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
_____ Наталія ЛУКОВА-ЧУЙКО
« 14 » червня 2022р.

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: студент IV курсу, групи КБ-41

_____ **Данило ЯЩЕНКО**
(підпис) (прізвище ім'я)

	Прізвище, ініціали	**Підпис**
Керівник	Яніна ШЕСТАК	

Нормоконтроль	Юрій ЩЕБЛАНІН	

Київ 2022

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
_____Наталія ЛУКОВА-ЧУЙКО
«01» листопада 2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студенту **КБ-41** **Данило Ященко Миколайович**
(група) (ім'я прізвище 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 №5 від 29.10.2021 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Стеганографія, авторське право

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Ознайомитися з поняттям авторського права, нормативно-правовою базою, яка забезпечує дотримання авторського права, ознайомитися з засобами захисту авторського права, обрати стеганографічний метод приховування даних та ознайомитися з його алгоритмом, розробити програмне забезпечення спрямоване на захист авторського права методом вбудовування водяного знаку.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розроблено програмний продукт, спрямований на захист авторського права аудіо файлів методами стеганографії.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29.10.2021 року

Завдання видав _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Данило ЯЩЕНКО (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.10.2021-27.01.2022	*виконано*
2	Аналіз літератури	28.01.2022-11.02.2022	*виконано*
3	Обґрунтування вибору рішення	12.02.2022-24.02.2022	*виконано*
4	Планування реалізації роботи	25.02.2022-24.03.2022	*виконано*
5	Вивчення нормативно правової бази у сфері авторського права	25.03.2022-07.04.2022	*виконано*
6	Аналіз проблем інформаційної безпеки у сфері авторського права	08.04.2022-20.04.2022	*виконано*
7	Дослідження методів та алгоритмів стеганографії	21.04.2022-05.05.2022	*виконано*
8	Аналіз можливих варіантів реалізації програмного забезпечення	06.05.2022-20.05.2022	*виконано*
9	Реалізація програмного забезпечення	21.05.2022-01.06.2022	*виконано*
10	Оформлення пояснювальної записки	02.06.2022-05.06.2022	*виконано*
11	Підготовка до захисту	06.06.2022-14.06.2022	*виконано*

Завдання видав _____ (підпис) Яніна ШЕСТАК (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Данило ЯЩЕНКО (ініціали, прізвище)

Термін подання дипломної роботи до ЕК 06 червня 2022 року

РЕФЕРАТ

Пояснювальна записка до дипломної роботи “Методи та моделі захисту авторського права аудіо об'єктів” складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 53 сторінок основного тексту, 22 рисунки та 1 формулу. Список використаних джерел містить 28 найменувань і займає 3 сторінки.

Мета роботи - практично реалізувати стеганографічний метод з метою захисту авторського права в аудіо об’єктах.

Для того, щоб досягти поставленої мети потрібно виконати наступні завдання:

- розглянути чинну нормативно-правову базу України, в напрямках захисту авторського права та процесу використання стеганографічних алгоритмів;
- дослідити проблематику захисту авторського права та використання методів стеганографії;
- дослідити вже існуючі стеганографічні методи та алгоритми для вибору оптимального і під ходячого критеріям алгоритму;
- розробити програмне забезпечення котре буде розв'язувати проблему вбудовування цифрового водяного знаку, задля забезпечення захисту авторського права аудіо об'єкта.

Об'єкт дослідження - є процес захисту авторського права методами стеганографії.

Предмет дослідження – методи і моделі захисту авторського права стеганографічними методами.

Практична цінність полягає у створенні практичної реалізації результатів аналізу для забезпечення захисту авторського права аудіо об’єктів.

Ключові слова*:* захист авторського права, стеганографія, стеганографічні алгоритми, комп’ютерна стеганографія, цифрова стеганографія, аудіо стеганографія, LSB 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

ВСТУП

Актуальність. Достатньо стрімкий розвиток інформаційних технологій провокує постійне питання інформаційної безпеки. Можливість отримання вільного доступу до будь-якої інформації росте в геометричній прогресії, а обсяги цієї інформації постійно збільшуються і всі ці об’єми рано чи пізно попадають в Інтернет, що й ставить першочергову задачу і питання захисту авторського права.

Об’єми даних, що попадають в мережу Інтернет пришвидшують розвиток проблеми захисту авторського права, а розв’язання цієї проблеми виходить на новий рівень. Саме така гонитва технології й приводить до стрімкого розвитку систем, котрих головною задачею є захист інформації від несанкціонованого копіювання, модифікації та розповсюдження.

Питання захисту авторського права існує з давніх часів до моменту як з’явились нові потреби через цифрові технології, популярними методами були ідентифікаційні номери та водяні знаки. У сьогоденні ці методи залишаються, змінилось лише те, якими вони стали і як їх реалізують. Покращення привело до того, що зараз, не просто створюються мітки які лише вказують хто власник, а й за допомогою цих міток можливо контролювати, що відбувається з поміченим об’єктом.

Цифрові водяні знаки вважають одним з найбільш ефективних технічних засобів захисту. Сутність полягає у тому, що в об’єкт, який потребує захисту, вибудовується невидима (інколи видима) мітка, що дозволяє контролювати використання мультимедійного об’єкту, на який було нанесено мітку.

Раніше цей метод використовувався зазвичай для зображень, наразі використання цього методу стало більш популярним і нанесення таких міток відбувається не тільки для зображень, а й для відео та аудіо об’єктів.

Якщо брати до уваги загальні вимоги до нанесення водяного знаку, то головною вимогою стає забезпечення найменш відчутного спотворення у порівнянні з оригінальним об'єктом. Наступною вимогою є забезпечення максимальну стійкість водяного знаку до видалення чи коригування. Додатковою вимогою до цифрових

водяних знаків стає підтримка вже сучасних форматів об’єкта, для прикладу WAV або JPEG.

Аналіз останніх досліджень та літератури. До вітчизняних науковців що внесли свій вклад в вивчення методів стеганографії можна віднести Гончаров Н.О., Конахович Г.Ф., Прогонов В.Г.

Результати здійснених у дипломній роботі досліджень можуть бути використані спеціалістами із захисту інформації та при подальшому проведенні науково-дослідницьких робіт.

Тези стосовно важливості забезпечення інформаційної безпеки за рахунок міжнародних стандартів, були апробовані на III Міжнародній науково-практичній конференції “Проблеми кібербезпеки інформаційно-телекомунікаційних систем” (PCSITS-2020).

РОЗДІЛ 1
СТЕГАНОГРАФІЯ ТА АВТОРСЬКЕ ПРАВО. ОСНОВНІ ТЕРМІНИ ТА ПОНЯТТЯ

1.1 Авторське право. Основні терміни та поняття. Актуальність питання захисту авторського права

Авторське право на сьогодні є напевно однією з найактуальніших проблем, адже майже вся інформація таким чи іншим способом потрапляє до мережі Інтернет, а вже в мережі у практично кожного користувача є вільний доступ до цієї інформації. Маючи доступ до будь-якої інформації стає питання її безпеки, адже доступ – безмежна можливість порушити цілісність, конфіденційність і, при певних можливостях, доступність. Для прикладу можливо розглянути будь-яку інтернет-сторінку, всі об’єкти які ми на ній бачимо, текст, фото, відео тим чи іншим шляхом може бути в небезпеці, і все це потребує захисту. Саме за для першочергової безпеки таких об’єктів існує авторське право.

Авторське право - особисті немайнові права і майнові права авторів та їх правонаступників, пов'язані зі створенням та використанням творів науки, літератури та мистецтва. Саме таке визначення тлумачиться Законом України “Про авторське право і суміжні права”, та саме цей закон регулює діяльність авторського права на території України. Стаття 8 Закону України “Про авторське право і суміжні права” зазначає, що до об’єктів авторського права відносяться:

- літературні письмові твори;
- виступи, промови та лекції;
- комп’ютерні програми та бази даних;
- музичні, драматичні та музично-драматичні твори;
- твори архітектури та садового мистецтва;
- фотографічні твори, ілюстрації, карти, ескізи та креслення;
- збірники творів та тексти перекладів.

З наведеного вище списку можна зазначити, що сфера діяльності авторського права поширюється як на оприлюднені, так і на не оприлюднені об’єкти [1].

Враховуючи проблематику роботи будуть розглядатися об’єкти, що є опублікованими в мережі або на будь-якому цифровому пристрої, а саме це будуть мультимедійні дані. Оскільки усі інформаційні чи медійні дані зараз можно оцифрувати, то необхідно звернути увагу на таке поняття, як керування цифровими правами, або Digital rights management.

Керування цифровими правами (далі DRM) - це спосіб захисту авторських прав цифрових медіа. Цей підхід включає використання технологій, які обмежують копіювання та використання захищених авторським правом творів і запатентованого програмного забезпечення. Головною задачею є обмеження несанкціонованого використання носіїв та цифрової інформації [2].

Розглядаючи питання авторського права в інтернеті, першочерговою проблемою стає процес доведення авторства того чи іншого об’єкту, адже коли він потрапляє в мережу, відбувається стрімкий процес модифікації інформації, вона оновлюється, редагуєтеся, видозмінюється. Розв'язання такої проблеми є закріплення права власності до розміщення об’єкту в мережі або оперативні дії для підтвердження цього права.

Щоб закріпити право власності достатньо надати відповідні докази та отримати нотаріальне посвідчення. Доказом в такому випадку буде вважатись будь-яка інформація, яка на пряму належить об'єкту. В такому випадку обов’язково потрібно брати до уваги Статтю 8 Закону України “Про авторське право і суміжні права” в якій зазначено, що передбачена цим Законом правова охорона поширюється тільки на форму вираження твору і не поширюється на будь-які ідеї чи теорії, навіть у випадку, якщо вони є чітко вираженими, описаними чи проілюстрованими у творі.

На жаль, процес закріплення авторського права об’єктів в Україні не є досконалим, тому для спрощення юридичного урегулювання даного питання є документ – “Рекомендації щодо вдосконалення механізму регулювання цифрового

використання об’єктів авторського права і суміжних прав через мережу Інтернет” [2].

Третій пункт цього документу, а саме “Способи захисту авторського права і суміжних прав в мережі Інтернет” наводить наступні приклади:

– Електронно цифровий підпис.

Суть електронно цифрового підпису полягає в тому, що його отримують в результаті шифрування набору електронних даних. Завдяки цьому можливо ідентифікувати автора.

– Ідентифікація об’єктів авторського права і суміжних прав.

Цей спосіб будується на певних рисах того чи іншого об’єкту, що дає можливість їх відрізняти. Такими методами ідентифікації можна вважати, Міжнародний стандартний книжковий номер – ідентифікаційний код ISBN, та ідентифікаційний код ISAN, який використовується для ефективного захисту фільмів та інших будь-яких аудіовізуальних творів.

Ідентифікаційний код ISBN є універсальним, створює єдину систему видання та книгорозповсюдження.

Ідентифікаційний код ISAN собою являє один зі способів систематизації аудіовізуальних об’єктів, використання цього коду дає змогу не тільки створити систематизовану базу об’єктів, а і регулювати особливості того чи іншого об’єкту.

– Цифрові водяні знаки

Ця технологія, створена для захисту мультимедійних даних методом впровадження в них міток з інформацією. Її принцип ідентичний до звичайних водяних знаків. Різниця лише в тому, що вони зазвичай не відображаються візуально, а інтегруються в цифрові дані невидимо. Але при застосуванні об’єкту з таким ідентифікатором, він буде містити додаткову інформацію в якій буде вказано власника.

Даний спосіб належить до технології керування цифровими правами, і є частиною такої системи [3].

1.2 Стеганографія, терміни та поняття

Технічний розвиток людства означає не лише створення нового, а й покращення вже наявного. З кожним днем зміни одного, змінюють пріоритет іншого, так покращення методів передачі даних, створює відповідний пріоритет з забезпечення безпеки цієї передачі. Єдине, що залишається незмінним – інформаційні ресурси та їх безпека, поява глобальної мережі спровокувала дуже легкий доступ до будь-якої інформації, а відразу за цим й похитнула загальні поняття безпеки. Загалом такий прогрес можна схарактеризувати як перегони методів безпеки та методів порушення.

Використання даних у цифровому форматі створює цілу низку переваг, а саме:

– швидкість передачі;
– можливість відновлення;
– практичність використання;
– практичність зберігання.

Беручи до уваги всі ці переваги, в очі одразу кидається факт можливих недоліків. І в цьому питані, відповідь знаходиться в самих перевагах, при “невдалому” використані даних, переваги стають недоліками, адже практичність використання і зберігання стає практичністю викрадення, модифікації, заміни або знищення. Напевно, неможливо сказати чи існують методи чи заходи, щоб захистити інформацію так, щоб доступу до неї не було ні у кого, але саме це й спонукає людство на розвиток. Саме завдяки такому розвитку і з’явилось поняття стеганографія [3].

Стеганографія – це давня практика тайнопису, при якому повідомлення закодовувалось так, щоб воно не виглядало як повідомлення. На відміну від свого “старшого” брата, тобто криптографії, головною перевагою стеганографії є приховування факту, повідомлення, а не його шифрування.

Завданням стеганографії є вивчення та практика приховування наявності будь-якої секретної інформації при передачі, обробці або зберіганні даних. Від свого

скромного походження, яке передбачало фізичне приховування комунікацій та використання невидимих чорнил, стеганографія перейшла у цифрову сферу.

При використанні цього методу, існує одна важлива задача, і цією задачею не неможливість виявити приховане повідомлення у разі перехоплення даних. Кажучи про передачу даних, звичайне повідомлення з певною прихованою інформацією може викликати підозру, тому й застосовується поєднання двох наук, криптографії та стеганографії. В такому випадку, інформація яка потребує захисту спочатку шифрується використовуючи криптографію, а потім вже використовуючи стеганографію приховують факт передачі зашифрованої інформації.

Історично так склалось, що стеганографія є менш популярним методом захисту, а ніж криптографія, але це не заважає їй розвиватись і покращувати свої методи.

В стеганографії є певний перелік основних понять та визначень

– повідомлення – дані які мають бути передані;
– стеганоконтейнер – оригінал файлу, призначений приховати дані;
– стеганоповідомлення – інформація, вбудована до стеганоконтейнеру;
– порожній контейнер – файл в якому повідомлення ще не вбудоване;
– заповнений контейнер – файл в якому повідомлення було вбудовано.

Додатково до загальних визначень відносять наступні види стеганографії:

– Класична

Класичною стеганографією вважають використання невидимих чорнил. Достатньо було нанести на клаптик паперу повідомлення, зачекати і все, без відповідної інформації, це був лише клаптик паперу. Класична стеганографія на цьому не зупинялась і далі стандартом стало нанесення двух шарів інформації, де першим шаром було повідомлення, а другим шаром інформація яка не мала жодної користі [5].

– Мережева

Мережева стеганографія – наймолодший вид стеганографії, вперше цей термін використав Кжиштоф Щипьорский в 2003 році, цей вид використовується коли прихована інформація передається через комп'ютерні мережі з використанням

особливостей роботи протоколів передачі даних. Мережева стеганографія охоплює широкий спектр методів:

– WLAN
– LACK
– DAB I DVB
– Комп’ютерна

Комп’ютерна стеганографія – заснована на особливості саме комп’ютерних платформ, зазвичай використовується в приховуванні даних в невикористовуваних областях форматів файлів або підміні символів в назві файлу.

Нижче наведено декілька прикладів, що можна віднести до комп’ютерної стеганографії:

- використання зарезервованих полів комп'ютерних форматів файлів;
- метод приховування інформації в невикористовуваних місцях гнучких дисків;
- використання особливостей файлових систем;
- метод приховування інформації використовуючи більшу частоту кадрів;
- приховування інформації в звукових доріжках;
- вбудовування повідомлення в червоний, зелений або синій канал зображення.

– Цифрова

Цифрова стеганографія – це нащадок класичної стеганографії, створений на основі впровадження додаткової інформації в цифрові об’єкти.

Потрібно розуміти, що до основних задач стеганографії відносять не лише задачу секретної передачі інформації, а й використання вбудованих ідентифікаційних номерів та цифрових водяних знаків. Розміщення саме цих елементів має бути таким, щоб користувач не міг помітити жодної різниці між оригінальним та модифікованим об’єктами. Виходячи з задачі розміщення можна виділити основні характеристики:

– безпека;

– стійкість;
– непримітність;
– ємність.

Поняття безпеки та стійкості є взаємопов’язаним. Стійкість вираховується за різними прикладами, одним з таких є оцінка кількості помилок котрі виникають при вилучені інформації зі стеганоконтейнеру, при проведені навмисних атак або випадкового спотворення, відповідно до такого прикладу, якщо результатом стає велика кількість помилок, такий метод не є безпечним. Інший приклад, оцінка при випадку пасивних атак, в такому разі звертається увага чи може користувач без використання особливих методів відчути, знайти, побачити різницю між заповненим контейнером та пустим.

Непримітність як характеристика відіграє важливу роль, адже саме вона є одним з головних факторів стійкості. Під непримітністю розуміється те, що повідомлення має бути вбудоване так, щоб його не було помітно. Для прикладу, якщо це зображення, то немає бути помітним різницю між пікселями, якщо це аудіо файл, то при прослуховуванні має бути нечутно вбудоване повідомлення. Щоб досягнути таких результатів, потрібно в першу чергу звернути увагу на особливості організму людини. Людина чує звук з частотами від 16 Гц до 20 кГц (приблизні дані) отже для аудіо достатньо використати частоту поза цим діапазоном [5].

Ємність, ще одна важлива характеристика, адже вона відповідає за кількість інформації, яка може бути вбудована в контейнер, при цьому не порушаючи фактори стійкості та непримітності. Кількість інформації вираховуєтеся за різними факторами, такими як

– вид можливих порушень;
– можливості контейнера;
– тип контейнера;
– повідомлення.

Хоч ці фактори і можна назвати плаваючими, є один статичний фактор який існує при будь якому з варіантів – наповненість контейнера, саме цей фактор відповідає за першочергову можливість функціонування прихованого повідомлення.

Для вимірювання наповненості зазвичай використовують відсотки. Наповненість контейнера не має перевищувати пропускну здатність створюваного стегоканалу, в іншому ж випадку, система не буде функціонувати або ненадійно.

Розглядаючи основні галузі застосування можна виділити наступне:

– Прихована комунікація.

Ця галузь в основному відноситься до військового та державного зв’язків, але може також використовуватись провідними компаніями.

– Захист від копіювання.

До цієї галузі можна віднести багато прикладів, від сфери комерції та контролю копіювання до регулювання розповсюдження мультимедійних об’єктів.

Розглядаючи використання саме комп’ютерної стеганографії для захисту інтелектуальної власності існує два напрямки вирішення задач. Перший напрямок не пов'язаний з використанням цифрової обробки сигналів, а саме розміщення повідомлення в заголовках переданих даних. Цей напрямок в загальній практиці майже не застосовується адже його проблема в тому, що він не вважається стійким, приховане повідомлення доволі легко виявити і далі видалити або модифікувати.

Другий напрямок напряму пов'язаний з використанням цифрової обробки сигналів, використовуючи його, відбувається вбудовування повідомлення в об’єкт.

Саме розвиток другого напрямку спровокував виникнення поняття цифрової стеганографії, що будується на основі використання для стеганоконтейнерів цифрових об’єктів.

Отже, відповідно до вище зазначеного, цифрова стеганографія – це напрямок стеганографії, в основі якого лежить використання цифрових об’єктів в якості стеганоконтейнера.

В свою чергу цифрова стеганографія має 4 основних напрямки:

- вбудовування заголовків;
- вбудовування ідентифікаторів;
- вбудовування інформації для прихованої передачі;
- вбудовування цифрових водяних знаків.

Вбудовування заголовків – метод який часто використовують у медичній сфері адже мета такого метода зберегти різноманітну інформацію в цілому, використовується наприклад для підпису рентгенівських знімків.

Вбудовування ідентифікаторів – назва методу каже саме за себе, цей метод використовується для вбудовування в об’єкт конкретного ідентифікатору (унікального номеру). Такий метод дозволяє відслідковувати всі можливі порушення, адже ідентифікатор дозволить відслідковувати дії з об’єктом [7].

Вбудовування інформації для прихованої передачі – тут все доволі зрозуміло, головною задачею є приховати факт передачі інформації в об’єкті.

Вбудовування цифрових водяних знаків – саме цей метод використовується для захисту авторських прав. Хоча цей метод не є прихованим, його основною задачею є факт ідентифікації власника об’єкту.

Піратство є гострою проблемою захисту авторського права, адже саме стирання даних про власника об’єкта є головною задачею піратства. Розглядаючи саме стеганографію як метод захисту можна розрізнити наступні два методи, що є основою використання стеганографії:

- Вбудований захист - цей захист виступає як окремий модуль безпеки.
- Додатковий захист – цей захист вважається лише додатковим модулем безпеки

Якщо проводити аналіз цих двох методів, можна прийти до наступних висновків. Вбудований захист є більш надійним але редагування будь яких модулів такого захисту може бути критичним. З іншого боку додатковий захист каже сам за себе, цей метод є більш гнучким, а отже й стабільнішим, але через відсутність “статичності” можливі проблеми при використанні тих самих конфігурацій з різними об’єктами [8].

1.3 Аналоги використання стеганографічних методів захисту інформації

З кожним днем технологій стає більше, вони покращуються, відкриваються нові методи, знання. Результатом таких змін є нові думки та нові можливості,

аналоги застарілих чи класичних методів. Одним з чудових прикладів який можна навести це ідея децентралізації, та технологія блокчейн.

Блокчейн — це децентралізований, розподілений і загальнодоступний цифровий реєстр, який використовується для запису транзакцій на багатьох комп'ютерах, так що запис не може бути змінений заднім числом без зміни всіх наступних блоків і консенсусу мережі [8].

Блокчейн отримав свою назву завдяки тому, як він зберігає дані транзакцій — у блоках, які з'єднуються між собою, утворюючи ланцюг. Зі збільшенням кількості транзакцій зростає і блокчейн. Кожен новий запис підтверджує час і послідовність транзакцій, які потім реєструються в блокчейні в дискретній мережі, яка керується правилами, погодженими учасниками мережі. Кожен блок містить хеш, пакети останніх дійсних транзакцій із мітками часу та хеш попереднього блоку. Хеш попереднього блоку зв'язує блок разом і запобігає зміні будь-якого блоку або вставлення блоку між двома наявними блоками. Таким чином, кожен наступний блок посилює перевірку попереднього блоку, а отже, і всього блокчейну. Блокчейн, надає ключовому атрибуту незмінність. Поки блокчейн по суті служить базою даних для запису транзакцій, його переваги виходять далеко за межі традиційних баз даних.

На разі технологія блокчейну, ще розвивається, але навіть зараз вона вже набрала популярність у всьому світі, і провідні компанії вже займаються вивченням та розробкою цієї технології. Це відбувається по причині того, що ця технологія має безліч застосувань. Серед яких можна виділити наступне:

– обробка платежів і грошових переказів.

Транзакції, оброблені через блокчейн, можуть бути розраховані за лічені секунди та зменшити (або виключити) комісію за банківські перекази.

– моніторинг ланцюгів постачання.

Використовуючи блокчейн, компанії можуть швидко виявляти неефективність у своїх ланцюгах постачання, а також знаходити предмети в режимі реального часу та бачити, як продукти працюють з точки зору контролю якості, коли вони подорожують від виробників до роздрібних продавців.

– цифрові ідентифікатори.

Microsoft експериментує з технологією блокчейн, щоб допомогти людям контролювати свою цифрову ідентичність, а також дати користувачам контроль над тим, хто отримує доступ до цих даних.

– обмін даними.

Блокчейн може виступати посередником для безпечного зберігання та переміщення корпоративних даних між галузями.

– управління мережею Інтернет речей.

Блокчейн може стати регулятором мереж, щоб визначати пристрої, підключені до бездротової мережі, відстежувати активність цих пристроїв і визначати, наскільки надійними є ці пристрої, а також автоматично оцінювати надійність нових пристроїв, які додаються до мережі, наприклад як автомобілі та смартфони.

– захист авторських прав.

Блокчейн можна використовувати для створення децентралізованої бази даних, яка гарантує, що виконавці зберігають своє авторство. Блокчейн також може зробити те ж саме для розробників з відкритим кодом.

Саме останній пункт є цікавим при розгляді проблематики роботи. Зараз вже існують проекти, що реалізують блокчейн, а саме потенціал забезпечення захисту авторських прав. Прикладом такого проекту є Non-fungible token (далі NFT).

NFT – вид унікальних криптографічних токенів, де кожен екземпляр є унікальним і його не можна замінити або підмінити іншим токеном, хоча за своєю основою задачею, токен є взаємозамінним. Цей унікальний токен собою являє криптографічний “сертифікат” який записується в блокчейн.

Наразі велику популярність NFT набрали завдяки блокчейну Ethereum (Ефіріум) та криптоплощадкам, де користувачі виставляють власні об’єкти котрі далі продаються за криптографічну валюту.

Проте на сьогодні в Україні немає закону який би міг регулювати питання авторського права та його підтвердження з використанням саме блокчейн технології, що робить використання стеганографічних методів для вирішення проблеми даної роботи більш актуальним.

Висновки за розділом 1

У першому розділі було наведено основні терміни та визначення, які використовуються у сфері авторського права та у стеганографії. Розглядаючи поняття, пов’язані зі сферою авторського права було зазначено, що переважна кількість визначень зазначається Законом України “Про авторське право та суміжні права”. Діяльність у сфері стеганографії та стеганографічного захисту інформації регламентується Законом України “Про захист інформації в інформаційно-телекомунікаційних системах”. Було також зазначено, що попри розвинутість рівня використання інформаційних технологій в Україні, дані сфери потребують подальшого нормативно-правового коригування.

Наведені вище закони дають змогу визначити поняття авторського права та стеганографії, а саме, 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, та стеганографічний захист інформації – це спосіб захисту даних методом приховання їх наявності в об’єкті.

У ході роботи зазначено, що авторське право регулює не тільки захист оприлюднених інформаційних об’єктів, а й тих, що не були опубліковані. Головною проблемою у процесі зазначення за певним об’єктом авторського права в мережі Інтернет є те, що будь-які дані генеруються та модифікуються дуже швидко.

Під час дослідження було виявлено, що, незважаючи на велику кількість сфер застосування стеганографічних методів, саме сфера авторського права є однією з найбільш перспективних для розвитку.

Стійкість, невідчутність, безпека та висока пропускна здатність є одними з основних характеристик стеганосистем.

Було наведено приклад інших способів доведення авторського права у мережі Інтернет, а саме використання технології блокчейну. Було зазначено, що блокчейн — це децентралізований, розподілений і загальнодоступний цифровий реєстр, який використовується для запису транзакцій на багатьох комп’ютерах, так що запис не

може бути змінений заднім числом без зміни всіх наступних блоків і консенсусу мережі.

Дослідженням було вивчено один з прикладів використання блокчейну, а саме NFT – це вид унікальних криптографічних токенів, де кожен екземпляр є унікальним і його не можна замінити або підмінити іншим токеном, хоча за своєю основою задачею, токен є взаємозамінним.

Проте через відсутність в Україні закону, який би міг регулювати питання авторського права та його підтвердження з використанням саме блокчейн технології, використання стеганографічних методів для вирішення поставленої проблеми є більш актуальним.

Проведені дослідження дають змогу визначити подальші кроки роботи:

1. необхідно визначити існуючі стеганографічні алгоритми, направлені на вирішення проблеми даної роботи;
2. необхідно навести загальну характеристику стеганографічних методів;
3. навести приклади використання обраного стеганографічного алгоритму.

РОЗДІЛ 2
АУДІО СТЕГАНОГРАФІЯ, ЯК МЕТОД ВИРІШЕННЯ ПОСТАВЛЕНОЇ ПРОБЛЕМИ

2.1 Способи використання стеганографічних алгоритмів з метою забезпечення авторського права

У ході дослідження було виявлено, що сфера захисту авторського права є однією з найбільш перспективних для розвитку стеганографії, як науки, адже з плином часу саме у цій сфері створюється все більше методик закріплення факту власності над об’єктами мультимедійної сфери.

Методи вбудовування цифрового водяного знаку або вшиття певного ідентифікаційного коду в файл є двома основними напрямками розміщення інформації, яка буде підтверджувати факт власності, у файлі.

Як і усі інші, ці методи мають спільні ознаки та відмінні. До спільних ознак можна віднести те, що обидва методи несуть за собою додавання до файлу певної інформації, що повідомить нам, хто володіє об’єктом.

Основною відмінністю між методами є те, яким чином визначається особлива інформація, котра буде свідчити про власника об’єкту.

Для методу вбудовування коду в файл унікальний код отримується в певному виконавчому органі і водночас долучається до певної бази, в якій міститься перелік об1єктів інтелектуальної власності та яка дасть змогу потім не просто ідентифікувати будь-яку копію, а й відслідкувати її шлях у мережі. Код книг у бібліотеці буде найвдалішим аналогом, адже там також навіть за відсутності книги можна виявити, де вона знаходиться.

ЦВЗ є більш простим у досягнені та не є проблематичним при використанні. Сутність не дуже відрізняється, обидва методи вбудовують певну інформацію у файл, проте для першого методу є необхідність отримати той самий код, а при використанні ЦВЗ мітка генерується самостійно, що і робить його простішим і зручнішим.

На жаль, як і будь-який інший метод, ЦВЗ теж має свої недоліки, такі як можливість вилучення цифрового водяного знаку з об’єкту методом стиснення файлу [12].

2.2 Методи і моделі стеганографії

За принципами приховування даних моделі стеганографії класифікують як форматні та неформатні, тобто ті, що базуються на використанні форматів файлів та ті що роблять зміни у безпосередньо даних, які створюють отриманий файл, відповідно.

До перших належать такі стеганографічні моделі, які аналізують формат файлу і вносять зміни до службових полів, редагування яких не вплине на стані стеганоконтейнеру. Цей метод має менший шанс на модифікацію кінцевого файлу, що є його переважним плюсом.

Другий метод не залежить від формату файлу а використовує складові файлу, наприклад, для зображень це біти, а для аудіо файлів – це фази або коливання. Перевагою такого методу є те, що він є більш стійким до будь-якого виду атак, а недоліком – він призводить до появи спотворень у початковому файлі, тому треба бути обережними, щоб ці спотворення не були помітними [13].

До найбільш відомих стеганографічних методів можна віднести наступні:

- метод з використанням особливостей формату файлу;
- LSB кодування;
- ехо кодування;
- фазове кодування.

2.2.1 Методи з використанням особливостей формату файлу

Даний метод приховування є одним з форматних моделей, він є простим у реалізації, не потребує особливого програмного забезпечення та не вимагає від

виконувача надзвичайної обачності для уникнення спотворень чи виявлення повідомлень.

Запис інформації у метадані чи використання службових полів формату є одними з найпростіших прикладів використання даного методу.

Метод має велику кількість переваг відносно інших, проте вони не перекривають усі недоліки. До переваг відносять те, що:

– метод є простим у використанні;

– метод є простим у реалізації;

– при використанні даного методу є змога приховати велику кількість інформації у файлі.

До недоліків методу відносять:

- можливість побудови повністю автоматичного алгоритму для виявлення факту приховування повідомлення;
- низьку стійкість до пасивних атак.

Метод приховування в палітрі є прикладом використання цього алгоритму. Він полягає у тому, що всі елементи палітри складаються з чотирьох байт, проте зазвичай лише перші три з них використовуються для кодування кольору. Останній байт зазвичай дорівнює нулю і не використовується.

2.2.2 Ехо кодування

Метод ехо кодування має таку назву, адже його суть полягає у вбудовуванні в аудіо сигнал даних за допомогою додавання в нього ехо сигналу.

Для кодування послідовності значень використовуються нерівномірні проміжки між вже наявними ехо сигналами, котрі, при накладені у відповідних умовах, будуть непомітними, що відповідає одній з основних вимог стеганографії – непомітність для людини.

Накладання повідомлення відбувається за допомогою заміни трьох, характерних для цього методу, параметрів, а саме:

– початкової амплітуди;

– ступеню загасання;

– затримки.

Зміна цих параметрів відбувається в рамках певного порогу між безпосередньо сигналом та ехо, а в утвореній точці людина не зможе знайти різницю між початковим та видозміненим сигналами. Проте треба брати до уваги, що факт наявності таких точки залежить безпосередньо від якості вихідного файлу [15].

При кодуванні нуля та одиниці потрібно використовувати два різних значення затримки, головною умовою для вибору даних значень є те, що вони мають бути на більшими за поріг чутливості слухача.

Інші параметри, а саме початкова амплітуда та ступінь загасання, повинні також обиратися таким чином, щоб не перевищувати поріг чутливості слухових систем людини.

Зворотній процес, тобто процес витягу прихованої інформації потребує виявлення інтервалу між ехо сигналами. Для цього необхідно провести наступні дослідження:

– порівняти амплітуду автокореляційної функції в двох позиціях;

– дослідити косинус перетворення Фур’є натурального логарифму спектра потужності кодованого сигналу.

Проведені обчислення наддадуть змогу виявлення інтервалу між ехо сигналом та вихідним сигналом [16].

Як і всі методи, цей має свої недоліки, а саме те, що:

– реалізація даного алгоритму потребує спеціального обладнання й особливо обережного виконання процесу;

– у випадку використанні даного алгоритму ймовірність внесення у стеганоконтейнер спотворень, які будуть помітними, є достатньо високою;

– іноді не є можливим точно визначити передану інформацію, зокрема був це нуль чи одиниця;

– даний алгоритм досить складно використовувати у якості каналу передачі повідомлень через низьку пропускну здатність.

Унаслідок досліджень можна зробити висновок, що через ряд недоліків при використанні ехо кодування, як методу стеганографії, він зустрічається дуже рідко та є складним при реалізації.

2.2.3 Фазове кодування

Відповідно до назви, метод фазового кодування базується на використанні особливостей сприйняття людського вуха, а саме на тому, як воно сприймає різницю фаз сигналу. Суть у тому що через особливості наших слухових органів, ми маємо змогу сприймати не значення самої фази, а відмінності між різними фазами.

Наведемо визначення фази, для більш повного розуміння. Повна фаза коливання ─ це аргумент періодичної функції, який описує коливальний процес.

Для використання 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 не можна було відрізнити між собою, щоб це було як мінімум складно, а краще неможливо [17].

Щоб мати змогу помістити повідомлення до сигналу необхідно взяти множину вже наявних фаз сигналу ы вирахувати набір рівномірно розподілених значень, які відповідають нулю та одиниці. Значення фази, яка кодується замінюється найближчим значенням, яке відповідатиме необхідному біту. Для закодовування біту береться певна послідовність змін фаз, яка відрізняється для нуля і для одиниці. Наведемо процес фазового кодування графічно (Рис.2.1-2.9):

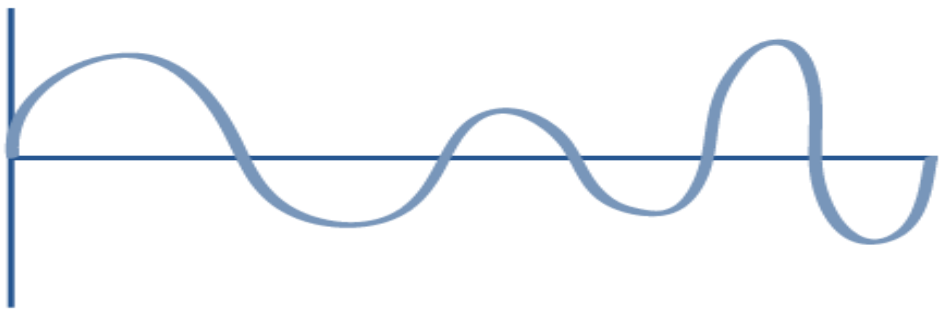

Рисунок 2.1 – Початковий сигнал

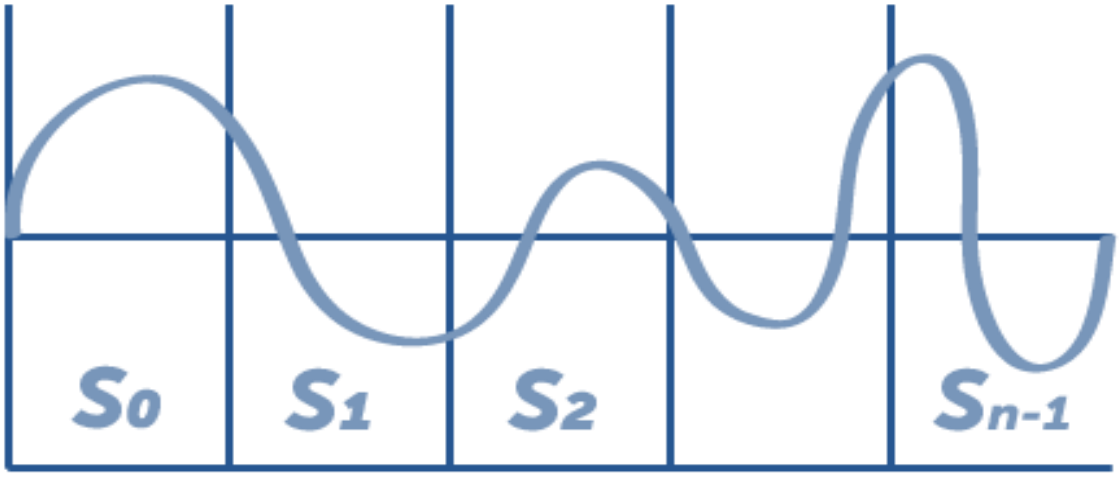

Рисунок 2.2 – Початковий сигнал розбивається на n сегментів

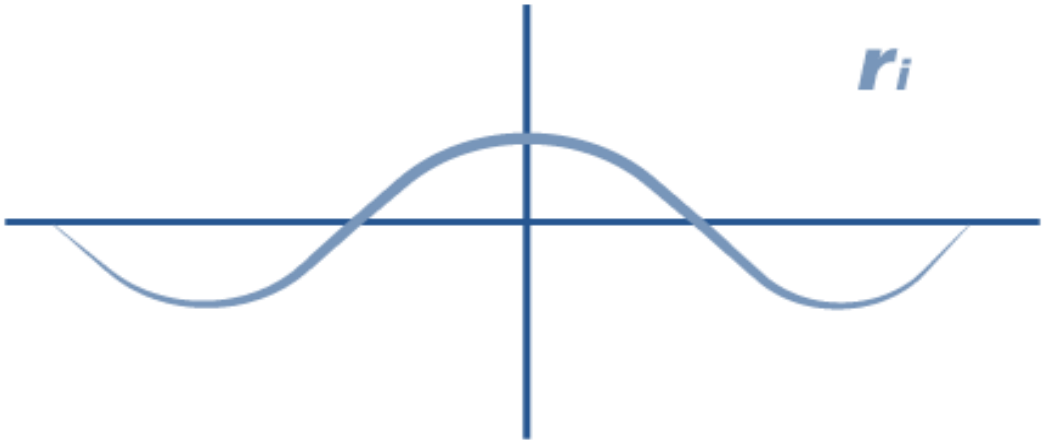

Рисунок 2.3 – Виділення амплітуди кожного сегменту

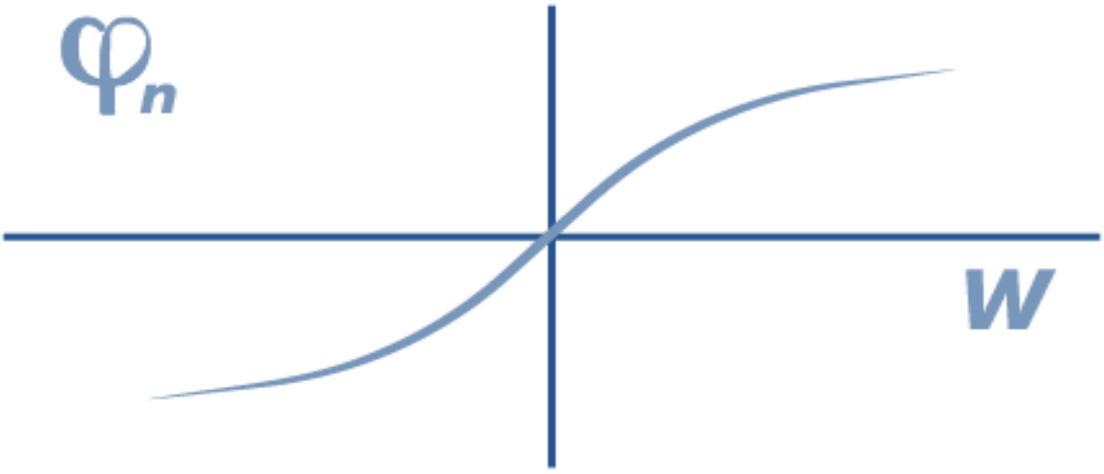

Рисунок 2.4 – Виділення фази кожного сегменту

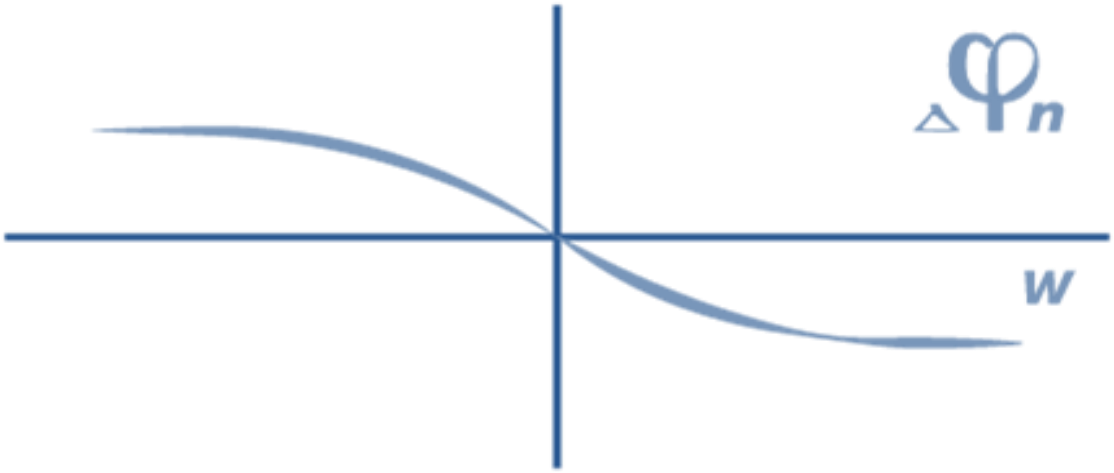

Рисунок 2.5 – Різниця фаз між сусідніми елементами

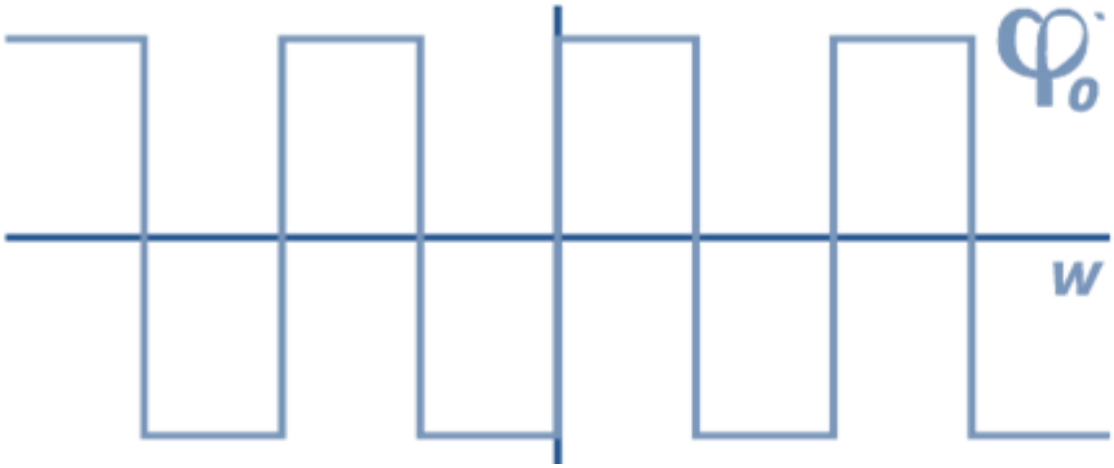

Рисунок 2.6 – Створення нової фази для сегменту S_0

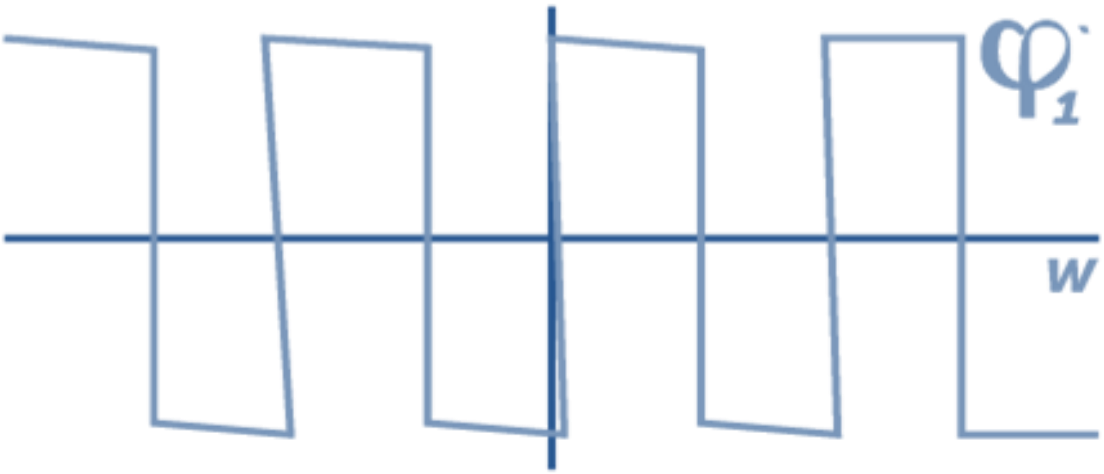

Рисунок 2.7 – Створення нової фази для інших сегментів

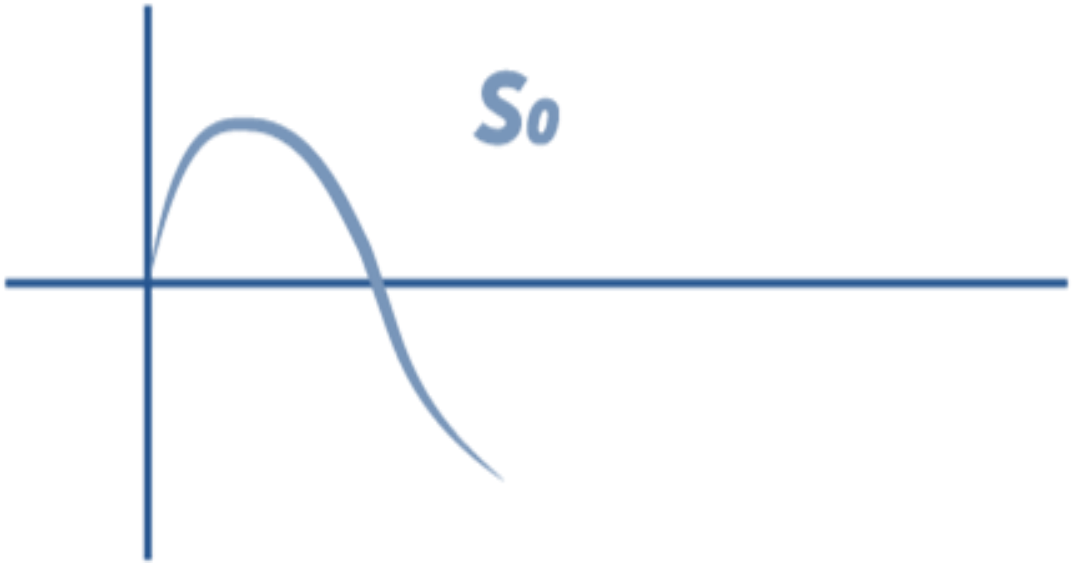

Рисунок 2.8 – Об’єднання нової фази та початкової амплітуди, щоб отримати новий сегмент S_0

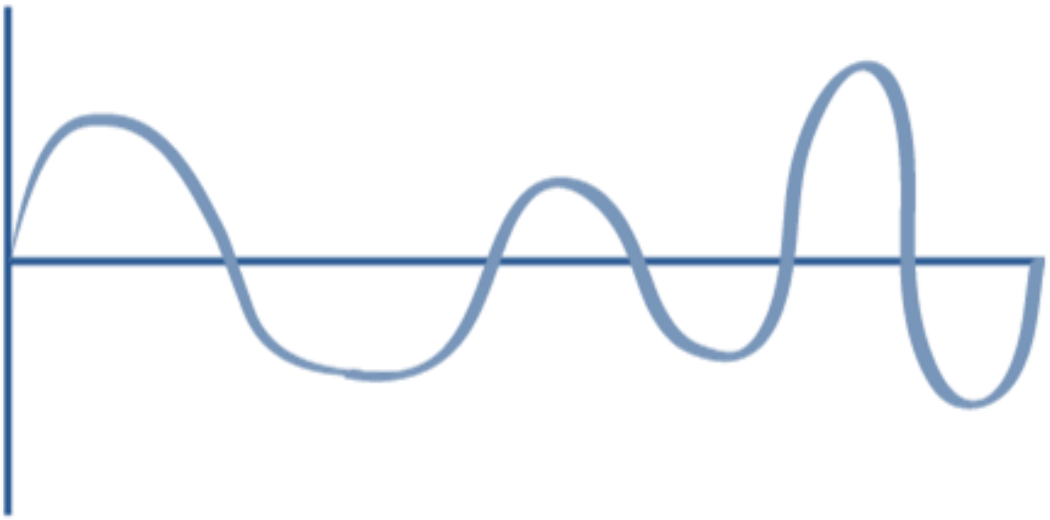

Рисунок 2.9 – Сигнал з вбудованим ЦВЗ, отриманий внаслідок об’єднання отриманих сегментів

Для вилучення прихованого повідомлення з файлу використовується спеціальна функція виявлення:30.06.2022

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

Позначення, використанні у даній формулі мають наступні значення:

де $u = \{\alpha_0, \beta_1, \alpha_2, \beta_3\}$— 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 отримується значення q. Якщо дане значення більше за нуль, то біт переданого повідомлення дорівнює одиниці, якщо він менший за нуль, то біт відповідно дорівнює нулю.

Як і інші, метод фазового кодування має недоліки, а саме:

– алгоритм має низьку швидкість передачі даних під час створення каналу передачі даних через те, що 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 – це високої ймовірності виявлення повідомлення через спотворення у разі його великих розмірів [18].

2.2.4 LSB кодування

Метод LSB (Least Significant Bit, найменший значущий біт) кодування — це класичний метод стеганографії, який використовується для приховування існування секретних даних всередині «публічної» обкладинки. Цей метод використовує надмірність файлів або молодші значущі біти для розміщення в них повідомлення. Така заміна майже не впливає на файл і не створює значних помітних спотворень.

Наведемо приклад для кращого розуміння. Десяткове число 170 може бути представлене у двійковому позначенні як 10101010 (ми припускаємо машину, яка використовує little-endian, тобто адреса якої починається справа і зростає вліво). Як показано на малюнку, молодший біт у цьому випадку дорівнює 0.

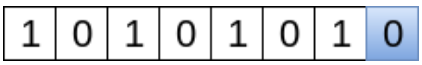

Рисунок 2.10 – Двійкове позначення у вигляді little-endian

У спрощеній формі алгоритм LSB замінює LSB кожного байту в даних «носія» одним бітом із «секретного» повідомлення. Ця концепція відображена на схемі нижче.

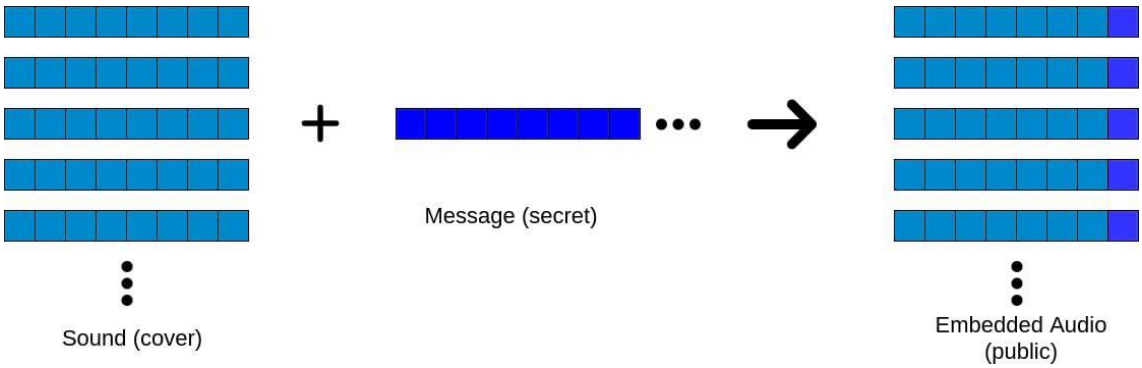

Рисунок 2.11 – Спрощена форма алгоритму LSB

Відправник виконує «вбудовування» бітів секретних повідомлень в дані носія побайтно. У той час як одержувач виконує процедуру «вилучення», зчитуючи біти LSB кожного байту отриманих даних, таким чином одержувач відновлює секретне повідомлення.

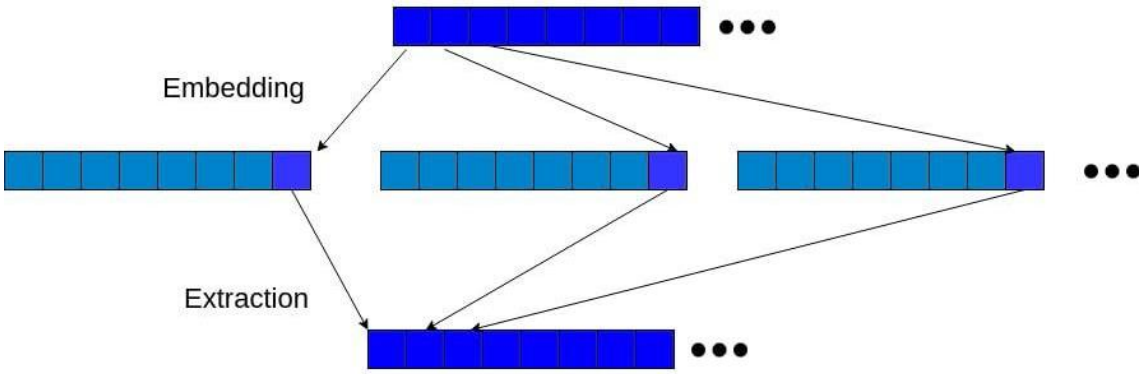

Рисунок 2.12 – LSB метод

LSB стеганографія дуже популярна для стеганографії зображень, тобто приховування секретів у зображеннях. І зміна LSB впливає на колір настільки незначно, що зміна кольору взагалі не помітна для людського ока. Однак людське вухо більш чутливе до незначних змін звуку, і, отже, «шум», який ми додаємо, матиме більшу ймовірність бути поміченим. Щоб подолати цю проблему цієї тривіальної форми алгоритму LSB, багато дослідників запропонували варіанти, які підвищують надійність у звуковій області [20].

Основною перевагою методу LSB можна віднести великий обсяг переданих даних. Проте 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.

Наведемо приклад використання даного методу з використанням зображення у форматі BMP в якості стеганоконтейнеру. Файли цього формату можна уявно розбити на чотири частини, а саме:

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

При використанні обраного методу 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. Далі записано відстань зміщення від початку файлу до байтів власне самого зображення. А пікселі кодуються трьома байтами RGB.

Відбувається заміна молодших бітів в байтах, які відповідають за кодування кольору. Далі наведено байт секретного повідомлення:

11001001,

а далі наведено байти безпосередньо зображення:

11011001 01000110 00110100 10010110 …

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

11 00 10 01

І відбувається безпосередньо заміна 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 замінено тільки два молодших біти, проте кількість замінюваних бітів є необмеженою. Хоча варто зазначити, що при захованні більшого об’єму інформації здійснюється більша кількість замін бітів, що спричиняє більше спотворень в оригінальному файлі.

2.3 Порівняння методів аудіо стеганографії

Серед розглянутих алгоритмів було проведено аналіз з метою виявлення найбільш вигідного для реалізації.

Метод використання форматів файлу, незважаючи на простоту у реалізації та використанні, має низьку стійкість до пасивних атак та високу ймовірність виявлення прихованих даних. Незважаючи на переваги, недоліки перемагають і роблять метод ненадійним у разі його використання з метою забезпечення авторського права.

Метод ехо кодування має перевагу у стійкості до атак, проте наступні недоліки роблять його ненадійним у використанні з метою забезпечення авторського права аудіо об’єктів:

– метод є складним у реалізації;

– метод має високу ймовірність внесення у стеганоконтейнер спотворень, які будуть помітними;

– при використані методу виникають складності у відтворенні переданого повідомлення після отримання закодованого сигналу.

Метод фазового кодування не є придатним для передачі великих об’ємів даних та має високу ймовірність спотворення при невдалому виконанні алгоритму, що робить цей алгоритм ненадійним [22].

Метод LSB дає нам змогу використовувати його для підтвердження факту наявності авторського права, а також надає змогу передавати великі об’єми даних. Хоча він і має досить високу ймовірність спотворення початкового сигналу, що робить його не досить надійним, цей метод є одним з найоптимальніших для використання у різних форматах файлів.

Висновки за розділом 2

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

Було виявлено, що існує два основних напрямки вбудовування інформації, яка засвідчує факт належності даних власникові, а саме цифровий водяний знак та вшиття певного ідентифікаційного коду в файл.

Обидва напрямки мають свої переваги і недоліки, проте основною перевагою, яка допомагає нам визначити напрям, є те, що вбудовування водяного знаку має широку кількість алгоритмів , які, на відміну від надання індивідуального коду, не потребує отримання особливого ідентифікатору від певних організацій.

Алгоритми вбудовування цифрового водяного знаку можна поділити на форматні та неформатні, перевагою перших є відсутність спотворень у самому файлі, що не є притаманним для другого методу. Проте неформатний метод, незважаючи на недоліки, є більш стійким до різних видів атак, що робить його більш актуальним для використання задля вирішення поставленої проблеми.

До найбільш відомих методів вбудовування повідомлень у інформаційні об’єкти можна віднести наступні:

- методи з використанням формату файлу;
- LSB кодування;
- ехо кодування;

– фазове кодування.

Під час проведення дослідження було проведено порівняння зазначених методів та виявлено переваги і недоліки кожного з них. Аналіз алгоритмів дав змогу обрати метод, який буде найоптимальнішим та зручнішим під час вирішення поставленої проблеми.

Алгоритм ехо кодування вбудовує повідомлення в аудіо сигнал способом додавання в нього ехо сигналу. Для кодування послідовності значень використовують нерівномірні проміжки між тими ехо сигналами, які вже є наявними у контейнері. Метод має високу ймовірність внесення у стеганоконтейнер спотворень, які будуть помітним, через що цей метод не є оптимальним і майже не використовується.

Алгоритм фазового кодування полягає у використанні відносної фази (секретного повідомлення) для заміни вихідного звукового елемента. Недоліком цього методу є те, що він не придатний для передачі великих об’ємів даних.

Метод найменшого значущого біта або LSB-метод використовує надмірність файлів, тобто молодші (останні) значущі біти, в яких практично немає корисної інформації, для розміщення в них секретного повідомлення. Цей метод є простим для написання програмного забезпечення і не має значних обмежень по кількості можливої записаної інформації, що робить його дуже зручним для вирішення поставленої проблеми, а саме для побудови власного програмного забезпечення спрямованого на захист авторського права у аудіо об’єктах.

Проведені у даному розділі аналіз та порівняння дають змогу визначити наступні кроки проведення дослідження та безпосередньо реалізації програмного забезпечення:

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

2. необхідно визначити загальні характеристики алгоритму, який реалізується для вирішення проблеми;

3. необхідно навести приклад результату виконання написаного програмного забезпечення.

РОЗДІЛ 3
ЗАХИСТ АВТОРСЬКОГО ПРАВА В АУДІО ОБ'ЄКТАХ

3.1 Порівняльна характеристика мов програмування

Для написання програмного забезпечення для приховування у аудіо файлі цифрового водяного знаку з використанням обраного стеганографічного алгоритму спочатку необхідно вибрати мову програмування, для реалізації скрипта.

Отриманні раніше знання дають змогу виділити серед існуючих мов програмування три основні для порівняння та проведення аналізу, а саме Java, C# та Python. Для подальшого вибору виділимо три основні параметри порівняння:

- простота написання програмного забезпечення;
- можливості та обмеження при написанні скриптів;
- кількість можливих бібліотек доступних для використання.

Розглянемо перший параметр. Мова програмування Python має переваги через простоту свого синтаксису, адже синтаксис даної мови не є складним для читання, у той час як мови програмування C# та Java мають і синтаксичні дужки, і складні конструкції, і модифікатори. Синтаксис C# потребує чіткого дотримання встановлених правил при створенні будь-яких методів або при спадкуванні класів, на відміну від коду написаного на Python, який не створює складностей у розборі великої кількості конструкцій. Мова програмування Java у порівнянні з Python також є набагато складнішою мовою програмування, тому без роботи з якимись мовами програмування, буде складно вивчити цю мову програмування.

Розглянемо другий параметр. Під час проведення аналізу було виявлено, що мова C# є більш обмеженою ніж мова Python, адже написання першої можна здійснювати тільки у IDE, у той час як друга є сумісною з різними платформами. Інтегрованість та кроссплатформенність мови Python позбавляють розробників необхідності вибору середовища для написання скриптів. Щодо мови Java, можна зазначити, що вона теж дає можливість розробляти кросплатформенні додатки і є сумісною з багатьма операційними системами.

При розглядані третього параметру, порівнянні кількісті бібліотек, котрі мови програмування пропонують для використання, можна зазначити, що навіть велика кількість стандартних бібліотек C# програє у порівнянні з кількістю бібліотек з відкритим кодом, запропонованих Python, що спрощує використання даної мови програмування.

На даний момент Python є мовою програмування, що постійно розвивається, набуває більшої актуальності і це призводить до росту кількості IT спеціалістів, які при вивчені мов програмування та написанні скриптів обирають саме цю мову програмування. У якості прикладу можна навести Google чи Yandex.

Обрати кращу мову програмування серед інших неможливо, адже, з точки зору розвитку технологій і потребностей у написанні програмних забезпечень, кожна з мов має свої переваги і недоліки, які є необхідними для того чи іншого проекту.

Варто зауважити, що через простоту у написанні, час розробки з використанням мови програмування Python може бути приблизно у 3-4 рази меншим аніж час, необхідний для розробки додатків з використанням, наприклад, Java. Що, в принципі, і спричиняє виникнення все більшої популярності саме даної мови програмування у порівнянні з іншим, особливо, беручи до уваги для новачків у сфері написання скриптів.

Підведемо підсумки за трьома розглянутими параметрами:

– за простотою написання мова програмування Python має перевагу, адже окрім простоти вона ще має велику кількість літератури, в якій описані процеси написання скриптів чи розробки веб додатків, що значно спрощує процес навчання чи взагалі роботу з даною мовою програмування;

– щодо можливостей мов програмування для вирішення поставленої проблеми було обрано мову програмування Python через її:

– кросплатформеність, тобто наявність інтерпретаторів для великої кількості різних платформ, що дає змогу для використання мови на будь-якій операційній системі;

– наявність великої кількості сервісів, середовищ розробки та фреймворків;

– щодо можливості використання бібліотек, то мова програмування Python також має перевагу через велику кількість бібліотек, а у тому числі через можливість підключення бібліотек написаних мовами С, що підвищує ефективність проектів;

Отже, можна дійти висновку, що для написання програмного забезпечення, націленого на приховування цифрового водяного знаку, найбільш оптимальною буде мова програмування Python через свою кроссплатформенність, простоту та велику кількість запропонованих для використання бібліотек.

3.2Вимоги до програмного забезпечення

Проведені дослідження надають змогу сформувати точне технічне завдання на виготовлення програмного забезпечення для вирішення поставленої проблеми, а саме захисту авторського права в аудіо об’єктах.

Для формування технічного завдання на реалізацію сформуємо певні питання, які є важливими аспектами під час розробки, а саме:

– які особливості початкових даних, які ми маємо;

– що необхідно отримати по завершенні роботи програми;

– що вже наявне для успішного написання та виконання програми;

– яким є алгоритм роботи запланованого програмного забезпечення;

– які є вимоги до розроблюваного програмного забезпечення.

До особливостей початкового стеганоконтейнеру з назвою audio_clear.wav відноситься те, що це сигнал, тривалість якого складає тридцять секунд, розширення файлу є WAV та за розміром файл складає 5,765 Мб.

WAVE є одним із найпопулярніших форматів стиснення без втрат. Python має рідну бібліотеку під назвою «wave», яка надає нам основні інструменти для маніпулювання аудіо даними [25].

Обране стеганоповідомлення, у вигляді змінної формату string необхідно розмістити у встановлений стеганоконтейнер, вмістом змінної є текст: “Danilo Yashchenko 2022!”, розмір самого повідомлення складає 184 біти.

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 — 5,765 Мб.

Для виконання поставленої задачі використовується мова програмування Python для написання двох скриптів, один з яких буде вбудовувати у заданий сигнал обране повідомлення, а другий буде вилучати з заповненого стеганоконтейнеру розміщене у ньому стеганоповідомлення відповідно.

Для дослідження якості результату необхідно застосовувати програмне забезпечення, яке допоможе побудувати спектральну і часову діаграми оригінального сигналу та сигналу з вбудованим цифровим водяним знаком, щоб побачити явні зміни у аудіо-файлі. Провівши дослідження було з’ясовано, що програмним забезпеченням, яке буде задовольняти дану потребу є програма Izotope Rx.

Основні маніпуляції з бітами в LSB досить прості. Далі наведемо алгоритм виконування кодування обраним методом. Спочатку необхідно виконати логічну операцію AND між кожним байтом аудіо-носія і бітовою маскою, яка скидає LSB байт носія:

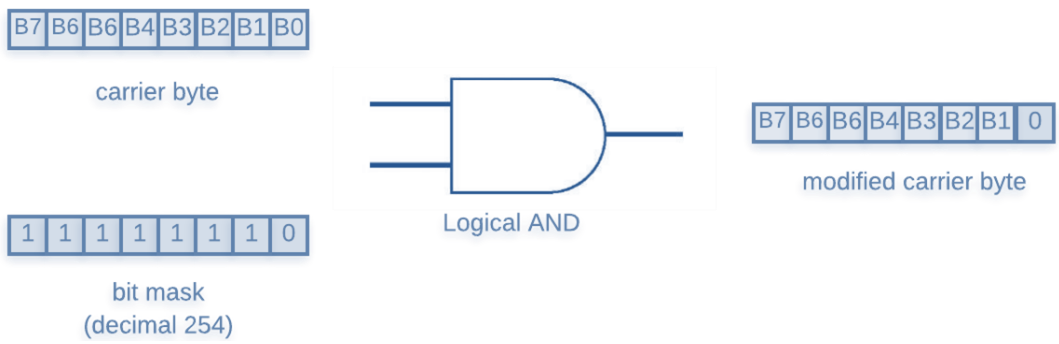

Рисунок 3.1 – Логічна операція AND між кожним байтом аудіо-носія і бітовою маскою

Потім ми виконаємо просту логічну операцію OR між модифікованим байтом-носієм і наступним бітом (0 або 1) із секретного повідомлення.

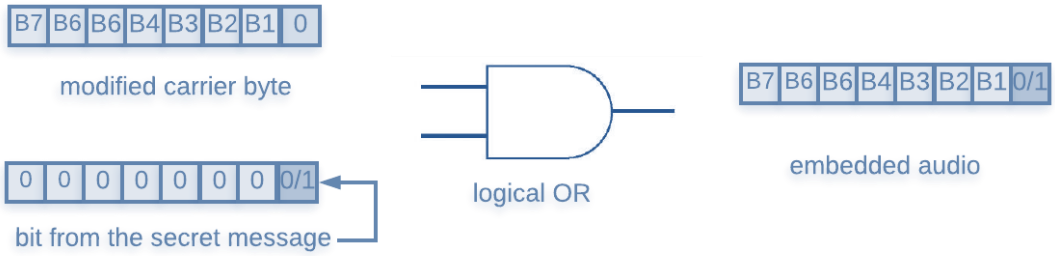

Рисунок 3.2 – Логічна операція OR між модифікованим байтом-носієм і наступним бітом

Отже головними вимогами до програмного забезпечення є:

- незмінність стеганоконтейнеру для органів чуття людини;
- незмінність розміру та основних властивостей стеганоконтейнеру;
- створення скрипту, спрямованого на вбудовування обраної мітки (цифрового водяного знаку), а також на його вилучення.

3.3 Результат виконання прописаного алгоритму

Маємо початковий стеганоконтейнер з назвою audio_clear.wav, до особливостей якого відноситься те, що це сигнал, тривалість якого складає тридцять секунд, розширення файлу є WAV та за розміром файл складає 5,765 Мб.

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

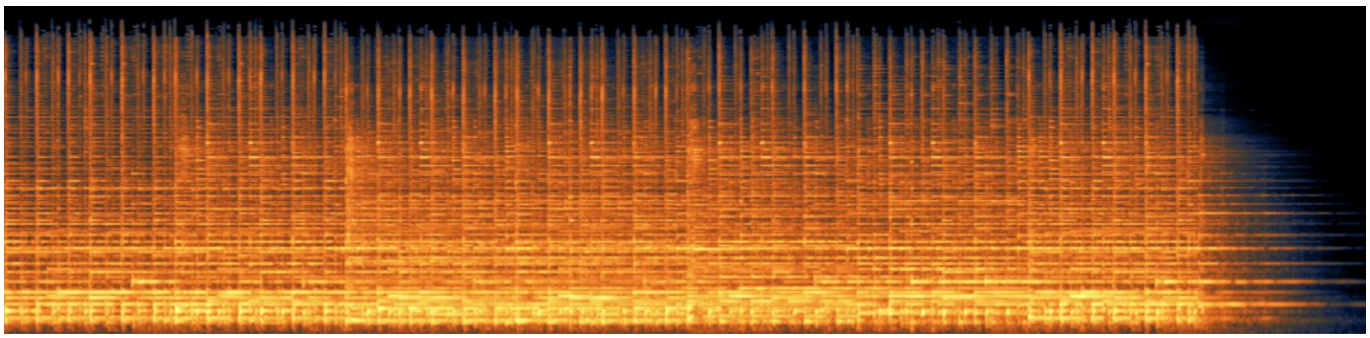

Рисунок 3.3 – Спектральна діаграма для порожнього стеганоконтейнеру.

Та будуємо часову діаграму оригінального сигналу:

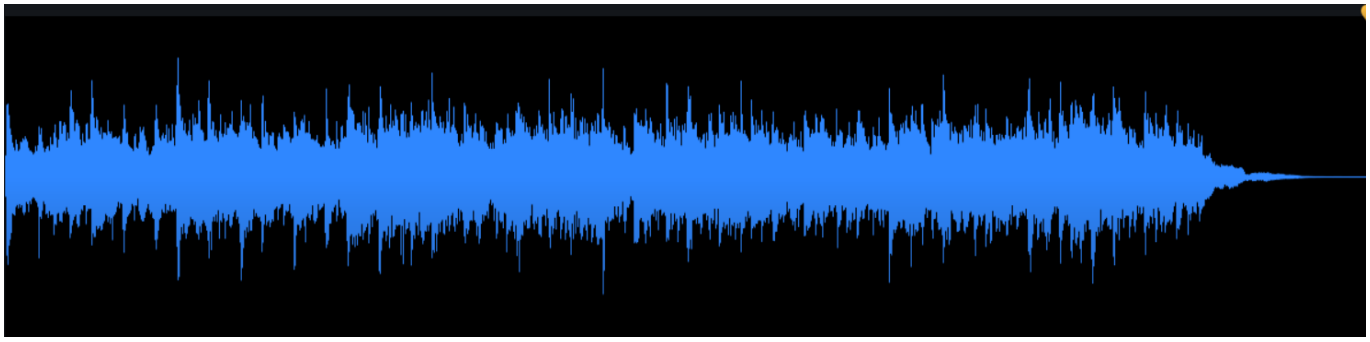

Рисунок 3.4 – Часова діаграма для порожнього стеганоконтейнеру

Далі, відповідно до поставленої задачі, необхідно здійснити приховування обраного стеганоповідомлення, розміщеного у змінній з розміром 184 біти, а саме:

“ Danilo Yashchenko 2022!”

Наступним кроком розглянемо, як змінилися спектральна і часова діаграми заданого стеганоконтейнеру після вбудовування в нього стеганоповідомлення, задля виявлення значних змін в отриманому файлі.

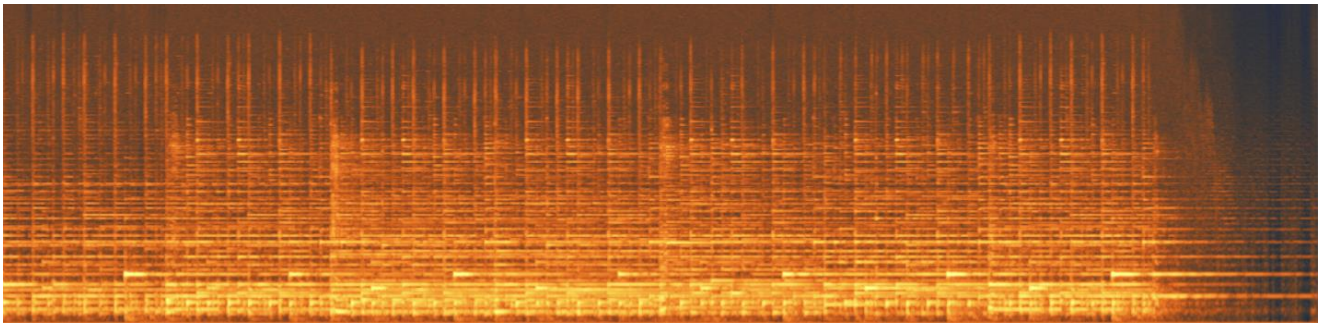

Рисунок 3.5 – Спектральна діаграма для заповненого стеганоконтейнеру

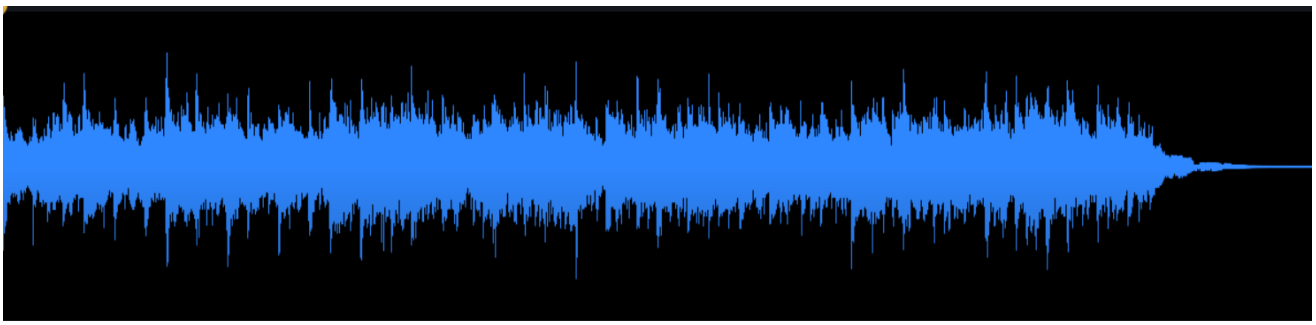

Рисунок 3.6 – Часова діаграма для заповненого стеганоконтейнеру

З наведених діаграм бачимо, що модифікація була здійснена для вбудовування повідомлення довжиною 184 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 кількості замін бітів у файлі.

Для отримання наглядного прикладу такого аудіо об’єкту використаємо цифровий водяний знаку розміром 15 мегабайт.

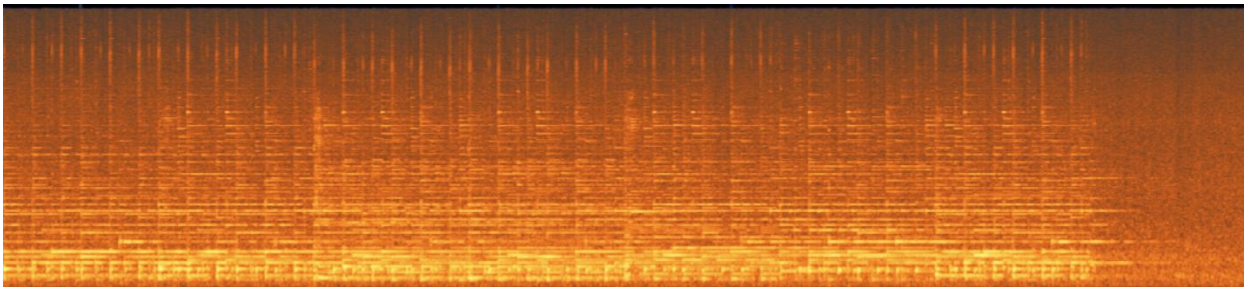

Рисунок 3.7 – Спектральна діаграма переповненого стеганоконтейнеру

Рисунок 3.8 – Часова діаграма порожнього та наповнених стеганоконтейнерів

Далі наведемо порівняльний приклад часової та спектральної діаграм:

Рисунок 3.9 – Спектральна діаграма порожнього та наповнених стеганоконтейнерів

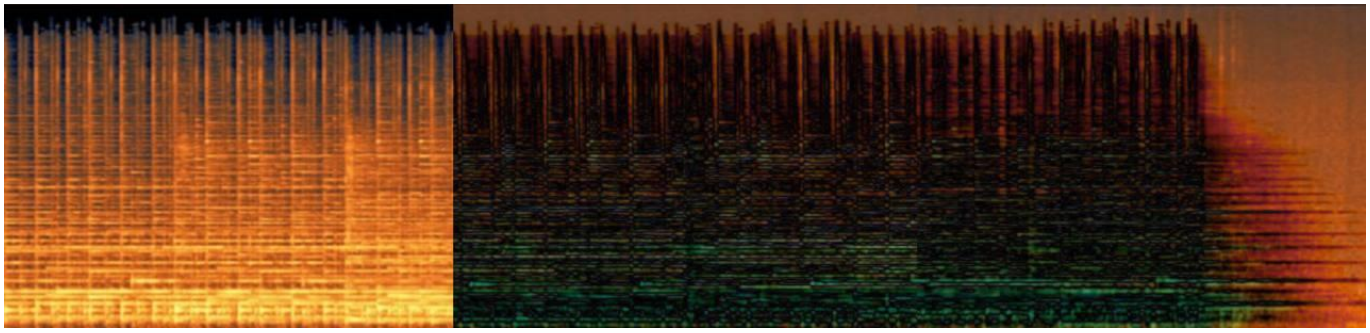

Рисунок 3.10 – Часова діаграма порожнього та наповнених стеганоконтейнерів

На рисунках наведено часову та спектральну діаграми порожнього стеганоконтейнеру, контейнеру з повідомленням оптимального розміру та контейнеру наповненого міткою занадто великого розміру накладену поверх діаграми порожнього.

Судячи з проведених досліджень можна зазначити, що аудіо контейнер з розміщеним у ньому ЦВЗ, відповідним до оптимальних умов, є не відмінним від оригінального контейнеру.

Проведене дослідження з використання методу LSB кодування доводить, що використання цього або подібних програмних продуктів є ефективним.

Висновки за розділом 3

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

Першим кроком було проведено порівняльну характеристику мов програмування C#, Java та Python. Порівняння мов програмування було проведене за трьома основними параметрами, а саме:

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

Внаслідок проведених досліджень було з'ясовано, що для написання програмного забезпечення, спрямованого на приховування ЦВЗ у файлі формату WAV, мова програмування Python буде найбільш оптимальною через свою кроссплатформенність, простоту та велику кількість запропонованих для використання бібліотек.

У даному розділі було визначено загальні характеристики реалізованого програмного забезпечення та вхідних даних і вихідних даних. Далі наведемо особливості порожнього стеганоконтейнеру, а саме те що вхідним у нас є аудіо сигнал, тривалість якого складає тридцять секунд, розширення файлу є WAV та його розмір складає 5,765 Мб.

Далі було зазначено особливості стеганоповідомлення, яке необхідно було розмістити у встановлений стеганоконтейнер. До них належить вміст стеганоповідомлення: "Danilo Yashchenko 2022!", формат змінної — string і розмір самого повідомлення — 184 бітів.

Було наведено алгоритм виконання створеного програмного забезпечення та зазначено його головні вимоги, а саме:

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

У цьому розділі було наведено приклад виконання створених скриптів, які розміщують та вилучають цифровий водяний знак в та з обраного аудіо файлу або стеганоконтейнеру.

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 — 5,765 Мб. Також було наведено приклад роботи обраного алгоритму з використанням стеганоповідомлення, яке не відповідає оптимальним умовам.

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 перших етапах проведення дослідження було висвітлено основні терміни, а також визначення, додатково стало ясним, що більша частина термінології котра стосується авторського права тлумачиться у Законі України “Про авторське право та суміжні права”. За регулювання діяльності напрямку стеганографічного захисту частково відповідає Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”. Також було виділено, що в Україні є потреба доопрацювання нормативно правової бази у сфері стеганографічного захисту.

Згідно з наведеними вище нормативно-правовими джерелами було визначено, що авторське право — це особисті немайнові права і майнові права авторів та їх правонаступників, пов’язані зі створенням та використанням творів науки, літератури й мистецтва, а стеганографія — це спосіб приховування секретного повідомлення всередині (або навіть поверх) об’єкту, що не є секретним. Для прикладу, у простій реалії сьогодення, стеганографія розрахована для вбудування секретного тексту всередину малюнка, або Word документа. Таке вбудування не готовому користувачеві є зазвичай не помітним.

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. Стеганографію можна розглядати як одну з форм спілкування, але прихованого. Додатково було виділено що стеганографія не визначається як різновид криптографії, а є окремим напрямком.

У ході дослідження було наведено велику кількість історичних аспектів використання методів стеганографії, простим прикладом можна вважати невидимі чорнила. Проте в сьогоденні ця наука все як і інші переходить в більш технічний

напрямок, впроваджуючи нові технології захисту, які вже відносять до поняття цифрової стеганографії.

Напрямок саме цифрової стеганографії 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.

Вшиття в файл індивідуального коду дає об’єкту певний ідентифікатор, по якому далі можна відділяти об’єкт. З іншої сторони вбудовування водяних знаків має більшу кількість певних алгоритмів, задачею яких стає - помістити цифровий водяний знак в об’єкт. Ці методи та алгоритми поділяються на так звані форматні та неформатні. Форматні використовуються при вбудовуванні в об'єкт особливості формату файлу, а неформатні не використовують . Форматний метод має одну велику перевагу, під час його використання цього методу, зміни вносяться в службові поля, котрі ніяк не відображаються на самому файлі. А використання неформатних методів, дає в результаті певні спотворення в початковому файлі, проте цей метод все одно вважається більш стійким до атак.

У розгляді даної роботи перевагу було надано вивченню особливостей та проведення аналізу і порівняння методів цифрової стеганографії:

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

Щоб вирішити завдання дипломної роботи потрібно більш детально дослідити методи аудіо стеганографії. З проведених досліджень було зроблено наступні висновки для ефективної стеганографічної схеми:

- надійність;
- не чутність спотворень.

Метод LSB (Least Significant Bit, найменший значущий біт) кодування — це класичний метод стеганографії, який використовується для приховування існування секретних даних всередині «публічної» обкладинки. Цей метод використовує надмірність файлів або молодші значущі біти для розміщення в них повідомлення. Така заміна майже не впливає на файл і не створює значних помітних спотворень

Серед вивчених методів було обрано метод LSB, цей метод полягає в використанні надмірності файлів або молодших значущих бітів для розміщення в них повідомлення. Така заміна майже не впливає на файл і не створює значних помітних спотворень. Основною перевагою методу LSB можна вважати великий обсяг переданих даних. Проте 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.

Наступним кроком дипломної роботи було вирішення практичної частини завдання, а саме створення програмного забезпечення, яке практично реалізує обраний метод.

Для вирішення поставленої задачі було проаналізовано та вирішено покрокові завдання:

- досліджено різні мови програмування, які дають можливість створити практичну реалізацію;
- було наведено та досліджено алгоритм LSB кодування;
- розроблено практичну реалізацію програм, котра вирішує поставлену задачу.

Для перевірки створеного коду було проведено практичні досліди на аудіо файлі. Обрано було невеликий стеганокотейнер, 30 секунда пісня в форматі WAV та водяний знак, текст якого обирає користувач під час запуску скрипту. Також за допомогою створеного скрипта було досліджено якість відтворення розміщеного у стеганоконтейнері секретного повідомлення. Та перевірено як і запис так і отримання секретного повідомлення.

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. Lowe D.G. Distinctive image features from scale-invariant keypoints / D.G. Lowe // International journal of computer vision. – 2004. – Vol. 60, №2. – P. 91–110.

5. Задірака В.К. Спектральні алгоритми комп’ютерної стеганографії / В.К. Задірака, С.С. Мельнікова, Н.В. Бородавка //Искусственный интеллект. – 2002. – № 3. – С. 532 –541.

6. Avcibas I. Image steganalysis with binary similarity measures / I. Avcibas¸ M. Kharrazi, N.D. Memon, B. Sankur //EURASIP Journal on Applied Signal Processing. – 2005. – P. 2749–2757.

7. Швідченко І.В. Аналіз програмного забезпечення зі стеганоаналізу / І.В. Швідченко //Искусственный интеллект. – 2012. – №3. – С. 487–495.92

8. Li F. JPEG steganalysis with high-dimensional features and bayesian ensemble classifier / F. Li, X. Zhang, B. Chen, G. Feng //IEEE signal processing letters. – 2013. – Vol. 20, № 3. – P. 233–236.

9. Yang S. Quantization-Based Digital Audio Watermar-king in Discrete Fourier Transform Domain / S. Yang, W. Tan, Y. Chen, W. Ma // Journal of Multimedia. – 2010. – Vol. 5, № 2. – P. 151–158.

10. Yang X. Universal image steganalysis based on wavelet packet decomposition and empirical transition matrix in wavelet domain / X. Yang, Y. Lei, X. Pan, J. Liu // International forum on computer science-technology and applications. – 2009. – Vol.2. – P. 179–182.

11. Sheikhan M. Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform / M. Sheikhan, M.S. Moin, M. Pezhmanpour //10th Int. Conf. on Intelligent Systems Design and Applications. – 2010. – P. 368–372.

12. Avcibas I. Image steganalysis with binary similarity measures / I. Avcibas¸ M. Kharrazi, N.D. Memon, B. Sankur //EURASIP Journal on Applied Signal Processing. – 2005. – P. 2749–2757.

13. Кошкіна Н.В. Стійкі до активних атак методи комп'ютерної стеганографії / Н.В. Кошкіна // Вісн. НАН України. – 2013. – № 4. – С. 61–66.

14. Кошкіна Н.В. До питання часо-частотного аналізу сигналів в задачах комп'ютерної стеганографії / Н.В. Кошкіна // Праці міжнар. конф. "Питання оптимізації обчислень-XXXVI. Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України. – 2011. – Том 1. – С. 351–355.

15. Мелешко Е.В. Метод встраивания двухуровневых цифровых водяных знаков в медиафайлы для защиты авторских прав / Е.В. Мелешко // Збірник наукових праць Харківського університету Повітряних Сил. – 2013. – № 4. – С. 127-131.

16. Suresh A. Image Texture Classification using Gray Level Co-Occurrence Matrix Based Statistical Features / A. Suresh, K.L. Shunmuganathan // European Journal of Scientific Research. – 2012. – Vol.75, № 4. – P. 591–597

17. Voloshynovskiy S.V. Visual communications with side information via distributed printing channels: extended multimedia and security perspectives / S.V. Voloshynovskiy, O. Koval, F. Deguillaume, T. Pun // Proc. of SPIE: Security, 93 Steganography, and Watermarking of Multimedia Contents VI, San Jose, USA, January 2004. – P. 428–445.

18. Lin C.-Y. Distortion Modeling and Invariant Extraction for Digital Image PrintandScan Process / C.-Y. Lin, S.-F. Chang // Intl. Symp. On Multimedia Information Processing, Taipei, December 1999. [Електронний ресурс]. — Режим доступу до документа http://www.ee.columbia.edu/ln/dvmm/publications/99/cylin-modelscan.pdf.

19. Методика використання інформаційно-комунікаційних технологій у навчальному процесі. Ч.4. Проектування методів управління навчальною

діяльністю:начальний посібник / Стариченко Б.Е., Коротаєва Е.В., Сардак Л.В., Єгоров А.Н. , Під ред. Стариченко Б.Е. Єкатеринбург: 2013. 141 с

20. Задирака В.К. К вопросу стойкости стеганосистемы при пассивных атаках / В.К. Задирака, Л.Л. Никитенко // Междунар. научно-техн. журнал «Проблемы управления и информатики». – 2009. – № 2. – С. 138 – 139.

21. PyCharm: the Python IDE for Professional Developers by JetBrains [Електронний ресурс] — Режим доступу: https://www.jetbrains.com/pycharm

22. 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

23. ECTS Users Guide. Office for Official Publications of the European Communi-ties: Luxembourg, 2009. [Електронний ресурс] – Режим доступу до ресурсу: http://ec.europa.eu/education/lifelong-learning-policy/doc/ects/guide_en.pdf

24. Chiu Y.-C. Copyright Protection against Print-and-Scan Operations by Watermarking for Color Images Using Coding and Synchronization of Peak Locations in Frequency

25. 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

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

27. Романчук Р.О., Поліщук А.О. Вплив стеганографії та схеми розподілу секрету зображень на безпеку криптографічного ключа / Матеріали міжнародної наукової конференції «Актуальні наукові дослідження в сучасному світі», 26-27 грудня 2017 р. – С. 27-33.

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

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИПЛОМУ

Тези наукових доповідей:

1. С.Ю. Даков, Д.М. Ященко, А.Є. Рогачова. Забезпечення інформаційної безпеки за рахунок стандартів ISO/IEC. III МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (PCSITS). – 2020. – С. 251

ДОДАТОК Б
МЕТОДИКА ВИКОНАННЯ ДИПЛОМНОЇ РОБОТИ

Програмний код для вшивання даних у аудіо файл

```
import wave
song = wave.open("audio_clear.wav", mode='rb')
frame_bytes = bytearray(list(song.readframes(song.getnframes())))
inputmessage = input("Enter a secret message: ")
inputmessage = inputmessage + int((len(frame_bytes)-(len(inputmessage)*8*8))/8)
*'*'
bits = list(map(int, ''.join([bin(ord(i)).lstrip('0b').rjust(8,'0') for i in inputmessage])))
for i, bit in enumerate(bits):
    frame_bytes[i] = (frame_bytes[i] & 254) | bit
frame_modified = bytes(frame_bytes)
with wave.open('audio_coded.wav', 'wb') as frame:
    frame.setparams(song.getparams())
    frame.writeframes(frame_modified)
song.close()
print("Text imported to audio")
```

Програмний код для вилучення даних з аудіо файлу

```
import wave
song = wave.open("audio_coded.wav", mode='rb')
frame_bytes = bytearray(list(song.readframes(song.getnframes())))
extracted_info = [frame_bytes[i] & 1 for i in range(len(frame_bytes))]
string_text = "".join(chr(int("".join(map(str,extracted_info[i:i+8])),2)) for i in
range(0,len(extracted_info),8))
```

```
decoded = string_text.split("***")[0]
print("Decoded information: "+decoded)
song.close()
```