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 АЛГОРИТМОВ КОЛИЧЕСТВЕННОЙ ОЦЕНКИ СКРЫТНОСТИ ПЕРЕДАВАЕМОЙ ИНФОРМАЦИИ

Выпускная квалификационная работа
обучающегося по направлению подготовки 11.03.02 Инфокоммуникационные технологии и системы связи
очной формы обучения, группы 07001307
Акаффу Аду Гарсия Думез

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

Рецензент
начальник отдела развития сети
филиала ПАО «МТС»
Белгородской области
Кошталев С.С.

БЕЛГОРОД 2017

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
(НИУ «БелГУ»)
ИНСТИТУТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ И ЕСТЕСТВЕННЫХ НАУК
КАФЕДРА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ
Направление подготовки *11.03.02 Инфокоммуникационные технологии и системы связи*
Профиль: *«Сети связи и системы коммутации»*

Утверждаю
Зав. кафедрой
«____» _____ 201_ г.

ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ

Акаффу Аду Гарсия Думез
(фамилия, имя, отчество)

1. Тема ВКР «Разработка алгоритмов количественной оценки скрытности передаваемой информации»

Утверждена приказом по университету от «____» _____ 201_ г. № _____

2. Срок сдачи студентом законченной работы 01.06.2017 г.
3. Исходные данные:
объект исследования – методы стеганографичекоого кодирования дополнительной информации;
предмет исследования – подходы к оценке скрытности информации в речевом сигнале;
цель работы: разработка алгоритмов оценки скрытности информации, закодированной методами стеганографии в речевой сигнал.
4. Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов):
4.1. Принципы стеганографического кодирования информации в аудио-сигнал.
4.2. Речевые данные как среда внедрения информации.
4.3. Методы и алгоритмы оценки скрытности информации, закодированной в речевом сигнале.
4.4. Экономическое обоснование результатов исследования.
5. Перечень графического материала (с точным указанием обязательных иллюстраций):
5.1. Результаты исследования частотно-временных свойств звуков речи (А1, лист 1).
5.2. Блок-схемы алгоритмы кодирования/декодирования информации (А1, лист 1).
5.3. Подходы к оценке скрытности стеганографически закодированной информации в речевой сигнал (А1, лист 1).
5.4. Результаты исследования скрытности стеганографически закодированной информации (А1, лист 1);
5.5. Технико-экономическое обоснование разработки (А1, лист 1);

6. Консультанты по работе с указанием относящихся к ним разделов

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

7. Дата выдачи задания _____

Руководитель

канд. техн. наук
доцент каф. ИТСиТ
кафедры Информационно-телекоммуникационных
систем и технологий»
НИУ «БелГУ» _____ *П.Г. Лихолоб*
(подпись)

Задание принял к исполнению _____
(подпись)

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ

					11070006.11.03.02.439.ПЗВК	Лист
Изм.	Лист	№ докум.	Подпись	Дата		2

ВВЕДЕНИЕ

Стеганография уже давно рассматривается как инструмент, используемый для нелегальных и уничтожающих целей, таких как преступность и война. В настоящее время цифровые инструменты также доступны обычным компьютерным пользователям. Система Стенографии допускает как незаконным так и законным пользователям скрывать сообщения, так что они не будут обнаружены при транспортировки.[1] Рассматриваем стеганографию как законным, при этим она использует для защиты информации между фирмами, внедрение база данных, аудио аутентификация, а так же для авторского права.

Эта бакалаврская работа над темой « Разработка алгоритмов количественной оценки скрытности передаваемой информации » разделяет на четыре части; на первой части описывает как с математическими формулами, на второй рассматриваем речевые данные как среда внедрения информации. Возникает вопрос, какие методы и алгоритмы использовать что б оценивать речевые данных с скрытности, в трети части будет сравнение между методами наименьшего значащих битов НЗБ (Least Signifiant Bit, LSB), является наиболее распространенным в электронной стеганографии; и расширенного спектра (Spread Spectrum SSP).

На последней части, расчет экономическую оценку результаты все исследования.

Для решения целей и задач работы использованы методы анализа и сбора информации, вычислительный эксперимент, сравнение.

Новизна данной работы в том, что воздействие шума (созданного с помощью ЭВМ) на речевой сигнал служит основой для дальнейшего исследования, сфера применения которого принятие решения о применении программных или аппаратных средств борьбы с воздействием или использования воздействия.

1. МАТЕМАТИЧЕСКИЕ ПОДХОДЫ ОЦЕНКИ ИЗМЕНЕНИЙ В АУДИО-СИГНАЛЕ

1.1. Метод наименее значащего бита

Метод наименее значащих битов (Least Significant Bit, LSB) является наиболее распространенным в электронной стеганографии. Основывается на ограниченных способностях органов чувств, вследствие чего людям очень тяжело различать. Дальше будет рассматривать метод НЗБ.

Метод замены наименьших значащих бит (НЗБ) бита (Least Significant Bit, LSB) является простейшим способом внедрить конфиденциальные данные в иные структуры данных. Используя звуковой сигнал, путем замены наименьших значащих бит каждой точки осуществления выборки, представленной двоичной последовательностью, можно зашифровать значительный объем информации. Сам процесс встраивания информации аналогичен тому, который используется для изображения-контейнера, то есть в каждом значении амплитуды наименьший значащий бит заменяется на бит сообщения. Недостаток метода – слабая устойчивость к посторонним воздействиям на сигнал (сжатие, воздействие шумов).[2]

На рисунке показывает как сформируется стего-контейнер, исходное сообщение преобразует в цифровую форму с аналого-цифрового преобразователя (АЦП). Младший бит(ы) образцов исходного сообщения модифицируются для встраивания секретного сообщения. Модифицированное сообщение или стего-контейнер передается через (АЦП).

На рисунке показывает декодирование процесса метода НЗБ, декодер

передает аналоговый стего сообщение через АЦП, чтобы получить образцы сообщения стего. На основе кодирования, декодирование выполняется, где биты с разными образцы извлекаются для получения полного секретного сообщения.

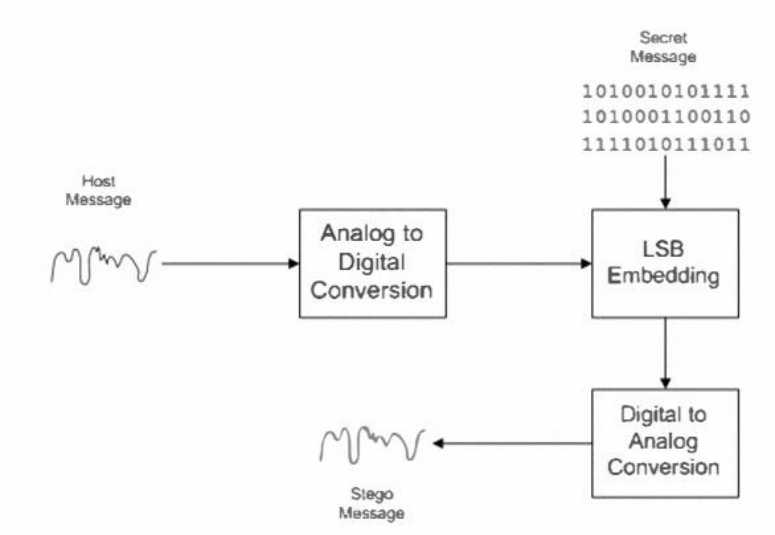

Рисунок 1.1 – НЗБ кодирование процедура

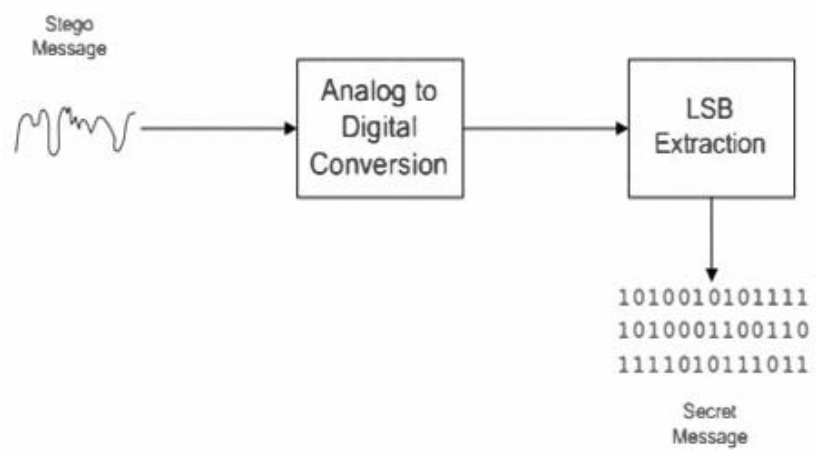

Рисунок 1.2 – НЗБ декодирование процедура

Сигналы, хранящиеся в виде несжатых данных (файлы формата wav), имеют избыточность, что позволяет скрытно закодировать в них информацию. Для этого скрытия данные в виде отчетов представляют в двоичной системе счисления:

$$F_{0b}(x_n) = c_b^n \cdot 2^{b-1} + c_{b-1}^n \cdot 2^{b-2} + \ldots + c_2^n \cdot 2^1 + c_1^n \cdot 2^0, \quad n = 1, \ldots, N \qquad (1)$$

где x_n - значение отчета отрезка данных, $\vec{x} = (x_1, \ldots, x_n, \ldots, x_N)^T$; n - номер отсчета сигнала; $F_{0b}(\ )$ - функция преобразования целочисленного значения отчета в двоичную запись чисел; c_b^n - двоичный символ n отчета отрезка данных, расположенный в b разряде $c_b^n \in \{0, 1\}$; c_b^n - двоичный символ соответствующий старшему биту n отчета сигнала; c_1^n двоичный символ соответствующий младшему биту n отчета сигнала; b - старший разряд кодовой последовательности; $\vec{c}_n = (c_b^n, c_{b-1}^n, \ldots, c_1^n)^T$ - значение отчета отрезка данных в двоичной системе счисления (контейнер).

Скрытое кодирование информации в данных осуществляется путем, замещения значения бита отчета контейнера, битом скрываемой информации. Самым простым примером реализации метода замены наименее значащего бита (метод НЗБ) является занесение битов информации в младший разряд отсчета:

$$c_1^n = m_k, \quad n = 1, \ldots, N, \quad k = 1, \ldots, K \le N \qquad (2)$$

где m_k - двоичный символ, соответствующий биту скрываемой информации $m_k \in \vec{W}$; k - номер символа; N - количество значений отчетов отрезка данных.

Модифицированные отсчеты аудиосигнала со скрытой информацией, хранятся и передаются в виде данных, объединенных в файлы (стего-контейнеры). Для формирования файла стего-контейнера данные из двоичной системы счисления, содержащие скрываемую информацию, преобразовывают в целочисленные значения:

$$F_{0b}^{-1}(y_n) = c_b^n \cdot 2^{b-1} + c_{b-1}^n \cdot 2^{b-2} + \ldots + c_2^n \cdot 2^1 + e_k \cdot 2^0, \quad n = 1, \ldots, N \qquad (3)$$

где y_n - целочисленное значение отчета отрезка данных с закодированной информацией, $\vec{y} = (y_1, \ldots, y_n, \ldots, y_N)^T$; $F_{0b}^{-1}(\ )$ - функция преобразования двоичной записи отчета в целочисленные значения.

Извлечение информации из стего-контейнера осуществляется также с использованием алгоритмов преобразования целочисленных значений отсчетов стего-контейнера в двоичную систему счисления. Скрытая информация содержится в одном из битов отсчета (младшем бите):

$$F_{0b}(y_n) = s_b^n \cdot 2^{b-1} + s_{b-1}^n \cdot 2^{b-2} + \ldots + s_2^n \cdot 2^1 + s_1^n \cdot 2^0 \quad (4)$$

$$\widetilde{e}_k = s_1^n \ n = 1, \ldots, N \quad (5)$$

где s_b^n - - двоичный символ n отчета отрезка данных y_n, занесенный в b разряд $s_b^n \in \{0, 1\}$; $\vec{c}_n = (c_b^n, c_{b-1}^n, \ldots, c_1^n)^T$ - значение отчета отрезка данных в двоичной системе счисления с занесенной в b разряд информацией (стего-контейнер); $k \le N$ - число скрываемых символов не превышает количества отчетов; $\widetilde{m}_k$ - двоичный символ, соответствующий извлекаемому биту скрытой информации.

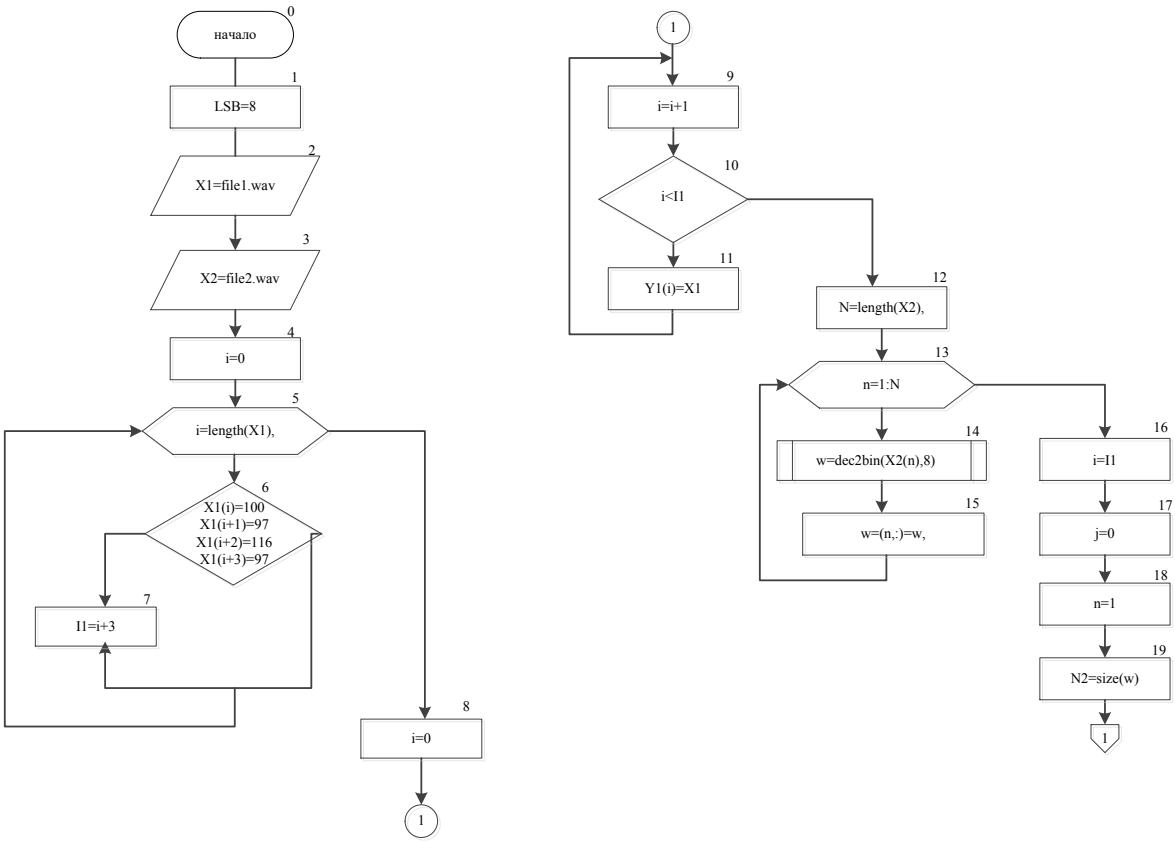

Рисунок 1.3 – Блок-схема кодирования методом LSB (часть 1)

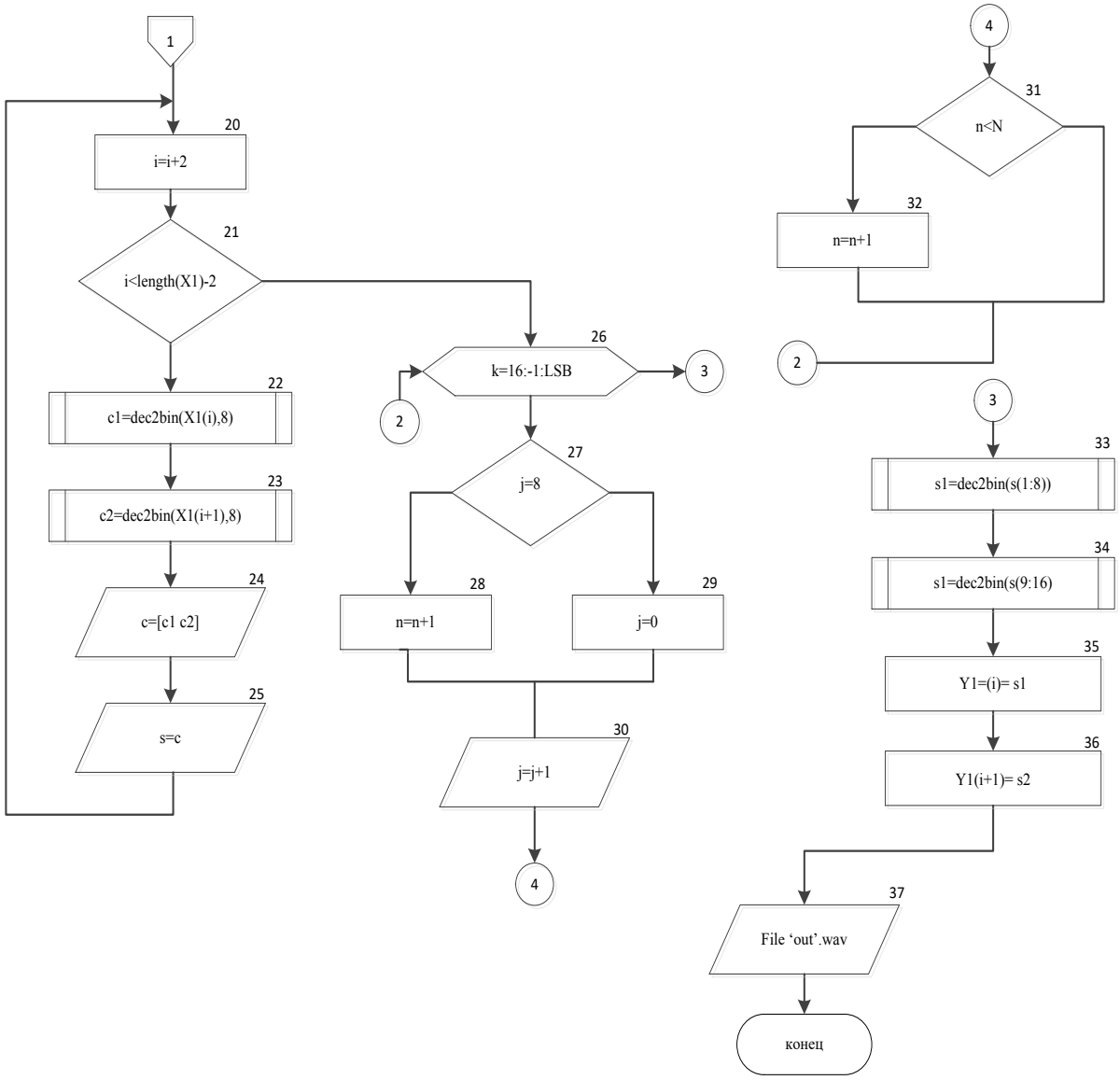

Рисунок 1.4 – Блок-схема кодирования методом LSB (часть 2)

словесный алгоритм (Блок-схема кодирования методом LSB)

0 начало алгоритма

1 инициализация

2 загрузка первый аудио файл

3 загрузка второй аудио файл

4 поиск метки данных к первому сигналу

5 начало создания стегофайла-контенера

6 процесс создания

7 ,-11, инкрементация

12 - 16 процесс перевода внедрения сообщения

17-25 сообщения в двоичные символы

26 -32 создание метода LSB

33 -36 процесс внедрения сообщения

37 стего-контенер или файл после стеганографии

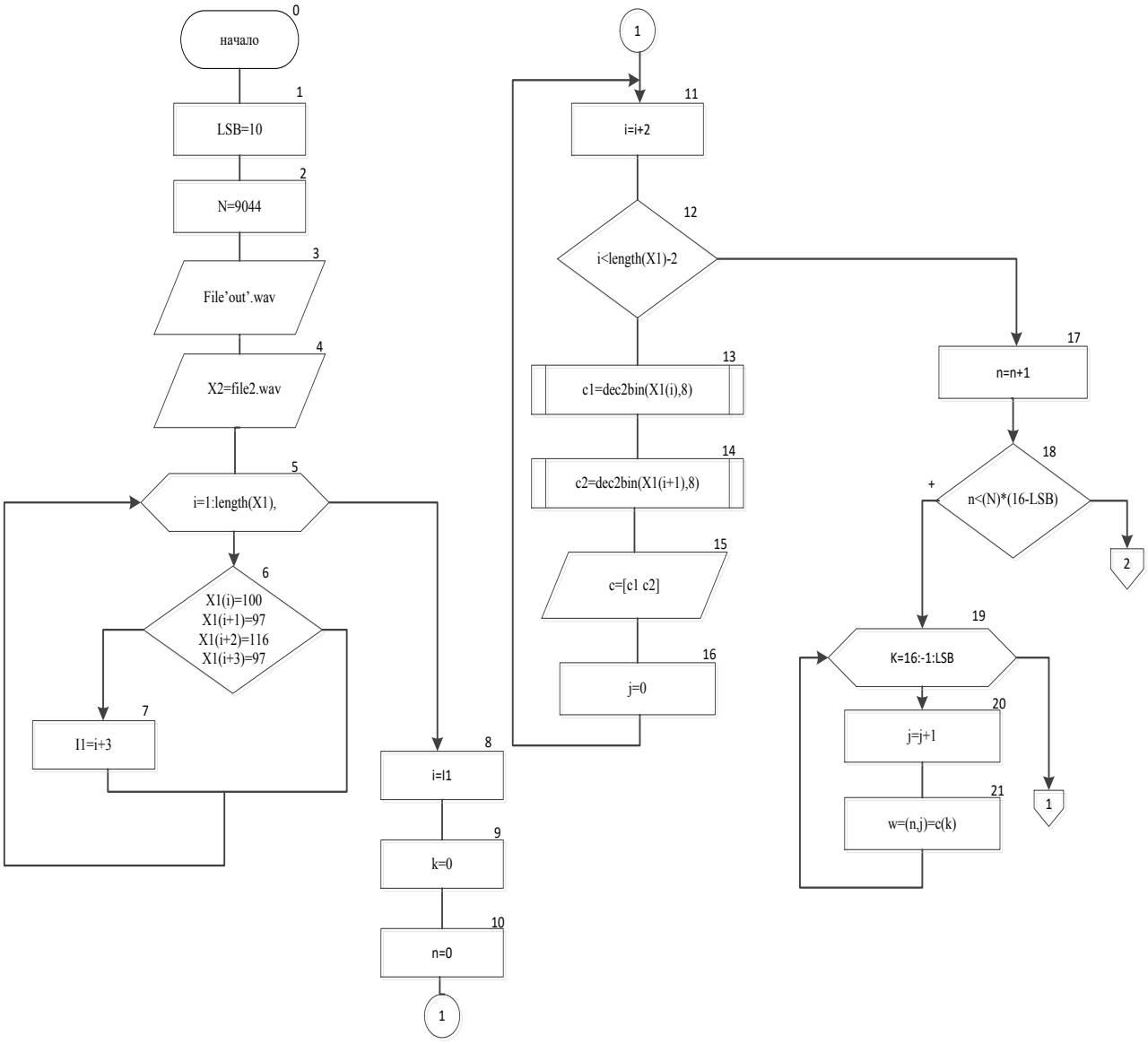

Рисунок 1.5 – Блок-схема декодирования методом LSB (часть 1)

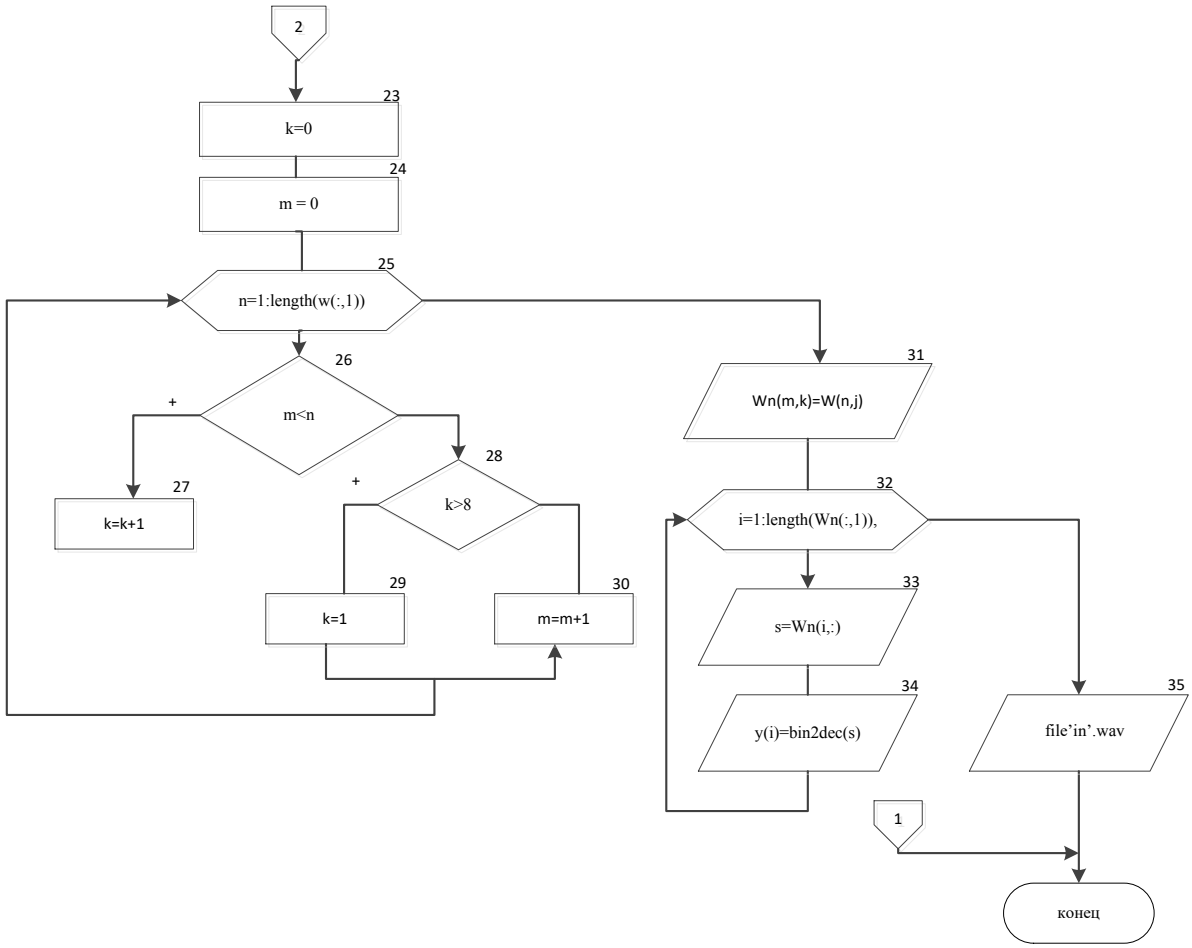

Рисунок 1.6 – Блок-схема декодирования методом LSB (часть 2)

словесный алгоритм (Блок-схема декодирования методом)

0 начало алгоритма

1 -2 инициализация

3 загрузка первый стего-файл

4 загрузка второй аудио файл

5 поиск метки данных к первому сигналу(обротно процедур)

6 начало создания стегофайла-контенера

7 -10 процесс разделения

11, декрементация

12 - 16 процесс перевода внедрения сообщения

25 -30 восстановление сообщения

31 -34 перевод сообщение в десятичные биты

35 аудио файл, восставлен

1.2. Метод расширенного спектра

С быстрой разработкой Интернет-технологии защита авторских прав становится более активным область исследования и цифровую технологию водяного знака рассматривают быть незаметной, устойчивой, безопасной коммуникацией информации, встраивая его в другие цифровые данные - стоящее решение для исследования. Цифровые технологии создания водяных знаков в аудиосигналах может быть разделен на две категории , каждый

метод создания водяных знаков на основе широкополосного создания водяных знаков (SSW- spread spectrum watermarking), где водяной знак распространен по очень многим мусорные ведра частоты так, чтобы энергия в любом мусорном ведре была очень маленькой и конечно необнаружимый

Метод SSW рассматривает исходный сигнал как канал передачи и водяной знак как переданный сигнал . Схема SSW, которая встраивает водяной знак во временной интервал цифрового аудиосигнала немного изменяя амплитуду каждого аудиосэмпла представленный. Тогда несколько механизмов, которые включают эффективный широкополосные системы создания водяных знаков аудио представлены лучшенный расширенный спектр, делающий водяные знаки на методе модуляции, который является расширением традиционного широкополосного создания водяных знаков (TSSW- the traditional spread spectrum watermarking) и может достигнуть лучшая производительность.[3]

Другая технология водяного знака к измените статистическую информацию сигнала узла во временном интервале или преобразуйте домен, такой как модуляция показателя преломления квантования (QIM), модуляция размытия (DC-QIM), и скалярная схема Costa (SCS), которая является субоптимальным методом, используя скалярные функции встраивания и приема.

Для хоста аудиосигнала вектора X с длиной N, чей элементы удовлетворяют Распределение Гаусса нулевым средним значением и дисперсия σ_x^2, полученный вектор после атакует дополнением Гауссовского шума.

Нормально распределенный шум. В методе TSSW, группе псевдо случайные числа u, элементы которых равны $\pm\sigma_u$, встроенные в хост аудиосигнала согласно значению, создание водяных знаков на символе $d = \pm 1$, тогда сигнал, на котором делают водяные знаки, может быть получен.

В первую очередь, определите функцию нормализованной внутренней суммы так:

$$(X,U) = \frac{1}{N}\sum_{i=1}^{N} x_i u_i , \tag{6}$$

и может выражать модуль вектора следующе

$$\|U\| = (U,U) = \frac{1}{N}\sum_{i=1}^{N} u_i^2 , \tag{7}$$

В общем (GSSW-generalized spread spectrum watermarking) внедрения процесса метода расширенного спектра описывает по формуле :

$$S = X + \alpha du - \lambda xu = x + (\alpha d - \lambda x)u , \tag{8}$$

Где

$$x = (X,U)/\|U\| , \tag{9}$$

Представляет собой корреляция между X и u которая является случайным Гауссовским переменим с дисперсией $\sigma_x^2 / N\sigma_u^2$ очевидно что x представлен чтобы компенсировать наложения взаимодействия (interference), λ-параметр который помогает управлять уровень компенсации, α использует для управления силой встраивания водяных знаков .

Когда $\lambda = 0$ и $\alpha = 1$, получает

$$S = X + d \cdot u \tag{10}$$

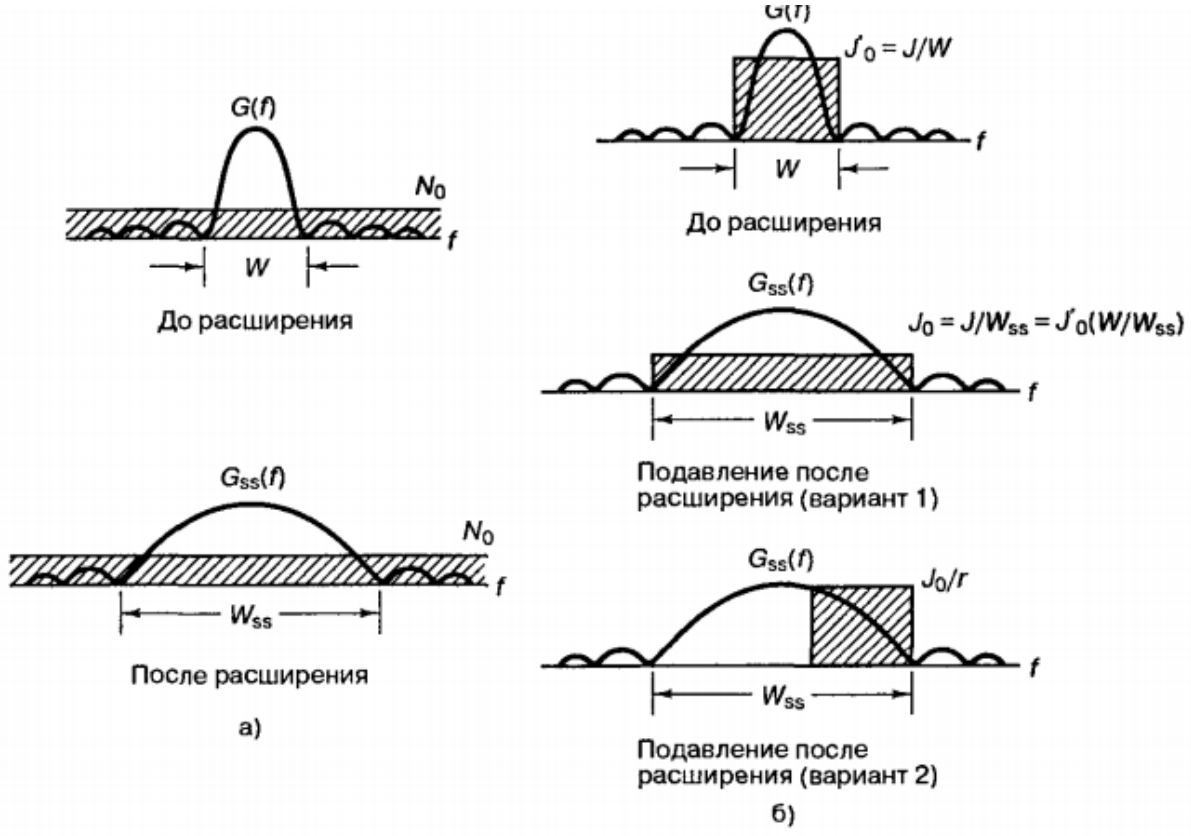

Рисунок 1.7– расширение спектра: а) при наличии белолго шума; б) при постановке намеренных помех

Тут можно понять, что такой метод создавался для разведывательных и военных целей идея состоит в том, чтобы распределить информационный сигнал в широкой полосе радиодиапазона, что позволит усложнить подавление или перехват сигнал. [4]

Одно из требований алгоритма создания водяных знаков - то, что водяной знак должен сопротивляться многократные типы атак удаления. Атаку удаления рассматривают как что-либо, что может ухудшиться или уничтожьте встроенный водяной знак. Другой фактор, который рассмотрят, то, что порог маскирования из фактического аудиосигнала определяет встраивание водяного знака, потому что водяной знак встроенный в “запасные компоненты” нашел использование психоакустической слуховой модели. От этого точка зрения, водяной знак должен быть наименее навязчивым к аудиосигналу, и поэтому, фактические аудиоданные могут быть рассмотрены

как основное препятствие для хорошего алгоритма создания водяных знаков.

Это потому что аудио будет использовать всю необходимую пропускную способность, и водяной знак будет использовать то, что оставляют после слуховой образцовый анализ.

Желаемый метод создания водяных знаков должен быть стойким к ухудшению из-за:

- Используемый канал передачи: аналог или цифровой.

- Высокоуровневый широкополосный шум (в этом случае, “шум” - фактический аудиосигнал). Это часто связываемый как “низкое отношение сигнал-шум”.

- Использование психоакустических алгоритмов на последним этапе водяные знаки на аудио. [5]

2. РЕЧЕВЫЕ ДАННЫЕ КАК СРЕДА ВНЕДРЕНИЯ ИНФОРМАЦИИ

Аудио волны (звук)- акустическая вольна или давление одноразмерность, эти импульсы, когда колеблются с помощью маленькими костями, передает раздражительные импульсы на мозг[6].

Слуховой аппарата человека принимает частоты, располагающие на диапазоне 20 Гц – 20000 Гц, а речь располагается между 600 Гц и 6000 Гц.

Речь составляет из гласных и согласных букв. Гласные произведены, когда переходу воздуха, происходящего из легких, не сталкивает с препятствием, создавая резонансы, от которых фундаментальная частота зависит от размера и от формы голосового аппарата с одной стороны, и от положения языка и челюсти, с другой стороны. Эти звуки длятся приблизительно 30 сек. Производятся согласные, когда голосовая труба частично, с препятствием, эти звуки менее регулярны чем гласные.

Звуковой сигнал любой природы может быть описан определением набором физических характеристик:

частота, интенсивность, длительность, временная структура, спектр и другие.

В нашем случае записал аудиозапись с следующими параметрами:

- Голос: мужской 28 лет
- Дата записи : 10 Декабрь 2016
- Размер 17,25 мб
- Длинна :3 мин 08 сек,
- Частота дискретизации: 48000 Гц,
- Разрядность 16 бит,
- Тип : .wav,
- Одно размерность (моно),

Исследований аудио файл содержит три языка, французский, английский и русский, дольше было рассматривать

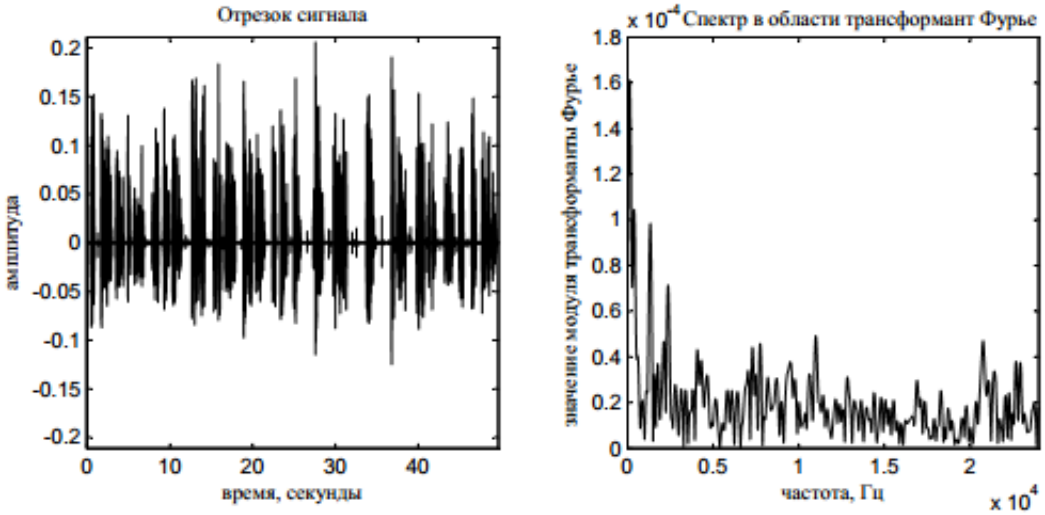

Рисунок 2.1– французская речь 1:а)временная область;б)частотная область

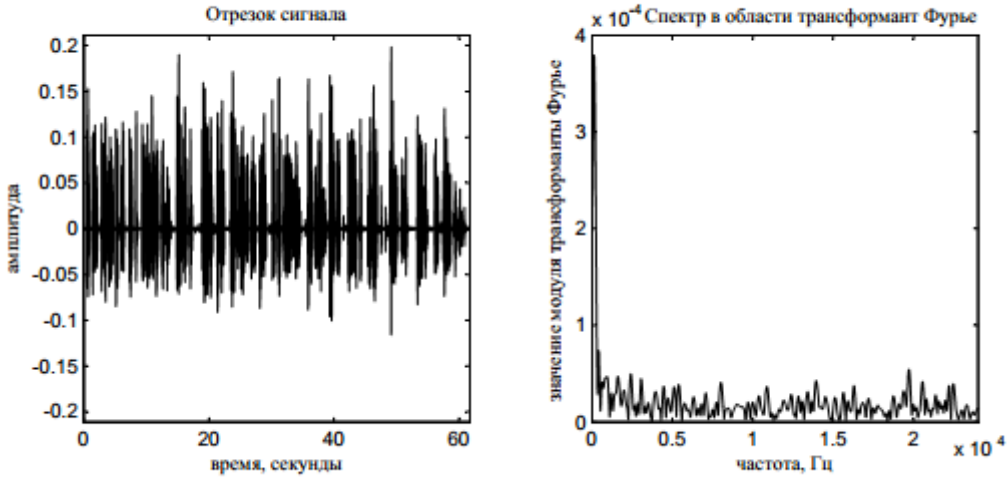

Рисунок 2.2– Английская речь 1:а)временная область;б)частотная область

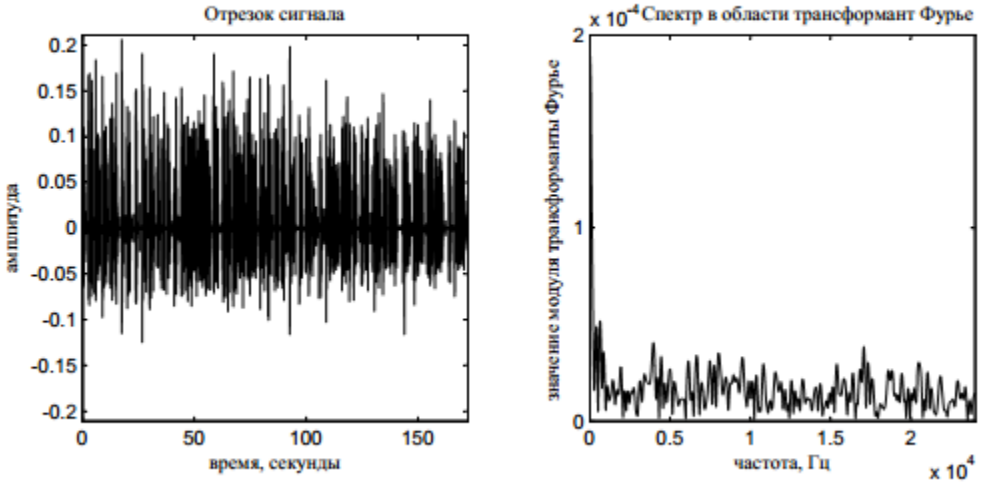

Рисунок 2.3– Русская речь 1:а)временная область;б)частотная область

2.1. Характеристики Французской речевой

На таблице 1, представляет слово, звук, максимальную частоту, длительность и описание букв.

Мы от сюда можем рассчитать частота появления который представляет таблице 2.

Таблица 1

Номер	Слово	Звука	Максимальная частота(Гц)	Длительность	Описание
3	a	a	5000		средине
11	a	a	3000		средине
14	a	a	2500		начало
16	a	a	2000		конец
18	a	a	2000		начало
23	a	a	3200		начало
25	a	a	2000		конец
36	a	a	2000		начало
43	a	a	4000		конец
53	a	a	4000		начало
57	a	a	2000		конец
59	a	a	2000		начало
66	a	a	3300		конец
82	a	a	2000		начало
87	a	a	4000		конец
90	a	a	3134		начало
96	a	a	2000		средине
113	a	a	-		начало
129	a	a	4000		средине
146	a	a	2000		начало
154	a	a	4000		средине
168	a	a	4000		конец
184	a	a	4000		конец
192	a	a	3351	0,15	начало
196	a	a	4000	0.09	начало
200	a	a	5000	0.07	начало
220	a	a	2000	0.05	начало
224	a	a	1500	0,06	средине
253	a	a	4000	0.08	начало
257	a	a	2000	0.07	средине

262	a	a	4000	0.06	начало
268	a	a	3000	0.06	начало
291	a	a	3100	0.04	средине
295	a	a	2000	0.06	начало
302	a	a	4000	0.07	начало
304	a	a	4000	0.12	конец
180	b	b	4000	0.07	начало
301	b	b	4000	0.06	начало
52	c	k		0.035	начало
81	c	k		0.04	начало
151	c	s	8000	0.12	начало
259	c	s		0.1	начало
282	c	k	4000	0.025	начало
286	c	q		0.07	конец
298	c	k		0.02	конец
19	d	d	8000	0.05	средине
40	d	d	6000	0.05	начало
46	d	d	4000	0.08	средине
49	d	d	4000	0.05	начало
58	d	d	4000	0.045	начало
60	d	d	4000	0.06	начало
71	d	d	4000	0.03	начало
110	d	d	4000	0.04	начало
123	d	d	2000	0.02	начало
137	d	d	4000	0.06	начало
149	d	d	2000	0.025	начало
159	d	d	2000	0.06	начало
176	d	d	4000	0.06	средине
215	d	d	2000	0.08	начало
217	d	d	2000	0.06	начало
235	d	d	2000	0.05	конец
265	d	d	2000	0.04	начало
278	d	d	2000	0.04	средине
41	e	e	4000	0.06	конец
73	e	e	2000	0.06	средине
102	e	e	2000	0.08	средине
117	e	e	2000	0.06	конец
120	e	e	4000	0.04	средине
124	e	è	2000	0.04	начало
134	e	e	2000	0.08	начало
150	e	e	2000	0.05	конец
156	e	è	2000	0.06	средине
198	e	è	2000	0.05	средине

202	e	è	2000	0.06	средине
204	e	e	2000	0.04	конец
241	e	e	2000	0.07	конец
251	e	e	2000	0.08	конец
266	e	e	2000	0.04	конец
275	e	e	2000	0.05	конец
279	e	e	2000	0.07	средине
297	e	è	2000	0.09	конец
8	f	f	4000	0.1	средине
83	f	f	4000	0.1	конец
194	f	f		0.16	начало
212	f	f		0.14	начало
258	f	f	4000	0.14	конец
153	g	g	4000	0.035	средине
254	g	j	6000	0.09	начало
303	g	g	4000	0.06	средине
305	g	j	4000	0.14	конец
20	i	i	3000	0.03	конец
31	i	i	4000	0.05	средине
33	i	i	4000	0.05	конец
45	i	i	4000	0.05	средине
63	i	i	4000	0.02	средине
109	i	i	3000	0.06	конец
115	i	i	4000	0.1	конец
152	i	i	4000	0.06	начало
171	i	i	4000	0.05	начало
206	i	i	2000	0.045	начало
213	i	i	2000	0.06	начало
226	i	i	4000	0.06	конец
228	i	i	2000	0.1	начало
239	i	i	4000	0.08	конец
255	i	i	2000	0.2	начало
270	y	i	2000	0.06	начало
272	i	i	2000	0.06	средине
288	i	i	3000	0.04	начало
294	i	i	2000	0.12	конец
165	j	j	2000	0.08	начало
254	g	j	2000	0.08	начало
305	g	j	4000	0.1	конец
52	c	k	4000	0.03	начало
81	c	k	4000	0.04	начало
298	c	k	8000	0.02	конец
15	l	l	2000	0.03	начало

24	l	l	2000	0.025	начало
28	l	l	2000	0.04	средине
38	l	l	2000	0.03	конец
42	l	l	2000	0.02	начало
78	l	l	1000	0.05	начало
89	l	l	1000	0.03	начало
101	l	l	1000	0.04	средине
116	l	l	1000	0.04	начало
161	l	l	1000	0.06	начало
169	l	l	2000	0.06	конец
178	l	l	2000	0.05	конец
199	l	l	2000	0.06	конец
229	l	l	2000	0.06	конец
240	l	l	2000	0.06	начало
252	l	l	1000	0.04	начало
261	l	l	1000	0.03	начало
263	l	l	2000	0.1	начало
267	l	l	1000	0.025	начало
274	l	l	1000	0.03	начало
276	l	l	2000	0.05	начало
289	l	l	2000	0.04	конец
2	m	m	4000	0.08	начало
10	m	m	2000	0.08	средине
54	m	m	2000	0.08	средине
61	m	m	2000	0.05	средине
72	m	m	2000	0.08	начало
142	m	m	1000	0.05	начало
174	m	m	2000	0.08	начало
187	m	m	1000	0.06	средине
214	m	m	2000	0.06	конец
219	m	m	2000	0.06	начало
223	m	m	2000	0.06	средине
246	m	m	2000	0.15	начало
280	m	m	2000	0.06	средине
51	n	n	1000	0.06	конец
62	n	n	2000	0.06	средине
76	n	n	2000	0.08	начало
135	n	n	2000	0.06	конец
141	n	n	2000	0.1	конец
167	n	n	1000	0.04	средине
21	o	o	2000	0.12	конец
48	o	o	2000	0.12	конец
75	o	o	2000	0.15	конец

106	o	o	1000	0.06	средине
175	o	o	2000	0.08	конец
35	p	p	2000	0.025	начало
93	p	p	2000	0.08	средине
145	p	p	1000	0.015	начало
233	p	p	1000	0.02	средине
290	p	p	1000	0.02	начало
147	q	q		0.025	конец
182	q	q		0.1	конец
197	q	q		0.03	начало
227	q	q		0.08	конец
250	q	q		0.03	начало
273	q	q		0.06	конец
17	r	r	1000	0.03	начало
37	r	r	2000	0.1	средине
56	r	r	2000	0.015	конец
95	r	r	1000	0.05	средине
107	r	r	1000	0.03	средине
119	r	r	2000	0.025	средине
155	r	r	2000	0.05	средине
191	r	r	3000	0.08	средине
231	r	r	2000	0.08	начало
256	r	r	2000	0.05	средине
292	r	r	2000	0.08	средине
12	t	s	2000	0.12	средине
64	s	s	4000	0.08	средине
67	t	s	4000	0.15	конец
99	s	s	5000	0.1	начало
105	s	s	4000	0.12	начало
130	t	s	2000	0.1	конец
151	c	s	4000	0.12	начало
183	s	s		0.1	начало
203	s	s		0.1	конец
205	s	s	5000	0.1	начало
238	s	s		0.15	начало
259	c	s		0.1	начало
299	s	s	6000	0.1	начало
4	t	t	1000	0.1	средине
26	t	t		0.025	начало
85	t	t		0.03	начало
91	t	t	6000	0.02	начало
97	t	t		0.08	конец
108	t	t		0.06	конец

112	t	t		0.02	начало
121	t	t		0.03	конец
128	t	t	6000	0.025	средине
133	t	t		0.03	начало
157	t	t		0.1	конец
170	t	t	6000	0.08	начало
207	t	t	4000	0.005	средине
221	t	t	6000	0.025	средине
225	t	t	6000	0.06	конец
293	t	t	6000	0.08	конец
50	u	u	2000	0.08	начало
98	u	u	2000	0.15	средине
111	u	u	2000	0.04	конец
140	u	u	2000	0.05	начало
195	u	u	2000	0.1	начало
208	u	u	2000	0.06	конец
287	u	u	2000	0.1	конец
30	v	v	2000	0.05	средине
44	v	v	3000	0.08	начало
103	v	v	2000	0.08	средине
209	v	v	1000	0.04	начало
284	v	v	2000	0.05	средине
296	v	v	1000	0.06	средине
114	x	x	6000	0.1	конец
125	x	x	3000	0.06	начало
32	s	z	4000	0.1	конец
139	s	z	3000	0.06	средине
193	s	z	6000	0.1	конец
242	z	z	5000	0.1	начало
271	s	z	2000	0.08	средине

Таблица 2 – Частота появления французского языка

	букво	количество	вороятность(%)
1	a	46	10,72
2	b	3	0,69
3	c	8	1,86
4	d	22	5,13
5	e	50	11,66
6	f	5	1,67
7	g	5	1,67
8	h	4	0,93
9	i	38	8,86

10	j	1	0,23
11	k	0	0
12	l	25	5,83
13	m	14	3,26
14	n	32	7,46
15	o	18	4,20
16	p	10	2,33
17	q	6	1,40
18	r	28	6,53
19	s	24	5,60
20	t	38	8,86
21	u	23	5,36
22	v	6	1,40
23	w	0	0
24	x	2	0,47
25	y	1	0,23
26	z	1	0,23
27	à	3	0,70
28	â	1	0,23
29	é	12	2,80
30	è	3	0,70

2.2. Характеристики русской и английской речевой

a) Русская речь

На рисунке 2.4 представляет вероятность появления букв в русском языке [7]

Буква	Частота появления букв		Буква	Частота появления букв	
	Сколько раз встречается	Частота появления (%)		Сколько раз встречается	Частота появления (%)
A	3	0,9	**N**	3	0,9
B	25	7,4	**O**	38	11,2
C	27	8,0	**P**	31	9,2
D	14	4,1	**Q**	2	0,6
E	5	1,5	**R**	6	1,8
F	2	0,6	**S**	7	2,1
G	1	0,3	**T**	0	0,0
H	0	0,0	**U**	6	1,8
I	11	3,3	**V**	18	5,3
J	18	5,3	**W**	1	0,3
K	26	7,7	**X**	34	10,1
L	25	7,4	**Y**	19	5,6
M	11	3,3	**Z**	5	1,5

Рисунок 2.4– частота появления букв русского языка

b) Английская речь

Таблица 3 – Частота появление букв английского языка

Буква	Частота	Буква	Частота	Буква	Частота	Буква	Частота
_	0,175	Р	0,040	Я	0,018	Х	0,009
О	0,090	В	0,038	Ы	0,016	Ж	0,007
Е,Ё	0,072	Л	0,035	З	0,016	Ю	0,006
А	0,062	К	0,028	Ь,Ъ	0,014	Ш	0,006
И	0,062	М	0,026	Б	0,014	Ц	0,003
Т	0,053	Д	0,025	Г	0,013	Щ	0,003
Н	0,053	П	0,023	Ч	0,013	Э	0,003
С	0,045	У	0,021	Й	0,012	Ф	0,002

Как видно наиболее часто употребляемая буква в английском тексте – “E”, а наименее «популярная» – “Z”. Соответственно в русском тексте это буквы “О” и ”Ф” а на французском языке буквы “E” и “W”

А теперь рассмотрим, как выглядеть некоторые буквы из каждого языка при временной и спектральной области.

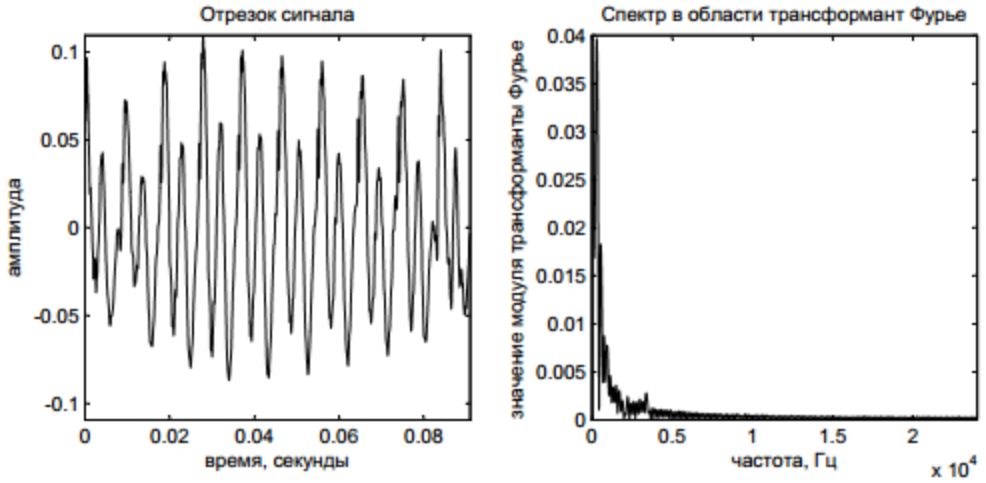

Рисунок . 2.5.1 – Звук «M» выделенный из слова ‘matin’ «: а) временная область; б) спектр (Пр.Г)

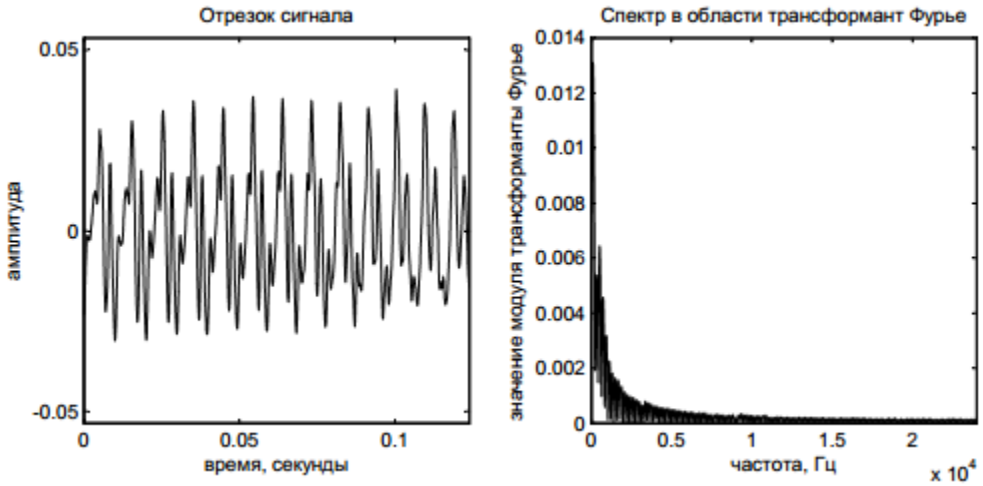

Рисунок . 2.5.2 – Звук «O» выделенный из слова ‘vidéo’ «: а) временная область; б) спектр (Пр.Г)

3. МЕТОДЫ И АЛГОРИТМЫ ОЦЕНКИ СКРЫТНОСТИ СТОЙКОСТИ ИНФОРМАЦИИ В РЕЧЕВЫХ ДАННЫХ

В случае использования в качестве объекта, в который будет внедряться информация (контейнера), речевого сигнала, результат внедрения, т.е. стегоконтенейр (контейнер вместе с внедренной информацией), «на слух» не должен отличаться от исходного контейнера. [8]

Очевидно, что наиболее эффективным способам обнаружения изменения (выявления степени изменения) являются субъективные оценки. Однако рост спроса на стегоалгоритмы и, как следствие, увеличение объемов, обрабатываемых речевых данных приводит к необходимости автоматизации процесса оценки результатов внедрения дополнительной информации.

В настоящее время наиболее широкое использование получили методы оценки различия этом используются такие оценки различия, как среднеквадратическая ошибка (СКО), относительная погрешность (НСКО), отношение сигнал-шум (ОСШ), коэффициент на корреляции (cor), мера расстояния Итакуры-Санто (расстояние наибольшего правдоподобия, ISD). Каждая из этих оценок позволяет выявить различия в сравниваемых сигналах. Однако они имеют разную чувствительность.

Рассматрим некоторые методы оценки.

Среднеквадратическая ошибка (*СКО*)

$$СКО = \sum_{n=1}^{N} \left(x_n - \widetilde{x}_n\right)^2 , \qquad (11)$$

Где x_n - значение амплитуды исходного отрезка да данных; $\widetilde{x}_n$ - значение амплитуды отрезка данных содержащего дополнительную информацию, N -количество отсчетов сравниваемых отрезков сигналов.

Данная мера позволяет выявить различия в огибающих амплитуд отрезков речевых сигналов.

Чем меньше изменений при внедрении дополнительной информации, тем ближе значение этой оценки к нулю.

Относительная погрешность (*НСКО*)

СКО не учитывает энергию самого сигнала, а это значит, что при выборе данной оценки возникают сложности с выбором порогового значения. Поэтому чаше используют нормированную оценку СКО к норм исходного сигнала :

$$НСКО = \sum_{n=1}^{N}(x_n - \widetilde{x}_n)^2 \Big/ \sum_{n=1}^{N} x_n{}^2 \qquad (12)$$

Отношение сигнал-шум (*ОСШ*)

$$ОСШ = 10 \cdot \lg \frac{\sum_{n=1}^{N} x_n{}^2}{\sum_{n=1}^{N}(x_n - \widetilde{x}_n)^2} \qquad (13)$$

Чем выше оценка *ОСШ*, тем меньше изменений было внесено.

Коэффициент на корреляции (*cor*)

$$\mathrm{cor} = \frac{\sum_{n=1}^{N}\left(x_n - \frac{1}{N}\sum_{n=1}^{N} x_n\right)\cdot\left(\widetilde{x}_n - \frac{1}{N}\sum_{n=1}^{N}\widetilde{x}_n\right)}{\sqrt{\sum_{n=1}^{N}\left(x_n - \frac{1}{N}\sum_{n=1}^{N} x_n\right)^2 \cdot \sum_{n=1}^{N}\left(\widetilde{x}_n - \frac{1}{N}\sum_{n=1}^{N}\widetilde{x}_n\right)^2}} \qquad (14)$$

Чем ближе значение корреляции к единице, тем выше схожесть отрезка данных содержащего контрольную информацию и исходного.

Все рассмотренные выше оценки вычисляют меру различия, используя для сравнения значения отсчетов во временной области.

Данная мера позволяет выявить различия в огибающих амплитуд отрезков речевых сигналов.

Чем меньше изменений при внедрении дополнительной информации, тем ближе значение этой оценки к нулю.

Мы на том разделе будем ввести результаты исследования, до этого показать по шагам как проведен эксперимент.

Для каждого метода использованы принцип один и тоже:

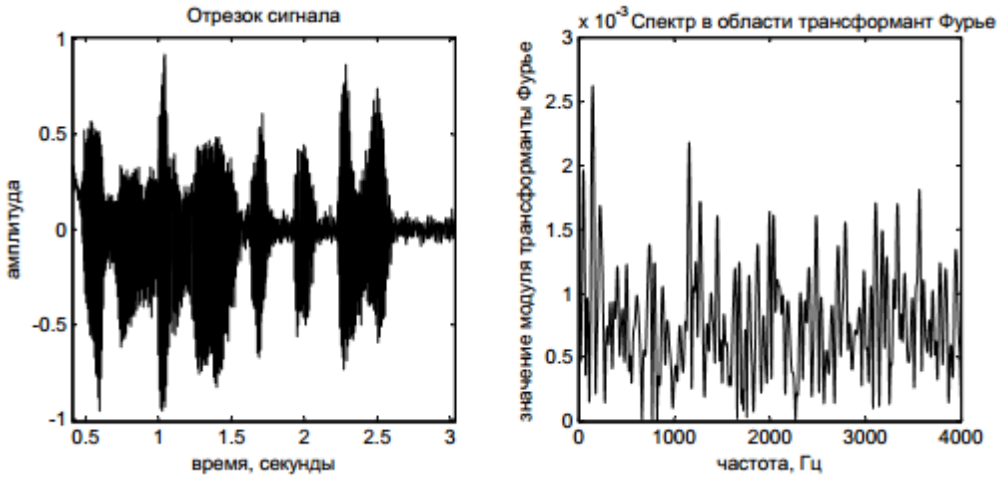

Рисунок 3.1- :исходная звуковой сигнал

План проведения эксперимента:

1. Загрузить звуковой сигнал $\vec{x}$

2. Загрузить внедренное сообщения $\vec{y}$

3. Внедрить сообщение $\vec{y}$ в звуковой сигнал $\vec{x}$ и сохранить результат внедрения в $\vec{g}$

4. Извлечь из синтезированного сигнала $\vec{g}$, речевое сообщение

5. Излечит из $\vec{q}$ закодированное речевое сообщение $\vec{\omega}$

6. Оделим различу между восстановленном речевым сигналом $\vec{v}$ и речевым сигналом $\vec{\omega}$ после воздействия стеганографии (ско, корреляция, SNR)

Эксперимент:

Исходной звуковой сигнал (рис 3.1)

- частота дискретизация: 8 кГц;

- разрядность: 8 бит;

- содержавшие сигнала

- длительность:3 секунд.

Внедренное сообщение

- текстовый

- символы :7

Таблица 4 - Результаты количественной оценки стего-контеров – стегоконтейнеров

Метод	***СКО***	***НСКО***	***ОСШ***	***Cor***
НЗБ (LSB)	164,4	27,08	0,04	0.6154i
РС(SSP)	2,48	0,13	2,92	0,67

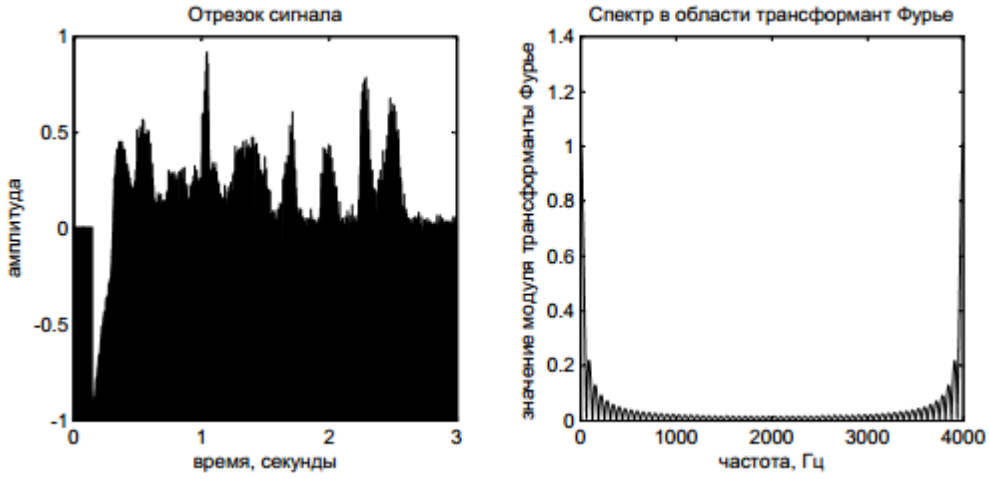

Рисунок 3.2- сигнал после стеганографии при методе наименее значащего бита

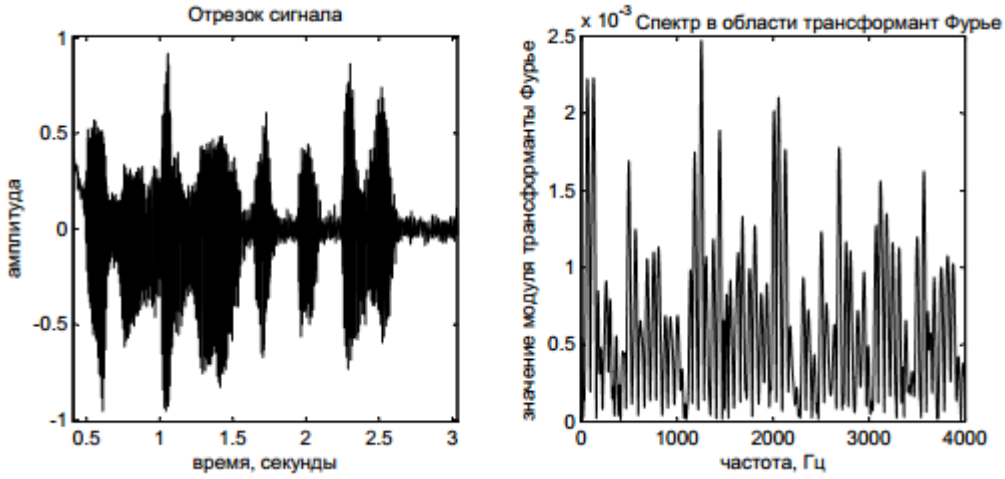

Рисунок 3.3- сигнал после стеганографии при методе расширенного спектра

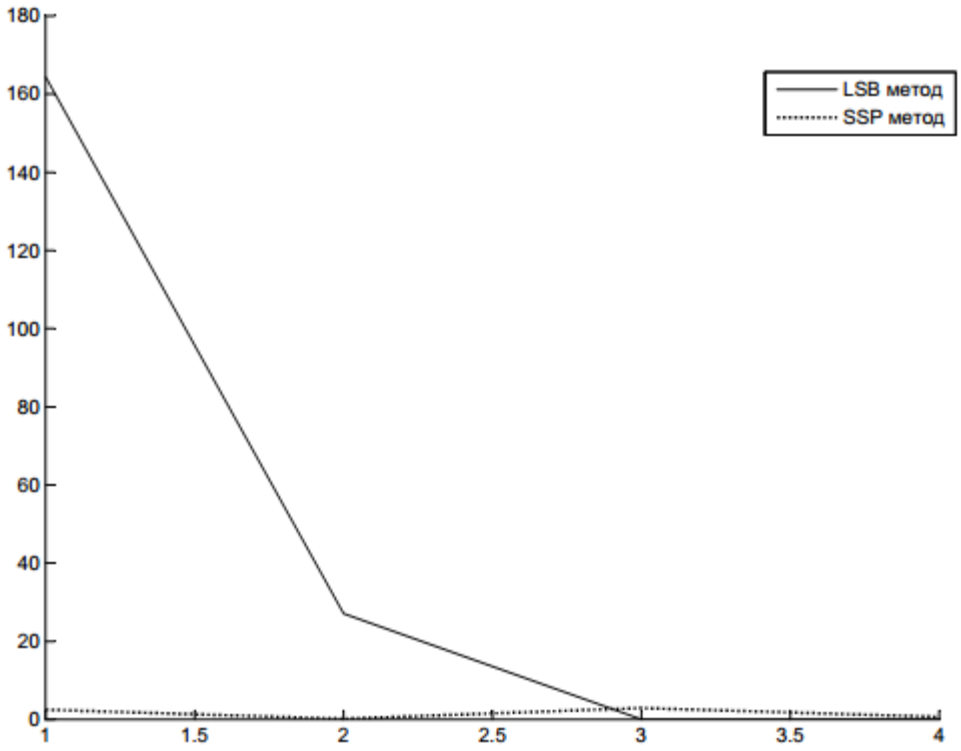

Рисунок 3.4- график показывающий результаты оценки методов

4. ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РЕЗУЛЬТАТОВ ИССЛЕДОВАНИЯ

Основной части о экономическом расчете, является проведение работ.

В этом работе, было использовать программной продукт, который представит инженерном первом категории и оцениваемого экономистом.

4.1. Планирование работ по исследованию

Таблица 5 - Планирование работ по исследованию

Наименование этапов работ	**Исполнитель**	**Трудоемкость, час**	**Продолжительность, дней**
1	**2**	**3**	**4**
1.Подготовительный			
1.1.Сбор информации	Младший научный сотрудник	40	5
1.2.Выработка идеи	Старший научный сотрудник	40 40	5 5
1.3.Определение объема исследовательских работ	Младший научный сотрудник	16	2
1.4.Формирование исследовательской работы	Младший научный сотрудник	8	1
1.5.Обработка и анализ информации	Младший научный сотрудник	64	8
Итого:		208	26
2.Основной (экономический анализ)			
2.1.Обоснование целесообразности работы	Старший научный сотрудник	24	3
2.2.Выполнение работы	Младший научный сотрудник	88	14

Итого:		112	17
3.Заключительный			
3.1.Технико-экономическое обоснование	Экономист	40	5
3.2.Оформление и утверждение документации	Младший научный сотрудник	40	5
Итого:		80	10

4.2. Расчет расходов на оплату труда на исследование

Расчет расходов на оплату труда разработки исследования представлен в таблице 6

Таблица 6 - Расчет расходов на оплату труда

Должность Исполнителей	**Трудоемкость, час**	**Оклад, руб**
1	**2**	**3**
Младший научный сотрудник	312	12000
Старший научный сотрудник	120	15000
Экономист	40	11000
Итого:	472	

Часовая тарифная ставка ($Ч_{ТС}$) рассчитывается по формуле:

$$Ч_{ТС} = \frac{Р}{F_{мес}} \quad (15)$$

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

Расход на оплату труда ($Р_{ОТ}$) находится следующим образом:

$$P_{OT} = Ч_{TC} * T_{сум} \quad (16)$$

где $Т_{СУМ}$ – суммарная трудоемкость каждого из исполнителей

Таблица 7 - Расчет расходов на оплату труда

Должность Исполнителей	**Трудоемкость, час**	**Оклад, руб**	**$Ч_{ТС}$, руб/час**	**$Р_{от}$, руб**
1	**2**	**3**	**4**	**5**
Младший научный сотрудник	312	12000	68,18	21272,16
Старший научный сотрудник	120	15000	85,23	10227,6
Экономист	40	11000	62,50	2500,00
Итого:	472			33999,76

4.3. Расчет продолжительности исследования

Согласно расчетам, трудоемкость исследования составила 472 часа.

Продолжительность исследования составит:

$$T_{иссл} = T_{сум} / T_{РД} \quad (17)$$

где $Т_{СУМ}$ = 472 часа суммарная трудоемкость исследования

$Т_{РД}$ = 8 часов – продолжительность рабочего дня

$$Т_{ИССЛ} = 472/8 = 59 \text{ дней.}$$

Продолжительность исследования составляет 59 дней, расчет производится без учета выходных и праздничных дне.

4.4. Расчет стоимости расходных материалов

В разделе стоимости расходных материалов учитываются расходы на приобретение основных материалов необходимых для проведения исследования, оформления соответствующей документации, а также учитывается стоимость картриджа. Расчет стоимости расходных материалов приведен в таблице

Таблица 8. Стоимость расходных материалов.

Наименование расходных материалов	**Цена за единицу, руб.**	**Количество, шт.**	**Сумма, руб.**
1	**2**	**3**	**4**
Бумага	120	2	240
Канцтовары	160	-	160
Расходные материалы для принтера (картридж)	3500	-	3500
приложение MatLab стандарт для обработки сигналов	69.165,52	1	69.165,52
Итого:			73.065,52

Определили, что для проведения исследования затраты на приобретение расходных материалов потребуется 73.065,52 рублей

Цена приложения был указана на официальном сайте MatLab [9] и для перевода на русский валют использован XE.com [10]

4.5. Расчет сметы расходов на исследование.

С учетом часового тарифной ставки рассчитаем общие расходы на разработку и проведение исследования. В данную статью расходов включаются премиальные выплаты, районный коэффициент и страховые взносы. Для оценки затрат на исследование составляем смету на разработку и проведение исследования.

Произведем расчет расходов:

Премиальные выплаты рассчитываются по формуле:

$$ПВ = Р_{ОТ} К_{ПВ} \quad (18)$$

где $К_{ПВ}$ - коэффициент премиальных выплат, составляет 20 %, в случае если премии не предусмотрены $К_{ПВ}$=1.

$$ПВ = 33999,76 \cdot 0,2 = 6799,95 \text{ руб.}$$

Дополнительные затраты на проведение исследования можно определить, как:

$$З_{ДОП} = Р_{ОТ} К \quad (19)$$

где К - коэффициент дополнительных затрат (К=14%).

$$З_{ДОП} = Р_{ОТ} \cdot 14\ \%.$$

$$З_{ДОП} = 33999,76 \cdot 0,14 = 4759,97$$

В заработной плате может быть предусмотрен районный коэффициент, которых характеризует доплату при работе в трудных условиях. Величина коэффициента определяется в зависимости от характера производства.

$$РК = Р_{ОТ} К_{РВ} \quad (20)$$

где $К_{РВ}$ – коэффициент районных выплат, для примера составляет 15 % от суммы.

РК =(33999,76) ·0,15 =5099,97 руб.

Общие расходы на оплату труда вычисляются по формуле:

$$P_{общ} = P_{ОТ} + ПВ + РК + З_{ДОП} \quad (21)$$

где РОТ - основная заработная плата; ПВ - премиальные выплаты; ЗДОП - дополнительные затраты; РК - районный коэффициент.

Σ РОТ =33999,76+4759,97+13599,92+5099,97

Σ РОТ =57459,65 руб.

Из таблицы 10 берется итоговая сумма стоимости расходных материалов по статье расходных материалов

$\Sigma Р_{РМ}$ =69.165,52 руб.

Страховые взносы рассчитываются по формуле:

$$СВ = P_{ОТ}\,0{,}3 \quad (22)$$

Амортизационные исчисления на использование компьютера вычисляются аналогично выражению (23). В данном примере они составляют 25% от стоимости компьютера.

$$АО = Т / F \quad (23)$$

где Т – стоимость оборудования,

F – срок службы этого оборудования.

$$АО = С_{ПК}\,0{,}25 \quad (24)$$

АО = 30000 ·0,25=7500 руб.

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

$$Р_{ИНТ}=1000 \text{ руб.}$$

Административно-хозяйственые расходы составляют 50% от основной заработной платы ($Р_{ОТ}$).

$$P_{AX} = P_{OT}\,0{,}5 \qquad (25)$$

$$Р_{АХ}=33999{,}76 \cdot 0{,}5=16999{,}9 \text{ руб.}$$

Результаты расчета расходов сведем в таблицу. Смета расходов на разработку и проведение исследования представлена в таблице 9

Таблица 9 - Смета расходов на разработку и проведение исследования

Наименование статей расходов	**Сумма, руб.**	**Удельный вес статей, %**
1	**2**	**3**
1.Стоимость расходных материалов	73.065,52	3,92
2. Расходы на оплату труда 2.1. Основная заработная плата	57459,65 33999,76	 33,36
2.2. Дополнительные затраты	4759,97	4,67
2.3. Премиальные выплаты	13599,92	13,35
2.4 Районный коэффициент	5099,97	5,0
3. Единый социальный налог	14939,51	14,66
4. Амортизационные исчисления на использование компьютера	7500	7,36
5. Расходы на использование Интернет	1000	0,99
6.Административно-хозяйственные расходы	16999,9	16,68
Итого:	228.424,2	100

Результатом экономической оценки исследования является определение затрат на разработку и реализацию исследования:

- продолжительность исследовательских работ составила 59 дней;
- сметы расходов на исследование – 228.424,2 рублей.

ЗАКЛЮЧЕНИЕ

В настоящее время компьютерная стеганография продолжает развиваться: формируется теоретическая база, ведется разработка новых, более стойких методов встраивания сообщений.

Среди основных причин наблюдающегося всплеска интереса к стеганографии можно выделить принятые в ряде стран ограничения на использование сильной криптографии, а также проблему защиты авторских прав на художественные произведения в цифровых глобальных сетях.

По сравниванию метода наименее значащих битов и метода расширенного спектра, который указан на таблице 4, видно, что метод наименее значащих битов (НЗБ) может содержать шум, так что такое метод в аудио очень чувствительно, из слухового аппарата. Проще его использовать в направление изображение.

Метод расширенного спектра (РС) очень стойкой, по мерам на рисунке 3.4 видно как его график к нолю стремиться .

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А

Функция (e)

```
function e = cod_ascii(m)
N=128;
%==================================
%CODAGE DU MESSAGE A CACHER%

% Initial message is a string
% m = 'AKAFFOU';
% Find the ASCII equivalent
n = double(m);
% Convert to benary
W = dec2bin(n,8);
k=0;
for t=1:length(m)
    for i=1:length(W)           % fonction mathematique e(n)=2Wn-1

        if W(t,i)=='0' %condition de remplacement de bite
            %comparaison
        k=k+1;
            e(k)=-1;
        else
            k=k+1;
            e(k)=1; %
        end;

    end
end

%replace symbole 0 ==> -1
%for i=1:length(n)
   % if

%p=unicode2native('AKAFFOU');%codage caractere==> ASCII
%b=dec2bin(p,8);%codage Decimal==>Binaire
%t=length(p);
%u=length(b);

   %if
```

ПРИЛОЖЕНИЕ Б

Метод наименее значащего бита

```
clc
clear
LSB=8;
%загрузка 1 сигнала
file1='D:\OneDrive - National Research University Belgorod State
University\diplom\methodes\bonjour.wav';
f1_id=fopen(file1);%
x1 = fread(f1_id);
fclose(f1_id);
%загрузка сообщения

N=128; %longueur de coupure
K=1E-5;%  seuil de  fixation
mess='AKAFFOU';%message a integrer
% load phrase_fr.txt
ee = cod_ascii(mess);
% ee=[-1 1 -1 -1 -1 -1 -1 1 -1 1 -1 -1 1 -1 1 1 -1 1 -1 -1 -1 -1 -1 1 -1 1 -
1 -1 -1 1 1 -1 -1 1 -1 -1 -1 1 1 -1 -1 1 -1 -1 1 1 1 1 -1 1 -1 1 -1 1 -1 1
]; %  bite de codage e = 1 or -1(0=-1;1=1)
e=[ee ee ee ee ee];
% ======================================================
% load u.mat % bruit  de issu de  la loi de spstre
% U=u(1:N)';% coupure  du  bruit  de la longueu  de N
M=length(e);%volume de l infortion en bites
%
y1=zeros(length(x1),1);
%поиск метки data
%1 сигнал
for i=1:length(x1)
    if x1(i) == 100 && x1(i+1) == 97 && x1(i+2) == 116 && x1(i+3) == 97
    I1=i+3;
    end
end
i=0;
% начало создания стегофайла-контейнера
while i<I1
    i=i+1;
    y1(i)=x1(i);
end
N=M;
for n=1:N
    w=dec2bin((n),7);
```

```
end
i=I1;
j=0;
n=1;
N2=size(w);
while i<length(x1)-2
    i=i+2;
    c1=dec2bin(x1(i),8);
    c2=dec2bin(x1(i+1),8);
    c=[c1 c2];
    s=c;
    for k=16:-1:LSB
        if j== 8
            n=n+1;
            j=0;
        end
        j=j+1;
        if n<N
        s(k)=w(1,j);
        end
    end
    s1=bin2dec(s(1:8));
%     s2=bin2dec(s(9:16));
    y1(i)=s1;
%     y1(i+1)=s2;
end
fcontan='test6.wav';
fileout_id=fopen(fcontan,'w+');
fwrite(fileout_id,y1);
fclose(fileout_id);
```

ПРИЛОЖЕНИЕ В

Метод расширенного спектра

```
clc
clear
tic
N=128; %longueur de coupure
K=1E-2;%  seuil de  fixation
mess='AKAFFOU';%message a integrer
% load phrase_fr.txt
ee = cod_ascii(mess);
e=[ee ee ee ee ee];
% ====================================================
load u.mat % bruit  de issu de  la loi de spstre
U=u(1:N)';% coupure  du  bruit  de la longueu  de N
M=length(e);%volume de l infortion en bites
X=wavread('bonjour.wav'); % fichier conteneur
L=length(X);
Y=X;%formation  du fichier de stego-contener
% n=1144;
n=1;%debut de decoupage
m=0;
while (L>n+N-1)
    m=m+1;
    if m>M m=1
   end;
%     e(m)les decoupage en bite du message coD
x=X(n:n+N-1);%segmentation (delimitage)
n=n+N;

Eu=sum(U.^2);% energie  issue  de du decoupage du bruit
un=U./sqrt(Eu); % normalisation a 1 du signel  bruit
alpha=un'*x; % projection de coupure  du  bruit  sur le signal
% ======= procedure de codage
%c=x-alpha*un; %( filtration ou conteneur  de steganographie)
%  K=-un'*x+e(m)*abs(un'*x)%*un; % (ces coefficients depandent  du
%  model)seuil d adaptation , == travaillant  sur l energie de voix , pour
%  adapter  le  signal audible (il se choisit parmi les methode
%  psychoaccoustiques .

% physchoaccoustique
 s=x+K*un;

%s=c+e(m)*abs(alpha)*un; % ajout  vers  la  filtration du signal bruit
/stego-contener
Y(n:n+N-1)=s;
end;% for i=1:M
wavwrite(Y,'tictac11.wav');
toc
```

Отношение сигнал-шум (*ОСШ*)

```
clc
clear
N=256;
[X,Fs]=wavread('bonjour.wav');%   first  signal
[Y,Fs]=wavread('test6.wav');% signal  after  stegono
n=3676;
x=X(n:n+N-1);%
y=Y(n:n+N-1);%

s1=0;
s2=0;
for i=1:N

    s1=s1+(x(i)^2);
    s2=s2+(x(i)-y(i))^2;


end
 SNR=(s1/s2);
```

Коэффициент на корреляции (*cor*)

```
clc
clear
N=128;
[X,Fs]=wavread('bonjour.wav');%   first  signal
[Y,Fs]=wavread('test6.wav');% signal  after  stegono
n=3676;
x=X(n:n+N-1);%
y=Y(n:n+N-1);%

s1=0;
s2=0;
s3=0;
s4=0;
for i=1:N

    s3=(s3+(x(i)-(1/N*(s1+x(i)))))*(s3+(y(i)-(1/N*(s2+y(i)))));
    s4=sqrt((s3+(x(i)-(1/N*(s1+x(i))))^2)*(s3+(y(i)-(1/N*(s2+y(i))))^2));

end
Cor=s3/s4;
```

ПРИЛОЖЕНИЕ Е

Среднеквадратическая ошибка (СКО)

```
clc
clear
N=256;
[X,Fs]=wavread('bonjour.wav');%   first  signal
[Y,Fs]=wavread('test6.wav');% signal  after  stegono
n=3676;
x=X(n:n+N-1);%
y=Y(n:n+N-1);%

s1=0;
s2=0;
for i=1:N

    s2=s2+(x(i)-y(i))^2;

end
sko=s2;
```

ПРИЛОЖЕНИЕ

Относительная погрешность (*НСКО*)

```
clc
clear
N=128;
[X,Fs]=wavread('bonjour.wav');%   first  signal
[Y,Fs]=wavread('test6.wav');% signal  after  stegono
n=3676;
x=X(n:n+N-1);%
y=Y(n:n+N-1);%

s1=0;
s2=0;
for i=1:N

    s1=s1+(x(i)^2);
    s2=s2+(x(i)-y(i))^2;


end
NSKO=s2/s1;
```

ПРИЛОЖЕНИЕ

Un matin ; une information à la radio et à la télévision parlait de la vidéo d’une caméra

d’administration près du métro non loin du café “théâtre’’.

La température, s’élevait, sorti du taxi le directeur d’exploitation, tenant dans une main un paquet de cigarette et dans l’autre un journal titré *model et banque*.

Sa première phrase fut : à quelle adresse se situe vôtre firme ?

Dans des mathématiques il lui répondait ainsi : Le zèbre est moins grand que la girafe, c’est la loi de la physique.

Le lendemain, convaincu, il partit avec ses bagages.

```
%SSP
clc
clear
tic
N=128; %longueur de coupure
K=1E-2;%  seuil de  fixation
mess='AKAFFOU';%message a integrer
% load phrase_fr.txt
ee = cod_ascii(mess);
e=[ee ee ee ee ee];
% ======================================================
load u.mat % bruit  de issu de  la loi de spstre
U=u(1:N)';% coupure  du  bruit  de la longueu  de N
M=length(e);%volume de l infortion en bites
X=wavread('bonjour.wav'); % fichier conteneur
L=length(X);
Y=X;%formation  du fichier de stego-contener
% n=1144;
n=1;%debut de decoupage
m=0;
while (L>n+N-1)
    m=m+1;
    if m>M m=1
   end;
%     e(m)les decoupage en bite du message coD
x=X(n:n+N-1);%segmentation (delimitage)
n=n+N;

Eu=sum(U.^2);% energie  issue  de du decoupage du bruit
un=U./sqrt(Eu); % normalisation a 1 du signel  bruit
alpha=un'*x; % projection de coupure  du  bruit  sur le signal
% ======= procedure de codage
%c=x-alpha*un; %( filtration ou conteneur  de steganographie)
%  K=-un'*x+e(m)*abs(un'*x)%*un; % (ces coefficients depandent  du
%  model)seuil d adaptation , == travaillant  sur l energie de voix , pour
%  adapter  le  signal audible (il se choisit parmi les methode
%  psychoaccoustiques .

% physchoaccoustiaue
 s=x+K*un;

%s=c+e(m)*abs(alpha)*un; % ajout  vers  la  filtration du signal bruit
/stego-contener
Y(n:n+N-1)=s;
end;% for i=1:M
wavwrite(Y,'tictac11.wav');
toc
```

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] M. Warkentin, M. B. Schmidt, and E. Bekkering, "Steganography," pp. 50-56, 2007.

[2] M. Asad, J. Gilani, and A. Khalid, "An enhanced least significant bit modification technique for audio steganography," 2011.

[3] Y. Zhang, Z. Xu, and B. Huang, "Channel Capacity Analysis of the Generalized Spread Spectrum Watermarking in Audio Signals," *IEEE Signal Processing Letters,* vol. 22, pp. 519-523, 2015.

[4] Б. Скляр, *Цифровая связь: Теоретические основы и практическое применение*. Los Angeles: Издательский дом Вильямс, 2004.

[5] R. A.Garcia, " Digital Watermarking of Audio Signals Using a Psychoacoustic Auditory Model And Spread Spectrum Theory," 1999.

[6] A. Tanenbaum, "Réseaux 4eme édition," ed: Pearson Education, 2003.

[7] С. Сингх, "Книга шифров: тайная история шифров и их расшифровки/Саймон Сингх;[пер. с англ. А. Галыгина]," *М.: АСТ: Астрель,* 2007.

[8] E.G. Zhilyakov, P.G. Likholob, A.A. Medvedva, and E. I. Prokhorenko, " Исследование чувствительности некоторых мер качества скрытия информации," *научный рецензируемый журнал,* vol. 9, pp. 3-8, 2016.

[9] URL: https://www.mathworks.com (Дата обращения:19.06.2017)

[10] URL: http://www.xe.com (Дата обращения:19.06.2017)

Выпускная квалификационная работа выполнена мной совершенно самостоятельно. Все использованные в работе материалы и концепции из опубликованной научной литературы и других источников имеют ссылки на них.

«___» _____ _____ г.

_____ /Акаффу А.Г./
(подпись)