

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет радиофизики и электроники

Кафедра кибернетики

**СТЕГАНОГРАФИЧЕСКАЯ СИСТЕМА СКРЫТИЯ ДАННЫХ
В ОБЛАСТИ ЧАСТОТНЫХ ПРЕОБРАЗОВАНИЙ ИЗОБРАЖЕНИЙ**

Дипломная работа студента 5 курса
РАИКА Георгия Александровича

Руководитель: канд. техн. наук, доцент
САДОВ В. С.

Рецензент: канд. техн. наук, доцент
ЧУДОВСКИЙ В. А.

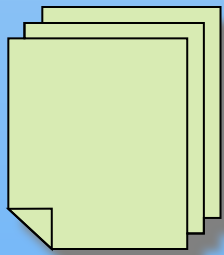
Минск, 2007

- **Цель работы:** разработка адаптивного стеганографического алгоритма встраивания информации в графические изображения, сжатые по стандарту JPEG, и его реализация на одном из языков программирования высокого уровня. Кроме **адаптивности** и **стойкости**, к алгоритму предъявлены требования **устойчивости к сжатию**, **гибкости** относительно встраиваемых объемов, **повторности адаптивного анализа** для возможности извлечения встроенной информации.

1. АНАЛИЗ ОСНОВНЫХ ПРИНЦИПОВ И АЛГОРИТМОВ

•АНАЛИЗ ОСНОВНЫХ ПРИНЦИПОВ СТЕГАНОГРАФИИ

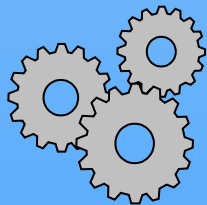
•ДЕТАЛЬНОЕ ИЗУЧЕНИЕ СВОЙСТВ ЧЕЛОВЕЧЕСКОГО ЗРЕНИЯ И ФОРМАТА СЖАТИЯ JPEG



JPEG Standard (JPEG ISO/IEC 10918-1 ITU-T Recommendation T.81)

JPEG File Interchange Format. Version 1.02

•ИССЛЕДОВАНИЕ СУЩЕСТВУЮЩИХ АЛГОРИТМОВ

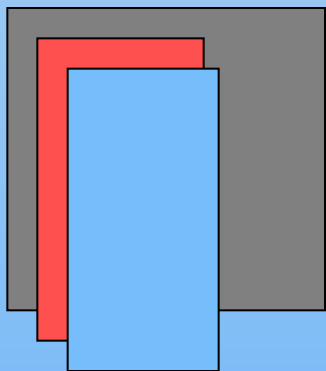


1. Алгоритм Коха (Koch)
2. Алгоритм Бенхама (Benham)
3. Алгоритм Подильчука (Podilchuk)
4. Алгоритм Хсу (Hsu)
5. Алгоритм Тао (Tao)

СТАНДАРТ СЖАТИЯ JPEG

Матричное дискретное косинусное преобразование (ДКП).

YCbCr



Каждая матрица цветового пространства разбивается на блоки размером 8 на 8 пикселей и к ним применяется ДКП

$$P_{DCT} = DCT * P * DCT^T,$$

где P – исходный блок изображения,
 DCT, DCT^T – матрицы ДКП (прямая и транспонированная).

Квантование: основной этап сжатия.

Каждый элемент полученной матрицы коэффициентов ДКП делится нацело на соответствующий коэффициент матрицы квантования.

Шаги
квантования
для области
низких частот

6	4	4	6	9	11	12	16
4	5	5	6	8	10	12	12
4	5	5	6	10	12	14	19
6	6	6	11	12	15	19	28
9	8	10	12	16	20	27	31
11	10	12	15	20	27	31	31
12	12	14	19	27	31	31	31
16	12	19	28	31	31	31	31

Шаги
квантования
для области
высоких частот

типичная матрица квантования

2. ИССЛЕДОВАНИЕ ИНФОРМАТИВНОСТИ КОЭФФИЦИЕНТОВ ИЗОБРАЖЕНИЙ

Классификация коэффициентов области частотных преобразований

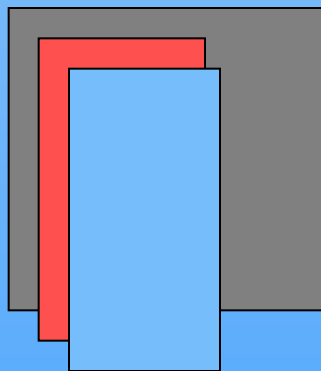
по частоте

- нулевая частота (DC);
- низкие частоты;
- средние частоты;
- высокие частоты;

DC	НЧ	НЧ	НЧ	НЧ	НЧ	СЧ	СЧ
НЧ	НЧ	НЧ	НЧ	НЧ	СЧ	СЧ	СЧ
НЧ	НЧ	НЧ	НЧ	СЧ	СЧ	СЧ	ВЧ
НЧ	НЧ	НЧ	СЧ	СЧ	СЧ	ВЧ	ВЧ
НЧ	НЧ	СЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ
НЧ	СЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ
СЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ
СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ

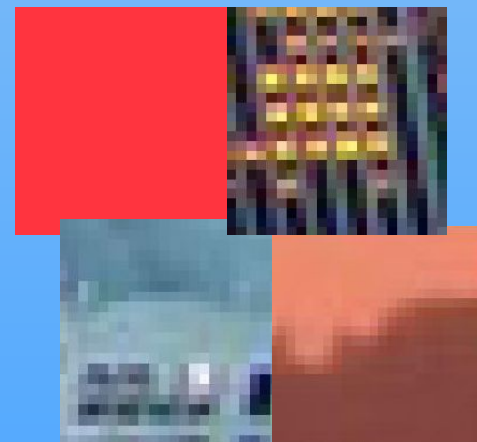
по типу матрицы

- матрица Y ;
- матрица S_b ;
- матрица S_r ;

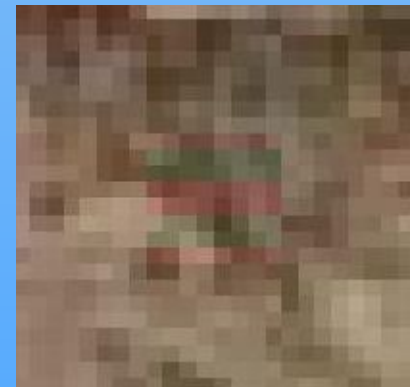
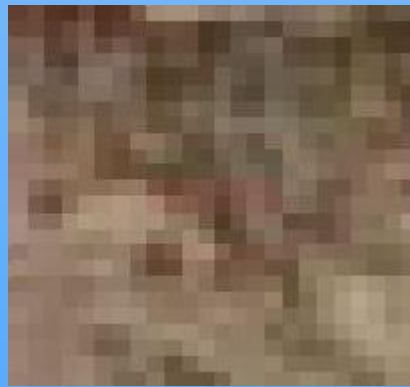


по характеру неоднородности блока

- однородные;
- слабо неоднородные;
- сильно неоднородные;
- с резким контуром;



Исследования информативности высокочастотных коэффициентов цветowych матриц в слабо неоднородных областях

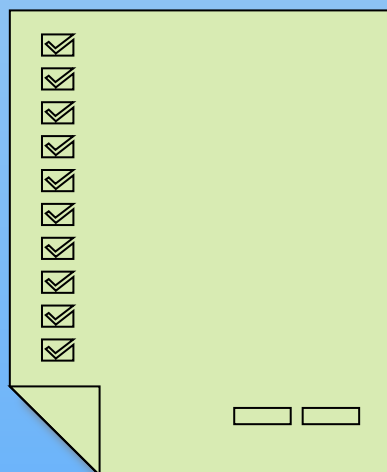


Результаты исследования информативности коэффициентов ДКП

1. Яркостная матрица более пригодна для встраивания, чем цветные.
2. С_b-матрица оказалась более пригодной для встраивания, чем С_r-матрица.
3. Наиболее пригодной для встраивания является сильно неоднородная область.
4. Предпочтительным является изменение спектра блока, при котором в спектр не добавляются новые частоты (то есть информация встраивается в ненулевые коэффициенты).
5. Наиболее пригодными являются коэффициенты с меньшей частотой (и с меньшим шагом квантования).

3. РАЗРАБОТКА АЛГОРИТМА ВСТРАИВАНИЯ

Основные требования к алгоритму встраивания



- Стойкость (скрытность);
- Адаптивность;
- Гибкость;
- Возможность повторного анализа;

Стойкость алгоритма

Порядок	Матрица	Частотная группа	Тип области
1	Y	DC	Сильно неоднородная
2	Y	НЧ	Сильно неоднородная
3	Cb	DC	Сильно неоднородная
4	Cb	НЧ	Сильно неоднородная
5	Y	СЧ	Сильно неоднородная
6	Cb	СЧ	Сильно неоднородная
7	Cr	DC	Сильно неоднородная

Адаптивность алгоритма

Предварительный анализ с сортировкой блоков изображения на три группы неоднородности: однородные, слабо неоднородные, сильно неоднородные

фактор неоднородности

$$H = \sum_{i=1}^8 \sum_{j=1}^8 |K_{i,j}| \cdot Q_{i,j} M_{i,j},$$

где $K_{i,j}$ – коэффициент оцениваемого блока,

$Q_{i,j}$ – шаг квантования для соответствующего коэффициента (элемент матрицы квантования),

$M_{i,j}$ – значение элемента матрицы оценки неоднородности.

0	1	1	1	1	1	2	2
1	1	1	1	1	2	2	2
1	1	1	1	2	2	2	3
1	1	1	2	2	2	3	3
1	1	2	2	2	3	3	3
1	2	2	2	3	3	3	3
2	2	2	3	3	3	3	3
2	2	3	3	3	3	3	3

матрица неоднородности

Адаптивность алгоритма

низкочастотный фактор

$$F_L = \sum_{i=1}^8 \sum_{j=1}^8 |K_{i,j}| \cdot Q_{i,j} \cdot T_{i,j};$$

0	2	1	0	0	0	0	0
2	2	1	0	0	0	0	0
1	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

матрица низких частот

высокочастотный фактор

$$F_H = \sum_{i=1}^8 \sum_{j=1}^8 |K_{i,j}| \cdot Q_{i,j} \cdot G_{i,j};$$

0	0	0	0	0	0	0	0
0	0	0	0	1	1	1	1
0	0	0	1	1	2	2	2
0	0	1	1	2	2	2	2
0	1	1	2	2	2	2	3
0	1	2	2	2	2	3	3
0	1	2	2	2	3	3	3
0	1	2	2	3	3	3	3

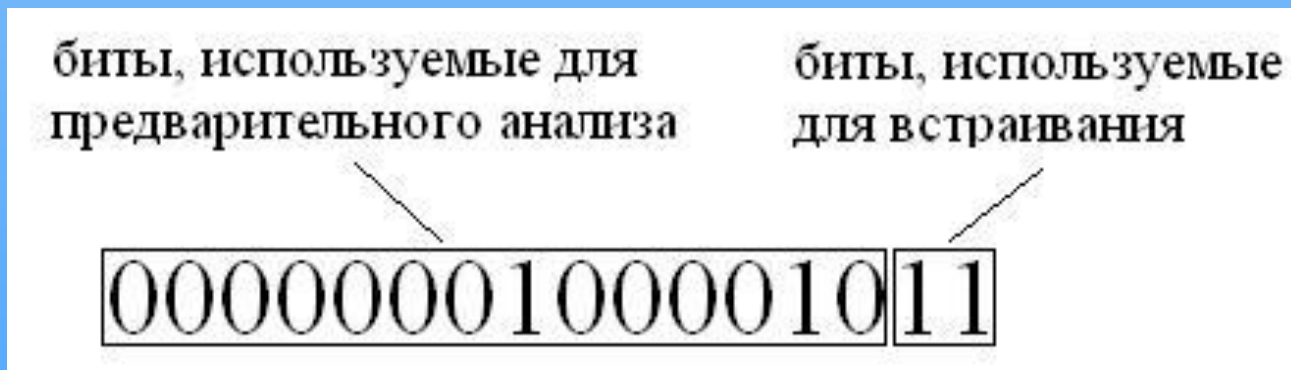
матрица высоких частот

Возможность повторного анализа

Предварительный анализ должен давать одинаковые результаты для пустого и заполненного контейнера, что позволяет извлекать встроенную информацию.

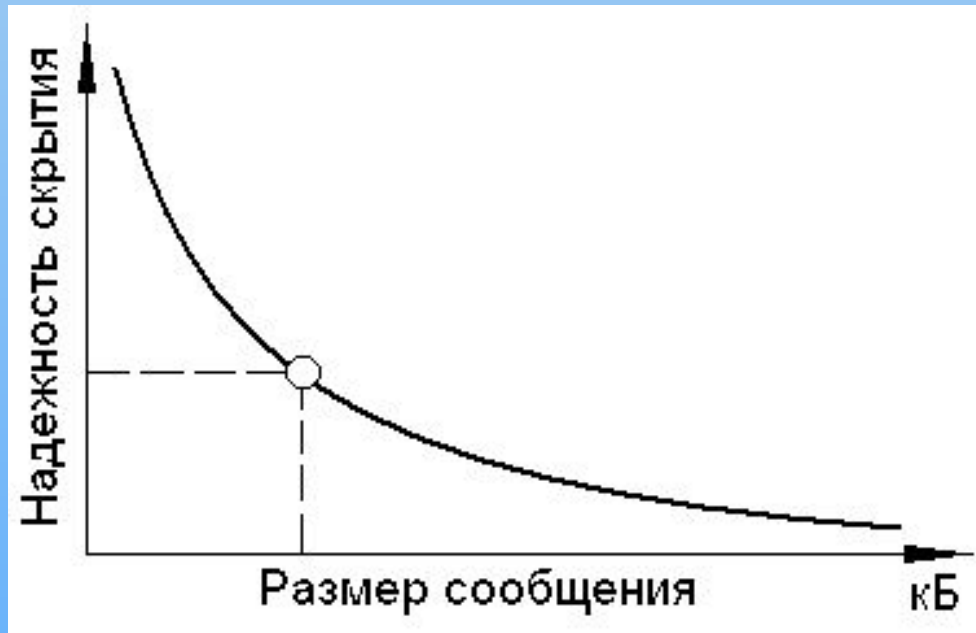
Достигается за счет исключения из анализа битов частотных коэффициентов, которые могут использоваться для встраивания, при определении степени неоднородности блока.

Коэффициент может использоваться для встраивания только в том случае, если среди битов, используемых для анализа, присутствует хотя бы один ненулевой!



Гибкость встраиваемых объемов

Зависимость надежности скрытия от размера встраиваемого сообщения при фиксированном контейнере



Алгоритм должен позволять задействовать для встраивания лишь необходимый минимум коэффициентов в наиболее приспособленных блоках.

Гибкость встраиваемых объемов

Вводим уровни безопасности.

- Каждый уровень имеет описание, позволяющее для любого блока однозначно определить какое количество бит и в какие коэффициенты будет встраиваться.
- Первый уровень самый безопасный, но позволяет встраивать сообщения небольших размеров.
- Каждый последующий уровень получается из предыдущего путем вовлечения во встраивание новых групп коэффициентов, увеличения количества используемых для встраивания коэффициентов уже используемых групп и т.д.
- Большое количество уровней повышает гибкость, но усложняет реализацию алгоритма и его вычислительную сложность.

Последовательность действий при модификации спектра

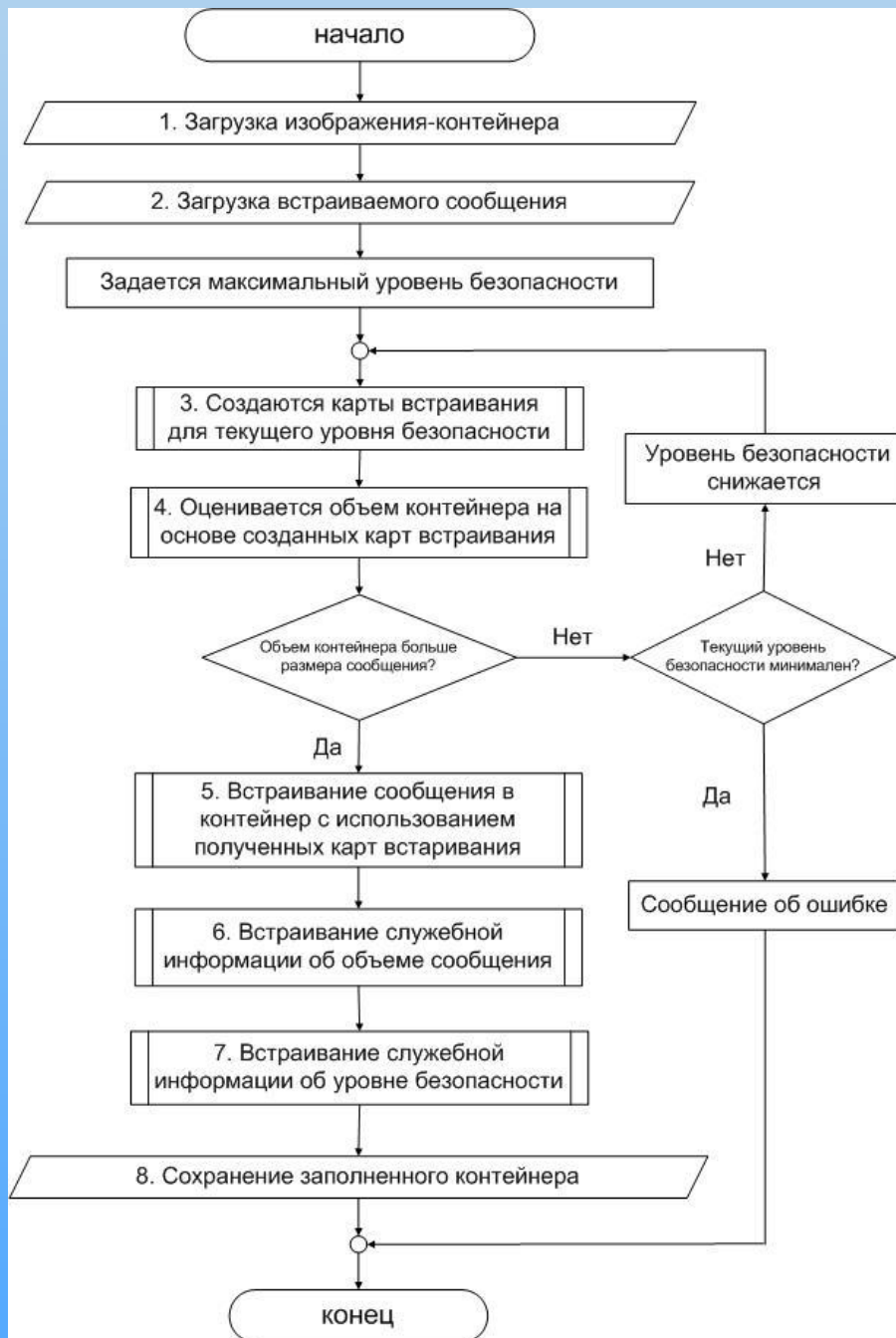
определение уровня безопасности

Тип матрицы	Тип блока	Частота	Кол-во бит	Кол-во
Y	сильно неоднородный	DC	2	-
Y	сильно неоднородный	НЧ	1	2
Y	сильно неоднородный	СЧ	1	1
Сb	сильно неоднородный	DC	1	-

блок для встраивания

35	4	2	4	0	0	0	0	0
1	2	3	0	0	0	0	0	0
1	5	1	2	1	0	0	0	0
0	3	4	0	1	0	0	0	0
2	0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

DC	НЧ	НЧ	НЧ	НЧ	НЧ	СЧ	СЧ
НЧ	НЧ	НЧ	НЧ	НЧ	СЧ	СЧ	СЧ
НЧ	НЧ	НЧ	НЧ	СЧ	СЧ	СЧ	ВЧ
НЧ	НЧ	НЧ	СЧ	СЧ	СЧ	ВЧ	ВЧ
НЧ	НЧ	СЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ
НЧ	СЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ
СЧ	СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ
СЧ	СЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ	ВЧ



Реализация алгоритма

TestJpeg *файлКонтейнер* *файлЗапКонтейнер* *файлСообщ*
уровень

файлКонтейнер – имя пустого контейнера, файла в формате JPEG;
файлЗапКонтейнер – имя, под которым будет сохранен заполненный контейнер.

файлСообщ – файл, содержащий сообщение;

уровень – используемый уровень безопасности;



**Пустой контейнер (разрешение 800x600,
размер 123665 байт)**



**Заполненный контейнер (разрешение 800x600,
размер 125015 байт, встроено 40196 бит)**



Результаты работы

- Исследована информативность коэффициентов ДКП, выявлены наиболее пригодные для встраивания области изображения. Результаты опубликованы в журнале «Электроника-инфо».
- Создан механизм предварительного адаптивного анализа, основанный на сортировке блоков в соответствии с разработанными критериями сортировки.
- Создана концепция уровней безопасности, придающая алгоритму встраивания гибкость относительно встраиваемых объемов.
- Алгоритм встраивания реализован C++.



СПАСИБО ЗА ВНИМАНИЕ

