МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

Кафедра математического моделирования и анализа данных

КОРРЕКТИРОВКА ГИСТОГРАММЫ КОНТЕЙНЕРА ПРИ ВСТРАИВАНИИ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ КОДОВ ХЭММИНГА

Курсовая работа

Новиковой Анастасии Владимировны
студентки 3 курса, специальность
«компьютерная безопасность»

Научный руководитель:
с. н. с. НИИ ППМИ
А. М. Капуста

Минск, 2015

ПЛАН ДОКЛАДА:

1. Введение.
2. Коды обнаружения и исправления ошибок. Блоковые коды. Коды Хэмминга.
3. Алгоритмы встраивания с использованием кодов Хэмминга. Применение разработанных алгоритмов к бинарным файлам.
4. Алгоритм сжатия JPEG. Применение разработанных алгоритмов к матрицам квантованных ДКП – коэффициентов.
5. Заключение.

ВВЕДЕНИЕ

Развитие компьютерных методов обработки информации позволило существенно повысить уровень обеспечения информационной безопасности. Так появилась стеганография – наука о способах передачи информации по каналам связи.

При передаче данных информация встраивается по определенному алгоритму в некий исходный объект (контейнер), в результате чего получается модифицированный контейнер. В стеганографии в качестве контейнеров могут выступать графические изображения, аудиофайлы и видеофайлы.

Основной задачей в стегосистеме является обеспечение сокрытия факта передачи информации. Задачу, обратную задаче стеганографии и состоящую в том, чтобы обнаружить наличие скрытого сообщения и, если возможно, извлечь, вскрыть, подменить или уничтожить его называют задачей стегоанализа.

Поэтому необходимо разрабатывать такие алгоритмы встраивания информации, которые были бы достаточно эффективны при проведении стегоанализа. Под эффективностью встраивания данных понимается наилучшее соотношение между пропускной способностью и стойкостью к стегоанализу (невозможность выявления факта наличия встроенной информации в контейнере). Таким образом целью данной работы является разработка такого алгоритма, который сохранял бы незаметность факта встраивания данных при максимально возможной пропускной способности.

Коды обнаружения и исправления ошибок

В процессе хранения данных и передачи информации по сетям связи неизбежно возникают ошибки. В системах связи возможны несколько стратегий борьбы с ошибками.

Корректирующие коды — коды, служащие для обнаружения или исправления ошибок, возникающих при передаче информации, а также при её хранении. С кодами, исправляющими ошибки, тесно связаны коды обнаружения ошибок.

Блоковые коды

Пусть кодируемая информация делится на фрагменты длиной k бит, которые преобразуются в кодовые слова длиной n бит. Тогда соответствующий блоковый код обычно обозначают: (n, k).

Коды, в которых возможно автоматическое исправление ошибок, называются самокорректирующимися. Количество контрольных разрядов r, необходимых для построения самокорректирующегося кода, рассчитанного на исправление одиночных ошибок, должно быть выбрано так, чтобы удовлетворялось неравенство

$$r \geq \log_2(r + k + 1).$$

Коды Хэмминга

Для каждого r существует $(2^r - 1,\ 2^r - 1 - r)$ - код Хэмминга, где r - количество контрольных разрядов.

Алгоритмы встраивания с использованием кодов Хэмминга

Синдром S, блок b и проверочная матрица кода Хэмминга H связаны соотношением:

$$bH^T = S.$$

$Number$ – номер бита, который нужно изменить (в двоичном представлении):

$$number = S \oplus S_0.$$

Применение разработанных алгоритмов к бинарным файлам

Гистограмма частот 0 и 1 при параметре r = 3.

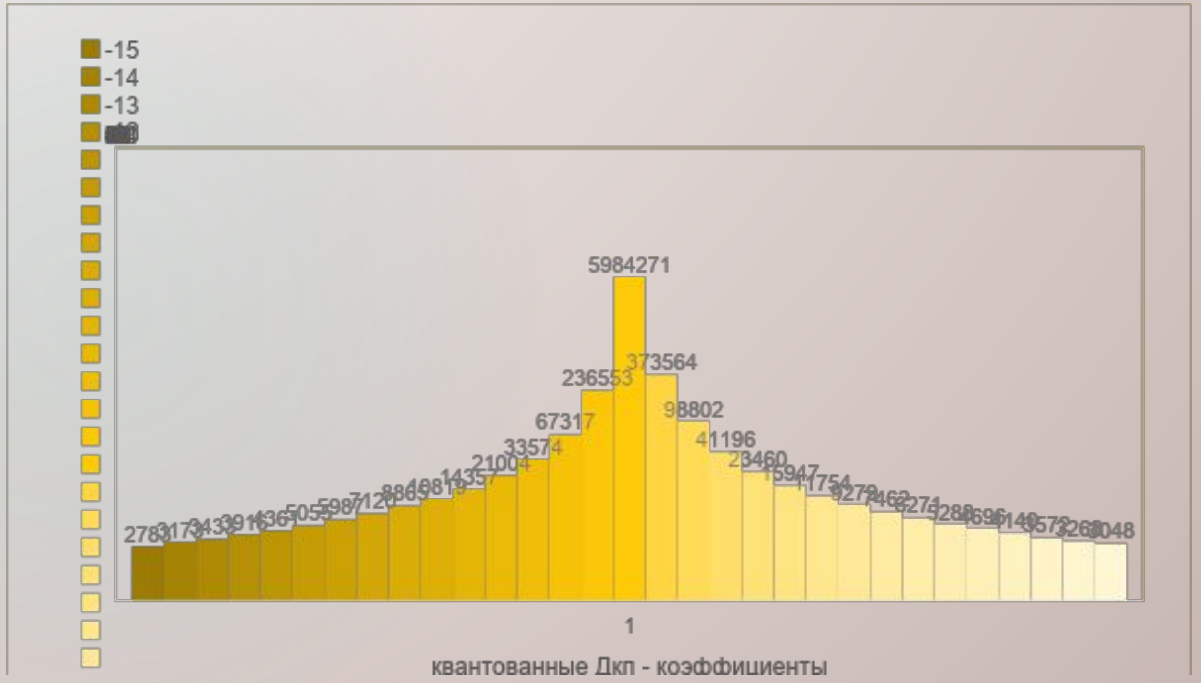
Гистограмма частот 0 и 1 при параметре r = 6.

Алгоритм сжатия JPEG

Сжатие изображение в формат JPEG осуществляется в несколько этапов:

- Преобразование цветового пространства.
- Сегментация.
- Дискретное косинусное преобразование.
- Квантование.
- Кодирование

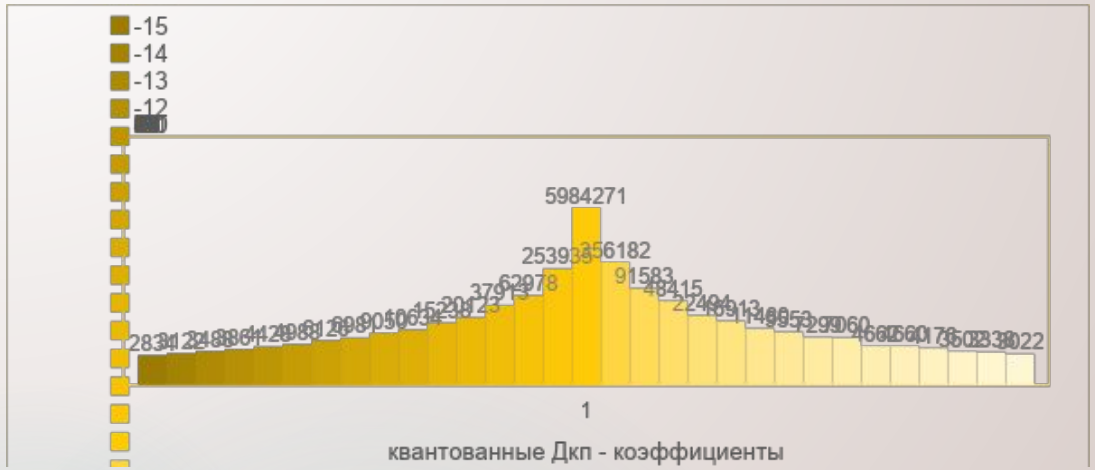
Применение разработанных алгоритмов к матрицам квантованных ДКП – коэффициентов



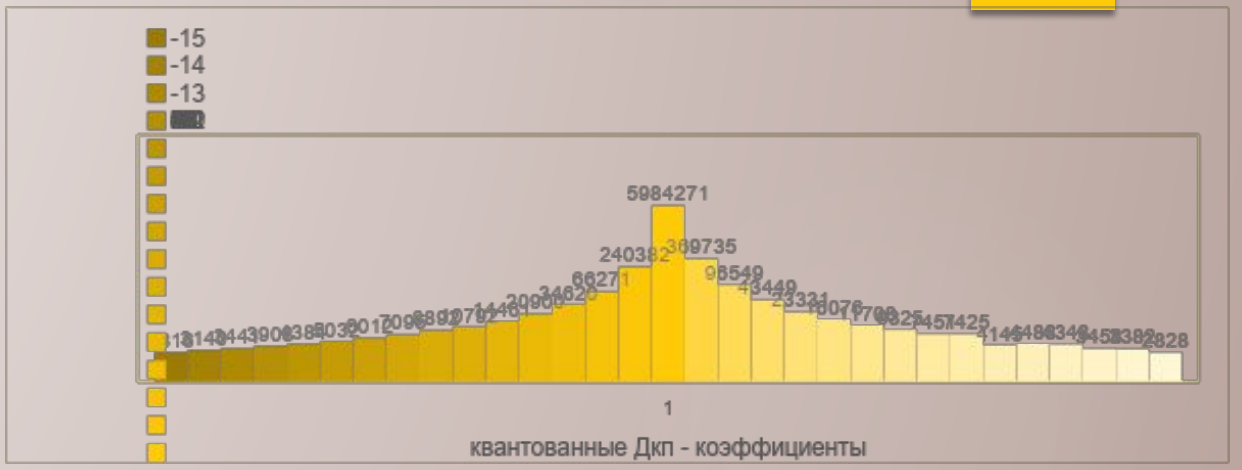
Гистограмма частот квантованных ДКП - коэффициентов до встраивания.

Гистограмма частот квантованных ДКП - коэффициентов после встраивания (параметр r = 3)

(1 алгоритм)

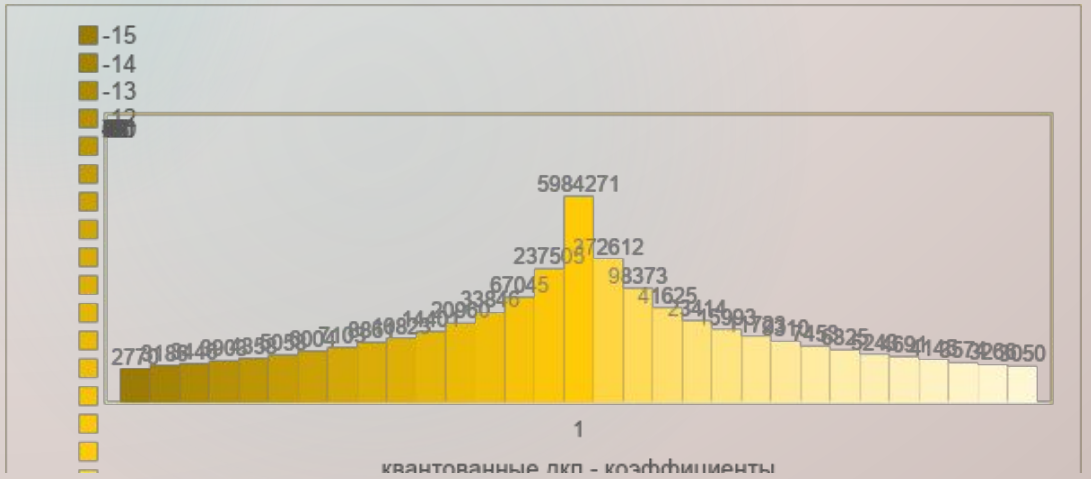


(2 алгоритм)

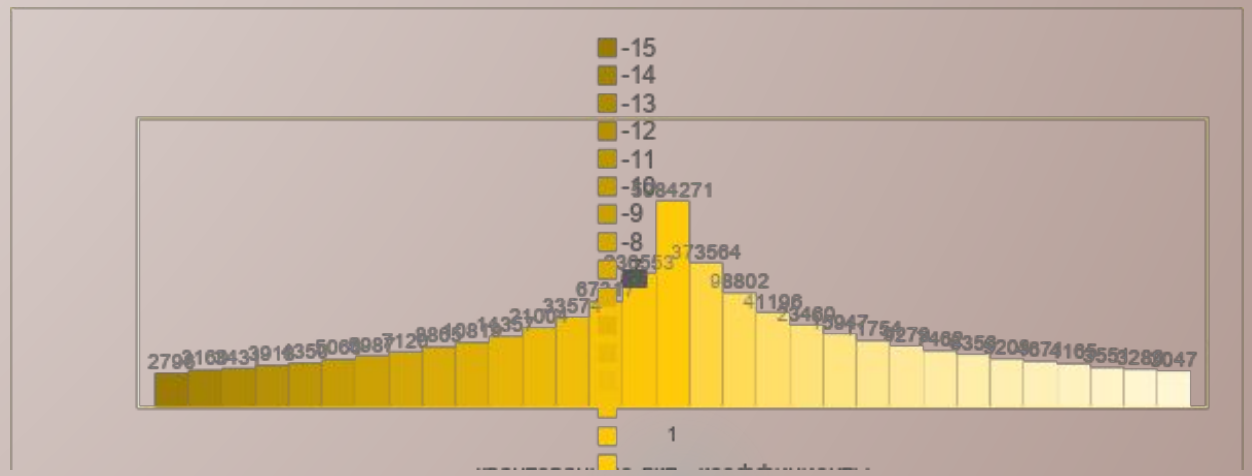


Гистограмма частот квантованных ДКП - коэффициентов после встраивания (параметр r = 7)

(1 алгоритм)



(2 алгоритм)



ЗАКЛЮЧЕНИЕ

В данной работе был реализован алгоритм встраивания информации в бинарные числовые последовательности с использованием кодов Хэмминга, а также разработан и реализован алгоритм встраивания информации в бинарные числовые последовательности с использованием кодов Хэмминга, минимизирующий искажения гистограмм контейнера.

Алгоритмы были применены к бинарным файлам и матрицам квантованных ДКП – коэффициентов.

Сравнение гистограмм показало, что второй алгоритм встраивания данных в бинарную последовательность минимизирует искажения гистограммы контейнера.