**АНАЛИЗ СТЕГАНОГРАФИЧЕСКОГО СОКРЫТИЯ ИНФОРМАЦИИ МЕТОДОМ ЗАМЕНЫ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА НА ОСНОВЕ РАЗРАБОТАННОЙ РЕАЛИЗАЦИИ**

Автор: Назаренко Ю. Л., студент ДГТУ

Аннотация. Статья посвящена анализу метода сокрытия информации «наименьший значащий бит» на основе разработанной программной реализации. При проведении анализа были рассмотрены такие параметры алгоритма, как соотношение размера скрываемой информации к размеру стеганоконтейнера, время работы алгоритма и надёжность при атаке на данный метод, а также сделаны выводы по каждому из этих пунктов.

1. **Введение**

Цель данной статьи – проанализировать основные характеристики метода замены наименьшего значащего бита (LSB), основываясь на программной реализации, реализованной на языке С#. Будут проанализированы такие характеристики, как соотношение размера скрытой информации и размера контейнера, время работы программы для разных размеров сообщения и контейнера, а также устойчивость к стеганографическим атакам. Для проведения анализов был проведет ряд опытов, в которых в качестве контейнера были выбраны изображения в формате BMP различных размеров, а в качестве скрываемой информации – текст, представленный в двоичном формате.

1. **О методе LSB.**

Суть метода з**амена** **наименее значащего бита (**Least Significant Bits**- LSB)** заключается в сокрытии информации путем изменения последних битов изображения, кодирующих цвет на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.



Рис. 1 – принцип работы метода.

Пусть, имеется 24-х битное изображение в градациях серого. Пиксел кодируется 3 байтами, и в них расположены значения каналов RGB. Изменяя наименее значащий бит, мы меняем значение байта на единицу. Такие градации, мало того, что незаметны для человека, могут вообще не отобразиться при использовании низкокачественных устройств вывода.

1. **Анализ метода.**
	1. **Соотношение размера скрываемых данных к размеру контейнера.**

Соотношение размера скрываемых данных к размеру контейнера – это отношение объёма информации, который можно скрыть в стеганоконтенере, к размеру самого стеганоконтейнера. Это величина иначе называется пропускным каналом. В данном методе это соотношение зависит от того, сколько бит будет выделено под сокрытие информации. Обычно для этого выделяют 1 бит из синей компоненты цвета одного пикселя. Учитывая, что один пиксель в формате BMP кодируется тремя байтами, получается соотношение 1/24. Однако заголовок фала при этом не должен быть поврежден, иначе изображение будет повреждено и не откроется. Однако можно скрывать и большее количество бит, тогда ёмкость контейнера повысится. При этом стоит помнить, что чем больше бит используется под сокрытие информации, тем более заметен будет факт сокрытия. Для эксперимента был выбран файл размером 100 кб. Результаты экспериментов соотношения показаны на графике 1.

График 1.

Эти результаты позволили составить формулу расчёта объёма скрываемой информации, в килобайтах:

$V=0,25\*(M-54)/(25-x)$,

где V – максимальный объем скрываемой информации, M – размер скрываемого сообщения, x – количество бит для сокрытия информации, 54 – количество байт заголовка файла. Например, при выборе 1 бита для сокрытия информации соотношение будет составлять 0,04167.

 **Вывод.** Данный алгоритм имеет одно из высочайших показателей ёмкости контейнера, поскольку для прочих методов стеганографии обычным является соотношение порядка 0,001.

* 1. **Время работы алгоритма**

Одним из важнейших показателей любого алгоритма является время его выполнения. Для определения быстродействия алгоритма программно подсчитывается время его выполнения, при этом на вход алгоритму даются разные параметры для наиболее полного анализа. В рамках анализа данной программы входным параметром был установлен объём скрываемого сообщения. Размер стеганоконтейнера при этом был выбран 1 мегабайт. Эксперименты проводились на ПК с процессором i5-4210H с тактовой частотой 2.9ггц. Результаты анализа показаны на графике 2.

График 2.

**Вывод.** Время работы алгоритма напрямую зависит от размера скрываемого сообщения, при этом наблюдается экспоненциальная зависимость. При этом даже при сокрытии большого объёма информации порядка 35 кб, что в текстовом виде будет составлять 35 тыс. символов, время работы алгоритма составляет менее 0,02 сек.

* 1. **Надёжность метода.**

Для стеганоанализа сообщения со скрытой информацией была использована программа EnhancedLSB.  Она устраняет все 7 старших битов для каждого пикселя, кроме последнего наименее значащего (LSB). Таким образом, все байты изображения принимают значения 0 или 1. Это даст в итоговом изображении  яркие цвета, и младшие разряды исходного изображения станут достаточно хорошо заметны  для визуальной проверки.

В таблице приведены результаты работы программы.

|  |  |  |  |
| --- | --- | --- | --- |
| **Что скрыто в файле** | **Каким образом выглядит** | **Как выглядит после обработки программой** | **Комментарий** |
| Ничего | стеганография | стеганография | Исходное изображение без скрытой информации. |
| 1 кб случайных данных | стеганография | стеганография | Случайные данные, скрытые в младших разрядах, становится очень заметными. Первая строка пикселов в файле BMP является последней строки изображения на экране, это особенность формата BMP.  |
| 5 кб случайных данных | стеганография | стеганография | Еще более случайные скрытые данные. |
| Поэма "If" Редьярда Киплинга, 1,5 Kb ASCII текст | стеганография | стеганография | Теперь скрытые данные не являются случайными, это простой текст, и видно появляются как артефакты в сгенерированном изображении. Они похожи на вертикальные линии, что связано с особенностью ASCII кодировки. В большинство писем (особенно обычных, написанных в нижнем регистре, в котором пишется подавляющее большинство обычного текста) есть много общих битов (в 3 из 8 в случаев используется нижний регистр).  |

**Вывод**. Факт сокрытия информации с помощью этого метода информация, хоть и не заметен глазу, без труда обнаруживается специальным ПО. Это плата за быструю работу алгоритма и очень высокое соотношение объёма скрываемых данных к размеру контейнера. Из этого можно сделать вывод, что данный метод можно применять, если вероятность перехвата стегоноконтейнера с последующим стеганоанализом мала.