УДК 004.021:004.624

РАЗРАБОТКА АЛГОРИТМА ВНЕДРЕНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА НА БАЗЕ МОРФОЛОГИЧЕСКОЙ ОБРАБОТКИ ИЗОБРАЖЕНИЯ И МОДУЛЯРНОЙ АРИФМЕТИКИ ДЛЯ ПРОТИВОДЕЙСТВИЯ УГРОЗАМ ХИЩЕНИЯ ОБЪЕКТОВ ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

Абасова А.М., Бабенко Л.К.

ФГАОУ ВО «Южный федеральный университет», Институт компьютерных технологий и информационной безопасности, Таганрог, e-mail: moonriel@yandex.ru, lkbabenko@sfedu.ru

В настоящей статье описывается реализация обеспечения защиты авторских прав, прав интеллектуальной собственности мультимедийного контента и скрытой передачи информации путем использования внедренных цифровых водяных знаков. В качестве контейнера рассматривается цветное цифровое изображение. Описан разработанный алгоритм преобразования цифрового водяного знака, не зависящий от его вида (цифровой водяной знак может представлять собой текст, бинарное изображение с логотипом организации, QR-код, содержащий знак охраны авторских прав или ссылку на сайт автора) для встраивания в цифровое изображение на основе использования математического аппарата модулярной арифметики, позволяющий обнаружить и скорректировать возникшую ошибку/искажение данных при наличии деструктивного воздействия на систему. Также описан разработанный алгоритм внедрения цифрового водяного знака в изображение-контейнер с целью доказательства авторских прав на основе морфологической обработки изображений, в рамках которого было предложено для внедрения цифрового водяного знака использовать значимые области изображения-контейнера, а именно пиксели, принадлежащие объектам переднего плана. Для преодоления проблемы последовательного заполнения бит изображения было предложено использовать геометрический центр объекта переднего плана как точку отсчета.

Ключевые слова: стеганография, стегоконтейнер, цифровой водяной знак, морфологическая обработка изображений, модулярная арифметика

THE DEVELOPMENT OF AN ALGORITHM OF THE DIGITAL WATERMARKING BASED ON MORPHOLOGICAL IMAGE PROCESSING AND MODULAR ARITHMETICS COUNTERING THE THREATS OF THE PROTECTION OF INTELLECTUAL PROPERTY OBJECTS

Abasova A.M., Babenko L.K.

Federal Autonomous Educational Institution of Higher Education «South Federal University» Institute of Computer Technologies and Information Security, Taganrog, e-mail: moonriel@yandex.ru, lkbabenko@sfedu.ru

This article describes the implementation of the protection of copyright, intellectual property rights of multimedia content and the hidden transmission of information through the use of embedded digital watermarks. The digital color images will be the container. Described a developed algorithm for converting digital watermark, independent of its form (a digital watermark can be a text, a binary image with the company logo, a QR – code containing a copyright protection symbol or a link to the author's site) for embedding in a digital image based on the use of the mathematical apparatus of modular arithmetic, which makes it possible to detect and correct the error/distortion of the data that arises when there is a destructive effect on the system. Also described the developed algorithm for introducing a digital watermark into a container image for the purpose of proving copyright that based on morphological image processing, within which it was proposed to use significant areas of the container image, the pixels of the container image belonging to the foreground objects for the introduction of the digital watermark. To overcome the problem of sequential filling of image bits, it was suggested to use the geometric center of the foreground object as a reference point.

Keywords: steganography, stego container, digital watermarkind, morphological image processing, modular arithmetic

Цифровое изображение, как частный случай аудиовизуального произведения, но без сопровождения звука, обладает повышенным риском нарушения авторского права, так как данный объект интеллектуальной собственности широко представлен в интернете и для злоумышленника не составляет трудности выполнить его копирование и распространение вне зоны авторского контроля [1]. Применение невидимых цифровых водяных знаков (далее – ЦВЗ) позволяет сократить потери от угроз хищения, в том числе незаконного копирования, использования изображений и является перспективным направлением в обеспечении защиты авторских прав, так как ЦВЗ обладает сравнительно невысокой стоимостью, в отличие от других технических методов, невидим для злоумышленника и подходит при регистрации цифровых изображений, в отличие от организационных методов.

В работах [2, 3] производится описание различных типов деструктивных воздействий на системы ЦВЗ. Известные алго-

ритмы повышения робастности к деструктивным воздействиям стеганографических методов ЦВЗ увеличивают их вычислительную сложность, однако не всегда обеспечивают высокую устойчивость ЦВЗ к широкому спектру деструктивных воздействий с учетом обеспечения незаметности ЦВЗ и слепого извлечения ЦВЗ. Целью работы является разработка алгоритма внедрения ЦВЗ в изображение, устойчивого к различным деструктивным воздействиям с учетом данных требований для повышения эффективности защиты от угроз хищения объектов интеллектуальной собственности.

Разработка алгоритма внедрения ЦВЗ в изображение

В рамках анализа литературы, освещающей способы и цели использования злоумышленником изображения, которое не является его объектом интеллектуальной собственности, а также методов, с помощью которых злоумышленник пытается обойти наличие ЦВЗ, был сделан вывод, что, как правило, при принятии решения об удалении части изображения злоумышленник оставляет нетронутыми объекты, которые находятся на переднем плане, так как именно они представляют ценность изображения. Таким образом, было предложено для внедрения ЦВЗ использовать пиксели изображения-контейнера, принадлежащие объектам переднего плана. Для определения объектов или определенных областей на изображении используют сегментацию. В работе [4] описаны алгоритмы выделения объектов переднего плана, но по причине высокой ресурсоемкости вычислительных операций алгоритмов, необходимости внесения со стороны пользователя понятийной информации в некоторых случаях, а также по причине обнаружения четких контуров объектов при выполнении сегментации (что позволит злоумышленнику легко обнаружить объект для внедрения ЦВЗ, зная алгоритм) было принято решение вычислять маркеры переднего плана изображений. Они определяются на основе анализа связности пикселей каждого объекта.

Пусть $I(x, y)$ – исходное изображение-контейнер, $I'(x, y)$ – исходное изображение-контейнер, преобразованное в полутоновое, $b(x, y)$ – структурный элемент или примитив (размера $g \times h$, причем будем считать, что $g = 2a_1 + 1$ и $h = 2a_2 + 1$, где a_1, a_2 – неотрицательные целые числа), который также является цифровым изображением меньшего чем I'(x, y) размера, I' и b соотносят значение яркости каждой группе координат.

Полутоновая дилатация I' по структурному элементу b отмечается как $I' \oplus b$ и определяется как

$$(I' \oplus b)(s,t) = \max\{I'(s-x,t-y) + b(x,y) \mid (s-x,t-y) \in D_{I'}; (x,y) \in D_b\}, \quad (1)$$

где $D_{I'}$, D_b – области определения I', b соответственно, s – сдвиг по координате x равный a_1, t – сдвиг по координате y равный a_2.

Полутоновая эрозия I' по примитиву b отмечается $I' \ominus b$, определяется как

$$(I' \ominus b)(s,t) = \min\{I'(s+x,t+y) - b(x,y) \mid (s+x,t+y) \in D_{I'}; (x,y) \in D_b\}. \quad (2)$$

Ограничение, указывающее, что координатам $(s - x)$ и $(t - y)$ / $(s + x)$ и $(t + y)$ необходимо состоять в области определения I', а x и y – в области определения b, подобно определению двоичной дилатации/эрозии, которое устанавливает, что два множества должны пересекаться хотя бы в одном элементе (для дилатации) или структурный элемент должен находиться внутри исходного множества (для эрозии) [5].

Операции дилатации и эрозии являются ключевыми при выполнении морфологического размыкания и замыкания. На практике при размыкании выполняемая на первом этапе эрозия удаляет небольшие объекты, но при этом изображение становится темнее, после чего применяется дилатация, которая восстанавливает общую яркость до прежнего уровня, не восстанавливая объекты, удаленные при эрозии. На практике замыкание, как правило, применяется для удаления темных объектов на изображении, при небольших изменениях ярких деталей.

Полученные маркированные блоки анализируются на предмет их применимости для внедрения информации (ЦВЗ), а именно учитывается их площадь, а также количество. В случае недостаточности количества маркированных блоков переднего плана или количества пикселей в данных блоках производится корректировка структурного элемента.

ЦВЗ может выступать как последовательность чисел [6] или символов [7], может быть представлен в виде текста, содержащего знак охраны авторских прав [8], бинарного изображения с логотипом организации (если автором является юридиче-

ское лицо), QR-кода, который также может содержать знак охраны авторских прав или ссылку на сайт автора. Независимо от того в каком виде выступает ЦВЗ, он может быть представлен модулярным кодом так, что при наличии деструктивного воздействия на систему будет возможно обнаружить и скорректировать возникшую ошибку.

Любой ЦВЗ может быть представлен матрицей положительных целых чисел. Для текстовых данных это будет матрица чисел, соответствующих каждой цифре/букве/символу согласно выбранной кодировке, для бинарного изображения/QR-кода это будет матрица чисел, которая получится после преобразования матрицы, состоящей из нулей и единиц в необходимую для обработки. Пусть заданы модули – положительные числа, взаимно простые основания системы: p_1, $p_2,\ldots,p_i,\ldots,p_k$, НОД($p_1$, p_q) = 1 для $i \neq q$. Информационный диапазон получившейся системы чисел определяет значение $P = \prod_{i=1}^{k} p_i$. Каждое неотрицательное целое число A можно описать в виде модулярного кода $A = \{\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_k\}$, который содержит натуральные числа, такие, что $0 \leq \alpha_i < p_i$, где $i = 1,2,\ldots,k$. Согласно положениям модулярной арифметики одним из признаков ошибки является выполнение условия $A \geq P$.

Отличительной способностью кода, обладающего свойствами обнаружения и исправления ошибок, будет являться присутствие двух диапазонов цифр – информационного $J_A = \{\alpha_1, \alpha_2, \ldots, \alpha_i\}$ и контрольного $K_A = \{\alpha_{k+1}, \ldots, \alpha_{k+n}\}$. В информационном диапазоне находятся цифры, составляющие числовое значение закодированной величины, а в контрольном диапазоне – цифры, которые введены для обеспечения возможности обнаружения и коррекции ошибок. При этом контрольный диапазон цифр будет являться избыточным.

В источнике [9] авторы формулируют теорему, из которой следует, что любое искажение цифры по одному какому-либо разряду превращает это число в неправильное и тем самым позволяет обнаружить наличие искажения. Более того, существует только одно-единственное значение этой цифры, которое может превратить неправильное число в правильное. Выявленная ошибка может быть исправлена одним из существующих корректирующих методов.

Для обеспечения целостности ЦВЗ был разработан алгоритм преобразования ЦВЗ для внедрения в цифровое изображение на основе использования математического аппарата модулярной арифметики. Входными данными для работы алгоритма является ЦВЗ, вне зависимости от формы его представления. Задача, стоящая на начальном этапе выполнения данного алгоритма, заключается в определении типа ЦВЗ, после чего необходимо привести изначальное представление к виду, пригодному для функционирования алгоритма.

Формируется двоичный массив, группы элементов которого, в зависимости от рабочего диапазона выбранной системы остаточных классов, преобразуются в блоки по T-бит. Далее данные блоки подвергаются преобразованию из двоичной системы в десятичную. На следующем этапе осуществляется процедура преобразования матрицы, элементами которой уже являются цифры в десятичной системе счисления в матрицу, элементами которой являются цифры, представленные избыточным модулярным кодом (далее – ИМК).

В процессе преобразования обязательным критерием вхождения символа в преобразованную матрицу является его принадлежность к рабочему диапазону выбранной системы оснований.

Остатки по каждому из выбранных модулей системы должны храниться в отдельных областях изображения-контейнера, откуда следует необходимость в разделении матрицы с остатками, полученную на предыдущем этапе, на n – матриц, содержащих значения по каждому модулю. Выполнение данного требования необходимо для обеспечения целостности ЦВЗ. В случае если изображение с вложенным ЦВЗ подвергается деструктивному воздействию, информация по каждому из оснований системы является относительно изолированной друг от друга, что позволяет с большей вероятностью восстановить утерянные данные.

Далее производится процедура внедрения ЦВЗ в изображение-контейнер. При реализации морфологических функций дилатации и эрозии используется структурный элемент (примитив). Выбор размера и формы структурного элемента (примитива) зависит от особенностей конкретного изображения-контейнера. В предложенном алгоритме структурный элемент (примитив) особой сложной формы будет использоваться в качестве ключевой информации.

На рисунке в виде блок-схемы представлен алгоритм внедрения ЦВЗ в изображение-контейнер. Входными данными для работы алгоритма является изображение-контейнер I и ЦВЗ, преобразованный к виду, пригодному для функционирования алгоритма.

Алгоритм внедрения ЦВЗ в изображение-контейнер

Задача, стоящая на начальном этапе выполнения данного алгоритма, заключается в определении блоков переднего плана, непосредственно в которые будет вноситься информация. Для этого первоначально необходимо произвести преобразование исходного изображения-контейнера I в полутоновое. Затем необходимо произвести формирование структурного элемента (примитива), который будет являться стегоключом и находиться в хранилище ключевой информации. На следующем этапе происходит вычисление маркеров переднего плана по заданному ранее структурному элементу. Для этого выполняются операции морфологического размыкания/замыкания [10].

На выходе после выполнения указанных операций имеется перечень маркированных

объектов переднего плана (маркированных блоков переднего плана), однако не все полученные объекты могут подойти для внедрения/встраивания ЦВЗ по причине недостаточного размера или неподходящего расположения на изображении-контейнере, поэтому на следующем этапе необходимо определить, какие из объектов переднего плана подойдут для встраивания информации. Для этого производится вычисление количества пикселей, из которых состоит каждый объект переднего плана, а также учитывается расположение самих объектов и их удаленность от края изображения. После выполнения данных операций имеем m блоков переднего плана, подходящих для встраивания информации.

В случае если количество блоков переднего плана оказалось меньше требуемого количества блоков *n*, то производится корректировка структурного элемента (примитива) и процедура поиска маркированных объектов переднего плана повторяется. В случае если количество блоков переднего плана оказалось больше требуемого количества блоков *n* (на практике данная ситуация наиболее вероятна), то маркированные объекты могут выбираться исходя из условий, которые также указываются в ключевой информации. Этим условием может быть выбор самых больших *n* блоков, либо *n* блоков, наиболее удаленных от края изображения, и т.п.

На следующем этапе производится вычисление координат центроидов маркированных объектов переднего плана [10]. В двухмерном пространстве изображения–контейнера первый момент относительно оси *x* рассчитывается по формуле

$$\bar{x}\iint b(x,y)\,dxdy = \iint xb(x,y)\,dxdy \ ,$$

а относительно оси *y* по формуле

$$\bar{y}\iint b(x,y)\,dxdy = \iint yb(x,y)\,dxdy \ ,$$

где $(\bar{x},\bar{y})$ – координаты геометрического центра.

Далее происходит выбор пикселей, в которые будет встраиваться ЦВЗ с учетом того, что начальной точкой отсчета в каждом маркированном блоке переднего плана будет являться координата центроида. На выходе на данном этапе будем иметь матрицу с координатами пикселей, в которые будет встраиваться ЦВЗ.

Координаты пикселей также будут зависеть от самого метода встраивания, так как есть методы, в которых для встраивания ЦВЗ недопустимо использование рядом находящихся пикселей. Так, например, в методе Куттера – Джордана – Боссена для извлечения ЦВЗ производится прогнозирование значения яркости синего цвета, которое основывается на значениях ближестоящих пикселей, что сказывается на недопустимости изменения их.

На последнем этапе происходит встраивание ЦВЗ в изображение-контейнер одним из известных методов. Встраивание будет происходить таким образом, что *n* матриц, содержащих значения ЦВЗ по каждому модулю, будут встраиваться в *n* маркированных блоков переднего плана, где каждому модулю будет соответствовать свой маркированный объект переднего плана (маркированный блок переднего плана).

Количество маркированных объектов переднего плана должно быть не менее количества модулей, по которым будет представляться ЦВЗ. Остатки по каждому отдельному модулю будут записываться в соответствующий по счету маркированный объект переднего плана. Таким образом, остатки по модулям $m_1, m_2, \ldots, m_i, \ldots, m_{k+1}, m_{k+2}, \ldots, m_{k+n}$ будут записываться в блоки $1, 2, \ldots, i, \ldots, k+1, k+2, \ldots, k+n$ соответственно.

Для извлечения ЦВЗ необходимо будет выполнить преобразования, аналогичные преобразованиям, выполняемым для встраивания ЦВЗ. Так, с использованием стегоключа производится вычисление маркированных объектов переднего плана. После выполнения данных операций вычисляются центроиды маркированных объектов переднего плана, и, в соответствии со схемой встраивания, определяются пиксели, в которые было встроено ЦВЗ.

Следующим этапом является проверка на наличие искажений и ошибок, а в случае их обнаружения – коррекция на основе метода проекций.

Выводы

Разработанный алгоритм внедрения ЦВЗ в цифровое изображение, отличающийся от известных использованием математического аппарата модулярной арифметики и морфологических методов, позволяет повысить его целостность при различных деструктивных воздействиях за счет использования механизмов контроля и самовосстановления, с учетом обеспечения незаметности ЦВЗ и слепого извлечения ЦВЗ, а также преодолеть проблему последовательного заполнения бит изображения и позволить осуществить запись бит в значимые области цифрового изображения.

Список литературы

1. Невская М.А. Авторское право в издательском бизнесе и СМИ / М.А. Невская, Е.Н. Тарасова, Е.Е. Сухарев. – М.: Дашков и К°, 2008. – 300 с.

2. Грибунин В.Г. Стеганографические системы. Атаки, пропускная способность каналов и оценка стойкости:

учебно-методическое пособие / В.Г. Грибунин, В.Е. Костюков, А.П. Мартынов, Д.Б. Николаев, В.Н. Фомченко, ред. В.Г. Грибунин. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2015. – 217 с.

3. Земцов А.Н. Методы цифровой стеганографии для защиты авторских прав. – LAP AcademicPublishing, 2012. – 148 с.

4. Кухаренко Б.Г. Алгоритмы выделения объектов переднего плана из фона и интерактивного редактирования изображений / Б.Г. Кухаренко // Приложение к журналу «Информационные технологии». – 2012. – № 4. – 32 с.

5. Гонсалес Р. Цифровая обработка изображений: пер. с англ. / Р. Гонсалес, Р. Вудс; под ред. П.А. Чочиа. – М.: Техносфера, 2012. – 1104 с.

6. Грибунин В.Г. Стеганографические системы. Критерии и методическое обеспечение: учебно-методическое пособие / В.Г. Грибунин, В.Е. Костюков, А.П. Мартынов, Д.Б. Николаев, В.Н. Фомченко, ред. В.Г. Грибунин. – Саров: ФГУП «РФЯЦ-ВНИИЭФ», 2016. – 324 с.

7. Chae J. Robust Techniques for Data Hiding in Images and Video. PhD thesis, Department for Electrical and Computer Engineering. Univ.of California, Santa Barbara, CA, USA, 1999. 82 p.

8. Гражданский кодекс Российской Федерации (часть четвертая): Федеральный Закон от 18.12.2006 № 230–ФЗ // Собрание Законодательства Российской Федерации. – 2006. – № 52. – С. 14803–14949.

9. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Советское радио, 1968. – 440 с.

10. Абасова А.М. Алгоритм повышения устойчивости к деструктивным воздействиям цифровых водяных знаков, встраиваемых в цветное изображение / А.М. Абасова // Известия ЮФУ. Технические науки. Комплексная безопасность сложных систем. – 2014. – № 8 (157). – С. 75–81.