УДК 004.056.5
DOI https://doi.org/10.32782/2521-6643-2022.2-64.10

Козіна Г. Л., кандидат технічних наук, доцент,
доцент кафедри захисту інформації
Національного технічного університету «Запорізька політехніка»
ORCID: 0000-0002-4787-6865

Савченко Ю. В., кандидат технічних наук,
доцент кафедри кібербезпеки та інформаційних технологій
Університету митної справи та фінансів
ORCID: 0000-0002-7177-6311

Воскобойник В. О., кандидат технічних наук, доцент,
доцент кафедри захисту інформації
Національного технічного університету «Запорізька політехніка»
ORCID: 0000-0003-3786-8666

Карпуков Л. М., доктор технічних наук, професор,
професор кафедри захисту інформації
Національного технічного університету «Запорізька політехніка»
ORCID 0000-0002-7098-6018

СИСТЕМА СТЕГАНОГРАФІЧНОГО ЗАХИСТУ ФОТОГРАФІЙ З ВИКОРИСТАННЯМ КРИХКИХ ВОДЯНИХ ЗНАКІВ

У статті представлено огляд досліджень, присвячених розгляду сучасної стеганології, завданням яких є не тільки розробка, аналіз або протидія засобам стеганографії, а й кваліфікований вибір існуючих засобів та їхнє уміле використання для вирішення конкретних прикладних завдань захисту інформації. Наявні в даний час публікації, присвячені стеганографії, або є науково-популярними, що не зачіпають математичних аспектів зазначеної науки, або зачіпають лише вузькі аспекти цієї науки. І тому, вони не в змозі повною мірою забезпечити зазначені потреби. Проведено аналіз стеганографічних методів захисту цифрових зображень, виокремлено можливі види атак на них. Наведено опис типів цифрових водяних знаків та їхнє призначення. Детально розглядаються крихкі цифрові водяні знаки, їхнє призначення, властивості та методи вбудовування в зображення. Виконано аналіз методу американського вченого P.W.Wong-а вбудовування цифрових водяних знаків у зображення. Показано, що для вирішення цілої низки практичних завдань інформаційної безпеки сьогодні недостатньо зробити інформацію недоступною для порушника (як відомо, вирішенням цього завдання займається криптографія). Найчастіше потрібно приховати сам факт її передавання – таким є класичне завдання стеганографії. Стеганографічний захист фотографій з використанням тендітних водяних знаків можна застосувати в тих випадках, коли перевірити справжність і цілісність цифрової фотографії може тільки її власник, оскільки секретний ключ і ЦВЗ зберігаються тільки у нього. Перевагою цього підходу є те, що під час перевірки не потрібне оригінальне зображення. Обґрунтовано вбудовування цифрових водяних знаків призначених для захисту авторських і майнових прав на цифрову інформацію різного роду, і впровадження в цифрові дані ідентифікаційних міток, призначених для маркування об'єктів у цифрових сховищах даних. На прикладі аналіз методу вбудовування цифрових водяних знаків у зображення Розроблено модифікований алгоритм, у якому використовуються конкретні функції, параметри яких узгоджені одна з одною. Цей алгоритм реалізовано мовою програмування С++. При цьому показано, що використання цифрових водяних знаків не регламентується спеціальними законами, сам цифровий водяний знак, секретний ключ шифрування, а також увесь алгоритм вбудовування і перевірки автентичності рекомендується засвідчити в нотаріуса. Після чого бажано записати на знімний носій, призначений тільки для читання і помістити до банківського сейфу або залишити на відповідальне зберігання в нотаріуса. Крихкі цифрові водяні знаки можуть застосовуватися в поєднанні з електронним цифровим підписом для забезпечення більшої надійності.

Ключові слова: *стеганографія, водяні знаки, крихкі водяні знаки, хешування, шифрування, цифрові зображення.*

Kozina G. L., Savchenko Iu.V., Voskoboynik V.O., Karpukov L.M. Steganographic photo protection system using fragile watermarks

The article presents a review of research on modern steganology, the task of which is not only to develop, analyse or counteract steganography tools, but also to select the existing tools and use them skilfully to solve specific applied information security problems. The currently available publications on steganography are either popular science publications that do not address

© Г. Л. Козіна, Ю. В. Савченко, В. О. Воскобойник, Л. М. Карпуков, 2022

the mathematical aspects of this science, or they address only narrow aspects of this science. Therefore, they are not able to fully meet these needs. The article analyses steganographic methods of digital image protection and identifies possible types of attacks on them. The types of digital watermarks and their purpose are described. Fragile digital watermarks, their purpose, properties and methods of embedding in images are considered in detail. The method of embedding digital watermarks in images by the American scientist P.W.Wong is analysed. It is shown that to solve a number of practical problems of information security today, it is not enough to make information inaccessible to an offender (as is known, cryptography is engaged in solving this problem). Most often, it is necessary to hide the very fact of its transmission – this is the classic task of steganography. Steganographic protection of photos using fragile watermarks can be applied in cases where only the owner of the digital photo can verify the authenticity and integrity of the photo, since the secret key and the digital signature are stored only by him. The advantage of this approach is that the original image is not required for verification. The article substantiates the embedding of digital watermarks intended to protect copyright and property rights to digital information of various kinds, and the introduction of identification labels into digital data intended to mark objects in digital data warehouses. The article analyses the method of embedding digital watermarks into images by means of an example. A modified algorithm has been developed which uses specific functions whose parameters are coordinated with each other. This algorithm is implemented in the C++ programming language. It is shown that the use of digital watermarks is not regulated by special laws, and it is recommended to notarise the digital watermark itself, the secret encryption key, and the entire algorithm for embedding and authentication. After that, it is advisable to record it on a removable read-only medium and place it in a bank safe or leave it for safe keeping with a notary. Fragile digital watermarks can be used in combination with an electronic digital signature to ensure greater reliability.

Key words: *steganography, watermarking, fragile watermarks, hashing, encryption, digital images.*

Вступ. До теперішнього часу для цілого кола фахівців з'явилася необхідність ознайомлення з основами сучасної стеганології, завданням яких є не тільки розробка, аналіз або протидія засобам стеганографії, а й кваліфікований вибір існуючих засобів та їх уміле використання для розв'язання конкретних прикладних завдань захисту інформації. Наявні в даний час публікації, присвячені стеганографії, або є науково-популярними, що не зачіпають математичних аспектів зазначеної науки, або зачіпають лише вузькі аспекти цієї науки. І тому, вони не в змозі повною мірою забезпечити зазначені потреби.

Легкість копіювання та редагування веде до несанкціонованого використання, незаконного привласнення та спотворення зображень. Для захисту цифрових фотографій від фальсифікацій застосовуються стеганографічні методи [1].

Одним із напрямів стеганографії та найбільш ефективних технічних засобів захисту мультимедійної інформації є вбудовування в об'єкт, що захищається, невидимих міток – цифрових водяних знаків (ЦВЗ) [2]. Вони можуть застосовуватися, в основному, для захисту від копіювання та несанкціонованого використання. На відміну від звичайних водяних знаків ЦВЗ можуть бути не тільки видимими, а й (як правило) невидимими. Невидимі ЦВЗ аналізуються спеціальним декодером, який виносить рішення про їхню коректність.

ЦВЗ можуть бути трьох типів: робастні, тендітні та напівтендітні.

Робастні стійкі до багатьох видів спотворень, тендітні руйнуються за невеликої модифікації контейнера, а напівкрихкі стійкі до одних спотворень і нестійкі до інших.

Крихкі ЦВЗ [3-6] руйнуються за незначної модифікації заповненого контейнера. Вони застосовуються для автентифікації сигналів. Відмінність від засобів електронного цифрового підпису (ЕЦП) полягає в тому, що тендітні ЦВЗ все ж таки допускають деяку модифікацію контенту. Це важливо для захисту мультимедійної інформації, оскільки законний користувач може, наприклад, побажати стиснути зображення. Інша відмінність полягає в тому, що тендітні ЦВЗ повинні не тільки відобразити факт модифікації контейнера, а й вид і місце розташування цієї зміни.

Напівкрихкі ЦВЗ стійкі щодо одних впливів і нестійкі щодо інших. Взагалі кажучи, всі ЦВЗ можуть бути віднесені до цього типу. Однак напівкрихкі ЦВЗ спеціально проєктуються так, щоб бути нестійкими щодо певного роду операцій. Наприклад, вони можуть дозволяти виконувати стиснення зображення, але забороняти вирізку з нього або вставлення в нього фрагмента.

У цій роботі детально розглянуто крихкі ЦВЗ. Тендітні ЦВЗ спроектовані так, щоб з високою точністю можна було виявити невеликі зміни в зображенні, в яке впроваджено водяний знак. Головне призначення крихких водяних знаків полягає в автентифікації зображення та захисті від модифікацій.

Постановка проблеми. Серед методів вбудовування тендітних ЦВЗ розрізняють вбудовування в просторову і частотну область зображення. Вони відрізняються ступенем стійкості до таких спотворень, як стиснення з втратами. Вбудовування в частотну область дає змогу стиснути зображення, наприклад, JPEG-компресією зі збереженням водяного знака в зображенні, а другий тип вбудовування передбачає руйнування знака за будь-якого виду модифікацій.

Одну з методик вбудовування крихких ЦВЗ у просторову область запропонував американський професор Ping Wah Wong [6].

У даній роботі ця ідея була доопрацьована включенням до методу конкретних функцій і алгоритмів таким чином, щоб їхні параметри узгоджувалися один з одним. На основі цього було розроблено алгоритми вбудовування тендітних ЦВЗ у цифрове зображення та перевірки його на факт модифікацій. Ці алгоритми було реалізовано мовою програмування C++.

Призначення і властивості крихких цифрових водяних знаків. Крихкий цифровий водяний знак одразу ж змінюється або руйнується при зміні зображення лінійним або нелінійним перетворенням. Тендітні мітки не підходять для захисту авторського права на цифрові зображення, оскільки зловмисник може зруйнувати впроваджений ЦВЗ, а тендітні ЦВЗ, за визначенням, легко зруйнувати. Завдяки чутливості крихких ЦВЗ до модифікації вони можуть бути використані під час ідентифікації зображення. Таким чином, це може становити інтерес для учасників обміну зображенням, щоб перевірити, що воно не було відредаговано, пошкоджено або змінено після впровадження в нього знака.

Системи автентифікації зображень застосовуються в судовій системі, торгівлі, безпеці та журналістиці. Оскільки цифрові зображення легко змінити, безпечна система автентифікації корисна для вказівки на те, що ніяке втручання не відбулося в тій ситуації, коли довіра до зображення може бути піддана сумніву. Прості приклади – впровадження ЦВЗ у зображення в базі даних для виявлення втручання, використання в журналістській фотокамері, щоб агентства преси могли гарантувати, що на зображенні не сфальсифіковано події, і впровадження ЦВЗ у зображення в торгівлі, щоб покупець був упевнений, що куплені зображення справжні. Також тендітні ЦВЗ використовуються на зображеннях, що є речовим доказом у суді, журналістських фотографіях, або зображеннях, які використовуються в електронному шпигунстві.

Інший спосіб перевірки автентичності цифрової роботи є використання системи електронного цифрового підпису. У цій системі підпис, яким будуть засвідчені дані, формується за допомогою криптографічних хеш-функцій [6]. Використовуючи отриманий хеш, дані криптографічно підписуються, таким чином, цей підпис пов'язаний з оригінальними даними. Потім одержувач перевіряє підпис, досліджуючи хеш (можливо змінений) даних і, використовуючи алгоритм перевірки, визначає, чи справжні дані. У той час як цілі створення тендітних водяних знаків і систем ЕЦП подібні, тендітні ЦВЗ мають невелику перевагу, оскільки вони все-таки припускають деяку модифікацію даних зображення (вставка водяного знака). Оскільки водяний знак впроваджено безпосередньо в зображення, ніяка додаткова інформація не потрібна для перевірки справжності (це не схоже на цифрові підписи, оскільки сам підпис має бути пов'язаний з переданими даними). Тому достатня інформація, необхідна в процесі перевірки автентичності, прихована, і її складніше видалити, ніж цифровий підпис. Крім того, системи ЕЦП розглядають зображення як довільний потік двійкових сигналів і не використовують його унікальну структуру. Тому система підпису може виявити, що зображення було змінено, але не може охарактеризувати зміни. На противагу цьому, багато систем створення крихких водяних знаків можуть визначити, які ділянки зображення були змінені, а які ні, а також оцінити природу змін.

Атаки на цифровий водяний знак. Існують потенційні атаки з боку зловмисних осіб на системи ЦВЗ. На сьогодні практично неможливо спроектувати систему, непроникну для всіх форм атак, і винайти вчасно нові методи захисту систем ЦВЗ. Але, звісно ж, знання загальних видів атак – важлива вимога для проєктування поліпшених систем.

Перший тип атаки – проста модифікація зображення з ЦВЗ (тобто, довільна зміна зображення, припускаючи, що ніякого ЦВЗ не присутній). Ця форма атаки має бути чітко розпізнана будь-яким крихким водяним знаком, вона є найпоширенішою атакою, яку має врахувати система ЦВЗ. Різновиди цієї атаки включають підрізання та локальну заміну (таку як заміна обличчя однієї людини на іншу). Останній тип модифікації – суттєва причина для виявлення пошкоджених областей у межах зміненого зображення.

Інший тип атаки – спроба змінити зображення безпосередньо з ЦВЗ, не зачіпаючи його або створюючи нове, яке детектор сприйняв би як справжнє. Деякі слабкі крихкі ЦВЗ легко виявляють випадкові зміни в зображенні, але можуть бути не в змозі виявляти ретельно створену зміну. Наприклад, крихкий ЦВЗ, впроваджений у молодші біти зображення. Спроба змінити зображення, не розуміючи, що ЦВЗ впроваджено в молодші біти, цілком імовірно порушить ЦВЗ і зміну буде виявлено. Однак, тоді атакувальник може спробувати змінити зображення, не порушуючи молодших біт, або замінити новою множиною молодших біт змінене зображення, яке детектор класифікує як справжнє.

Атаки можуть також включати використання відомого правильного ЦВЗ з одного зображення як ЦВЗ для іншого, довільного зображення. Ця атака полегшується, якщо можливо дізнатися, як впроваджено ЦВЗ. Цей тип атаки може також бути виконаний на тому ж самому зображенні: знак спочатку видаляється, потім зображення змінюється, і, нарешті, ЦВЗ повторно вставляється.

Зловмисник може зацікавитися повним видаленням водяного знака, не залишаючи жодних слідів його існування. Щоб зробити так, атакувальник може спробувати додати білий шум у зображення, використовуючи методи, розроблені для видалення міток, або використовуючи статистичний аналіз оригінального зображення.

Атакувач може також спробувати обчислити ключ, за допомогою якого згенеровано ЦВЗ. Ключ тісно пов'язаний із впровадженим ЦВЗ, тож якщо можливо виділити водяний знак, то атакувальник може вивчити його у спробі вивести ключ (або зменшити область пошуку ключа, тобто його розмір). Щойно ключ виведено, атакувальник може підробити ЦВЗ і впровадити його в будь-яке довільне зображення.

Опис методу P.W. Wong-а захисту зображень. Одним із прикладів систем впровадження крихких ЦВЗ у просторову область є система, яку запропонував американський учений Ping Wah Wong.

Для вбудовування ЦВЗ у зображення в методі Wong-а зображення ділиться на блоки пікселів, що не перетинаються, ці блоки мають бути однакового розміру для всього зображення. Цифровий водяний знак, який необхідно вбудувати, являє собою довільну послідовність нулів і одиниць. Для кожного блоку водяні знаки створюються окремо, тому перед вбудовуванням ЦВЗ також розбивається на такі ж блоки. Після того, як зображення і ЦВЗ готові до початку операції вбудовування, для кожного блоку зображення виконується певний набір операцій:

1. Для семи старших значущих біт усіх пікселів блоку обчислюється хеш-функція.
2. До отриманого хеш-образу і відповідної цьому блоку частини ЦВЗ застосовується операція XOR (виключне «або»).
3. Отримане значення зашифровується симетричним криптоалгоритмом.
4. Зашифрована послідовність вбудовується в молодші біти цього блоку.

Для того щоб після закінчення деякого часу перевірити справжність цього зображення і відсутність у ньому модифікацій, застосовують алгоритм перевірки. Для цього зображення знову розбивається на блоки такі самі, як і в алгоритмі вбудовування. У наявності має бути вбудований цифровий водяний знак. Після цього для кожного блоку зображення проводиться набір операцій:

1. Як і в алгоритмі вбудовування, для семи старших значущих біт усіх пікселів блоку обчислюється хеш-функція.
2. З молодших біт витягується вбудована послідовність.
3. Ця послідовність біт розшифровується, використовуючи той самий симетричний алгоритм шифрування.
4. Для розшифрованої послідовності та хеш-образу проводиться операція XOR.
5. Результат порівнюється з двійковою послідовністю ЦВЗ для цього блоку і робиться висновок про те, чи втручався хтось у цей блок.

Вбудоване ЦВЗ, а також закритий ключ шифрування тримаються в секреті.

Після того, як цей алгоритм застосовано до всіх блоків зображення, стає зрозуміло, чи справжнє це зображення і чи була змінена якась частина зображення.

Саме розбиття на блоки зображення перед використанням алгоритму дає змогу провести локалізацію вироблених модифікацій і з'ясувати, що саме на зображення було замінено.

Опис розробленої системи. Для цього методу ЦВЗ являє собою довільну послідовність нулів і одиниць, однак у ролі впроваджуваного крихкого ЦВЗ може бути і двійкове зображення з графічним значенням (наприклад, логотип фірми) або безладно згенерований чорно-білий шаблон. Якщо ЦВЗ матиме візуально розпізнавану структуру, області, в які втрутився зловмисник, можуть бути виявлені візуально в порівнянні.

Розмір блоку має бути обраний так, щоб у нього міг бути впроваджений цілий хеш- образ, залежно від обраної хеш-функції. Наприклад, для хеш-функції MD5 – 128 біт і можливий розмір блоку може бути 8x16 пікселів.

Для цієї програми зображення, у яке буде вбудовуватися ЦВЗ, необхідно представити у 24-хрозрядному bmp-форматі. Це зображення програмно розбивається на однакові блоки 8x16 пікселів, де 8 пікселів – ширина блоку, а 16 – висота. У ті ділянки зображення, які не потрапили в блоки (менші за 8 пікселів завширшки і 16 заввишки), не вбудовується водяний знак. Однак, з огляду на те, що такі ділянки можуть бути тільки в правій і у верхній частині фотографії, а також те, що їхній розмір досить малий, можна зробити висновок про те, що зміни цих ділянок торкнуться і прилеглих ділянок. Ці зміни покаже вбудований крихкий ЦВЗ, а отже, областями, що відмовилися без ЦВЗ, можна знехтувати.

Сам цифровий водяний знак являє собою текст, розміром 16 байт. Це може бути прізвище, ім'я, нік власника в поєднанні з різними символами. Цей текст буде вбудований у кожен блок фотографії. При перевірці автентичності ЦВЗ можна порівняти не тільки програмно, а й візуально.

Ми використовуємо 24-хрозрядні малюнки, у яких один піксель зображення кодується трьома байтами, тобто містить три компоненти кольору – червоний, синій і зелений (RGB). Кожна компонента в пікселі займає 1 байт. Для правильної роботи програми необхідно ЦВЗ вбудовувати тільки в одну з компонент, розміром 1 байт. Програма для вбудовування вибирає червону компоненту.

Усі операції над одним блоком циклічно повторюються над кожним.

Зашифровану послідовність необхідно вбудувати в молодші біти всього блоку. Для цього використано метод заміни найменш значущого біта LSB (Least Significant Bit).

Цей метод найпоширеніший серед методів у просторовій області. Молодший значущий біт зображення несе в собі найменше інформації. Відомо, що людина в більшості випадків не здатна помітити змін у цьому біті. Фактично, LSB – це шум, тому його можна

використовувати для вбудовування інформації шляхом заміни найменш значущих біт пікселів зображення бітами нашої послідовності.

Популярність цього методу зумовлена його простотою і тим, що він дає змогу впроваджувати у відносно невеликі файли досить великі обсяги інформації. Метод найчастіше працює з растровими зображеннями, представленими у форматі без компресії (наприклад, GIF і BMP).

Таким чином, після вбудовування було змінено молодші біти червоної компоненти фотографії та остаточно впроваджено цифровий водяний знак.

Друга програма test.exe здійснює перевірку зображення на факт модифікації. Принцип роботи цієї програми схожий з першою, проте дії відбуваються у зворотному порядку: хешування семи старших біт даного блоку хеш-функцією MD5, з молодших біт витягується послідовність, довжиною 128 біт, розшифровується за допомогою закритого ключа, для отриманої 128-бітної послідовності та хеш-образу застосовується операція XOR. На виході цієї операції виходить послідовність, яка програмно порівнюється з оригінальним ЦВЗ. Якщо вони збігаються, програма видає результат про те, що зображення не модифіковано, якщо ж ні і зображення змінено, то програма сповіщає про модифікацію і створює окремий файл із зображенням, в якому вказує червоним кольором ті блоки, в яких відбулися зміни.

Під час тестування цієї програми були проведені різні зміни в оригінальному зображенні – підмальовування, вирізання фрагмента, обрізання фотографії, зміна одного пікселя зображення, зміна яскравості, контрастності всього зображення й окремого фрагмента та ін., на які програма відреагувала як на зміни зображення та відмітила змінені ділянки червоним кольором (рис. 1).

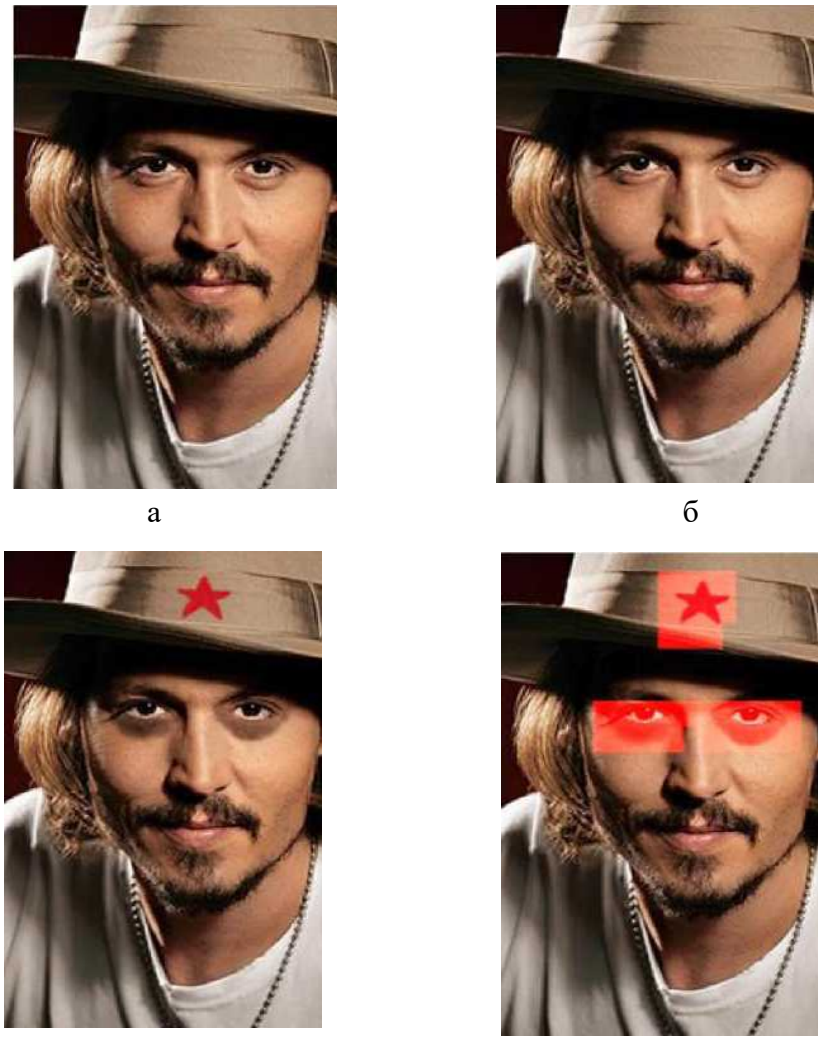
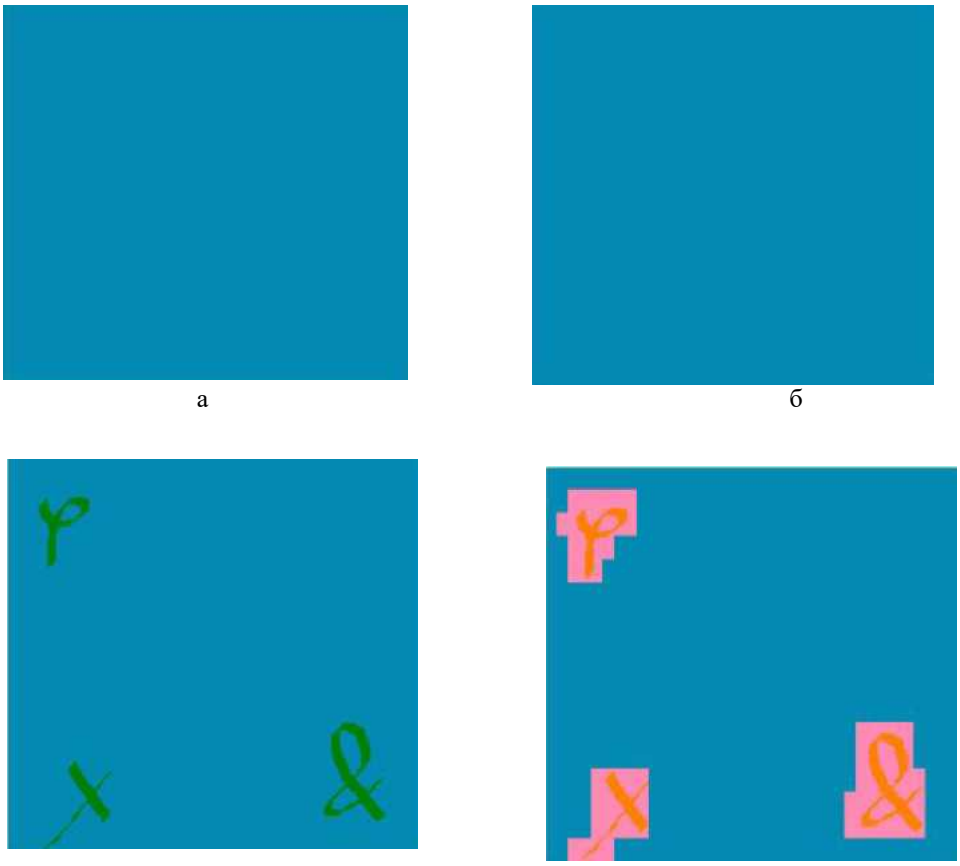


Рис. 1. Приклади роботи програм mark.exe і test.exe (а – оригінал фотографії, б – фотографія з вбудованим ЦВЗ, в – змінена фотографія, г – фотографія після перевірки)

Для наочності роботи програм було проведено експерименти над однотонним цифровим зображенням. Результати показано на рисунку 2.



а б в г

Рис. 2. Приклади роботи програм mark.exe і test.exe на однотонному зображенні (а – оригінал світлини, б – світлина з вбудованим ЦВЗ, в – змінена світлина, г – світлина після перевірки)

Висновки. Наявні в даний час публікації, присвячені стеганографії, або є науково-популярними, що не зачіпають математичних аспектів зазначеної науки, або зачіпають лише вузькі аспекти цієї науки. І тому, вони не в змозі повною мірою забезпечити зазначені потреби.

Проведено аналіз стеганографічних методів захисту цифрових зображень, виокремлено можливі види атак на них. Наведено опис типів цифрових водяних знаків та їхнє призначення. Детально розглядаються крихкі цифрові водяні знаки, їхнє призначення, властивості та методи вбудовування в зображення.

Виконано аналіз методу американського вченого P.W.Wong-а вбудовування цифрових водяних знаків у зображення. Показано, що для вирішення цілої низки практичних завдань інформаційної безпеки сьогодні недостатньо зробити інформацію недоступною для порушника (як відомо, вирішенням цього завдання займається криптографія). Найчастіше потрібно приховати сам факт її передавання – таким є класичне завдання стеганографії. Стеганографічний захист фотографій з використанням тендітних водяних знаків можна застосувати в тих випадках, коли перевірити справжність і цілісність цифрової фотографії може тільки її власник, оскільки секретний ключ і ЦВЗ зберігаються тільки у нього. Перевагою цього підходу є те, що під час перевірки не потрібне оригінальне зображення.

Обґрунтовано вбудовування цифрових водяних знаків призначених для захисту авторських і майнових прав на цифрову інформацію різного роду, і впровадження в цифрові дані ідентифікаційних міток, призначених для маркування об’єктів у цифрових сховищах даних.

На прикладі аналіз методу вбудовування цифрових водяних знаків у зображення розроблено модифікований алгоритм, у якому використовуються конкретні функції, параметри яких узгоджені одна з одною. Цей алгоритм реалізовано мовою програмування C++. При цьому показано, що використання цифрових водяних знаків не регламентується спеціальними законами, сам цифровий водяний знак, секретний ключ шифрування, а також увесь алгоритм вбудовування і перевірки автентичності рекомендується засвідчити в нотаріуса. Після чого бажано записати на знімний носій, призначений тільки для читання і помістити до банківського сейфу або залишити на відповідальне зберігання в нотаріуса. Крихкі цифрові водяні знаки можуть застосовуватися в поєднанні з електронним цифровим підписом для забезпечення більшої надійності.

Список використаних джерел:

1. Хорошко В.О., Азаров О.Д., Шелест М.Є., Яремчик Ю.Є. Основи комп'ютерної стеганографії: Навчальний посібник для студентів та аспірантів. – Вінниця: ВДТУ, 2003. – 143 С.

2. Shivani S., Agarwal S., Suri J. S. Fragile Watermarking. – Глава в «Handbook of Image- based Security Techniques» – eBook – Published28 May 2018 – Pub. Location: New York, Imprint: Chapman and Hall/CRC, DOI https://doi.org/10.1201/9781315166964

3. Нейл Ф. Джонсон, Зоран Дуріч, Сушил Джаджодіа, Приховування інформації: стеганографія та водяні знаки. – Атаки та контрзаходи. Kluwer Academic Publishers. 2001. 160p.

4. He, H.; Chen, F.; Tai, H.; Kalker, T.; Zhang, J. Аналіз продуктивності схеми фрагментарного водяного знаку, що ґрунтується на самопоновленні, на основі блок- сусідства. IEEE Trans. Inf. Forensics Secur. 2012, 7, 185-196.

5. Lin C.C., He S.L., Chang C.C. Піксельне парне крихке водяне маркування крихких зображень, що ґрунтується на кодуванні блочного зрізання абсолютного моменту на основі HC. Electronics 2021, 10, 690.

6. P. W. Wong, «A public key watermark for image verification and authentication,» Proceedings of the IEEE International Conference on Image Processing, vol. 1, pp. 455-459, Chicago, Illinois, October 1998.

References:

1. Khoroshko V.O., Azarov O.D., Shelest M.YE., Yaremchyk YU.YE. Osnovy komp'yuternoyi stehanohrafiyi: Navchal′nyy posibnyk dlya studentiv ta aspirantiv. – Vinnytsya: VDTU, 2003. – 143 S.

2. Shivani S., Agarwal S., Suri J. S. Fragile Watermarking. – Hlava v «Handbook of Image- based Security Techniques» – eBook – Published28 May 2018 – Pub. Location: New York, Imprint: Chapman and Hall/CRC, DOI https://doi.org/10.1201/9781315166964

3. Neyl F. Dzhonson, Zoran Durich, Sushyl Dzhadzhodia, Prykhovuvannya informatsiyi: stehanohrafiya ta vodyani znaky. – Ataky ta kontrzakhody. Kluwer Academic Publishers. 2001. 160p.

4. He, H.; Chen, F.; Tai, H.; Kalker, T.; Zhang, J. Analiz produktyvnosti skhemy frahmentarnoho vodyanoho znaku, shcho gruntuyet′sya na samoponovlenni, na osnovi blok- susidstva. IEEE Trans. Inf. Forensics Secur. 2012, 7, 185-196.

5. Lin C.C., He S.L., Chang C.C. Piksel′ne parne krykhke vodyane markuvannya krykhkykh zobrazhen′, shcho gruntuyet′sya na koduvanni blochnoho zrizannya absolyutnoho momentu na osnovi HC. Electronics 2021, 10, 690.

6. P. W. Wong, «A public key watermark for image verification and authentication,» Proceedings of the IEEE International Conference on Image Processing, vol. 1, pp. 455-459, Chicago, Illinois, October 1998.