

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
**«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»**
(Н И У « Б е л Г У »)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ
СИСТЕМ И ТЕХНОЛОГИЙ

**РАЗРАБОТКА МЕТОДА И АЛГОРИТМА СКРЫТОГО КОДИРОВАНИЯ
РЕЧЕВОГО СИГНАЛА В ИЗОБРАЖЕНИИ**

Выпускная квалификационная работа
обучающегося по направлению подготовки 11.03.02 Инфокоммуникационные
технологии и системы связи
очной формы обучения, группы 07001410
Мишиной Ольги Олеговны

Научный руководитель
ст. преп. кафедры
Информационно-
телекоммуникационных
систем и технологий
НИУ «БелГУ» Лихолоб П.Г.

Рецензент
начальник отдела
серийного сопровождения
АО НПП «СПЕЦ-РАДИО»,
к.ф.-м.н Туяков С.В.

БЕЛГОРОД 2018

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
**БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**
(НИУ «БелГУ»)

ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
Направление подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
Профиль: «Сети связи и системы коммутации»

Утверждаю
Зав. кафедрой 
« 19 »  2018 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Мишина Ольга Олеговна
(фамилия, имя, отчество)

1. Тема ВКР «Разработка метода и алгоритма скрытного кодирования речевого сигнала в изображении»

Утверждена приказом по университету от « 23 » апреля 2018 г. № 2169-УР

2. Срок сдачи студентом законченной работы 09.06.2018

3. Исходные данные:

Объект исследования – метод скрытного кодирования информации.

Предмет исследования – процедуры, обеспечивающие скрытность речевого сигнала в синтезированном изображении.

Цель работы: разработка алгоритма скрытного кодирования/декодирования речевого сигнала в изображение.





4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов):

- 4.1. Анализ методов скрытного кодирования информации в изображениях;
- 4.2. Разработка решающих процедур анализа/синтеза изображений и алгоритмов их реализующих;
- 4.3. Разработка прототипа программной поддержки и оценка работоспособности предложенных решений;
- 4.4. Экономическое обоснование результатов исследования.

5. Перечень графического материала (с точным указанием обязательных иллюстраций):

- 5.1. Математическая модель скрытного кодирования речевого сигнала в изображении;
- 5.2. Модели принятия решений при обработке изображений (А1, лист 1);
- 5.3. Алгоритм скрытного кодирования речевого сигнала в изображении (А1, лист 1);
- 5.4. Оценка скрытности и вероятности обнаружения скрытной информации в изображении (А1, лист 1);
- 5.5. Технико-экономическое обоснование разработки.

6. Консультанты по работе с указанием относящихся к ним разделов

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
4.1. – 4.3	Старший преподаватель каф. ИТСиТ Лихолоб П.Г.		
4.4	канд. техн. наук старший преподаватель каф. ИТСиТ Болдышев А.В.		

7. Дата выдачи задания 30.04.2018

Руководитель

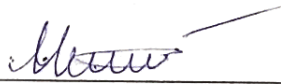
Старший преподаватель
кафедры «Информационно-телекоммуникационных
систем и технологий»
НИУ «БелГУ»



П.Г. Лихолоб

(подпись)

Задание принял к исполнению



(подпись)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	6
1 МЕТОДЫ СКРЫТНОГО КОДИРОВАНИЯ	7
1.1 Подходы представления информации в виде цифровых кодов	8
Цифровая модель речевого сигнала	8
Цифровая модель изображения	10
1.2 Стеганографические методы кодирования.....	11
Метод наименее значащего бита	11
Метод расширения спектра.....	13
Метод Коха-Жао.....	13
1.3 Методы оценки работоспособности стеганографических методов кодирования	15
1.4 Постановка задач исследования	16
2 ФОРМИРОВАНИЕ МЕТОДОВ СКРЫТНОГО ВНЕДРЕНИЯ.....	19
2.1 Методы анализа/синтеза изображения	19
2.2 Описание моделей принятия решений при обработке изображений	22
2.3 Разработка алгоритмов скрытного внедрения	24
2.4 Основные результаты и выводы по главе.....	29
3 ПРОТОТИП И ОЦЕНКИ ЕГО РАБОТОСПОСОБНОСТИ.....	30
3.1 Построение архитектуры прототипа.....	30
3.2 План оценки работоспособности.....	34
3.3 Результаты экспериментальной оценки работоспособности	35
3.4 Основные результаты и выводы	39

11070006.11.03.02.436.ПЗВКР

	№ докум.	Подпись		Лист	Лист	Листов
Разработал	Мишина О.О.		Разработка метода и алгоритма скрытного кодирования речевого сигнала в изображении			
Проверил	Лихолоб П. Г.					
Рецензент	Тюяков С.В.					
Н. Контроль	Лихолоб П. Г.					
Утвердил	Жуляков Е. Г.					
					2	
				НИУ «БелГУ» гр.07001410		

4 ЭКОНОМИЧЕСКА ОЦЕНКА РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ	30
4.1 Планирование работ по исследованию	30
4.2 Расчет финансовых затрат на оплату труда и исследование	34
4.3 Расчет продолжительности исследования.....	35
4.4 Расчет финансовых затрат на расходные материалы	35
4.5 Составление схемы расходов на исследование.....	35
ЗАКЛЮЧЕНИЕ	48
ПРИЛОЖЕНИЕ А	50
ПРИЛОЖЕНИЕ Б.....	58
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	60

Изм.	Лист	№ докум.	Подпись	Дата

11070006.11.03.02.436.ПЗВКР

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

LSB	–	абривиатура стеганографического метода наименее значащего бита
DCT	–	Дискретно-косинусное преобразование
SNR	–	соотношение сигнал/шум
MSE	–	среднеквадратическая ошибка
IF	–	качество изображения
NC	–	нормированная взаимная корреляция
$\ \cdot\ $	–	энергия фрагмента
ρ	–	коэффициент корреляции
\vec{e}	–	вектор данных
$f_{m,k}$	–	пиксель исходного изображения
$\tilde{f}_{m,k}$	–	пиксель синтезированного изображения содержащего дополнительную информацию
\tilde{F}	–	блок синтезированного изображения
$\phi_{i,j}$	–	коэффициенты ортогонального базиса
D	–	базис представленный в виде двухмерного блока
Φ	–	блок коэффициентов дискретного-косинусного преобразования
j	–	индекс дискретной пространственной частоты по столбцам
i	–	индекс дискретной пространственной частоты по строкам
ω_i, ω_j	–	пространственные частоты
$\mathbb{E}[\cdot]$	–	оператор математического ожидания
K	–	количество пикселей в строке изображения
M	–	количество пикселей в столбце изображения
PC	–	речевой сигнал (дополнительная информация)
\vec{x}	–	отрезок речевого сигнала
\vec{y}	–	восстановленный отрезок речевого сигнала

- B – разрядность речевого сигнала
- b – значение речевого сигнала
- $\frac{h}{m}$ – значение разрядности изображения
- ν_D – частота дискретизации
- x_t – мгновенное значение амплитуды речевого сигнала
- N – размерность вектора

					<i>11070006.11.03.02.436.ПЗВКР</i>	5
Изм.	Лист	№ докум.	Подпись	Дата		

ВВЕДЕНИЕ

В связи с постоянно увеличивающимися объемами информации, представленной в цифровом виде, возникает необходимость в быстром простом способе её описания. Различные государственные учреждения, музеи, частные компании и т.д. имеют большие объемы информации, хранящиеся на бумажных носителях. Для упрощения документы подвергаются переводу в электронный вид, оцифровыванию (сканированию). В некоторых случаях это могут быть изображения или снимки, к которым и прилагается описание.

Наиболее простой и быстрый способ – это сформировать информацию о изображении в виде речевого сообщения, что может привести к увеличению объема хранимой информации о документе.

Естественно, целесообразно чтобы объем данных о документе представленный в виде изображения был минимален. Для того чтобы оптимизировать работу с базами данных и уменьшить объемы хранимых данных, предлагается использовать методы стеганографического кодирования. Под оптимизацией тут понимается неизменность объема памяти выделенной на документ (изображение).

Так как предполагается кодирование информации, об изображении внутри самого изображения, то это приведет к тому, что объем памяти, занимаемый изображением и информацией о нем, не изменится.

Цель работы: разработка алгоритма скрытного кодирования/декодирования речевого сигнала в изображении.

Объект исследования – изображение.

Предмет исследования – методы, обеспечивающие скрытность речевого сигнала в синтезированном изображении.

В работе рассматриваются вопросы относящиеся к скрытности внедренной методами стеганографии информации и возможности её восстановления.

					<i>11070006.11.03.02.436.ПЗВКР</i>	6
Изм.	Лист	№ докум.	Подпись	Дата		

1 МЕТОДЫ СКРЫТНОГО КОДИРОВАНИЯ

Информация в электронном виде загружается в базы данных для более удобного хранения и использования. Если помещать изображения в базы данных отдельно от описания, информация может теряться, искажаться, а также будет занимать большой объем памяти. Введение электронного документооборота, подразумевает обработку документов не только в текстовом виде, но и в виде изображений. При этом возникает задача сортировки и защиты документации, решаемая посредством кодирования в структуре документа дополнительной информации. В связи с этим в работе предполагается использовать терминологию принятую в стеганографии [5-8, 35, 44, 46]. Методы стеганографии (скрытного кодирования) базируются на основных понятиях, таких как:

Скрытность информации обуславливается степенью ее маскировки по отношению к остальным данным, а также определяет способность информации сопротивляться рассекречиванию смысла информационного массива, выявлению состава сохраняемого информационного массива или правообладателя передаваемого информационного массива, определение факта передачи информационного массива.

Кодирование информации различного вида данных обуславливается изменением речевого сигнала из формы, приемлемой для непосредственного применения данных, в форму, позволяющую обрабатывать, передавать и хранить данные.

Под речевыми сигналами принято понимать электрические колебания, регистрируемые на выходе микрофона под воздействием акустических волн, порождаемых речевым аппаратом человека [38-40].

Цифровым изображением называют результат регистрации датчиками светового потока [5, 52].

11070006.11.03.02.436.ПЗВКР

7

В цифровых системах СИ монохромными называются изображения, при воспроизведении которых используются только два базовых цвета (чаще всего - черный и белый), образующие различные оттенки за счет смешения в разных пропорциях.

Контейнер – блок данных фиксированной размерности с заранее известными характеристиками и свойствами [5, 44, 46].

Стегоконтейнер – синтезированный блок данных содержащий дополнительную информацию [5, 44, 46].

Дополнительная информация – последовательность бит содержащая сведения об объекте [41, 46, 47]. Далее в работе под дополнительной информацией будем понимать фрагмент речевого сигнала.

1.1 Подходы представления информации в виде цифровых кодов

Цифровая модель речевого сигнала

Цифровая обработка речевого сигнала предполагает приведение аналогового сигнала к цифровому виду. Для выполнения преобразования используются аналого-цифровые преобразователи (АЦП), которые имеют собственные характеристик, такие как:

1. Частота дискретизации $\nu_d (\nu_d = 1/\Delta t)$.
2. Разрядность B .

В следствии аналогово-цифрового преобразований непрерывный сигнал преобразуется в ряд дискретных отсчетов, представляющих из себя целое число, описывающее аналоговый сигнал в данной точке.

Разбиение речевого сигнала на отдельные отсчеты принято называть дискретизацией сигнала, а частотой дискретизации ν_d , называют число отсчетов зафиксированных за секунду. Частота дискретизации по теореме Котельникова обязана быть в два раза больше максимальной частоты в спектре сигнала [13, 27, 33, 38-40, 43, 52].

					11070006.11.03.02.436.ПЗВКР	8
Изм.	Лист	№ докум.	Подпись	Дата		

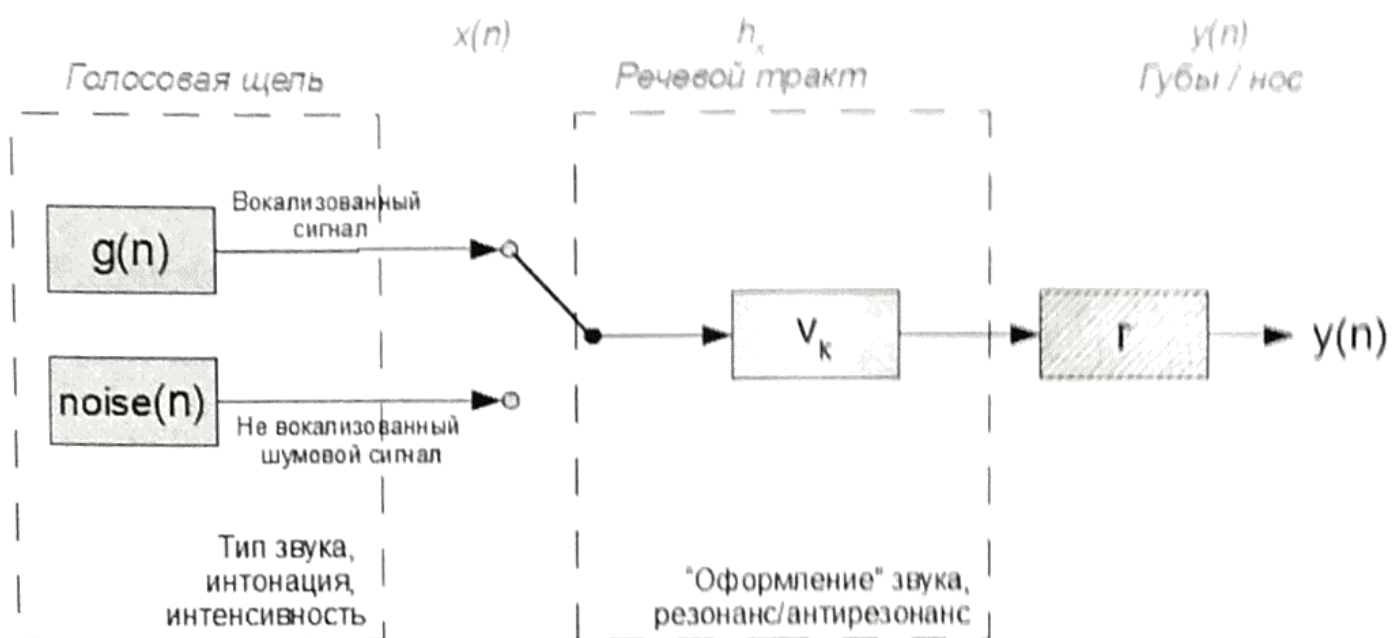


Рисунок 1.1 – Модель формирования речевого сигнала

Под отрезком сигнала будет пониматься вектор:

$$\vec{x} = (x_1, x_2, \dots, x_n, \dots, x_N)^T, \quad (1.1)$$

где x_n – текущий отсчет, $x_n \in (-1; 1)$; N – размерность вектора; T – знак транспонирования.

Метод поразрядного кодирования [43, 57] (поразрядного взвешивания) имеет в своем составе несколько эталонов, равных по величине степеням двойки, и данные эталоны сравниваются с изначальным сигналом. Первым сравнивается эталон старшего разряда. Благодаря этому сравнению образуется старший разряд кода на выходе. Если при сравнении оказывается что эталон больше входной величины, в этом случае в старшем разряде ставится ноль и дальше выполняется упорядочивание входной величины следующим по значению эталоном. А в случае если эталон окажется меньше входной величины или будет равен ей, в старшем разряде ставится единица и в последствии нужно произвести упорядочивание разности между первичным эталоном и величиной подаваемой на вход:

$$f_{i,k} = \sum_{\substack{b=1 \\ b \neq h}}^{B-1} W_b \cdot 2^{b-1} + W_h \cdot 2^h, \quad (1.2)$$

где W_h – внедряемый бит $W_h \in \{0; 1\}$; B – разрядность.

Цифровая модель изображения

Числовые массивы используются для обработки изображений [34] и создания алгоритмов. Матрицу размерностью $[M \times N]$ можно представить следующим соотношением:

$$\mathbf{F} = \begin{bmatrix} f_{1,1} & f_{1,2} & \dots & f_{1,M} \\ f_{2,1} & f_{2,2} & \dots & f_{2,M} \\ \vdots & \vdots & & \vdots \\ f_{N,1} & f_{N,2} & \dots & f_{N,M} \end{bmatrix}, \quad (1.3)$$

где \mathbf{F} – изображение; $f_{m,k}$ – пиксель изображения.

Данное равенство состоит из двух частей, которые являются равносильными способами количественного описания цифрового изображения. Правая часть представляет из себя матрицу действительных чисел. Все составляющие матрицы определяются элементом $f_{m,k}$ цифрового изображения или пикселем.

Монохромная модель [34]

Монохромным является изображение, для создания которого используются цвета, образующиеся в следствии смешивания в различных пропорциях пары базовых цветов. Промежуточные цвета по отношению к основным цветам монохромной модели, принято называть оттенками. Отличие оттенков друг от друга заключается в процентном содержании в них базовых цветов. Обычно, в наименовании оттенка указывают содержание только одного базового цвета. То есть, если базовым цветом переднего плана выбран черный, а в качестве фонового – белый.

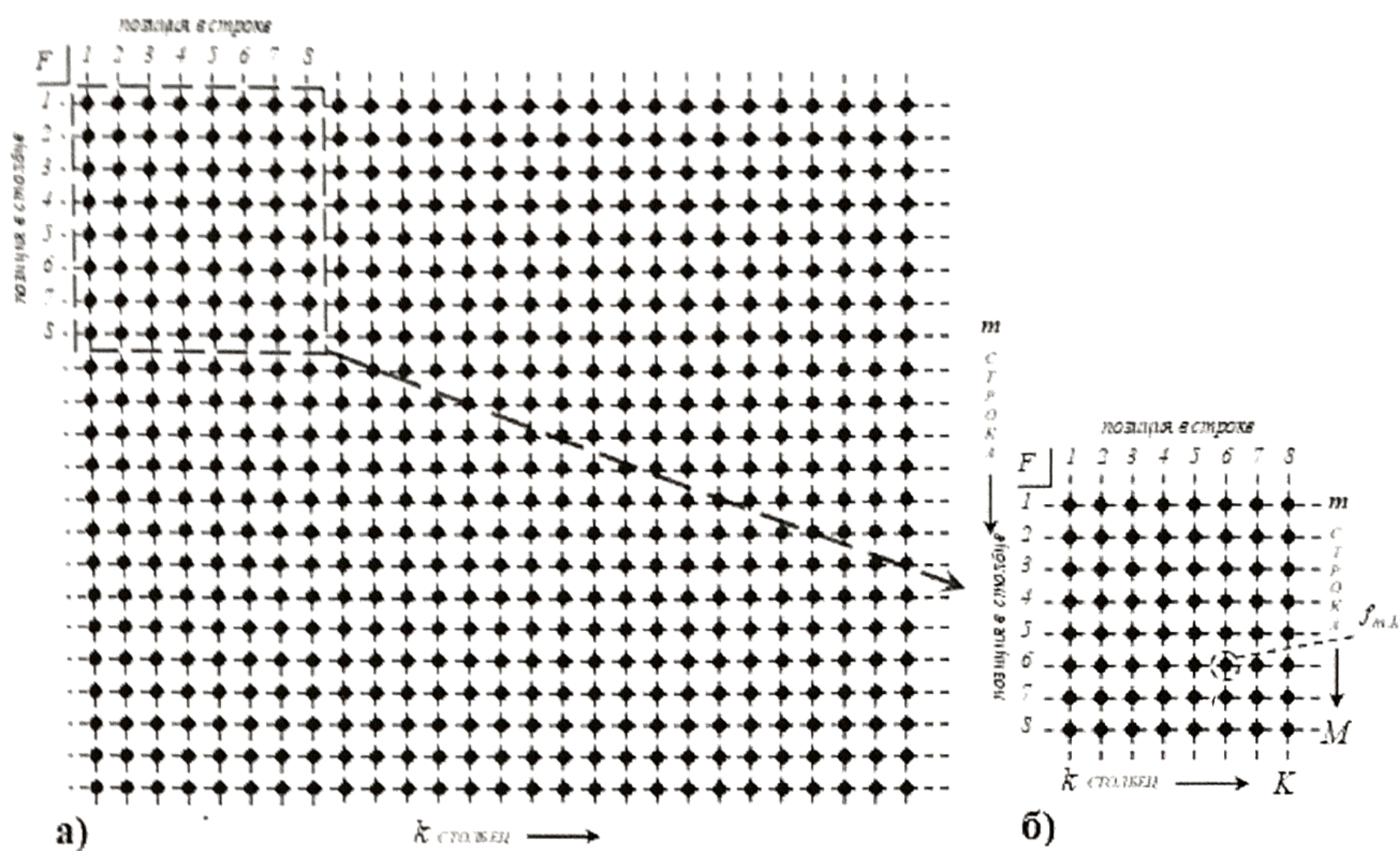


Рисунок 1.2 – Пространственная модель изображения

а) изображение; б) фрагмент изображения

Необходимо отметить, что для преобразований в частотную область достаточно часто используют фрагмент размерностью $[8 \times 8]$, модель которого приведена на рисунке (1.2 б))

1.2 Стеганографические методы кодирования

Метод наименее значащего бита

Метод наименее значащего бита [5, 6, 9, 44, 46] наиболее часто используется среди методов скрытного кодирования в пространственной области. Старший бит в пикселе который несет в себе меньше всего информации принято называть наименее значащий бит (рис. 1.3).

Метод расширения спектра

Модуляция методом расширения спектра (прямой последовательностью) [5-8, 15-17, 44, 46] производится следующим образом, отдельно каждый бит e_n преобразуется в некоторую базисную функцию \mathbf{U} размерностью $[M \times N]$, посредством умножения, в зависимости от того какое значение имеет бит внедряемой информации («1» или «0»), то есть e_n принимает значение «+1» или «-1».

$$\mathbf{F} = \mathbf{F} + e_n \cdot \mathbf{U} \cdot \alpha, \quad (1.5)$$

где \mathbf{U} – матрица ПСП вида; α – коэффициент пропорциональности

$$\mathbf{U} = \begin{pmatrix} -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}. \quad (1.6)$$

Сообщение прошедшее модуляцию и нормировку, попиксельно складывается с одной из цветных матриц исходного изображения [44, 46]. Результатом является стеганоизображение (изображение с закодированной информацией).

Главным преимуществом данного метода является относительно высокая стойкость к всевозможным преобразованиям проводимым над изображением. Метод позволяет закодировать один бит информации в одном блоке изображения.

Несовершенством метода является необходимость хранения ПСП. А так же в этом методе искажения проявляются в виде дробных шумов.

Метод Коха-Жао

Идея метода Коха-Жао [1, 5, 21, 44, 46], заключается в том, что изображение разбивается на блоки \mathbf{F} размером $[8 \times 8]$ пикселей. Далее операция кодирования рассматривается относительно блока \mathbf{F} . К блоку применяется

дискретно-косинусное преобразование (ДКП) [1] в результате чего получается матрица размером $[8 \times 8]$ состоящая из коэффициентов ДКП. После чего в каждой матрице кодируется один бит информации путем изменения коэффициентов [1, 44, 46].

$$\tilde{\phi}_{i,j} = \begin{cases} \phi_{i,j} - \mu, & \text{если } e_m = 1 \\ \phi_{i,j} + \mu, & \text{иначе} \end{cases} \quad (1.7)$$

$$\mu = \frac{1}{8} \sum_{i=1}^8 \sum_{o=1}^8 \phi_{i,j} \quad (1.8)$$

В эксперименте для скрывающего кодирования будет использоваться модификация метода Коха-Жао, использующая для кодирования не изменение коэффициента, а инверсию его знака, т.к. в этом случае внедрённая информация будет более стойкой [46].

Достоинством данного стеганографического метода является его способность внесения специфических искажений в произвольный контур, что не затрудняет восприятие информации. При этом, для достижения компромисса между скрытностью и стойкостью, предлагается информацию помещать в блоки с энергией близкой к среднему значению.

Несовершенство метода заключается в том, что при переходе в область коэффициентов ДКП и обратно в результате конечности разрядности представления данных на ЭВМ (операция округления) возникают искажения в пространственной области изображения. Искажения проявляются в виде размытия в модифицируемом блоке, степень искажений зависит от влечения модифицированной частотной компоненты.

1.3 Методы оценки работоспособности стеганографических методов кодирования

Меры и оценки применяемые для выявления изменений в синтезированном изображении относительно исходного:

Среднеквадратическая ошибка (*mean squared error* – MSE), отражает изменение энергии пикселей [5, 6, 44, 46]:

$$\text{MSE} = \frac{1}{K \cdot M} \sum_{m=1}^M \sum_{k=1}^K (f_{k,m} - \tilde{f}_{k,m})^2, \quad (1.9)$$

где $f_{k,m}$ – пиксель исходного изображения; $\tilde{f}_{k,m}$ – пиксель изображения содержащего дополнительную информацию; M – количество пикселей в столбце; K – количество пикселей в строке.

Оценка определяющая порядок изменения энергии синтезированного изображения по отношению к общей энергии (signal-to-noise ratio – SNR) [5, 6, 44, 46]:

$$\text{SNR} = 10 \cdot \log_{10} \frac{255}{\text{MSE}}, \quad (1.10)$$

Коэффициент корреляции (ρ), оценивающий степень схожести двух изображений, по нормированной взаимной энергии этих сигналов [5, 6, 44, 46]:

$$\rho = \frac{\sum_{m=1}^M \sum_{k=1}^N (f_{k,m} - \mathbb{E}[\mathbf{F}]) \sum_{m=1}^M \sum_{k=1}^N (\tilde{f}_{k,m} - \mathbb{E}[\tilde{\mathbf{F}}])}{\sqrt{\sum_{m=1}^M \sum_{k=1}^N (f_{k,m} - \mathbb{E}[\mathbf{F}])^2 \sum_{m=1}^M \sum_{k=1}^N (\tilde{f}_{k,m} - \mathbb{E}[\tilde{\mathbf{F}}])^2}}, \quad (1.11)$$

$$\mathbb{E}[\cdot] = \frac{1}{M \cdot N} \sum_{m=1}^M \sum_{k=1}^N f_{k,m}, \quad (1.12)$$

где $\mathbb{E}[\cdot]$ – математическое ожидание.

Качество изображения (**IF**), [5, 6, 44, 46]:

$$\mathbf{IF} = 1 - \frac{\sum_{m=1}^M \sum_{k=1}^K (f_{k,m} - \tilde{f}_{k,m})^2}{\sum_{m=1}^M \sum_{k=1}^K (f_{k,m})^2}, \quad (1.13)$$

Нормированная взаимная корреляция (**NC**) [5, 6, 44, 46]:

$$\mathbf{NC} = \frac{\sum_{m=1}^M \sum_{k=1}^K (f_{k,m} \cdot \tilde{f}_{k,m})}{\sum_{m=1}^M \sum_{k=1}^K f_{k,m}^2}, \quad (1.14)$$

Под энергией фрагмента изображения будем понимать квадрат евклидовой нормы ($\|\mathbf{F}\|^2$), [5, 6, 44, 46]:

$$\|\mathbf{F}\|^2 = \sum_{m=1}^M \sum_{k=1}^K (f_{k,m})^2. \quad (1.15)$$

Меры и оценки применяемые для выявления изменений восстановленного речевого сигнала относительно исходного [5, 10, 11, 14, 20]. Среднеквадратическая ошибка (MSE) [5, 6, 10, 11, 14, 20]:

$$\text{MSE} = \frac{1}{N} \sum_{i=1}^N (x_i - y_i)^2, \quad (1.16)$$

где x_i – мгновенное значение амплитуды речевого сигнала

Коэффициент корреляции (ρ), оценивающий степень схожести двух сигналов [5, 6, 10, 11, 14, 20, 49]:

Изм.	Лист	№ докум.	Подпись	Дата

$$\rho = \frac{\sum_{n=1}^N (x_n - \mathbb{E}[\vec{x}]) \sum_{n=1}^N (y_n - \mathbb{E}[\vec{y}])}{\sqrt{\sum_{n=1}^N (x_n - \mathbb{E}[\vec{x}])^2 \sum_{n=1}^N (y_n - \mathbb{E}[\vec{y}])^2}}, \quad (1.17)$$

$$\mathbb{E}[\cdot] = \frac{1}{N} \sum_{i=1}^N x_i, \quad (1.18)$$

где $\mathbb{E}[\cdot]$ – математическое ожидание [49].

Отношение сигнал/шум (SNR) – это мера, используемая для сравнения сигнала с фоновым шумом [5, 6, 10, 11, 14, 20].

$$\text{SNR} = 10 \cdot \log_{10} \frac{\|\vec{x}\|^2}{\text{MSE}}, \quad (1.19)$$

где $\|\vec{x}\|^2$ – квадрат евклидовой нормы отрезка речевого сигнала (энергия отрезка):

$$\|\vec{x}\|^2 = \sum_{i=1}^N x_i^2. \quad (1.20)$$

1.4 Постановка задач исследования

В результате анализа методов стеганографии используемых для внедрения информации в изображение было выявлено, что метод наименее значащего бита и метод Коха-Жао обладают наибольшей емкостью.

При этом стоит отметить, что метод наименее значащего бита имеет не высокую стойкость к разрушающим воздействиям по сравнению с рассмотренными методами. Метод Коха-Жао позволяет скрытно поместить объем информации достаточный для скрытия РС, однако для его безошибочного извлечения необходимо осуществить выбор компонент в параметрах которых осуществляется внедрение.

11070006.11.03.02.436.ПЗВКР

17

Поэтому для обеспечения скрытности и стойкости внедряемой информации в виде речевого сигнала необходимо решить следующие задачи:

1. Анализ методов скрытного кодирования информации в изображениях
2. Реализовать процедуры анализа изображений
3. Разработать прототип программной поддержки
4. Разработать алгоритм скрытного кодирования речевого сигнала в изображении
5. Оценить работоспособность разработанных алгоритмов и программной поддержки
6. Выполнить экономическое обоснование результатов исследования

2 ФОРМАЛИЗАЦИЯ МЕТОДОВ СКРЫТНОГО ВНЕДРЕНИЯ

В разделе описан математический аппарат и приведены алгоритмы реализующие внедрение речевого сообщения в изображение методами стеганографии. Также приведено описание для трех наиболее встречаемых в литературных источниках методах стеганографии, таких как: метод наименее значащего бита, метод расширения спектра, метод Коха-Жао.

2.1 Методы анализа/синтеза изображения

При обработке изображений широко используется анализ спектров изображений. Наиболее распространенный способ получения спектра изображения за счет использования прямого двумерного преобразования Фурье [37, 52]:

$$F(\omega_x, \omega_y) = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f(k, m) \exp(-i(\omega_x k + \omega_y m)) dk dm, \quad (2.1)$$

где ω_x, ω_y - пространственные частоты $j = \sqrt{-1}$ мнимая единица.

Функция $\exp(-j \cdot (\omega_x x + \omega_y y))$ при зафиксированных значениях пространственных частот описывает плоскую волну в плоскости изображения (k, m) (рисунок 2.1). Формула (2.1) объединяет вещественную функцию, характеризующая яркость изображения $f(k, m)$ с комплексной функцией частоты – спектром изображения $F(\omega_x, \omega_y)$.

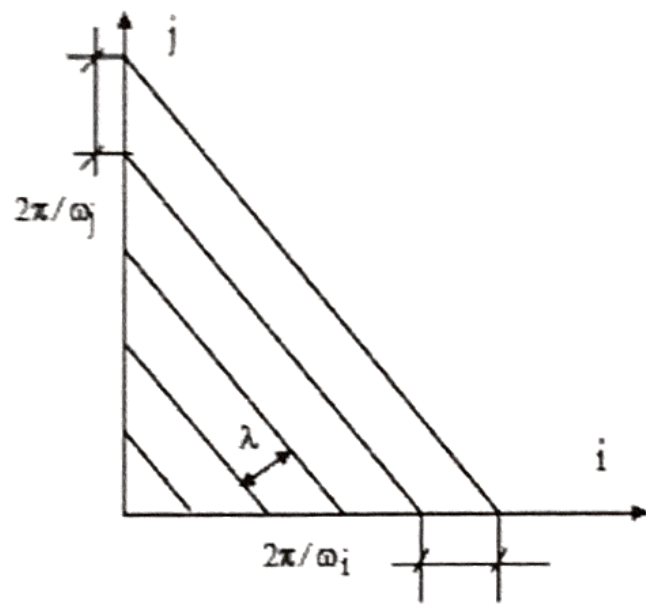


Рисунок 2.1 – Определение пространственных частот изображения

Амплитуда спектра определяются по формуле:

$$F(\omega_v, \omega_j) = \sqrt{Re(\omega_v, \omega_j)^2 + Im(\omega_v, \omega_j)^2} \quad (2.2)$$

где Re – действительная часть числа, Im – мнимая часть комплексного числа

Обратное преобразование Фурье позволяет восстановить изображение по его спектру [37, 52]:

$$f(k, m) = \left(\frac{1}{4}\pi^2\right) \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} F(\omega_v, \omega_j) \exp(-i(\omega_v k + \omega_j m)) d\omega_v d\omega_j \quad (2.3)$$

Спектральная интенсивность изображения характеризует распределение энергии по пространственным частотам. Она определяется как квадрат модуля спектра изображения [37, 52]:

$$S(\omega_v, \omega_j) = Re(\omega_v, \omega_j)^2 + Im(\omega_v, \omega_j)^2 = F^2(\omega_v, \omega_j) \quad (2.4)$$

Для ее названия используются термины спектральная плотность и энергетический спектр. Энергия изображения определяется как интеграл

энергетического спектра по пространственным частотам. В соответствии с теоремой Парсеваля энергия изображения может быть вычислена [37, 52]:

$$\int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f^2(k, m) dk dm = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} |F(\omega_i, \omega_j)|^2 d\omega_i d\omega_j \quad (2.5)$$

Дискретно косинусное преобразование(ДКП)

Рассмотрим еще один из известных методов применяемый для анализа изображения $\mathbf{D} = \{\phi_{i,j}\}$ с коэффициентами вида [1, 18, 37, 52]:

$$\phi_{i,j} = \frac{1}{\sqrt{M \cdot N}} C_i C_j \sum_{m=1}^M \sum_{k=1}^N \cos \left[\frac{\pi(2k+1)i}{2N} \right] \cos \left[\frac{\pi(2m+1)j}{2M} \right], \quad (2.6)$$

где i – шаг дискретной частоты по строкам $i = 1, 2, \dots, M$,

j – шаг дискретной частоты по столбцам $j = 1, 2, \dots, K$ C_i – коэффициенты:

$$C_i = \begin{cases} 1/\sqrt{2}, & i = 1; \\ 1, & i > 0. \end{cases} \quad (2.7)$$

Для получения коэффициентов дискретно-косинусного преобразования (ДКП), принято использовать матричные операции.

$$\Phi = \mathbf{D} \cdot \mathbf{F} \cdot \mathbf{D}^T, \quad (2.8)$$

где \mathbf{F} – блок изображения размера $[M \times N]$, со значениями пикселей $f_{k,m}$;

Φ – блок коэффициентов дискретного-косинусного преобразования, и обратное ДКП:

$$\tilde{\mathbf{F}} = \mathbf{D}^T \cdot \Phi \cdot \mathbf{D}, \quad (2.9)$$

где $\tilde{\mathbf{F}}$ – блок изображения, восстановленного из частотных коэффициентов ДКП.

Ниже на рисунке 2.2, приведена гафическая иллюстрация выделения фрагмента из изображения.

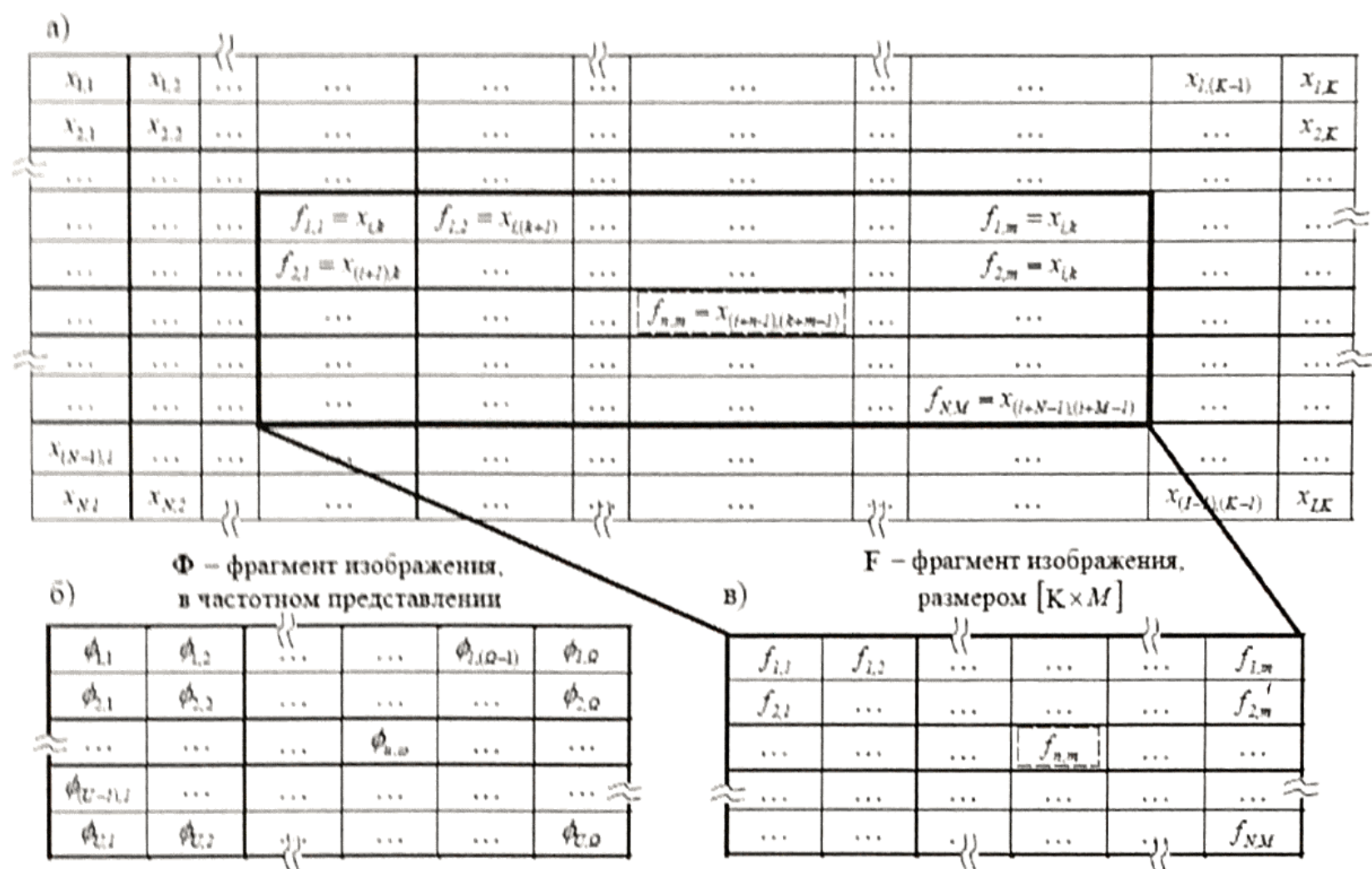


Рисунок 2.2 – Модель матричного представления изображения: а) исходное изображение; б) фрагмент изображения в частотном представлении размером $[M \times K]$; в) фрагмент изображения размером $[M \times K]$

2.2 Описание моделей принятия решений при обработке изображений

Эксперименты приведенные в [6, 46] показали, что в качестве наименее значащего бита могут выступать значения отличные от младшего бита рисунок 2.3.

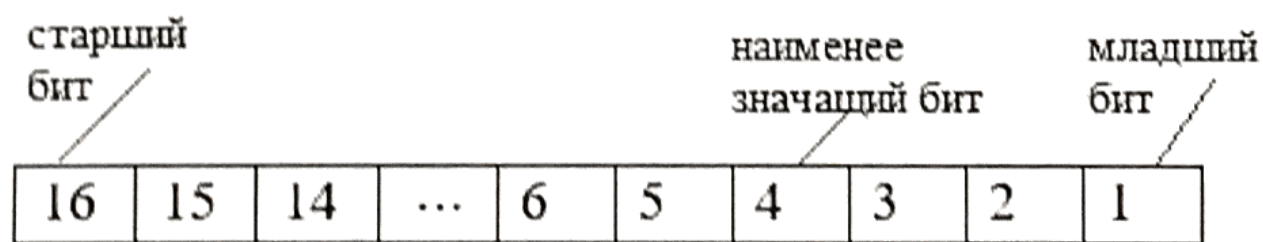


Рисунок 2.3 – Представления пикселя в двоичном виде

В таблице 2.1, приведены значения наименее значащего бита для наиболее распространенных разрядностей изображений.

Таблица 2.1 – Значение наименее значащего бита для изображения

Разрядность	Наименее значащий бит
24 бита	8
16 бит	4
8 бит	2

Использование для внедрения с младшего разряда по наименее значащие разряды, позволяет скрытно закодировать достаточно большой объем информации.

Ниже представлена известная частотная модель изображения, в которой осуществлено разделение матрицы коэффициентов ДКП на частотные области. Так, самые низкие частоты расположены в левом верхнем углу изображения, а высокие частоты – в правом нижнем. Известно, что наиболее эффективным является кодирование информации в области средних частот, так как низкие частоты содержат наибольшую часть энергии изображения и внесение изменений будет визуально заметно, а высокие наиболее подвержены искажениям, вносимых цифровыми преобразованиями, в частности операциями округления при сохранении на носитель информации. Они так же наиболее сильно изменяются при других процедурах обработки изображений.

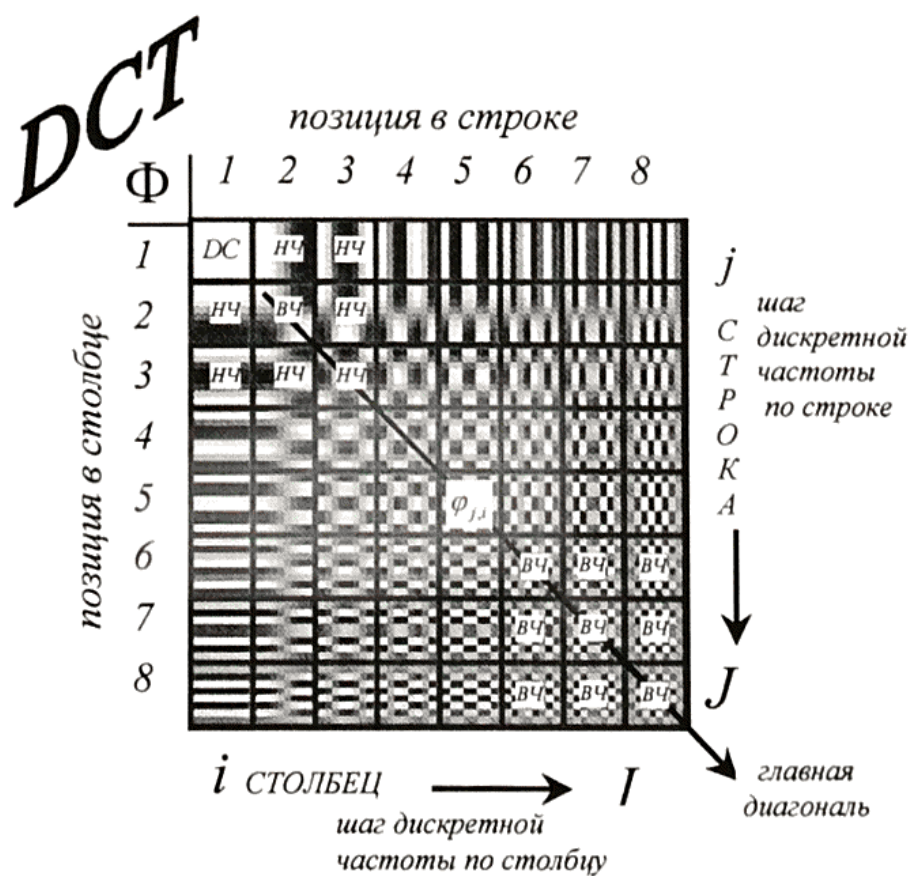


Рисунок 2.4 – Модель разбиения DCT на частотные области

Для кодирования в изображении речевого сигнала с использованием метода Коха-Жао предлагается использовать коэффициенты пренадлежащие средней частотной области. Использование для кодирования этих коэффициентов позволяет достиг сопоставимого с методом наименее значащего бита объема скрытной кодируемой информации.

2.3 Разработка алгоритмов скрытного внедрения

Словестный алгоритм стеганографического речевого сигнала в изображении на основе метода наименее значащего бита:

Вход: \mathbf{F} – фрагмент изображения ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$) размерностью $[M \times N]$, разрядностью 8 бит, цветовая схема – монохром; \vec{x} – отрезок речевого сигнала состоящий из отсчетов $x_n \in \vec{x}$, $n = 1, 2, \dots, N$, разрядностью 16 бит, режим моно.

Выход: $\tilde{\mathbf{F}}$ – фрагмент синтезированного изображения ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$) размерностью $[M \times N]$, разрядностью 8 бит, цветовая схема – монохром;

1. Задать номер отсчета РС $n = 1$
2. Задать начальные координаты пикселя $m = 1$ и $k = 1$
3. Преобразовать отсчет в набор бит $\vec{w} = dec2bin(x_n)$,

$$\vec{w} = (w_1, w_2, \dots, w_b, \dots, w_B)^T$$

4. Задать кодируемый бит пикселя $b = 1$
5. Преобразовать пиксель в набор бит $\vec{y} = dec2bin(f_{m,k})$,

$$\vec{y} = (y_1, y_2, \dots, y_b, \dots, y_B)^T$$

6. Заменить бит изображения битом речевого сигнала

$$\tilde{y} = (y_1, y_2, \dots, y_b, \dots, y_B)^T$$

7. Восстановить пиксель изображения

$$\tilde{f}_{m,k} = \sum_{\substack{h=1 \\ h \neq b}}^{B-1} \gamma_h \cdot 2^h + W_b \cdot 2^b$$

8. Изменить номер внедренного бита $h = b + 1$ отсчета РС
9. Проверить внедрены ли все биты отсчета речевого сигнала: $b < B$
– если условие выполняется, то п.10
– если условие ложно, то п.14
10. Изменить номер пикселя в столбце $k = k + 1$
11. Проверить внедрены ли во все биты строки: $k < K$
– если условие ложно, то п.5
12. Изменить номер пикселя строки $t = t + 1$
13. Проверить внедрено ли во все биты строки: $t < M$
– если условие выполняется, то п.
14. Перейти к следующему отсчету $n = n + 1$
15. Проверить внедрены ли все отсчеты: $n < N$
– если условие выполняется, то п.16 иначе, п. 10
16. Вывести синтезируемое изображение
17. Конец

Словесный алгоритм метода расширения спектра:

Вход: \mathbf{F} – фрагмент изображения ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$)
размерностью $[M \times N]$; \vec{x} – отрезок речевого сигнала состоящий из отсчетов $x_n \in \vec{x}$, $n = 1, 2, \dots, N$; \mathbf{U} – ПСП матрица ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$)
размерностью $[M \times N]$,

Выход: $\tilde{\mathbf{F}}$ – фрагмент синтезированного изображения ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$) размерностью $[M \times N]$, разрядностью 8 бит,
цветовая схема – монохром;

Кодирование:

1. Из исходного изображения F размером $[M \times N]$ выделяем блок $[8 \times 8]$;
2. Дополнительная информация, подлежащая внедрению в блок изображения, представляется в виде блоков $m_i = (m_0, m_1 \dots N - 1)$
3. Каждый блок сообщения соотносится с каждым блоком монохромного изображения.
4. Каждый информационный бит блока $m_{i,j}$ преобразуется в информационный сигнал $m_{i,j}(t) = \{-1; 1\}$
5. Производится модулирование информационного сигнала для каждого информационного блока

$$E_i(t) = \sum_{j=0}^{N-1} m_{i,j}(t) * \Phi_i$$

– Φ_i псевдослучайная последовательность

6. Выполняется попиксельное суммирование полученного блока сообщения с подблоком контейнера. $S_i = C_i + GE_i$

– G коэффициент усиления расширяющего спектра

– S_i заполненный контейнер

7. Сохраняем в стегофайл контейнер \tilde{F}

Декодирование:

1. Изображения с содержащимся в нем РС делим на блоки \tilde{F} размером $[8 \times 8]$;
2. Блоки представляются в виде вектора $C_i = (C_0, C_1, \dots, C_{m-1})$
3. Вычисляется коэффициент корреляции между Φ_i и полученным блоком представленным в виде вектора.
4. Найти знак коэффициента корреляции, который соответствует дополнительной информации

Словесный алгоритм метода Коха-Жао:

Вход: \mathbf{F} – фрагмент изображения ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$) размерностью $[M \times N]$, разрядностью 8 бит, цветовая схема – монохром; \vec{x} – отрезок речевого сигнала состоящий из отсчетов $x_n \in \vec{x}$, $n = 1, 2, \dots, N$, разрядностью 16 бит, режим моно; \mathbf{U} – ПСП матрица ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$) размерностью $[M \times N]$.

Выход: $\tilde{\mathbf{F}}$ – фрагмент синтезированного изображения ($m = 1, 2, \dots, M$ и $k = 1, 2, \dots, K$) размерностью $[M \times N]$, разрядностью 8 бит, цветовая схема – монохром;

Кодирование:

1. Изображение, представленное в цифровом виде, разбить на блоки \mathbf{F} $[N \times M]$ пикселей.
2. Представить кодируемую информацию в виде символов $e_w \in \{1, -1\}$.
3. Задать размер частотных областей ДКП $[U \times \Omega]$.
4. Рассчитать матрицу ДКП \mathbf{D} .
5. Найти коэффициенты ДКП: $\Phi = \{\phi_{u,\omega}\}$, $u = 1, 2, \dots, U$, $\omega = 1, 2, \dots, \Omega$.
6. Согласно решающего правила выбрать номера коэффициентов ДКП: $u \in U$, $\omega \in \Omega$ (выбор коэффициентов производится в области средних частот, в тех местах где сосредоточено меньше всего энергии)
7. Согласно кодируемого символа e_w осуществить кодирование:

$$\hat{\phi}_{u,\omega} = \begin{cases} |\phi_{u,\omega}| & , \text{при кодировании } e_w=1 \\ -|\phi_{u,\omega}| & , \text{при кодировании } e_w=-1 \end{cases}$$

8. Осуществить обратное ДКП, $\hat{\Phi} = \{\hat{\phi}_{u,\omega}\}$.

Изм.	Лист	№ докум.	Подпись	Дата

Декодирование:

1. Изображение, представленное в цифровом виде, разбить на блоки $\hat{\mathbf{F}} [N \times M]$ пикселей.
2. Задать размер частотных областей ДКП $[U \times \Omega]$.
4. Рассчитать матрицу ДКП \mathbf{D} .
5. Найти коэффициенты ДКП: $\hat{\Phi} = \{\hat{\phi}_{u,\omega}\}$, $u = 1, 2, \dots, U$, $\omega = 1, 2, \dots, \Omega$.
6. Согласно решающего правила выбрать номера коэффициентов ДКП: $u \in U$, $\omega \in \Omega$.
7. Декодировать символ информации e_w :

$$\hat{e}_w = \text{sign}(\hat{\phi}_{u,\omega})$$

Для минимизации искажений вызываемых методом Коха-Жао был модифицирован метод, т.е. кодирование и декодирование осуществляется не в паре коэффициентов ДКП, а в одном. Частотные координаты определяются при помощи заранее известного решающего правила (выбор коэффициентов производится в области средних частот, в тех местах где сосредоточено меньше всего энергии). Кодирование в одном коэффициенте уменьшает искажения и увеличивает пропускную способность метода. Блок-схема кодирования и декодирования метода Коха-Жао представлена на рисунках 7 и 8. Стоит отметить в методе Коха-Жао, имеется неявное округление значения пикселей после обратного ДКП, следовательно, это приводит к потере информации. Так как при кодировании значения пикселей и коэффициентов ДКП вычисляются с плавающей точкой, а хранение происходит в целочисленном виде.

2.4 Основные результаты и выводы по главе

1. Изложены методы, которые возможно применять для скрытного внедрения речевого сигнала в изображение.
2. Описаны модели принятия решений при выборе пространства в изображении обеспечивающие скрытность кодируемой информации
 - для метода наименее значащего бита, принцип выбора разрядов зависящий от разрядности изображения;
 - для метода Коха-Жао принцип выбора частотных коэффициентов.
3. Разработаны алгоритмы скрытного внедрения речевых данных в изображение, такие как:
 - словестный алгоритм стеганографического кодирования речевого сигнала в монохромном изображении на основе метода наименее значащего бита, который позволяет кодировать биты речевого сигнала в наименее значащих разрядах монохромного изображения;
 - словестный алгоритм стеганографического кодирования информации в монохромном изображении на основе метода расширения спектра, который позволяет кодировать бит речевого сигнала в выделенном блоке изображения;
 - словестный алгоритм стеганографического кодирования информации в монохромном изображении на основе метода Коха-Жао, который позволяет кодировать биты речевого сигнала в коэффициентах ДКП принадлежащие средней полосе частот монохромного изображения.

3 ПРОТОТИП И ОЦЕНКИ ЕГО РАБОТОСПОСОБНОСТИ

В разделе приведено описание прототипа программной поддержки алгоритмов внедрения речевого сигнала в изображение. Представлены результаты выполнения программ и проанализированы на основе оценок приведенных в первой главе.

3.1 Построение архитектуры прототипа

Используемая архитектура мобильного приложения выполняющего скрытное кодирование речевого сигнала в изображении состоит из следующих элементов:

Модуль загрузки РС

Модуль предназначен для отображения речевого сигнала в мобильном приложении. Он представляет из себя специализированный программный интерфейс, со встроенным аудиоредактором, используемым для выявления основных параметров информации необходимых для верной работы приложения, а так же прослушивания РС.

Модуль загрузки изображения

Данный модуль используется для отображения изображения в приложении. В него входит графический редактор способный определить его изначальные параметры, и преобразовать для обеспечения максимального уровня скрытности и емкости.

Модуль преобразования речевого сигнала в последовательность бит

В модуле реализованы алгоритмы позволяющие преобразовывать речевой сигнал в битовую последовательность пригодную для кодирования стеганографическим методам.

11070006.11.03.02.436.ПЗВКР

30

Модуль анализа изображения

Модуль используется для разбиения изображения на фрагменты, определение их характеристик и выявления тех частей изображения (анализ изображения) которые пригодны для скрытного внедрения РС.

Модуль внедрения РС в изображение

В этом модуле используются данные, получаемые из остальных модулей. Он выполняет выбор стеганографического метода который сможет обеспечить максимальную степень скрытности РС, затем скрытно внедряет контрольную информацию в изображение путем помещения преобразованного в битовую последовательность речевого сигнала в изображение в соответствии с выбранным методом кодирования.

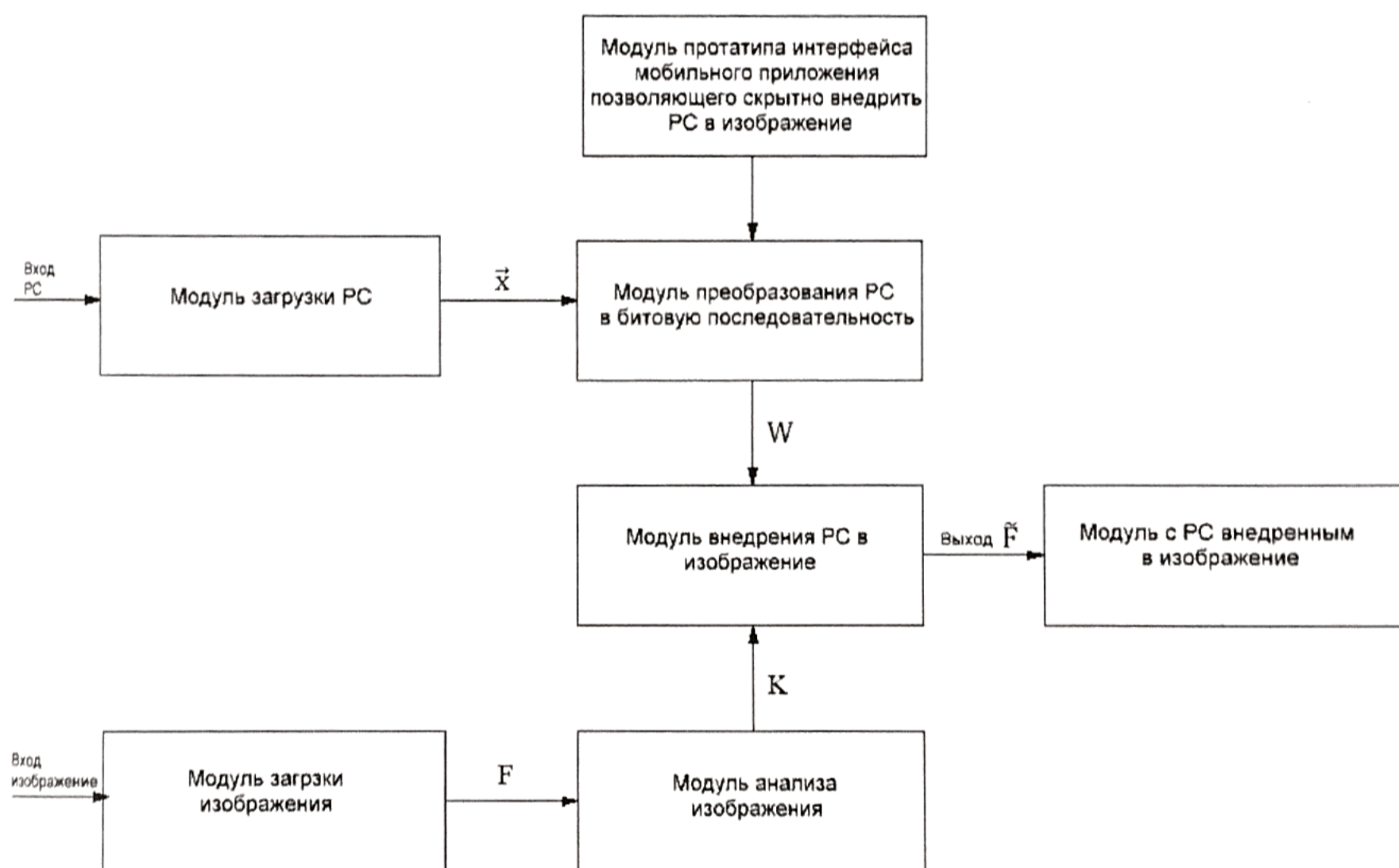


Рисунок 3.1 – Структурная схема взаимодействия модулей мобильного приложения позволяющего кодировать речевой сигнал в изображение, с обеспечением его скрытности

В рамках дипломного проекта было создано мобильное приложение работающее на платформе (android), способное кодировать с обеспечением скрытности и извлекать речевые сигналы в изображения. Работы по созданию

приложения проводились в интегрированной среде разработки (IDE) для работы с платформой Android – Android Studio.

Разработанное приложение позволяет осуществлять загрузку речевого сигнала и изображения, преобразовывать их. Так же позволяет осуществить скрытное кодирование РС в изображении, после чего его можно декодировать.

Мобильное приложение выполняет следующие функции:

- загрузку речевого сигнала;
- загрузку изображения
- анализ параметров речевого сигнала и изображения
- выбор стеганографического метода способного максимально скрытно закодировать речевой сигнал ;
- преобразование РС и изображения в форму необходимую для работы выбранного стеганографического метода
- скрытное внедрение информации.

На рисунке 3.2 представлен интерфейс главной страницы мобильного приложения (StegoBoom), позволяющего скрытно внедрить РС в изображение, в интегрированной среде разработки.



Рисунок 3.2 – Главная страница интерфейса мобильного приложения выполняющий кодирование речевого сигнала в изображении

Изм.	Лист	№ докум.	Подпись	Дата	11070006.11.03.02.436.ПЗВКР	32
------	------	----------	---------	------	-----------------------------	----

На рисунке 3.3 представлен интерфейс страницы мобильного приложения (StegoBoom), осуществляющий кодирование РС в изображении. Предполагается загрузка выбранного отправителем изображения – «загрузить изображение» и речевого сигнала – «загрузить речь», который нужно скрытно внедрить в изображение. Функции «Изменить» и «Прослушать» встроены для проведения анализа РС и изображения и редоктирования их параметров в соответствии с выбранным стеганографическим методом. Функция – «Внедрить» непосредственно производит кодирование РС в изображение.



Рисунок 3.3 – Интерфейс мобильного приложения выполняющий кодирование речевого сигнала в изображении

На рисунке 3.4 представлен интерфейс страницы мобильного приложения (StegoBoom), осуществляющий ивлечение РС из изображения. Функция – «Восстановить» позволяет получателю извлечь РС из изображения. Функция – «Запись» позволяет сохранить скрытно передаваемую звукозапись на используемом устройстве.



Рисунок 3.4 – Интерфейс мобильного приложения выполняющий извлечение речевого сигнала из изображения

Представленный прототип мобильного приложения позволит осуществить кодирование речевого сигнала в изображении с обеспечением его скрытности и восстановления, одним из трех наиболее распространенных методов стеганографии.

3.2 План оценки работоспособности

План оценки работоспособности метода LSB:

1. Загрузить фрагмент изображения, Φ
2. Загрузить фрагмент речевого сигнала, \vec{x}
3. Преобразовать отсчеты РС x_i в двоичную форму e_n
4. Определить порог h внедрения в изображение
5. Внедрить РС преобразованный в двоичную форму в изображении и получить стегоконтейнер $\tilde{\Phi}$
6. Оценить искажения в синтезированном изображении, Φ относительно $\tilde{\Phi}$ (MSE, SNR, NC)

7. Осуществить восстановление речевого сигнала \tilde{x}
8. Оценить изменения в восстановленном речевом сигнале относительно исходного (MSE, SNR, корреляция)
9. Осуществить воздействие шума на изображение с соотношением сигнал/шум = 0.1 раз (0.01 раз, 0.5 раз) $F = \tilde{\Phi} + h_0^2 \cdot U$
10. Извлечь речевой сигнал \vec{y}
11. Оценить изменения в восстановленном РС из стегоконтейнера подверженного воздействию \vec{y} , относительно исходного речевого сигнала.

3.3 Результаты экспериментальной оценки работоспособности

В качестве контейнера использовалось монохромное изображение разрядностью 8 бит, размером $[512 \times 512]$. И эталонный отрезок речевого сигнала длительностью 1 секунда, разрядностью 8 бит, частота дискретизации 8 кГц, режим моно (рисунок 3.5). Речевое сообщение соответствует слову «научный».

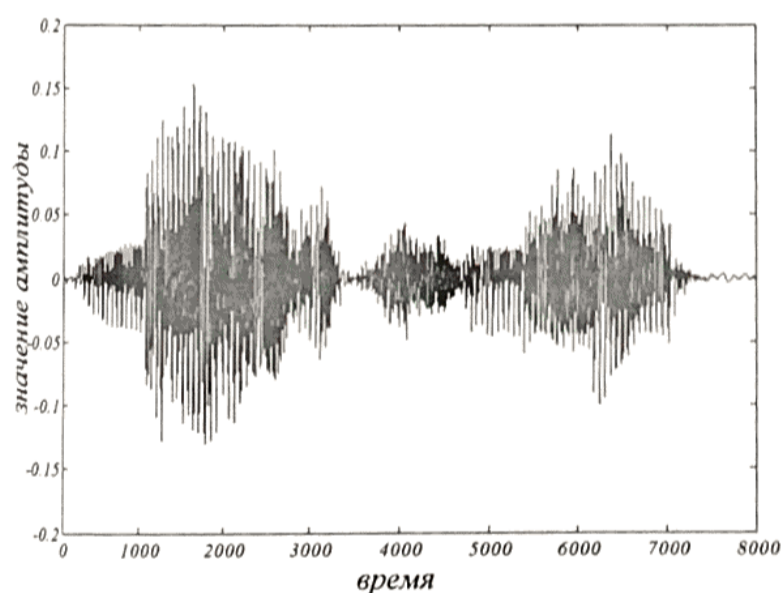
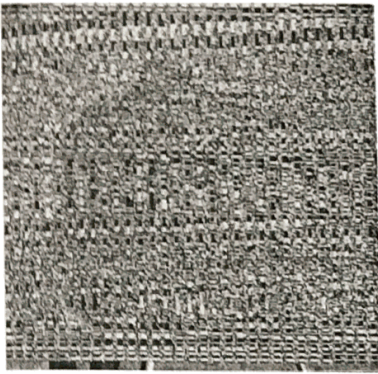


Рисунок 3.5 – Эталон:
а) речевое сообщение б) контейнер

Ниже на рисунке 3.6 приведены результаты моделирования и оценки скрытности речевого сигнала в изображении.

Лист	№ докум.	Подпись	Дата



а)



б)



в)



г)

Рисунок 3.6 – Стегоконтейнеры, полученные в результате внедрения речевого сообщения методом наименее значащего бита:

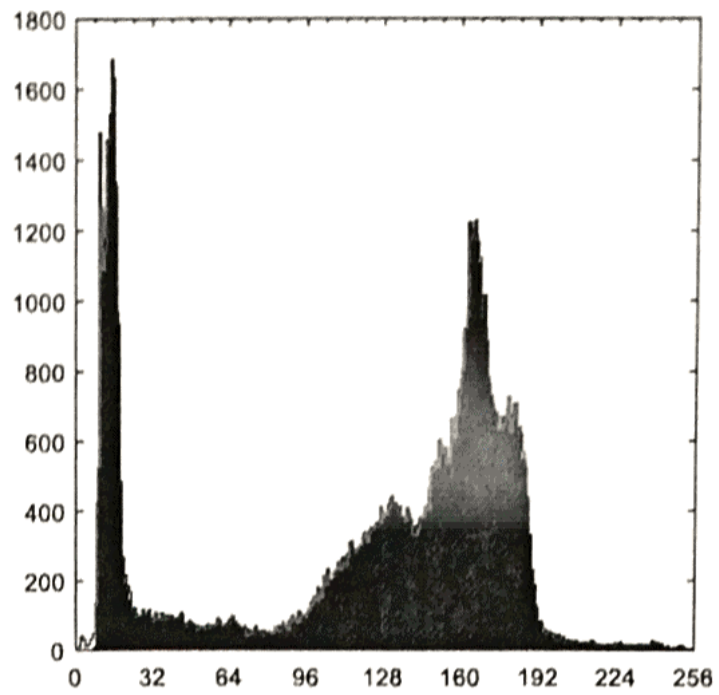
- а) результат внедрения в 1-й и 2-й разряды каждого из пикселей;
- б) результат внедрения в 4-й и 2-й разряды каждого из пикселей;
- в) результат внедрения в 5-й и 6-й разряды каждого из пикселей;
- г) результат внедрения в 6-й и 7-й разряды каждого из пикселей;

Таблица 3.1 – Результат оценки скрытности речевого сигнала в внедренного в изображение «Камеромен»

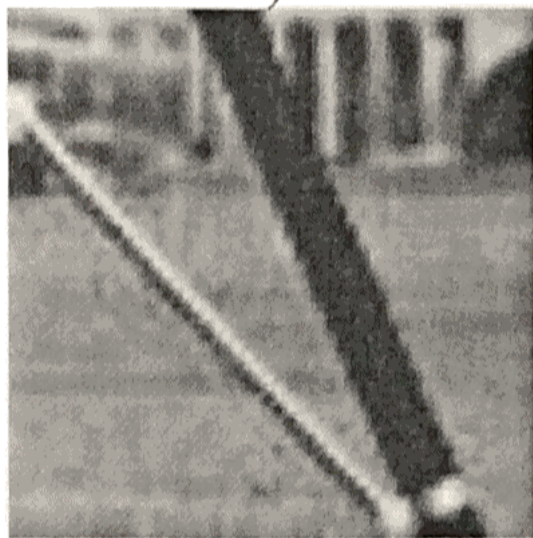
№	Замещаемы разряд	MSE	SNR	COR	NS	IF
1	7 и 8	165336	1.4030e-04	0.99970	2.6362e+04	0.9999
2	56	2705312	0.0023	0.9951	2.6484e+04	0.9977
3	34	42309120	0.0359	0.9133	2.48856e+04	0.9641
4	12	55631028	0.4721	0.1302	2.3192e+04	0.5276
5	67	671804	5.7007e-04	0.9987	2.63698+04	0.9994



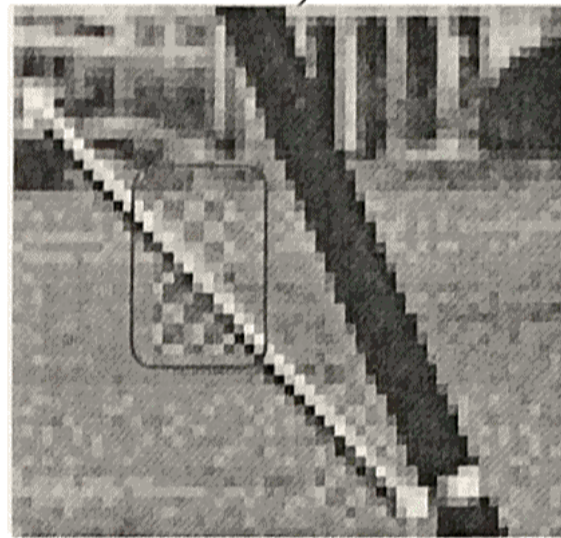
а)



б)



в)



г)

Рисунок 3.7 – Стегоконтейнеры, полученные в результате внедрения речевого сообщения методом Коха-Жжао:

- а) стегоконтейнер; б) гистограммы распределения монохромного цвета;
 в) исходный фрагмент изображения; г) искаженный фрагмент

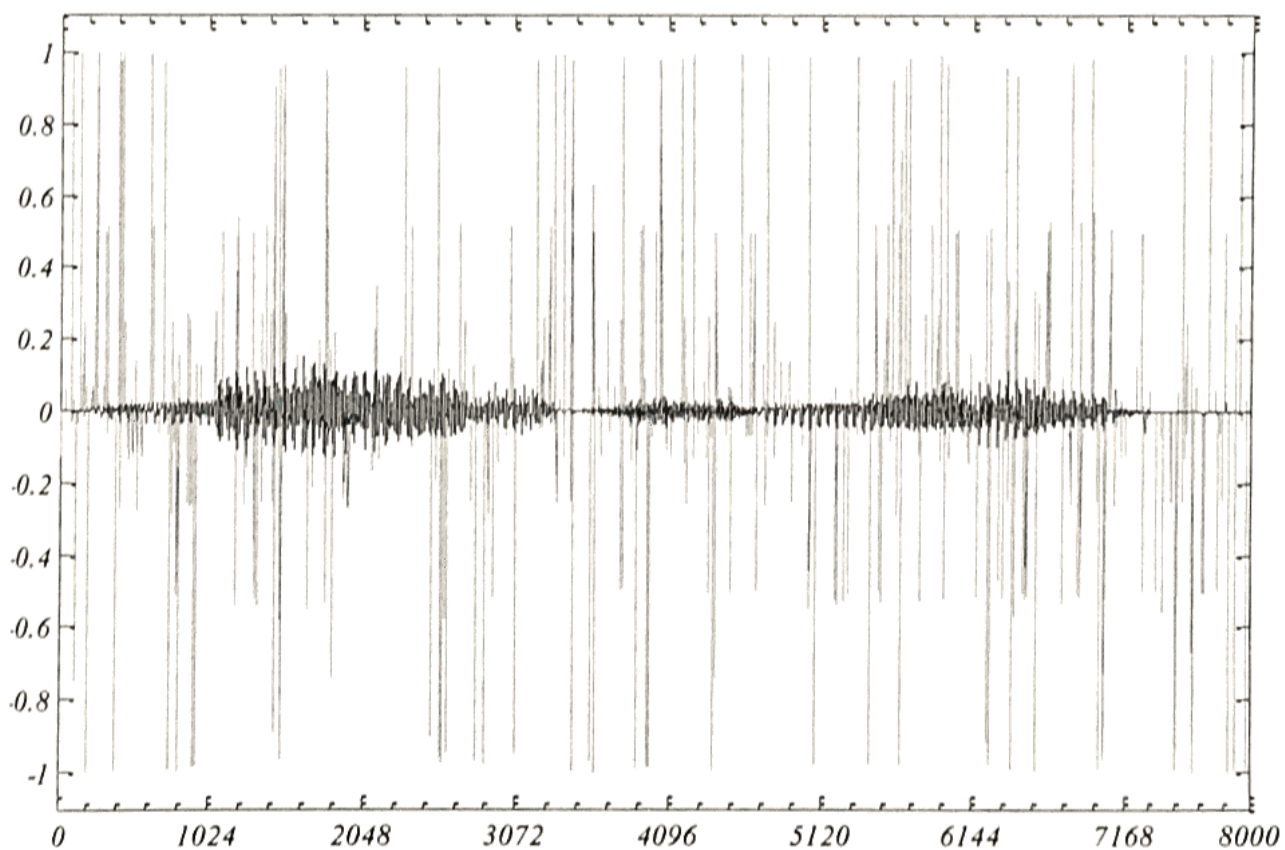
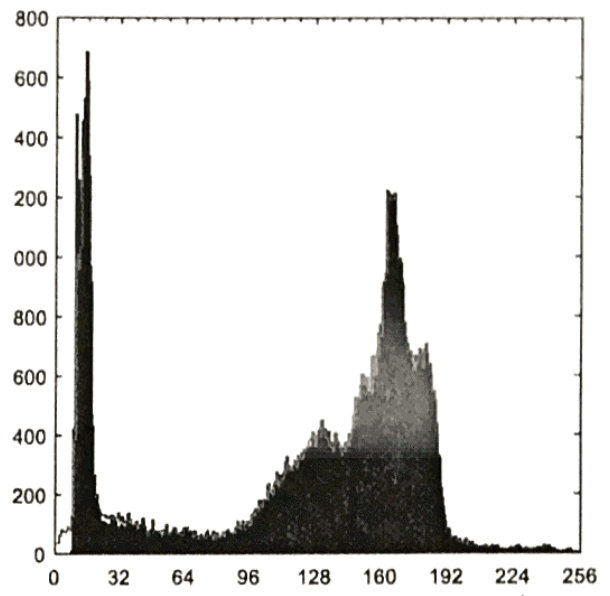


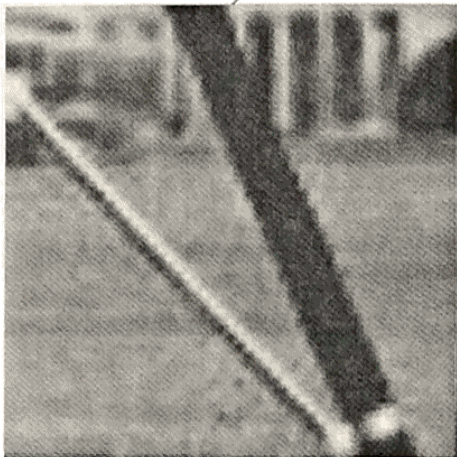
Рисунок 3.8 – Речевое сообщение:
 черный цвет – эталон; красный цвет – восстановленное



а)

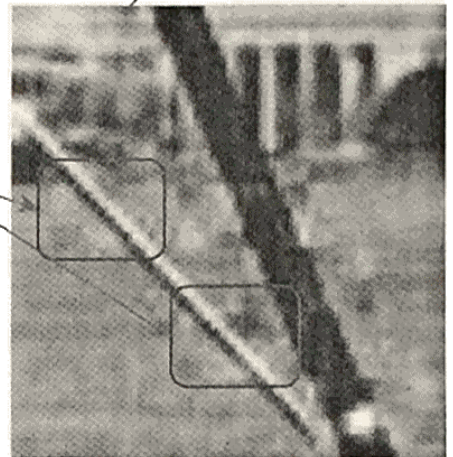


б)



в)

изменения



г)

Рисунок 3.9 – Стегоконтейнеры, полученные в результате внедрения речевого сообщения методом Коха-Жжао:

- а) стегоконтейнер; б) гистограммы распределения монохромного цвета;
 в) исходный фрагмент изображения; г) искаженный фрагмент

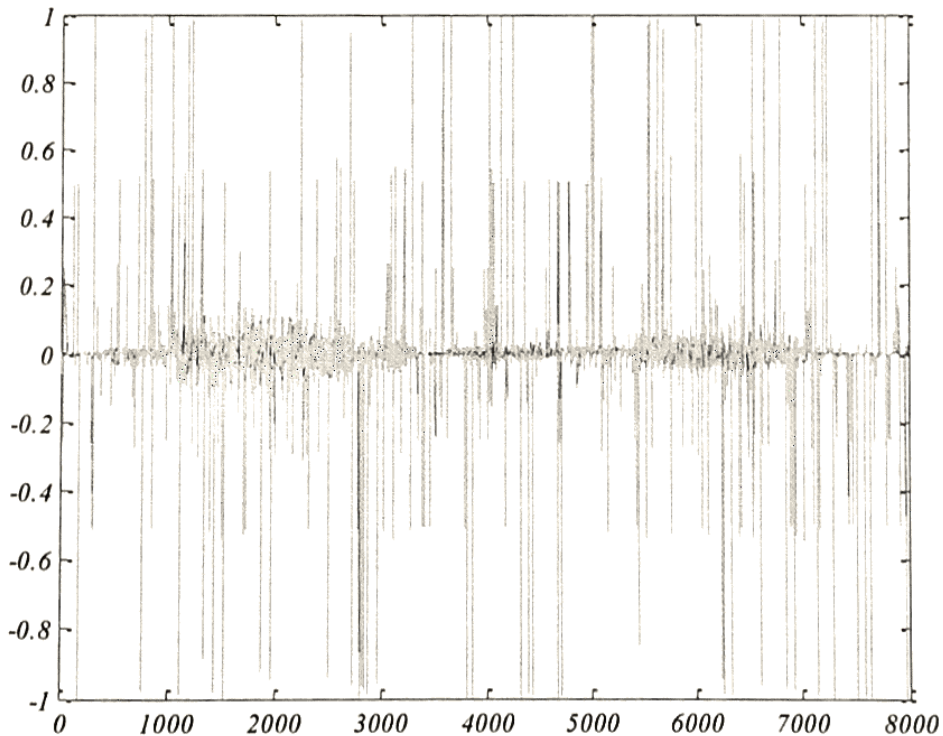


Рисунок 3.10 – Речевое сообщение:
 черный цвет – эталон; красный цвет – восстановленное

Лист	№ докум.	Подпись	Дата
------	----------	---------	------

Таблица 3.2 – Результаты оценки восстановления речевого сообщения из стегоконтейнера

№	Оценка	Скрытность			
		Алгоритм I		Алгоритм II	
		$M_e(\cdot)$	$M_x(\cdot)$	$M_e(\cdot)$	$M_x(\cdot)$
1	2	3	4	5	6
1	MSE, [5]	10.05	12.05	12.05	14.05
2	SNR, [20]	30.02	31.07	33.02	34.07
3	ρ , [49]	0.42	0.32	0.22	0.12
4	σ , [38]	6.37	5.64	6.34	5.14

$M_e(\cdot)$ – имеет смысл, наимвероятнейшего значения; $M_x(\cdot)$ – имеет смысл математического ожидания

Сопоставительный анализ показывает, что для внедрения речевого сигнала в изображение можно использовать метод наименее значащего бита и метод Коха-Жао, но последний метод не дает высокой степени достоверности восстановления речевого сообщения

3.4 Основные результаты и выводы

1. Выполнена разработка программной поддержки информационной технологии кодирования речевого сигнала в изображении.

2. Приведен прототип интерфейса мобильного приложения, позволяющий пользователю осуществить кодирование речевого сигнала в изображении с обеспечением его скрытности и восстановления, одним из трех наиболее распространенных методов стеганографии.

3. Проведена оценка работоспособности разработанных алгоритмов и их программной поддержки.

4 ЭКОНОМИЧЕСКАЯ ОЦЕНКА РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Конечным результатом данной научно-исследовательской работы будет
- прототип программы внедрения дополнительной информации в
изображение

4.1 Планирование работ по исследованию

Для выполнения работ по данному исследованию нам понадобятся
следующие специалисты:

- старший научный сотрудник, в его обязанности будет входить
руководство проектом;

- младший научный сотрудник, его обязанности заключаются в
проведении исследований, с целью определения работоспособности и
исправления ошибок допущенных в программной поддержке, выполнении
расчетов и составлении технической документации проекта;

- экономист, оценивающий рентабельность и бухгалтерское
сопровождение.

Ниже в таблице 4.1. приведены расчеты описывающие сроки
выполнения требуемых исследований

Таблица 4.1 – Планирование этапов работ по проекту

Наименование этапов работ	Исполнитель	Трудоемкость, час	Продолжительность, дней
1	2	3	4
1.Этап подготовки			
1.1.Сбор данных	Младший научный сотрудник	51	7
1.2.Разработка идеи	Старший научный сотрудник	83	11

Окончание таблицы 4.1

1	2	3	4
1.3.Обозначение объема исследовательских работ	Младший научный сотрудник	17	3
1.4.Организация исследовательской работы	Младший научный сотрудник	17	3
1.5.Обработка и анализ данных	Младший научный сотрудник	79	9
Итого:		247	33
2.Основной этап			
2.1.Обоснование уместности работы	Старший научный сотрудник	42	6
2.2.Производство работ	Младший научный сотрудник	131	21
Итого:		173	27
3.Заключительный этап			
3.1.Технико-экономическое обоснование	Экономист	39	4
3.2.Создание и утверждение технической документации	Младший научный сотрудник	39	4
Итого:		78	8

Приведенное выше планирование предназначено для оценки трудоемкости исследования по количеству затраченных на его выполнение времени и средств. Выявлено число необходимых специалистов, а также производственного персонала, требуемых для реализации проекта.

4.2 Расчет финансовых затрат на оплату труда и исследование

Ниже в таблице 4.2 произведен расчет финансовых затрат на оплату труда сотрудников и выполнение исследования.

Таблица 4.2 – Расчет финансовых затрат на оплату труда

Должность исполнителей	Трудоемкость, час	Оклад, руб
Младший научный сотрудник	334	16000
Старший научный сотрудник	125	22000
Экономист	39	14000
Итого:	498	

Расчет оплаты труда исполнителя в единицу времени, то есть часовая тарифная ставка ($Ч_{ТС}$) производится по формуле:

$$Ч_{ТС} = P / F_{мес}, \quad (4.1)$$

где $F_{мес}$ – фонд рабочего времени месяца, составляет 176 часов (22 рабочих дня по 8 часов в день); P – оклад сотрудника.

Финансовые затраты на оплату труда (P_{OT}) находятся следующим образом:

$$P_{OT} = Ч_{ТС} \cdot T_{сум}, \quad (4.2)$$

где $T_{сум}$ – суммарная трудоемкость каждого из исполнителей.

В таблице 4.3. приведены итоговые расчеты

Таблица 4.3 – Расчет финансовых затрат на оплату труда

Должность Исполнителей	Трудоемкость, час	Оклад, руб	Ч _{ТС} , руб/час	Р _{ог} , руб
1	2	3	4	5
Младший научный сотрудник	334	16000	90.91	30363.94
Старший научный сотрудник	125	22000	125	15625
Экономист	39	14000	79.55	3102.45
Итого:	498	52000	295.46	49091.39

4.3 Расчет продолжительности исследования

В соответствии с выполненными расчетами, трудоемкость исследования составит 498 часов.

Узнав общую трудоемкость исследования, становится возможным расчет продолжительности исследования, которая составит:

$$T_{\text{иссл}} = \frac{Ч_{\text{ТС}}}{T_{\text{СУМ}}}, \quad (4.3)$$

где, $T_{\text{СУМ}}$ – суммарная трудоемкость исследования, $T_{\text{РД}}$ – продолжительность рабочего дня.

Для расчетного периода примем $T_{\text{СУМ}} = 498$ часов и $T_{\text{РД}} = 8$ часов

$$T_{\text{иссл}} = 498/8 = 63 \text{ дня,}$$

Исследование будет проводиться в течении 63 рабочих дней (не учитывая выходных и праздничных дней).

В данном разделе выполняется учет расходов на покупку основных материалов, использующихся персоналом в ходе исследования, создание документации, а также берется во внимание стоимость принтерных картриджей. В таблице 3.4. произведен расчет финансовых затрат на расходные материалы.

Таблица 4.4 – Стоимость расходных материалов

Наименование расходных материалов	Цена за единицу, руб.	Количество, шт.	Сумма, руб.
1	2	3	4
Бумага офисная формата А4	200	4	800
Канцтовары	400	-	400
Расходные материалы для принтера (картридж)	4500	-	4500
Итого:	5100	4	5700

Финальные затраты на закупку расходных материалов для проведения исследования составят 5700 рублей.

4.5 Составление схемы расходов на исследование

Произведем расчет общих расходов, затраченных на разработку и выполнение исследования. В этом расчёте обязательно учитывается часовая тарифная ставка, выплаты премий, районный коэффициент и страховые взносы. Для оценивания произведенных финансовых затрат на данное исследование выполним составление сметы на разработку и проведение исследования.

Премииальные выплаты рассчитываются по следующей формуле:

$$ПВ = P_{OT} \cdot K_{ПВ}, \quad (4.4)$$

где, $K_{ПВ}$ - коэффициент премиальных выплат

Пусть он составляет 25 %, в случае если премии не предусмотрены $K_{ПВ}=1$.

$$ПВ = 49091.39 \cdot 0,25 = 12272.85 \text{ (руб)},$$

Дополнительные финансовые затраты на проведение исследования можно определить по следующей формуле:

$$З_{доп} = P_{OT} \cdot K, \quad (4.5)$$

где K - коэффициент дополнительных затрат ($K=14\%$).

$$З_{доп} = 49091.39 \cdot 0.14 = 6872.79 \text{ (руб)},$$

Так же в заработной плате нужно предусмотреть районный коэффициент [], который доплачивается за работу в трудных или удаленных от центральных районов страны условиях. Определение размера коэффициента производится в зависимости от характера производства и может достигать 70%.

$$PK = P_{OT} \cdot K_{РВ}, \quad (4.6)$$

где $K_{РВ}$ – коэффициент районных выплат, возьмем для примера коэффициент для Новосибирска на 2018 г

$$PK = 49091,39 \cdot 0,15 = 7363.71 \text{ (руб)}, \quad (4.7)$$

Общие финансовые затраты на оплату труда рассчитываются по формуле:

$$P_{общ} = P_{OT} + PK + ПВ + З_{доп}, \quad (4.8)$$

где P_{OT} – основная заработная плата; $ПВ$ – премиальные выплаты; $З_{доп}$ – дополнительные затраты; PK – районный коэффициент.

$$P_{\text{общ}} = 49091.39 + 7363.71 + 12272.85 + 6872.79 = 75599.95 \text{ (руб)}$$

Из таблицы 4.4 берется итоговая сумма стоимости расходных материалов по статье расходных материалов.

$$P_{\text{PM}} = 5700 \text{ (руб)}.$$

Страховые взносы рассчитываются по формуле:

$$CB = P_{\text{OT}} \cdot 0.3, \quad (4.9)$$

$$CB = 49091.39 \cdot 0.30 = 14727.42 \text{ (руб)}$$

Амортизационные исчисления на использование компьютера в данном составляют 25% от стоимости компьютера $C_{\text{ПК}}$.

$$AO = C_{\text{ПК}} \cdot 0.25, \quad (4.10)$$

$$AO = 55000 \cdot 0.25 = 13750 \text{ (руб)},$$

Расходы на услуги связи и использование Интернета берутся из расчета месячной абонентской платы для предприятия. Пусть:

$$P_{\text{ИНТ}} = 1700 \text{ (руб)}.$$

Административно-хозяйственные расходы составят не менее 50% от основной заработной платы (P_{OT}).

$$P_{\text{АХ}} = P_{\text{OT}} \cdot 0.5 \quad (4.11)$$

$$P_{\text{АХ}} = 49091.39 \cdot 0.5 = 24545.70 \text{ (руб)}.$$

таблицу 4.5.

Таблица 4.5 – Смета расходов на проведение исследования

Наименование статей расходов	Сумма, руб.	Удельный вес статей, %
1	2	3
1.Стоимость расходных материалов	5700,00	2,39
2. Расходы на оплату труда, из них:	75599,95	55,58
2.1. Основная заработная плата	49091,39	36,09
2.2. Дополнительные затраты	6872,79	5,05
2.3. Премияльные выплаты	12272,85	9,02
2.4 Районный коэффициент	7363,71	5,41
3. Единый социальный налог	14727,42	10,83
4. Амортизационные исчисления на использование компьютера	13750,00	10,11
5. Расходы на использование Интернет	1700,00	1,25
6.Административно-хозяйственные расходы	24545,70	18,04
Итого:	136027,07	100

В следствии проведения экономической оценки исследования мы определили финансовые затраты на разработку и реализацию исследования:

- продолжительность исследовательских работ составила 63 дня;
- смета расходов на исследование – 136027.07 рубля.

ЗАКЛЮЧЕНИЕ

В работе были проанализированы основные методы стеганографии, используемые для внедрения информации в изображение. Так как в качестве внедряемой информации выступал аудио сигнал то дальнейшее рассмотрение ограничилось методам LSB и методам Коха-Жао. Выбранные для дальнейшего прототипирования методы позволяют стеганографически закодировать большие, по сравнению с другими методами объемы информации.

Для методов LSB и Коха-Жао алгоритмы, по сравнению с существующими разработанные позволяют использовать их для внедрения речевого сигнала.

Разработаны алгоритмы скрытного внедрения речевых данных в изображение, такие как:

– словестный алгоритм стеганографического кодирования речевого сигнала в монохромном изображении на основе метода наименее значащего бита, который позволяет кодировать биты речевого сигнала в наименее значащих разрядах монохромного изображения;

– словестный алгоритм стеганографического кодирования информации в монохромном изображении на основе метода расширения спектра, который позволяет кодировать бит речевого сигнала в выделенном блоке изображения;

– словестный алгоритм стеганографического кодирования информации в монохромном изображении на основе метода Коха-Жао, который позволяет кодировать биты речевого сигнала в коэффициентах ДКП принадлежащих средней полосе частот монохромного изображения.

В качестве среды моделирования использовали пакет MatLab, разработанные на нем программные протоколы тестировались на монохромных изображениях с глубиной цвета 8 бит (Cameroman) и аудиозаписями (8 бит, 8 КГц, режим: моно).

11070006.11.03.02.436.ПЗВКР

48

Оценка качества внедрения для изображения осуществлялась по MSE, SNR, NC. Качество восстановленного речевого сигнала составило MSE, SNR, корреляция. Значения оценок усреднены для приведенных выше изображений и речевого материала.

Результаты исследований обнародованы на конференциях: Ежегодная межвузовская научно-техническая конференция студентов, аспирантов и молодых специалистов имени Е.В. Арменского (г. Москва, 2017); Конгресс молодых ученых (г. Санкт-Петербург, 2017); представлены на ежегодной Курчатовской школе (г. Москва, 2016, 2017) и изложены в материалах из списка РИНЦ [19, 58-60].

				<i>11070006.11.03.02.436.ПЗВКР</i>	
Лист	№ докум.	Подпись	Дата		49