УДК 621.391

АНАЛІЗ ХАРАКТЕРИСТИК АЛГОРИТМІВ ВБУДОВУВАННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ НА ТЛІ АТАК І ЗАВАД У КАНАЛАХ ЗВ'ЯЗКУ

Н.В. ШОСТАК
Харківський національний університет радіоелектроніки

Abstract *– In this paper, an overview of the algorithms of concealing information in the video, which can be used to protect copyright, has been made. A new algorithm is proposed that allows increasing the bandwidth and stability of existing methods by increasing the number of coefficients for embedding and application of noise immunity codes. An effective way to resolve copyright issues is to provide authentication through the introduction of digital watermarks embedded with steganographic algorithms. The scientific novelty of the work is that the theory of embedding information in video files has been further refined by taking into account factors that arise in communication channels, such as attacks and interference. This enhancement makes it possible to increase the efficiency of the system of transmission of hidden (embedded) information by interference channels through the use of fault-tolerant codes and the selection of the optimal latency criteria of transmission parameters (including the embedding threshold). The practical significance of the work is determined by the fact that most of the copyrighted information has to be transmitted by the communication channels and, in order to ensure an adequate level of effectiveness, the parameters of the copyright protection system must be consistent with the parameters of the communication channel.*

Анотація *– В даній роботі зроблено огляд алгоритмів приховування інформації в відео, що можуть бути використані для захисту авторських прав. Запропоновано новий алгоритм, що дозволяє підвищити ефективність системи передачі прихованої (вбудованої) інформації каналами зв'язку із завадами завдяки використанню завадостійких кодів та обранню оптимальних за критеріями прихованість-швидкість параметрів передачі (в тому числі порога вбудовування). Практична значущість результатів роботи визначається тим, що для забезпечення відповідного рівня ефективності параметри системи захисту авторських прав мають бути узгодженими з параметрами каналу зв'язку.*

Аннотация *– В данной работе сделан обзор алгоритмов скрытия информации в видео, которые могут быть использованы для защиты авторских прав. Предложен новый алгоритм, позволяющий повысить эффективность системы передачи скрытой (встроенной) информации по каналам связи с помехами благодаря использованию помехоустойчивых кодов и выбору оптимальных по критериям скрытность-скорость параметров передачи (в том числе порога встраивания). Практическая значимость результатов работы определяется тем, что для обеспечения соответствующего уровня эффективности параметры системы защиты авторских прав должны быть согласованы с параметрами канала связи.*

Вступ

Сьогодні власники контенту з нетерпінням шукають технології, які б могли захистити їхні права та контент від піратства, несанкціонованого використання і дозволяли б відстежувати і засуджувати медіа піратів. Ефективним шляхом вирішення проблеми захисту авторського права, що дозволяє перевірити правовласника цифрових відеофайлів, є організація забезпечення автентичності за рахунок впровадження цифрових водяних знаків (ЦВЗ), що вбудовуються за допомогою стеганографічних алгоритмів. На сьогоднішній день пропонуються алгоритми, які здійснюють автентифікацію відеофайлів, проте наявні розробки не позбавлені ряду істотних недоліків, залишаючи актуальним завдання розробки нових стеганографічних алгори-

тмів, що дозволяють одночасно забезпечувати приховану передачу даних і автентифікацію відеофайлу.

Незважаючи на значне поширення і вдосконалення алгоритмів вбудовування ЦВЗ, не вирішеним залишається завдання аналізу стійкості сформованих ЦВЗ на тлі завад та атак у каналах зв'язку. Також відсутня кількісна та якісна оцінка застосування завадостійких кодів для підвищення стійкості ЦВЗ. Саме ці телекомунікаційні складові мають найбільший вплив на всю систему захисту авторських прав і аналізуються нижче.

I. Аналіз існуючих алгоритмів вбудовування цифрових водяних знаків у відео

Загалом всі існуючі алгоритми можна класифікувати за типом області, в яку вбудовується або вилучається цифровий водяний знак, їх пропускною здатністю, продуктивністю в режимі реального часу та стійкістю до конкретних типів атак. В залежності від області, в яку вбудовується ЦВЗ, сучасні алгоритми вбудовування в відеофайли можна умовно поділити на три основні групи: алгоритми вбудовування в просторовій області, в області перетворень та алгоритми вбудовування в відеофайли, що стиснені за стандартом MPEG [1, 2].

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

- алгоритм вбудовування ЦВЗ на основі заміни найменш значимого біту (НЗБ);
- алгоритм вбудовування ЦВЗ на основі алгоритму Коха-Жао;
- алгоритм вбудовування ЦВЗ на основі дискретного вейвлет-перетворення (ДВП).

Також були проаналізовані відкриті джерела щодо алгоритмів вбудовування ЦВЗ в відео, що мають схожі властивості з реалізованими алгоритмами. Для порівняльного аналізу з реалізованими алгоритмами були обрані два алгоритми:

- автентифікація відео на основі вмісту за допомогою ДВП;
- ефективне вбудовування ЦВЗ в відео з використанням ДВП.

В реалізованих алгоритмах 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 наступному кроці виконується перетворення у просторове кодування YCbCr за допомогою формул:

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

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

$$C_r = 128 + 122 \times R - 93,786 \times G - 18,214 \times B, \quad (3)$$

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 компонента яскравості кольорового простору YCbCr. Зворотне перетворення виконується за допомогою формул:

$$R = Y + 1,371(C_r - 128), \tag{4}$$

$$G = Y + 0,698(C_r - 128) - 0,336(C_b - 128), \tag{5}$$

$$B = Y + 1,732(C_r - 128). \tag{6}$$

ЦВЗ зчитується у форматі адитивної кольорової моделі RGB. У зв'язку з тим, що ЦВЗ – чорно-біле зображення, можливі лише два значення кольору пікселів: 0xFF для білого і 0x00 для чорного. Тому при зчитуванні ЦВЗ використовується двійкове кодування: 0xFF кодується як «1», а 0x00 – «0» [3].

Завдяки застосуванню двійкового кодування алгоритми пристосовані до вбудовування будь-якої двійкової інформації.

Алгоритм вбудовування ЦВЗ на основі заміни найменш значимих бітів – найбільш поширений серед алгоритмів заміни в просторовій області. Найменш значимі біти пікселя несуть в собі найменшу кількість інформації. Відомо, що людина в більшості випадків не здатна помітити змін в цьому біті. Саме тому його можна використовувати для вбудовування інформації шляхом заміни найменш значимих бітів пікселів зображення бітами ЦВЗ. При цьому обсяг вбудованих даних може становити одну восьму від загального обсягу контейнера. Якщо модифікувати два молодших біта, що також практично непомітно, то таку пропускну здатність можна збільшити вдвічі. Популярність цього алгоритму обумовлена тим, що він дозволяє приховувати у відносно невеликих файлах досить великі обсяги інформації. Процес вбудовування інформації за допомогою алгоритму НЗБ наведено на рис. 1.

У ході дослідження була реалізована можливість вбудовування до 3 бітів інформації у кожен піксель кадру відео файлу [4]. Алгоритм вбудовування ЦВЗ на основі заміни НЗБ складається з наступних кроків:

- зчитування відеофайлу;
- розбиття відеофайлу на кадри;
- перетворення відеокадру з кольорової моделі RGB до кольорової моделі YCbCr;
- зчитування ЦВЗ;

- перетворення ЦВЗ з чорно-білої кольорової моделі до двійкової послідовності;
- вбудовування ЦВЗ у компоненту яскравості відеокадру за допомогою заміни найменш значимих бітів пікселів компоненти яскравості відеокадру бітами ЦВЗ;
- перетворення відеокадру з кольорової моделі YCbCr до кольорової моделі RGB;
- формування відео з кадрів;
- збереження відео файлу.

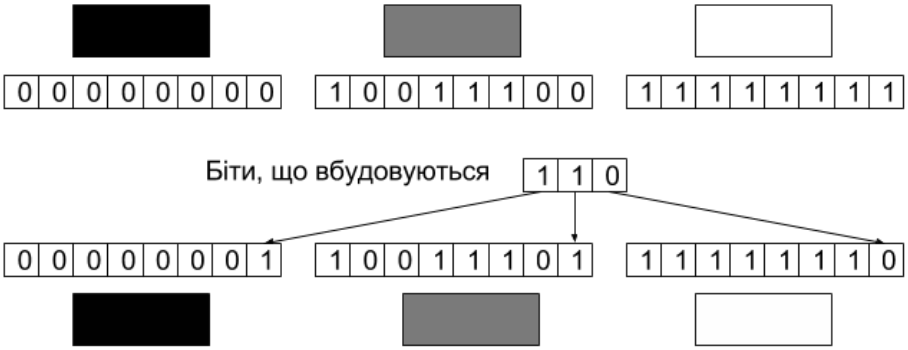

Рис. 1. Процес вбудовування інформації за допомогою заміни найменш значимих бітів

Алгоритм вбудовування ЦВЗ на основі алгоритму Коха-Жао для приховування даних використовує частотну область стегаконтейнеру і полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення (ДКП). Зображення розбивається на блоки розмірністю 8×8 пікселів і до кожного блоку застосовується ДКП. Кожен блок придатний для запису одного біта інформації. Далі обираються два коефіцієнта ДКП із області середніх частот (див. рис. 2), які задаються координатами (u_1, u_1) і (u_2, u_2), і величина порогу вбудовування P.

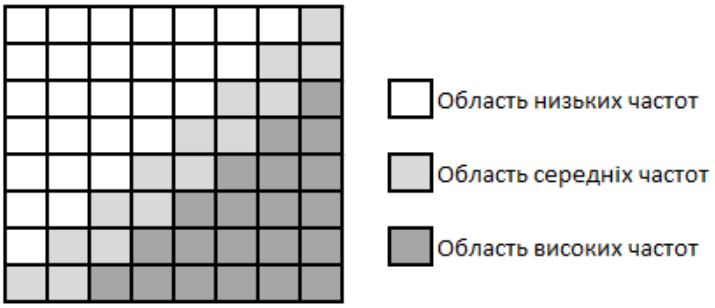

Рис. 2. Частотні області дискретного косинусного перетворення

Для передачі біта «0» ці коефіцієнти змінюються таким чином, щоб різниця між ними стала рівною величині порогу вбудовування P. Для передачі біта «1» ця різниця повинна стати P.

Після цього застосовується зворотне ДКП. Від вибору параметрів u_1, u_1, u_2, u_2, P залежить величина внесених змін при вбудовуванні інформації в стеганоконтейнер і стійкість стеганосистеми.

Алгоритм вбудовування цифрового водяного знаку на основі ДВП, як і алгоритм на основі алгоритму Коха-Жао, для приховування даних використовує частотну область стегаконтейнеру, розбиває кадр на блоки розмірністю 8×8 пікселів і полягає у відносній заміні величин коефіцієнтів.

Застосування ДВП розділяє блок на такі елементи:

- LL – апроксимація первинного блоку;
- HL – результат проходження вейвлету по горизонталях;
- LH – результат проходження вейвлету по вертикалях;
- HH – результат проходження вейвлету по діагоналях.

Потім процес може бути повторений для розрахунку вейвлет-компонентів більш високого порядку, наприклад, рівня 2, як показано на рис. 3.

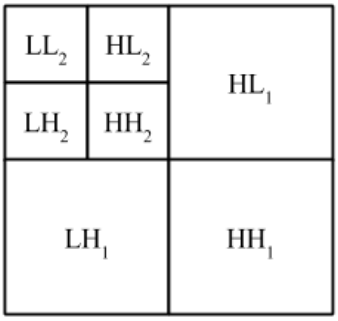

Рис. 3. Дворівневе дискретне вейвлет-перетворення

Існує велика кількість різних вейвлет-функцій. В дослідженні було використано однорівневе вейвлет-перетворення на основі вейвлет-функції Хаара. Вейвлет Хаара – один із найперших і найпростіших вейвлетів. Він базується на ортогональній системі функцій, що була запропонована математиком Альфредом Хааром в 1909 році.

Після застосування ДВП блоку виконується ДКП підблоку HL чи LH. Надалі вбудовування відбувається аналогічно алгоритму на основі Коха-Жао. Після цього застосовуються зворотне ДКП та зворотне дискретне вейвлет-перетворення.

Алгоритм вбудовування ЦВЗ на основі ДВП складається з наступних кроків:

- зчитування відеофайлу;
- розбиття відеофайлу на кадри;
- перетворення відеокадру з кольорової моделі RGB до кольорової моделі YCbCr;
- розбиття відеокадру на блоки 8x8;
- застосування ДВП до блоків;
- застосування ДКП до LH_2 HL_2 підблоків;
- зчитування ЦВЗ;
- перетворення ЦВЗ з чорно-білої кольорової моделі до двійкової послідовності;
- вбудовування бітів ЦВЗ у ДКП підблоки;
- застосування зворотнього ДКП до LH_2 HL_2 підблоків;
- застосування зворотнього ДВП;
- нормалізація блоків 8x8;

- формування кадрів з блоків 8x8;
- перетворення відеокадру з кольорової моделі YCbCr до кольорової моделі RGB;
- формування відео з відеокадрів;
- збереження відеофайлу.

В алгоритмі "Автентифікація відео на основі вмісту за допомогою дискретного вейвлет-перетворення" (АВ) [5] в якості стегоконтейнеру виступає кольоровий трьохканальний відеофайл з розміром кадрів 352×288 пікселів. В якості інформації, що вбудовується, використовується чорно-біле (одноканальне) зображення (ЦВЗ) розмірністю 256×198 пікселів.

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

Завдяки застосуванню двійкового кодування алгоритми пристосовані до вбудовування будь-якої двійкової інформації.

Цей алгоритм використовує ДВП для вбудовування ЦВЗ в області перетворень. Однак алгоритм вбудовування значно відрізняється від реалізованого алгоритму вбудовування ЦВЗ на основі ДВП. В якості функції вейвлет-перетворення використовується вейвлет-функція Хаара.

Алгоритм застосування ДВП складається з наступних кроків:

1) Застосування 2D ДВП до всього відеокадру, зображено на рис. 4.

Рис. 4. 2D дискретне вейвлет-перетворення відеокадру

2) Застосування 2D ДВП до кожного ДВП підблоку.

3) Вбудовування в LL та HH ДВП підблоки, зображено на рис. 5.

Вбудовування ЦВЗ виконується за допомогою формули:

$$VW_i = V_i + x \times W_i, \quad (7)$$

де V_i – значення ДВП коефіцієнтів оригінального відеокадру;

VW_i – значення ДВП коефіцієнтів відеокадру з ЦВЗ;

W_i – значення двійкової послідовності ЦВЗ;

x – коефіцієнт сили вбудовування ЦВЗ.

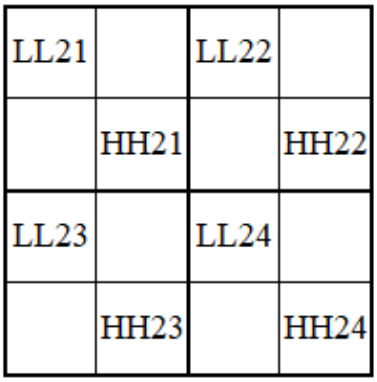

Рис. 5. LL та HH підблоки

Алгоритм вбудовування ЦВЗ складається з наступних кроків:

- зчитування відеофайлу;
- розбиття відеофайлу на кадри;
- перетворення відеокадру з кольорової моделі RGB до кольорової моделі YUV;
- до кадрів застосовується дворівневе ДВП;
- зчитування ЦВЗ;
- перетворення ЦВЗ з чорно-білої кольорової моделі до двійкової послідовності;
- ця послідовність розділяється на 8 частин;
- вбудовування ЦВЗ у відео;
- кожна частина ЦВЗ вбудовується в відповідні LL і HH піддіапазони;
- застосування зворотного дворівневого ДВП;
- перетворення відеокадру з кольорової моделі YUV до кольорової моделі RGB;
- формування відео з відеокадрів;
- збереження відеофайлу.

В алгоритмі "Ефективне вбудовування цифрових водяних знаків в відео з використанням дискретного вейвлет-перетворення" (ЕВ) [6] в якості стегоконтейнеру виступає кольоровий трьохканальний відеофайл з розміром кадрів 352×288 пікселів. В якості інформації, що вбудовується, використовується чорно-біле (одноканальне) зображення (ЦВЗ) розмірністю 256×198 пікселів.

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

Завдяки застосуванню двійкового кодування алгоритми пристосовані до вбудовування будь-якої двійкової інформації.

Цей алгоритм використовує дворівневе 2D ДВП для вбудовування ЦВЗ в області перетворень. В якості функції вейвлет-перетворення використовується вейвлет-функція Хаара.

Однак цей алгоритм має значні відмінності від інших алгоритмів вбудовування:

1) Цей алгоритм не використовує перетворення з кольорової моделі RGB в кольорову модель з компонентою яскравості.

2) Цей алгоритм вбудовує ЦВЗ в усі 3 канали трьох-канального (кольорового) відео файлу.

3) До ЦВЗ застосовуються ті ж самі перетворення, що й до відеокадру.

4) Для вбудовування ЦВЗ використовується Сингулярний розклад матриці (СРМ).

5) Цей алгоритм використовує ДВП для вбудовування ЦВЗ в області перетворень.

В якості функції вейвлет-перетворення використовується вейвлет-функція Хаара.

Алгоритм вбудовування ЦВЗ складається з наступних кроків:

- зчитування відеофайлу;
- розбиття відеофайлу на кадри;
- розбиття відеокадру на блоки 8х8;
- до блоків застосовується дворівневе ДВП;
- застосування СРМ до LL ДВП підблоку;
- зчитування ЦВЗ;
- розбиття ЦВЗ на блоки 8х8;
- до блоків застосовується дворівневе ДВП;
- застосування СРМ до LL ДВП підблоку;
- вбудовування ЦВЗ у відео;
- застосування зворотного СРМ до LL ДВП підблоку;
- застосування зворотного дворівневого ДВП;
- формування відео з відеокадрів;
- збереження відеофайлу.

Однак для вилучення ЦВЗ необхідні оригінальний відеофайл та оригінальна ЦВЗ.

II. Синтез вдосконаленого алгоритму з підвищеною стійкістю до атак на основі алгоритму Коха-Жао та ДКП-ДВП

В ході дослідження для покращення характеристик були внесені модифікації до алгоритму Коха-Жао, що дозволило отримати новий алгоритм з підвищеним рівнем стійкості до атак та завад в каналах зв'язку. Запропоновані вдосконалення наведені нижче:

1) Як область вбудовування була вибрана побічна діагональ матриці ДКП.

2) 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.

3) Реалізована нормалізація блоку після зворотного ДКП.

Якщо інформація вбудовується в блок, що має елементи зі значеннями яскравості Y, близькими до значень граничних елементів діапазону (0 та 255), після зворотного 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 зворотного 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 [7].

Для підвищення ефективності алгоритму на основі ДВП в ході дослідження були реалізовані можливість вбудовування до 2 бітів ЦВЗ в кожен підблок і нормалізація блоку після зворотного ДВП.

III. Підвищення стійкості досліджуваних алгоритмів до атак за допомогою завадостійких кодів

Стійкість реалізованих алгоритмів до певних атак можна покращити при використанні завадостійких кодів. Завадостійкими кодами називаються коди, що дозволяють виявляти або виявляти та виправляти помилки в отриманих кодових комбінаціях. Коди Хемінга це, ймовірно, одні з найвідоміших кодів, що дозволяють виявляти та виправляти помилки. Вони побудовані для роботи з двійковими даними. Коди Хемінга дозволяють виправляти одиничну помилку (помилка в одному біті) і знаходити подвійну помилку.

Для підвищення стійкості реалізованих алгоритмів були вибрані коди Хемінга (7,4). Це означає, що чотири біта ЦВЗ кодуються сьома бітами коду. В такому випадку чотири біта будуть інформативними, а три – контрольними. 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, як показано на рис. 6.

k_1	k_2	a_1	k_3	a_2	a_3	a_4
1	2	3	4	5	6	7

Рис. 6. Розташування елементів в кодах Хемінга (7,4)

Для розрахунку контрольних бітів використовуються наступні формули:

$$k_1 = a_1 \oplus a_2 \oplus a_3, \quad (8)$$

$$k_2 = a_1 \oplus a_3 \oplus a_4, \quad (9)$$

$$k_3 = a_2 \oplus a_3 \oplus a_4, \quad (10)$$

де k_i – i-й елемент коду; a_i – i-й елемент даних.

При декодуванні спочатку перевіряється наявність помилок в коді. Для цього необхідно розрахувати додаткові контрольні біти. Вони розраховуються за формулами:

$$k_1^* = k_1 \oplus a_1 \oplus a_2 \oplus a_4, \quad (11)$$

$$k_2^* = k_2 \oplus a_1 \oplus a_3 \oplus a_4, \quad (12)$$

$$k_3^* = k_3 \oplus a_2 \oplus a_3 \oplus a_4, \quad (13)$$

де k_i^* – i -й контрольний біт коду; k_i – i -й елемент коду; a_i – i -й елемент даних.

Якщо всі додаткові контрольні біти дорівнюють 0 – в коді немає помилок. Якщо хоча б один біт дорівнює 1 – в коді є помилка. Для того щоб виправити помилку, необхідно знайти індекс елемента з помилкою. Він розраховується за допомогою наступної формули:

$$j = \sum_{i=0}^{2} 2^i \cdot k_{i+1}^*, \quad (14)$$

де j – індекс елемента з помилкою; k_i^* – додатковий i-й контрольний біт.

Наступним кроком необхідно виправити помилку. Для цього достатньо інвертувати j-й елемент коду. Після виправлення помилки інформативні біти вилучаються з коду. Коди Ріда-Соломона – недвійкові досконалі систематичні лінійні блокові коди, що відносяться до класу циклічних кодів з числовим полем, відмінним від GF(2), і є підмножиною кодів Боуза-Чоудхурі-Хоквінгема. Коригувальні здатності кодів Ріда-Соломона безпосередньо залежать від кількості контрольних байт. Додавання r контрольних байт дозволяє виявляти r довільним чином перекручених байт, гарантовано відновлюючи половину r байт з них. У кодах Ріда-Соломона повідомлення представляється у вигляді набору символів деякого алфавіту. Тобто якщо ми хочемо закодувати повідомлення, представлене двійковим кодом, то ми розбиваємо його (у випадку, якщо ми використовуємо поле Галуа з 16 елементів) на групи по 4 біта і далі працюємо з кожною групою як з числом з цього поля Галуа.

При побудові коду Ріда-Соломона задається пара чисел N, K, де N – загальна кількість символів, а K – «корисна» кількість символів, решта N-K символів є надлишковим кодом, призначеним для відновлення помилок.

Повідомлення при кодуванні Ріда-Соломона представляються поліномами. Оригінальні дані зображуються як коефіцієнти полінома p(x) ступеня K-1, що має K коефіцієнтів.

Кодування Ріда-Соломона виконується досить просто. Взагалі, існує два різновиди кодування: систематичний і несистематичний код. У несистематичному коді закодоване повідомлення не містить в явному вигляді оригінального повідомлення:

закодоване повідомлення отримується як добуток вихідного повідомлення та породжуючого многочлену.

Цей поліном додається до початкового поліному, зрушеному на N-K символів. Для систематичного коду очевидно, що K старших коефіцієнтів отриманого коду C (x) містять вихідне повідомлення. Це зручно при декодуванні, тому було вирішено використовувати саме систематичний варіант.

Декодування кодів Ріда-Соломона значно складніше кодування. Очевидно, що першим кроком необхідно виконати поділ полінома на породжуючий поліном g(x). Якщо залишок дорівнює нулю, то повідомлення не спотворене і декодування (для систематичного коду) тривіальне: слід виділити з повідомлення перевірочні коефіцієнти, це і буде головне повідомлення.

Декодування засноване на побудові многочлена синдрому помилки S (x) і знаходженні відповідного йому многочлена локаторів L (x). Локатори помилок – це елементи поля Галуа, ступінь яких збігається з позицією помилки. Якщо цей поліном буде знайдено, то можна легко визначити локатори помилок – для цього буде потрібно лише визначити його коріння, що легко зробити звичайним перебором. Обчислення полінома локаторів зводиться до побудови матриці M, знаходженню зворотної їй і добутку на вектор V. Можливо, що матриця M виявиться лінійно-залежною. Це означає, що помилок менше ніж *t*, в цьому випадку слід повторити побудову матриці для *t*, зменшеного на 1. Таким чином, складається поліном помилки. Його коефіцієнтами є значення помилок Y_i , що стоять в позиціях, які визначаються локаторами помилок.

IV. Порівняльний аналіз характеристик алгоритмів вбудовування цифрових водяних знаків

При вбудовуванні ЦВЗ у відеофайл важливими характеристиками алгоритмів є продуктивність, пропускна здатність та прихованість вбудованої інформації. Саме тому ці характеристики були вибрані для аналізу та порівняння реалізованих алгоритмів [8-10]. Продуктивність алгоритму – кількісна характеристика швидкості виконання алгоритму. Продуктивність важлива в системах передачі відеоінформації в форматі реального часу. Продуктивність характеризується часом, необхідним алгоритму для вбудовування чи вилучення ЦВЗ з відеофайла.

Результати розрахунків продуктивності наведені на рис. 7 і 8. На рис. 7 наведені графіки залежності часу вбудовування ЦВЗ алгоритмами в залежності від кількості біт, що вбудовуються. На рис. 8 наведені графіки залежності часу вилучення ЦВЗ.

Як видно з рис. 7 і рис. 8 алгоритм на основі заміни НЗБ має значну перевагу в продуктивності перед іншими алгоритмами. До того ж можна зауважити, що немає значної різниці в часі між вбудовування і вилученням ЦВЗ алгоритмом на основі заміни НЗБ. Алгоритм на основі Коха-Жао та алгоритм на основі ДВП має незначну різницю в продуктивності як вбудовування, так і вилучення ЦВЗ. Крім того, на відміну від алгоритму на основі заміни НЗБ, продуктивність вилучення ЦВЗ майже в два

рази більша ніж вбудовування. Між продуктивністю вбудовування ті вилучення алгоритмів АВ та ЕВ немає значної різниці. До того ж в цілому ці алгоритми мають більш високу продуктивність, ніж реалізовані алгоритми (крім алгоритму на основі заміни НЗБ).

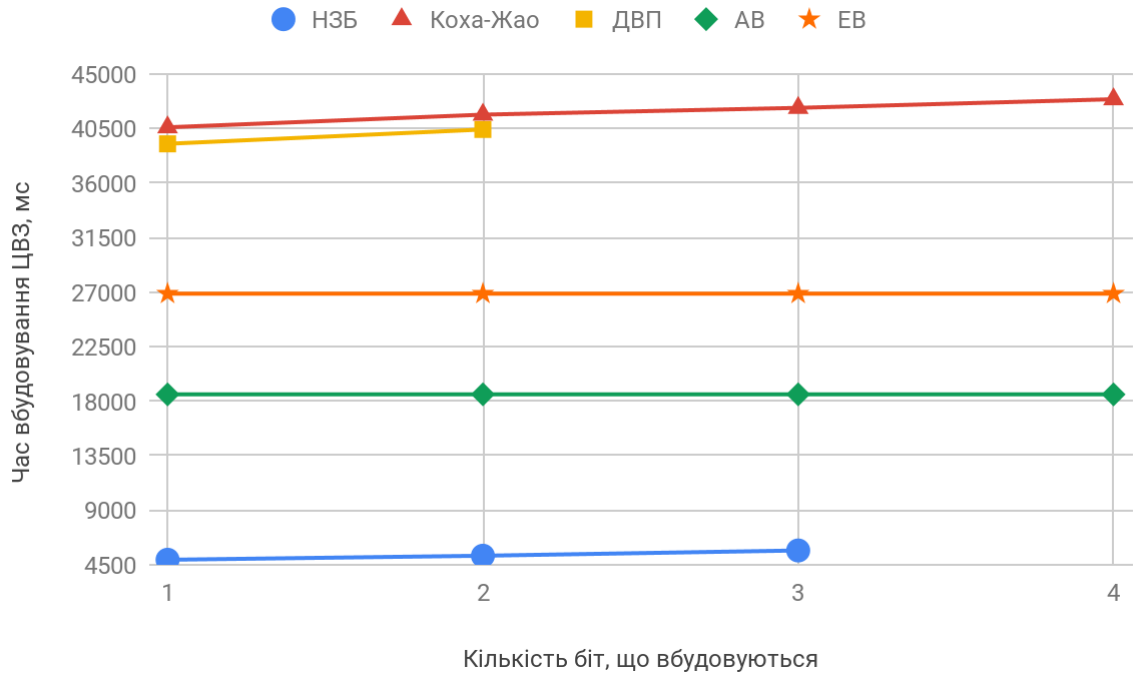

Рис. 7. Графіки залежності часу вбудовування цифрових водяних знаків від кількості біт, що вбудовуються в один блок (піксель)

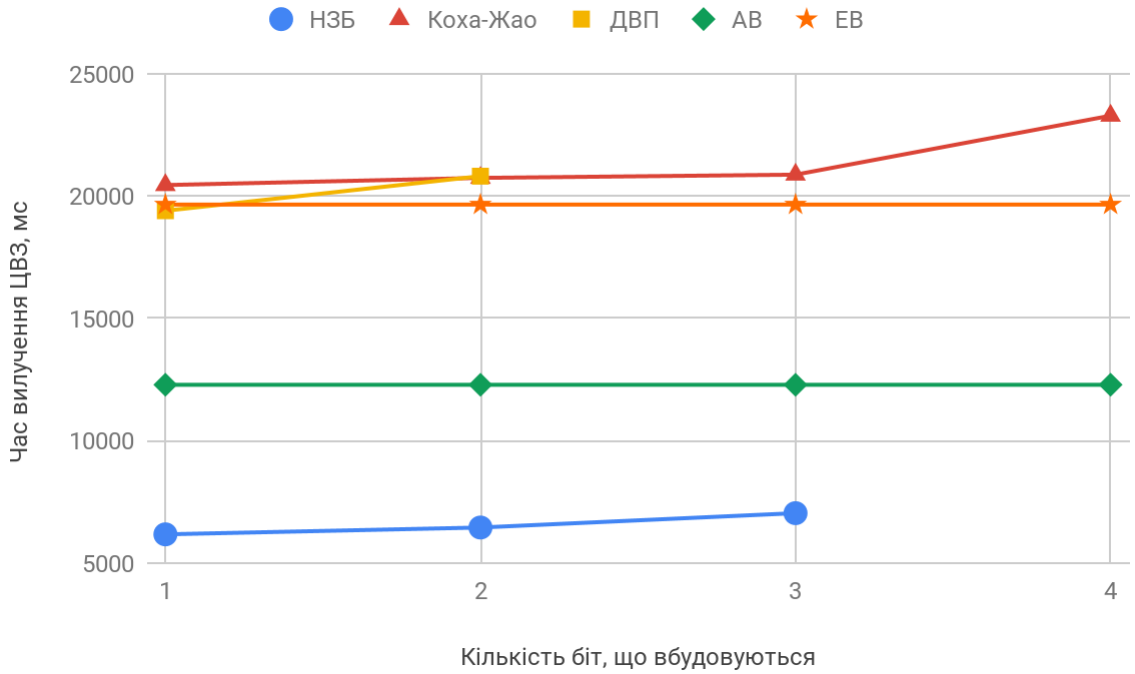

Рис. 8. Графіки залежності часу вилучення цифрових водяних знаків від кількості біт, що були вбудовані в один блок (піксель)

Пропускна здатність алгоритму – це обсяг інформації, який можна вбудувати у контейнер. Пропускна здатності відео файлу C розраховується за формулою:

$$C = \frac{V_{wm}}{V_{fr}} \cdot 100\%, \quad (15)$$

де V_{wm} – максимальний розмір ЦВЗ в бітах, що можна вбудувати в один кадр відео файлу; V_{fr} – розмір кадру в бітах.

Результати розрахунків пропускної здатності реалізованих алгоритмів наведені в табл. 1. В таблиці показані значення пропускної здатності C при різній кількості біт, що вбудовуються в один блок.

Таблиця 1. Результати розрахунку пропускної здатності

Алгоритм	Кількість бітів, що вбудовуються			
	1	2	3	4
Алгоритм на основі заміни ЦВЗ	0,0416	0,0833	0,125	-
Алгоритм на основі Коха-Жао	0,0052	0,0104	0,0156	0,0208
Алгоритм на основі ДВП	0,0052	0,0104	-	-
Алгоритм АВ	-	-	-	0,0208
Алгоритм ЕВ	-	-	-	0,0208

В табл. 1 не були внесені результати оцінки пропускної здатності алгоритму на основі заміни НЗБ, бо пропускна здатність цього алгоритму значно перевищує (в 64 рази) пропускну здатність інших алгоритмів, що не дає змогу адекватно оцінити результати інших алгоритмів.

Інші ж алгоритми мають схожі характеристики пропускної здатності.

Для аналізу прихованості ЦВЗ необхідно провести порівняльний аналіз оригінального відеофайлу з відеофайлом, в який був вбудований ЦВЗ. Величина спотворення оригінального відеофайлу при вбудовуванні ЦВЗ і буде характеристикою прихованості вбудованої інформації.

Для кількісної оцінки величини спотворення оригінального відеофайлу використовувалися два показника PSNR і SSIM. PSNR або пікове відношення сигналу до шуму – це показник співвідношення максимально можливого значення пікселя і потужності (величини) спотворень, що вноситься вбудовуванням ЦВЗ. PSNR можна розрахувати за формулою:

$$PSNR = 10 \cdot \mathbf{log}_{10}(\frac{MAX^2}{MSE}), \quad (16)$$

де MAX – максимальне значення пікселю; MSE – середньоквадратичне відхилення.

MSE розраховується за допомогою формули:

$$MSE = \frac{1}{m \cdot n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (V_{ij} - V_{ij}^*)^2 , \quad (17)$$

де V – значення пікселю оригінального відеофайлу; V^* – значення пікселю відеофайлу з ЦВЗ; m – кількість строк кадру; n – кількість стовпців кадру.

Як показує (16), PSNR вимірюється логарифмічною шкалою в децибелах. Якщо в середньому PSNR ≥ 28 дБ, то величину внесених спотворень можна вважати припустимою. Величину 28 дБ можна використовувати як межу значень PSNR, нижче якої створюються занадто великі спотворення оригінального відеофайлу, що унеможливлює приховану передачу інформації, в даному випадку – ЦВЗ.

Результати розрахунків PSNR реалізованих алгоритмів наведені на рис. 9. Розрахунки наведені у вигляді графіку, на якому показана залежність PSNR від порога вбудовування P, при різній кількості біт, що вбудовуються, в один елемент вбудовування. Як і у випадку з MSE результати розрахунків алгоритмів на основі заміни НЗБ наведені у вигляді прямих лінії, які паралельні осі абсцис.

Аналіз рис. 9 показує, що при малих значеннях P розбіг значень майже в усіх алгоритмах незначний, крім алгоритму AB, який при малих значення порогу вбудовування має значно вищий показник PSNR. Це означає, що алгоритм AB завдає значно менше спотворень до відеофайлу, ніж інші алгоритми. Однак при значеннях P=20 і більше алгоритми, що працюють в області перетворень, мають менші, а при значеннях P, близьких до 50, значно менші величини PSNR, ніж алгоритм на основі заміни НЗБ. Це означає, що при вбудовуванні інформації алгоритми, що працюють в області перетворень, в більшій мірі впливають на відеофайл. Але важливо зауважити, що графіки жодного алгоритму не опустилися нижче 28 дБ, отже можна зробити висновки, що всі реалізовані алгоритми мають таку характеристику, як прихованість вбудованої інформації, і що їх можна використовувати для прихованого вбудовування ЦВЗ у відеофайл.

Індекс структурної подібності (SSIM) – алгоритм вимірювання подібності між двома зображеннями шляхом повного зіставлення. SSIM є розвитком традиційних алгоритмів, таких як PSNR, які виявилися несумісні з фізіологією людського сприйняття. Відмінною особливістю цього алгоритму, на відміну від PSNR, є те, що він враховує «сприйняття помилки» завдяки врахуванню структурної зміни інформації. Ідея полягає в тому, що пікселі мають сильний взаємозв'язок, особливо коли вони близько розташовані.

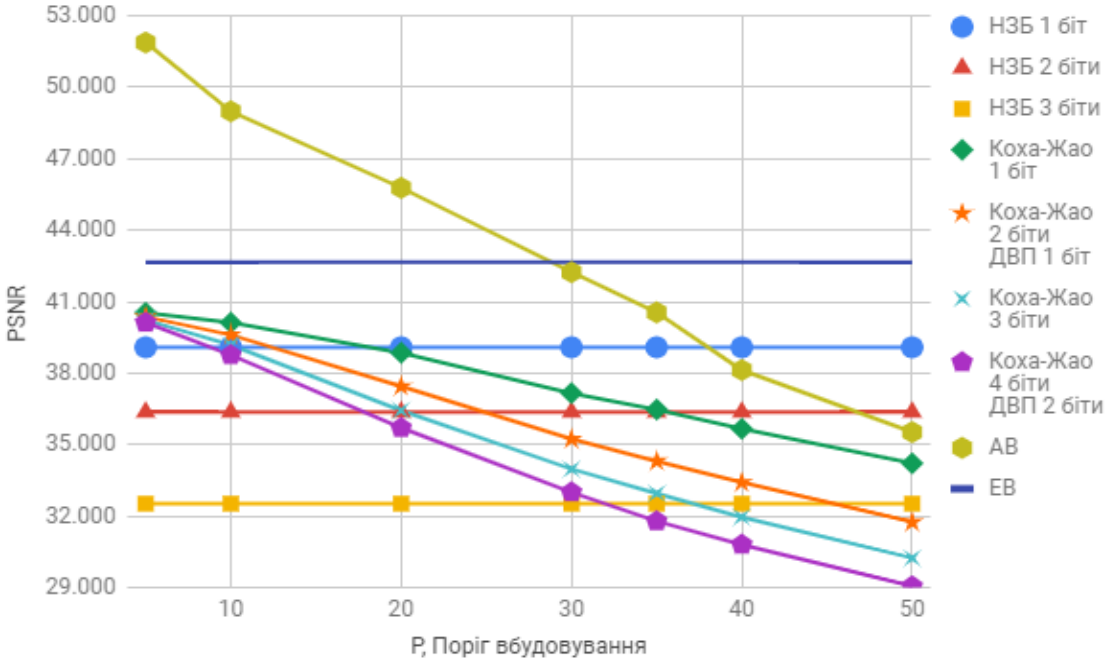

Рис. 9. Графіки залежності PSNR від порогу вбудовування

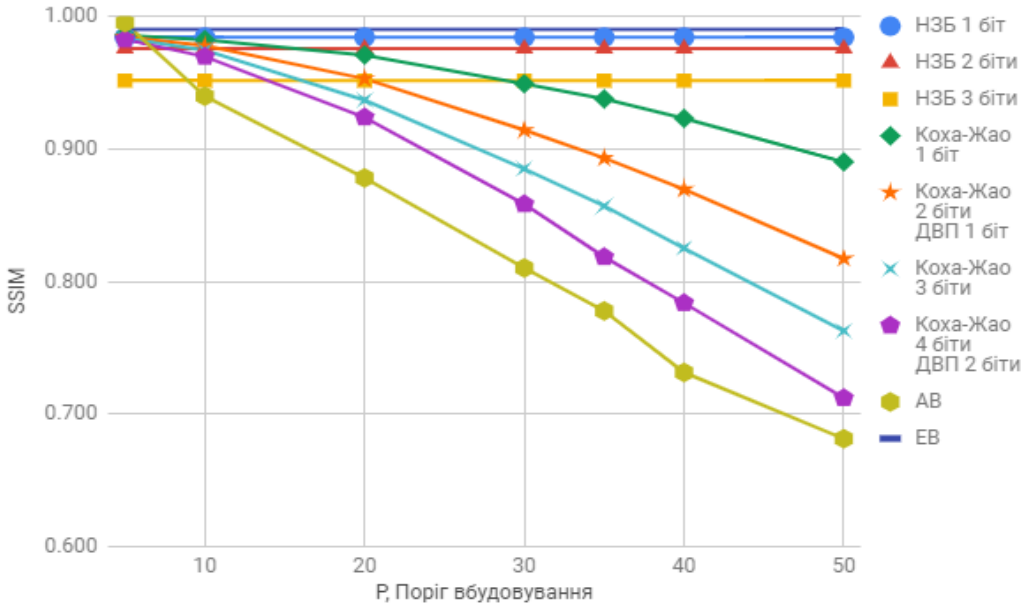

Рис. 10. Графіки залежності SSIM від порогу вбудовування

SSIM розраховується тільки для компоненти яскравості зображення, по якій і відбувається оцінка якості. Отриманий SSIM-індекс лежить в межах від -1 до +1. Значення +1 досягається тільки при повній автентичності зразків.

Аналіз рис. 10 показує, що результати дуже схожі на результати розрахунку PSNR. Однак на відміну від результатів PSNR, можна зробити висновки, що алгоритми, які працюють в області перетворень, завдають значно більші спотворення, ніж алгоритми, що працюють в просторовій області.

Провівши аналіз реалізованих алгоритмів, можна зробити висновки, що алго-

ритми, які працюють в просторовій області, мають більшу продуктивність і пропускну здатність. При невеликих значеннях порогу вбудовування P прихованість всіх реалізованих алгоритмів приблизно однакова, проте при великих значеннях порогу (P більше 30) алгоритми на основі Коха-Жао та ДВП створюють значно більші спотворення відеофайлу. В табл. 2 наведено результати розрахунків пропускної здатності для алгоритму Коха-Жао без використання завадостійких кодів та з використанням коду Хемінга та Ріда-Соломона.

Таблиця 2. Результати розрахунків пропускної здатності

Алгоритм	Кількість бітів, що вбудовуються
	1
Алгоритм на основі алгоритму Коха-Жао без використання завадостійких кодів	0,0416
Алгоритм на основі алгоритму Коха-Жао з кодами Хемінга	0,0237
Алгоритм на основі алгоритму Коха-Жао з кодами Ріда-Соломона	0,0305

Як видно з табл. 2, використання кодів Хемінга зменшує пропускну здатність майже у два рази, але це можна компенсувати, вбудовуючи в два рази більше бітів в один блок. Алгоритм на основі алгоритму Коха-Жао з кодами Ріда-Соломона має середнє значення пропускної здатності серед представлених алгоритмів.

Висновки

В роботі був проведений порівняльний аналіз основних характеристик алгоритмів вбудовування цифрових водяних знаків у відео файли на тлі можливих атак та завад у каналах зв'язку. Науковою новизною роботи є те, що набула подальшого вдосконалення теорія вбудовування інформації у відеофайли шляхом врахування факторів, що виникають в каналах зв'язку, таких як атаки та завади. Наведене вдосконалення дозволяє підвищити ефективність системи передачі прихованої (вбудованої) інформації каналами зв’язку з завадами завдяки використанню завадостійких кодів та обранню оптимальних за критеріями прихованість-швидкість параметрів передачі (в тому числі порога вбудовування). Практична значущість роботи визначається тим, що більшість інформації, яка підлягає захисту авторських прав, має бути передана каналами зв'язку і для забезпечення відповідного рівня ефективності параметри системи захисту авторських прав мають бути узгодженими з параметрами каналу зв'язку.

Аналіз пропускної здатності показав, що більш стійкі до завад алгоритми (ДКП, ДКП-ДВП,...) забезпечують пропускну здатність на рівні 0,02 біт/піксель зображення. При цьому, алгоритм АВ при низьких значеннях порогу вбудовування (P<30) забезпечує істотну перевагу над іншими алгоритмами за внесеним співвідношенням сигнал-шум (PSNR = 53, а наступний показник лише 41), тобто забезпечує більшу прихованість при меншому рівні внесених спотворень відео, яке передавалось. Також важливо зауважити, що графіки жодного алгоритму не опустилися нижче 28 дБ, що означає можливість їх використання у каналах зв'язку з завадами.

Використання завадостійких кодів Хемінга знижує пропускну здатність на 44% (у порівнянні з системою без кодів), а застосування кодів Ріда-Соломона – на 27%, що показує більшу ефективність кодів Ріда-Соломона як за можливостями виявлення і виправлення помилок, так і за пропускною здатністю.

Список літератури:

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

2. *Конахович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. Москва: СОЛОН-Прес, 2002. 272 с.

3. *Essaouabi A., Ibnelhaj E., Regragui F.* A Wavelet-based object watermarking system for MPEG4 Video. International Journal of Computer Science and Security (IJCSS). 2010. Vol. 3, No. 6. P. 449-461.

4. *Nikolaidis N., Pitas I.* Robust image watermarking in the spatial domain. Signal processing. 1998. Vol. 66, No. 3. P. 385-403. DOI: https://doi.org/10.1016/S0165-1684(98)00017-6.

5. Content Based Video Authentication UsingDWT, 2019. URL: https://github.com/ryokugyu/ContentBasedVideoAuthenticationUsingDWT.

6. An Efficient Video Watermarking Using DWT Fractional Order SVD. URL: https://github.com/manish2kk/An-Efficient-Video-Watermarking-Using-DWT-Fractional-Order-SVD.

7. *Koch E., Zhao J.* Towards robust and hidden image copyright labeling. In IEEE Workshop on Nonlinear Signal and Image Processing. 1995. Vol. 1. P. 123-132.

8. *Shostak N., Astrakhantsev A., Romanko S.* Comparative analysis of effectiveness video watermarking techniques. Science of Europe. 2017. Vol. 15. P. 92–95. URL: https://cyberleninka.ru/article/n/comparative-analysis-of-effectiveness-video-watermarking-techniques.

9. *Arena S., Caramma M., Lancini R.* Digital watermarking applied to MPEG-2 coded video sequences exploiting space and frequency masking. 2000 Image Processing (Cat. No. 00CH37101): Proceedings of the International Conference. Vancouver, BC, Canada, 10-13 Sept. 2000. Vol. 1. IEEE, 2000. P. 438-441. DOI: https://doi.org/10.1109/ICIP.2000.900989.

10. *Swanson M.D., Zhu B., Chau B., Tewfik A.H.* Multiresolution video watermarking using perceptual models and scene segmentation. Image Processing: Proceedings of International Conference. Santa Barbara, CA, USA, 26-29 Oct. 1997. Vol. 2. IEEE, 1997. P. 558-561. DOI: https://doi.org/ 10.1109/ICIP.1997.638832.