

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 И ИССЛЕДОВАНИЕ АЛГОРИТМА СКРЫТОЙ ПЕРЕДАЧИ
СИГНАЛА**

Выпускная квалификационная работа
обучающегося по направлению подготовки 11.03.02 Инфокоммуникационные
технологии и системы связи
очной формы обучения, группы 07001410
Зубков Тимур Николаевич

Старший преподаватель
кафедры информационно-
телекоммуникационных
систем и технологий
НИУ «БелГУ» Лихолоб П.Г.

Рецензент начальник
систем коммутации №1
Белгородского филиала
ПАО «Ростелеком»
Тельбуков Д.Ф.

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 11.03.02 Инфокоммуникационные технологии и системы связи
Профиль подготовки «Сети связи и системы коммутации»

Утверждаю
Зав. кафедрой

« 19 »



2018 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Зубкова Тимура Николаевича
(фамилия, имя, отчество)

1. Тема ВКР «Разработка и исследование алгоритма скрытой передачи сигнала»

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

2. Срок сдачи студентом законченной работы 09.06.2018

3. Исходные данные:

объект проектирования – методы стеганографии, сигнал;

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

4.1 Модели анализа/синтеза речевых сигналов при скрытной передаче информации

4.2 Методы скрытной передачи сигнала

4.3 Метод наименее значащего бита

4.4 Метод дискретно-косинусного преобразования и его модификации

4.5 Разработка алгоритмов и оценка их работоспособности

4.5.1 Описание алгоритмов скрытного кодирования и декодирования сигналов

4.5.2 Методика оценки работоспособности алгоритмов стеганографического кодирования и декодирования сигналов

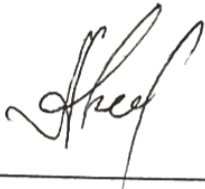
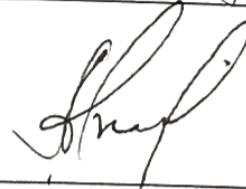
4.5.3 Результаты оценки работоспособности и эффективности алгоритмов

4.5.4 Основные результаты и выводы

4.6 Концепция прототипа и оценки его работоспособности

4.7 Технико-экономическое обоснование проекта

6. Консультанты по работе с указанием относящихся к ним разделов

Раздел	Консультант	Подпись, дата	
		Задание выдал	Задание принял
4.1-4.6	ст. преп. каф. ИТСиТ Лихолоб П.Г.		
4.7	канд. техн. наук доцент каф. ИТСиТ Болдышев А.В.	 20.04.2018	 20.04.2018

7. Дата выдачи задания 30.04.2018

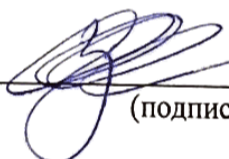
Руководитель

ст. преподаватель
кафедры Информационно-телекоммуникационных
систем и технологий,
НИУ «БелГУ»


(подпись)

П.Г. Лихолоб

Задание принял к исполнению


(подпись)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ.....	3
1 Модели анализа/синтеза речевых сигналов при скрытой передаче информации	5
1.1 Математические основы анализа/синтеза речевых сигналов.....	5
1.2 Методы скрытой передачи сигнала.....	7
1.2.1 Метод наименее значащего бита	10
1.2.2 Метод расширения спектра и его модификации	13
1.2.3 Метод дискретно – косинусного преобразования и его модификации	17
1.3 Методы оценки скрытности.....	24
1.4 Постановка задач исследования	26
2 РАЗРАБОТКА АЛГОРИТМОВ И ОЦЕНКА ИХ РАБОТОСПОСОБНОСТИ	27
2.1 Описание алгоритмов скрытого кодирования и декодирования	27
2.2 Методика оценки работоспособности алгоритмов стеганографического кодирования и декодирования сигналов.....	28
2.3 Результаты оценки работоспособности и эффективности алгоритмов.....	36
2.4 Основные результаты и выводы	37
3 КОНЦЕПЦИЯ ПРОТОТИПА И ОЦЕНКИ ЕГО РАБОТОСПОСОБНОСТИ..	38
3.1 Построение архитектуры программной реализации	38
3.2 Результаты экспериментальной оценки работоспособности и описание результатов работы	39
3.3 Основные результаты и выводы	41
4 ЭКОНОМИЧЕСКАЯ ОЦЕНКА РЕЗУЛЬТАТОВ ИЗМЕРЕНИЯ.....	41
4.1 Планирование работ по исследованию	41
4.2 Расчет финансовых затрат на оплату труда сотрудников и на исследование.....	43
4.3 Расчет продолжительности исследования.....	45
4.4 Расчет финансовых затрат на расходные материалы	45
4.5 Составление сметы расходов на исследование.....	46
ЗАКЛЮЧЕНИЕ	50
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ	51

					<i>11070006.11.03.02.826.ПЗВКР</i>			
Изм.	Лист	№ докум.	Подпись	Дата	Разработка и исследование алгоритма скрытой передачи сигнала	Лит.	Лист	Листов
Разработал		Зубков Т.Н.					2	53
Проверил		Лихолоб П.Г						
Рецензент		Тебульков Д.Ф						
Н. Контроль		Лихолоб П.Г						
Утвердил		Жиляков Е.Г.				<i>НИУ «БелГУ» гр.07001410</i>		

ВВЕДЕНИЕ

Несанкционированное копирование и распространение звукозаписей значительно упростилось в связи с доступностью персональных компьютеров и мобильных устройств, использования недорогих и надежных узлов хранения данных, сетей широкополосного доступа и множества программ для записи и редактирования звука. Интенсивное развитие информационных технологий привело к необходимости защиты и обеспечения прав интеллектуальной собственности на звукозаписи в цифровом виде, в частности предотвращение их незаконного копирования, воспроизведения и подделки. Такая ситуация особенно актуальна для музыкальной индустрии, которая ищет надежные решения проблем, связанных с защитой авторских прав на музыкальные файлы.

Общедоступность средств редактирования, в настоящее время позволяет изменять цифровые аудио файлы, не оставляя признаков принадлежности тому или иному автору. Поэтому то, что вы услышали, не всегда может быть правдой и принадлежать конкретному человеку. Возникает необходимость в разработке эффективной технологии аутентификации, чтобы авторы могли защищать свои законные права. Цифровая водяная маркировка и цифровая подпись – это два типичных метода аутентификации цифрового звука. Тем не менее, эти методы теряют эффективность во многих реальных ситуациях из-за их потребности в дополнительной информации (водяной знак или подпись) в процессе аутентификации, способствует возникновению подозрительного звука.

Поэтому технология нацелена на внедрение водяного знака в файлы мультимедиа без ухудшения их восприятия. Встроенные водяные знаки могут быть сгенерированы для обозначения отправителей, приемников, уникальных серийных номеров или временных меток. Эти водяные знаки обеспечивают целостность и подлинность исходного файла мультимедиа без ухудшения его общего качества. Непроходимость и устойчивость водяных знаков к удалению или деградации являются двумя необходимыми требованиями для любых

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						3
Изм.	Лист	№ докум.	Подпись	Дата		

эффективных звуковых данных, скрывающий алгоритм. Поэтому на практике существует фундаментальный компромисс между двумя требованиями таким образом, чтобы обеспечить эффективное внесение водяного знака. Тем не менее, прослушиванию следует уделять особое внимание, поскольку, если качество оригинального аудио не может быть сохранено, ни пользователи, ни владельцы не смогут его идентифицировать.

Целью работы является исследование методов скрытого внедрения информации в звуковые файлы посредством исследования алгоритмов скрытой передачи информации.

Для успешного выполнения поставленной цели необходимо выполнить ряд задач, а именно:

1. Разработать алгоритм скрытого кодирования речевого сообщения в речевые данные.
2. Провести качественную оценку скрытности передаваемого сигнала.
3. Провести количественную оценку скрытности передаваемого сигнала.
4. Выполнить экономическое обоснование результатов исследования.

Иными словами, необходимо выявить закономерности изменения качества звучания и восприятия искажений при скрытном кодировании информации различными методами.

Работа изложена на стр. 53, содержит 9 таблиц, 16 рисунков, список литературных источников из 15 наименований.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						4
Изм.	Лист	№ докум.	Подпись	Дата		

1 МОДЕЛИ АНАЛИЗА/СИНТЕЗА РЕЧЕВЫХ СИГНАЛОВ ПРИ СКРЫТОЙ ПЕРЕДАЧЕ ИНФОРМАЦИИ

1.1 Математические основы анализа/синтеза речевых сигналов

Коммуникация является важным компонентом функционирования любой системы. Под информацией, понимается приращение знаний. Знания – это результат освоения сведений или то, что позволяет прогнозировать его поведение при любых условиях, знания оформляется в виде некоторой модели.

Модель – это описание объектов или процесса для решения стоящих задач. Важнейшими характеристиками информации являются; актуальность, достоверность, информативность и полнота. Современные информационные технологии позволяют производить множество манипуляций с информацией. В данной работе мы выделим кодирование и скрытность.

Сигнал в системах связи, обработке сигналов, является функцией, которая передает информацию о поведении или атрибутах какого-либо явления [1]. В физическом мире любая величина, показывающая изменение во времени или изменение пространства, потенциально представляет собой сигнал, который может предоставлять информацию о статусе физической системы или передавать сообщение между объектами.

Речь – это особый тип сигнала, не стационарный во времени, что в свою очередь затрудняет её анализ и моделирование. Основными характеристиками речевого сигнала, являются разборчивость и согласованность, поэтому в инфокоммуникационных технологиях принято, что число дискретных значений необходимых для описания одной секунды речевого сигнала, соответствует 8000 выборкам. Речевое кодирование или сжатие представляет собой, процесс получения компактного представления, для речевых сигналов с целью эффективной передачи по ограниченному диапазону проводных или беспроводных каналов, а также для их эффективного хранения.

На данный момент существует множество способов описания речевого

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						5
Изм.	Лист	№ докум.	Подпись	Дата		

сигнала посредством математических моделей. В данной работе мы рассмотрим дискретное преобразование Фурье, дискретно–косинусное и Вейвлет преобразование.

Дискретное преобразование Фурье (ДПФ) является эквивалентом непрерывного преобразования Фурье, для сигнала N , известных только в моменты времени T (т.е. конечная последовательность данных). Пусть $f(t)$ непрерывный сигнал, который является источником данных. Пусть количество отсчетов равно N $f[0], f[1], f[2], \dots, f[k], \dots, f[N - 1]$ тогда ДСП выглядит следующим образом

$$F(j\omega) = \int f(t) e^{-j\omega t} dt \quad (1.1)$$

Рассмотрим каждый отсчет $f[k]$, как импульс с площадью $f[k]$. Тогда как подынтегральное выражение существует только в точке выборки, получим;

$$F(j\omega) = \int_0^{(N-1)T} f(t) e^{-j\omega t} dt$$

$$= f[0]e^{-j\omega 0} + f[1]e^{-j\omega T} + \dots + f[k]e^{-j\omega kT} + f[N - 1]e^{-j\omega(N-1)T} \quad (1.2)$$

$$F(j\omega) = \sum_{k=0}^{N-1} f[k] e^{-j\omega kT} \quad (1.3)$$

Допускается оценка по ω , но при условии, что точки N заданы изначально, только N конечные элементы будут иметь значения.

Важно помнить, что непрерывное преобразование Фурье может произвести точную оценку на конечном интервале времени. Аналогично, поскольку существует только конечное число входных данных, ДПФ обрабатывает данные, так как если бы они были периодическими.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						6
Изм.	Лист	№ докум.	Подпись	Дата		

Следовательно, последовательность, показанная ниже на рисунке 1.1 (а), считается одним из периодов, периодической последовательности на графике (в).

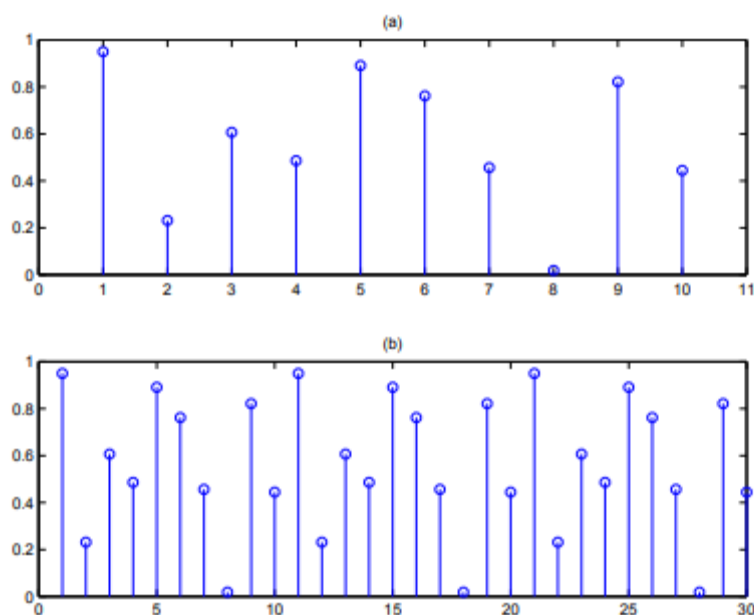


Рисунок 1.1 – а) Последовательность при N=10 отсчетах, в) не явная периодичность в ДФТ.

Поскольку операция обрабатывает данные таким образом, что при условии её последовательности мы вычисляем уравнения ДПФ для основной частоты и их гармоники, не забывая при этом про коэффициент:

$$F[n] = \sum_{k=0}^{N-1} f[k]e^{-j\frac{2\pi}{N}nk} \quad (1.4)$$

где $F[n]$ является дискретным преобразованием последовательности $f[k]$

1.2. Методы скрытной передачи сигнала

Методы скрытной передачи сигнала базирующиеся, во временной области, такие как методы замещения наименее значимого бита (LSB) или методы скрывтия эха, встраивают водяной знак непосредственно во временную область. В LSB информационные биты водяного знака встроены в младшие

значащие биты аудиосигнала. Методы водяного знака с использованием частотной области используют человеческие перцептивные свойства и частотные маскирующие характеристики человеческой системы восприятия. Эти методы обычно используют DFT (дискретное преобразование Фурье), DST (дискретное косинусное преобразование) или DWT (преобразование дискретных волн), чтобы преобразовать аудиосигнал. Водяной знак во временной области довольно прост в реализации и требует меньших вычислительных ресурсов, по сравнению с водяным знаком частотной области, однако он имеет минусы в после обработки сигналов, таких как сжатие звука и фильтрация и другие. Точно так же подходы к частотной области могут проявлять не надежность в сигналах с очень небольшим количеством компонентов преобразования.

Расширение спектра водяных знаков базируется на понятиях, заимствованных из широкополосных систем связи, в которых расширение спектра скрывает сигнал от постороннего слушателя и обеспечивает конфиденциальность информации. Однако, вычислительная сложность и время синхронизации может быть неприемлемо высокой. В таких методах, водяной знак встраивается непосредственно в уже сжатый аудио поток битов, чтобы предотвратить потерю водяных знаков. Таким образом, во время декодирования цифровых водяных знаков, вставлять водяные знаки снова не требуется, что приводит к их низкой вычислительной стоимости. Однако, эти методы не используют психоакустическую модель и кроме того, сама архитектура стандартных аудио систем сжатия должны быть изменена, чтобы включить модули водяных знаков.

Звуковая стеганография требует незаметной модификации несущей звукового сигнала. На рисунке 1.2. представлена общая модель звуковой стеганографии. Несовместимость и надежность – это два необходимых требования для любого эффективного алгоритма стеганографии звука. Особого внимания следует уделить неотложности, поскольку, если качество исходного

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						8
Изм.	Лист	№ докум.	Подпись	Дата		

сигнала несущей звука не может быть сохранено, то технология стеганографии будет терпеть неудачу.



Рисунок 1.2 – Структурная схема стеганографии звуковой стеганографии

Исследования в области звуковой стеганографии не так зрелы, по отношению к исследованиям в области стеганографии изображений. Причиной тому является человеческая слуховая система, которая гораздо более чувствительна, чем визуальная. Стеганография предполагает, что обложка, используемая для скрытия секретного сообщения, не должна вызывать подозрения у злоумышленников. Более того, аудио-файлы более популярны, что делает их достаточно подходящими для передачи секретного сообщения. Вторая причина может заключаться в том, что большая часть атак более ориентировано на цифровые изображения, поэтому оставляя стеганографию звука относительно неизведанным.

Можно выделить четыре основные характеристики звуковой стеганографии:

1. Невосприимчивость к слуховой системе человека. Звуковая стеганография требует незаметной модификации несущей сигнала. его основное требование – обеспечить сохранение исходного качества сигнала. Кроме того, неслучайно следует уделять этому особое внимание, поскольку,

если качество звука не может быть сохранено, пользователи не удовлетворит данная технология.

2. Надежность от различных видов искажений. Сигнал должен быть устойчивым к искажениям, таким как усиление, сжатие и т. д.

3. Простота обнаружения и извлечения Для пользователя, который обладает секретным ключом для извлечения секретного сообщения, ему должно быть достаточно просто извлечь секретное сообщение. Гарантия, того что стеганография проведена и может быть расшифрована только предполагаемым пользователем.

Высокая пропускная способность данных. Несущая аудиосигнала должен иметь возможность передавать достаточное количество секретного сообщения без искажения несущей исходного сигнала. Аудиосигналы должны быть представлены гораздо меньшим числом выборок за интервал времени.

1.2.1 Метод наименее значащего бита

Чтобы скрыть секретное сообщение, нам нужна оболочка или контейнер в качестве файла хоста. Для скрытия секретного сообщения используются другие обертки или файлы хоста, например: изображение, аудио, видео, текст.

Кодирование с наименьшим значащим битом (LSB) является самым простым способом встраивания информации в цифровой аудиофайл [9]. Подставляя в младший значащий бит каждой точки выборки двоичным сообщением, кодирование LSB позволяет кодировать большой объем данных. Следующая диаграмма на риске 1.3 иллюстрирует, как сообщение «HEY» кодируется в 16–разрядном образце качества CD с использованием метода LSB: при кодировании LSB идеальная скорость передачи данных составляет 1 кбит / с на 1 кГц. Однако в некоторых реализациях LSB–кодирования два младших значащих бита образца заменяются двумя битами сообщения. Это увеличивает объем данных, которые могут быть закодированы, но также увеличивает

количество результирующего шума в звуковом файле. Таким образом, перед принятием решения о работе LSB следует рассмотреть содержимое сигнала. Например, звуковой файл, записанный в оживленной станции метро, будет маскировать низкий уровень кодирования шума. С другой стороны, тот же шум будет слышен в звуковом файле, содержащем фортепианное соло.

Sampled audio stream(16bit)	HEY in binary	Audio stream with message encoded
1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0	0	1 0 0 1 0 1 0 0 0 1 0 0 1 1 0 0
1 1 1 0 1 0 1 0 1 1 1 1 1 1 1 1	1	1 1 1 0 1 0 1 0 1 1 1 1 1 1 1 1
1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1	0	1 0 0 0 0 0 0 0 0 0 0 1 1 0 1 1
0 1 1 1 1 1 1 0 0 1 0 1 0 1 0 1 0	0	0 1 1 1 1 1 1 0 0 1 0 1 0 1 0 1 0
0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1	1	0 0 0 0 0 0 1 1 1 0 1 0 1 1 0 1
0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 0 1 0 1 0 1 0 1 0 1 0 1
0 1 1 1 1 0 0 1 1 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 0 1 1 1 0 1 0 1 0 1 0
0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1	0	0 0 0 0 0 1 0 1 0 1 1 1 0 1 0 1
1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1	0	1 1 1 1 0 1 0 1 1 0 1 0 1 0 1 1
0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0	1	0 1 1 1 0 0 1 1 0 0 1 0 1 0 1 0
1 0 1 0 1 0 1 0 1 1 1 0 0 0 1 1 1	0	1 0 1 0 1 0 1 0 1 1 1 0 0 0 1 1 1
0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1	0	0 1 1 1 1 1 0 1 0 1 0 1 0 1 0 1
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0 0
0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0	1	0 1 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0
0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1 0	0	0 0 0 0 0 0 0 0 0 1 0 1 0 1 0 1 0
1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0	1	1 1 1 1 1 1 1 1 1 1 1 1 1 0 1 0
0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0
0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0	1	0 1 0 1 0 1 0 1 0 0 1 0 0 0 1 0
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1	0	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0 1
0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1	1	0 1 1 1 1 1 1 1 1 1 1 0 0 0 0 1
0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1	1	0 1 0 1 0 1 0 1 0 0 0 1 0 1 0 1
0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1	0	0 1 0 1 0 1 1 1 1 1 1 1 1 0 0 1
0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0	0	0 1 1 1 1 0 1 0 1 0 1 0 1 0 1 0
0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0	1	0 0 1 0 0 1 0 1 0 1 0 0 1 0 1 0

↑
LSB COLUMN

Рисунок 1.3 – Кодирование методом LSB

Чтобы извлечь секретное сообщение из звукового файла, закодированного в LSB, получателю нужен доступ к последовательности выборочных индексов, используемых в процессе внедрения. Обычно длина секретного сообщения, подлежащего кодированию, меньше, чем общее количество выборок в звуковом файле. Затем необходимо решить, как выбрать подмножество образцов, которые будут содержать секретное сообщение, и сообщать это решение получателю. Один простой способ – начать с начала звукового файла и выполнить кодирование LSB до тех пор, пока сообщение не будет полностью внедрено,

оставив оставшиеся образцы неизменными. Но это создает проблему безопасности, потому, что первая часть звукового файла будет иметь разные статистические свойства, чем вторая часть звукового файла, который не был изменен. Одним из решений этой проблемы является заполнение секретного сообщения случайными битами, так что длина сообщения равна общему количеству выборок. Но теперь процесс внедрения заканчивается тем, что он меняет гораздо больше выборок, чем передача требуемого секретного кода. Это увеличивает вероятность того, что злоумышленник будет подозревать тайный обмен данными.

Скрытие данных в младших значащих битах (LSB) аудиопоследовательностей во временной области является одним из простейших алгоритмов с очень высокой скоростью передачи данных дополнительной информации [2]. Кодировщик водяных знаков LSB обычно выбирает подмножество всех доступных звуковых образцов хоста, выбранных секретным ключом. Операция подстановки на LSB выполняется в том подмножестве, где бит, подлежащий скрытию, заменяет исходные значения бит. Процесс извлечения водяного знака прост, мы считывая значение этих битов из объекта звукового стегофайла. Поэтому декодеру нужны все образцы звукового сигнала, которые были использованы во время процесса внедрения. Случайный выбор образцов, используемых для внедрения, вводит белый гауссовский шум с низкой мощностью (AWGN). В психоакустической литературе хорошо известно, что человеческая слуховая система (HAS) очень чувствительна к AWGN. Этот факт ограничивает количество LSB, которые могут быть незаметно изменены во время внедрения водяных знаков. Основным преимуществом метода LSB-кодирования является битовая скорость канала с очень высоким уровнем водяного знака; использование только одного LSB аудио ввода хоста дает емкость 44,1 кбит / с (частота дискретизации 44 кГц, все сэмплы, используемые для скрытия данных) и низкая вычислительная сложность. Очевидным недостатком, является значительно низкая надежность,

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						12
Изм.	Лист	№ докум.	Подпись	Дата		

из-за того, что простые случайные изменения LSB уничтожают кодированный водяной знак. По мере увеличения количества используемых LSB во время LSB-кодирования и это тоже самое, что и увеличение глубины модифицированного слоя LSB, в следствии чего, вероятность того, что встроенное сообщение будет статистически обнаруживаемым, будет уменьшаться, а перцептивная прозрачность объектов стего будет уменьшена. Следовательно, существуют ограничение на глубину используемого слоя LSB в каждом образце хост-аудио, который может использоваться для скрытия данных. Субъективный тест на прослушивание показал, что в среднем максимальная глубина LSB, которая может использоваться для водяного знака на основе LSB, не вызывая заметного перцепционного искажения, когда используются 16 бит на выборочные аудиопоследовательности. Тестирование проводилось с большой коллекцией аудиоматериалов и людьми с различным опытом и музыкальным опытом. Ни одна из проверенных звуковых последовательностей не имела перцептуальных артефактов. Надежность водяного знака, внедренного с использованием метода LSB-кодирования, увеличивается с увеличением глубины LSB, используемой для скрытия данных. Поэтому улучшение устойчивости к водяным знакам, полученное путем увеличения глубины используемого слоя LSB, ограничено перцептивной прозрачностью.

1.2.2 Метод расширения спектра и его модификации

В контексте звуковой стеганографии метод базового расширенного спектра (SS) пытается максимально распространять секретную информацию в частотном спектре аудиосигнала. Это аналогично системе, использующей реализацию LSB-кодирования, которая случайным образом распространяет биты сообщения по всему звуковому файлу. Однако, в отличие от LSB-кодирования, метод SS распространяет секретное сообщение по частотным

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						13
Изм.	Лист	№ докум.	Подпись	Дата		

спектрам звукового файла, используя код, который не зависит от реального сигнала. В результате конечный сигнал занимает полосу пропускания, превышающую требуемую для передачи. В аудио стеганографии можно использовать две версии SS: схемы прямой последовательности и частоты прыжков. В SS с прямой последовательностью секретное сообщение распространяется с помощью константы, называемой скоростью элементарных посылок, а затем модулируется псевдослучайным сигналом. Затем он чередуется с сигналом покрытия. В SS с частотным прыжком частотный спектр аудиофайла изменяется так, что он быстро перескакивает между частотами. скрытия информации для стеганографии и цифрового водяного знака. Следующая процедурная диаграмма иллюстрирует дизайн этой системы применительно к аудио стеганографии.

В базовой схеме рисунок 1.4 вставка водяного знака в сжатом видео V выполняется путем извлечения закодированных 8x8 блоков аудио и обработки их вместе с соответствующими блоками сигнала W водяного знака. В частности, битовый поток разделяется на его основные компоненты, и только модули сигнала, закодированные в DCT, являются актуальными. Каждый закодированный блок представлен последовательностью кодов, каждая из которых, представляет один (начальный) –пары и один квантованный ненулевой коэффициент DCT текущего блока сигналов.

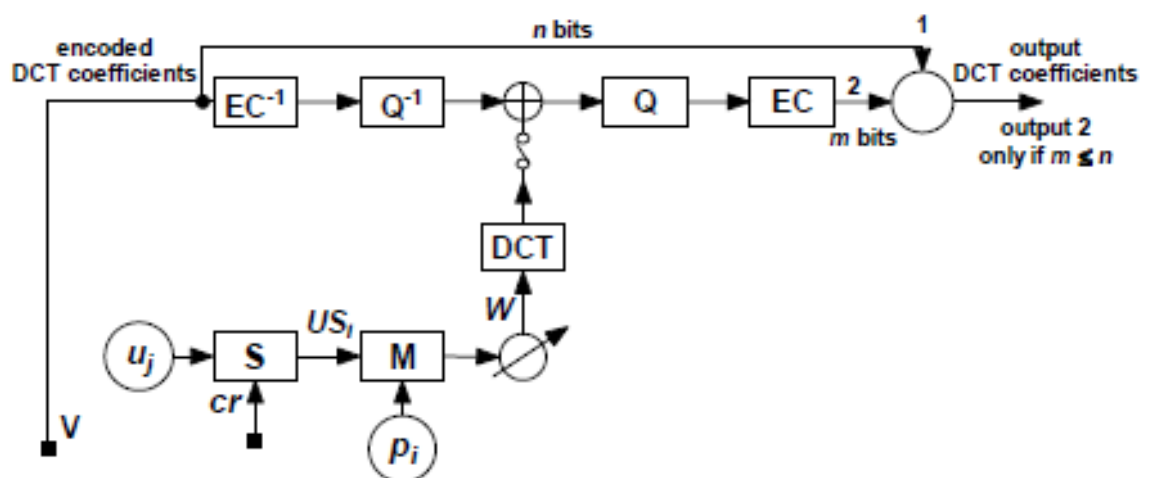


Рисунок 1.4: Схема базового водяного знака.

Предлагаемая процедура добавляет шумоподобный сигнал в обработанный блок кодированного видеосигнала блоком. Сигнал водяного знака рисунок 1.3.1 генерируется из последовательности бит $u_j \in \{-1,1\}$, который используется для идентификации пользователя и распространяется (S) на большой коэффициент cr , называемый скоростью элементарных посылок, таким образом получаем разброс последовательности:

$$us_i = u_j, j \times cr \leq i < (j + 1) \times cr \quad (1.5)$$

Затем шумоподобный сигнал генерируется посредством модуляции (M) последовательности с двоичной псевдошумовой последовательностью $p_i \in \{-1,1\}$, который в предлагаемом решении должен быть однозначно связан с защищенным аудио. Таким образом, как только защищенное аудио было выбрано, можно использовать псевдошумовую последовательность p_i , связанную с ней, для извлечения водяного знака и, следовательно, получить последовательность пользователей $u_j \in \{-1,1\}$.

С этой целью сигнал защищенного видео может быть скоррелирован с последовательностью p_i , над cr широким окном корреляции, и извлеченный водяной знак можно затем проанализировать, чтобы получить последовательность бит, идентифицирующую пользователя, который купил аудио. Наконец, стоит отметить, что последовательности u_j назначаются для идентификации пользователей в соответствии с методом анти-сговар и использование кода исправления ошибок.

Схема, приведенная на рисунке 1.3.1, базируется на простой формуле:

$$s = x + ut \quad (1.6)$$

где вектор x является сигналом хозяина, t – последовательность микросхем, построенная из p_i , u представляет бит из последовательности u_j , а вектор s

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						15
Изм.	Лист	№ докум.	Подпись	Дата		

является сигналом с водяными знаками.

В частности, (1.17) предполагает, что один бит информации из последовательности u_j встроен в вектор s , где значений cr в соответствии с общими методами SS. Однако фактически внедренная схема водяных знаков основана на небольшой модификации подхода SS, в качестве линейной версии усовершенствованной методики SS (ISS). Фактически, этот вариант предполагает, что амплитуда вставленной последовательности микросхем может изменяться по линейной функции

$$s = x + (au - \lambda x)t \quad (1.7)$$

где $x \triangleq \langle x, m \rangle / \langle m, m \rangle$ и $\langle x, m \rangle$ скалярное произведение определяется как:

$$\langle x, m \rangle \triangleq \frac{1}{cr} \sum_{i=0}^{cr-1} x_i m_i \quad (1.8)$$

На практике, выражение (1.19) также определяет номы, например когда используется $\langle x, x \rangle$.

Параметры a и λ контролируют и устраняют искажения по мере их появления. На самом деле, если y является доступной версией для s путем добавления к s шума n , моделируется как некоррелированный белый гауссовский случайный процесс, достаточно допустимая статистика для выведения водяного знака r :

$$r = \frac{\langle y, m \rangle}{\langle m, m \rangle} = au + (1 - \lambda x) + n \quad (1.9)$$

где $n \triangleq \langle n, m \rangle / \langle m, m \rangle$.

Поэтому, используя знания энкодера о сигнале, производительность

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						16
Изм.	Лист	№ докум.	Подпись	Дата		

системы водяных знаков. может быть повышена путем изменения энергии вставленного водяного знака для компенсации помех сигнала исходного. В частности, чем ближе λ к 1, тем больше влияние x удаляется из r . Детектор такой же, как и в методах водяных знаков SS, то есть обнаруженный бит является знаком r . Кроме того, традиционные методы SS можно получить, установив $a=1$ и $\lambda=0$.

Полученные результаты позволяют рассчитывать оптимальные значения и для системы водяных знаков. В частности, низкие значения вероятности ошибки могут быть достигнуты путем установки:

$$a = \sqrt{\frac{cr - \lambda^2 \sigma_x^2}{cr}} \quad (1.10)$$

Значение близко к 1 (т. е. в диапазоне 0: 9, 1) в предположении, что cr достаточно велико, а SNR выше 10 дБ.

1.2.3 Метод дискретно–косинусного преобразования и его модификации

Дискретное косинусное преобразование является методом преобразования сигнала в элементарные частотные составляющие. DCT может использоваться как для одномерных, так и для двумерных сигналов, таких как аудио и изображение, соответственно. Дискретное косинусное преобразование – это спектральное преобразование, обладающее свойствами дискретного преобразования Фурье. DCT использует только косинусные функции различных волновых чисел в качестве основных функций и работает с реальными оценками и спектральными коэффициентами.

В следующих, $f_{dct}(x)$ является исходной последовательностью, $C_{dct}(U)$, где DCT – коэффициенты последовательности.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						17
Изм.	Лист	№ докум.	Подпись	Дата		

$$Cdct(U) = a(u) \sum_{x=1}^{N_{It}-1} fdct(x) \cos \left[\frac{\pi(2x+1)u}{2N_{It}} \right], \text{ for } u = 0, 1, 2, \dots, N_{It} - 1 \quad (1.11)$$

$$fdct(x) = \sum_{u=1}^{N_{It}-1} a(u) Cdct(u) \cos \left[\frac{\pi(2x+1)u}{2N_{It}} \right] \text{ for } u = 0, 1, 2, \dots, N_{It} - 1 \quad (1.12)$$

$$a(u) = \begin{cases} \sqrt{\frac{1}{N_{It}}} & \text{for } u = 0 \\ \sqrt{\frac{2}{N_{It}}} & \end{cases} \quad (1.13)$$

Из уравнения 1.11 можно сделать вывод, что для $u = 0$ компонент является средним значением сигнала, также называемого как dc -коэффициент в литературе. И все остальные коэффициенты преобразования называются a -коэффициентами. Некоторые из важных применений DCT – сжатие сигнала. Наиболее полезными приложениями двумерного (2-d) DCT являются сжатие и шифрование сигнала. 1-й DCT-уравнения, рассмотренные выше, могут быть использованы для нахождения 2-d DCT, рассматривая каждую строку как индивидуальный 1-й сигнал.

Преобразование дискретных всплесков (DWT) является дисциплиной, способной давать частотно-временное представление любого сигнала. Начиная с исходного аудиосигнала S , DWT создает два набора коэффициентов, как показано на рисунке 1.5 Приблизительные коэффициенты A (низкие частоты) создаются путем пропускания сигнала S через фильтр нижних частот y . Детали коэффициенты D (высокие частоты) создаются путем пропускания сигнала S через фильтр низких частот g .

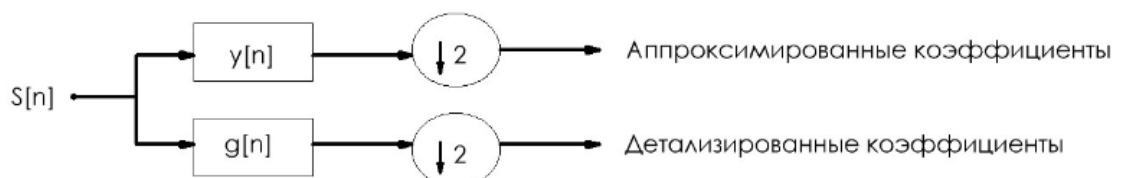


Рисунок 1.5 – Одноуровневое разложение DWT

В зависимости от приложения и длины сигнала часть низких частот может

быть разложена далее на две части высоких и низких частот. На рисунке 1.6 показано трехуровневое DWT–разложение сигнала S. Исходный сигнал S может быть восстановлен с использованием обратного процесса DWT.

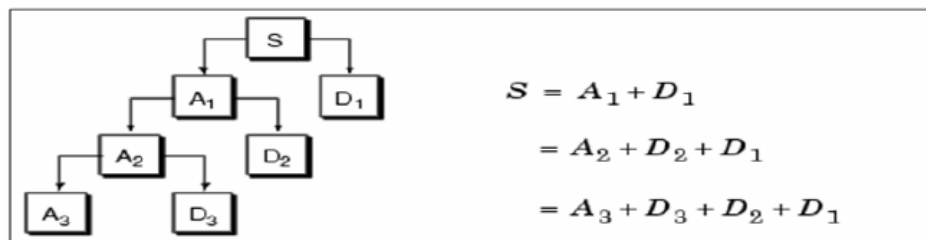


Рисунок 1.6 – Разложение DWT на три уровня

Благодаря превосходным свойствам пространственно–частотной локализации, DWT очень подходит для определения областей в звуковом сигнале, где водяной знак может эффективно внедряться.

Традиционные частотные преобразования; Преобразования FFT, DCT и DWT пытаются разложить изображение с точки зрения стандартного базового набора. Это необязательно должно быть оптимальным представлением для данного изображения. С другой стороны, разложение сингулярных значений (SVD) является численным методом для диагонализующих матриц, в которых преобразованная область состоит из базисных состояний, которые в некотором смысле являются оптимальными SVD матрицы NxN рисунок 1.7, где A определяется операцией:

$$SVD(A) = U * S * V^T \quad (1.14)$$

$$\begin{bmatrix} V_{1,1} & \dots & V_{1,n} \\ V_{2,1} & \dots & V_{2,n} \\ \dots & \dots & \dots \\ V_{n,1} & \dots & V_{n,n} \end{bmatrix}^T \begin{bmatrix} \sigma_{11} & 0 & 0 & 0 \\ 0 & \sigma_{22} & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \sigma_m \end{bmatrix} \begin{bmatrix} U_{1,1} & \dots & U_{1,n} \\ U_{2,1} & \dots & U_{2,n} \\ \dots & \dots & \dots \\ U_{n,1} & \dots & U_{n,n} \end{bmatrix}$$

Рисунок 1.7 – SVD–операция $SVD(A) = U S V^T$

Диагональные элементы S называются сингулярными значениями A и предполагаются расположенными в порядке убывания $\sigma_i > \sigma_{i+1}$. Столбцы U -матрицы, называются левыми сингулярными векторами, а столбцы матрицы V называются правыми сингулярными векторами A .

В силу того, что незначительные изменения в элементах матрицы S не влияют на визуальное восприятие качества контейнера, алгоритмы водяного знака, основанные на SVD , добавляют информацию водяного знака к сингулярным значениям диагональной матрицы S таким образом, чтобы соответствовать требованиям незаметности (неразборчивости) и надежности для эффективных алгоритмов цифровых водяных знаков.

В предлагаемой схеме рисунок 1.8 используется каскад двух преобразований; дискретное вейвлет-преобразование и преобразование декомпозиции сингулярного значения. Схема описанная в этом разделе, излагает основные этапы двух процедур; процедуры внедрения водяных знаков и процедуры извлечения водяных знаков.

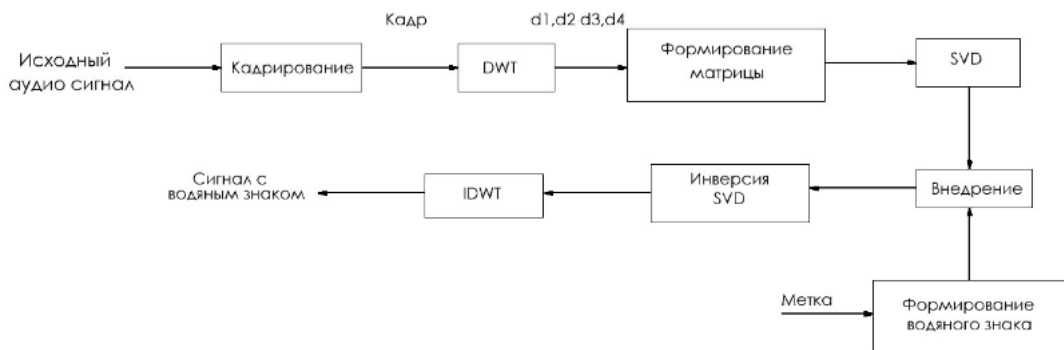


Рисунок 1.8 – Структурная схема внедрения водяных знаков

Процедуру внедрения водяного разложить на несколько этапов:

Этап № 1. Преобразуем водяной знак двоичной метки в одномерный вектор W длинны $m \times x$

$$w_t = \{[0,1] | 1 \leq t \leq (m \times n)\} \quad (1.16)$$

Этап № 2. Возьмем за образец исходный аудиосигнала с частотой

дискретизации 44100 выборок в секунду. Затем разбиваем дискретизированный файл на фреймы, каждый из которых имеет 50000 выборок. Суммирование N кадров составляет общий дискретизированный аудиосигнал, как показано в следующем уравнении:

$$A = \sum_{i=1}^N A_i \quad (1.17)$$

Этап № 3. Выполнить четырехуровневое преобразование DWT на каждом кадре A_i . Эта операция создает пять поддиапазонов с несколькими разрешениями: D1, D2, D3, D4 и A4. Ds представляют собой поддиапазоны детализации, а A4 представляет собой поддиапазон аппроксимации.

Этап №4: Расположим четыре подканала D1, D2, D3 и D4 в матричной форме, как показано на рисунке 1.9 ниже. Затем матрица с именем DC имеет размер $4 \times (L / 2)$, где L – длина каждого кадра.

D1							
D2				D2			
D3		D3		D3		D3	
D4	D4	D4	D4	D4	D4	D4	D4

Рисунок 1.9 – Разложение подканала D1, D2, D3 и D4

Этап № 5: Разложим матрицу DC с помощью оператора SVD. Эта операция позволяет вывести три ортонормальные матрицы S, U и V^T следующим образом:

$$DC = U \times S \times V^T \quad (1.18)$$

где S – следующая 4×4 диагональная матрица:

$$S = \begin{pmatrix} S_{11} & 0 & 0 & 0 \\ 0 & S_{22} & 0 & 0 \\ 0 & 0 & S_{33} & 0 \\ 0 & 0 & 0 & S_{44} \end{pmatrix} \quad (1.19)$$

Диагональные элементы S_{ii} представляют собой ненулевые сингулярные значения матрицы DC. Значение S_{11} используется для внедрения, как будет показано ниже, и поэтому его необходимо сохранить для последующего использования в процедуре извлечения водяных знаков.

Этап № 6: Вставим биты водяного знака двоичной метки в аудиосигнал, преобразованный в DWT–SVD, в соответствии со следующей формулой:

$$S_{11w} = S_{11} \times (1 + a \times w(n)) \quad (1.20)$$

где $w(n)$ – бит водяного знака: 0 или 1, a – интенсивность водяного знака, s_{11} – верхнее левое значение в матрице S а S_{11w} – водяной знак в S_{11} .

Этап №7: Произведем конечный звуковой сигнал с водяным знаком следующим образом: Применим инверсную операцию SVD с использованием матриц U и V^T , которые остались неизменными, и S –матрицу, которая была модифицирована согласно уравнению (1.8). Матрица CDW представляет собой DC тока с водяным знаком уравнения (1.6)

$$CDW = U \times S_W \times V^T \quad (1.21)$$

Примените обратную операцию DWT на матрицу CDW , чтобы получить каждый водяной знак A_{iw} . Общий звуковой сигнал A_W с водяным знаком получен путем суммирования всех кадров с водяными знаками.

$$A_W = \sum_i A_{tw} \quad (1.22)$$

Процедура извлечения водяного знака требует от звукового сигнала с водяными знаками дополнительный вес каждого кадра исходного звукового сигнала. Процедура показана схеме на рисунке 1.10, и детально описаны в следующих этапах

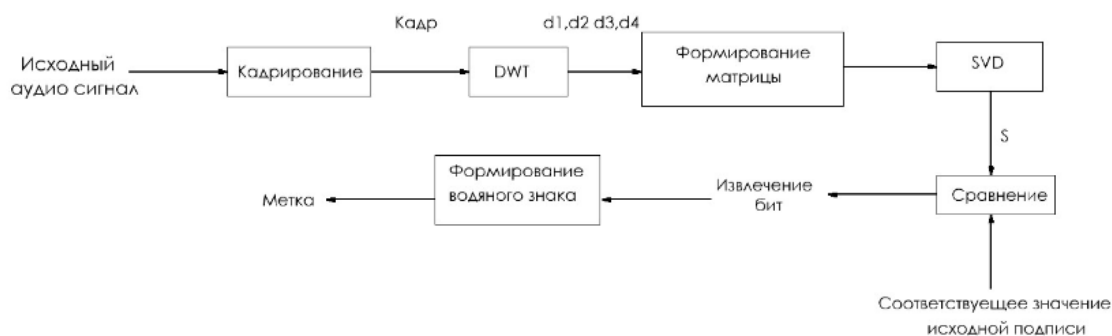


Рисунок 1.10 – Процедура извлечения водяных знаков

Этап №1: Выполните этапы с 1 по 5 процедуры вложения до получения S–матрицы для всех кадров звукового сигнала с водяным знаком.

Этап №2: Если исходный аудиосигнал использовался вместо исходных сингулярных значений для каждого кадра, тогда следует выполнить этапы с 1 по 5 процедуры вложения до получения S–матрицы для всех кадров исходного сигнала.

Этап №3: Определить количество бит $w(n)$ водяного знака, напомнив, что для вставки бит в кадр S_{11} был изменен в соответствии с уравнением (1.8). Следовательно, бит $w(n)$ водяного знака будет иметь значение 1, если S_{11w} / S_{11} равно 1,2, а 0, если s_{11w} / s_{11} равно 1,0.

Этап №4: Собрать извлеченные биты из отдельных кадров и создав исходный водяной знак двоичной метки.

Наконец, можно отметить, что предложенные схемы удовлетворяют требуемым функциям оптимального внедрения в аудио водяных знаков, которые были установлены МФЗ. МФЗ гласит, что водяной знак не должен ухудшать восприятие звука, алгоритм должен предложить больше, чем 20 дБ С/Ш, водяные знаки должны быть способны противостоять большинству

распространенных процессов аудио обработки и атак, а водяной знак должен предотвратить несанкционированное извлечение информации.

1.3 Методы оценки скрытности

Среднеквадратическая ошибка (MSE), отражает изменение энергии пикселей:

$$MSE = \sum_{n=1}^N (x_n - \tilde{x}_n)^2 \quad (1.23)$$

где x_n – амплитуды исходного отрезка данных; \tilde{x}_n – амплитуда отрезка данных, содержащего дополнительную информацию; N – количество отсчетов анализируемых сигнальных отрезков.

Математическое представление PSNR выглядит следующим образом:

$$PSNR = 20 \log_{10} \left(\frac{MAX_f}{\sqrt{MSE}} \right) \quad (1.24)$$

где MSE (средняя квадратная ошибка):

$$MSE = \left(\frac{1}{(m \times n)} \times \text{sum}(\text{sum}((f - g)^2)) \right) \quad (1.25)$$

Существует много новых методов стеганографии, которые обеспечивают лучшую защиту цифровых данных. В этой работе был проведен опрос по различным методам аудио стеганографии. Аудио-стеганография реализована с использованием двух подходов, основанных на преобразовании: быстрое преобразование Фурье и QR-подход. Внедрение FFT в аудио стеганографии демонстрирует, что частотная область аудиосигнала может быть эффективно использована для скрытия секретного сообщения. Но это не сложный алгоритм, так как изображение низкого качества восстанавливается. Низкое значение PSNR означает, что восстановленный сигнал более искажен шумом.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						24
Изм.	Лист	№ докум.	Подпись	Дата		

Оценка, определяющая порядок изменения энергии по отношению к общей энергии (SNR). Как определено выше, отношение сигнал / шум для встроенного водяного знака вычисляется как:

$$SNR = 10 \log_{10} \frac{\sum n \times x^2(n)}{\sum n [x^2(n) - y^2(n)]} \quad (1.26)$$

где $x(n)$ представляет образец входной аудиопоследовательности, а $y(n)$ обозначает образец звука с модифицированными LSB.

Вероятность ошибки (BER):

$$BER = \frac{1}{N} \sum_{m=1}^M (b_m \oplus \tilde{b}_m) \quad (1.27)$$

где N – количество кодируемых/декодируемых бит; \oplus – операция «сумма по модулю два»; b_m – кодируемый бит; \tilde{b}_m – декодируемый бит.

Производительность алгоритмов водяного знака звука обычно оценивается в отношении верности, незаметности (неразборчивости) и надежности. В дальнейшем мы дадим краткое описание каждой метрики.

Незаметность связана с перцепционным качеством данных встроенных водяных знаков в исходном аудиосигнале. Это гарантирует, что качество сигнала не будет заметно искажено, а водяной знак незаметен для слушателя. Для измерения незаметности мы используем соотношение сигнал / шум (SNR) как объективную меру и тест на прослушивание как субъективную меру. Отношение сигнал/шум (SNR) – это статистическая разница, которая используется для измерения подобия между неискаженным исходным аудиосигналом и искаженным звуковым сигналом с водяными знаками. Вычисление SNR выполняется в соответствии с уравнением (1.25), где A соответствует исходному сигналу, а A' соответствует поп-сигналу с водяными знаками.

$$SNR(db) = 10 \log_{10} \frac{\sum_n A_n^2}{\sum_n (A_n - A'_n)^2} \quad (1.28)$$

Хотя SNR – это простой способ измерения шума, введенного встроенным водяным знаком, и может дать общее представление о незаметности, он не учитывает специфические характеристики слуховой системы человека. Поэтому мы также использовали измерение качества восприятия звука.

В показано, что соотношение между RAQM и средним значением оценки (MOS) составляет 0,98. Поэтому в наших экспериментах оценки RAQM будут отображены на шкалу оценки MOS, которая показана в таблице 1.1.

Таблица 1.1 - Шкала оценки MOS.

Уровни MOS	Описание
1	Незаметный
2	Восприимчивый, но не раздражающий
3	Немного раздражает
4	Раздражает
5	Очень раздражает

1.4 Постановка задач исследования

Основной задачей работы является исследование и выбор оптимального метода скрытия информации в сигнале. С целью повышения устойчивости к сжатию сигнала или к вредоносным атакам. Увеличение шансов слышимого искажения, если метод вставки водяного знака неправильно настроен. Существует компромисс между высоким порогом маскировки и слышимостью. Наличие порога маскировки как можно выше, сохраняя искажение как незаметное, являются ключевыми проблемами при использовании психоакустической модели.

2. РАЗРАБОТКА АЛГОРИТМОВ И ОЦЕНКА ИХ РАБОТОСПОСОБНОСТИ

2.1 Описание алгоритмов скрытного кодирования и декодирования сигналов

Биты встраиваемого сообщения кодируются значениями числа бит, необходимых для кодирования коэффициентов дискретно-косинусного преобразования (ДКП) и масштабирования кодом Хаффмана. Если необходимо закодировать нулевой бит, то значение этого числа должно быть четным, а если единичный, то нечетным. Необходимую четность получают следующим образом: уменьшается шаг квантования; осуществляется квантование коэффициентов ДКП с новым шагом; подсчитывается число бит, необходимых для кодирования коэффициентов ДКП, и суммируется с числом бит, необходимых для кодирования коэффициентов масштабирования. Если результат соответствует необходимой четности и уровень шума квантования ниже порогового значения, то осуществляется переход к кодированию следующего бита, если же нет, то уменьшается шаг квантования, и процедура повторяется. Пороговое значение вычисляется психоакустической моделью. Блок-схема алгоритма встраивания одного бита информации представлена на рис. 2.1

Исходными данными для работы программы являются: файл ИКМ, 16-битное кодирование отсчетов, частота дискретизации 44 100 Гц (файл формата wav); текстовый файл, содержащий встраиваемое сообщение; секретный пароль.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						27
Изм.	Лист	№ докум.	Подпись	Дата		

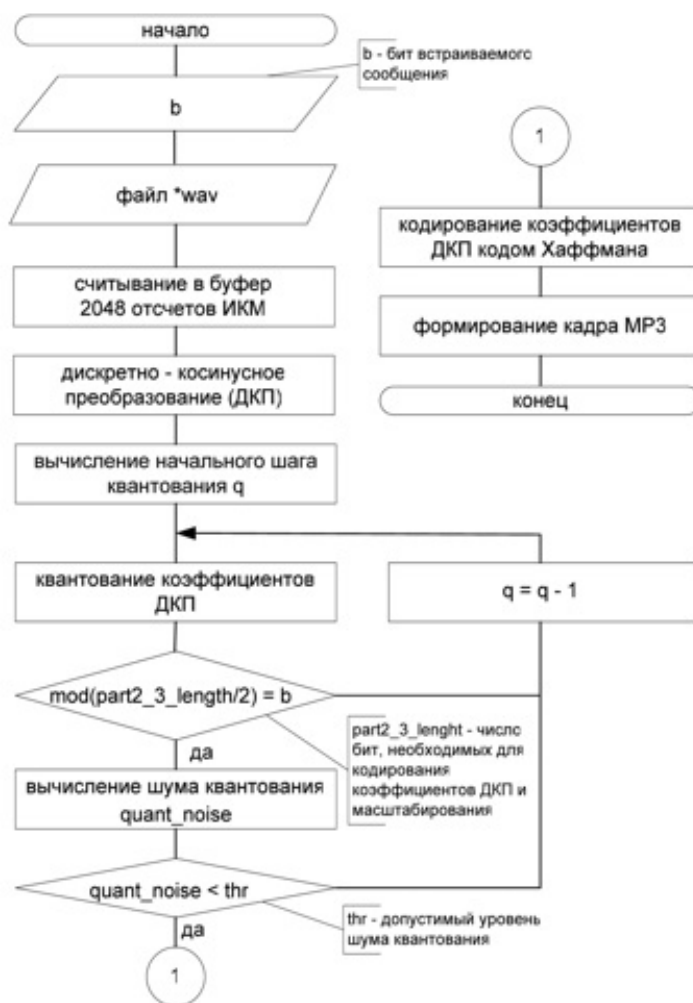


Рисунок 2.1 – Блок-схема алгоритма алгоритмов стеганографического кодирования

2.2 Методика оценки работоспособности алгоритмов стеганографического кодирования и декодирования сигналов

Приводится методика оценки скрытности и стойкости, для визуального анализа и анализа на основании выбранных мер

В этой работе мы изучаем применение меры среднего структурного сходства (MSSIM) [8], разработанной для оценки качества восстановления сжатых сигнала, к проблеме оценки качества звука. MSSIM – это статистический метод, который сравнивает соответствующие сегменты данного ухудшенного изображения с теми же сегментами исходного изображения, и было показано, что он дает результаты, которые точно соответствуют

субъективным результатам теста.

Индекс сходства основан на идее, что мера изменения структурной информации является хорошим приближением к воспринимаемому изменению качества. Например, звуковые последовательности, соответствующие спектрограммам на рис. 1 (а) и (б), имеют одинаковые ошибки среднего квадрата, но очень разные средние оценки (MOS) и показатели индекса подобия структурных единиц. Последовательность на рисунке 1 (а) имеет частоты, усеченные выше 8 кГц, Вт. исходный (опорный) сигнал и имеет постоянное шипение, генерируемое аддитивным гауссовским шумом. С другой стороны, последовательность на рисунке 1 (б) генерируется сжатием аудиопоследовательности с алгоритмом AAC–BSAC со скоростью 16 кбит / с. Эта последовательность содержит много кликов и clacks, которые гораздо более заметны, чем постоянное слышимое шипение последовательности (а). В методе структурного сходства учитываются три различные измеренные различия между оригинальными и восстановленными сигналами: яркость, контраст и структура. Светимость представляет собой сравнение средних значений сигналов. Если x и y – соответствующие сегменты звука с N выборками каждый, сравнение светимости дается формулой

$$l(x, y) = \frac{2\mu_x\mu_y + C1}{\mu_x^2 + \mu_y^2 + C1} \quad (2.1)$$

где $\mu = \frac{1}{N \sum_i^N x_i}$, $\mu_y = 1/N \sum_i^N y_i$ и $C1 (K_1 L^2)$, где $K_1 \ll 1$. Динамический диапазон элементов x и y обозначается переменной L .

Игнорируя $C1$, форма (1) очень похожа на форму коэффициента корреляции, кроме как по отношению к двум средним. Сравнение яркости не особенно полезно для аудио, так как средние значения не сильно меняются даже при большой деградации в звуковых последовательностях (все аудиопоследовательности по существу равны нулю по длине). Неудивительно,

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						29
Изм.	Лист	№ докум.	Подпись	Дата		

что в разделе 5 мы находим, что когда относительный вес светимости оптимизирован для субъективных данных аудио–теста, он мал. Сравнение контраста или дисперсии определяется аналогично сопоставлению яркости, данному (1), но относительно относительных стандартных отклонений двух сегментов: т. е.

$$c(x, y) = \frac{2\sigma_x\sigma_y - C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad (2.2)$$

где $\sigma_x = \left(1/(N - 1) \sum_{i=1}^N (x_i - \mu_x)^2\right)^{\frac{1}{2}}$, $\sigma_y = \left(1/(N - 1) \sum_{i=1}^N (y_i - \mu_y)^2\right)^{\frac{1}{2}}$ и $C_2 = (K_2L)^2$ где $K_2 \ll 1$.

Сравнение структуры выполняется после локального среднего вычитания и локальной нормировки дисперсии. Сравнение структуры измеряет сходство между двумя N–мерными единичными векторами, $\bar{x} = (x - \mu_x)/\sigma_x$ и $\bar{y} = (y - \mu_y)/\sigma_y$, и это просто точечный продукт между двумя единичными векторами $\bar{x} \times \bar{y} = \bar{x}^t \times \bar{y}$ что является эффективным способом количественной оценки структурного сходства между ними. Это эквивалентно коэффициенту корреляции между исходными x и y. Структурная мера в терминах исходных векторов x и y задается формулой

$$s(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \quad (2.3)$$

где $\sigma_{xy} = \frac{1}{(N-1)} \sum_{i=1}^N (x_i - \mu_x)(y_i - \mu_y)$ и $C_3 = (K_3L)^2$ где $K_3 \ll 1$.

Сравнение подобия (1), (2) и (3) также удовлетворяет следующим свойствам (где «S» ниже может быть либо «l», «с», либо «s»):

1. Симметрия: $S(x, y) = S(y, x)$,

2. Ограниченность: $S(x, y) \leq 1$,

3. Уникальный максимум: $S(x, y) = 1$ if и только если каждый элемент из x равно соответствующему элементу y.

									Лист
									30
Изм.	Лист	№ докум.	Подпись	Дата	<i>11070006.11.03.02.826.ПЗВКР</i>				

Наконец, три компонента объединяются, чтобы получить общую меру подобия для сегмента,

$$S(x, y) = f(l(x, y)c(x, y)s(x, y)) = l(x, y)^{\alpha}c(x, y)^{\beta}s(x, y)^{\gamma} \quad (2.4)$$

где $\alpha > 0$, $\beta > 0$ и $\gamma > 0$ используются для корректировки относительной важности трех компонентов. Функция в (4) также удовлетворяет трем свойствам, перечисленным выше.

Меры SSIM, описанные выше, явно статистически обоснованы. Хотя можно применить SSIM для всей аудиопоследовательности для извлечения одного номера качества для этой последовательности, информация о локальной структуре будет потеряна, а сложность будет довольно высокой. Вместо этого мы вычисляем среднее значение SSIM, взятое по сегментам исходных данных. Это выгодно как с точки зрения сложности, так и потому, что оно допускает возможность неравного взвешивания сегментных значений SSIM (например, значения в конце последовательности могут быть более взвешены, чтобы учесть, что воспринимаемое качество в последнее время слышимый звук в наибольшей степени влияет на мнение слушателя о его качестве). Эта глобальная мера называется средним SSIM или MSSIM.

Структуру в аудио можно рассматривать двумя способами. В первом случае мы предполагаем, что структура зависит от каждой временной выборки и ее положения относительно небольшой временной окрестности проб вокруг нее. Чтобы применить MSSIM с этой точки зрения, мы разбиваем последовательности на временные кадры длиной 128 с перекрытием 50%, а затем применяем SSIM к каждому кадру отдельно. Среднее значение SSIM вычисляется путем усреднения отдельных значений SSIM для каждого кадра. Это сравнивает только временную структуру аудиопоследовательностей. Мы ссылаемся на этот метод как временный MSSIM (T-MSSIM). Во втором подходе мы применяем частотно-временное преобразование к звуковым

последовательностям. В частности, мы используем 256–точечное модифицированное дискретное косинусное преобразование (MDCT) с 50% перекрывающимся окном. Это означает, что аудиоданные представляют собой временную декомпозицию. Очевидно, что это представление одномерных аудиопоследовательностей аналогично изображению, как показано на рисунке 1. Применяя SSIM к двумерным блокам частотно–частотного представления, мы можем оценивать структурные сходства как во временной, так и в частотной областях одновременно, Мы будем ссылаться на этот метод как временный MSSIM (TF–MSSIM). MDCT, используемый здесь, может рассматриваться как критически–подвыборный квадратный фильтр–фильтр (QMF). В нашем случае мы реализуем MDCT с использованием синусоидального окна с последующим преобразованием косинуса. Входной кадр имеет 50% перекрытие с каждым смежным временным кадром.

Мы используем семь различных моноауральных аудиопоследовательностей, отобранных на частоте 44,1 кГц для следующих экспериментов. Для генерации различных наборов тестов мы модифицируем эти аудиопоследовательности, добавляя различные типы шумов, ограничивая полосы звуковых последовательностей и применяя различные алгоритмы сжатия звука. Результаты субъективного теста, используемые для сравнения результатов MSSIM с результатами других показателей, получены у 15 испытуемых с использованием протокола MUSHRA (Multi Stimulus test with Hidden Reference and Anchor) [9]. Для T–MSSIM звуковые последовательности разбиваются на временные рамки по 128 выборок каждый. В начальном тестировании значения α , β и γ просто устанавливаются на 1, что означает, что каждая из трех компонент метрики одинаково взвешена. Рисунок 2 показывает график рассеяния временного MSSIM в отношении субъективных результатов теста для 17 разных случаев. Сплошная линия представляет собой линию регрессии между MSSIM и субъективными результатами.

Таблица 2.1. Экспоненциальные веса, полученные для различных компонентов MSSIM

Параметры	T-MSSIM	TF-MSSIM
α	0.2	0
β	0.5	0.8
γ	0.7	0.2

Полученный коэффициент корреляции равен 0,98, что показывает, что MSSIM и субъективные тесты сильно коррелированы. Однако из линии регрессии мы видим, что в данных MSSIM имеется смещение 0,21.

Аналогично, на рисунке 3 показан график рассеяния для TF-MSSIM в отношении субъективных результатов теста. Временно-частотное представление получается путем выполнения 256-точечного MDCT с перекрытием 128 выборок. Размер отдельного блока, по которому выполняется SSIM, имеет размер 8×8 выборок. Коэффициент корреляции, полученный путем сравнения временного MSSIM, равен 0,976, что подразумевает хорошую корреляцию между MSSIM и субъективными тестами. T-MSSIM и TF-MSSIM, по-видимому, одинаково хорошо работают на основе коэффициента корреляции по отношению к субъективным данным. Из (2.4) мы знаем, что параметры α , β и γ управляют относительной важностью средних, дисперсионных и структурных компонентов SSIM. Чтобы получить значения этих параметров, чтобы MSSIM соответствовал результатам субъективных тестов, мы выполняем аппроксимацию наименьших квадратов следующим образом. Мы предполагаем, что MSSIM приблизительно равен взвешенному произведению среднего значения компонентов светимости, контраста и структуры, т.е.

$$S_m(x, y) \approx l_m(x, y)^{\alpha} \times c_m(x, y)^{\beta} s_m(x, y)^{\gamma} \quad (2.5)$$

Подстрочный индекс m в (2,5) означает среднее из трех компонентов. Взяв натуральный логарифм по обе стороны от (2.5), получим линейное уравнение.

$$\ln S_m(x, y) = a \ln l_m(x, y) + \beta \ln c_m(x, y) + \gamma \ln s_m(x, y) \quad (2.6)$$

Из которых можно найти наименьшее квадратное приближение экспоненциальных параметров, при этом считая параметры положительными. В таблице 2.1 приведены значения параметров для временных и частотно–временных случаев. Из этой таблицы видно, что средний или яркостной компонент взвешен очень низко для временного и частотно–временного случаев. В T–MSSIM структурный компонент подчеркивается больше, чем компонент дисперсии или контраста, в то время как TF–MSSIM точно противоположный. На рисунках 2.3 и 2.4 показаны графики разброса результатов субъективных испытаний по отношению к оптимизированным по времени временным и временным MSSIM соответственно. Набор тестов, представленный на этих графиках, отличается от тех, которые используются для оценки весов. Коэффициенты корреляции для взвешенных временных и временных MSSIM составляют 0,998 и 0,988 соответственно. Из графиков мы видим, что постоянное смещение уменьшается и что коэффициенты корреляции не значительно улучшились.

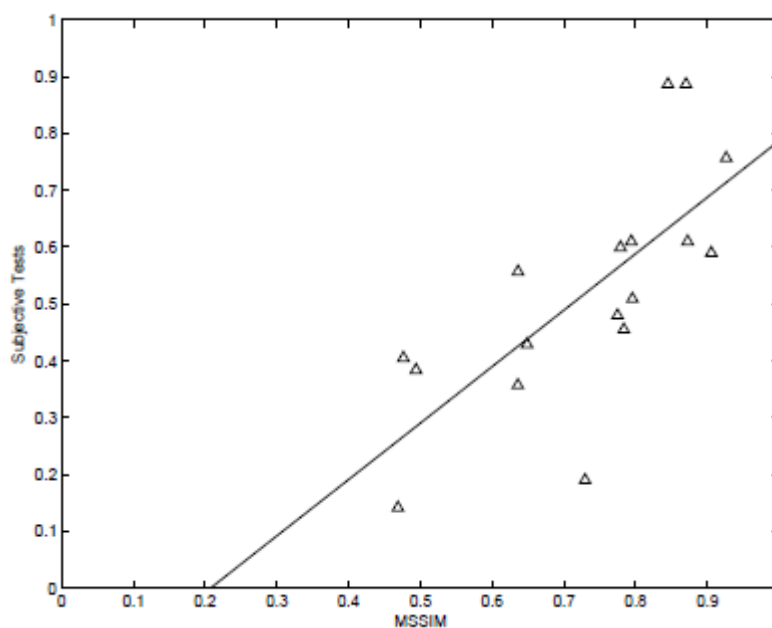


Рисунок 2.2– Диаграмма рассеяния субъективных результатов теста против T–MSSIM

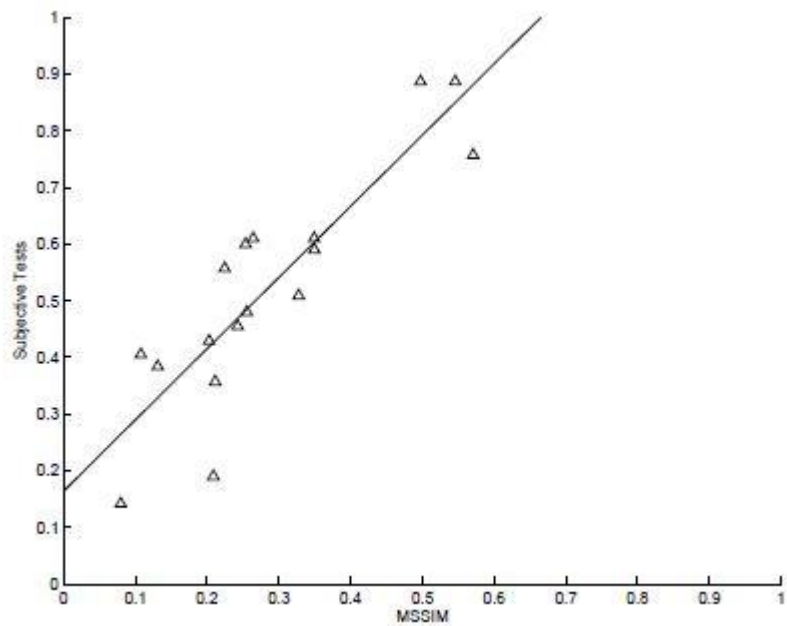


Рисунок 2.3–Диаграмма рассеяния субъективных результатов теста против TF–MSSIM

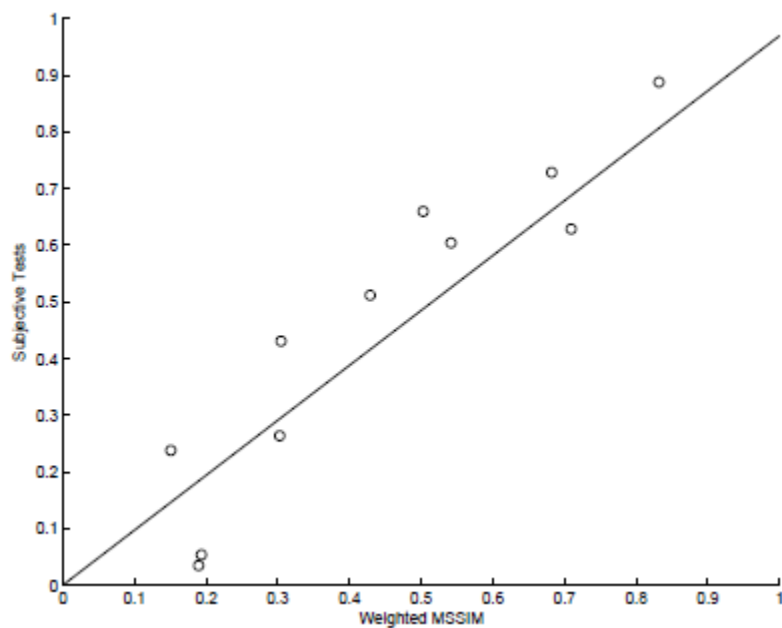


Рисунок 2.4 – Диаграмма рассеяния субъективных результатов теста Vs. T–MSSIM после оптимизации

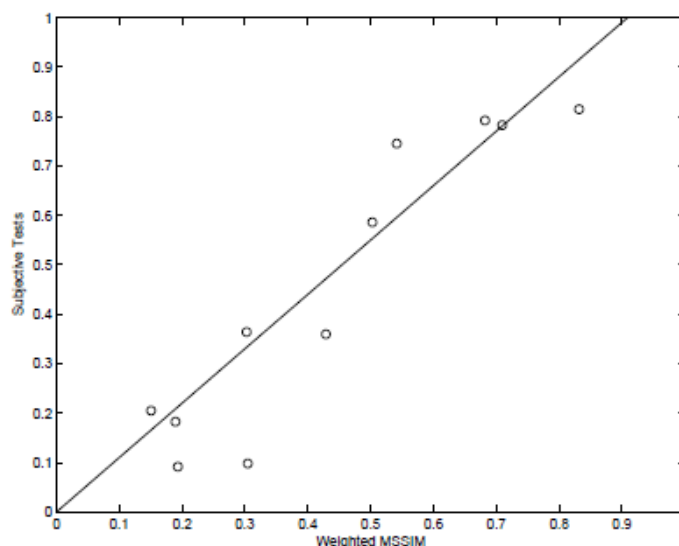


Рисунок 2.5 – Диаграмма рассеяния субъективных результатов теста Vs. TF–MSSIM после оптимизации

В этой работе мы описываем использование MSSIM в контексте оценки качества звука. Мы представили два разных способа применения MSSIM к аудиоданным.

Поскольку MSSIM является дифференцируемым, мы можем как максимизировать, так и минимизировать его, сохраняя постоянную MSE для создания пар аудиопоследовательностей, которые затем могут быть субъективно оценены: если MSSIM является хорошей перцептивной метрикой, такие минимальные / максимальные оптимизированные сопоставления восприятия должны сделать это очень очевидным. Кроме того, если MSSIM можно показать действительно хорошим предсказателем качества восприятия звука, то использование его вместо моделей маскировки частоты в аудиокодеках может значительно упростить их реализацию

2.3 Результаты оценки работоспособности и эффективности алгоритмов

Цифровая обработка Аудио Матлаб поддерживает многоканальный Wave Формат с 16 бит на Сэмпл [6]. Для того чтобы загрузить звуковой файл, вы

можете использовать “[Г, Ф, Nbits] = wavread (wave_filename)”, где wave_filename—это название файла в Wave-файл, г выборки данных с Размер Кол-во проб Кол-во каналов, ФС (в Гц), Частота дискретизации, и Nbits количество битов на выборку, используемые для кодирования данных в файле. Значения амплитуды в г вектора приведены к диапазону [-1, +1] по формуле, $G = X / [2(Nbits-1)] - 1$, где x—это неподписанных Nbits целое выражение. Например, пока x 128 с Nbits = 8, Y равно 0. Чтобы создать звуковой файл и сохранить его на жестком диске, вы можете использовать “wavwrite(Г, Ф, Nbits, wave_filename)”. Чтобы playbackthe сигнала в вектор Y, кнопками “звук (Г, Ф, Nbits)”.

Измененный алгоритм водяного знака LSB был протестирован на 11 звуковых последовательностях из разных музыкальных стилей (поп, рок, техно, джаз). Аудио фрагменты были выбраны так, чтобы они представляли широкий диапазон музыкальных жанров, то есть аудиоклипов с различными динамическими и спектральными характеристиками. LSB.

2.4 Основные результаты и выводы

Экспериментальные результаты показывают, что оба этих метода одинаково эффективны при поиске качества звука. Однако оптимальные веса, используемые для объединения трех компонентов SSIM, различны для каждого случая. Оба эти метода имеют хорошую корреляцию с субъективными данными даже с равными весами. Все музыкальные фрагменты были отмечены водяным знаком с использованием предложенного и модифицированного алгоритма водяных знаков LSB. Они составляли аудиофайлы с частотой дискретизации 44,1 кГц, представленные 16 бит на выборку. Продолжительность образцов составляла от 10 до 15 секунд.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						37
Изм.	Лист	№ докум.	Подпись	Дата		

3 КОНЦЕПЦИЯ ПРОТОТИПА И ОЦЕНКИ ЕГО РАБОТОСПОСОБНОСТИ

В данном разделе производится оценка работоспособности методов скрытия данных в сигнале, разработка программной поддержки этих метода и предложено оптимальное решение поставленной задачи.

3.1 Построение архитектуры программной реализации

На рисунке 3.1 представлена структурная схема программной поддержки скрытного кодирования контрольной информации в звуковом сигнале, созданная на основе обзореваемых алгоритмов.

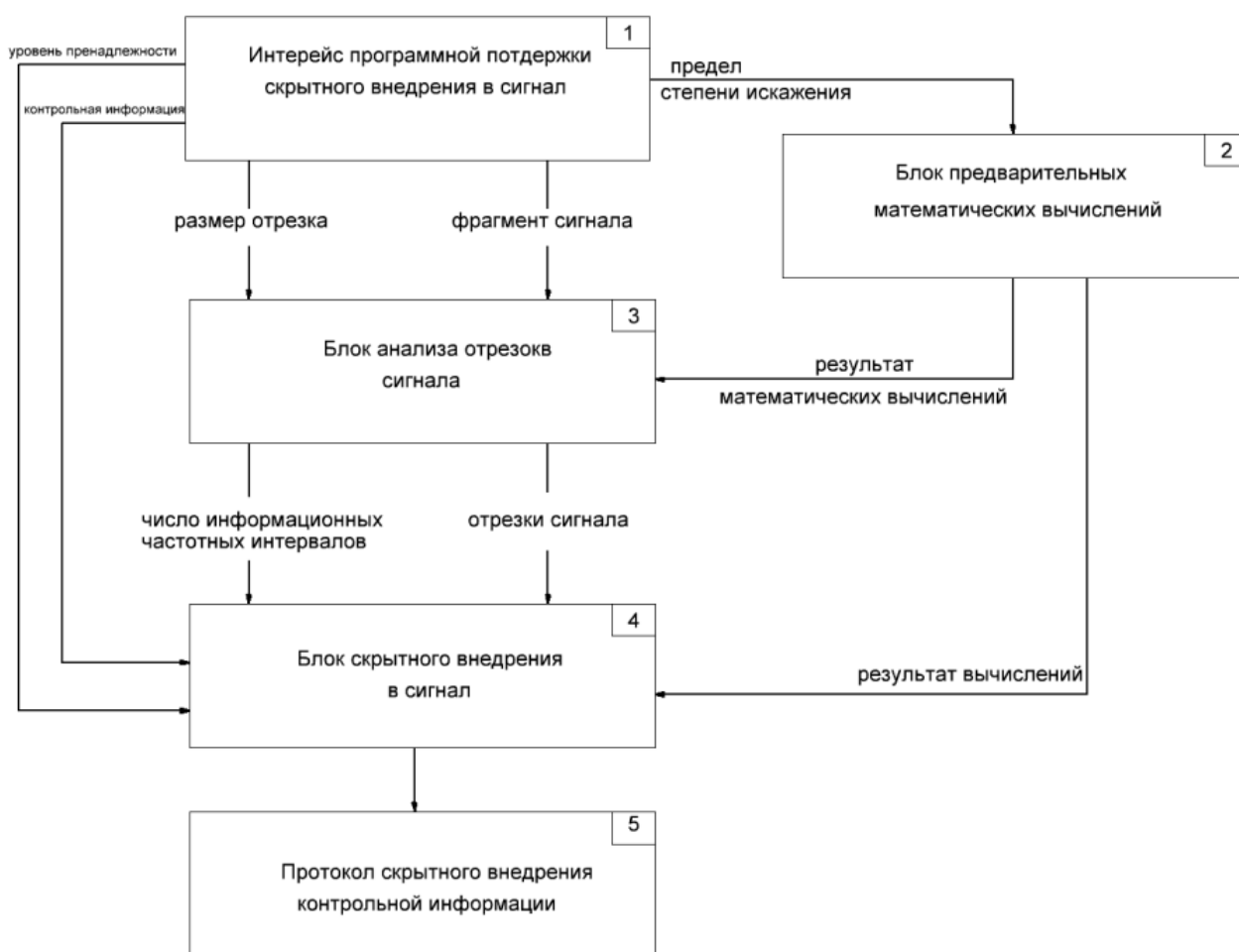


Рисунок 3.1 – Структурная схема программной поддержки скрытного кодирования контрольной информации

Разработанная программная поддержка метода скрывающего кодирования контрольной информации, позволяет при скрытном внедрении использовать параметры скрытности и стойкости, определяемые оператором.

3.2 Результаты экспериментальной оценки работоспособности и описание результатов работы

На основе существующего метода LSB скрытия информации в сигнале, был разработан алгоритм, выполнена оценка его работоспособности, результаты приведены в таблице 3.1. Исходным материалом является файл формата wav с частотой дискретизации 44 100 Гц, изменяемым параметром является количество бит в которые внедряется информация.

Таблица 3.1 – Оценка работоспособности алгоритма LSB

Кол- во бит	СКО	SNR	r
1	2,42E-02	0,015	0,999
2	3,33E-02	0,022	0,997
3	4,69E-02	0,032	0,988
4	5,86E-02	0,038	0,986
5	7,06E-02	0,041	0,910
6	8,62E-02	0,087	0,810
7	9,75E-02	0,092	0,725
8	0,108002	0,107	0,707
9	0,120821	0,121	0,634
10	0,130809	0,132	0,574
11	0,141723	0,141	0,488
12	0,152101	0,154	0,455
13	0,156449	0,177	0,421
14	0,159938	0,185	0,375
15	0,177789	0,193	0,364

Реализован алгоритм скрытия данных методом широкого спектра (SS), выполнена оценка его работоспособности, результаты приведены в таблице 3.2 . Исходным материалом является файл формата wav с частотой дискретизации 44

100 Гц, изменяемым параметром является коэффициент усиления добавляемого шума.

Таблица 3.2 – Оценка работоспособности алгоритма SS

Коэф. ус.	СКО	SNR	r
1,20	1,31E-01	0,005	0.999
1,30	1,40E-01	0,08	0.997
1,40	1,51E-01	0,011	0.988
1,50	1,61E-01	0,018	0.986
1,60	1,71E-01	0,021	0.805
1,70	1,80E-01	0,023	0.710
1,80	1,92E-01	0,028	0.725
1,90	0,200083	0,031	0.707
2,00	0,20914	0,034	0.701
2,10	0,21785	0,042	0.684
2,20	0,227859	0,050	0.667
2,30	0,239177	0,058	0.624
2,40	0,24673	0,064	0.610
2,50	0,255674	0,070	0.567
2,60	0,265621	0,078	0.554

Так же был реализован алгоритм скрытия данных методом DCT, выполнена оценка его работоспособности, результаты приведены в таблице 3.3 . Исходным материалом является файл формата wav с частотой дискретизации 44 100 Гц, изменяемым параметром является количество коэффициентов DCT используемые для хранения бита.

Таблица 3.3 – Оценка работоспособности алгоритма DCT

Кол. коэф бит	СКО	SNR	r
1	2,42E-02	0,005	0.999
2	3,33E-02	0,08	0.999
3	4,69E-02	0,011	0.998
4	5,86E-02	0,018	0.997
5	7,06E-02	0,021	0.994
6	8,62E-02	0,023	0.989
7	9,75E-02	0,028	0.984
8	0,108002	0,031	0.894
9	0,120821	0,034	0.754
10	0,130809	0,042	0.720
11	0,141723	0,050	0.710

Кол. коэф бит	СКО	SNR	r
12	0,152101	0,058	0.709
13	0,156449	0,064	0.703
14	0,159938	0,070	0.694
15	0,177789	0,078	0.692

3.3 Основные результаты и выводы

По результатам количественной оценки было выявлено, что наиболее оптимальным является использование метода дискретно-косинусного преобразования (DCT).

Величина среднеквадратической ошибки в данном случае приближена к нулю при минимальном коэффициенте внедрения, но по мере его увеличения, СКО незначительно возрастает. Тем не менее, допустимая степень идентичности исходного и синтезированного сигнала сохраняется. Также видно, что при увеличении интенсивности кодирования, отношение сигнал/шум уменьшается, что свидетельствует об увеличении искажений. Корреляция при исследовании каждого набора звуков и при всех вариациях коэффициента K не опускается ниже 0,97, следовательно, сохраняется достаточная схожесть между сигналами.

4 ЭКОНОМИЧЕСКАЯ ОЦЕНКА РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Задача научно–исследовательского проекта заключается в разработке алгоритма скрытой передачи сигнала. По ходу выполнения работы, возникал ряд не значительных экономических затрат.

4.1 Планирование работ по исследованию

Для реализации данного проекта были задействованы следующие сотрудники:

- старший научный сотрудник, обязанностью которого является консультация, курирование и контроль над проектом;
- младший научный сотрудник, его обязанности заключаются в проведении требуемых исследований, выполнении сбора и обработки необходимой информации, требуемых расчетов, составление технической документации по результату проектирования.
- экономист, обязанностью которого является, предоставления экономической оценки исследования.

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

Таблица 4.1 – Планирование работ по исследованию

Наименование этапов работ	Исполнитель	Трудоемкость, час	Продолжительность, дней
1	2	3	4
1.Этап подготовки			
1.1.Сбор данных	Младший научный сотрудник	54	8
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	16	3
1.4.Организация исследовательской работы	Младший научный сотрудник	18	3
1.5.Обработка и анализ данных	Младший научный сотрудник	78	10
Итого:		249	35
2.Основной этап			
2.1.Обоснование уместности работы	Старший научный сотрудник	45	7
2.2.Производство работ	Младший научный сотрудник	133	22
Итого:		178	29
3.Заключительный этап			
3.1.Технико–экономическое Обоснование	Экономист	38	4
3.2.Создание и утверждение технической документации	Младший научный сотрудник	38	4
Итого:		76	8

Результатом планирования, приведенным в таблице выше, было определено штатное количество сотрудников, подсчитаны временные ресурсы, затрачиваемые на исследование. Обнаружено, что наибольшая временная нагрузка приходится на младшего сотрудника, а обработка и анализ данных требуют самое большое количество временных ресурсов.

4.2 Расчет финансовых затрат на оплату труда сотрудников и на 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	337	18050
Старший научный сотрудник	128	25030
Экономист	38	11100
Итого:	498	

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

$$Ч_{ТС} = \frac{P}{F_{мес}} \quad (4.1)$$

где $F_{мес}$ – фонд рабочего времени месяца, составляет 176 часов (24 рабочих дня по 8 часов в день); P – оклад сотрудника.

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

$$Ч_{от} = Ч_{ТС} * T_{сум} \quad (4.2)$$

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	$P_{от}$, руб
1	2	3	4	5
Младший научный сотрудник	337	18050	102,5	34543
Старший научный сотрудник	128	25030	142,3	18215
Экономист	38	11100	63.06	2400
Итого:	503			55158

4.3 Расчет продолжительности исследования

В соответствии с выполненными расчетами, трудоемкость исследования составит 503 часов.

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

$$T_{\text{иссл}} = \frac{q_{\text{мс}}}{T_{\text{сум}}} \quad (4.3)$$

где $T_{\text{сум}} = 503$ часов – суммарная трудоемкость исследования; $T_{\text{рд}} = 8$ часов – продолжительность рабочего дня.

$$T_{\text{иссл}} = \frac{503}{8} = 63 \text{ дня} \quad (4.4)$$

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

4.4 Расчет финансовых затрат на расходные материалы

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 необходимых 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	210	4	840
Канцтовары	500	–	500
Расходные материалы для принтера (картридж)	4100	–	4100
Итого:			5440

Окончательные затраты на закупку расходных материалов для проведения исследования составят 5440 рублей.

4.5 Составление сметы расходов на исследование

Общий расход, затраченный на разработку, включает в себя районные коэффициенты, страховые взносы и премиальные выплаты. Для оценивания произведенных финансовых затрат на исследование выполним составление сметы на разработку и проведение математических операций.

Премиальные выплаты рассчитываются по следующей формуле:

$$ПВ = P_{OT} * K_{ПВ} \quad (4.5)$$

где $K_{ПВ}$ – коэффициент премиальных выплат, пусть он составляет 30%, в случае если премии не предусмотрены $K_{ПВ}=1$.

$$ПВ = 55158 * 0,3=16547,4$$

Дополнительные финансовые затраты на проведение исследования можно

определить по следующей формуле:

$$З_{доп} = P_{OT} * K \quad (4.6)$$

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

$$З_{доп} = 55158 * 0,14 = 7722,12руб,$$

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%.

$$PK = P_{OT} * K_{PB} \quad (4.7)$$

где K_{PB} – коэффициент районных выплат, возьмем для примера коэффициент в 15 % от суммы.

$$PK = 55158 * 0,15 = 8273,7руб, \quad (4.8)$$

Общие финансовые затраты на оплату труда рассчитываются по формуле:

$$P_{общ} = P_{OT} + PK + ПВ + З_{доп} \quad (4.9)$$

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

$$P_{общ} = 55158 + 8273,7 + 16547,4 + 7722,12 = 87702руб$$

Из таблицы 3.4 берется итоговая сумма стоимости расходных материалов

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						47
Изм.	Лист	№ докум.	Подпись	Дата		

по статье расходных материалов.

$$P_{PM} = 5440 \text{ руб}$$

Страховые взносы рассчитываются по формуле:

$$CB = P_{OT} * 0,3, \quad (4.10)$$

$$CB = 55158 * 0,3 = 16547,42 \text{ руб}$$

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

$$AO = C_{ПК} * 0,25, \quad (4.11)$$

$$AO = 40000 * 0,25 = 10000 \text{ руб},$$

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

$$P_{ИНТ} = 1500 \text{ руб}$$

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

$$P_{АХ} = P_{OT} * 0,5 \quad (4.12)$$

$$P_{АХ} = 55158 * 0,5 = 27579 \text{ руб}$$

Получившиеся в процессе расчёта финансовые затраты заносим в таблицу 4.5.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						48
Изм.	Лист	№ докум.	Подпись	Дата		

Таблица 4.5 – Смета расходов на проведение исследования

Наименование статей расходов	Сумма, руб.	Удельный вес статей, %
1	2	3
1.Стоимость расходных материалов	5440	2,56
2. Расходы на оплату труда, из них:	87702	41,41
2.1. Основная заработная плата	55158	26,04
2.2. Дополнительные затраты	7722,12	3,64
2.3. Премияльные выплаты	16547,4	7,81
2.4 Районный коэффициент	8273,7	3,87
3. Единый социальный налог	16547,42	7,81
4. Амортизационные исчисления на использование компьютера	10000	4,7
5. Расходы на использование Интернет	1500,00	0,70
6.Административно–хозяйственные расходы	27579	12,07
Итого:	211749	100

В результате проведения экономической оценки исследования были получены финансовые затраты на разработку и реализацию исследования:

- продолжительность исследовательских работ составила 63 дня;
- смета расходов на исследование – 211749рубля.

ЗАКЛЮЧЕНИЕ

В реализованной работе были рассмотрены основные стеганографические методы, позволяющие осуществлять скрытную передачу информации. Проанализировав преимущества и недостатки было выявлено, что наиболее оптимальным с точки зрения емкости скрываемой информации, маскировки и сложности реализации является алгоритм, основанный на методе дискретно-косинусного преобразования.

В процессе исследовательской работы была выполнена основная цель, проведена оценка работоспособности и внедрения информации в звуковые файлы. Для достижения поставленной цели был проведен мониторинг изменений качества звука и восприятия искажений при скрытном кодировании информации различными методами.

Проанализировав речевой материал, содержащий преимущественно взрывные, звонкие и шипящие согласные было выявлено, что наиболее оптимальным сигналом для скрытия в него информационного сообщения является предложение, содержащее шипящие звуки ввиду минимального наличия визуальных искажений на осциллограмме. +9

При количественной оценке были определены величины отношения сигнал шум, среднеквадратической ошибки и корреляции. Было выявлено, что наибольший объем информации может быть закодирован при помощи метода дискретно-косинусного преобразования, вычисленное СКО не много больше нуля, но при этом слышимые изменения в сигнале появляются только при кодирование 8 и более бит, в отличие от метода LSB где изменения начинаются после кодирования 4 бит и метода широкого спектра где изменения начинаются с 1.5 бит.

Разработанные алгоритмы стеганографического кодирования и речевого сообщения в речевые данные были реализованы в среде программирования Matlab в соответствии с приведенными словесными алгоритмами.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
						50
Изм.	Лист	№ докум.	Подпись	Дата		

Программный код позволил за короткое время получить достоверные результаты расчетов с использованием общеизвестных и разработанных формул.

В результате экономической оценки исследования удалось оценить продолжительность исследовательских работ – 63 дней и сумму расходов на исследование – 211749 рублей с учетом отчислений и единого социального налога.

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
Изм.	Лист	№ докум.	Подпись	Дата		51

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Yong Xiang Spread Spectrum–Based High Embedding Capacity Watermarking Method for Audio Signals [Электронный ресурс] / Yong Xiang, Iynkaran Natgunanathan, Yue Rong, , Song Guo // IEEE.ACM TRANSACTIONS ON AUDIO, SPEECH, AND LANGUAGE PROCESSING. 23(12). 2015. pp. 2228 – 2237 Режим доступа: https://www.researchgate.net/publication/281930141_Spread_Spectrum–Based_High_Embedding_Capacity / (Дата обращения: 04.05.2018)

2. Ahmed Hussain Ali A Review on Audio Steganography Techniques [Электронный ресурс] / Mohd Rosmadi Mokhtar, LoayEdwar George // Research Journal of Applied Sciences, Engineering and Technology. 12(2). 2016. pp. 154–162 Режим доступа: https://www.researchgate.net/publication/292361595_A_Review_on_Audio_Steganography_Techniques (Дата обращения: 05.05.2018)

3. Таравков, А.В. Разработка алгоритма синхронизации для внедрения цифрового водяного знака в потоковое видео [Электронный ресурс]/ Григорьев А.С., Баженов Р.И.// Современная техника и технологии. № 11. 2014. Режим доступа: <https://d.docs.live.net/99ddf781f115b8ed/Литература%20к%20диплому/3.html> (Дата обращения 18.04.2018)

4. Zhenghui Liu A security watermark scheme used for digital speech forensics [Электронный ресурс] / Jiwu Huang, Xingming Sun, Chuanda Qi // Springer Science+Business Media New York. 10.1007/s11042–016–3533–9. 2016. pp 1–21. Режим доступа: https://www.researchgate.net/publication/301576015_A_security (Дата обращения 25.04.2018)

5. Коробейников, А.Г. Встраивание цифровых водяных знаков в аудиосигнал методом расширения спектра [Электронный ресурс] / А.Г. Даурских, Н.В. Павлова // Научно–технический вестник Санкт–Петербургского государственного университета информационных технологий, механики и оптики. № 1(59). 2009. Режим доступа: <http://cyberleninka.ru/article/n/vstraivanie–>

tsifrovyh–vodyanyh–znakov–v–audiosignal–metodom–rasshireniya–spektra

(Дата обращения 27.04.2018)

6. Сюзев, В.В. Основы спектрального анализа в базисах Хаара [Электронный ресурс] // Вестник Московского государственного технического университета им. Н.Э. Баумана. Серия «Приборостроение». № 2. 2011. URL: <http://cyberleninka.ru/article/n/spektralnyy-analiz-v-bazisah-funktsiy-haara> (дата обращения 29.04.2016)

7. Nedeljko Cvejic. Spread spectrum audio watermarking using frequency hopping and attack characterization [Электронный ресурс] / Nedeljko Cvejic, Tapio Seppanen// Signal Processing 84. 2004. pp 207 – 213. Режим доступа: <http://www.mediateam oulu.fi/publications/pdf/465.pdf> (Дата обращения 04.05.2018)

8. Saito S. A digital watermarking for audio data using band division based on QMF bank [Электронный ресурс] / S. Saito, T. Furukawa, K. Konishi // IEEE International Conference on Acoustics, Speech, and Signal Processing. 2002. – V. 4. pp 3473–3476. Режим доступа: <http://books.google.ru/books?id> (Дата обращения 05.05.2018)

9. Boney, L. Digital watermarks for audio signals Tewfic [Электронный ресурс] / А.Н., Hamdy A.K. // Department of Electrical engineering, University of Minnesota. DOI: 10.1109/MMCS.1996.535015. 1996. Режим доступа: https://www.researchgate.net/publication/3639217_Digital_watermarks_for_audio_signals (Дата обращения 11.05.2018)

10. Ле, Н. В. Предварительная обработка речевых сигналов для системы распознавания речи [Электронный ресурс] / Н. В. Ле, Д. П. Панченко // Молодой ученый. — 2011. — №5. Т.1. — С. 74–76. Режим доступа: <http://www.moluch.ru/archive/28/3171/> (Дата обращения 18.04.2018)

11. Горшков, Ю.Г. Обработка речевых сигналов на основе вейвлетов [Электронный ресурс] // Т-Comm. 2015. №2. Режим доступа: <http://>

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
Изм.	Лист	№ докум.	Подпись	Дата		53

cyberleninka.ru/article/n/obrabotka-rechevyh-signalov-na-osnove-veyvletov (Дата обращения: 18.05.2018).

12. Белов, С.П. Метод частотно – временного анализа сигналов [Электронный ресурс] / С.П. Белов, Е.И. Прохоренко, А.С. Белов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2009. №1 (56). Режим доступа: <http://cyberleninka.ru/article/n/metod-chastotno-vremennogo-analiza-signalov-1> (Дата обращения: 20.05.2018).

13. Жиляков, Е.Г. Алгоритмы обнаружения основного тона речевых сигналов [Электронный ресурс] / Е.Г Жиляков, А.А. Фирсова, Н.А. Чеканов // Научные ведомости Белгородского государственного университета. Серия: Экономика. Информатика. 2012. №1 (120). Режим доступа: <http://cyberleninka.ru/article/n/algorithmy-obnaruzheniya-osnovnogo-ona-rechevyh-signalov> (Дата обращения: 18.05.2018).

14. Zhengguang Xu. Channel Capacity Analysis of the Multiple Orthogonal Sequence Spread Spectrum Watermarking in Audio Signals [Электронный ресурс] / Zhengguang Xu, Chenghuan Ao, and Benxiong Huang // IEEE SIGNAL PROCESSING LETTERS. 2016. 23(1). pp. 20–24 Режим доступа: https://www.researchgate.net/publication/283805432_Channel_Capacity_Analysis_of_multiple_Orthogonal_Sequence_Spread_Spectrum_Watermarking_in_Audio_Signals (Дата обращения 26.04.2016)

15. Крыжевич, Л.С. Стеганографические методы сокрытия данных в звуковых файлах на основе всплесковых преобразований // Л.С. Крыжевич, Д.А. Белобородов // Signals [Электронный ресурс] / Auditorium: электронный научный журнал Курского государственного университета. – Курск: № 2, 2014г. «Аудиториум» электронный научный журнал <http://auditorium.kursksu.ru>. URL: <http://auditorium.kursksu.ru/index.php?page=6&new=2> (Дата обращения 26.04.2018)

					<i>11070006.11.03.02.826.ПЗВКР</i>	Лист
Изм.	Лист	№ докум.	Подпись	Дата		55