МЕТОДЫ И СРЕДСТВА СТЕГАНОГРАФИИ ДЛЯ ЗАЩИТЫ ГРАФИЧЕСКИХ ОБРАЗОВ

В.Н. Матюшик
Кафедра программного обеспечения информационных технологий,
факультет компьютерных систем и сетей,
Белорусский государственный университет информатики и радиоэлектороники
Минск, Республика Беларусь
E-mail: vitaly851001@mail.ru

В данной работе проведен анализ методов скрытия информации в графических файлах, разработка программного средства для встраивания текстовой информации в графические файлы, с учетом недостатков рассмотренных программных аналогов, а также корректности и высокой эффективности функционирования.

Введение

Для обеспечения безопасного обмена информацией в настоящее время используется множество техник. Стеганография является лишь одной из них, но именно с ее помощью достигается возможность скрыть факт общения за счет сокрытия информации в мультимедийном контейнере, не вызывая подозрения. Методы стеганографии по типу модификаций контейнера делятся на следующие группы [1-2]:

- методы младшего значащего бита (Least Significant Bit, LSB) – наиболее простые методы, заменяющие наименее значимые биты в байтах контейнера на биты секретного сообщения,
- методы преобразований в частотной области (Transform Domain Techniques) -– внедрение секретной информации в частотной области сигнала (имеют большее значение в сравнении с методами наименее значимого бита), что позволяет говорить о более высокой надежности данных методов относительно методов группы LSB к различного рода атакам: компрессия, обрезке, некоторым видам обработки изображений,
- статистические методы -– методы, изменяющие статистические свойства контейнера, которые используются в процессе извлечения для доказательства факта внедрения,
- искажающие методы -– методы, основывающиеся на том факте, что получателю известен исходный контейнер и он может отследить модификации отправителя.

В данной работе были рассмотрены и реализованы 3 метода, относящиеся к первым двум группам: LSB, BPCS и ABCDE.

Описание методов

С точки зрения реализации наиболее простым методом является LSB, т.к. для внедрения достаточно лишь определить количество бит каждой цветовой составляющей, которая может быть использована в процессе сокрытия. Однако простота внедрения информации является в том числе причиной невысокой надежности данного метода: процесс моделирования может быть повторен нарушителем, что приведет к обнаружению скрытого сообщения.

BPCS и ABCDE [3-4] являются более надежными, однако ценой этому служит возросшая сложность метода, которая заключается в определении протокола, необходимого для обмена сообщениями.

Алгоритм сокрытия данных в случае BPCS состоит в последовательном выполнении следующих шагов:

- разбиение на битовые плоскости,
- разбиение на блоки,
- вычисление меры сложности каждого блока,
- вычисление меры сложности секретного сообщения,
- замена сложного блока изображения на блок сообщения.

Процедура извлечения секретных данных противоположна процедуре внедрения и состоит из следующих шагов:

- разбиение на битовые плоскости,
- разбиение на блоки,
- вычисление меры сложности каждого блока,
- извлечение карты внедрения (содержится в первом шумоподобном блоке),
- извлечение сообщения.

ABCDE (A Block Complexity Based Data Embedding) работает аналогично методу BPCS, но по-другому вычисляет меру сложности образа: BPCS просто считает число переходов между черным и белым значением в каждой строке и столбце для блока, полагая, что данное число может служить индикатором отсутствия структурированности. ABCDE же использует две метрики определения нерегулярной структуры блока, т. к. большое значение частоты, полученное для метода BPCS, может быть характерно для определенных шаблонов, которые, к примеру, могут быть получены при внесении водяного знака.

Первая из них ищет шаблоны по строкам и столбцам и, таким образом, поможет обна-

ружить и отбросить шахматный шаблон. Эту метрику называют метрикой «неравномерности длин серий». Вторая метрика позволяет искать границы образов, что в свою очередь позволяет избежать размытия границ, характерного для BPCS. Это метрика «зашумленности границы». Таким образом, данные метрики позволяют отсеять простые шаблоны, представленные на рис. 1.

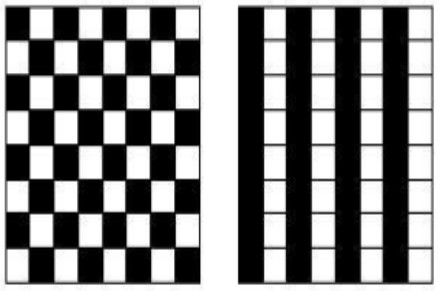

Рис. 1 – Простые шаблоны

Структура данных, внедряемых в контейнер при использовании метода ABCDE примет вид, представленный на рис. 2. В состав внедряемых данных входят:

- ключ M-последовательности,
- заголовочная секция,
- секции сообщения.

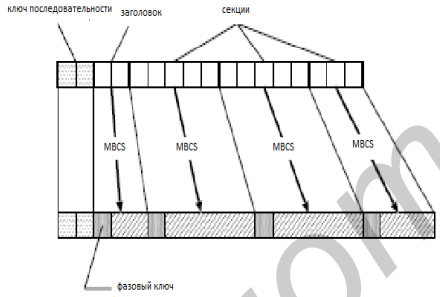

Рис. 2 – Структура внедряемых данных

Заключение

В процессе выполнения данной работы был проведён анализ предметной области и рассмотрены существующие аналоги разрабатываемого программного средства [4-5]. После завершения разработки было проведено тестирование на экспериментальных данных, которое показало высокое значение меры сложности для внедренных образов. На практике было показано отсутствие возможности определения измененных бит для классической реализации приведенных выше методов.

Кроме того, были учтены требования, поставленные в ходе анализа предметной области, и достигнуты следующие цели:

- корректная реализация внедрения и извлечения информации из графических файлов с помощью методов LSB и BPCS,
- высокая скорость обработки изображений за счет использования наиболее современных техник работы с ними.

1. Грибунин, В. Г., Оков, И. Н., Туринцев, И. В. Компьютерная стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // «Солон-Пресс» – 2002. -– 272с.
2. Конанович, Г. Ф., Пузыренко, А. Ю. Компьютерная стеганография. Теория и практика /Г. Ф. Конанович, А. Ю. Пузыренко //«МК-Пресс» – 2006. -– 288с.
3. Cox, J. I., Miller, L. M. Digital Watermarking and Steganography / J. I. Cox, L. M. Miller // Burlington – 2008. -– 542p.
4. Аграновский, А. В., Балакин, А. В. Стеганография, цифровые водяные знаки в стегоанализе /А. В. Аграновский,А. В. Балакин //«Вузовская книга» – 2009. - – 202с.
5. QuickCrypto Software [Электронный ресурс]. -– Режим доступа: http://www.quickcrypto.com/free-steganography-software.html.
6. Chameleon Image Steganography [Электронный ресурс]. -– Режим доступа: http://chameleon-stego.tripod.com/home.html