УДК 004.056.5

Стеганографический анализ файла изображения на предмет обнаружения сокрытой информации

Строкин Д.И., Пономарев И.В.
Алтайский государственный университет, г. Барнаул
mega.strokin@mail.ru, igorpon@mail.ru

Аннотация

В статье рассматриваются метод обеспечения конфиденциальности данных средствами Цифровой Стеганографии, использующий в качестве файлов-контейнеров изображения формата GIF, описывается и производится возможная атака на данный метод. Как результат, предлагаются возможные средства повышения стойкости системы против проводимой атаки.

Ключевые слова: контейнер, сообщение, палитра, индекс цвета, наименее значащий бит.

Данный метод подробно описан в работах [1, 2]. Здесь же приведем только основные сведения и алгоритм.

Определение. Контейнером (носителем) называют несекретные данные, которые используют для сокрытия сообщений. Пустой контейнер – контейнер без встроенного сообщения; заполненный контейнер или стего–контейнер, содержащий встроенную информацию [1]. В качестве носителей информации были выбраны изображения формата .GIF, использующие LZW-сжатие без потерь. Отличительными чертами данного формата являются [3]:

1) Использование блочной структуры данных;

2) Использование палитры цветов - фиксированного набора (диапазона) цветов и оттенков, имеющего физическую или цифровую реализацию в том или ином виде.

Использование палитры подразумевает, что каждая точка изображения содержит лишь номер цвета из палитры, а не информацию о ее цвете в цветовом пространстве.

В основе алгоритма лежит метод замены Наименее Значащего Бита (Least Significant Bit), основной принцип которого заключается в том, что передаваемая информация встраивается в значения младших битов изображения. Такие биты несут в себе меньше всего информации, а, следовательно, их модификация не восприимчива человеческим зрением [1, 4].

Однако заметим, что пиксели GIF-изображений – это поток индексов из цветовой палитры. Это значит, что прямая модификация пикселей изображения непригодная для нашего случая. Наилучшем решением в подобной ситуации будет использование «подобных» элементов палитры [1]. Под подобными, в данном случае, понимаются пары элементов, цветовая интенсивность которых отличается на незначительное число d.

Алгоритм встраивания сообщения.

Шаг 1. Сортировка палитры цветов по возрастанию веса W, где: $W = R \cdot 65536 + G \cdot 256 + B$.

Шаг 2. Поиск пар элементов в отсортированной палитре, для которых разность весов W меньше заданной пороговой величины d. Обозначим одну такую пару за (j_i, j_k), где i и k – это индексы элементов в неотсортированной палитре, причем в отсортированной таблице j_i от j_k отличается на 1.

Шаг 3. Сокрытие сообщения. Последовательно просматриваются все точки изображения, по значению точки k определяется соответствующий номер j_k. Если элемент отсортированной палитры j_k пригоден для сокрытия, то его Наименее Значащий Бит заменяется на очередной бит сообщения. Затем по получившемуся номеру $j_{k'}$ определяется связанный с ним элемент исходной таблицы k', который и присваивается текущей точке.

Шаг 4. Извлечение сообщения происходит аналогичным способом. Для текущей точки k ищется номер j_k в отсортированной по весу W палитре цветов и если:

• Младший бит индекса j_k равен нулю, смотрим, удовлетворяет ли пара (j_k, j_{k+1}) условию: $W_{j_{k+1}} - W_{j_k} < d$. Если удовлетворяет, значит, из индекса j_k извлекаем младший бит и записываем его в сообщение.

• Младший бит индекса j_k равен единице, смотрим, удовлетворяет ли пара (j_{k-1}, j_k) условию: $W_{j_k} - W_{j_{k-1}} < d$. Если удовлетворяет, значит, из индекса j_k извлекаем младший бит и записываем его в сообщение.

Алгоритм обнаружения факта скрытия сообщения.

Выявление факта сокрытия информации внутри файла-контейнера – отдельный вид стеганографических атак, часто основывающихся на различных статистических закономерностях контейнеров. Модификацию одной из таких атак мы и рассмотрим.

Гистограммный метод или метод, основанный на критерии χ^2 [1,4,5] предполагает, что вероятность одновременного появления соседних (то есть отличных на наименее значащий бит) цветов в незаполненном контейнере крайне мала. А при последовательном встраивании равномерного сообщения, пиксели изображения, напротив, приобретают равномерное распределение.

Поэтому степень различия между вероятностными распределениями элементов естественных контейнеров и полученных из них стего может быть использована для оценки вероятности существования стегоканала.

Шаг 1. Сортировка палитры цветов по возрастанию веса W, где: $W = R \cdot 65536 + G \cdot 256 + B$.

Шаг 2. Разбиение изображение на отдельные блоки. Гораздо удобнее оценивать вероятность внедрения секретной информации в отдельный блок, чем во все изображение целиком.

Шаг 3. Для текущего блока подсчитывается, сколько раз n_i^* её элемент x_i принял рассматриваемые значения, где всего k элементов. Иными словами, мы строим эмпирическую гистограмму по количеству вхождений для каждого элемента палитры.

Шаг 4. Далее происходит построение теоретической гистограммы на основе эмпирической, путём нахождения среднего арифметического количества пикселей элементов с соседними номерами:

$$n_0 = n_1 = \frac{n_0^* + n_1^*}{2}$$

Шаг 5. Величина χ^2 для сравниваемых распределений последовательности и ожидаемого распределения стего равна:

$$\chi^2 = \sum_{i=1}^{v} \frac{(n_i - n_i^*)^2}{n_i^*}$$

Шаг 6. Таким образом, вероятность p того, что два распределения одинаковы [4], определяется:

$$p = 1 - \frac{1}{2^{\frac{k-1}{2}}\Gamma\left(\frac{k-1}{2}\right)} \int_0^{\chi^2_{k-1}} e^{\frac{x}{2}} x^{\frac{k-1}{2}}\, dx,$$

где Γ – гамма-функция Эйлера; k – количество цветов в палитре.

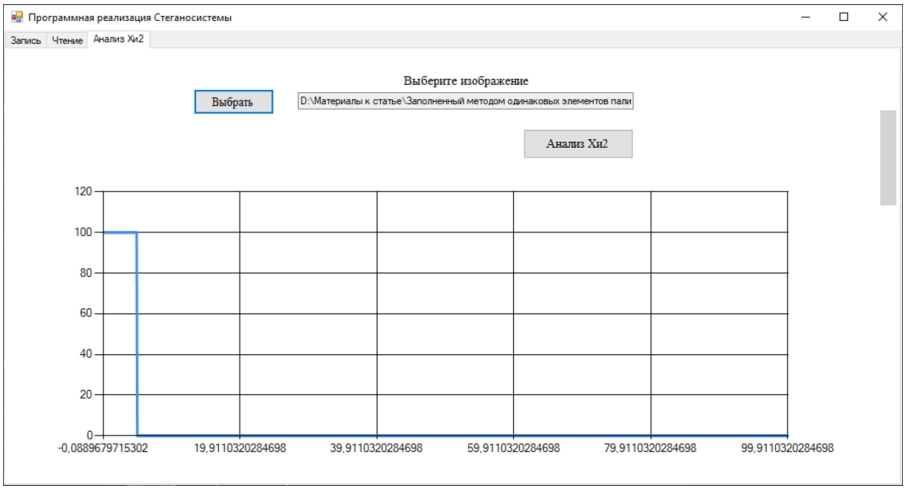

Рисунок 1. Результат анализа файла-контейнера (заполненного на 5%) на наличие скрытого сообщения

Предполагается, что снижение вероятности обнаружения стегосообщения атаками, основанными на критерии χ^2, можно добиться использованием псевдослучайных интервалов при скрытии очередного бита сообщения. Иными словами, лучше всего встраивать сообщение не последовательно, а рассеяно по всему контейнеру.

Для этого необходимо ввести в систему генератор псевдослучайных чисел и настроить его на генерацию случайных чисел по заданному сиду (иными словами ключу, паролю). Возвращаемые значения ГПСЧ – это отступы между пикселями изображения с секретной информацией.

Таким образом, при скрытии сообщения программа будет генерировать ключ, без которого дальнейшее извлечение информации из заполненного файла-контейнера не представляется возможным. При этом атака гистограммным методом будет безуспешной, так как не будет выполняться основная гипотеза.

Список литературы

1. Аргановский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. — М. : Вузовская книга, 2009.

2. Пономарев И.В., Строкин Д.И. Стеганографические методы встраивания и обнаружения сокрытых сообщений, использующие GIF-изображения в качестве файлов-контейнеров // Известия АлтГУ. Математика и Механика. — 2022. — № 1(123). — DOI: 10.14258/izvasu(2022)1-18.

3. Сэломон Д. Сжатие данных, изображений и звука. — М. : Техносфера, 2004.

4. Куркина М.В., Пономарев И.В., Строкин Д.И. Стеганографические методы, устойчивые к JPEG сжатию // Известия АлтГУ. Математика и Механика. — 2021. — № 1(117). — DOI: 10.14258/izvasu(2021)1-17.

5. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. — М. : СОЛОН-ПРЕСС, 2009.