

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение
высшего образования
«МИРЭА – Российский технологический университет»
РТУ МИРЭА**

КАФЕДРА КБ-3 «Управление и моделирование систем»

**Тема: Разработка механизма обмена скрытой
информацией в видеофайлах со сжатием с помощью
стеганографии**

Автор проекта студент:

Барашков Д.А.

Разработка механизма обмена скрытой информацией в видеофайлах с помощью стеганографии

Актуальность проекта: заключается в возможности скрытия факта коммуникации между пользователями

Новизна проекта: состоит в разработке системы с простым для пользователя интерфейсом, которая позволяет скрыть сообщение в видеофайл со сжатием без потери информации

Практическая значимость проекта: заключается в разработке оптимального средства позволяющего встраивать секретную информацию в видеофайл, что так же может быть использовано для подтверждения авторских прав.

Задачи проекта

- ❖ **Исследование принципов реализации механизмов сокрытия данных в видеофайлах с помощью стеганографии;**
- ❖ **Разработка математической модели внедрения информации в видеоряд;**

Анализ существующих систем встраивания информации методами стеганографии

Название ПО	Описание	Достоинства	Недостатки
JSTEG	Алгоритм работы представляет собой замену наименее значимых бит (метод LSB)	Бесплатная для работы с JPEG; простота использования.	Не устойчива к анализу гистограмм; не устойчива к визуальным атакам; поддерживает только формат JPEG; только один алгоритм шифрования; мало возможностей.
S-Tools	Данная программа позволяет скрывать любые файлы в GIF, BMP и WAV	Поддержка нескольких алгоритмов шифрования; без пароля невозможно установить факт работы STools.	Поддерживает мало форматов; мало возможностей; в некоторых случаях наблюдалось искажение встраиваемой информации.
TrueCrypt	Позволяет шифровать логические диски, разделы жесткого диска или usb-накопителя.	Умеет создавать виртуальный зашифрованный диск; При генерации ключей шифрования использует хэш-функции;	В мае 2014, в ходе проверки TrueCrypt, были обнаружены серьезные уязвимости и нарушения.
CyberSafe	Предоставляет широкий спектр услуг таких как: шифрование файлов, папок, каталогов и дисков, электронной почты и т.д	Широкий спектр возможностей для шифрования абсолютно любых видов информации; неограниченная длина пароля для шифрования;	Данное программное обеспечение является платным и требует специальной установки.

Процесс сокрытия информации в видеофайле

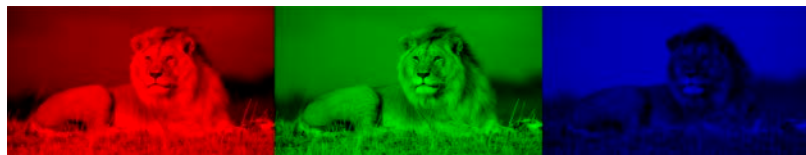


Процесс сокрытия информации в видеофайле



Цветовые пространства

Пространство RGB



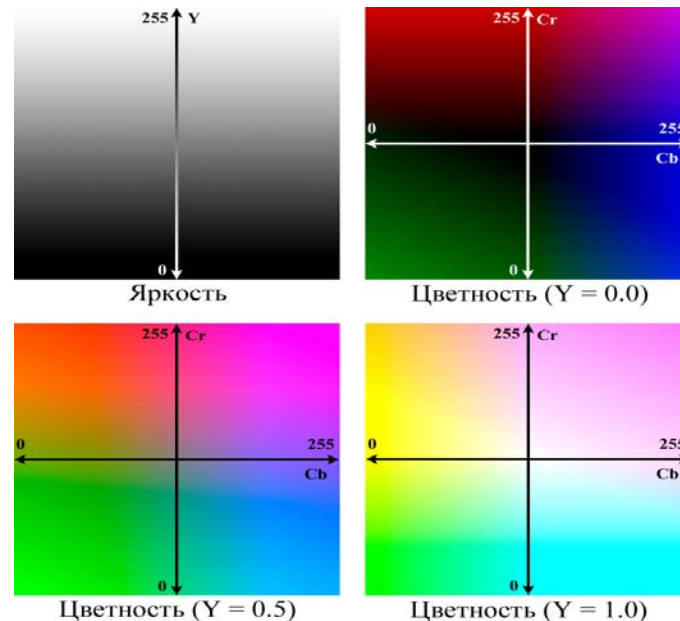
Три цветовых канала модели RGB



Объединение трех компонентов в цвет

$$\begin{cases} R = Y + 1.402(C_r - 128) \\ G = Y - 0.34414(C_b - 128) - 0.71414(C_r - 128) \\ B = Y + 1.772(C_b - 128) \end{cases}$$

Пространство YCbCr



$$\begin{cases} Y = 0.299R + 0.597G + 0.114B \\ Cb = 128 - 0.1687R - 0.3313G + 0.5B \\ Cr = 128 + 0.5R - 0.4187G - 0.0813B \end{cases}$$

Процесс сокрытия информации в видеофайле



Процесс сокрытия информации в видеофайле



Дискретно косинусное преобразование

Прямое:
$$F_{\text{DCT}}[x, y] = \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} a(u)a(v)F[x, y] \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N}$$

Обратное:
$$F[u, v] = a(u)a(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} F_{\text{DCT}}[x, y] \cos \frac{(2x+1)u\pi}{2N} \cos \frac{(2y+1)v\pi}{2N}$$

$[u_0, v_0]$	$[u_0, v_1]$	$[u_0, v_2]$	$[u_0, v_3]$	$[u_0, v_4]$	$[u_0, v_5]$	$[u_0, v_6]$	$[u_0, v_7]$
$[u_1, v_0]$	$[u_1, v_1]$	$[u_1, v_2]$	$[u_1, v_3]$	$[u_1, v_4]$	$[u_1, v_5]$	$[u_1, v_6]$	$[u_1, v_7]$
$[u_2, v_0]$	$[u_2, v_1]$	$[u_2, v_2]$	$[u_2, v_3]$	$[u_2, v_4]$	$[u_2, v_5]$	$[u_2, v_6]$	$[u_2, v_7]$
$[u_3, v_0]$	$[u_3, v_1]$	$[u_3, v_2]$	$[u_3, v_3]$	$[u_3, v_4]$	$[u_3, v_5]$	$[u_3, v_6]$	$[u_3, v_7]$
$[u_4, v_0]$	$[u_4, v_1]$	$[u_4, v_2]$	$[u_4, v_3]$	$[u_4, v_4]$	$[u_4, v_5]$	$[u_4, v_6]$	$[u_4, v_7]$
$[u_5, v_0]$	$[u_5, v_1]$	$[u_5, v_2]$	$[u_5, v_3]$	$[u_5, v_4]$	$[u_5, v_5]$	$[u_5, v_6]$	$[u_5, v_7]$
$[u_6, v_0]$	$[u_6, v_1]$	$[u_6, v_2]$	$[u_6, v_3]$	$[u_6, v_4]$	$[u_6, v_5]$	$[u_6, v_6]$	$[u_6, v_7]$
$[u_7, v_0]$	$[u_7, v_1]$	$[u_7, v_2]$	$[u_7, v_3]$	$[u_7, v_4]$	$[u_7, v_5]$	$[u_7, v_6]$	$[u_7, v_7]$

Коэффициенты:

Низкочастотные

Среднечастотные

Высокочастотные

	1	2	3	4	5	6	7	8
1	1603	203	11	45	-30	-14	-14	-7
2	108	-93	10	49	27	6	8	2
3	-42	-20	-6	16	17	9	3	2
4	56	69	7	-25	-10	-5	-2	-2
5	-33	-21	17	8	3	-4	-5	3
6	-16	-14	8	2	-4	-2	1	1
7	0	-5	-6	-1	2	3	0	1
8	9	5	-6	-9	0	3	3	1

	- НЧ компоненты;
	- СЧ компоненты;
	- ВЧ компоненты

Процесс сокрытия информации в видеофайле



Квантование коэффициентов

Блок коэффициентов ДКП

1104	-6	-24	15	-14	0	0	0
-108	-8	4	0	8	0	0	0
8	16	20	7	1	0	0	0
24	10	0	9	0	1	0	0
10	35	0	0	0	0	0	0
7	-11	17	0	24	0	0	1
15	0	0	0	0	0	0	0
0	0	0	1	0	1	0	0

÷

Матрица квантования

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

=

Блок квантованных
коэффициентов

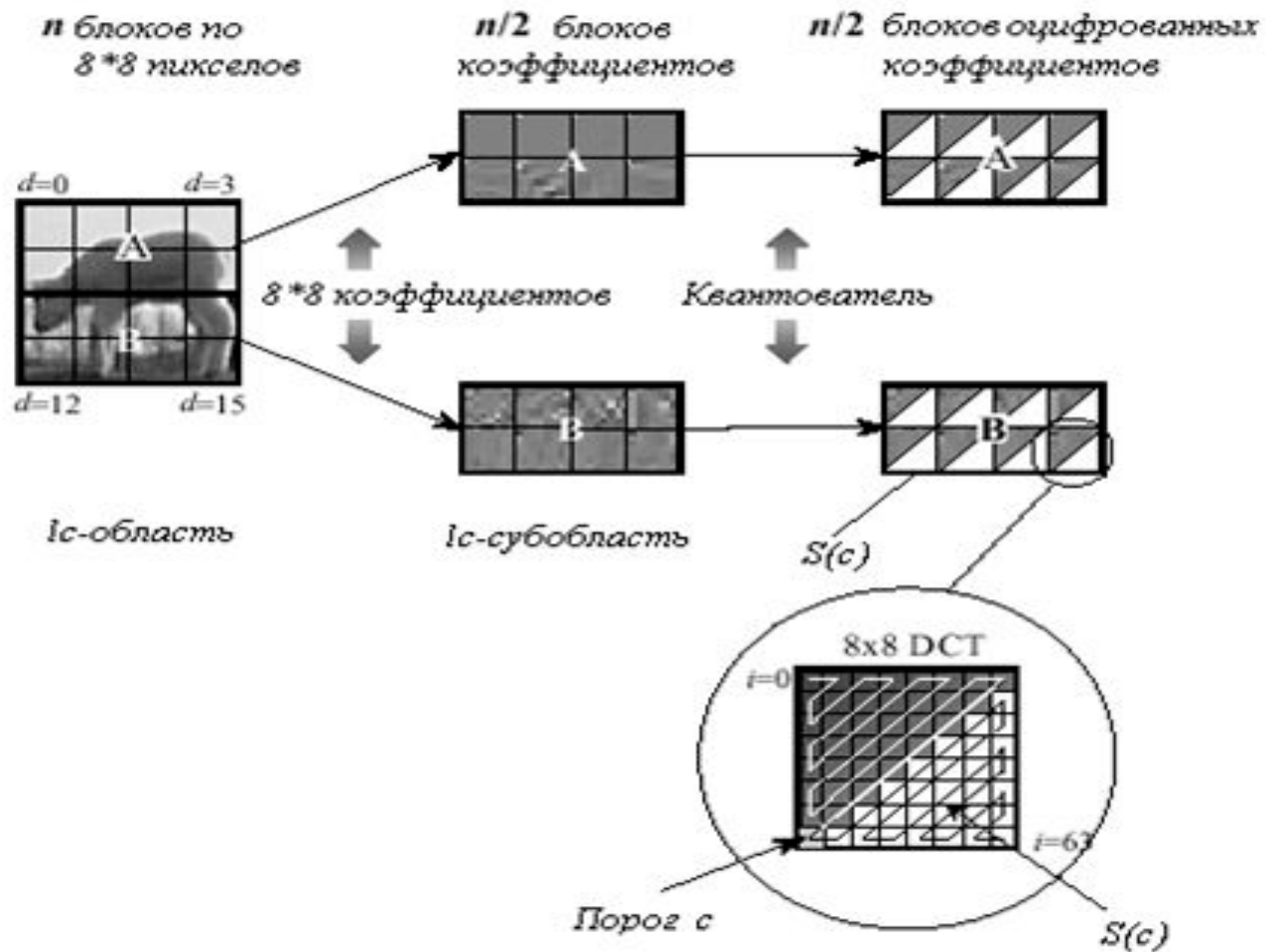
69	-1	-2	1	-1	0	0	0
-9	-1	0	0	0	0	0	0
1	1	1	0	0	0	0	0
2	1	0	0	0	0	0	0
1	2	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

*Коэффициенты почленно делятся на значения матрицы квантования и округляются.
Здесь используется стандартная матрица, приведенная в спецификации JPEG.*

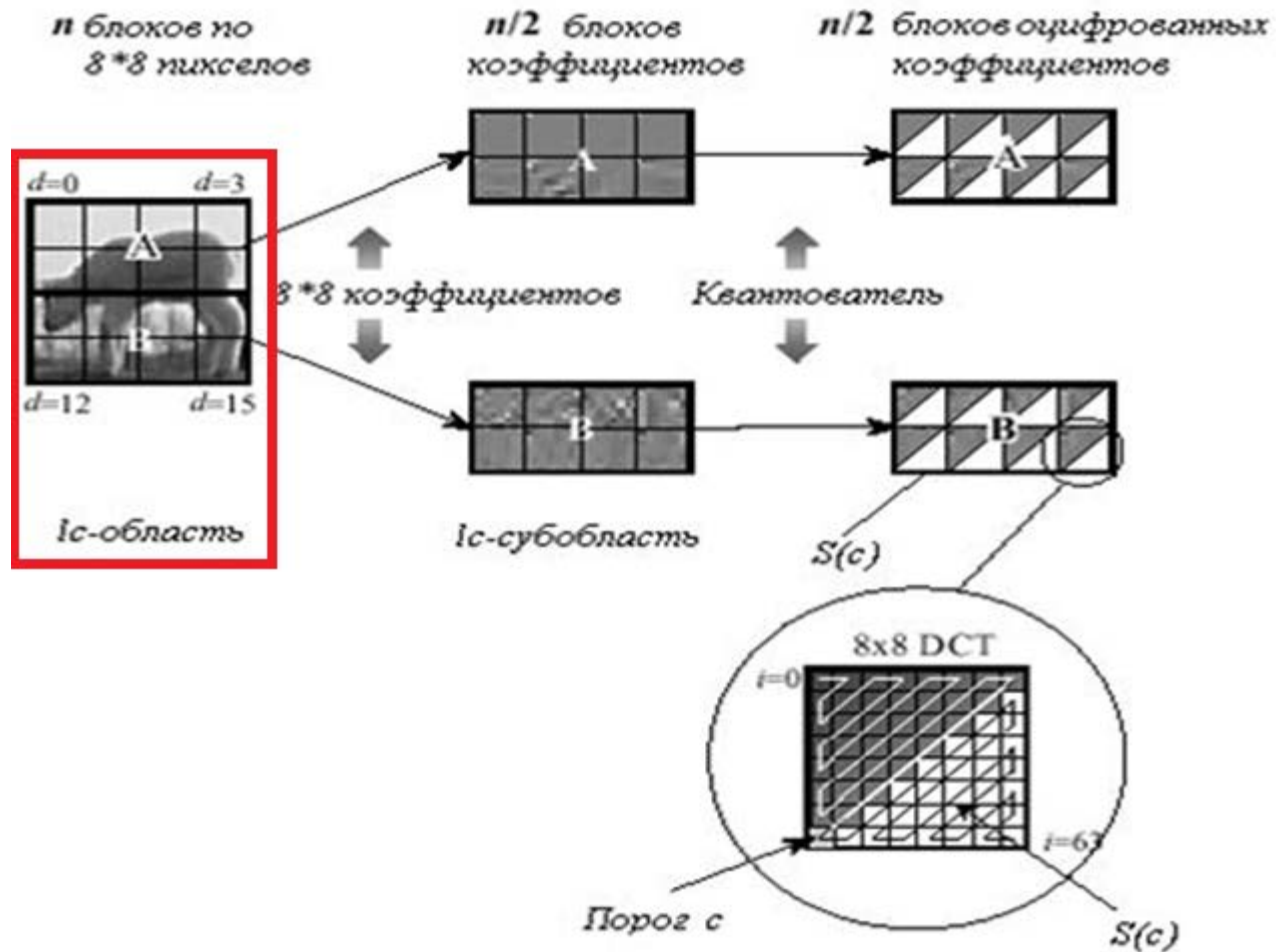
Процесс сокрытия информации в видеофайле



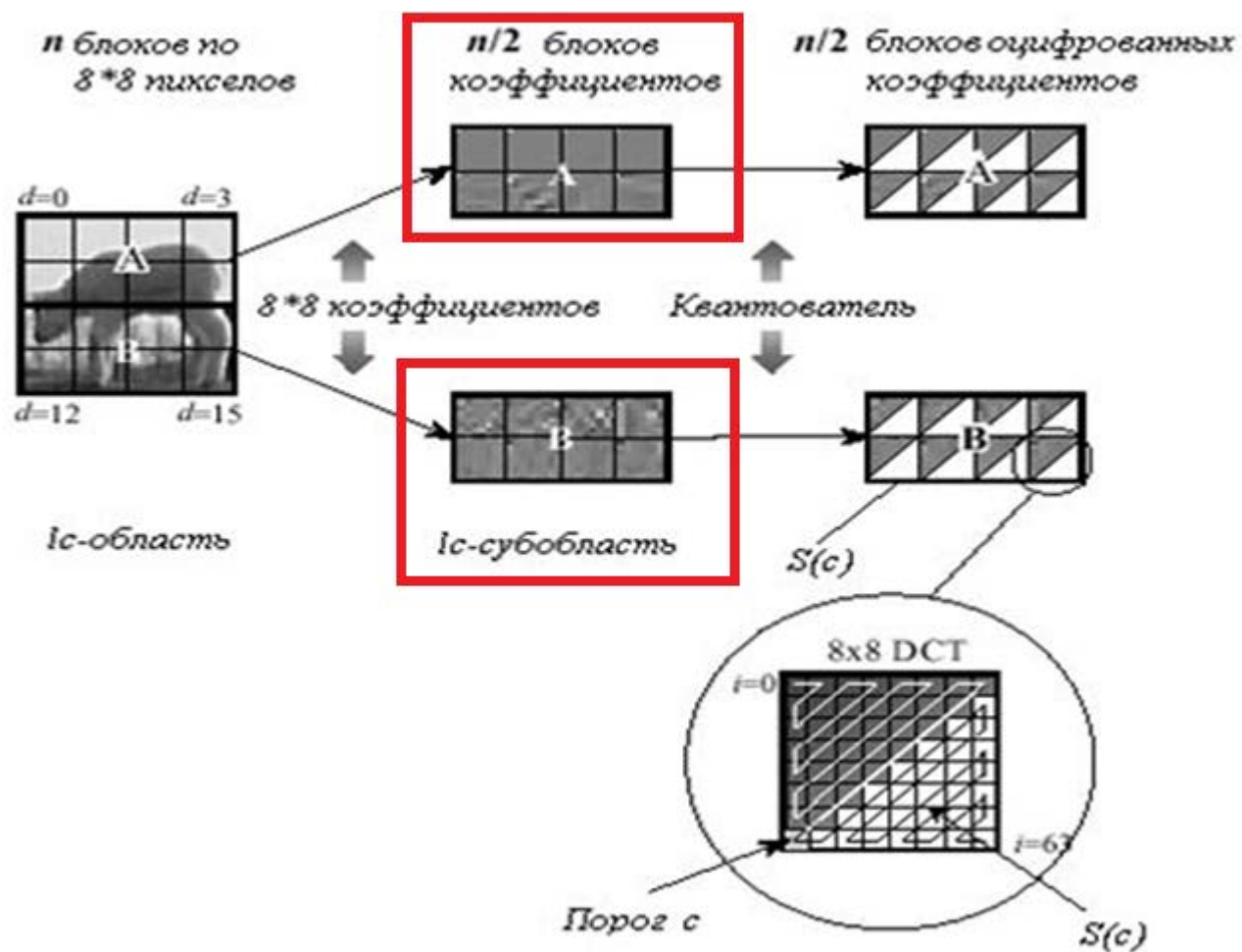
Встраивание данных



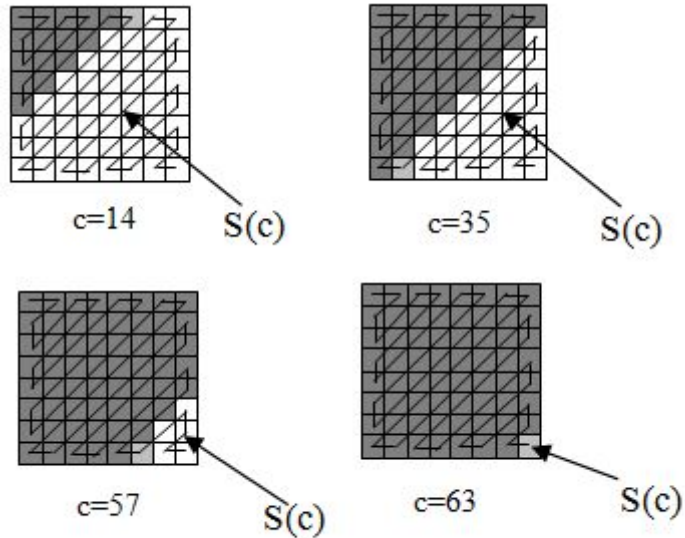
Встраивание данных



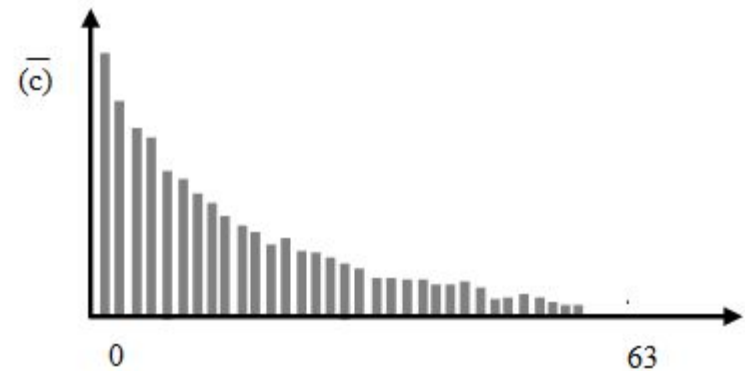
Встраивание данных



Зависимость энергий от размера подмножества $S(c)$

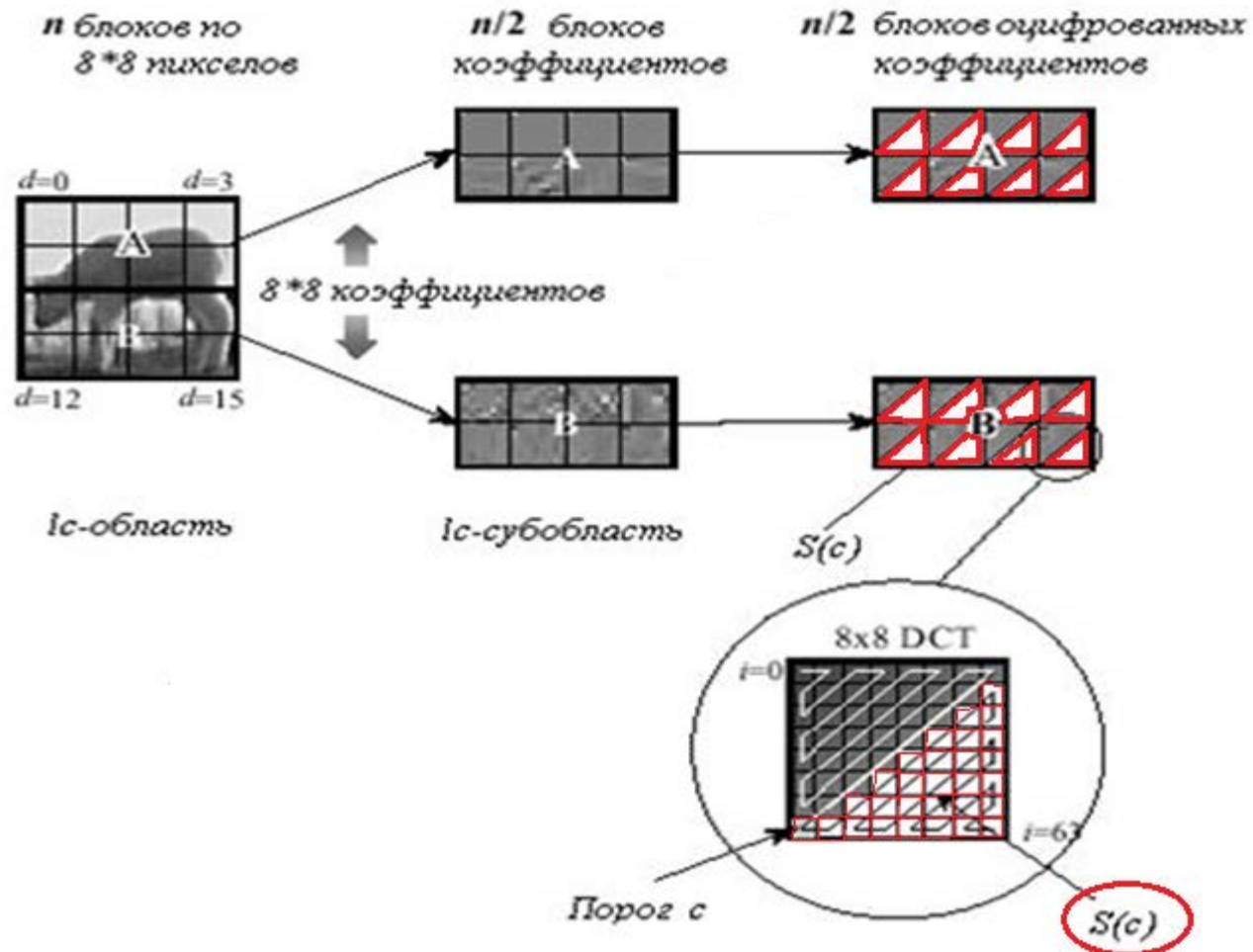


(а) Подмножества, определяемые индексом среза



(б) Зависимость "энергий" субобластей от индексов среза

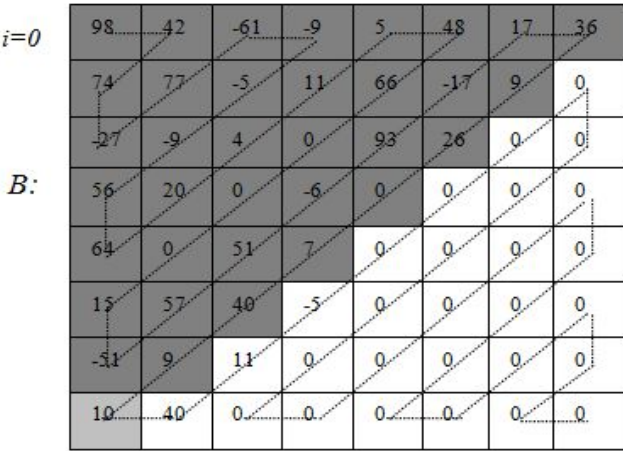
Встраивание данных



Встраивание бита в 1с-область, состоящую из n = 2 блоков ДКП



$E_A(0)=59930$
 $E_A(1)=58906$
 $E_A(35)=725>D=500$
 $E_A(36)=100$
 $E_A(37)=0$
 $E_A(63)=0$



$E_B(35)=1846$
 $E_B(36)=725>D=500$
 $E_B(37)=146$
 $E_B(38)=25$
 $E_B(39)=0$
 $E_B(63)=0$



Полная процедура встраивания водяного знака:

Шаг 1. Перемешивание блоков 8x8 коэффициентов изображения псевдослучайным образом.

Шаг 2. Для каждого бита

водяного знака выполнить:

- а) выбор 1с-подобласти А, состоящей из $n/2$ блоков 8x8 коэффициентов ДКП;
- б) выбор 1с-подобласти В, состоящей из оставшихся $n/2$ блоков 8x8 коэффициентов ДКП;
- в) расчет значения порога c :

$$c(n, Q_{jpeg}, D, c_{min}) = \max \{c_{min}, \max\{g \in \{1,63\} \mid (E_A(g, n, Q_{jpeg}) > D) \wedge (E_B(g, n, Q_{jpeg}) > D)\}\}$$

где

$$E_{A,B}(c, n, Q_{jpeg}) = \sum_{d=0}^{n/2-1} \sum_{i \in S(c)} ([\theta_{i,d}] Q_{jpeg})^2;$$

г) если $b_i = 0$, то удаление коэффициентов подмножества $S(c)$ области А;

д) иначе, если $b_i = 1$, то удаление коэффициентов подмножества $S(c)$ области В.

Шаг 3. Растановка всех блоков ДКП коэффициентов по своим начальным позициям.

Полная процедура извлечения водяного знака:

Шаг 1. Перемешивание блоков 8x8 коэффициентов изображения псевдослучайным образом.

Шаг 2. Для каждого бита

водяного знака выполнить:

- а) выбор 1с-подобласти А, состоящей из $n/2$ блоков 8x8 коэффициентов ДКП;
- б) выбор 1с-подобласти В, состоящей из оставшихся $n/2$ блоков 8x8 коэффициентов ДКП;
- в) расчет значения порога c :

$$c(n, Q_{jpeg}, D, c_{min}) = \max \{c_{min}, \max \{g \in \{1, 63\} \mid (E_A(g, n, Q_{jpeg}) > D) \wedge (E_B(g, n, Q_{jpeg}) > D)\}\}$$

где

$$E_{A,B}(c, n, Q_{jpeg}) = \sum_{d=0}^{n/2-1} \sum_{i \in S(c)} ([\theta_{i,d}] Q_{jpeg})^2;$$

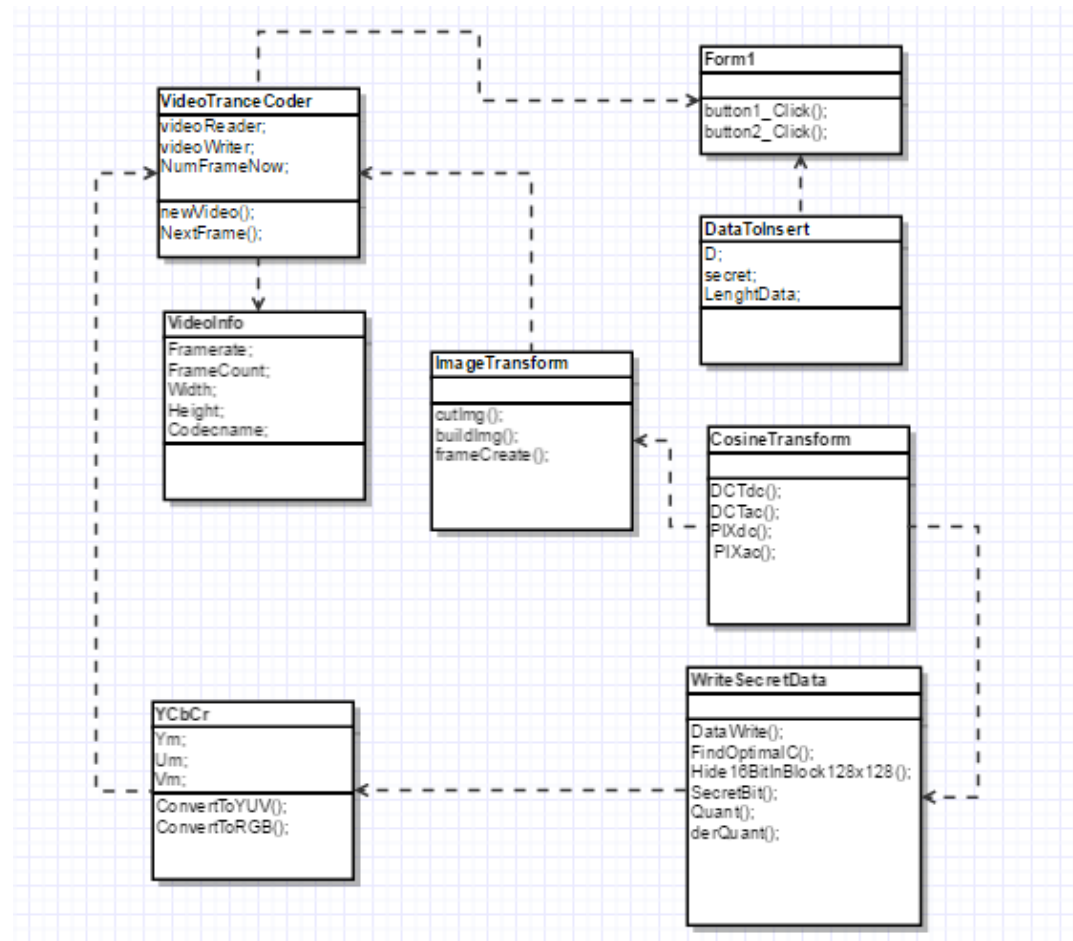
- г) расчет разности энергий:

$$D = E_A(c^{extract}, n, Q'_{jpeg} Q_{jpeg}) - E_B(c^{extract}, n, Q'_{jpeg} Q_{jpeg});$$

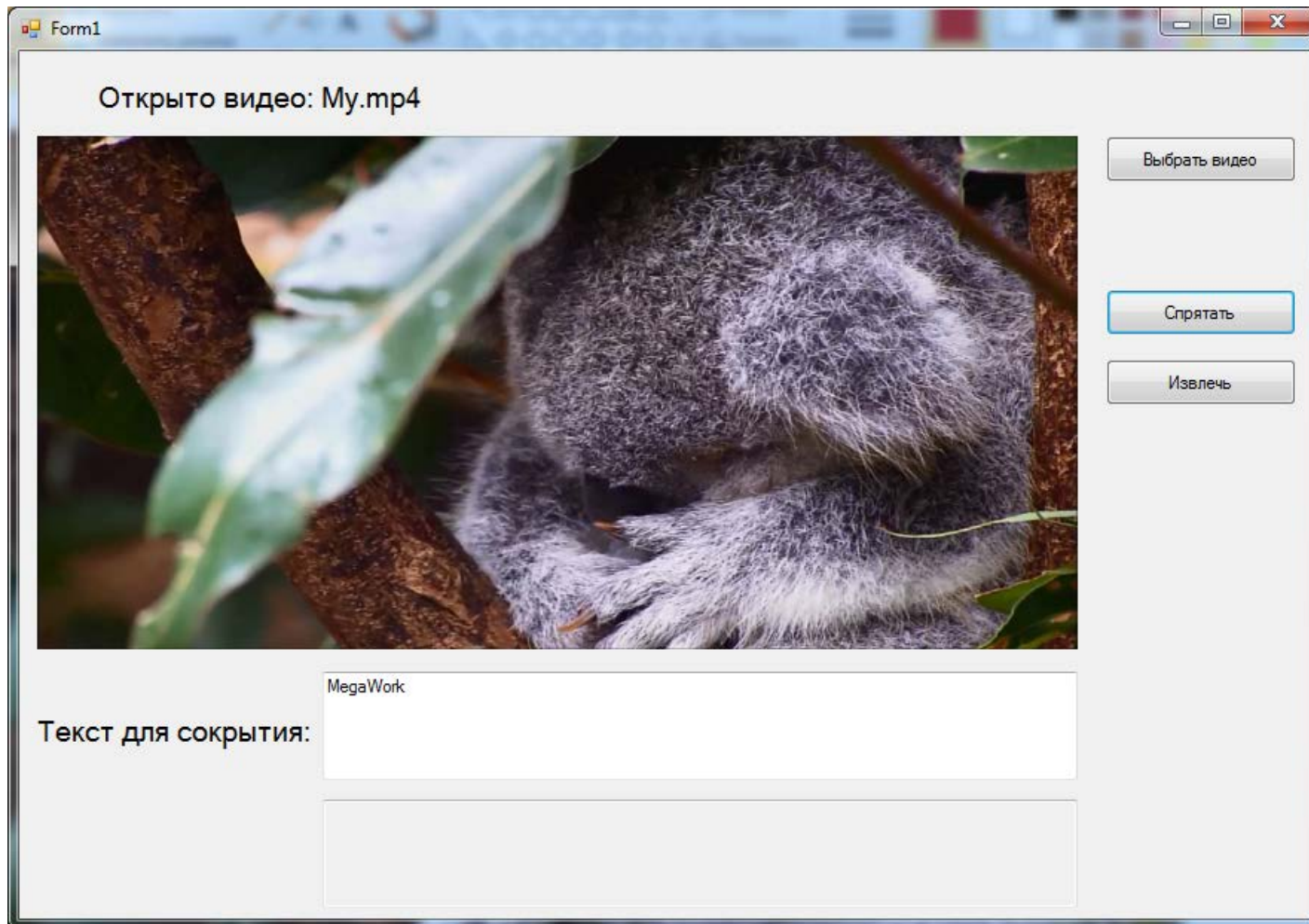
- д) если $D > 0$, то $b_i = 1$, иначе $b_i = 0$

Архитектура ПО

- VideoTranscoder.cs
- VideoInfo.cs
- WriteSecretData.cs
- Form1.cs
- CosineTransform.cs
- ImageTrasnform.cs
- YCbCr.cs
- DataToInsert.cs



Интерфейс приложения



Заключение

- ❖ **Проведено исследование принципов реализации механизмов сокрытия данных в видеофайлах с помощью стеганографии;**
- ❖ **Разработана математическая модель внедрения информации в видеоряд;**
- ❖ **Разработан программный комплекс для сокрытия информации в видеоряде;**

Спасибо за внимание!