Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Кваліфікаційна наукова
праця на правах рукопису

БОЛОГОВА НАТАЛІЯ МИКОЛАЇВНА

УДК 004.93.1: 004.032.26

ДИСЕРТАЦІЯ

МОДЕЛЬ, МЕТОДИ ТА ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ АВТЕНТИФІКАЦІЇ ЦИФРОВИХ ЗОБРАЖЕНЬ У ПРИКЛАДНИХ СИСТЕМАХ КОРИСТУВАЧА

Спеціальність: 126 – Інформаційні системи та технології
Галузь знань: 12 – Інформаційні технології

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело _____ Н.М. Бологова

Науковий керівник
Рубан Ігор Вікторович,
доктор технічних наук, професор

Харків – 2023

АНОТАЦІЯ

Бологова Н.М. Модель, методи та інформаційна технологія автентифікації цифрових зображень у прикладних системах користувача. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 126 «Інформаційні системи та технології» (12 – Інформаційні технології). – Харківський національний університет радіоелектроніки, Міністерство освіти і науки України, Харків, 2023.

Дисертаційну роботу присвячено актуальному завданню розробці інформаційної технології підтвердження права власності на цифрові зображення, яка використовує сучасні тенденції в області галузі цифрових водяних знаків та блокчейну для створення нової децентралізованої технології підтвердження права власності цифрових зображень. У дисертаційній роботі на основі отриманих теоретичних та експериментальних досліджень вирішена задача побудови методів генерації стійкого до спотворень цифрового водяного знака на основі хаотичних карт та розробки інформаційної технології підтвердження права власності на цифрові зображення.

Метою дисертаційної роботи є розробка інформаційної технології підтвердження права власності на цифрові зображення, яка використовує сучасні тенденції в галузі цифрових водяних знаків та блокчейну для створення нової децентралізованої технології підтвердження права власності на цифрові зображення.

Об’єкт дослідження – процес підтвердження права власності на цифрові зображення.

Методи дослідження – системний аналіз; процесний підхід – для вивчення процесів, які відбуваються при забезпеченні авторського права на твір; моделювання; теорія множин – для опису моделі автентифікації цифрових зображень; стеганографічні методи – для реалізації приховування

самого факту використання цифрового підпису зображення, що забезпечує процес підтвердження права власності.

Наукова новизна дисертаційної роботи полягає в такому:

1. Вперше запропоновано комплексний критерій оцінки ефективності методів вбудови цифрових водяних знаків на зображення, який побудований з урахуванням ключових характеристик та визначенням вагових коефіцієнтів, та дозволяє провести комплексну оцінку ефективності методу нанесення цифрових водяних знаків.

2. Вдосконалено метод надійної перевірки справжності цифрового зображення з високим ступенем захисту. Надійність досягається за рахунок того, що ЦВЗ ховається не в усьому зображенні, а в його фрагменті, який найбільше підходить для приховування зображення, а також застосування як ЦВЗ завадових кодів.

3. Вдосконалено метод підвищення стійкості стегосистеми за рахунок врахування ключових показників. Описаний у роботі метод псевдоголографічного кодування цифрових водяних знаків є ефективним для протидії усім типам атак, що розглядалися, окрім повороту зображення.

4. Отримали подальший розвиток методи генерації ЦВЗ для цифрових зображень, а саме розроблено методи генерації ЦВЗ на основі хаотичних карт та додаткової фільтрації цифрового водяного знаку. Описані у роботі методи є ефективними для забезпечення стійкості ЦВЗ до локальних спотворень. Як показали дослідження, при 60 % спотворення зображення можливо відновити 90 % ЦВЗ.

5. Удосконалено інформаційну технологію підтвердження права власності на цифрові зображення, що основуються на технології блокчейн та цифрових водяних знаках для забезпечення надійної гарантії встановлення авторських прав.

У дисертаційній роботі проведено аналіз сучасного стану проблеми і особливості задач забезпечення авторського права та підтвердження автентичності цифрових зображень. Проаналізовано методи нанесення

цифрових водяних знаків на зображення та представлено сучасні підходи до їх реалізації.

Розроблено функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення, яка основана на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку. Описаний у роботі метод псевдоголографічного кодування цифрових водяних знаків є ефективним для протидії усім типам атак, що розглядалися, окрім повороту зображення. Проведення комплексної оцінки методики підвищення стійкості методу вбудови цифрового водяного знаку на основі вейвлет-перетворення показало, що її використання на 20 % покращує стійкість до різних типів атак.

В роботі представлено показник оцінки стійкості методів нанесення цифрових водяних знаків, який враховує всі типи атак і дозволяє провести комплексну оцінку стійкості методу вбудови цифрових водяних знаків.

Проведено експериментальне дослідження щодо запропонованої методики. Найбільш ефективною ця методика є при втраті частини зображення. При попередній фільтрації цифрового водяного знаку найбільш ефективним є третій метод фільтрації. Цей метод і представляє собою усереднення по клітинці і подальшу бінаризацію. Для оцінки кута повороту знаходиться матриця афінного перетворення, що отримується по узгодженому набору відповідних ORB-дескрипторів. Використання цього методу дозволяє безпомилково виділяти цифровий водяний знак для всього діапазону кутів, що досліджувалися.

Проведено аналіз хаотичних карт на предмет забезпечення стійкості ЦВЗ. Аналіз показав, що використання хаотичних карт для перемішування біт пікселів або самих пікселів на зображенні можуть забезпечити захищеність та стійкість до спотворень. Розрахунки коефіцієнта кореляції сусідніх пікселів при використанні хаотичних карт свідчать про ефективність їх використання.

Розроблені методи генерації ЦВЗ на основі хаотичних карт та

додаткової фільтрації цифрового водяного знаку. Описані у роботі методи є ефективними для забезпечення стійкості ЦВЗ до локальних спотворень. Як показали дослідження, при 60 % спотворення зображення можливо відновити 90 % ЦВЗ.

Проведено експериментальне дослідження щодо запропонованих методів. Гістограми ЦВЗ показали, що обидва методи забезпечують генерацію ЦВЗ випадкової незрозумілої форми. Але метод заснований на комбінації карт кота Арнольда та карт Генона має помітні піки, на відміну від метода, який заснований на перемішуванні пікселів та їх біт виключно за допомогою карт кота Арнольда. Це свідчить про те, що метод заснований тільки на картах кота Арнольда має більш хаотичний характер. Про це також свідчить і значення коефіцієнта кореляції між сусідніми пікселями, який наближається до 0 і дорівнює 0.0109 для кольорових ЦВЗ та 0.030 для чорно-білих зображень.

Враховуючи загальнодоступність мережі інтернет і постійне зростання випадків порушення авторського права на цифровий контент, сучасні технології, що використовуються для захисту авторських прав, мають бути вдосконалені.

Технологія блокчейн володіє такими характеристиками, як децентралізація, захист від підробки та шифрування, розширюваності та гнучкості, що дозволяє ефективно вирішити питання реєстрації та підтвердження цифрового авторського права, вона відіграє значну роль у захисті прав та інтересів авторів.

У роботі запропоновано інформаційну технологію підтвердження права власності на цифрові зображення, яка використовує цифрові водяні знаки, блокчейн, хеш-функції для зображення і IPFS для створення нової децентралізованої технології підтвердження права власності у цифрову епоху інтернету.

Що стосується типів файлів, згадується лише управління авторськими правами на цифрові зображення. У майбутньому технологію можна буде

розширити на аудіо, відео та інші типи мультимедійних файлів, щоб сформувати єдину систему для підтвердження права власності на будь-який цифровий контент.

В дисертаційній роботі розв'язано актуальне науково-практичне завдання розробки інформаційної технології підтвердження права власності на цифрові зображення, яка використовує сучасні тенденції в області цифрових водяних знаків та блокчейну для створення нової децентралізованої технології підтвердження права власності цифрових зображень.

Практичне значення отриманих результатів полягає в такому:

- розроблено функціональний алгоритм вбудови цифрових водяних знаків в цифрові зображення, основані на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку, що дозволяє протидіяти типам атак, окрім повороту зображення;

- розроблено алгоритм надійної перевірки справжності цифрового зображення з високим ступенем захисту, що дозволяє сховати ЦВЗ в його фрагменті;

- удосконалено інформаційну технологію підтвердження права власності на цифрові зображення, що основується на технології блокчейн та цифрових водяних знаках для забезпечення надійної гарантії встановлення авторських прав.

Отриманий в роботі метод надійної перевірки справжності цифрового зображення з високим ступенем захисту від спотворення та підробки, був підтверджений результатами проведених випробувань, які доказали стійкість даної конструкції до геометричних і не геометричних атак (ТОВ «ОБОРОННІ ТЕХНОЛОГІЇ», м.Київ), про що свідчить акт від 26.02.2023. Також результати дисертаційного дослідження використані в освітньому процесі Харківського національного університету радіоелектроніки, зокрема, у навчальній дисципліні «Системне програмне забезпечення» для здобувачів першого (бакалаврського) рівня вищої освіти за освітньо-професійною

програмою «Комп’ютерна інженерія» (акт від 14.11.2023.)

Матеріали дисертації повною мірою викладені у 14 публікаціях, зокрема 7 статей, з них – 6 статей у фахових періодичних виданнях України з технічних наук, з яких 2 – категорії А (індексується в Scopus); 4 – категорії Б, 1 стаття у інших виданнях (Індія), 7 тез доповідей у матеріалах міжнародних наукових конференцій.

Ключові слова: інформаційна технологія, дискретне косинусне перетворення, цифровий водяний знак, розподіл даних, вейвлет-перетворення, хаотичний сигнал, відношення сигнал/шум, ключова точка зображення, детектор, дескриптор, метод мульти-Отцу, обробка зображень, випадкова величина, кореляційна обробка, модель даних.

Список публікацій здобувача

1. Бологова Н.М. Дослідження моделей та методів обробки зображень та шляхи вдосконалення технологій розпізнавання маркерів в системах доповненої реальності / Н.М. Бологова, І. В. Рубан // Сучасний стан наукових досліджень та технологій в промисловості. – 2019. – № 1 (7). – С. 25 –33 (Належить до категорії Б).

2. Ruban I. Method of sustainable detection of augmented reality markers by changing deconvolution / I. Ruban, N. Bolohova, V. Martovytskyi, V. Lebediev, N. Lukova-Chuiko // International Journal of Advanced Trends in Computer Science and Engineering. 2020. – № 9 (2). – P. 1113–1120.

3. Makoveichuk O. Development of a method for improving stability method of applying digital watermarks to digital images / O. Makoveichuk, I. Ruban, N. Bolohova, A. Kovalenko, V. Martovytskyi, T. Filimonchuk // Eastern-European Journal of Enterprise Technologies. 2021. – № 3 (2 (111)). – P. 45–56. (Належить до категорії А, входить до міжнародної наукометричної бази Scopus).

4. Ruban I. Digital image authentication model / I. Ruban, N. Bolohova, V. Martovytskyi, O Koptsev // Advanced Information Systems. 2021. – № 5 (1). – P. 113–117 (Належить до категорії Б).

5. Ruban I. Methodology for assessing the effectiveness of methods for embedding digital watermarks / I. Ruban, N. Bolohova, V. Martovytskyi, R. Yaroshevych // Advanced Information Systems. 2021. – № 5 (3). – P. 112–118 (Належить до категорії Б).

6. Martovytskyi V. Development of methods for generation of digital watermarks resistant to distortion / V. Martovytskyi, I. Ruban, N. Bolohova, O. Sievierinov, O. Zhurylo, O. Permiakov, A. Nosyk, D. Nepokrytov, I. Krylenko // Eastern-European Journal of Enterprise Technologies. 2021. – № 6 (2 (114)). – P. 103–116. (Належить до категорії А, входить до міжнародної наукометричної бази Scopus).

7. Ruban I. Information technology for confirming property rights to digital images / I. Ruban, N. Bolohova, V. Martovytskyi // Advanced Information Systems. 2022.– № 6 (1). – P. 118–123 (Належить до категорії Б).

8. Ruban I. et al. Method of neural network recognition of ground-based air objects //2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – IEEE, 2018. – С. 589-592.

9. Бологова Н.М. Аналіз сучасного підходу обробки зображень для розпізнавання маркерів в системі доповненої реальності / Н.М. Бологова, І.В. Рубан, К.Р. Локотецька // Тези доповідей шостої міжнародної науково-практичної конференції «Проблеми інформатизації». 14 – 16 листопада 2018 р., Черкаси, Баку, Бельско-Бяла, Харків. – 2018. – С.36.

10. Bolohova N. Analysis of restoration methods for optical-electronic images lubricated at motion / N. Bolohova, Y. Kortiak // Тези доповідей шостої міжнародної науково-практичної конференції «Проблеми інформатизації». 13 – 15 листопада 2019 р., Черкаси, Харків, Баку, Бельско-Бяла. – 2019. – С.8.

11. Bolohova N. Analysis of the current status of additional reality technologies / N. Bolohova, Y. Kortyak, A. Liashova // Proceedings of Fourth International Scientific and Technical Conference on COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. – Kharkiv, April 22-23, 2020. – P.12–13.

12. Bolohova N. Method for evaluating the effectiveness of methods for embedding digital watermarks / N. Bolohova, V. Martovytskyi, V. Diachenko, O. Kolomiitsev, V. Fedorchenko // Матеріали XX міжнародної науково-практичної конференції «Інформаційні технології і безпека». Київ. – 2020. С. 75–83.

13. Пересада Р.А. Аналіз методів підвищення стійкості водяних знаків у цифрових зображеннях / Р.А. Пересада, Н.М. Бологова // Тези доповідей восьмої міжнародної науково-технічної конференції «Проблеми інформатизації». 26 – 27 листопада 2020 р., . Черкаси, Харків, Баку, Бельсько-Бяла. – 2020. – С. 53.

14. Бологова Н.М. Модель автентифікації цифрового зображення / Н.М. Бологова // Тези доповідей десятої міжнародної науково-практичної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління». 8 – 9 квітня 2021р., – Баку, Харків, Жиліна. – С. 41.

ABSTRACT

Bolohova N.M. Model, methods, and Information technology for digital image authentication in user-oriented systems. - Qualification scientific work on the rights of manuscript.

Thesis submitted for the degree of Doctor of Philosophy in the specialty 126 "Information Systems and Technologies" (12 - Information Technologies) - Kharkiv National University of Radio Electronics, Ministry of Education and Science of Ukraine, Kharkiv, 2023.

The thesis is devoted to the current problem of the urgent task of developing an information technology for confirming the ownership of digital images, which uses modern trends in the field of digital watermarks and blockchain to create a completely new decentralised technology for confirming the ownership of digital images. The thesis, based on theoretical and experimental studies, solves the problem of building methods for generating a distortion-resistant digital watermark based on chaotic maps and developing an information technology for confirming ownership of digital images.

The aim of the thesis is to develop an information technology for confirming the ownership of digital images that uses modern trends in digital watermarking and blockchain to create a completely new decentralised technology for confirming the ownership of digital images.

The object of research – the process of confirming ownership of digital images.

Research methods – system analysis, process approach – to study the processes that take place when securing copyright to a work, modelling, set theory – to describe the model of digital image authentication, steganographic methods – to implement the concealment of the very fact of using a digital image signature, which ensures the process of confirming ownership. Experimental studies were conducted in the laboratory and on real objects.

The scientific novelty of the dissertation is as follows:

1. First of all, a comprehensive criterion for evaluating the effectiveness of methods for embedding digital watermarks in images is proposed, which is built taking into account the key characteristics and determining the weighting coefficients, allowing for a comprehensive assessment of the effectiveness of the method of applying digital watermarks.

2. A method for reliable authentication of a digital image with a high degree of protection has been improved. Reliability is achieved due to the fact that the DW is not hidden in the entire image, but in its fragment, which is most suitable for hiding the image, as well as the use of interference codes as DW.

3. The method of increasing the stability of the stegasystem by taking into account key indicators is improved. The method of pseudo-holographic encoding of digital watermarks described in this paper is effective in counteracting all types of attacks considered, except for image rotation.

4. The methods of generating digital watermarks for digital images have been further developed, namely, methods of generating digital watermarks based on chaotic maps and additional filtering of the digital watermark. The methods described in this paper are effective in ensuring the robustness of the DW to local distortions. Studies have shown that with 60% image distortion, it is possible to recover 90% of the DW.

5. An improved information technology for confirming ownership of digital images based on blockchain technology and digital watermarks to provide a reliable guarantee of copyright establishment.

The thesis analyses the current state of the problem and the specifics of the tasks of copyright enforcement and authentication of digital images. The methods of applying digital watermarks to images are analysed and modern approaches to their implementation are presented.

A functional model of the process of ensuring the increase of stability of methods of embedding digital watermarks in digital images based on pseudoholographic coding and additional filtering of the digital watermark is developed. The method of pseudoholographic encoding of digital watermarks

described in this paper is effective in counteracting all types of attacks considered, except for image rotation. A comprehensive evaluation of the methodology for improving the resilience of the digital watermark embedding method based on Wavelet transforms showed that its use improves resilience to various types of attacks by 20 %.

The paper presents an indicator for assessing the robustness of digital watermarking methods, which takes into account all types of attacks and allows a comprehensive assessment of the robustness of the digital watermarking embedding method.

An experimental study of the proposed methodology has been carried out. This technique is most effective when part of the image is lost. When pre-filtering a digital watermark, the third filtering method is the most effective. This method is cell averaging and subsequent binarisation. The least effective is the first method of binarisation and finding a statistical mode by cell. It is advisable to perform binarisation using the Otsu algorithm. For an affine attack, which is a rotation of the image, this method is effective only when compensating for the rotation. To estimate the angle of rotation, the affine transformation matrix is obtained from an agreed set of corresponding ORB descriptors. Using this method, it is possible to accurately extract a digital watermark for the entire range of angles under study.

The chaotic maps were analysed to ensure the stability of the DW. The analysis showed that the use of chaotic maps to shuffle pixel bits or pixels themselves in an image can provide security and resistance to distortion. Calculations of the correlation coefficient of neighbouring pixels when using chaotic maps indicate the effectiveness of their use. Since images have high redundancy of information, it is desirable to have an algorithm that breaks this redundancy.

We have developed methods for generating DW based on chaotic maps and additional digital watermark filtering. The methods described in this paper are effective in ensuring the DW robustness to local distortions. Studies have shown that with 60 % image distortion, it is possible to recover 90 % of the DW.

An experimental study of the proposed methods was conducted. The histograms of the DW showed that both methods generate DW of random incomprehensible shape. However, the method based on the combination of Arnold cat maps and Genon maps has noticeable peaks, unlike the method based on mixing pixels and their bits using only Arnold cat maps. This indicates that the method based only on Arnold's cat maps is more chaotic. This is also evidenced by the value of the correlation coefficient between neighbouring pixels, which is close to 0 and equal to 0.0109 for colour DW and 0.030 for black and white images.

Given the public accessibility of the Internet and the constant increase in cases of copyright infringement of digital content, the current technologies used for copyright protection must be improved.

The blockchain technology has such characteristics as decentralisation, protection against counterfeiting and encryption, extensibility (can be replaced by scalability) and flexibility, which allows to effectively solve the issues of registration and confirmation of digital copyright, and it plays a significant role in protecting the rights and interests of authors.

This paper proposes an information technology for proving ownership of digital images that uses digital watermarks, blockchain, image hash functions and IPFS to create a completely new decentralised technology for proving ownership in the digital age of the Internet.

In terms of file types, only digital image copyright management is mentioned. In the future, the technology could be extended to audio, video, and other types of multimedia files to form a single system for proving ownership of any digital content.

The thesis solves the urgent scientific and practical task of developing an information technology for confirming ownership of digital images, which uses modern trends in the field of digital watermarks and blockchain to create a completely new decentralised technology for confirming ownership of digital images.

The practical value of the obtained results is as follows:

- a functional algorithm for embedding digital watermarks in digital images based on pseudo-holographic encoding and additional digital watermark filtering was developed, which allows to counteract types of attacks other than image rotation;
- developed an algorithm for reliable authentication of a digital image with a high degree of protection, which allows to hide the digital watermark in its fragment;
- improved information technology for confirming the ownership of digital images based on blockchain technology and digital watermarks to provide a reliable guarantee of copyright establishment.

The method of reliable authentication of a digital image with a high degree of protection against distortion and forgery obtained in this work was confirmed by the results of tests that proved the resistance of this design to geometric and non-geometric attacks (LLC "Defense Technologies", Kyiv), as evidenced by the act of 26.02.2023. Also, the results of the dissertation research are used in the educational process of Kharkiv National University of Radio Electronics, in particular, in the discipline "System Software" for applicants for the first (bachelor's) level of higher education in the educational and professional program "Computer Engineering" (act of 14.11.2023).

The materials of the dissertation are fully presented in 14 publications, including 7 articles, including 6 articles in professional periodicals of Ukraine in technical sciences, of which 2 are category A (indexed in Scopus); 4 - category B, 1 article in other publications (India), 7 abstracts in the proceedings of international scientific conferences.

Keywords: information technology, discrete cosine transform, digital watermark, data distribution, wavelet transform, chaotic signal, signal-to-noise ratio, image keypoint, detector, descriptor, multi-otzu method, image processing, stochastic process,correlation processing, data model.

List of publications of the applicant

1. Бологова Н.М. Дослідження моделей та методів обробки зображень та шляхи вдосконалення технологій розпізнавання маркерів в системах доповненої реальності / Н.М. Бологова, І. В. Рубан // Сучасний стан наукових досліджень та технологій в промисловості. – 2019. – № 1 (7). – С. 25 –33 (Належить до категорії Б).

2. Ruban I. Method of sustainable detection of augmented reality markers by changing deconvolution / I. Ruban, N. Bolohova, V. Martovytskyi, V. Lebediev, N. Lukova-Chuiko // International Journal of Advanced Trends in Computer Science and Engineering. 2020. – № 9 (2). – P. 1113–1120.

3. Makoveichuk O. Development of a method for improving stability method of applying digital watermarks to digital images / O. Makoveichuk, I. Ruban, N. Bolohova, A. Kovalenko, V. Martovytskyi, T. Filimonchuk // Eastern-European Journal of Enterprise Technologies. 2021. – № 3 (2 (111)). – P. 45–56. (Належить до категорії А, входить до міжнародної наукометричної бази Scopus).

4. Ruban I. Digital image authentication model / I. Ruban, N. Bolohova, V. Martovytskyi, O Koptsev // Advanced Information Systems. 2021. – № 5 (1). – P. 113–117 (Належить до категорії Б).

5. Ruban I. Methodology for assessing the effectiveness of methods for embedding digital watermarks / I. Ruban, N. Bolohova, V. Martovytskyi, R. Yaroshevych // Advanced Information Systems. 2021. – № 5 (3). – P. 112–118 (Належить до категорії Б).

6. Martovytskyi V. Development of methods for generation of digital watermarks resistant to distortion / V. Martovytskyi, I. Ruban, N. Bolohova, O. Sievierinov, O. Zhurylo, O. Permiakov, A. Nosyk, D. Nepokrytov, I. Krylenko // Eastern-European Journal of Enterprise Technologies. 2021. – № 6 (2 (114)). – P. 103–116. (Належить до категорії А, входить до міжнародної наукометричної бази Scopus).

7. Ruban I. Information technology for confirming property rights to digital

images / I. Ruban, N. Bolohova, V. Martovytskyi // Advanced Information Systems. 2022.– № 6 (1). – P. 118–123 (Належить до категорії Б).

8. Ruban I. et al. Method of neural network recognition of ground-based air objects //2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – IEEE, 2018. – С. 589-592.

9. Бологова Н.М. Аналіз сучасного підходу обробки зображень для розпізнавання маркерів в системі доповненої реальності / Н.М. Бологова, І.В. Рубан, К.Р. Локотецька // Тези доповідей шостої міжнародної науково-практичної конференції «Проблеми інформатизації». 14 – 16 листопада 2018 р., Черкаси, Баку, Бельско-Бяла, Харків. – 2018. – С.36.

10. Bolohova N. Analysis of restoration methods for optical-electronic images lubricated at motion / N. Bolohova, Y. Kortiak // Тези доповідей шостої міжнародної науково-практичної конференції «Проблеми інформатизації». 13 – 15 листопада 2019 р., Черкаси, Харків, Баку, Бельско-Бяла. – 2019. – С.8.

11. Bolohova N. Analysis of the current status of additional reality technologies / N. Bolohova, Y. Kortyak, A. Liashova // Proceedings of Fourth International Scientific and Technical Conference on COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. – Kharkiv, April 22-23, 2020. – P.12–13.

12. Bolohova N. Method for evaluating the effectiveness of methods for embedding digital watermarks / N. Bolohova, V. Martovytskyi, V. Diachenko, O. Kolomiitsev, V. Fedorchenko // Матеріали XX міжнародної науково-практичної конференції «Інформаційні технології і безпека». Київ. – 2020. С. 75–83.

13. Пересада Р.А. Аналіз методів підвищення стійкості водяних знаків у цифрових зображеннях / Р.А. Пересада, Н.М. Бологова // Тези доповідей восьмої міжнародної науково-технічної конференції «Проблеми інформатизації». 26 – 27 листопада 2020 р., . Черкаси, Харків, Баку, Бельсько-Бяла. – 2020. – С. 53.

14. Бологова Н.М. Модель автентифікації цифрового зображення / Н.М.

Бологова // Тези доповідей десятої міжнародної науково-практичної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління». 8 – 9 квітня 2021р., – Баку, Харків, Жиліна. – С. 41.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ЦВЗ – цифровий водяний знак

DCT – дискретне косинусне перетворення, (англ. Discrete Cosine Transform)

DWT – дискретне вейвлет-перетворення

LSB – найменший значущий біт

KLT – перетворення Кархунена-Лоева

САПР – система автоматизованого проектування

GA – генетичний алгоритм

AC – змінний струм (анг.alternating current)

DC – постійний струм (анг.direct current)

JPEG – тип формату зображення (англ. joint photographic expert group)

PRNU – нерівномірність фотографічної реакції зображення (англ. photo-response non-uniformity)

RPoW – алгоритм захисту розподілених систем від зловживань (англ. Reusable Proof Of Work)

ВСТУП

Актуальність теми дослідження.

За останні роки спостерігається значне збільшення трафіку через різні мережі та канали. Розвиток нових технологій, значне зростання обсягів даних і тотальне споживання контенту в цифровому середовищі змінюють екосистему сучасних медіа. Проте виникли питання щодо інформаційної безпеки, які привернули велику увагу. Інтернет це вільна зона де легко можна відкрити та зкопіювати та тиражувати будь-яку відкриту інформацію, навіть не замислюючись що даний цифорвий контент має авторів, які є правовлансиками

Майже до всіх дописів в інтернеті додається візуальний матеріал. Але, на превеликий жаль, розміщені в мережі ілюстрації, фотографії використовуються без ліцензій та відома самих авторів, тому виникла потенційна можливість незаконного використання цифрових зображень.

Щоб підтвердити аналіз цього напрямку, предоставляємо дані про ступінь порушення авторських прав на зображення, Copytrack регулярно досліджує, як, де і якою мірою вони використовуються незаконно. Звіт Copytrack про глобальні порушення за 2019 рік складається зі статистичного аналізу понад 12 000 профілів користувачів Copytrack. Незаконне використання цифрових зображень було розслідувано на основі всіх пошукових запитів, визнаних незаконними власниками індивідуальних облікових записів, а також даних власників вебсайтів, що базуються на інформації, зібраній внутрішніми пошуковими роботами. Відсоткові значення, які зазначені в цьому звіті, стосуються кількості потенційних порушень авторських прав, оброблених Copytrack за період з грудня 2017 року до грудня 2018 року.

Згідно з наведеним звітом [15], щодня крадеться понад 2,5 мільярда зображень. Ці порушення ліцензії можуть призвести до щоденних збитків до

532,5 мільярдів євро. Отже, право власності на авторські права є важливим аспектом інформаційної безпеки [1].

Цифрові зображення захищені законом про авторське право, як і будь-які інші оригінальні роботи. Але порядок державної реєстрації авторського права на зображення, визначений у Законах України, має ряд недоліків, таких як тривалий процес перевірки авторства, відсутність предметної перевірки, складність доказу, висока вартість, централізоване зберігання та інші. Саме тому актуальним є розробка новітніх технологій підтвердження авторства на цифрові зображення, які в свою чергу дозволять удосконалити та покращити сам процес захисту авторського права на цифрові зображення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана відповідно до плану науково-дослідних робіт Харківського національного університету радіоелектроніки в рамках держбюджетної НДР «Дослідження сучасних методів криптографічного захисту для застосування у постквантовий період» (№ ДР 0120U100109), затверджених Міністерством освіті і науки України. Автор був одним із виконавців робіт за даними темами.

Мета та задачі дослідження. Виникла потенційна можливість незаконного використання цифрових зображень, тому в дисертаційній роботі визначено мету, завдання.

Метою дисертаційної роботи є розробка інформаційної технології автентифікації цифрових зображень, яка використовує сучасні тенденції в області цифрових водяних знаків та блокчейну для створення нової децентралізованої технології підтвердження права власності на цифрові зображення

Для досягнення поставленої мети необхідно вирішити такі завдання:

- проаналізувати стан проблеми й особливості задач забезпечення авторського права та підтвердження автентичності цифрових зображень;

- розглянути методи нанесення цифрових водяних знаків на зображення й провести їх порівняльний аналіз;

- розглянути критерії оцінки ефективності методів нанесення цифрових водяних знаків;

- запропонувати комплексний критерій оцінки ефективності методів нанесення цифрових водяних знаків;

- розробити модель автентифікації цифрових зображень, що дозволить реалізувати ефективний спосіб захисту авторських прав на цифрові зображення;

- розробити функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків у зображення;

- розробити методи генерації стійкого до спотворень цифрового водяного знаку на основі хаотичних карт;

- розробити інформаційну технологію підтвердження права власності на цифрові зображення.

Об’єкт дослідження – процес підтвердження права власності на цифрові зображення.

Предмет дослідження – методи, модель та інформаційна технологія для забезпечення ефективного підтвердження права власності на цифрові зображення.

Методи дослідження – системний аналіз; процесний підхід – для вивчення процесів, які відбуваються при забезпеченні авторського права на твір; моделювання; теорія множин – для опису моделі автентифікації цифрових зображень; стеганографічні методи – для реалізації приховування самого факту використання цифрового підпису зображення, що забезпечує процес підтвердження права власності.

1. Вперше запропоновано комплексний критерій оцінки ефективності методів вбудови цифрових водяних знаків на зображення, який побудований з урахуванням ключових характеристик та визначенням вагових коефіцієнтів, та дозволяє провести комплексну оцінку ефективності методу нанесення цифрових водяних знаків.

2. Вдосконалено метод надійної перевірки справжності цифрового

зображення з високим ступенем захисту. Надійність досягається за рахунок того, що ЦВЗ ховається не в усьому зображенні, а в його фрагменті, який найбільше підходить для приховування зображення, а також застосування як ЦВЗ завадових кодів.

3. Вдосконалено метод підвищення стійкості стегосистеми за рахунок врахування ключових показників. Описаний у роботі метод псевдоголографічного кодування цифрових водяних знаків є ефективним для протидії усім типам атак, що розглядалися, окрім повороту зображення.

4. Отримали подальшого розвитку методи генерації ЦВЗ для цифрових зображень, а саме розроблено методи генерації ЦВЗ на основі хаотичних карт та додаткової фільтрації цифрового водяного знаку. Описані у роботі методи є ефективними для забезпечення стійкості ЦВЗ до локальних спотворень. Як показали дослідження, при 60 % спотворення зображення можливо відновити 90 % ЦВЗ.

5. Удосконалено інформаційну технологію підтвердження права власності на цифрові зображення, що основується на технології блокчейн та цифрових водяних знаках для забезпечення надійної гарантії встановлення авторських прав.

У дисертаційній роботі проведено аналіз сучасного стану проблеми і особливості задач забезпечення авторського права та підтвердження автентичності цифрових зображень. Проаналізовано методи нанесення цифрових водяних знаків на зображення та представлено сучасні підходи до їх реалізації.

Розроблено функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення, яка основана на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку. Описаний у роботі метод псевдоголографічного кодування цифрових водяних знаків є ефективним для протидії усім типам атак, що розглядалися, окрім повороту зображення. Проведення комплексної оцінки методики підвищення стійкості методу вбудови цифрового водяного

знаку на основі вейвлет-перетворення показало, що її використання на 20 % покращує стійкість до різних типів атак.

В роботі представлено показник оцінки стійкості методів нанесення цифрових водяних знаків, який враховує всі типи атак і дозволяє провести комплексну оцінку стійкості методу вбудови цифрових водяних знаків.

Проведено експериментальне дослідження щодо запропонованої методики. Найбільш ефективною ця методика є при втраті частини зображення. При попередній фільтрації цифрового водяного знаку найбільш ефективним є третій метод фільтрації. Цей метод і представляє собою усереднення по клітинці і подальшу бінаризацію. Для оцінки кута повороту знаходиться матриця афінного перетворення, що отримується по узгодженому набору відповідних ORB-дескрипторів. Використання цього методу дозволяє безпомилково виділяти цифровий водяний знак для всього діапазону кутів, що досліджувалися.

Проведено аналіз хаотичних карт на предмет забезпечення стійкості ЦВЗ. Аналіз показав, що використання хаотичних карт для перемішування біт пікселів або самих пікселів на зображенні можуть забезпечити захищеність та стійкість до спотворень. Розрахунки коефіцієнта кореляції сусідніх пікселів при використанні хаотичних карт свідчать про ефективність їх використання.

Розроблені методи генерації ЦВЗ на основі хаотичних карт та додаткової фільтрації цифрового водяного знаку. Описані у роботі методи є ефективними для забезпечення стійкості ЦВЗ до локальних спотворень. Як показали дослідження, при 60 % спотворення зображення можливо відновити 90 % ЦВЗ.

Проведено експериментальне дослідження щодо запропонованих методів. Гістограми ЦВЗ показали, що обидва методи забезпечують генерацію ЦВЗ випадкової незрозумілої форми. Але метод заснований на комбінації карт кота Арнольда та карт Генона має помітні піки, на відміну від метода, який заснований на перемішуванні пікселів та їх біт тільки за

допомогою карт кота Арнольда. Це свідчить про те, що метод заснований тільки на картах кота Арнольда має більш хаотичний характер. Про це також свідчить і значення коефіцієнта кореляції між сусідніми пікселями, який наближається до 0 і дорівнює 0.0109 для кольорових ЦВЗ та 0.030 для чорно-білих зображень.

Враховуючи загальнодоступність мережі інтернет і постійне зростання випадків порушення авторського права на цифровий контент, сучасні технології, що використовуються для захисту авторських прав, мають бути вдосконалені.

Технологія блокчейн володіє такими характеристиками, як децентралізація, захист від підробки та шифрування, розширюваності та гнучкості, що дозволяє ефективно вирішити питання реєстрації та підтвердження цифрового авторського права, вона відіграє значну роль у захисті прав та інтересів авторів.

У роботі запропонована інформаційна технологія підтвердження права власності на цифрові зображення, яка використовує цифрові водяні знаки, блокчейн, хеш-функції для зображення і IPFS для створення нової децентралізованої технології підтвердження права власності у цифрову епоху інтернету.

Що стосується типів файлів, згадується лише управління авторськими правами на цифрові зображення. У майбутньому технологію можна буде розширити на аудіо, відео та інші типи мультимедійних файлів, щоб сформувати єдину систему для підтвердження права власності на будь-який цифровий контент.

В дисертаційній роботі розв’язано актуальне науково-практичне завдання розробки інформаційної технології підтвердження права власності на цифрові зображення, яка використовує сучасні тенденції в області цифрових водяних знаків та блокчейну для створення нової децентралізованої технології підтвердження права власності цифрових зображень.

Практичне значення отриманих результатів полягає в такому:

- розроблено функціональний алгоритм вбудови цифрових водяних знаків в цифрові зображення, основані на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку, що дозволяє протидіяти типам атак, окрім повороту зображення;

- розроблено алгоритм надійної перевірки справжності цифрового зображення з високим ступенем захисту, що дозволяє сховати ЦВЗ в його фрагменті;

- удосконалено інформаційну технологію підтвердження права власності на цифрові зображення, що основується на технології блокчейн та цифрових водяних знаках для забезпечення надійної гарантії встановлення авторських прав.

Отриманий в роботі метод надійної перевірки справжності цифрового зображення з високим ступенем захисту від спотворення та підробки, був підтверджений результатами проведених випробувань, які доказали стійкість даної конструкції до геометричних і не геометричних атак (ТОВ «ОБОРОННІ ТЕХНОЛОГІЇ», м.Київ), про що свідчить акт від 26.02.2023. Також результати дисертаційного дослідження використані в освітньому процесі Харківського національного університету радіоелектроніки, зокрема, у навчальній дисципліні «Системне програмне забезпечення» для здобувачів першого (бакалаврського) рівня вищої освіти за освітньо-професійною програмою «Комп’ютерна інженерія» (акт від 14.11.2023.)

В [1] – запропонована модель надійної перевірки справжності цифрового зображення з високим ступенем захисту. Надійність досягається за рахунок того, що ЦВЗ ховається не в усьому зображенні, а в його фрагменті, який найбільше підходить для приховування зображення, а також застосування як ЦВЗ завадових кодів; в [2] – обґрунтовано визначення шляхів удосконалення методів обробки зображень для застосування в технологіях, які забезпечують технічну підтримку при захисті авторських прав на цифрові зображення; в [3] – запропоновано метод боротьби з

локальним згладжуванням у цифрових зображеннях, що дає змогу підвищити стійкість методів вбудови цифрових водяних знаків у зображення; в [4] – розроблена функціональна модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків у цифрові зображення, основана на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знака; в [5] – визначено параметри для формування розрахункового показника для оцінки ефективності методів нанесення цифрових водяних знаків на зображення, що дає змогу комплексного порівняння роботи декількох методів нанесення ЦВЗ; в [6] – запропоновано метод генерації ЦВЗ для цифрових зображень, а саме розроблено методи генерації ЦВЗ на основі карт кота Арнольда та додатковій фільтрації цифрового водяного знака; в [7] – представлено удосконалену інформаційну технологію підтвердження права власності на цифрові зображення для забезпечення надійної гарантії встановлення авторських прав.

Апробація результатів дисертації.

Основні положення дисертаційної роботи представлено на таких конференціях:

- на IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT) (Kyiv, 2018) [8] ;
- на 6-й Міжнародній науково-технічній конференції «Проблеми Інформатизації» (Харків, 2018) [9];
- на 7-й Міжнародній науково-технічній конференції «Проблеми Інформатизації» (Харків, 2019) [10];
- на 4-h International Scientific and Technical Conference on COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES (Kharkiv, 2020) [11];
- на XX-й Міжнародній науково-практичній конференції «ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ І БЕЗПЕКА» (Київ, 2020) [12];
- на 8-й Міжнародній науково-технічній конференції «Проблеми Інформатизації» (Черкаси, Харків, Баку, Бельсько-Бяла, 2020) [13];
- на 11-й Міжнародній науково-технічній конференції «Сучасні

напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (Баку, Харків, Київ, Жиліна, 2021) [14].

Публікації.

За результатами дослідження опубліковано 14 наукових праць, а саме: 7 наукових статей, серед яких 6 – у наукових фахових періодичних виданнях України з технічних наук, з яких 2 – категорії А (проіндексовано у міжнародній науковометричній базі Scopus); 1 стаття в періодичному виданні інших держав (Індія); 7 тез доповідей у матеріалах наукових міжнародних конференцій.

Структура й обсяг роботи.

Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації складає 217 сторінки, що містять 165 сторінки основного тексту, анотація на 17 сторінках, 91 рисунок, 3 таблиці, список використаних джерел із 125 найменувань на 15 сторінках, 5 додатків на 34 сторінках.

1 АНАЛІЗ СУЧАСНОГО СТАНУ У СФЕРІ ЗАХИСТУ АВТОРСЬКИХ ПРАВ НА ЦИФРОВИЙ КОНТЕНТ

1.1 Технологія блокчейн для захисту авторських прав

Використання сучасних методів обробки цифрових зображень дозволяє людині отримати матеріал порушуючи права власності, тому що технології отримання зображення не забезпеченні інструментами, які підтверджують власність цього зображення до конкретного автора чи користувача, в системних настройках пристроїв є відповідні позиції, де записується автор, але використовуючи тривіальні підходи в операційній системі можна змінити автора і використовувати, як своє.

На даний час це питання є ключовим, актуальним і потребує розроблення підходів та інформаційних технологій забезпечуючи механізми автентифікації зображень стійких до зовнішнього впливу і виключення можливостей модифікації.

Ступінь порушення авторських прав на зображення, Copytrack регулярно досліджує – як, де і якою мірою вони використовуються незаконно. Звіт Copytrack про глобальні порушення за 2019 рік складається зі статистичного аналізу понад 12 000 профілів користувачів Copytrack. Згідно з наведеним звітом [15], щодня крадеться понад 2,5 мільярда зображень. Ці порушення ліцензії можуть призвести до щоденних збитків до 532,5 мільярдів євро, представлено на рисунку 1.1.

Рисунок 1.1 – Статистика порушення авторських прав під час використання зображення за континентами [15]

Поточна ситуація в сучасному світі, зокрема інтелектуальної власності та інших сфер людської діяльності, характеризується одним загальним аспектом – цифровізацією [16]. На думку низки фахівців, цифровізація має забезпечити підвищення ефективності управління функціональними процесами, а також надати нові, раніше не використані можливості [17,18].

Сучасні технології дають змогу швидко та якісно підробляти різні документи, що засвідчують особу. Для підтвердження їхньої автентичності деякі організації використовують онлайн-верифікацію, де користувачу потрібно відсканувати документ або ввести кодову послідовність символів. Якщо всі дані зберігаються в хмарі, це може бути досить витратно. При використанні блокчейна немає необхідності створювати свою систему ідентифікації: для зберігання ідентифікаційних даних можна просто використовувати публічний блокчейн Ethereum, а перевірити їхню достовірність зможе будь-який учасник мережі в будь-який момент часу.

Проблема полягає в тому, що 85 % зображень, розміщених в інтернеті, використовуються без згоди й отримання прав на їх використання у власника фотографій. Для багатьох людей можливість використання розміщених у мережі матеріалів без дозволу автора є звичним явищем.

У міру того, як попит на зображення неухильно зростає, фотографи втрачають потенційний дохід від використання свого матеріалу.

Способи вирішення цієї проблеми, які існували раніше, були малоефективні. Один із найпоширеніших методів запобігання крадіжці зображень – водяні знаки, інший – відстеження пікселів.

Використання стеганографії в галузі захисту мультимедійної інформації має великий пріоритет. Одним із напрямів стеганографії є цифрове маркування, що здійснює непомітне вбудовування в об’єкт захисту невидимої людському оку цифрової мітки – цифрового водяного знака. Наявність вбудованого в об'єкт захисту ЦВЗ дає змогу однозначно визначити автора документа, це стримує потенційного зловмисника від незаконного

поширення мультимедійної інформації. Однак, сьогодні існує досить багато способів, якими зловмисники можуть скористатися для видалення вбудованого в графічний файл водяного знака, щоб унеможливити визначення джерела витоку інформації. Прикладами таких шкідливих впливів є зашумлення, фільтрація, зміна розміру та яскравості.

Застосовуючи ці атаки, зловмисник може значно ускладнити процес відстеження незаконного копіювання інформаційних ресурсів. У зв'язку з глобальним розповсюдженням мережі інтернет, більшої поширеності набув формат JPEG, що дає змогу здійснювати ефективне стиснення зображень, не спричиняючи сильних видимих спотворень. Використовуючи JPEG компресію, зловмисники здатні знищити вбудований у зображення водяний знак, зберігши при цьому комерційну якість зображення. Нині існує більш ефективний формат стиснення JPEG2000, але він не набув широкого розповсюдження в мережі інтернет, у той час як JPEG зберігає позицію лідера. Отже, завдання розроблення та дослідження методів цифрового маркування нерухомих зображень, стійких до компресії JPEG та інших шкідливих впливів є актуальним.

Вбудовування ЦВЗ на даний момент – один із найефективніших методів захисту зображень від незаконного розповсюдження. Цифрове маркування налічує велику кількість алгоритмів, що володіють різним ступенем ефективності [19]. Вбудовування цифрових водяних знаків є одним із методів цифрової стеганографії. Цей напрям є ефективним для вирішення завдань щодо запобігання незаконному копіюванню та модифікації мультимедійної інформації, захисту авторських прав. Його можна розглядати як найкращий варіант запобігання крадіжці зображення, але це не зупинить нове покоління хакерів. Технологія блокчейн сприяє створенню децентралізованого реєстру авторських прав на фотографії, підкріпленого смарт-контрактами.

Так, технології, що називаються узагальненим терміном блокчейн, надають можливість прямого передання прав власності іншій особі без

залучення додаткових зовнішніх гарантів з одночасним контролем історії транзакцій і захисту їхньої цілісності. При цьому одиницею обробки даних у «блокчейні» є токен, який можна розглядати як універсальний описувач прав власності [20]. Таким чином, токен – цифровий актив, що підтверджує право володіння, користування і розпорядження якимось майном або послугою. Функція токена – це надання права суб'єкту (своєрідна ліцензія) на отримання якихось заздалегідь визначених благ або можливість авансом оплатити майбутні товари та послуги [21]. Прикладами токенів, реалізованих у вигляді окремих носіїв з фіксованим або змінним номіналом, можуть бути транспортний квиток, виконаний на машинозчитуваному носії, подарунковий сертифікат або страховий поліс, медична картка пацієнта [22].

Найбільш загальними властивостями токена є:

- вказівка інформаційної системи, у межах якої функціонує токен і, як наслідок, у межах якої він визнається як цінність;
- асоціація з власником токена у вигляді прямої вказівки ідентифікаційних даних власника або за правом володіння носієм токена;
- наявність порядку обміну права, що описується токеном, на товар або послугу, наявність порядку переуступки прав;
- строк дії токена;
- відсутність додаткових умов або механізмів придбання товару або послуги.

Аутентифікація – це процес, під час якого на підставі пароля, ключа або будь-якої іншої інформації користувач підтверджує, що є тим, за кого себе видає.

Недосконаліть застосовуваних стандартних «багаторазових» паролів і, як наслідок, високий рівень вразливості в системі безпеки в процесі роботи на сторонньому обладнанні послужили поштовхом до розвитку ринку автентифікації та створення апаратних генераторів «одноразових паролів». В основі такої методики з використанням багатофакторної автентифікації закладено застосування персональних апаратних пристроїв – токенів, які

підтримують кілька методів автентифікації і є своєрідним ключем для доступу до інформаційних активів. Це може бути електронний підпис, біометричні дані, криптографічний ключ. Токени доволі універсальні: їх можна використовувати як замість пароля, так і разом із ним, крім того, вони дають змогу генерувати та зберігати ключі шифрування, забезпечуючи тим самим сувору автентифікацію.

Спробуємо розглянути кілька видів токенів з точки зору як переваг, так і недоліків.

1. USB-токени. Серед переваг – мобільність (токен можна використовувати на будь-якому комп'ютері, де є USB-порт). Можливість підтримки великої кількості додатків IT-безпеки. Очевидна належність токена користувачеві. Недоліком є необхідність встановлення ПЗ користувачеві.

2. Смарт-картки. Безсумнівною перевагою цього типу токенів (ідентифікаторів) є високий рівень безпеки, невеликі габарити, підтримка великої кількості застосувань і належність користувачеві. До недоліків слід віднести вимогу встановлення ПЗ користувачеві та низьку мобільність (потрібен зчитувальний пристрій). Слід зауважити, що в цьому випадку переваг більше, ніж недоліків.

3. USB-токени з вбудованим чипом. Переваги: високий рівень безпеки, мобільність, підтримка великої кількості застосунків і очевидна належність користувачеві. На тлі важливих переваг один незначний недолік, характерний для всіх вищерозглянутих типів токенів – користувачу потрібно встановити необхідне ПЗ.

4. Програмні токени. Цьому типу токенів не потрібен апаратний пристрій. Однак кількість недоліків зростає . Серед них слабка захищеність секретного ключа, обмежене коло підтримуваних додатків, та також необхідність наявності сервера аутентифікації [23].

Сучасне суспільство є свідком якісної трансформації інформаційних комп'ютерних мереж, де система ідентифікації та автентифікації є опорною

точкою для запобігання несанкціонованому доступу до інформаційних ресурсів, що охороняються. Зрозуміло, що простих і швидких вирішень усіх питань і проблем, що виникають у процесі перевірки автентичності, не існує. Ефективність і якість інструментів ідентифікації та автентифікації мають бути належним чином пов'язані з важливістю інформаційних активів. При цьому не слід забувати, що підвищення ступеня безпеки, у свою чергу, супроводжується подорожчанням. Тому вирішувати завдання ідентифікації та автентифікації потрібно комплексно, установивши розумний баланс між ефективністю, вартістю, зручністю користування та адміністративним управлінням засобів забезпечення систем безпеки.

Технологія блокчейн – це вдосконалений механізм бази даних, який дає можливість організувати відкритий обмін інформацією в межах мережі. База даних блокчейна зберігає дані в блоках, пов'язаних між собою в ланцюжок. Дані є хронологічно послідовними, оскільки не можна видаляти або змінювати ланцюжок без консенсусу з боку мережі. У результаті слід використовувати технологію блокчейн для створення незмінного або безстрокового реєстру для відстеження замовлень, платежів, рахунків та інших транзакцій. Система має вбудовані механізми, які запобігають несанкціонованому введенню транзакцій і створюють узгодженість у загальному поданні цих транзакцій [24].

Блокчейн передбачає подібні проблеми шляхом створення децентралізованої, захищеної від несанкціонованого доступу системи для запису операцій. У разі угоди з нерухомістю блокчейн створює єдиний реєстр для покупця і продавця. Усі транзакції мають бути схвалені обома сторонами й автоматично оновлюватися в їхніх реєстрах у режимі реального часу. Будь-яка невідповідність в історії транзакцій відобразиться в усьому реєстрі. Ці властивості блокчейн зробили технологію популярною в різних секторах. Наприклад, її використовували під час створення цифрової валюти Bitcoin.

Блокчейн – це універсальний інструмент для побудови різних баз

даних.

Переваги блокчейну:

1. Децентралізація. Відсутній головний сервер зберігання даних. Усі записи зберігаються в кожного учасника системи.

2. Повна прозорість. Будь-який учасник може відстежити всі транзакції, що проходили в системі.

3. Конфіденційність. Усі дані зберігаються в зашифрованому вигляді. Користувач може відстежити всі транзакції, але не може ідентифікувати одержувача або відправника інформації, якщо він не знає номера гаманця. Для проведення операцій потрібен унікальний ключ доступу.

4. Надійність. Будь-яка спроба внесення несанкціонованих змін буде відхилена через невідповідність попереднім копіям. Для легальної зміни даних потрібен спеціальний унікальний код, виданий і підтверджений системою.

5. Компроміс. Дані, які додаються в систему, перевіряються іншими учасниками, тобто здійснюється перерахування хешу.

Дозволяючи цифровій інформації поширюватися, але не копіюватися, технологія блокчейн створила основу нового виду інтернету. Технологію блокчейн спочатку розробили для цифрової валюти, біткоїна, але наразі технічне співтовариство шукає інші потенційні варіанти використання цієї технології.

Застосування шифрування гарантує, що користувачі можуть змінювати тільки ті частини ланцюжка блоків, якими вони «володіють», тобто у них є закриті ключі, без яких запис у файл неможливий. Крім того, шифрування гарантує синхронізацію копій розподіленого ланцюжка блоків у всіх користувачів.

У технологію блокчейн, від початку, закладено безпеку на рівні бази даних. Концепцію ланцюжків блоків запропонував у 2008 р. Сатоші Накамото [25.]. Уперше її було реалізвано у 2009 р. як компонент цифрової валюти – біткоїна, де блокчейн є головним спільним реєстором для всіх

операцій з біткоїнами. Завдяки технології блокчейну біткоїн став першою цифровою валютою, яка вирішує проблему подвійних витрат (на відміну від фізичних монет або жетонів, електронні файли можуть дублюватися й витрачатися двічі) без використання будь-якого авторитетного органу або центрального сервера.

Безпека в технології блокчейн забезпечується децентралізованим сервером, що проставляє мітки часу й однорангові мережеві з'єднання. Таким чином, формується база даних, яка управляється автономно, без єдиного центру. Це робить ланцюжки блоків дуже зручними для реєстрації подій (наприклад, внесення медичних записів) і операцій з даними, управління ідентифікацією та підтвердження автентичності джерела.

Блокчейн використовується не тільки для фінансових транзакцій. Завдяки прозорому і безпечному принципу роботи, технологія практично універсальна для будь-яких галузей:

- авторських прав;
- криптовалюти;
- кібербезпеки;
- бухгалтерського обліку;
- документообігу;
- логістики;
- енергетики;
- освіти;
- охорони здоров'я.

Способів підтвердження авторських прав на творчі напрацювання не так багато. А ті, що є, не завжди можна назвати надійними. Особливо якщо йдеться про цифровий об'єкт – фото, рисунок, векторне зображення, відео- чи аудіозапис тощо. Блокчейн дає змогу раз і назавжди закріпити за собою авторське право на будь-який інтелектуальний твір, перетворюючи його на NFT.

NFT – це криптографічний токен, розміщений у блокчейні, який може

представляти будь-яки цифровий актив. Невзаємозамінність NFT означає, що ці цифрові активи представляють право власності на унікальні предмети, такі як: твори мистецтва, внутрішньоігрові предмети, колекційні картки, віртуальна нерухомість та інші цифрові товари.

Ставши невзаємозамінним токеном, творча робота є абсолютно унікальним активом із цифровим сертифікатом відповідності. Завдяки цьому свої NFT можна продавати на відповідних маркетплейсах і заробляти на цьому.

Прикладом застосування в Україні блокчейну є український банк, який запустив пілотний проект електронних грошей на блокчейні. ТАСКОМБАНК та фінтех-компанія Bitt запускають пілотний проект електронних грошей на блокчейні Stellar для аналізу потенціалу використання блокчейн-технології при випуску е-гривні. Проект реалізується під наглядом Національного банку та за підтримки Міністерства цифрової трансформації. У рамках пілотного проекту об’єднана команда досліджуватиме використання електронних грошей для програмованих виплат заробітної плати співробітникам ДП «Дія», проведення p2p платежів та розрахунків з мерчантами. Проект побудовано відповідно до чинного законодавства України про електронні гроші [26]. Очікується, що закон про платіжні послуги, який регулюватиме обіг цифрових грошей та майбутню емісію цифрової валюти під егідою Національного Банку, набув чинності у 2022 році [27].

Іншим прикладом законного використання блокчейну є проект закону №3637 «Про віртуальні активи» [28], який розроблено Мінцифри, депутатським об’єднанням Blockchain4Ukraine та БАУ. Міністерство цифрової трансформації працювало над законопроектом про внесення змін до Податкового кодексу, які необхідні для легалізації ринку віртуальних активів. Зазначається, що міністерство також підписало меморандум з Асоціацією «Блокчейн Україна», відповідно до якого вона долучилосься до роботи над документом.

Меморандум передбачає співпрацю в наступних питаннях погодження

з міжнародними стандартами та рекомендаціями щодо запобігання відмиванню коштів і фінансуванню тероризму стосовно віртуальних активів; розробки державної стратегії стимулювання розвитку сфери та створення інвестиційних умов для ведення бізнесу в Україні; створення концепції та умов транспарентності державних процедур і розвитку інструментів суспільного моніторингу; створення концепції впровадження технології блокчейн у роботу державних реєстрів та інституцій України. [29]. На даний час законопроект відправлено на доопрацювання.

1.2 Цифрова фотографія

Фотографія існує з початку 1800-х років, коли Джозеф Нікофор Ньєпс зробив перше фотографічне зображення за допомогою так званої камери-обскури [30]. Цей пристрій мав на одному кінці крихітний отвір, який фокусував світло, що потрапляло на екран, який у той час використовувався для перегляду, малювання та розваг. Джозеф Ньєпс зробив першу фотографію, розмістивши гравюру на металевій пластині, покритій світлочутливою хімічною речовиною, а потім виставив пластину на світло.

Для того, щоб повернути зображення до початкового, позитивного стану, негатив необхідно збільшити і спроектувати на інший світлочутливий папір. На цьому папері проявляють і виготовляють відбиток.

Наприкінці 20-го століття цифрові фотоапарати почали витісняти традиційні плівкові. Приблизно в 2003 році багато виробників таких пристроїв повідомили, що продажі цифрових фотокамер перевищили продажі плівкових [31]. Основна функція цифрової камери полягає в перетворенні нескінченного діапазону рівнів інтенсивності світла в цифрове середовище, яке має обмежену кількість двійкових значень.

Ширококутні об’єктиви мають невеликий розмір і коротку фокусну відстань. Такі типи використовуються для охоплення якомога більшого діапазону сцени. Макрооб’єктиви довгі та мають більшу фокусну відстань.

Вони зазвичай використовуються для зйомки об’єктів, розташованих дуже близько до об’єктива, і допомагають створювати зображення, які перевищують натуральну величину. Телеоб'єктиви мають фокусну відстань, більшу за фактичну довжину об'єктива, тому використовуються для зйомки зображень із далеких відстаней.

Перш ніж сфокусоване світло буде записане, воно проходить через серію фільтрів, які готують його до перетворення в цифрову область. Артефакти згладжування можуть включати спотворення або артефакти, яких немає на оригінальному зображенні. Додатково до фільтра згладжування потрібен ще інфрачервоний (ІЧ) фільтр, оскільки цифрові датчики надзвичайно чутливі до ІЧ-світла [32]. Відфільтроване світло потрапляє на датчик зображення.

Датчик зображення є одним з найважливіших компонентів цифрової камери. Два основних типи датчиків – це датчик зображення із зарядженим зв'язком (Charged-Coupled Device (CCD)) і комплементарний метал-оксид-напівпровідник (Complimentary Metal-Oxide-Semiconductor (CMOS)). Хоча технології, що лежать в основі CCD і CMOS-чіпів, відрізняються, фундаментальна робота кожного з них однакова. Ці датчики, які містять багато фотонночутливих елементів, що називаються «пікселями», перетворюють рівні інтенсивності світла в електронну напругу. Однак піксель може розрізняти лише рівні інтенсивності світла, що робить його монохроматичним компонентом. Оскільки пікселі не є кольорочутливими елементами, для розрізнення різних частотних діапазонів світла використовується масив кольорових фільтрів (CFA).

CFA – це масив кольорових фільтрів, які розділяють світло за кольоровою частотою на кожен дискретний піксель, що монтується безпосередньо на датчик зображення. Існує багато різних типів масивів, але найчастіше використовується масив кольорових фільтрів

Цифрові зображення можна швидко копіювати, передавати та дублювати без втрати інформації та якості зображення. Цифрові копії, або

клони, можуть не відрізнятися від оригіналу. Ці файли можна надсилати в електронному вигляді на великі відстані за лічені секунди друзям.

1.3 Огляд методів автентифікації зображень

Формат файлу цифрового зображення можна вважати контейнером, у якому знаходиться інформація, що складається з медіаданих. У цьому підрозділі розглядається інформація про дані, які представляють власне вміст зображення. Аналіз яких у цілому допомагає визначити, чи відхиляється загальна структура зображення від нормальної роботи пристрою зйомки. Для того, щоб із файлом цифрового зображення можна робити різні маніпуляції, його потрібно відкрити, обробити й зберегти. Збережене зображення може мати невеликі відхилення від оригіналу, або зображення 1-го покоління. Модифікації можуть змінити випадковий розподіл числових значень в оригінальних зображеннях і ввести взаємозв'язки, яких немає в оригінальних, непідроблених зображеннях. Ці взаємозв'язки можна виявити за допомогою математики, а потім порівняти зі зразками з камери.

Термін «первинне зображення» використовується для позначення зображення, створеного в процесі зйомки, яке було оброблено лише за допомогою звичайних функцій цього пристрою [33]. Іншими словами, як камера обробляє двійкове представлення світла від CFA через обробку в камері, таку як баланс білого і гамма-корекція, до стиснення JPEG (якщо воно стискається), доки воно не буде збережене у вигляді файлу зображення на носії інформації.

Багато методів, розглянутих стосуються аспектів зображень у форматі JPEG, тому необхідно мати глибоке розуміння методу стиснення JPEG. Після опису стандарту стиснення JPEG будуть розглянуті різні методи аналізу зображень за глобальною структурою.

Стандарт був створений у 1991 році Об'єднаною групою фотографічних експертів для задоволення зростаючого попиту на

універсальний стандарт, який міг би підтримувати широкий спектр застосувань та обладнання від різних виробників [34]. Він також був створений для того, щоб допомогти вирішити проблему, пов'язану з тим, що обсяг пам'яті, необхідний для зберігання нестисненого зображення, може бути досить великим. Алгоритм стиснення JPEG можна налаштувати так, щоб забезпечити компроміс між розміром файлу та якістю зображення. Схема стиснення JPEG є одним з найпоширеніших стандартів стиснення з втратами. Оскільки стандарт стиснення JPEG широко використовується майже в кожній сучасній камері, коротке обговорення його етапів є дуже важливим для правильного розуміння аналізу, представленого в даному розділі.

Стандарт зображення JPEG підтримує глибину розрядності 8 або 12 біт для кожного кольорового каналу. Однак із моменту запровадження стандарту широко використовується 8-бітна модель. Ефективність стиснення JPEG досягається завдяки використанню дискретного косинусного перетворення (DCT) [35]. DCT не вносить жодних втрат у якість зображення, натомість переводить його з просторової області в частотну, де воно може бути більш ефективно закодоване.

Етапи кодування триканального кольорового зображення з використанням стандарту стиснення JPEG є наступними [34]:

1. Зображення перетворюється з кольорового простору RGB у кольоровий простір яскравості/колірності (YCbCr).

2. Зображення розбивається на блоки розміром 8x8 пікселів, що не перекриваються.

3. Значення в блоці перетворюються з цілих чисел без знаку (від 0 до 255) в цілі зі знаком (від –128 до 127).

4. Кожен блок перетворюється з просторової області на частотну за допомогою DCT-обробки.

5. Отримані значення квантуються.

6. Потім коефіцієнти DCT кодуються без втрат.

7. До результуючого потоку даних додається заголовок.

Крок 1, перетворення кольорового простору в (YCbCr) – це перший крок у процесі стиснення JPEG. Він розділяє зображення на один компонент яскравості та два компоненти кольоровості. Це бажано, оскільки людське око більш чутливе до інформації про яскравість, освітленість і має меншу просторову чутливість до зміни кольору, кольоровості [36]. Через цю особливість людського зору інформація для каналів кольоровості може бути значно зменшена без помітної втрати якості зображення. Канали кольоровості (CbCr), як правило, зменшуються вдвічі в порівнянні з каналом яскравості [37].

Крок 2, потім зображення розділяється на блоки 8x8 пікселів, що не перекриваються, для обробки.

Крок 3, отримані значення зсуваються із беззнакових цілих чисел [0, 255] до знакових [–128, 127].

Крок 4, кожен блок обробляється окремо за допомогою DCT і перетворюється з просторової області в частотну, яка складає спектр вхідного сигналу. Ділянки з повільними змінами, наприклад, однорідне небо, складаються з низькочастотної інформації.

Поняття частоти є важливим, оскільки стиснення JPEG має більш виражений вплив на високочастотну інформацію у вигляді втрати деталей. Результатом перетворення DCT є набір із 64 амплітуд на основі сигналу, які називаються коефіцієнтами DCT. У кольоровому зображенні кожен кольоровий шар обробляється окремо як незалежне зображення.

Крок 5, після виходу з DCT, кожне значення коефіцієнта з компонентів яскравості та кольоровості розділяється за допомогою 64-елементної таблиці квантування. Таблиці квантування, що використовуються для каналів кольоровості та яскравості, відрізняються. Менші значення в таблиці вказують на вищу якість зображення, а більші – на нижчу. Кожен елемент таблиці квантування може бути цілим числом від 1 до 255. Після квантування отримані значення округлюються до найближчого розміру кроку

квантування або найближчого цілого числа. Це є основною причиною втрати інформації в енкодерах на основі DCT і називається помилкою квантування. Ця помилка, яка відповідає за невелику зміну значення для кожного пікселя між вихідним зображенням і після його стиснення.

Крок 6, після квантування, ентропійне кодування без втрат використовується для подальшого стиснення зображення шляхом кодування коефіцієнтів на основі їхніх статистичних характеристик. Процес квантування створює багато нульових значень. Вони кодуються як рядки нульових прогонів, на відміну від шістнадцяткового значення «0», що повторюється багато разів.

Крок 7, заголовок JPEG поєднується з ентропійно закодованим потоком даних для створення файлу JPEG.

Процес декодування використовує ті ж кроки, але у зворотному порядку. Дані відновлюються з ентропійного кодування, потім квантовані DCT-коефіцієнти множаться на ту саму таблицю квантування, що використовувалася для квантування, щоб відновити деквантовані DCT-коефіцієнти, на цьому етапі генеруються додаткові похибки через округлення та усікання отриманих значень частоти.

Стиснення JPEG в середньому може ефективно зменшити розмір файлу до 1/10 його початкового розміру з дуже незначною втратою якості зображення. Якщо розмір зменшити ще більше, то відбудеться погіршення якості зображення у вигляді артефактів JPEG, які включають блочність, різкі кольорові переходи та облямівку навколо країв деталей. Стиснення JPEG – це алгоритм стиснення з втратами, що означає, що інформація, втрачена в процесі стиснення, не може бути відновлена.

Інтерполяційний аналіз. Хоча Галлахер [38] використовує другі похідні для виявлення періодичності в масштабованих зображеннях, цей метод може бути застосований для аналізу стиснення JPEG, щоб визначити чи було зображення JPEG стиснуте один раз чи більше одного разу. Сліди періодичності у вигляді повторюваних патернів у другій похідній указують

на те, що зображення, імовірніше, не є зображенням першого покоління.

Алгоритм виявлення інтерполяції працює, спочатку обчислюючи другу похідну кожного рядка матриці зображення. Галлахер зазначає, що стовпці також можуть бути використані, оскільки алгоритми інтерполяції зазвичай використовують значення в обох напрямках, як по рядках, так і по стовпцях, щоб досягти найбільш точного інтерпольованого значення. Потім абсолютні значення усереднюються по всіх рядках для обчислення середнього значення, й обчислюється дискретне перетворення Фур'є (DFT) для визначення частотних піків другої похідної сигналу.

Алгоритм, запропонований Галлахером, добре працює на нестиснених зображеннях, які були збережені у форматі JPEG.

Інтерполяція пікселів також може відбуватися при зміні розміру або повороті зображення. Попеску та Фарід пропонують методику ідентифікації інтерпольованих областей за допомогою алгоритму очікування/максимізації) [39]. Власне кажучи, алгоритм використовує ітераційний процес для оцінки невідомого параметра, у цьому конкретному випадку – методу інтерполяції, який використовується для масштабування або повороту зображення. Алгоритм використовується для визначення того, чи корелюють значення сусідніх пікселів між собою за допомогою набору періодичних вибірок. За результатами етапу максимізації математичного сподіванн. створюється карта ймовірностей, яка може бути використана для визначення того, чи було змінено розмір або повернуто зображення. Перетворення Фур'є обчислюється на карті ймовірностей, і будь-які закономірності, що з'являються при перетворенні, є ознакою інтерполяції. При використанні нестиснутих зображень частота хибних спрацьовувань становила менше 1% для висхідної дискретизації та поворотів більше ніж на 1 градус. Точність алгоритму падає з 99 %, коли дискретизація вниз перевищує 20 %. Алгоритм також добре працює за наявності гамма-корекції та при низькому співвідношенні сигнал/шум. Цей метод також добре працює із зображеннями, стиснутими у форматі JPEG, з невеликими недоліками. Розмір блоку JPEG втручається в

роботу алгоритму, коли частота дискретизації вниз становить 20 % або коли частота дискретизації вгору становить 60 %. Однак ці артефакти не впливають на виявлення обертання. Цей метод також може бути використаний для визначення того, чи були змінені розміри та повернуті невеликі складові частини зображення, щоб уписати їх у нове зображення) [39].

Пікселі майже всіх CMOS- і CCD-сенсорів чутливі лише до інтенсивності світла та не розрізняють різні довжини хвиль спектра. Наразі єдиним винятком є сенсор Foveon X3, який має можливість записувати інформацію про колір у кожному пікселі [40]. Щоб подолати це обмеження CMOS і CCD сенсорів, над ними розміщують масив кольорових фільтрів, які фільтрують світло за кольором. Таким чином, кожен піксель записує інформацію про інтенсивність світла лише для певного діапазону довжин хвиль, що залежить від кольору. Цей фільтр називається масивом кольорових фільтрів (CFA). Існує багато типів CFA, але найпоширенішим є CFA Bayer, зазвичай містить більше зелених фільтрів, ніж червоних і синіх. Вихідна інформація з датчика – це набір значень інтенсивності зеленого, червоного та синього кольорів, розподілених по одній матриці [41-43].

Аналіз коефіцієнтів DCT може виявити ознаки фальсифікації зображення у вигляді подвійного стиснення JPEG. Зазвичай, коли зображення піддається маніпуляціям, його спочатку завантажують у програму для редагування фотографій. Після внесення змін зображення перезаписується. У випадку зображення у форматі JPEG цей процес групує значення коефіцієнта DCT у числа, кратні розміру кроку квантування [44].

Аналіз коефіцієнтів DCT доступний лише для зображень, стиснутих у форматі JPEG. Дискретне косинусне перетворення перетворює зображення з просторової області в частотну. Це перетворення можна пояснити, якщо розглядати пряме DCT як частотний аналізатор, а зворотне DCT – як синтезатор частоти.

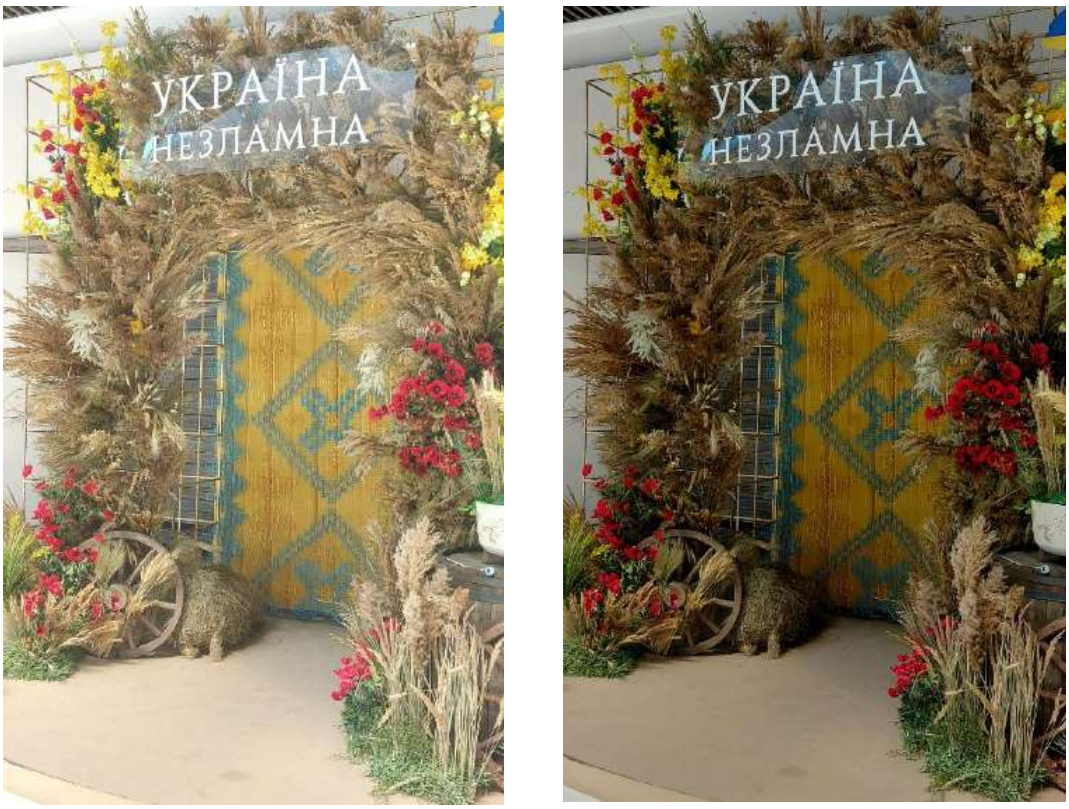
Стамм М. К. та ін. виявили слабке місце в DCT-аналізі, коли вони

маніпулювали коефіцієнтами DCT зображення JPEG під час декомпресії файлу зображення [45]. До нормованих коефіцієнтів DCT додається невелика кількість адитивного шуму, що приховує вплив помилки квантування. У результаті розподіл коефіцієнтів DCT у маніпульованому зображенні нагадує розподіл коефіцієнтів нестисненого зображення. Щоб протистояти цій антикриміналістичній атаці, дослідження високочастотних піддіапазонів зображення може визначити, чи була застосована вищезгадана атака на зображення [46].

Аналіз локальної структури зображення.

Хоча аналіз глобальної структури зображення може допомогти визначити, чи було змінено у великому масштабі, він не зможе встановити, де саме зображення було змінено.

Розглянемо зображення, зроблене в умовах неякісного освітлення. Зображення вважається засвітленим, оскільки значна частина деталей сцени втрачається в світлих частинах зображення. Щоб виправити це, виконується просте регулювання експозиції для підвищення загального рівня чіткості, що, у свою чергу, виявляє деталі, які раніше були приховані. Цей тип обробки не змінює зміст зображення, представлено на рисунку 1.2.



а) б)

Рисунок 1.2 – Нешкідливі зміни

Зловмисні маніпуляції можна визначити як застосування технологій з метою створення ілюзії або обману щодо подій на зображенні, представлено на рисунку 1.3.

Рисунок 1.3 – Зловмисна зміна

Виявлення зловмисних змін у вмісті зображення є важливою частиною автентифікації зображень. Одним із найпоширеніших методів є використання копіювання та вставки, коли інформація береться із зображення або окремої його частини і копіюється поверх наявного вмісту. Цей тип техніки можна використовувати двома способами. Перший – замінити вміст, який існував у сцені на момент зйомки зображення. Другий – додати в сцену вміст, якого не було на оригінальному зображенні. Таким чином створюється зв'язок, якого не існувало на момент зйомки. Ці типи технік можуть додавати або видаляти вміст зображення і не залишати візуально видимих слідів змін.

Мо Чен та ін. описують процес, у якому PRNU пристрою для отримання зображень порівнюється блок за блоком з PRNU підозрілої фотографії [47]. Основний принцип полягає в тому, що будь-які змінені області на підозрілому зображенні не будуть містити таку саму сигнатуру PRNU, що й зображення з тієї самої камери. Цей метод передбачає, що експерт має доступ до підозрюваної камери або до неманіпульованих зображень. Шаблон PRNU можна оцінити з підозрюваної камери, зробивши кілька розфокусованих зображень рівномірно освітленої сцени, наприклад, ясного неба. Надійний шаблон PRNU можна створити з 8 зображень, отриманих таким чином [48]. Якщо підозрювана камера недоступна, то рекомендується використовувати 50 зображень для створення сильної сигнатури PRNU [49]. У роботі [47] для пом'якшення вмісту сцени використовували вейвлет-фільтри, а отримані зображення усереднювали, щоб видалити залишки вмісту сцени та випадковий шум. Аналогічні кроки були виконані для підозрюваного зображення.

Дослідники зазначають, що помилково ідентифіковані пікселі, як правило, розташовувалися навколо області підробки та, імовірно, були позначені як такі через розмір блоку 128x128 у ковзному вікні. На тестових фотографіях також були помилково ідентифіковані пікселі на ділянках з високою частотою інформації. Також було визначено, що помилкова

ідентифікація підроблених ділянок була спричинена великими темними областями. PRNU залежить від кількості світла, що потрапляє на датчик, і природно пригнічується в таких областях [50].

Зміни в зображеннях JPEG можна виявити за допомогою помилок квантування та округлення, притаманних процесу стиснення JPEG. Зображення перетворюється з просторової області в частотну за допомогою дискретного косинусного перетворення (DCT). Потім таблиця квантування квантує отримані частотні коефіцієнти DCT.

Вейкі Ло та ін. запропонували метод, який дозволяє виявити сліди стиснення JPEG у нестисненому зображенні [51]. Згаданий метод працює шляхом перетворення підозрілого зображення в частотну область та аналізу отриманих коефіцієнтів змінної напруги. Якщо зображення було попередньо стиснене у форматі JPEG, то розподіл коефіцієнтів змінної напруги матиме періодичність, як пояснювалося раніше. Запропонована методика свідчить про точність 98,6 % для блоків 256x256 пікселів, до 95,08 % для блоків 8x8 пікселів. Хоча метод було застосовано лише до глобального зображення, він може бути використаний для визначення, чи будь-яка частина нестисненого зображення походить від попередньо стисненої фотографії у форматі JPEG.

Хані Фарід запропонував метод ідентифікації маніпульованих ділянок зображення шляхом виявлення наявності «привидів JPEG» [52].

Підроблені ділянки легко виявити, якщо взяти підозріле зображення, повторно стиснути його з послідовно різними значеннями якості JPEG і відняти кожне повторно стиснене зображення від початкового підозрілого. Будь-які ділянки, які були раніше змінені, призведуть до появи на зображенні JPEG-примари навколо певного значення якості JPEG, отриманого шляхом повторного стиснення підозрілого зображення.

Запропонована методика, однак, корисна лише в тому випадку, якщо область, якою маніпулюють, була взята із зображення, стисненого з нижчим коефіцієнтом якості, ніж зображення, про яке йде мова. Крім того, будь-яке зміщення в структурі решітки JPEG 8x8 перешкоджатиме появі JPEG-

примари. Цю проблему можна вирішити, зсунувши зображення по горизонталі та вертикалі на кожне з 64 можливих вирівнювань перед повторним стисненням зображення з різними параметрами якості.

Ідентифікація джерела зображення – це процес визначення походження зображення для ідентифікації пристрою, який створив його. Цей процес важливий для визначення того, чи мають два набори зображень схожі характеристики. Ідентифікація здійснюється шляхом виявлення характеристик, унікальних для окремої камери, сканера чи іншого пристрою, які присутні на зображенні. Найнадійніші з цих методів використовують недосконалості, які вносяться сенсором цифрової камери.

Характеристики, які демонструє нерівномірність фотографічного відгуку (PRNU), роблять цей компонент цифрового зображення унікальним і корисним інструментом для ідентифікації «відбитків пальців» цифрових датчиків [49] [53-56]. PRNU притаманний усім сенсорам візуалізації, що робить його універсальним ідентифікатором. PRNU містить велику кількість інформації, що робить його унікальним компонентом, специфічним для окремого сенсора. Сигнал присутній на всіх зображеннях і не залежить від налаштувань камери, вмісту сцени та оптики камери. Було показано, що він залишається стабільним з часом і в широкому діапазоні умов навколишнього середовища [55]. Також було показано, що він певною мірою витримує стиснення з втратами у форматі JPEG і зміни в процесі обробки зображень, такі як регулювання яскравості, кольору і гами [53].

Хоча PRNU є індивідуальним компонентом усіх цифрових датчиків зображення, на здатність витягувати сигнал впливає якість датчика, кількість світла, що взаємодіє з датчиком, і вміст сцени. Сенсори камер низької якості, наприклад, у мобільних телефонах і недорогих фотоапаратах, більш схильні до дефектів компонентів сенсора, ніж камери вищого класу.

Додатковим інструментом для ідентифікації джерела зображення є дефектні пікселі. Через велику кількість пікселів у датчику зображення ймовірність того, що різні камери мають дефектні пікселі в одному і тому ж

місці, дуже низька і зменшується лише зі збільшенням кількості дефектних пікселів. Існує п’ять різних типів дефектів пікселів [57]. Одним з найбільш помітних є дефект гарячої точки, який визначають як піксель, що має дуже високу вихідну напругу. Ці дефекти пікселів призводять до появи яскравих плям на вихідному зображенні. Через CFA вони мають вигляд яскравих ділянок червоних, зелених, синіх або білих плям. Іншим дефектом, який можна ідентифікувати, є мертвий піксель, такий, що більше не функціонує або має погану чутливість до світла. Цей тип дефекту має вигляд чорної плями на зображенні. Точковий дефект – це піксель, який відхиляється більш ніж на 6 % при освітленні сенсора до 70 %. Піксельна пастка призводить до часткової або повної втрати стовпчика, тому кластерний дефект визначається як скупчення точкових дефектів.

Герадтс З. Ж. та ін. пояснюють, що для найбільш точного визначення того, чи походять два зображення з одного джерела, необхідно виконати три умови [57]. По-перше, помилка через дефектні пікселі є випадковою і не спричинена дефектами виробничого процесу. По-друге, температура сенсора під час зйомки зображень була порівнянною. По-третє, дефектний піксель не залежить від інших пікселів. По-четверте, не представлене в [57], полягає в тому, що умови роботи камери (тобто налаштування, швидкість ISO) є порівнюваними з налаштуваннями підозрілого зображення. Оскільки матриці цифрових камер можуть містити мільйони пікселів, імовірність того, що дві камери мають дефектні пікселі за однією й тією ж адресою, починає зменшуватися зі збільшенням кількості дефектів, які можна ідентифікувати. Чим більше дефектів пікселів, які можна ідентифікувати, тим переконливішими стають докази того, що два зображення походять з одного джерела. Сучасні моделі камер можуть мати внутрішню обробку, яка виявляє й компенсує ці дефектні пікселі.

Ще одним недоліком цього підходу є те, що кількість видимих пікселів залежить від вмісту сцени, який може приховати або замаскувати наявність дефектних пікселів. Було проведено тест на встановлення залежності

кількості дефектних пікселів від температури. Під час дослідження протестовано камери в діапазоні температур від 0 до 40 градусів Цельсія. Виявлено, що зі зниженням температури було важче знайти дефектні пікселі. Зазначено, що коли місцезнаходження дефектного пікселя було відоме, його можна легко ідентифікувати на інших зображеннях з тієї ж камери.

Ще один тест був проведений для визначення впливу стиснення JPEG на видимість і розташування дефектних пікселів [57]. Зроблено висновок, що видимість і розташування не зазнали значного впливу, доки зображення не було стиснуте приблизно до 50 %. Унаслідок роботи функції JPEG плями на пікселях почали зміщуватися й поширюватися на сусідні пікселі залежно від положення матриці DCT.

1.4 Опис процесів захисту авторських прав на цифровий контент

У підрозділах 1.1 – 1.3 йшла мова про блокчейн, цифрову фотографію та автентифікацію. На даний момент це актуальна тема, тому що в сучасному світі відбувається «цифровізація» і зараз дуже складно захистити свої авторські права на інтелектуальну власність та цифровий контент, тому в наступних розділах даної роботи пропонується, як захистити свої права на цифровий контент та як коректно та згідно з законодавством передати авторські права іншому користувачеві.

Права на інтелектуальну власність, зокрема авторські права, стали одним із найважливіших факторів належного забезпечення інтересів авторів художніх та літературних творів, а також фінансових і ринкових позицій компаній, які розробляють програмне забезпечення, комп'ютерне устаткування, телерадіокомпаній, видавництв тощо [58].

Захист авторських і суміжних прав та інтересів, які захищаються державою та здійснюється в передбаченому законом порядку, тобто за допомогою застосування належної форми, засобів і способів захисту.

Згідно з ст. 433 ЦКУ і ст. 6. ЗУ «Про авторське право і суміжні права»

об’єктами авторського права є [59]:

Об’єктами авторського права є твори у сфері літератури, мистецтва, науки, зокрема:

1) літературні твори белетристичного, публіцистичного, наукового, технічного або іншого характеру (книги, брошури, статті тощо) у письмовій, електронній (цифровій) чи іншій формі;

2) театральні постановки, сценічні переробки творів, зазначених у пункті 1 цієї частини, і обробки нематеріальної культурної спадщини, придатні для сценічного показу;

3) аудіовізуальні твори;

4) тексти перекладів для озвучення (у тому числі дублювання), субтитрування аудіовізуальних творів іншими мовами;

5) фотографічні твори;

6) твори художнього дизайну;

7) похідні твори;

8) збірки творів, збірки обробок нематеріальної культурної спадщини, енциклопедії та антології, збірки звичайних даних, інші складені твори, за умови що вони є результатом творчої діяльності за добором або упорядкуванням змісту;

9) ілюстрації, карти, плани, креслення, ескізи, пластичні твори, що стосуються географії, геології, топографії, техніки, будівництва та інших сфер діяльності;

10) комп’ютерні програми;

11) бази даних (компіляції даних), якщо вони за добором або упорядкуванням їх складових частин є результатом інтелектуальної діяльності;

12) інші твори.

На рисунку 1.4 зображені твори, які можуть бути захищені авторським правом.

Рисунок 1.4 – Види творів, які можуть бути захищені авторським правом

Слід розрізняти такі поняття, як охорона авторських прав та їх захист. Поняття «охорона» слід розуміти як встановлення всієї системи правових норм, спрямованих на дотримання прав авторів і їх правонаступників. Тоді як захист прав – це сукупність заходів, метою яких є відновлення та визнання прав у разі їх порушення, що включає передбачену законодавством діяльність відповідних державних органів поновлення та визнання прав, а також усунення перешкод, що заважають реалізації прав та законних інтересів їх суб’єктів.

Поняття «авторські права» охоплює дві основні групи прав: особисті немайнові права автора та виняткове право на використання твору. Усі авторські права об'єднує те, що вони передбачають у праві автора (правовласника) здійснювати певні дії й забороняти такі дії іншим особам. При цьому дозвіл автора не обов’язковий. Недотримання заборони є неправомірним. Таким чином, порушення авторських прав – це дії суб'єктів права, що виражаються в недотриманні особистих немайнових прав автора або виняткового права на використання твору.

Відповідно до вищевикладеного визначення умовно можна виділити дві групи порушень авторських прав. Для кожної з них характерні свої умови залучення до відповідальності, способи й порядок захисту. Таким чином, захист авторських прав охоплює захист виключного права й захист особистих немайнових прав авторів творів літератури, науки й мистецтва, рисунок 1.5.

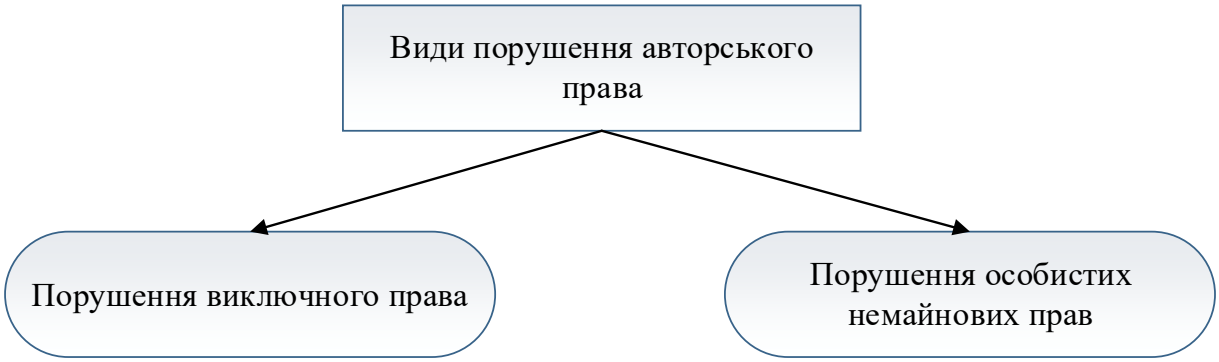


Рисунок 1.5 – Види порушення авторського права

Захист авторських прав здійснюється способами, передбаченими цивільним законодавством. Спосіб захисту – це вимоги, які автор може пред'явити до порушника виключного права або особистих немайнових прав. Найбільш ефективні такі способи захисту авторських прав [60]:

- припинення дій, що порушують авторські права або створюють загрозу порушення. Зокрема, така вимога може бути направлено на заборону поширення контрафактних примірників твору;

- відшкодування збитків, якщо неправомірне використання твору без укладення ліцензійного договору з правовласником заподіяло останньому збитки або призвело до упущеної вигоди;

- вилучення контрафактних примірників творів, а також обладнання і предметів, призначених переважно для створення таких екземплярів. Захист авторських прав у такий спосіб дозволяє припинити порушення в майбутньому;

- публікація рішення суду із зазначенням дійсного правовласника;

- стягнення компенсації за порушення авторських прав. Захист авторських прав у такий спосіб найбільш поширена на практиці.

Коли мова йде про засоби захисту авторських прав у всесвітній мережі інтернет, то їх можливо умовно поділити на два види засобів, які використовуються на етапі, що передує порушенню і вже після порушення [61].

Захист на етапі, що передує порушенню. Основні засоби захисту, які власники авторських прав можуть використовувати при розміщені в інтернеті своїх творів для запобігання порушення своїх прав та застосовувати для контролю за використанням цих творів, такі:

- обмежена функціональність. За такого підходу власник авторського права надає користувачеві примірник твору з функціональними обмеженнями, наприклад, бетаверсії програм;

- часова обмеженість. Використовуючи такий підхід, власник авторських прав розповсюджує функціонально повноцінний об’єкт, але встановлює дату або обмежує кількість разів користування, після чого доступ до твору буде неможливим;

- захист від копіювання. Використовуючи цей засіб, власник прав унеможливлює або значно ускладнює копіювання файлу або тексту;

- криптографічні конверти. Це програмне забезпечення, яке зашифровує твори так, що доступ до них може бути отриманий лише із застосуванням електронного ключа до шифру.

Захист на етапі після порушення. Автори та їх правонаступники можуть використовувати певні технічні та правові засоби для доведення факту порушення своїх прав на розміщені в інтернеті твори та встановлення кола правопорушників, а значить, для забезпечення ефективності реалізації своїх прав. До таких засобів належать:

- агент – це комп’ютерні програми, які можуть автоматично виконувати попередньо визначені команди. Власники авторських прав можуть використовувати агентів для пошуку в інтернеті контрафактних примірників творів;

- стеганографія, засіб який застосовують в електронних файлах означає процес приховування інформації у файлах у такий спосіб, що вона не може бути легко віднайдена користувачем. Використовуючи дану технологію, власник авторських прав має можливість доводити, що файл, який містить контрафактний примірник твору, було створено саме власником

авторських прав, а не їх порушником; а також він має змогу вистежити джерело не санкціонованої автором появи в інтернеті примірників творів;

- судове переслідування, навіть при тому, що далеко не кожне порушення авторських прав стає предметом судового розгляду, загроза подання позову до суду – це досить ефективний стримуючий фактор. судовий розгляд порушень авторського права не тільки дозволяє власнику авторських прав отримати компенсацію за порушення його прав, він також публічно застерігає інших від негативних наслідків їх поведінки. Незважаючи на всі переваги судового переслідування порушників авторських прав, винесення та виконання судового рішення проти іноземного порушника авторських прав на розміщені в інтернеті твори пов’язано з чисельними процесуальними ускладненнями [62].

1.4.1 Водяні знаки, як засіб охорони авторського права

З розвитком технологій та глобальної мережі зростає і кількість мультимедійного трафіку. Щоб встановити автентичність та уникнути зловживання, дані слід захищати водяними знаками. Цифровий водяний знак запобігає незаконному копіюванню та розповсюдженню мультимедійного контенту, приховуючи нічим не примітні дані про право власності [63, 64]. Цифровий водяний знак – це технологія, що використовується в інформаційній безпеці для вирішення проблеми захисту авторських прав на певну комп’ютерну інформацію, приклад застосування ЦВЗ представлено на рисунку 1.6. При цьому на комп’ютерні графічні зображення наноситься спеціальна мітка, яка може залишатись видимою чи невидимою для людини.

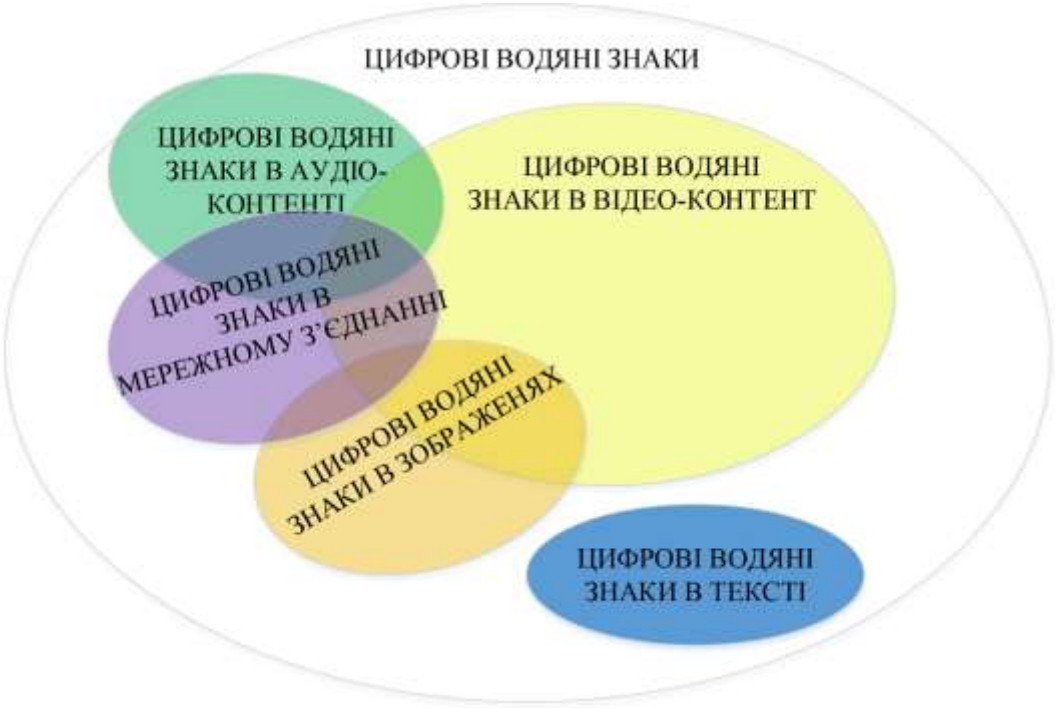


Рисунок 1.6 – Основні засоби інформації, які здатні підтримувати цифрові водяні знаки

Процес вбудови водяних знаків може бути визначений на основі домену та різних груп. Відповідно до домену, можемо розділити методи вбудови цифрових водяних знаків як у просторі домену, так і при перетворенні домену наприклад, методи основані на SVD [65]. Спочатку використовувалися підходи до просторового домену, при якому процес вбудови водяних знаків може здійснюватися шляхом безпосередньої зміни пікселів зображення. Він має переваги, такі як низька обчислювальна складність і простота для реалізації. Найпоширенішим у цій галузі є метод найменш значущий біт (LSB) та метод розширення спектру та кореляція. Однак такі методи, як дискретні косинусні перетворення (DCT), дискретні вейвлет-перетворення (DWT), дискретні перетворення Фур'є (DFT), декомпозиція сингулярних значень (SVD) та перетворення Кархунена-Лоева (KLT) є прикладом методів перетворення домену. У контексті видимості ЦВЗ є дві різні категорії цифрового водяного знаку: видимі і невидимі. Крім того існують різні класи невидимих водяних знаків, які є надійними та крихкими. Повна класифікація цифрових водяних знаків представлена в роботі [65].

1.4.2 Процес вбудови та вилучення водяних знаків

Система вбудовування та вилучення водяних знаків представлена на рисунку 1.7, виконує завдання вбудови та вилучення ЦВЗ з зображення-контейнера.

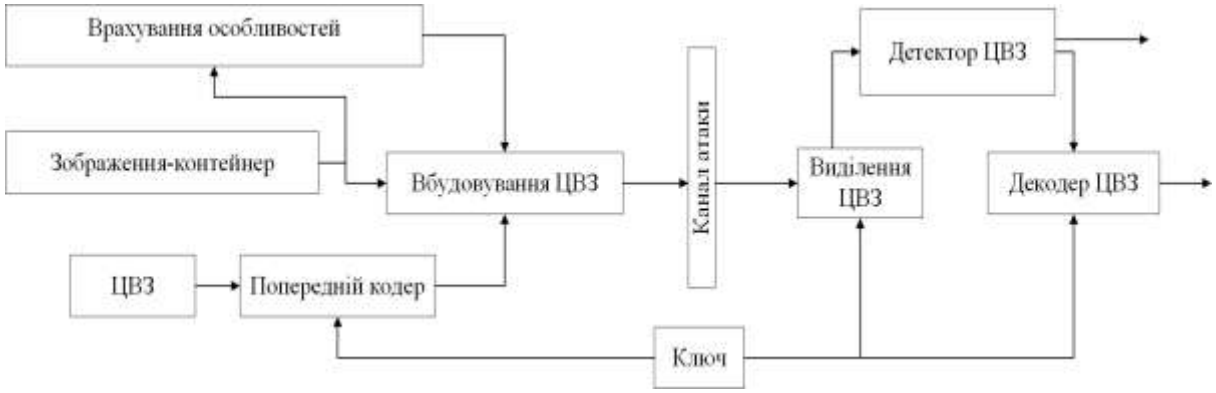


Рисунок 1.7 – Процес вбудови та вилучення водяних знаків

Попередній кодер-пристрій, призначений для перетворення приховуваного водяного знака до вигляду, зручного для вбудови в контейнер. Пристрій вбудови ЦВЗ призначений для здійснення вбудовування (вкладення) прихованого ЦВЗ в зображення-контейнер. У системі відбувається об’єднання двох типів інформації так, щоб вони могли бути помітні двома принципово різними детекторами. У якості одного з детекторів виступає система виділення ЦВЗ, у якості іншого – людина. Попередня обробка часто виконується з використанням ключа для підвищення секретності даних, які вбудовуються. Далі ЦВЗ «вкладається» в контейнер, наприклад, шляхом модифікації молодших значущих біт коефіцієнтів. Цей процес можливий завдяки особливостям системи сприйняття людини. Добре відомо, що зображення мають велику психовізуальну надмірність. Око людини подібне до низькочастотного фільтру, що пропускає дрібні деталі.

Існують три різні класи цифрових водяних знаків, які залежать від характеристик та способу їх детектування [66-68]. Короткий зміст цієї

системи розглядається на рисунку 1.8.

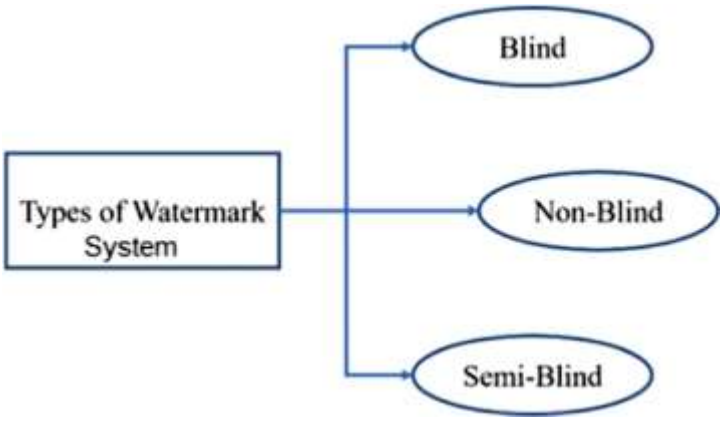


Рисунок 1.8 – Важливі класи водяних знаків

Важливі класи водяних знаків:

- сліпий метод вбудови ЦВЗ: у цьому типі системи вбудова водяних знаків потребує лише зображення із водяним знаком, для вилучення ЦВЗ не потрібне оригінальне зображення. Сферою застосування методу сліпої вбудови водяних знаків є охорона здоров'я, захист авторських прав, електронна система голосування тощо.

- несліпий метод вбудови ЦВЗ: у такій системі копіюється оригінальне зображення та вбудоване, для вилучення ЦВЗ необхідні водяний знак та оригінальне зображення. Сферою застосування цього типу систем водяних знаків є негласне спілкування та захист авторських прав.

- напівсліпий водяний знак: він працює як несліпова система, необхідні додаткові вхідні дані. Деякі важливі сфери застосування такої системи – це аутентифікація зображень, моделі САПР тощо.

Існує безліч важливих параметрів, які характеризують водяний знак і є дуже важливими для цифрових систем водяного маркування. На рисунку 1.9 зображені основні параметри водяних знаків.

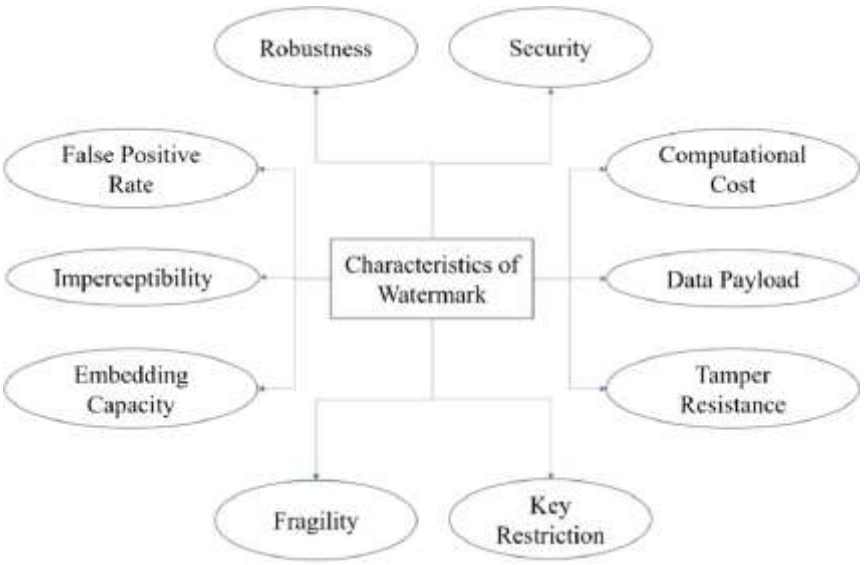


Рисунок 1.9 – Параметри водяного знаку

Стійкість – це здатність алгоритму захищатися від шуму. Безпека означає, що водяний знак важко змінити або видалити, не руйнуючи зображення-контейнер. Розмір ЦВЗ виражається як кількість інформації, яку містить контейнер. Непомітність досягається шляхом невидимої для людського ока або беззвучної для вуха зміни файлу. ЦВЗ називається крихким, якщо при найменшій модифікації його вже не можна виявити. Такі ЦВЗ зазвичай використовують для перевірки цілісності. Обмеження ключа беруться до уваги як ще одна характеристика – це рівень обмеження, що застосовується до можливості зчитування водяного знаку. Обчислювальна складність визначається загальними витратами ресурсів при вбудові та вилученні ЦВЗ. Інші важливі характеристики чітко визначені в [69].

Застосування водяного знаку. Потенційні дослідники використовують різні схеми водяних знаків для різних сфер діяльності людини. До них належать захист авторських прав, цифрова криміналістика, військова справа, цифрова криміналістика, охорона здоров’я, медичні програми тощо. Деякі сфери застосування представлені на рисунку 1.10.

Рисунок 1.10 – Сфери застосування цифрового водяного знаку

Застосунки для захисту авторських прав. Головною метою є захист авторських прав на цифрову інформацію шляхом приховування секретної інформації. Захист цифрового авторського права – це технологія захисту прав, контролю використання та управління цифровими контентом. В епоху інформаційних технологій та мультимедіа зловмисна експлуатація та піратство стали глобальним явищем. Водяні знаки використовуються для вирішення незліченних дилем, пов’язаних із проблемами в галузі управління цифровими правами та мультимедійної безпеки. Відповідно до потреб того чи іншого застосування, для захисту авторських прав цифрових об’єктів були розроблені різні відповідні процедури нанесення водяних знаків на зображення [70].

Застосунки для забезпечення конфіденційності контенту. Головною метою є забезпечення конфіденційності різних типів цифрового контенту, які передаються по незахищеним каналам зв`язку. У нинішній мультимедійній мережній інфраструктурі порушення конфіденційності через кібератаки призводять до величезних економічних втрат. Незважаючи на ці загрози, постійно зростає попит на обмін даними через різні незахищені мережі для

виконання численних завдань. За такого сценарію виникає потреба в розробці нових алгоритмів для розширення існуючих рамок кібербезпеки, гарантії безпеки, конфіденційності, захисту авторських прав та аутентифікації даних. І для цього починають широко використовуватися цифрові водяні знаки, що продемонстровано в роботах [61,70].

Застосунки для дистанційного навчання. Головною метою є забезпечення авторського права на цифровий контент та запобігання несанкціонованого використання цифрового контенту. У сучасну цифрову еру дуже легко копіювати, маніпулювати та поширювати мультимедійні дані по відкритому каналу. Захист авторських прав, автентифікація вмісту, викрадення особистих даних та ідентифікація власності стали складними проблемами для авторів дистанційних курсів [71].

Застосунки для електронного голосування. Головною метою є забезпечення конфіденційності електронної системи голосування. Відповідно до результатів останніх звітів про вибори в різних частинах світу виявлено, що корумповані політики та корумповані виборчі працівники дійсно мають змогу маніпулювати результатами, що може призвести до небажаних наслідків. Це означає, що результати виборів не були належним чином захищені від атак, таких як підміна результатів.

Застосунки для захисту CAD моделей. Система автоматизованого проектування (САПР) створює 2D- та 3D-дизайн об'єктів, які зазвичай використовуються для проектування. Ці елементи даних загальнодоступні в мережі інтернет. Через легку доступність до цих моделей стає нагальним і важливим питання безпеки. Ці елементи можуть бути захищені від несанкціонованого доступу за допомогою криптографії, цифрового підпису або водяних знаків. У роботі [72] пропонується схема водяних знаків для тривимірного об’єкта, створеного за допомогою автоматизованого проектування (САПР), що зберігає геометричну форму та якість об’єктів із водяними знаками.

Застосунки у сфері охорони здоров’я. Інтелектуальна система охорони

здоров’я представляє собою систему обміну електронними картами пацієнтів, політику доступу та обміну даними електронними картами пацієнтів і забезпечує відповідну медичну допомогу пацієнтам. Однак безпека даних електронних карт пацієнтів досі залишається серйозною проблемою в таких системах. У роботі [73] представлено схему подвійного водяного знака на основі стиснення, а потім шифрування для захисту даних електронних карт пацієнтів для системи охорони здоров’я.

Застосунки для моніторингу трансляції. Дозволяє власникам контенту автоматично перевіряти, коли, де й скільки часу контент транслювався через кабельне, супутникове телебачення. Цифрові водяні знаки для відео є потенційним рішенням для захисту цифрових мультимедіа від таких потоків. Методика передбачає приховування аутентифікованої інформації в мультимедійних ресурсах, таких як зображення, аудіо чи відео таким чином, щоб вона не впливала на якість відеооб’єктів і могла бути легко вилучена сертифікованим користувачем, коли це потрібно [74].

Застосунки для цифрової криміналістики. Цифрова криміналістика – це процес, за допомогою якого контейнер із водяними знаками містить ідентифікатор одержувача з метою простеження джерела незаконного розповсюдження [75].

Застосунки для медицини. Застосування реверсивних цифрових водяних знаків для верифікації медичних зображень. У зв’язку з широким поширенням медичних зображень та покращенням комунікаційних та комп’ютерних технологій в останні роки достовірність зображень стала своєрідним викликом для програм електронної охорони здоров’я. І тому потенційними дослідниками удосконалюються вже відомі методи нанесення водяних знаків [76].

Захист чипів та апаратних засобів: Mohanty C. П. [77] розповів про роль водяних знаків у захисті апаратного дизайну. Захист ядра та апаратного забезпечення інтелектуальної власності (IP) – це багатошарова проблема, що містить Trojan Security, безпеку власності покупця, захист від піратства. На

основі вибору дизайнера цифрові водяні знаки можуть бути вбудовані в багаторівневу концепцію апаратного дизайну.

Захищені дані в хмарі. Зі збільшенням кількості зображень у повсякденному житті розглядається пошук зображень на основі вмісту. Зображення займають більше місця в порівнянні з текстом. Тому для зберігання зображень може використовуватися хмарне сховище. Деякі чутливі зображення, такі як медичні та немедичні, повинні бути автентифіковані перед перенесенням в інше місце. Хмарним сервером унікальний водяний знак вставляється в зашифровані зображення, перш ніж вони надсилаються користувачеві. Коли виявлено нелегальне зображення, методом вилучення водяного знаку може бути виявлений несанкціонований користувач.

Завдання вбудовування і видобування інформації з контейнера виконує стеганосистема, яка складається з стеганокодера і стеганодекодера. Стеганокодер перетворює приховане повідомлення до вигляду, зручного для вбудовування в сигнал-контейнер і вбудовує приховане повідомлення в сигнал-контейнер з урахуванням його моделі. Стеганодекодер визначає наявність прихованого повідомлення в контейнері і, за наявності, видобуває й відновлює приховане повідомлення.

Стеганографія тісно пов'язана з криптографією, проте ці науки мають різні підходи до захисту інформації. Зокрема криптографія приховує інформацію за допомогою операції шифрування, тобто наперед відомо, що в криптограмі міститься зашифрована інформація. А стеганографія приховує факт наявності секретної інформації, тому заповнений контейнер не повинен відрізнятися від порожнього. Для підвищення захищеності інформації методи криптографії та стеганографії можуть поєднуватися.

Стеганосистема утворює стеганоканал, по якому передається заповнений контейнер. Доступ до цього каналу можуть отримати порушники. Опишемо коротко, якої шкоди вони можуть завдати. Для таємного обміну повідомленнями двоє адресатів повинні мати відомий обом секретний ключ,

який визначатиме місцезнаходження прихованого повідомлення.

У першу чергу порушник може встановити факт наявності стеганоканалу й читати повідомлення. Можливість читання повідомлення визначається стійкістю використаної системи приховування. Розглянутий тип порушників вважається пасивним.

Існує також активний порушник, який може видаляти або руйнувати приховані повідомлення. Хоча факт втручання буде відомий, проте мета порушника зламування стеганосистеми буде досягнуто. Найбільш небезпечним є зловмисний порушник, який, крім руйнування, може здійснювати підміну стеганоповідомлень.

Для реалізації загроз порушники використовують наступні атаки:

- активні атаки: у такого типу атак хакер навмисно намагається видалити водяний знак або просто зробити так, щоб його неможливо було виявити. вони спрямовані на спотворення вбудованого водяного знаку до невпізнання.

- пасивні атаки: зловмисники намагаються визначити, чи є водяний знак. жодного знищення або видалення не робиться. ці типи атак важливі в негласному спілкуванні.

- атаки підробки. Хакер не видаляє водяний знак, а вставляє новий дійсний водяний знак.

- атаки змови: цей вид не відрізняється від активних атак. Хакер використовує різні екземпляри однієї й тієї ж інформації, що містять кожен раз різний знак, для створення копії від копії без ЦВЗ.

- прості атаки: це атака форми сигналу та шумова атака. Вони є простими, оскільки зловмисник намагався завдати шкоди вбудованому водяному знаку, змінивши весь водяний знак. прикладами цих атак є фільтрація, додавання шуму, стиснення на основі сигналу (JPEG, MPEG) та гамма-корекція.

- атака неоднозначності: ці атаки намагаються заплутати, створюючи підроблені дані з водяними знаками або підроблені оригінальні дані,

інверсійна атака є прикладом такого типу.

- криптографічні атаки: основна мета цієї атаки полягає в порушенні методу безпеки в техніках нанесення водяних знаків та знаходженні способу видалення вставленої інформації про водяний знак. Через високу обчислювальну складність застосування цих атак обмежено.

- атака на видалення: без порушення безпеки ЦВЗ, повне видалення даних водяних знаків із даних контейнера.

- геометрична атака: у зворотному порядку від атак видалення, ці атаки насправді не видаляють сам вставлений водяний знак, а мають на меті змінити синхронізацію детектора водяних знаків із вставленою інформацією.

1.5 Аналіз сучасних методів нанесення ЦВЗ

Проаналізовано й виділено різні надійні підходи для нанесення водяних знаків щодо захисту конфіденційної інформації в різних сферах застосування.

Розроблено надійну техніку водяного маркування кольорових зображень із використанням індукції дерева рішень в області DCT [78]. Метод використовує DCT спочатку для перетворення контейнера та зображення водяного знака та метод індукції дерева рішень використовує для приховування секретного водяного знаку.

У статті [79] представлено надійну багатобітну схему нанесення водяних знаків зображення, щоб зробити неефективними звичайні атаки обробки зображень, а також афінні спотворення. Ця схема поєднує в собі контрастну модуляцію й ефективну синхронізацію для великого корисного навантаження й високої надійності. Ефективність і переваги запропонованої схеми підтверджені експериментальними результатами, які показують чудові характеристики в порівнянні з декількома сучасними методами нанесення водяних знаків.

Автори розробили алгоритм водяних знаків із використанням SVD та

генетичного алгоритму [65,80]. Метод застосовує сингулярний вектор для вставки водяного знака в контейнер. Крім того, методика GA впроваджується для підвищення ефективності запропонованої схеми.

Водяні знаки на основі вейвлетів представлені в [81]. Метод використовує масштабний коефіцієнт для модифікації окремого вектора зображення-контейнера та водяного знака. Крім того, для оптимізації балансу між суперечливими факторами водяних знаків застосовується багатоцільова оптимізація рою частинок (MOPSO).

Для цього автори розробили схему водяних знаків із використанням правил асоціації та векторного квантування. Спочатку правила визначаються як для 2D-штрих-коду, так і для інформації про водяний знак. У процесі вбудови сформовані правила інформації про водяний знак вбудовуються в правила асоціації інформації про штрих-код контейнера. Результати показали, що схема безпечна та має найкращу здатність до вбудови [82].

Техніка зворотного нанесення водяних знаків із високою ємністю з використанням шаблону ромба, сортування та методу зсуву гістограми запропонована в роботі [83]. Спочатку контейнер розділяють на два різні набори даних, а потім інформацію про корисне навантаження вбудовують в обидва набори. Запропонований спосіб надійний і непомітний для різних атак.

У роботі [84] автори розробили піксельний підхід до приховування даних. Метод використовує шуми на зображенні, щоб приховати дані водяних знаків. Поняття таблиці пошуку використовуються для швидкого відновлення прихованих водяних знаків.

У роботі [85] автор запропонував метод збурення для автентифікації секретних даних у вихідних і повертає збурені дані назад до вихідних. Метод використовує підхід з регульованим зважуванням для оцінки ступеня помилок вихідних даних. Продемонстровані результати чітко свідчать про те, що метод надійний і безпечний при великому об’ємі корисного навантаження.

Автор розробив надійний водяний знак через DWT, усі фази дискретного косинусного ортогонального перетворення (APDCBT) та SVD [86]. Зображення-контейнер трансформується DWT, а вибрані області використовуються для вбудови двох подібних водяних знаків. Завдяки відмінній концентрації енергії, автор використовує APDCBT для забезпечення кращого захисту секретних даних (водяних знаків). Крім того, непомітність покращується за допомогою використання коефіцієнтів постійної енергії.

На рисунку 1.11 зображено різні методи для підвищення надійності методів нанесення водяних знаків.

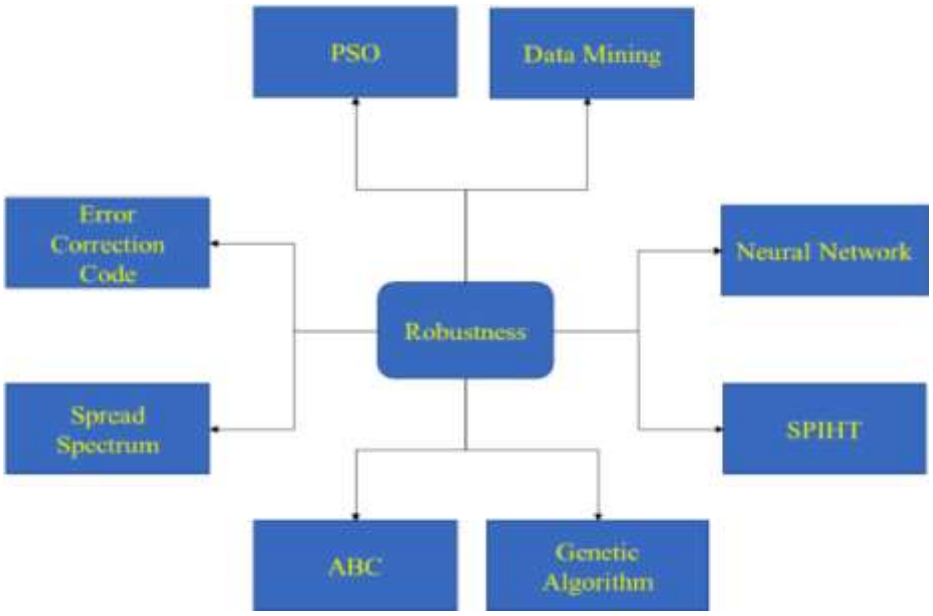


Рисунок 1.11 – Визначені методи, що використовуються для підвищення надійності методів нанесення водяних знаків

1.6 Постановка задач дослідження

На основі проведеного аналізу сучасного стану проблеми й особливостей задач забезпечення авторського права та підтвердження автентичності цифрових зображень можна зробити висновок щодо актуальності задач та необхідності їх подальшого дослідження з метою

підвищення ефективності автентичності підтвердження права власності цифрових зображень.

Проаналізовано методи нанесення цифрових водяних знаків на зображення та представлено сучасні підходи до їх реалізації.

Цифрові зображення захищені законом про авторське право, як і будь-які інші оригінальні роботи. Але порядок державної реєстрації авторського права на зображення, визначений у законах України, має ряд недоліків, таких як тривалий процес перевірки авторства, відсутність предметної перевірки, складність доказу, висока вартість, централізоване зберігання та інші. Саме тому актуальним є розробка новітніх технологій підтвердження авторства на цифрові зображення, які дозволять удосконалити та покращити сам процес захисту авторського права на цифрові зображення.

У зв’язку з тим, що метою дисертаційної роботи є розробка інформаційної технології автентифікації цифрових зображень, яка використовує сучасні тенденції в області цифрових водяних знаків та блокчейну для створення нової децентралізованої технології підтвердження права власності цифрових зображень, для досягнення поставленої мети необхідно вирішити такі завдання:

- проаналізувати стан проблеми й особливості задач забезпечення авторського права та підтвердження автентичності цифрових зображень;
- розглянути методи нанесення цифрових водяних знаків на зображення й провести їх порівняльний аналіз;
- розглянути критерії оцінки ефективності методів нанесення цифрових водяних знаків;
- запропонувати комплексний критерій оцінки ефективності методів нанесення цифрових водяних знаків;
- розробити модель автентифікації цифрових зображень, що дозволить реалізувати ефективний спосіб захисту авторських прав на цифрові зображення;
- розробити функціональну модель процесу забезпечення підвищення

стійкості методів вбудови цифрових водяних знаків у зображення;

- розробити методи генерації стійкого до спотворень цифрового водяного знака на основі хаотичних карт;

- розробити інформаційну технологію підтвердження права власності на цифрові зображення.

Вирішенню поставлених завдань, що виникають у процесі підтвердження права власності на цифрові зображення на основі моделі інформаційної технології та блокчейну для створення нової децентралізованої технології підтвердження права власності цифрових зображень, присвячені наступні розділи.

1.7 Висновки за першим розділом

1. Проведено системний аналіз проблеми й особливості задач забезпечення авторського права та підтвердження автентичності цифрових зображень. В результаті зроблено висновки:

– існуючи методи основних засобів захисту авторських прав на твори, розміщені в інтернеті: обмежена функціональність, часова обмеженість, захист від копіювання, криптографічні конверти. Вони сприяють уникненню порушення авторських прав та застосовуються для контролю щодо використання цих творів іншими відвідувачами мережі. Проведений порівняльний аналіз методів дозволив виявити їх переваги та недоліки;

– захист відбувається на етапі після виявлення порушення, автори та їх правонаступники можуть використовувати певні технічні та правові засоби, до яких належать агент, стенографія, судове переслідування.

2. Здійснено огляд та аналіз технології блокчейн та токену як засобу охорони авторського права.

3. Здійснено огляд та аналіз водяних знаків як засобу охорони авторського права.

4. Проаналізовано три різні класи цифрових водяних знаків, які

залежать від характеристик та способу їх детектування.

5. Проаналізовано атаки на водяні знаки, проведено аналіз та виділено різні надійні підходи для нанесення водяних знаків для захисту конфіденційної інформації в різних сферах застосування.

6. Сформульовано мету та задачі дослідження дисертаційної роботи. Список використаних джерел у даному розділі наведено в повному списку використаних джерел під номерами: 1-86.

2 МОДЕЛЬ АВТЕНТИФІКАЦІЇ ЦИФРОВИХ ЗОБРАЖЕНЬ

2.1 Розробка комплексного критерію оцінки ефективності методів нанесення цифрових водяних знаків

На основі проведеного аналізу сфер застосування та особливостей ЦВЗ в таблиці 2.1 представлені важливі параметри ЦВЗ.

Таблиця 2.1 – Характеристики ЦВЗ

Характеристики	Визначення
Надійність	Здатність алгоритму протистояти атакам
Непомітність	У результаті вбудови ЦВЗ зображення повинне мати мінімальне відхилення з оригінальним зображенням
Помилково позитивне вилучення ЦВЗ	Помилка при вилученні ЦВЗ з порожнього контейнера
Крихкість	При найменшій модифікації контейнера модифікується і ЦВЗ
Безпека	Здатність протистояти навмисним атакам
Ємність	Визначається кількістю водяних знаків, що вбудовуються в дані

Проаналізовано сучасний стан досліджень методів ЦВЗ та значущі параметри ЦВЗ, сформовано наступну модель комплексного критерію оцінки ефективності методів ЦВЗ:

$$EF = R \bullet \alpha_r + SR \bullet \alpha_{sr} + ER \bullet \alpha_{er} + SC \bullet \alpha_{sc} + DT \bullet \alpha_{dt,} \quad (2.1)$$

де $R, R \in [0,1]$ – це критерій оцінки надійності методу вбудови ЦВЗ;

$SR, SR \in [0,1]$ – це критерій оцінки непомітності ЦВЗ на зображенні;

$ER, ER \in [0,1]$ – це ймовірність помилки першого й другого роду;

$SC, SC \in [0,1]$ – це критерій оцінки крихкості ЦВЗ;

DT – це кількість вбудованих ЦВЗ;

$\alpha_r, \alpha_{sr}, \alpha_{er}, \alpha_{sc}, \alpha_{dt}$ – це коефіцієнти значимості відповідних параметрів методу ЦВЗ.

Вони потрібні, оскільки не існує універсального методу вбудови ЦВЗ, тому завдяки таким коефіцієнтам можна регулювати значимість кожного параметра і тим самим впливати на остаточну ефективність методу для певної задачі, яка стоїть перед методом нанесення ЦВЗ. З огляду умов застосування та цільової функції, визначено такі значення коефіцієнтів [1].

Для прикладу опишемо критерії ефективності методу ЦВЗ для зображень.

Надійність методу вбудови ЦВЗ можна уточнити в статистичному сенсі, прийняв наступні припущення:

Метод ЦВЗ W може бути визначений як набір деяких функцій F і G, які описують процес вбудови й вилучення ЦВЗ на множині всіх даних, таких, що кожен елемент $E_i \in E$ представляють собою набір даних, необхідних для роботи методу ЦВЗ:

$$E = (E_i, i = 1, 2, ..., N), \tag{2.2}$$

Для спрощення будемо вважати, що набір вхідних даних включає пару значень: контейнер для вбудови *Im* та цифровий водяний знак Wm, це $E_i = \{Im_j, Wm_i\}$. Робота методу складається з двох етапів: вбудова $F(E_i) = Im_i^*$ та вилучення $G(Im_i^*) = Wm_i$. Оскільки надійність – це здатність алгоритму протистояти атакам, то введемо функцію атаки $At_j \in At$, де At – це множина допустимих атак на ЦВЗ.

$$At = (At_j, j = 1, 2...., M), \tag{2.3}$$

Застосувавши функцію $At_j(Im_i^*) = Im_i^{*'}$, призведе до спотворень

контейнера з ЦВЗ. Тоді для деяких значень E_i отримане значення від $G(Im_i^{*'})$ може знаходитися в допустимих межах $\triangle i$, $\left|G(Im_i^{*'}) - G(Im_i^{*})\right| \leq \triangle i$. Для всіх інших E_i, що утворюють підмножину $E_l \in E$, виконання $G(Im_i^{*'})$ не забезпечує прийнятного результату, тобто $\left|G(Im_i^{*'}) - G(Im_i^{*})\right| > \triangle i$. Усі такі випадки називаються хибними.

Кожне значення E_i представляють можливу комбінацію, які можуть бути вхідними даними функціям F і G. Число N можливих E дуже велике, але кінцеве. Сукупність дій:

Кожне значення E_i представляють можливу комбінацію, які можуть бути вхідними даними функціям F і G. Число N можливих E дуже велике, але кінцеве. Сукупність дій:

$$F \rightarrow \forall At_j, At_j \in At \rightarrow G, \tag{2.4}$$

яка закінчується результатом коректного зчитування ЦВЗ з контейнеру або хибним спрацюванням. Таким чином, імовірність P того, що після використання атаки на контейнер з ЦВЗ $At_j(Im_i^{*}) = Im_i^{*'}$ вилучення ЦВЗ з нього призведе до хибного результату, дорівнює ймовірності, що набір вхідних даних E_i який використаний при j-й атаці, належить множині E_l. Нехай $n_{l,j}$ – число різних наборів вхідних даних, що містяться в E_l, для j-ї атаки, тоді $Q_j = n_{l,j} / N$ є ймовірність, що виконання послідовності функцій (2.4) на наборі даних E_i, випадково вибраних з E серед рівноймовірних, закінчиться хибним вилученням ЦВЗ. При цьому $P_j = 1 - Q_j = 1 - n_{l,j} / N$ є ймовірність, що при j-й атаці на наборі вхідних даних E_i, випадково вибраних з множини E, призведе до коректного вилучення ЦВЗ вираз. Оскільки проведення різних атак є незалежними подіями, то ймовірність того, що всі атаки не призведуть до хибного вилучення ЦВЗ вираз (2.6), дорівнюватиме добутку ймовірностей кожної атаки:

$$R = \prod_{j=1}^{n}. \tag{2.5}$$

Цей добуток ймовірностей і буде оцінювати надійність методу ЦВЗ.

Для оцінки непомітності можна використовувати різні метрики оцінки різниці між двома зображеннями, наприклад метрику сигнал-шум. Але така метрика буде більш високого порядку ніж всі інші доданки, що може призвести до хибної оцінки ефективності методу. Тому було запропоновано для оцінки непомітності наступну метрику:

$$SR = \frac{h_x + h_y}{2};$$

$$h_x = \frac{1}{W_h} \bullet \sum_{i=1}^{W_h - 1} \left[\frac{1}{\sigma_x^i \bullet \sigma_x^i} \bullet \sum_{j=0}^{H_t - 1} \left(Di_{i-1,j} - m_x^{i-1} \right) \bullet \left(Di_{i,j} - m_x^i \right) \right]^2;$$

$$h_y = \frac{1}{H_t} \bullet \sum_{i=1}^{H_t - 1} \left[\frac{1}{\sigma_x^{i-1} \bullet \sigma_x^{i-1}} \bullet \sum_{j=0}^{W_h - 1} \left(Di_{i,j-1} - m_y^{i-1} \right) \bullet \left(Di_{i,j} - m_x^i \right) \right]^2;$$

$$Di_{x,y} = | Y(Pixel'_{x,y}) - Y(Pixel_{x,y});$$

$$m_x^i = \frac{1}{H_t} \bullet \sum_{i=0}^{H_t - 1} Di_{i,j};$$

$$m_y^i = \frac{1}{W_h} \bullet \sum_{i=0}^{W_h - 1} Di_{i,j};$$

$$\sigma_x^i = \frac{\sqrt{\sum_{i=0}^{W_h} (Di_{i,j} -) m_x^{i\,2}}}{H_t};$$

$$\sigma_x^i = \frac{\sqrt{\sum_{i=0}^{W_h} (Di_{i,j} -) m_x^{i\,2}}}{W_h}. \tag{2.6}$$

де SR – показник для оцінки внесених змін при вбудові ЦВЗ спотворень;

h_x, h_y – середнє значення квадрата коефіцієнта лінійної кореляції внесених змін при вбудові ЦВЗ спотворень зображення по вертикалі та по горизонталі, відповідно;

m_x^i, m_y^i – математичне очікування величини спотворень в відповідному стовпці або рядку матриці пікселів;

σ_x^i, σ_y^i – середньоквадратичне відхилення величини спотворень у відповідному стовпці або рядку матриці пікселів;

$Di_{x,y}$ – величини спотворення яскравості у відповідному пікселі;

W_h – ширина зображення в пікселях;

H_t – висота зображення в пікселях;

$Pixel'$ – матриця пікселей отриманого зображення;

$Pixel$ – матриця пікселей оригінального зображення;

Y – оператор визначення яскравості пікселя;

ER – це сума помилки першого та другого роду при вилученні ЦВЗ з контейнера.

Для оцінки крихкості ЦВЗ будемо використовувати наступні вирази. Нехай існує деяка функція спотворення $H(k, imige)$, де k – кількість пікселів спотворення, а $imige$ – зображення із вбудованим ЦВЗ. Тоді оцінка крихкості буде мати наступний вигляд:

$$
\begin{aligned}
&F(E_i) = Im_i^*;\\
&G(Im_i^*) = Wm_i;\\
&H = (k, Im_i^*) = Im_i'^*;\\
&G(Im_i'^*) = Wm_i';\\
&count = \sum_{x=0}^{W}\sum_{y=o}^{H}\begin{cases}1, if\ Wm'_{i[x,y]} \neq Wm_{i[x,y]}\\ 0, Wm'_{i[x,y]} \neq Wm_{i[x,y]}\end{cases};\\
&SC = count / (W \bullet H).
\end{aligned}
\qquad (2.7)
$$

де Ei – набір даних;

Im – контейнер для вбудови;

Wm – цифровий водяний знак;

F – вбудова ЦВЗ;

G – вилучення ЦВЗ;

H – функція спотворення;

$count$ – кількість пікселів ЦВЗ, які не співпадають з оригінальним ЦВЗ після спотворення k пікселів контейнера с ЦВЗ;

W, H – ширина та висота зображення в пікселях.

2.2 Підходи до автентифікації цифрових зображень

Автентифікація зображень важлива в багатьох сферах діяльності людини: зображення місцевості, які використовуються у військових цілях, зображення, які можуть використовуватися в судових справах як докази, цифрові документи нотаріусів, зображення фармацевтичних досліджень та контролю якості. Усі ці зображення повинні бути захищені, щоб уникнути можливості фальсифікації.

Існування великої кількості сучасних інструментів цифрової обробки зображень забезпечує безперешкодний доступ до інформації, породжує маніпуляції з нею та повторне використання різного роду цифрової продукції. Це може призвести до великих фінансових або людських утрат.

Ці проблеми можна краще зрозуміти на простому прикладі. Стан пацієнта із серйозною хворобою, яка виявлена на основі медичних діагностичних зображень, з часом може покращитися завдяки лікуванню. Медичне спостереження за цим пацієнтом включає інтерпретацію зображень з його історії хвороби, щоб вчасно оцінити прогресування хвороби. Помилковий діагноз може поставити під загрозу життя пацієнта, якщо збережене зображення зазнало зловмисних маніпуляцій, помилок зберігання або стиснення так, що отримані спотворення не можуть бути виявлені

лікарем. Це приклад, коли модифікації не допускаються. Однак у багатьох сучасних застосуваннях, які забезпечують передавання інформації, відбуваються операції з обробки зображень для передачі, стиснення або відновлення. Тому потрібно мати можливість виявляти одночасно будь-які суттєві зміни у вмісті зображення.

Існує неоднозначність, оскільки в деяких випадках можливі зміни в зображенні дозволено, а в інших – ні. Отже, автентифікацію зображення можна розділити на дві групи: сувору та часткову автентифікацію. Сувора автентифікація використовується для програм, де не допускаються зміни в зображенні кожного пікселя зображення, що потребує захисту. З іншого боку, часткова автентифікація використовується особливо тоді, коли деякі операції з обробки зображень допускаються, такі як стиснення, різні алгоритми фільтрації та/або навіть деякі геометричні перетворення [62].

Для суворої автентифікації рішення, що включать традиційну криптографію та крихкі водяні знаки, дають хороші результати, які задовольняють користувачів, хоча деякі дослідження ще потрібно провести для покращення локалізації та реконструкції областей зображення, які були підроблені. Натомість вибіркова автентифікація використовує методи, засновані на напівкрихких водяних знаках або підписах вмісту зображення, щоб забезпечити певну надійність проти конкретних і бажаних маніпуляцій. Результати задовільні, але проблема далеко не вирішена. Нині дослідження більш зосереджені у сфері підписів вмісту зображень, а кількість запропонованих рішень за останні роки стрімко зросла через велику кількість додатків. Тим не менше, складніші рішення, які дозволяють поєднувати декілька бажаних модифікацій, ще мають бути виявлені.

У цьому розділі представимо, класифікуємо та порівняємо різні алгоритми, які забезпечують сувору та часткову автентифікації. Порівняння ґрунтуються на різних критеріях, таких як виявлення, локалізація, відновлення.

Суворі методи автентифікації поділяються на звичайну криптографію

та крихкі підгрупи з водяними знаками. Часткові методи автентифікації також поділяються на напівкрихкі підгрупи алгоритмів на основі цифрових підписів. Алгоритми, які засновані на традиційній криптографії, порівнюються між собою; алгоритми, що засновані на крихких водяних знаках, порівнюються між собою; потім порівнюється традиційна криптографія та крихкі методи водяних знаків.

Методи автентифікації зображень на основі криптографії розраховують код автентифікації повідомлення (MAC) із зображень за допомогою хеш-функції [61, 70, 71, 87-90] Отриманий хеш (h) далі зашифровується секретним закритим ключем *S* відправника, а потім додається до зображення. Для більш безпечного обміну даними між суб'єктами хеш може бути зашифрований за допомогою відкритого ключа K1 одержувача [91] і представлено на рисунку 2.1. Процес перевірки представлено на рисунку 2.2.

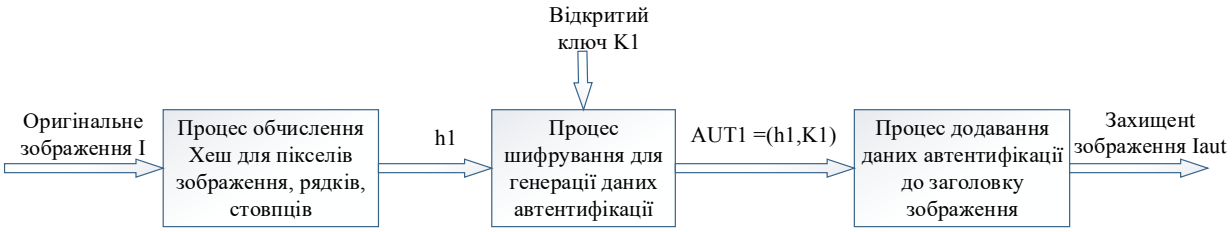


Рисунок 2.1 – Схема генерації даних автентифікації

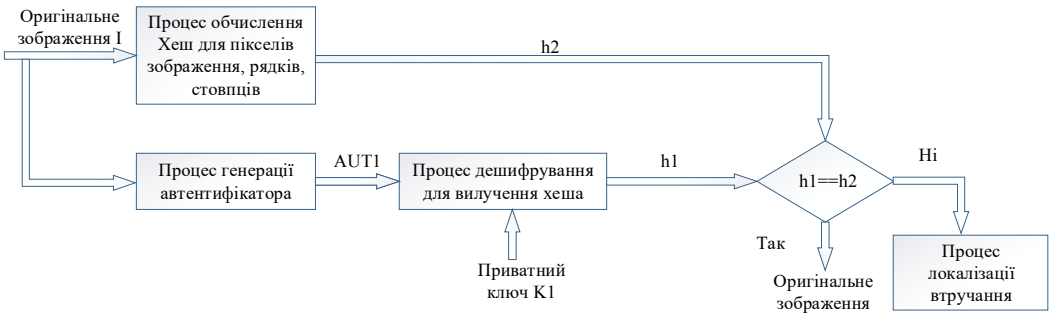


Рисунок 2.2 – Схема верифікації даних автентифікатора

Одержувач обчислює хеш з отриманого зображення. Хеш, який був доданий до отриманого зображення, витягується та розшифровується за допомогою приватного ключа K1. Потім видобутий хеш та обчислений

порівнюються.

Методи, які ґрунтуються на хеш-обчисленні рядків і стовпців зображення, відомі як хеш-функції рядка-стовпця [92]. Окремі хеші отримуються для кожного рядка та стовпця зображення. Ці хеші зберігаються та потім порівнюються з тими, які отримані для кожного рядка та стовпця зображення, що перевіряється. Якщо виявлено будь-які зміни в хешах, то зображення вважатиметься модифікованим, в іншому випадку воно вважатиметься справжнім.

Локалізація спотворень може бути досягнута шляхом визначення рядків і стовпців, для яких хеші відрізняються. Але локалізацію змін можна легко втратити, якщо було пошкоджено декілька областей зображення. Це називається проблемою двозначності хеш-функції рядок-стовпець. Для вирішення цієї проблеми Вольфганг Р. Б. та Дельп Е.Жзапропонували інший підхід [90]. Цей прийом полягає в отриманні хешу блоків зображень окремо. Якщо зображення потрібно перевірити, користувач обчислює хеші для кожного блоку, використовуючи однаковий розмір блоку і порівнює результати з хешами вихідного зображення, щоб з’ясувати, чи зображення є справжнім. Блоки, для яких різні хеші, дозволяють локалізувати спотворення. Обчислення хешів для кожного блоку окремо збільшило можливості локалізації. Однак ці методи не можуть відновити ділянки зображення, які були спотворені.

Звичайна криптографія була розроблена для вирішення проблеми автентифікації повідомлень і мала великий успіх з моменту її появи. Алгоритми, засновані на звичайній криптографії, показують задовільні результати для суворої автентифікації зображення з високим виявленням фальсифікації. Локалізація не дуже хороша, але може бути прийнятною для деяких застосувань. Хеш-функції дуже чутливі до будь-яких невеликих змін у пікселях зображення або навіть у двійкових даних зображення. Як результат, зображення класифікується як маніпульоване, коли змінюється лише один біт цього зображення; це може створювати серйозні проблеми для

більшості програм.

Методи, засновані на крихких водяних знаках. Суть водяних знаків полягає в обчисленні водяного знака, приховуванні його на зображенні, а потім вилученні, коли це необхідно. Крихкі водяні знаки належать до класу суворої автентифікації, а напівкрихкі – до класу часткової автентифікації.

Деякі автори визначають зворотні водяні знаки, які також належать до крихких водяних знаків. Ідея таких знаків полягає в реконструкції точного оригінального зображення і тільки тоді воно оголошується оригінальним. Таким чином, метод реконструює інформацію, втрачену під час процесу додавання водяного знака. Зазвичай, це стисла версія зображення без втрат, у яку було вбудовано водяний знак. Після цього ця стисла версія без втрат об'єднується з водяним знаком, уставляється всередину зображення та витягується для реконструкції лише тоді, коли зображення оголошується оригінальним. Однак у більшості алгоритмів додавання водяних знаків зображення модифікується, але ці модифікації, викликані функціями вбудовування, насправді незначні. Тому зворотні водяні знаки бажані лише для конкретних застосувань, наприклад, для високочутливих зображень. Більше того, їх основною метою є усунення артефактів спотворення, викликаних функціями вбудовування.

Відновлення – це здатність алгоритму відновлювати пошкоджені дані. Коли алгоритм виявляє та локалізує область з деякими небажаними маніпуляціями, іноді треба, щоб цей алгоритм міг відновити вихідні дані, ця вимога бажана для широкого кола застосувань.

Основна ідея крихких методів додавання водяного знаку – створити водяний знак і вставити його в зображення для захисту таким чином, щоб будь-яка зміна, унесена до зображення, також відображалась у вставленому водяному знаку. Просто перевіряючи наявність вставленого водяного знака, можна перевірити справжність зображення і локалізувати підроблені області. Зображення вважається справжнім лише тоді, коли всі його пікселі залишаються незмінними.

Перші алгоритми крихких водяних знаків базувалися на генеруванні водяних знаків лише на основі інформації про зображення, як показано на рисунку 2.3. Водяний знак обчислюється з набору пікселів зображення. Обчислення водяного знаку відрізняється між різними методами автентифікації. Набір пікселів можна вибрати за допомогою секретного ключа K1. Обчислений водяний знак може бути зашифрований ключем K3. Потім він вставляється в найменш значущі біти іншого набору пікселів. З метою підвищення безпеки алгоритму набір пікселів, де вбудований водяний знак, може бути визначений за допомогою іншого секретного ключа K2.

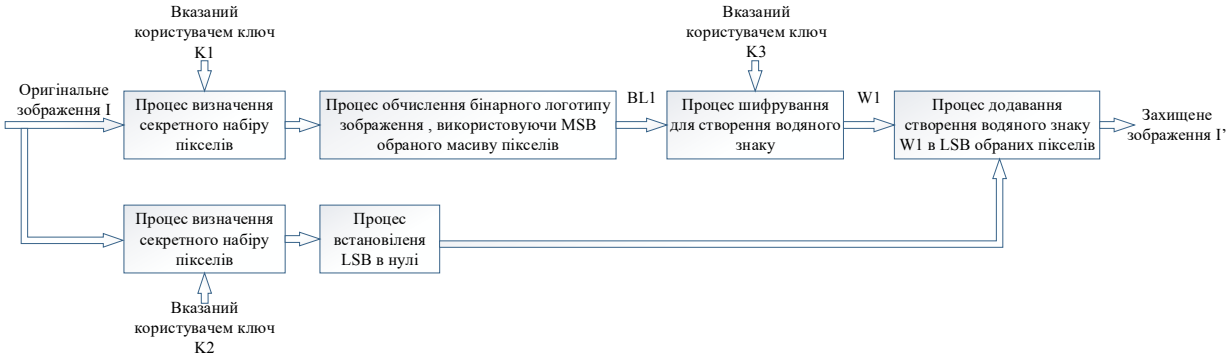


Рисунок 2.3 – Схема автентифікації зображення за допомогою крихкого водяного знаку

Аналогічно схема верифікації показана на рисунку 2.4. Секретні ключі також повинні бути відомі одержувачу. Приймач використовує той самий ключ K2, щоб визначити набір пікселів, де водяний знак розташовано, щоб витягти його. Крім того, приймач використовує ті ж алгоритми, щоб обчислити водяний знак з отриманого зображення, а потім порівнює обчислений водяний знак з вилученим, щоб вирішити, автентичне це зображення чи ні.

Рисунок 2.4 – Схема верифікації даних автентифікатора за допомогою крихкого водяного знаку

Один з перших методів, який використав автентифікацію зображення за допомогою крихких водяних знаків, був запропонований Уолтоном С.[91]; використовував лише інформацію про зображення для створення водяного знака. Цей метод базується на вставці в найменш значущих бітах (LSB) контрольної суми, обчисленої за рівнем сірого для семи найбільш значущих бітів псевдовипадково вибраних пікселів. Такий метод може виявити й локалізувати маніпуляції але без можливості відновлення.

Сувора автентифікація зображення підходить для багатьох програм. Наприклад, зміна лише одного або двох пікселів на деяких медичних або військових зображеннях може різко змінити рішення лікарів або військових стратегів відповідно і призвести до значних збитків. Більшість існуючих графічних додатків використовують операції обробки зображень, які зберігають вміст, щоб заощадити простір пам’яті та пропускну здатність або покращити якість зображення: стиснення, фільтрацію, геометричні перетворення та методи покращення зображення. Тому потрібні деякі толерантні алгоритми автентифікації зображень.

Автентифікація зображень на основі вмісту або часткова автентифікація. Раніше було визначено зміну вмісту як появу або зникнення об’єкта, зміну його положення або текстури, кольору чи країв. Було перераховано операції з обробки зображень, які зберігають їх вміст. Таким чином, багатьом застосуванням, які використовують операції попередньої

обробки зображень без зміни змісту, потрібні методи автентифікації, здатні переносити маніпуляції, що зберігають вміст і в той же час виявляти будь-які маніпуляції, які змінюють вміст зображення. Це призводить до появи нових методів водяних знаків, відомих як напівкрихкі водяні знаки, та до нових підходів, відомих як підписи на основі вмісту. У цьому розділі було представлено та порівняно напівкрихкі методи та підходи на основі вмісту підписів, які надають послугу часткової автентифікації зображень.

Напівкрихкий водяний знак. Стійкий водяний знак розроблений з метою протистояти всім спробам знищити водяний знак. Його основне призначення полягає в охороні інтелектуальної власності та ідентифікації власника. Стійкість вбудованого водяного знака має вирішальне значення для протистояння будь-яким навмисним і ненавмисним маніпуляціям. Метою цих методів є не перевірка автентичності зображення, а швидше за все перевірка їх походження. І навпаки, крихкий водяний знак призначений для легкого руйнування вбудованого водяного знаку після будь-яких маніпуляцій із захищеним зображенням. Це корисно для додатків, де потрібна сувора автентифікація, тобто там, де основною метою є визначення того, чи було змінено зображення, чи ні, з можливістю визначення та реконструкції областей зображення, які були підроблені. З іншого боку, напівкрихкі водяні знаки [72, 92, 93] поєднують характеристики крихких і надійних методів водяних знаків.

Ідея напівкрихкого водяного знаку полягає в тому, щоб вставити водяний знак у вихідне зображення таким чином, аби захищене зображення могло пройти деякі специфічні операції з обробки, поки ще можна виявити шкідливі зміни, а також знайти та відновити області зображення, які були змінені. Для автентифікації зображення алгоритми водяних знаків повинні бути непомітними. Видимі алгоритми водяних знаків застосовуються для онлайн-розповсюдження вмісту, відстеження транзакцій або ідентифікації власника. Процедури створення водяного знаку та вбудовування його в зображення можуть залежати від приватної чи публічної, симетричної чи

асиметричної системи шифрування з метою підвищення загальної безпеки системи. Це компроміс між безпекою та обчислювальною складністю. Як правило, симетричні системи ключів менш безпечні, ніж асиметричні, а асиметричні системи ключів споживають більше ресурсів, а отже, потребують більше часу на обчислення.

Загальна схема методів напівкрихких водяних знаків показана на рисунку 2.5. Водяний знак обчислюється на основі алгоритму обробки кожного пікселя зображення. Обчислення водяного знака змінюється, оскільки можуть бути використані різні алгоритми обробки зображень. Секретний ключ К1 можна використовувати для вилучення конкретної інформації із зображення. Для створення водяного знака вилучену інформацію зображення часто поєднують з двійковим логотипом за допомогою іншого секретного ключа К2. Зазвичай сформований водяний знак потім вставляється в набір частотних коефіцієнтів, які знаходяться в середньому діапазоні. Набір коефіцієнтів, де вставляється водяний знак, можна визначити за допомогою секретного ключа К3. Обчислений водяний знак може бути зашифрований ключем К4.

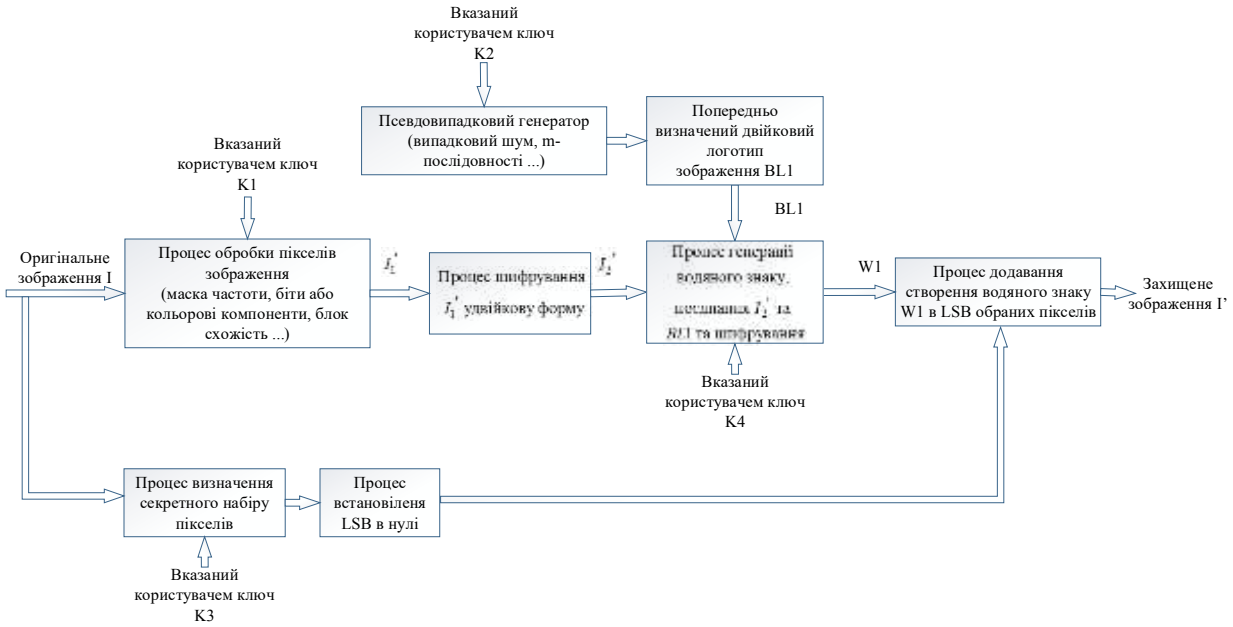


Рисунок 2.5 – Схема автентифікації зображення за допомогою напівкрихкого водяного знака

Аналогічна, загальна схема перевірки показана на рисунку 2.6.

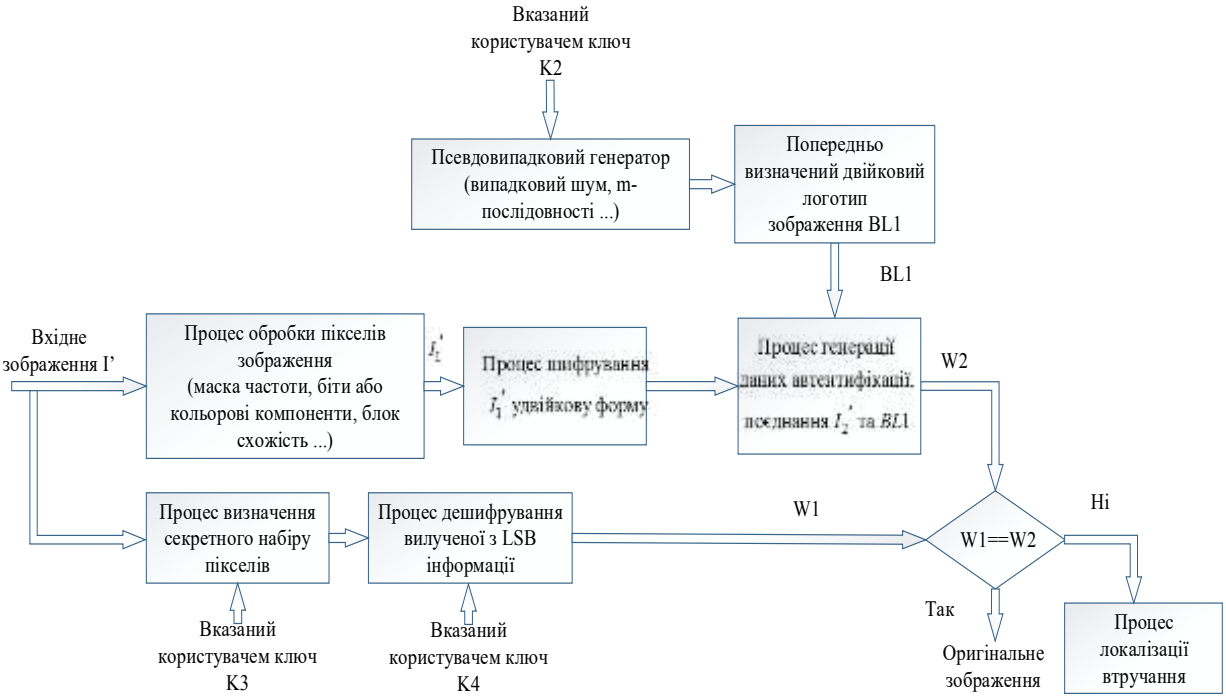


Рисунок 2.6 – Схема верифікації даних автентифікатора за допомогою крихкого водяного знака

Секретні ключі також повинні бути відомі отримувачу. Отримувач використовує той самий ключ, щоб визначити набір пікселів, де міститься водяний знак, щоб витягти його. Крім того, приймач використовує ті ж алгоритми, щоб обчислити водяний знак з отриманого зображення, а потім порівнює обчислюваний водяний знак з отриманим, щоб вирішити, автентичне це зображення чи ні.

Використання інформації про вміст для автентифікації підвищує надійність системи та можливість відновлення пошкоджених регіонів. Однак основним недоліком напівкрихких технік є їх обмежена толерантність до комбінацій маніпуляцій із збереженням вмісту. Справді, більшість із цих методів є успішними навіть за наявності операцій з обробки зображень, які зберігають вміст зображення, наприклад стиснення JPEG, фільтрацію, таку як середнє значення, додавання та інверсія шуму. Однак інші маніпуляції, які

зазвичай використовуються при обробці зображень, такі як помилки передачі або зберігання, геометричні перетворення та корекція гами або яскравості, також повинні бути допущені методами автентифікації. Тому були досліджені інші методи. Вони відомі як алгоритми автентифікації зображень за допомогою цифрових підписів, які базуються на семантичному змісті зображення.

Останні дослідження у сфері автентифікації зображення були зосереджені на цифрових підписах, нанесених на вміст зображення, ці підходи пропонують високу продуктивність.

Системи автентифікації зображень, які використовують цифровий підпис на основі семантичного змісту зображень, можна описати в загальному вигляді наступним чином:

1. Вилучення специфічних характеристик високого рівня з вихідного зображення.

2. Застосування хеш-функції до цих характеристик з метою зменшення їх розміру.

3. Формування цифрового підпису значення хешу за допомогою існуючого алгоритму цифрового підпису, такого як система приватного або відкритого ключа для підвищення загальної безпеки.

4. Прикріплення підпису до вихідного зображення або вставлення його у зображення за допомогою методів приховування даних.

За аналогією, процедура перевірки справжності зображення полягає в наступному:

1. Формування підпису зображення за допомогою того самого алгоритму.

2. Вилучення прикріпленого підпису.

3. Зіставлення цих двох підписів за допомогою алгоритму порівняння, з метою з’ясування, чи було змінено зображення.

4. Визначення областей зображення, які підлягали маніпуляціям.

Коли зображення оголошується недійсним, інформація з оригінального

підпису може бути використана для часткового або навіть повного відновлення пошкоджених областей.

Схематично автентифікація зображення за допомогою цифрових підписів на основі вмісту зображення представлена на рисунку 2.7.

Багато параметрів безпосередньо впливають на продуктивність системи автентифікації зображення на основі підпису вмісту зображення. Ці параметри включають вибір відповідних характеристик: вибір хеш-функції та алгоритму цифрового підпису, вибір методу приховування даних у зображеннях, а також вибір алгоритму, який порівнює підписи для прийняття рішення про достовірність зображення. Вміст зображення і метод приховування даних – особливі параметри, які в основному впливають на продуктивність методів автентифікації зображення. Фактично на чутливість, надійність, відновлення, переносимість, безпеку та складність безпосередньо впливає вибір характеристик, які використовуються для створення підпису на основі вмісту. На них також впливає вибір методу приховування даних.

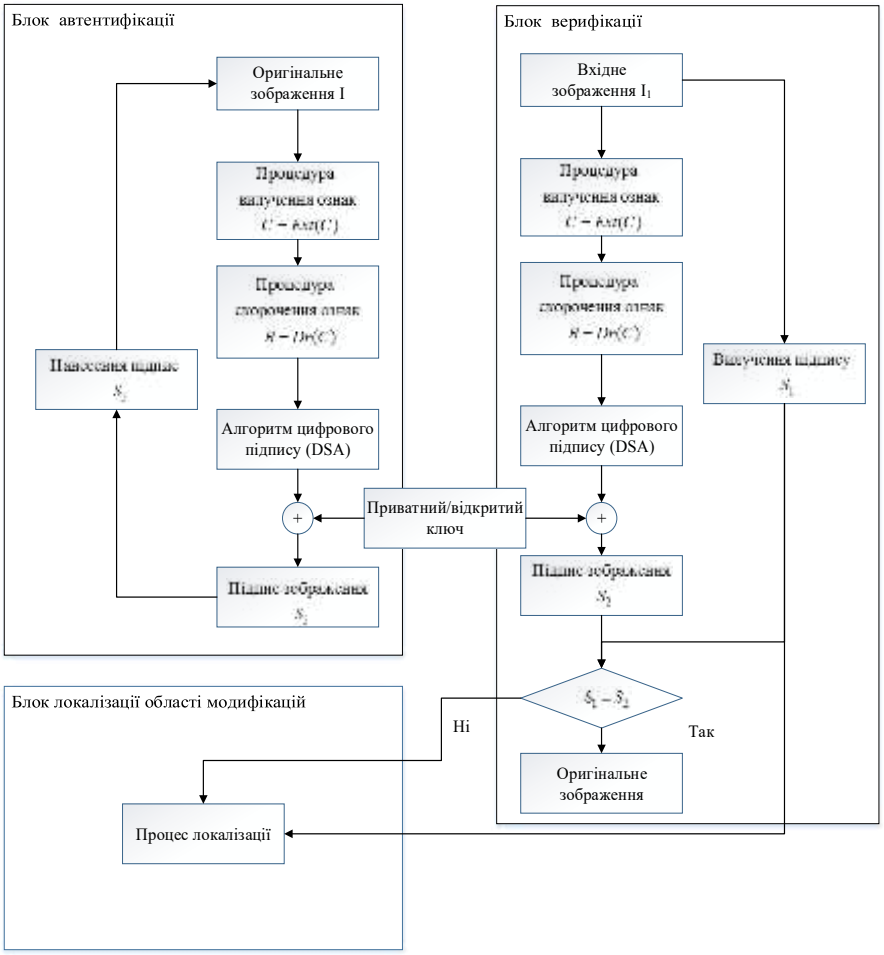


Рисунок 2.7 – Система часткової автентифікації за допомогою цифрового підпису на основі вмісту зображення

Хеш-функція та алгоритми цифрового підпису майже однакові для всіх методів. Алгоритм, який використовується для порівняння підписів, безпосередньо залежить від обраних характеристик та методу приховування.

2.3 Функціональна модель перевірки автентичності цифрового зображення

Модель перевірки автентичності цифрового зображення може бути розглянута як стеганографічна система, у якій передається інтегрований зашифрований ідентифікатор в область зображення, яке є цифровим водяним знаком.

Процес перевірки справжності цифрового зображення за допомогою

ЦВЗ представлений на рисунку 2.8 і складається з таких основних етапів:

1. Визначення області для вбудови.

2. Генерація ЦВЗ автора, отримано подальший розвиток критерію оцінки ефективності методів нанесення ЦВЗ на зображення, який відрізняється від існуючих можливістю тим, що враховує всі типи атак та дозволяє провести комплексну оцінку ефективності методу нанесення).

3. Вбудова ЦВЗ у фрагмент зображення (вклад автора, було розроблено функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків у цифрові зображення, основана на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку).

4. Попередня обробка зображення після вбудовування фрагмента з ЦВЗ у вихідне зображення.

5. Виявлення фрагмента з ЦВЗ (вклад автора, уперше запропоновано модель надійної перевірки справжності цифрового зображення з високим ступенем захисту).

6. Вилучення ЦВЗ з фрагмента.

7. Виправлення помилок у ЦВЗ при добуванні (вклад автора, розроблено методи генерації ЦВЗ на основі хаотичних карт та додатковій фільтрації цифрового водяного знаку. Описані в роботі методи є ефективними для забезпечення стійкості ЦВЗ до локальних спотворень. Як показали дослідження, при 60 % спотворення зображення можливо відновити 90 % ЦВЗ).

8. Отримання мітки правовласника (вклад автора, удосконалено інформаційну технологію підтвердження права власності на цифрові зображення, що основується на технології блокчейн та цифрових водяних знаках для забезпечення надійної гарантії встановлення авторських прав).

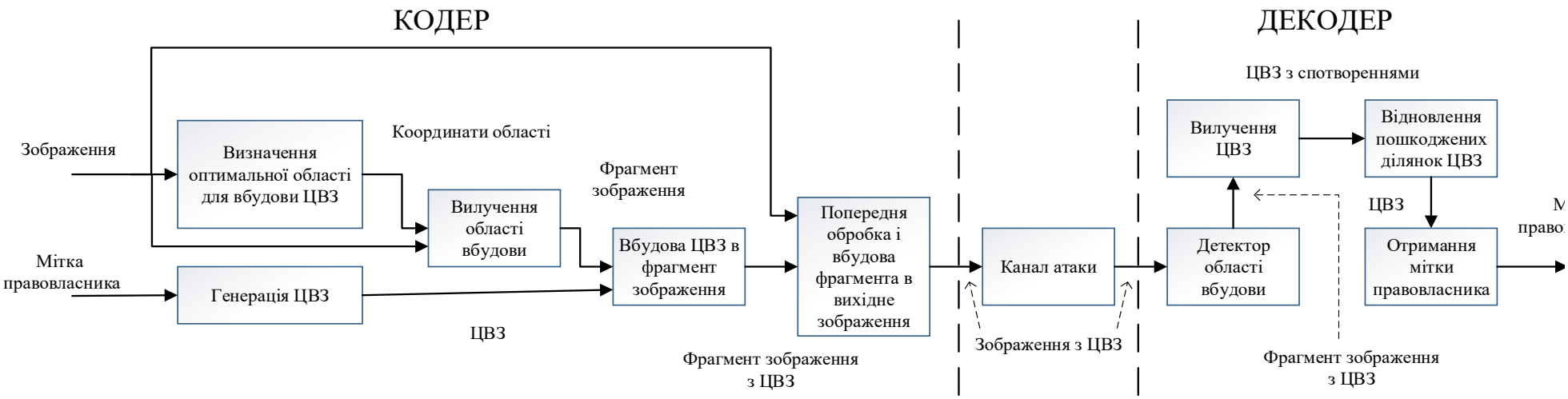


Рисунок 2.8 – Модель перевірки справжності цифрового зображення

Розглянемо ці етапи.

Етап 1 – Визначення області для вбудовування.

Нехай є зображення $\mathrm{Im}[\mathrm{N},\ \mathrm{M}]$, у яке необхідно вбудувати ЦВЗ. Тоді в найпростішому випадку процедуру визначення оптимальної області для вбудовування ЦВЗ можна представити за допомогою методу ковзаючого вікна. Схема алгоритму визначення області для вбудовування представлена на рисунку 2.9. Аналітично обробку ковзаючим вікном можна представити таким чином:

$$\mathrm{E}(\mathrm{Im}_{\mathrm{i,j}}) = \mathrm{Q}\left|\mathrm{q}(\mathrm{Im}_{\mathrm{i,j}}), \mathrm{q}(\mathrm{Im}_{\mathrm{i,j+1}}), \mathrm{q}(\mathrm{Im}_{\mathrm{i,j-1}}), \ldots\right| = \mathrm{Q}\left|\mathrm{q}(\mathrm{Im}_{\mathrm{i+k}}, \mathrm{Im}_{\mathrm{j+1}})\right| \langle \mathrm{k,l} \rangle \in \mathrm{S}, \quad (2.11)$$

де $\mathrm{E}\ \left(\mathrm{Im}_{\mathrm{i,\ j}}\right)$ – значення оптимальності області для вбудовування;

Q – функція, яка описувала правила оцінки пікселів, що входять в околицю S;

S – околиця точки, безліч точок (пікселів), що оточують робочу точку (зазвичай це буває центральний піксель);

$\mathrm{k},\ \mathrm{l}$– розмір ковзаючого вікна, що задається множиною S зміщення координат по осі абсцис й осі ординат відповідно.

Етап 2 – Генерація ЦВЗ.

Нехай $\mathrm{W}', \mathrm{I}', \mathrm{K}', \mathrm{B}'$ є множина можливих ЦВЗ, контейнерів (форми подання ЦВЗ) ключів і приховуваних ідентифікаторів правовласників відповідно. Тоді генерація ЦВЗ може бути представлена у вигляді:

$$\mathrm{F}:\ \mathrm{I}' \times \mathrm{K}' \times \mathrm{B}' \to \mathrm{W},\ \mathrm{W} = \mathrm{F}(\mathrm{I}, \mathrm{K}, \mathrm{B}), \quad (2.12)$$

де $\mathrm{W}, \mathrm{I}, \mathrm{K}, \mathrm{B}$ – елементи відповідних множин. Узагалі, функція може бути довільною але на практиці вимоги робастності ЦВЗ накладають на неї певні обмеження. Так, у більшості випадків, $\mathrm{F}(\mathrm{I}, \mathrm{K}, \mathrm{B}) \approx \mathrm{F}(\mathrm{I} + \varepsilon, \mathrm{K}, \mathrm{B})$, тобто

незначна зміна контейнера не призводить до зміни приховуваних ідентифікаторів правовласників. Функція зазвичай є складовою:

$$F = T \circ G, \text{ де } G : K' \times B' \to C' \text{ та } T : C' \times I' \to W', \tag{2.13}$$

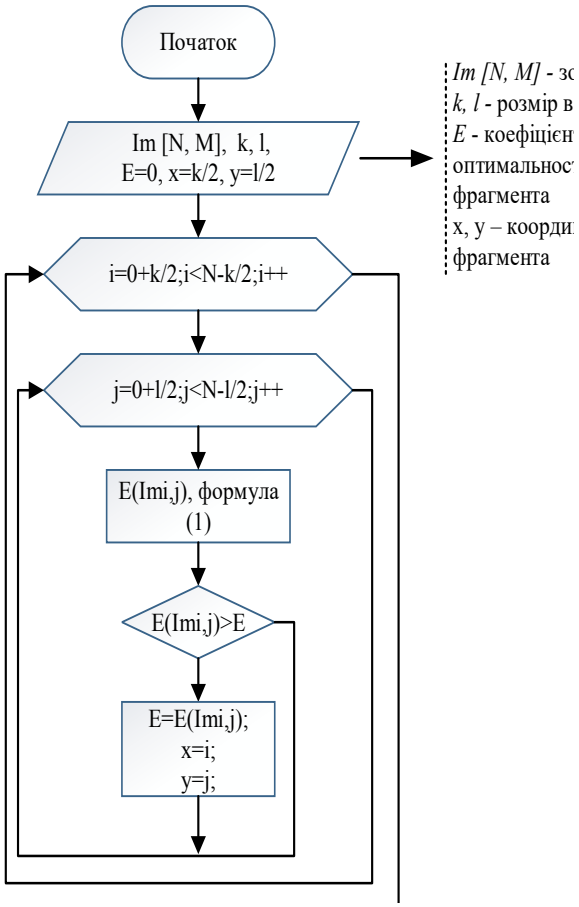


Рисунок 2.9 – Схема алгоритму визначення області для вбудовування

На рисунку 2.9 представлено схему алгоритму визначення області для вбудовування. Тобто ЦВЗ залежить від властивостей контейнера. Функція G може бути реалізована за допомогою криптографічно безпечного генератора ПВП з K у якості початкового значення.

Для підвищення робастності ЦВЗ можуть застосовуватися завадостійкі коди, наприклад, коди БЧХ, згорткові коди [94].

Оператор T модифікує кодові слова C', у результаті чого виходить ЦВЗ W'. На цю функцію можна не накладати обмеження незворотності, так

як відповідний вибір G уже гарантує незворотність F. Функція T повинна бути обрана так, щоб незаповнений контейнер I_0, заповнений контейнер I_W і незначно модифікований заповнений контейнер I'_W породжували б один і той же ЦВЗ:

$$T(C, I_0) = T(C, I_W) = T(C, I'_W), \tag{2.14}$$

Етап 3 – генерація ЦВЗ

Процес вбудови ЦВЗ $W(i,j)$ у вихідне зображення $I_0(i,j)$ в загальному випадку може бути описаний як суперпозиція двох сигналів:

$$\varepsilon:\ I' \times W' \times L' \to I_W,\ \ I_W(i,j) = I_0(i,j) \oplus L(i,j) W(i,j) p(i,j), \tag{2.15}$$

де – $L(i,j)$ маска вбудови ЦВЗ, що враховує характеристики зорової системи людини, служить для зменшення помітності ЦВЗ;

$p(i,j)$ – функція, що проектує;

знаком $\oplus$ позначений оператор суперпозиції, що включає в себе, складання, усічення і квантування.

Функція, що проектує, здійснює «розподіл» ЦВЗ по області зображення. Її використання може розглядатися як реалізація рознесення інформації по паралельних каналах. Крім того, ця функція має певну просторову структуру й кореляційні властивості, що використовуються для протидії геометричним атакам.

Етап 4 – Попередня обробка зображення після вбудовування фрагмента з ЦВЗ у вихідне зображення.

На даному етапі відбувається вставка фрагмента зображення I_W у вихідне зображення Im. Оскільки I_W є модифікацією початкового фрагмента I_0, який служить контейнером для ЦВЗ. При встановленні його у

вихідне зображення Im, фрагмент із ЦВЗ буде відрізнятися від загального розподілу яскравості зображення $I_0(i,j)+\alpha$, де α – це коефіцієнт модифікації, який виник у процесі вбудови. І для усунення цього недоліку після вбудовування фрагмента з ЦВЗ у вихідне зображення застосовується згладжування по краях вбудованого фрагмента для усунення помітності присутності ЦВЗ на зображенні.

Етап 5 – Виявлення фрагмента з ЦВЗ.

Завдання виявлення полягає у встановленні наявності на зображенні об’єктів (ЦВЗ) із певними властивостями, а також, якщо об’єкти виявлені, у визначенні їх координат на площині зображення. Основний принцип лінійної регресії на зображенні полягає в зіставленні функції яскравості зображення з деяким «еталоном» – фрагментом поля яскравості, що містить шуканий об’єкт. При реалізації процедури виявлення еталон послідовно переміщається полем зображення, і в кожному положенні досліджується його схожість з реальною функцією яскравості на фрагменті. Повного збігу зразка і зображення, як правило, не буває через шуми й спотворення , а також через те, що, зазвичай, відсутня повна інформація щодо форми й структури об’єкта (доводиться використовувати еталон, що лише наближено описує об’єкт).

Оскільки ЦВЗ мають різну структуру й приховані в зображенні таким чином, щоб бути менш помітними, то для виявлення й локалізації найкраще застосовувати перцептивне хешування; виявлення об'єктів.

Етап 6 – Вилучення ЦВЗ з фрагмента. Для вилучення використовується операція, зворотна операції на етапі 3 і залежна від методу вбудовування.

Етап 7 – Виправлення помилок у ЦВЗ при добуванні. Оскільки для підвищення стійкості (робасності) рекомендується використовувати перешкодостійкі коди, наприклад, коди БЧХ, згорткові коди, то на цьому етапі відбувається виправлення викривлень в ЦВЗ.

Етап 8 – Отримання мітки правовласника. Даний етап зворотний етапу 2 й залежить від застосовуваного методу генерації ЦВЗ.

Існує ймовірність того, що декодер не виявить наявний ЦВЗ і

ймовірність помилкового знаходження ЦВЗ у порожньому контейнері (імовірність помилкової тривоги). Зниження однієї ймовірності призводить до збільшення іншої. Надійність роботи декодера характеризують імовірністю помилкового виявлення. Дана модель перевірки справжності цифрового зображення побудована таким чином, щоб мінімізувати ймовірність виникнення обох помилок, так як кожна з них може призвести до відмови від обслуговування.

2.4 Висновки за другим розділом

1. У цьому розділі представлено, класифіковано та порівняно різні алгоритми, які забезпечують сувору та часткову автентифікації. Порівняння ґрунтуються на різних критеріях, таких як виявлення, локалізація, відновлення.

2. Розглянуто автентифікацію зображення за допомогою цифрових підписів на основі вмісту зображення. Останні дослідження у сфері автентифікації зображення були зосереджені на цифрових підписах, нанесених на вміст зображення, ці підходи пропонують високу продуктивність.

3. Досліджено особливості функціональної моделі перевірки автентичності цифрового зображення. Модель перевірки автентичності цифрового зображення може розглядатися як стеганографічна система, у якій передається інтегрований зашифрований ідентифікатор в область зображення, яке є цифровим водяним знаком.

4. Розроблено комплексний критерій оцінки ефективності методів нанесення цифрових водяних знаків.

Список використаних джерел у даному розділі наведено в повному списку використаних джерел під номерами: 1, 61, 62, 70-72, 87-94.

3 УДОСКОНАЛЕННЯ МЕТОДУ НАНЕСЕННЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКУ

3.1 Генерація стійкого цифрового водяного знаку

Сучасні дослідження для створення ефективної системи водяних знаків використовують різні методи щодо вдосконалення та збалансування таких характеристик, як: стійкість, непомітність, надійність.

Зауважимо, що в роботі не накладається ніяких обмежень на вид атак, тому вимагається, щоб пропонований метод стеганографії був стійким по відношенню до втрати частини зображення, у яке додано водяний знак.

Напрямок вирішення цієї проблеми дає так звана голографічна метафора – розподілена форма представлення цифрових зображень, яка є стійкою стосовно завад [95-99].

Ідея запропонованого перетворення досить прозора: цифрове зображення розгортається в одновимірну послідовність так, щоб «далекі» точки зображення мали «близькі» номери в одновимірній послідовності.

При цьому кожній точці з координатами (m, n) на зображенні ставиться у відповідність деяке число k, яке і визначає номер даної точки в псевдоголографічній послідовності. При порядковому скануванні та запису отриманої послідовності формується «псевдоголограма».

Таке перетворення дозволяє за довільним зв’язним фрагментом отриманої послідовності реконструювати зменшену копію вихідного зображення (або, застосовуючи інтерполяційні методи, реконструювати повномасштабну апроксимацію вихідного зображення). Тобто фрагмент одновимірної послідовності подібно аналоговій голограмі містить достатньо інформації про все зображення в цілому.

Подібне «голографічне» представлення зображень є стійким по відношенню до пошкоджень даних, оскільки навіть при втраті частини інформації зображення можна відновити з певною точністю, яка залежить від

розміру втрат.

Таким чином, пропонується для зображення водяного знака проводити процедуру псевдоголографічного кодування, яка полягає в перемішуванні пікселів зображення за допомогою відомої псевдовипадкової перестановки [100]:

$$w_{perm} = w[p]. \tag{3.1}$$

де w_{perm} – результат перемішування пікселів;

p – відома псевдовипадкова перестановка.

Для отримання такої перестановки зручно скористатися алгоритмом, який полягає в генерації псевдовипадкової рівномірно розподіленої послідовності x, яка потім сортується за зростанням і приймається як перестановка p (індекси у відсортованій послідовності). Зауважимо, що доцільно розглядати лише глобальні перестановки, використання блочних перестановок вимагає виконання умови на розмір блоку, який повинен бути більшим за кореляційний радіус зображення (що в даному випадку є співмірним із розміром QR-коду) [101] .

Зауважимо, що в роботі не накладається ніяких обмежень на вид атак, тому вимагається, щоб пропонований метод стеганографії був стійким по відношенню до втрати частини зображення, у яке додано водяний знак.

При додаванні цифрових знаків (watermark) до зображень пропонується використовувати вейвлет-перетворення (Digital Wavelet Transform, DWT [102-104]. При цьому зображення-контейнер перетворюється за допомогою DWT на чотири піддіапазони: низький-високий (LH), високий-низький (HL), високий-високий (HH) та низький-низький (LL) [105]. Формально можемо це записати у вигляді:

$$\left[\mathrm{LL},\ \mathrm{HL},\ \mathrm{LH},\ \mathrm{HH}\right] = \mathrm{DWT}\left(\mathrm{f}\right), \tag{3.2}$$

де f – зображення-контейнер;

DWT – функція, яка здійснює DWT;

$\left[\mathrm{LL},\ \mathrm{HL},\ \mathrm{LH},\ \mathrm{HH}\right]$ – відповідні піддіапазони вейвлет-перетворення.

При цьому можна використовувати більшість відомих типів DWT, у роботі використовувалися вейвлети Добеши [106].

Водяний знак мультиплікативно модифікує піддіапазон LL, у якому зосереджена основна інформація про зображення:

$$\mathrm{LL}_{\mathrm{w}} = \mathrm{LL} \bullet \left(1 + \alpha \mathrm{w}\right), \tag{3.3}$$

де w – зображення-водяний знак;

LL_{w} – модифікований піддіапазон LL;

α – параметр;

оператор $\left(\bullet\right)$, який означає поелементне множення матриць. Зауважимо, що зображення з водяним знаком повинно мати вдвічі менший розмір, ніж зображення-контейнер. Вихідне зображення (із доданим водяним знаком) створюється за допомогою оберненого вейвлет-перетворення:

$$\mathrm{f}_{\mathrm{w}} = \mathrm{DWT}^{-1}\left(\left[\mathrm{LL}_{\mathrm{w}},\ \mathrm{HL},\ \mathrm{LH},\ \mathrm{HH}\right]\right), \tag{3.4}$$

де f_{w} – зображення-контейнер із доданим водяним знаком;

DWT^{-1} – функція оберненого перетворення DWT.

Для виділення цифрових водяних знаків описана вище процедура виконується у зворотному порядку:

1) аналогічно до (3.1) проводиться вейвлет-перетворення:

$$[\mathrm{LL'},\ \mathrm{HL'},\ \mathrm{LH'},\ \mathrm{HH'}] = \mathrm{DWT}(\mathrm{f_w}), \tag{3.5}$$

де $[\mathrm{LL'}, \mathrm{HL'}, \mathrm{LH'}, \mathrm{HH'}]$ – відповідні піддіапазони вейвлет-перетворення;

2) знаходиться оцінка цифрового водяного знака w' як різниця LL – піддіапазонів зображення з водяним знаком та зображення-контейнера:

$$\mathrm{w'} = \mathrm{LL'} - \mathrm{LL}, \tag{3.6}$$

3) оскільки оцінка цифрового водяного знака *w'* буде модульована LL (вирази (3.3) та (3.5)), то пропонується проводити фільтрацію зображення w' з урахуванням наявності шуму. У важливому окремому випадку, коли цифровий водяний знак є бінарним матричним кодом (наприклад, QR-код), для фільтрації можна використати такі процедури, які будуть виконуватися для кожної клітинки матричного коду w_q^1.

– бінаризація та знаходження статистичної моди по клітинці:

$$\mathrm{w}_\mathrm{q}^1 = \mathrm{mode}\left(\mathrm{w}'_\mathrm{q} > \tau_1\right), \tag{3.7}$$

де w_q^1 – результат фільтрації для першого методу;

mode – функція, що повертає значення статистичної моди;

τ_1 – поріг бінаризації;

– усереднення по бінаризованих значеннях по клітинці та подальша бінаризація:

$$\mathrm{w}_\mathrm{q}^2 = \mathrm{mean}\left(\mathrm{w}'_\mathrm{q} > \tau_1\right) > \tau_2, \tag{3.8}$$

де w_q^2 – результат фільтрації для другого методу;

mean – функція усереднення;

τ_2 – поріг бінаризації;

– усереднення по клітинці та подальша бінаризація:

$$w_q^3 = \mathrm{mean}\left(w'_q\right) > \tau_3, \tag{3.9}$$

де w_q^3 – результат фільтрації для другого методу;

τ_3 – поріг бінаризації.

Пороги бінаризації $\tau_{1,2,3}$ знаходяться по алгоритму Отсу [107] або використовуючи адаптивну бінаризацію [108].

Дане дослідження враховує основні фактори та нові методики, що використовуються потенційними дослідниками для створення надійної системи нанесення ЦВЗ на цифрові зображення.

Функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків у цифрові зображення показано на рисунку 3.1.

Рисунок 3.1 – Функціональна модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків на цифрові зображення

На рисунку 3.1 використано наступні позначення: f – зображення-контейнер, w – цифровий водяний знак, p – відома псевдовипадкова перестановка, w_{perm} – перемішаний цифровий водяний знак, f' – зображення-контейнер із доданим водяним знаком, w'_{perm} – виділений перемішаний цифровий водяний знак, w' – відновлений цифровий водяний знак зі спотвореннями.

Метод процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків у цифрові зображення описано на рисунку 3.1, де включає в себе наступні етапи:

1. Перемішування пікселів цифрового водяного знаку. Суть даного етапу полягає в тому, що за допомогою генератора псевдовипадкових чисел формується послідовність індексів $l = \{l_1, l_2, \ldots, l_{n \times m}\}$, де n, m – розмір водяного знаку w в пікселях. Після чого k-піксель водяного знаку переміщується на місце пікселя з індексом l_k. Таким чином отримуємо перемішаний відомою послідовністю цифровий водяний знак (w_{perm}).

2. Вбудова перемішаного цифрового водяного знака (w_{perm}) в зображення-контейнер із цифровим (f). На цьому етапі за допомогою будь-якого методу вбудови цифрового водяного знака відбуваються нанесення (w_{perm}). У даній роботі для нанесення цифрового знака застосовувався метод із використанням вейвлет перетворень, для представлення зображення-контейнера (f) та перемішаного цифрового водяного знака (w_{perm}) – вейвлети Добеши [106]. Після чого, використовуючи коефіцієнт LL та деякий коефіцієнт α, за допомогою формул (3.3), (3.4) здійснюється додавання частотного спектру перемішаного цифрового водяного знака (w_{perm}) в

частотний спектр зображення-контейнера (f).

3. Вилучення перемішаного цифрового водяного знака (w_{perm}) із зображення-контейнера з цифровим водяним знаком (f'). На даному етапі за допомогою формули (3.3) здійснюється вейвлет перетворення та представлення зображення в частотному спектрі. За допомогою формули (3.6) знаходиться оцінка цифрового водяного знака w' як різниця LL–піддіапазонів зображення з водяним знаком та зображення-контейнера.

4. Відновлення нормальної послідовності пікселів цифрового водяного знака. Цей етап є зворотною процедурою, представленою на першому етапі, результатом якої є отримання нормальної послідовності пікселів цифрового водяного знака.

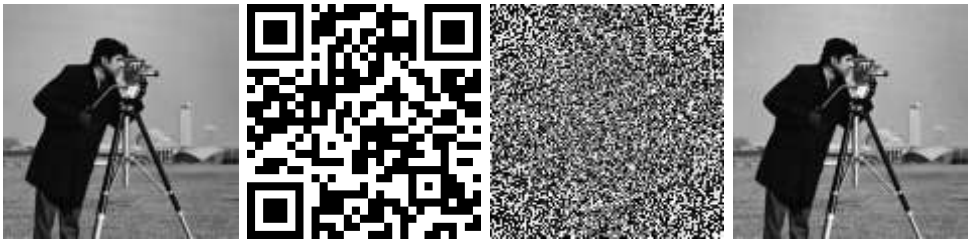
5. Використання фільтрації цифрового водяного знака. На цьому етапі для покращення цифрового водяного знака використовуються різні методи фільтрації зображення. У роботі використовувалися три методи фільтрації зображення, описані формулами (3.7)–(3.9).

У даній методиці за рахунок псевдоголографічного кодування відбувається перетворення ЦВЗ, яке є стійкою по відношенню до різного типу спотворень. Це у свою чергу в комбінації з методами фільтрації зображень після виділення ЦВЗ і відновлення нормального розподілу пікселів ЦВЗ дозволяє досягти високого рівня стійкості методів нанесення ЦВЗ при різних атаках, частково продемонстровано програмну реалізацію псевдоголаграфічного кодування в додатку А.

3.2 Експериментальне дослідження

Для експериментів в якості зображення-контейнера було використано тестове зображення в градаціях сірого Cameraman, яке представлено на рисунку 3.2, а. Для зображення цифрового водяного знака – бінарне зображення QR-code, що є матрицею 29×29 елементів, де закодовано

повідомлення «KHARKIV NATIONAL UNIVERSITY OF RADIO ELECTRONICS», яке зображено на рисунку 3.2, б. При цьому розмір зображення QR-code є 464×464 пікселів (тобто, розмір одної клітинки 16×16), Cameraman було перемасштабовано до розміру 928×928. Для отримання цифрового водяного знака пікселі зображення QR-code були перемішані за допомогою описаної вище процедури, що представлено на рисунку 3.2 в. Результат додавання цифрового водяного знаку (значення параметру α=0.1) наведено на рисунку 3.2 г.



а б в г

Рисунок 3.2 – Вхідні зображення: *а* – зображення-контейнер Cameraman; б – QR-code.; в – цифровий водяний знак (перемішаний Cameraman); г – результат додавання цифрового водяного знака

При проведенні експерименту були досліджені впливи атак таких типів:

– додавання нормально розподіленого шуму із заданим середнім і дисперсією;

– додавання шуму типу «сіль-і-перець» із заданою густиною;

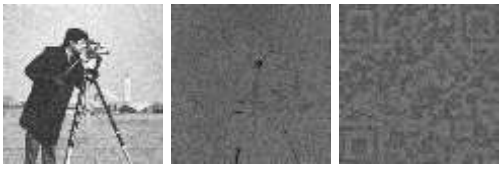
– поворот на заданий кут;

– видалення частини зображення заданого розміру;

– JPEG-компресія із заданим параметром якості.

Для кожного типу атак визначалась загальна кількість помилок у матриці QR-коду, яка отримується з виділеного цифрового водяного знака.

Досліджувався вплив нормально розподіленого адитивного шуму з середніми μ=0:0,001:0,05 і дисперсіями σ^2=0:0,001:0,05. Результати представлено на рисунках 3.3 – 3.7.



а б в

Рисунок 3.3 – Вплив нормально розподіленого адитивного шуму:
а – додавання шуму, μ=0.2, σ^2=0.25; б – виділення цифрового водяного знака;
в – відновлення правильного розташування пікселів у цифровому водяному знаку

а б

Рисунок 3.4 – Перший метод фільтрації: *а* – бінаризація зображення;
б – застосування операції статистичної моди до кожної клітинки

а б

Рисунок 3.5 – Другий метод фільтрації: *а* – усереднення бінаризованого зображення по кожній клітинці; *б* – бінаризація зображення

а б

Рисунок 3.6 – Третій метод фільтрації: *а* – усереднення зображення по кожній клітинці; *б* – бінаризація зображення

При дослідженні впливу нормально розподіленого адитивного шуму,

представленого на рисунку 3.3, можна побудувати графіки залежності кількості помилок від параметрів шуму, які продемонстровані на рисунках 3.7 – 3.9.

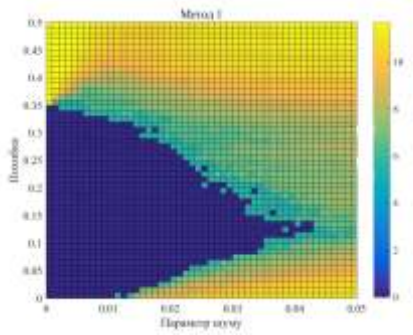


Рисунок 3.7 – Графіки залежності кількості помилок від параметрів шуму для першого методу фільтрації

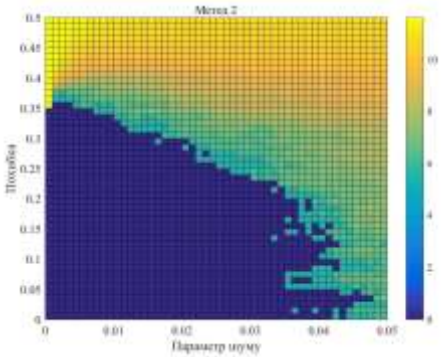


Рисунок 3.8 – Графіки залежності кількості помилок від параметрів шуму для другого методу фільтрації

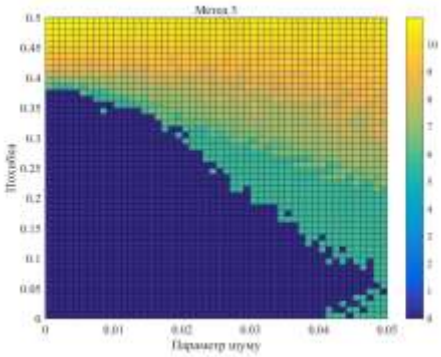


Рисунок 3.9 – Графіки залежності кількості помилок від параметрів шуму для третього методу фільтрації

Проаналізувавши графіки на рис. 3.7–3.9, можна зробити висновок, що найбільш ефективним є третій метод фільтрації, тому що, чим більше параметру шуму, тим менше похибка.

Далі досліджувався вплив шуму типу «сіль-і-перець» з густиною ρ=0:0,01:0,5. Результати наведено на рисунках 3.10 – 3.13.

а *б* *в*

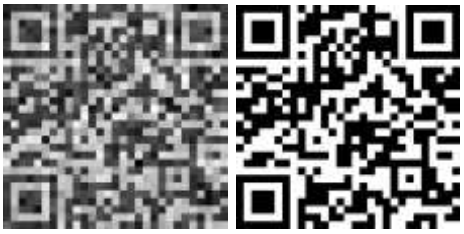
Рисунок 3.10 – Вплив нормально розподіленого адитивного шуму:
а – додавання шуму, ρ=0,15; *б* – виділення цифрового водяного знаку;
в – відновлення правильного розташування пікселів у цифровому водяному знаку

а б в

Рисунок 3.11 – Перший метод фільтрації: а – бінаризація зображення;
б – застосування операції статистичної моди до кожної клітинки; в – різниця між фільтрованим зображенням й оригінальним QR-кодом

а *б*

Рисунок 3.12 – Другий метод фільтрації: *а* – усереднення бінаризованого зображення по кожній клітинці; *б* – бінаризація зображення



а б

Рисунок 3.13 – Третій метод фільтрації: а – усереднення зображення по кожній клітинці; б – бінаризація зображення

При досліджені впливу шуму типу «сіль-і-перець», представлених на рисунках 3.10 – 3.13, можна побудувати графіки залежності кількості помилок від параметрів шуму, представленого на рисунку 3.14.

Дослідження впливу повороту зображення на цифровий водяний знак проводилося у два етапи.

На першому етапі досліджувався вплив повороту зображення на кути φ= 2°:0,1°: 2°. Результати представлено на рисунках 3.15 – 3.18.

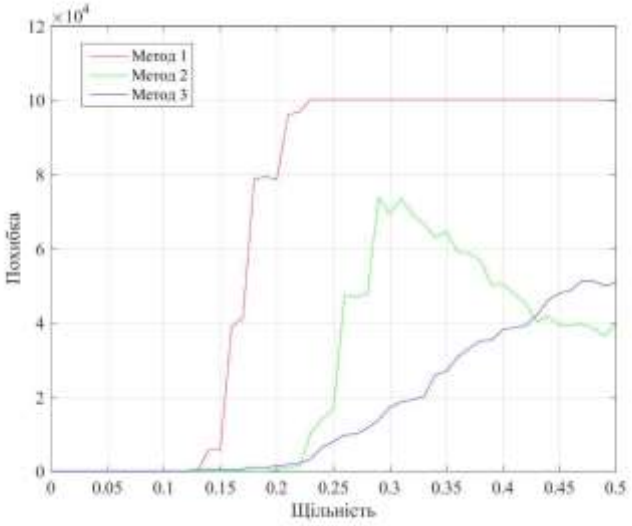


Рисунок 3.14 – Графіки залежності кількості помилок від параметрів шуму

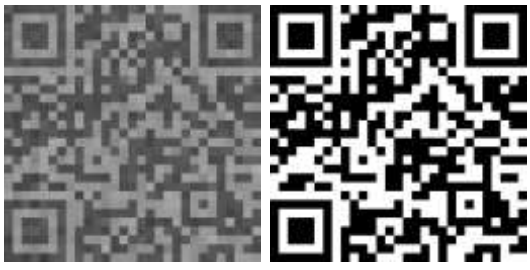
а б в

Рисунок 3.15 – Вплив нормально розподіленого адитивного шуму:
а – додавання шуму, φ=0,2°; б – виділення цифрового водяного знака;
в – відновлення правильного розташування пікселів у цифровому водяному знаку

а б

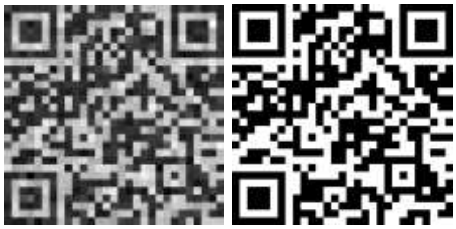
Рисунок 3.16 – Перший метод фільтрації: а – бінаризація зображення;
б – застосування операції статистичної моди до кожної клітинки

Для кожного методу фільтрації наведено графіки залежності кількості помилок від кута повороту, представлено на рисунку 3.19. Усі методи фільтрації для даного типу атаки є однаково неефективними.



а *б*

Рисунок 3.17 – Другий метод фільтрації: а – усереднення бінаризованого зображення по кожній клітинці; б – бінаризація зображення



а б

Рисунок 3.18 – Третій метод фільтрації: а – усереднення зображення по кожній клітинці; б – бінаризація зображення

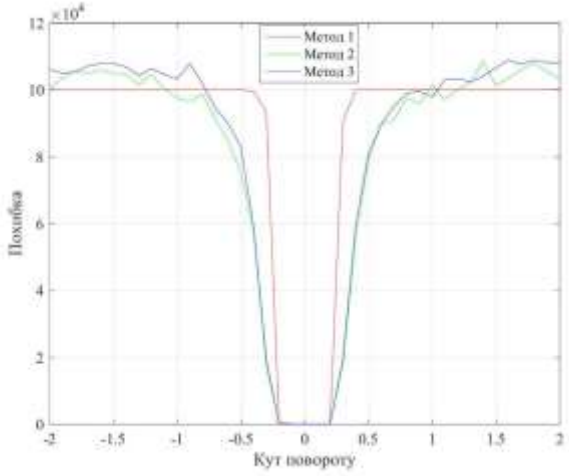


Рисунок 3.19 – Графіки залежності кількості помилок від параметрів шуму

Другий етап включає в себе дослідження використання компенсації повороту перед вилученням цифрового водяного знака з зображення-контейнера.

Щоб оцінити кут повороту, знайдемо матрицю афінного перетворення між оригінальним і повернутим зображеннями-контейнерами. Для цього на кожному із цих зображень визначимо розташування точок особливостей у якості яких будемо використовувати дескриптори ORB [109]. Зауважимо, що для детектування достатньої кількості дескрипторів ці зображення необхідно згладити за допомогою гаусівського фільтра з $\sigma=3$, це показано на рисунку 3.20.

а *б*

Рисунок 3.20 – Згладжені зображення-контейнери: *а* – оригінальне зображення; *б* – повернуте зображення, кут повороту 10°

Знаходження відповідних точок дескрипторів ORB проводиться за допомогою алгоритму RANSAC [110]. RANSAC (абр. RANdom SAmple Consensus) – це ітеративний метод, що використовується для оцінки параметрів математичної моделі для набору спостережуваних даних які містять викиди, показано на рисунку 3.21.

Знайшовши таким чином відповідні набори точок, будуємо матрицю афінного перетворення T [109]. Тоді кут повороту знаходяться із співвідношення [110]:

$$\varphi = \operatorname{atan}\frac{T_{21}}{T_{11}}. \tag{3.10}$$

Рисунок 3.21 – Знаходження відповідних точок дескрипторів Oriented FAST and Rotated BRIEF

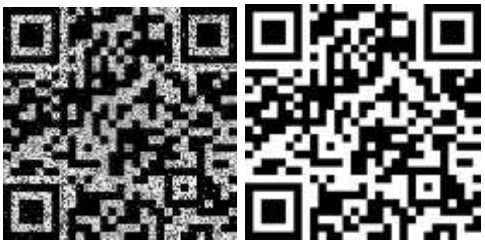
Описаний метод компенсації легко узагальнюється на інші координатні перетворення, що є перспективним напрямком подальших досліджень.

Знаючи кут повороту, повернемо зображення в протилежному напрямку, як показано на рисунку 3.22.

а б в

Рисунок 3.22 – Компенсація повороту: а – зображення-контейнер; б – виділення цифрового водяного знаку; в – відновлення правильного розташування пікселів у цифровому водяному знаку

Результати роботи повернення зображення у протилежному напрямку під певним кутом представлено на рисунках 3.23 – 3.25.



а б

Рисунок 3.23 – Перший метод фільтрації: *а* – бінаризація зображення; *б* – застосування операції статистичної моди до кожної клітинки

а б в

Рисунок 3.24 – Другий метод фільтрації: а – усереднення бінаризованого зображення по кожній клітинці; б – бінаризація зображення; в – різниця між фільтрованим зображенням й оригінальним QR кодом

а б

Рисунок 3.25 – Третій метод фільтрації: а – усереднення зображення по кожній клітинці; б – бінаризація зображення

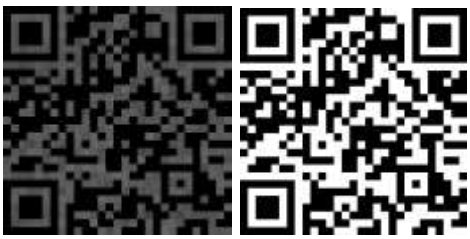
Наступним етапом було дослідження впливу видалення частини зображення – центрального квадрата зі стороною a=0:50:900. Результати показано на рисунках 3.26 – 3.29.

а б в

Рисунок 3.26 – Вплив видалення частини зображення: а – видалення центрального квадрата зі стороною a=750; б – виділення цифрового водяного знака; в – відновлення правильного розташування пікселів у цифровому водяному знаку

а б в

Рисунок 3.27 – Перший метод фільтрації: а – бінаризація зображення; б – застосування операції статистичної моди до кожної клітинки – усі результуючі значення рівні 0; в – різниця між фільтрованим зображенням і оригінальним QR-кодом



а б

Рисунок 3.28 – Другий метод фільтрації: а – усереднення бінаризованого зображення по кожній клітинці; б – бінаризація зображення

а б

Рисунок 3.29 – Третій метод фільтрації: а – усереднення зображення по кожній клітинці; б – бінаризація зображення

Для кожного методу фільтрації наведено графіки залежності кількості помилок від розмірів видаленого квадрата показано на рисунку 3.30.

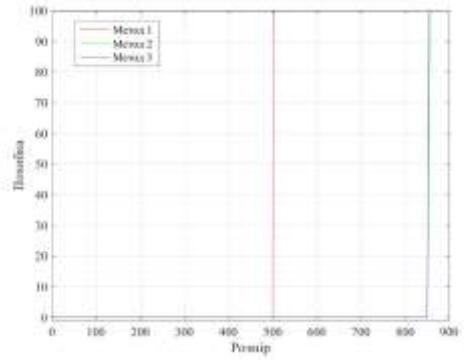


Рисунок 3.30 – Графіки залежності кількості помилок від розмірів видаленого квадрата

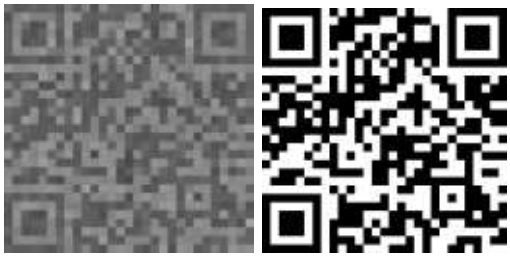
Далі досліджувався вплив компресії зображення за допомогою алгоритму JPEG у залежності від значення параметра якості q=1:100. Результати представлено на рисунках 3.31 – 3.34.

а б в

Рисунок 3.31 – Вплив JPEG-компресії зображення: а – JPEG-компресія, q=9; б – виділення цифрового водяного знака; в – відновлення правильного розташування пікселів у цифровому водяному знаку

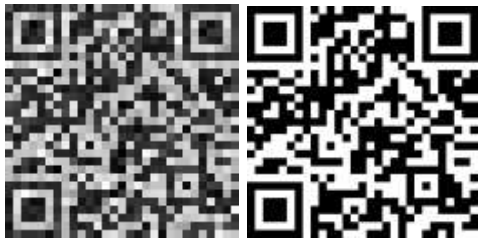
а б в

Рисунок 3.32 – Перший метод фільтрації: а – бінаризація зображення; б – застосування операції статистичної моди до кожної клітинки; в – різниця між фільтрованим зображенням і оригінальним QR-кодом



а б

Рисунок 3.33 – Другий метод фільтрації: а – усереднення бінаризованого зображення по кожній клітинці; б – бінаризація зображення



а б

Рисунок 3.34 – Третій метод фільтрації: а – усереднення зображення по кожній клітинці; б – бінаризація зображення

При досліджені впливу компресії зображення за допомогою алгоритму JPEG у залежності від значення параметра якості, представлених на рисунках 3.31 – 3.34, можна побудувати наступні графіки, які показано на рисунку 3.35.

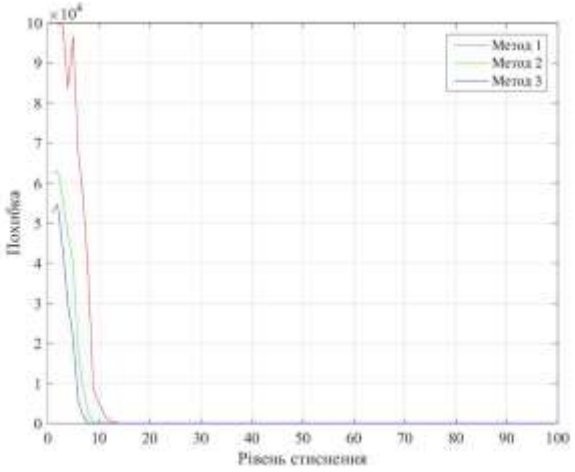


Рисунок 3.35 – Графіки залежності кількості помилок від параметра якості

Далі була проведена оцінка стійкості запропонованої методики.

При оцінці надійності запропонованої методики використовувалося п’ять типів атак:

– додавання нормально розподіленого шуму із заданим середнім і дисперсією;

– додавання шуму типу «сіль-і-перець» із заданою густиною;

– поворот на заданий кут;

– видалення частини зображення заданого розміру;

– JPEG-компресія із заданим параметром якості.

Кожен тип атак складався із 500 різних варіацій. Результати тестування наведено в таблиці 3.1.

Таблиця 3.1 – Результати оцінки надійності

Методи вбудови цифрових водяних знаків	Оцінка надійності методу нанесення цифрового водяного знака
Класичний метод нанесення цифрового водяного знака з використанням вейвлет-перетворення	0,6348
Нанесення цифрового водяного знаку на основі вейвлет-перетворення з використанням запропонованої методики	0,8344

Таким чином, виходячи з результатів, наведені в таблиці дані 3.1 свідчать, що використання запропонованої методики підвищило надійність методу на 20 %.

Вище зазначене дозволяє визначити, що запропонований метод має переваги в тому, що незалежно від методу вбудови цифрового водяного знаку буде забезпечуватися приріст стійкості.

3.3 Методи генерації стійкого до спотворень цифрового водяного знаку на основі хаотичних карт

Хаотичні карти віднесені до дискретних і безперервних часових областей. Дискретні карти зазвичай мають форму повторюваних функцій, які відповідали раундам у криптосистемах. Дана подібність між криптографією та дискретними хаотичними динамічними системами використовується для розробки хаотичних криптосистем. Кожна карта має деякі параметри, еквівалентні ключам шифрування в криптографії. У потоковому шифрі застосовується хаотична система для генерування псевдовипадкового потоку ключів, а в блокових шифрах відкритий або секретний ключ використовуються як початкові та контрольні параметри. Після цього застосовується певна кількість ітерацій до хаотичних систем для отримання зашифрованого тексту. Безпека та складність є серйозною проблемою в криптосистемах. Це слід враховувати при виборі карти та її параметрів для

використання в криптографії.

Деякі алгоритми на основі хаосу забезпечують вдале поєднання швидкості, високої безпеки та низьких обчислювальних витрат. Крім того, деякі алгоритми на основі хаосу та інші динамічні системи мають багато важливих властивостей, таких як: чутливість від вихідних параметрів, псевдовипадкові властивості, ергодичність, неперіодичність згенерованих знаків.

У роботі було розглянуто декілька типів хаотичних карт: карти кота Арнольда, карти Генона, логістичні карти хаосу зі змішуванням ключів. Це дає змогу оцінити їх можливості на предмет забезпечення стійкості ЦВЗ.

У математиці карта кота Арнольда є хаотичним відображенням з тора в себе, названа на честь Володимира Арнольда, який продемонстрував свої дослідження в 1960-х роках, використовуючи зображення кішки, звідси й назва.

Карта кота Арнольда задається перетворенням [111]:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix}, \tag{3.11}$$

де x_{n+1} та y_{n+1} обчислюються по модулю 1.

Відображення карти кота Арнольда є негамільтоновим, неаналітичним та змішувальним, однак воно зберігає площу.

1. Характеристичні показники Ляпунова задаються виразом:

$$\begin{vmatrix} 1-\sigma & 1 \\ 1 & 2-\sigma \end{vmatrix} = \sigma^2 - 3\sigma + 1 = 0,$$

звідси, (3.12)

$$\sigma_{\pm} = \frac{1}{2}(3 \pm \sqrt{5}).$$

Власні вектори знаходяться підстановкою $\sigma_{\pm}$ у матричне рівняння:

$$\begin{bmatrix} 1-\sigma_{\pm} & 1 \\ 1 & 2-\sigma_{\pm} \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{3.13}$$

Для σ_{+} рішення є:

$$y = \frac{1}{2}(1+\sqrt{5})x \equiv \phi x, \tag{3.14}$$

де ϕ – золотий перетин, тому нормований власний вектор дорівнює:

$$\xi_{+} = \frac{1}{10}\sqrt{50-10\sqrt{5}} \begin{bmatrix} 1 \\ \frac{1}{2}(1+\sqrt{5}) \end{bmatrix}. \tag{3.15}$$

Аналогічно для σ_{-} рішення є:

$$y = -\frac{1}{2}(1-\sqrt{5})x \equiv -\phi^{-1}x, \tag{3.16}$$

та нормований власний вектор дорівнює:

$$\xi_{-} = \frac{1}{10}\sqrt{50+10\sqrt{5}} \begin{bmatrix} 1 \\ \frac{1}{2}(1-\sqrt{5}) \end{bmatrix}. \tag{3.17}$$

Тобто з одиницею виміру, що дорівнює ширині квадратного зображення, воно зрізається на одну одиницю вгору, потім на дві одиниці вправо. Усе, що знаходиться за межами цього одиничного квадрата, зміщується на одиницю назад, поки не виявиться всередині квадрата.

Карта Генона, яку іноді називають атрактором/картою Енона-Помо [112], є динамічною системою з дискретним часом. Це один з найбільш вивчених прикладів динамічних систем, які демонструють хаотичну поведінку. Карта Генона бере точку (x_n, y_n) на площині й відображає її на нову точку відповідно до формули [113]:

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n \end{cases}. \quad (3.18)$$

Карта залежить від двох параметрів, a і b, які для класичного відображення Генона мають значення a=1,4 і b=0,3. Для класичних знаків відображення Генона хаотично. Для інших значень a і b карта може бути хаотичною, переривчастою або сходитися до періодичної орбіти.

Логістична карта – це одновимірна дискретна хаотична карта, яка може породжувати хаотичну поведінку з використанням простого нелінійного динамічного рівняння. Математично логістична карта обчислюється таким рівнянням [114]:

$$x_{n+1} = rx_n(1 - x_n), \quad (3.19)$$

де r (іноді також позначається μ) – позитивна константа, відома як «біотичний потенціал», дає так звану логістичну карту. Ця квадратична карта може вести себе дуже складно.

3.3.1 Аналіз хаотичних карт на предмет забезпечення стійкості цифрового водяного знака

Теорія хаосу застосовується в багатьох наукових дисциплінах: математиці, біології, інформатиці, економіці, інженерії, фінансах, філософії,

фізиці, політиці, психології та робототехніці. Теорія хаосу стверджує, що складні системи надзвичайно залежні від початкових умов і невеликі зміни в навколишньому середовищі можуть призвести до непередбачуваних наслідків.

Теорія хаосу вже багато років використовується в криптографії. Протягом останніх 10 років теорія хаосу й нелінійна динаміка використовувалися при розробці сотень криптографічних примітивів. Ці дії складаються з алгоритмів шифрування зображень, геш-функцій, безпечних генераторів псевдовипадкових чисел, потокових шифрів [115].

Для аналізу придатності застосування хаотичних карт щодо створення стійкого цифрового знака було обрано три варіанти хаотичних карт: логістична карта, карти Генона та карти кота Арнольда.

Для аналізу результатів перетворень вихідного зображення логістичними картами використали аналіз гістограми зображення та автокореляцію між сусідніми пікселями.

Аналіз гістограм зображення – один із найпростіших методів демонстрації якості шифрування. Вдалий метод шифрування зображень має тенденцію перетворювати зображення у вигляді відкритого тексту у випадкову незрозумілу форму. Таким чином, вдала методика шифрування зображень дозволяє генерувати зашифроване зображення з рівномірно розподіленою гістограмною інтенсивністю.

Оскільки зображення мають надмірність інформації, бажано використати алгоритм шифрування, який порушує цю надмірність. Таким чином, у ролі показника ефективності шифрування знаходимо кореляцію між сусідніми пікселями в потрібному напрямку (горизонтальному, вертикальному або діагональному). Розглянули горизонтальний напрямок, із зображення обираються 1024 випадкових пікселі, потім визначається кореляція пікселів між крайнім правим сусідом. Для надійного алгоритму графік кореляції може бути випадковим, без будь-якої помітної закономірності.

В якості вихідного зображення використовувалось зображенням було зображення розміром 200x200, яке представлено на рисунку 3.36. На рисунках 3.37, 3.38 представлено гістограму оригінала рисунка 3.36 за кожним каналом R , G і B відповідно та його автокореляцію між сусідніми пікселями, код програмної реалізації наведено в додатку Б

Гістограма зображення показує відносну кількість пікселів з певною яскравістю при заданій глибині кольору зображення. При цьому вважається, що по абсцисі (тобто по горизонтальній осі) відкладаються значення яскравості зображення (або сумарної, або по якомусь із каналів: наприклад, як у моделі RGB, у якій є три таких канали – R , G і B відповідно), а по ординаті (тобто вертикальної осі) відкладається відносна кількість (або навіть відсоток) пікселів з певною яскравістю.

Рисунок 3.36 – Оригінальне зображення

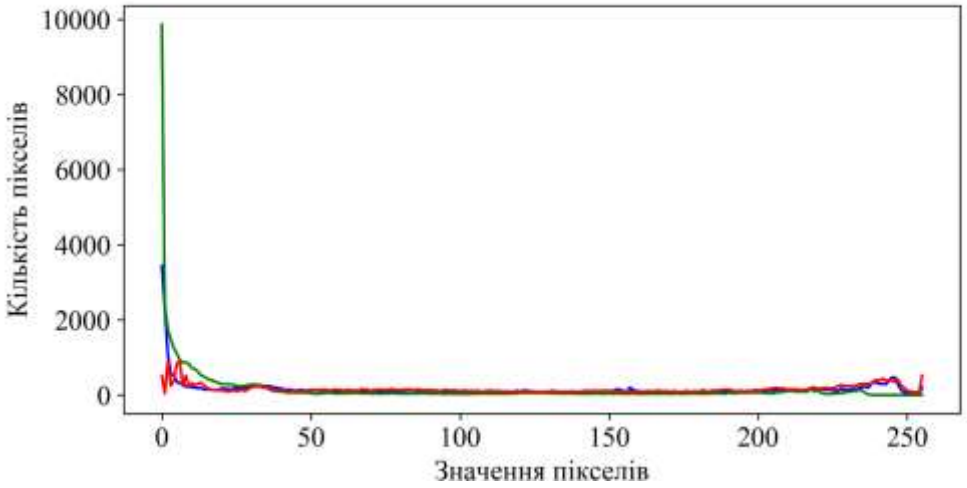


Рисунок 3.37 – Гістограма оригінального зображення

На рисунку 3.37 показано звичайний розподіл яскравості пікселів за кожним каналом окремо, а рисунок 3.38 демонструє кореляцію значення пікселів між їх правим сусідом.

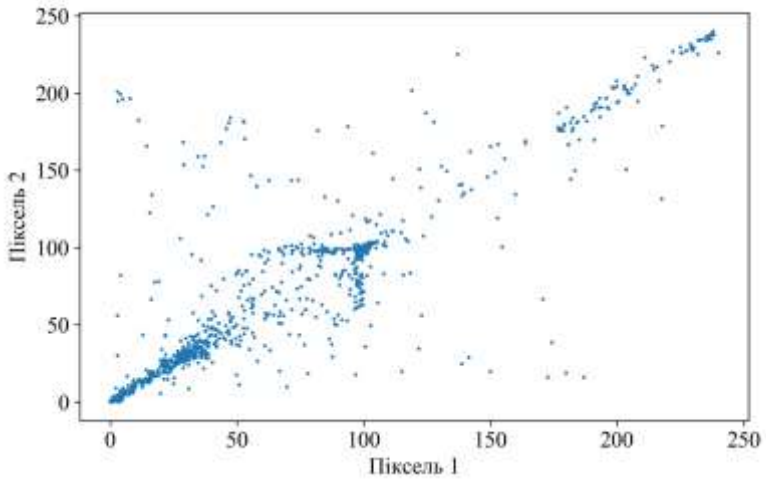


Рисунок 3.38 – Кореляція пікселів оригінального зображення та між їх крайнім правим сусідом

Першим було зашифровано зображення за допомогою карт кота Арнольда, алгоритм роботи якого має наступні кроки:

Перший крок – задати параметри для роботи алгоритму k, де k – це кількість ітерацій перемішування пікселів.

Другий крок – згідно з (3.11) перемішати кожен піксель зображення та повторити цю ітерацію k-разів.

Таким чином отримано зашифроване зображення, яке представлено на рисунку 3.39. На рисунках 3.40, 3.41 представлено гістограму зашифрованого зображення та автокореляцію між сусідніми пікселями.

Рисунок 3.39 – Зображення зашифроване за допомогою карт кота Арнольда k=44

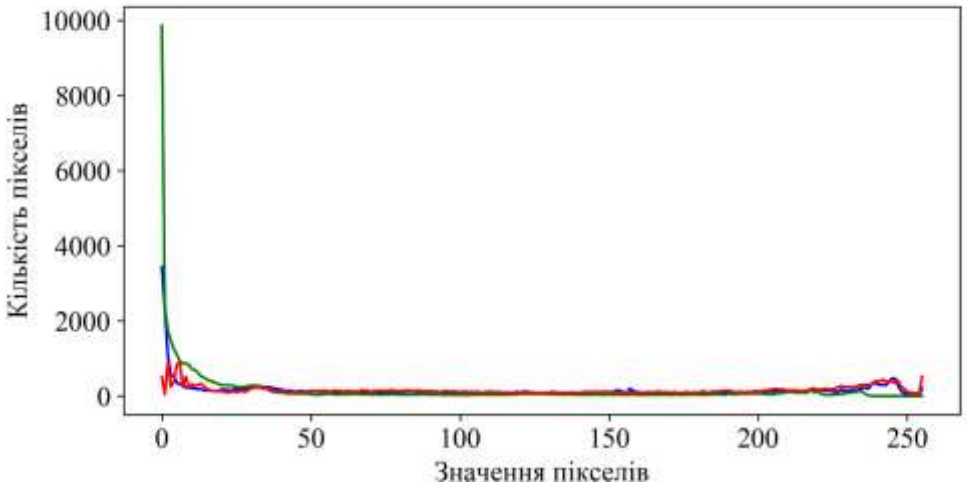


Рисунок 3.40 – Гістограма зображення після перемішування за допомогою карт кота Арнольда

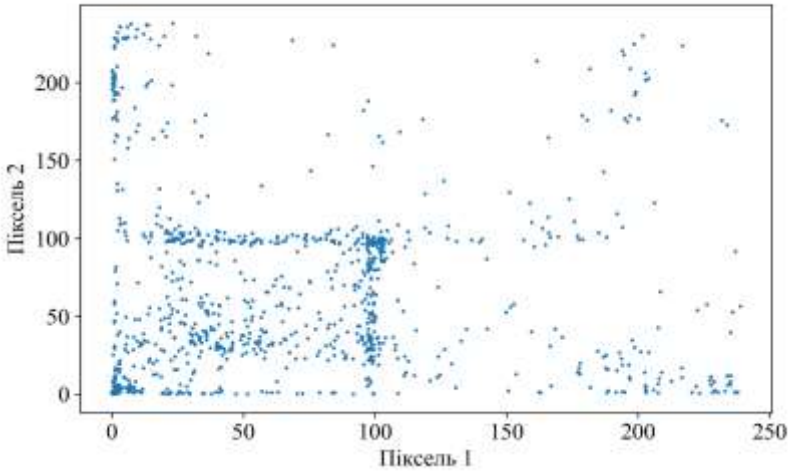


Рисунок 3.41 – Кореляція пікселів зображення після перемішування за

допомогою карт кота Арнольда

На рисунку 3.40 видно, що карти Арнольда ніяким чином не порушують розподіл яскравості пікселів, оскільки рисунки 3.37 та 3.40 однакові. Однак застосування карт кота Арнольда демонструє нам більш хаотичний розподіл пікселів у порівнянні з оригінальним зображенням, про що свідчить корелограми, показані на рисунку 3.41.

Для використання карт Генона було запропоновано наступний алгоритм шифрування зображення. Використовуючи (3.17), генерувалась послідовність біт довжиною 200*200*8, якщо xn<=0.4, то відповідний біт дорівнює 1. Після цього послідовність перетворювалась у двовимірний масив розміром 200x200, кожен елемент якого побітово складався з оригінальним зображенням. На рисунку 3.42 представлено зображення після перемішування біт пік селів, а на рисунках 3.43, 3.44 – гістограму зашифрованого зображення та автокореляцію між сусідніми пікселями.

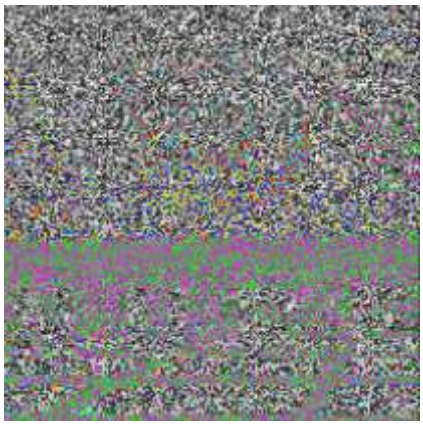


Рисунок 3.42 – Зображення зашифровано за допомогою карт Генона, початкове значення (x_0, y_0)=(1.1, 1.3)

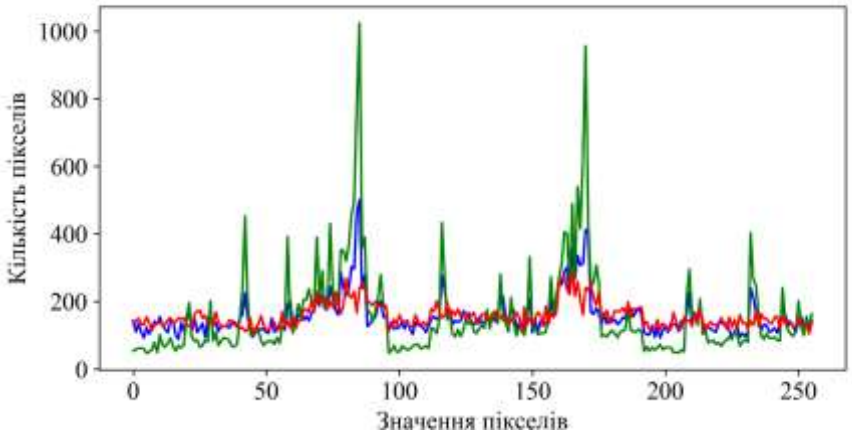


Рисунок 3.43 –Гістограма зображення після перемішування біт пікселів за допомогою карт Генона

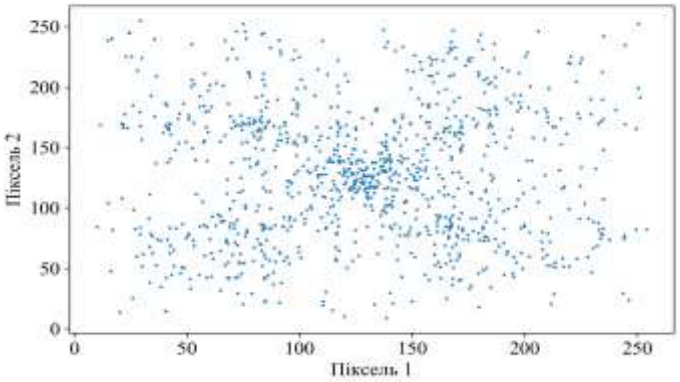


Рисунок 3.44 – Кореляція пікселів зображення після перемішування біт пікселів за допомогою карт Генона

На рисунку 3.43 видно, що карти Генона за рахунок побітового перемішування пікселів порушують розподіл яскравості пікселів, оскільки розподіл яскравості пікселів має хаотичний розподіл по всьому діапазону значень яскравості по кожному з каналів. Також можна побачити більш хаотичний розподіл пікселів у порівнянні з оригінальним зображенням, про що свідчить корелограма, представлена на рисунку 3.44.

Алгоритм на основі логістичних карт працює аналогічно з алгоритмом карт Генона, з одним лише винятком: для значення кожного пікселя послідовно за (3.19) перераховується значення і побітово додаються, таким

чином формується шифроване зображення.

На рисунку 3.45 представлено зображення після перемішування біт пікселів за допомогою логістичної карти. На рисунках 3.46, 3.47 представлено гістограму зашифрованого зображення та автокореляцію між сусідніми пікселями.

На рисунках 3.46 та 3.47 бачимо, що значення яскравості пікселів зображення мають хаотичний характер розподілу й жодним чином не корелюються між собою.

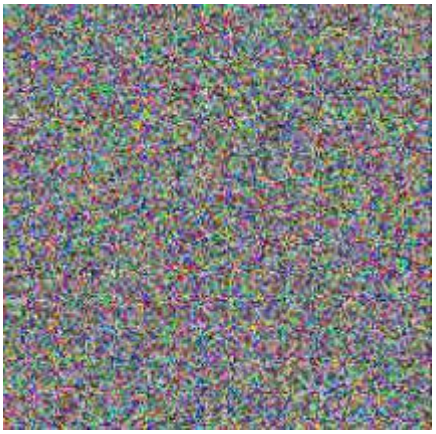


Рисунок 3.45 – Зображення зашифроване за допомогою логістичних карт

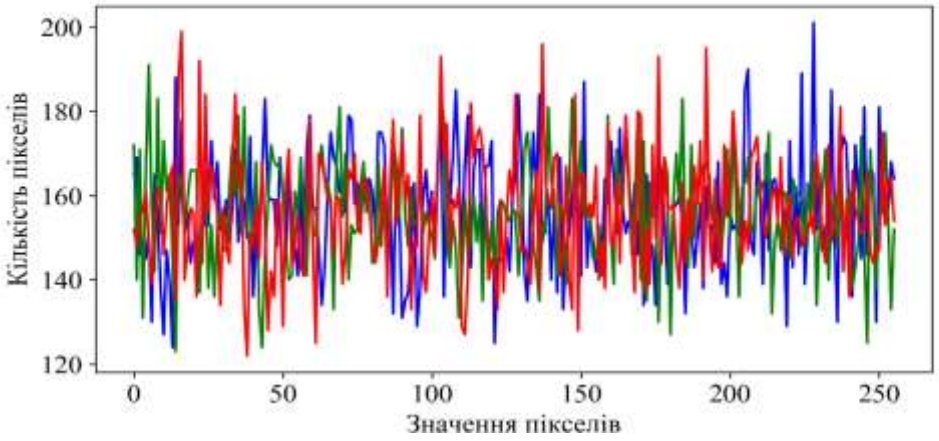


Рисунок 3.46 – Гістограма зображення після перемішування біт пікселів за допомогою логістичних карт

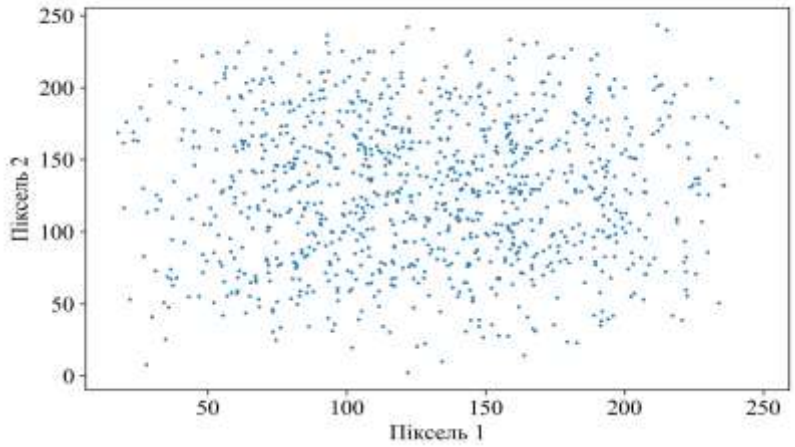


Рисунок 3.47 – Кореляція пікселів зображення після перемішування біт пікселів за допомогою логістичних карт

Таким чином, проаналізувавши результати використання різних за природою типів хаотичних карт, робимо наступні висновки:

- карти кота Арнольда завдяки просторовим змінам у розташуванні пікселів забезпечують стійкість до локальних спотворень. Але за рахунок того, що карти кота Арнольда ніяким чином не порушують розподіл яскравості пікселів, буде страждати непомітність вбудови такого ЦВЗ у контейнер;

- карти Генона й логістичні карти навпаки унаслідок хаотичного розподілу яскравості пікселів можуть забезпечити непомітність такого ЦВЗ після вбудови, оскільки такий ЦВЗ у контейнері буде виглядати як адитивний шум.

3.3.2 Принципи використання хаотичних карт для методів генерації цифрових водяних знаків

Проаналізувавши стан останніх досліджень, описаних вище, та враховуючи сучасні тенденції у сфері захисту інформації, пропонуємо для ідентифікації користувачів використовувати застосовувати/упроваджувати технологію токенізації.

Токенізація – це процес перетворення конфіденційних даних у нечутливі, так звані «токени», які використовують у базі даних або внутрішній системі, не вводячи їх в область видимості. Токенізація може застосовуватися для захисту конфіденційних даних шляхом заміни вихідних даних непов'язаними значеннями тієї ж довжини і формату. Потім токени відправляються у внутрішні системи організації для використання, а вихідні дані зберігаються в безпечному сховищі токенів. На відміну від зашифрованих, токенізовані дані не піддаються розшифруванню та є незворотними. Ця різниця особливо важлива: оскільки немає математичного зв'язку між токеном і його вихідним номером, токени не можуть бути повернуті в їх вихідну форму [116].

Для досягнення непомітності нанесення ЦВЗ на цифровий контент бажано використовувати ЦВЗ, яке однакове за природою з об'єктом вбудови [111, 117], тому пропонується токен правовласника перетворювати в один з різновидів QR-коду. Це потрібно для того, щоб токен представити у вигляді зображення, тим самим забезпечити непомітності нанесення ЦВЗ на зображення.

Представлено два методи генерації ЦВЗ, принцип яких схожий. Відрізняються вони складністю приватних ключів та обчислювальною складністю, хоча й мають однаковий загальний принцип.

Метод генерації стійкого ЦВЗ буде складатися з двох частин: блоку генерації та шифрування ЦВЗ і блоку розшифрування ЦВЗ та додаткової фільтрації – та має наступні кроки:

Крок 1 – ініціалізація параметрів методу P, Q – параметри для перемішування зображення за допомогою карт кота Арнольда, k – це кількість ітерацій перемішування пікселів, (x, y) – параметри для генерації масиву бітових масок за допомогою карт Генона. Ініціалізація унікального токену зображення та розміру самого ЦВЗ.

Крок 2 – генерація QR-коду на основі токену та його розміщення на зображені ЦВЗ.

Крок 3 – перемішування ЦВЗ *k* разів, використовуючи вираз (3.20).

Крок 4 – використовуючи (3.18), генерується послідовність біт довжиною m*m*8, якщо x_n<=0.4, то відповідний біт дорівнює 1, де m – розмір у пікселях ЦВЗ Після цього послідовність перетворювалась на двовимірний масив розміром m x m.

Крок 5 – кожен елемент масиву бітових масок, який був отриманий на кроці 4, побітово складається з перемішаним ЦВЗ, який було отримано на кроці 3. У результаті отримуємо ЦВЗ.

Процес розшифрування включає в себе наступні кроки:

Крок 1 – ініціалізація параметрів методу P, Q – параметри для перемішування зображення за допомогою карт кота Арнольда, k – це кількість ітерацій перемішування пікселів, (x, y) – параметри для генерації масиву бітових масок за допомогою карт Генона. Ініціалізація ЦВЗ.

Крок 2 – перемішування ЦВЗ k разів, використовуючи вираз (3.20).

Крок 3 – використовуючи (3.18), генерується послідовність біт довжиною m*m*8, якщо x_n<=0.4, то відповідний біт дорівнює 1, де m – розмір у пікселях ЦВЗ Після цього послідовність перетворювалась на двовимірний масив розміром mxm.

Крок 4 – кожен елемент масиву бітових масок, який був отриманий на кроці 3. Метод заснований на картах перемішаним ЦВЗ, який було отримано на кроці 2.

Крок 5 – вилучення розміщених на ЦВЗ QR-кодів.

Крок 6 – побітове складання отриманих з попереднього кроку QR-кодів та фільтрація отриманого QR-коду.

Крок 7 – сканування QR-коду та отримання токену зображення.

Блок генерації та шифрування представлено на рисунку 3.48.

Рисунок 3.48 – Структурна схема блоку генерації та шифрування

Даний метод базується на картах Генона та кота Арнольда. На вхід методу подаються токен зображення, розмір ЦВЗ, початкові координати (x, y) для генерації масиву бітових масок та параметрів для перемішування зображення – кількість ітерацій перемішування k та параметри (3.20) P, Q.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & P \\ Q & PQ+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(m). \qquad (3.20)$$

Процес генерації ЦВЗ включає в себе генерацію QR-коду на основі токену та його розміщення на зображенні ЦВЗ, розмір якого повинен бути більшим за розмір QR-коду. Дана процедура потрібна для того, щоб забезпечити додаткову стійкість до певного типу атак на ЦВЗ, тому використовується на етапі додаткової фільтрації. Наприклад, QR-код, згенерований на основі токену, має розмір 40x40 пікселів, а вимога до розміру ЦВЗ свідчить про те, що розмір ЦВЗ повинен бути 200x200 пікселів. Отже, необхідно розмістити 4 копії QR-коду на ЦВЗ і цим самим забезпечити додаткову стійкість до спотворень. Крім того, можна використати це для

додаткової фільтрації ЦВЗ після розшифрування зображення та збільшити вірогідність безпомилкового розшифрування токена зображення.

Процес фільтрації складеться з двох етапів:

1) перемішування пікселів зображення k – a разів (3.20), чим забезпечується стійкість всього ЦВЗ до локальних змін;

2) перемішування біт кожного пікселя окремо. Це дозволяє забезпечити захищеність ЦВЗ.

Блок розшифрування ЦВЗ та додаткової фільтрації представлено на рисунку 3.49.

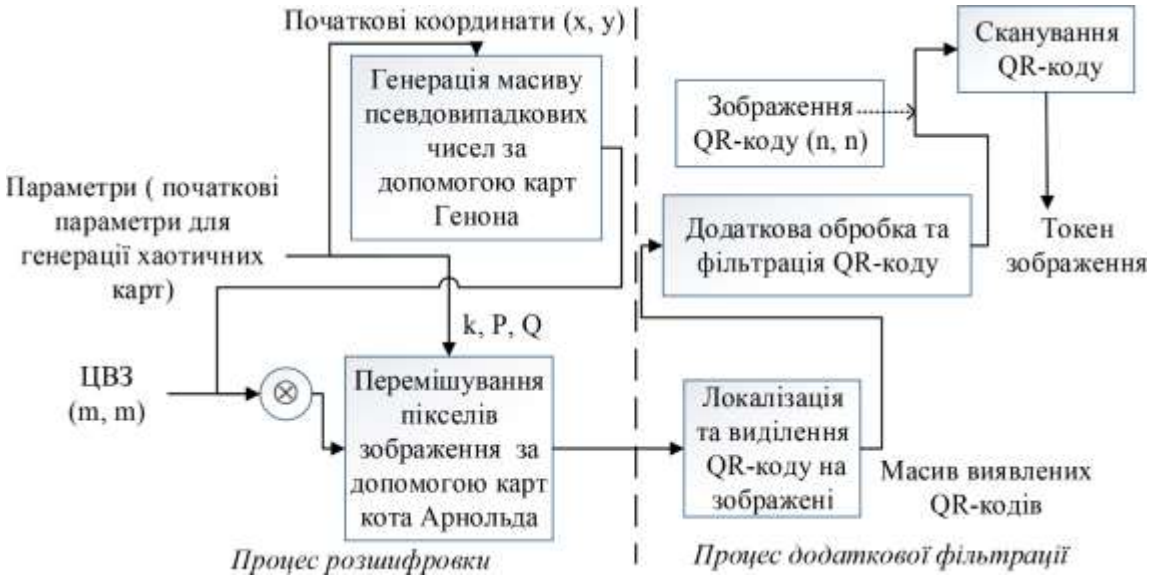


Рисунок 3.49 – Структурна схема блоку розшифрування та додаткової фільтрації

Для розшифрування та отримання токену на вхід подається зображення ЦВЗ та параметри для генерації карт Генона (3.20) та для зворотного перемішування зображення за допомогою карт кота Арнольда. У якості останніх береться k – кількість ітерацій перемішування; P, Q – параметри (3.21), за допомогою яких відбувається зворотна операція перемішування пікселів зображення.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} PQ+1 & -P \\ -Q & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \mathrm{mod}(m). \quad (3.21)$$

Процес розшифрування включає в себе спочатку використання побітової маски для кожного пікселя зображення, а потім, відповідно до (3.21), зворотну операцію перемішування, яка виконуються k-а разів.

Процес додаткової фільтрації включає в себе локалізацію всіх екземплярів QR-кодів. Якщо знайдено більше, ніж один QR-код, то можна побітово скласти кожен піксель й отримане зображення відфільтрувати.

Як метод фільтрації пропонується використовувати усереднення по клітинці та подальшу бінаризацію. Цей фільтр було обрано на основі проведених раніше досліджень, про що свідчать результати, розглянуті в роботі [118].

Поріг бінаризації τ визначають, застосовуючи алгоритм Отсу або використовуючи адаптивну бінаризаціїю [108].

Другий метод генерації ЦВЗ схожий за принципом з першим, але процес перемішування пікселів і бітів окремого пікселя відбувається одночасно на основі карт кота Арнольда та має наступні кроки:

Крок 1 – ініціалізація параметрів методу P, Q – параметри для перемішування зображення за допомогою карт кота Арнольда, k – це кількість ітерацій перемішування пікселів. Ініціалізація унікального токену зображення та розміру самого ЦВЗ.

Крок 2 – генерація QR-коду на основі токену та його розміщення на зображені ЦВЗ.

Крок 3 – перемішування пікселів ЦВЗ, використовуючи вираз (3.20) k разів, та перемішування біт пікселів, використовуючи алгоритм, зображений на рисунку 3.52. У результаті отримуємо необхідний ЦВЗ.

Процес розшифрування включає в себе наступні кроки:

Крок 1 – ініціалізація параметрів методу P, Q – параметри для перемішування зображення за допомогою карт кота Арнольда, k – це

кількість ітерацій перемішування пікселів. Ініціалізація ЦВЗ.

Крок 2 – перемішування ЦВЗ k разів, використовуючи вираз (3.21), та перемішування біт пік селів, використовуючи алгоритм, зображений на рисунку 3.52, у якому замість формули (3.20) використовується формула (3.21) .

Крок 3 – вилучення розміщених на ЦВЗ QR-кодів.

Крок 4 – побітове складання отриманих із попереднього кроку QR-кодів та фільтрація отриманого QR-коду.

Крок 5 – сканування QR-коду та отримання токену зображення.

На рисунках 3.50, 3.51 представлено процес генерації та розшифрування ЦВЗ, а на рисунку 3.52 – алгоритм процесу перемішування.

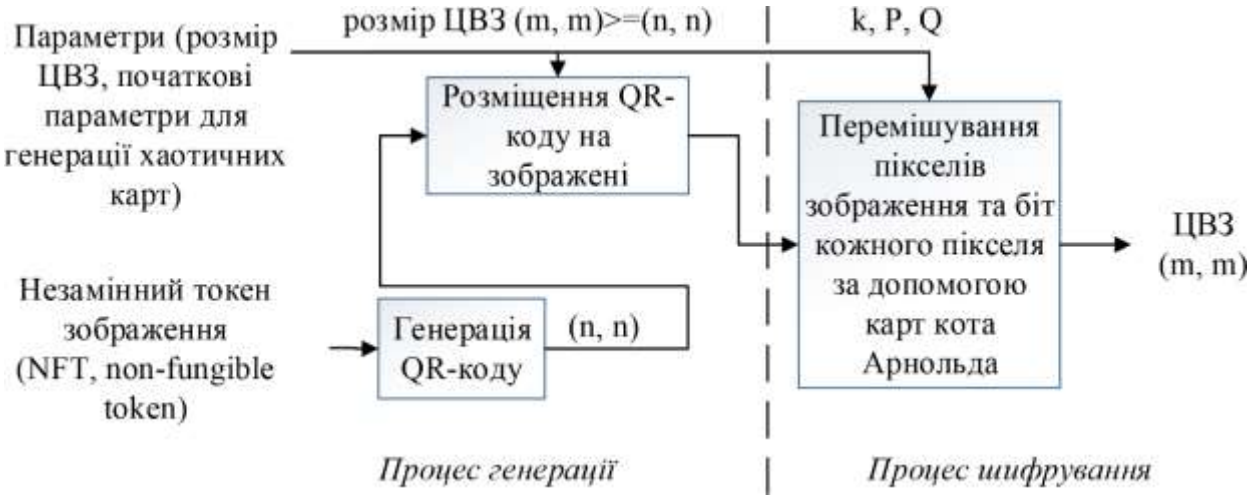


Рисунок 3.50 – Генерація цифрового водяного знаку на основі карт кота Арнольда

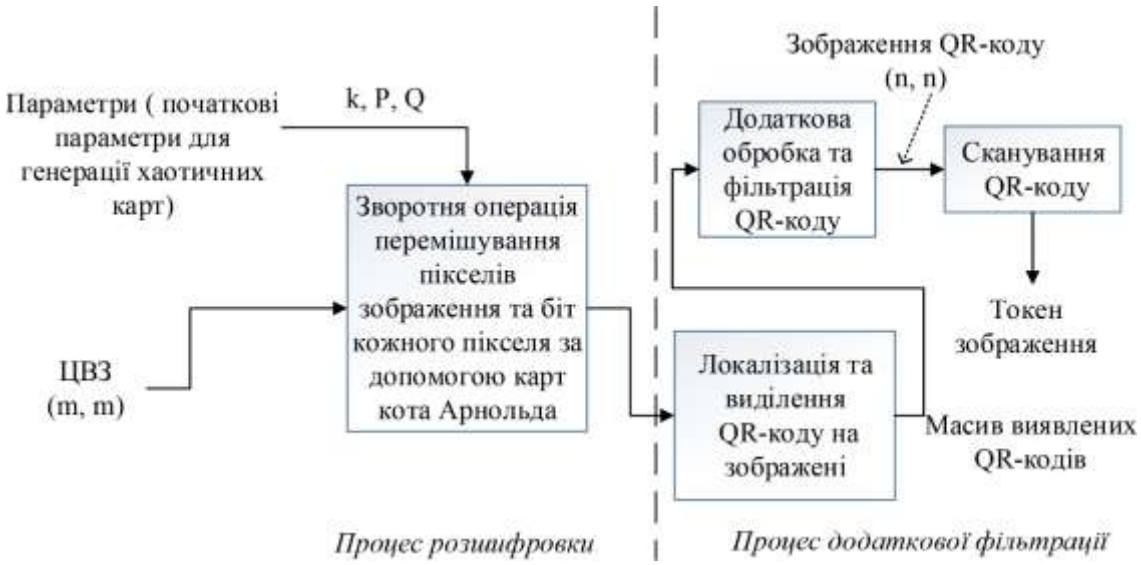


Рисунок 3.51 – Розшифровка цифрового водяного знаку на основі карт кота Арнольда

Алгоритм зворотного перемішування працює аналогічно алгоритму, представленому на рисунку 3.52, але замість (3.20) використовується (3.21), а відновлення біт кожного пікселя розраховується за формулою:

$$img\_arnold[x', y'] = Image[x, y] \oplus ((x + y) * (k - i) \bmod 256) \qquad (3.22)$$

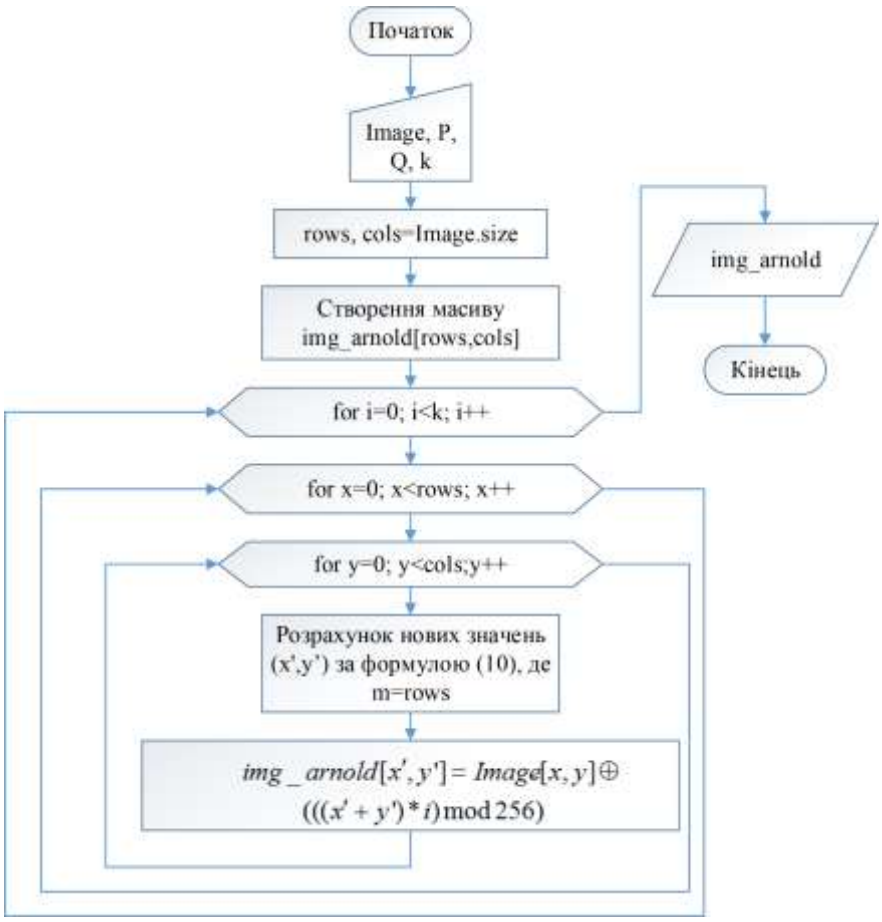


Рисунок 3.52 – Алгоритм перемішування пікселів зображення та біт пікселів

Даний метод генерації ЦВЗ має меншу обчислювальну складність і, при відносно простих значеннях, ключа володіє високим рівнем захищеності.

3.3.3 Експериментальне дослідження методів генерації цифрового водяного знака

Для проведення експериментів було згенеровано токен для зображення, показаний на рисунку 3.36. Структура токена продемонстрована на рисунку 3.53.

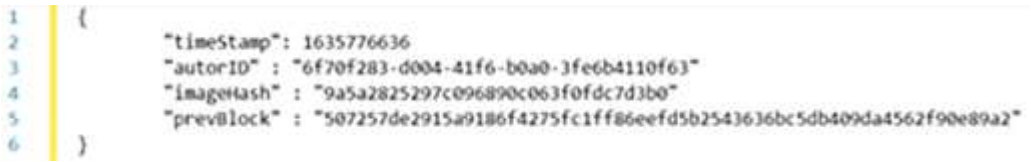
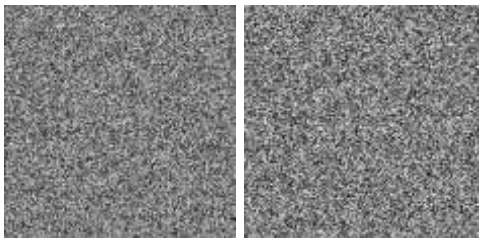


Рисунок 3.53 – Структура токена зображення

На основі цього токену було згенеровано QR-код з розмірами 159x159, який згідно із запропонованим методом було розміщено по центру на ЦВЗ, який має розмір 200x200. Даний ЦВЗ представлено на рисунку 3.54.

Рисунок 3.54 – Згенерований QR-код токену та розміщений на цифровому водяному знаку

Наступний крок алгоритму – це перемішування ЦВЗ. На рисунку 3.55 *а* представлено перемішування за допомогою карт кота Арнольда та карт Генона, а на рисунку 3.55 *б* – перемішування з використанням лише карт кота Арнольда.



а *б*

Рисунок 3.55 – Цифровий водяний знак після перемішування: *а* перемішування за допомогою карт кота Арнольда та карт Генона (x, y)=(1.1,1.3), P=2, Q=1, k=5; *б* – перемішування за допомогою карт кота Арнольда P=2, Q=1, k=5

Для аналізу захищеності методів генерації було побудовано гістограми зображень ЦВЗ рисунок 3.56, ЦВЗ після перемішування рисунках 3.57, 3.58.

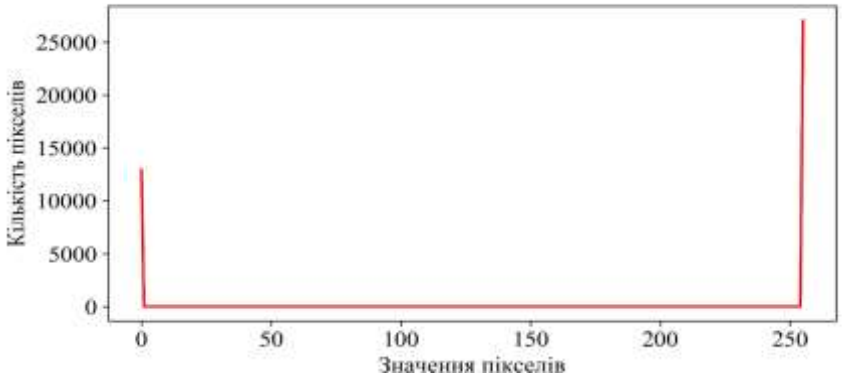


Рисунок 3.56 – Гістограма цифрового водяного знаку зображеного на рисунку 3.54

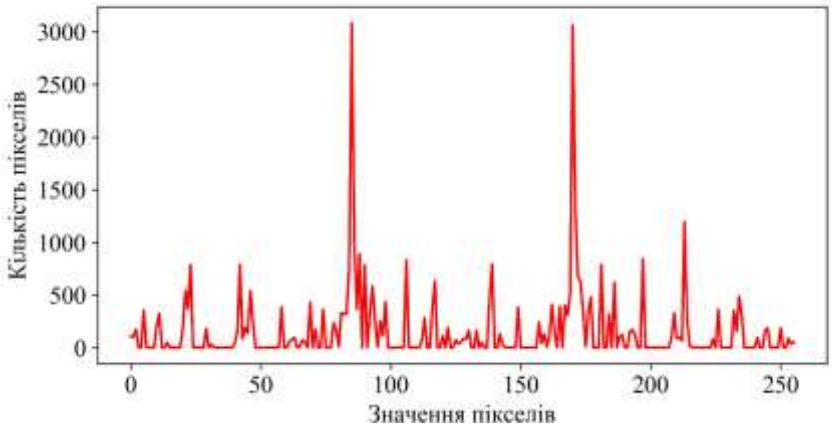


Рисунок 3.57 – Гістограма цифрового водяного знаку після перемішування за допомогою карт кота Арнольда та карт Генона рисунку 3.55 а)

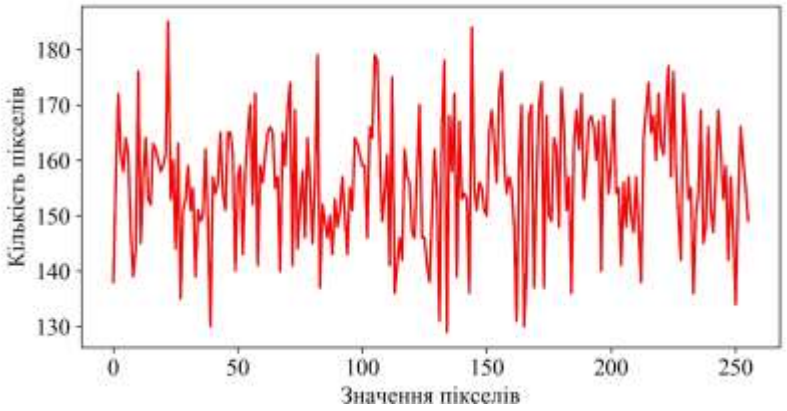


Рисунок 3.58 – Гістограма цифрового водяного знаку після перемішування за допомогою карт кота Арнольда рисунку та карт Генона рис. 3.55 (б)

В якості показника ефективності шифрування знаходимо кореляцію між сусідніми пікселями в горизонтальному напрямку. Із зображення обираються 1024 випадкових пікселі, і визначає та відображає його кореляція між крайнім правим сусідом. На рисунку 3.59 діаграма кореляції ЦВЗ, зображеного на рисунку 3.54. На рисунках 3.60, 3.61 кореляція після перемішування.

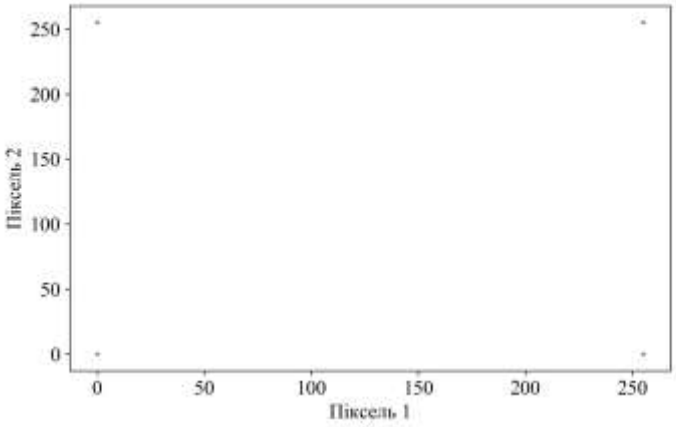


Рисунок 3.58 – Кореляція пікселів цифрового водяного знаку зображеного на рисунку 3.54

Для демонстрації стійкості методу формування ЦВЗ побудовано графік відношення відсотка видалених пікселів до відсотка некоректно відновлених пікселів вихідного ЦВЗ, представленого на рисунку 3.61.

У таблиці 3.2 представлено значення коефіцієнтів кореляції для кольорового та бінарного зображень (QR-коду).

Таблиця 3.2 – Значення коефіцієнта кореляції для сусідніх пікселів

Вид перетворення	Кольорове зображення	Бінарне зображення
Оригінальне	0.877	0.73
Карти Арнольда	0.034	0.052
Карти Генона	0.027	0.038
Логістичні карти	0.005	0.034
Карти Арнольда + Генона	0.011	0.028
Карти Арнольда +Арнольда	0.0109	0.030

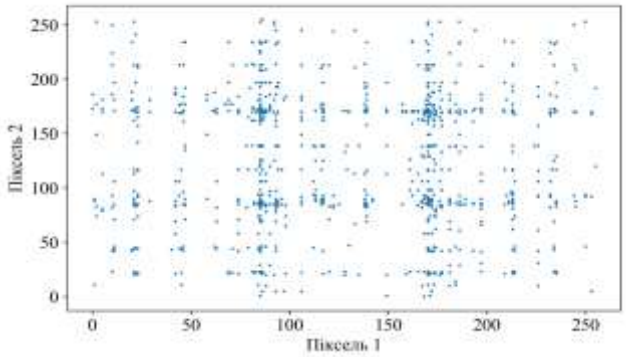


Рисунок 3.59 – Кореляція пікселів цифрового водяного знака після перемішування за допомогою карт кота Арнольда та карт Генона на рисунку 3.55 а)

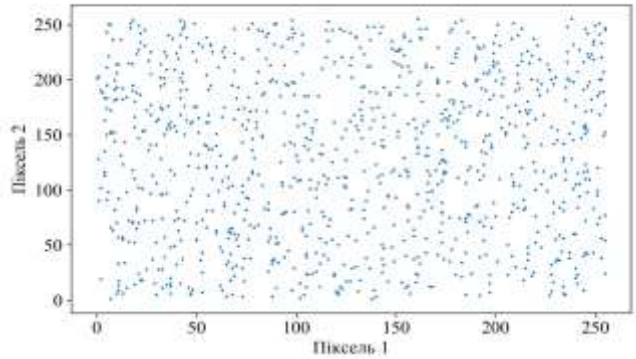


Рисунок 3.60 – Кореляція пікселів цифрового водяного знака після перемішування за допомогою карт кота Арнольда на рисунку 3.55 б)

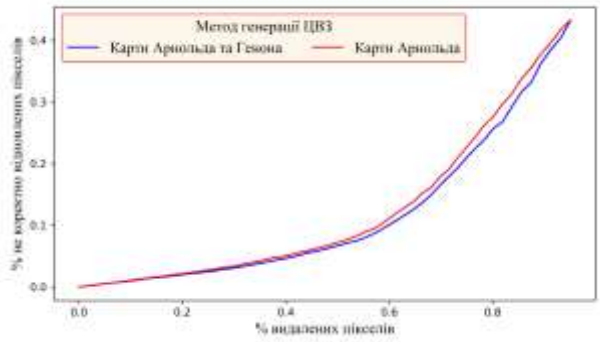


Рисунок 3.61 – Графік залежності втрачених пікселів до коректно відновлених

На рисунку 3.61 видно, що обидва методи генерації ЦВЗ при втраті 60 % пікселів забезпечують коректне відновлення майже 90 % пікселів.

Для аналізу результатів роботи методів проаналізовано гістограми ЦВЗ, які представлені на рисунках 3.56 – 3.58. Із гістограм, наведених на рисунках 3.59 – 3.60, видно що обидва методи забезпечують генерацію ЦВЗ випадкової незрозумілої форми. Але метод, заснований на комбінації карт кота Арнольда та карт Генона, що представлені на рисунках 3.57, 3.58, має помітні піки, на відміну від метода, який заснований на перемішуванні пікселів та їх біт тільки за допомогою карт кота Арнольда. Це свідчить про те, що метод, представлений на рисунках 3.50 – 3.52, має більш хаотичний характер.

Переглянувши таблицю 3.2 можемо зробити висновок, що обидва методи забезпечують прийнятний рівень захищеності, оскільки коефіцієнт кореляції між сусідніми пікселями відносно малий. Отже, статистично виявити такий ЦВЗ після вбудови майже неможливо, не кажучи вже про його розшифрування без точних значень ключа.

Розглянувши графік, зображений на рисунку 3.61, можемо сказати, що обидва методи є достатньо стійкими до спотворень пікселів локального характеру. Оскільки при 60 % знищення ЦВЗ можемо відновити майже 90 % QR-коду.

На відміну від методів генерації ЦВЗ, представлених у роботах [119,120] за ідентифікатор права власності використовується токен, для генерації якого можна використовувати алгоритм консенсуса Proof-of-Work. На відміну від біометричних даних це не потребує додаткового обладнання й забезпечує захист розподілених систем від зловживань. У роботі [117] в якості ЦВЗ використовується QR-код, але запропоновані методи за рахунок перемішуванню та додатковій фільтрації позбавлені недоліків звичайних QR-кодів, які детально розглянуті в роботі [118] .

Для забезпечення стійкості ЦВЗ було запропоновано перемішування

пікселів зображення, оскільки хаотичність розташування пікселів забезпечує нам стійкість до локальних змін самого ЦВЗ. Проаналізувавши отримані результати, продемонстровані на рисунках 3.54 – 3.61, можна зробити висновок, що запропоновані методи генерації ЦВЗ здатні забезпечити приріст стійкості методів вбудови ЦВЗ.

В якості обмеження запропонованих методів можна зазначити, що розмір генерованого QR-коду на основі токену зображення повинен бути меншим або дорівнювати розміру ЦВЗ. Це призведе або до неуможливлення використання представлених методів з даним методом токенізації, або до перегляду вимог до самого ЦВЗ.

Недоліком запропонованих методів можна вважати те, що один із механізмів, за допомогою яких досягається стійкість до спотворень, є надмірність інформації. Тому для подальшого розвитку запропонованих методів та технологій захисту авторських прав планується проведення досліджень із використанням кодів, які здатні виправляти помилки.

3.4 Висновки за третім розділом

1. Розроблена функціональна модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків у цифрові зображення основана на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знака. Описаний у роботі метод псевдоголографічного кодування цифрових водяних знаків є ефективним для протидії усім типам атак, що розглядалися, окрім повороту зображення. Проведення комплексної оцінки методики підвищення стійкості методу вбудови цифрового водяного знака на основі вейвлет-перетворення показало, що її використання на 20 % покращує стійкість до різних типів атак.

2. У роботі представлено показник оцінки стійкості методів нанесення цифрових водяних знаків, який враховує всі типи атак і дозволяє провести комплексну оцінку стійкості методу вбудови цифрових водяних знаків.

3. Проведено експериментальне дослідження щодо запропонованої методики. Найбільш ефективною ця методика є при втраті частини зображення. При попередній фільтрації ЦВЗ найбільш ефективним є третій метод фільтрації, який полягає в усередненні по клітинці й подальшій бінаризації. Найменш ефективним є перший метод бінаризації та знаходження статистичної моди по клітинці. Бінаризацію доцільно проводити за алгоритмом Отсу. Для атаки афінного типу, що представляє собою поворот зображення, даний метод є буде ефективним за умови компенсації повороту. Для оцінки кута повороту знаходиться матриця афінного перетворення, що отримується по узгодженому набору відповідних ORB-дескрипторів. Використання цього методу дозволяє безпомилково виділяти цифровий водяний знак для всього діапазону кутів, що досліджувалися.

4. Проведено аналіз хаотичних карт на предмет забезпечення стійкості ЦВЗ, який показав, що використання хаотичних карт для перемішування біт пікселів або самих пікселів на зображенні можуть забезпечити захищеність та стійкість до спотворень. Розрахунки коефіцієнта кореляції сусідніх пікселів при використанні хаотичних карт свідчать про їх ефективність. Оскільки зображення мають високу надмірність інформації, бажано мати алгоритм, який порушить її.

5. Розроблено методи генерації ЦВЗ на основі хаотичних карт та додатковій фільтрації цифрового водяного знаку. Описані у роботі методи є ефективними для забезпечення стійкості ЦВЗ до локальних спотворень. Як показали дослідження, при 60 % спотворення зображення можливо відновити 90 % ЦВЗ.

6. Проведено експериментальне дослідження щодо запропонованих методів. Гістограми ЦВЗ показали, що обидва методи забезпечують генерацію ЦВЗ випадкової незрозумілої форми. Але метод, заснований на комбінації карт кота Арнольда на карт Генона, має помітні піки на відміну від метода, який заснований на перемішуванні пікселів та їх біт лише за

допомогою карт кота Арнольда. Це свідчить про те, що метод, заснований тільки на картах кота Арнольда, має більш хаотичний характер. Про це також свідчить і значення коефіцієнта кореляції між сусідніми пікселями, який наближається до 0 і дорівнює 0.0109 для кольорових ЦВЗ та 0.030 для чорно-білих зображень.

Список використаних джерел у даному розділі наведено у повному списку використаних джерел під номерами: 95-120.

4 ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ ПІДТВЕРДЖЕННЯ ПРАВА ВЛАСНОСТІ НА ЦИФРОВІ ЗОБРАЖЕННЯ

4.1 Інформаційна технологія підтвердження права власності на цифрові зображення

У сучасному світі зображення стає потужнішим засобом спілкування. В епоху діджиталізації люди мають змогу виражати свої думки, почуття та інше у вигляді зображень. Презентації, слайд-шоу тощо документуються у вигляді електронних копій. Багато користувачів публікують в інтернеті свої фотографії, у соціальних мережах, в особистих блогах, на корпоративних сайтах, фотобанках, надсилають електронною поштою. Щодня записуються мільрди фотографій та відео [7]. Більшість з них призначені для спільного використання в соціальних мережах і збереження пам'яті, але все більше використовуються нові застосування, такі як доповнена реальність і штучний інтелект. Згідно звіту Keypoint Intelligence у 2020 році населення світу зробило 1,44 трильйона фотографій, при цьому в 2023 році загальна кількість фотографій може перевищити 1,6 трильйона фотографій, представлено на рисунку 4.1 [15].

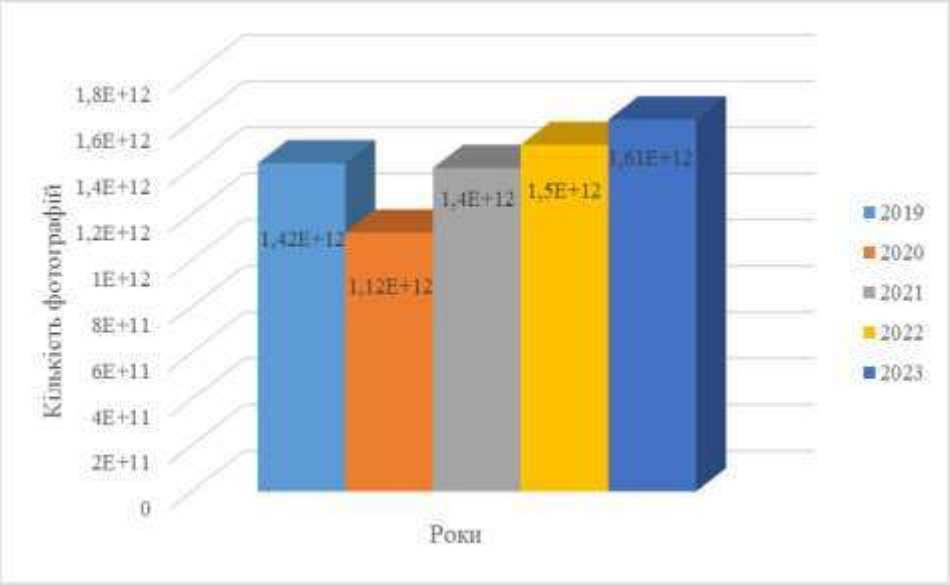


Рисунок 4.1 –Кількість зроблених фотографій у світі

Реєстрація авторських прав не впливає на факт їх виникнення, оскільки вони виникають із моменту створення твору. Проте ця процедура дозволяє додатково зафіксувати факт створення твору, особу автора та передати державі копію твору для публічного зберігання. У деяких юрисдикціях, наприклад у США, реєстрація авторських прав впливає на обсяг процесуальних прав позивача при захисті авторських прав у суді.

Порядок державної реєстрації авторського права визначений у законах України «Про авторське право і суміжні права» [59] та «Порядку державної реєстрації авторського права і договорів» [121]. Реєстрація здійснюється за допомогою національного органу інтелектуальної власності – державної організації, що входить до державної системи правової охорони інтелектуальної власності, та визначена Кабінетом Міністрів України, та має право представляти Україну в міжнародних та регіональних організаціях. Але порядок державної реєстрації авторського права на цифрові зображення, визначений у Законах України, має ряд недоліків, таких як тривалий процес перевірки авторства, відсутність предметної перевірки, складність доказу, висока вартість, централізоване зберігання та інші. Для подолання цих недоліків у розділі пропонується технологія підтвердження авторського права, заснована на сучасній концепції блокчейн.

Ідея технології блокчейн була описана ще в 1991 році, коли вчені-дослідники Стюарт Хабер та У. Скотт Шторнетта впровадили обчислювально-практичне рішення для цифрових документів зі штампом часу, щоб вони не могли бути оформлені заднім числом або підробитися.

Система використовувала криптографічно закріплений ланцюжок блоків для зберігання документів із позначкою часу. Однак ця технологія не використовувалася, і патент втратив чинність у 2004 році.

У 2004 році вчений у галузі комп’ютерних технологій та криптографічний активіст Хел Фінні представив систему під назвою Reusable Proof Of Work (RPoW). Система працювала, отримавши незмінний або

невзаємозамінний Hashcash токен, заснований на proof of work і підписаний RSA, який потім міг бути переданий від людини до людини.

RPoW вирішив проблему подвійного використання, зберігши право власності на токени, зареєстровані на довіреному сервері, який був розроблений, щоб дозволити користувачам у всьому світі перевірити його правильність та цілісність у режимі реального часу.

На сьогоднішній день сфера використання блокчейн надзвичайно масштабне: від фінансової сфери до програм військового призначення. Блокчейн знайшов своє використання і в галузі захисту інтелектуальної власності.

Беручи до уваги сучасні тренди та результати застосування блокчейн для захисту авторських прав [122], запропоновано інформаційну технологію підтвердження права власності на цифрові зображення, що основується на технології блокчейн та цифрових водяних знаках для забезпечення надійної гарантії встановлення авторських прав.

Відповідно до моделі автентифікації цифрових зображень, яка детально представлена в роботі [2], пропонується наступна загальна схема інформаційної технології підтвердження права власності на цифрові зображення на рисунку 4.2.

Процес підтвердження права власності на цифрове зображення пропонується проводити поетапно, які представлені на рисунку 4.3.

Розглянувши рисунок 4.3, можемо виділити основні процеси, які забезпечують роботу технології підтвердження права власності на цифрове зображення:

1) реєстрація користувачів відповідними органами та компаніями, які відповідають за реєстрацію права власності. За результатами цього користувач отримує права на внесення своїх зображень у систему та згідно з технологією блокчейн смарт-контракт, який буде його ідентифікатором у системі та дозволить здійснювати передачу авторських прав на зображення;

Рисунок 4.2 – Загальна схема інформаційної технології підтвердження права власності на цифрові зображення

2) перевірка зображення на наявність цифрового водяного знака та пошуку дубліката зображення. Цей процес забезпечує захист від можливих повторних підписів захищених зображень та пошук дублікатів зображень для уникнення різного роду колізій;

3) генерація цифрового водяного знака. Даний процес на основі даних користувача (смарт-контракт користувача), вхідного зображення створює смарт-контракт зображення та формування на його основі цифрового водяного знака. Смарт-контракт зображення містить інформацію про зображення, про правовласника та час внесення в систему. За допомогою цього смарт-контракту відповідно до блокчейн технології відбуватимуться підтвердження права власності та можливість його передачі в комерційних цілях;

4) нанесення цифрового підпису на зображення. Даний процес на основі згенерованого ЦВЗ наносить підпис цифрового зображення та видає користувачеві захищену копію зображення. Цей процес після підпису зображення забезпечує збереження оригінала зображення у розподіленій системі зберігання даних IPFS та внесення інформації про захищене

зображення до блокчейн сховища;

5) перевірка автентичності зображення. Даний процес забезпечує локалізацію та вилучення цифрового водяного знака з зображення, після чого перевіряє автентичність смарт-контракт зображення відповідно до технології блокчейн, цим самим забезпечуючи достовірність права власності на цифрове зображення.

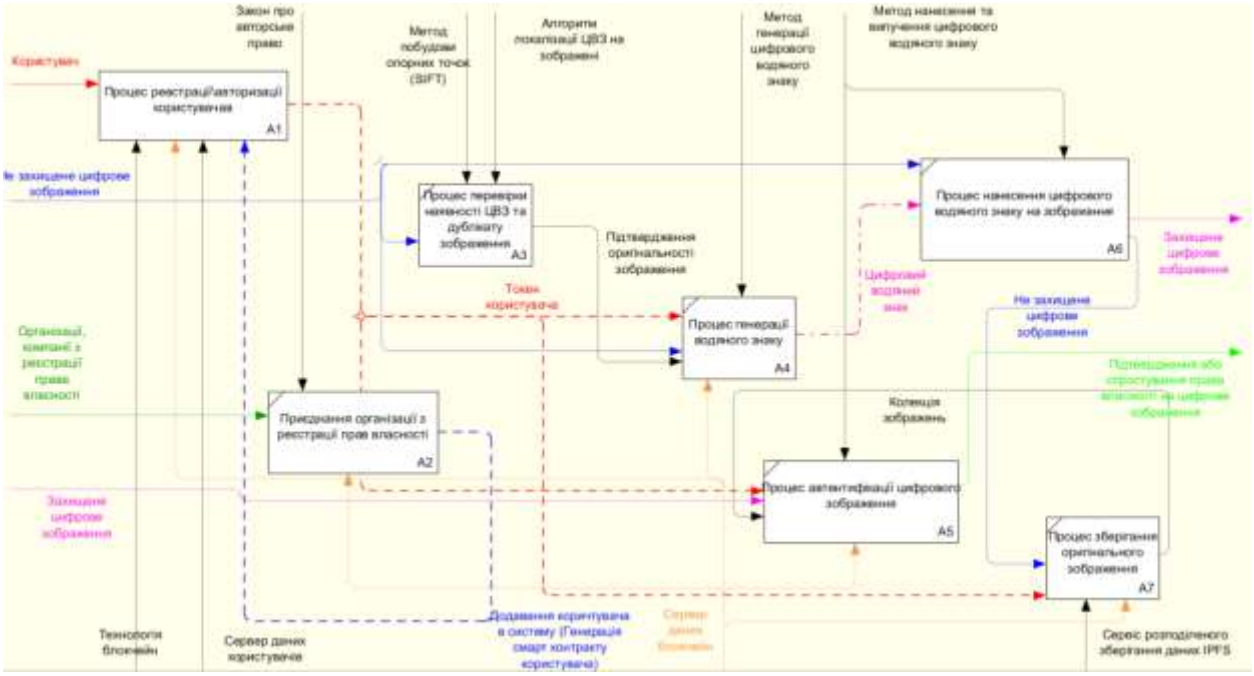


Рисунок 4.3 – Процес підтвердження права власності на цифрове зображення

4.2 Порівняльна характеристика існуючих архітектурних систем для підтвердження права власності на цифрові зображення

Інтерфейси прикладного програмування (API) відіграють найважливішу роль в сучасній розробці програмного забезпечення.

API (Application Programming Interface) – це технологія, яка з’єднує два додатки для надлишкового обміну даними та послугами в моделі клієнт-сервер. API дають змогу двом додаткам передавати об’єкти даних і є технічною революцією для додатків, що працюють за протоколом клієнт-сервер. Використання API для веб-сервісівсприяє організації IT-інфраструктури, автоматизації робочих процесів та передачі даних між

кількома мобільними пристроями. Варто знати про гаранти безпеки під час обміну та передачі даних між програмами.

Отже, використання API – це безпечний і перевірений спосіб підключення веб-сервісів за лічені секунди. Він дає можливість додатку розширити функціональність завдяки вилученню інформації з інших додатків. Саме особливості побудови API для свого додатка пояснюють, як API надсилає запит, завантажує дані та передає їх у певному форматі.

Щоб сприяти швидкій і масштабній інтеграції застосунків, API реалізуються з використанням протоколів та/або специфікацій, що визначають семантику й синтаксис переданих повідомлень. Ці специфікації складають архітектуру API.

З часом з’явилися різні архітектурні стилі API. Кожен із них містить власні схеми стандартизації обміну даними. Наявність вибору викликає нескінченні суперечки про те, який архітектурний стиль кращий.

Існують різні API, включно з Web API, Native API і Framework API. У веб-розробці API зазвичай забезпечують взаємодію між сервером і клієнтом або між різними сервісами. До побудови API у світі веб-розробки – це SOAP GraphQL і REST.

REST розшифровується як Representational State Transfer, архітектурна система, розроблена Роєм Філдінгом 2000 року [123]. Для створення масштабованих і підтримуваних веб-сервісів у REST API використовується протокол HTTP, а також певні рекомендації та обмеження. В основному REST API орієнтовані на ресурси, якими можуть бути будь-які дані, сервіси або функціональні можливості, що надаються через API. Унікальні URL-адреси, звані endpoints, ідентифікують ці ресурси. На рисунку 4.4 представлено історію API за роками [124].

Рисунок 4.4 – Історія API у часі [124]

Щоб зрозуміти, яка архітектурна система краща, розглянемо детальніше кілька з них.

Архітектурна система REST.

Передача стану подання (REST): надання даних як ресурсів.

REST – самоописна архітектурна система API, що визначається набором архітектурних обмежень і призначений для широкого впровадження багатьма споживачами API.

Найпоширеніший сьогодні стиль API було вперше описано 2000 року Роєм Філдінгом у його докторській дисертації. REST робить доступними дані на стороні сервера, представляючи подаючи їх у простих форматах – найчастіше це JSON і XML.

REST визначено не так строго, як SOAP. RESTful-архітектура повинна відповідати шести архітектурним обмеженням:

– єдиний інтерфейс, що дає змогу однаково взаємодіяти із сервером незалежно від типу пристрою або застосунку;

– відсутність стану: необхідний стан обробки запиту міститься в самому запиті без того, щоб сервер зберігав будь-які дані, що стосуються сесії;

– кешування;

– клієнт-серверна архітектура: дозволяє незалежний розвиток двох сторін;

– багаторівнева система додатка;

– можливість для сервера забезпечувати виконуваний код на клієнті.

Насправді деякі сервіси відповідають стандарту RESTful лише певною мірою. Вони беруть за основу стиль RPC, розбивають більші служби на ресурси й ефективно використовують інфраструктуру HTTP. По суті це означає, що з кожною відповіддю REST API надає метадані, які пов’язують всю інформацію про застосування API. Це те, що дозволяє відокремити клієнта від сервера.

У результаті й постачальник API, і споживач API можуть розвиватися незалежно, і це не ускладнює їхню комунікацію. На рисунку 4.5 представлено архітектуру REST API [124].

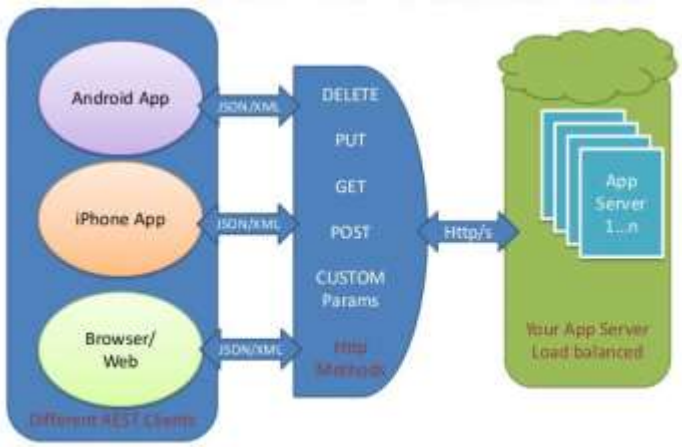


Рисунок 4.5 – Архітектура REST API [124]

У REST усе робиться за допомогою HTTP-методів, таких як GET, POST, PUT, DELETE, OPTIONS.

Архітектурна система SOAP.

Протокол доступу до простих об’єктів (SOAP): надання даних у вигляді сервісів.

SOAP – це високостандартизований протокол веб-комунікацій,

заснований на форматі XML. Випущений Microsoft через рік після XML-RPC, SOAP багато чого від нього успадкував. Коли на сцену вийшов REST, вони спочатку застосовувалися паралельно, але незабаром REST виграв конкурс популярності [125].

Формат XML тягне за собою багато формальностей. У поєднанні з масивною структурою повідомлень він робить SOAP найдетальнішим стилем API.

SOAP-повідомлення складається з:

– тега конверта <envelope>, яким починається і закінчується кожне повідомлення;

– тіла, що містить запит або відповідь;

– заголовка, якщо повідомлення повинно визначати будь-які особливості або додаткові умови;

– повідомлення про помилку, що інформує про будь-які помилки, які можуть виникнути в процесі обробки запиту.

Логіка SOAP API написана мовою опису веб-служб (WSDL). Дана мова опису API визначає кінцеві точки й описує всі процеси, які можуть бути виконані, що дає можливість різним мовам програмування та IDE швидко налагоджувати комунікацію.

SOAP підтримує обмін повідомленнями з відстеженням стану і без такого. У сценарії з відстеженням стану сервер зберігає отриману інформацію, яка є надзвичайно важливою. Але це виправдано для багатосторонніх операцій і складних транзакцій.

Архітектурна система GraphQL.

GraphQL: запит тільки необхідних даних.

Для того, щоб повернути щось потрібне, необхідно багаторазово викликати REST API. Щоб це змінити, було винайдено GraphQL.

GraphQL – це синтаксис, який описує, як зробити точний запит даних. Реалізація GraphQL варта того, якщо задіяна модель даних застосунку з великою кількістю складних сутностей, що посилаються одна на одну

GraphQL починається з побудови схеми, яка є описом усіх запитів, що можливо зробити в API GraphQL, і всіх типів даних, котрі вони повертають. Будувати схему складно, оскільки вона вимагає суворої типізації мовою визначення схеми (Schema Definition Language, SDL).

Клієнт, який має схему перед надсиланням запиту, може перевірити свій запит і переконатися, що сервер зможе відповісти на нього. Діставшись до бекенда, операція GraphQL інтерпретується за всією схемою і вирішується за допомогою даних для фронтенда. Відправивши один масивний запит на сервер, API повертає відповідь у форматі JSON із тими даними, на які був оформлений запит. На рисунку 4.6 представлено використання запитів GraphQL [126].

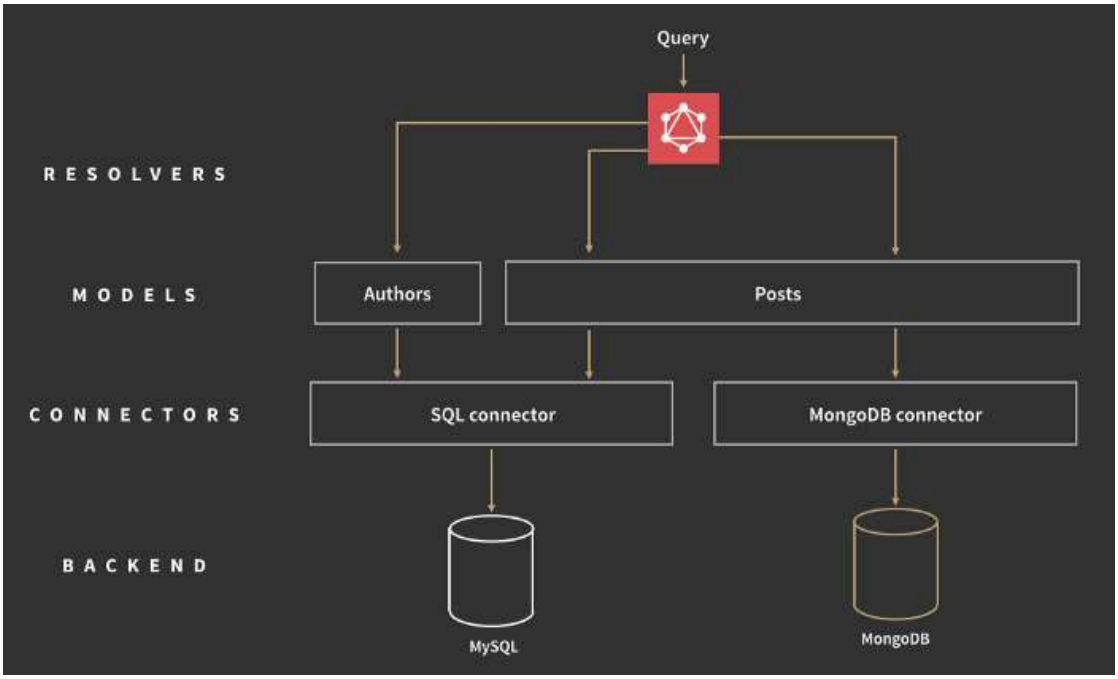


Рисунок 4.6 – Використання запитів GraphQL[126]

GraphQL API заснований на строго типізованій схемі, яка визначає типи даних, запити й мутації, доступні для використання і забезпечує ясний доступний контракт між клієнтом і сервером, що спрощує розуміння і перевірку обмінюваних даних.

Таблиця 4.1 – Порівняльна характеристика архітектурних систем

		SOAP	REST	GraphQL
1	Визначення	SOAP – це протокол для забезпечення комунікації між додатками	REST – це архітектурний стиль для проектування комунікаційних інтерфейсів	GraphQL – це специфікація, мова запитів API і набір інструментів
2	Проектування	Розкриває операцію	Обробка запитів на основі передачі стану (REST API) даних	Обробка запитів на основі передачі стану
3	Транспортний протокол	Незалежний і може працювати з будь-яким транспортним протоколом	Працює тільки з HTTP	Працює тільки з HTTP
4	Формат даних	Підтримує обмін даними тільки у форматі XML	XML, JSON, звичайний текст і HTML	JSON, AVRO
5	Продуктивність	Повідомлення SOAP мають більший розмір, через що сповільнюється комунікація	Вирізняється вищою продуктивністю завдяки меншому розміру повідомлень і підтримці кешування	Забезпечує можливість оптимізувати продуктивність і отримувати саме ті дані, які необхідні в даний момент
6	Можливість масштабування	SOAP складно масштабувати. Сервер підтримує стан, зберігаючи всі попередні повідомлення, які передавалися клієнту	REST легко масштабується. Системи на основі REST не зберігають стан, тому кожне повідомлення обробляється незалежно від попередніх	Легко масштабується, можна змінювати їх, уносячи зміни в наявну розробку. За необхідності деякі функції можна не тільки розширювати, а й зменшувати.
7	Безпека	Підтримує шифрування з додатковими накладними витратами	Підтримує шифрування без шкоди для продуктивності	Підтримує шифрування з додатковими накладними витратами
8	Приклад використання	Корисний у застарілих додатках і приватних API	У сучасних застосунках і загально доступних API	У сучасних застосунках, мобільних додатках і загальнодоступних API

Проаналізувавши порівняльну характеристику, робимо висновок, що найбільш оптимальним для нас є REST API.

SOAP – це клопітно, але його великий функціонал у плані безпеки, як і раніше, незамінний для білінгових операцій, систем бронювання та платежів.

REST API також підходить для створення загальнодоступних API (коли ними користується широке коло клієнтів із різними можливостями та вимогами), це те, що так потрібно для нашої інформаційної системи.

GraphQL складніший, ніж REST, і вимагає додаткового часу на вивчення. GraphQL також не має такої широкої підтримки спільноти, як і REST, що може призвести до обмежень у доступних інструментах і бібліотеках.

REST API варто застосовувати для роботи з великими наборами даних, які не надто часто оновлюються, а також для веб-додатків, які потребують кешування. Це означає, що REST можна використовувати для створення швидких і масштабованих API-інтерфейсів.

GraphQL може бути гарним вибором для застосунків з обмеженою пропускною спроможністю, таких як мобільні застосунки, яким потрібне швидке завантаження та економія трафіку.

REST має найвищу абстракцію і найкраще моделювання API.

REST набагато простіше зрозуміти, ніж GraphQL, оскільки він заснований на наявних протоколах HTTP. REST також має багато наявної документації, що полегшує роботу початківцям-розробникам. Порівняно з GraphQL, синтаксис REST простіший і легший для розуміння.

REST відомий своєю масштабованістю і гнучкістю при роботі з численними запитами від різних пристроїв. Веб-додатки часто використовують його через здатність обробляти безліч запитів клієнтів.

API REST спроектовані таким чином, що вони не мають статичних даних, тобто запити до сервера містять усі дані, необхідні для виконання поставленого завдання. Це дає можливість легко створювати, читати,

оновлювати та видаляти дані без необхідності відстежувати будь-які додаткові дані.

Простий синтаксис REST API робить його більш зрозумілим, ніж GraphQL, а наявна документація полегшує початківцям-розробникам швидке введення в експлуатацію.

Для реалізації даної технології була розроблена архітектура системи підтвердження права власності на цифрове зображення, яку показано на рисунку 4.7.

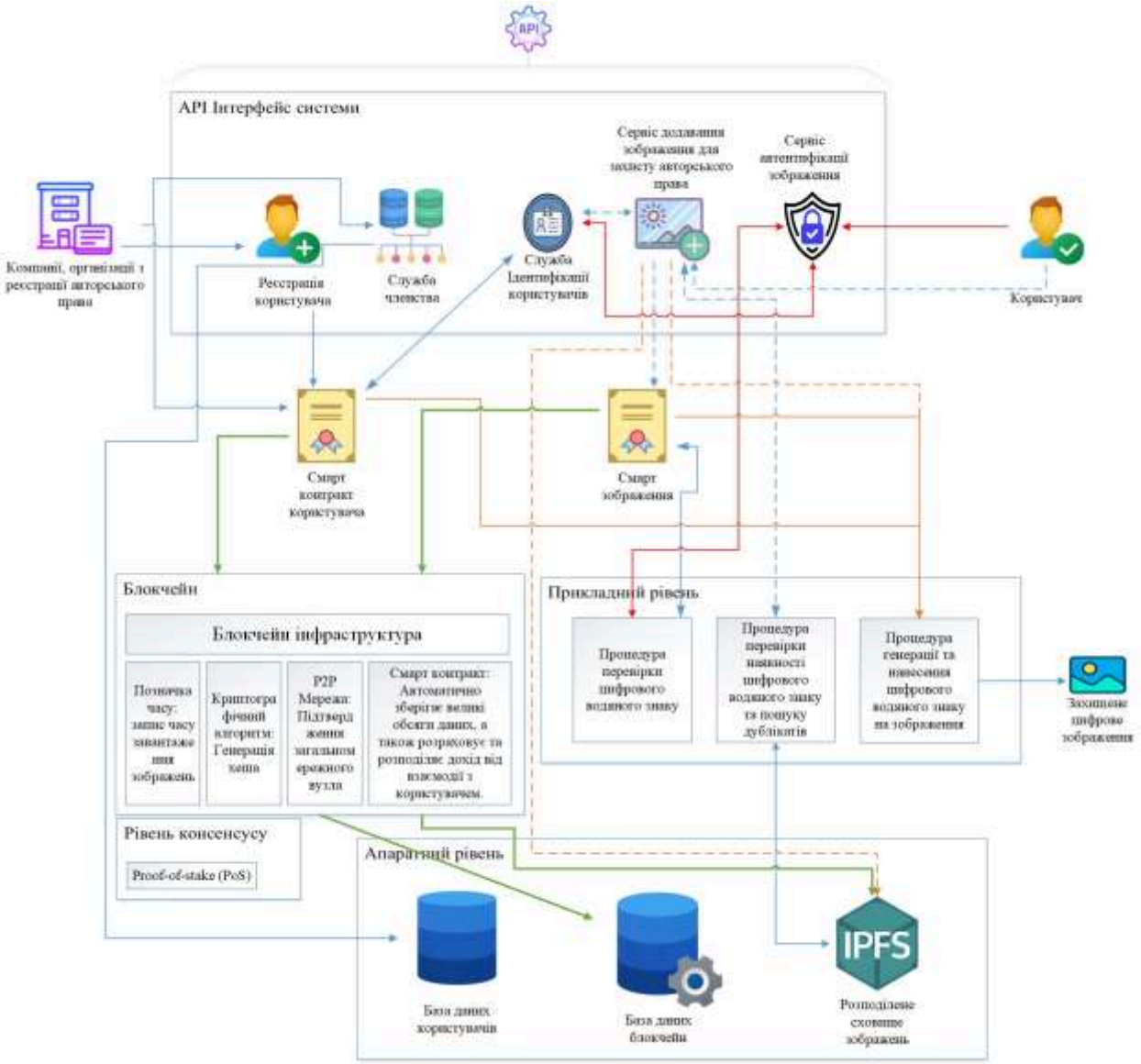


Рисунок 4.7 – Архітектура системи підтвердження права власності на цифрові зображення

На рисунку 4.7 показаний процес підтвердження автентичності цифрового зображення, який включає в себе обробку даних поза ланцюжком блокчейн й обробку даних у мережі блокчейн. Ураховуючи різноманітність організацій, сервісів та систем, які можуть надавати послуги реєстрації авторського права, з точки зору структури збережених даних та функціональних можливостей доцільно запропонувати Rest API-рішення, як універсальну технологію для інтеграції таких систем та платформи обміну блокчейнами.

API – інтерфейс системи дозволяє всім зацікавленим особам та організаціям здійснювати з нею основні операції, такі як:

– приєднання нової організації забезпечення права власності;

– створення відповідними організаціями користувачів системи (реєстрація користувача);

– додавання зображення для захисту права власності на нього;

– перевірка автентичності зображення. Увесь процес перевірки поділяється на дві процедури, залежно від потреб організацій. Перша – автентифікація власника захищеного зображення за допомогою смарт-контракту користувача. Друга процедура автентифікації – отримання детальної інформації про захищене цифрове зображення за допомогою смарт-контракту зображення.

Прикладний рівень забезпечує реалізацію основних процесів захисту та автентифікації цифрових зображень. Він надає інтерфейс користувача, за допомогою якого здійснюється процедура нанесення цифрового підпису та автентифікації зображення. Також саме через цей рівень здійснюється процедура зберігання зображень, які підлягають захисту авторського права.

Рівень блокчейн. Даний процес починається зі створення «Початкового блока» для кожного зареєстрованого в системі користувача, який хоче забезпечити підтвердження авторства на свої цифрові зображення. Після чого всі транзакції записуються в блокчейн. Кожен блок містить унікальний

заголовок, що ідентифікується по хешу заголовка блока. Блок складається з таких компонентів: хеш попереднього блока, інформація про правовласника, хеш-зображення, яке захищається, і мітка часу. Цей процес повторюється кожен раз, коли користувач додає нове зображення в систему.

Рівень консенсусу. Оскільки система основується на блокчейн технології, то вона є децентралізованою і не контролюється жодною з організацій реєстрації авторського права. Тому потрібен спосіб перевірки транзакцій у системі. Одним із методів, який використовують багато систем, заснованих на блокчейн, є доказ частки (Proof of Stak). Цей метод є альтернативою методу доказу роботи (Proof of Work), першим механізмом консенсусу, розробленим для криптовалют. Оскільки доказ частки (Proof of Stak) набагато енергоефективніший, тому він пропонується для перевірки транзакцій у системі. Модель proof-of-stake дозволяє власникам робити ставки на активи системи та створювати свої власні вузли-валідатори. Стейкінг – це процес, коли учасник мережі блокчейн зобов'язуєтеся використовувати свої активи для перевірки транзакцій. Коли блок транзакцій буде готовий для обробки, протокол підтвердження частки обирає вузол-валідатор для перевірки блоку. Валідатор перевіряє правильність транзакцій у блоці. Якщо це так, вони додають блок у ланцюжок блоків та отримують крипто-нагороди за свій внесок. Однак, якщо валідатор пропонує додати блок з неточною інформацією, він втрачає частину своїх стейкінгових активів як штраф.

Апаратний рівень. Як показано на рисунку 4.6, апаратний рівень складається з трьох основних компонентів:

– сховища авторизованих користувачів – централізованої бази даних організації (державних органів, організацій забезпечення права власності), зареєстрованих як користувачі. Він використовує службу членства, яка має доступ до отримання даних за допомогою RestAPI;

– сховища блокчейн даних – блокчейн консорціуму, який функціонує під керівництвом групи організацій, що забезпечує спільну трансформацію

бізнесу між організаціями. У даному випадку координатор призначає унікальний доступ для кожного користувача (державних органів, організацій забезпечення права власності);

– розподіленого сховища – децентралізованого сховища зображень, для яких система забезпечує можливість підтвердження автентичності.

4.3 Інформаційна система підтвердження права власності на цифрові зображення

У запропонованому блокчейн-застосунку для підтвердження права власності є три типи користувачів: власники авторських прав, користувачі, які можуть реєструвати ці права, та користувачі такі, як автори зображень, комерційні сторони, медіа-студії й т. ін. Щоб задовольнити потреби всіх користувачів, ця система виконує три основні функції для маніпуляції авторськими правами: реєстрацію авторських прав, підтвердження авторських прав, пошук авторських прав у режимі реального часу, авторизацію та передачу авторських прав.

Користувач реєструє інформацію про авторські права, заповнюючи форму, і система проводить певний аудит та сертифікацію всієї інформації про авторські права на зображення завантажені користувачем. Цей процес можливий лише шляхом систематичного аналізу та дослідження блокчейн запитів у системі, і, якщо немає плагіату та порушень, реєстраційну інформацію можна внести в ланцюжок блокчейн. Час на обробку та реєстрацію права власності в такому випадку буде займати всього декілька секунд. Процес реєстрації авторського права на зображення не вимагає сплати коштів за обробку. Дана процедура доступна всім користувачам мережі, що дозволяє уникнути недоліків традиційного процесу реєстрації авторських прав: значний період часу, необхідність сплати коштів, небажана публічність. Усе це сприятиме забезпеченню зручності користувача.

Хеш-покажчики використовуються для реалізації взаємних посилань

між блоками, оскільки кожен хеш-покажчик є хеш-значення, що вказує на дані, які зберігаються в попередньому блоці. Дані, що зберігаються в цьому блоці, також пов'язані зі своїм попереднім блоком. Якщо виявлено дані, які були підроблені, це означає, що зловмиснику необхідно змінити всі дані в ланцюжку та зламати алгоритм шифрування, що майже неможливо, виходячи з розвитку сучасних обчислювальних можливостей це майже не здійсненно. Отже, алгоритм максимально захищає незмінність пов’язаних інформаційних даних. Завдяки зв’язкам між собою, кожен блок може не лише відображати позицію попереднього блоку, але й надавати попереднє значення хеш-функції, щоб перевірити, чи змінилися дані, що містяться в попередньому блоці, і чи правильне значення хеш-функції. Схематично цей процес показано на рисунку 4.8.

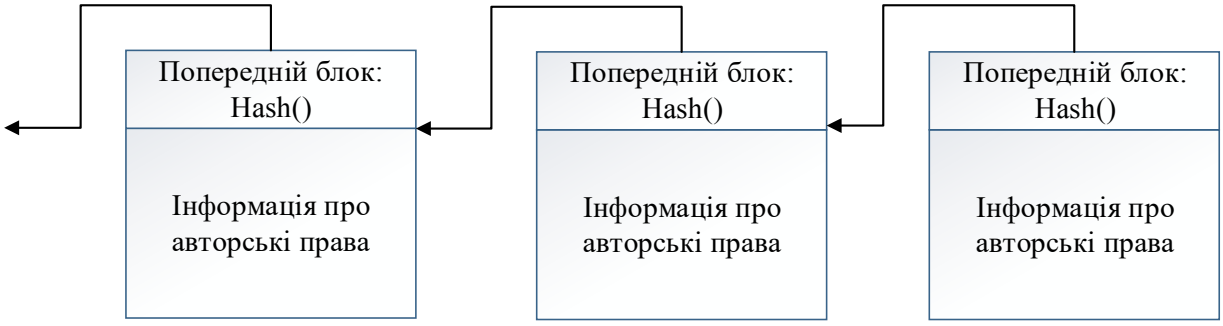


Рисунок 4.8 – Схема ланцюга блокчейн

Оскільки вміст, на який вказує хеш-покажчик у зв’язаному списку не може бути зміненим, то дані вузла у зв’язаному списку можуть бути виявлені після того, як вони були підроблені.

Для перевірки правовласності користувачі запитують інформацію про авторські права через систему, включаючи інформацію про правовласника та зображення з ЦВЗ, яке містить відповідну інформацію про блок та правовласника. У результаті чого отримує відповідну інформацію,: чи має користувач право на володіння зображенням та його використання. Передача

даних здійснюється через інтерфейс. Вміст інтерфейсу запиту включає захищене зображення з ЦВЗ, яке містить усю необхідну інформацію про правовласника та відповідний блок у ланцюзі блокчейну, тобто номер авторського права (copyrightID) і хеш-значення блоку (blockhash).

Авторизація та передача цифрових авторських прав використовує механізм децентралізації блокчейну для гарантії безпечного та надійного середовища торгівлі авторськими правами. Система підтримує вільний обіг авторських цифрових активів між користувачами. Реалізація механізму передачі авторських цифрових активів, у ролі яких виступають зображення, показано на рисунку 4.9.

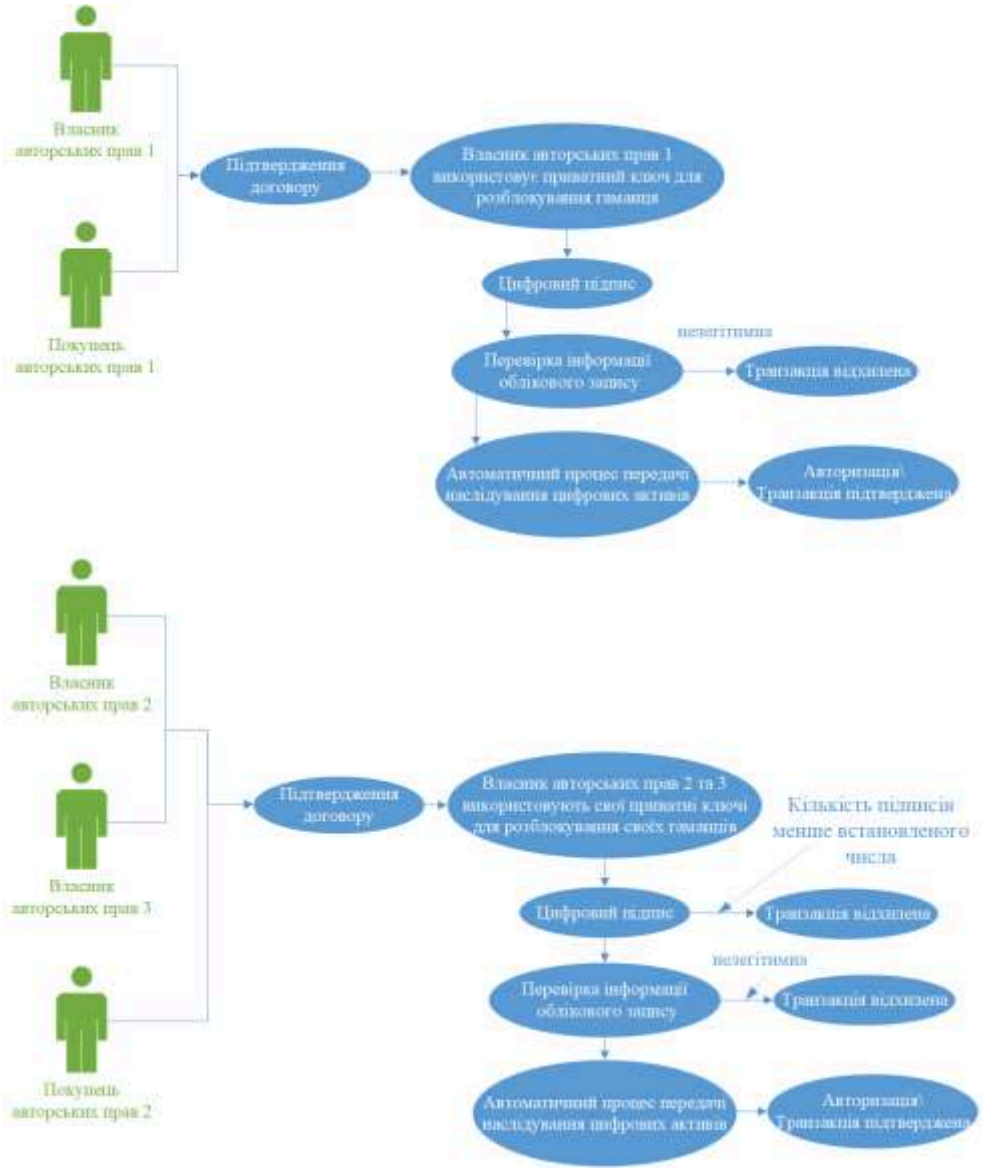


Рисунок 4.9 – Схема передачі права власності

Якщо власник авторських прав на зображення один, то йому спочатку потрібно підтвердити договір із покупцем авторських прав. Потім розблокувати гаманець і підписати транзакцію особистим цифровим ключем після того, як контракт буде визначено. На цьому етапі блокчейн-система перевірить інформацію облікового запису. Якщо він нелегітимний, транзакція буде невдалою. Якщо легітимний, то система автоматично передасть у спадщину цифровий актив згідно з умовами контракту. Якщо власник авторських прав не є унікальним, покупцеві необхідно визначити зміст договору, підписати договір разом з усіма правовласниками. Система блокчейн виконуватиме інформацію облікового запису лише після того, як цифровий підпис власника досягне встановленої ваги. Тільки після підпису контракту всіма правовласниками транзакція буде завершена.

4.4 Висновки за четвертим розділом

1. Ураховуючи загальнодоступність мережі інтернет і постійне зростання випадків порушення авторського права на цифровий контент, сучасні технології, що використовуються для захисту авторських прав, мають бути вдосконалені.

2. Технологія блокчейн володіє такими характеристиками, як децентралізація, захист від підробки та шифрування, розширюваність та гнучкість, що дозволяє ефективно вирішити питання реєстрації та підтвердження цифрового авторського права. Вона відіграє значну роль у захисті прав та інтересів авторів.

3. У розділі запропонована інформаційна технологія підтвердження права власності на цифрові зображення, яка використовує цифрові водяні знаки, блокчейн, хеш-функції для зображення і IPFS для створення нової децентралізованої технології підтвердження права власності в цифрову епоху інтернету.

4. Що стосується типів файлів, у цьому розділі згадується лише управління авторськими правами на цифрові зображення. У майбутньому технологію можна буде розширити на аудіо, відео та інші типи мультимедійних файлів, щоб сформувати єдину систему для підтвердження права власності на будь-який цифровий контент.

Список використаних джерел у даному розділі наведено у повному списку використаних джерел під номерами 7,15, 59, 121-125.

ВИСНОВКИ

У дисертаційній роботі розв’язано актуальне науково-практичне завдання розробки інформаційної технології підтвердження права власності на цифрові зображення, яку використовують як сучасну тенденцію в області цифрових водяних знаків та блокчейну для створення нової децентралізованої технології підтвердження права власності на цифрові ображення. При цьому були отримані такі наукові та практичні результати.

1. Проведено аналіз сучасного стану проблеми й особливості задач забезпечення авторського права та підтвердження автентичності цифрових зображень. Проаналізовано методи нанесення цифрових водяних знаків

2. Проаналізовано методи нанесення цифрових водяних знаків на зображення та представлено сучасні підходи до їх реалізації.

3. Отримав подальший розвиток критерій оцінки ефективності методів нанесення цифрових водяних знаків на зображення, який відрізняється від існуючих можливістю тим, що враховує всі типи атак на ЦВЗ та дозволяє провести комплексну оцінку ефективності методу нанесення цифрових водяних знаків.

6. Вперше запропоновано комплексний критерій оцінки ефективності методів вбудови цифрових водяних знаків на зображення, який побудований з урахуванням ключових характеристик та визначенням вагових коефіцієнтів, дозволяє провести комплексну оцінку ефективності методу нанесення цифрових водяних знаків. Розроблено функціональну модель процесу забезпечення підвищення стійкості методів вбудови цифрових водяних знаків в цифрові зображення, яка основана на псевдоголографічному кодуванні та додатковій фільтрації цифрового водяного знаку.

4. Вдосконалено метод надійної перевірки справжності цифрового зображення з високим ступенем захисту. Надійність досягається за рахунок того, що ЦВЗ ховається не в усьому зображенні, а в його фрагменті, який

найбільш підходить для приховування зображення, а також застосування ЦВЗ як завадових кодів.

5. Отримали подальшого розвитку методи генерації ЦВЗ для цифрових зображень, а саме розроблено методи генерації ЦВЗ на основі хаотичних карт та додатковій фільтрації цифрового водяного знаку. Описані у роботі методи є ефективними для забезпечення стійкості ЦВЗ до локальних спотворень. Як показали дослідження, при 60 % спотворення зображення можливо відновити 90 % ЦВЗ.

6. Удосконалено інформаційну технологію підтвердження права власності на цифрові зображення, що основується на технології блокчейн та цифрових водяних знаках для забезпечення надійної гарантії встановлення авторських прав.

7. Проведено апробацію та впровадження результатів розроблених модель, методів та технології, а саме модель надійної перевірки справжності цифрового зображення з високим ступенем захисту від спотворення та підробки. Використання зазначених результатів дозволяє здійснювати вбудову інформації в цифровий контент, у даному випадку цифрове зображення.

Таким чином, застосування запропонованої моделі дозволяє забезпечити справжність цифрового зображення на основі застосування прихованого водяного знаку.

Результати проведених випробувань підтвердили стійкість даної конструкції до геометричних і негеометричних атак.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бологова Н.М. Дослідження моделей та методів обробки зображень та шляхи вдосконалення технологій розпізнавання маркерів в системах доповненої реальності / Н.М. Бологова, І. В. Рубан // Сучасний стан наукових досліджень та технологій в промисловості. – 2019. – № 1 (7). – С. 25–33 (Належить до категорії Б).

2. Ruban I. Method of sustainable detection of augmented reality markers by changing deconvolution / I. Ruban, N. Bolohova, V. Martovytskyi, V. Lebediev, N. Lukova-Chuiko // International Journal of Advanced Trends in Computer Science and Engineering. 2020. – № 9 (2). – P. 1113–1120.

3. Makoveichuk O. Development of a method for improving stability method of applying digital watermarks to digital images / O. Makoveichuk, I. Ruban, N. Bolohova, A. Kovalenko, V. Martovytskyi, T. Filimonchuk // Eastern-European Journal of Enterprise Technologies. 2021. – № 3 (2 (111)). – P. 45–56. (Належить до категорії А, входить до міжнародної наукометричної бази Scopus).

4. Ruban I. Digital image authentication model / I. Ruban, N. Bolohova, V. Martovytskyi, O Koptsev // Advanced Information Systems. 2021. – № 5 (1). – P. 113–117 (Належить до категорії Б).

5. Ruban I. Methodology for assessing the effectiveness of methods for embedding digital watermarks / I. Ruban, N. Bolohova, V. Martovytskyi, R. Yaroshevych // Advanced Information Systems. 2021. – № 5 (3). – P. 112–118 (Належить до категорії Б).

6. Martovytskyi V. Development of methods for generation of digital watermarks resistant to distortion / V. Martovytskyi, I. Ruban, N. Bolohova, O. Sievierinov, O. Zhurylo, O. Permiakov, A. Nosyk, D. Nepokrytov, I. Krylenko // Eastern-European Journal of Enterprise Technologies. 2021. – № 6 (2 (114)). – P. 103–116. (Належить до категорії А, входить до міжнародної

наукометричної бази Scopus).

7. Ruban I. Information technology for confirming property rights to digital images / I. Ruban, N. Bolohova, V. Martovytskyi // Advanced Information Systems. 2022.– № 6 (1). – P. 118–123 (Належить до категорії Б).

8. Ruban I. et al. Method of neural network recognition of ground-based air objects //2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). – IEEE, 2018. – С. 589-592.

9. Бологова Н.М. Аналіз сучасного підходу обробки зображень для розпізнавання маркерів в системі доповненої реальності / Н.М. Бологова, І.В. Рубан, К.Р. Локотецька // Тези доповідей шостої міжнародної науково-практичної конференції «Проблеми інформатизації». 14 – 16 листопада 2018 р., Черкаси, Баку, Бельско-Бяла, Харків. – 2018. – С.36.

10. Bolohova N. Analysis of restoration methods for optical-electronic images lubricated at motion / N. Bolohova, Y. Kortiak // Тези доповідей шостої міжнародної науково-практичної конференції «Проблеми інформатизації». 13 – 15 листопада 2019 р., Черкаси, Харків, Баку, Бельско-Бяла. – 2019. – С.8.

11. Bolohova N. Analysis of the current status of additional reality technologies / N. Bolohova, Y. Kortyak, A. Liashova // Proceedings of Fourth International Scientific and Technical Conference on COMPUTER AND INFORMATION SYSTEMS AND TECHNOLOGIES. – Kharkiv, April 22-23, 2020. – P.12–13.

12. Bolohova N. Method for evaluating the effectiveness of methods for embedding digital watermarks / N. Bolohova, V. Martovytskyi, V. Diachenko, O. Kolomiitsev, V. Fedorchenko // Матеріали XX міжнародної науково-практичної конференції «Інформаційні технології і безпека». Київ. – 2020. С. 75–83.

13. Пересада Р.А. Аналіз методів підвищення стійкості водяних знаків у цифрових зображеннях / Р.А. Пересада, Н.М. Бологова // Тези доповідей восьмої міжнародної науково-технічної конференції «Проблеми інформатизації». 26 – 27 листопада 2020 р., . Черкаси, Харків, Баку, Бельсько-Бяла. –

2020. – С. 53.

14. Бологова Н.М. Модель автентифікації цифрового зображення / Н.М. Бологова // Тези доповідей десятої міжнародної науково-практичної конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління». 8 – 9 квітня 2021р., – Баку, Харків, Жиліна. – С. 41.

15. Copytrack Global Infringement Report. International Image Theft in Comparison, 2019 [Електроний ресурс]. – Режим доступу: https://www.copytrack.com/wpcontent/uploads/2019/04/190328_Global_Infringement_Report_ 2019_EN_Online.pdf.

16. Панасюк В. М. Інформатизація та цифровізація: тренди та напрями розвитку в Україні. Інтелект XXI. / В.М. Панасюк,. М.О.Фіщук, В.Е.Матюшко, Є.А.Чернєв // Україна 2030Е – країна з розвинутою цифровою економікою Укр. ін-т майбутнього. – Київ, 2020. – № 1. С. 163. [Електроний ресурс]. – Режим доступу: https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html

17. Миськовець Н. П. Цифровізація в Україні та світі. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Економіка і управління / Н.М. Миськовець. –2019. – Т. 30. № 4. С. 63.

18. Цифровізація та Розумні технології. Агенція Європейських Інновацій. [Електроний ресурс]. – Режим доступу: https://aei.org.ua/cyfryzaciya-tasmart-tehnologii/.

19. Osborne C.F. A Digital Watermark, / C.F. Osborne, R.V. Schyndel, A.Z. Tirkel // IEEE Intern. Conf. on Image Processin.– 1994. – P. 86–90.

20. Ali M. Blockstack: A global naming and storage system secured by blockchains / M. Ali, J. Nelson, R. Shea, M.J. Freedman // Annual Technical Conference. – 2016. –P. 181 – 194.

21. Non-Fungible Tokens A Brief Introduction and Histor, 2020. [Електронний ресурс] – Режим доступу: https://assets.ctfassets.net/fgyig42jimx/6A8K5H6VrTydTDuEFHXQ5P/3cca896ad77bd967859a7a1256a5a91f/Crypto.co

m_Macro_Report_-_Non-Fungible_Tokens.pdf

22. Hoy M. B. An introduction to the Blockchain and its implications for libraries and medicine / M. B. Hoy // Medical reference services quarterly. – 2017. – Vol. 36, –No 3. – P. 273–279. DOI: 10.1080/02763869.2017.1332261

23. What Is Token-Based Authentication? [Електронний ресурс] // Okta. – 2020. [Електронний ресурс] – Режим доступу: https://www.okta.com/identity-101/what-is-token-based-authentication/

24. Tapscott D., Tapscott A. BLOCKCHAIN REVOLUTION: How the Technology Behind Bitcoin is Changing Money / D. Tapscott, A. Tapscott //. Business, and the World. First Edition. Penguin. – 2016. – 324 p.

25. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System, Bitcoin / S. Nakamoto. – 2008. [Електроний ресурс]. – Режим доступу: https://bitcoin.org/bitcoin.pdf

26. Рябокінь М.В. Виклик впровадження цифрової валюти центрального банку у контексті нової еволюційної форми грошей в Україні: світовий досвід. / М.В. Рябокінь // Економіка та суспільство. – 2022. – № 37. [Електроний ресурс]. – Режим доступу: https://economyandsociety.in.ua/index.php/journal/article/view/1231/1186

27. Український банк запустить пілотний проєкт електронних грошей на блокчейні. Економічна правда. [Електроний ресурс]. – Режим доступу: https://www.epravda.com.ua/news/2021/12/16/680731/

28. Проект закону №3637 «Про віртуальні активи». [Електроний ресурс]. – Режим доступу: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf35 11= 69110

29. В Мінцифри працюють над легалізацією криптовалют та блокчейну. Економічна правда. [Електроний ресурс]. – Режим доступу: https://www.epravda.com.ua/news/2020/07/14/662909/

30. Baatz W. Photography: An illustrated historical overviewBarron’s / W. Baatz . – N. Y, 1997. – p. 16.

31. Rudinjanto A.Digital camera starts to gain ground in local market. from

the Jakarta, 2003. [Електроний ресурс]. – Режим доступу: http://www.thejakartapost.com/news/2003/12/14/digital-camera- starts-gain-ground-local-market.html

32. Hannemyr G. Photography. Retrieved, from the DPanswers, 2006 [Електроний ресурс]. – Режим доступу:http:///dpanswers.com/content/irphoto.php

33. Scientific Working Groups on Digital Evidence and Imaging Technology. SWGDE and SWGIT digital & multimedia evidence glossary from the Scientific Working Group on Digital Evidence. [Електроний ресурс]. – Режим доступу: http://www.swgde.org/documents/current-documents/

34. Wallace G.K. The JPEG still picture compression standard / G.K. Wallace // IEEE Transactions on Consumer Electronics. – 199. – V.134(4). – P.30-44.

35. Ahmed N., Natarajan T., Rao, K. R. Discrete cosine transform / N. Ahmed, T. Natarajan, K.R. R // IEEE Transactions on Computers. – V.23(1). – P. 90-93.

36. Campbell, F.W., Robson, J.G. Application of fourier analysis to the visibility of gratings. The Journal of Physiology // F.W. Campbell, J.G Robson. – 1968. – V.197. – P. 551-566.

37. Mahdian B., Saic S. Detecting double compressed JPEG images / B Mahdian., S Saic // IET Seminar Digests. – 2009. – V.2. – P. 12-17.

38. Gallagher A.C. Detection of linear and cubic interpolation in JPEG compressed images / A.C. Gallagher //T he 2nd Canadian Conference on Computer and Robot Vision. – 2005. – P 65-72.

39. Popescu A.C., Farid H. Exposing digital forgeries by detecting traces of re-sampling / A.C. Popescu, H. Farid // IEEE Transactions on Signal Processing. – 2005. – V. 53(2). – P. 12-17.

40. Foveon. Inc. X3 Technology. Retrieved, 2011. [Електроний ресурс]. – Режим доступу: http://www.foveon.com/article.php?a=69

41. Popescu, A.C., Farid, H. Exposing digital forgeries in color filter array interpolated images / A.C. Popescu, H. Farid // IEEE Transactions on Signal. –

2005. – V. 53(10). – P. 3948-3959.

42. Bayram S. Source camera identification based on CFA interpolation / S Bayram, H. T Sencar, N Memon,., I Avcibas // IEEE International Conference on Image. – 2005. – V. 3. – P. 69-72.

43. Bayram S., Sencar H. T.. Classification of digital camera-models based on demosaicing artifacts / S Bayram, H. T Sencar, N Memon // Digital Investigation. – 2008. – V. 5(1-2). – P. 49-59.

44. Luo W., Haung, J. JPEG error level analysis and its applications to digital image forensics / W. Luo, J Haung, G Qiu // IEEE Transactions on Information Forensics and Securit. – 2010. – V. 5(3). – P. 480-491.

45. Stamm, M.C. Anti-forensics of JPEG compression / M.C. Stamm, S.K. Tjoa, W.S. Lin, K.J. Liu // IEEE International Conference on Acoustics Speech and Signal. – 2010. – P. 1694-169.

46. Lai, S., & Bohme, R.. Countering counter-forensics: The case of JPEG compression / S. Lai, R Bohme // 13th International Conference on Information Hiding. – Prague:Springer. – 2011. – P. 285-298.

47. Chen M. Digital imaging sensor identification (further study). Proc. SPIE, Electronic Imaging, Security / M. Chen., J. Fridrich, M. Goljan //. Steganography and Watermarking of Multimedia Contents IX, . – 2007. – P. 0P-0Q.

48. Fridrich J. Digital image forensics / J. Fridrich // IEEE Signal Processing Magazine. – 2009. – V. 26(2). – P.26-37.

49. Khanna N.Forensic camera classification: Verification of sensor pattern noise approach / N. Khanna., A.K. Mikkilineni, E.J Delp // Forensic Science Communications. – 2009. – V. 11(1) – P.45-50.

50. Reininger R C. Distributions of the two-dimensional DCT coefficients for images / R.C. Reininger, J.D. Gibson // IEEE Transactions on Communications. – 1983. – V. 31(6) – P.835-839.

51. Weiqi L.A survey of passive technology for digital image forensics / L Weiqi, Q. Zhenhua., P. Feng, H. Jiwu // Frontiers of Computer Science. – 2007. –

P. 166-179.

52. Farid H. Exposing digital forgeries from JPEG ghosts / H. Farid // IEEE Transactions on Information Forensics and Security. – 2008. – V. 4(1) – P.154-160.

53. Fang Y. Source class identification for DSLR and compact cameras / Y Fang, A.E. Dirik, Z. Sun, N Memon // IEEE International Workshop on Multimedia Signal Processing. – 2009. – P. 1-5.

54. Alles E.J. Source camera identification for heavily compressed low resolution still images / Alles, E. J., Z.J. Geradts, C.J. Veenman //Journal of Forensic Sciences. – 2009. – V. 54(3) – P. 628-638.

55. Chen M.Imaging sensor noise as digital x-ray for revealing forgeries. / M. Chen, J. Fridrich, J. Lukas, M Goljan // Proceedings of the 9th International Conference on Information Hiding, – 2007. – P.342-358.

56. Chierchia G. On the influence of denoising in PRNU based forgery detection / G. Chierchia, S. Parrilli, G Poggi,. C Sansone, L.Verdoliva // Proceedings of the 2nd ACM Workshop on Multimedia in Forensics, Security and Intelligence. – 2010. – P. 77-82.

57. Geradts Z. J. at all. Methods for identification of images acquired with digital cameras. Proc. SPIE. – 2001. – P. 505-512.

58. Логвиненко, М.І. Проблеми захисту об’єктів авторського права в мережі інтернет [Текст] / М.І. Логвиненко, І.В. Каріх, А.В. Диковець // Правові горизонти. – 2019. – Вип. 15 (28). – С. 21-25

59. ЗАКОН УКРАЇНИ Про авторське право і суміжні права № 2811-IX від 01.12.2022, ст.6. [Електроний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2811-20#Text

60. Миронюк, С. А., Волошина Г. Ю. «Захист авторських прав в інтернеті» «Порівняльно-аналітичне право». Електронне наукове фахове видання юри-дичного факультету ДВНЗ «Ужгородський національний університет». – 2017. – №5. – С.107-109.

61. Yang J. Encryption scheme with mixed homomorphic signature based on

message authentication for digital image / J Yang, F. Mingyu, W. Guangwei // The Journal of Supercomputing. – 2020. – V. 76(2) – P. 1201-1211

62. Yeung MM Digital watermarking introduction. Commun ACM. . – 1998. – V. 41(7) – P. 31–33.

63. Van Schyndel, R.G. A digital watermark/ R.G. Van Schyndel, A.Z. Tirkel, C.F Osborne // Proceedings of 1st international conference on image processing, IEEE. – 1994. – V.2 – P. 86-90

64. Islam M.Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM / M. Islam, R.H. Laskar // Multimedia Tools and Applications. – 2018. – V.11– P. 14407-14434.

65. Loukhaoukha, K. On the security of digital watermarking scheme based on SVD and tiny-GA. Journal of Information Hiding and Multimedia Signal Processing. – 2012. – V. 3(2) – P. 135-141.

66. Mun S.M..Finding robust domain from attacks: A learning framework for blind watermarking. Neurocomputing. – 2010. – V. 337. – P. 191-202.

67. Roy A. An HVS inspired robust non-blind watermarking scheme in YCbCr color space / A. Roy, A.K. Maiti, K. Ghosh // International Journal of Image and Graphics. – 2018. – V. 18(03). DOI: https://doi.org/10.1142/S0219467818500158.

68. Vaidya P.A robust semi-blind watermarking for color images based on multiple decompositions / P. Vaidya, // Multimedia Tools and Applications, . – 2017. – V. 76(24) – P. 256.23-256.56.

69. Ruban I.The Model and the Method for Forming a Mosaic Sustainable Marker of Augmented Reality / I. Ruban,H. Khudov, O. Makoveychuk V, Khudov, V Lishchenko // Proceedings - 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET. – 2020. – P. 402-406.

70. Xie L. Approximate image message authentication codes / L. Xie, R.. Gonzalo, F. Graveman // IEEE Transactions on Multimedia 3.2. – 2001. – P. 242-

252.

71. Sato S., Shikata, J. Interactive aggregate message authentication scheme with detecting functionality / S. Sato, J. Shikata. // In International Conference on Advanced Information Networking and Applications. –Springer – Cham, 2019. – P. 1316-1328.

72. Yu, X. Review on semi-fragile watermarking algorithms for content authentication of digital images / X. Yu, C. Wang, X. Zhou // Future Internet. – 2017. – P.56.

73. Egorova A. A classification of semi-fragile watermarking systems for JPEG images / A. Egorova, V. Fedoseev // Computer Optics 43.3. – 2019. – V. 43(3) – P. 419-433.

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

75. Fridrich J. Steganography in Digital Media Principles, Algorithms, and Application, Cambridge University Press. – 2009.

76. Singh A.K. A Medical image watermarking: techniques and applications / A.K., Singh, B. Kumar, G. Singh // Book series on Multimedia Systems and Applications, Springer, 2017. – ISBN: 978-3319576985

77. Mohanty S.P. Everything you want to know about watermarking: From Paper marks to hardware protection / S.P. Mohanty, A. Sengupta., P. Guturud, E. Kougianos // IEEE Consumer Electronics Magazine. – 2017. – V. 6(3) – P. 83–91.

78. Moosazadeh M, Ekbatanifard G. Robust image watermarking algorithm using DCT coefficients relation in YCoCg-R color space / M. Moosazadeh, G. Ekbatanifard // 2016 Eighth Int. Conference on Information and Knowledge Technology (IKT), IEEE. – 2016. – P. 263-267.

79. Zhong X. Robust Multibit Image Watermarking Based on Contrast Modulation and Affine Rectification / , X. Zhongand, F.Y Shih // Int. J. of Pattern Recognition and Artificial Int.. – 2019. – V. 33(14) DOI: https://doi.org/10.1142/S0218001419540363

80. Paikaray D. Genetic Algorithm-Based Image Watermarking Using Multiple Location / D. Paikaray, A. Mustafi // Proc. of the Fourth Int. Conference on Microelectronics, Computing and Communication Systems, Springer. – Singapore, 2020. – P. 617-627

81. Loukhaoukha, K., Nabti, M. and Zebbiche, K. (2014), "A Robust SVD-based Image Watermarking Using a MultiObjective Particle Swarm Optimization", Opto-Electronics Review. – V. 22 (1) – P. 45-54.

82. Shen J.J. A Fragile Associative Watermarking on 2D Barcode for Data Authentication, International Journal of Network Security. – 2008. – V. 7(3) – P. 301–309.

83. Sachnev V.Reversible Watermarking Algorithm Using Sorting and Prediction / V. Sachnev, H.J. Kim, J. Nam, S.. Suresh, Y.Q. Shi // IEEE Transactions on Circuits and Systems for Video Technology. – 2000. – V. 19(7). – P. 989–999.

84. Pei S.C. Hybrid Pixel-Based Data Hiding and Block-Based Watermarking for Error-Diffused Halftone Images / S.C. Pei, J.M. Guo // IEEE transactions on Circuits and Systems for Video Technology. – 2003. – V. 13(8) – P. 867–884.

85. Lin CY.A Reversible Data Transform Algorithm Using Integer Transform for Privacy Preserving Data Mining / CY. Lin // The Journal of Systems & Software. – 2006. – V. 117(7) – P. 104–112.

86. Zhou X. A Robust Image Watermarking Technique Based on DWT, APDCBT, and SVD / X. Zhou.,H. Zhang, Wang. // Symmetry MDPI. – 2018 – V. 10(3) – P. 1–15.

87. Maeno, K. New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization / K. Maeno // IEEE Transactions on Multimedia. – 2006. – V. 8(1) – P. 32-45.

88. UR-REHMAN, Obaid; ZIVIC, Natasa; RULAND, Christoph. Approximate Image Authentication and Correction using Spatial and Frequency Domain Features. In: SCC 2017; 11th International ITG Conference on Systems,

Communications and Coding. VDE. – 2017. – P. 1–6.

89. Venkatesan R. Robust image hashing / R. Venkatesan, S. Koon, M. Jakubowski // In: Proceedings of the IEEE international conference on image processing. – 2000. – V. 3 – P. 664–666.

90. Wolfgang R.B.Techniques for watermarking digital imagery: further studies / R.B. Wolfgang., E.J. Delp // In: Proceedings of the international conference on imaging science, systems, and technology. – 1997. – V. 1 – P. 279–287.

91. Walton S. Information authentication for a slippery new age. Dr Dobb's J. – 1995. – V. 20(4) – P.18-26.

92. Zauner C. Implementation and benchmarking of perceptual image hash functions. – 2010.

93. Мельник С.В. Світові тенденції розвитку цифрової стеганографії в контексті завдань забезпечення інформаційної безпеки держави / С.В.Мельник, С.В.Кондакова // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф. –К. : Наук.-вид. відділ НА СБ України, 2010. – С. 134-138.

94. Kjell H. Rate k/(K+1) Minimal punctured convolutional encoders / H. Kjell // IEEE Transactions on Information Theory. – 1991. – V. 37(3) – P. 38-45.

95. Bruckstein A.M. Holographic image representations: the subsampling method / A.M Bruckstein, R.J. Holt, A.N Netravali // Proceedings of International Conference on Image Processing. – 1997. DOI: https://doi.org/10.1109/icip.1997.647439

96. Bruckstein A. M.. Holographic representations of images / A.M Bruckstein, R.J. Holt, A.N Netraval // IEEE Transactions on Image Processing. – 1998. – V. 7(11) – P. 1583–1597. DOI: https://doi.org/10.1109/83.725365.

97. Markovskii A. V.On Quasiholographic Coding of Digital Images. Automation and Remote Control. – 2001. – V. 62 – P. 1688–1697. doi: https://doi.org/10.1023/A:1012470618018.

98. Kuznetsov O. P., Markovskiy A. B. Kvazigolograficheskiy podhod k kodirovaniyu graficheskoy informatsii. Iskusstvenniy intellekt. – 2002. – V. 2 – P.

474–482.

99. Dovgard R. Holographic Image Representation With Reduced Aliasing and Noise Effects. IEEE Transactions on Image Processing. – 2004. – V. 13(7) – P. 867–872.DOI: https://doi.org/10.1109/tip.2004.827228

100. Makoveychuk O. A new type of augmented reality markers. Advanced Information Systems. – 2019. – V. 3(3) – P. 43–48. DOI: https:// doi.org/10.20998/2522-9052.2019.3.06.

101. Makoviechuk O. Using genetic algorithms to find inverse pseudo-random block permutations / O. Makoviechuk, I. Ruban, G Hudov // Control, Navigation and Communication Systems. – 2019. – V. 4 – P. 72-81. DOI: https://doi.org/10.26906/sunz.2019.4.072.

102. Lai C.-C., Tsai C.-C. Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition / C.-C. Lai, C.-C. Tsai // IEEE Transactions on Instrumentation and Measurement. – 2010. – V. 59(11) – P. 3060–3063. DOI: https://doi.org/10.1109/tim.2010.2066770

103. Yusof Y. Digital watermarking for digital images using wavelet transform / Y. Yusof, O.O. Khalifa // IEEE International Conference on Telecommunications and Malaysia International Conference on Communications. – 2007. DOI: https://doi.org/10.1109/ ictmicc.2007.4448569.

104. Mallat S.G. A theory for multiresolution signal decomposition: the wavelet representation / S.G Mallat //IEEE Transactions on Pattern Analysis and Machine Intelligence. – 1989. – V. 11(7) – P. 674–693. DOI: https://doi.org/10.1109/34.192463.

105. Xia X. G., Boncelet C., Arce G. Wavelet transform based watermark for digital images. Optics Express. – 1998. – V. 3 (12) – P.497. DOI: https://doi.org/10.1364/oe.3.000497

106. Daubechies I. Ten Lectures on Wavelets. CBMS-NSF Regional Conference Series in Applied Mathematics. – 1992. DOI: https:// doi.org/10.1137/1.9781611970104.

107. Otsu N. A Threshold Selection Method from Gray-Level Histograms.

IEEE Transactions on Systems, Man, and Cybernetics. – 1979. – V. 9(1) – P. 62-66. DOI: https://doi.org/10.1109/tsmc.1979.4310076.

108. Bradley D., Roth G. Adaptive Thresholding using the Integral Image. Journal of Graphics Tools. – 2007. – V. 12(2) – P. 13-21. DOI: https://doi.org/10.1080/2151237x.2007.10129236.

109. Yeromina N.. The Synthesis of the Optimal Reference Image Using Nominal and Hyperordinal Scales / N. Yeromina, S. Petrov, N. Antonenko, I. Vlasov, V. Kostrytsia, V. Korshenko. // International Journal of Emerging Trends in Engineering Research. – 2020. – V. 8(5) – P. 2080–2084. DOI: https://doi.org/10.30534/ijeter/2020/98852020

110. Liashko O.The Criterion and Evaluation of Effectiveness of Image Comparison in Correlation-Extreme Navigation Systems of Mobile Robots / O. Liashko, V. Klindukhova, N. Yeromina, T. Karadobrii, O. Bairamova, A. Dorosheva // International Journal of Emerging Trends in Engineering Research. – 2020. – V. 8(6) – P. 2841–2847. DOI: https://doi.org/10.30534/ijeter/2020/97862020

111. Peterson, G. Arnold's cat map. – 1997. Електроний ресурс]. – Режим доступу: http://anyflip.com/jwch/llux

112. Hsu C. S. Cell-to-cell mapping: a method of global analysis for nonlinear systems: Springer, 354, 1987. DOI: https://doi.org/ 10.1007/978-1-4757-3892-6.

113. Wu J. Image encryption using 2D Hénon-Sine map and DNA approach / J. Wu., X. Liao, B. Yang //Signal Processing. – 2018. – V. 153 – P. 11-23. DOI: https://doi.org/10.1016/j.sigpro.2018.06.008

114. Ye G., Huang X.. An efficient symmetric image encryption algorithm based on an intertwining logistic map. Neurocomputing,. – 2017. – V. 251 – P. 45-53. DOI: https://doi.org/10.1016/j.neucom.2017.04.016

115. Akhavan A. A symmetric image encryption scheme based on combination of nonlinear chaotic maps / A. Akhavan, A. Samsudin, A. Akhshani // Journal of the Franklin Institute. – 2011. – V. 348(8) – P. 1797–1813. DOI: https://doi.org/10.1016/j.jfranklin.2011.05.001.

116. What is Tokenization? Available at: [Електроний ресурс]. – Режим доступу: https://www.tokenex.com/resource-center/what-is-tokenization

117. Cho D.-J. Study on Method of New Digital Watermark Generation Using QR-Code. 2013 Eighth International Conference on Broadband and Wireless Computing, Communication and Applications. – 2013. DOI: https://doi.org/10.1109/bwcca.2013.102

118. Makoveichuk O. Development of a method for improving stability method of applying digital watermarks to digital images / O. Makoveichuk, I. Ruban, N Bolohova, A. Kovalenko, V. Martovytskyi, T. Filimonchuk // Eastern-European Journal of Enterprise Technologie. – 2021. – V. 3(2(111)) – P. 45–56. DOI: https://doi.org/10.15587/1729-4061.2021.235802

119. Dutta M. K.Watermark generation from fingerprint features for digital right management control / M.K. Dutta, A. Singh., K.M. Soni, R. Burget, K. Riha // 36th International Conference on Telecommunications and Signal Processing (TSP). – 2013. DOI: https:// doi.org/10.1109/tsp.2013.6614031.

120. Dutta M.K. Generation of biometric based unique digital watermark from iris image / M.K Dutta, A. Singh, R., Burget, H. Atassi, A.Choudhary, K.M. Soni // 36th International Conference on Telecommunications and Signal Processing (TSP). – 2013. DOI: https:// doi.org/10.1109/tsp.2013.6614024.

121. ПОСТАНОВА від 27 грудня 2001 р. № 1756 Про державну реєстрацію авторського права і договорів, які стосуються права автора на твір. Верховна Рада України Законодавство України. 2001. [Електроний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/3792-12#Text

122. Shi J. A blockchain and sift based system for image copyright protection / J. Shi, D. Yi, J. Kuang // Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications, December. – 2019. – P. 1–6. DOI: https://doi.org/10.1145/3376044.3376051. – 2019

123. Pro Spring 5: An In-Depth Guide to the Spring Framework and Its Tools – Iuliana Cosmina. – 217. – P. 849.

124. REST API документація. [Електроний ресурс]. – Режим доступу:

https://www.altexsoft.com/blog/what-is-api-definition-types-specifications-documentation/.

125. SOAP API документація. [Електроний ресурс]. – Режим доступу: https://www.w3.org/TR/soap12/