электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.82

Анализ методов сокрытия информации в контейнерах типа jpeg-файлы

***Сторожук О. Ю.**, студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Программное обеспечение ЭВМ и информационные технологии»

Научный руководитель: Филиппов М.В.., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана
bauman@bmstu.ru

Большинство методов сокрытия используют файлы с избыточной информацией. Это, например, BMP- и wav- файлы. Однако наибольшее распространение получили файлы типа jpeg и mp3, которые реализованы путем сжатия исходных данных с потерями. Основной принцип построения таких файлов — это удаление избыточной информации. Этот принцип использует особенности зрительного и звукового восприятия человека. Однако, с точки зрения сокрытия данных в таких файлах, удаление избыточной информации приводит к определенным проблемам. Данная работа посвящена анализу в алгоритмах сокрытия информации.

В данной статье будут рассмотрены стеганографические методы сокрытия информации в частотной области контейнера, так как сокрытие данных в пространственной области изображения являются нестойкими к большинству из известных видов искажений. Так, например, использование операции компрессии с потерями (например, JPEG-компрессии) приводит к частичному или, что более вероятно полному уничтожению встроенной контейнер информации.

Алгоритм обработки данных JPEG

JPEG основан на схеме кодирования, базирующейся на дискретных косинус-преобразованиях (DCT). Алгоритмы, базирующиеся на DCT, стали основой различных методов сжатия. Эти алгоритмы сжатия базируются не на поиске одинаковых атрибутов пикселов (как в RLE и LZW), а на разнице между ними. Схема JPEG эффективна только при сжатии многоградационных изображений, в которых различия между соседними пикселями, как правило, весьма незначительны.

Процесс сжатия по схеме JPEG включает ряд этапов (рис. 1):

- Преобразование изображения в оптимальное цветовое пространство.

- Субдискретизация компонентов цветности усреднением групп пикселей.
- Применение дискретных косинус-преобразований для уменьшения избыточности данных изображения.
- Квантование каждого блока коэффициентов DCT с применением весовых функций, оптимизированных с учетом визуального восприятия человеком.
- Кодирование результирующих коэффициентов (данных изображения) с применением алгоритма Хаффмана для удаления избыточности информации.

Рассмотрим вкратце особенности каждого из перечисленных этапов. При этом хотелось бы обратить внимание на то, что декодирование JPEG осуществляется в обратном порядке.

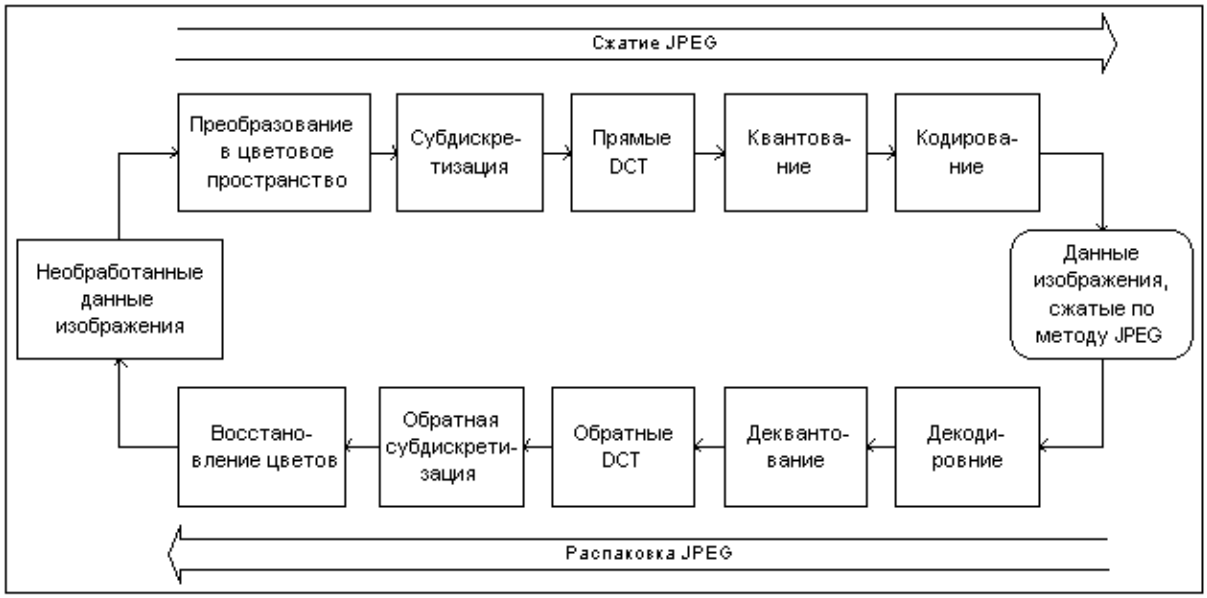

Рис. 1. Структура JPEG - преобразований

Шаг 1. Переводим изображение из цветового пространства RGB в цветовое пространства яркость/цветность, например такого, как YUV или YcbCr. При этом достигается лучшая степень сжатия. Компонента Y представляет собой интенсивность, а U и V - цветность. Поэтому появляется возможность архивировать массивы Cr и Cb компонент с большими потерями, а значит с большими степенями сжатия.

Преобразование цветовой модели RGB в модель YCbCr осуществляется с помощью следующих соотношений:

$$Y = 0{,}229R + 0{,}587G + 0{,}114B$$
$$Cb = -0{,}1687R - 0{,}3313G + 0{,}5B + 128$$
$$Cr = 0{,}5R - 0{,}4187G - 0{,}0813B + 128$$

Шаг 2. Разбиваем исходное изображение на матрицы 8x8. Формируем из каждой 3 рабочие матрицы ДКП — по 8 бит отдельно для каждой компоненты. При больших степенях сжатия этот шаг может выполняться чуть сложнее. Изображение делиться по компоненту Y, как и в первом случае, а для компонент Cr и Cb матрицы набираются через строчку и через столбец. То есть из исходной матрицы размером 16x16 получается только одна рабочая матрица ДКП. При этом, как нетрудно заметить, мы теряем ¾ полезной информации о цветовых составляющих изображения и получаем сразу же сжатие в 2 раза.

Шаг 3. Формулы прямого и обратного дискретного косинусного преобразования представлены ниже. Дискретное косинусное преобразование преобразует матрицу пикселов размером NxN в матрицу частотных коэффициентов соответствующего размера. Несмотря на видимую сложность, закодировать эти формулы достаточно просто.

$$\text{ДКП}(i,j) = \frac{1}{\sqrt{2N}} C(i)C(j)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} pixel(x,y)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

$$C(x) = \begin{cases} \frac{1}{\sqrt{2}}, x = 0 \\ 1, x > 0 \end{cases}$$

Применяем ДКП к каждой рабочей матрице. При этом мы получаем матрицу, в которой коэффициенты в левом верхнем углу соответствуют НЧ составляющей изображения, а в правом нижнем — ВЧ. Понятие частоты следует из рассмотрения изображения как двумерного сигнала. Плавное изменение цвета соответствует НЧ составляющей, а резкие скачки — ВЧ.

Шаг 4. Производим квантование. В принципе это просто деление рабочей матрицы на матрицу квантования поэлементно. Матрица для Y компонент:

3	5	7	9	11	13	15	17
5	7	11	13	15	17	19	21
7	11	13	15	17	19	21	23
9	11	13	15	17	19	21	23

11	13	15	17	19	21	23	25
13	15	17	19	21	23	25	27
15	17	19	21	23	25	27	29
17	19	21	23	25	27	29	31

Шаг 5. Заключительная стадия работы кодера JPEG - это собственно кодирование. Оно включает три действия над округленной матрицей дискретного косинусного преобразования, для того, чтобы повысить степень сжатия.

Первое действие - это замена абсолютного значения коэффициента, расположенного в ячейке (0,0) матрицы, на относительное. Так как соседние блоки изображения в значительной степени “похожи” друг на друга, то кодирование очередного (0,0) элемента как разницы с предыдущим дает меньшее значение.

Коэффициенты матрицы дискретного косинусного преобразования обходятся зигзагом. После чего нулевые значения кодируются с использованием алгоритма кодирования повторов (RLE), а потом результат обрабатывается с помощью “кодирования энтропии”, то есть алгоритмов Хаффмана или арифметического кодирования, в зависимости от реализации.

“Кодирование энтропии”. Результатом работы, упрощенной схемы кодирования, являются тройки следующего вида:

<**Количество Нулей**, **Количество Битов**, **Коэффициент**>

Здесь:

Количество Нулей - количество повторяющихся нулей, предшествующих текущему (ненулевому) элементу матрицы дискретного косинусного преобразования;

Количество Битов - количество битов, следующих далее, кодирующих значение коэффициента;

Коэффициент - значение ненулевого элемента матрицы дискретного косинусного преобразования.

Соответствие между полями Количество Битов и Коэффициент приведено в таблице 1.

Таблица 1

Соответствие между Количеством Битов и Коэффициентами

Количество Битов	Коэффициент
1	[-1, 1]
2	[-3, -2], [2, 3]
3	[-7, -4], [4, 7]
4	[-15, -8], [8, 15]
5	[-31, -16], [16, 31]
6	[-63, -32], [32, 63]
7	[-127, -64], [64, 127]
8	[-255, -128], [128, 255]
9	[-511, -256], [256, 511]
10	[-1023, -512], [512, 1023]

Такое кодирование не столь эффективно, как кодирование Хаффмана, но на определенных данных оно дает аналогичные результаты.

После завершения этого этапа поток данных JPEG готов к передаче по коммуникационным каналам или инкапсуляции в формат файла изображения.

Структура JPEG

Файл JPEG состоит из маркеров, встречаемых при декодировании файлов формата JPEG, которые представлены в таблице 2.

Таблица 2

Маркеры JPEG-файла

Тип маркера	Иденти-фикатор	Обозначение стандарта	Определение
SOF0	C016	Baseline DCT	Начало кадра, базовый метод
SOF1	C116	Extended sequential DCT	Начало кадра, расширенный, последовательный метод
SOF2	C216	Progressive DCT	Начало кадра, прогрессивный метод
DHT	C416	Define Huffman table(s)	Определение таблиц Хаффмана

SOI	D816	Start of image	Начало изображения
EOI	D916	End of image	Конец изображения
SOS	DA16	Start of scan	Начало скана
DQT	DB16	Define quantization table(s)	Определение таблиц квантования

В приведенной таблице показаны те маркеры, которые являются обязательными в любом файле формата JPEG и требуют обязательной обработки.

Структура типичного маркера:

| Идентификатор | Длина | Данные маркера |

Идентификатор – два байта, которые указывают на тип маркера.

Длина – два байта, которые содержат длину данных маркера в байтах (Обратный порядок) и собственную длину. То есть если данные маркера имеют длину 10 байт, то значение длинны будет равно 10 (длинна данных маркера) + 2 (два байта со значением длинны) = 12.

Данные маркера – набор байт, требующих обработки в соответствии с типом маркера.

Стеганографические алгоритмы сокрытия информации в частотной области.

Реальные изображения вовсе не являются случайным процессом с равномерно распределенными значениями величин. Хорошо известно, и это используется в алгоритмах сжатия, что большая часть энергии изображений сосредоточена в низкочастотной части спектра. Отсюда и потребность в осуществлении декомпозиции изображения на субполосы. Стегосообщение добавляется к субполосам изображения. Низкочастотные субполосы содержат подавляющую часть энергии изображения и, следовательно, носят шумовой характер. Высокочастотные субполосы наиболее подвержены воздействию со стороны различных алгоритмов обработки, будь то сжатие или НЧ фильтрация. Таким образом, для вложения сообщения наиболее подходящими кандидатами являются среднечастотные субполосы спектра изображения. Типичное распределение шума изображения и обработки по спектру частоты показано на рисунке 2.

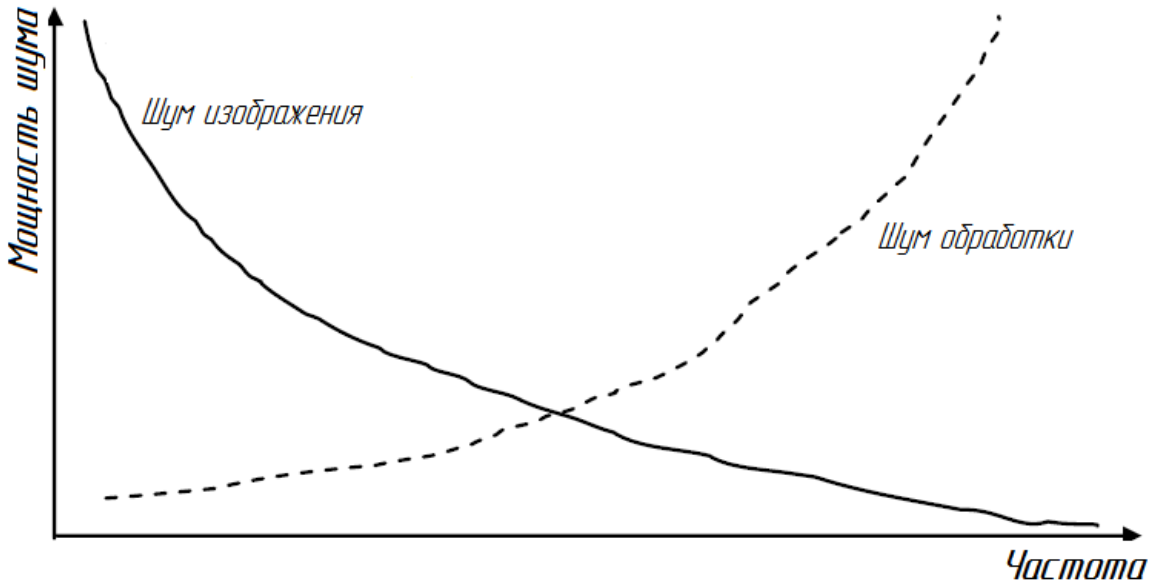

Рис. 2. Зависимость шума изображения и шума обработки от частоты

Шум обработки появляется в результате квантования коэффициентов трансформанты. Его можно рассматривать как уменьшение корреляции между коэффициентами трансформанты исходного изображения и квантованными коэффициентами. Например, при высоких степенях сжатия может возникнуть ситуация, когда будут отброшены целые субполосы. То есть дисперсия шума в этих субполосах, вообще говоря, бесконечна. Налицо уменьшение корреляции между коэффициентами субполосы до квантования и после. Для получения приемлемых результатов необходимо усреднить значение шума обработки по многим изображениям.

Преобразования можно упорядочить по достигаемым выигрышам от кодирования: единичное, Адамара, Хаара, ДКП, Вейвлет, Карунена-Лоэва (ПКЛ). Под выигрышем от кодирования понимается степень перераспределения дисперсий коэффициентов преобразования.

Наибольший выигрыш дает преобразование Карунена-Лоэва (ПКЛ), наименьший – разложение по базису единичного импульса (то есть отсутствие преобразования). Преобразования, имеющие высокие значения выигрыша от кодирования, такие как ДКП, вейвлет-преобразование, характеризуются резко неравномерным распределением дисперсий коэффициентов субполос. Высокочастотные субполосы не подходят для вложения из-за большого шума обработки, а низкочастотные – из-за высокого шума изображения. Поэтому приходится ограничиваться среднечастотными полосами, в которых шум изображения примерно равен шуму обработки. Так как таких полос

немного, то пропускная способность стегоканала невелика. В случае применения преобразования с более низким выигрышем от кодирования, например, Адамара или Фурье, имеется больше блоков, в которых шум изображения примерно равен шуму обработки. Следовательно, и пропускная способность выше. Следовательно, для повышения пропускной способности стеганографического канала лучше применять преобразования с меньшими выигрышами от кодирования, плохо подходящие для сжатия сигналов.

Эффективность применения вейвлет-преобразования и ДКП для сжатия изображений объясняется тем, что они хорошо моделируют процесс обработки изображения в СЧЗ, отделяют «значимые» детали от «незначимых». Значит, их более целесообразно применять в случае активного нарушителя, так как модификация значимых коэффициентов может привести к неприемлемому искажению изображения. При применении преобразования с низкими значениями выигрыша от кодирования существует опасность нарушения вложения, так как коэффициенты преобразования менее чувствительны к модификациям.

Встраивание данных в коэффициенты дискретного косинусного преобразования

При использовании данного метода, контейнер разбивается на блоки размером 8x8 пикселов, которые показаны на рисунке 3. ДКП применяется к каждому блоку, в результате чего получаются матрицы коэффициентов ДКП, также размером 8x8. Коэффициенты обозначаются через, где b – номер блока, - позиция коэффициента внутри блока. Если блок сканируется в зигзагообразном порядке (как это имеет место в JPEG), то коэффициенты обозначаются через. Коэффициент в левом верхнем углу обычно называется DC-коэффициентом. Он содержит информацию о яркости всего блока. Остальные коэффициенты называются AC-коэффициентами. Иногда выполняется ДКП всего изображения, а не отдельных блоков. Далее рассмотрим некоторые из алгоритмов внедрения ЦВЗ в области ДКП.

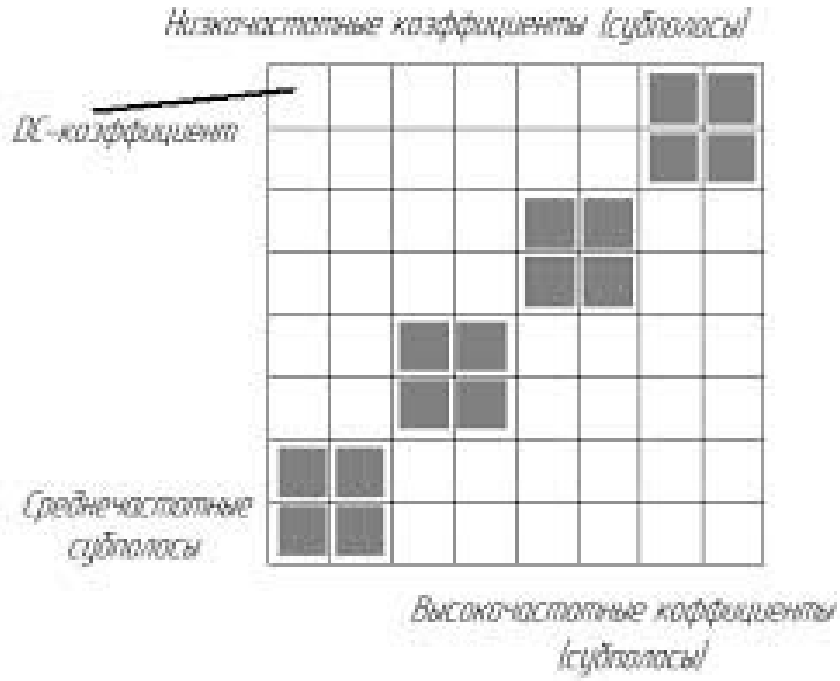

Рис. 3. Блок 8x8 пикселей с расположением коэффициентов ДКП

Алгоритм Коча (Koch)

В данном алгоритме в блок размером 8x8 осуществляется встраивание 1 бита ЦВЗ. Описано две реализации алгоритма: псевдослучайно могут выбираться два или три коэффициента ДКП. Рассмотрим вариацию алгоритма с двумя выбираемыми коэффициентами.

Встраивание информации осуществляется следующим образом: для передачи бита 0 добиваются того, чтобы разность абсолютных значений коэффициентов была бы больше некоторой положительной величины, а для передачи бита 1 эта разность делается меньше некоторой отрицательной величины:

$$\left|c_b(j_{i,j},k_{i,1})\right| - \left|c_b(j_{i,2},k_{i,2})\right| > s, \text{если } \varepsilon_i = 0,$$

$$\left|c_b(j_{i,j},k_{i,1})\right| - \left|c_b(j_{i,2},k_{i,2})\right| < -s, \text{если } \varepsilon_i = 1.$$

Алгоритм Кокса (Cox)

Этот алгоритм является робастным ко многим операциям обработки сигнала. Обнаружение встроенного ЦВЗ в нем выполняется с использованием исходного изображения. Внедряемые данные представляют собой последовательность вещественных чисел с нулевым средним и единичной дисперсией. Для вложения информации

используются несколько АС-коэффициентов ДКП всего изображения с наибольшей энергией. Автором предложено три способа встраивания ЦВЗ в соответствии со следующими выражениями:

$$c'_i = c_i + \alpha s_i;\ c'_i = c_i(1+\alpha s_i);\ c'_i = c_i e^{\alpha s_i}$$

Первый вариант может использоваться в случае, когда энергия ЦВЗ сравнима с энергией модифицируемого коэффициента. В противном случае либо ЦВЗ будет неробастным, либо искажения слишком большими. Поэтому так встраивать информацию можно лишь при незначительном диапазоне изменения значений энергии коэффициентов.

При обнаружении ЦВЗ выполняются обратные операции: вычисляются ДКП исходного и модифицированного изображений, находятся разности между соответствующими коэффициентами наибольшей величины.

Алгоритм Барни (Barni)

Этот алгоритм является улучшением алгоритма Кокса, и в нем также выполняется ДКП всего изображения. В нем детектору уже не требуется исходного изображения, то есть схема слепая. Для встраивания ЦВЗ используются не наибольшие АС-коэффициенты, а средние по величине. В качестве ЦВЗ выступает произвольная строка бит.

Выбранные коэффициенты модифицируются следующим образом: $c'_i = c_i + \alpha s_i |c_i|$. Далее выполняется обратное ДКП, и производится дополнительный шаг обработки: исходное и модифицированное изображения складываются с весовыми коэффициентами:

$$l''(x,y) = \beta(x,y)l'(x,y) + (1-\beta)l(x,y)$$

Здесь $\beta \approx 1$ для текстурированных областей (в которых человеческий глаз мало чувствителен к добавленному шуму) и $\beta \approx 0$ в однородных областях. Значение находится не для каждого пикселя в отдельности, а для неперекрывающихся блоков фиксированного размера. Например, в качестве целесообразно использовать нормализованную дисперсию блоков. В детекторе ЦВЗ вычисляется корреляция между модифицированным изображением и ЦВЗ - $\sum_{i=1}^{n} c''_i s''_i$

Сравнение стойкости стеганографических алгоритмов.

Под стойкостью стеганографических алгоритмов понимается вероятность успешного восстановления скрытого сообщения после воздействия атак на контейнер.

На основе анализа рассмотренных методов получены результаты, приведенные в таблице 3.

Таблица 3

Устойчивость алгоритмов к различным воздействиям

Алгоритмы	Одно-значность восста-новления	Устойчивость к фильтрации	Устойчивость к геометрии-ческим преобра-зованиям	Устойчивость к сжатию	Устойчивость к средствам статического анализа
Коч	+	-	-	-	-
Кокс	+	-	+	+	-
Барни	-	+	-	+	+

Выводы

Рассмотренные основные алгоритмы сокрытия информации, использующие преобразования ДКП, не удовлетворяют всем основным критериям стегоситем. Алгоритмы Коча, Кокса и Барни сравнивались по следующим критериям: однозначность восстановления, устойчивость к фильтрации, устойчивость к геометрическим преобразованиям, устойчивость к сжатию и устойчивость к средствам статического анализа. Алгоритм Коча является устойчивым только к однозначному восстановлению. Алгоритм Кокса устойчив к однозначному восстановлению, геометрическим преобразованиям и к сжатию. Алгоритм Барни устойчив к фильтрации, сжатию и средствам статического анализа.

Список литературы

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: СОЛОН-Пресс, 2002. 272 с.
2. Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. М: Издательство МК-Прес, 2006. 283 с.
3. Сэломон Д. Сжатие данных, изображений и звука. М.: Техносфера, 2004. 368 с. [Salomon D. A Guide to Data Compression Methods, 2002. 295 p.]