

Міністерство освіти і науки України
Кам'янець-Подільський національний університет імені Івана Огієнка
Фізико-математичний факультет
Кафедра комп'ютерних наук

Дипломна робота
магістра

з теми: **«РОЗРОБКА МЕТОДУ ПРИХОВАННЯ ІНФОРМАЦІЇ
В МУЛЬТИМЕДІЙНОМУ ПОТОЦІ ДЛЯ ПІДВИЩЕННЯ ЇЇ БЕЗПЕКИ»**

Виконав: студент 1 курсу,
групи KN1-M22
спеціальності 122 Комп'ютерні науки
Ткачук Валерій Віталійович

Кам'янець-Подільський – 2023

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В МУЛЬТИМЕДІЙНИХ ПОТОКАХ	6
1.1. Поняття і визначення приховування інформації в мультимедійних потоках.....	6
1.2. Класифікація методів приховування інформації в мультимедійних потоках.....	8
1.3. Аналіз існуючих методів приховування інформації в мультимедійних потоках.....	10
1.4. Огляд стеганографічних атак на мультимедійні потоки	16
РОЗДІЛ 2. РОЗРОБКА МЕТОДУ ДЛЯ ОПТИМІЗАЦІЇ ІСНУЮЧОГО ПІДХОДУ ДО ПРИХОВУВАННЯ ІНФОРМАЦІЇ В МУЛЬТИМЕДІЙНИХ ПОТОКАХ.....	23
2.1. Математична модель розробленого оптимізаційного застосунку	23
2.2. Опис оптимізації методу приховування інформації в мультимедійному потоці	32
РОЗДІЛ 3. ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО ОПТИМІЗАЦІЙНОГО ЗАСТОСУНКУ ДЛЯ МЕТОДУ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В МУЛЬТИМЕДІЙНОМУ ПОТОЦІ.....	40
3.1. Опис експериментального стенду	40
3.2. Результати експериментального дослідження розробленого методу ..	43
3.3. Порівняння розробленого застосунку з існуючими методами приховування інформації в мультимедійних потоках	51
ВИСНОВКИ	57
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	59

ВСТУП

Сьогоднішній світ, насичений мультимедійною інформацією, ставить перед нами виклик забезпечення безпеки цієї інформації в умовах постійно зростаючого числа кіберзагроз та стеганографічних атак. Захист інформації стає важливим завданням для організацій, установ і індивідуальних користувачів, оскільки конфіденційні дані, такі як особиста інформація, комерційні та фінансові документи, медичні записи та інші чутливі дані, потребують надійного захисту.

Разом зі зростанням загроз, постають нові можливості для розробки ефективних методів приховування інформації в мультимедійних потоках. Приховування інформації в мультимедійних даних виявляється як перспективний підхід, оскільки ці дані масово використовуються в сучасному світі, наприклад, в цифрових зображеннях, аудіо та відеофайлах. Приховування інформації може бути використано для непомітного передачі та збереження конфіденційної інформації, уникнення виявлення та забезпечення безпеки передачі цих даних через відкриті мережі.

Актуальність даної теми полягає в тому, що зростаюче значення мультимедійної інформації та загрози кібербезпеки ставлять під загрозу конфіденційність та цілісність даних. Забезпечення безпеки цих даних стає надзвичайно важливим завданням. Розробка нових та вдосконалення існуючих методів приховування інформації в мультимедійних потоках стають необхідністю для забезпечення безпеки передачі та збереження конфіденційної інформації. Ця тема вимагає постійного дослідження та розробки нових алгоритмів та технологій, що сприятимуть покращенню безпеки мультимедійних даних.

Метою даної магістерської роботи є висвітлення новітніх методів приховування інформації в мультимедійних потоках та покращення та оптимізація вже існуючих засобів приховування інформації в

мультимедійному потоці з метою підвищення безпеки цієї інформації. Результати цього дослідження сприятимуть створенню більш стійких систем захисту, здатних впоратися зі сучасними кіберзагрозами та стеганографічними атаками.

Для досягнення поставленої мети, у даній роботі будуть вирішені наступні завдання:

1. Аналіз існуючих методів приховування інформації в мультимедійних потоках: проведення огляду різних методик та алгоритмів, виявлення їх переваг та недоліків.
2. Оптимізування існуючого методу приховування інформації в мультимедійному потоці: розроблення нового підходу, що базується на використанні передових технологій та алгоритмів, які забезпечують високу стійкість та непомітність приховування інформації.
3. Дослідження ефективності розробленого методу в мультимедійному потоці: проведення експериментальних випробувань для оцінки ефективності та надійності розробленого методу.
4. Оцінка стійкості розробленої моделі оптимізації приховування інформації до різних видів атак: проведення аналізу та тестування стійкості розробленого методу перед відомими атаками, такими як стеганаліз та атаки з використанням статистичних методів.
5. Порівняння розробленого методу з існуючими методами приховування інформації в мультимедійних потоках: виконання порівняльного аналізу розробленого методу з найбільш поширеними та відомими методами приховування інформації з метою визначення його переваг та обмежень.
6. Аналіз можливостей застосування розробленого методу приховування інформації у реальних сценаріях: дослідження потенційних сфер застосування розробленого методу та оцінка його ефективності та придатності у реальних умовах.

Об'єктом роботи є методи приховування інформації в мультимедійних потоках

Предметом роботи є розробка методу оптимізації приховування інформації в мультимедійних потоках для підвищення безпеки.

Новизна роботи полягає у розробці унікального методу оптимізації існуючих методів приховування інформації в мультимедійних потоках. Цей метод включає в себе вдосконалення алгоритмів приховування та виявлення інформації, що дозволяє підвищити ефективність та стійкість процесу приховування.

ВИСНОВКИ

В ході проведення магістерської роботи було здійснено аналіз існуючих методів приховування інформації в мультимедійних потоках. Було розроблено метод оптимізації існуючих заходів для приховування інформації, який використовує передові технології та алгоритми для забезпечення високої стійкості та непомітності процесу приховування.

Застосування розробленого методу було перевірено шляхом проведення експериментальних випробувань, що дозволило оцінити його ефективність та надійність. Результати аналізу та тестування підтвердили стійкість розробленого методу до різних видів атак, включаючи стеганаліз та атаки з використанням статистичних методів.

Крім того, було проведено порівняльний аналіз розробленого методу з найбільш поширеними і відомими методами приховування інформації в мультимедійних потоках. Цей аналіз дозволив виявити переваги та обмеження розробленого методу, підтвердивши його ефективність і потенціал в забезпеченні безпеки мультимедійних даних.

Отримані результати демонструють значний внесок у сферу захисту інформації в мультимедійних потоках. Розроблений метод приховування інформації виявився ефективним та стійким до різних атак, що забезпечує його використання для збереження конфіденційної інформації та підвищення безпеки передачі даних через відкриті мережі.

Основні завдання, які були вирішені в рамках магістерської роботи, сприяють подальшому розвитку області захисту мультимедійних даних. Використання розробленого методу може мати значні переваги у реальних сценаріях, де конфіденційність та цілісність даних є надзвичайно важливими.

Отже, результати даної магістерської роботи свідчать про успішну розробку методу оптимізації приховування інформації в мультимедійних потоках, що сприятиме покращенню безпеки та захисту цінної інформації в сучасному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фрідріх, Дж., Гольян, М., та Ду, Р. (2001). Надійне виявлення стеганографії за допомогою найменших значущих бітів в кольорових та відтінках сірого зображення. Матеріали 5-го семінару з приховування інформації, 27-28.
2. Проц, Н., Хоніман, П., та Мавромматіс, П. (2003). Приховування і пошук: вступ до стеганографії. Безпека та приватність IEEE, 1(3), 32-44.
3. Бендер, В., Грул, Д., Морімото, Н., та Лу, А. (1996). Техніки приховування даних. Журнал IBM Systems, 35(3.4), 313-336.
4. Джонсон, Н. Ф., та Джаджодія, С. (1998). Дослідження стеганографії: бачимо невидиме. Комп'ютер IEEE, 31(2), 26-34.
5. Кетцер, Дж., та де Вільє, М. (2002). Огляд стеганографічних технік. Південноафриканський журнал комп'ютерів, 28, 40-47.
6. Хармсен, Й., та Перлман, У. (1998). Стеганаліз адитивного шуму для приховування інформації. Приховування інформації, 1(3), 222-235.
7. Фрідріх, Дж., Гольян, М., та Ду, Р. (2001). Виявлення стеганографії за допомогою найменших значущих бітів в кольорових та відтінках сірого зображення. Мультимедіа IEEE, 8(4), 22-28.
8. Джонсон Н., Дурік З., Джаджодія С. Сховання інформації: стеганографія та водяні знаки - атаки та протидія. 1-е вид. Вірджинія: SPRINGER-SCIENCE+BUSINESS MEDIA, LLC, 2001. 398 с.
9. Мустакмал М.Е. Аудіо-стеганографія з алгоритмом LSB для захисту цифрових даних. Йог'якарта, 2018. 34 с.
10. Бхаттачар'я С., Кунду А., Саньял Г. Новий метод аудіо-стеганографії за допомогою M16MA. Int. J. Comput. Appl., 2011, т. 30, № 8, с. 26–34.
11. Куніаді Б., Пуспітанінгрум Д., Коастера Ф.Ф. Проектування та розробка програм застосування стеганографії текстових повідомлень на цифровому

аудіо за допомогою методу найменших значущих бітів. *J. Rekursif*, 2017, т. 5, № 3, с. 285–297.

12.Роласріс. Аналіз аудіо-водяного знаку на основі методів дискретного вейвлет-перетворення та фазового кодування в режимі амбієнту. 2016, т. 3, № 2, с. 52.

13.Бендер В., Грул Д., Морімото Н., Лу А. Техніки сховання даних. *IBM Syst. J.*, 1996, т. 35, № 3–4, с. 313–335.

14.Альсабхані А.А., Рідзуан Ф., Азні А.Г. Адаптивний багаторівневий метод фазового кодування в аудіо-стеганографії. *IEEE Access*, 2019, т. 7, с. 129291–129306.