ПРИМЕНЕНИЕ СКРЕМБЛИРОВАНИЯ ДЛЯ УСЛОЖНЕНИЯ ОБНАРУЖЕНИЯ СКРЫТОЙ ИНФОРМАЦИИ, ЗАПИСАННОЙ МЕТОДОМ LSB

Фримучков А. Н.

Фримучков Андрей Николаевич / Frimuchkov Andrey Nikolaevich — студент, факультет кибернетики, Московский технологический университет, г. Москва

Аннотация: *в статье анализируется возможность применения скремблирования для увеличения стойкости к обнаружению метода стеганографии - LSB (последний значащий бит). Сам метод LSB является достаточно простым и легко обнаруживается, поэтому область его применения на данный момент очень невелика, однако, несмотря на это, при использовании скремблирования обнаружить присутствие информации в контейнере статистическими методами становится почти невозможно, что говорит о существенно недооценённом потенциале метода LSB.*

Ключевые слова: *информационная безопасность, стеганография.*

Введение

Стеганография (пер. с греч, «тайнопись») — наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. Здесь важно отметить, что в отличие от криптографии, которая защищает информацию в передаваемом сообщении, стеганография скрывает само существование сообщения [1].

В конце 90-х годов было выделено 3 основных направления стеганографии:

- Классическая стеганография
- Компьютерная стеганография
- Цифровая стеганография

Безусловно, стоит отметить, что в последнее время было зарегистрировано больше число патентов в этой сфере (есть даже патент на «Продовольственную стеганографию»), однако, перечисленные 3 направления до сих пор остаются основными.

В рамках этой статьи мы рассматриваем возможность скрытой передачи цифровой информации, поэтому нам будет интересен 3-ее направление, а именно «Цифровая стеганография»

Цифровая стеганография — направление стеганографии, основанное на введении дополнительной информации в цифровые объекты, вызывая незначительные искажения этих объектов. Конечно же, в виде объектов могу выступать совершенно любые объекты, однако, чаще всего это — мультимедиа объекты и допустимые искажения основаны на пороге чувствительности органов восприятия человека.

Все алгоритмы внедрения скрытой информации делятся на несколько подгрупп:

- Работа напрямую с самим сигналом
- Наложение скрываемых данных поверх оригинала(часто используется при встраивании водяных знаков)
- Использование особенностей контейнера, например, запись в метаданные

Одним из наиболее простых в реализации методов является метод LSB.

Использование метода LSB

LSB(Least Significant Bit, наименьший значащий бит) — суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека [2].

Для примера возьмем изображение размером 10 пикселей на 10 пикселей и заполним его белым цветом. Изображение использует палитру RGB, в этой палитре цвет получается в результате смешения красного, зелёного и синего цветов. Для белого цвета значения будут следующими: R=255, G=255, B=255.

В данном случае мы можем побитово записывать имеющуюся информацию в последний бит красного, синего, зелёного канала, можно даже брать два последних бита. Однако стоит учесть, что чем больше информации будет записано в один пиксель, тем сильнее будет искажено исходное изображение.

Итак, как уже было сказано, у нас имеется изображение 10x10 пикселей, используем разработанную программу для метода LSB и запишем в это изображение тестовую строку(запись производится в последний бит красного канала). На рисунке 1 в левой части представлен файл с записанной строкой, а на в правой выделены изменённые пиксели.

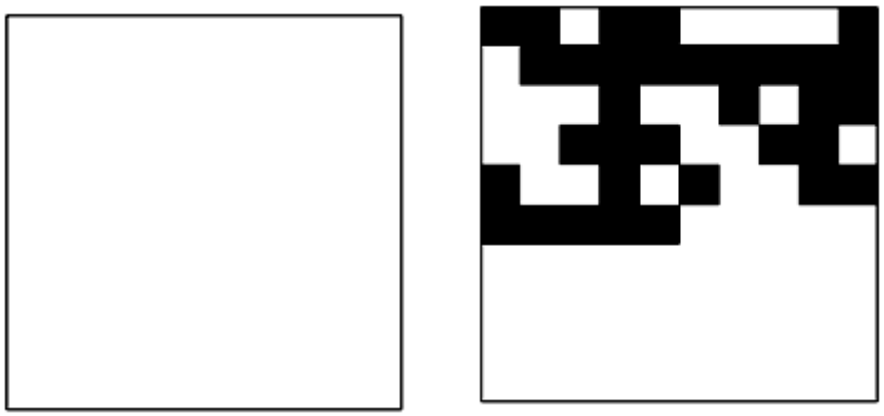

Рис. 1. Подсветка изменённых пикселей в изображении

Как можно увидеть, при отсутствии шумов в исходном файле, обнаружение факта передачи информации не составляет труда. В изображении на рисунке 2 обнаружить информацию так просто уже не получится, потому что файл представляет из себя случайный набор пикселей(т.е. шум).

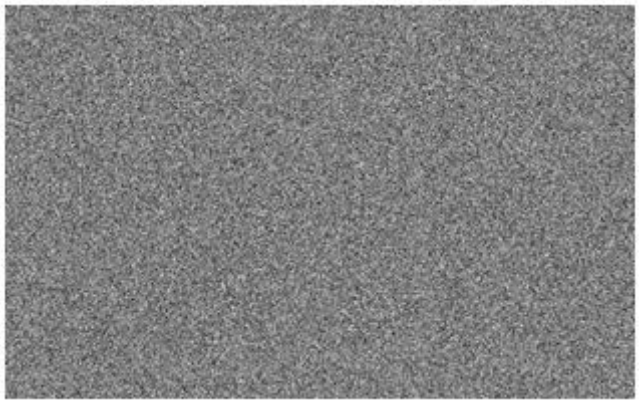

Рис. 2. Пример зашумлённого изображения

Казалось бы, что присутствие шумов в файле будет является гарантией сокрытия информации, но это не так.

Метод LSB, несмотря на свою простоту, имеет один существенный недостаток: информация, скрытая этим методом, легко обнаруживается.

Задача обнаружения обычно решается методами статистического анализа. Для примера, если необходимо спрятать некий фрагмент текстового сообщения, это сообщение будет содержать только символьную информацию: 52 знака латиницы, 66 знаков кириллицы, знаки препинания и некоторые служебные символы. Если сравнить статистические характеристики такого сообщения и статистические характеристики младших битов красного спектра, то будут видны существенные отличия. Это обусловлено тем, что последовательность последних битов красного спектра представляет из себя случайную двоичную последовательность, а наше сообщение такой последовательностью не является.

Модификация алгоритма

Возникает вопрос: как добиться того, чтобы спектральная характеристика нашей последовательности битов и последовательности последних битов красного канала (если записываем в красный канал) была одинакова? Для решения этой задачи нам понадобится решение, разработанное для сферы телекоммуникаций — скремблер.

Скремблер (англ. scramble — шифровать, перемешивать) — программное или аппаратное устройство (алгоритм), выполняющее скремблирование — обратимое преобразование цифрового потока без изменения скорости передачи с целью получения свойств случайной последовательности[3] .

Применим скремблирование на практике и будем записывать слово «Стеганография», в двоичном виде оно представляет из себя последовательность: «11010000101000011101000110000010110100000101110101110100000101100111101000010111000011010000101111011010000101100111101000110000000011010000101100001101000110000100110100000101110001101000110000111». Проверку будем выполнять по 2-м первым постулатам Голомба:

1. Количество «1» в каждом периоде должно отличаться от количества «0» не более чем на единицу.
2. В каждом периоде половина серий (отрезков из одинаковых символов) должна иметь длину один, одна четверть должна иметь длину два, одна восьмая должна иметь длину три и т.д. Более того, для каждой из этих длин должно быть одинаковое количество серий из «1» и «0».

Здесь, вероятно, стоит немного пояснить эти два постулата. Первый постулат понятен без объяснений: количество нулей и единиц должно быть равно с точностью до единицы. Второй постулат говорит о том, что в нашей последовательности больше всех должно быть подпоследовательностей вида 010 и 101, в два раза

меньше 0110 и 1001 и т.д.

До скремблирования в последовательности 115 нулей и 93 единицы, распределение по подпоследовательностям представлено на схеме 1.

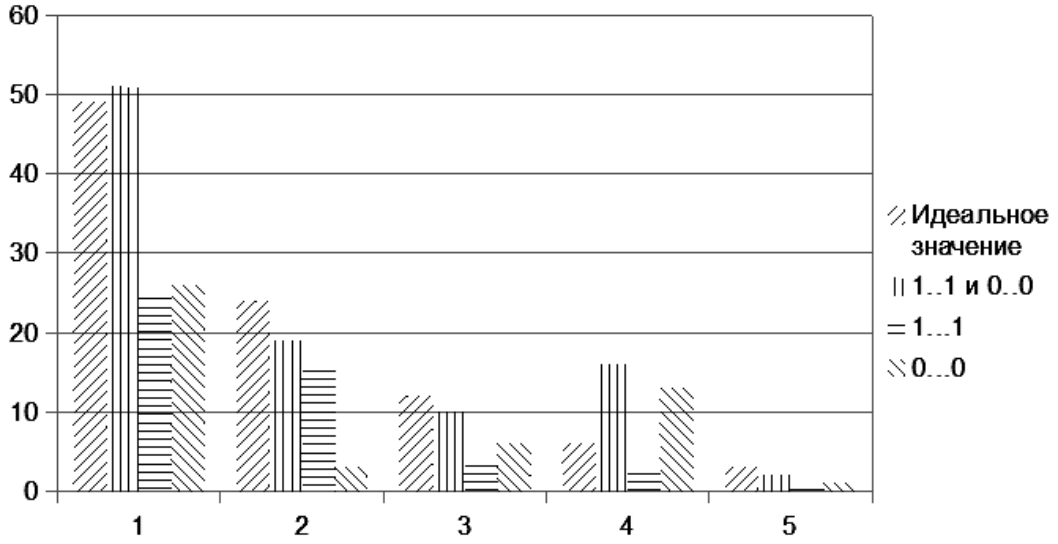

Рис. 3. Схема 1. Гистограмма до скремблирования

Из схемы 1 можно сделать вывод, что последовательность не является псевдослучайной. Проскремблируем её. Результат скремблирования:
«11011000010111111111000100101100111001101001010011111111101101000101001000011011110001100011100011000010101010100101010110010001111001000001010000000101000010000100110011011101001100100011100100100101011101111»

После скремблирования в последовательности 107 нулей и 101 единица, распределение по подпоследовательностям представлено на схеме 2.

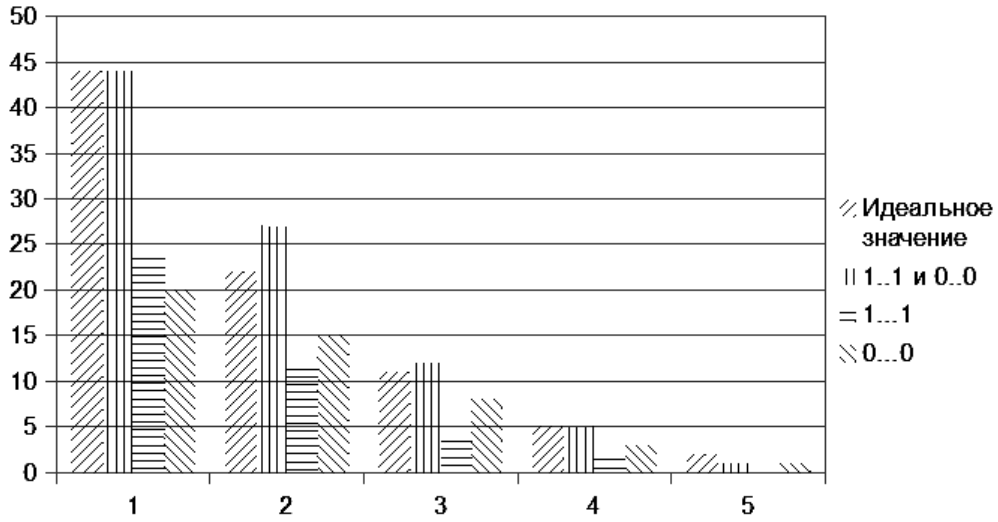

Рис. 4. Схема 2. Гистограмма после скремблирования

Конечно же, результат не идеален, но он гораздо лучше приближен к идеальному, чем полученный ранее.

Вывод

Из-за специфики метода LSB, информация очень неустойчива к внешнему воздействию и подвержен шумам в канале. Однако, в настоящее время мы имеем возможность передавать информацию без потерь, сетевые карты званого запрашивают ошибочные пакеты, каналы связи экранированы и т.д., поэтому этот недостаток алгоритма не является толь существенным. А для сокрытия обнаружения информации можно успешно применять скремблирование, поэтому я считаю, что возможности алгоритма ещё не исчерпаны и при помощи этого него можно не только передавать скрытую информацию, но ещё и очень удачно скрывать факт её присутствия.

Литература

1. *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с. Ил.

2. *Генне О. В*. Основные положения стеганографии // Защита информации. Конфидент, 2000. № 3.
3. *Кунегин С. В.* Системы передачи информации. Курс лекций. М., в/ч 33965, 1997. 317 с., с ил.