УДК 681.3

СТЕГАНОГРАФИЧЕСКОЕ СКРЫТИЕ ИНФОРМАЦИИ В СТАТИЧЕСКИХ ИЗОБРАЖЕНИЯХ

Богуш Р.П., *к.т.н., доцент, зав. кафедрой вычислительных систем и сетей Полоцкого государственного университета, Беларусь, bogushr@mail.ru*

Ключевые слова: стеганографическая система, статические изображения, дискретное преобразование, скрытие информации.

Рассматривается стеганографическая система скрытия информации, представленной в виде изображения в цветных статических изображениях. Для скрытия информации используется дискретное косинусное преобразование либо двумерное вейвлет-преобразование, адаптированные к современным алгоритмам сжатия изображений JPEG и JPEG2000 соответственно. Криптостойкость системы обеспечивается применением ассиметричного алгоритма RSA. Рассматриваются вопросы эффективности и робастности предлагаемой системы. Представлены результаты исследований, которые подтвердили возможность ее использования в системах скрытой передачи информации.

Введение

Широкое распространение мультимедийных технологий, сети Internet, непрерывное совершенствование компьютерной техники, методов обработки цифровой информации определило развитие стеганографии, которая позволяет обеспечивать обмен конфиденциальной информацией таким образом, что скрывается сам факт передачи такой информации.

В цифровой стеганографии используются следующие термины [1,2]:

- стегосистема – система скрытия данных на основе стеганографии;
- цифровой контейнер - любая цифровая информация, предназначенная для сокрытия конфиденциальных сообщений;
- скрытое сообщение – сообщение, встраиваемое в контейнер;
- стегоконтейнер - контейнер с внедренным в него скрытым сообщением.

Следует отметить, что используемый цифровой контейнер оказывает значительное влияние на безопасность передаваемой информации. Среди ряда возможных стегоконтейнеров - статические и динамические изображения. Это обусловлено наличием в большинстве реальных изображений текстурных областей, имеющих шумовую структуру и, следовательно, пригодных для встраивания дополнительной информации, слабой чувствительностью человеческого глаза к незначительным изменениям яркостных, цветовых и др. характеристик изображения, а также бурно развивающимися методами цифровой обработки изображений.

Стегосистема, использующая в качестве цифрового контейнера статическое изображение, должна удовлетворять следующим основным требованиям: свойства контейнера должны быть модифицированы так, чтобы изменения невозможно было определить при визуальной атаке; стегоконтейнер должен быть устойчив преднамеренным и непреднамеренным искажениям - сжатию с потерей информации, преобразованию в другой формат и т. д. В настоящее время существует ряд стеганографических систем [1-5], однако совершенствование методов обработки и сжатия изображений требует непрерывного их развития, так как чем более совершенными становятся методы сжатия, тем меньше остается возможностей для внедрения дополнительной информации. Поэтому в данном направлении непрерывно проводятся исследования, а число публикаций по данной тематике постоянно возрастает. Наиболее эффективны стегосистемы, реализующие скрытие данных в области спектральных преобразования с учетом особенностей алгоритмов сжатия изображений [3-5].

Целью данной работы является разработка и исследование алгоритмов скрытия данных в изображениях на основе дискретного косинусного преобразования и вейвлет-преобразования для стандартов сжатия JPEG и JPEG2000.

Внедрение и восстановление скрываемой информации

В разработанной стегосистеме сообщение, представляемое в виде изображения, внедряется в цифровой контейнер (статическое изображение) путем изменения амплитуд спектральных коэффициентов, полученных в результате прямого дискретного преобразования на основе выражения:

$$E = S + \frac{A}{255} \cdot (W - 128), \quad (1)$$

где S - амплитуда спектральной составляющей цифрового контейнера, E - амплитуда спектральной компоненты стегоконтейнера, W – компонента скрываемого сообщения, A - весовой коэффициент, определяемый величиной энергии, которую можно добавить к изображению без его существенного искажения.

В связи с тем, что свойства контейнера должны быть модифицированы так, чтобы изменение невозможно было выявить при визуальном контроле, энергия, добавленная к изображению, должна рассчитываться на этапе внедрения информации. Определение весового коэффициента для контейнера размером $N \times M$ выполняется на основе выражения:

$$A = \sqrt{\frac{4 \cdot k}{N_1} \cdot \sum_{i=1}^{N \cdot M} |S_i|^2}, \quad (2)$$

где N_1 - общее число компонент скрываемого сообщения; k – коэффициент внедрения, подбираемый для контейнера и скрываемого сообщения.

Для обеспечения высокой криптостойкости стегосистемы можно использовать ассиметричный современный криптографический алгоритм RSA, безопасность которого основана на сложности разложения на множители больших чисел [8]. Для скрытия в стегоконтейнере встроенного сообщения с помощью алгоритма RSA и обеспечения высокого быстродействия шифруются номера спектральных составляющих, в которых содержатся компоненты скрытого сообщения. При этом перед шифрованием каждый номер соответствующей спектральной составляющей дополняется строкой случайных бит длиной M (в зависимости от длины выбранного модуля).

Известно, что реальные изображения не являются случайным процессом с равномерно распределенными значениями величин, и большая часть энергии изображений сосредоточена в низкочастотной части спектра. Высокочастотные составляющие наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие, низкочастотная (размытие) или медианная фильтрация. Поэтому, для обеспечения устойчивости стегосистемы к алгоритмам сжатия использованы низкочастотные компоненты контейнера.

Таким образом, алгоритм скрытия сообщения требует выполнения следующих основных шагов: выполнение прямого дискретного преобразования для контейнера - ДКП при использовании алгоритма JPEG и вейвлет-преобразования при использовании JPEG2000; расчёт весового коэффициента для контейнера с использованием выражения (2); скрытие сообщения с использованием выражения (1) и алгоритма RSA; выполнение обратного дискретного преобразования.

Восстановление скрываемого сообщения требует наличие контейнера, стегоконтейнера и закрытого ключа алгоритма RSA. При этом требуется выполнить прямое дискретное преобразование для стегоконтейнера и извлечь сообщение с использованием закрытого ключа алгоритма RSA на основе выражения:

$$W = \frac{255}{A} \cdot (E - S) + 128,$$

где S - амплитуда спектральной составляющей цифрового контейнера, E - амплитуда спектральной компоненты стегоконтейнера,

Экспериментальные исследования

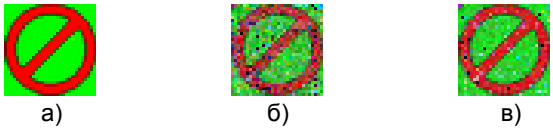
На первом этапе экспериментов при скрытии информации использовалось дискретное косинусное преобразование, а стегоконтейнеры подвергались JPEG сжатию и преобразованию в формат GIF и обратно. По результатам исследований установлено, что JPEG сжатие приводит к более существенным искажением встроенных сообщений по сравнению с преобразованием палитры стегоконтейнера (примеры показаны на рис. 1 - 3).

На втором этапе экспериментов при скрытии информации использовалось вейвлет-преобразование, а стегоконтейнеры, полученные с различными весовыми коэффициентами, подвергались JPEG2000 кодированию с разными степенями сжатия. По результатам исследований установлено, что для используемого стегоконтейнера необходим выбор оптимального весового коэффициента на основе визуального контроля стегоконтейнера при внедрении, а также установлено, что значительное увеличение степени сжатия все же приводит к потерям качества скрываемой информации. Поэтому дальнейшее совершенствование разработанной стегосистемы предполагается за счет применения помехоустойчивого кодирования. Результаты экспериментов представлены на рис. 4 и в таблицах 1 - 2. Размер цветного контейнера (24 бита на пиксель) составляет 305×200 пикселей. Внедряемое сообщение (рис. 4.1в) размером 42×39 пикселей (на рис. 4.1в и далее представлено увеличенным в два раза) использовалось без рамки, она показана на рисунке для наглядности границ. В ходе экспериментов рассчитывалась степень сходства восстановленного сообщения $D' = \{d'_{ij}\}$ и внедряемого $D = \{d_{ij}\}$ по формуле:

$$R^{SSD} = 1 - \frac{1}{256} \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (d_{ij} - d'_{ij})^2}{\sqrt{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (d_{ij})^2} \sqrt{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (d'_{ij})^2}}.$$

Рис.1. Контейнер

Рис.2. Стегоконтейнер



а) б) в)

Рис.3. Скрываемое изображение: а) исходный вид; б) восстановленное после JPEG сжатия стегоконтейнера; в) восстановленное после преобразования цветовой палитры стегоконтейнера.

а) б) в)

Рис. 4. Результаты экспериментов: а) цифровой контейнер (179КБ); б) стегоконтейнер (179КБ); в) скрытое сообщение (5 КБ).

Таблица 1

Размер файла стегоконтейнера, КБ Весовой коэффициент	115	45	21	12	8
50	0,996	0,995	0,989	0,958	0,899
100	0,996	0,995	0,989	0,965	0,916
200	0,996	0,995	0,989	0,973	0,942

Рассчитанные значения коэффициента схожести R^{SSD} для скрываемой и восстановленной информации приведены в Таблице 1, а в Таблице 2 даны восстановленные сообщения при различных степенях сжатия в формате JPEG2000.

Визуальный анализ результатов (таблица 2) и анализ рассчитанных коэффициентов схожести (таблица 1) показывает, что при оптимальном значении весового коэффициента для заданного контейнера значительное увеличение степени сжатия приводит к потерям качества восстановленного сообщения, в тоже время с увеличением весового коэффициента ухудшается качество стегоизображения.

Далее тестировалась робастность стегосистемы к потере или преднамеренной порче части стегоконтейнера при передаче или хранении. Стабильность стегосистемы проверялась следующим образом: в стегоконтейнере имитировалась потеря фрагмента изображения (до 30%) в произвольном месте. Результаты экспериментов показаны на рисунке 5 и в Таблице 3.

Из Таблицы 3 следует, что результаты экспериментов по робастности алгоритма к потере части информации стегоконтейнера.

Анализ полученных результатов показывает, что восстановленное изображение визуально распознаваемо даже при потере 25% контента стегоконтейнера.

Заключение

Для обеспечения робастности стегосистемы к компрессии изображений в форматах сжатия JPEG и JPEG-2000 предусмотрено возможность использования ДКП или вейвлет-преобразования на этапе внедрения скрываемого сообщения. Разработанный алгоритм скрытия информации использует низкочастотные компоненты изображения, что увеличивает его устойчивость к алгоритмам сжатия, при этом различие между стегоконтейнером и контейнером при оптимальном выборе параметров стегосистемы визуально установить достаточно сложно. Криптостойкость системы обеспечивается применением ассиметричного криптографического алгоритма RSA при внедрении информации в контейнер. Восстановление скрываемого сообщения требует наличие контейнера, стегоконтейнера и закрытого ключа алгоритма RSA.

Проведен ряд экспериментов, которые подтвердили эффективность данной стегосистемы и показали ее перспективность для скрытой передачи информации, в системах встраивания цифровых водяных знаков и идентификационных номеров. Однако по результатам исследований установлено, что при оптимальном коэффициенте внедрения для заданного контейнера значительное увеличение степени сжатия или фильтрация стегоконтейнера приводит к потерям качества восстановленного сообщения. В связи с этим, дальнейшее совершенствование разработанной стегосистемы возможно путем применения помехоустойчивых кодов на этапе внедрения информации в контейнер.

Таблица 2

Размер файла стегоконтейнера, КБ Весовой коэффициент	115	45	21	12	8
50					
100					
200					

а) б) в)

Рис.5. Стегоконтейнер с потерей части контента: а) с потерей 6,5 % контента в левом верхнем углу; б) с потерей 12,8 % контента в центральной части; в) с потерей 26 % контента в нижней части.

Таблица 3

Местоположение и количество утерянного изображения стегоконтейнера, %	в левом верхнем углу, 6,5 %	в центральной части, 12,8 %	в нижней части, 3 %	в нижней части, 13 %	в нижней части, 26 %
Восстановленное сообщение					
R^{SSD}	0,982	0,972	0,994	0,985	0,961

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г.Грибунин, И.Н Оков, И.В. Туринцев. - М.: СОЛОН-Пресс, 2002. - 261с.
2. Кащеев, А.А. Стеганографическая защита цифровых изображений / А.А. Кащеев, С.Б. Саломатин // Известия Белорусской инженерной академии. - 2003. - №1(15)/1. - С.215 - 217.
3. Akansu, A.N. Data hiding in multimedia - theory and applications/ A.N. Akansu //Doctoral Dissertation Department of ECE New Jersey Institute of Technology University Heights, Newark, NJ 07032, 1999.
4. Pereira, S. A framework for optimal adaptive DCT watermarks using linear programming / S. Pereira, T. Pun // Proc. of Tenth European Signal Processing Conf., EUSIPCO'2000, Tampere, Finland, Sep. 5 - 8 2000.- Tampere,2000. - P.42 - 46
5. Hassanien,A. Watermarking for copyright protection using discrete wavelet transform / A.Hassanien // Proc. of the 8 Int. Conf. Pattern Recognition and Information Processing, PRIP'2005, Minsk, May 18-20 2005 / Belarusian State University of Informatics and Radioelectronics.-Minsk, 2005 - P.185-191
6. Ватолин, Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. - М.: ДИАЛОГ-МИФИ, 2002. - 384 с.
7. Chen, G. Applications of Wavelet Transforms in Pattern Recognition and De-noising / G. Chen.- Montreal, Concordia University, Canada, 1999. - 120p.
8. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер.- М.: Триумф, 2002. - 816 с.