УДК 004.056

ВИБІР ПЕРЕВАЖНОГО АЛГОРИТМУ ВБУДОВУВАННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ В ВІДЕОФАЙЛИ

Шостак Н. В. – аспірант кафедри інформаційно-мережної інженерії Харківського національного університету радіоелектроніки, Харків, Україна.

Безрук В. М. – д-р техн. наук, професор, завідувач кафедри інформаційно-мережної інженерії Харківського національного університету радіоелектроніки, Харків, Україна.

Астраханцев А. А. – канд. техн. наук, доцент, доцент кафедри інформаційно-мережної інженерії Харківського національного університету радіоелектроніки, Харків, Україна.

АНОТАЦІЯ

Актуальність. За останній час значно збільшилась кількість атак на інтелектуальну власність, яка, відповідно до результатів опитувань, займає провідне місце у структурі сучасного суспільства. Всебічний розвиток країни неможливий без генерації власних інтелектуальних даних і їх захисту, який на тлі інформаційних війн є найбільш актуальною задачею в сучасному суспільстві. Оскільки інтелектуальні дані мають не лише генеруватися та зберігатися а й передаватися по відкритих каналах зв'язку, то підвищується важливість та актуальність дослідження стійкості методів захисту інтелектуальних даних до дії завад в каналах. Вирішенню цієї актуальної задачі присвячена дана робота.

Мета роботи – визначення стеганографічного алгоритму приховування цифрового водяного знаку в відеоконтейнері, оптимального за критеріями швидкодії, стійкості до атак, прихованості та пропускної здатності за допомогою програмного моделювання та методу аналізу ієрархій.

Метод. Досліджені алгоритми вбудовування цифрових водяних знаків в рухомі зображення. 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. Алгоритми 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. В алгоритмах вбудовування в область перетворень, водяний знак, розподіляється по області перетворення і який важко видалити після вбудовування. Для алгоритмів в області перетворень, існує кілька класів методів, що базуються на різних функціях перетворення, основними з яких є дискретне косинусне перетворення, дискретне вейвлет-перетворення та дискретне перетворення Фур'є.

Результати. За результатами розрахунків визначені оптимальні за сукупністю критеріїв алгоритми приховування цифрових водяних знаків в відеофайли.

Висновки. В даній статті використано метод аналізу ієрархій для визначення переважного за сукупністю показників якості алгоритму вбудовування інформації у відеофайли. Переважний алгоритм отримано на основі сформованих матриць порівнянь відносної важливості показників якості та результатів програмного моделювання стеганографічних алгоритмів вбудовування в відеофайли. Якщо, в якості переважаючого критерію була обрана пропускна здатність, то найкращі значення за вказаним критерієм забезпечує метод на основі НЗБ, підвищення стійкості якого забезпечується додатковим використанням коду Хемінга з значенням вектору пріоритетів 0,24. При використанні в якості переважаючого критерію стійкість до атак результати досліджень показали ефективність методу дискретного вейвлет-перетворення з можливістю вбудовування 2 бітів цифрового водяного знака в блок ДКП в частотну область LH. Наукова новизна роботи полягає в тому, що вперше визначений переважний за критеріями швидкодії, пропускної здатності та стійкості до завад в каналах зв'язку метод вбудовування у відеофайли та набула подальшого розвитку теорія приховання інформації у відеофайлах шляхом підвищення завадостійкості існуючих алгоритмів.

Практична значимість роботи визначається застосованістю досліджуваних алгоритмів для захисту інтелектуальної власності на відеопродукцію, що передається каналами зв'язку з завадами, вирішення цієї задачі є актуальною проблемою в сучасному світі.

КЛЮЧОВІ СЛОВА: стеганографія, відео, алгоритм, ЦВЗ, метод аналізу ієрархій.

АБРЕВІАТУРИ

LSB – найменш значущий біт;
ЦВЗ – цифровий водяний знак;
МАІ – метод аналізу ієрархій;
ДКП – дискретне косинусне перетворення;
ДВП – дискретне вейвлет-перетворення.

НОМЕНКЛАТУРА

MSE – середньоквадратичне відхилення;
V – значення пікселю вихідного зображення;
V^* – значення пікселю стегозображення;
m – кількість рядків кадру;
n – кількість стовпців кадру;
PSNR – пікове відношення сигнал/шум;
MAX – максимальне значення пікселю;
a_{ij} – оцінки парних порівнянь елементів вибору;
V_j – компоненти головного власного вектора;
P_j – компоненти вектора пріоритетів показників якості;
C_i – компонент вектора глобальних пріоритетів;
N – число проектних варіантів систем, що порівнюється.

ВСТУП

Стеганографія – наука про методи захисту інформації шляхом приховання факту її існування в тому або іншому середовищі. Приховання факту існування таємного повідомлення завжди видавалося доцільним для його захисту, а наявність різних технічних, хімічних, фізичних і психологічних методів такого приховання забезпечувало можливість його реалізації. Сьогодні стеганографія являє собою

DOI 10.15588/1607-3274-2018-3-18

сукупність алгоритмів і технічних рішень, що реалізують захист інформації, заснований на різних принципах. Однак в умовах стрімкого зростання інформаційно-телекомунікаційних технологій найбільш активно розвиваються комп'ютерні алгоритми стеганографії 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 в відеофайли.

Об'єкт дослідження: процеси приховування конфіденційної інформації в стеганографічних контейнерах (відео-файлах), які передаються по відкритих каналах звязку з завадами.

Предмет досліджень – комбіновані методи захисту мультимедійних даних із застосуванням стеганографії, завадостійкого кодування та паралельної обробки даних, а також оцінки стійкості та швидкодії стеганографічних методів.

Метою даної роботи є визначення стеганографічного алгоритму приховування цифрового водяного знаку в відеоконтейнері, оптимального за критеріями швидкодії, стійкості до атак, прихованості та пропускної здатності за допомогою програмного моделювання та методу аналізу ієрархій.

1 ПОСТАНОВКА ЗАДАЧІ

Задано методи прихования інформації, які мають широке поширення та забезпечують високі показники якості – методи НЗБ, Коха-Жао та метод на основі ДВП-ДКП. Вказані методи мають бути програмно реалізовані та по отриманих реалізаціях мають бути оцінені наступні критерії якості: пропускна здатність, швидкість вбудовування та витягнення повідомлення, ступінь спотворення початкового контейнеру та стійкість до атак. Використовуючи методи аналізу ієрархій та математичного моделювання необхідно визначити методи найкращі по сукупності критеріїв за умови максимізації пропускної здатності та стійкості до атак. В якості результуючих значень має бути отриманий глобальний вектор пріоритетів, що містить інтегровану оцінку наведених критеріїв. Додаткові обмеження накладає необхідність використання методів боротьби з завадами в каналах звязку для підвищення стійкості досліджуваних методів захисту інформації.

2 ОГЛЯД ЛІТЕРАТУРИ

Алгоритми вбудовування цифрових водяних знаків в нерухомі зображення та в відео можуть бути розділені на 3 основні групи в залежності від області, в яку вбудовується ЦВЗ: алгоритми вбудовування в просторову область, в область перетворень та в відео, що стиснене за стандартом MPEG. Основними перевагами просторових алгоритмів 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. Основною перевагою алгоритмів в області перетворень, є те, що вони можуть використати особливі властивості альтернативних областей для усунення обмежень методів вбудовування в просторовій області або для підтримки додаткових функцій [1, 2, 3].

З метою визначення переважного алгоритму вбудовування цифрового водяного знаку було виконано розрахунки сукупності показників якості для різних алгоритмів, що наведений у [9], а потім на основі їх порівняльного аналізу використано один із методів багатокритеріального вибору єдиного варіанту – метод аналізу ієрархій [10].

3 МАТЕРІАЛИ І МЕТОДИ

Метод заміни найменш значущого біту є найбільш поширеним серед алгоритмів вбудовування ЦВЗ в просторовій області. Загальний принцип цього алгоритму полягає у заміні надмірності, малозначущої частини зображення бітами секретного повідомлення [1].

Одним з найпоширеніших алгоритмів приховування конфіденційної інформації в області перетворень зображення полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення, який описується Кохом та Жао [2]. Для застосування алгоритму 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 алгоритму:

– 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.

Характеристики стійкості до певних атак модифікованого алгоритму можна покращити, використовуючи коди Хемінга. Коди Хемінга це, ймовірно, одні с найвідоміших кодів, що самоконтролюються і самокоригуються. Коди

DOI 10.15588/1607-3274-2018-3-18

Хемінга дозволяють виправляти одиничну помилку (помилка в одному біті) і знаходити подвійну помилку. При реалізації цього алгоритму використовувалися коди Хемінга (7,4). Це означає, що чотири біта ЦВЗ кодувалися сьома бітами коду. В даному коді чотири біта будуть інформативними, а три – контрольними.

Ще одним поширеним алгоритмом вбудовування в область перетворень є метод дискретного вейвлет-перетворення. Основна ідея дискретного вейвлет-перетворення у процесі обробки зображення полягає в розкладанні зображення в підзображення різних просторових та частотних областей. ДВП розділяє зображення на апроксимацію первинного кадру 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 вейвлет-компонентів більш високого порядку [3, 4, 5].

В даній роботі для дослідження використовувались такі алгоритми: метод заміни найменш значущого біту, метод заміни величин коефіцієнтів ДКП (Коха-Жао) та метод дискретного вейвлет-перетворення. Також ці алгоритми були реалізовані з додаванням кодів Хеммінга, а алгоритм Коха-Жао та ДВП з можливістю вбудовування 1, 2 або 4 бітів цифрового водяного знака в блок ДКП та ДВП і алгоритм ДВП з можливістю вбудовування в різні частотні області (HL або LH) [6, 7, 8].

Всі ці алгоритми були проаналізовані і оцінені з використанням набору наступних метрик (показників якості):

– час вбудовування – це час, який необхідний для вбудовування прихованого повідомлення в відео файл;

– час зчитування – це час, який необхідний для вилучення прихованого повідомлення із відео файл;

– пропускна спроможність – кількість бітів прихованого повідомлення, які можуть бути передані за допомогою цього методу в відеофайлі фіксованого розміру;

– MSE – відносний показник розсіювання значень. MSE для відеофайлу це показник розсіювання значень пікселів вихідного зображення і стегозображення. MSE розраховується для кожного кадру відеофайлу окремо і розраховується за формулою:

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

– PSNR – 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:

$$PSNR = 10 \cdot \log_{10}(\frac{\mathrm{MAX}^2}{MSE}). \qquad (2)$$

Результат розрахунків показників якості для алгоритмів, описаних вище, наведено у роботі [9]. З їх аналізу витікає, що показники якості стеганографічних алгоритмів зв'язані між собою та є антагоністичними. Це означає, що при переході від одного алгоритму до іншого алгоритму одні показники стають кращими, а інші погіршуються. В такому випадку для вибору єдиного переважного стеганографічного алгоритму з урахуванням сукупності показників якості необхідно використовувати методи багатокритеріальної оптимізації.

4 ЕКСПЕРИМЕНТИ

Розглянемо особливості вибору єдиного переважного алгоритму вбудовування ЦВЗ з урахуванням сукупності показників якості за допомогою методу аналізу ієрархій [10]. Суть цього методу зводиться до формування досвідченими експертами парних порівнянь відносної важливості показників якості проектних варіантів (у нашому випадку стеганографічних алгоритмів), а також оцінок відносної важливості самих проектних варіантів (стеганографічних алгоритмів).

Результати парних порівнянь елементів вибору наводяться у матричній формі:

$$A = \begin{pmatrix} a_{11} a_{12} \ldots a_{1j} \\ a_{21} a_{22} \ldots a_{2j} \\ \ldots \\ a_{i1} a_{i2} \ldots a_{ij} \end{pmatrix} \qquad (3)$$

Далі над сформованими матрицями парних порівнянь виконуються математичні перетворення, зокрема, розраховується головний власний вектор, який відповідає максимальному власному значенню матриці. Компоненти головного власного вектора матриці парних порівнянь показників якості обчислюються як середнє геометричне значення в рядку матриці парних порівнянь

$$V_j = \sqrt[n]{\prod_{i=1}^{n} a_{ij}}, \; j = \overline{1,n}, \qquad (4)$$

де n – число показників якості.

Через компоненти головного власного вектора обчислюються відповідні компоненти вектора пріоритетів показників якості як нормовані значення:

$$P_j = \frac{V_j}{S}, \; j = \overline{1,n}, \qquad (5)$$

де $S = \sum_{j=1}^{n} V_j$. (6)

Аналогічно знаходяться оцінки матриць парних порівнянь стеганографічних алгоритмів окремо по відношенню до кожного показника якості. На основі цих матриць обчислюються компоненти відповідних головних власних векторів і векторів пріоритетів

DOI 10.15588/1607-3274-2018-3-18

систем $\vec{Q}_j$ по відношенню до окремих показниками якості. З використанням отриманих даних обчислюються значення компонент вектора глобальних пріоритетів $\vec{C}$ згідно співвідношення:

$$C_i = \sum_{j=1}^{n} P_j Q_{ij}, i = \overline{1,N}. \quad (7)$$

За максимальним значенням компонента вектора глобальних пріоритетів (7) вибирається відповідний переважний варіант стеганографічного алгоритму вбудовування ЦВЗ.

5 РЕЗУЛЬТАТИ

Згідно описаного методу аналізу ієрархій сформована матриця парних порівнянь для показників якості стеганографічних алгоритмів (табл. 1). Для заповнення цієї таблиці за допомогою досвідченого експерта виконані парні порівняння важливості показників якості алгоритмів вбудовування ЦВЗ в відеофайли. Діагональ цієї матриці заповнена значеннями «1», а елементи матриці, що лежать нижче діагоналі, заповнені зворотними значеннями.

Далі отримані відповідні матриці парних порівнянь алгоритмів вбудовування ЦВЗ в відеофайл окремо по відношенню до обраних показниками якості: час вбудовування, час зчитування, MSE, PSNR, а також і отримані відповідні матриці парних порівнянь. Для прикладу в табл. 2 приведена матриця парних порівнянь алгоритмів вбудовування ЦВЗ в відео по відношенню до часу зчитування, а також обчислені власний вектор і вектор пріоритетів (табл. 2). Аналогічні матриці парних порівнянь алгоритмів вбудовування ЦВЗ отримані також по відношенню і до інших показників якості.

У табл. 3 зведені отримані оцінки компонент вектора пріоритетів показників якості, а також векторів пріоритетів алгоритмів вбудовування в відео, по відношенню до часу вбудовування, часу зчитування, MSE та PSNR. З використанням цих векторів пріоритетів обчислені значення компонент глобального вектора пріоритетів згідно (7), які наведені в останньому стовпчику табл. 3.

Таблиця 1 – Матриця парних порівнянь показників якості алгоритмів вбудовування ЦВЗ в відеофайли і обчислені оцінки компонент вектора пріоритетів

	Час вбудовування	Час зчитування	Пропускна здатність	MSE	PSNR	Компоненти головного власного вектора, V_i	Компоненти вектора пріоритетів, P_i
Час вбудовування	1	2	1/7	7	3	1,43	0,20
Час зчитування	1/2	1	1/5	4	3	1,04	0,14
Пропускна здатність	7	5	1	7	4	3,97	0,54
MSE	1/7	1/4	1/7	1	1/3	0,28	0,04
PSNR	1/3	1/3	1/4	3	1	0,61	0,08

Таблиця 2 – Матриця парних порівнянь алгоритмів вбудовування ЦВЗ в відео по відношенню до часу зчитування і обчислені оцінки компонент вектора пріоритетів

	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8	A_9	A_{10}	A_{11}	A_{12}	A_{13}	A_{14}	$V_П$	$P_П$
A_1	1	2	8	7	7	7	7	8	8	7	9	7	7	7	5,84	0,27
A_2	1/2	1	9	7	7	8	7	8	8	7	9	6	6	8	5,31	0,24
A_3	1/8	1/9	1	1/3	1/3	1/2	1/3	1/2	2	1/3	3	1/4	1/4	1/2	0,43	0,02
A_4	1/7	1/7	3	1	2	3	2	3	4	2	5	1/3	1/3	3	1,27	0,06
A_5	1/7	1/7	3	1/2	1	3	2	3	3	2	6	1/3	1/3	3	1,14	0,05
A_6	1/7	1/8	2	1/3	1/3	1	1/3	2	3	1/3	5	1/3	1/3	2	0,66	0,03
A_7	1/7	1/7	3	1/2	1/2	3	1	3	3	2	5	1/3	1/3	3	1,02	0,05
A_8	1/8	1/8	2	1/3	1/3	1/2	1/3	1	3	1/3	4	1/3	1/3	2	0,58	0,03
A_9	1/8	1/8	1/2	1/4	1/3	1/3	1/3	1/3	1	1/3	3	1/4	1/4	1/3	0,35	0,02
A_{10}	1/7	1/7	3	1/2	1/2	3	1/2	3	3	1	5	1/3	1/3	3	0,92	0,04
A_{11}	1/9	1/9	1/3	1/5	1/6	1/5	1/5	1/4	1/3	1/5	1	1/5	1/5	1/3	0,23	0,01
A_{12}	1/7	1/6	4	3	3	3	3	3	4	3	5	1	2	3	1,90	0,09
A_{13}	1/7	1/6	4	3	3	3	3	3	4	3	5	1/2	1	3	1,72	0,08
A_{14}	1/7	1/8	2	1/3	1/3	1/2	1/3	1/2	3	1/3	3	1/3	1/3	1	0,52	0,02

DOI 10.15588/1607-3274-2018-3-18

Таблиця 3 – Результати обчислення оцінок компонент глобального вектора пріоритетів

Методи вбудовування	Q_{ij}					$\vec{C}$
LSB	0,24	0,27	0,15	0,18	0,02	**0,18**
LSB + HammingCodes	0,28	0,24	0,25	0,25	0,02	**0,24**
Koch-Zhao (1 bit / block)	0,06	0,02	0,03	0,12	0,16	**0,05**
Koch-Zhao (1 bit / block) + Hamming Codes	0,02	0,06	0,01	0,12	0,16	**0,04**
Koch-Zhao (4 bit / block)	0,07	0,05	0,19	0,03	0,10	**0,13**
Koch-Zhao (4 bit / block) + Hamming Codes	0,04	0,03	0,09	0,03	0,10	**0,07**
DWT-DCT HL (1 bit / block)	0,04	0,05	0,02	0,02	0,07	**0,03**
DWT-DCT HL (1 bit / block) + Hamming Codes	0,05	0,03	0,01	0,01	0,07	**0,03**
DWT-DCT HL (2 bit / block)	0,05	0,02	0,07	0,01	0,07	**0,06**
DWT-DCT HL (2 bit / block) + Hamming Codes	0,04	0,04	0,03	0,01	0,07	**0,04**
DWT-DCT LH (1 bit / block)	0,03	0,01	0,03	0,04	0,05	**0,03**
DWT-DCT LH (1 bit / block) + Hamming Codes	0,03	0,09	0,01	0,06	0,04	**0,03**
DWT-DCT LH (2 bit / block)	0,03	0,08	0,07	0,05	0,03	**0,06**
DWT-DCT LH (2 bit / block) + Hamming Codes	0,02	0,02	0,03	0,06	0,03	**0,03**
$\vec{P}$	**0,20**	**0,14**	**0,54**	**0,04**	**0,08**	

6 ОБГОВОРЕННЯ

Захист авторських прав на відеопродукцію може забезпечуватися за допомогою вбудовування ЦВЗ в різних областях. Найбільше поширення отримали методи приховання в просторовій області, частотній області та області вейвлет-перетворення. Для визначення найкращого алгоритму на фоні завад в каналах зв'язку були обрані алгоритми, які мають найкращі показники в кожній з цих областей. Таким чином були досліджені параметри методів НЗБ, Коха-Жао, ДВП-ДКП. Згідно з методом аналізу ієрархій переважний проектний варіант вибраний за результатами аналізу значень компонент вектора глобальних пріоритетів, що наведений в табл. 3. Максимальному значенню компоненти вектора глобальних пріоритетів відповідає переважний алгоритм вбудовування ЦВЗ в відеофайл з урахуванням введених показників якості. Відповідно до результатів досліджень найкращим за умови забезпечення найвищої критеріями стійкості до атак став метод ДВП-ДКП, а найкращим за умови забезпечення найвищої швидкодії – метод НЗБ. Ці методи не мають захисту від дії завад в каналах зв'язку і потребують подальшого удосконалення шляхом додавання завадостійких кодів, наприклад коду Хемінга. Підвищення прихованості для вказаних методів можна досягти застосуванням додаткових алгоритмів перемежіння даних.

ВИСНОВКИ

В даній статті використано метод аналізу ієрархій для визначення переважного за сукупністю показників якості алгоритму вбудовування інформації у відеофайли. Переважний алгоритм отримано на основі сформованих матриць порівнянь відносної важливості показників якості та результатів програмного моделювання стеганографічних алгоритмів вбудовування в відеофайли. Якщо, в якості переважного критерія була обрана пропускна здатність, то найкращі значення за вказаним критерієм забезпечує метод на основі НЗБ, підвищення стійкості якого забезпечується додатковим використанням коду Хемінга з значенням вектору пріоритетів 0,24. При використанні в якості переважаючого критерію стійкість до атак результати досліджень показали ефективність методу дискретного вейвлет-перетворення з можливістю вбудовування 2 бітів цифрового водяного знака в блок ДКП в частотну область LH.

Наукова новизна роботи полягає в тому, що вперше визначений переважний за критеріями швидкодії, пропускної здатності та стійкості до завад в каналах зв'язку метод вбудовування у відеофайли та набула подальшого розвитку теорія приховання інформації у відеофайлах шляхом підвищення завадостійкості існуючих алгоритмів.

Практична значимість роботи визначається застосованістю досліджуваних алгоритмів для захисту інтелектуальної власності на відеопродукцію, що передається каналами зв'язку з завадами, вирішення цієї задачі є актуальною проблемою в сучасному світі.

ПОДЯКИ

Результати отримані в рамках аспірантської підготовки і використані при виконанні держбюджетної НДР (№ДР0117U002528) Харківського національного університету радіоелектроніки.

DOI 10.15588/1607-3274-2018-3-18

ЛІТЕРАТУРА / ЛИТЕРАТУРА

1. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин. – М. : СОЛОН-Пресс, 2002. – 272 с.
2. Конахович Г. Ф. Компьютерная стеганография. Теория и практика / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.
3. Essaouabi A. Waveletbased object watermarking system for mpeg4 video / A. Essaouabi, E. Ibnelhaj, F.A. Regragu // International Journal of Computer Science and Security. – 2010. – Vol. 3, Issue 6. – P. 448.
4. Nikolaidis N. Robust image watermarking in the spatial domain / N. Nikolaidis, I. Pitas // Signal Processing, Special Issue on Copyright Protection and Control. – 1998. – Vol. 66, № 3. – P. 385–403.
5. Arena S. Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking / S. Arena, M. Caramma // Proceedings International Conference on Image Processing. – 2000. – Vol. 3. – P. 438–441.
6. Koch E. Towards Robust and Hidden Image Copyright Labeling / E. Koch, J. Zhao // IEEE Workshop on Nonlinear Signal and Image Processing. – 1995. – Vol. 1. – P. 123–132.
7. Langelaar G. Watermarking Digital Image and Video Data / G. Langelaar, I. Setyawan, R. Lagendijk // IEEE Signal Processing Magazine. – 2000. – Vol 17. – P. 20–43.
8. Hartung F. Watermarking of Uncompressed and Compressed Video / F. Hartung, B. Girod // Signal Processing. – 1998. – Vol. 66, № 3. – P. 283–301.
9. Shostak N. Comparative analysis of effectiveness video watermarking techniques / N. Shostak, A. Astrakhantsev, S. Romanko // Science of Europe. – 2017. – Vol. 15. – P. 92–95.
10. Безрук В. М. Многокритериальный анализ и выбор средств телекоммуникаций / В. М. Безрук, Д. В. Чеботарева, Ю. В. Скорик. – Х. : СМИТ, 2017. – 268 с.

Стаття надійшла до редакції 10.04.2018.
Після доробки 25.05.2018.

УДК 004.056

ВЫБОР ПРЕДПОЧТИТЕЛЬНОГО АЛГОРИТМА ВСТРАИВАНИЯ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ВИДЕОФАЙЛЫ

Шостак Н. В. – аспирант кафедры информационно-сетевой инженерии Харьковского национального университета радиоэлектроники, Харьков, Украина.

Безрук В. М. – д-р техн. наук, профессор, заведующий кафедры информационно-сетевой инженерии Харьковского национального университета радиоэлектроники, Харьков, Украина.

Астраханцев А. А. – канд. техн. наук, доцент, доцент кафедры информационно-сетевой инженерии Харьковского национального университета радиоэлектроники, Харьков, Украина.

АННОТАЦИЯ

Актуальность. В последнее время существенно увеличилось количество атак на интеллектуальную собственность, которая, в соответствии с результатами опросов, занимает ведущее место в структуре современного общества. Всестороннее развитие страны невозможно без генерации собственных интеллектуальных данных и их защиты, которая на фоне информационных войн является наиболее актуальной задачей в современном обществе. Поскольку интеллектуальные данные должны не только генерироваться и храниться, но и передаваться по открытым каналам связи, то повышается важность и актуальность исследования стойкости методов защиты интеллектуальных данных к действию помех в каналах. Решению этой актуальной задачи посвящена данная работа.

Цель работы – определение стеганографического алгоритма скрытия цифрового водяного знака в видеоконтейнер, оптимального по критериям быстродействия, стойкости к атакам, скрытности и пропускной способности с помощью программного моделирования и метода анализа иерархий.

Метод. Рассмотрены алгоритмы встраивания цифровых водяных знаков в видео. В последнее время огромное внимание уделяется методам встраивания, имеющие такие свойства, как стойкость к атакам и скрытность встроенной информации. Эти алгоритмы можно классифицировать по типу области в которую встраивается или извлекается цифровой водяной знак, их пропускной способности, производительности в режиме реального времени и устойчивости к конкретным типам атак. Существующие алгоритмы встраивания в видео можно условно разделить на три основные группы, в зависимости от области в которую встраивается ЦВЗ: методы встраивания в пространственной области, в область преобразований и методы встраивания в видео, которое сжато по стандарту MPEG. Алгоритмы встраивания ЦВЗ в пространственной области применяются для несжатого видео. Встраиваемый ЦВЗ обычно прилагается к компоненту яркости и некоторых компонентов цветов или только к компонентам цветов. В алгоритмах встраивания в область преобразований водяной знак распределяется по области преобразования и его трудно удалить после встраивания. Для алгоритмов в области преобразований, существует несколько классов методов, основанных на различных функциях преобразования, основными из которых являются дискретное косинусное преобразование, дискретное вейвлет-преобразование и дискретное преобразование Фурье.

Результаты. По результатам расчетов выполнен выбор преимущественного алгоритма скрытия цифровых водяных знаков в видеофайлы.

Выводы. В данной статье использован метод анализа иерархий для определения предпочтительного по совокупности показателей качества алгоритма встраивания информации в видеофайлы. Предпочтительный алгоритм получен на основе сложившихся матриц сравнений относительной важности показателей качества и результатов программного моделирования стеганографических алгоритмов встраивания в видеофайлы. Если в качестве преобладающего критерия была выбрана пропускная способность, то наилучшие значения по указанному критерию обеспечивает метод на основе НЗБ, повышение стойкости которого обеспечивается дополнительным использованием кода Хемминга со значением вектора приоритетов 0,24. При использовании в качестве преобладающего критерия стойкость к атакам результаты исследований показали эффективность метода дискретного вейвлет-преобразования с возможностью встраивания 2 битов цифрового водяного знака в блок ДКП в частотную область LH. Научная новизна работы заключается в том, что впервые определен преимущественный по критериям быстродействия, пропускной способности и устойчивости к помехам в каналах связи метод встраивания в видеофайлы и получила дальнейшее развитие теория сокрытия информации в видеофайлах путем повышения помехоустойчивости существующих алгоритмов.

DOI 10.15588/1607-3274-2018-3-18

Практическая значимость работы определяется применимостью исследуемых алгоритмов для защиты интеллектуальной собственности на видеопродукцию, передаваемой по каналам связи с помехами, решение этой задачи является актуальной проблемой в современном мире.

КЛЮЧЕВЫЕ СЛОВА: стеганография, видео, алгоритм, ЦВЗ, метод анализа иерархий.

UDC 004.056

SELECTING THE PREFERRED ALGORITHM FOR THE EMBEDDING OF DIGITAL WATERMARKS INTO VIDEOFILES

Shostak N. V. – Postgraduate Student, Department of Information and Network Engineering, Kharkiv National University of radioelectronics, Kharkiv, Ukraine.

Bezruk V. M. – Dr.Sc. Professor, Superintendent of Department of Information and Network Engineering, Kharkiv National University of radioelectronics, Kharkiv, Ukraine.

Astrakhantsev A. A. – PhD, Associate Professor, Associate Professor of Department of Information and Network Engineering, Kharkiv National University of radioelectronics, Kharkiv, Ukraine.

ABSTRACT

Context. Recently, the number of attacks on intellectual property has increased significantly, which, according to the polls, occupies a leading position in the structure of modern society. The comprehensive development of the country is impossible without generating its own intellectual data and their protection, which, in the face of information wars, is the most urgent task in modern society. Since intellectual data must not only be generated and stored, but also transmitted through open communication channels, the importance and urgency of the study of the stability of methods for protecting intellectual data to the effect of interference in channels is increasing. This work is dedicated to solving this urgent task.

Objective – definition of a steganographic algorithm for hiding a digital watermark in a video container optimal for performance criteria, resistance to attacks, concealment and bandwidth using software simulation and hierarchy analysis method.

Method. The algorithms for embedding of digital watermarks in a moving image are considered. Recently, much attention has been paid to embedding algorithms that have properties such as resistance to attacks and the concealment of embedded information. These algorithms can be classified by the type of area in which the digital watermark is embedded or seized, their bandwidth, real-time performance, and resistance to specific attack types. Existing embedding algorithms in a video can be conventionally divided into three main groups, depending on the area in which the embedded digital watermark: embedding methods in the spatial domain, in the region of transformation, and embedding methods in video compressed by the MPEG standard. The embedding algorithms of the digital watermark in the spatial area are used for uncompressed video. The embedding digital watermark is usually added to the brightness component and some color components, or only to the color components. In embedding algorithms in the transformation region, the watermark is distributed over the transformation region and difficult to remove after embedding. For methods in the field of transformation, there are several classes of methods based on different transformation functions, the main of which are the discrete cosine transform, discrete wavelet transform and discrete Fourier transform.

Results. As a result of calculations the choice of the preferred algorithm of concealment of digital watermarks in a video file was made.

Conclusions. In this article, a hierarchy analysis method is used to determine the preferred algorithm for integrating information into video files according to a combination of quality indicators. The preferred algorithm is obtained on the basis of existing matrices of comparisons of the relative importance of quality indicators and the results of software modeling of steganographic embedding algorithms in video files. If the bandwidth was chosen as the prevailing criterion, the best method based on this criterion is provided by a method based on the LSB, which is enhanced by the additional use of the Hamming code with the value of the priority vector 0.24. When the resistance to attacks was used as the predominant criterion, the results of the studies showed the effectiveness of the discrete wavelet transform method with the possibility of embedding 2 bits of the digital watermark in the DCT block into the frequency domain of LH. The scientific novelty of the work is that for the first time the method of embedding in the video file was prevailing on the criteria of speed, bandwidth and resistance to interference in communication channels, and the theory of concealing information in video files was further developed by increasing the noise immunity of existing algorithms.

The practical significance of the work is determined by the applicability of the investigated algorithms for protecting intellectual property on video products transmitted by channels of communication with the obstacles, the solution of this problem is an actual problem in the modern world.

KEYWORDS: steganography, video, algorithm, digital watermark, method of hierarchy analysis.

REFERENCES

1. Gribunin V. G. Digital Steganography. Moscow, Solon-press, 2002, 272 p.
2. Konakhovich G. F., Puzyrenko A. U. Computer steganography. Theory and Practice. Kiev, MK-Press, 2006, 288 p.
3. Essaouabi A., Ibnelhaj E., Regragu F. A. Waveletbased object watermarking system for mpeg4 video, *International Journal of Computer Science and Security*, 2010, Vol. 3, Issue 6, P. 448.
4. Nikolaidis N., Pitas I. Robust image watermarking in the spatial domain, Signal Processing, *Special Issue on Copyright Protection and Control*, 1998, Vol. 66, No. 3, pp. 385–403.
5. Arena S., Caramma M. Digital watermarking applied to MPEG2 coded video sequence exploiting space and frequency masking, *Proceedings International Conference on Image Processing,* 2000, Vol. 3, pp. 438–441.
6. Koch E., Zhao J. Towards Robust and Hidden Image Copyright Labeling, *IEEE Workshop on Nonlinear Signal and Image Processing,* 1995, Vol. 1, pp. 123–132.
7. Langelaar G., Setyawan I., Lagendijk R. Watermarking Digital Image and Video Data, *IEEE Signal Processing Magazine,* 2000, Vol. 17, pp. 20–43.
8. Hartung F., Girod B. Watermarking of Uncompressed and Compressed Video, *Signal Processing*, 1998, Vol. 66, No. 3. pp. 283–301.
9. Shostak N., Astrakhantsev A., Romanko S. Comparative analysis of effectiveness video watermarking techniques, *Science of Europe,* 2017, Vol. 15, pp. 92–95.
10. Bezruk V. M., Chebotaryova D. V., Skoruk J. V. Multi-criteria analysis and choice of means of telecommunications. Xar'kov, SMIT, 2017, 268 p.

DOI 10.15588/1607-3274-2018-3-18