УДК 004.056

Н.В. Шостак, А.А. Астраханцев, С.В. Романько

Харківський національний університет радіоелектроніки, Харків

ДОСЛІДЖЕННЯ СТІЙКОСТІ АЛГОРИТМІВ ЗАХИСТУ АВТОРСЬКИХ ПРАВ НА ВІДЕОПРОДУКЦІЮ

Останні роки зростає інтерес до стеганографії саме як до ефективного методу приховання даних, що дозволяє зберігати конфіденційність інформації. У даній роботі вирішується питання синтезу алгоритму захисту авторських прав на відеопродукцію, що має бути стійким до дії завад у каналах зв'язку та основних атак, та забезпечує підвищений рівень пропускної здатності. Проведено порівняльний аналіз існуючих методів вбудовування ЦВЗ у відеофайли з метою виявлення методів з найкращими показниками по стійкості до атак та скритності вбудовування ЦВЗ. Також, запропоновано власний метод для вбудовування водяних знаків.

***Ключові слова**: frequency domain watermarking, error-correction, capacity of videowatermarking, ЦВЗ, стійкість.*

Вступ

Одним з найважливіших питань, що вирішуються суспільством, на сьогоднішній день є забезпечення захисту інформації. Одним з ефективних шляхів вирішення проблеми захисту авторського права, що дозволяють перевірити правовласника цифрових відео файлів, є організація забезпечення автентичності за рахунок впровадження цифрових водяних знаків (ЦВЗ). Розробка методів вбудовування ЦВЗ з метою прихованої передачі утворює два основних напрямки розвитку сучасної стеганографії – аутентифікацію правовласника і організацію прихованої передачі інформації. На даний час у відкритій пресі пропонуються велика кількість стеганоалгорітми, які не позбавлені ряду істотних недоліків, залишаючи актуальним завдання розробки нових стеганографічних алгоритмів, що дозволяють одночасно забезпечувати приховану передачу даних і аутентифікацію відеофайлу.

Сьогодні у публікаціях [1; 2] запропонована дуже велика кількість різних стеганографічних методів, частина з яких є універсальними, або призначена для широкого кола завдань.

Існує велика кількість методів вбудовування ЦВЗ в нерухомі зображення та в відео. Більшість з них призначена для вбудовування у нестиснене відео, в той час як інші вбудовують ЦВЗ безпосередньо у стиснене відео.

I. Огляд стеганографічних алгоритмів

Останнім часом багато уваги приділяється алгоритмам вбудовування, що мають такі властивості, як стійкість до атак та прихованість вбудованої інформації. Ці алгоритми можна класифікувати за типом області, в яку вбудовується або вилучається цифровий водяний знак, їх пропускної здатності, продуктивності в режимі реального часу та стійкості до конкретних типів атак. 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 (рис. 1).

Рис. 1. Класифікація методів вбудовування в відео

Методи вбудовування ЦВЗ в просторовій області застосовуються для нестисненого відео. ЦВЗ, що вбудовується, зазвичай додається до компоненту яскравості та деяких компонентів кольорів, або тільки до компонентів кольорів. Перевагою цих методів є їх простота реалізації але їх не можна назвати стійкими. Алгоритми цього типу, як правило мають такі характеристики:

– ЦВЗ вбудовується в піксель або координатну область;

– до вихідного зображення не застосовуються ніякі перетворення під час вбудовування ЦВЗ;

– ЦВЗ вилучається з відео за допомогою модуляції з розширенням спектру;

– ЦВЗ може бути виявлений шляхом зіставлення очікуваного зображення з отриманим.

Основними перевагами просторових методів є те, що вони концептуально прості і мають дуже низьку обчислювальну складність. В результаті вони стали найбільш привабливими для застосування в відео, де функціонування в режимі реального часу є головним завданням. Однак, ці методи демонструють також деякі значні недоліки: необхідність повної просторової синхронізації призводить до високої чутливості до атак; відсутність врахування міжкадрових змін в часі робить ці методи вразливими до обробки відео та значному погіршенню прийнятих фреймів.

Найпростіший методом вбудовування в просторовій області полягає в заміни найменш значимих бітів (НЗБ) пікселів кадру бітами секретного повідомлення [3]. ЦВЗ малого розміру може бути вбудована кілька разів.

Головною перевагою методу НЗБ є те, що після вбудовування повідомлення в кадр максимальне відхилення значення інтенсивності в кадрі всього лише одиниця. Це не вплине на якість кадрів. Тому, при звичайних обставинах людина не зможе виявити вбудоване у кадр повідомлення, отже, передача повідомлення залишиться непоміченою для звичайної людини.

Можна зауважити, що даний метод є стійким до таких атак, як обрізка, тому що навіть якщо більшість з множини водяних знаків втрачається у разі такої атаки на кадр, хоча б один водяний знак можна буде вилучити.

Методи на основі кореляції дозволяють вбудовування ЦВЗ в просторову область завдяки використанню кореляційних властивостей шумових псевдовипадкових схем, які є адитивними [4]. Ці схеми використовуються для вбудовування водяних знаків, оскільки вони мають хороші кореляційні властивості і стійкі до перешкод. Псевдовипадкові шумові (ПШ) послідовності використовуються з причин, зазначених нижче:

1. Для їх формування необхідне лише знати ініціалізуючу послідовність.

2. Дуже важко передбачити цю послідовність, якщо не буде відома ініціалізуюча послідовність і алгоритм формування.

В методах вбудовування в область перетворень, водяний знак розподіляється по області перетворення. Для методів в області перетворень існує кілька класів методів, що базуються на різних функціях перетворення, основними з яких є дискретне косинусне перетворення (ДКП), дискретне вейвлет-перетворення (ДВП) та дискретне перетворення Фур'є (ДПФ).

Основною перевагою запропонованих методів в області перетворень є те, що вони можуть використовувати особливі властивості альтернативних областей для усунення обмежень методів вбудовування в просторовій області або для підтримки додаткових функцій.

Одними з найбільш поширених на сьогодні методів є методи дискретного косинусного перетворення. ДКП застосовується в відео, яке розділене на кадри, що розділені на різні частотні діапазони і дозволяє набагато легше вставляти цифрові водяні знаки в середню смугу частот зображення. Середні смуги частот вибирають тому, що в них немає візуально важливих частин зображення (низьких частот) і які не видаляються під час компресії та не псуються під час дії шуму (високі частоти). Один з таких методів використовує порівняння коефіцієнтів ДКП середнього діапазону для кодування одного біта в блок ДКП.

Іншою можливою областю для вбудовування водяних знаків є простір вейвлетів. Основна ідея дискретного вейвлет-перетворення у процесі обробки зображення полягає в розкладанні зображення в підзображення різних просторових та частотних областей. ДВТ розділяє зображення на апроксимацію первинного кадра відео (зображення з низькою роздільною здатністю) (LL) а також результату проходження його по горизонталях (HL), вертикалях (LH) та діагоналях (HH). Потім процес може бути повторений, для розрахунку вейлет-компонентів більш високого порядку (наприклад, рівня 2, як показано на рис. 2).

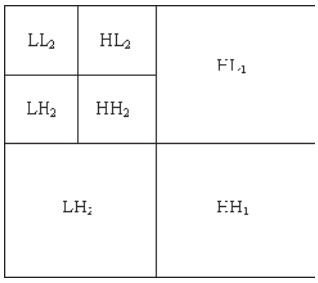

Рис. 2. 2-рівневе дискретне вейвлет-перетворення

В основному методи вбудовування ЦВЗ в відео використовують MPEG-1, MPEG-2 і MPEG-4 стандарти. У цих методиках впровадження ЦВЗ і стиснення об'єднані, щоб зменшити складність обробки відео. Стиснення в блокових методах, таких як MPEG-2 отримується за допомогою двонаправленого і прямого передбачення кадру для усунення часової надмірності, а у статистичних методах для усунення просторової надмірності. Методи вбудовування цифрового водяного знаку в відео, що стиснене за стандартом MPEG дуже чутливі до повторної компресії з різними параметрами, а також до переформатування. Це один

з основних недоліків. Існує велика кількість методів, на основі форматів MPEG-2 і -4, в тому числі алгоритми, засновані на модифікації групи кадрів, високочастотного перетворення ДКП коефіцієнтів та класифікації ДКП блоків.

В стандарті MPEG використовуються три типи кадрів: I-кадри, P-кадри і B-кадри. Кодування I кадрів схоже на JPEG, через використання сусідніх пікселів простору кадру для стиснення надлишкової інформації; P-кадр повинен використовувати попередній кадр при кодуванні і поточний кадр може бути використаний в якості опорного кадру для прогнозування. B-кадру потрібен попередній кадр і наступний кадр для прогнозування. Методика впровадження водяних знаків в стиснене відео, полягає у вбудовуванні водяного знаку в послідовність бітів стиснених за допомогою стандарту кодування, наприклад, MPEG-2 або MPEG-4 і т.д. Цей метод має більш низьку обчислювальну складність, в порівнянні з іншими методами.

II. Модифікований метод на основі заміни частотних коефіцієнтів

В рамках дослідження були реалізовані декілька стеганографічних алгоритмів вбудовування інформації в відео:

- метод на основі НЗБ;
- метод Коха-Жао;
- модифікований метод на основі заміни частотних коефіцієнтів (Коха-Жао) з використанням кодів Хемінга.

В якості стегоконтейнеру виступає кольоровий трьохканальний відеофайл з розміром кадрів 1280×720 пікселів. В якості інформації, що вбудовується, використовується чорно-біле (одноканальне) зображення (ЦВЗ) розмірністю 160×90 пікселів.

Відеофайл зчитується і розбивається на кадри у форматі адитивної кольорової моделі RGB. На наступному 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 кольроворізницева компонента моделі YCbCr;

C_r – червона кольроворізницева 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:

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

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

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

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".

Для застосування методу заміни частотних коефіцієнтів, відеофайл необхідно розглядати як послідовність кадрів. Кожен кадр розглядається як незалежне зображення і ЦВЗ вбудовується у кожний кадр.

Під час дослідження були запропоновані наступні модифікації методу:

- в якості області вбудовування була вибрана побічна діагональ матриці ДКП;
- реалізована можливість вбудовування до 4 бітів ЦВЗ в кожен блок ДКП. У кожному блоці вибирається до 4 пар різних елементів матриці ДКП, і в кожну з цих пар вбудовується біт ЦВЗ;
- реалізована нормалізація блоку після зворотнього ДКП. Якщо інформація вбудовується в блок, що має елементи зі значеннями яскравості Y, близькими до значень граничних елементів діапазону (0 та 255), після зворотнього ДКП значення цих елементів можуть вийти за граничні значення діапазону. При записуванні у відеофайл ці елементи будуть призводити до значних спотворень, навіть до повної інверсії кольору пікселя. У зв'язку з цим після зворотнього ДКП блоку потрібно нормалізувати значення елементів блоку. Нормалізація полягає у детектуванні значень, що вийшли за межі діапазону, і приведенні цих значень до значення найближчої межі діапазону;
- додано завадостійке кодування кодом Хемінга.

Для вилучення ЦВЗ з відеофайлу необхідно зробити ті самі операції, що й для вбудовування, аж до ДКП. Надалі вилучення полягає у порівнянні коефіцієнтів ДКП. Якщо різниця між ними більше або дорівнює 0, тоді вбудований біт – "0". Якщо різниця між ними менше 0, тоді вбудований біт – "1".

Характеристики стійкості до певних атак модифікованого методу можна покращити, використовуючи коди Хемінга. Коди Хемінга це, ймовірно, одні с найвідоміших кодів, що самоконтролюються і самокоригуються. Коди Хемінга дозволяють виправляти одиничну помилку (помилка в одному біті) і знаходити подвійну помилку. При реалізації цього алгоритму використовувалися коди Хемнга (7,4). Це означає, що чотири біта ЦВЗ кодувалися сіма бітами коду. В данному коді чотири біта будуть інформативними, а три – контрольними.

Використання кодів Хемінга можна поділити на два етапи: кодування інформації і декодування інформації.

Для кодування інформації необхідно сформувати семибітну послідовність. контрольні біти будуть елементами, у яких індекси це ступені 2, тобто це індекси 1, 2, 4. В інші елементи послідовно записуються дані (рис. 3).

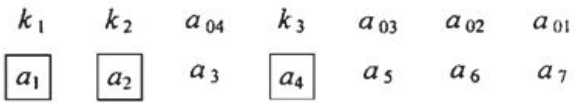

Рис. 3. Розташування інформаційних та перевірочних символів в кодах Хемінга (7,4)

Для розрахунку контрольних бітів використовуються наступні формули:

$$k_1 = k_3 \oplus k_5 \oplus k_7, \quad (7)$$

$$k_2 = k_3 \oplus k_6 \oplus k_7, \quad (8)$$

$$k_4 = k_5 \oplus k_6 \oplus k_7, \quad (9)$$

де k_i – і-й елемент коду.

Отриманий код використовується в якості ЦВЗ при вбудовуванні інформації.

III. Результати досліджень

При вбудовуванні ЦВЗ у відеофайл важливими характеристиками методів є стійкість до атак, пропускна здатність, складність реалізації та прихованість вбудованої інформації. Саме тому ці характеристики були вибрані для аналізу та порівняння реалізованих методів.

Для аналізу прихованості ЦВЗ необхідно провести порівняльний аналіз оригінального відеофайлу (ОВ) з відеофайлом, в який був вбудований ЦВЗ (ВВ). Величина спотворення ОВ при вбудовуванні ЦВЗ відображає рівень прихованості вбудованої інформації.

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.

Пропускна здатність методу – це обсяг інформації, який можна вбудувати у контейнер.

Пропускна здатність відеофайлу C розраховується за формулою:

$$C = \frac{V_{wm}}{V_{fr}} \cdot 100\% \quad (10)$$

де V_{wm} – максимальний розмір ЦВЗ в бітах, що можна вбудувати в один кадр відеофайлу,

V_{fr} – розмір кадру в бітах.

За результатами розрахунків встановлено, що пропускна здатність методу на основі НЗБ значно перевищує (приблизно в 60 разів) пропускну здатність методів на основі заміни частотних коефіцієнтів. З цього можна зробити висновки, що метод НЗБ можна ефективно використовувати не тільки для вбудовування ЦВЗ, а також для прихованої передачі великих обсягів даних, тобто створення прихованого каналу передачі даних.

Під атакою на стеганографічну систему розуміється спроба виявити, витягти, змінити або видалити приховану інформацію [5]. Здатність стеганографічної системи протистояти атакам називається стеганографічною стійкістю.

В рамках дослідження була проаналізована стійкість реалізованих методів до трьох видів атак:

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

Шум – це випадкові або навмисні спотворення даних в процесі їх зберігання, обробки чи передачі по системам зв'язку. В рамках дослідження в якості використовувалася псевдовипадкова числова послідовність (ПВЧП), яка накладалася на кадри відеофайлу. ПВПЧ характеризується мірою шуму N. Міра шуму показує до яких максимальних спотворень ПВПЧ може привести.

При переформатуванні відеофайлу використовуються різні методи для перетворення і збереження відеофайлу на носіях інформації, що може вплинути на вбудований водяний знак. Досліджувався вплив на ЦВЗ переформатування у популярні формати відеофайлів: mkv, mpeg, wmv.

Стиснення відеофайлу – технологія цифрової компресії телевізійного сигналу, що дозволяє скоротити кількість даних, які використовуються для відображення відеопотоку. Стиснення відео дозволяє ефективно зменшувати потік, необхідний для передачі відео по каналах зв'язку, зменшувати простір, необхідний для зберігання даних на носії. 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. Тому для оцінки стійкості методів до стиснення було використано кодування відеофайлу у формат mp4.

Результати проведення атак на ВВ представлені на рис. 4.

Як видно з рис. 4, методи на основі НЗБ не є стійкими до досліджених видів атак, тому недоцільно використовувати ці методи для вбудовування ЦВЗ у відео файл. З іншого боку методи на основі Коха-Жао мають велику стійкість до атаки стиснення відеофайлу. Це пояснюється тим, що в алгоритмі H.264 використовується ДКП.

Розроблений метод на основі зміни частотних коефіцієнтів має більшу стійкість до атак переформатування, а при значеннях порогу вбудовування P=30 і більше, дозволяє вилучати ЦВЗ без жодних спотворень. Використання кодів Хемінга для кодування ЦВЗ

перед його вбудовування, дозволяє в більшості випадків, навіть для малих значень Р, вилучати ЦВЗ з незначними або зовсім відсутніми спотвореннями.

Рис. 4. Результати проведення атак

Для кількісної оцінки величини спотворення оригінального відеофайлу використовувалися два показника MSE і PSNR.

MSE або середньоквадратичне відхилення – відносний показник розсіювання значень. MSE для відеофайлу це показник розсіювання значень пікселів ОВ і ВВ (величини спотворення ОВ). MSE розраховується для кожного кадру відеофайлу окремо. MSE відеофайлу буде середнє арифметичне значення MSE кадрів, що видно з наступної формули:

$$\mathrm{MSE} = \frac{1}{m \cdot n} \cdot \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (V_{ij} V_{ij}^{*})^2 , \qquad (11)$$

де V – значення пікселю ОВ; V^{*} – значення пікселю ВВ; m – кількість строк кадру; n – кількість стовпців кадру.

Результати розрахунків MSE реалізованих методів представлені на рис. 5.

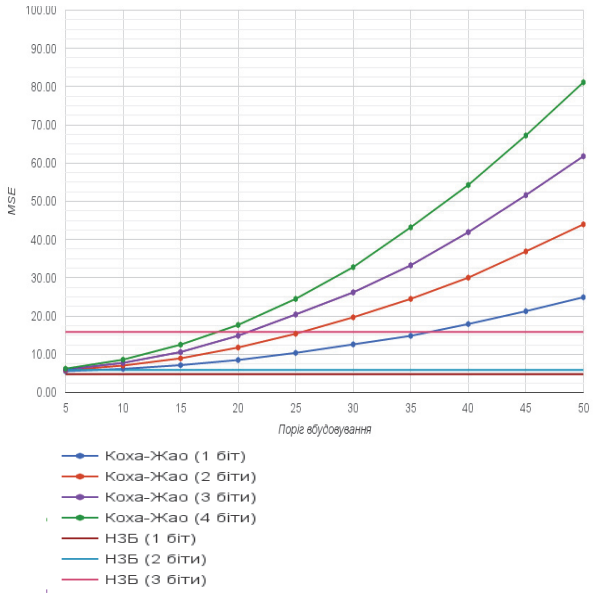

Рис. 5. Результати розрахунків MSE

Розрахунки представлені у вигляді діаграми, на якій показана залежність MSE від порога вбудовування Р, при різній кількості біт, що вбудовується, в один елемент вбудовування. Елементом вбудовування для методу на основі НЗБ є піксель зображення, а для методів на основі Коха-Жао – блок 8×8. У зв'язку з тим, що у метода на основі НЗБ немає параметра Р, результати розрахунків цього методу представлені у вигляду прямих ліній, що паралельні осі абсцис. Як видно з рис. 5, при малих значення Р розбіг значень MSE усіх методів, окрім методу на основі НЗБ з вбудовуванням 3 бітів у піксель, незначний. Однак, при значеннях Р=30 і більше методи на основі Коха-Жао створюють більші, а при значеннях Р близьких до 50 – значно більші, спотворення, ніж методи на основі НЗБ. Можна зробити висновки, що загалом методи, що працюють в області перетворень, схильні до більших спотворень відеофайлу, ніж методи, що працюють в просторовій області.

PSNR або пікове відношення сигналу до шуму – показник співвідношення максимально можливого значення пікселя і потужності (величини) спотворень, що визвані вбудованим ЦВЗ. У зв'язку з тим, що величину спотворень можна представити за допомогою показника MSE, PSNR можна розрахувати за допомогою MSE, використовуючи наступну формулу формулу:

$$\mathrm{PSNR} = 10 \cdot \log_{10} \left(\frac{\mathrm{MAX}^2}{\mathrm{MSE}} \right), \qquad (12)$$

де MAX – максимальне значення пікселя.

PSNR, як і MSE, розраховується для кожного кадру відеофайлу окремо.

Результати розрахунків PSNR реалізованих методів представлені на рис. 6. Розрахунки представлені у вигляді графіку, на якому показана залежність PSNR від порогу вбудовування Р, при різній кількості біт, що вбудовується, в один елемент вбудовування. Як і у випадку з MSE, результати розрахунків методів на основі НЗБ представлені у вигляді прямих ліній, які паралельні осі абсцис.

Аналіз рис. 6 показує, що при малих значення Р розбіг значень, як і у випадку з MSE, майже в усіх методах незначний. Однак при значеннях Р=20 і більше методи на основі зміни частотних коефіцієнтів мають менші, а при значеннях Р близьких до 50 – значно менші, величини PSNR, ніж методи на основі НЗБ. Це означає, що при вбудовуванні інформації ці методи в більшій мірі впливають на відеофайл, в порівнянні з методами на основі НЗБ. Однак важливо зауважити, що графіки жодного методу не опустилися нижче межі, отже можна зробити висновки, що всі реалізовані методи мають таку характеристику, як прихованість вбудованої інформації і що вони можуть бути використані для прихованого вбудовування ЦВЗ в відеофайл.

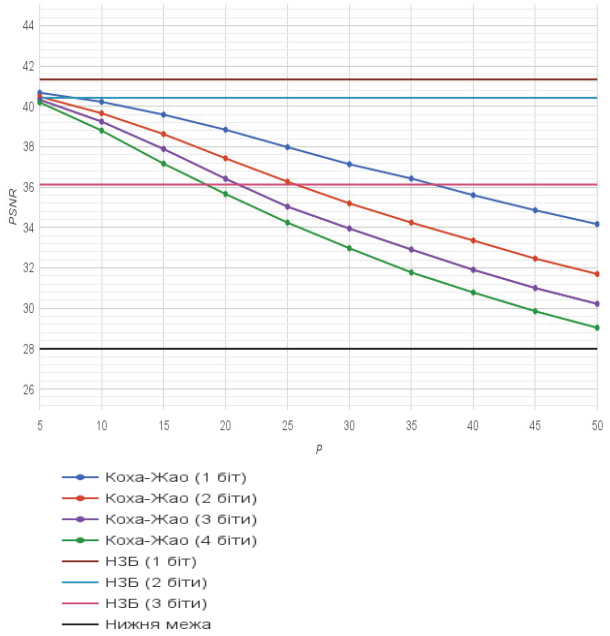

Рис. 6. Результати розрахунків PSNR

Висновки

Провівши аналіз реалізованих алгоритмів, можна зробити висновки, що методи просторової області недоцільно використовувати для вбудовування ЦВЗ, незважаючи на велику пропускну здатність. ЦВЗ, вбудований цими методами, можна легко зруйнувати атаками накладання шуму і переформатування. Тому навіть за наявності дуже малої пропускної здатності, методи області перетворень більш доцільно використовувати для вбудовування ЦВЗ.

В даній роботі запропонований новий алгоритм, що дозволяє підвищити пропускну здатність та стійкість існуючого метода, шляхом розширення числа коефіцієнтів для вбудовування, застосування завадостійких кодів та попереднього аналізу блоків вбудовування.

Запропонований алгоритм при значеннях порогу вбудовування в діапазоні від 5 до 50 дозволяє вбудовувати ЦВЗ в відеофайл зі збереженням заданого значення прихованості (PSNR > 28 дБ) і демонструє стійкість до атак стиснення та переформатовування, а також до завад в каналах передачі інформації, що дозволяє ефективно використовувати цей алгоритм для захисту прав на відеофайли.

Список літератури

1. M. Swanson, B. Zhu, A. Tewfik, "Multiresolution Video Watermarking using Perceptual Models and Scene Segmentation," Proceedings International Conference on Image Processing (ICIP '97), 3-Volume Set-Volume 2, Washington, DC, Oct. 26-29, 1997.

2. S. Arena, M. Caramma, "Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking," Proceedings International Conference on Image Processing (ICIP-2000), Vol. 3, pp. 438-441, Vancouver, Canada, 2000.

3. N. Johnson, S. Katezenbeisser, "A Survey of Steganographic Techniques in Information Techniques for Steganography and Digital Watermarking," S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, pp. 43-75, Dec. 1999.

4. G. Langelaar, I. Setyawan, R. Lagendijk, "Watermarking Digital Image and Video Data," IEEE Signal Processing Magazine, Vol 17, pp. 20-43, Sept. 2000.

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

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

Надійшла до редколегії 6.03.2017

Рецензент: д-р техн. наук проф. С.Г. Удовенко, Харківський національний економічний університет імені Семена Кузнеця, Харків.

ИССЛЕДОВАНИЕ СТОЙКОСТИ АЛГОРИТМОВ ЗАЩИТЫ АВТОРСКИХ ПРАВ НА ВИДЕОПРОДУКЦИЮ

Н.В. Шостак, А.А. Астраханцев, С.В. Романько

В последние годы растёт интерес к стеганографии именно как к эффективному методу сокрытия данных, который позволяет сохранять конфиденциальность информации. В данной работе решается вопрос синтеза алгоритма защиты авторских прав на видеопродукцию, который должен быть стойким к действию помех в каналах связи и основных атак и обеспечивать повышенный уровень пропускной способности. Проведен сравнительный анализ существующих методов встраивания ЦВЗ в видеофайлы с целью выявления методов с наилучшими показателями стойкости к атакам и скрытия встраивания ЦВЗ. Также, предложен собственный метод для встраивания водяных знаков.

Ключові слова: *frequency domain watermarking, error-correction, capacity of videowatermarking, ЦВЗ, стойкость.*

INVESTIGATION OF STABILITY OF ALGORITHMS OF COPYRIGHT PROTECTION IN VIDEO PRODUCTION

N.V. Shostak, A.A. Astrahancev, S.V. Romanko

Great interest to steganography grows exactly as to the effective method of hiding data, which allows to maintain the confidentiality of information. In this paper the problem of synthesis of the algorithm of the copyright protection in video, which is robust to interference in communication channels and basic attacks, and provides a higher level of capacity is solved. A comparative analysis of existing methods of embedding watermarks in the video to identify the methods with the best performance in terms of resistance to attacks and stealth embedding watermarks is held. Also a proprietary watermarking algorithm which is based on method Koha-Jao is proposed.

Keywords: *frequency domain watermarking, error-correction, capacity of videowatermarking, watermark, robustness.*