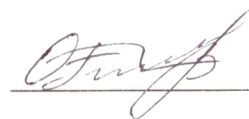


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ

ПОЯСНЮВАЛЬНА ЗАПИСКА

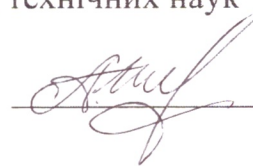
до випускної кваліфікаційної роботи магістра
на тему: «Методи та технології стеганографічного захисту інформації»

Виконав студент 2-го курсу групи ЗКбм-22-1
спеціальності 125 «Кібербезпека»



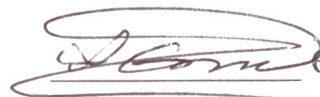
Опанасюк Г.В.

Керівник доцент кафедри комп'ютерної інженерії
та кібербезпеки, кандидат технічних наук



Шелуха О.О.

Рецензент завідувач кафедри комп'ютерної інженерії та
кібербезпеки, кандидат технічних наук, доцент



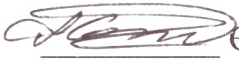
Єфіменко А.А.

Житомир – 2023

ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА КІБЕРБЕЗПЕКИ
СПЕЦІАЛЬНІСТЬ 125 «КІБЕРБЕЗПЕКА»

ЗАТВЕРДЖУЮ

Завідувач кафедри
комп'ютерної інженерії
та кібербезпеки

 Сфіменко А.А.
«13»  2023 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу

Студента Опанасюка Григорія Васильовича

Тема роботи: Методи та технології стеганографічного захисту інформації

Затверджена Наказом університету від 13 жовтня 2023 р. № 573/с

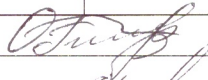
Термін здачі студентом закінченої роботи 25 грудня 2023 р.

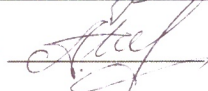
Вихідні дані роботи:

1. Літературні джерела із стеганографії
2. Програмне забезпечення для практичної реалізації

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів,
що їх стосуються

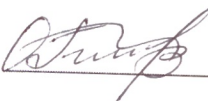
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	В.В. Воротніков	13.10.2023	13.10.2023
2	В.В. Воротніков	10.11.2023	10.11.2023
3	В.В. Воротніков	01.12.2023	01.12.2023

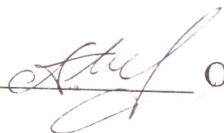
Студент  Г.В. Опанасюк

Керівник  О.О. Шелуха

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	01.11.2023 – 03.11.2023	Виконано
2	Розробка вимог до проекту	04.11.2023 – 06.11.2023	Виконано
3	Аналіз актуальності застосування стеганографічних методів	10.11.2023 – 13.11.2023	Виконано
4	Аналіз стеганографічних методів	15.11.2023 – 17.11.2023	Виконано
5	Розгляд методів комп'ютерної стеганографії	18.11.2023 – 23.11.2023	Виконано
6	Практична реалізація	24.11.2023 – 1.12.2023	Виконано
7	Аналіз результатів	3.12.2023 – 4.12.2023	Виконано
8	Написання пояснювальної записки	5.12.2023 – 9.12.2023	Виконано
9	Підготовка презентації	10.12.2023 – 12.12.2023	Виконано
10	Захист	25.12.2023	Виконано

Студент  Г.В. Опанасюк

Керівник  О.О. Шелуха

АНОТАЦІЯ

У кваліфікаційній роботі 39 сторінок, 9 рисунків та 26 літературних джерел.

Метою кваліфікаційної роботи є вивчення та реалізація основних методів вбудовування стеганографічних повідомлень та застосування цифрових водяних знаків.

У кваліфікаційній роботі отримано такі результати:

- 1) Реалізовано метод вставки молодшого біта для контейнерів великого і малого розмірів,
- 2) Реалізовано метод приховування бінарних даних у HTML-документі,
- 3) Реалізовано впровадження водяного знака в PDF-документ.

Кваліфікаційна робота має практичний характер. Її результати можуть бути використані для впровадження та вилучення цифрових водяних знаків і прихованих повідомлень у зображеннях і цифрових документах.

ЦИФРОВИЙ ВОДЯНИЙ ЗНАК, СТЕГANOГPAФІЯ, ВЕЙВЛЕТ-ПЕРЕТВОРЕННЯ, КОНТЕЙНЕР, СТЕГОПОВІДОМЛЕННЯ.

ANNOTATION

The qualified work has 39 pages, 9 drawings and 26 literary pieces.

The method of qualified work is the development and implementation of basic methods for the creation of steganographic information and the creation of digital watermarks.

The following results were obtained from qualified robots:

- 1) The method of inserting a young bit has been implemented for containers of large and small sizes,
- 2) A method for capturing binary data from an HTML document has been implemented,
- 3) Adding a watermark to a PDF document has been implemented.

Qualified work is practical in nature. The results can be used to develop and obtain digital watermarks and information on images and digital documents.

DIGITAL WATERMARK, STEGANOGRAPHY, WAVELET TRANSFORMATION, CONTAINER, STEGOGRAPHY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	7
ВСТУП	8
РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМАТИКИ ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ.....	10
1.1 Аналіз актуальності застосування стеганографічних технологій	10
1.2 Аналіз стеганографічної термінології	11
1.3 Цифрова стеганографія	13
1.3.1 Методи цифрової стеганографії	13
1.3.2 Цифрові відбитки.....	14
1.3.3 Стеганографічні водяні знаки.....	14
1.3.4 Цифрові водяні знаки	15
1.4 Практичне застосування стеганографії	16
Висновок до розділу 1	18
РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ СТЕГANOГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ.....	19
2.1 Комп'ютерна стеганографія	19
2.2 Вбудовування в молодші біти контейнера.....	20
2.3 Вбудовування бінарних даних в HTML-документ.....	23
2.4 Математичні методи.....	24
Висновки до розділу 2	28
РОЗДІЛ 3 РЕАЛІЗАЦІЯ МЕТОДІВ ВБУДОВИ	29
3.1 Метод вставки молодшого біта	29
3.2 Застосування стеганографічних методів у HTML-документі	31
Висновки до розділу 3	35
ВИСНОВКИ.....	36
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	37

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КС – комп’ютерна стеганографія

ЦС – цифрова стеганографія

ЦВЗ – цифровий водяний знак

ЦВ – цифровий відбиток

СВЗ – стеганографічний водяний знак

СЕДО – система електронного документообігу

HTML – HyperText Markup Language

DLP – Data Leak Prevention

ПХ – перетворення Хаара

ВСТУП

Актуальність теми. З появою комп'ютерної технології захист особистої та корпоративної інформації стає критично важливим.

Комп'ютерна стеганографія вивчає використання елементів та особливостей сучасного програмного забезпечення та обчислювальної техніки для приховування інформації. Основана на двох принципах: можливість змін в файлах, де точність не обов'язкова (зображення), та невідмінність для людських органів чуття невеликих змін у відредагованих файлах. Основні методи включають виділення малозначущих фрагментів середовища та заміну їх іншими даними з метою приховування інформації.

Дослідження методу вставки молодшого біта в контейнери різних розмірів як способу захисту від несанкціонованого доступу.

Розробка методу приховування бінарних даних у HTML-форматі для додаткового захисту електронних ресурсів.

Аналіз та впровадження багаторівневого вейвлет-перетворення як ефективного методу внедрення водяних знаків в PDF-документи.

Під час дослідження активно використовувались PNG-зображення, текстові контейнери та HTML-розмітка.

У першому розділі роботи розкривається предмет дослідження - концепція стеганографії, її ключові поняття та методи. У другому розділі обговорюється об'єкт дослідження - методи вставки молодшого біта, впровадження бінарних даних у HTML і багатовимірне вейвлет-перетворення. У третьому розділі детально аналізується конкретна реалізація цих методів в рамках кваліфікаційної роботи.

Мета кваліфікаційної роботи. Мета роботи полягає в дослідженні методів та технологій комп'ютерної стеганографії, та побудови на його основі практичних засобів вбудовування прихованих повідомлень в зображення та захист файлі за допомогою водяних знаків.

Для досягнення поставленої мети було сформульовано наступні завдання:

1. Розглянути та визначити основні методи прихованої передачі повідомлень.

2. Провести аналіз методів комп'ютерної стеганографії, вбудовування прихованих повідомлень та захисту файлів від копіювання.

3. Розробити засоби для практичної реалізації методів вбудовування прихованих повідомлень в зображення та захисту файлі за допомогою водяних знаків.

Об'єктом дослідження є процес модифікації інформації для прихованої передачі, зберігання та захисту від несанкціонованого копіювання.

Предметом дослідження є методи стеганографічного захисту інформації та технології їх практичної реалізації.

РОЗДІЛ 1. АНАЛІЗ ПРОБЛЕМАТИКИ ПРИХОВАНОЇ ПЕРЕДАЧІ ДАНИХ

1.1 Аналіз актуальності застосування стеганографічних технологій

Протягом усієї історії нашої цивілізації існувала проблема захищеної передачі даних. З давніх часів людство використовувало тайнопис та моноалфавітні шифри для захисту своїх повідомлень. В цей час з'явилися перші приклади стеганографії, тобто приховування інформації в зображеннях [1,2].

Розвиток комп'ютерної техніки призвів до появи стеганографії та криптографії. З'явилися нові напрямки стеганографії та методи вбудовування інформації. Мобільні термінали, такі як смартфони і планшети, внесли свій внесок у розвиток стеганографії. Різноманіття контейнерів для приховування інформації, шляхів передачі та популярність мобільних платформ підкреслюють актуальність розвитку стеганографічних методів.

Стеганографія є методом організації зв'язку, який вміщує у себе приховання самого факту комунікації [2]. У відмінну від криптографії, де ворог може точно визначити, чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в безпечні передачі так, щоб неможливо було підозрювати наявність вбудованого таємного повідомлення.

Термін "стеганографія" у перекладі з грецької буквально означає "тайнопис" (steganos – секрет, таємниця; graphy – запис). Цей метод включає в себе різноманітні засоби зв'язку, такі як невидиме чорнило, мікрофотознімки, умовне розташування знаків, таємні канали та засоби зв'язку на плаваючих частотах і так далі. Стеганографія займає своє місце в сфері безпеки, доповнюючи криптографію. Приховування повідомлення методами стеганографії суттєво зменшує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення ще й зашифровано, воно отримує додатковий рівень захисту.

Отже, що є стеганографією? Стеганографія включає в себе процедури та технології, способи та методи приховування конфіденційних даних в зображеннях

з метою приховування факту існування таємних даних при передачі, зберіганні або обробці зображення.

Останні роки відзначають відродження стеганографії через широке поширення технологій мультимедіа. Розвиток цифрових технологій спричинив появу нових каналів передачі інформації, що в свою чергу призвело до розвитку і удосконалення стеганографії та цифрових водяних знаків [1].

Найпоширеніші стеганографічні методи використовують просторову область зображення чи область його перетворення для приховування інформації. У сучасних областях застосування стеганографічних методів, пов'язаних з прихованою передачею даних та мультимедійними технологіями, існує широкий спектр застосувань. Кожен програмний продукт висуває вимоги до методу вбудовування даних, і важливо враховувати, що різні стеганографічні методи мають свої переваги та недоліки для конкретних областей використання.

Оцінка стеганографічних методів та технологій стає важливою проблемою.

1.2 Аналіз стеганографічної термінології

Стеганографія визначає ключові принципи вбудовування інформації: забезпечення аутентичності та цілісності файлів, врахування відомостей про можливі методи атак та підтримка базових властивостей вихідних файлів. Задача викликати обчислювальні труднощі при вилученні секретного повідомлення покладається в основу безпеки. Стеганографія, як напрямок, зазнає активного розвитку, і хоча термінологія не є повністю сформованою, її основні поняття визначено вже на початку 90-х років.

Ключові положення для вбудовування інформації включають наступне:

- 1) Методи приховування повинні забезпечувати автентичність та цілісність файлу.
- 2) Припускається, що можливі стеганографічні методи добре відомі потенційному атакуючому.

3) Безпека методів повинна базуватися на збереженні основних властивостей відкритого файлу, що передається стеганографічним перетворенням.

4) Вилучення секретного повідомлення повинно ускладнювати обчислювальну задачу для противника, навіть якщо він знає про сам факт приховування.

Стеганографія, як самостійний напрямок, виділилася недавно, тому повністю сформованої термінології поки що немає. Основні поняття стеганографії були сформульовані на 1-й Міжнародній конференції з приховування даних в 1996 році.

Визначимо основні терміни що узагальнюють основні поняття прихованої передачі інформації:

- Скрита (стеганографічна) передача інформації - це процеси передачі інформації, при яких можлива як передача, так і зберігання додаткової інформації в структурі цифрових даних, які використовуються як контейнер завдяки своїй зайвості.

- Контейнер - це певні цифрові дані, використання зайвості яких дозволяє передавати додаткову інформацію, не виявляючи самого факту передачі.

- Порожній контейнер - контейнер, який не має жодної додаткової інформації, окрім, можливо, ініціалізаційних даних.

- Стегосистема - це сукупність засобів та методів передачі та прийому порожнього контейнера, які функціонують взаємозалежно від засобів, використовуваних для створення прихованого каналу передачі інформації.

Також можна розширити існуючі визначення наступними:

- Заповнений контейнер - контейнер, який має вбудовану певну інформацію.
- Приховане повідомлення (стегоповідомлення) - повідомлення, вбудовуване в контейнер.

- Стегоканал - канал передачі прихованого повідомлення.

- Стегоключ - секретний ключ, необхідний для сховування інформації та, відповідно, отримання її.

Різні типи файлів можуть виконувати функцію контейнера, включаючи:

1) Текстові файли,

- 2) Графічні файли,
- 3) Аудіо файли,
- 4) Електронні документи та інші.

Ці файли містять інформацію, яку можна трошки змінити так, щоб ця зміна залишалася непомітною для людських органів чуття, але водночас була достатньою для виявлення програмою-обробником. Вибір саме цих файлових типів базується на цьому принципі.

1.3 Цифрова стеганографія

Термін "цифрова стеганографія" представляє собою науку про надійне приховування одних послідовностей бітів в інших бітових послідовностях, які мають аналогову природу. Тут "незамітність" передбачає включення людини в стегосистему, "надійність" - стійкість до спотворень різних видів, а "аналогова природа" - вбудовування в оцифрований неперервний сигнал. Людина розглядається як додатковий приймач інформації, який висуває до стегосистеми досить важко формалізовані вимоги.

У українокомовних працях, присвячених стеганографічній науці, часто використовується термін "цифровий водяний знак" (ЦВЗ). Під цим розуміють або стеганографічний водяний знак (СВЗ), або цифровий відбиток (ЦВ) (іноді і СВЗ, і ЦВ одночасно). Виникають проблеми та завдання при реалізації ЦВ і СВЗ, які принципово відрізняються. Зокрема, СВЗ однаковий у всіх копіях електронного документа, тоді як ЦВ різниться у всіх копіях документа.

1.3.1 Методи цифрової стеганографії

В останні роки цифрова стеганографія розвивається як окрема наукова галузь. У ній виділяються наступні напрямки:

- Вбудовування інформації з метою її передачі,
- Вбудовування цифрових водяних знаків,
- Вбудовування ідентифікаційних номерів,

- Вбудовування заголовків.

Окремою класифікаційною групою серед методів стеганографії є внесення цифрових водяних знаків та організація стежоканалів з використанням шумоподібних сигналів (ШПС), які також називають методами з розширенням спектра. Порівняно з вбудовуванням у частотну та просторову області, в цьому випадку модифікується всі зображення в цілому. Адже змінюються лише елементи та коефіцієнти, де людське око з менше чутливе, або такі, що змінення статистики зображення є менш помітним.

1.3.2 Цифрові відбитки

Дана форма стеганографії передбачає наявність стеганографічних міток-повідомлень у кожній копії контейнера. Наприклад, цифрові водяні знаки (ЦВ) можуть використовуватися для захисту виключного права. Якщо противник за допомогою якого-небудь алгоритму може видобути ЦВ з контейнера, то визначити його буде неможливо. Поки противник не буде підробляти ЦВ, він не зможе розповсюджувати захищений контейнер без виявлення факту. Таким чином, при видобутті ЦВ третя сторона може мати за мету досягнення двох цілей:

- 1) Видобуття ЦВ з контейнера (слабка мета),
- 2) Підробка одного ЦВ іншим ЦВ (сильна мета).

1.3.3 Стеганографічні водяні знаки

Дана форма стеганографії в порівнянні з ЦВ, передбачає наявність однакових міток у кожній копії контейнера. СВЗ також можна використовувати для підтвердження авторських прав.

1.3.4 Цифрові водяні знаки

Стеганографія, особливо застосування цифрових водяних знаків (ЦВЗ), надає значні переваги у збереженні та захисті електронної інформації. Вбудовання невидимих меток в об'єкт захисту є ефективним засобом захисту від крадіжок та модифікацій. Розробка методів ЦВЗ тільки розпочалася, і виникає багато невизначених проблем, які потребують ретельного вирішення.

Цифрові водяні знаки можуть містити інформацію власника, аутентичний код або управлінську інформацію. Файли аудіо- та відеоданих, а також нерухомі зображення є найбільш підходящими об'єктами для застосування ЦВЗ.

Термін "цифрова стеганографія" отримав своє розв'язання як засіб захисту цінних документів, у тому числі грошей від підробки. ЦВЗ можуть бути як видимими, так і невидимими, відрізняючись від звичайних водяних знаків.

ЦВЗ представляє собою один з найпопулярніших напрямків, що отримало розвиток останнім часом. Це обумовлено потребою взаємодії з несанкціонованою поширенням інформації, яка є інтелектуальною власністю. Організація стеганографічних каналів стає актуальною для організацій, де забезпечення безпеки є пріоритетним вимогам.

Основні цілі при використанні ЦВЗ різняться, і основні вимоги до розроблюваних методів стеганографії мають ряд відмінностей. Як інструмент захисту від несанкціонованого доступу, ЦВЗ не вимагає обов'язкового розкриття факту їх вбудовування, відмінності в робастності стають основним аспектом. Головним видом атак у цьому випадку є геометрична атака.

Однією з ключових вимог при організації прихованого каналу є його непомітність, і, відповідно, основними атаками є візуальна атака та статистичний аналіз. Забезпечення достовірності прийому прихованих даних та прихованої пропускної спроможності залишається завданням, що вимагає уваги, і відрізняється від забезпечення відсутності залежності від вигляду передаваних повідомлень.

1.4 Практичне застосування стеганографії

Далі будуть наведені завдання, для яких стеганографія буде актуальною:

1) Непомітна передача інформації. Непомітна передача інформації через стеганографію стає важливою, особливо у порівнянні з криптографічними методами, які, хоча забезпечують конфіденційність, все ж не гарантують абсолютної непомітності. Це "класично практичне застосування" стеганографії, яке дозволяє надійно та непомітно передавати інформацію.

2) Приховане зберігання інформації. Приховане зберігання інформації через стеганографію використовується не лише для передачі, але й для безпечного зберігання даних. Виявлення цієї інформації, навіть якщо вона зашифрована, небажане для користувача. Це завдання ефективно реалізоване на рівні носіїв даних, і в деяких випадках може виявитися надто значущим.

3) Не деклароване зберігання інформації. Зазвичай інформаційні ресурси здійснюють зберігання даних лише одному вигляді. Проте, використовуючи стеганографію, можна забезпечити збереження інших форматів, розширюючи можливості зберігання інформації та підвищуючи її функціональність.

4) Захист авторського права. Захист авторських прав стає можливим завдяки використанню стеганографії. У випадках, коли контент, такий як фотографії, публікується без дозволу автора, стеганографічні знаки можуть допомогти підтвердити авторство. Вбудована інформація, така як дата створення знімка та інші деталі, дозволяє "прив'язати" фотографію до конкретного фотоапарата, забезпечуючи надійний захист прав на твір.

5) Захист справжності документів. Стеганографія використовується для захисту справжності документів, подібно технології, яка застосовується в захисті авторського права. Вона підтверджує не лише авторство, але і справжність самого документа. Якщо документ не містить СВЗ (стеганографічного захисту), його можуть визнати неправдивим або підробленим. Такий підхід забезпечує надійний механізм визначення справжності важливих документів.

6) Індивідуальний відбиток у системі електронного документообігу. Застосування індивідуального відбитку у системі електронного документообігу внутрішньо документної системи може бути реалізоване за допомогою спеціальних додатків та драйверів, які встановлені і працюють в системі. При належному виконанні цього завдання індивідуальний відбиток дозволяє ідентифікувати особу, яка працювала з конкретним документом. Хоча стеганографія не повинна бути єдиним критерієм ідентифікації, вона може служити додатковим інструментом для точного визначення учасників, що взаємодіють з документами у системі.

7) Водяний знак у DLP-системах (Data Leak Prevention). Застосування водяного знаку в системах запобігання витоку інформації (DLP) може бути забезпечено стеганографією. Під час створення документа, який містить конфіденційну інформацію, вбудовується мітка за допомогою стеганографічних методів. Незалежно від кількості копій документа, мітка змінюється, і для її отримання потрібен стегоключ, який зберігається в таємниці від більшості користувачів. DLP-система перевіряє наявність водяного знака перед схваленням чи відхиленням видачі документа з системи. Якщо знак присутній, система блокує передачу документів назовні.

8) Прихована передача управляючого сигналу. У випадку прихованої передачі управляючого сигналу стеганографія використовується для надання сигналу системі, коли відправником виступає оператор, а отримувачем — деяка автоматизована система. Якщо система може змінювати свій стан, і ми не хочемо, щоб противник виявив перехід системи в інший стан, стеганографія стає ефективним методом. У порівнянні з криптографією, яка просто повідомляє противника про зміни, стеганографія не розголошує факт змін, запобігаючи виклику небажаних дій.

9) Підтвердження достовірності переданої інформації. У контексті підтвердження достовірності переданої інформації, стегоповідомлення включає дані, що підтверджують правильність вміщених у контейнер даних. Ця функція реалізується за допомогою хеш-функції чи контрольної суми. Важливо, коли противник намагається підробити дані у контейнері. Щодо захисту достовірності

документів, важливо додатково захищатися від третьої сторони, що може намагатися підробити дані між відправником і одержувачем. На ринку існує багато класичних рішень, зокрема криптографічних, для цієї проблеми, а стеганографія виступає як ефективний метод вирішення цього завдання.

10) Невідчужуваність інформації. У разі необхідності забезпечення невіддільності інформації у документах, зокрема медичних знімках, використання стеганографії стає ключовим. Резервування даних, призначене для збереження цілісності, може ускладнити відокремлення однієї інформації від іншої. Важливо відзначити, що в даному контексті, стеганографія використовується для невіддільності від додаткової інформації, вбудованої у самі знімки, спираючись на довіру користувачів. Такий підхід може виявитися ефективнішим у порівнянні з супроводженням кожної фотографії додатковою інформацією.

Висновок до розділу 1

В розділі розглянуто основні аспекти стеганографії, зокрема використання цифрових водяних знаків (ЦВЗ) та інших методів прихованої передачі інформації. Описано принципи стеганографії та її відмінності від криптографії, підкреслено актуальність розвитку стеганографічних методів в сучасному інформаційному суспільстві.

Детально розглянуто різноманітні напрямки використання стеганографії, такі як встрайвання інформації для передачі, використання ЦВЗ для захисту авторських прав, а також роль стеганографії в організації стегоканалів та захисті інтелектуальної власності.

Зазначено, що стеганографія служить ефективним доповненням до криптографії, знижуючи ймовірність виявлення факту передачі інформації. Також висвітлені ключові аспекти забезпечення безпеки та робастності методів стеганографії, а також розглянуто різні напрямки застосування цих технологій в сучасному інформаційному середовищі.

Також розглядаються основні можливості її практичного застосування.

РОЗДІЛ 2. ПРОЄКТУВАННЯ ПІДСИСТЕМИ СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Комп'ютерна стеганографія

Комп'ютерна стеганографія – це наука, що базується на використанні елементів та функціоналу сучасного програмного забезпечення та обчислювальної техніки як контейнера. Основні методи цієї галузі будуються на двох принципах:

- 1) Існують файли, які не вимагають абсолютної точності (наприклад, зображення), і можуть бути змінені без помітних втрат інформативності.
- 2) Органи чуття людини не в змозі розрізнати незначні відхилення у вищезгаданих файлах, а також відсутні спеціалізовані засоби для розв'язання цієї задачі.

Серед основних підходів до реалізації методів комп'ютерної стеганографії в межах інформаційного середовища варто визначити виділення малозначущих фрагментів цього середовища та їх заміну даними, які необхідно приховати. Оскільки комп'ютерна стеганографія розглядає середовища, що підтримуються обчислювальними засобами та комп'ютерними мережами, вся інформаційна среда може бути представлена у цифровому вигляді.

Фрагменти, малозначущі для "кадра інформаційного середовища", замінюються фрагментами прихованої інформації відносно певного алгоритму чи методу. "Кадр інформаційного середовища" – це певна частина середовища, виділена за характерними ознаками. Такими ознаками часто служать семантичні характеристики виділеної частини інформаційного середовища, такі як окреме зображення, веб-сторінка або аудіофайл.

Розглянемо основні методи комп'ютерної стеганографії

За способом приховування, методи комп'ютерної стеганографії розділяються на дві категорії: методи прямої заміни та спектральні методи. Перші

використовують зайвисть інформаційного середовища у часовому (для звуку) чи просторовому (для зображення) аспектах. Їх сутність полягає в заміні невеликої частини контейнера бітами стегосповідження. Другі використовують спектральні методи для представлення елементів середовища, куди вбудовуються приховані дані.

Основним напрямком у комп'ютерній стеганографії є використання властивостей зайвості контейнера-оригіналу. При цьому слід враховувати, що приховання інформації призводить до порушення структури контейнера або спотворення деяких його статистичних властивостей та цілісності. Отже, необхідно зменшувати ефект демаскуючих ознак.

Окремо можна виділити групу методів, які використовують особливості форматів файлів:

- Зарезервовані методи розширення полів файлів, де поля заповнюються нулями та не враховуються програмою.
- Навмисне форматування даних (зсув слов, речень, абзаців або вибір певних позицій символів).
- Використання неактивованих участків магнітних та оптичних носіїв.
- Видалення файлових заголовків-ідентифікаторів і т.д.

Зазвичай для методів такого типу характерні низька пропускну спроможність, слабка продуктивність та низький рівень приховуваності.

За призначенням виділяють стеганометоди для саме приховування даних в цифрових об'єктах та методи для прихованого зберігання (або прихованої передачі) даних для захисту їх авторства. За типом контейнера стеганографічні методи розрізняються як методи з контейнерами у вигляді тексту, аудіофайла, зображення та відео.

2.2 Вбудовування в молодші біти контейнера

Вбудовування інформації у менш значущі біти контейнера визначається як відомий та один із перших методів захисту сигналів через ЦВЗ і стеганографії. Цей підхід дозволяє вбудовувати значну кількість інформації, мінімізуючи помітні

зміни у контейнері. Зазвичай такі методи виявляють низьку стійкість до змін у носії інформації і можуть піддаватися стегоаналізу, що обмежує їх застосовність. Основна концепція полягає у тому, що будь-яке зображення може бути представлене як сукупність бітових площин, зміст контейнера $C(n_1, n_2)$ виглядає наступним чином:

$$C(n_1, n_2) = C_1(n_1, n_2) + C_2(n_1, n_2) \cdot 2 + \dots + C_K(n_1, n_2) \cdot 2^{K-1}$$

де $C_k(n_1, n_2) \in [0,1]$ – бітові площини, k – номер бітової площини, $K = 8$ – їх кількість.

Найменш і найбільш значущими бітовими площинами є відповідно C_1 і C_8 : зміна значення біта $C_1(n_1, n_2)$ призводить до зміни яскравості на одиницю, тоді як зміна біта $C_8(n_1, n_2)$ впливає на яскравість зі зміною на 128.

Основна ідея полягає в використанні молодших бітів у колірному каналі кожного пікселя як місця для приховування інформації. Робота цього методу відбувається на бітовому рівні, забезпечуючи ефективність використання методу приховування інформації.

Розміри зображення (ширина, довжина та RGB-шари) визначають кількість піксельних каналів для приховування повідомлення. Після відповідного підгону каналів стегоповідомлення під кількість доступних у контейнері, інформацію можна успішно приховати.

Процес відновлення включає отримання молодших бітів від кожного піксельного каналу та їх подальше групування у слова. Однак метод має обмеження на розмір стегоповідомлення, і великі об'єми можуть спричинити деформації контейнера, не відповідаючи меті непомітного передавання інформації.

У разі невеликих розмірів контейнера і великої кількості вміщеної інформації ймовірно з'являться спотворення початкового вигляду та шуми. Щоб приховати велике повідомлення без значних змін у контейнері, слід обрати більший контейнер. Проте це може викликати проблеми, особливо якщо потрібно передати дуже велике повідомлення, оскільки розмір контейнера повинен бути в декілька разів більший за розмір самого повідомлення.

А вже це може завдати шкоди стійкості до стійкості, оскільки потенційний противник першочергово перевірить великі зображення. Хоча це можна обіграти і на свою користь, надсилаючи багато великих файлів. Таким чином, противник буде просто завантажений непотрібним аналізом і роботою.

У цій ситуації допоможе створення стегосистеми із застосуванням ключа. Необхідно, щоб ключ нерівномірно змінював координати наступного пікселя, де буде розміщена наступна частина інформації.

Таким чином за контейнер у цьому підході можна взяти зображення чи текст.

Потрібно почати з ключа. Ключ буде набір груп з трьох координат, де кількість груп буде відповідати довжині стегоповідомлення. Координати можна дати по двох осях x та y . Але, маючи набори трьох кольорів RGB, потрібно ще й третю вісь z , де буде значення від 0 до 2.



Рисунок 2.1 - а) Розширення координат; б) Розширена вісь x після розділення значення RGB за шириною

Поєднавши різні координати трьох осей, отримаємо одну унікальну координату x . Це робиться зменшення розміру ключа. Одне зі значень кольору відповідає значенню символу в таблиці ASCII. За рахунок цього контейнер може розмістити більше інформації.

Сенс алгоритму полягає у пошуку координати, значення якої буде відповідати значенню символу.

У разі приховування тексту в текстовому рядку, весь набір слів можна подати як рядок. І кожен елемент його матиме певну координату по осі x .

Підхід не дуже добрий тим, що користувач сам ключ не вигадує, а його виводить алгоритм. Виходить, що новий ключ передається при кожній подальшій передачі даних, що є поганим тоном для стеганографії.

Незважаючи на те, що алгоритм видає ключі, їх можна використовувати необмежено. Для цього необхідно взяти інший контейнер так, щоб у заданих координатах щоразу було інше повідомлення. Це можна зробити по-різному: взяти за основу зображення у відкритому доступі або з нуля створити таке зображення. Коли контейнер – текст, то дії аналогічні зазначеним раніше зображення.

Залежно від розмірів зображення кількість ключів може бути дуже великою. Крім того, передача повідомлення може бути необмежена одним форматом контейнера або одним контейнером. Якщо, наприклад, стегосообщение передаємо через блог, одна частина повідомлення може бути у тексті, іншу – у відео.

В одне зображення або великий текст може поміститися безліч повідомлень. Краще, якщо зображення є різнобарвним, оскільки це забезпечує різноманітність варіантів. У чорно-білому зображенні передати велике повідомлення буде важко.

У цьому підході контейнер не піддається деформації: оригінал і використовується як контейнер.

2.3 Вбудовування бінарних даних в HTML-документ

Неможливо вставити в HTML-документ, оскільки все вставлене буде видимим у браузері або у вихідному тексті як марний матеріал. Проте, звертаючись до структури HTML-документа, важливо зауважити, що він складається з тегів і відповідних атрибутів. Хоча порядок тегів важливий, порядок атрибутів можна змінювати, не впливаючи на зовнішній вигляд документа або розмір файлу.

У класичній текстовій стеганографії зазвичай потрібно 80 рядків тексту для приховання 10 символів секретного тексту. Однак у випадку HTML-документів, які мають більш загальні комбінації атрибутів, особливо з використанням стилів CSS, можливі більш ефективні методи приховування інформації, забезпечуючи невидимість для звичайного спостерігача.

Суть полягає в наступному: для кожного тега з двома або більше атрибутами виділяється пара його атрибутів, порядок якої відповідає значенню 1, істині. При заміні місцями даних атрибутів виходить хибна пара, що відповідає значенню 0. Отже, маючи бінарне представлення повідомлення та набір пар атрибутів, можна за допомогою зміни порядку їхнього розташування приховати це повідомлення.

Зворотний процес отримання вихідного повідомлення також не буде складним, якщо відомо, які саме пари атрибутів використовувалися для приховування і який порядок атрибутів прийнято за істинний. Недоліком цього методу є обмежений розмір повідомлення, яке можна успішно приховати.

2.4 Математичні методи

До математичних методів обробки сигналів та зображень, який можна віднести дискретні вейвлет-перетворення, яке використовує вейвлети - короткі функції, що можуть виявлювати локальні зміни в сигналах. Вейвлет-перетворення дозволяє аналізувати сигнали та зображення на різних масштабах і визначати їхні частотні характеристики та просторові властивості.

Основна ідея полягає в розкладанні сигналу чи зображення на декілька компонентів вейвлету різних масштабів і частот. Цей процес відрізняється від традиційних методів, таких як перетворення Фур'є, оскільки вейвлети можуть добре адаптуватися до локальних змін в сигналі, що дозволяє отримувати інформацію про сигнал в залежності від часу та просторових характеристик.

Дискретне вейвлет-перетворення є потужним інструментом для обробки зображень, а особливо воно ефективно для виявлення локальних особливостей та аналізу текстур. Одним з популярних вейвлетів для DWT є вейвлет Хаара.

Вейвлет Хаара представляє собою кусочно-постійну функцію, яка розглядається на кінцевих інтервалах різного масштабу та має значення +1 або -1. Материнський вейвлет Хаара, або вейвлет Хаара нульового зміщення та одиничного масштабу, можна представити як функцію, яка дорівнює +1 на проміжку $[0, 1/2)$ і -1 на проміжку $[1/2, 1]$.

Одна з переваг вейвлет-перетворення Хаара в порівнянні з іншими вейвлетами полягає в його простоті та легкості обчислення, а також в здатності ефективно виявляти краї та деталі в зображеннях.

DWT може бути використане для поділу зображення на різні частини (approximation та detail) на різних масштабах, що дозволяє виявляти і аналізувати різні аспекти зображення.

Перетворення Хаара вважається одним із найпростіших базисних вейвлет-преобразовань. Розглянемо одновимірний сигнал $f = (f_1, f_2, \dots, f_N)$. Процес ПХ розкладає сигнал на дві компоненти: різницю та середнє.

На першому рівні для сигналу довжини N значення середнього $a^1 = (a_1, a_2, \dots, a_{N/2})$ обчислюється за формулою:

$$a_k = \frac{f_{2k-1} + f_{2k}}{\sqrt{2}}, \quad k = 1, 2, \dots, \frac{N}{2}.$$

Це визначає перше середнє значення на першому рівні вейвлет-розкладу Хаара. Відповідно, різниця $d^1 = (d_1, d_2, \dots, d_{N/2})$ обчислюється як:

$$d_k = \frac{f_{2k-1} - f_{2k}}{\sqrt{2}}, \quad k = 1, 2, \dots, \frac{N}{2}.$$

Отримані значення середнього та різниці представляють собою перший рівень вейвлет-розкладу Хаара для заданого сигналу.

Ось так буде виглядати другий варіант вейвлет-перетворення Хаара:

$$a_k = \frac{f_{2k-1} + f_{2k}}{\sqrt{2}}, \quad k = 1, 2, \dots, \frac{N}{2},$$

$$d_k = \frac{f_{2k-1} - f_{2k}}{\sqrt{2}}, \quad k = 1, 2, \dots, \frac{N}{2}.$$

Отримані значення a_k представляють собою другий рівень апроксимації (середнього), а значення d_k - другого рівня деталізації (різниці). Таким чином, другий рівень вейвлет-розкладу Хаара будується на основі результатів першого рівня.

Швидке перетворення Хаара включає віднімання, додавання і ділення на 2, внаслідок чого воно є ефективним і зводить обчислювальну задачу порівняно з ПХ. Щоб розкласти зображення, одновимірне ПХ спочатку слід застосувати до кожного рядка піксельних значень матриці, що відображає, а після вже і до кожного стовпця. Усі деталізуючі коефіцієнти є результуючими значеннями, крім окремого загального середнього коефіцієнта.

Розглянемо також двовимірне вейвлет перетворення.

Двовимірне вейвлет-перетворення матриці має на увазі почергове одновимірне вейвлет-перетворення рядків та стовпців даної матриці. Спочатку для кожного рядка проводиться одновимірне вейвлет-перетворення, після чого перетворений рядок записується на попередньому місці. Аналогічно вейвлет-перетворення застосовується до всіх стовпців. Як результат, зображення розбивається на чотири рівні частини:

- A1 (А перше): Складається з верхньої лівої частини матриці, яка є високочастотною складовою (деталі) після вейвлет-перетворення рядків та стовпців.
- H1 (Горизонтальне перше): Містить верхню праву частину матриці, що є результатом вейвлет-перетворення рядків з високочастотними складовими.
- V1 (Вертикальне перше): Складається з нижньої лівої частини матриці, що виникає в результаті вейвлет-перетворення стовпців з високочастотними складовими.
- D1 (Діагональне перше): Представляє нижню праву частину матриці, яка є високочастотною складовою після вейвлет-перетворення рядків та стовпців.

Цей процес може бути рекурсивно застосований до кожної отриманої частини для отримання подальших рівнів деталізації.

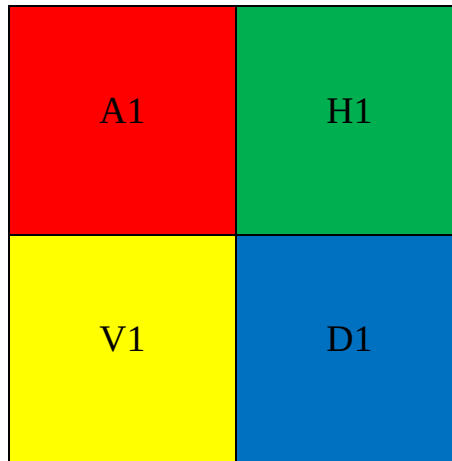


Рисунок 2.2 Приклад впливу двовимірного вейвлету-перетворення на зображення квадратної форми

N-кратне двовимірне вейвлет-перетворення передбачає застосування двовимірного вейвлет-перетворення N разів, причому кожне наступне двовимірне вейвлет-перетворення застосовується до молодшої чверті матриці:

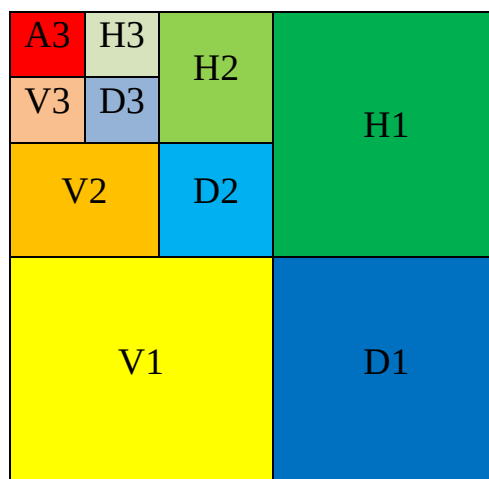


Рисунок 2.3 Застосування двовимірного вейвлет-перетворення послідовно 3 рази до зображення квадратної форми

Зворотнє двовимірне вейвлет-перетворення рекурсивно перетворює молодший квадрант матриць. Зазначене перетворення є ієрархічним. Іншими словами, якщо при використанні зворотного вейвлет-перетворення обчислюються не всі рівні, а менше їх кількість, то в квадранті LL утворюється зменшена копія зображення. Якщо не передбачається застосування зворотного вейвлет-перетворення, молодший квадрант, таким чином, стає зменшеною копією

зображення. Зворотне перетворення, звідси, дозволяє вирізати фрагменти зображень різного масштабу. Однак доступні масштаби визначаються кількістю рівнів вейвлет-перетворення та масштаби мимовільні, а збільшені вдвічі.

Висновки до розділу 2

У цьому розділі було проведено аналіз методів застосування комп'ютерної стеганографії, а також таких технічних методів як вставка молодшого біта, впровадження бінарних даних у HTML-документ та математичних методів, що базуються на перетвореннях Хаара.

На основі проведеного аналізу вищезазначених методів розкриваються їх переваги та недоліки.

РОЗДІЛ 3 РЕАЛІЗАЦІЯ МЕТОДІВ ВБУДОВИ

3.1 Метод вставки молодшого біта

Розглянемо практичну реалізацію вказаних алгоритмів.

Для цього ми використовуємо мову Python:

```
from PIL import Image

def encode_message(image_path, message, output_path):
    # Відкриття зображення
    img = Image.open(image_path)
    # Конвертація текстового повідомлення в бінарний вигляд
    binary_message = ''.join(format(ord(char), '08b') for char in message)
    # Перетворення пікселів зображення
    pixels = list(img.getdata())
    # Перехід по кожному пікселю та приховання біт повідомлення
    encoded_pixels = []
    message_index = 0
    for pixel in pixels:
        encoded_pixel = list(pixel)
        for i in range(3): # Проходження через кожен кольоровий канал RGB
            if message_index < len(binary_message):
                # Заміна молодших бітів на біти повідомлення
                encoded_pixel[i] = int(format(pixel[i], '08b')[:-1] + binary_message[message_index], 2)
                message_index += 1
            encoded_pixels.append(tuple(encoded_pixel))
    # Створення нового зображення з прихованим повідомленням
    encoded_img = Image.new('RGB', img.size)
    encoded_img.putdata(encoded_pixels)
    # Збереження нового зображення
    encoded_img.save(output_path)
    print("Повідомлення успішно заховано у зображенні.")

def decode_message(encoded_image_path):
    # Відкриття зображення з прихованим повідомленням
    encoded_img = Image.open(encoded_image_path)
    # Отримання пікселів зображення
    pixels = list(encoded_img.getdata())
    # Відновлення бінарного повідомлення з молодших бітів
    binary_message = ""
    for pixel in pixels:
        for i in range(3): # Проходження через кожен кольоровий канал RGB
            binary_message += format(pixel[i], '08b')[-1]
    # Конвертація бінарного повідомлення в текст
    decoded_message = ''.join([chr(int(binary_message[i:i+8], 2)) for i in range(0, len(binary_message), 8)])
    print("Заховане повідомлення:", decoded_message)

# Приклад використання
image_path = 'original_image.png'
output_path = 'encoded_image.png'
message_to_hide = 'Hello, steganography!'
# Заховати повідомлення у зображенні
encode_message(image_path, message_to_hide, output_path)
# Доступ до захованого повідомлення
decode_message(output_path)
```

У ролі стежоконтейнера було взято довільне зображення (рис. 3.1)

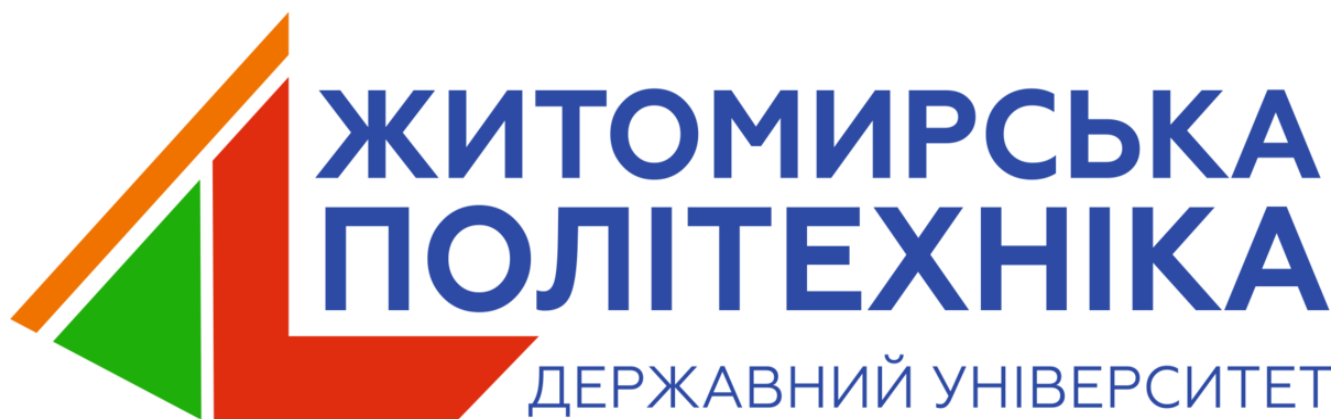


Рисунок 3.1 – Вихідне зображення

В якості секретного повідомлення повідомлення сформоване у ASCII-кодванні.

Оскільки операції виконуються на рівні окремих бітів, необхідно також отримати бітове представлення цього стегоповідомлення. Потім виникає питання про те, як вставити повідомлення в контейнер, особливо якщо їхня кількість бітових каналів різниться. Простим рішенням цього питання є доповнення відсутніх каналів нулями до параметрів зображення.

Все, що залишається зробити, це скласти бітове представлення контейнера та повідомлення. Візуально зображення з вставленим повідомленням виглядатиме так:

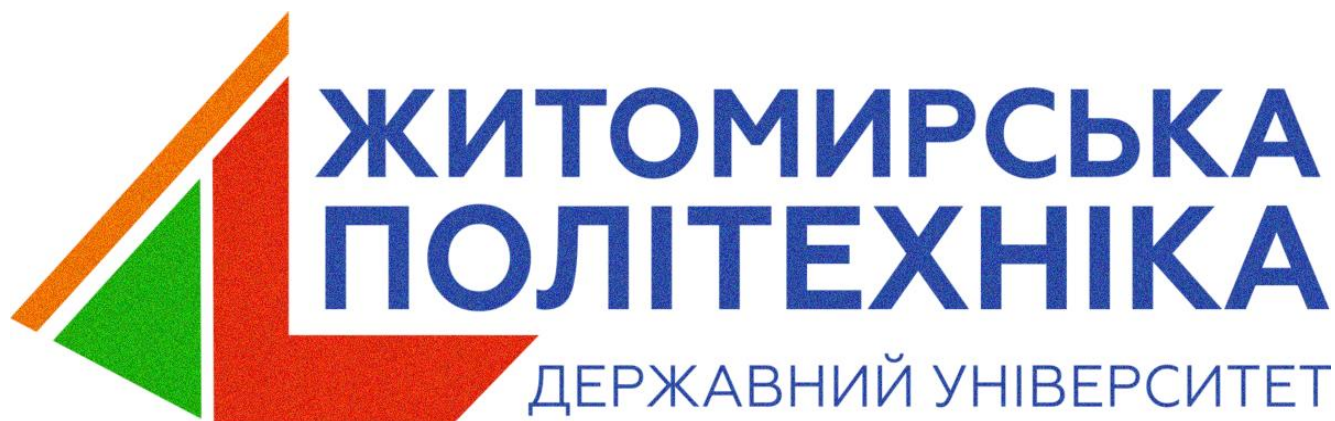


Рисунок 3.2 – Зображення з вбудованим стеганоповідомленням

Як можна побачити, візуально різницю не помітно, але якщо відняти від фінального контейнеру вихідну картинку, то отримуємо наступне зображення:

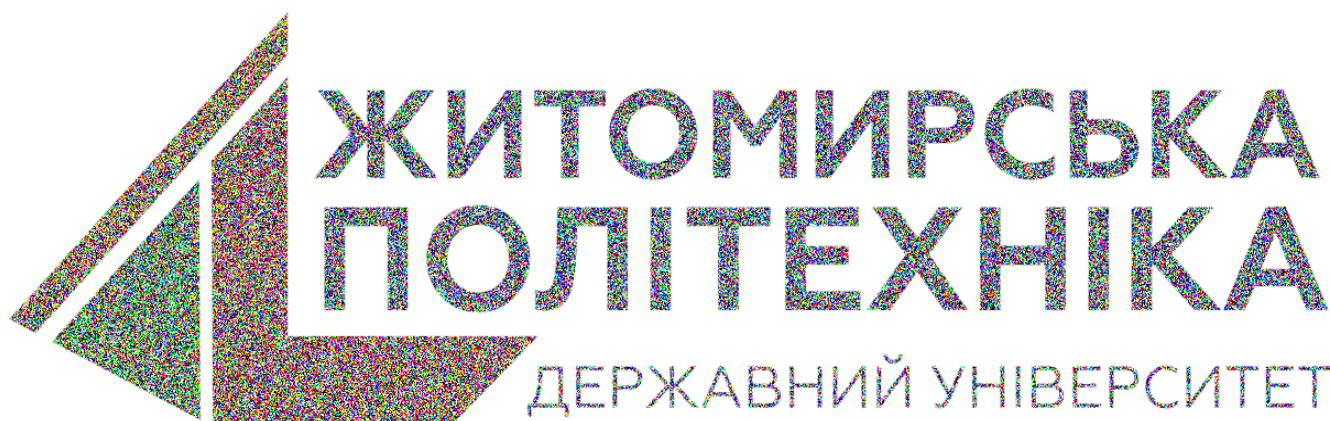


Рисунок 3.3 – Результат віднімання вихідного зображення із зображення із стегоповідомленням

Різнокольорові ділянки на зображенні підтверджують факт змін, що відбулися з контейнером. Різниця лише в тому, що одні кольорові ділянки є результатом приведення зображення до 8-бітних піксельних каналів, інші – вставки стегоповідомлення, а треті – комбінації цих двох операцій. Для отримання повідомлення назад потрібно зібрати молодші біти зі всіх бітових каналів, з'єднати їх у 8-бітові слова і сконвертувати до текстових символів.

3.2 Застосування стеганографічних методів у HTML-документі

Внесення стеганографічного повідомлення у HTML документ вимагає обробки HTML-коду та вставлення прихованого тексту. Ось невеликий приклад коду на Python, який може внести текст у властивість "alt" тегу "img" в HTML-документі:

```
def hide_message_in_html(original_html, secret_message):  
    # Пошук тегів <img> у HTML-коді  
    img_tags = re.findall(r'<img\s+.*?>', original_html, flags=re.IGNORECASE)  
    if not img_tags:  
        print("Зображення не знайдено в HTML-документі.")  
        return original_html  
    # Обираємо перший тег <img> (можна модифікувати логіку відповідно до потреб)  
    target_img_tag = img_tags[0]  
    # Вставляємо приховане повідомлення у властивість "alt" тегу "img"  
    modified_img_tag = target_img_tag.replace('>', f' alt="{secret_message}">')  
    # Замінюємо оригінальний тег у HTML-документі на модифікований
```

```

        modified_html = original_html.replace(target_img_tag, modified_img_tag)
    return modified_html

# Приклад використання
original_html_content = """
<!DOCTYPE html>
<html>
<head>
    <title>Steganography HTML</title>
</head>
<body>
    
</body>
</html>
"""

secret_message = "Це секретне повідомлення"
modified_html = hide_message_in_html(original_html_content, secret_message)
# Виведення модифікованого HTML
print(modified_html)

```

3.3 Застосування водяного знаку для PDF-документу

Використовуючи розглянуте раніше двовимірне вейвлет-перетворення зображення, можна надати йому практичного застосування для теми, що розглядається в кваліфікаційній роботі.

Досить часто можна спостерігати, що PDF-документи позначені певними зображеннями, або впродовж усієї сторінки там розміщений розпливчастий напис із зазначенням власника документа. Це також водяний знак.

Як мовилося раніше, вейвлет-перетворення можна послідовно застосувати до зображення кілька разів, тобто зробити багатовимірне вейвлет-перетворення. Для зображення це загрожує тим, що його можна масштабувати до скільки завгодних розмірів, аж до розмірів 1×1 px. Не варто забувати і про зворотне вейвлет-перетворення, що відновлює зображення.

Слід зазначити, що процедуру прямого вейвлет-перетворення надалі називатимемо «аналізом», а процес зворотного вейвлет-перетворення — «синтезом».

Реалізація буде полягати в тому, що, вибравши деяке зображення квадратної форми, можна стиснути його до малих розмірів і підставити PDF-документ. Програма-обробник, отримавши деяке зображення, відновлює його за допомогою синтезу до грубих обрисів. Таким чином, якщо це зображення є водяним знаком, документ деформується.



Рисунок 3.4 – Процес формування водяного знаку за допомогою вейвлет перетворень

Наступним кроком буде вбудовування водяного знаку у PDF-документ.

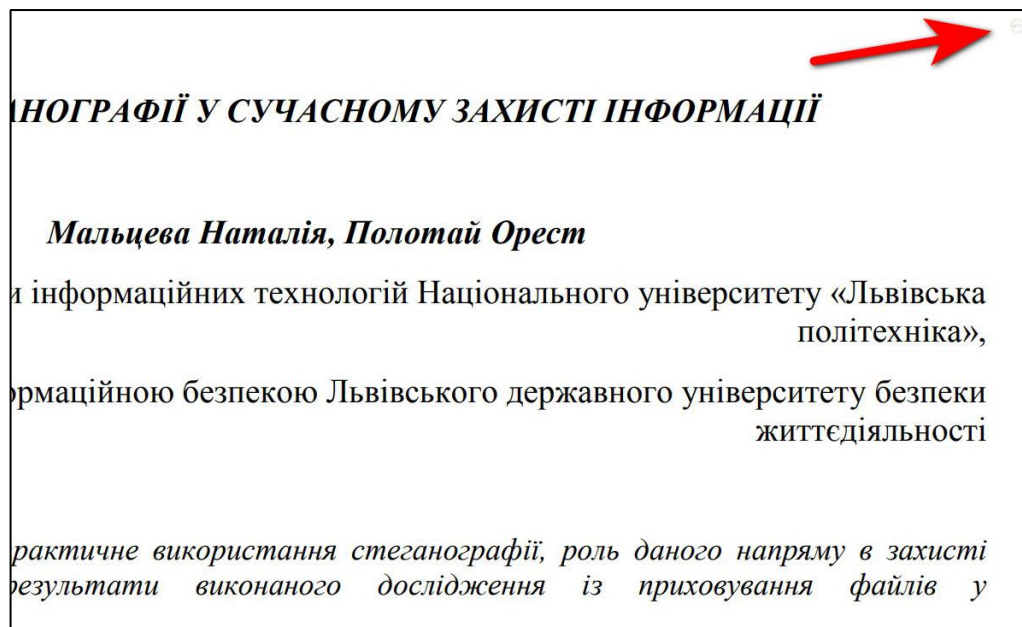


Рисунок 3.5 – Приклад застосування водяного знаку до PDF-документа

При обробці документа за водяним знаком можна ідентифікувати версію, а також при спробі видобути текст, наприклад 1 абзац (рис.3.6) – він буде зруйнованим.

РОЛЬ СТЕГАНОГРАФІЇ У СУЧАСНОМУ ЗАХИСТІ ІНФОРМАЦІЇ

Мальцева Наталія, Полотай Орест

кафедра безпеки інформаційних технологій Національного університету «Львівська політехніка»,

кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності

У роботі наведено практичне використання стеганографії, роль даного напрямку в захисті інформації, приведено результати виконаного дослідження із приховування файлів у стегоконтейнері.

Ключові слова: стеганографія, секретний ключ, стегоконтейнер, приховування інформації.

This work presents the practical use of steganography, the purpose and objectives of this area in the information security and also contains results of the research based on hiding files in the stegocontainer.

Key words: steganography, secret key, stegocontainer, information hiding.

В першу чергу, визначимо поняття стеганографії. Стеганографія — наука, предметом якої є приховування факту присутності секретної інформації. Саме в цьому і полягає відмінність даної науки від не менш поширеного напрямку захисту інформації — криптографії, при використанні якого читання вмісту повідомлення стає неможливим.

Сучасну стеганографію прийнято розділяти на класичну, комп'ютерну і цифрову [1, ст. 65], також виділяють мережеву. Класична пов'язана із приховуванням текстових даних,

Рисунок 3.6 – Спроба скопіювати текст із статті

Отриманий результат (з порушенням кодування тексту):

«? ????? ?????, ????????? ??????? ??????????????. ?????????????? — ?????, ?????????????? ?
????????????? ????? ?????????????? ?????????? ??????????. ??? ? ????? ? ?????? ?????????????? ?????
????? ??? ?? ??? ?????????? ?????????? ?????????? —?????????????, ??? ?????????????? ?????
????????? ?????? ?????????????? ??? ??????????????»

Описаний вище процес є спрощеною модифікацією реального вставлення. Як відбір зображення для внесення, так і сам процес вставлення можуть бути більш складними за допомогою додаткових методів.

Висновки до розділу 3

В даному розділі розглядалися практичні аспекти стеганографії, зокрема вбудовування інформації у менш значущі біти контейнера. Розглянуті етапи включають вибір контейнера, перетворення повідомлення у бітовий формат, а також методи вставлення і видобування інформації. Також розглянуті питання впливу на контейнер, візуальні артефакти та можливі методи ускладнення виявлення стеганографії.

Важливо враховувати, що використання стеганографії потребує уважності і дотримання відповідних норм та правил. Застосування стеганографії може мати практичні застосування в області захисту інформації, але також повинно враховувати етичні та юридичні аспекти.

ВИСНОВКИ

У першому розділі були розглянуті основні аспекти стеганографії, зокрема використання цифрових водяних знаків (ЦВЗ) та інших методів прихованої передачі інформації. Зазначено принципи стеганографії та відмінності від криптографії, відзначена актуальність стеганографічних методів у сучасному інформаційному суспільстві. Проведено детальний аналіз різноманітних напрямків використання стеганографії, включаючи встрайвання інформації для передачі, використання ЦВЗ для захисту авторських прав та роль стеганографії в організації стегоканалів та захисті інтелектуальної власності.

У другому розділі був проведений аналіз методів застосування комп'ютерної стеганографії, також враховуючи технічні аспекти, такі як вставка молодшого біта, впровадження бінарних даних у HTML-документ та математичні методи, базовані на перетвореннях Хаара. Здійснено розкриття переваг і недоліків кожного з методів на основі проведеного аналізу.

Третій розділ розглядав практичні аспекти стеганографії, зокрема вбудовування інформації у менш значущі біти контейнера. Описано етапи вибору контейнера, перетворення повідомлення у бітовий формат, а також методи вставлення та видобування інформації. Піднято питання впливу на контейнер, візуальних артефактів та можливих методів ускладнення виявлення стеганографії.

Важливо пам'ятати, що використання стеганографії вимагає уважності і дотримання відповідних норм і правил. Ця технологія може бути ефективним інструментом у сфері захисту інформації, проте також повинна враховувати етичні та юридичні аспекти.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кузнєцов, О.О. Стеганографія: навчальний посібник / О.О.Кузнєцов, С.П. Євсєєв; під загальною редакцією О.Г. Короля. –Харків: Вид. ХНЕУ, 2011. – 232с.
2. Конахович, Г.Ф. Комп'ютерна стеганографія. Теорія і практика / Г.Ф. Конахович, А.Ю. Пузиренко. – К.: МК-Пресс, 2006. – 288с.
3. Туровський, О., Лазаренко, С., Щербак, Т., Рябова, Л., & Мелешко, Т. (2022). Методика оцінки стеганографічних методів приховування інформації в зображеннях. / Інфокомунікаційні та комп'ютерні технології, 2(02). <https://doi.org/10.36994/2788-5518-2021-02-02-23>
4. Корченко О.Г., Сіденко В.П., Дрейс Ю.О. Прикладна криптологія: системи шифрування. Київ: ДУТ, 2014. 448 с.
5. Кухарська Н.П. Програмна реалізація алгоритмів приховування інформації методами довільного інтервалу. Вісник ЛДУ БЖД. Львів, 2018. № 16. С. 41-48.
6. Лагун А.Е. Використання стеганографічних алгоритмів для приховування текстової інформації. Вісник ЛДУ БЖД. Львів, 2018. № 18. С. 49-56.
7. Швідченко І.В. Побудова криптостеганосистем для розв'язання задач інформаційної безпеки: дис. ... на здобуття наук. ступеня канд. фіз.-мат. наук : 01.05.01. Київ, 2011. 128 с
8. Abdullah A. M., Aziz R. H. New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm. International Journal of Computer Applications. 2016. Vol. 143, No 4. P. 11-17.
9. Abdullah, A. M. (2017). Advanced Encryption Standard (AES). Algorithm to Encrypt and Decrypt Data. Cryptography and Network Security. URL: <https://www.researchgate.net/publication/317615794>
10. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань за-безпечення інформаційної безпеки держави / С.В.Мельник, С.В.Кондакова // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. – К. : Наук.-вид. відділ НА СБ України, 2010. – С. 134-138.

11. Mallat S. A Theory For Multiresolution Signal Decomposition: The Wavelet Representation // IEEE Transactions on Pattern Analysis and Machine Intelligence, 1989. – Vol. 11. – P. 674-693.
12. Shapiro J. Embedded Image Coding Using Zerotrees Of Wavelet Coefficients // IEEE Transactions on Signal Processing, 1993. – Vol. 41, No. 12.
13. Said A., Pearlman W. A New Fast And Efficient Image Codec Based On Set Partitioning in Hierarchical Trees // IEEE Transactions on Circuits and Systems for Video Technology, 1996. – Vol. 6. – P. 243-250. 90
14. Antonini M., Barlaud M., Mathieu P., Daubechies I. Image Coding Using Wavelet transform // IEEE Transactions On Image Processing, 1992. – Vol. 1, № 2. – P. 205-220
15. Кошкіна Н.В. Методи стеганоаналізу з навчанням та класифікацією за характеристичними векторами / Н.В. Кошкіна // Праці міжнар. конф. “Питання оптимізації обчислень-XL”. □ Київ: Ін-т кібернетики ім. В.М. Глушкова НАН України. – 2015. – С. 153–154.
16. Zadiraka V. Spectral methods of computer steganography problem decision / V. Zadiraka, N. Koshkina // Methods of effective protection of information flows /ed. by V. Zadiraka, Y. Nykolaichuk. – Ternopil: Ternograf, 2014. – P. 96–120.
17. Кошкіна Н.В. Інформаційно-теоретична модель безпеки стеганографічних систем / Н.В. Кошкіна // Поступ в науку. – 2011. – №6, Т.1. – С.117–120.
18. Хорошко В.А. Введение в компьютерную стеганографию / В.А. Хорошко, М.Е. Шелест. – Киев: Національний Авіаційний Університет, 2002. – 152 с.
19. 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
20. 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
21. Steganography, and Watermarking of Multimedia Contents VI, San Jose, USA, January 2004. – P. 428–445.

22. Lin C.-Y. Distortion Modeling and Invariant Extraction for Digital Image PrintandScan Process [Электронный ресурс] / C.-Y. Lin, S.-F. Chang // Intl. Symp. on Multimedia Information Processing, Taipei, December 1999. – Режим доступа: <http://www.ee.columbia.edu/ln/dvmm/publications/99/cylin-modelscan.pdf>
23. Yang S. Quantization-Based Digital Audio Watermarking in Discrete Fourier Transform Domain / S. Yang, W. Tan, Y. Chen, W. Ma // Journal of Multimedia. – 2010. – Vol. 5, № 2. – P. 151–158.
24. Manjula Devi T.H. Detecting original image using histogram, DFT and SVM / T.H. Manjula Devi, H.S. Manjunatha Reddy, K.B. Raja, K.R. Venugopal, L.M. Patnaik //Intern. journal of recent trends in engineering. – 2009. – Vol. 1, №1. – P. 367–371.
25. 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.
26. 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.