https://doi.org/10.31891/2219-9365-2023-75-23
УДК 004.056.5:003.27(045)

САЛІЄВА Ольга
Вінницький національний технічний університет
https://orcid.org/0000-0003-2388-7321
salieva8257@gmail.com
ГРИЦАК Анатолій
Вінницький національний технічний університет
https://orcid.org/0000-0002-0776-9889
grytsak.a.v@gmail.com
ГУМЕНЮК В'ячеслав
Вінницький національний технічний університет
https://orcid.org/0009-0004-0348-7616
tienergo@i.ua
БІЛИК Олександр
Вінницький національний технічний університет
bilyk.alex55@gmail.com

УДОСКОНАЛЕННЯ СТЕГАНОГРАФІЧНОГО МЕТОДУ ВБУДОВУВАННЯ КРИХКИХ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ ПОТОКОВОГО ВІДЕО ВІД НЕСАНКЦІОНОВАНОЇ МОДИФІКАЦІЇ

У сучасному інформаційному суспільстві одним із найпопулярніших мультимедійних даних, що поширюється в мережі Інтернет є потокове відео. З цієї причини, вагоме значення має забезпечення конфіденційності та цілісності відеоконтенту, що є вразливим перед різними видами зловмисних атак. Зокрема, варто звернути увагу на загрози, пов'язані з ймовірністю несанкціонованої модифікації, що може призвести до порушення авторських прав, розповсюдження фейкової інформації, або інших небажаних наслідків. Для вирішення даної проблеми у роботі пропонується застосувати стеганографічні методи, які дозволяють приховано вбудовувати у відеофайли водяні знаки. У зв'язку з цим, було проаналізовано можливість захисту відео за допомогою крихких цифрових водяних знаків. Запропоновано покращення методу їх вбудовування шляхом збільшення об'єму інформації для вбудовування, удосконаленого вибору контейнерів та використання функції з секретним ключем HMACSHA-256. Проаналізовано метод із запропонованим покращенням та проведено його порівняння з існуючим аналогом, визначено переваги. Здійснено програмну реалізацію удосконаленого алгоритму вбудовування крихких цифрових водяних знаків.

Ключові слова: стеганографія, крихкі цифрові водяні знаки, захист авторського права, аутентифікація, алгоритми вбудовування цифрових водяних знаків.

SALIIEVA Olha, HRYTSAK Anatoliy, BILYK Oleksandr, HUMENIUK Viacheslav
Vinnytsia National Technical University

IMPROVEMENT OF THE STEGANOGRAPHIC METHOD FOR EMBEDDING FRAGILE DIGITAL WATERMARKS TO IMPROVE SECURITY OF STREAMING VIDEO FROM UNAUTHORIZED MODIFICATION

In today's information society, one of the most popular multimedia data distributed on the Internet is streaming video. For this reason, it is important to ensure the confidentiality and integrity of video content, which is vulnerable to various types of malicious attacks. In particular, it is worth paying attention to the threats associated with the possibility of unauthorized modification, which may lead to copyright infringement, the spread of fake information, or other undesirable consequences. To solve this problem, the work proposes to apply steganographic methods that allow you to covertly embed watermarks in video files. In this regard, the possibility of protecting videos using fragile digital watermarks was analyzed. It is proposed to improve their embedding method by increasing the amount of information for embedding, improving the selection of containers, and using the HMACSHA-256 secret key function. The method with the proposed improvement was analyzed and compared with the existing analogue, the advantages were determined. The software implementation of the improved algorithm for embedding fragile digital watermarks was carried out.

Keywords: steganography, fragile digital watermarks, copyright protection, authentication, digital watermarking algorithms.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Потокове відео є надзвичайно популярним способом передачі відеоконтенту через незахищене середовище – мережу Інтернет. У зв'язку із цим, існують проблеми безпеки та захисту цифрових даних, які можуть бути легко перехоплені, скопійовані з оригінальної версії, модифіковані, що в свою чергу, призводить до компрометації джерела даних. Отже постають питання, пов'язані із можливістю доведення авторства та оригінальності переданого контенту. Одним із способів вирішення даної проблеми є застосування стеганографічних методів вбудовування цифрового водяного знаку (ЦВЗ) у потоковий

відеофайл. При цьому варто звернути увагу на застосування крихких ЦВЗ, які легко пошкоджуються або видаляються при несанкціонованій модифікації відеоконтенту.

Існують різні методи вбудовування ЦВЗ, що поділяються на просторові, частотні та стиснені за стандартом MPEG. Дані методи відрізняються підходом до вбудовування та їхнім впливом на якість та безпеку медіа-контенту [1].

У даній роботі для підвищення захищеності потокового відео від модифікації пропонується удосконалити стеганографічний метод вбудовування крихких ЦВЗ. Для досягнення поставленої мети необхідно провести аналіз предметної області; дослідити відомі алгоритми; розробити покращений алгоритм вбудовування крихких ЦВЗ; провести тестування вдосконаленого методу, оцінити його ефективність; здійснити програмну реалізацію запропонованого алгоритму.

Аналіз досліджень та публікацій

Методи вбудовування ЦВЗ є найбільш поширеними у стеганографії, яка являє собою сукупність методів та засобів їхньої реалізації, що базуються на різних принципах і дозволяють приховувати сам факт існування секретної інформації в тому або іншому середовищі [2]. У свою чергу, ЦВЗ слугують інструментом для захисту авторських прав, забезпечення конфіденційності цифрових даних та їх захисту від фальсифікацій. З кожним роком кількість робіт, присвячених даній тематиці збільшується. Так, у [3] представлено різні підходи до захисту авторських прав для відео з використанням водяних знаків. Для створення автоматичної фільтрації конфіденційності особи під час передачі потокового відео запропоновано метод пікселяції обличчя [4]. Автори праці [5] для збереження конфіденційності потокового відео демонструють аудіовізуальне автокодування з вилученням аудіо, яке працює як випадковий шум із нешаблонним розподілом. Інноваційна схема для захисту конфіденційності та візуальної якості стисненого відео відображена у роботі [6]. Детальний огляд специфікацій передачі відеовмісту та його захисту на основі ЦВЗ наведено в [7]. У роботі [8] запропоновано вбудовування ЦВЗ за допомогою дискретних косинусного та синусного перетворень, які демонструють високий рівень чутливості. Особливий інтерес представляє праця [9], де автори пропонують алгоритм вбудовування водяних знаків крихкого типу, за допомогою якого можна успішно виявити зміни, внесені до вмісту відеопотоків, і визначити конкретне місце, в якому ці зміни були зроблені.

Виділення невирішених раніше частин загальної проблеми

Стеганографічні методи є потужними інструментами, які можуть використовуватися для: надсилання стегоповідомлень, вбудовування ЦВЗ, ідентифікаційних номерів та заголовків. В свою чергу, ЦВЗ можуть бути вбудовані у просторову область та область перетворення. Серед найпоширеніших методів просторової області є метод заміни найменших значущих бітів (LSB), метод різниці значень пікселів (PVD), метод зсуву гістограми. Для збереження цілісності та захисту авторських прав цифрових даних важливо забезпечити крихкість методів вдовування ЦВЗ, а це потребує додаткових покращень, адже переважна більшість алгоритмів не може задовольнити всі вимоги системи автентифікації потокового відео та вбудовувати достатній обсяг інформації, необхідної для досягнення поставлених цілей. У зв'язку з цим, у роботі пропонується вирішити зазначені проблеми, удосконаливши метод вбудовування крихких ЦВЗ за для виявлення незаконних змін та використання вмісту потокового відео.

Формулювання цілей статті

Метою дослідження є удосконалення стеганографічного методу вбудовування крихких ЦВЗ для підвищення захищеності потокового відео від несанкціонованої модифікації.

Виклад основного матеріалу

Розглянемо алгоритм Вонга [9], який здатний виявляти зміни (значення пікселів і розмір зображення) шляхом використання алгоритму шифрування з відкритим ключем RSA і контрольної суми MD5 для хеш-функції. Алгоритм вбудовування крихких ЦВЗ відображено на рис. 1.

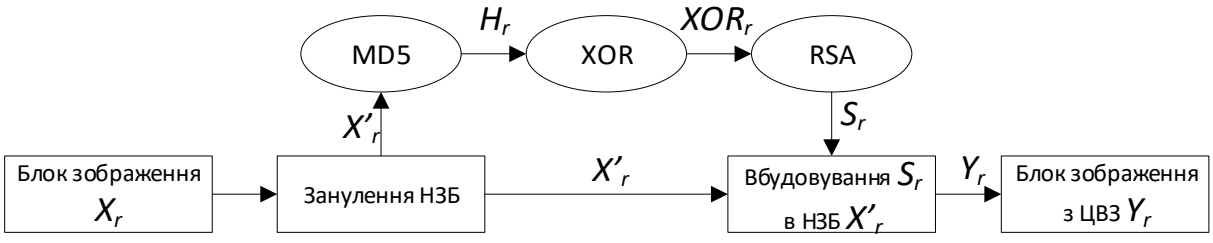

Рис. 1. Вбудовування крихкого ЦВЗ

Опишемо кожен крок роботи даного алгоритму:

1. поділ початкового зображення X на субзображення X_r;
2. поділ водяного знаку W на частини W_r;
3. для кожного субзображення X_r отримуються X_r' шляхом занулення незначущих біт (НЗБ);
4. для кожного X_r' обраховуються коди H_r з використанням криптографічної хеш-функції (MD5);
5. XOR_r отримується шляхом виконання операції над H_r та W_r;
6. S_r отримується шляхом шифрування XOR_r за допомогою алгоритму RSA з приватним ключем K';
7. S_r вбудовується у LSB субзображення, у результаті чого отримуємо субзображення Y_r із ЦВЗ;
8. субзображення Y_r об'єднуються у результуюче зображення Y.

У свою чергу, алгоритм вилучення крихких ЦВЗ зображено на рис. 2.

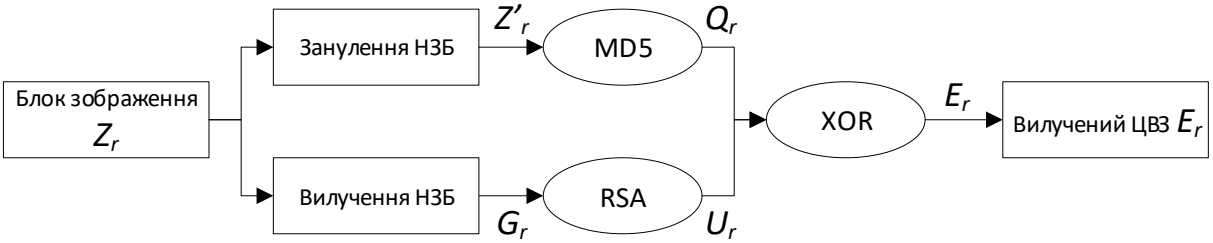

Рис. 2. Вилучення крихкого ЦВЗ

Здійснимо опис алгоритму вилучення крихкого ЦВЗ Вонга:

1. поділ зображення Z із ЦВЗ на субзображення Z_r;
2. для кожного субзображення Z_r отримуються Z_r' шляхом занулення незначущих біт;
3. G_r отримуються шляхом вилучення незначущих біт із субзображення Z_r;
4. U_r є результатом дешифрування G_r з використанням алгоритму RSA та публічного ключа K;
5. для кожного субзображення Z_r обраховуються коди Q_r з використанням хеш-функцій (MD5);
6. вилучений ЦВЗ E_r отримується шляхом виконання операції XOR із аргументами Q_r та G_r.

Для підвищення безпеки алгоритму Вонга, при створенні водяного знаку замінимо хеш-функцію MD5 на HMAC-SHA-256. Також з ціллю збільшення надійності, при знаходженні позиції для вбудовування блоків згенерованого ЦВЗ, використаємо псевдовипадкову послідовність, поріг значень якої генерується динамічно. При цьому біти згенерованого ЦВЗ вбудовуються у два останні найменш значущі біти векторів руху, що сприяє розширенню корисного навантаження вбудовування (до 256 біт) завдяки функції HMAC-SHA256.

Щоб забезпечити ефективність автентифікації слід використовувати сильні візуальні особливості, які застосовуються для генерації крихких ЦВЗ та складаються з набору коефіцієнтів, отриманих із передбачуваних INTRA та INTER блоків при стисненні відеопотоку. Дані характеристики містять квантовані постійні коефіцієнти (DC) і перші два змінні коефіцієнти (AC), що входять до низькочастотних коефіцієнтів у порядку сканування зигзагом кожного блоку (в межах INTRA 4×4 та INTER 4×4). Далі обирається DC-коефіцієнт, який є показником середньої енергії по всіх 4×4 пікселях та коефіцієнти з найбільшою енергією, що міститься в межах перших декількох низькочастотних коефіцієнтів [10].

Усі отримані дані та коефіцієнти зберігаються в буфері до моменту миттєвого оновлення декодера (IDR). Кадри IDR є I-кадрами (ключові кадри оновлення, що кодуються незалежно від інших кадрів), тому вони не надсилаються поза межі поточної групи кадрів (GOP). Дана група складається з I-кадру та всіх інших P-кадрів, що містять інформацію про змінені дані відносно попереднього кадру і розташовані між кадрами IDR. Тому кодована підпослідовність відео починається з кадру IDR і закінчується, коли з'являється новий кадр IDR, сигналізуючи про наявність нової підпослідовності, що підлягає кодуванню або про закінчення передачі. У кінці кожної групи кадрів ознаки, що присутні в буфері, проходять через захищену функцію хешування HMAC-SHA256, яка використовується для перевірки автентичності повідомлень.

Таким чином, процес створення ЦВЗ складається з декількох етапів:

1. змішування характеристик, що зберігаються у буфері, з секретним ключем К;
2. створення хешу з отриманої послідовності за допомогою SHA-256;
3. змішування хешу з секретним ключем К;
4. застосування обробки SHA-256.

Отримана хеш-послідовність довжиною 256 біт використовується в якості крихкого ЦВЗ, який вбудовується у вектори руху (MV) в H.264/AVC.

Вбудовування крихкого ЦВЗ виконується над векторами руху в межах Р-кадрів, які мають високі показники руху (зміни) та належать до вибраних блоків вбудовування. Секретний ключ К використовується для генерування псевдовипадкової послідовності для вибору позиції блоків вбудовування.

Для ретельного вибору блоків вбудовування необхідно розглянути два обмежувальні параметри. Перше обмеження – сусідні блоки пропущених блоків відкидаються, оскільки в декодері вектори руху пропущених блоків генеруються лише на основі передбачення вектора руху. Отже, помилка вектора руху в пропущеному блоці, який не може бути компенсований, вбудовується в сусідні блоки. Але зміна цих блоків може збільшити бітрейт відео. Інше обмеження, яке необхідно врахувати – необхідність уникнення вбудовування інформації в блоки з відсутністю руху та блоки з незначними рухами, адже будь-які зміни в цих блоках будуть сприйняті візуально людиною без спеціального обладнання й призведуть до збільшення бітрейту та, відповідно, розміру відео.

Кадри з високим рівнем руху вибираються відповідно до інтенсивності рухової активності в кожному кадрі. Для кожного Р-кадру обчислюється матриця просторової активності [11]:

$$C = \{MV(i,j)\},$$

$$MV(i,j) = \sqrt{\left(MV_x(i,j)\right)^2 + \left(MV_y(i,j)\right)^2},$$

де (i,j) позначають індекси блоку.

Середнє значення матриці активності C^{avg} Р-кадру визначається за формулою:

$$C^{avg} = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1} C(i,j),$$

де M та N – ширина та висота блоку, відповідно.

Рухова активність кадру визначається як стандартне відхилення величини вектора руху:

$$\sigma_{Fi} = \sqrt{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left(C(i,j) - C^{avg}(i,j)\right)^2}.$$

Кадри з високою руховою активністю вибираються лише за умови, що стандартне відхилення задовольняє умову $\sigma \geq T$, де T – це поріг, який отримується експериментально.

Завдяки такому вибору неозброєним оком важко помітити зміни, викликані вбудовуванням ЦВЗ.

Для зменшення спотворення над кожним компонентом обраних векторів руху, перед вбудовуванням, виконується квантування:

$$Q(MVx) = \begin{cases} (2 + MVx)\&(0xFFFC) & MVx \geq 0 \\ -\left((2 - MVx)\&(0xFFFC)\right) & MVx < 0 \end{cases},$$

$$Q(MVy) = \begin{cases} (2 + MVy)\&(0xFFFC) & MVy \geq 0 \\ -\left((2 - MVy)\&(0xFFFC)\right) & MVy < 0 \end{cases}.$$

де XOR (&) використовується для видалення найменш значущого біту векторів руху.

Біти ЦВЗ вбудовуються в останні два найменш значущі біти контейнеру:

$$\overline{MVx} = \begin{cases} Q(MVx) - a, & \text{якщо } Q(MVx) \geq 0 \text{ та } a = 2 \\ Q(MVx) + a, & \text{у іншому випадку} \end{cases},$$

$$\overline{MVy} = \begin{cases} Q(MVy) - a & \text{якщо } Q(MVy) \geq 0 \text{ та } a = 2 \\ Q(MVy) + a & \text{у іншому випадку} \end{cases},$$

де a – значення бітів ЦВЗ: -1, 0, 1 та 2, що відповідають парі бітів 11, 00, 01 та 10, відповідно.

Для мінімізації спотворень, спричинених вбудовуванням ЦВЗ, процес вбудовування повинен забезпечити умову рівності:

$$Q(\overline{MV_x}) = Q(MV_x) \text{ та } Q(\overline{MV_y}) = Q(MV_y).$$

Вихідний вектор руху (MV) складається з векторів руху різних координат (MV_x та MV_y).

Отже, алгоритм роботи удосконаленого методу вбудовування крихких ЦВК матиме вигляд:

1.розбиття послідовності на групи кадрів;
2.збереження властивостей яскравості та насиченості;
3.вибір основного кадру з групи;
4.використання функції HMAC-SHA256 із секретним ключем та збереженими даними;
5.вибір кадрів із значною руховою активністю;
6.вибір задовільних векторів руху;
7.квантування обраних векторів руху;
8.перевірка виконання рівності квантових та оригінальних векторів;
9.при виконанні рівності – вбудовування даних у кадр.

Процес вилучення ЦВЗ виконується на рівні декодеру H.264/AVC та без потреби в оригінальному відеопотоці. Цей процес схожий на процес вбудовування, адже включає в себе обчислення кадрів з найбільшою руховою активністю, вибір позиції вбудовування на основі ключа K, ентропійне декодування векторів руху і застосування двох умов, які виконуються в процесі вбудовування. Біти водяного знаку потім вилучаються з двох останніх найменш значущих бітів компонентів MV_x і MV_y для кожного блоку вбудовування.

Удосконалений алгоритм автентифікації відео з крихким ЦВЗ.

На етапі автентифікації необхідно визначити візуальні особливості, які були використані при вбудовуванні. Це відбувається перед оберненим квантуванням і операціями перетворення усередині алгоритму H.264/AVC-декодера. Наприкінці кожної незалежної групи кадрів, визначеної декодером, дані шифруються з використанням функції HMAC-SHA-256. Це сприяє перевірці цілісності інформації, адже отримане хеш-значення порівнюється з вилученими бітами водяного знаку. Будь-які зміни особливостей або хеш-значень будуть означати зміни у контейнері. Таким чином, вміст автентифікується лише в тому випадку, коли оригінальні та обчислені значення хешу однакові.

Удосконалений алгоритм автентифікації відображено на рис. 3.

У разі невдалої автентифікації виявлення фальшивих кадрів виконується окремо. Щоб визначити розташування фальсифікованих кадрів в межах пошкодженої групи кадрів, отримувач обчислює хеш-значення всіх кадрів у GOP на рівні декодера та хеш-значення оригінальної групи кадрів. Після цього, порівнюється значення хешу кожного кадру окремо і якщо хеш не однаковий, то виявляється змінений кадр.

Аналіз запропонованого алгоритму

Для аналізу ефективності удосконаленого методу вбудовування крихких ЦВЗ необхідно провести перевірку на можливість втручання у просторову, часову області та область кольору. Втручання можливе шляхом зміни порядку кадрів, їх заміни, зміни розмірів, повертання та зміни кольору області чи окремих областей.

Також необхідно проаналізувати максимальну корисну завантаженість, вплив вбудовування на візуальну складову відео, якість відео, зміну розміру вихідного відео та стійкість проти випадкових спотворень чи змін.

Кількість бітів корисного навантаження або ємності водяного знаку по відношенню до деградації відео є важливою характеристикою крихких ЦВЗ. У запропонованому алгоритмі ємність водяного знаку залежить від рухової активності та спотворення, що спричиняються вбудовуванням. Для потокового відео зі

значною руховою активністю ($\sigma \geq 3{,}870$) кількість блоків для вбудовування звичайно більша, ніж у відео з незначною руховою активністю, отже і об'єм даних для вбудовування може бути збільшений.

У табл. 1 наведено порівняння можливої кількості даних для вбудовування при зміні одного найменш значущого біта у векторах руху запропонованого методу (ЗМ) та існуючого методу (ІМ) для оригінальної відеопослідовності (ОВ) та відео з крихким ЦВЗ.

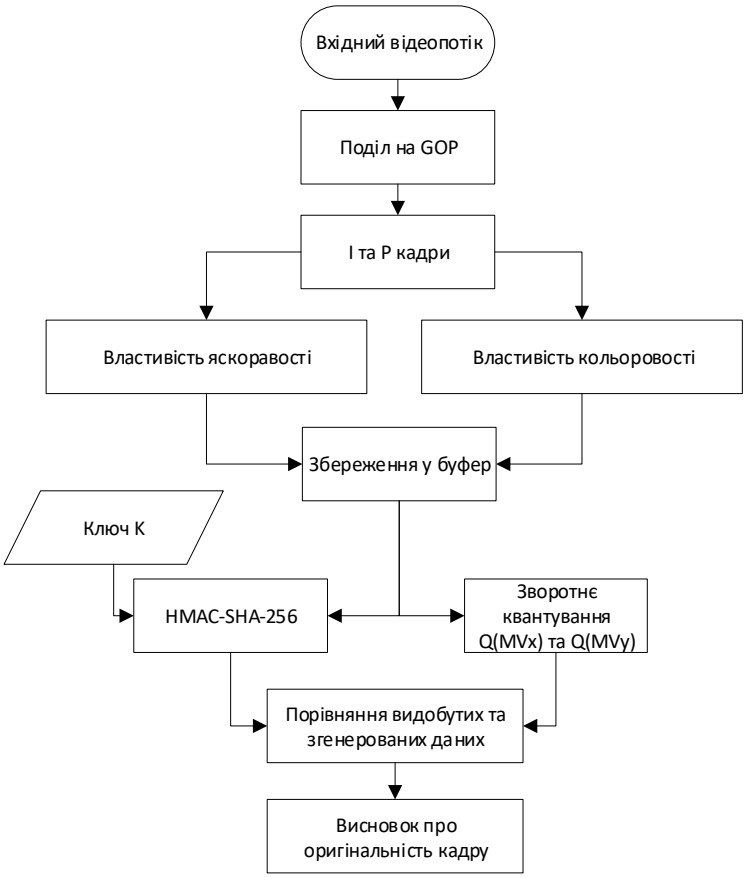

Рис. 3. Удосконалений алгоритм автентифікації

Таблиця 1.

Порівняння з існуючим аналогом

Відеопослідовність	**Середнє корисне навантаження (біт)**		**PSNR**				
	ЗМ	**ІМ**	**ОВ**	**ЗМ**	**Різниця між ОВ та ЗМ**	**ІМ**	**Різниця між ЗМ та ІМ**
Miss America	162	88	40.056	40.056	0	40.04	0.016
Claire	238	135	39.681	39.681	0	39.67	0.011
Akiyo	248	133	38.205	38.205	0	38.17	0.035
Bridgeclose	518	264	34.847	34.847	0	34.85	0.03
Carphone	2960	1495	37.340	37.315	0.025	37.29	0.025
Coastguard	5334	2806	34.181	34.026	0.155	34.02	0.006
Flower	8578	4304	34.336	34.308	0.028	34.31	0.02
Foreman	7688	2569	36.687	36.45	0.237	35.75	0.3
Suzie	2760	1349	37.357	37.141	0.216	37.12	0.021
Table	9992	5182	35.23	34.915	0.315	34.91	0.05

Пікове співвідношення сигналу до шуму (PSNR) – це об'єктивна міра візуальної якості стисненого відео. Даний показник зчитується з файлу журналу, створеного під час виконання кодеку H.264/AVC. Як видно з даних, PSNR залишається майже незмінним для відео з низькою руховою активністю та однорідними областями.

Програмні засоби оцінювання якості відео (VQM) та індексу структурної подібності (SSIM) використовуються для вимірювання тимчасових та структурних якостей відеопотоку. Значення VQM, яке є близьким до 0 означає наявність меншого спотворення (табл. 2).

Таблиця 2

Результати аналізу VQM та SSIM

Відеопослідовність	VQM	SSIM
Miss America	0.192	0.998
Claire	0.206	0.978
Akiyo	0.187	0.995
Bridgeclose	0.245	0.981
Carphone	0.292	0.987
Coastguard	0.234	0.998
Flower	0.290	0.995
Foreman	0.351	0.976
Suzie	0.289	0.983
Table	0.398	0.968

Як показано в табл. 2, значення VQM лежать у діапазоні від 0,292 до 0,398, що призводить до незначного розходження між оригіналом та відеопослідовністю з водяним знаком. Індекс SSIM, зазвичай, використовується при порівнянні відео з водяними знаками та оригіналу з точки зору подібності або розбіжностей яскравості, контрасту і структурних змін. Значення SSIM, близьке до 1, вказує на високу подібність двох відео і 0 – на повну невідповідність. З отриманих результатів аналізу відео можна зробити висновок, що на відео немає ніяких видимих змін після процесу вбудовування, оскільки всі значення дуже близькі до 1.

Програмна реалізація удосконаленого алгоритму вбудовування крихких ЦВЗ.

Використовуючи технологію ASP.NET створимо програний додаток, що дозволить виявити несанкціоновані модифікації кадрів та відображення для подальшого їхнього аналізу.

Оскільки вбудовування ЦВЗ відбувається на рівні кодування відео, необхідно розробити методи, що можуть приймати необхідне відео, аналізувати його, проводити операцію кодування з вбудовуванням певних даних та подальшою обробкою результату.

З врахуванням вищезазначених умов, опишемо кроки розробленого алгоритму роботи додатку:

1. запуск серверу;
2. вибір секретних ключів;
3. створення сесії відеопотоку;
4. запуск процесу вбудовування крихкого ЦВЗ у відеопотік;
5. підключення користувачів;
6. запуск процесу видобування крихкого ЦВЗ;
7. аналіз на наявність несанкціонованих модифікацій;
8. відображення областей з модифікаціями (при їх наявності).

Для використання алгоритму розроблено зручний інтерфейс з можливістю вибору доступної камери, перегляду поточного зображення з обраної камери та вибору секретного ключа шифрування (рис. 4).

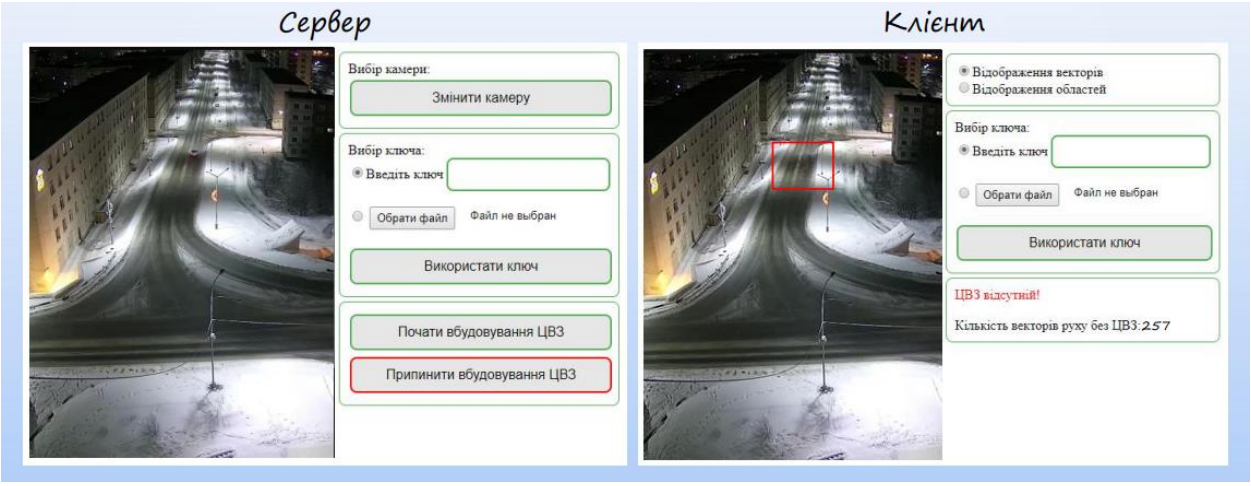

Рис. 4. Інтерфейс розробленого додатку

У клієнтській частині додатку відображається поточне зображення з камери, що уже містить у собі крихкий ЦВЗ та список модифікованих кадрів, кожний з яких містить позначення зміненої області.

Обговорення результатів та перспективи подальшого розвитку досліджень

Отримані результати показують, що за рахунок використання удосконаленого методу вбудовування крихких ЦВЗ підвищується захищеність потокового відео від несанкціонованої модифікації. Це відбувається, зокрема, за рахунок використання функції з секретним ключем HMACSHA-256, вбудовування інформації у два останні найменш значущі біти та вибору кадрів з достатньою руховою активністю.

Проте подальших досліджень потребує пошук нових шляхів виявлення атак на ЦВЗ, що дозволить підвищити захищеність потокового відео від несанкціонованого копіювання та розповсюдження. Зокрема, варто звернути увагу на застосування нейронних мереж, які дозволяють створювати більш складні та стійкі до атак алгоритми вбудовування.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі

У даній роботі було детально розглянуто метод вбудовування крихких ЦВЗ у відео, проаналізовано можливі шляхи його вдосконалення. На основі отриманих даних запропоновано покращення методу вбудовування крихких ЦВЗ у вектори руху блоків кадрів у відеопотоці. При цьому для підвищення надійності, при знаходженні позиції для вбудовування блоків згенерованого ЦВЗ, використано псевдовипадкову послідовність, поріг значень якої генерується динамічно. Крім того, біти згенерованого ЦВЗ було вбудовано у два останні найменш значущі біти векторів руху, що спричинило розширенню корисного навантаження вбудовування (до 256 біт) завдяки функції HMAC-SHA256.

У результаті оцінювання ефективності удосконаленого методу виявлено, що він дозволяє вбудувати у середньому в 2,03 рази більше інформації зі збільшенням пікового співвідношення сигналу до шуму на 0.05, що є непомітним для неозброєного ока. В свою чергу, при порівнянні існуючого методу та запропонованого щодо можливої кількості даних для вбудовування, було виявлено переваги останнього. Крім того, відео немає ніяких видимих змін після процесу вбудовування, оскільки всі значення індексу структурної подібності близькі до одиниці. Таким чином, алгоритм є дієвим та забезпечує можливість виявлення несанкціонованої модифікації потокового відео.

Також для удосконаленого методу вбудовування крихких ЦВЗ було розроблено програмне забезпечення, яке дозволяє виявляти несанкціоновані модифікації кадрів та відображення для їхнього подальшого аналізу, що в свою чергу, сприяє підвищенню захищеності відеоконтенту.

Література

1. Козак Д. О. Захист авторського права на відеофайли з використанням цифрового водяного знака [Електронний ресурс] / Д. О. Козак, О. В. Салієва // Матеріали L науково-технічної конференції підрозділів ВНТУ, Вінниця, 10-12 березня 2021 р. – Електрон. текст. дані. – 2021. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2021/paper/view/12438

2. Конахович Г. Ф., Прогонов Д. О., Пузиренко О. Ю. Комп’ютерна стеганографічна обробка й аналіз мультимедійних даних: підручник. – К. : «Центр навчальної літератури», 2018. 558 с.

3. Kothari A. M., Dwivedi V., Thanki R. M. Watermarking techniques for copyright protection of videos. – Cham : Springer International Publishing, 2019.

4. Zhou J., Pun C. M. Personal privacy protection via irrelevant faces tracking and pixelation in video live streaming // IEEE Transactions on Information Forensics and Security. – 2020. – Т. 16. – С. 1088-1103.

5. Xu H. et al. Audio-visual autoencoding for privacy-preserving video streaming // IEEE Internet of Things Journal. – 2021. – Т. 9. – №. 3. – С. 1749-1761.

6. Gillani S. M. et al. VQProtect: Lightweight Visual Quality Protection for Error-Prone Selectively Encrypted Video Streaming //Entropy. – 2022. – Т. 24. – №. 6. – С. 755.

7. Favorskaya M. N., Buryachenko V. V. Authentication and copyright protection of videos under transmitting specifications // Computer Vision in Advanced Control Systems-5: Advanced Decisions in Technical and Medical Applications. – 2020. – С. 119-160.

8. Sripradha, R., and K. Deepa. A new fragile image-in-audio watermarking scheme for tamper detection // 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). IEEE, 2020.

9. Wang, Chuen-Ching, and Yi-Chuan Lin. Watermarking algorithm with post-compression capability for digital video surveillance // SIP. 2007.

10. Huang, Jiwu, Yun Q. Shi, and Yi Shi. Embedding image watermarks in DC components // IEEE transactions on circuits and systems for video technology 10.6 (2000): 974-979.

11. Хорошко В. О., Яремчук Ю. Є., Карпінець В. В. Комп'ютерна стеганографія: навчальний посібник. – Вінниця : ВНТУ, 2017. 155 с.

References

1. D. O. Kozak. Copyright protection of video files using a digital watermark [Electronic resource] / D. O. Kozak, O. V. Saliieva // Materials L of the scientific and technical conference of VNTU divisions, Vinnytsia, March 10-12, 2021 - Electron. text. data. – 2021. – Access mode: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2021/paper/view/12438

2. Konakhovich G. F., Progonov D. O., Puzyrenko O. Yu. Computer steganographic processing and analysis of multimedia data: a textbook. - K.: "Center for Educational Literature", 2018. 558 p.

3. Kothari A. M., Dwivedi V., Thanki R. M. Watermarking techniques for copyright protection of videos. – Cham : Springer International Publishing, 2019.

4. Zhou J., Pun C. M. Personal privacy protection via irrelevant faces tracking and pixelation in video live streaming // IEEE Transactions on Information Forensics and Security. – 2020. – Т. 16. – С. 1088-1103.

5. Xu H. et al. Audio-visual autoencoding for privacy-preserving video streaming // IEEE Internet of Things Journal. – 2021. – Т. 9. – №. 3. – С. 1749-1761.

6. Gillani S. M. et al. VQProtect: Lightweight Visual Quality Protection for Error-Prone Selectively Encrypted Video Streaming //Entropy. – 2022. – Т. 24. – №. 6. – С. 755.

7. Favorskaya M. N., Buryachenko V. V. Authentication and copyright protection of videos under transmitting specifications // Computer Vision in Advanced Control Systems-5: Advanced Decisions in Technical and Medical Applications. – 2020. – С. 119-160.

8. Sripradha, R., and K. Deepa. A new fragile image-in-audio watermarking scheme for tamper detection // 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS). IEEE, 2020.

9. Wang, Chuen-Ching, and Yi-Chuan Lin. Watermarking algorithm with post-compression capability for digital video surveillance // SIP. 2007.

10. Huang, Jiwu, Yun Q. Shi, and Yi Shi. Embedding image watermarks in DC components // IEEE transactions on circuits and systems for video technology 10.6 (2000): 974-979.

11. Khoroshko V.O., Yaremchuk Yu.E., Karpinets V.V. Computer steganography: a tutorial. – Vinnytsia: VNTU, 2017. 155 p.