УДК 004.056.5 к.т.н. **Бобок І.І.** (ОНПУ)

ПІДВИЩЕННЯ ІНФОРМАТИВНОСТІ РЕЗУЛЬТАТІВ ВИЯВЛЕННЯ КЛОНУВАННЯ В ЦИФРОВОМУ ЗОБРАЖЕННІ

Клонування залишається на сьогоднішній день одним з найпоширеніших і часто використовуваних при несанкціонованих змінах цифрових зображень (ЦЗ) програмних інструментів, реалізованим у всіх сучасних графічних редакторах. У роботі розроблений метод і запропонована його поліноміальна (степеня 4) алгоритмічна реалізація для виявлення результатів клонування з наступним відокремленням області клону від області прообразу в цифровому зображенні в умовах відсутності відмінностей у постобробці (якщо вона має місце) областей клону й прообразу з метою підвищення інформативності результатів виявлення клонування. Процес відокремлення клону від прообразу, результат якого часто дуже важливий для зацікавлених сторін, відбувається за допомогою використання цифрового водяного знаку (ЦВЗ), який спочатку вбудовується в зображення з метою організації його захисту від порушення цілісності. Вбудова ЦВЗ відбувається за допомогою стійкого до атак проти вбудованого повідомлення стеганографічного алгоритму, що забезпечує можливість відокремлення клону від прообразу в умовах постобробки ЦЗ після здійснення клонування. Основна ідея такого відокремлення, яка реалізована в розробленому методі, полягає у відмінності коефіцієнтів кореляції для декодованої інформації (частин ЦВЗ) з областей, що відповідають клону, прообразу, які є неоригінальною й оригінальною областями аналізованого ЦЗ відповідно. Для алгоритмічної реалізації методу запропоновані два способи формування областей ЦЗ, що відповідають клону й прообразу.

Ключові слова: цифрове зображення, клонування, цифровий водяний знак, клон, прообраз, стеганографічний алгоритм, відокремлення області клону від області прообразу.

Вступ. Важливу роль у сучасному інформаційному просторі відіграють цифрові контенти, зокрема цифрові зображення (ЦЗ), які широко використовуються в пресі, медицині, науці, судових розглядах і т.п. Очевидно, що їхнє коректне використання можливе тільки при збереженні цілісності.

Сучасні програмні середовища, такі, як Adobe Photoshop, Gimp і ін., дозволяють настільки якісно проводити зміни в ЦЗ, що виявити такі підробки часто стає неможливим. Високопрофесійні підробки цифрових контентів можуть привести до серйозних негативних наслідків як для окремо взятих людей, так і для суспільства в цілому. Це приводить до необхідності проведення експертизи цілісності цифрових контентів для можливості їх використання з метою, що відрізняється від розважальної, а також до необхідності забезпечення ефективності такої експертизи.

Одним з найпоширеніших на сьогоднішній день інструментів, реалізованих у всіх сучасних графічних редакторах, що використовується при проведенні фальсифікацій ЦЗ, є клонування [1-3]. При клонуванні одна область зображення, що називається прообразом, копіюється й вставляється в іншу область цього ж зображення, заміняючи собою його оригінальну частину й утворюючи клон прообразу. Описана процедура часто використовується у випадку, коли з ЦЗ усувається «небажаний» об'єкт, змінюється взаємне розташування об'єктів, дублюється об'єкт/об'єкти. Практично всі існуючі методи виявлення клонування навіть у випадку правильного визначення областей клону й прообразу не в змозі відокремити один від іншого, тобто визначити, що з них є клоном, а що прообразом, у той час, як розв'язок такого питання часто є дуже важливим для зацікавлених сторін, підвищуючи інформативність результатів виявлення клонування. У відкритій пресі існує дуже обмежена кількість робіт, присвячених цієї темі. З врахуванням того, що на практиці при здійсненні клонування область клону часто піддається якійсь постобрабці для її кращої «адаптації» у новій для неї області ЦЗ, деякі існуючі методи будують процес відокремлення клону від прообразу на основі виявлення саме результатів локальної обробки клону. Так основою методу, що вирішує задачу, яка розглядається, в [4] стало виявлення результатів розмиття

границі клону, що робиться часто на практиці для зниження ймовірності виникнення артефактів на клонованому ЦЗ.

Однак постобробка частин/частини клонованого ЦЗ (клону) є зовсім необов'язковою, більше того, для «автора» неавторизованої зміни ЦЗ вона стає небажаною у світі появи методів, аналогічних запропонованому в [4]. Тому в даний момент найбільш актуальною стає задача відокремлення клону від прообразу в умовах, коли вони або піддаються однаковій обробці, або не обробляються взагалі [5,6]. Необхідно відзначити, що останній варіант, при якому візуально клон не створює артефактів на ЦЗ, є можливим на практиці (рис. 1), крім того, відсутність відмінностей в обробці різних областей зображення не дає можливості по непрямих покажчиках визначити область клону.

а б

Рис. 1. Ілюстрація можливості проведення операції клонування без постобробки ЦЗ: а – оригінальне ЦЗ; б – результат проведеного клонування без будь-якої постобробки (частин) зображення

З врахуванням вищесказаного в [7] був запропонований метод виявлення клонування шляхом використання цифрових водяних знаків (ЦВЗ), що дає можливість відокремлювати область клону від прообразу у випадку відсутності відмінностей у постобробці. Однак останній метод має ряд істотних недоліків: необхідний перебір можливих варіантів розташування сітки розбивки ЦЗ на непересічні блоки для пошуку відповідної області на зображенні, яка є прообразом клону, що значно збільшує обчислювальну складність; пошук відповідної області здійснюється за ознакою точного збігу частин секретного ключа, які в загальному випадку при наявності збурних дій на клоноване ЦЗ можуть і не співпадати для відповідних областей клону й прообразу, тобто прообраз може бути не знайдений (у цьому випадку порушення цілісності ЦЗ не буде трактуватися як клонування).

Таким чином, задача виявлення результатів клонування в ЦЗ із наступним відокремленням області клону від прообразу до цього моменту не має задовільного розв'язку, залишаючись *актуальною*.

Мета статті та постановка задач. Метою роботи є підвищення інформативності результатів виявлення порушення цілісності ЦЗ шляхом розробки методу виявлення результатів клонування з наступним відокремленням області клону від області прообразу в ЦЗ в умовах відсутності відмінностей у постобробці (якщо вона має місце) областей клону й прообразу.

Для досягнення мети в роботі вирішуються наступні задачі:

1. Обґрунтувати вибір стеганометоду (стеганоалгоритму) для вбудови ЦВЗ при організації захисту ЦЗ від порушення цілісності;

2. Обґрунтувати вибір методу (алгоритму) виявлення областей клону й прообразу в ЦЗ в умовах наявності/відсутності додаткових (значних) збурних дій;

3. Розробити спосіб відокремлення області клону від області прообразу в ЦЗ в умовах відсутності відмінностей у способах їх обробки;

4. Розробити метод та поліноміальний алгоритм, що його реалізує, виявлення результатів клонування з наступним відокремленням області клону від області прообразу в умовах відсутності відмінностей у способах їх обробки.

Викладення основного матеріалу. Не обмежуючи спільності міркувань, для спрощення викладу матеріалу як формальне представлення ЦЗ буде розглядатися одна $m \times n -$матриця F, не зважаючи на те, кольоровим чи в градаціях сірого є зображення.

Всі методи виявлення фальсифікації ЦЗ, частковим випадком якої є клонування, з урахуванням необхідності наявності інформації про оригінальне зображення можуть бути поділені на активні й пасивні (сліпі) [8]. Активні методи для організації своєї роботи потребують інформацію про оригінальне зображення. Більшість із активних методів використовують цифровий підпис або стеганографічне вкладення ЦВЗ [9], що знайшло відображення в даній роботі.

Для організації захисту ЦЗ від несанкціонованого порушення цілісності пропонується у відповідну йому матрицю F за допомогою деякого стеганографічного методу (SM), стійкого до атак проти вбудованого повідомлення [10], вбудувати ЦВЗ, у якості якого може виступати, наприклад, бінарна послідовність

$$p_1, p_2, ..., p_t, \ \ p_i \in \{0,1\}, \tag{1}$$

що є частиною секретного ключа [10], але яка для розв'язку задач, поставлених у роботі, не зобов'язана нести в собі ніякої інформації про ЦЗ, може бути сформована випадковим чином. Результатом стеганоперетворення буде ЦЗ з матрицею F_S. Оскільки стійкість SM відіграє ключову роль у варіанті, що пропонується, розв'язку розглядаємої задачі, важливим є вибір способу її оцінки. Кількісна оцінка стійкості стеганоалгоритму до збурних дій у роботі проводиться стандартним чином [11]: за допомогою коефіцієнта кореляції NC для декодованого з можливо збуреного після стеганоперетворення зображення з матрицею $\overline{F}$ (при цьому $\overline{F} \neq F_S$) ЦВЗ $\overline{p}_1, \overline{p}_2, ..., \overline{p}_t$, $\overline{p}_i \in \{0,1\}, i = \overline{1,t}$, який визначається наступним чином:

$$NC = \sum_{i=1}^{t} p_i' \times \overline{p}_i' \Big/ t, \tag{2}$$

де $p_i' = 1$, $\overline{p}_i' = 1$, якщо $p_i = 1$, $\overline{p}_i = 1$ відповідно; $p_i' = -1$, $\overline{p}_i' = -1$, якщо $p_i = 0$, $\overline{p}_i = 0$ відповідно.

Вимога стійкості стеганометоду SM обумовлена можливістю постобробки ЦЗ після здійсненого клонування. Саме частина вбудованого в оригінальне зображення ЦВЗ дасть можливість відокремити область клону від прообразу, при цьому необхідно забезпечити таку стійкість стеганометоду, щоб області прообразу (тобто умовно (оскільки вона піддалася стеганоперетворенню) оригінальній області) відповідала декодована частина ЦВЗ, для якої NC буде близьким до одиниці.

Основні кроки експертного методу, що пропонується, який далі називається KP, будуть виглядати наступним чином.

Крок 1. Провести експертизу ЦЗ з матрицею $\overline{F}$ з метою виявлення результатів клонування, використовуючи для цього метод, ефективний в умовах наявності/відсутності додаткових (значних) до клонування збурних дій.

Якщо

результати клонування не виявлені,

то

перехід на крок 4;

інакше

нехай P_1, P_2 – виявлені області клону і прообразу такі,
що на цьому етапі не розрізняються.

Крок 2.

2.1. З областей ЦЗ T_1, T_2, які ставляться у відповідність P_1, P_2 за деяким законом, при цьому T_1, T_2 не обов'язково співпадають з P_1, P_2, але для них забезпечуються умови:

$$T_1 \bigcap P_1 \neq \varnothing,\ T_2 \bigcap P_2 \neq \varnothing, \qquad (3)$$

провести декодування відповідних частин ЦВЗ, вбудованого в ЦЗ з матрицею F.

2.2. Обчислити для областей T_1, T_2 значення коефіцієнтів кореляції NC_1 і NC_2 відповідно для декодованих з них частин ЦВЗ з врахуванням F_S.

Крок 3 *(відокремлення області клоні від області прообразу)*. Порівняти NC_1 і NC_2:

якщо

$$NC_1 < NC_2,$$

то

T_1 – область клону, T_2 – область прообразу,

інакше

T_1 – область прообразу, T_2 – область клону.

Крок 4. Вихід.

Для розробки алгоритмічної реалізації методу KP потрібна конкретизація кожного його кроку, крім того, у світі розв'язку задачі 1 зі списку задач даної роботи, необхідно зробити вибір стеганометоду (стеганоалгоритму) для здійснення вбудови ЦВЗ, у якості якого розглядається сформована випадковим чином бінарна послідовність (1), в оригінальне ЦЗ.

В [12] нещодавно був розроблений стеганографічний алгоритм *SNG*, стійкий до атак проти вбудованого повідомлення, ефективність якого перевищує ефективність сучасних аналогів. Алгоритм є блоковоорієнтованим і заснований на sign-нечутливості сингулярних векторів блоків матриці зображення, що відповідають максимальним сингулярним числам. *SNG* забезпечує значення $NC > 0.93$ в умовах значних збурних дій (порівнянних зі стиском ЦЗ з втратами з коефіцієнтом якості $QF = 10$). У силу своєї високої стійкості до атак проти вбудованого повідомлення цей алгоритм є кращим для попередньої вбудови ЦВЗ при організації захисту ЦЗ від несанкціонованих змін. Однак область застосовності *SNG* обмежується деякими властивостями використовуваного в якості контейнера зображення, зокрема наявністю в ЦЗ погано обумовлених (близьких до вироджених) блоків, отриманих після стандартної розбивки матриці. Ці блоки не використовуються в процесі стеганоперетворення. Такі обмеження є значним недоліком стеганоалгоритму з погляду його використання для досягнення поставленої в роботі мети, оскільки з врахуванням того, що при клонуванні може в загальному випадку бути задіяна будь-яка частина ЦЗ, для забезпечення можливості відокремлення клону від прообразу з використанням ЦВЗ цей ЦВЗ повинен вбудовуватися практично в усі блоки зображення, що захищається. При цьому порядок використання блоків для стеганоперетворення, як правило, є частиною секретного ключа.

Для усунення зазначеного недоліку *SNG* в [13] запропоновано його вдосконалення, одним з розроблювачів якого був автор даної статті: передобробка блоків ЦЗ-контейнера, що здійснюється перед безпосередньою вбудовою додаткової інформації. Результатом передобробки є зменшення числа обумовленості більшості блоків матриці контейнера зі збереженням надійності сприйняття зображення, що дозволяє розширити область застосовності алгоритму *SNG*, залишаючи його поліноміальним степені 2 і роблячи його використання доцільним для вбудови ЦВЗ у ЦЗ для розв'язку задач, поставлених у даній роботі.

Розглянемо докладно реалізацію кроку 1 методу KP. В [5,6] нещодавно був запропонований метод KL для виявлення результатів порушення цілісності ЦЗ, що відбулося

внаслідок клонування, розроблений для знаходження в ЦЗ областей клону й прообразу в умовах наявності/відсутності додаткових збурних дій (у тому числі, значних) на зображення, ефективність якого перевищує сучасні аналоги. Так помилки 1-го роду (пропуск клонування) в умовах стиску ЦЗ з втратами при коефіцієнті якості QF>75 відсутні взагалі, а при $25 \le QF \le 75$ становлять менше 6% [6]. Аналогічні високі результати були отримані й в умовах інших додаткових збурних дій [5]. У силу своєї високої ефективності даний метод, який є блоковоорієнтованим, що зручно й логічно в силу блокової орієнтованості стеганографічного алгоритму *SNG*, використовуваного для вбудови ЦВЗ у ЦЗ, пропонується для здійснення на кроці 1 виявлення областей клону й прообразу.

Необхідно відзначити, що кожна з областей клону й прообразу в методі KL визначається у вигляді об'єднання (пересічних) $l \times l$ – блоків матриці ЦЗ (рис. 2(б) – області, які виділені червоним кольором), причому тут розбіжність сітки стандартної розбивки [14] для областей клону й прообразу не відіграє ніякої ролі, на відміну від [5,6].

А б

Рис. 2. Результат роботи методу KL: а – ЦЗ, що зазнало клонування; б – виявлені області клону і прообразу (обмежені червоними замкненими ламаними лініями)

Метод KL визначає шукані області клону й прообразу (P_1, P_2) такими, що складаються з блоків ЦЗ, які не обов'язково відповідають блокам, отриманим у результаті стандартної розбивки [14] матриці і які задіюються в процесі стеганоперетворення ЦЗ (якщо використовувати для вбудови ЦВЗ алгоритм *SNG*, як пропонується вище). З врахуванням задачі, що розв'язується в роботі, як T_1, T_2, що фігурують у запропонованому вище методі, доцільно розглядати області, що представляють об'єднання блоків ЦЗ, отриманих у результаті стандартної розбивки його матриці. Для цього пропонуються наступні можливості:

Спосіб 1. T_1, T_2 сформувати з тих блоків, отриманих у результаті стандартної розбивки ЦЗ, які повністю знаходяться в P_1, P_2 відповідно, за умови виконання (3) (рис. 2(б): області, що обмежені коричневими замкненими ламаними лініями). В цьому випадку:

$$T_1 \subseteq P_1,\ T_2 \subseteq P_2. \qquad (4)$$

Спосіб 2. T_1, T_2 сформувати з тих блоків, отриманих у результаті стандартної розбивки ЦЗ, які мають непусте перетинання з P_1, P_2 відповідно (рис. 2(б): області, що обмежені синіми замкненими ламаними лініями). В цьому випадку:

$$P_1 \subseteq T_1,\ P_2 \subseteq T_2. \qquad (5)$$

Через виконання співвідношення (4) спосіб 1 формування T_1, T_2 забезпечить для кроку 3 запропонованого методу більшу ймовірність отримання вірного результату порівняння NC_1 і

NC_2, маючи очевидно меншу ймовірність включення до свого складу блоків, що не належать клону/прообразу, ніж спосіб 2. Однак, якщо абсолютні розміри клону/прообразу малі, то кількість блоків, які увійдуть в T_1, T_2 у відповідності зі способом 1, може виявитися настільки незначною, що помилки при декодуванні біт ЦВЗ, які можуть бути допущені через наявність додаткових збурних дій на клоноване ЦЗ, можуть привести до отримання хибного результату порівняння NC_1 і NC_2. У силу цього, якщо абсолютні розміри P_1, P_2 малі, то доцільно при формуванні T_1, T_2 використовувати спосіб 2. Цей спосіб у загальному випадку не просто додасть до P_1, P_2 блоки ЦЗ, що відповідають його стандартній розбивці, забезпечуючи (5), але й може збільшити аналізовані області, що відповідають безпосередньо клону й прообразу (див. рис.2(б): області, обмежені синіми замкненими ламаними лініями, містять у собі більші частини реальних клону й прообразу, ніж області P_1, P_2, що визначені за допомогою KL), що дасть можливість уточнити результат порівняння значень NC_1 і NC_2.

Експериментально встановлено, що якщо P_1, P_2 містять у своєму складі більше, ніж по 5 блоків, що визначаються стандартною розбивкою матриці ЦЗ, то для формування областей T_1, T_2 доцільно використовувати варіант 1, інакше – варіант 2.

Таким чином, алгоритмічна реалізація, що далі називається AKP, запропонованого вище метода KP з врахуванням того, що попередньо в ЦЗ удосконаленим алгоритмом *SNG*, що використовує стандартну розбивку матриці зображення на $8\times 8-$блоки, був вбудований ЦВЗ, який представляє собою бінарну послідовність, буде виглядати наступним чином.

Крок 1. За допомогою алгоритмічної реалізації методу KL, що використовує розбивку матриці $\overline{F}$ аналізованого ЦЗ на $8\times 8-$блоки, провести аналіз ЦЗ з метою виявлення результатів клонування. Подальші дії проводяться у випадку виявлених у ЦЗ областей клону й прообразу: P_1, P_2.

1.1. Визначити k_1, k_2 - кількості блоків, отриманих у результаті стандартної розбивки матриці $\overline{F}$, що належать P_1, P_2 відповідно.

1.2. Сформувати області T_1, T_2 з врахуванням нижченаведеного:

якщо

$$\min\{k_1, k_2\} > 5$$

то для формування областей T_1, T_2 використовувати спосіб 1,

інакше для формування областей T_1, T_2 використовувати спосіб 2.

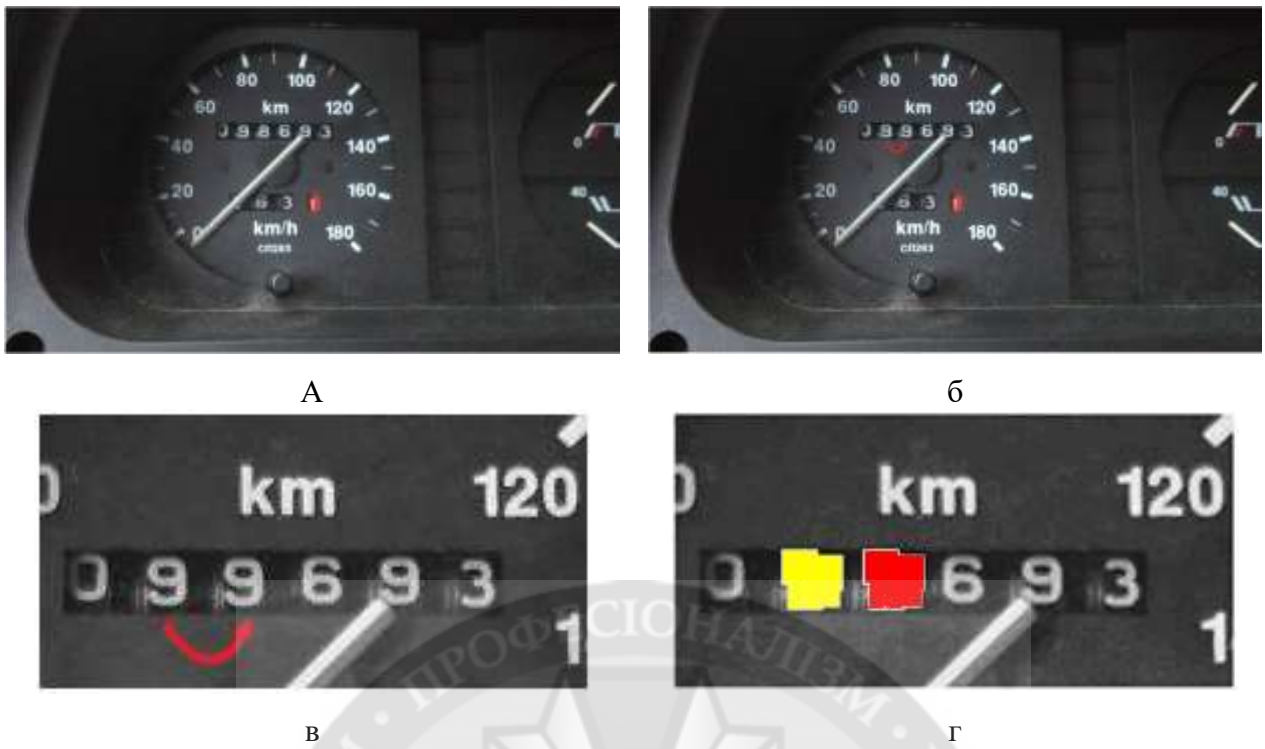
Крок 2.

2.1. З кожного блоку T_1, T_2 за допомогою вдосконаленого алгоритму *SNG*, що використовує розбивку матриці зображення на $8\times 8-$блоки, провести декодування біта додаткової інформації.

2.2. З врахуванням геометричного розташування T_1, T_2 в аналізованому ЦЗ, а також секретного ключа, що визначає порядок використання блоків ЦЗ у процесі стеганоперетворення/декодування ЦВЗ, за допомогою F_S обчислити для областей T_1, T_2 значення коефіцієнтів кореляції NC_1 і NC_2 відповідно для декодованих з них частин ЦВЗ, користуючись формулою (2).

Крок 3 *(відокремлення області клону від області прообразу)*. Повторює однойменний крок розробленого методу KP.

Тестування алгоритму *AKP* проводилося в середовищі *Matlab*. Приклад результатів роботи *AKP* для клонованого ЦЗ в умовах додаткових збурних дій, який ілюструє його високу ефективність для розв'язку задач, що розглядаються, наведений на рис. 3.



А б

в г

Рис. 3. Приклад роботи розробленого алгоритму *AKP*: а – оригінальне ЦЗ; б – ЦЗ, що зазнало клонування з наступним маштабуванням з коефіцієнтом 0.2 і збереженням у форматі Jpeg з $QF = 75$; в – частина фальсифікованого ЦЗ, що містить області клону й прообразу (для більшої наочності); г – результат відокремлення області клону (пофарбована в червоний колір) від області прообразу (пофарбована в жовтий колір), проведеного за допомогою *AKP*

Зауваження. Розроблений алгоритм *AKP*, що реалізує метод KP виявлення результатів клонування з наступним відокремленням області клону від області прообразу в умовах відсутності відмінностей у способах їх обробки, з урахуванням попередньої вбудови ЦВЗ у ЦЗ, є поліноміальним степеня 4. Дійсно, для стеганоперетворення ЦЗ с $n \times n$ – матрицею F за допомогою модифікованого алгоритму *SNG* з урахуванням блокової організації цього перетворення буде потрібно $\underline{O}\left(n^2\right)$ операцій. Найбільш витратною в обчислювальному сенсі частиною, що і визначає обчислювальну складність *AKP*, є частина, що відповідає кроку 1.1: алгоритмічна реалізація методу KL [5,6] для $n \times n$ – ЦЗ потребує $\underline{O}\left(n^4\right)$ операцій.

Висновки. В роботі розроблений метод і запропонована його ефективна поліноміальна (степеня 4) алгоритмічна реалізація виявлення результатів клонування з наступним відокремленням області клону від області прообразу в ЦЗ в умовах відсутності відмінностей у постобробці (якщо вона має місце) областей клону й прообразу, що дало можливість підвищити інформативність результатів виявлення порушення цілісності ЦЗ, що відбулося внаслідок клонування.

Процес відокремлення клону від прообразу реалізований з використанням ЦВЗ, вбудова якого з урахуванням можливості постобробки клонованого ЦЗ проводиться стеганографічним алгоритмом, стійким до атак проти вбудованого повідомлення, який за цим параметром перевищує існуючі аналоги. Основним кількісним показником, що аналізується в ході експертизи зображення для відокремлення клону від прообразу, є коефіцієнт кореляції для декодованої з областей, що відповідають клону, прообразу, додаткової інформації. В силу стійкості використаного стеганоалгоритму до збурних дій для області прообразу, що є оригінальною, коефіцієнт кореляції вище, ніж для області клону, яка, замінюючи оригінальну частину ЦЗ, замінює й відповідну частину ЦВЗ, що приводить до помилок при декодуванні додаткової інформації й дозволяє відокремити клон від прообразу.

ЛІТЕРАТУРА

1. Kakar, P. Exposing postprocessed copy-paste forgeries through transform-invariant features / P. Kakar, N. Sudha // IEEE Transactions on Information Forensics and Security. – 2012. – Vol. 7, No. 3. – pp. 1018–1028.

2. Ali Qureshi, M. A review on copy move image forgery detection techniques / M. Ali Qureshi, M. Deriche // Proceedings of 11th International Multi-Conference on Systems, Signals & Devices (SSD), 11-14 Feb. 2014, Barcelona, Spain. – 2014. – pp. 1–5.

3. Copy-move forgery detection using multiresolution local binary patterns / R. Davarzani, K. Yaghmaie, S. Mozaffari, M. Tapak // Forensic Science International. – 2013. – Vol. 231, No. 1. – pp. 61–72.

4. Лебедева, Е.Ю. Метод локализации и идентификации оригинальной и клонированной областей изображения / Е.Ю. Лебедева // Інформатика та математичні методи в моделюванні. – 2014. – Т. 4, № 1. – С. 76–84.

5. Григоренко, С.М. Розвиток методу виявлення клонування в цифровому зображенні в умовах додаткових збурних дій / С.М. Григоренко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2016. – Вип. 1(31). – С. 85–98.

6. Кобозева, А.А. Метод выявления нарушения целостности цифрового изображения, проведенного путем клонирования, робастный к сжатию с потерями / А.А. Кобозева, И.И. Бобок, С.Н. Григоренко // Материалы 17-й Международная научно-практической конференции «Современные информационные и электронные технологии «СИЭТ–2016». – Одесса, 2016. – С. 127-128.

7. Кобозева, А.А. Выявление нарушений целостности цифрового изображения путем использования стеганографических алгоритмов / А.А. Кобозева, И.И. Бобок, Л.М. Дзюбинская // Інформатика та математичні методи в моделюванні. – 2015. – Т. 5, № 2. – С. 129–134.

8. Singh, R. Copy move tampering detection techniques: A review / R. Singh, M. Kaur // International Journal of Applied Engineering Research. – 2016. – Vol. 11, No. 5. – pp. 3610–3615.

9. Mahdian, B. A bibliography on blind methods for identifying image forgery / B. Mahdian, S. Saic // Signal Processing: Image Communication. – 2010. – Vol. 25, No. 6. – pp. 389–399.

10. Стеганография, цифровые водяные знаки и стеганоанализ: монография / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С.А. Сапожников. – М.: Вузовская книга, 2009. – 220 с.

11. A blind watermarking method using maximum wavelet coefficient quantization / W.-H. Lin, Y.-R. Wang, S.-J. Horng et al. // Expert Systems with Applications. – 2009. – Vol. 36, No. 9. – pp. 11509–11516.

12. Кобозева, А.А. Стеганографический алгоритм, основанный на sign-нечувствительности сингулярных векторов матрицы изображения / А.А. Кобозева, М.А. Мельник // Системи обробки інформації. – 2013. – Вип. 3(110), Т. 2. – С. 90–94.

13. Усовершенствование стеганографического алгоритма, основанного на sign-нечувствительности сингулярных векторов блоков матрицы изображения / А.А. Кобозева, В.А. Мокрицкий, Л.Е.М. Батиене, И.И. Бобок // Інформатика та математичні методи в моделюванні. – 2017. – Т. 7, № 1-2. – С. 19–28.

14. Гонсалес, Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс; пер. с англ. П.А. Чочиа. – М.: Техносфера, 2006. – 1070 с.

REFERENCES:

1. Kakar, P., Sudha, N. (2012). Exposing postprocessed copy-paste forgeries through transform-invariant features. *IEEE Transactions on Information Forensics and Security*, 7(3), 1018–1028.

2. Ali Qureshi, M., Deriche, M. (2014). A review on copy move image forgery detection techniques. In *Proceedings of 11th International Multi-Conference on Systems, Signals & Devices (SSD), 11-14 Feb. 2014, Barcelona, Spain.* Barcelona. 1–5.

3. Davarzani, R., Yaghmaie, K., Mozaffari, S., Tapak, M. (2013). Copy-move forgery detection using multiresolution local binary patterns. *Forensic Science International*, 231(1), 61–72.

4. Lebedeva, H.J. (2014). Localization and identification method of original and cloned image areas. *Informatics and Mathematical Methods in Simulation*, 4(1), 76–84.

5. Grigorenko, S. (2016). Development of method for detection of cloning in digital images under additional disturbing influences. Legal, Regulatory and Metrological Support Information Security System in Ukraine, 1(31), 85–98.

6. Kobozeva, A.A., Bobok, I.I., Grigorenko, S.N. (2016). The robust method for detection of digital images integrity violation by image cloning. In *Processing of the 17th International Scientific and Practical Conference on Modern Information and Electronic Technologies*. Odessa. 127-128.

7. Kobozeva, A., Bobok, I., Dzubinskaya, L. (2015). Identifying the unauthorized changes of images areas that exposed to steganography algorithm. *Informatics and Mathematical Methods in Simulation*, 5(2), 129–134.

8. Singh, R., Kaur, M. (2016). Copy move tampering detection techniques: A review. *International Journal of Applied Engineering Research*, 11(5), 3610–3615.

9. Mahdian, B., Saic, S. (2010). A bibliography on blind methods for identifying image forgery. *Signal Processing: Image Communication*, 25(6), 389–399.

10. Agranovskiy, A.V., Balakin, A.V., Gribunin, V.G., Sapozhnikov, S.A. (2009). *Steganography, Digital Watermarkings, and Steganalysis*. Moscow. 220 p.

11. Lin, W.-H., Wang, Y.-R., Horng, S.-J., Kao, T.-W., Pan, Y. (2009). A blind watermarking method using maximum wavelet coefficient quantization. *Expert Systems with Applications*, 36(9), 11509–11516.

12. Kobozeva, A.A., Melnik, M.A. (2013). The steganography algorithm based on the sign-insensitivity of the singular vectors of the digital image matrix. *Information Processing Systems*, 3(110), 90–94.

13. Kobozeva, A.A., Mokritsky, V.A., Batiiene, L.E.M., Bobok, I.I. (2017). Improvement of the steganography algorithm based on the sign-insensitivity of the singular vectors of blocks of the digital image matrix. *Informatics and Mathematical Methods in Simulation*, 7(1-2), 19–28.

14. Gonzalez, R., Woods, R. (2006). *Digital Image Processing*. Moscow. 1070 p.

Рецензент: Кобозєва Алла Анатоліївна, доктор технічних наук, професор, завідуюча кафедри інформатики і управління захисту інформаційних систем, Одеський національний політехнічний університет

к.т.н. Бобок И.И.

ПОВЫШЕНИЕ ИНФОРМАТИВНОСТИ РЕЗУЛЬТАТОВ ВЫЯВЛЕНИЯ КЛОНИРОВАНИЯ В ЦИФРОВОМ ИЗОБРАЖЕНИИ

Клонирование остается на сегодняшний день одним из самых распространенных и часто используемых при несанкционированных изменениях цифровых изображений (ЦИ) программных инструментов, реализованным во всех современных графических редакторах. В работе разработан метод и предложена его полиномиальная (степени 4) алгоритмическая реализация для выявления результатов клонирования с последующим отделением области клона от области прообраза в цифровом изображении в условиях отсутствия различий в постобработке (если она имеет место) областей клона и прообраза с целью повышения информативности результатов выявления клонирования. Процесс отделения клона от прообраза, результат которого часто очень важен для заинтересованных сторон, происходит при помощи используемого цифрового водяного знака (ЦВЗ), который предварительно погружается в изображение с целью организации его защиты от нарушения целостности. Погружение ЦВЗ происходит при помощи устойчивого к атакам против встроенного сообщения стеганографического алгоритма, обеспечивающего возможность отделения клона от прообраза в условиях постобработки ЦИ после осуществления клонирования. Основная идея такого отделения, реализованная в разработанном методе, заключается в отличии коэффициентов корреляции для декодированной информации (частей ЦВЗ) из областей, отвечающих клону, прообразу, являющихся соответственно неоригинальной и оригинальной областями анализируемого ЦИ. Для алгоритмической реализации метода предложены два способа формирования областей ЦИ, отвечающих клону и прообразу.

Ключевые слова: цифровое изображение, клонирование, цифровой водяной знак, клон, прообраз, стеганографический алгоритм, отделение области клона от области прообраза.

Ph.D. Bobok I.I.

IMPROVING THE INFORMATIVITY OF THE RESULTS OF CLONING DETECTION IN A DIGITAL IMAGE

The cloning is one of the most common and often used software tool for unauthorized changes of digital images that implemented in all modern graphics editors. In this work we develop the new method for detection the results of cloning, followed by the separation of the clone region from the pre-image region in the digital image in the absence of differences in the post-processing (if any) of the clone and pre-image regions. Also, we present its polynomial (degree 4) algorithmic implementation. The process of separating the clone from the pre-image takes place using the digital watermark used, which is preliminarily added to digital image in order to organize its protection against integrity violation. The watermarking occurs with

the help of a steganographic algorithm, resistant to attacks against the built-in message, which makes it possible to separate the clone from the pre-image in post-processing of the digital image after cloning. The main idea of such separation, realized in the developed method, is the difference of the correlation coefficients for the decoded information (parts of the digital watermark) from the regions corresponding to the clone and pre-image, which are respectively the non-original and original regions of the analyzed digital image. For the algorithmic implementation of the method we proposed two methods for the formation of digital image regions corresponding to a clone and a pre-image.

Keywords: digital image, cloning, digital watermark, clone, pre-image, steganographic algorithm, separation clone from pre-image.