msg_vec = str_2_vec(message)
    msg_bits = [d_2_b(msg_vec[t]) for t in range(0, len(message))]
    msg_bits = [item for sub_list in msg_bits for item in sub_list]  # msg is a list of bits now

    segment_width_half = segment_width / 2
    phase_data = (segment_width_half + 1) * [None]  # preallocate list where msg will be
stored
    for k in range(0, segment_width_half + 1):
        if k <= len(msg_bits):
            if k == 0 or k == segment_width_half:    # do not modify phases at the ends
                phase_data[k] = phases[0][k]
            if 0 < k < segment_width_half:          # perform integration begining with the hi-
freq. components
                if msg_bits[k-1] == 1:
                    phase_data[segment_width_half+1-k] = -pi / 2.0
                elif msg_bits[k-1] == 0:
                    phase_data[segment_width_half+1-k] = pi / 2.0
        if k > len(msg_bits):                    # original phase
            phase_data[segment_width_half+1-k] = phases[0][segment_width_half+1-k]
    phases_modified = [phase_data]
    for n in range(1, segment_count):
```

```
        phases_modified.append((phases_modified[n-1] + delta_phases[n]))
    # ------------------------------------
    # convert data back to the frequency domain: amplitude * exp(1j * phase)
    def to_frequency_domain (amp, ph): return amp * cmath.exp(1j * ph)
    vto_fft_result = np.vectorize(to_frequency_domain)
    delta_modified = [vto_fft_result(amps[n], phases_modified[n]) for n in range(0,
segment_count)]
    # restore segments
    segments_modified = [np.fft.irfft(delta_modified[n])  for n in range(0, segment_count)]
    # join segments
    container_modified = [item for sub_list in segments_modified for item in sub_list]
    # sync the size of unmodified channel with the size of modified one
    right_synced = len(container_modified) * [None]
    for i in range(0, len(container_modified)):
        if i < len(right):
            right_synced[i] = right[i]
        else:
            right_synced[i] = 0
  print 'saving stego container...'
    wav_io.wav_save(destination, (container_modified, right_synced),
                    nchannels, sampwidth, framerate, nframes, comptype, compname)
    # to recover the message the one must know the segment width, used in the process
    print "\nDone.\n"
    return segment_width
def recover(source, segment_width):
    # read wav file with integrated message
    print 'reading wave container...'
    (nchannels, sampwidth, framerate, nframes, comptype, compname),\
    (left, right) = wav_io.wav_load(source)
    container = left    # take left channel for msg recovering
```

```
container_len = len(container)
print 'preparing container...'
segment_count = int(container_len / segment_width)
# split signal in 'segment_count' segments with 'width' width
segments = chunks(container, segment_width)
# apply FFT
print 'performing fft transform...'
delta = [np.fft.rfft(segments[0])]
# extract phases
varg = np.vectorize(arg)    # apply vectorization
phases = [varg(delta[0])]
phases_0_len = len(phases[0])
# recover message
print 'recovering message...'
b = []
for t in range(0, segment_width / 2):
    d = phases[0][phases_0_len-1-t]
    if d < -pi / 3.0:
        b.append(1)
    elif d > pi / 3.0:
        b.append(0)
    else:
        break
msg_bits_len = int(floor(len(b) / 8.0))
msg_bits_splitted = chunks(b, 8)
msg_vec = []
for i in range(0, msg_bits_len):
    msg_vec.append(b_2_d(msg_bits_splitted[i]))
message = vec_2_str(msg_vec)
print "\nDone.\n"
```

```
    return message

def main(argv):
    input_container_file_name = ''
    message_file_name = ''
    output_container_file_name = ''
    segment_width = -1
    try:
      opts, args = getopt.getopt(argv, "hi:m:o:k:", ["ifile=", "mfile=", "ofile=", "karg="])
    except getopt.GetoptError:
      print_usage()
      sys.exit(2)
    for opt, arg in opts:
       if opt == '-h':
          print_usage()
          sys.exit()
       elif opt in ("-i", "--ifile"):
          input_container_file_name = arg
       elif opt in ("-m", "--mfile"):
          message_file_name = arg
       elif opt in ("-o", "--ofile"):
          output_container_file_name = arg
       elif opt in ("-k", "--karg"):
          segment_width = int(arg)

    if input_container_file_name == '':
       print_usage()
       sys.exit()

    if not output_container_file_name == '':
```

```
        message = ''
        try:
            with open(message_file_name, "r") as reader:
                message = reader.read()
        except IOError as e:
            print "I/O error({0}): {1}".format(e.errno, e.strerror)
        if not message == '':
            segment_width = hide(input_container_file_name,  output_container_file_name,
message)
            print "Remember segment width to recover message: {0}".format(segment_width)
    elif segment_width > 0:
        message = recover(input_container_file_name,  segment_width)
        try:
            with open(message_file_name, "w") as writer:
                writer.write(message)
        except IOError as e:
            print "I/O error({0}): {1}".format(e.errno, e.strerror)
  else:
        print_usage()
if __name__ == "__main__":
    main(sys.argv[1:])
```