СКРЫТОЕ ВНЕДРЕНИЕ ИНФОРМАЦИИ В РАСТРОВОЕ ИЗОБРАЖЕНИЕ

А.Г. Шрубиков, О.Б. Зельманский

Для скрытой передачи информации применяется множество различных методов и инструментов. Одним из них является стеганография. Под стеганографией понимают скрытие полезных данных в контейнере таким образом, чтобы неавторизованный пользователь не имел возможности обнаружить факт наличия сообщения. В качестве контейнера может использоваться текст, изображение, аудиофайлы, видеофайлы, а также неиспользуемые биты заголовков полей TCP/IP протокола [1]. К наиболее популярным методам скрытия можно отнести пространственные методы, при использовании которых изменения вносятся в значения пикселей таким образом, чтобы быть незаметными для человеческого глаза, и методы преобразования в частотной области. В настоящей работе рассмотрен метод LSB из первой группы. LSB (Least Significant Bit – наименее значащий бит) метод заключается в изменении младших значащих битов пикселей с целью кодирования в них скрываемого сообщения. Согласно [2] изменение младших битов в каждом пикселе не влияет на восприятие изображения человеческим глазом. Таким образом, алгоритм скрытия информации может выглядеть следующим образом: преобразование скрываемого

сообщения в двоичный код, вычисление его длины, преобразование длины массива в двоичный код, кодирование длины скрываемого сообщения в младших битах первых пикселей изображения, кодирование скрываемого сообщения в последующих битах.

Следует отметить, что более высокую скрытность можно достичь, используя в качестве контейнера зашумленные изображения (фотографии, отсканированные изображения) [2]. Это происходит по причине низкой закономерности используемых цветов. Уменьшить вероятность несанкционированного обнаружения информации возможно благодаря непоследовательному использованию пикселей, например, 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 дальнейшем это значение используется для более оптимального распределения информационных битов по контейнеру. Например, если размер информационного сообщения меньше размера контейнера в 24 раза это означает, что для скрытия должен использоваться младший бит составляющей синего цвета каждого пикселя. В случае если сообщение меньше контейнера в 48 раз, возможно использование данного бита через один пиксель и т.д. Наиболее удобным для стеганографии форматом является PNG, так как он использует сжатие без потерь, а также является широко распространенным.

Литература

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

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