А. Н. Боброва

ЦИФРОВАЯ СТЕГАНОГРАФИЯ

Рассматривается наиболее распространённый метод встраивания скрытых данных в цифровые изображения. На основе выявленных достоинств и недостатков данного метода делается вывод о дальнейших направлениях развития цифровой стеганографии.

Введение

На сегодняшний день цифровая стеганография находится на начальной стадии своего развития. Однако, актуализация проблем защиты авторских прав в цифровых глобальных сетях и запрет на использование криптографических средств в ряде стран способствуют формированию теоретической базы, тщательному анализу уже существующих методов, а, следовательно, и разработке новых методов встраивания данных.

Наиболее распространённым стеганографическим методом [2] является метод LSB (Least Significant Bit – LSB). Исследование данного метода с целью выявления достоинств и существенных недостатков должно послужить толчком к развитию современной цифровой стеганографии.

I. LSB-метод

Цифровые изображения представляют собой матрицу пикселей [1]. Пиксель – это единичный элемент изображения, имеющий фиксированную разрядность двоичного представления. Младшие биты в байтах цифрового изображения отвечают за кодирование цвета. Как правило, органы восприятия человека не способны заметить искажения этих битов. Именно поэтому младшие биты могут быть использованы для внедрения информации в цифровое изображение, или контейнер. Однако необходимо помнить, что объём внедряемого объекта не должен превосходить объём самого цифрового изображения. Для полутонового изображения объём внедряемых данных должен быть не более $\frac{1}{8}$ объёма контейнера. Например, если использовать только младший значащий бит каждого байта изображения размером 512×512 пикселей, то в этом изображении можно скрыть до $\frac{512^2}{8} = 32786$ байтов или 32 килобайтов данных.

Достоинствами данного метода являются неизменность размера контейнера при внедрении данных, большой объём внедряемых данных, простота его применения.

Главным его недостатком является неспособность скрыть внедряемую информацию должным образом, поскольку при побитовом просмотре цифрового изображения со скрытой инфомацией, отчётливо видна модификация младших битов изображения.

На рисунке 1 приведено сравнение изображений при побитовом просмотре без внедрения информации и с внедрением 2 КБ случайных данных слева и справа соответственно:

Рис. 1 – Различие изображений без внедрённых данных и с ними при побитовом просмотре

Для преодоления данного недостатка был разработан модифицированный метод LSB [2].

II. Модифицированный метод LSB

Модифицированный метод LSB заключается во встраивании цифровых объектов не во все пиксели изображения, а лишь в некоторые из них, определяемые по псевдослучайному закону в соответствии с ключом, известному только законному пользователю. Эта особенность позволяет справиться с главным недостатком обычного метода LSB.

Выводы

Исследование метода LSB позволило выявить его существенный недостаток. Преодолеть данный недостаток позволила модифицированная версия данного метода. Однако, практически во всех ныне применяемых методах цифровой стеганографии наблюдаются такие недостатки, как неустойчивость к фильтрации, конвертации цветов, вставке различных фрагментов в цифровое изображение, что требует дальнейших исследований и переработок.

1. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Осков, И. В. Туринцев. – Минск: СОЛОН-Пресс, 2002. – 261 с.
2. Генне, О. В. Основные положения стеганографии / О. В. Генне // Защита информации. Конфидент. – 2000. – № 3. – С. 20 – 25

Боброва Анна Николаевна, студентка 4 курса факультета информационных технологий и управления Белорусского государственного университета информатики и радиоэлектроники, icenine@bk.ru.

Научный руководитель: Герман Олег Витольдович, доцент кафедры информационных технологий автоматизированных систем Белорусского государственного университета, кандидат технических наук, доцент, ovgerman@tut.by.