

УДК 519.683.8.004.424

Рекиш А.О., Шаталова В.В., Шахно Н.В., Алексеев В.Ф.
**ИССЛЕДОВАНИЕ МЕТОДА ЗАМЕНЫ МЛАДШИХ БИТ
ПРИМЕНЯЕМОГО В КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ**
*УО «Белорусский Государственный Университет Информатики и
Радиоэлектроники», Минск*

Развитие вычислительной техники и большого количества каналов передачи информации привело к появлению новых методов стеганографии, в основе которых лежат особенности представления информации в файлах, вычислительных сетях и т. п. В данной статье рассматривается один из методов компьютерной стеганографии, называемый «Метод замены младших бит».

Стеганография – метод организации связи между отправителем и получателем, при котором скрывается само наличие связи. Если целью криптографии является блокировка несанкционированного доступа к информации путем шифрования сообщения, то цель стеганографии состоит в скрытии самого факта существования сообщения.

Компьютерная стеганография базируется на двух основных принципах:

1. Первый принцип заключается в некотором видоизменении файлов, содержащих оцифрованное изображение или звук, без потери их функциональности.

2. Второй принцип заключается в неспособности органов чувств человека распознать незначительные изменения в цвете изображения и качестве звука [1].

Одним из наиболее распространенных методов стеганографии является метод замены младших бит. Суть метода состоит в замене нескольких бит в байтах данных.

При оцифровке изображения или звука всегда существует погрешность дискретизации, которая обычно находится на уровне младшего значащего бита. Это значит, что фактически неизвестно, что будет стоять в младшем значащем разряде цифрового изображения или звука. Поэтому при замене только одного младшего бита говорить о каком-либо искажении не имеет смысла. Однако при замене только одного младшего бита такой метод имеет достаточно малую емкость от объема файла контейнера, поэтому на практике используют замену более одного бита.

Рассмотрим использование данного метода на примере формата BMP (BitMAP), хранящего изображение в естественных цветах и являющийся основным форматом растровой графики для системы Windows. В файлах BMP информация о цвете каждого пиксела задается тремя байтами. Каждый байт содержит одну из трех составляющих цвета RGB: красную (Red), зеленую (Green), синюю (Blue). Интенсивность каждой составляющей лежит в пределе от 0 до 255. Варьируя интенсивностью каждой составляющей можно добиться получения различных оттенков. Рассмотрим пример скрытия девяти бит данных, например, 101101101 в 24-разрядном изображении. Для этого необходимо изменить максимум 3 пиксела (9 байт). Пусть 3 пиксела 24 разрядного изображения представлены в следующем виде рисунок 1:

R	G	B	
(1 байт)	(1 байт)	(1 байт)	
10010101	00001101	11001001	1 пиксел (3 байта)
10010110	00001111	11001010	1 пиксел (3 байта)
10011111	00010000	11001011	1 пиксел (3 байта)

Рисунок 1 – Структурная схема пикселей 24 разрядного изображения

Меняя младший разряд слева направо и сверху вниз, получаем следующий результат рисунок 2 (измененные биты выделены жирным шрифтом):

R	G	B	
(1 байт)	(1 байт)	(1 байт)	
10010101	000011 00	11001001	1 пиксел (3 байта)
10010111	000011 10	11001011	1 пиксел (3 байта)
10011111	00010000	11001011	1 пиксел (3 байта)

Рисунок 2 – Результат замены младших разрядов

Таким образом, для скрытия девяти бит данных потребовалось заменить всего четыре бита только в 2 пикселях исходного изображения, что составляет менее 50 % младших разрядов, используемых для этой цели и как результат, изменения не будут заметны человеческому глазу. Данный метод достаточно прост, обладает большой емкостью и высокой степенью защиты от стегоанализа [2].

Список использованных источников

1. О. В. Генне, “Основные положения стеганографии. //Конфидент.2000. №3. С. 20-24 Журнал “Защита информации. Конфидент”, №3, 2000.
2. Кустов В.Н., Федчук А.А Методы встраивания скрытых сообщений //Конфидент. 2000. №3. С. 26-33.

Rekish A.O., Shatalova V.V., Shahno N.V., Alekseev V.F.

STUDY OF THE METHOD OF REPLACING LOWER BITS APPLICABLE IN COMPUTER STEGANOGRAPHY

Belarusian State University Informatics and Radioelectronics, Minsk

Summary

This article explores one of the methods of computer steganography, called "Method of replacing the lower bits".