ПРОГРАММНЫЙ МОДУЛЬ ВНЕДРЕНИЯ ИНФОРМАЦИИ В РАСТРОВОЕ ИЗОБРАЖЕНИЕ

Шрубиков А.Г.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Зельманский О.Б. – канд. техн. наук

Разработано программное средство на основе алгоритма LSB. Предложены способы улучшения характеристики скрытности данных, в том числе способ оптимизации используемого пространства в медиаконтейнере.

Существует множество различных методов и инструментов для защиты информации. Одним из таковых является стеганография. Стеганография – это способ сокрытия полезных данных в контейнере таким образом, чтобы неавторизованный пользователь не имел возможности обнаружить факт наличия сообщения. Под контейнером может подразумеваться текст, изображение, аудиофайлы, видеофайлы и даже неиспользуемые биты заголовков полей TCP/IP протокола [1]. Однако теме данной работы соответствует стеганография в растровых изображениях.

Существует несколько типов методов сокрытия:

– Пространственные методы. Изменения вносятся в значения пикселей таким образом, чтобы быть незаметными для человеческого глаза.

– Методы преобразования в частотной области. Более сложные методы, имеющие большую, чем в вышеописанном методе вычислительную сложность. Заключается в сокрытии информации в частотной области изображения, что, в свою очередь, повышает надёжность к различного рода атакам.

– и др.

В данной работе, был рассмотрен метод LSB из первой группы методов.

LSB (Least Significant Bit – наименее значащий бит) метод заключается в изменении младших значащих битов пикселей с целью кодирования в них секретного сообщения. Доказано, что изменение младших битов в каждом пикселе не влияет на восприятие изображения человеческим глазом [2].

Таким образом базовый алгоритм сокрытия информации может выглядеть следующим образом:

1. Преобразование секретного сообщения в массив битов.
2. Вычисление длины данного массива.
3. Преобразование длины массива в массив битов.
4. Кодирование битовой длины информационного сообщения в младших битах первых пикселей изображения.
5. Кодирование информационного сообщения в последующих битах.

Извлечение скрытой информации осуществляется обратным образом с той особенностью, что в начале требуется извлечь длину сообщения в младших битах каждого пикселя, после чего считать соответствующее количество битов.

Усложнение алгоритма может быть произведено с целью увеличения сложности раскрытия факта наличия внедрённой информации. Положительный результат может быть достигнут следующими способами:

1. Гораздо более высокую скрытность можно достичь, используя в качестве контейнера зашумлённые изображения (фотографии, отсканированные изображения) [2]. Это происходит по причине низкой закономерности используемых цветов.

2. Уменьшить вероятность несанкционированного обнаружения информации возможно благодаря непоследовательному использованию пикселей, к примеру использование каждого второго или третьего пикселя. Для оптимизации данного процесса предлагается внедрение в вышеописанный алгоритм условий, которые проверяют частное размера скрываемого сообщения и размера используемого контейнера. В результате, это значение используется для более оптимального распределения информационных битов по контейнеру. К примеру, если размер информационного сообщения меньше размера контейнера в 24 раза это означает, что для сокрытия должен использоваться младший бит составляющей синего цвета каждого пикселя. В случае если сообщение меньше контейнера в 48 либо меньше раз, возможно использование данного бита через один пиксель и т.д.

Следует упомянуть, что лучшим форматом для стеганографии данного типа является PNG, так как он использует сжатие без потерь, а также широко распространён, что позволяет избежать лишнего внимания.

Список использованных источников:

1. Kaur, H., Rani, J. A Survey on different techniques of steganography / H. Kaur, H. Rani // MATEC Web of Conferences. – 2016. – №57 – 02003.

2. Конанович, Г.Ф., Пузыренко, А.Ю. Компьютерная стеганография. Теория и практика /Г.Ф. Конанович, А.Ю. Пузыренко // «МК-Пресс» – 2006. – 288с.