

ИДЕИ И ПРОЕКТЫ МОЛОДЕЖИ РОССИИ

СКРЫТИЕ ИНФОРМАЦИИ В ИЗОБРАЖЕНИИ

*Галкин Георгий Павлович,
4 курс, СибГУТИ ИВТ,
г. Новосибирск*

Аннотация. Реализована программа для проверки следующей гипотезы: если зашифровать данные в изображение формата .jerg так, чтобы проверка на наличие информации в изображении, с помощью метода многократного архивирования, не увенчалась успехом. Другими словами, изучить внедрение информации в изображение формата .jerg. В качестве информации, которую требуется зашифровать, будет небольшое секретное послание из нескольких предложений. Будет проведена проверка на эффективность данной задачи.

Ключевые слова: шифрование, изображение, метод Хаффмана, стеганография.

1. Введение

Целью работы является проверить следующую гипотезу: если зашифровать секретное послание в изображение формата .jerg, с дальнейшей перспективой сжатия, используя метод Хаффмана, так чтобы узнать о наличии информации методом многократного архивирования не представлялось возможным. При шифровании будут учтены особенности алгоритма сжатия изображения.

Требования, предъявляемые к данной задаче:

1. Требования к зашифрованным данным: они не должны быть слишком большие в объеме, так как с увеличением объема их будет труднее скрыть.

2. Изображение должно быть именно формата .jerg. Так как это самый распространённый формат, и его пересылка через открытый источник не вызовет подозрений.

В качестве открытого источника будет использован популярный ресурс [instagram.com](https://www.instagram.com), при передаче данных на сервер он использует нижеописанный алгоритм сжатия. Сжатие изображения будет происходить непосредственно при передаче данных на сервер, до размера 2048x2048.

2. Описание алгоритма

В первую очередь стоит ознакомиться с алгоритмом сжатия формата .jerg. Он будет состоять из 7 основных этапов. Для реализации данной задачи указанный ниже алгоритм не будет написан с нуля, будут использоваться готовые решения. Краткое описание алгоритма:

1. Переводим изображение из цветового пространства RGB, с компонентами, отвечающими за красную (R), зеленую (G), синюю (B). То

ИДЕИ И ПРОЕКТЫ МОЛОДЕЖИ РОССИИ

есть составляющие цвета точки, в цветовое пространство YCrCb. В нем Y – это яркостная составляющая, а Cr, Cb – это компоненты, которые отвечают за цвет (хроматический красный и хроматический синий). Зная особенности человеческого глаза, что он менее чувствителен к свету, чем к яркости, мы имеем возможность архивировать массивы для Cr и Cb компонент с большими потерями и коэффициентами сжатия.

2. Исходное выражение мы разобьем на матрицы размером 8x8. Сформируем из каждой матрицы по три рабочие матрицы ДКП, выделяя по 8 бит отдельно для каждой компоненты. Изображение делится по компоненте Y, то есть как и в самом первом случае, а для двух других компонент Cr и Cb набор идет через строчку и через столбец. Из исходной матрицы размером 16x16 получается только одна рабочая матрица ДКП. При таком раскладе, мы теряем 70% полезной информации о цветовых составляющих изображения, но получаем сжатие в два раза. Мы можем поступать так благодаря работе в пространстве YCrCb.

2. Вышеуказанное будем применять к каждой рабочей матрице. После этого будет получена матрица, с высокочастотными и низкочастотными коэффициентами изображения. Низкочастотные будут находиться в левом верхнем углу, а в правом нижнем низкочастотные.

3. Производим квантование. На этом этапе будут самые большие потери, так как мы будем управлять степенью сжатия, тем больше будут заданы коэффициенты, тем больше будет нулей, следовательно, степень сжатия будет увеличиваться.

4. Переводим матрицу 8x8 в вектор при помощи "зигзаг"-сканирования, т.е. берем элементы с индексами (0,0), (0,1), (1,0), (2,0), (1,1) и т.д. Тогда в начале вектора мы получаем коэффициенты матрицы, которые будут соответствовать низким частотам, а в конце вектора, соответственно, высоким.

5. Свертываем вектор с помощью алгоритма группового кодирования. При этом получаем пары типа (счетчик пропускаемых нулей, число), где вместо "число" - значение, которое необходимо будет поставить в следующую ячейку. Так, вектор 42 3 0 0 0 -2 0 0 0 0 1 ... будет свернут в пары (0,42) (0,3) (3,-2) (4,1) ...

6. Теперь свернем получившиеся пары кодированием по Хаффману с использованием фиксированной таблицы.

Теперь, зная об особенностях алгоритма сжатия, выдвигается гипотеза: понимая, как будет кодироваться изображение на 7-ом этапе, можно учесть особенности алгоритма Хаффмана и использовать их при шифровании текста в изображение. Другими словами, на 5-6 этапе запомним, какие данные можно изменить, а после 7 этапа произведем

ИДЕИ И ПРОЕКТЫ МОЛОДЕЖИ РОССИИ

шифрование используя особенности алгоритма Хаффмана.

3. Выводы

В этой статье выставлена на проверку гипотеза о шифровании текста в изображение сжатием Хаффмана. Для выполнения задачи использовались изображение формата .jerg, средства для его сжатия и алгоритм Хаффмана. При попытке расшифровать данные с помощью многократного архивирования мы не должны получить однозначного результата, в этом заключается гипотеза. При положительных результатах это дает возможность предполагать, что в данный метод можно использовать на практике.

СПИСОК ЛИТЕРАТУРЫ

- 1. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии М.: Горячая линия–Телеком, 2005. – 229 с.*
- 2. [http: compression.ru](http://compression.ru) (дата обращения: 19.06.2016).*
- 3. [http: ntuit.ru](http://ntuit.ru) (дата обращения: 21.06.2016).*