УДК 621.384.3

Б. В. Павленко, Д. П. Присяжний,
В. В. Карпінець, Я. Ю. Яремчук
Вінницький національний технічний університет
Хмельницьке шосе, 95, 21021 Вінниця, Україна

Підвищення стійкості методу захисту забезпечення автентичності растрових зображень доказової бази від несанкціонованого доступу

Запропоновано метод на основі комбінації і модифікації існуючих стеганографічних методів. Визначено критерії і метрики оцінювання, за якими досліджено його стійкість до несанкціонованих модифікацій при низькому рівні спотворення. Запропонований комбінований метод увібрав у себе сильні сторони існуючих методів і показав значно вищу вказану стійкість. Метод удосконалено шляхом вбудовування цифрових водяних знаків за методом Коха-Жао. Цей метод представлено у формалізованій формі, розроблено алгоритм, здійснено його опис і практичну реалізацію у вигляді програмного продукту, наведено результат роботи програми.

Ключові слова: *захист інформації, стеганографія, цифрові водяні знаки, метод заміни найменш значущого біта, метод Куттера-Джордана-Боссена, метод Ленгелаара, метод Коха-Жао.*

Вступ

У слідчій і судовій практиках кримінального судочинства зустрічаються факти знищення або підроблення доказів. Такі випадки найбільш характерні для досудового провадження. Зафіксовані такі випадки також з боку співробітників правоохоронних органів і навіть владних структур. Оскільки цифрові зображення можуть відігравати роль основних доказів правопорушення, необхідно контролювати їхню цілісність протягом усього часу їхнього зберігання.

Існує доцільність розробки програмних засобів, які можуть підвищити ефективність вирішення проблем захисту інформації у сфері банківської діяльності та електронної комерції, в інформаційних системах військового призначення, судовій системі тощо [1].

Наприклад, перевірка автентичності цифрового зображення, що входить до доказової бази судової системи, є одним із важливих процесів, оскільки зображення можуть виступати в ролі головних доказів. Зміна доказів або їхня модифікація

можуть значно вплинути на розгляд справи у суді, тому доцільно перевіряти автентичність файлів [2].

Для вирішення задач перевірки автентичності файлів і їхньої цілісності використовуються цифрові водяні знаки, хеш-функції [3]. Одними із найбільш розповсюджених методів є стеганографічні методи накладання цифрових водяних знаків, які застосовуються для вирішення таких завдань:

— захисту конфіденційної інформації від несанкціонованого доступу;

— захисту авторського права на інтелектуальну власність;

— підтвердження автентичності файлу.

Найбільшої популярності здобули методи вбудовування цифрових водяних знаків, що використовують як контейнер зображення. Наприклад, одними із найбільш розповсюджених методів є стеганоалгоритми, які вбудовують інформацію у частотну область. Перевагами таких методів є висока швидкодія, стійкість до частотного детектування, руйнування молодших біт контейнера, атак JPEG-стисненням, обрізання країв. Однак такі методи мають недоліки стійкості до атак зашумлення.

Усі наявні методи перевірки автентичності можна розділити на такі групи:

1) метод на основі контролю EXIF-інформації;

2) методи, що базуються на захисті сховища даних;

3) методи, що базуються на використанні хеш-функцій;

4) методи, що базуються на використанні стеганографічних алгоритмів;

5) методи, що базуються на використанні комбінованих алгоритмів;

6) методи можуть базуватися на використанні комбінованих алгоритмів, це поєднання двох чи більше наведених вище методів, що дозволяє значно підвищити стійкість захисту. До таких методів відносяться поєднання електронного цифрового підпису та цифрових водяних знаків (ЦВЗ), поєднання ЦВЗ і хеш-функцій.

Постановка задачі та методика дослідження

Провести дослідження стійкості методів забезпечення автентичності зображень до спотворень, виявити та проаналізувати їхні недоліки щодо стійкості. Проаналізувати можливості підвищення стійкості до несанкціонованих модифікацій.

Розробити вдосконалений метод забезпечення автентичності цифрових зображень для використання у судовій системі зі збільшенням стійкості до несанкціонованих модифікацій. Здійснити програмну реалізацію та проаналізувати стійкість удосконаленого методу.

Дослідження стійкості методів перевірки автентичності до спотворень

Під час стеганографічного аналізу методів, які використовуються для вбудовування інформації, зазвичай аналізується спотворення контейнеру після обробки певним методом. Показники спотворення, або критерії якості, можуть бути віднесені, незалежно від їхнього виду, до різних груп показників спотворення.

Проведено аналіз стійкості таких методів ЦВЗ:

— заміни найменш значущого біта;

— Коха-Жао (далі — метод Коха);

— Куттера-Джордана-Боссена (далі — Куттера);

— Лангелаара [4].

Обґрунтування вибору методів для аналізу відбувається за двома критеріями. Перший критерій — методи мають відноситися до відкритих стеганографічних систем, що автоматично підвищує можливість їхнього використання. Також у даних методах перевірка ЦВЗ відбувається без початкового контейнеру (оригіналу), що значно розширює сферу застосування. Другий критерій — варіативність технік модифікації зображень. Тобто, кожен обраний метод повинен мати свою відмінну техніку модифікації.

У цьому зв'язку метод Коха оперує частотним представленням інформації зображення, а методи Куттера та Лангелаара — просторовим поданням. Проте у методів Коха та Лангелаара є спільна особливість — вони працюють поблоково з інформацією, у той час коли метод Куттера використовує покрокове вбудовування зображення.

Для аналізу було обрано такі критерії стійкості: додавання рівномірного та гауссівського шуму, застосування імпульсного шуму, размиваюча фільтрація та стиснення з утратами за алгоритмом JPEG.

Для проведення аналізу кожного методу було вбудовано 512 байт інформації в канал яскравості зображення, щоб тестування відбувалося в однакових умовах. Було обрано повідомлення, згенероване псевдовипадковим генератором, що представляє послідовність довжиною 32 байти, та продубльовано шістнадцять разів для збільшення надійності та приведення до реальних умов використання. Після того, як збережено зображення із вбудованим повідомленням, було накладено перетворення, яке спотворює зображення. Під час вилучення ЦВЗ отриманий вектор довжиною 512 байт ділився на 16 послідовностей (підвекторів) довжиною 32 байти. Як результат приймалося усереднене значення з отриманих 16 підвекторів.

Як основний показник коректності розпізнавання використовувалося відношення кількості невірно розпізнаних бітів повідомлення до їхньої загальної кількості, Bit Error Rate (BER), що має значення у діапазоні (0, 1). Для надійності виміряне значення BER усереднювалося по 5-ти дослідах. У ролі контейнера виступало кольорове зображення Lena розміром 512×512 пікселів, що широко використовується у тестах стеганоалгоритмів.

Кожен із методів вбудовування ЦВЗ має параметр, що відповідає за силу вбудовування. При збільшенні сили підвищується стійкість ЦВЗ, проте також збільшується спотворення зображення. При порівнянні різних методів є необхідність використовувати оптимальне відношення між стійкістю ЦВЗ до зовнішнього впливу та візуальною модифікацією зображення.

Виведення метрики, яка би показала візуальну значимість змін, є серйозною проблемою, яка на сьогодні не має задовільного вирішення. Візуальну значимість змін поки може оцінювати тільки людина, проте можна вирахувати за статистичними метриками. Тому для визначення раціональних параметрів вбудовування застосовується такий напівавтоматичний підхід. Спочатку за одним із методів створюється серія зображень з поступовим збільшенням параметра, що впливає на силу вбудовування, від зображення до зображення. З цієї серії вибирається таке зображення, яке візуально показує прийнятний рівень спотворень. Для значення параметра, відповідного даному зображенню, вимірюється пікове співвідношення

сигнал/шум, яке оголошується еталонним. Далі для всіх інших методів підбираються параметри, які відповідають еталонному значенню метрики. Для цих параметрів з невеликим відхиленням створюється кілька зображень. За результатами візуальних спостережень значення параметрів коригуються від тих, які дають еталонне значення метрики.

Дослідження стійкості обраних методів проводилося за кількома відомими тестами. За результатами тестування найбільшу стійкість до спотворення рівномірним шумом показали методи Лангелаара та Куттера, для яких значення BER було близько до нуля при рівнях шуму до 50. Метод Куттера, однак, має більший запас міцності, оскільки показав значення BER менше 0,1, навіть при рівні шуму 100.

Найбільш стійким до додавання гауссівського шуму (нормально розподіленої величини з нульовим математичним очікуванням) виявився метод Куттера.

Також було перевірено стійкість методів до додавання шуму в області перетворення. Для цього було обрано два перетворення, з якими не працює жоден із досліджуваних методів: перетворення Фур'є та вейвлет-перетворення.

У Фур'є-перетворенні було застосовано імпульсний шум, привласнюючи великі значення фіксованої кількості випадково обраних коефіцієнтів Фур'є-спектра. У вейвлет-перетворенні застосовувався рівномірний шум у піддіапазоні HH-коефіцієнтів першого рівня перетворення.

Проведено тести на стійкість до таких фільтрів: середньоарифметичний, адаптивний локальний, медіанний, фільтр серединної точки та білатеральний. Вимірювалося значення BER при різній кількості застосувань фільтра, найбільш стійким до усіх видів фільтрів виявився метод Коха.

У тесті на стійкість до JPEG-стиску зображення стискалося за алгоритмом JPEG з різними значеннями параметра, що відповідає за якість стиснення, найбільшу стійкість до цього типу спотворення показав метод Коха.

Виходячи з отриманих результатів досліджень, можна сказати, що жоден з обраних методів недостатньо стійкий до усіх видів атак.

Запропонований комбінований метод полягає в незалежному вбудовуванні одного ЦВЗ кожним зі складових методів. На етапі вилучення враховується вплив спотворення, якому був підданий стегоконтейнер: при впливі шумом вилучається ЦВЗ, вбудований за методом Куттера, при впливі фільтрацією — ЦВЗ, вбудований за методом Коха. Була протестована стійкість комбінованого методу у відповідних видах впливу, яким піддавалися раніше окремі способи. Виявилося, що ЦВЗ, вбудовані трьома обраними методами, можуть співіснувати в одному зображенні, лише незначно збільшуючи значення BER один одного при добуванні ЦВЗ (до 0,03). У результаті комбінований метод виявляється стійким до шуму, як метод Куттера, стійким до фільтрації як метод Коха, і стійким до JPEG-стиску як метод Лангелаара. Щоб застосовувати такий метод на практиці треба створити стегосистему з можливістю або визначення типу впливу на стегоконтейнер, або відбору серед декількох ЦВЗ потрібного за деякими критеріями [5].

Метод забезпечення автентичності цифрових зображень складається з двох основних частин, а саме: стеганографічного методу вбудовування ЦВЗ та алгоритму хешування.

Детально розглянуто саме стеганографічний метод і можливості його модифікації, оскільки ЦВЗ відіграє важливу роль у перевірці автентичності зображень.

Для цього розглянуто використання стеганографічного методу Коха-Жао для вбудовування цифрових водяних знаків, який використовує частотну область контейнера та полягає у відносній заміні величин коефіцієнтів дискретного косинусного перетворення (ДКП). Перевагами методу є використання частотної області, важкість випадкового знаходження ЦВЗ, легкість виявлення порушень. До недоліків можна віднести труднощі реалізації та низьку пропускну здатність.

Шляхи до вдосконалення методу для підвищення стійкості до несанкціонованих модифікацій

Одними із варіантів удосконалення методу Коха-Жао є використання заміни величин коефіцієнтів ДКП і збалансований вибір величин коефіцієнтів ДКП. Дане вдосконалення полягає у виборі лише середньочастотних коефіцієнтів ДКП, оскільки модифікації низькочастотних коефіцієнтів призводять до значного спотворення зображень, а модифікація високочастотних коефіцієнтів піддається сильним змінам при атаках стиснення. Дане вдосконалення дозволяє отримати середнє покращення відношення сигнал/шум на 11,67 % відносно початкового методу та підвищення робастності на 8,26 %.

Також одним із можливих удосконалень є підвищення стійкості до завад шляхом використання завадостійкого кодування, яке дозволяє при внесенні надмірності кодованої інформації надати можливість корегування помилок, які виникають при передаванні даних або при атаках зловмисника. Спотворення, які внесені шумом або атаками на стеганограму, викликають імовірність того, що метод не зможе розпізнати цифровий водяний знак. Метод Коха-Жао дозволяє знаходити початок повідомлення за допомогою спеціальних міток, які додані до повідомлення або ЦВЗ. Для підвищення стійкості стеганографічного методу доцільно використовувати завадостійке кодування саме для цих міток, оскільки тоді можна буде визначити наявність самого повідомлення або водяного знаку в контейнері. Перевагою такого методу є спрацьовування методу при меншому значенні сигнал/шум [6].

Однією із можливих модифікацій є порогова величина P, яка є різницею між абсолютними значеннями ДКП. При збільшенні порогової величини збільшується стійкість до атак стиснення та атак накладення шуму, проте це зменшує якість вихідного зображення.

Ще одним напрямком удосконалення є збільшення пропускної здатності стеганоалгоритму — це використання не лише синьої компоненти зображення, але і зеленої, як колірної компоненти, зміни якої малопомітні оку людини. Також можна використовувати перехід до іншої колірної моделі, що дозволяє використовувати нестандартні підходи до використання методу Коха-Жао.

Збільшення стійкості відбувається за рахунок використання комплексного підходу, а саме використання криптографічних засобів та алгоритмів для модифікації вбудованого повідомлення або ЦВЗ. У разі виявлення факту передавання стеганографічним каналом, зловмисник не має доступу до повідомлення. У іншому випадку це може становити додатковий етап перевірки автентичності, оскільки тільки справжнє повідомлення буде зашифровано та розшифровано коректно обома сторонами обміну.

Важливою складовою методу є алгоритм хешування. В роботі запропоновано використовувати алгоритм SHA-512. Розглянемо деталі та можливості його модифікації.

У 2001 році NIST прийняв як стандарт три хеш-функції з істотно більшою довжиною хеш-коду. Дані функції входять до групи SHA-2, в їхній назві вказана довжина створюваного хеш-коду (SHA-256, SHA-384 та SHA-512) [7].

Перевагами даного методу є більша довжина дайджесту повідомлення та його вища стійкість. До недоліків можна віднести повільність обрахування.

Шляхом удосконалення алгоритму хешування є зміна розрядності алгоритму SHA-2 або використання іншого алгоритму хешування.

При зміні розрядності в межах групи алгоритмів SHA-2 ми не отримаємо виграшу у стійкості, оскільки обраний алгоритм при однаковій складності обрахування з SHA-384 має більшу довжину дайджесту в 512 біт.

Для зміни алгоритму хешування можна розглянути алгоритми SHA-1, SHA-3 та MD-5 як одні з найпопулярніших алгоритмів, які застосовуються у системах безпеки.

Алгоритм SHA-1 є застарілим та має багато проведених успішних атак на отримані дайджести. Алгоритм MD-5 — також застарілий, який має безліч відомих атак та малу довжину вихідного дайджесту.

Використання алгоритму SHA-3 дозволяє збільшити стійкість методу, проте програмна реалізація даного алгоритму хешування є складнішою.

Виходячи з проаналізованих можливостей модифікацій, було визначено, що алгоритм хешування SHA-2 є раціональним за рахунок відношення стійкості до швидкодії. При аналізі можливості вдосконалення стеганографічного методу було проаналізовано наявні шляхи модифікації методу та визначено що для покращення характеристик методу буде доцільно використовувати завадостійке кодування та підвищити надійність самого ЦВЗ, що вбудовується, шляхом криптографічних перетворень.

Удосконалення методу забезпечення автентичності растрових зображень

Запропонований метод вбудовування ЦВЗ має дві основних частини: частину вбудовування та частину забезпечення надійності ЦВЗ. Підсистема забезпечення надійності вбудовування ЦВЗ створена для покращення властивостей початкового методу Коха-Жао, а саме складності отримання цифрового водяного знаку, навіть знаючи алгоритм вбудовування. Для цього буде використано хаотичний алгоритм шифрування та кодування Арнольда.

Хаотичний алгоритм шифрування є ефективним методом для шифрування даних. Хаотичні сигнали характерні якостями псевдовипадковості, незворотності та динамічної поведінки. Системи, що мають хаотичний характер, мають високу чутливість до початкових параметрів. Вихідна хаотична послідовність схожа на білий шум, що має випадкову поведінку з покращеною кореляцією та складністю відтворення [8, 9], і визначається формулою

$$C_{n+1} = \mu \times C_n \times (1 - C_n), \tag{1}$$

де $0 < \mu < 4$, стандартно використовують значення 3,9 для досягнення найбільшої випадковості, та $0 < C_n < 1$.

Різні значення C_n можуть бути отримані зміною значення n від 0 до $L-1$, де L — максимальна кількість потрібних хаотичних значень. При встановленні початкових значень μ та C_0 можливо отримати необхідний хаотичний сигнал.

Оскільки це пропонує спільну перевагу швидкості та безпеки, доведено, що використання хаотичного шифрування збільшує безпеку [10]. Безпека інформації може бути збільшена, використовуючи різні методи шифрування, одним з ефективних методів є перетворення Арнольда [11]. Даний метод шифрування є двомірним і добре працює у програмах для шифрування зображень типу $N \times N$. Математична модель перетворення Арнольда:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} (\mathrm{mod}\, N), \tag{2}$$

де (x_n, y_n) — вхідні координати зображення.

Результатами перетворення є зміна позицій пікселів для генерації зображення,яке буде невпорядковане та буде відрізнятися від початкового. Результатом перетворення Арнольда є зашифроване зображення, яке має відповідність один до одного з оригінальним зображенням. Псевдовипадковість перетворення Арнольда у результаті дає спотворене зображення, яке неможливо повернути до початкового стану без знання відповідної послідовності, яка була використана [12]. Стійкість шифрування залежить від кількості ітерацій, що можуть бути визначені окремо для кожного зображення на початку роботи алгоритму.

Зворотне перетворення Арнольда використовується для розшифровування повідомлення яке було вбудовано, та повернення зображення до початкового вигляду

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ -11 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (\mathrm{mod}\, N), \tag{3}$$

де (x, y) — зашифровані координати пікселів зображення, що відображені як двовимірна матриця.

Виходячи з розглянутих алгоритмів, можна побудувати модифікацію методу Коха-Жао, яка буде використовувати дані методи для підвищення захисту. Початкове зображення проходить через процес передобробки, який конвертує вхідне зображення з кольоровою схемою RGB у зображення з кольоровою схемою YCbCr, де Y — компонента освітленості, Cb — компонента синього кольору, Cr — компонента червоного кольору зображення.

Компонента яскравості Y висувається як параметр для модифікацій для вбудовування водяного знаку, оскільки модифікація цієї частини зображення приносить менш помітну зміну до фактичного зображення порівняно з модифікаціями компонентів кольору.

Після передобробки зображення отримана матриця розбивається на блоки 16×16. Для початкового зображення розмірами $M\times N$ кількість блоків буде дорівнювати:

$$\frac{M}{16}\times\frac{N}{16}. \tag{4}$$

Кожному з таких блоків можна присвоїти індекс B_x. Блок B_x далі буде поділений на чотири блоки 8×8 з індексами B_{x1}, B_{x2}, B_{x3}, B_{x4}. Загальна кількість блоків 8×8 буде:

$$4\times\left(\frac{M}{16}\times\frac{N}{16}\right). \tag{5}$$

Загальна кількість біт інформації, що може бути поміщена у контейнер, буде дорівнювати загальній кількості блоків розмірністю 8×8. Запропонований метод використовує переваги дискретного косинусного перетворення, а саме кореляцію суміжних блоків. Для цього обраховується значення дискретного косинусного перетворення для кожного з блоків 8×8. Нехай коефіцієнти ДКП блоку B_x відображені коефіцієнтами C_{x1}, C_{x2}, C_{x3}, C_{x4}. Для вбудовування біту ЦВЗ обраховується різниця між двома обраними коефіцієнтами ДКП двох сусідніх блоків:

$$D = C_{xy}(i,j) - C_{xy+1}(k,l), \tag{6}$$

де $(i,j)\neq(k,l)$ — позиція обраного коефіцієнту підблоків $1\le i,j,k,l\le8$.

Для поточної реалізації i,j,k,l відповідно обрано значення: 3; 3; 3; 2.

З формули (3) можна зробити висновок, що для вбудовування першого біту ЦВЗ береться різниця між коефіцієнтами, що отримані з блоку C_{x1} та блоку C_{x2}. Відповідно вбудовування наступного біту цифрового водяного знаку відбувається за різницею коефіцієнтів C_{x2} та C_{x3}. Різниця D модульована відповідно до біту інформації, що вбудовується.

Різниця змінюється додаванням коефіцієнта та віднімання іншого коефіцієнта на значення $\Delta/2$, де Δ — сума модифікації, яку потрібно внести між двома коефіцієнтами ДКП ітераційно до різниці, яка досягає певної зони. Це необхідно для забезпечення модифікації значення на величину, а не для зміни лише одного коефіцієнта на велике значення.

Розрахунок фактору модифікації:

$$\Delta_{xy} = \alpha\times\frac{DC(C_{xy}) - Median(C_{xy})}{DC(C_{xy})}, \tag{7}$$

де α — коефіцієнт множення, який варіюється від 0,2 до 2,5, ним задають рівень надійності системи (чим вище значення α, тим більший рівень надійності); $DC\left(C_{xy}\right)$ — коефіцієнт ДКП блоку C_{xy} і $Median(C_{xy})$ є середньою частотою перших тринадцяти низькочастотних коефіцієнтів [13]. З формули (6) можна побачи-

ти, що фактор модифікації Δ адаптивний для різних блоків залежно від даних даного блоку.

Перед вбудовуванням ЦВЗ проводиться дворівневе шифрування ЦВЗ для підвищення безпеки. Перший етап — застосування хаотичного шифрування до ЦВЗ на основі формул:

$$C'(x) = round(C(x) \times 10^4), \tag{8}$$

$$C''(x) = binary(C'(x)), \tag{9}$$

$$b(x) = xor\ all\ bits\ of\ C''(x), \tag{10}$$

де C — згенерована послідовність за допомогою хаотичного кодування; C' — чотиризначне ціле число, що отримане в результаті множення C на число 104 і округлене до найближчого цілого; C'' — бінарна послідовність, яка визначена з C' та функції $b(x)$, визначеної за допомогою операції виключної диз'юнкції між операндами.

З отриманих даних після хаотичного кодування обирається 4096 значень. Перший рівень шифрування ЦВЗ виконується за допомогою операції виключної диз'юнкції між послідовностями w та b:

$$w_{e1} = w(x)\, XOR\, b(x), \tag{11}$$

де w_e — ЦВЗ після першого етапу шифрування.

Наступним етапом перетворення ЦВЗ є трансформація Арнольда, що проводиться з отриманим значенням w_{e1} для отримання ЦВЗ w_e. Перевагою цих двох методів є те, що немає необхідності зберігати велику кількість ключів. Необхідно зберігати кількість ітерацій, проведених для зображення, значення ініціалізації алгоритму та логічні зв'язки параметрів. Проте безпека ЦВЗ у такому випадку не є високою, оскільки при відомих значеннях μ, C_0, та L можна згенерувати таку ж послідовність за формулою (1) та розшифрувати значення ЦВЗ.

Логічний параметр μ обмежений значеннями від 1,34 до 3,9 і обраховується за допомогою 8-бітного ключа за формулою

$$\mu = 1{,}35 + \frac{decimal(K_1)}{100}, \tag{12}$$

де K_1 — це 8-бітний ключ, який вносить параметр безпеки до логічного параметра μ.

За схожим принципом можливо обраховувати початкове значення C_0, використовуючи 4-бітний ключ K_2:

$$C_0 = 0{,}1 + \frac{decimal(K_2)}{17}, \tag{13}$$

де C_0 може знаходитися в рамках 0,1 та 0,9.

Кількість хаотичних значень L у хаотичній послідовності обчислюється, використовуючи 19-бітний ключ K_3:

$$L = 4096 + decimal(K_3). \tag{14}$$

Хаотична послідовність C розділена на частини, кожна з яких має розмірність 2048 бітів, та набір з n_c частин. З цих частин обирається лише дві частини, для чого використовується вісім бітів для обрання частин. K_4 — адреса першої частини, тоді наступна частина обирається за формулою

$$K_5 = n_c - decimal(K_4), \tag{15}$$

де K_5 — адреса другої частини.

Ці дві частини при поєднанні формують послідовність з 4096 біт, що складає довжину ЦВЗ. На наступному етапі шифрування використовується лише число ітерацій для трансформації Арнольда, яке генерується із використанням 6-бітного ключа K_6. Отримуємо загальний ключ K довжиною 53 біти, який підвищує стійкість ЦВЗ:

$$K = K_1 : K_2 : K_3 : K_4 : K_5 : K_6 . \tag{16}$$

Логічний параметр μ обмежений значеннями 1,35 та 3,9 з найбільшим хаотичними змінами при встановленні значення, що дорівнює 3,9, яке надає найбільшу стійкість ЦВЗ. Початкове значення C_0 може бути обмежене значеннями 0 та 1; для покращення статистичних властивостей було обрано генерувати даний параметр на основі ключа.

Для вбудовування ЦВЗ обирається блок 16×16, в якому міститься 4 біти зашифрованого ЦВЗ, як показано на рис. 1.

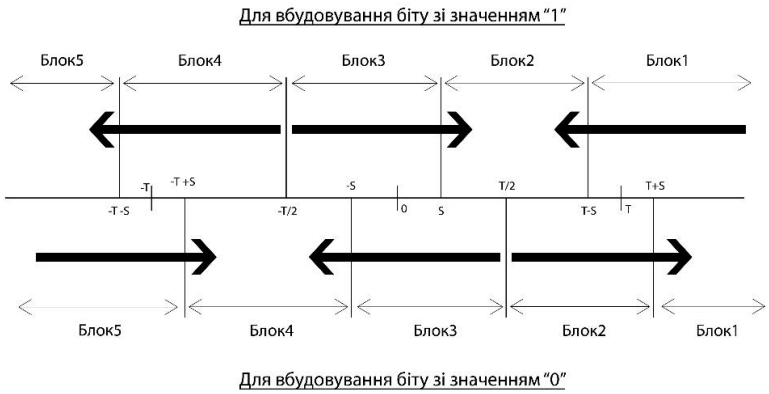

Рис. 1. Модифікації значень при вбудовуванні бітів 1 та 0

Для приховування біту зі значенням 1 (рис. 1), обирається блок 2 або блок 5 відповідно до різниці між коефіцієнтами D до вбудовування. Якщо коефіцієнт D знаходиться у блоці 1 або 3, тоді коефіцієнти $C_{xy}(i,j)$ та $C_{xy+1}(k,l)$ модифікуються

для того, щоб увійти до блоку 2, який являється найближчою коректною зоною для вбудовування біту зі значенням 1. Якщо різниця між коефіцієнтами D належить до блоку 4, то коефіцієнти модифікуються так, щоб різниця знаходилася у блоці 5. Виходячи з цього, для вбудовування біту зі значенням 1 будуть використані блоки 2 та 5. Формалізований алгоритм модифікації значення коефіцієнтів представлений на рис. 2.

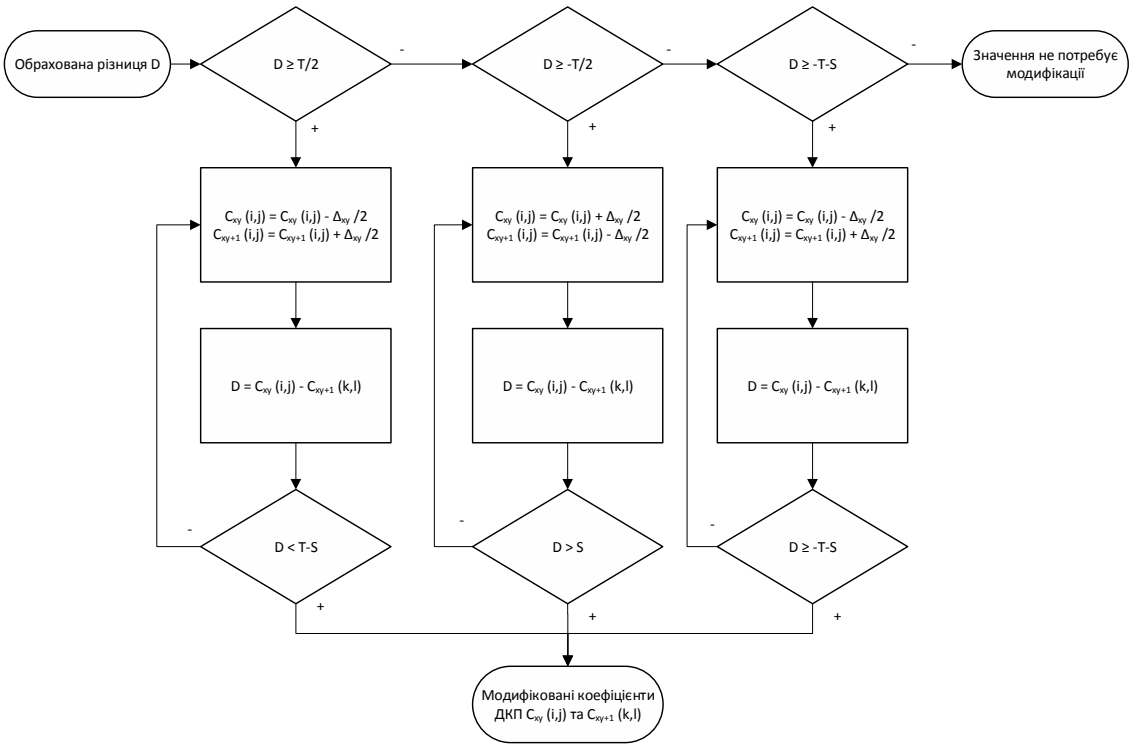

Рис. 2. Алгоритм модифікації коефіцієнтів для вбудовування біту зі значенням 1

Отже для вбудовування біту зі значенням 0, якщо різниця початкових значень лежить у блоці 2, коефіцієнти модифікуються так, щоб різниця належала до блоку 1. Якщо різниця між коефіцієнтами належить 5-му або 3-му блокам, коефіцієнти модифікуються так, щоб різниця належала блоку 4. Алгоритм модифікації коефіцієнтів зображений на рис. 3.

З рис. 1 можна побачити, що блоки для певного біта розділені захисним значенням $2S$, де S — енергія вбудовування, яка визначає надійність системи водяних знаків. Значення S доцільно обирати в межах від 5 до 20. Надійність системи прямо пропорційна обраному значенню S. Після вбудовування проводиться зворотне ДКП кожного з модифікованих блоків. Після виконання зворотного ДКП відбувається процес обробки зображення, який включає у себе додавання до значення кожного модифікованого блоку 128 так, щоб інтенсивність була у межах від 0 до 255. Також до процесу обробки зображення входить процес конвертування з кольорової схеми YCbCr до схеми RGB, після чого отримується остаточне зображення з накладеним цифровим водяним знаком.

Для видобування ЦВЗ із зображення необхідно провести процес передобробки, аналогічний процесу при вбудовуванні цифрового водяного знаку, а саме

розбиття зображення на блоки 16×16 і потім на підблоки 8×8, обчислення дискретного косинусного перетворення. Для подальшої роботи обираються лише ті коефіцієнти ДКП, які були модифіковані при вбудовуванні.

Біт інформації ЦВЗ обчислюється як різниця між двома коефіцієнтами. Якщо ця різниця знаходиться у блоці 2 або 5 (рис. 1), тоді обирається біт зі значенням 1, якщо отримана різниця знаходиться у блоці 1 або 4, тоді це свідчить про вбудований біт зі значенням 0. Після вилучення усіх бітів ЦВЗ виконується зворотній процес трансформації Арнольда та хаотичне кодування для отримання оригінального водяного знаку.

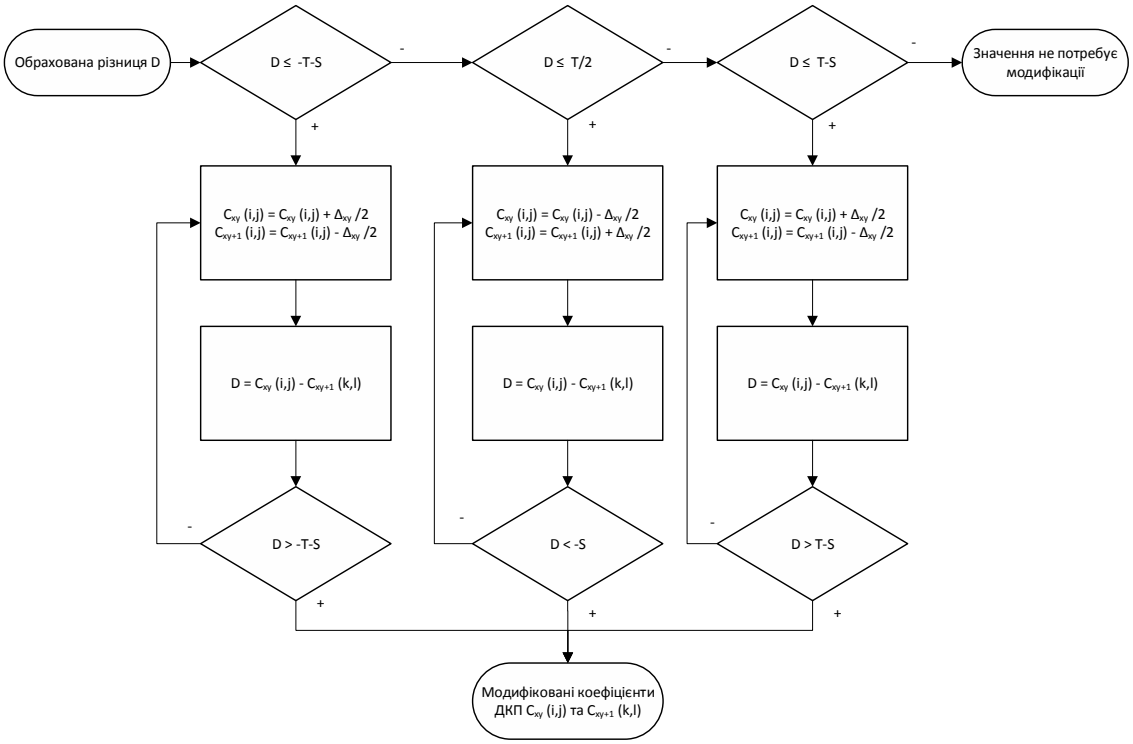

Рис. 3. Алгоритм модифікації коефіцієнтів для вбудовування біту зі значенням 0

Для вдосконалення методу забезпечення автентичності цифрових зображень необхідно модифікувати програму, яка буде включати два модулі: середовище, де дані будуть зберігатися, та модуль для вбудовування ЦВЗ і його перевірки, який необхідно розбити на підмодулі передобробки, криптографічних перетворень та обробки зображення, а також отримання хешу документа, що відповідатиме за основну логіку системи захисту.

Під час перевірки автентичності цифрового зображення, модуль захисту повинен перевіряти, чи співпадають хеші документів, і наявність і цілісність ЦВЗ. У випадку, якщо перевірка пройдена успішно, модуль захисту повинен повідомити користувача, відобразивши відповідне вікно.

Далі розглянемо детальніше кроки виконання алгоритму.

Крок 1. Вибір цифрового зображення.

Крок 2. Отримання унікального ключа користувача та генерація ключів для алгоритмів трансформації.

Крок 3. Розбиття на блоки та обраховування ДКП. Обране зображення згідно стеганографічного алгоритму розбивається на блоки розмірністю 16×16 пікселів, і до кожного блоку застосовується ДКП. Обираються коефіцієнти ДКП згідно запропонованих модифікацій.

Крок 4. Виконання перетворень ЦВЗ на основі хаотичного кодування.

Крок 5. Виконання перетворення отриманих на попередньому кроці даних за допомогою трансформації Арнольда.

Крок 6. Вбудовування модифікованого ЦВЗ.

Крок 7. Обробка отриманих даних після вбудовування ЦВЗ, після чого формується новий графічний файл.

Крок 6. Генерація значення хеш-функції. На основі отриманого файлу обраховується хеш-функція, що виконуватиме роль додаткового елемента перевірки автентичності файлу.

Крок 7. Внесення даних до сховища. Отримане значення хеш-функції, «тіло» файлу, та ключ ініціалізації алгоритму модифікації ЦВЗ вносимо до бази даних з додатковою інформацією у вигляді дати та часу вбудовування та інформації про користувача, що працював із системою.

Крок 8. Повідомлення користувача про результат роботи. Вивід користувачеві повідомлення про успішне опрацьовування вхідного зображення та збереження файлу у початкове розташування.

Даний алгоритм було реалізовано у вигляді програмного продукту.

Експериментальне дослідження вдосконаленого методу

Для аналізу стеганографічних методів використовуються такі показники: пікове відношення сигналу до шуму (PSNR), нормалізована крос-кореляція (NCC), відношення бітових помилок (BER).

Для оцінки якості зображення після вбудовування використовуються параметри SSIM та PSNR як параметри, які найкраще відображають зміни в початковому стеганоконтейнері. Модифікований метод у результаті вбудовування генерує високоякісні зображення, з високим рівнем PSNR від 39 до 47,7 децибел при тестуванні звичайних знімків, та від 40,6 до 51 децибел при використанні знімків документів. У таблиці наведено значення метрик на еталонних зображеннях.

Результати тестування запропонованого алгоритму

Зображення	PSNR (db)	SSIM	BER (%)	NCC	Безпечність (у бітах)
Lena	46,31	0,9927	0	1	80
Pepper	46,30	0,9924	0,02	0,99	128
Plane	46,10	0,9920	0	1	192
Baboon	42,72	0,9940	0	1	256

Розглянемо візуальну відмінність стеганоконтейнеру, відображеного на рис. 4,*а*, та зображення із вбудованим ЦВЗ (рис. 4,*б*). Для вбудовування використовувалася послідовність, яка буде вбудована у вигляді ЦВЗ при роботі методу забезпечення автентичності.

а) б)

Рис. 4. Вбудовування ЦВЗ у стеганоконтейнер Lena: а) вигляд стеганоконтейнеру Lena; б) вигляд зображення з вбудованим ЦВЗ у стеганоконтейнер

Як можна побачити, візуальної відмінності для ока людини між стеганоконтейнером і зображенням із вбудованим ЦВЗ немає, що свідчить про те, що алгоритм виконує одну з основних функцій стеганографії — непомітно зберігати додаткову інформацію. У даному випадку це мітка користувача та хеш-сума файлу.

Також було проведено дослідження стійкості до атаки поворотом зображення, для чого було обрано повороти на 1, 5, 10, 30 та 45 градусів як основні контрольні точки перевірки. Для кращого візуального сприйняття замість послідовності даних використовувалося зображення у якості ЦВЗ. У даному тесті використовувалося декілька зображень для перевірки методу при різних основних характеристиках стеганоконтейнеру насиченості, яскравості, кольорової гами.

Досліджено стійкість до атак зміни розміру та атак відсічення частини зображення, проаналізовано значення коефіцієнта нормалізованої середньої кореляції при відсіченні четвертей зображення. Можна відзначити, що значення нормалізованої середньої кореляції не значно змінюється залежно від контейнеру.

Проведено аналіз стійкості до накладання фільтрів або внесення шуму. В результаті можна побачити, що активні фільтри не призводять до великих спотворень. Найгірші результати отримані при використанні атаки шуму «сіль і перець», яка призвела до 14,28 % помилково зчитаних бітів.

Провівши аналіз запропонованого методу до набору атак, можна відзначити, що метод має високу стійкість до пасивних атак і, на відміну від більшості методів, має високу стійкість до активних атак зловмисника, що наведено у результатах тестування застосування фільтрів, обрізання, повороту зображення.

Висновки

Розроблено вдосконалений метод автентифікації цифрових зображень для доказової бази судової системи та відповідне програмне забезпечення.

Проаналізовано існуючі стеганографічні методи забезпечення автентичності зображень щодо їхньої стійкості та проведено аналіз можливості модифікації методу. В результаті обрано для модифікації метод вбудовування ЦВЗ на основі методу Коха-Жао. Отриманий удосконалений метод вбудовування ЦВЗ дозволив значно підвищити стійкість до несанкціонованих модифікацій. Також було визначено, що попередньо обраний алгоритм хеш-функцій SHA-512 задовольняє вимогам системи, оскільки має високу стійкість до колізій та атак «першого дня». Розроблено алгоритм реалізації удосконаленого методу, здійснено його програмну реалізацію.

Проведено дослідження стійкості запропонованого методу до несанкціонованих модифікацій цифрових зображень. У цілому результати свідчать про високий рівень стійкості; модифікований метод у результаті вбудовування генерує високоякісні зображення з високим рівнем PSNR від 39 до 47,7 децибел при тестуванні звичайних знімків, і від 40,6 до 51 децибел при використанні знімків документів. Найгірші результати отримані при використанні атаки шуму «сіль і перець», яка призвела до 14,28 % помилково зчитаних бітів.

1. Хорошко В.О., Яремчук Ю.Є., Карпінець В.В. Комп'ютерна. Вінниця: ВНТУ, 2017. 155 с.

2. Дудикевич В.Б., Хорошко В.О., Яремчук Ю.Є. Основи інформаційної безпеки: навч. посіб. Вінниця: ВНТУ, 2018. 316 с.

3. Karpinets V., Yaremchuk Ju., Prokofjev M. Матеріали конференції «Technical University of Gabrovo. International scientific conference UNITECH'12». Gabrovo. Proceedings. 16–17 Nov. 2012. Vol. I. P. 348 – 352.

4. Langelaar G.C., Lagendijk R.L. Optimal differential energy watermarking of DCT encoded images and video. IEEE Trans Image Process. Jan. 2001. Vol. 10(1). P. 148–158.

5. Guo P. Zheng, and Huang J. Secure watermarking scheme against watermark attacks in the encrypted domain. *Journal of Visual Communication and Image Representation*. Jul. 2015. Vol. 30. P. 125–135.

6. Білинський Й.Й., Огородник К.В., Юкиш М.Й. Електронні системи: навч. посіб. Вінниця: ВНТУ, 2011. 109 с.

7. Eastlake D.E., Hansen T. US Secure Hash Algorithms (SHA and HMAC–SHA): RFC 4634. Milford: Motorola Laboratories; Middletown: AT&T Laboratories, 2006. 108 p.

8. Lingling W., Jianwei Z., and Qi G. Arnold Transformation and Its Inverse Transformation. *J. Micro Computer*. 2010. Vol. 14.

9. Nasrin M.Makbol, Bee EeKhoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition" Digital Signal Processing, vol. 33, pp. 134-147, Oct. 2014.

10. Wang K., Wong W., Liao X.F., and Chen G.R. A new chaosbased fast image encryption algorithm. *Applied soft computing*. 2011. Vol. 11. P. 514–522.

11. Patidar V., Pareek N.K., Purohit G., Sud K.K. A robust and secure chaotic standard map based pseudorandom permutationsubstitution scheme for image encryption. *Opt. Commun*. 2011. Vol. 284. P. 4331–4339.

12. Ferdowsi A., and Saad W. Deep Learning-Based Dynamic Watermarking for Secure Signal Authentication in the Internet of Things. arXiv: 1711.01306v1 [cs. IT] 3 Nov 2017.

13. Masilamani. An efficient visually meaningful image encryption using Arnold transform. In Proc. TechSym, Kharagpur, India. 2016. P. 266–271.

Надійшла до редакції 08.12.2018