УДК 519.7

Стеганографические методы, устойчивые к JPEG сжатию

М.В. Куркина[1], И.В. Пономарев[2], Д.И. Строкин[2]

[1] Югорский государственный университет (Ханты-Мансийск, Россия)
[2]Алтайский государственный университет (Барнаул, Россия)

Steganographic Methods Resistant to JPEG Compression

M.V. Kurkina[1], I.V. Ponomarev[2], D.I. Strokin[2]

[1] Ugra State University (Khanty-Mansiysk, Russia)
[2]Altai State University (Barnaul, Russia)

Активное развитие компьютерных систем и информационных технологий подразумевает под собой рост значимости обеспечения защиты и безопасности информации при ее передаче или хранении. На сегодняшний день выполнение необходимых требований конфиденциальности данных развивается в направлении криптографии и стеганографии. Выбор применяемого метода кодирования информации напрямую зависит от целей пользователя, а также имеющихся программных средств. Основным требованием, предъявляемым к процессу кодирования сообщения, является наличие приемлемой вычислительной сложности реализации.

В статье рассматриваются методы обеспечения конфиденциальности данных средствами цифровой стеганографии, использующиеся в качестве файлов-контейнеров изображения формата BMP и проводящие их последующее сжатие к формату JPEG без потери скрываемой информации. Изучаются математические методы построения стеганосистемы для кодирования ASCII-сообщения, каждый символ которого кодируется ровно одним байтом. В результате была создана компьютерная программа на базе среды программирования Microsoft Visual Studio 2017 и языка программирования C# (платформа .NET Framework). Стегоключом в данном случае является последовательность шагов между пикселями изображения, в которые происходит встраивание информации. При этом алгоритм позволяет запоминать не всю последовательность шагов (т.е. не весь стегоключ), а лишь первые 5 символов ключа или половину ключа.

Ключевые слова: стеганосистема, метод Коха — Жао, цветовое пространство, файл-контейнер.

DOI: 10.14258/izvasu(2021)1-17

The active development of computer systems and information technologies implies an increase in the importance of ensuring the protection and security of information during its transfer or storage. Today, the fulfillment of the necessary data confidentiality requirements tends to the direction of cryptography and steganography. The choice of the applied method of encoding information directly depends on the goals of the user, as well as the available software. The main requirement for the message encoding process is the availability of acceptable computational complexity of the implementation.

The article discusses methods of ensuring data confidentiality employing digital steganography, using BMP images as container files, and carrying out their subsequent compression to the JPEG format without losing hidden information. Mathematical methods of constructing a stegosystem for encoding ASCII are studied — a message, each character of which is encoded with exactly one byte. As a result, a computer program was created based on the Microsoft Visual Studio 2017 programming environment and the C# programming language (.NET Framework). The stereotype, in this case, is a sequence of steps between image pixels, into which information is embedded. In this case, the algorithm allows you to memorize not the entire sequence of steps (that is, not the entire keystroke), but only the first five characters of the key or half of the key.

Key words: stegosystem, Koha — Zhao method, color space, file container.

Введение, постановка задачи. Основная задача стеганографических методов заключается не только в том, что необходимо произвести сокрытие конфиденциальной информации, но и в сокрытии самого факта существования данной информации при передаче, хранении или обработке [1, 2].

Определение. Контейнером (носителем) называют несекретные данные, которые используют для сокрытия сообщений. Пустой контейнер — контейнер без встроенного сообщения; заполненный контейнер или стегоконтейнер, содержащий встроенную информацию.

В качестве носителей информации будем рассматривать статические растровые изображения без сжатия, т.е. формата BMP. Для сокрытия сообщений мы могли бы использовать распространенный стеганографический метод LSB (метод наименее значащего бита), заключающийся в том, что передаваемая информация встраивается в значения младших битов изображения [3, 4]. Но у такого способа есть значительные недостатки:

- неоправданно большой размер стегоконтейнеров;
- практически полное отсутствие устойчивости конечного зашифрованного сообщения к модификациям изображения (изменениям яркости и контрастности, различным сжатиям).

Поэтому весьма целесообразно было бы совместно с сокрытием данных проводить одновременное сжатие файла контейнера, но для этого необходимо разобраться с особенностями формата JPEG.

Алгоритм сжатия JPEG. Рассмотрим алгоритм более подробно, в качестве исходного файла-контейнера выберем 24-битное растровое изображение (каждый пиксель является комбинацией трех составляющих цветов по модели RGB: красного, зеленого и синего; насыщенность каждого цвета кодируется 8 битами) [5].

Шаг 1. Перевод изображения из цветового пространства RGB в цветовое пространство $YCrCb$. Здесь: Y — яркостная составляющая, а Cr, Cb — компоненты, отвечающие за цвет (хроматический красный и хроматический синий). За счет того что человеческий глаз менее чувствителен к цвету, чем к яркости, появляется возможность архивировать массивы для Cr и Cb компонент с большими потерями и, соответственно, большими степенями сжатия.

$$\begin{cases} Y &= 0.299R + 0.587G + 0.114B, \\ Cr &= 0.5R - 0.4187G - 0.0813B + 128, \\ Cb &= -0.1687R - 0.3313G + 0.5B + 128. \end{cases} \quad (1)$$

Шаг 2. Исходное изображение разбивается на матрицы размером 8×8 пикселей.

Шаг 3. К каждой полученной матрице (по каждой компоненте Y, Cr, Cb) применяется дискретное косинусное преобразование Фурье (ДКП) [6]:

$$T_{ij} = C_i C_j \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} p_{xy} \cos \frac{(2y+1)j\pi}{2n} \cos \frac{(2x+1)i\pi}{2n},$$

$$C_i = \begin{cases} \sqrt{\frac{1}{N}}, & \text{если } i = 0, \\ \sqrt{\frac{2}{N}}, & \text{если } i \neq 0 \end{cases},$$

где p_{xy} — значение атрибута пикселя, зависящее от цветовой модели представления изображения.

DC	НЧ	НЧ	НЧ	НЧ	НЧ	НЧ	СЧ
НЧ	НЧ	НЧ	НЧ	НЧ	НЧ	СЧ	СЧ
НЧ	НЧ	НЧ	НЧ	НЧ	СЧ	СЧ	ВЧ
НЧ	НЧ	НЧ	НЧ	СЧ	СЧ	ВЧ	ВЧ
НЧ	НЧ	НЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ
НЧ	НЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ
НЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ
СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ

Компоненты матрицы ДКП: DC — коэффициент, содержащий информацию о яркости всего блока; НЧ — низкочастотные; СЧ — среднечастотные; ВЧ — высокочастотные коэффициенты

Шаг 4. Квантование полученных матриц (основной этап сжатия). Преобразование выполняется последовательным делением каждого коэффициента матрицы ДКП на значение шага квантования и округлением полученного значения. Шаг квантования определяется по формуле:

$$Q_{ij} = 1 + ((1 + i + j)q),$$

где q — это степень сжатия (обычно берется небольшое значение, например, $q = 2$). Получаемая матрица квантования:

$$\begin{vmatrix} 3 & 5 & 7 & 9 & 11 & 13 & 15 & 17 \\ 5 & 7 & 9 & 11 & 13 & 15 & 17 & 19 \\ 7 & 9 & 11 & 13 & 15 & 17 & 19 & 21 \\ 9 & 11 & 13 & 15 & 17 & 19 & 21 & 23 \\ 11 & 13 & 15 & 17 & 19 & 21 & 23 & 25 \\ 13 & 15 & 17 & 19 & 21 & 23 & 25 & 27 \\ 15 & 17 & 19 & 21 & 23 & 25 & 27 & 29 \\ 17 & 19 & 21 & 23 & 25 & 27 & 29 & 31 \end{vmatrix}.$$

После деления элементов матрицы, полученной после ДКП, на элементы матрицы квантования получается матрица, в которой небольшое число элементов, отличных от нуля, например:

$$\begin{vmatrix} 30 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -7 & -8 & 1 & 1 & 0 & 0 & 0 & 0 \\ -11 & 6 & 0 & 1 & 0 & 0 & 0 & 0 \\ -5 & -3 & 0 & 0 & 0 & 0 & 0 & 0 \\ -7 & -3 & 2 & 0 & 0 & 0 & 0 & 0 \\ -4 & 4 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}.$$

На этом же шаге проводится встраивание сообщения в имеющийся блок. Это может быть организовано с помощью метода Коха – Жао [7] или метода Бенгама – Мемона – Эо – Юнга [8].

Реализация первого метода заключается в том, что во время организации секретного канала абоненты должны предварительно договориться о двух конкретных среднечастотных коэффициентах ДКП из каждого блока, которые будут использоваться для сокрытия данных. Зададим данные коэффициенты их координатами в массивах коэффициентов ДКП: (u_1, v_1) и (u_2, v_2).

Далее выбираем b-ый блок Cb, предназначенный для передачи b-го бита сообщения. Встраивание информации осуществляется следующим образом: для передачи бита 0 необходимо, чтобы разница абсолютных значений коэффициентов ДКП превышала некоторую положительную величину, а для передачи бита 1 эта разница делается меньшей по сравнению с некоторой отрицательной величиной:

$$m_b = \begin{cases} 0, \text{ если } |\Omega_b(u_1, v_1)| - |\Omega_b(u_2, v_2)| > P; \\ 1, \text{ если } |\Omega_b(u_1, v_1)| - |\Omega_b(u_2, v_2)| < -P, \end{cases}$$

где $\Omega_b(u_1, v_1)$ — элемент матрицы ДКП.

Для извлечения скрытого сообщения применяется формула:

$$M_b = \begin{cases} 0, \text{ если } |\Omega_b(u_1, v_1)| - |\Omega_b(u_2, v_2)| > P; \\ 1, \text{ если } |\Omega_b(u_1, v_1)| - |\Omega_b(u_2, v_2)| < -P. \end{cases}$$

Здесь значение P задается заранее, и чем оно больше, тем стеганосистема, созданная на основе данного метода, является более стойкой к компрессии, однако качество изображения при этом значительно ухудшается.

Второй метод оптимизирует предыдущий метод путем встраивания сообщения не во все блоки, а только наиболее подходящие для этого. Игнорируемые блоки характеризуются наличием слишком больших значений низкочастотных коэффициентов ДКП, сопоставимых по своей величине с DC-коэффициентом. Также сообщение не встраивается в блоки, в которых большинство высокочастотных коэффициентов равны нулю.

Встраивание в блок бита сообщения совершается следующим образом. Выбираются три среднечастотных коэффициента ДКП блока с координатами (u_1, v_1), (u_2, v_2) и (u_3, v_3). Если необходимо провести встраивание 0, эти коэффициенты изменяются таким образом, чтобы третий коэффициент стал меньше любого из первых двух; если необходимо скрыть 1, он делается большим по сравнению с первым и вторым коэффициентами:

$$b = \begin{cases} 0, \text{ если } \begin{cases} |\Omega_b(u_3, v_3)| < |\Omega_b(u_1, v_1)| \\ |\Omega_b(u_3, v_3)| < |\Omega_b(u_2, v_2)| \end{cases}, \\ 1, \text{ если } \begin{cases} |\Omega_b(u_3, v_3)| > |\Omega_b(u_1, v_1)| \\ |\Omega_b(u_3, v_3)| > |\Omega_b(u_2, v_2)| \end{cases}. \end{cases}$$

Как и в предыдущем методе, для принятия решения о достаточности различия указанных коэффициентов ДКП вводится значение порога различения P:

$$m_b = 0, \text{ если } |\Omega_b(u_3, v_3)| < |\min(\Omega_b(u_1, v_1), \Omega_b(u_2, v_2))| - P;$$
$$m_b = 1, \text{ если } |\Omega_b(u_3, v_3)| > |\min(\Omega_b(u_1, v_1), \Omega_b(u_2, v_2))| + P.$$

Шаг 5. На этом этапе значения полученной матрицы можно экономно запомнить, применяя, например, кодирование по Хаффмену или другие схемы эффективного кодирования вместе с кодированием длин серий последовательностей (RLE – Run Length Encoding). Далее добавляется заголовок из использованных параметров JPEG и результат выводится в сжатый файл. Сжатый файл может представлять собой формат обмена, когда файл содержит сжатый образ и все необходимые декодеру таблицы (в основном это таблицы квантования и коды Хаффмана).

Декодирование JPEG происходит в обратном порядке, т.е. с помощью формулы обратного дискретного косинусного преобразования:

$$p_{xy} = \sum_{x=0}^{n-1} \sum_{y=0}^{n-1} C_i C_j T_{ij} \cos \frac{(2y+1)j\pi}{2n} \cos \frac{(2x+1)i\pi}{2n},$$

$$C_i = \begin{cases} \sqrt{\frac{1}{N}}, \text{ если } i = 0, \\ \sqrt{\frac{2}{N}}, \text{ если } i \neq 0 \end{cases}$$

и формулы обратного преобразования из цветового пространства YCrCb в RGB-пространство:

$$\begin{cases} R &= Y + 1.402(Cr - 128), \\ G &= Y - 0.34414(Cb - 128) - 0.71414(Cr - 128), \\ B &= Y + 1.772(Cb - 128). \end{cases}$$

Заключение и выводы. Приведенный в работе метод позволяет решать задачи сохранения конфиденциальности сообщения при передаче и хранении. Основанный на данном методе алгоритм имеет оптимальную сложность для кодирования информации небольшого объема. В результате была разработана компьютерная программа, реализующая указанный подход. Тестирование программы показало преимущества данного метода при декодировании полученного сообщения, оценке надежности и времени извлечения скрываемого сообщения [9, 10].

Дальнейшая работа будет направлена на разработку менее заметных способов сокрытия информации путем модификации палитры изображения, а также проведение стеганографического анализа устойчивости разработанных методов к различным атакам со стороны потенциального злоумышленника.

Библиографический список

1. Баричев С. Криптография без секретов. СПб., 2003.

2. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации. Киев, 2003.

3. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Киев, 2006.

4. Грибунин В.Г., Осков И.Н., Турницев И.В. Цифровая стеганография. М., 2009.

5. Сэломон Д. Сжатие данных, изображений и звука. М., 2004.

6. Филиппов М.В., Балашова С.А. Метод сокрытия информации в квантованных коэффициентах дискретного косинус преобразования // Инженерный вестник. 2016. № 8.

7. Koch E., Zhao J. Towards Robust and Hidden Image Copyright Labeling // IEEE Workshop on Nonlinear Signal and Image Processing. Neos Marmaras, 1995.

8. Аргановский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. М., 2009.

9. Shannon C.E. The communication theory of secrecy systems // Bell Sys. Tech. J. 1949. Vol. 28. № 4.

10. Урбанович П.П. Защита информации методами криптографии, стеганографии и обфускации. Минск, 2016.