

УДК 004.056.5

## НОВЫЙ ПОДХОД ДЛЯ АУТЕНТИФИКАЦИИ JPEG-ИЗОБРАЖЕНИЙ

М. А. Козина, А. В. Ахметьева

Одесский национальный политехнический университет  
Украина, г. Одесса  
mashaK1989@rambler.ru

*Предлагается новый стеганографический алгоритм, который реализует проверку целостности контейнера, использующий повторное сжатие изображения для его анализа. В качестве контейнера рассматривается цветное цифровое изображение. Исследован результат работы алгоритма на изображениях в различных форматах (без потерь и с потерями).*

*Ключевые слова: стеганографический алгоритм, аутентификация, цифровое изображение, JPEG, дискретно-косинусное преобразование.*

Отрасль информационных технологий является одной из наиболее динамично развивающихся отраслей в мире. Сегодня информация является одним из ценнейших ресурсов общества, наряду с такими традиционными материальными видами ресурсов как нефть, газ, полезные ископаемые и др., а значит, процесс ее обработки и использования по аналогии с процессами переработки материальных ресурсов можно воспринимать как технологию.

Разработкой средств и методов скрытия факта передачи секретной информации занимается стеганография. В современной стеганографии существуют два основных направления — аутентификация контейнера и организация канала скрытой передачи информации. Чаще всего эти два направления существуют и используются обособленно: стеганографические методы осуществляют либо только передачу конфиденциальных данных, либо только аутентификацию контейнера, в качестве которого в настоящей работе выступает цифровое изображение [1]. Актуальным вопросом остается разработка новых стеганографических методов и стеганоалгоритмов, которые объединяют эти два направления [2—5].

Одной из важных задач на сегодняшний день при передаче данных является минимизация объема передаваемой информации. Для сжатия изображений существует множество специальных методов, которые можно разделить на два больших класса: с потерями информации и без потерь. Наиболее распространенным форматом сжатия является JPEG. Метод сжатия JPEG относится к классу сжатия изображений с потерями информации. Его сильной стороной является большой коэффициент сжатия при сохранении исходной цветовой глубины. Именно это свойство обусловило его широкое применение в Интернете, где уменьшение размера файлов имеет первостепенное значение.

Целью данной работы является разработка основ алгоритма для решения задачи аутентификации JPEG-изображений.

Для достижения поставленной цели необходимо решить ряд задач:

- провести анализ JPEG-сжатия изображения при различных коэффициентах сжатия;
- выбрать размер блока разбиения;
- сделать анализ максимальной относительной ошибки.

В ходе решения поставленных задач был проведен вычислительный эксперимент, в котором было задействовано 400 цветных изображений размером 500×500 пикселей в форматах как без потерь (TIFF), так и с потерями (JPEG) [6].

Контейнер с матрицей размером  $M \times N$  разбивался на  $s \times s$ -блоки, соответственно величина  $B = [M/s] \times [N/s]$  определяла количество блоков, где  $[ \cdot ]$  — целая часть аргумента.

Пусть  $Y$  — матрица изображения после пересылки,  $Y_1$  — изображение, полученное адресатом, которое преднамеренно подверглось повторному сжатию.

Алгоритм сжатия JPEG использует разбиение изображения на блоки, размер которых  $s=8$ , далее для каждого из блоков строится дискретно-косинусное преобразование (ДКП).

В разрабатываемом алгоритме предлагается использовать разбиение матрицы изображения на блоки с размером  $s=2$ , увеличивая тем самым пропускную способность организуемого стеганографического канала связи, в предположении, что блок используется непосредственно как единица контейнера для погружения информации. В процессе стеганообразования изображения алгоритмом, устойчивым к сжатию, внедряется дополнительная информация. После этого изображение может быть сохранено в формате JPEG с коэффициентом качества, обеспечивающим сохранение надежности восприятия стеганосообщения и позволяющим эффективно декодировать погруженную информацию после сжатия.

Для проверки аутентичности изображение сжимается повторно (путем повторного пересохранения в формат JPEG). Для каждого блока изображений  $Y$  и  $Y_1$  соответственно строится ДКП, после чего оценивается относительная погрешность повторного сжатия:

$$\frac{|DCT_Y(i,j) - DCT_{Y_1}(i,j)|}{DCT_{Y_1}(i,j)} \times 100\%, \quad i, j = \overline{1, s}, \quad (1)$$

где  $DCT_Y$  и  $DCT_{Y_1}$  — ДКП для блоков изображения  $Y$  и  $Y_1$ , соответственно.

В каждом блоке выбирается максимальная погрешность, которая усредняется для всего изображения. Результат такого усреднения обозначается  $H$ .

На основании проведенного эксперимента в работе собраны статистические данные для значений  $H$  как для изображений, которые не подверглись атаке сжатием в процессе передачи по каналу связи, так и для изображений, которые были повергнуты атаке сжатия со значительными коэффициентами качества. Полученная статистика дает возможность определить пороговое значение  $H$ , позволяющее отделить JPEG-изображения, целостность которых была нарушена, от аутентичных, и является основой для нового стеганографического алгоритма.

#### ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Конахович Г. Ф., Пузиренко А. Ю. Комп'ютерна стеганографія. Теорія і практика. — Київ: «МК-Пресс», 2006. — 288 с., іл.
2. Глузов Н. И., Митекин В. А. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации // Компьютерная оптика.— 2011.— Т. 35, № 2.— С. 262—267.
3. Mandal, J. K., Ghoshal, N. Image Authentication Technique in Frequency Domain based on Discrete Fourier Transformation (IATFDDFT) / Proceedings of ICCS.— 2010.— P. 144—150.
4. Кобозева А. А., Шовкун А. Д. Стеганографический алгоритм скрытой передачи информации, обеспечивающий аутентификацию контейнера // Науковий вісник Міжнародного гуманітарного університету — 2012.— № 4.— С. 21—28.
5. Кобозева А. А., Козина М. А. Стеганографический метод двухэтапного декодирования, обеспечивающий аутентификацию контейнера // Інформатика та математичні методи в моделюванні.— 2013.— Т. 3, № 2.— С. 169—178.
6. NRCS Photo Gallery: [Электронный ресурс] // United States Department of Agriculture. Washington, USA. Режим доступа: <http://photogallery.nrcs.usda.gov> (Дата обращения: 15.12.2013).

М. О. Kozina, А. V. Ahmametieva

#### **New approach for authentication of JPEG - images.**

The authors present a new steganography method which realizes verification of integrity of the container and is based on the image analysis using re-compression. The colored digital image is considered as a container. The results of algorithm operation are tested on different formats of images, both lossless and lossy.

Keywords: *steganography method, authentication, digital image, JPEG, discrete cosine transformation.*