УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol. 5 (2015), No. 2, pp. 129-134

ВЫЯВЛЕНИЕ НАРУШЕНИЙ ЦЕЛОСТНОСТИ ЦИФРОВОГО ИЗОБРАЖЕНИЯ ПУТЕМ ИСПОЛЬЗОВАНИЯ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ

А.А. Кобозева, И.И. Бобок, Л.М. Дзюбинская

Одесский национальный политехнический университет,
просп. Шевченко 1, Одесса, 65044, Украина; e-mail: alla_kobozeva@ukr.net

В работе предлагается метод обнаружения нарушений целостности цифровых изображений, основанный на стеганопреобразовании оригинального изображения. В случае устойчивого к возмущающим воздействиям используемого стеганографического алгоритма обеспечивается возможность определения неоригинальной области в изображении даже при сохранении измененного изображения в формате с потерями. Разработанный метод дает возможность среди имеющихся различных способов нарушений целостности выделить конкретный – клонирование, выявить клонированную область и ее прообраз, отделить клон в случае отсутствия его постобработки от найденного оригинального прообраза, что не делалось ранее.

Ключевые слова: целостность цифрового изображения, стеганопреобразование, цифровой водяной знак, клонирование, прообраз клона

Введение

Современные информационные контенты все чаще имеют цифровое представление: цифровые изображения (ЦИ), видео (ЦВ), аудио. При их использовании с целью, отличной от развлекательной, необходимо быть уверенными в отсутствии несанкционированных изменений этих контентов, что делает задачу проверки их целостности чрезвычайно *актуальной* на сегодняшний день.

Современный уровень развития IT-технологий привел к тому, что различного рода фальсификации ЦИ средствами графических редакторов, таких как Adobe Photoshop, Coral Drow и другие, являются чрезвычайно распространенными, приводя к необходимости повышения эффективности методов пассивной защиты информации. И хотя задача выявления нарушений целостности ЦИ не является новой, существующие методы ее решения по тем или иным причинам не являются удовлетворительными [1-3].

Актуальной на сегодняшний день является задача выявления областей клонирования ЦИ. Ее удовлетворительное решение получено в случае сохранения измененного ЦИ в формате без потерь, например, в [4], но предложенный здесь метод оказывается неэффективным, если после осуществления клонирования ЦИ сохраняется в формате с потерями, что вносит дополнительные возмущения в изображение.

Часто при нахождении клонированной области и ее прообраза важным является точное установление «что есть что». Алгоритм отделения клона от прообраза совсем недавно был предложен в [5], однако основой этого алгоритма является выявление результатов постобработки клонированной области (ее контура) – размытия, без наличия которого предложенный алгоритм является нерабочим.

Цель статьи и постановка заданий

Стеганографические алгоритмы (СА), внедряющие цифровые водяные знаки (ЦВЗ) в цифровые контенты, широко используются в настоящее время для обеспечения проверки их аутентичности и целостности. В связи с этим

Целью работы является разработка метода выявления (областей) нарушений целостности ЦИ, основанного на использовании ЦВЗ, эффективного, в том числе, в условиях сохранения измененного ЦИ в формате с потерями, позволяющего при выявленном клонировании отделить клон от его прообраза в случае отсутствия какой-либо постобработки области клонирования.

Для достижения поставленной цели в работе решаются *задачи*:

- определения свойств стеганографического метода/алгоритма, используемого для погружения ЦВЗ в ЦИ, с учетом характеристик возможных атак на полученное стеганосообщение;
- определения алфавита для элементов ЦВЗ;
- определения способа выявления области клонирования в случае несовпадения сеток разбиения матрицы ЦИ для клона и области прообраза;
- отделения клона при отсутствии его постобработки от прообраза.

Основная часть

Рассматривается цветное ЦИ. Пусть F - это одна из матриц его формального представления (одна из цветовых матриц, если ЦИ хранится, например, в схеме RGB; матрица яркости в схеме YUV). Для обеспечения решения задачи контроля нарушений целостности ЦИ матрица F размера $n \times n$ разбивается стандартным образом на $l \times l$ – блоки, обозначаемые далее B_{ij}, $i, j = 1,...,\lfloor n/l \rfloor$, где $\lfloor \bullet \rfloor$ - операция выделения целой части аргумента. Каждый блок B_{ij} разбивается на квадратные $m \times m$ – подблоки B_{ij}^{gh}, где $g, h = 1,...,l/m$ (в предположении, что l кратно m) (рис.1). Для ЦИ генерируется случайным образом секретный ключ в виде двумерной $\lfloor n/l \rfloor \times \lfloor n/l \rfloor$ – матрицы K, с элементами k_{ij}, $i, j = 1,...,\lfloor n/l \rfloor$. Элементы $k_{ij} \in \{0,1,2,...,2^0 + 2^1 + 2^2 + ... + 2^r\}$, где r - количество $m \times m$ – подблоков блока B_{ij}. Ключ K играет роль ЦВЗ, погружаемого при помощи СА в оригинальное ЦИ (в матрицу F). Предложенное определение алфавита для элементов ЦВЗ даст возможность увеличить его чувствительность по сравнению с общеиспользуемым [6] бинарным представлением.

В каждый блок B происходит погружение одного элемента K после его предварительного представления в двоичной системе счисления с использованием r разрядов (например, если очередное значение $k_{ij} = 2$, а $r = 4$, то k_{ij} кодируется в виде: 0010). Каждый подблок B_{ij}^{gh} используется для погружения в него одного бита двоичного представления k_{ij}. Такая блочная организация процесса стеганопреобразования (СП) ЦИ, помимо всего прочего, обеспечит разрабатываемый стеганометод наличием внутреннего параллелизма [7], что при его использовании позволит значительно сократить время работы метода при обработке изображения, по сравнению с его последовательной реализацией. Наличие внутреннего параллелизма обеспечит также возможность использования предлагаемого метода выявления нарушений целостности для ЦВ.

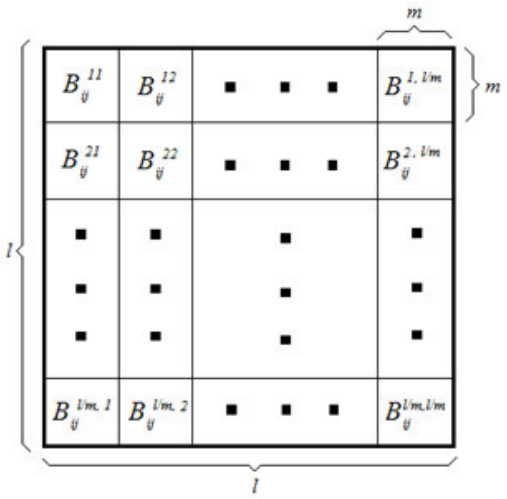

Рис. 1. Разбиение $l \times l$ – блока B_{ij} на $m \times m$ – подблоки B_{ij}^{gh}

Основные шаги метода следующие.

Организация стеганопреобразования.

1. Разбить матрицу ЦИ F на непересекающиеся $l \times l$ – блоки B_{ij}, $i, j = 1,...,\lceil n/l \rceil$.

2. Сформировать $\lceil n/l \rceil \times \lceil n/l \rceil$ – матрицу секретного ключа K, которая передается адресату по защищенному каналу связи.

3. Для каждого очередного блока B_{ij}, $i, j = 1,...,\lceil n/l \rceil$:

3.1. Разбить B_{ij} стандартным образом на r непересекающихся $m \times m$ – подблоков B_{ij}^{gh}, где $g, h = 1,...,l/m$.

3.2.Представить очередной погружаемый в B_{ij} элемент k_{ij} матрицы ключа K в виде: $p_1 p_2 ... p_r$, где $p_i \in \{0,1\}, i = \overline{1,r}$.

3.3. Для каждого подблока B_{ij}^{gh}, участвующего в процессе СП, погрузить в него очередной элемент $p_1 p_2 ... p_r$, используя для этого некоторый СА, обеспечивающий надежность восприятия получаемого ЦИ-стеганосообщения с матрицей $F^{(S)}$.

Организация декодирования.

1. Разбить матрицу возможно измененного в процессе пересылки или хранения ЦИ $\overline{F}$ (в общем случае $\overline{F} \neq F^{(S)}$) на непересекающиеся $l \times l$ – блоки $\overline{B}_{ij}$, $i, j = 1,...,\lceil n/l \rceil$. Каждый блок $\overline{B}_{ij}$ используется для декодирования из него 1 возможно измененного элемента $\overline{k}_{ij}$ матрицы ключа K.

2. Для каждого очередного блока $\overline{B}_{ij}$, $i, j = 1,...,\lceil n/l \rceil$, задействованного в СП:

2.1. Разбить $\overline{B}_{ij}$ стандартным образом на r непересекающихся $m \times m$ – подблоков $\overline{B}_{ij}^{gh}$, где $g, h = 1,...,l/m$.

2.2. Из каждого подблока $\overline{B}_{ij}^{gh}$, участвующего в СП, извлечь очередной бит информации $\overline{p}_s$, используя для этого СА, который применялся на этапе погружения информации в ЦИ. Все извлеченные биты, выстроенные в порядке, определяемом секретным ключом алгоритма, определят двоичное представление $\overline{p}_1 \overline{p}_2 ... \overline{p}_r$ элемента $\overline{k}_{ij}$.

3. *Если* существует элемент матрицы K, для которого $\bar{k}_{ij} \neq k_{ij}$, *то* целостность ЦИ нарушена, а несовпадения в K дадут возможность локализовать эти области, *иначе* целостность ЦИ не нарушена, переход на шаг 8.

4. *Если* целью анализа ЦИ было выявление лишь факта нарушения его целостности, *то* переход на шаг 8, *иначе* для того, чтобы проверить, является ли выявленная область клонированной, необходимо найти ее же в анализируемом ЦИ, т.е. найти ее прообраз. Для этого необходимо в матрице $\bar{K}$, составленной из декодированных элементов $\bar{k}_{ij}$, найти область ее элементов, аналогичную выявленной неоригинальной. Если область найдена, переход на шаг 8.

Частный случай иллюстрации шага 4 представлен на рис.2. Однако такой случай, а именно, когда сетка разбиения клонированной области и ее прообраза на блоки будет совпадать, является маловероятным. Чаще всего даже в случае прямоугольной области клона будет иметь место случай, иллюстрация которого представлена на рис.3 (красным выделена область клона, зеленым цветом – прообраз), когда блоки (их количество и расположение) в пределах области клона не будут напрямую отвечать блокам прообраза. Тогда поиск прообраза в ЦИ будет затруднен, поскольку точного совпадения частей ключа для клона и прообраза в анализируемом ЦИ наблюдаться не будет. В этом случае процесс анализа ЦИ должен быть продолжен.

Рис. 2. Выявление клонированной области и ее прообраза в ЦИ на основании декодированной матрицы ключа

5. Выделенная неоригинальная область должна содержать некоторые блоки целиком. Из таких блоков произвести декодирование части ключа (рис.2(б)). С учетом того, что блоки, находящиеся на границе области, могут лишь частично входить в клонированную область, удалить из выделенной области ключа значения, лежащие на ее границе. Перейти на шаг 4. Если аналог неоригинальной части ЦИ найден, то он является прообразом выявленной неоригинальной части ЦИ - клона. Переход на шаг 8.

6. *Перебор всех возможных расположений сетки разбиения в пределах выделенной неоригинальной области ЦИ*. Произвести сдвиг сетки разбиения на 1 пиксель. Переход на шаг 5.

7. Если все возможные варианты сетки разбиения с шагом в один пиксель проверены, при этом прообраз неоригинальной области не обнаружен, то она не является клонированной областью.

8. Выход.

а **б**

Рис. 3. Пример возможного несовпадения сеток разбиения области клонирования и прообраза: а – оригинальное ЦИ; б – ЦИ, подвергнутое обработке

Замечание. Для того, чтобы предлагаемый метод обеспечивал чувствительность к нарушению целостности, охватывающему ЦИ целиком (наложение шума, сжатие с потерями, фильтрация ЦИ), погружение элементов K на шаге 3.3 организации СП должно происходить неустойчивым к возмущающим воздействиям стеганоалгоритмом. Для организации выявления областей нарушений целостности, происходящих на ЦИ локально (области локально проведенных геометрических атак, в частности, клонирования), алгоритм погружения элементов K должен быть устойчивым к атакам против встроенного сообщения. В этом случае разработанный метод позволит отделять область клона от прообраза при имеющем место клонировании и в условиях отсутствия какой-либо постобработки области клона; кроме того с учетом предложенной организации СП, клонирование будет выявляться и в случае сохранения измененного ЦИ с потерями, что, как можно судить по источникам, доступным из открытой печати, не делалось ранее.

Выводы

Разработан метод обнаружения нарушений целостности цифровых изображений, основанный на СП оригинального изображения, который позволяет в зависимости от свойств используемого для погружения ЦВЗ стеганоалгоритма выявлять как результаты изменений ЦИ целиком (наложение шума, сжатие с потерями, фильтрация), так и области локальных нарушений целостности, в частности, области клонирования. В отличие от существующих аналогов, разработанный метод принципиально позволяет обнаруживать результаты клонирования в ЦИ, сохраненных в форматах с потерями, а также отделять клон от области прообраза в случае отсутствия какой-либо постобработки клона.

При разработке алгоритма, реализующего предложенный метод, для обеспечения его эффективной работы на основании представительных вычислительных экспериментов необходимо осуществить выбор размеров блока (l) и подблока (m), количества подблоков в границах блока, над чем сейчас работают авторы.

Список литература

1. Rey, C. A survey of watermarking algorithms for image authentication / C. Rey, J.-L. Dugelay // EURASIP J. Appl. Signal Process. – 2002. — №1. — С.613–621.
2. Amerini, I. Copy-move forgery detection and localization by means of robust clustering with J-linkage / I. Amerini, L. Ballan, R. Caldelli, A. del Bimbo, L. del Tongo, G. Serra // Signal Processing. — 2013. — Т.28. — №6. — С.659–669.
3. Farid, H. Image Forgery Detection / H. Farid // IEEE Signal processing magazine. – 2009. — С.16-25.
4. Кобозева, А.А. Разработка нового подхода к выявлению замещающей области в цифровом изображении / А.А.Кобозева, Е.Ю.Лебедева // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2013. – Вип 1(25). – С.67-74.
5. Лебедева, Е.Ю. Метод локализации и идентификации оригинальной и клонированной областей изображения / Е.Ю. Лебедева // Інформатика та математичні методи в моделюванні. 2014. Том 4, №1. С. 76 – 84.
6. Аграновский, А.В. 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.
7. Воеводин, В.В. Параллельные вычисления / В.В.Воеводин, Вл.В.Воеводин. — СПб.: БХВ-Петербург, 2002. — 608 с.

ВИЯВЛЕННЯ ПОРУШЕНЬ ЦІЛІСНОСТІ ЦИФРОВОГО ЗОБРАЖЕННЯ ШЛЯХОМ ВИКОРИСТАННЯ СТЕГАНОГРАФІЧНИХ АЛГОРИТМІВ

А.А.Кобозєва, І.І. Бобок, Л.М. Дзюбинська

Одеський національний політехнічний університет,
просп. Шевченко 1, Одеса, 65044, Україна; e-mail: alla_kobozeva@ukr.net

У роботі пропонується метод виявлення порушень цілісності цифрових зображень, заснований на стеганоперетворенні оригінального зображення. У випадку стійкого до збурних дій використовуваного стеганографічного алгоритму забезпечується можливість визначення неоригінальної області в зображенні навіть при збереженні зміненого зображення у форматі з втратами. Розроблений метод дає можливість серед наявних різних способів порушень цілісності виділити конкретний - клонування; виявити клоновану область і її прообраз; відокремити клон у випадку відсутності його постобробки від знайденого оригінального прообразу, що не робилося раніше.

Ключові слова: цілісність цифрового зображення, стеганоперетворення, цифровий водяний знак, клонування, прообраз клону

IDENTIFYING THE UNAUTHORIZED CHANGES OF IMAGES AREAS THAT EXPOSED TO STEGANOGRAPHY ALGORITHM

A. Kobozeva, I. Bobok, L. Dzubinskaya

Odessa national polytechnic university,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: alla_kobozeva@ukr.net

In this paper we propose a method for identifying the changes of image completion based on stegano transformation of original image. In the case of using the steganography algorithm that resistant for disturbing influences proposed method provides the possibility of identifying non-original areas of the image, even when image was saved in lossy formats. The developed method allows to allocate a specific method of image completion violations - cloning; identify the cloned area and its prototype; separate clone in the case of absence of post-processing from the original image that has not been done before.

Keywords: image completion, stegano transformation, watermarking, clone stamp, prototype of clone