УДК 004.056 DOI: 10.30748/soi.2019.158.13

Н.В. Шостак, А.А. Астраханцев

Харківський національний університет радіоелектроніки, Харків

АНАЛІЗ СТІЙКОСТІ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ВБУДОВУВАННЯ ДАНИХ В ВІДЕОФАЙЛИ ДО АТАК

В умовах стрімкого зростання інформаційно-телекомунікаційних технологій найбільш активно розвиваються стеганографічні алгоритми та способи їхнього застосування в кібернетичному просторі. Цифрове відео є одним з найпопулярніших мультимедійних даних, що поширюється в мережі Інтернет. Тому набувають широкого впровадження алгоритми вбудовування цифрових водяних знаків (ЦВЗ) у відеофайли. В даній роботі зроблено порівняльний аналіз сучасних методів вбудовування ЦВЗ у відеофайли з метою виявлення методів з найкращими показниками по стійкості до атак та скритності вбудовування ЦВЗ, та дослідження методів підвищення завадостійкості та стійкості до основних атак.

Ключові слова: *стеганографія, відеофайл, алгоритм, ЦВЗ, аутентифікація, Кох-Жао, завадостійкий код, Рід-Соломон.*

Вступ

Постановка проблеми. В даний час кількість людей, які активно використовують мережу Інтернет в якості основного джерела отримання інформації, неухильно зростає. При цьому частка онлайн відеоглядачів вже істотно перевищує частку телеглядачів. При цьому спектр доступного відеоконтенту дуже широкий. Це можуть бути відеоподкасти або відеоблог, створювані користувачами-любителями, або професійні репортажі новинних агентств, записи телевізійних програм, повнометражні фільми та серіали. І якщо простих авторів-відеоблогерів не надто хвилює питання захисту авторських прав, то для студій і творчих об'єднань, для яких виробництво відео є основною діяльністю і джерелом доходу, це питання є досить важливим. Проблема піратства в області відеоконтенту сьогодні актуальна як ніколи.

Аналіз останніх досліджень і публікацій. В ході досліджень було проведено аналіз сучасних публікацій. У роботах [1–2] описано методи вбудовування в просторову область зображення та в область перетворень. У роботі [4] виконано дослідження стійкості алгоритмів захисту авторських прав на відеопродукцію з урахуванням показників якості.

Мета статті – виконати аналіз сучасних стеганографічних методів вбудовування ЦВЗ в відео з метою виявлення методів з найкращими показниками по стійкості до атак та скритності вбудовування ЦВЗ, та дослідження методів підвищення завадостійкості та стійкості до основних атак.

Виклад основного матеріалу

I. Огляд алгоритмів та принципів вбудовування ЦВЗ в відео

На сьогоднішній день ЦВЗ використовується як засіб захисту документів з фотографіями – паспортів, водійських посвідчень, кредитних карток з фотографіями. Об'єкти мультимедіа в цьому випадку будуть являти собою контейнери (носії) даних. Основні переваги використання ЦВЗ полягають в наявності умовної залежності між подією підміни об'єкта ідентифікації (фотографії) та наявності елемента захисту (прихованого ЦВЗ), та можливістю однозначно ідентифікувати джерело створення об'єкта ідентифікації. Існуючі алгоритми вбудовування в відео можна умовно поділити на три основні групи, в залежності від області, в яку вбудовується ЦВЗ: методи вбудовування в просторовій області, в область перетворень та методи вбудовування в відео, що стиснене за стандартом MPEG [1–2].

В ході дослідження були реалізовані декілька стеганографічних алгоритмів вбудовування інформації в відеофайли:

– метод вбудовування ЦВЗ на основі заміни НЗБ;

– метод вбудовування ЦВЗ на основі алгоритму Коха-Жао;

– метод вбудовування ЦВЗ на основі ДВП.

Також були проаналізовані відкриті джерела щодо методів вбудовування ЦВЗ у відео, що мають схожі властивості з реалізованими методами [3]. Для порівняльного аналізу з реалізованими методами були вибрані два алгоритми:

– автентифікація відео на основі вмісту за допомогою ДВП;

– ефективне вбудовування ЦВЗ в відео з використанням ДВП.

В реалізованих методах відеофайл розглядається як послідовність кадрів. Кожен кадр обробляється як незалежне зображення і ЦВЗ вбудовується у кожний кадр окремо.

Відеофайл зчитується і розбивається на кадри у форматі адитивної кольорової моделі RGB. На на-

ступному кроці виконується перетворення у просторове кодування YCbCr за допомогою формул:

$$Y = 0,299 \cdot R + 0,587 \cdot G + 0,144 \cdot B; \quad (1)$$

$$C_b = 128 + 37,797 \cdot R - 74,203 \cdot G + 112 \cdot B; \quad (2)$$

$$C_r = 128 + 112 \cdot R - 93,786 \cdot G - 18,214 \cdot B, \quad (3)$$

де Y – компонента яскравості моделі YCbCr;

C_b – синя кольороворізницева компонента моделі YCbCr;

C_r – червона кольороворізницева компонента моделі YCbCr;

R – червона компонента моделі RGB;

G – зелена компонента моделі RGB;

B – синя компонента моделі RGB.

Для приховування використовується лише компонент яскравості Y кольорового простору YCbCr. Зворотне перетворення виконується за допомогою формул:

$$R = Y + 1,371 \cdot (C_r - 128); \quad (4)$$

$$G = Y - 0,698 \cdot (C_r - 128) - 0,336 \cdot (C_b - 128); \quad (5)$$

$$B = Y + 1,372 \cdot (C_b - 128) \cdot \quad (6)$$

ЦВЗ зчитується у форматі адитивної кольорової моделі RGB. У зв'язку з тим, що ЦВЗ – чорно-біле зображення, можливі лише 2 значення кольору пікселів – *0xFF* для білого і *0x00* для чорного. Тому при вбудовуванні інформації використовується двійкове кодування: *0xFF* кодується як "1", а *0x00* – "0".

II. Пропозиції щодо підвищення стійкості алгоритмів вбудовування

Стійкість реалізованих методів до певних атак можна покращити використанням завадостійких кодів. Завадостійкими кодами називаються коди, що дозволяють виявляти або виявляти та виправляти помилки в отриманих кодових комбінаціях. Одним з поширених прикладів таких кодів є код Хемінга. Коди Хемінга дозволяють виправляти одиничну помилку (помилка в одному біті) і знаходити подвійну помилку.

Для підвищення стійкості реалізованих методів було запропоновано використовувати завадостійкі коди Хемінга (7,4) – в цьому випадку чотири біта ЦВЗ кодується сьома бітами коду [4] та коди Ріда-Соломона.

У кодах Ріда-Соломона повідомлення представляється у вигляді набору символів деякого алфавіту. Тобто при кодуванні повідомлення, представленого двійковим кодом, розбиваємо його на групи по 4 біта і далі працюємо з кожною групою як з елементом поля Галуа відповідного ступеню.

Отриманий код використовується в якості ЦВЗ при вбудовуванні інформації.

III. Основні типи атак на ЦВЗ та аналіз стійкості алгоритмів формування ЦВЗ

Під атакою на стеганографічну систему розуміється спроба виявити, витягти, змінити або видалити приховану інформацію. Здатність стеганографічної системи протистояти атакам називається стеганографічною стійкістю.

В роботі розглядалися лише атаки, що направленні на порушення цілісності ЦВЗ. Атаки, що направлені на порушення цілісності ЦВЗ, можна поділити на 2 групи: геометричні атаки та атаки обробки сигналів. Геометричні атаки модифікують кадри зображень завдяки різним геометричним перетворенням. Серед геометричних атак були реалізовані:

- афінні перетворення;
- локальні спотворення.

При використанні атак обробки сигналів відеофайли розглядаються як сигнали. Тому атаки направлені на спотворення сигналу, а не кадрів. Серед атак обробки сигналів були реалізовані наступні:

- накладення шуму на відеофайл;
- перекодування відеофайлу;
- стиснення відеофайлу.

Для аналізу стійкості методу вбудовування ЦВЗ у відеофайл до певних видів атак необхідно провести порівняльний аналіз оригінального ЦВЗ з вилученим ЦВЗ з відеофайлу, що піддався атакам.

Афінні перетворення – перетворення площини, що мають такі властивості:

- множина точок, яка в початковій системі координат задовольняє деяке рівняння, переходить у множину точок, координати яких у новій системі задовольняють таке саме рівняння;
- відношення площ і об'ємів геометричних фігур зберігається;
- зберігається просте співвідношення трьох точок;
- існує єдине перетворення площини, що переводить трійку точок, які не належать одній прямій, у нову трійку точок, які також не належать прямій;
- якщо початкова та нова системи координат є декартовими з однаковими одиничними відрізками по осях, то при перетвореннях зберігаються всі метричні властивості геометричних фігур.

До афінних перетворень відносять повороти, стиснення, масштабування зображень. Афінні перетворення характеризуються мірою перетворення *ZZ*.

Приклад афінних перетворень представлений на рис. 1.

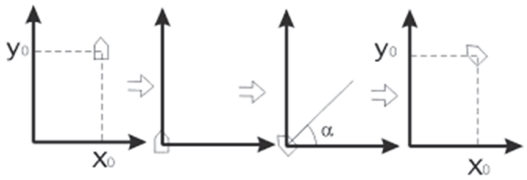

Рис. 1. Приклад афінних перетворень

Локальні спотворення – це такі спотворення кадру відеофайлу, при яких з певною ймовірністю можливі перестановки сусідніх пікселів.

Для дослідження стійкості реалізованих методів були використані атаки з використанням афінних перетворень при Z = (0.03, 0.06, 0.09) і атаки з використанням локальних спотворень при P = (0.1, 0.15, 0.2).

Як видно з рис. 2, всі методи при різних значеннях порогу вбудовування P є нестійкими до атак з використанням афінних перетворень. Однак до атак з використанням локальних спотворень методи на основі Коха-Жао та ДВП мають більшу стійкість, ніж метод на основі НЗБ [5].

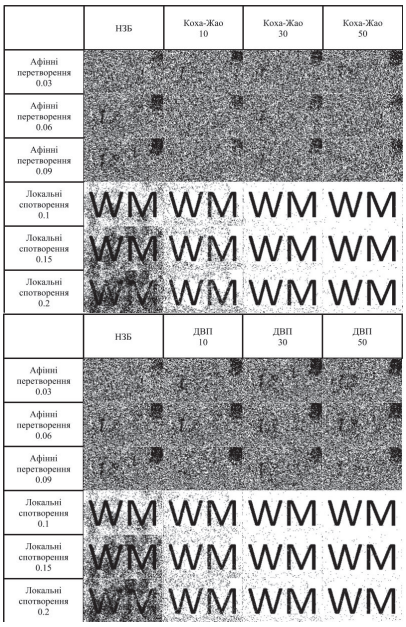

Рис. 2. Результати вилучення цифрових водяних знаків після проведення геометричних атак (джерело відпрацьовано автором)

Також можна зробити висновки, що при збільшені значенні порогу вбудовування P стійкість алгоритмів до атак збільшується.

Результати вилучення ЦВЗ після проведення геометричних атак представлені на рис. 3.

Як видно з рис. 3, проаналізовані методи при різних значеннях порогу вбудовування P є нестійкими до атак з використанням афінних перетворень.

Однак і до атак з використанням локальних спотворень проаналізовані методи не мають більшу стійкість, ніж метод на основі ДВП.

Шум – це випадкові або навмисні спотворення даних в процесі їх зберігання, обробки чи передачі по системам зв'язку [6]. В ході дослідження в якості шумової послідовності використовувалися:

1) Псевдовипадкова числова послідовність (ПВЧП), яка накладалася на кадри відеофайлу. ПВЧП характеризується мірою шуму N. Міра шуму показує, до яких максимальних спотворень ПВПЧ може привести. Приклад шуму на основі ПВЧП приведений на рис. 4.

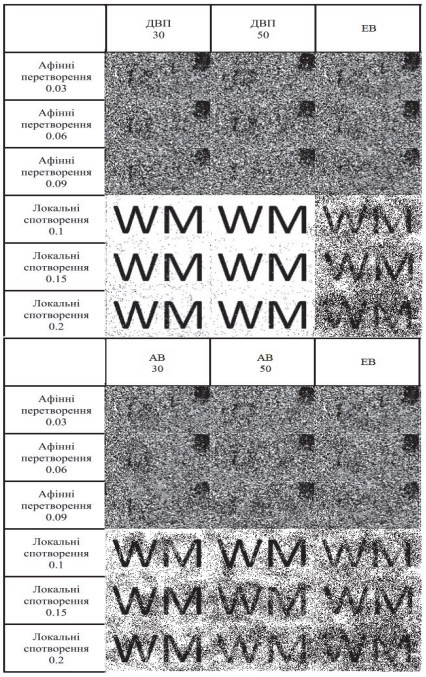

Рис. 3. Результати вилучення цифрових водяних знаків після проведення геометричних атак (джерело відпрацьовано автором)

Рис. 4. Приклад шуму на основі псевдовипадкової числової послідовності

2) Шум сіль-перець, що представляє собою псевдовипадкові повністю білі або чорні пікселі. Цей вид шуму характеризується імовірністю появи спотворення p. Приклад накладання шуму сіль-перець наведений на рис. 5 [7].

Рис. 5. Приклад накладання шуму сіль-перець на зображення

При перекодуванні відеофайлів використовуються різні методи для перетворення і збереження відеофайлу на носіях інформації, що може вплинути на вбудований водяний знак. Були використані вбудовані кодеки бібліотеки ffmpeg: flv, h.264, mpeg1, mpeg2, mpeg4.

Стиснення відеофайлу – технологія цифрової компресії телевізійного сигналу, що дозволяє скоротити кількість даних, які використовуються для відображення відеопотоку. Стиснення відеофайлу дозволяє ефективно зменшувати потік, необхідний для передачі відеофайлу каналами радіомовлення. Однак при стисненні з відеофайлу видаляються маловажливі дані, що може вплинути на вбудований водяний знак. Одним із сучасних міжнародних стандартів в області стиснення відеофайлів є H.264. Саме цей алгоритм стиснення використовується у mp4 відеофайлах. Для оцінки стійкості методів до стиснення була використана бібліотека ffmpeg з вбудованою можливістю стиснення відеофайлів формата mp4. Стиснення файлів mp4 характеризується параметром *qq*, що характеризує ступінь стиснення [8].

Для дослідження стійкості реалізованих методів були використані атаки перекодування, стиснення при параметрі q = (3, 6, 9), накладення шумів: ПВЧП при мірі шуму N=(0.03,0.06,0.09), шум сіль-перець при ймовірності появи спотворення P=(0.01,0.015,0.02).

Результати проведення атак наведені на рис. 6.

Як видно з рис. 6, методи на основі НЗБ не є стійкими до досліджених видів атак, тому недоцільно використовувати ці методи для вбудовування ЦВЗ у відеофайли. З іншого боку, методи на основі Коха-Жао та ДВП мають велику стійкість до атак накладення шуму. До того ж ці методи мають більшу стійкість до атак перекодування, а при значеннях порогу вбудовування P = 30 і більше дозволяють вилучати ЦВЗ без жодних спотворень.

Результати проведення атак наведені на рис. 7.

Як видно з рис. 7, проаналізовані методи не є стійкими до досліджених атак стиснення відеофайлів, тому недоцільно використовувати ці методи для вбудовування ЦВЗ у стиснені відеофайли. З іншого боку проаналізований алгоритм ЕВ не є стійким до атак накладення шуму і зазнає більші спотворення при накладенні шуму сіль-перець. Однак проаналізований алгоритм АВ, як і реалізований метод на основі ДВП, має більшу стійкість до атак перекодування, а при значеннях порогу вбудовування P = 30 і більше, дозволяють вилучати ЦВЗ без жодних спотворень.

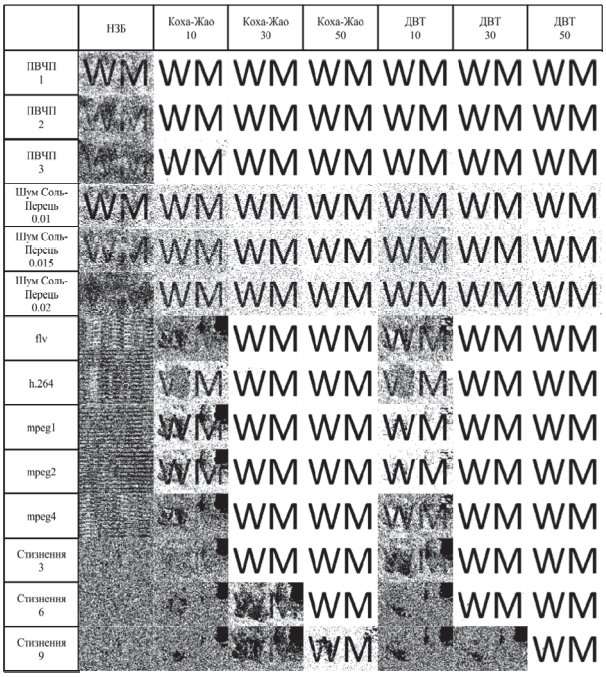

Рис. 6. Результати вилучення цифрових водяних знаків після проведення атак обробки сигналів (джерело відпрацьовано автором)

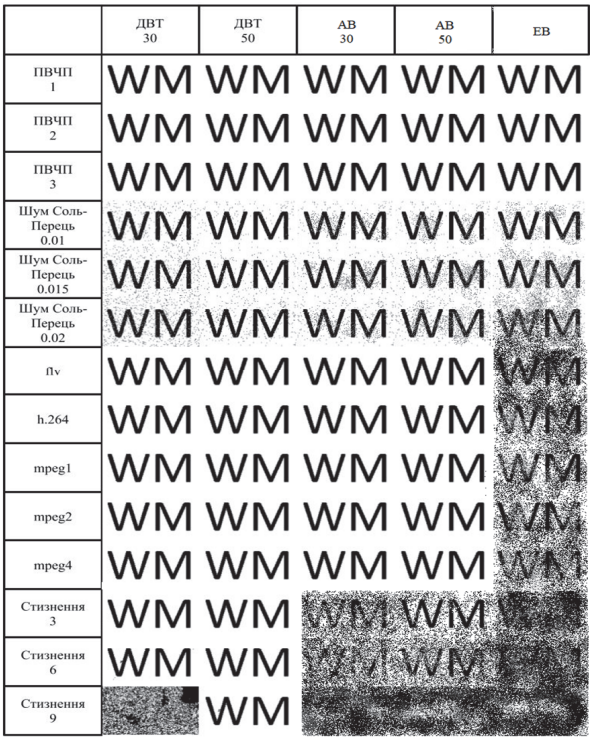

Рис. 7. Результати вилучення цифрових водяних знаків після проведення атак обробки сигналів (Джерело: відпрацьовано автором)

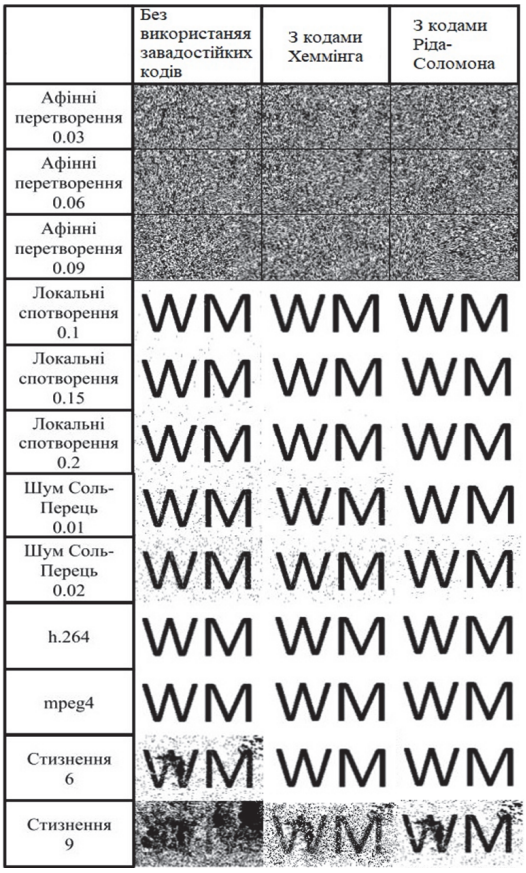

Рис. 8. Результати вилучення цифрових водяних знаків після проведення атак при застосуванні завадостійких кодів
(Джерело: відпрацьовано автором)

Для дослідження впливу використання завадостійких кодів Хеммінга та Ріда-Соломона на стійкість реалізованих методів до атак були використані тільки атаки, що мали найбільший вплив на ЦВЗ, що вилучається з атакованого відеофайлу, а саме:

– афінні перетворення;
– локальні спотворення;
– стиснення відео файлу;
– переформатування відео файлу.

Для порівняльного аналізу завадостійких кодів був використаний алгоритм вбудовування ЦВЗ на основі алгоритму Коха-Жао. Алгоритм вбудовування ЦВЗ на основі алгоритму Коха-Жао був вибраний у зв'язку з тим, що цей алгоритм займає середнє положення по стійкості до атак, що дає змогу оцінити переваги використання завадостійких кодів.

Результати проведення атак при використанні завадостійких кодів представлені на рис. 8.

Проаналізувавши результати, можна зробити висновок, що використання завадостійких кодів значно підвищує стійкість алгоритмів до проаналізованих атак. До того ж застосування завадостійких кодів Ріда-Соломона, через кращі самокоригувальні властивості, значно підвищує стійкість алгоритмів вбудовування цифрових водяних знаків у відеофайли.

Висновки

Також можна зробити висновки, що для того, щоб ЦВЗ, що вбудовується у відеофайл, був стійким до більшості атак, необхідно використовувати метод на основі ДВП і кодувати цифровий водяний знак за допомогою завадостійких кодів, що самокоригуються. Для найбільшої стійкості необхідно використовувати завадостійкі коди Ріда-Соломна. А у зв'язку з тим, що вбудовування ЦВЗ методом на основі ДВП не призводить до значних спотворень відеофайлу, це дає змогу вбудовувати два біти ЦВЗ у кожен блок ДВП.

Список літератури

1. Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с.

2. Грибунин В.Г. Цифровая стеганография / В.Г. Грибунин. – М.: СОЛОН-Пресс, 2002. – 272 с.

3. Офіціальний сайт IEEEXPLORE. Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking [Електронний ресурс]. – Режим доступу: http://ieeexplore.ieee.org/iel5/7221/19490/00900989.pdf.

4. Офіціальний сайт IEEEXPLORE. Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation [Електронний ресурс]. – Режим доступу: http://ieeexplore.ieee.org/abstract/document/638832.

5. Шостак Н.В. Дослідження стійкості алгоритмів захисту авторських прав на відеопродукцію / Н.В. Шостак, А.А. Астраханцев, С.В. Романько // Системи обробки інформації. – 2017. – № 2(148). – С. 138-143.

6. Офіціальний сайт RESEARCHGATE. A Survey of Steganographic Techniques in Information Techniques for Steganography and Digital Watermarking [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/245096254_A_survey_of_steganographic_techniques.

7. Офіціальний сайт RESEARCHGATE. Watermarking Digital Image and Video Data [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/3321350_Watermarking_digital_image_and_video_data_A_state-of-the-art_overview.

8. Офіціальний сайт CVML. Robust 3d dft video watermarking [Електронний ресурс]. – Режим доступу: http://cvml.unige.ch/publications/postscript/99/DeguillaumeCsurkaORuanaidhPun_eiswmc99.pdf.

9. Офіціальний сайт CSCJOURNALS. A waveletbased object watermarking system for mpeg4 video [Електронний ресурс]. – Режим доступу: http://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-160.

10. Офіціальний сайт RESEARCHGATE. Robust Digital Video Watermarking in the Spatial and Wavelet Domain [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/282323833_Robust_Digital_Video_Watermarking_in_the_Spatial_and_Wavelet_Domain.

11. Офіціальний сайт RESEARCHGATE. Review of Robust Video Watermarking Algorithms [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/43297129_Review_of_Robust_Video_Watermarking_Algorithms.

12. Офіціальний сайт RESEARCHGATE. A review of robust video watermarking technique [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/323970385_A_review_of_robust_video_watermarking_technique.

References

1. Konahovych, G.Ph. (2006), "*Komputernaia steganographyia. Teoryia y praktyka*" [*Computer steganography. Theory and practice*], MK-Press, Kyiv, 288 p.

2. Hrybunyn, V.G. (2002), "*Tsyfrovaia steganographia*" [*Digital steganography*], SOLON-Press, Moscow, 272 p.

3. The official site of IEEEXPLORE (2002), *Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking*, available at: www.ieeexplore.ieee.org/iel5/7221/19490/00900989.pdf.

4. The official site of IEEEXPLORE (2002), *Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation*, available at: https://ieeexplore.ieee.org/abstract/document/638832.

5. Shostak, N.V. and Astrahantsev, A.A. (2017), "Doslidzhennia stiikosti alhorytmiv zahystu avtorskyh prav na videoprodukciiu" [Investigating the Stability of Video Production Copyright Algorithms], *Information Processing systems*, No. 2(148), pp. 138-143.

6. The official site of RESEARCHGATE (1999), *A Survey of Steganographic Techniques in Information Techniques for Steganography and Digital Watermarking*, available at: https://www.researchgate.net/publication/245096254_A_survey_of_steganographic_techniques.

7. The official site of RESEARCHGATE (2000), *Watermarking Digital Image and Video Data*, available at: https://www.researchgate.net/publication/3321350_Watermarking_digital_image_and_video_data_A_state-of-the-art_overview.

8. The official site of CVML (1999), *Robust 3d dft video* watermarking, available at: www:cvml.unige.ch/publications/postscript/99/DeguillaumeCsurkaORuanaidhPun_eiswmc99.pdf.

9. The official site of CSCJOURNALS (2010), *A wavelet based object watermarking system for mpeg4 video*, available at: https://www.cscjournals.org/library/manuscriptinfo.php?mc=IJCSS-160.

10. The official site of RESEARCHGATE (2012), *Robust Digital Video Watermarking in the Spatial and Wavelet Domain*, available at: https://www.researchgate.net/publication/282323833_Robust_Digital_Video_Watermarking_in_the_Spatial_and_Wavelet_Domain.

11. The official site of RESEARCHGATE (2010), *Review of Robust Video Watermarking Algorithms*, available at: https://www.researchgate.net/publication/43297129_Review_of_Robust_Video_Watermarking_Algorithms.

12. The official site of RESEARCHGATE (2017), *A review of robust video watermarking* technique, available at: https://www.researchgate.net/publication/323970385_A_review_of_robust_video_watermarking_technique.

Надійшла до редколегії 30.05.2019
Схвалена до друку 13.08.2019

Відомості про авторів:

Шостак Наталя Володимирівна
аспірант
Харківського національного університету
радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0002-1267-1042

Астраханцев Андрій Анатолійович
кандидат технічних наук доцент кафедри
Харківського національного університету
радіоелектроніки,
Харків, Україна
https://orcid.org/0000-0002-6664-3653

Information about the authors:

Natalya Shostak
Doctoral Student
of Kharkiv National University
of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-1267-1042

Andrii Astrakhantsev
Candidate of Technical Sciences Senior Lecturer
of Kharkiv National University
of Radio Electronics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-6664-3653

АНАЛИЗ УСТОЙЧИВОСТИ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ВСТРАИВАНИЯ ДАННЫХ В ВИДЕОФАЙЛЫ К АТАКАМ

Н.В. Шостак, А.А. Астраханцев

В условиях стремительного роста информационно-телекоммуникационных технологий наиболее активно развивающимися являются стеганографические алгоритмы и способы их применения в кибернетическом пространстве. Цифровое видео является одним из самых популярных мультимедийных данных, распространяемых в сети Интернет.

Поэтому широкое применение получают алгоритмы встраивания цифровых водяных знаков (ЦВЗ) в видеофайлы. В данной работе сделан сравнительный анализ современных методов встраивания ЦВЗ в видеофайлы с целью выявления методов с лучшими показателями по устойчивости к атакам и скрытности встраивания ЦВЗ, и исследовании методов повышения помехоустойчивости и устойчивости к основным атакам.

Ключевые слова: *стеганография, видеофайл, алгоритм, ЦВЗ, аутентификация, Кох-Жао, помехоустойчивый код, Рид-Соломон.*

ANALYSIS OF THE STABILITY OF STEGANOGRAPHIC METHODS OF INTEGRATING DATA IN VIDEO FILES TO ATTACKS

N. Shostak, A. Astrakhantsev

In the conditions of rapid growth of information and telecommunication technologies, steganographic algorithms and methods of their application in cybernetic space are the most actively developing. Digital video is one of the most popular multimedia data that is distributed over the Internet. Therefore, widespread adoption of algorithms for embedding digital watermark in a video file. In this paper, In this paper, we study the embedding method based on the replacement of the least significant bit, the embedding method based on the Koch-Zhao algorithm, the embedding method based on the discrete wavelet transform (DWT), the method of authenticating video based on the content using the fiberboard, and the method of effectively embedding the watermark in the video using fiberboard. Also it was made a comparative analysis of modern methods of embedding a digital video player into a video file is made in order to identify methods with the best indicators for attack resistance and secrecy of the embedding of the digital watermark, and the study of methods to increase the noise immunity and resilience to the main attacks. After analyzing the results it can be concluded that the use of noise-proof codes greatly increases the stability of the algorithms to the analyzed attacks. In addition, the use of Reed-Solomon's jamming codes, due to better self-adjusting properties, greatly enhances the stability of embedding algorithms for digital watermarks in a video file. It is also possible to conclude that in order for the embedded digital watermark to be in the video file to be resistant to most attacks, it is necessary to use a fiber-based method and encode a digital watermark using self-regulating self-regulating codes with forward error correction. For the most stability it is necessary to use the jam-resistant codes of Reed-Solomon. And due to the fact that the embedding of the DWT by the method based on the fiberboard does not result in significant distortions of the video file, it enables to embed two bits of the DWT into each fiberboard unit.

Keywords: *steganography, videofile, algorithm, watermark, authentication, Koch-Zhao, error code, Reed-Solomon.*