ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ імені І.І.МЕЧНИКОВА

(повне найменування вищого навчального закладу)

Факультет математики, фізики та інформаційних технологій

(повне найменування інституту, назва факультету (відділення))

Кафедра математичного забезпечення комп'ютерних систем

(повна назва кафедри (предметної, циклової комісії))

Дипломна робота

на здобуття ступеня вищої освіти «магістр»

(освітньо– кваліфікаційний рівень)

на тему: Методи приховування інформації у відеофайлах

Techniques for hiding information in video files

Виконав: студент денної форми навчання

спеціальності 123 – Комп'ютерна інженерія

(шифр і назва напряму підготовки, спеціальності)

Тарабаєва Дарія Денисівна

(прізвище, ім'я, по– батькові)

Керівник к.фіз.-мат.н., доц.Шпінарева І. М.

(науковий ступінь, вчене звання, прізвище та ініціали, підпис)

Рецензент д.техн.н., доц. Гунченко Ю.О.

(науковий ступінь, вчене звання, прізвище та ініціали)

Рецензент к.техн.н, доц. Рудніченко М.Д.

(науковий ступінь, вчене звання, прізвище та ініціали)

Рекомендовано до захисту:

Протокол засідання кафедри

№_____ від «___»_____ 2019 р.

Завідувач кафедри

_____ _Є.В. Малахов_

(підпис) (прізвище, ініціали)

Захищено на засіданні ЕК № ___

протокол № __ від «___» ____ 2019 р.

Оцінка_____/_____/_____

(за національною шкалою, шкалою ECTS, бали)

Голова ЕК

_____ _О.О. Арсірій_

(підпис) (прізвище, ініціали)

Одеса – 2019

АНОТАЦІЯ

У дипломній роботі розробляється тема «Методи приховування інформації в відеофайлах».

Задача приховування інформації для її непомітної передачі стає все більш актуальною з кожним днем. Різноманітність існуючих стеганографічних алгоритмів та величезна кількість стегоконтейнерів для приховування інформації, роблять цю область привабливою та необхідною для спеціалістів та звичайних користувачів. Через ріст пропускної здатності каналів зв'язку і збільшення обсягів інформації, що поставляється, все більшої актуальності набуває питання приховування інформації в відеофайлах.

Метою даної роботи є підвищення ефективності методів вбудовування інформації в відеофайл за допомогою модифікації існуючих алгоритмів.

В результаті проведених в роботі досліджень було розглянуто структури відеоформатів, досліджені стеганографічні підходи для приховування інформації в відео контейнерах, розглянуто існуючі алгоритми. У дипломній роботі були сформовані вимоги до стегосистеми та був запропонований модифікований алгоритм на основі алгоритмів Ouled–Zaid, Makhloufi & Olivier і Wang, що дозволило збільшити стійкість і непомітність вбудовування повідомлення. Виконано програмну реалізацію системи для вбудовування/вилучення інформації з відеофайлу.

В роботі проведено аналіз модифікованого алгоритму та алгоритмів Ouled–Zaid, Makhloufi & Olivier і Wang на якість приховування інформації у зображенні (PSNR) та пропускну здатність. Аналіз продемонстрував, що модифікований алгоритм має більшу стійкість до атак, а також більшу непомітність наявності вбудовування.

В результаті проведеної роботи отримано алгоритм, який дозволяє надійно приховувати повідомлення у відеофайл.

АННОТАЦИЯ

В дипломной работе разрабатывается тема «Методы сокрытия информации в видеофайлах».

Задача сокрытия информации для ее незаметной передачи становится все более актуальной с каждым днем. Разнообразие существующих стеганографических алгоритмов и огромное количество стегоконтейнер для сокрытия информации, делают эту область привлекательной и необходимой для специалистов и обычных пользователей.

Целью данной работы является повышение эффективности методов встраивания информации в видеофайл с помощью модификации существующих алгоритмов.

В результате проведенных в работе исследований были рассмотрены структуры видеоформатов, исследованы стеганографические подходы для сокрытия информации в видео контейнерах, рассмотрены существующие алгоритмы. В дипломной работе были сформированы требования к стегосистеме и был предложен модифицированный алгоритм на основе алгоритмов Ouled–Zaid, Makhloufi & Olivier и Wang, что позволило увеличить устойчивость и незаметность встраивания сообщения.

В работе проведен анализ модифицированного алгоритма и алгоритмов Ouled–Zaid, Makhloufi & Olivier и Wang на качество сокрытия информации в изображении (PSNR) и пропускную способность. Анализ показал, что модифицированный алгоритм имеет большую устойчивость к атакам, а также большую незаметность наличия встраивания.

В результате проведенной работы получен алгоритм, который позволяет надежно скрывать сообщения в видеофайл.

ANNOTATION

The thesis develops the topic "Methods of hiding information in video files".

The task of hiding information for unnoticed transmission is becoming more and more relevant every day. The variety of existing steganographic algorithms and the huge number of information containers make this area attractive and necessary for professionals and ordinary users. With the increase in bandwidth of communication channels and the increasing volume of information supplied, the issue of hiding information in video files is becoming increasingly relevant.

The purpose of this work is to improve the efficiency of embedding information in a video file by modifying existing algorithms.

As a result of the researches, the structures of video formats were examined, steganographic approaches for concealing information in video containers were investigated, and existing algorithms were considered. In the thesis the requirements for the stegosystem were formed and a modified algorithm was proposed based on the algorithms Ouled–Zaid, Makhloufi & Olivier and Wang, which allowed to increase the stability and invisibility of embedding the message. The system implementation for embedding / removing information from a video file is executed. This paper analyzes the modified algorithm and the Ouled – Zaid, Makhloufi & Olivier, and Wang algorithms for the quality of image hiding (PSNR) and bandwidth. The analysis showed that the modified algorithm has greater resistance to attacks, as well as greater invisibility of the presence of embedding.

The result of the work obtained an algorithm that allows you to safely hide messages in a video file.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

MPEG (Moving Picture Experts Group – група експертів по рухомому зображенню)

PSNR – peak signal–to–noise ratio – ПВСШ – пікове відношення сигнал/шум;

ДВП – дискретно вейвлет перетворення;

ДКП – дискретно косинусне перетворення;

ОДВП – обратне дискретно вейвлет перетворення;

ЦВЗ – цифровий водяний знак.

ВСТУП

Використання стеганографії обумовлено (більшою мірою) необхідністю виконувати захист від несанкціонованого доступу, від копіювання або від крадіжки інформації. У зв'язку з інтенсивним розвитком мультимедійних технологій питання захисту інтелектуальної власності та авторських прав на інформацію, яка представлена в цифровому вигляді стало актуальним. Як приклади можна згадати аудіо-файли, фотографії та відеозаписи. Очевидно, що всі достоїнства, що забезпечуються поданням і передачею інформації в цифровому вигляді, можуть бути знецінені при їх несанкціонованій зміні або крадіжці. Отже, необхідними є розробка різноманітних захисних методів (як технічного, так і організаційного характеру).

Одним з найбільш перспективних напрямків у цій галузі є вбудовування тексту, невидимих міток (цифрових водяних знаків) в об'єкт захисту. Практично всі провідні світові фірми зацікавлені і активно займаються розробками подібного роду. Популярність додатків, в основі яких лежить використання цифрового відео, диктує необхідність захищати авторські права, а також реалізовувати комплекс заходів, пов'язаних із запобіганням незаконного копіювання і поширення інформації.

Одним з найбільш добре вивчених напрямків в даній області є методика вставки даних аутентифікації, таких як інформації про власника і логотипу, в цифрове медіа без порушення його якості. У разі виникнення суперечок про авторське право існує можливість отримання даних аутентифікації з контенту, що є досить авторитетним доказом права володіння.

Одним з таких методів вставки є використання цифрового водяного знаку в якості даних аутентифікації. ЦВЗ може бути вставлений в мультимедіа об'єкт з можливістю його подальшого вилучення для підтвердження права володіння. Як об'єкт зазвичай виступають зображення, аудіо або відео. Алгоритми стеганографії повинні відповідати критеріям непомітності, а також надійності

при спробі атак всіх видів, спрямованих на його видалення або зміна. Велика частина стеганографічних алгоритмів орієнтовані на нерухомі зображення або відеоролики. Частина алгоритмів розроблена для нестислого відео, однак існують алгоритми вставки інформації безпосередньо в стислий відео. У зв'язку з властивим структурі відеокадрів надмірності, відеосигнали є досить вразливими до атак, таким як усереднення кадру, підміна кадрів, видалення кадрів і атакам, пов'язаними зі статистичним аналізом кадрів.

Технологія використання цифрових водяних знаків та повідомлення у відео – контент має низку особливостей. Одним з головних вимог до таких алгоритмів є досягнення необхідної надійності. Більшість використовуваних методик впровадження ЦВЗ/інформації в відео–контент подібні технологіям, які застосовують для статичних зображень. Однак впровадження інформації в відео–ролики тягне за собою ряд труднощів, яких не було при впровадженні цифрових водяних знаків в статичне зображення.

Актуальність даної теми полягає в запобігання відео піратства – нелегального розповсюдження копій фільмів і телепередач на дисках, цифрових носіях і шляхом копіювання через комп'ютерні мережі. За допомогою методів стеганографії можливо зберегти авторські права на відеофайли [1].

Метою даної роботи є підвищення ефективності методів вбудовування інформації в відеофайл за допомогою модифікації існуючих алгоритмів.

Для виконання поставленої мети необхідно вирішити такі задачі:

– провести аналіз існуючих відео форматів;

– провести огляд існуючих аналогічних стегосистем;

– дослідити стенографічні підходи і методи вбудовування інформації в відеофайли.

Об'єктом дослідження є процесс вбудовування інформації у відеофайли.

Предметом дослідження є методи вбудовування інформації у відеофайли різних форматів.

ВИСНОВКИ

В рамках даної дипломної роботи були досліджені існуючи методи та алгоритми вбудовування інформації у відеофайли, було прийнять рішення використовувати алгоритми основані на ДВП. Після дослідження алгоритмів, що використовують ДВП, було обрано алгоритм Ouled – Zaid,Makhloufi & Olivier та алгоритм Wang. Також розглянути структури існуючих стегоконтейнерів у які можна вбудовувати повідомлення.

У дипломній роботі були сформовані вимоги до стегосистеми та був запропонований модифікований алгоритм на основі алгоритмів Ouled – Zaid, Makhloufi & Olivier і Wang, що дозволило збільшити стійкість і непомітність вбудовування повідомлення.

Було проведено проектування додатку на обраному інструментальному середовищі розробки та виконано програмну реалізацію системи для вбудовування/вилучення інформації в/з відеофайлу. Результатом роботи є модифікований алгоритм який вбудовує повідомлення на третій рівень розкладання у LL, LH, HH діапазони, та демонструє високий показник PSNR, не потребує наявності вхідного контейнеру для отримання повідомлення, крім того демонструє задовільні результати пропускної здатності.

У дипломній роботі проведено аналіз модифікованого алгоритму на основі порівняння з двома існуючими. Аналіз продемонстрував, що модифікований алгоритм має більшу стійкість до атак, а також більшу непомітність наявності вбудовування, а саме 45,3 для модифікованого алгоритму, для порівняння алгоритм Wang має 40,1, а алгоритм Ouled – Zaid, Makhloufi & Olivier 36,2.

СПИСОК ЛІТЕРАТУРИ

1. Грибунин В.Г., Оконов И.Н., Туринцев И.В. Цифровая стеганография. – М.:Солон– Пресс, 2002.– 272 с.
2. Хорошко В.О., Азаров О.Д., Шелест М.Э., Основы компьютерной стеганографии: Учебное пособие для студентов и аспирантов.– Винница: ВДТУ, 2003.– 143 с.
3. K. Anusudha, S. Ayeswarya A Robust Digital Watermarking of Satellite Image at Third Level DWT Decomposition // Proceedings of the International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007) – 2007. – Volume 4. – P. 78– 82.
4. Li Fan, Tiegang Gao A Novel Blind Robust Watermarking Scheme Based on Statistic Characteristic of Wavelet Domain Coefficients // Proceedings of the 2009 International Conference on Signal Processing Systems – 2009 – P. 121– 125.
5. Li Zhiyong An Improved Algorithm of Digital Watermarking Based on Wavelet Transform // Proceedings of the 2009 WRI World Congress on Computer Science and Information Engineering – 2009. – Volume 7. – P. 280– 284.
6. T. Bianchi, A. Piva, and M. Barni Composite signal representation for fast and storage– efficient processing of encrypted signals // IEEETrans. Inf. Forensics Security – Mar. 2010. – vol. 5, no. 1 – P. 180–187.
7. Ouled– Zaid A., Makhlou A., Olivier C. Improved QIM– Based Watermarking Integrated to JPEG2000 Coding Scheme // Springer journal of Signal, Image and Video Processing – 2009. – Vol. 3, P. 197– 207.
8. Fan Y., Chiang A., Shen J. ROI– based watermarking scheme for JPEG 2000 // Springer journal of Circuits, Systems, and Signal Processing. V27(5) – 2008. – P. 763– 774.

9. Perez– Freire L., Perez – Gonzalez F. Security of lattice– based data hiding against the watermarked– only attack. // IEEE Transactions on Information Forensics and Security – Vol. 3(4) – 2008 – P. 593– 610.

10. Braci S., Boyer R., Delpha C. Security evaluation of informed watermarking schemes // In: 16th IEEE International Conference on Image Processing (ICIP), Cairo, Egypt, Proc. ICIP 2009 – November 2009 – P. 117– 120.

11. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография: Теория и практика И: "МК– Пресс" 2006. – 283 с.

12. Chuang Lin , Jeng– Shyang Pan , Chia– An Huang, A Subsampling– Based Digital Image Watermarking Scheme Resistant to Permutation Attack // IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences – March 2008. – v.E91– A n.3 – P.911– 915.

13. Husrev T. Sencar, Mahalinggam Pamkumar, Data Hiding Fundamentals And Applications. Content Security In Digital Multimedia/ ELSEVIER science and technology books – 2004. – P. 364.

14. Трегулов Т. С. Оценка устойчивости цифрового водяного знака встроенного в изображение формата JPEG 2000 к внешним воздействиям // Естественные и технические науки. – Москва: изд. –Спутник +‖, декабрь 2013 г. – No6 (68), С. 445– 448.

15. Тарабаєва Д.Д., Шпінарева І.М. Вейвлет перетворення для приховування інформації в відеофайлах.//Тезіси VIII Міжнародна науково – практична конференція «Інформаційні управляючі системи та технології . Одеса, 2019. – С. 82.

16. Тарабаєва Д.Д., Шпінарева І.М. Аналіз вбудовування інформації у зображення за допомогою вейвлет перетворень.// Збірник тез доповідей III Всеукраїнської науково-практичної конференції молодих учених,

студентів і курсантів «Захист інформації в інформаційно– комунікаційних системах», Львів, 2019 – С.118-120

17. Тарабаєва Д.Д., Шпінарева І.М. Методи приховування інформації у відеофайлах. //XVI Всеукр.конференції студентів і молодих науковців «Інформатика, інформаційні системи та технології».Одеса, 27 квітня 2019 р. – Одеса, 2019. – С.196-198