ВОРОНЕЖСКИЙ ИНСТИТУТ ВЫСОКИХ ТЕХНОЛОГИЙ – АНОО ВО

НАПРАВЛЕНИЕ 09.03.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ

ФОРМА ОБУЧЕНИЯ ЗАОЧНАЯ

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

на тему: Разработка программных модулей для стеганографии и анализа распределения данных в электронных документах

Студент	Тарасов В.В. (ФИО)	_____ (подпись)
Научный руководитель	Коденцев Е.И. (ФИО)	_____ (подпись)
Руководитель направления подготовки	Преображенский Ю.П. (ФИО)	_____ (подпись)
Руководитель департамента	Цуберт О.К. (ФИО)	_____ (подпись)

Воронеж 2017

ВОРОНЕЖСКИЙ ИНСТИТУТ ВЫСОКИХ ТЕХНОЛОГИЙ – АНОО ВО

Направление 09.03.02 Информационные системы и технологии
Форма обучения заочная
Студент группы ИСз-128

Тарасов Владислав Валентинович

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

1. Тема выпускной квалификационной работы Разработка программных модулей для стеганографии и анализа распределения данных в электронных документах

утверждена распоряжением №_____ от « »_____201_ г.

2. Технические условия _____
_____
_____
_____
_____

3. План выполнения выпускной квалификационной работы
с «_____»_____201_г. по « »_____201_ г.

Название элементов работы	%	Сроки	% выполнения	Подпись рук., консультанта
Исследование предметной области	20		100%	
Разработка алгоритма	50		100%	
Реализация	30		100%	

4. Выпускная квалификационная работа закончена
«_____»_____201_г. _____
(подпись студента)

5. Нормоконтроль пройден
«_____»_____201_г. _____
(подпись нормоконтролера)

6. Пояснительная записка и все материалы просмотрены.

Оценка научного руководителя _____

Научный руководитель _____
(Фамилия, имя, отчество) (подпись)

Руководитель направления _____
(Фамилия, имя, отчество) (подпись)

РЕФЕРАТ

Пояснительная записка: 54 страницы, 36 рисунков, 8 таблиц, 9 источников.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ.....5
1. СКРЫТИЕ ДАННЫХ В АУДИО-СИГНАЛАХ.....8
1.1 Методы кодирования с расширением спектра.....8
1.2 Внедрение информации модификацией фазы аудио-сигнала.....15
1.3 Встраивание информации за счет изменения времени задержки эхо-сигнала.....17
1.4 Методы маскирования ЦВЗ.....23
1.5 Вывод по главе.....27
2. РАЗРАБОТКА АЛГОРИТМА СКРЫТИЯ ИНФОРМАЦИИ В АУДИОСИГНАЛАХ.....28
2.1 Стандарт шифрования данных Data Encryption Standard.....28
2.2 Алгоритм скрытия информации в аудиосигналах.....39
2.3 Блок-схема программы.....41
2.4 Зависимость скрытия информации от размера секретного файла.....43
2.5 Вывод по главе.....45
3. ОПИСАНИЕ ПРОГРАММНОГО ПРОДУКТА ANALITIC CRYPTOSYSTEM.....46
3.1 Меню «Файл».....48
3.2 Меню «Анализ».....48
3.3 Меню «Запуск».....49
3.4 Меню «Справка».....51
3.5 Вывод по главе.....52
ЗАКЛЮЧЕНИЕ.....53
СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ.....54

ВВЕДЕНИЕ

Задача защиты информации от несанкционированного доступа решалась во все времена на протяжении истории человечества. Уже в древнем мире выделилось два основных направления решения этой задачи, существующие и по сегодняшний день: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии скрывается сам факт существования тайного сообщения.

Развитие средств вычислительной техники дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу. Это – речь, аудиозаписи, изображения, видео. Известны также предложения по встраивании информации в текстовые файлы и в исполняемые файлы программ. [1]

Актуальность данной темы заключается в необходимости защиты информации и оптимального распределения данных, с использованием криптографических и стегонаграфических систем, в организации

Цель дипломной работы заключается в разработке программного средства реализующий алгоритмы криптографии и стеганографии, и разработки подсистемы анализа распределения данных в электронных документах, при защите информации.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Выбор алгоритма стеганографии для скрытия информации в звуковых сигналах.
2. Построение обобщенного алгоритма анализа распределение данных в электронных документах.
3. Разработка программного средства реализующих выбранный алгоритм стеганографии и криптографии.

4. Определение границ применимости исследуемого алгоритма.

Чтобы решить задачу выбора алгоритмов стеганографии, а также выбрать методы шифрования и дешифрования необходимо провести анализ скрытия данных в аудио-сигналов. Т.е. необходимо рассмотреть требования, которые могут быть предъявлены к стегасистемам, применяемым для встраивания информации в аудио-сигналы, методы скрытия данных в аудио-сигналах, методы внедрения информации модификацией фазы аудио-сигнала, методы маскирования ЦВЗ.

После выбора метода стеганографии можно приступить к построению программного продукта.

Для того чтобы разработать программное средство реализующий выбранный алгоритм стеганографии необходимо построить блок-схему программы и выбрать язык программирования.

Выбор языка программирования – не менее сложная задача, потому что в каждом языке существуют свои определенные возможности, и каждый язык предназначен для определенных целей. Лучше всего для создания программного средства подойдет языки программирования Visual C++ и Object Pascal.

На основе построенного программного средства реализующего алгоритм стеганографии можно определить границы применимости рассматриваемого алгоритма стеганографии.

Дипломная работа состоит из пяти глав:

1. Скрытие данных в аудио сигналах.
2. Разработка алгоритма скрытия информации в аудио-сигналах.
3. Описание программного продукта.
4. Организационно-экономическая часть
5. Безопасность жизнедеятельности

В первой главе описывается стеганографические методы скрытия информации в аудиосигналах.

Во второй главе рассматриваются алгоритм шифрования и скрытия информации в аудиосигналах, состоящий из трех разделов. В первом разделе описывается метод и реализация алгоритма «DES», в втором разделе описывается метод внедрения информации в аудио-сигнал. В третьем разделе находится блок-схема работы программы.

В третьей главе приведены данные по ресурсам требуемые для нормальной работы программы, и описание «CriptoSystem» с точки зрения пользователя.

В приложении приводится листинг программы.

1. СКРЫТИЕ ДАННЫХ В АУДИО-СИГНАЛАХ

1.1 Методы кодирования с расширением спектра

Требования, которые могут быть предъявлены к стегосистемам, применяемым для встраивания информации в аудио-сигналы:

- скрываемая информация должна быть стойкой к наличию различных окрашенных шумов, сжатию с потерями, фильтрованию, аналогово-цифровому и цифро-аналоговому преобразованиям;
- скрываемая информация не должна вносить в сигнал искажения, воспринимаемые системой слуха человека;
- попытка удаления скрываемой информации должна приводить к заметному повреждению контейнера (для ЦВЗ);
- скрываемая информация не должна вносить заметных изменений в статистику контейнера;

Для внедрения скрываемой информации в аудио-сигналы можно использовать методы, применимые в других видах стеганографии. Например, можно внедрять информацию, замещая наименее значимые биты (все или некоторые). Или можно строить стегосистемы, основываясь на особенностях аудио-сигналов и системы слуха человека. [2]

Систему слуха человека можно представить, как анализатор частотного спектра, который может обнаруживать и распознавать сигналы в диапазоне 10 – 20000 Гц. Систему слуха человека можно смоделировать, как 26 пропускающих фильтров, полоса пропускания, которых увеличивается с увеличением частоты. Система слуха человека различает изменения фазы сигнала слабее, нежели изменения амплитуды или частоты.

Аудио-сигналы можно разделить на три класса:

- разговор телефонного качества, диапазон 300 – 3400 Гц;
- широкополосная речь 50 – 7000 Гц;
- широкополосные аудио-сигналы 20 – 20000 Гц.

ЦВЗ внедряется в аудио-сигналы (последовательность 8- или 16-битных отсчетов) путем незначительного изменения амплитуды каждого отсчета. Для обнаружения ЦВЗ не требуется исходного аудио-сигнала. [3]

Пусть аудио-сигнал состоит из N отсчетов $x(i)$, $i = 1, \ldots, N$, где значение N не меньше 88200 (соответственно 1 секунда для стереоаудиосигнала, дискретизированного на частоте 44,1 кГц). Для того чтобы встроить ЦВЗ, используется функция $f(x(i), w(i))$, где $w(i)$ - отсчет ЦВЗ, изменяющийся в пределах $[-\alpha; \alpha]$, α - некоторая константа. Функция f должна принимать во внимание особенности системы слуха человека во избежание ощутимых искажений исходного сигнала. Отсчет результирующего сигнала получается следующим образом:

$$y(i) = x(i) + f(x(i),w(i)) \tag{1.1}$$

Отношение сигнал-шум в этом случае вычисляется как

$$SNR = 10 \log_{10} \frac{\sum_n x^2(n)}{\sum_n [x(n)-y(n)]^2} \tag{1.2}$$

Важно отметить, что применяемый в схеме генератор случайных чисел должен иметь равномерное распределение. Стойкость ЦВЗ, в общем случае, повышается с увеличением энергии ЦВЗ, но это увеличение ограничивается сверху допустимым отношением сигнал-шум.

Обнаружение ЦВЗ происходит следующим образом. Обозначим через S следующую сумму:

$$S = \sum_{i=1}^{N} y(i)w(i). \tag{1.3}$$

Комбинируя (1.1) и (1.3), получаем

$$S = \sum_{i=1}^{N} [x(i)w(i) + f(x(i), w(i))w(i)]. \tag{1.4}$$

Первая сумма в (1.4) равна нулю, если числа на выходе ГСЧ распределены равномерно и математическое ожидание значения сигнала равно нулю. В большинстве же случаев наблюдается некоторое отличие, обозначаемое Δw, которое необходимо также учитывать. [4]

Следовательно, (1.4) принимает вид

$$S = \sum_{i=1}^{N-\Delta w} x(i)w(i) + \sum_{i=1}^{\Delta w} x(i)w(i) + \sum_{i=1}^{N} f(x(i), w(i))w(i). \quad (1.5)$$

Сумма $\sum_{i=1}^{N-\Delta w} x(i)w(i)$, как показано выше, приблизительно равна нулю. Если в аудио-сигнал не был внедрен ЦВЗ, то S будет приблизительно равна $\frac{\Delta w}{N}\sum_{i=1}^{N} x(i)w(i)$. С другой стороны, если в аудио-сигнал был внедрен ЦВЗ, то S будет приблизительно равна $\frac{\Delta w}{N}\sum_{i=1}^{N} x(i)w(i) + \sum_{i=1}^{N} f(x(i), w(i))w(i)$. Однако, $x(i)$ - это исходный сигнал, который по условию не может быть использован в процессе обнаружения ЦВЗ. Сигнал $x(i)$ можно заменить на $y(i)$, это приведет к замене $\sum_{i=1}^{\Delta w} x(i)w(i)$ на $\frac{\Delta w}{N} S$, ошибка при этом будет незначительной.

Следовательно, вычитая величину $\frac{\Delta w}{N} S$ из S, и деля результат на $\sum_{i=1}^{N} f(y(i), w(i))w(i)$, получим результат r, нормированный к 1. Детектор ЦВЗ, используемый в этом методе, вычисляет величину r, задаваемую формулой

$$r = \frac{S - \frac{\Delta w}{N}|S|}{\sum_{i=1}^{N} f(y(i), w(i))w(i)}. \quad (1.6)$$

Пороговая величина обнаружения теоретически лежит между 0 и 1, с учетом аппроксимации этот интервал сводится к $[0 - \varepsilon;\ 1 + \varepsilon]$. Опытным

путем установлено, что для того чтобы определить действительно ли определенный ЦВЗ находится в сигнале, пороговое значение ЦВЗ должно быть выше 0,7. Если требуется большая достоверность в определении наличия ЦВЗ в сигнале, пороговое значение необходимо увеличить. Работа кодера и декодера представлены на рис.1.1. [5]

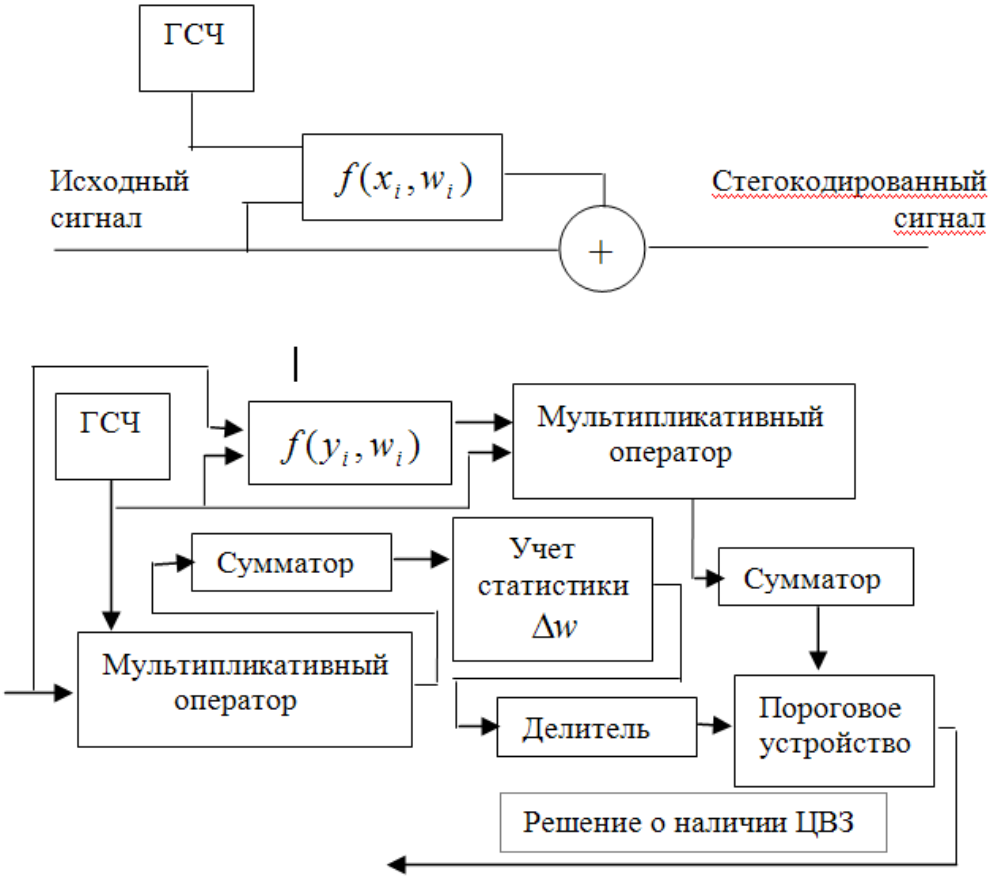


Рисунок 1.1 – Блок-схема стегокодера и стегодекодера

На рис. 1.2 показана эмпирическая функция плотности вероятности для аудио-сигнала с ЦВЗ и без ЦВЗ.

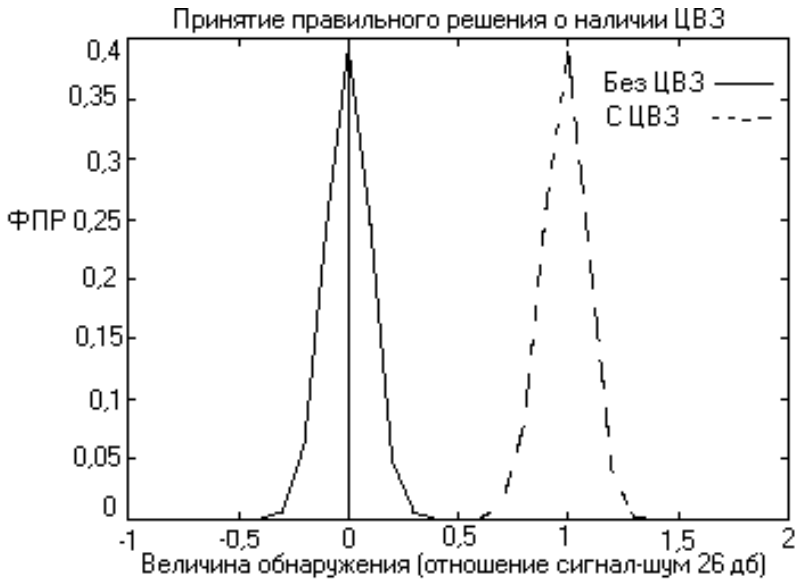


Рисунок 1.2 – Функция плотности распределения величины обнаружения для сигналов с ЦВЗ и без ЦВЗ

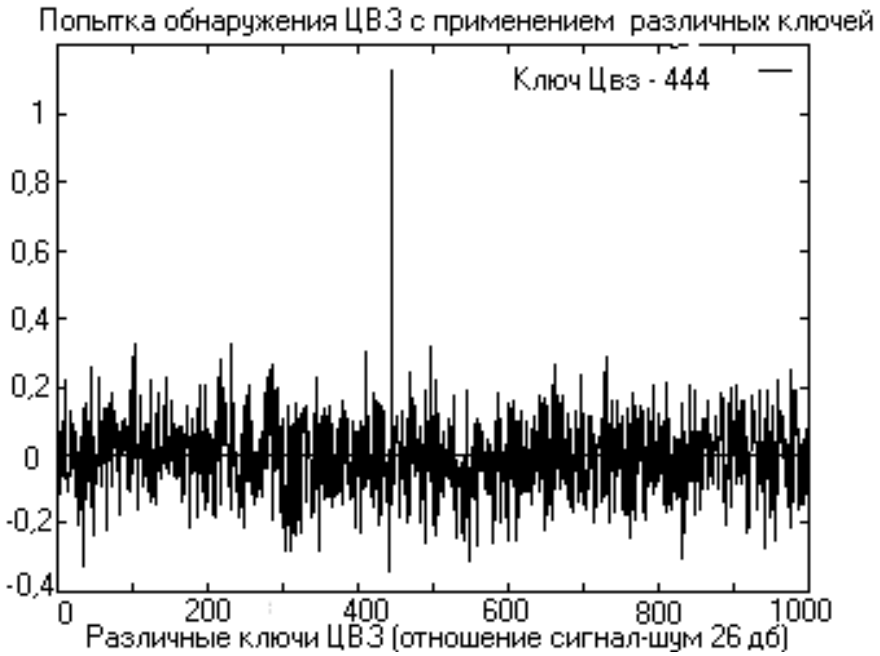


Рисунок 1.3 – Распознавание заданного ключа встраивания ЦВЗ

Эмпирическая функция плотности вероятности аудио-сигнала без ЦВЗ показана непрерывной кривой, пунктирная кривая описывает эмпирическую функцию плотности вероятности аудио-сигнала с встроенным ЦВЗ. Оба распределения были вычислены с использованием 1000 различных значений ЦВЗ при отношении сигнал-шум 26 дб. [6]

Внедрение в один аудио-сигнал большого количества различных ЦВЗ приводит к увеличению слышимости искажений. Максимальное число ЦВЗ ограничено энергией каждого из них. Декодер способен правильно восстановить каждый ЦВЗ при условии использования кодером уникальных ключей. На рис.1.3 показан пример обнаружения ЦВЗ с использованием 1000 различных ключей, из которых только один – верный.

После восстановления при сжатии до скорости 80 кб/с можно наблюдать незначительное уменьшение пороговой величины обнаружения в аудио-сигналах с ЦВЗ. При сжатии аудио-сигнала до 48 кб/с появляются звуковые эффекты, ощутимо снижающие качество сигналов с ЦВЗ. [7]

Стойкость алгоритма встраивания ЦВЗ к фильтрации проверена применением к нему скользящего фильтра средних частот и фильтра нижних частот. Аудио-файлы с внедренным ЦВЗ профильтрованы скользящим фильтром средних частот длины 20, который вносит в аудиоинформацию значительные искажения.

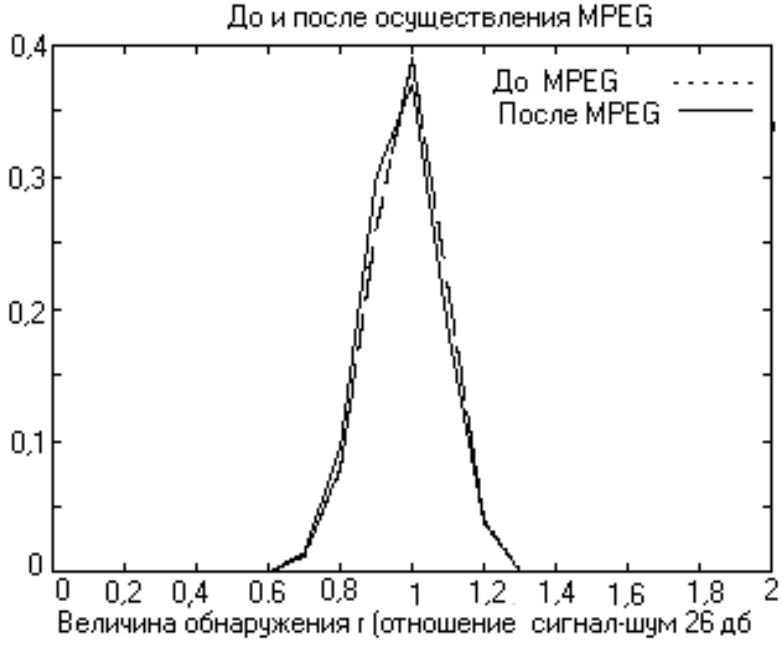


Рисунок 1.4 – Влияние сжатия данных на ЦВЗ

На рис.1.5 показано, как изменяется пороговая величина обнаружения при применении вышеописанного фильтра. В общем, порог обнаружения увеличивается в отфильтрованных сигналах. Это происходит по причине того, что функция плотности распределения сигналов после фильтрации сдвигается вправо по сравнению с относительной функцией распределения сигналов, не подвергавшихся фильтрации.

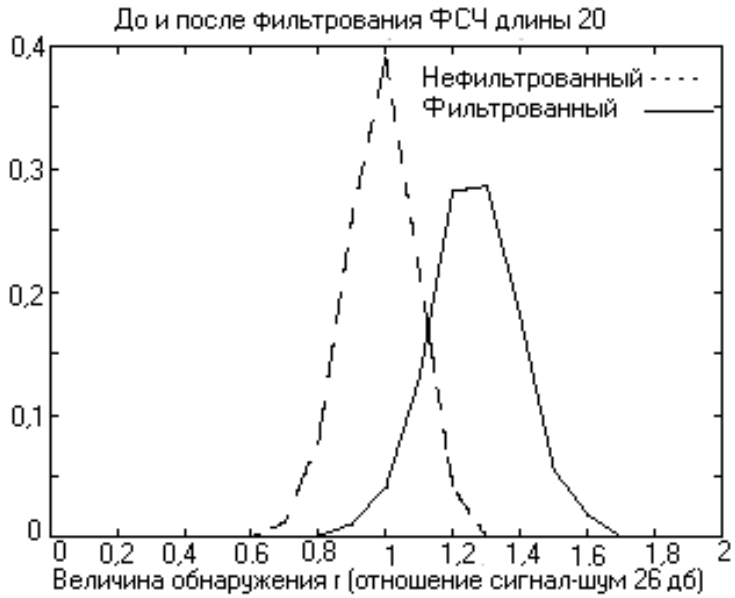


Рисунок 1.5 – Влияние на ЦВЗ применения к аудио-сигналу скользящего фильтра средних частот

ЦВЗ сохраняется и при применении к аудио-сигналу фильтра нижних частот. Однако при фильтрации аудис-игналов с ЦВЗ фильтром нижних частот Хэмминга 25-го порядка с частотой среза 2205 Гц имело место уменьшение вероятности обнаружения наличия ЦВЗ. [8]

Для проверки стойкости ЦВЗ к передискретизации Р. Бассиа и И. Питасом аудио-сигналы были передискретизированы на частоты 22050 Гц и 11025 Гц и назад на начальную частоту. ЦВЗ сохранялся.

При переквантовании аудио-сигнала из 16-битного в 8-битный и обратно внедренный ЦВЗ сохраняется, несмотря на частичную потерю информации. На рис.1.6 показано насколько хорошо ЦВЗ сохраняется в 1000

аудио-сигналах при их переквантовании в 8-битные отсчеты и обратно в 16-битные.



Рисунок 1.6 – Влияние переквантования сигнала на ЦВЗ

Девиация функции плотности распределения переквантованного сигнала увеличивается, как и в случае применения фильтра нижних частот, следовательно, имеет место уменьшение эффективности обнаружения.

1.2 Внедрение информации модификацией фазы аудио-сигнала

Метод, предлагающий использовать слабую чувствительность системы слуха человека к незначительным изменениям фазы сигнала, был предложен В. Бендером, Н. Моримото и др. [9]

Внедрение информации модификацией фазы аудио-сигнала – это метод, при котором фаза начального сегмента аудио-сигнала модифицируется в зависимости от внедряемых данных. Фаза последующих сегментов согласовывается с ним для сохранения разности фаз. Это необходимо потому, что к разности фаз человеческое ухо более чувствительно. Фазовое кодирование, когда оно может быть применено,

является одним из наиболее эффективных способов кодирования по критерию отношения сигнал-шум.

Процедура фазового кодирования состоит в следующем:

1. Звуковой сигнал $s[i],(0 \le i \le I-1)$ разбивается на серию N коротких сегментов $s_n[i](0 \le n \le N-1)$ рис. 1.7(а), 1.7(б).

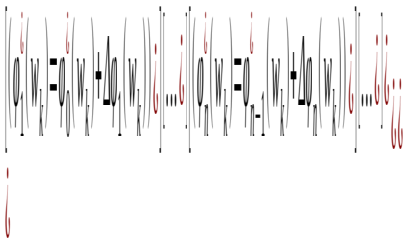
2. К *n*-му сегменту сигнала $s_n[i]$ применяется *k*-точечное дискретное преобразование Фурье, где *K=I/N*, и создаются матрицы фаз $\varphi_n(w_k)$ и амплитуд $A_n(w_k)$ для $(0 \le k \le K-1)$ (рис 1.7(в)).

3. Запоминается разность фаз между каждыми двумя соседними сегментами $(0 \le n \le N-1)$ рис. (1.7(г)).

$$\Delta\varphi_{n+1}(w_k)=\varphi_{n+1}(w_k)-\varphi_n(w_k) \tag{1.7}$$

4. Бинарная последовательность данных представляется, как $\pi/2$ и $-\pi/2$ (рис 1.2.1 (д)), $\varphi_0^{i}=\varphi_{data}^{i}$.

5. С учетом разности фаз создается новая матрица фаз для n > 0, (рис. 1.7(е)):



(1.8)

Стегокодированный сигнал получается путем применения обратного дискретного преобразования Фурье, к исходной матрице амлитуд и модифицированной матрице фаз. (рис. 1.7(ж) и 1.7(з)).

Получателю должны быть известны: длина сегмента, и точки ДПФ. Перед декодированием последовательность должна быть синхронизирована.

Недостатком этой схемы является ее низкая пропускная способность. В экспериментах В. Бендера и Н. Моримото пропускная способность канала варьировалась от 8 до 32 бит в секунду.

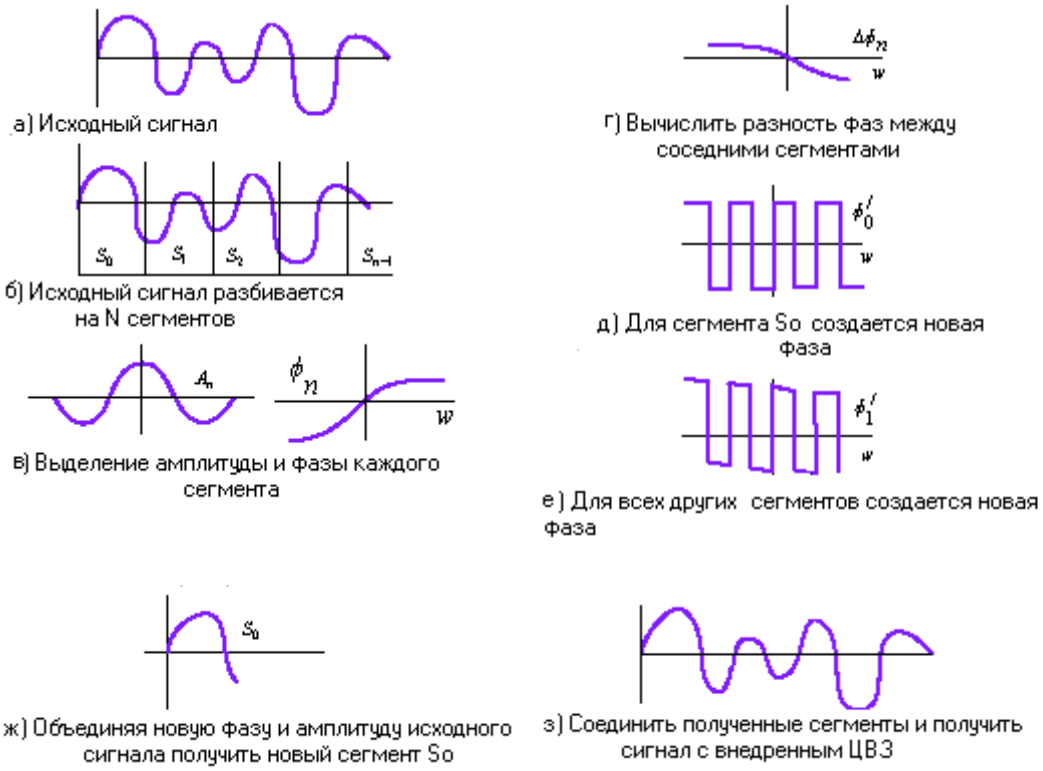


Рисунок 1.7 – Блок-схема фазового кодирования

1.3 Встраивание информации за счет изменения времени задержки эхо-сигнала

Теми же авторами был предложен метод внедрения информации с использованием эхо-сигнала.

Этот метод позволяет внедрять данные в сигнал прикрытия, изменяя параметры эхо сигнала. К параметрам эхо, несущим внедряемую информацию (рис. 1.8), относятся: начальная амплитуда, время спада и сдвиг (время задержки между исходным сигналом и его эхо). При уменьшении сдвига два сигнала смешиваются. В определенной точке человеческое ухо перестает различать два сигнала, и эхо воспринимается, как добавочный

резонанс. Эту точку трудно определить точно, так как она зависит от исходной записи, типа звука и слушателя. В общем случае, по исследованиям В. Бендера и Н. Моримото, для большинства типов сигналов и для большинства слушателей слияние двух сигналов происходит при расстоянии между ними около 0,001 секунды.

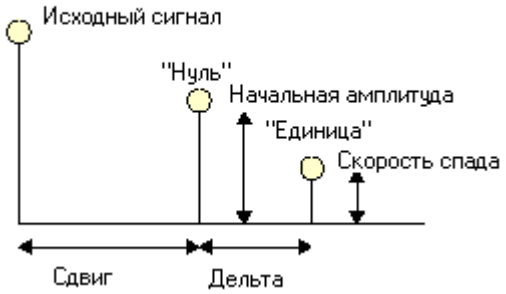


Рисунок 1.8 – Параметры эхо-сигнала

Кодер использует два времени задержки: одно для кодирования нуля, другое для кодирования единицы. И то, и другое время задержки меньше того, на котором человеческое ухо может распознать эхо. Кроме уменьшения времени задержки необходимо добиться установлением начальной амплитуды и времени спада того, чтобы внедренная информация не могла быть воспринята системой слуха человека.

Кодирование. Для простоты, был выбран пример только двух импульсов (один для копирования исходного сигнала, другой для формирования эхо сигнала). Увеличение количества импульсов приведет к увеличению количества отсчетов эхо-сигналов.

Пусть на рис. 1.9(а) показан способ кодирования «единицы» а на рис. 1.9(б) – способ кодирования «нуля». Внедрение данных показано на рис.1.10.

Задержка (δ_h) между исходным сигналом и его эхо зависит от внедряемых в данный момент данных. Единице соответствует задержка (δ_1), а нулю – задержка эхо-сигнала (δ_0).

Для того чтобы закодировать более одного бита, исходный сигнал разделяется на маленькие участки. Каждый участок рассматривается как

отдельный сигнал, и в него внедряется один бит информации. Результирующий закодированный сигнал (содержащий несколько бит внедренной информации) представляет собой комбинацию отдельных участков. На рис. 1.11 показан пример, в котором сигнал разделяется на семь участков – a, b, c, d, e, f, g.

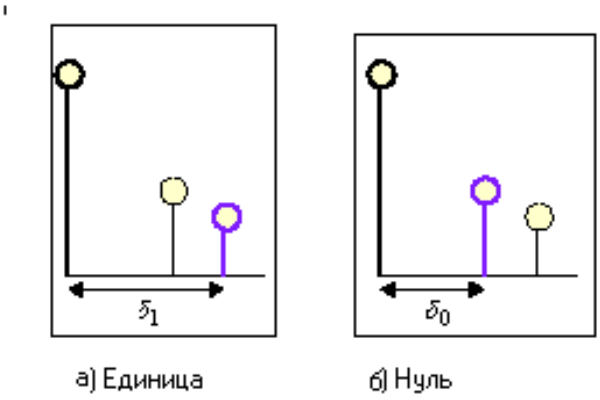


Рисунок 1.9 – Кодирование одного бита информации

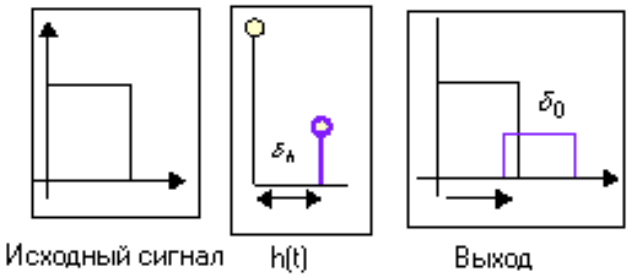


Рисунок 1.10 – Внедрение одного бита информации

В участки a, c, d, g будет внедрена единица. Следовательно, на этих участках система будет функционировать так, как показано на рис. 1.9(а). Нули будут внедрены в участки b, e, f, на этих участках система будет функционировать так, как показано на рис.1.9(б).

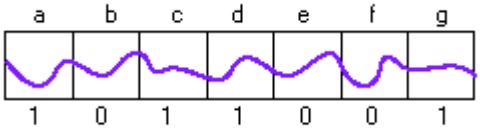


Рисунок 1.11 – Разделение сигнала на участки

Для достижения минимума заметности сначала создаются два сигнала: один, содержащий только "единицы", и другой – содержащий только нули. Полученные в результате сигналы показаны на рис. 1.12.

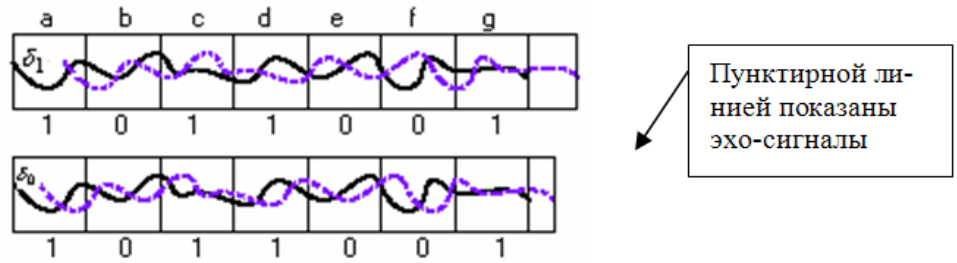


Рисунок 1.12 – Сигналы, содержащие только одно бинарное значение

Затем создаются два переключающих сигнала – нулевой и единичный (рис. 1.13). Каждый из них представляет собой бинарную последовательность, состояние которой зависит от того, какой бит должен быть внедрен в данный участок звукового сигнала.

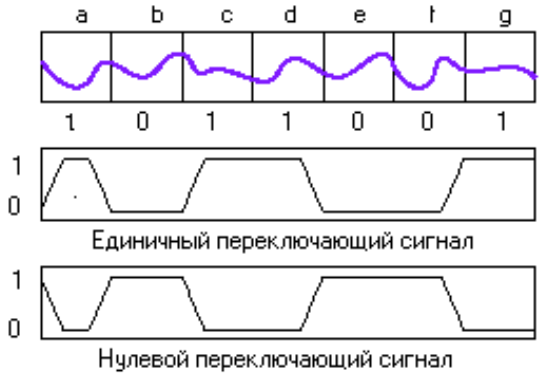


Рисунок 1.13 – Переключающие сигналы

Далее вычисляется сумма произведений нулевого смешивающего сигнала и аудио-сигнала с задержкой «нуль», а также единичного смешивающего сигнала и аудио-сигнала с задержкой «единица». Другими словами, когда в аудио-сигнал необходимо внедрить «единицу», на выход подается сигнал с задержкой «единица», в противном случае – сигнал с задержкой "нуль". Так как сумма двух смешивающих сигналов всегда равна

единице, то обеспечивается гладкий переход между участками аудио-сигнала, в которые внедрены различные биты. Блок-схема стегокодера показана на рис. 1.14.

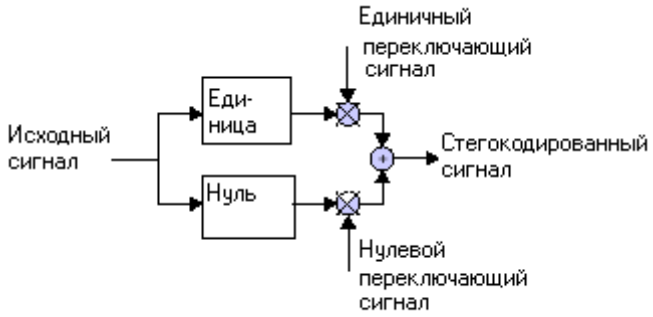


Рисунок 1.14-Блок-схема стегокодера

Декодирование. Декодирование внедренной информации представляет собой определение промежутка времени между сигналом и эхо. Для этого необходимо рассмотреть амплитуду (в двух точках) автокорреляционной функции дискретного косинусного преобразования логарифма спектра мощности (кепстра).

В результате вычисления кепстра получится последовательность импульсов (эхо, дублированное каждые δ секунд) (рис. 1.15).

Для определения промежутка времени между сигналом и его эхом необходимо рассчитать автокорреляционную функцию кепстра.

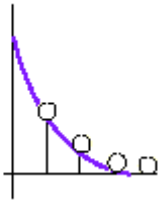


Рисунок 1.15 – Результат вычисления кепстра

Всплеск автокорреляционной функции будет иметь место через δ_1 или δ_0 секунд после исходного сигнала (рис. 1.16). Правило декодирования основано на определении промежутка времени между исходным сигналом и всплеском автокорреляции.

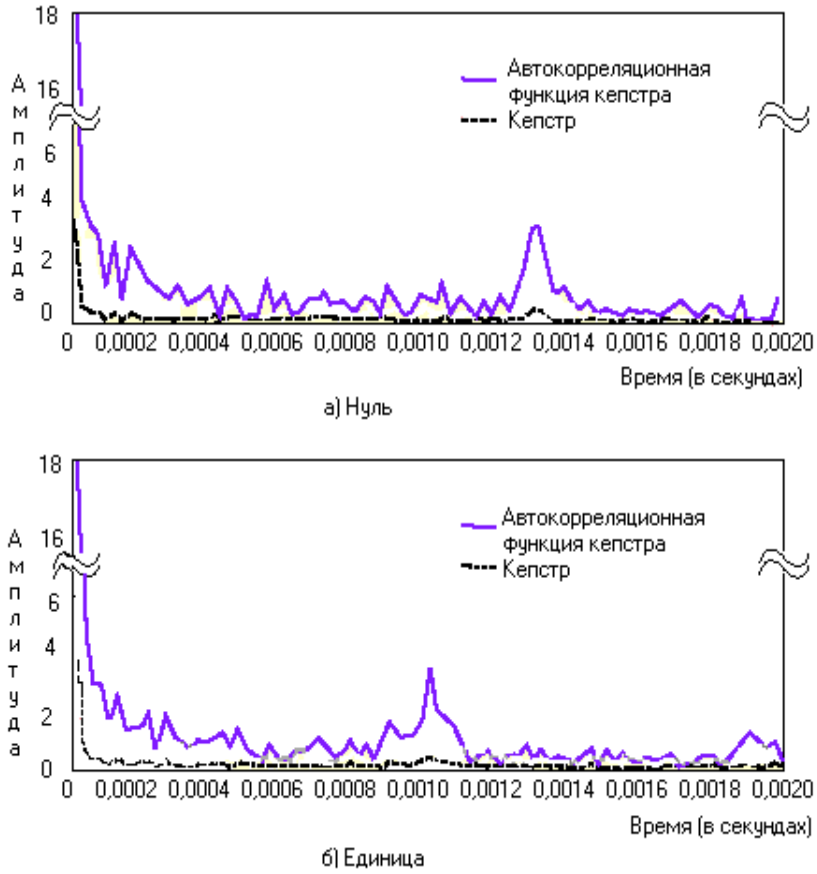


Рисунок 1.16-Поведение автокорреляционной функции при различной внедренной информации

При декодировании "единица" принимается, если значение автокорреляционной функции через δ_1 секунд больше чем через δ_0 секунд, в противном случае – "нуль".

По исследованиям В. Бендера и Н. Моримото данная схема позволяет внедрять 16 бит в одну секунду аудиозаписи незаметно, без потери ее качества.

1.4 Методы маскирования ЦВЗ

К методам, использующим не только особенности строения аудио-сигналов, но и системы слуха человека относится также метод маскирования сигнала. Маскированием называется эффект, при котором слабое, но слышимое звуковое колебание становится неслышимым при наличии другого более громкого (сигнал маскирования). Эффект маскирования зависит от спектральных и временных характеристик маскируемого сигнала и сигнала маскирования.

Можно говорить о маскировании по частоте и маскировании по времени. Первое заключается в следующем: если два сигнала одновременно находятся в ограниченной частотной области, то более слабый сигнал становится неслышимым на фоне более сильного. Порог маскирования зависит от частоты, уровня подавления сигнала и тональной или шумовой характеристик маскируемого сигнала и сигнала маскирования. Легче широкополосным шумовым сигналом маскировать тональное колебание, чем наоборот. Кроме того, более высокочастотные колебания маскировать легче. Маскирование по времени определяет следующий эффект: более слабый сигнал становится не слышимым за 5 – 20 мс до включения колебания маскирования и становится слышимым через 50 – 200 мс после его выключения.

Воспользовавшись информацией о маскировании по частоте для системы слуха человека, мы можем определить спектральные характеристики внедряемой информации. Обработка импульсных сигналов, таких как звук кастаньет, может привести к образованию слышимого пре-эхо. Для устранения этого эффекта при внедрении информации его также необходимо учитывать.

Рассмотрим конкретный метод внедрения ЦВЗ (псевдослучайной последовательности) с использованием эффекта маскирования. Каждый аудиосигнал помечается уникальным кодовым словом. Для того, чтобы

использовать маскирующие характеристики системы слуха человека по частоте необходимо соотнести ПСП с порогом маскирования сигнала, при этом необходимо также учесть эффект временного маскирования. Невозможно внести большое количество информации в сигнал малой мощности, в противном случае внедренная информация может стать слышимой. Это происходит из-за того, что преобразование Фурье фиксированной длины не может сразу обладать хорошей локализацией в частотной и временной областях. Если время длительности сигнала высокой мощности больше длительности окна, то его энергия распространяется по всем частотам. Следовательно, необходимо взвешивать ЦВЗ с энергией сигнала.

Для внедрения ЦВЗ необходимо вычислить порог маскирования сигнала. Порог маскирования определяется для сегментов аудио-сигнала длиной 512 отсчетов, взвешенных при помощи окна Хэмминга, с 50% перекрытием текущих блоков. Он аппроксимируется идеальным фильтром 10-го порядка, *M(w)*, с использованием критерия наименьших квадратов. ПСП фильтруется с применением фильтра *M(w)*, чтобы обеспечить то, что спектральная плотность мощности ЦВЗ была ниже порога маскирования.

ЦВЗ, находящийся ниже порога маскирования в частотной области, распространяется на все окно 512 отсчетов. Если внутри блока имеются пиковые изменения амплитуды, то области сигнала высокой мощности распространяются на области сигнала низкой мощности, создавая ощутимые искажения. Слышимым эффектом будет шум, предшествующий пиковому изменению амплитуды. Поэтому ЦВЗ взвешивается во временной области с взятой в квадрат и нормированной огибающей сигнала,

$$w(n)=w(n)*\frac{envelope(u)^2}{\sum_{k=1}^{N} envelope(k)^2}. \qquad (1.9)$$

Для облегчения обнаружения ЦВЗ нужно увеличить его мощность, но при этом необходимо, чтобы спектральная плотность мощности ЦВЗ

оставалась ниже порога маскирования. Если «вычисленный ЦВЗ» меньше шага квантования его нужно увеличить во столько раз, чтобы ЦВЗ в процессе квантования не был потерян.

Если во всех отрезках времени ЦВЗ ниже порога маскирования, то можно утверждать, что ЦВЗ неслышим.

На рис. 1.17 изображена блок-схема устройства встраивания ЦВЗ в аудио-сигнал. В базовой схеме внедрения ЦВЗ кодовое слово фильтруется при помощи фильтра, приближенного по характеристикам к системе слуха человека. Полученный результат сравнивается во времени с исходным аудио-сигналом, для исключения временных эффектов, таких, как пре-эхо. Затем результат добавляется к оригинальному аудио-сигналу, давая в результате

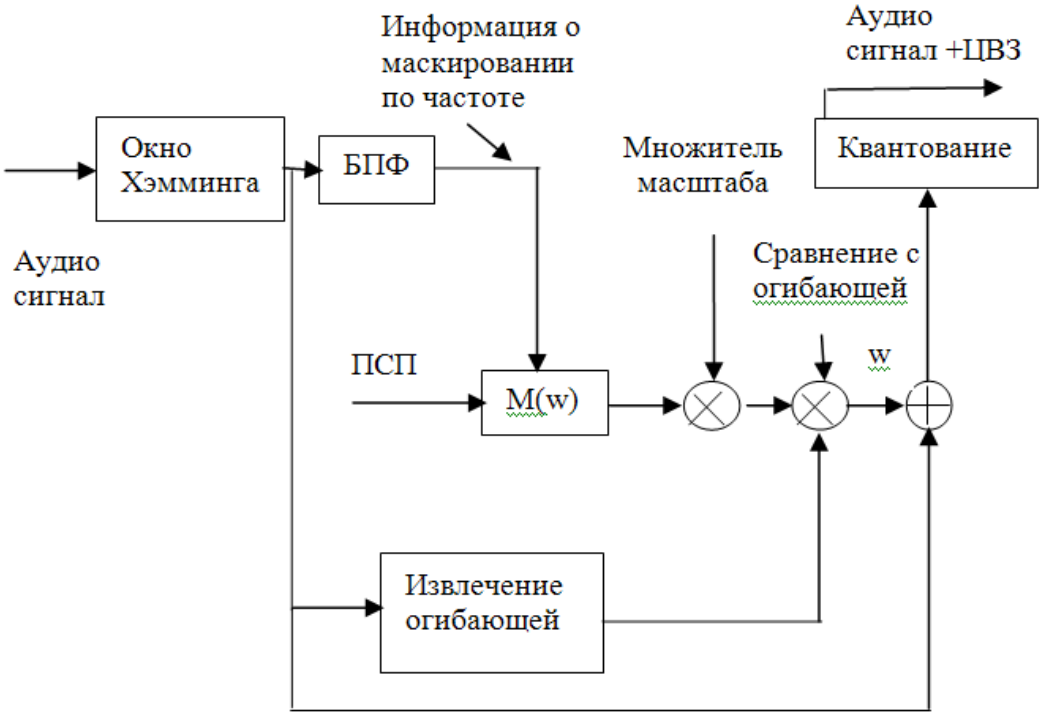


Рисунок 1.17 – Блок-схема генератора ЦВЗ

$$Watermark_{firststage}=(original\ signal)+w, \qquad (1.10)$$

где под *w* понимается отфильтрованная ПСП.

Исследования А. К. Хамди и др. показывают, что ЦВЗ лучше размещать в высокочастотной области сигнала.

Незарегистрированный пользователь будет пытаться сделать невозможным распознавание ЦВЗ, добавляя к нему окрашенный шум, фильтруя его, кодируя, осуществляя над ним цифро-аналоговое и аналогово-цифровое преобразование, сжатие и т.д. При рассмотрении проблемы распознавания предполагается, что оригинальный сигнал доступен, как распознавателю, так и автору ПСП.

Необходимо различить пиратский аудио-сигнал $s(t)$ и подлинный аудио-сигнал $r(t)$, на который наложились помехи и ЦВЗ. При этом подлежат проверке следующие гипотезы:

$$\begin{aligned} H_0: &\quad x(t)=r(t)-s(t)=n(t) \\ H_1: &\quad x(t)=r(t)-s(t)=w(t)+n(t). \end{aligned} \tag{1.11}$$

Отметим, что ЦВЗ неслышим, и нас интересуют случаи, когда искажения, вносимые незарегистрированным пользователем также неслышны. Можно использовать взаимную корреляцию между *x* и *w*, чтобы обнаружить наличие ЦВЗ с помехами, сравнивая его с порогом. Исследования А.Хамди и др. показывают, что возможно надежно определять наличие ЦВЗ при использовании 50 или более блоков по 512 отсчетов для порога приблизительно равного 0,7. Необходимо отметить, что это определено для 0,8 секунды аудио-сигнала (при частоте дискретизации 32 к Гц).

Тогда можно вычислить вероятность определения и вероятность ложного определения для каждого сегмента из 50 блоков по 512 отсчетов. При этом, даже если ЦВЗ произведены при помощи одинаковых псевдослучайных последовательностей для всего аудио-сигнала, то в течение сигнала они будут изменяться в зависимости от порога маскирования и мощности сигнала для каждого блока из 512 отсчетов.

Автор должен выбирать различные ПСП для каждого аудио-сигнала, чтобы его подписи невозможно было найти сравнением или изучением зависимости между несколькими аудио-сигналами.

Вероятность обнаружения ЦВЗ и вероятность ложного обнаружения были соответственно равны 1 и $3.1285 * 10^{-4}$, для порога 0,7.

Данная система является также стойкой к аналого-цифровым и цифро-аналоговым преобразованиям.

Несмотря на то, что в рассмотренном методе используются свойства, присущие аудио-сигналам, он может быть после некоторой модификации успешно применен и для внедрения информации в видео.

1.5 Вывод по главе

Мною были рассмотрены требования, которые предъявляются к стегосистемам, применяемым для встраивания информации в аудиосигналы и сделал вывод, что практически все аудиосигналы имеют характерную особенность. Любой из них представляет собой достаточно большой объем данных, для того, чтобы использовать статистические методы внедрения информации.

Также рассмотрены методы кодирования с расширением спектра, методы внедрения информации в аудио сигналы, методы маскирования ЦВЗ.

Проведенный обзор позволяет сделать выбор методов, которые удовлетворяют поставленным задачам.

2. РАЗРАБОТКА АЛГОРИТМА СКРЫТИЯ ИНФОРМАЦИИ В АУДИОСИГНАЛАХ

2.1 Стандарт шифрования данных Data Encryption Standard

В 1977 году Национальное бюро Стандартов США (NBS) опубликовало стандарт шифрования данных Data Encryption Standard (DES), предназначенный для использования в государственных и правительственных учреждениях США для защиты от несанкционированного доступа важной, но несекретной информации. Алгоритм, положенный в основу стандарта, распространялся достаточно быстро, и уже в 1980 году был одобрен ANSI. С этого момента DES превращается в стандарт не только по названию (Data Encryption Standard), но и фактически. Появляются программное обеспечение и специализированные микро-ЭВМ, предназначенные для шифрования/дешифрования информации в сетях передачи данных и на магнитных носителях. К настоящему времени DES является наиболее распространенным алгоритмом, используемым в системах защиты коммерческой информации.

Основные достоинства алгоритма DES:

- используется только один ключ длиной 56 битов;
- зашифровав сообщение с помощью одного пакета, для расшифровки вы можете использовать любой другой;
- относительная простота алгоритма обеспечивает высокую скорость обработки информации;
- достаточно высокая стойкость алгоритма.

DES осуществляет шифрование 64-битовых блоков данных с помощью 56-битового ключа. Расшифрование в DES является операцией обратной шифрованию и выполняется путем повторения операций шифрования в обратной последовательности.

Процесс шифрования заключается в начальной перестановке битов 64-битового блока, шестнадцати циклах шифрования и, наконец, обратной перестановки битов (рис.2.1).



Рисунок 2.1 – Обобщенная схема шифрования в алгоритме DES

Все перестановки и коды в таблицах подобраны разработчиками таким образом, чтобы максимально затруднить процесс расшифровки путем подбора ключа. Структура алгоритма DES приведена на рис. 2.2.

Пусть из файла считан очередной 8-байтовый блок T, который преобразуется с помощью матрицы начальной перестановки IP (табл.2.1) следующим образом: бит 58 блока T становится битом 1, бит 50 – битом 2 и т.д., что даст в результате: T(0) = IP(T).

Полученная последовательность битов T(0) разделяется на две последовательности по 32 бита каждая: L(0) – левые или старшие биты, R(0) – правые или младшие биты.

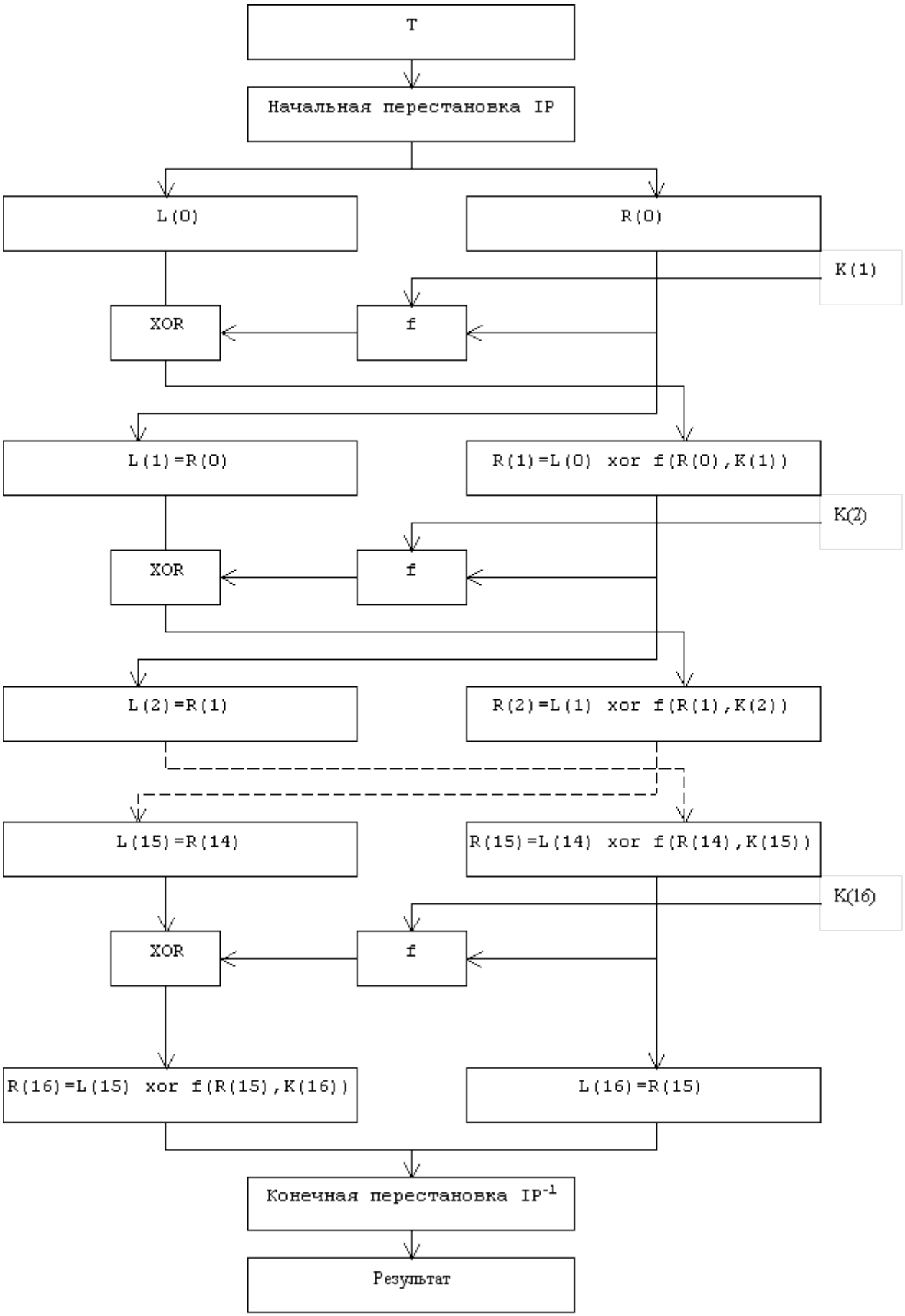


Рисунок 2.2 – Структура алгоритма шифрования DES

Таблица 2.1 – Матрица начальной перестановки IP

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Затем выполняется шифрование, состоящее из 16 итераций. Результат i-й итерации описывается следующими формулами:

$$L(i) = R(i-1)$$
$$R(i) = L(i-1)\ xor\ f(R(i-1),\ K(i))$$

где xor – операция «исключающее или».

Функция f называется функцией шифрования. Ее аргументы – это 32-битовая последовательность R(i-1), полученная на (i-1)-ой итерации, и 48-битовый ключ K(i), который является результатом преобразования 64-битового ключа K.

На 16-й итерации получают последовательности R(16) и L(16) (без перестановки), которые конкатенируют в 64-битовую последовательность R(16)L(16).

Затем позиции битов этой последовательности переставляют в соответствии с матрицей IP-1 (табл.2.2).

Таблица 2.2 – Матрица обратной перестановки IP^{-1}

40	08	48	16	56	24	64	32
39	07	47	15	55	23	63	31
38	06	46	14	54	22	62	30
37	05	45	13	53	21	61	29
36	04	44	12	52	20	60	28
35	03	43	11	51	19	59	27
34	02	42	10	50	18	58	26

```
33 01 41 09 49 17 57 25
```

Матрицы IP-1 и IP соотносятся следующим образом: значение 1-го элемента матрицы IP-1 равно 40, а значение 40-го элемента матрицы IP равно 1, значение 2-го элемента матрицы IP-1 равно 8, а значение 8-го элемента матрицы IP равно 2 и т.д.

Процесс расшифрования данных является инверсным по отношению к процессу шифрования. Все действия должны быть выполнены в обратном порядке. Это означает, что расшифровываемые данные сначала переставляются в соответствии с матрицей IP-1, а затем над последовательностью бит R(16)L(16) выполняются те же действия, что и в процессе шифрования, но в обратном порядке.

Итеративный процесс расшифрования может быть описан следующими формулами:

$$L(i) = R(i-1),\ i = 1, 2, \ldots, 16$$
$$R(i) = L(i-1)\ xor\ f(R(i-1), K(i)), = 1, 2, \ldots, 16$$

На 16-й итерации получают последовательности L(0) и R(0), которые конкатенируют в 64-битовую последовательность L(0)R(0).

Затем позиции битов этой последовательности переставляют в соответствии с матрицей IP. Результат такой перестановки – исходная 64-битовая последовательность.

Теперь рассмотрим функцию шифрования f(R(i-1),K(i)). Схематически она показана на рис. 2.3.

Для вычисления значения функции f используются следующие функции-матрицы:

- E – расширение 32-битовой последовательности до 48-битовой,
- S1, S2, ... , S8 – преобразование 6-битового блока в 4-битовый,
- P - перестановка бит в 32-битовой последовательности.

Функция расширения E определяется табл.2.3. В соответствии с этой таблицей первые 3 бита E(R(i-1)) – это биты 32, 1 и 2, а последние – 31, 32 и 1.

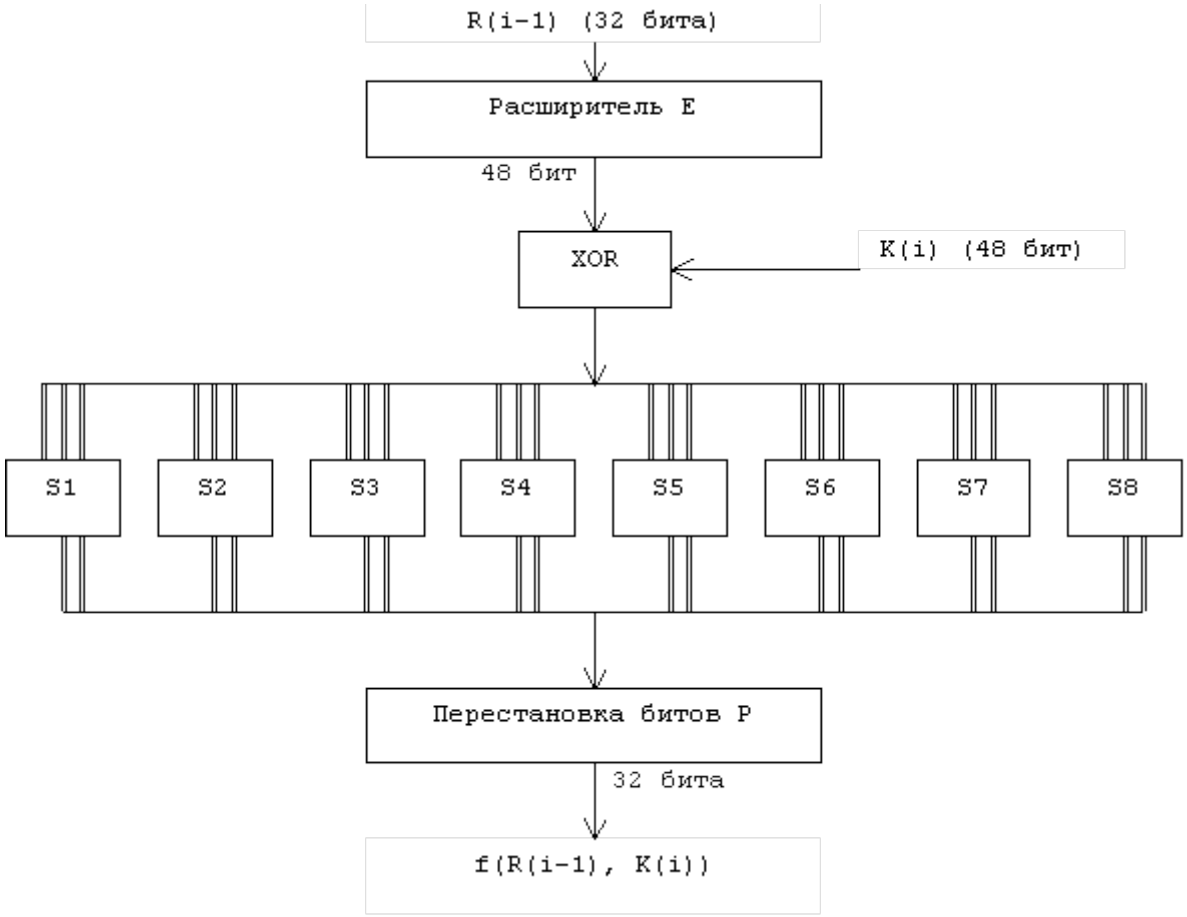


Рисунок 2.3 - Вычисление функции f(R(i-1),K(i))

Таблица .2.3 – Функция расширения E

```
32 01 02 03 04 05
04 05 06 07 08 09
08 09 10 11 12 13
12 13 14 15 16 17
16 17 18 19 20 21
20 21 22 23 24 25
24 25 26 27 28 29
28 29 30 31 32 01
```

Результат функции E(R(i-1)) есть 48-битовая последовательность, которая складывается по модулю 2 (операция xor) с 48-битовым ключом K(i). Получается 48-битовая последовательность, которая разбивается на восемь 6-битовых блоков B(1)B(2)B(3)B(4)B(5)B(6)B(7)B(8). То есть:

$$E(R(i-1)) \; xor \; K(i) = B(1)\; B(2) \cdots B(8)$$

Функции S1, S2, ... , S8 определяются табл.2.4.

Таблица 2.4 – Функции преобразования S1, S2, ..., S8

Номер строки	Номер столбца 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15	
0	14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7	S1
1	0 15 7 4 14 2 13 1 10 6 12 11 9 5 3 8	
2	4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0	
3	15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13	
0	15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10	S2
1	3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5	
2	0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15	
3	13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9	
0	10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8	S3
1	13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1	
2	13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7	
3	1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12	
0	7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15	S4
1	13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9	
2	10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4	
3	3 15 0 6 10 1 13 8 9 4 5 11 12 7 2 14	
0	2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9	S5
1	14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6	
2	4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14	
3	11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3	
0	12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11	S6
1	10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8	
2	9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6	
3	4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13	
0	4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1	S7
1	13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6	
2	1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2	
3	6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12	
0	13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7	S8
1	1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2	
2	7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8	
3	2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11	

К табл.2.4. требуются дополнительные пояснения. Пусть на вход функции-матрицы Sj поступает 6-битовый блок B(j) = b1b2b3b4b5b6, тогда

двухбитовое число b1b6 указывает номер строки матрицы, а b2b3b4b5 - номер столбца. Результатом Sj(B(j)) будет 4-битовый элемент, расположенный на пересечении указанных строки и столбца.

Например, B(1)=011011. Тогда S1(B(1)) расположен на пересечении строки 1 и столбца 13. В столбце 13 строки 1 задано значение 5. Значит, S1(011011)=0101.

Применив операцию выбора к каждому из 6-битовых блоков B(1), B(2), ...,B(8), получаем 32-битовую последовательность S1(B(1))S2(B(2))S3(B(3))...S8(B(8)).

Наконец, для получения результата функции шифрования надо переставить биты этой последовательности. Для этого применяется функция перестановки P (табл.2.5). Во входной последовательности биты перестанавливаются так, чтобы бит 16 стал битом 1, а бит 7 - битом 2 и т.д.

Таблица 2.5 – Функция перестановки P

16	07	20	21
29	12	28	17
01	15	23	26
05	18	31	10
02	08	24	14
32	27	03	09
19	13	30	06
22	11	04	25

Таким образом,

$$f(R(i-1), K(i)) = P(S1(B(1)), \ldots, S8(B(8)))$$

Чтобы завершить описание алгоритма шифрования данных, осталось привести алгоритм получения 48-битовых ключей K(i), i=1...16. На каждой итерации используется новое значение ключа K(i), которое вычисляется из начального ключа K. K представляет собой 64-битовый блок с восемью

битами контроля по четности, расположенными в позициях 8,16,24,32,40,48,56,64.

Для удаления контрольных битов и перестановки остальных используется функция G первоначальной подготовки ключа (табл.2.6).

Таблица 2.6 – Матрица G первоначальной подготовки ключа

```
57 49 41 33 25 17 09
01 58 50 42 34 26 18
10 02 59 51 43 35 27
19 11 03 60 52 44 36
63 55 47 39 31 23 15
07 62 54 46 38 30 22
14 06 61 53 45 37 29
21 13 05 28 20 12 04
```

Результат преобразования G(K) разбивается на два 28-битовых блока C(0) и D(0), причем C(0) будет состоять из битов 57, 49, ..., 44, 36 ключа K, а D(0) будет состоять из битов 63, 55, ..., 12, 4 ключа K. После определения C(0) и D(0) рекурсивно определяются C(i) и D(i), i=1...16. Для этого применяют циклический сдвиг влево на один или два бита в зависимости от номера итерации, как показано в табл.2.7.

Таблица 2.7 – Таблица сдвигов для вычисления ключа

Номер итерации	Сдвиг (бит)
01	1
02	1
03	2
04	2
05	2
06	2
07	2
08	2
09	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Полученное значение вновь "перемешивается" в соответствии с матрицей H (табл.2.8). Ключ K(i) будет состоять из битов 14, 17, ..., 29, 32 последовательности C(i)D(i). Таким образом:

$$K(i)=H(C(i)\ D(i))$$

Блок-схема алгоритма вычисления ключа приведена на рис.2.4.

Таблица 2.8 – Матрица H завершающей обработки ключа

14	17	11	24	01	05
03	28	15	06	21	10
23	19	12	04	26	08
16	07	27	20	13	02
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

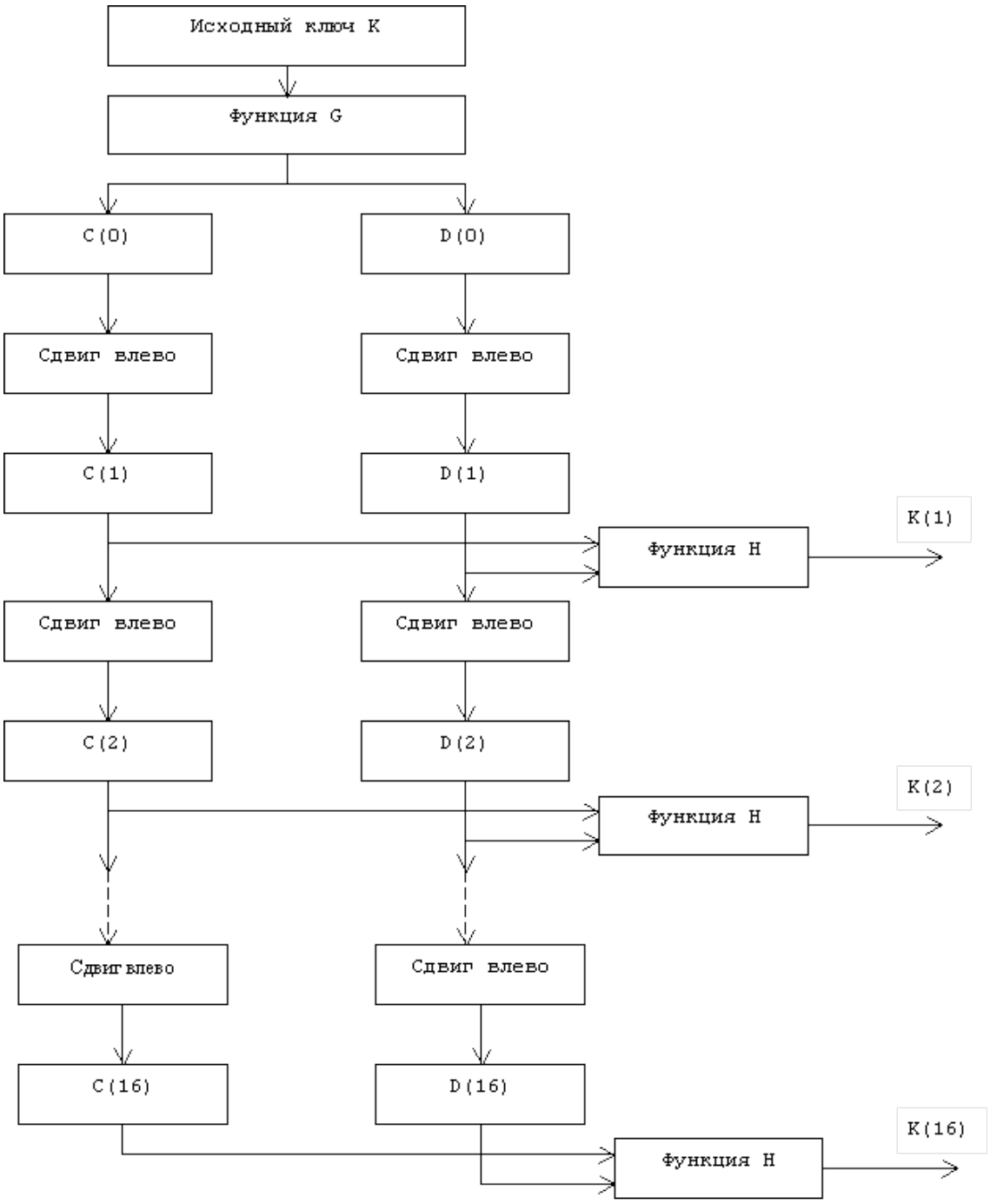


Рисунок 2.4 - Блок-схема алгоритма вычисления ключа K(i)

Восстановление исходного текста осуществляется по этому алгоритму, но вначале используется ключ K(15), затем - K(14) и так далее.

2.2 Алгоритм скрытия информации в аудиосигналах

Реализация программного продукта данной дипломной работы будет проходить с использованием именно LSB. LSB-метод для большинства стандартов файлов-контейнеров не требуют значительных затрат времени и сил — идея указанного метода проста.

Наиболее распространенным на сегодняшний день методом цифровой стеганографии является метод, заключающейся во вложении скрываемого сообщения путем модификации наименее значимых бит (LSB).

Достоинства метода заключаются в его простоте и сравнительно большом объеме встраиваемых данных.

Один из методов улучшения робастности LSB-методов заключается в использовании избыточности и управления местом размещения сообщения с помощью секретного ключа.

Восемь бит, расположенных рядом, называют байтом (byte). Два байта, то есть шестнадцать бит – словом (word). Основное использование байта – хранение двоичных чисел из восьми цифр. Хотя не менее часто он используется для хранения символов.

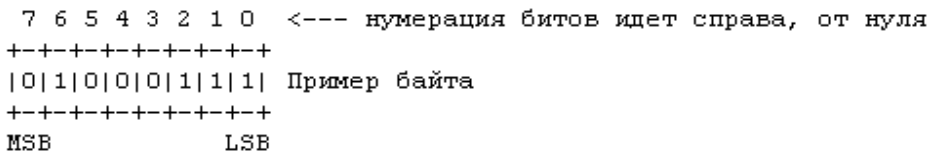


Рисунок 2.5 – Порядок нумерации битов в байте

MSB обозначает Most Significant Bit – старший значащий бит или просто старший бит. Обычно он имеет номер семь. LSB – Least Significant Bit, младший (значащий) бит, бит номер ноль.

```
151413121110 9 8 7 6 5 4 3 2 1 0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1|1|0|1|1|1|1|1|1|1|0|0|1|1|1|0| Пример слова
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
MSB                             LSB
```

Рисунок 2.6 – Порядок нумерации битов в слове

Здесь старший бит (MSB) уже имеет номер 15. Биты с нулевого по седьмой образуют младший байт (low byte), биты с восьмого по пятнадцатый – старший байт (high byte).

Алгоритм скрытия. Любой файла представляет собой последовательность нулей и единиц, а значит его можно представить как поток бит. Разбивая его на маленькие группы по 1-6 бит, можно вписывать эти группы в очередную порцию мультимедиа-данных из файла-носителя (далее будем называть его источником). Процесс скрытия изображен на рис. 2.7.

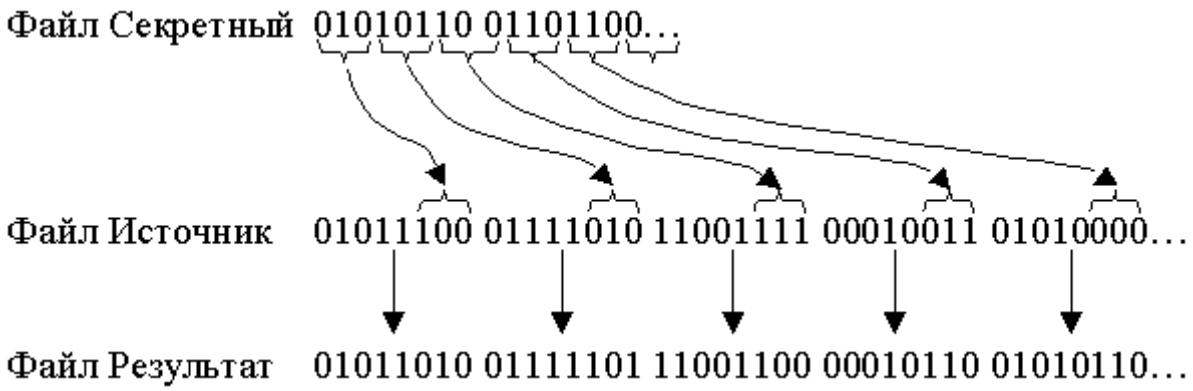


Рисунок 2.7 – Процесс скрытия изображения

На рисунке весь файл Секретный, который будем прятать, разбит на группки по 3 бита. В каждом байте файла Источник, который будет носителем скрытой информации, выделяются три младших бита. Эти три младших бита (в каждом байте источника) заменяются на три очередных бита из секретного файла. Таким образом, файл Результат является файлом того же типа, что и файл Источник (то есть WAV-файл), причем каждый его байт сформирован следующим образом: первые пять бит берутся из файла

Источник, а оставшиеся три – очередная группка из файла Секретный. Самое главное, что при такой замене результат звучит так же, как и источник. Конечно, заметность изменений тем больше, чем больше младших бит заменяется.

Если заменяется только один младший бит, то абсолютное значение величины звукового сигнала может измениться только на единицу (если младший бит был 0, а стал 1, или наоборот).

Если заменяется два младших бита, то сигнал может измениться максимум на 3 единицы (если два младших бита были 00, а стали 11, или наоборот).

Аналогично при замене 3 бит возможно уже изменение на 7 единиц (000111 или наоборот), 4 бита – на 15, и 6 бит – на 63. Однако, важно не абсолютное изменение сигнала, а относительное. Так, для 8-битного звука (сигнал лежит в пределах 0 – 255) разность в 63 единицы может равняться половине сигнала, что изменит его до неузнаваемости, в то время как для 16-битного (сигнал в пределах 0 – 65535) такое изменение хотя и заметно, но не приводит к катастрофической потере качества.

2.3 Блок-схема программы

Листинг программы приведен в приложении А.

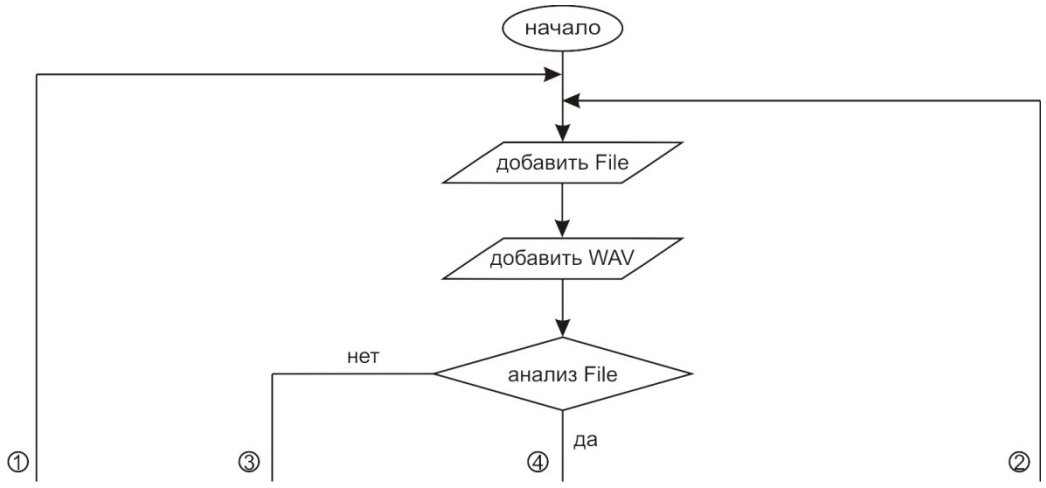


Рисунок 2.8 – Алгоритм работы программы (начало)

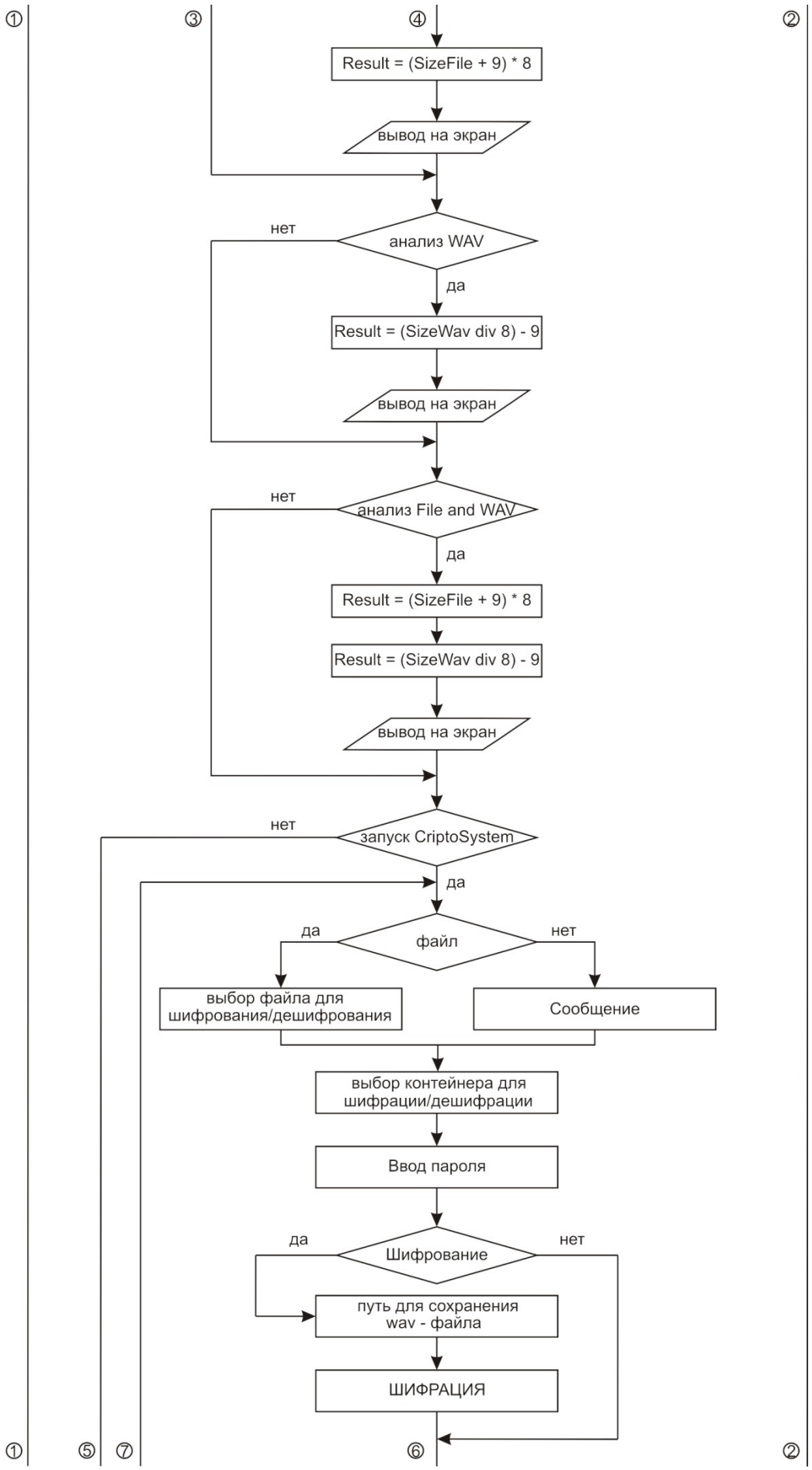


Рисунок 2.8 – Алгоритм работы программы (продолжение)

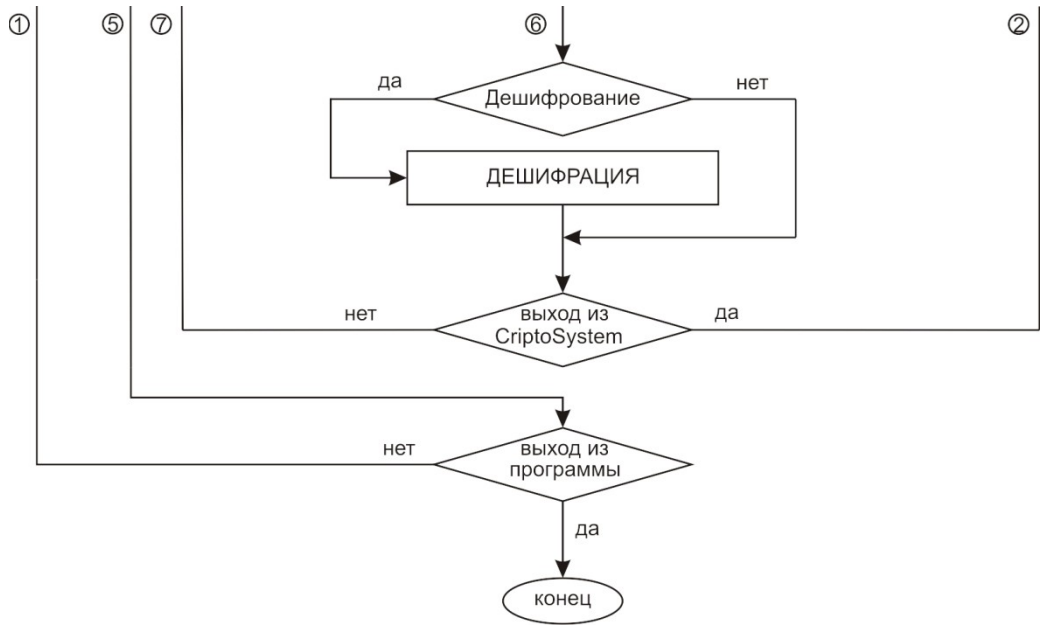


Рисунок 2.8 – Алгоритм работы программы (окончание)

2.4 Зависимость скрытия информации от размера секретного файла

При исследовании использовался контейнер (WAV-файл) размером 150 Mb. И скрываемая информация форматов DOC и TXT (4 DOC-файла и 4 TXT-файла), файлы были размером 2.5 Mb, 5 Mb, 10 Mb и 15 Mb. Также в DOC-файлах помимо текста находились изображения.

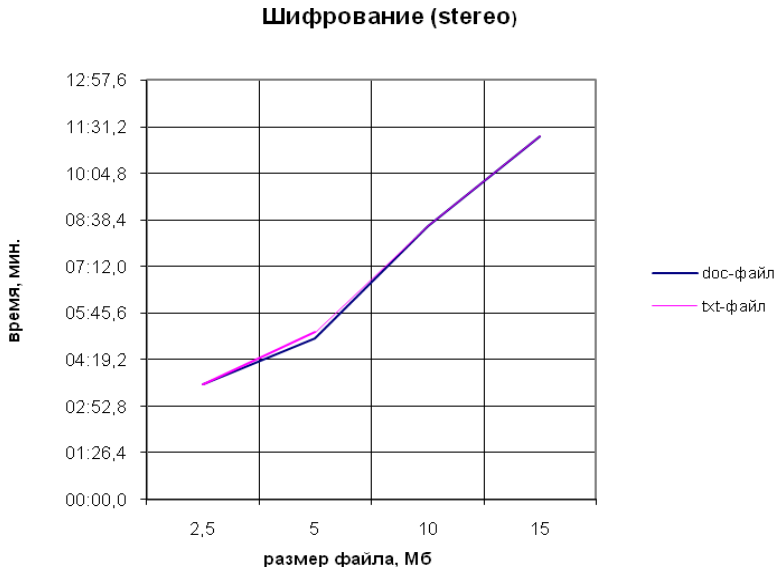


Рисунок 2.9 – Шифрование в Stereo сигнале

Контейнеры использовались двух видов первый с stereo сигналом, второй с mono сигналом.

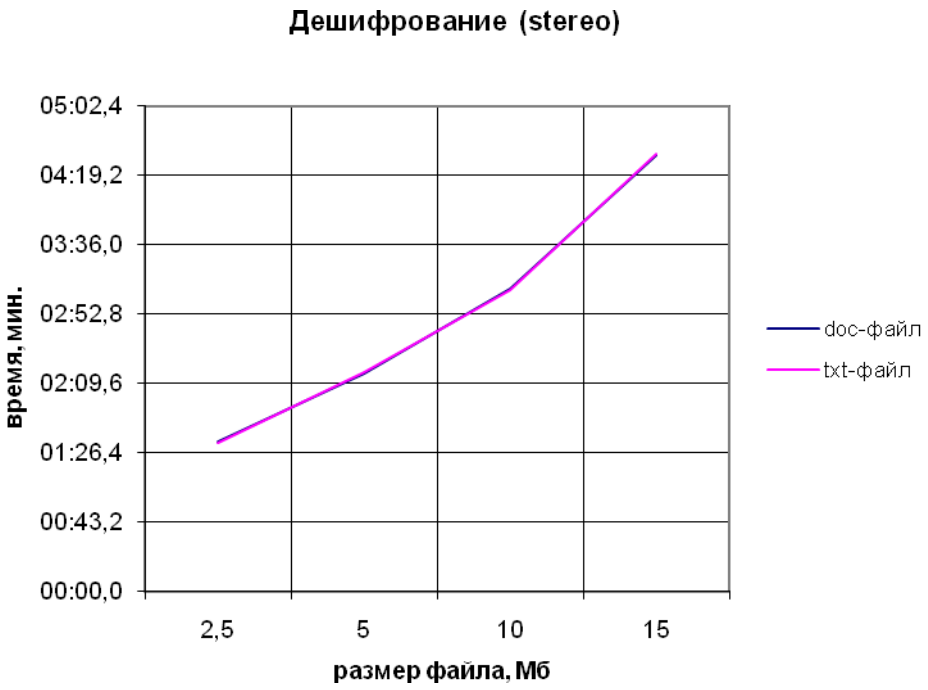


Рисунок 2.10 – Дешифрование в Stereo сигнале



Рисунок 2.11 – Шифрование в mono сигнале

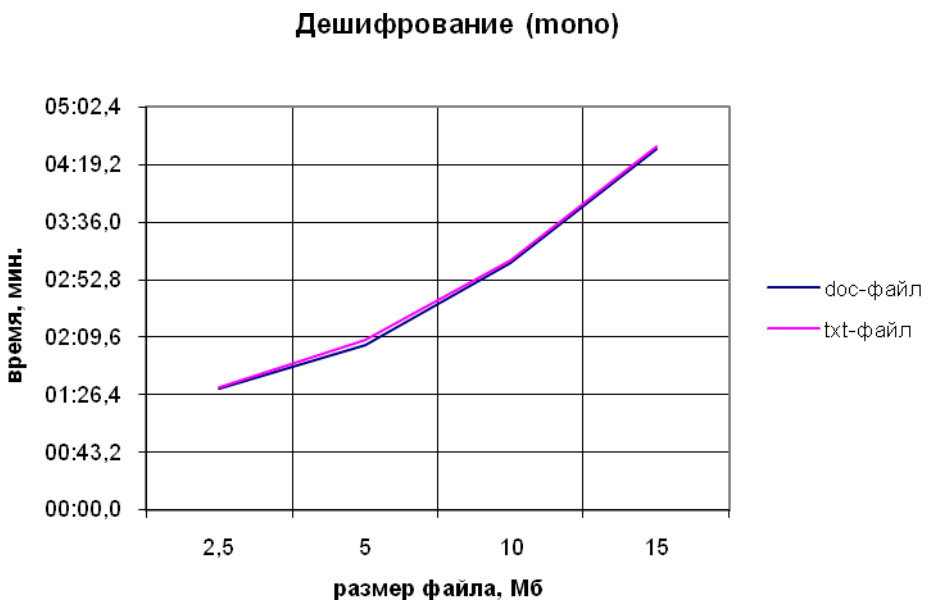


Рисунок 2.12 – Дешифрование в mono сигнале

2.5 Вывод по главе

В результате проведенных исследований было выявлено, что шифрование и скрытие информации происходит по линейной зависимости. На рисунках 2.8-2.11 показаны результаты по кодирование и декодированию информации txt и doc файлах, в stereo и mono сигналах.

На основе проведенных тестовых расчетов можно сделать следующее заключение о том, что скорость шифрования и дешифрования исследуемого алгоритма стеганографии не зависит от того, какая информация подается на вход системы шифрования/дешифрования. То есть, время шифрования и дешифрования изображения или какого-либо текстового файла будет одинакова, как в одном, так и в другом случае.

Так же наблюдается линейная зависимость времени шифрования/дешифрования от исходного объема информации подаваемой на вход стегосистемы исследуемого алгоритма. Причем дешифрование происходит на 50% быстрее чем шифрование.

3. ОПИСАНИЕ ПРОГРАММНОГО ПРОДУКТА ANALITIC CRYPTOSYSTEM

При шифровании в виде контейнера используется звуковой аудио сигнал с расширением WAV. В качестве секретного файла можно использовать любой файл, либо лично вводить текстовое сообщение в отдельном окне программы.

Analitic CriptoSystem – Эта программа предназначена для анализа и определения совместимости шифруемой информации и файла-контейнера.

После запуска программы Analitic CriptoSystem появляется окно (рис. 3.1)

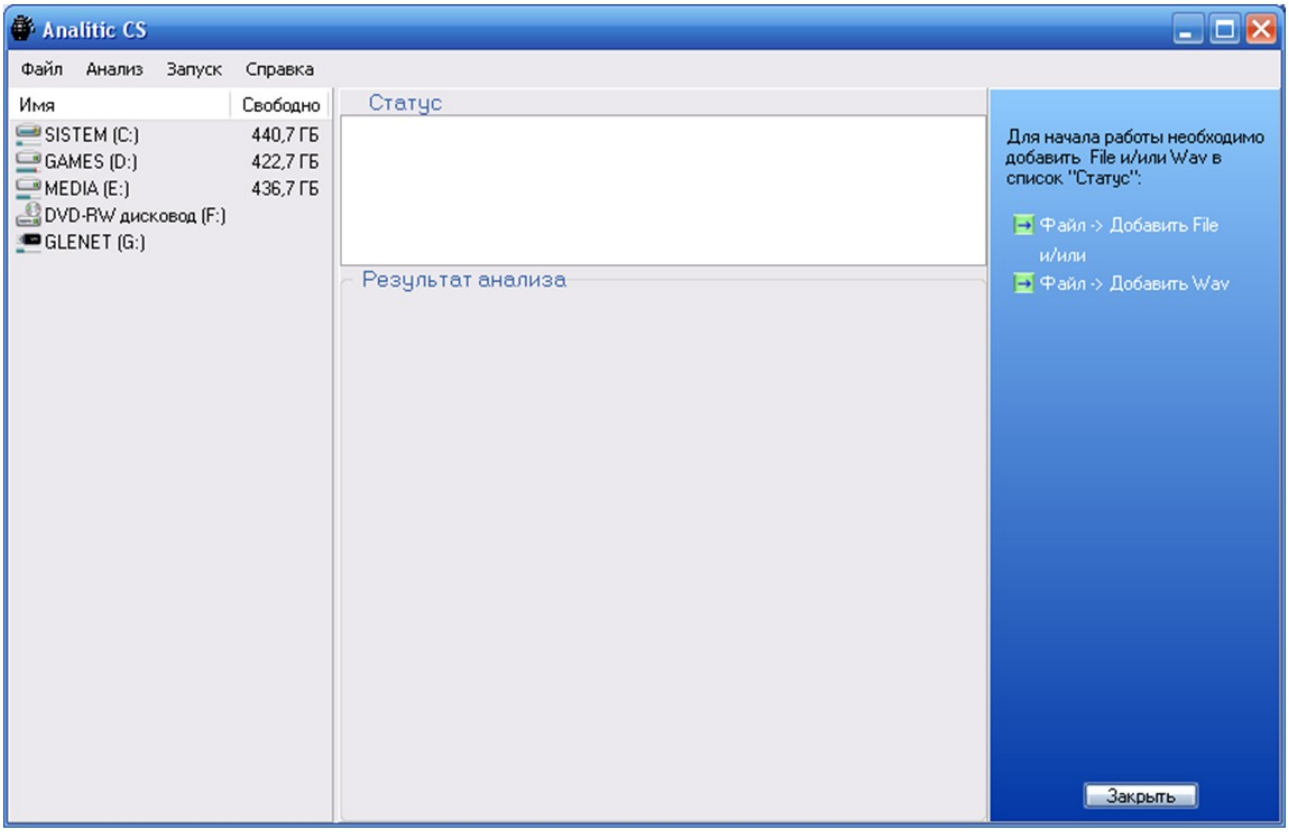


Рисунок 3.1 – Главное окно Analitic CriptoSystem

В левой части окна программы расположена информация о имеющихся жестких дисках и носителях (рис 3.2)

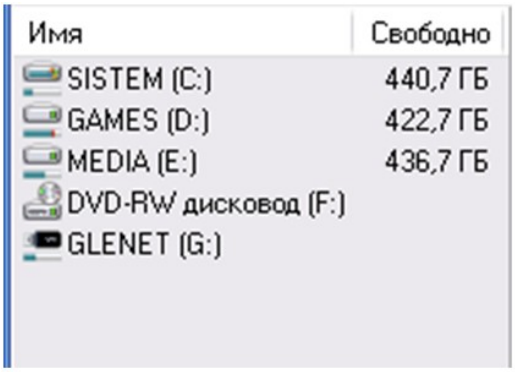


Рисунок 3.2 – Информация о жестких дисках и насителях

В правой части окна находится подсказка для пользователя. При желании пользователь может убрать подсказку нажа на кнопку «Закрыть» (см. рис 3.1).

В центральной части окна в поле «статус» отображается информация о текущей задачи. В разделе «Результат анализа» отображается конечный результат проводимых операций (рис 3.3).

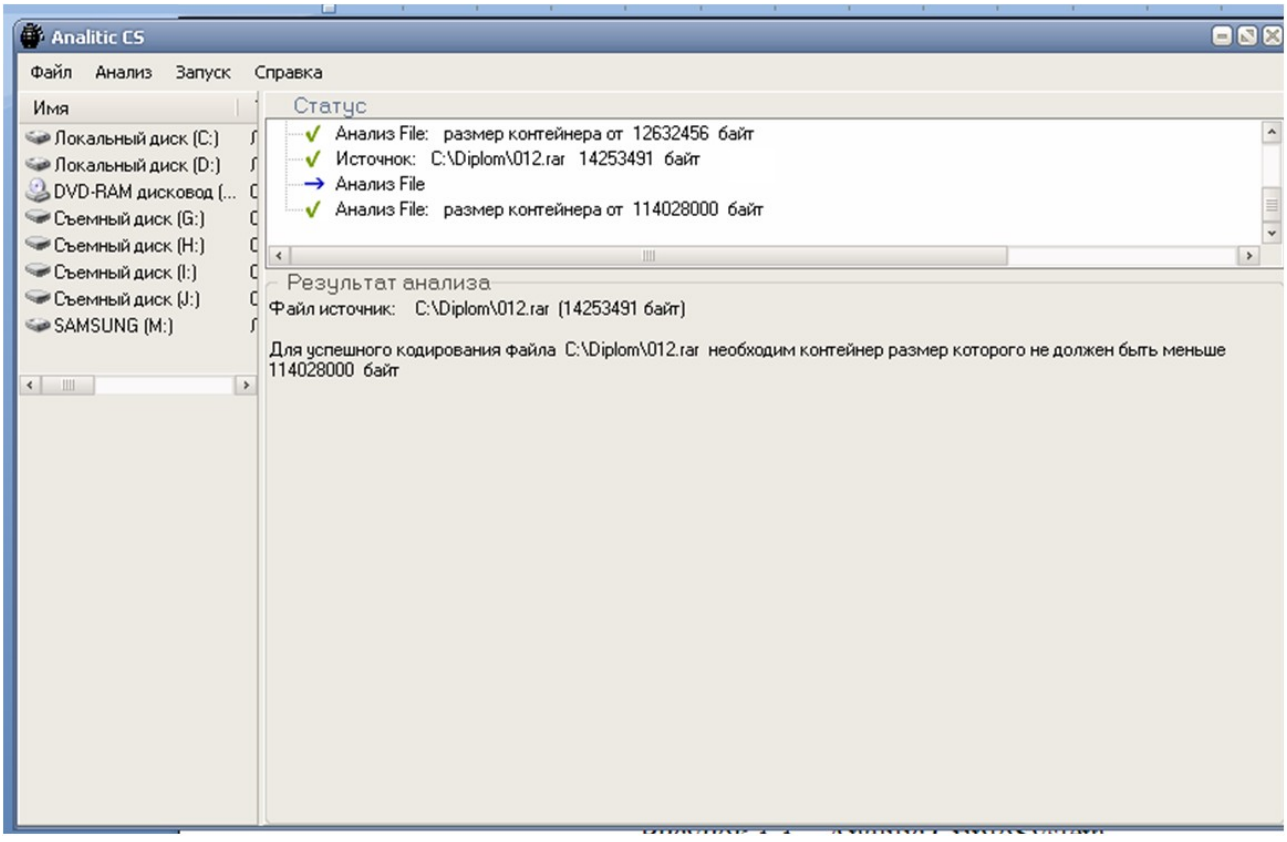


Рисунок 3.3 – Analitic CriptoSystem

3.1 Меню «Файл»

Меню «Файл» состоит из:

- Добавить File
- Добавить WAV
- Выход

При выборе «Добавить File» открывается диалоговое окно, в котором необходимо выбрать любой файл который предназначен для скрытия.

При выборе «Добавить WAV» открывается диалоговое окно, в котором необходимо выбрать файл-контейнер (WAV-файл).

При выборе «Выход» осуществляется закрытие программы.

3.2 Меню «Анализ»

Меню «Анализ» состоит из:

- Анализ File
- Анализ WAV
- Анализ File and WAV

При выборе «Анализ File» осуществляется анализ открытого файла который предназначен для скрытия. Если не выполнена операция «Добавить File», то операция «Анализ File» является не доступной.

При выборе «Анализ WAV» осуществляется анализ открытого WAV-файла который предназначен для скрытия информации. Если не выполнена операция «Добавить WAV», то операция «Анализ WAV» является не доступной.

При выборе «Анализ File and WAV» осуществляется анализ двух файлов: файла-контейнера и файла-источника. Так же если не выполнены операции «Добавить File» и «Добавить WAV», то операция «Анализ File and WAV» не доступна.

3.3 Меню «Запуск»

При выборе «Запуск CryptoSystem» открывается программа «CryptoSystem» (рис 3.4).

CryptoSystem-Это стеганографическая программа предназначенная для скрытия информации в аудио-сигнале. После запуска программы появляется окно. Рассмотрим программу.

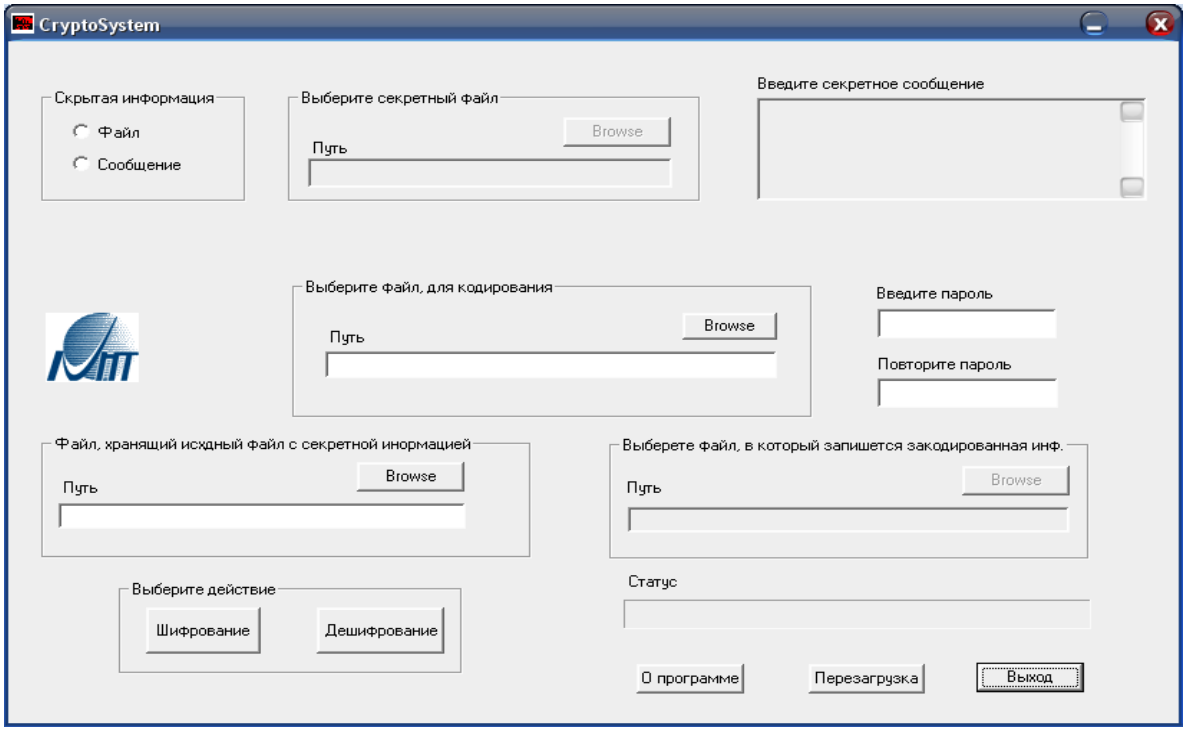


Рисунок 3.4 – CryptoSystem

В окне «Скрытая информация» нужно установить такой тип информации который нужно скрыть. После выбора пункта «Файл», нужно выбрать путь к секретному файлу в окне «Выберете секретный файл», рисунок 3.5.

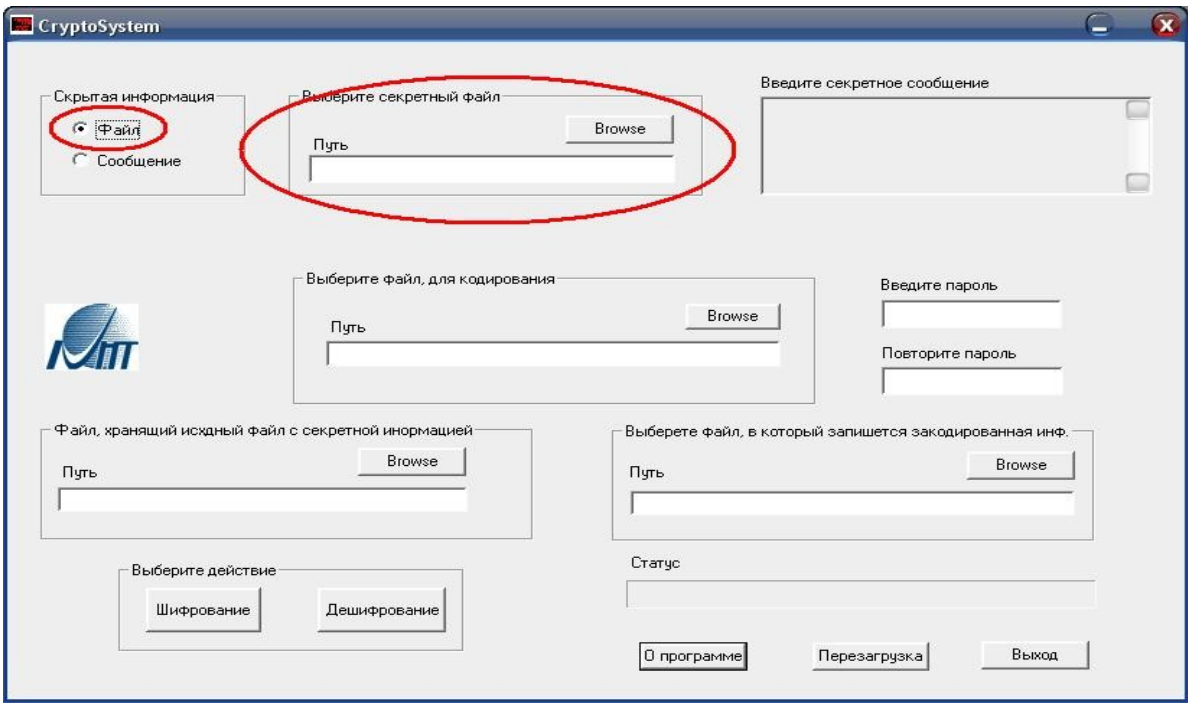


Рисунок 3.5 – Выбор секретного файла

При выборе пункта «Сообщение», можно ввести текстовое сообщение вручную в поле «Введите секретно сообщение» (рис. 3.6), так же при дешифровании в это окне будет выводиться извлеченное сообщение из контейнера.

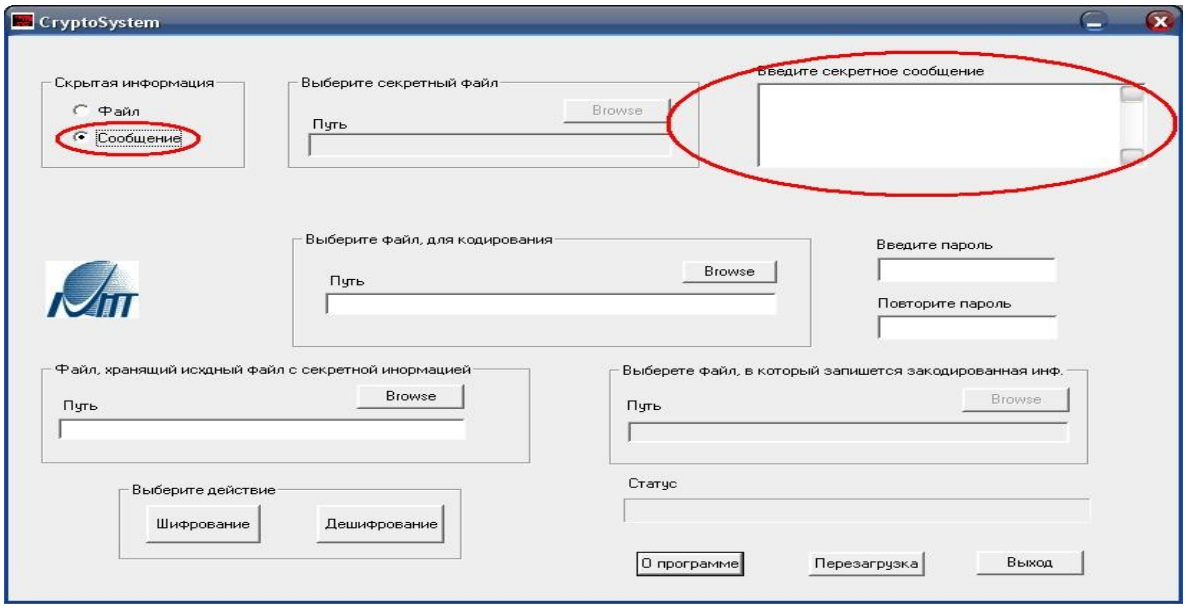


Рисунок 3.6 – Ввод секретного сообщения

В окне «Выберете файл, для кодирования» выбирается WAV файл кодирование или декодирование в него информации.

После выбора файла нужно ввести пароль и повторить его, рисунок 3.7.

В окне «Файл, хранящий исходный файл с секретной информацией» прописываем, путь, имя и расширение WAV файла, для сохранения после нажатия кнопки «Шифрование».

В окне «Выберете файл, в который запишется закодированная инф.», прописывается путь, и имя файла, для извлекаемой информации если это файл, после нажатии кнопки «Дешифрование».

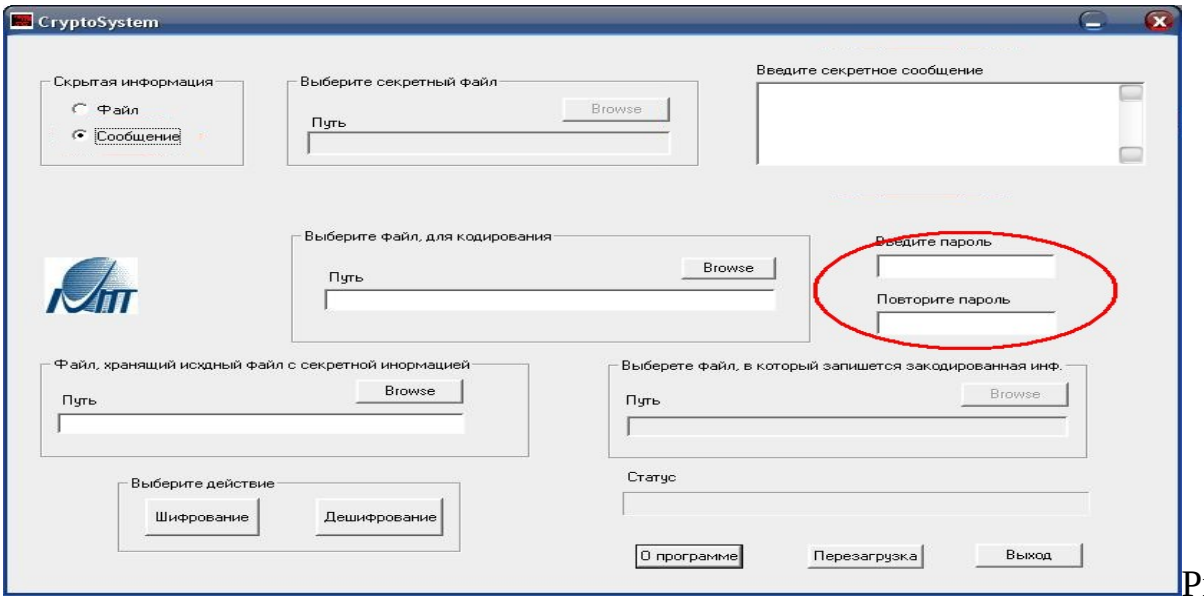


Рисунок 3.7 – Ввод пароля

3.4 Меню «Справка»

При выборе «Подсказка», открывает или закрывает подсказку для пользователя.

При выборе «О программе» открывается окно в котором отображается информация о программе Analitic CriptoSystem.

3.5 Вывод по главе

В ПП реализованный два метода: криптографии (DES) и стеганографии (LSB). Для удобства пользователя предоставляется возможность провести анализ совместимости файла-источника с файла-контейнера.

На основе анализа выбрать наиболее подходящий размер файла-сообщения для определенного Wav-файла и/или наоборот, что в свою очередь позволяет пользователю эффективно распределять электронные документы в зашифрованном виде.

Для быстро освоения программно продукта предусмотрена подсказка для пользователя.

ЗАКЛЮЧЕНИЕ

В дипломной работе были рассмотрены требования, которые предъявляются к стегосистемам, применяемым для встраивания информации в аудиосигналы и сделан вывод, что практически все аудиосигналы имеют характерную особенность. Любой из них представляет собой достаточно большой объем данных, для того, чтобы использовать статистические методы внедрения информации. Рассмотрены методы кодирования с расширением спектра, методы внедрения информации в аудио сигналы, методы маскирования ЦВЗ.

Разработан алгоритм внедрения информации в звуковой сигнал. Исследована работоспособность алгоритма в зависимости от вида и объема информации.

На основе разработанного алгоритма, была реализована программа, с помощью которой были проведены исследования. С помощью полученных результатов можно сделать вывод, что формат файла не влияет на продолжительность скрытия информации в звуковом сигнале, и извлечения происходит быстрее, чем скрытие информации точно такого объема и зависимость скрытие и извлечение информации является линейно зависимой.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1 М. А.Борисов, И. В Заводцев., И. В.Чижов Основы программно-аппаратной защиты информации. М.: Книжный дом «ЛИБРОКОМ», 2012. — 376 с

2 В. Ф.Шаньгин Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с.

3 В. Г. Грибунин, И. Н. Оков, И. В. Туринцев Цифровая стеганография. Издательство: Солон-Пресс, 2012 г – 272 с.

4 В.П.Мельников В.П. Информационная безопасность и защита информации: Учебное пособие для вузов. Издательство М.: Академия 2006 - 336 с.

5 Arnold M., Kanka S. MP3 robust audio watermarking // International Watermarking Workshop. 1999.

6 В.Жельников Криптография от папируса до компьютера. М., 1996 – 375с.

7. А.А.Торокин Инженерно-техническая защита информации: Учебное пособие.М.: Гелиос АРВ, 2005, 960 с

8 А.А.Грушо, Е.Е.Тимонина Теоретические основы защиты информации, М.: Агентство "Яхтсмен", 1996, 186 с.

9 Е.В.Васильева Оценка эффективности информационных систем: Учебное пособие ГОУ ВПО / Е.В. Васильева. – М., 2010.