Раздел II. Криптографические методы защиты информации

УДК 004.021:004.624

А.М. Абасова

АЛГОРИТМ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ К ДЕСТРУКТИВНЫМ ВОЗДЕЙСТВИЯМ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, ВСТРАИВАЕМЫХ В ЦВЕТНОЕ ИЗОБРАЖЕНИЕ

Описывается реализация обеспечения защиты авторских прав, прав интеллектуальной собственности мультимедийного контента и скрытой передачи информации путем использования внедренных цифровых водяных знаков (ЦВЗ). В качестве контейнера рассматривается цветное цифровое изображение. Приводятся общие требования к стегосистемам, осуществляющим встраивание ЦВЗ, представлены категории воздействия на стегосистемы. Рассматривается алгоритм повышения устойчивости стегоалгоритма внедрения ЦВЗ к деструктивным воздействиям путем совместного использования математического аппарата модулярной арифметики и морфологических методов обработки изображений. Предложено представить ЦВЗ в избыточном модулярном коде, позволяющем извлечь и восстановить ЦВЗ при возникновении различных воздействий на изображение. Задан способ встраивания бит сообщения в блоки переднего плана, позволяющий преодолеть проблему последовательного заполнения бит изображения, что обеспечит повышение стойкости алгоритма к стегоанализу. Описан алгоритм и приведена структурная схема внедрения ЦВЗ в цветное изображение, учитывающая требования к стегосистемам встраивания ЦВЗ.

Стеганография; стегоконтейнер; цифровой водяной знак; морфологическая обработка изображений; модулярная арифметика.

A.M. Abasova

ALGORITHM INCREASED THE STABILITY TO THE DESTRUCTIVE INFLUENCES OF DIGITAL WATERMARKING, EMBEDDED IN COLOUR IMAGE

In this article we consider the implementation of ensure and safeguard copyright and intellectual property rights for multimedia content and secure communication through the use of embedded digital watermarking (DW). As the container is considered a color digital image. We provide general requirements for performing insertion stegosystem DW, present by exposure category stegosystem. In this article we discusse a method for increasing the stability stegoalgoritma DWintroduction to destructive influences by sharing the mathematical apparatus of modular arithmetic and morphological image processing techniques. We provides a method of representation in excess DW modular code that allows to extract and recover in the event of DW various effects on the image. We provides a specified method of embedding bits posts in the foreground blocks, allowing to overcome the problem of sequential filling bit image. We describe an algorithm and show structural circuit implementation DW in color image, taking into account the requirements for embedding stegosystem DW.

Steganography; stego container; digital watermarkind; morphological image processing; modular arithmetic.

Введение. Цифровые водяные знаки (ЦВЗ) обеспечивают защиту авторских прав, прав интеллектуальной собственности мультимедийного контента, а также скрытой передачи информации [1, 2, 3]. Алгоритм встраивания ЦВЗ в цветное изображение должен учитывать требования по обеспечению помехоустойчивости, невидимости встроенного ЦВЗ для зрительной системы человека [4]. Устойчивость к преднамеренным воздействиям также является важным требованием к ЦВЗ цветного изображения, так как встроенный ЦВЗ может быть удален или изменен до такой степени, что его невозможно будет обнаружить и извлечь. Устойчивость ЦВЗ зависит и от непреднамеренных воздействий, которые могут возникнуть в результате изменения в цветовом пространстве или в случае общего искажения сигнала.

Можно выделить следующие категории воздействий на стегосистемы встраивания ЦВЗ [5]:

- воздействия против встроенного сообщения (линейная фильтрация, сжатие изображений, добавление шума, выравнивание гистограммы, изменение контрастности);
- воздействия против стегодетектора (масштабирование, сдвиги, повороты, усечение изображения, перестановка пикселов);
- воздействия против протокола использования ЦВЗ (создание ложных ЦВЗ добавлением нескольких ЦВЗ);
- воздействия против ЦВЗ (атаки сговора, статистического усреднения, методы очистки сигналов от шумов, нелинейная фильтрация).

Известные алгоритмы повышения робастности стеганографических методов ЦВЗ к деструктивным воздействиям увеличивают вычислительную сложность методов внедрения ЦВЗ, обеспечивая безопасность информации на заданном уровне.

В данной статье предложен алгоритм повышения устойчивости стегоалгоритма встраивания ЦВЗ в цветное изображение к преднамеренным и непреднамеренным воздействиям на аналогичном уровне безопасности без применения вычислительно сложных алгоритмов на примере модификации метода замены младшего значащего бита (LSB).

Алгоритм встраивания ЦВЗ путем замены младшего бита (LSB). Метод встраивания ЦВЗ путем замены младшего бита (LSB) является самым известным и не требующим больших вычислительных ресурсов методом, работающим в пространственной области [5]. Встраивание ЦВЗ будет происходить в 24-битовое растровое изображение I, представленное в виде файлов форматом bmp, png, tiff и др. ЦВЗ будет представлять собой бинарное изображение n на m бит. Это может быть как логотип, так и QR-код. Изображение I цветового пространства RGB представляет собой трехмерный массив со значениями компонентов, отвечающих за красную (Red) M_R, зеленую (Green) M_G и синюю (Blue) M_B составляющие цвета элемента изображения I. Встраивание ЦВЗ будет осуществляться в два последних младших бита пикселей, окружающие центроиды блоков переднего плана, способом, представленным на рис. 1. Для определения данных блоков было предложено выполнить морфологическую эрозию и дилатацию изображения по примитиву b, который представляет собой стего–ключ, необходимый для извлечения ЦВЗ, а также определить локальные максимумы изображения.

При реализации вычисления координат для внедрения ЦВЗ выполняются следующие этапы:

- преобразование RGB изображения I в полутоновое I'

$$Y = 0{,}299R + 0{,}587G + 0{,}114B, \quad (1)$$

где Y – яркостное значение; R, G, B – соответственно значение красной, зеленой, голубой компонент в данной точке;

- формирование примитива b для осуществления операций морфологической дилатации и эрозии. Примитив может представлять собой ромбообразный, прямоугольный, диагональный и др. структурный элемент;
- нахождение объектов переднего плана, используя морфологическую дилатацию и эрозию.

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

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

где $D_{I'}$, D_b – области определения изображений I', b соответственно.

В случае, если значения примитива положительные, результирующее изображение становится темнее исходного, яркие детали ослабляются в зависимости от значений яркости элементов изображения вокруг этих деталей, а также от формы и амплитудных значений примитива [6, 7].

Полутоновая дилатация I' по примитиву b, обозначаемая $I' \oplus b$, определяется как

$$(I' \oplus b)(s,t) = \\ = \max\{I'(s-x,t-y) + b(x,y) | (s-x,t-y) \in D_{I'}; (x,y) \in D_b\}, \quad (3)$$

где $D_{I'}$, D_b – области определения изображений I', b соответственно.

В случае, если значения примитива положительные, результирующее изображение становится ярче исходного, темные детали ослабляются в зависимости от соотношения их размеров и яркостей с параметрами используемого при дилатации примитива [6, 7].

Применение методов морфологической дилатации и эрозии приведет к перемещению темных пятен и формированию блоков переднего плана по вычисленным значениям локальных максимумов.

- вычисление координат центроидов блоков переднего плана и окружающих их пикселей для внедрения ЦВЗ, согласно способу, указанному на рис. 1, где x, y – координаты пикселя.

				$x_{c+\frac{n}{4}}, y_c$				
				...				
				x_{c+2}, y_c				
				x_{c+1}, y_c				
$x_c, y_{c-\frac{n}{4}}$	...	x_c, y_{c-2}	x_c, y_{c-1}	x_c, y_c	x_c, y_{c+1}	x_c, y_{c+2}	...	$x_c, y_{c+\frac{n}{4}}$
				x_{c-1}, y_c				
				x_{c-2}, y_c				
				...				
				$x_{c-\frac{n}{4}}, y_c$				

Рис. 1. Последовательность окружающих центроид точек для внедрения ЦВЗ

Исходное изображение I разделяется на компоненты RGB. Таким образом, выделяются необходимые двумерные матрицы полученных блоков, которые будут служить стегоконтейнером. Так как система человеческого зрения менее восприимчива к изменениям в синем цвете и более восприимчива к зеленому, то внедрение ЦВЗ будет происходить в матрицу M_B и M_R. Изменение двух последних (младших) бит в матрицах M_B и M_R позволяет записывать любую информацию в битовом представлении. Принимая во внимание категории воздействия на стегосистемы, для обеспечения устойчивости данного алгоритма и эффективного исправления ошибок представим ЦВЗ в виде корректирующего кода.

Учитывая возможность параллельной обработки данных модулярного кода [8], обеспечивающего быстродействие работы системы, будем использовать его для представления ЦВЗ.

Общие сведения о модулярной арифметике. Пусть заданы попарно взаимно простые модули (основания): положительные числа $m_1, m_2, \dots, m_i, \dots, m_k$,

$$\text{НОД}\left(m_i, m_j\right) = 1 \text{ для } i \neq j. \quad (4)$$

Значение $P = \prod_{i=1}^{k} m_i$ определяет информационный диапазон получившейся числовой системы. Любое неотрицательное число A может быть однозначно представлено модулярным кодом:

$$A = \{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_k\}, \quad (5)$$

компонентами которого являются натуральные числа, удовлетворяющие условию: $0 \leq \alpha_1 < m_i$, где $i = 1,2, \dots, k$.

Фундаментальным положением, лежащим в основе модулярных вычислений, является Китайская теорема об остатках.

Пусть даны попарно взаимно простые модули $m_1, m_2, \dots, m_i, \dots, m_k$ и число $X \in Z(P)$, модулярное представление которого $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_k\}$ определяется выражением

$$\alpha_1 = |A|_{m_i}, \text{ где } i = 1,2, \dots, k. \quad (6)$$

Для каждого специального кода, от которого требуется, чтобы он обладал способностью к обнаружению и коррекции ошибок, характерно наличие двух групп цифр – информационной $J_A = \{\propto_1, \propto_2, \dots, \propto_i\}$ и контрольной $K_A = \{\propto_{k+1}, \dots, \propto_{k+n}\}$ части кода соответственно.

Под ошибкой будем понимать любое искажение значения, соответствующего какому-либо модулю в модулярном представлении числа. Выявленная ошибка может быть исправлена одним из существующих корректирующих методов [8, 9].

Организация встраивания ЦВЗ в изображение. Для представления ЦВЗ в модулярный код достаточно найти остатки по модулям $m_1, m_2, \dots, m_i, \dots, m_{k+1}, m_{k+2}, \dots, m_{k+n}$, определить информационный диапозон P и полный диапазон системы с контрольными основаниями $P' = \prod_{i=1}^{k+n} m_i$. Полученные остатки будут представлены данными размерностью по четыре бит. Данные остатки занесем в младшие биты матриц M_B, M_R по схеме, представленной на рис. 2.

Таким образом, остатки по модулям $m_1, m_2, \dots, m_i, \dots, m_{k+1}, m_{k+2}, \dots, m_{k+n}$ будут записываться в блоки $1,2, \dots, i, \dots, k+1, k+2, \dots, k+n$ соответственно.

Согласно положениям модулярной арифметики, числа, с которыми оперирует устройство, лежат в диапазоне $[0, P')$. Признаком ошибки является выполнение условия

$$A > P. \quad (7)$$

Структурная схема алгоритма встраивания ЦВЗ приведена на рис. 3.

Считывание ЦВЗ. Для извлечения информации, содержащейся в ЦВЗ, производится процедура вычисления координат точек, окружающих центроиды блоков переднего плана, с выполнением этапов, указанных ранее.

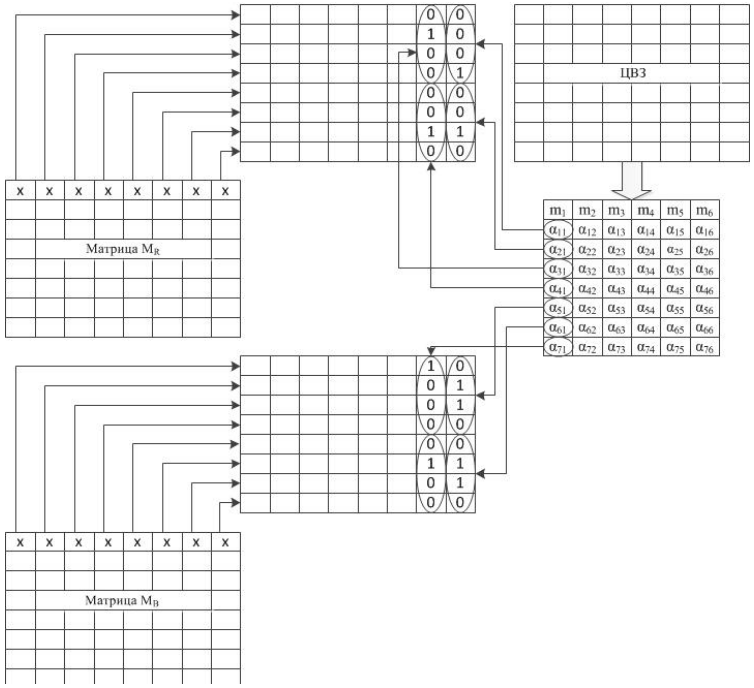

Рис. 2. Схема встраивания ЦВЗ

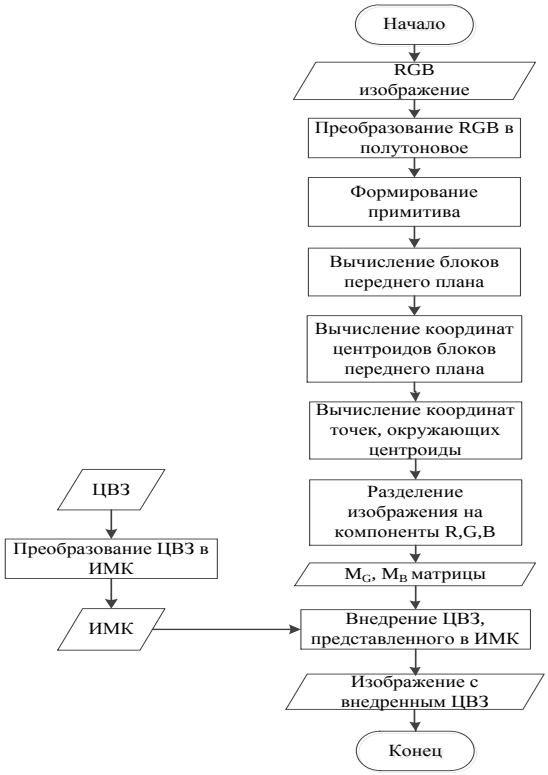

Рис. 3. Структурная схема алгоритма внедрения ЦВЗ

Таким образом, определяются точки, в которых записана информация о ЦВЗ. Эта информация представляет систему чисел $\{\alpha_1, \alpha_2, \dots, \alpha_i, \dots, \alpha_{k+n}\}$, обладающую свойствами обнаружения и исправления ошибок [10]. Данные подвергаются проверке в соответствии с условием (7). В случае, если данные не подвержены изменению, осуществляется процедура считывания информации и обратное преобразование из ИМК в ЦВЗ, представляющее собой бинарное изображение n на m бит в позиционной системе счисления. В случае, если данные подвергнуты изменению, осуществляется процедура коррекции свойствами ИМК, а только затем осуществляется процедура считывания и преобразования информации.

Выводы. Предложенный алгоритм повышения устойчивости стегоалгоритма встраивания ЦВЗ путём объединения математического аппарата модулярной арифметики и морфологических методов обработки изображений обеспечивает невосприимчивость к большинству известных атак на стегосистемы. Предложенный способ представления ЦВЗ в избыточном модулярном коде позволяет извлечь и восстановить ЦВЗ при возникновении различных воздействий на изображение. Новый способ встраивания бит ЦВЗ позволяет преодолеть проблему последовательного заполнения бит изображения, что позволит повысить стойкость алгоритма LSB к стегоанализу.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Petitcolas F., Anderson R., Kuhn M.* Attacks on Copyright Marking Systems // Lecture Notes in Computer Science. – 1998. – P. 218-238.
2. *Коханович Г.Ф., Пузыренко А.Ю.* Компьютерная стеганография. Теория и практика. – Киев: МК-Пресс, 2006. – 288 с.
3. *Swathi B., Shalin K.i, Naga Prasanthi K.* A review on steganography using images // Asian Journal of Computer Science and Information Technology. – 2013. – P. 234-237.
4. *Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А.* Стеганография, цифровые водяные знаки и стегоанализ. – М.: Вузовская книга, 2009. – 220 с.
5. *Грибунин В.Г.* Цифровая стеганография. – М.: СОЛОН–Пресс, 2002. – 272 с.
6. *Гонсалес Р., Вудс Р.* Цифровая обработка изображений: Пер. с англ. / Под ред. П.А. Чочиа. – М.: Техносфера, 2005. – 882 с.
7. *Грузман И.С., Киричук В.С., Косых В.П., Перетягин Г.И., Спектор А.А.* Цифровая обработка изображений в информационных системах: Учебное пособие. – Новосибисрк: Изд-во НГТУ, 2002. – 352 с.
8. *Акушский И.Я., Юдицкий Д.И.* Машинная арифметика в остаточных классах. – М.: Советское радио, 1968. – 440 с.
9. *Omondi, Amos R., and Benjamin Premkumar.* Residue number systems theory and implementation. London: Imperial College Press, 2007. – 296 p.
10. *Амербаев В.М.* Теоретические основы машинной арифметики. – Алма-Ата: Наука, 1976. – 323 с.

REFERENCES

1. *Petitcolas F., Anderson R., Kuhn M.* Attacks on Copyright Marking Systems, *Lecture Notes in Computer Science*, 1998, pp. 218-238.
2. *Kokhanovich G.F., Puzyrenko A.Yu.* Komp'yuternaya steganografiya. Teoriya i praktika [Computer steganography. Theory and practice]. Kiev: MK-Press, 2006, 288 p.
3. *Swathi B., Shalin K.i, Naga Prasanthi K.* A review on steganography using images, *Asian Journal of Computer Science and Information Technology*, 2013, pp. 234-237.
4. *Agranovskiy A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S.A.* Steganografiya, tsifrovye vodyanye znaki i stegoanaliz [Steganography, digital watermarking and steganalyst]. Moscow: Vuzovskaya kniga, 2009, 220 p.
5. *Gribunin V.G.* Tsifrovaya steganografiya [Digital steganography]. Moscow: SOLON–Press, 2002, 272 p.
6. *Gonzalez R. C., Woods R.E.* Digital Image Processing. Prentice Hall, 2002, 813 p. (Russ. ed.: Gonsales R., Vuds R. Tsifrovaya obrabotka izobrazheniy. Moscow: Tekhnosfera Publ., 2005, 882 p).

7. *Gruzman I.S., Kirichuk V.S., Kosykh V.P., Peretyagin G.I., Spektor A.A.* Tsifrovaya obra-botka izobrazheniy v informatsionnykh sistemakh [Digital image processing in information systems]: Uchebnoe posobie. Novosibisrk: Izd-vo NGTU, 2002, 352 p.
8. *Akushskiy I.Ya., Yuditskiy D.I.* Mashinnaya arifmetika v ostatochnykh klassakh [Machine arithmetic in residual classes]. Moscow: Sovetskoe radio, 1968, 440 p.
9. *Omondi, Amos R., and Benjamin Premkumar.* Residue number systems theory and implementation. London: Imperial College Press, 2007, 296 p.
10. *Amerbaev V.M.* Teoreticheskie osnovy mashinnoy arifmetiki [Theoretical foundations of computer arithmetic. Alma-Ata: Nauka, 1976, 323 p.

Статью рекомендовал к опубликованию д.т.н., профессор Я.Е. Ромм.

Абасова Анастасия Михайловна – Южный федеральный университет; e-mail: moonriel@yandex.ru; 347928, г. Таганрог, ул. Чехова, 22; тел.:+79615006290; кафедра безопасности информационных технологий; аспирантка.

Abasova Anastasiya Mikhailovna – Southern Federal University; e-mail: moonriel@yandex.ru; 22, Chekhova street, Taganrog, 347928, Russia; phone: +79615006290; the department of security in data processing technologies; postgraduate student.

УДК 621.396.624:621.396.96

К.Е. Румянцев, А.П. Плёнкин

СИНХРОНИЗАЦИЯ СИСТЕМЫ КВАНТОВОГО РАСПРЕДЕЛЕНИЯ КЛЮЧА ПРИ ИСПОЛЬЗОВАНИИ ФОТОННЫХ ИМПУЛЬСОВ ДЛЯ ПОВЫШЕНИЯ ЗАЩИЩЁННОСТИ*

Исследования посвящены оценке вероятностных характеристик системы квантового распределения ключа (СКРК) в режиме вхождения в синхронизм. Описаны методы синхронизации оптических систем, принцип действия которых основывается на приёме многофотонных и фотонных импульсов. Предложен алгоритм поиска фотонного импульса при использовании идеального счетчика фотоэлектронов, на основе которого разработана программа для ЭВМ, имитирующая алгоритм вхождения в синхронизм системы КРК на предварительном этапе поиска. Получены аналитические выражения для расчёта вероятностных характеристик СКРК на предварительном этапе поиска при использовании фотонных импульсов для повышения защищённости СКРК от несанкционированного съёма информации. Оценено влияние параметров фотонного импульса, однофотонного фотоэмиссионного прибора и аппаратуры поиска при идеальной регистрации фотонов на вероятность правильного обнаружения сигнального временного окна. Определено выражение для расчёта предельно реализуемой вероятности ошибочного обнаружения сигнального временного окна. Обоснован выбор параметров аппаратуры поиска, фотонного импульса, однофотонного детектора. Предложена методика проектирования СКРК в режиме вхождения в синхронизм при идеальной однофотонной регистрации. Квантовое распределение ключа; защищённость, синхронизация; фотонный импульс, вероятность обнаружения.

Квантовое распределение ключа; защищённость, синхронизация; фотонный импульс; вероятность обнаружения.

* Работа выполнена в рамках государственного задания Министерства образования и науки РФ высшим учебным заведениям в части проведения научно-исследовательских работ. Тема № 213.01-11/2014-9.