ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

АКАДЕМИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Институт криптографии связи и информатики

Факультет информационной безопасности

Кафедра 731

**КУРСОВАЯ РАБОТА**

Разработка стеганографического алгоритма скрытой передачи информации в системе VoIP телефонии Skype

Слушателя учебной группы 7351

факультета информационной безопасности

рядового Четверикова Ильи Сергеевича \_\_\_\_\_\_\_\_\_

(подпись)

Руководитель доцент кафедры 731

майор Зырянов Александр Владимирович \_\_\_\_\_\_\_\_\_

(подпись)

Рекомендуемая оценка \_\_\_\_\_\_\_\_\_

Оценка работы \_\_\_\_\_\_\_\_\_

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

МОСКВА 2015

Оглавление

[Оглавление 2](#_Toc431319254)

[Введение 3](#_Toc431319255)

[Глава 1. Исследование структуры программного обеспечения Skype 4](#_Toc431319256)

[Архитектура Skype 4](#_Toc431319257)

[Кодек Opus 5](#_Toc431319258)

[Глава 2. Описание известных методов робастного сокрытия информации в аудиосигналах. 12](#_Toc431319259)

[Внедрение сообщения в фазовую часть сигнала 12](#_Toc431319260)

[Метод сокрытия на основе шумоподобных сигналов 14](#_Toc431319261)

[Метод внедрения с использованием эхо-сигнала 17](#_Toc431319262)

[Глава 3. Метод робастного внедрения скрытой информации в аудиопоток программного обеспечения Skype 20](#_Toc431319263)

[Глава 4. Тестирование метода сокрытия 29](#_Toc431319264)

[Заключение 33](#_Toc431319265)

[Литература 34](#_Toc431319266)

Введение

Стеганография *–* это наука о тайной передаче информации путем сокрытия самого факта передачи. В связи с компьютеризацией всех областей человеческой деятельности в настоящее время быстро развивается компьютерная стеганография – та ее область, где информация скрывается в различные данные, для обработки которых используется компьютер. Это могут быть аудиоданные, видеопотоки, текстовые файлы и многие другие различные виды информации.

В данной работе рассматривается возможность сокрытия информации в аудиопоток программного обеспечения Skype — одной из наиболее широко используемых программ для коммуникации в сети Интернет. Аудиопоток кодируется с помощью гибридного кодека Opus, специально разработанного для использования в приложениях реального времени. Видеопоток в рамках данной работы не рассматривается.

**Целью** работы является разработка стеганографического алгоритма скрытного внедрения информации в аудиопоток системы VoIP телефонии Skype, устойчивого к перекодированию, и дальнейшего извлечения информации из этого потока.

**Задачи** работы:

1. Анализ кодека Opus на предмет возможности скрытого внедрения информации.
2. Разработка стеганографического алгоритма сокрытия информации в аудиопоток.
3. Программная реализация разработанного алгоритма.
4. Экспериментальная проверка эффективности алгоритма.

Глава 1. Исследование структуры программного обеспечения Skype

Объектом исследования курсовой работы является аудиокодек бесплатного проприетарного программного обеспечения Skype, являющегося одним из самых популярных средств аудио- и видеокоммуникации в сети Интернет, использующее технологии пиринговых сетей. Протокол Skype закрыт, не документирован и может использоваться только оригинальным программным обеспечением Skype [1]. Существует API, с помощью которого можно предоставить доступ к его функциям программам сторонних разработчиков.

Архитектура Skype

В отличие от многих других программ IP-телефонии, для передачи данных Skype изначально использовал децентрализованную P2P-архитектуру. Сеть состояла из трех типов сущностей: обычных узлов (ordinary nodes), суперузлов (supernodes) и сервера идентификации (login server) . Каталог пользователей Skype был распределён по компьютерам пользователей сети Skype, что позволяло сети легко масштабироваться до очень больших размеров (десятки миллионов пользователей) без увеличения дорогой инфраструктуры централизованных серверов. Skype мог маршрутизировать звонки через компьютеры других пользователей.

Единственным центральным элементом для Skype является сервер идентификации, на котором хранятся учётные записи пользователей и резервные копии их списков контактов. Центральный сервер нужен только для установки связи. После того как связь установлена, компьютеры могли пересылать голосовые данные напрямую друг другу (если между ними есть прямая связь) или через Skype-посредник - суперузел. Ранее в качестве суперузла мог выступать любой компьютер, у которого есть внешний IP-адрес и открыт TCP-порт для Skype, однако затем в 2012 все суперузлы были перенесены на сервера Microsoft.

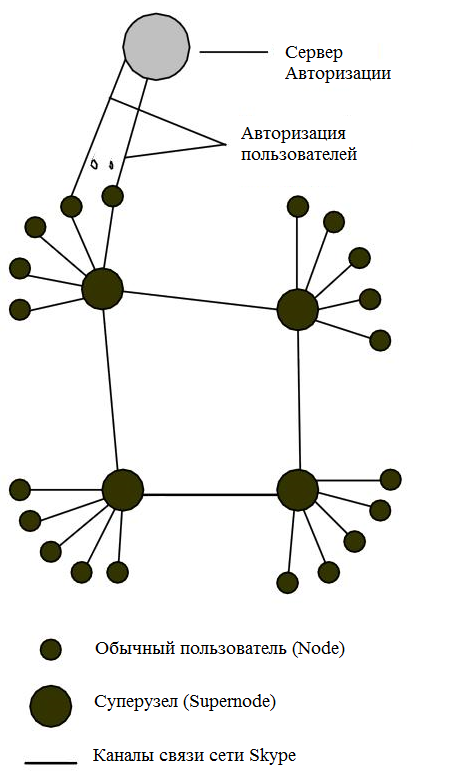


Рис. 1. Архитектура Skype

Кодек Opus

Opus — аудиокодек для сжатия с потерями, разработанный сообществом Internet Engineering Task Force (IETF) специально для применения в приложениях реального времени в интернете. Является открытым форматом, стандартизованным в RFC 6716 [2]. Примером применения этого кодека выступают программы Firefox и Thunderbird компании Mozilla, а также программа VoIP-телефонии Skype.

Разработчики Opus большое внимание уделили гибкости. Так, битрейт варьируется в пределах 6–510 кбит/с, частота дискретизации может составлять от 8 до 48 кГц, а длительность кадров изменяется от 2,5 до 20 мс. Opus объединяет кодеки CELT (Constrained Energy Lapped Transform) и SILK в модифицированном виде. CELT принадлежит к семейству кодеков OGG — он разрабатывался с прицелом на возможность работы в режиме реального времени; SILK — продукт создателей Skype, используемый в четвертой и более поздних версиях клиента для кодирования речи. Структура и принцип работы кодера в Opus просты: поток данных, в зависимости от частотного диапазона входящего сигнала, передается на обработку кодекам CELT или SILK.

SILK хорошо подходит для передачи низко- и среднечастотных сигналов с частотой дискретизации до 16 кГц. В основе этого кодека лежит техника Линейного Предсказания (LP). Сигналы с более широким диапазоном частот используют кодек CELT. Как и MP3, и AAC, он преобразует частоты посредством модифицированного дискретного косинусного преобразования и удаляет в ходе последующего квантования частоты, которые человеческое ухо воспринимает с трудом или не воспринимает вовсе. Так как SILK и CELT могут использоваться одновременно, разработчики предусмотрели для Opus три схемы работы: режим SILK для передачи только речи при низкой пропускной способности, гибридный режим для трансляции речи в наилучшем качестве и режим CELT для передачи одной только музыки. Схема кодека Opus представлена на схеме ниже.

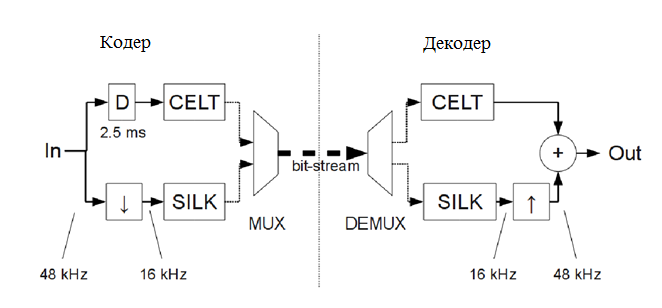
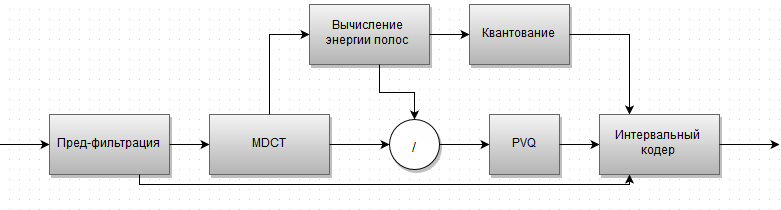


Рис. 2. Кодек Opus

Далее приведена схема CELT составляющей кодера.

 Рис. 3. Кодер CELT

В кодере CELT можно выделить следующие блоки:

1. Пред-фильтрация. Входной сигнал предварительно пропускается через фильтр, параметры которого зависят от самого входного сигнала, которые затем передаются на интервальный кодер.
2. MDCT (Модифицированное Дискретное Косинусное Преобразование). Используется для получения спектра сигнала. Формула преобразования:

,

где - временные отсчеты исходного сигнала, – спектральные отсчеты сигнала.

1. Блок вычисления энергии критических полос. Спектральные отсчеты разбиваются на группы, в соответствии с критическими диапазонами частот [3]. Для каждой группы высчитывается энергия полосы – масштабный коэффициент, на который потом нормируются спектральные отсчеты, принадлежащие данной полосе. Для полос, расположенных в более высокой области, масштабный коэффициент может высчитываться исходя из значения энергии более низких полос. Таким образом, масштабный коэффициент таких полос не передается. Эта техника называется спектральным наложением.
2. Квантование масштабных коэффициентов. На данном этапе масштабные коэффициенты квантуются и отправляются на интервальный кодер.
3. PVQ (Пирамидальное Векторное Квантование). Здесь спектральные отсчеты одной группы квантуются как вектор в пространстве, разбитом на области квантования, которые кодируются по словарю. Такая техника имеет преимущество в скорости обработки по сравнению с обычным скалярным квантованием [4]. Далее кодовый вектор передается на интервальный кодер.
4. Интервальный кодер. На данном этапе все необходимые данные сжимаются с помощью интервального кодирования [5]. На этом кодирование аудиосигнала завершается.

Ниже приведена схема CELT декодера.

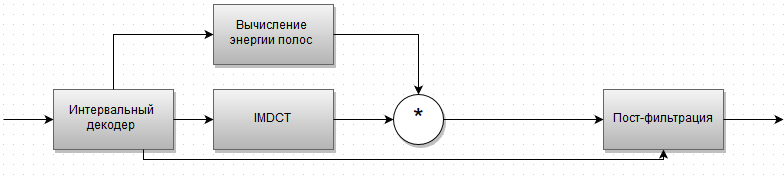


Рис. 4. Декодер CELT

В декодере CELT можно выделить следующие блоки:

1. Интервальный декодер. Здесь происходит распаковка пришедших данных.
2. IMDCT (Обратное Модифицированное Дискретное Косинусное Преобразование). Используется для получения временных отсчетов сигнала. Формула преобразования:

,

где - временные отсчеты исходного сигнала, – спектральные отсчеты сигнала.

1. Вычисление энергии спектральных полос. Для каждой полосы вычисляется масштабный коэффициент, учитывая инструмент спектрального наложения.
2. Пост-фильтрация. На данном этапе из пришедших параметров вычисляется импульсная характеристика фильтра и восстанавливается аудиосигнал.

Далее приведена схема SILK кодера.

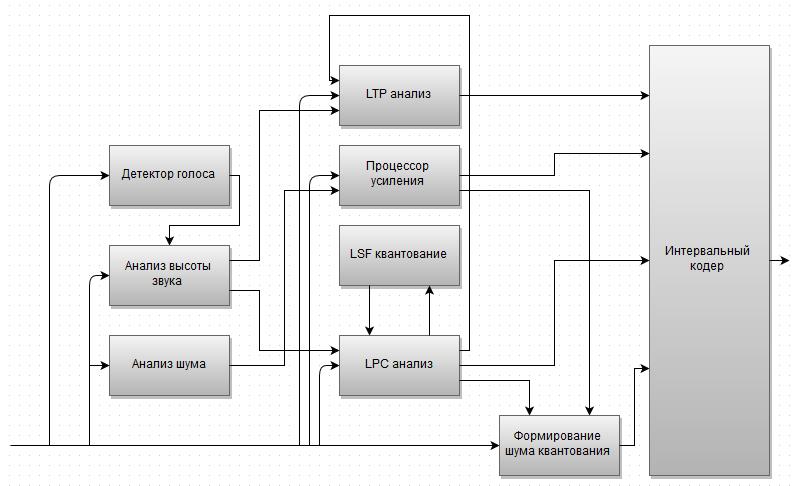


Рис. 5. Кодер SILK

В кодере SILK можно выделить следующие блоки:

1. Детектор голоса. Определяет наличие речевой составляющей в сигнале.
2. Анализ высоты звука.
3. Анализ шума. Предназначен для оценки уровня шума.
4. Процессор усиления. Оценка коэффициента усиления.
5. LPC анализ. LPC(Linear Predictive Coding – метод линейного предсказания) предназначен для кодирования речи, путем нахождения параметров звукообразующего тракта [6].
6. LSF квантование. LSF(Line Spectral Frequencies – Линейные Спектральные Частоты) квантование преобразует параметры LPC кодирования в более компактный вид [6].
7. LPT анализ. После прохождения этапа LPC анализа, LPT(Long Term Prediction) анализатор в остаточном сигнале ищет зависимости, которые можно предсказать, таким образом, сокращая количество бит, необходимых для кодирования звука [6].
8. Интервальный кодер. На данном этапе все необходимые данные сжимаются с помощью интервального кодирования. На этом кодирование аудиосигнала завершается.

Ниже приведена схема SILK декодера.

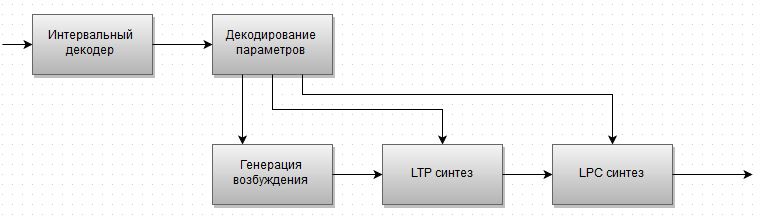


Рис. 6. Декодер SILK

В кодере SILK можно выделить следующие блоки:

1. Интервальный декодер. Здесь происходит распаковка пришедших данных.
2. Декодирование параметров. На данном этапе вычисляются параметры, необходимые для синтеза речевого синтеза.
3. Генерация возбуждения. Здесь генерируется сигнал, который послужит основой для дальнейшего восстановления сигнала.
4. LTP синтез. Происходит применение параметров LTP кодирования для модификации сгенерированного сигнала.
5. LPC синтез. Происходит применение параметров LPC кодирования для модификации сгенерированного сигнала.

Глава 2. Описание известных методов робастного сокрытия информации в аудиосигналах.

Перед рассмотрением методов внедрения информации в аудиосигналы, необходимо рассмотреть требования, которые могут быть предъявлены к стегосистемам, применяемым для надежного встраивания информации в аудиосигналы [7]:

- 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;

- скрываемая информация не должна вносить заметных изменений в статистику контейнера;

Внедрение сообщения в фазовую часть сигнала

Основываясь на том факте, что человеческое ухо невосприимчиво к абсолютному значению фазы гармоник, составляющих сигнал, в [8] был предложен алгоритм внедрения передаваемого сообщения в фазовую часть аудиосигнала. Суть данного метода состоит в модификации фазы начального сегмента в зависимости от внедряемых данных. Фаза последующих сегментов согласовывается с новой фазой первого сегмента для сохранения разности фаз. Аудиосигналом-контейнером в данном методе выступает оцифрованный несжатый аудиосигнал. Сообщение представляет собой битовую последовательность ограниченной длины. Метод внедрения описывается следующим алгоритмом:

1. Исходный аудио сигнал s*,* разбивается на последо­вательность из *N* непересекающихся сегментов *.*
2. Используя *К*-точечное дискретное преобразование Фурье, на каждом сегменте вычисляется фаза и амплитуда для каждой гармоники.
3. Вычисляется разность фаз между соседними сегментами:
4. Очередная порция скрываемых данных представляется как *К*-точечный набор , состоящий из чисел π/2 или -π/2, представляющих двоичные 0 и 1 соответственно. Построенная последовательность выбирается в качестве фазы начального сегмента:
5. Основываясь на вычисленных в п. 3 разностях фаз, вычисляем значения фазы на остальных сегментах:

. . . . . . . . . . . . . . . . . . . . . . . .

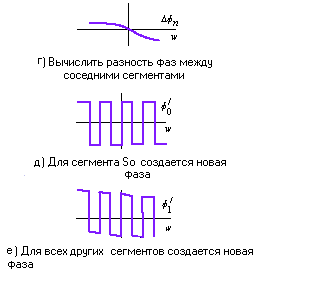
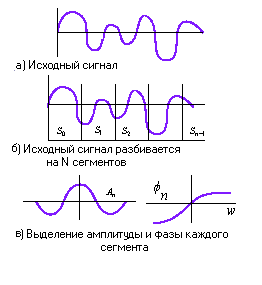
1. Используя модифицированную фазу и исходные значения амплитуды *,* восстанавливаем аудиосигнал с использованием обратного преобразования Фурье.

Обратное преобразование описывается следующим алгоритмом:

1. Исходный аудиосигнал s*,* разбивается на последо­вательность из непересекающихся сегментов
2. Используя *К*-точечное дискретное преобразование Фурье, на 0-м сегменте вычисляется фаза для каждой гармоники.
3. Из извлекается очередная порция бит скрываемого сообщения.

При практической реализации аудиосигнал разбивается в последо­вательность исходных аудиосигналов длины , на каждом из которых про­изводится сокрытие или извлечение порции данных.

Ниже приведен вид сигналов при сокрытии методом фаз.



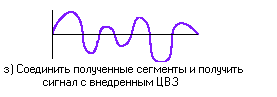


Рис. 7. Сокрытие с помощью метода фаз

Данный метод характеризуется достаточной степенью скрытности, но достаточно небольшим коэффициентом использования сигнала-контейнера. Кроме того, на основе анализа непрерывности фазы можно находить точки начала исходных аудио сигналов, что может быть использовано для построения метода стеганоанализа.

Метод сокрытия на основе шумоподобных сигналов

Метод сокрытия на основе шумоподобных сигналов [9] широко известен из теории радиосвязи, где он используется для повышения по­мехозащищенности. Он состоит в генерации псевдослучайного шума, являющегося функцией внедряемого сообщения, и подмешивании по­лученного шума к основному сигналу-контейнеру в качестве аддитивной составляющей. В качестве приемника используется известный из теории радиосвязи оптимальный приемник, основанный на вычислении функции корреляции между предсказанным сигналом и реально принятым.

Рассмотрим работу алгоритма внедрения более подробно. Типичный метод создания шумоподобного сигнала состоит в модуляции фазы тонального сигнала псевдослучайной последовательностью. В матема­тическом выражении это выглядит следующим образом:

где - число сэмплов в секунду; - частота опорного сигнала;  *-* псевдослучайная последовательность с минимальным расстоянием между сменами значений ; - передаваемые данные с минимальным расстоянием между сменами значений . Функции и являются отображениями из множества в бинарное множество {-1,1}. Для обеспечения шумоустойчивости данного метода расстояния и должны удовлетворять следующему соотношению: должен быть как минимум в несколько раз больше *.* Ниже изображен пример функции .

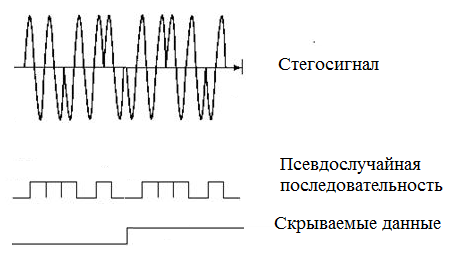


Рис. 8. Пример шумоподобного сигнала

Параметр *,* частота опорного сигнала и функция являются ключом данной стеганографической системы. В качестве функции *,* как правило, выбирается линейная конгруэнтная функция, генерирующая псевдослучайную последовательность, и следовательно, для ее задания достаточно трех чисел.

Результирующий аудиосигнал получается путем аддитивного подмешивания сформированной последовательности в ис­ходный аудиосигнал контейнер :

Для построения обратной функции извлечении информации в теории радиосвязи корреляционные приемники.

Корреляционный приемник основан на вычислении функции корре­ляции между принятым сигналом и предсказанным :

Поскольку задача извлечения информации может быть представлена как задача приема сигнала с неизвестными параметрами, то для организации приема бинарных данных необходимо наличие двух корреляционных приемников. В первом приемнике в качестве предсказанного сигнала выбирается сигнал , соответствующий бинарной единице, т.е. сигнал *,* вычисленный при для всех *.* Во втором приемнике выбирается сигнал , соответствующий бинарному нулю. Функции корреляции в этом случае определяются следующим образом:

Решение о приеме в -ой позиции скрытого сообщения бинарного нуля принимается в случае, если ***,*** в противном случае принимается решение о приеме бинарной единицы.

К достоинствам метода использования шумоподобных сигналов можно отнести высокую скрытность и помехоустойчивость, к недостаткам коэффициент использования сигнала контейнера. Данный метод можно использовать для скрытой передачи информации по реальным каналам даже в случае, если известно, что передаваемый сигнал будет подвергаться преобразованиям по пути следования от отправителя до получателя, например при использовании в качестве среды передачи аналоговой телефонной сети или радиосвязи.

Метод внедрения с использованием эхо-сигнала

Одной из вариаций предыдущего метода является метод [8], основанный на использовании в качестве шумоподобного сигнала самого аудиосигнала, задержанного на различные периоды времени в зависимости от внедряемого сообщения. Этот метод позволяет внедрять данные в сигнал прикрытия, изменяя параметры эхо-сигнала. К параметрам эхо, несущим внедряемую информацию, 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 для большинства типов сигналов и для большинства слушателей слияние двух сигналов происходит при расстоянии между ними около 0,001 секунды.

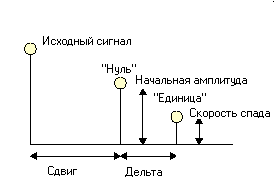
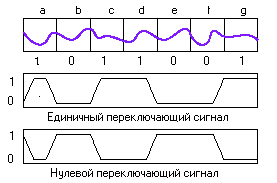


Рис. 9 Параметры эхо-сигнала

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.

Ключом данной стеганографической системы являются сдвиг и время спада эхо-сигналов, а также длительность сегмента, на котором кодируется один бит.

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. Схема кодера представлена ниже.



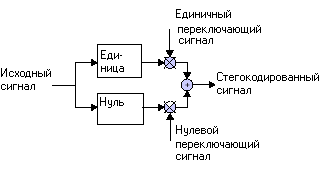


Рис. 10. Схема стегокодера.

Декодирование внедренной информации представляет собой определение промежутка времени между сигналом и эхо. Для этого необходимо рассмотреть амплитуду (в двух точках) автокорреляционной функции дискретного преобразования Фурье логарифма спектра мощности (кепстра). Правило декодирования основано на определении промежутка времени между исходным сигналом и всплеском автокорреляции. Если всплеск на времени задержки, соответствующем единице, больше чем на времени задержки, соответствующем нулю, то принимается единица, иначе - ноль.

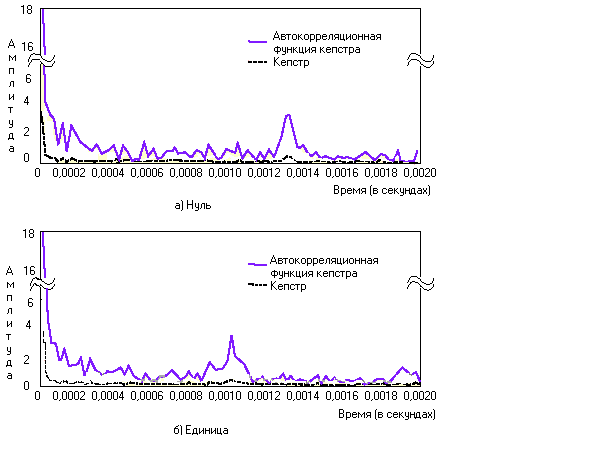


Рис. 11. Поведение автокорреляционной функции кепстра при различной внедренной информации

Данный метод характеризуется высокой степенью скрытности и достаточной степенью устойчивости. Однако ценой этому является достаточно низкая пропускная способность.

Глава 3. Метод робастного внедрения скрытой информации в аудиопоток программного обеспечения Skype

В качестве основной идеи представленного в работе алгоритма используется метод шумоподобных сигналов [9]. В оригинальном методе внедрение одного бита информации в сегмент аудиоданных производится по формуле:

где T - число сэмплов в секунду; ω - частота опорного сигнала; – линейная конгруэнтная функция, – внедряемый бит сообщения. В описываемом в работе методе внедрение одного бита в сегмент аудиоданных, на которые разбивается аудиопоток, осуществляется по формуле:

где – линейная конгруэнтная функция, – внедряемый бит сообщения, – весовая функция Хэмминга, – масштабный множитель, значение которого определяется экспериментально (см. Главу 4), 0 < , – длина сегмента.

Линейная конгруэнтная функция (ЛКФ) – кусочно-постоянная функция, отображающая во множество {-1, 1} – строится на основе двоичной записи числа, генерируемого линейной рекуррентой, параметры которой (три числа) являются ключом стеганографической системы. На каждый бит генерируется два члена рекуррентной последовательности, одна для скрытия единицы, другая для сокрытия нуля. Затем выбранное число приводится по модулю 216 с целью получения 16 двоичных цифр. На основе этой двоичной записи и строится линейная конгруэнтная функция. Ниже на рисунке приведен пример такой функции.

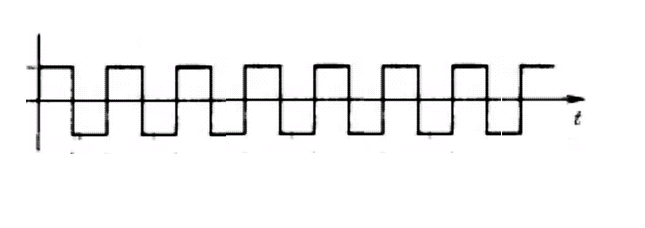


Рис. 12. Пример ЛКФ, построенной на последовательности “101010101010101”

Результирующий аудиосигнал , - ключ стегосистемы, как и в оригинальном методе, получается путем аддитивного подмешивания сформированной последовательности в исходный аудиосигнал контейнер :

Алгоритм извлечения данных, также как и в оригинале, основан на функции корреляции, но с учетом особенностей внедрения в аудиопоток, приведенных далее, будет описан несколько ниже.

В отличие от стеганографических методов, применяемых для сокрытия данных в аудиофайлах, внедрение информации в оцифрованные данные, записанные с устройства записи, которые после этого сразу же передаются на вход программному обеспечению Skype, имеет ряд специфических особенностей:

1. Внедрение должно происходить в режиме реального времени. Не должно быть большой, ощутимой на слух задержки аудиопотока.
2. Необходим инструмент, позволяющий определить на стороне приемника факт начала передачи скрытого сообщения.
3. При извлечении информации, с вероятностью близкой к единице, используется другое разбиение аудиопотока на сегменты, чем это происходило при внедрении информации.

Описанный в работе метод учитывает все эти особенности. Во- первых, подсчитаем сложность алгоритма в зависимости от n – размера сегмента аудиопотока, выраженного в сэмплах. На генерацию двух чисел с помощью линейного рекуррентного соотношения требуется 2 операции умножения и 2 операции сложения, на получение линейной конгруэнтной функции требуется O(n) операций. Перемножение двух дискретных сигналов длиной в n сэмплов имеет сложность O(n) операций. Умножение сигнала в n сэмплов на число также имеет сложность O(n) операций. Таким образом, сложность внедрения одного бита равна 3\* O(n) + 4 = O(n), то есть линейна.

Во-вторых, перед началом внедрения самой информации внедряется по аналогичной формуле стегосигнал, у которого вместо конгруэнтной функции, основанной на генерируемом числе, берется конгруэнтная функция, основанная на строго определенной двоичной последовательности. В работе для этой цели используется последовательность «1010101010101010». Таким образом, перед началом извлечения информационных символов требуется детектировать эту последовательность в аудиопотоке. Это возможно с использованием функции “максимальной корреляции”, описанной далее. Если значение функции “максимальной корреляции” больше чем пороговое значение, обозначаемое в данной работе , то устанавливается, что стартовая последовательность детектирована, иначе – недетектирована. После проведения серии экспериментов (см. Главу 4), это пороговое значение было принятым равным 0,27.

В-третьих, вместо сокрытия в один сегмент аудиопотока одного информационного символа предлагается использовать несколько сегментов на один бит. Это позволяет при извлечении скрытой информации обрабатывать сегменты того же размера, что использовались при сокрытии, в которых гарантировано внедрен один и тот же бит, пропуская сегменты, которые были использованы при сокрытии разных битов сообщения.

Далее возможны две ситуации, показанные на рисунке ниже, которые образованы тем, что при извлечении в обрабатываемый сегмент аудиопотока может попасть лишь часть сигнала, в которую внедрена стартовая последовательность. Она может быть как детектирована, так и не детектирована Красным цветом показаны сегменты, которыми обрабатывался сигнал при сокрытии, при чем в сегментах 1-3 скрыта стартовая последовательность, 4-6 – один и тот же информационный бит. Зеленым показаны сегменты, которыми обрабатывался сигнал при извлечении. В верхней части рисунка сегмент извлечения с номером 1 не детектировал входящую последовательность, но детектировали сегменты извлечения 2 и 3 (сегмент закрашен желтым цветом). В нижней части рисунка сегменты извлечения с номером 1, 2, 3 детектировали входящую последовательность. Таким образом, при извлечении после детектирования двух стартовых последовательностей, необходимо пропустить два следующих сегмента, и извлекать бит сообщения из третьего сегмента (на рисунке сегменты 5 и 6 соответственно).

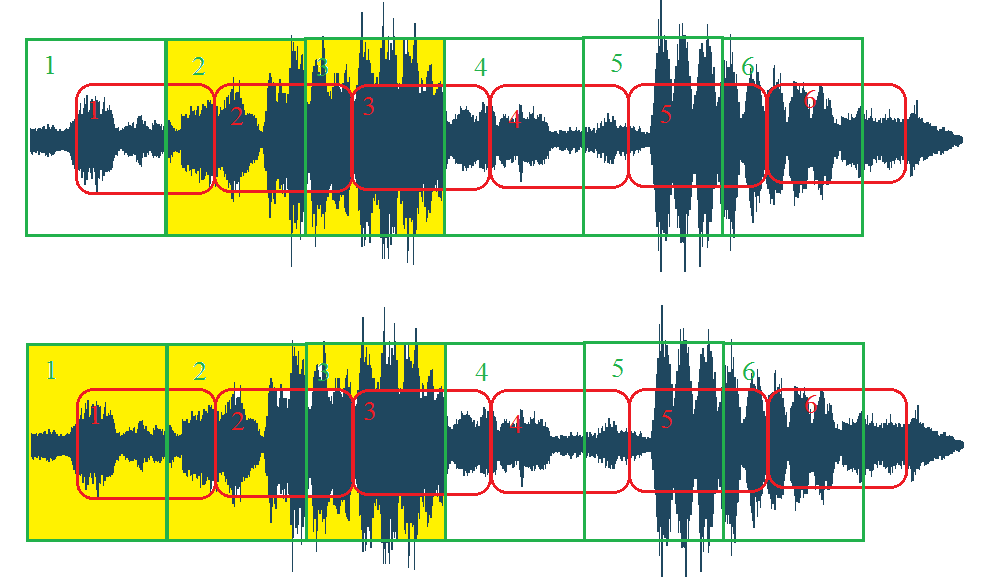


Рис. 13. Типичное расположение сегментов, используемых при сокрытии, относительно сегментов, используемых при извлечении (зеленым обозначены сегменты, используемые при извлечении, красным – при сокрытии, при чем в сегментах 1-3 внедрена стартовая последовательность, в 4-6 один и тот же информационный бит)

Исходя из вышеперечисленных особенностей, алгоритм извлечения одного бита информации, после детектирования стартовой последовательности, заключается в следующем: аналогично тому, как делалось при сокрытии, необходимо сгенерировать две двоичные последовательности, соответствующие 0 и 1, найти значения функции “максимальной корреляции” между сегментом и ЛКФ, основанными на этих последовательностях и сравнить их. Если больше значение, соответствующее нулю, то принимается ноль, иначе – единица.

Функция “максимальной корреляции” двух сигналов заключается в следующем. Находится значение коэффициента корреляции между этими сигналами по формуле:

,

где – сигналы, , – средние значения амплитуды сигналов [11]. Затем один из них циклически сдвигается на один отсчет, опять находится значение коэффициента корреляции и т.д., пока первый сигнал не сдвинется на начальную позицию. Затем из всех найденных значений необходимо взять максимальное значение, являющееся результатом функции. Такая функция необходима, так как при извлечении одного бита сообщения, сегмент представляет собой исходный сигнал с внедренной циклически сдвинутой на некоторое количество отсчетов ЛКФ, за счет того, что сегмент извлечения попадает на границу сегментов сокрытия.

Сложность извлечения составляет O(n2), где n – длина сегмента, так как нахождение коэффициента корреляции занимает O(n) операций, а сдвигов происходит ровно n штук.

Длина сегмента выбирается экспериментально. В данной работе эксплуатировалось значение 4096 отсчетов на сегмент (см. Главу 4).

Весовая функция Хэмминга при сокрытии применяется в разработанном методе затем, чтобы минимизировать корреляцию между двумя псевдослучайными последовательностями, которые используются для сокрытия 0 и 1 соответственно, для более четкого детектирования при извлечении информации.

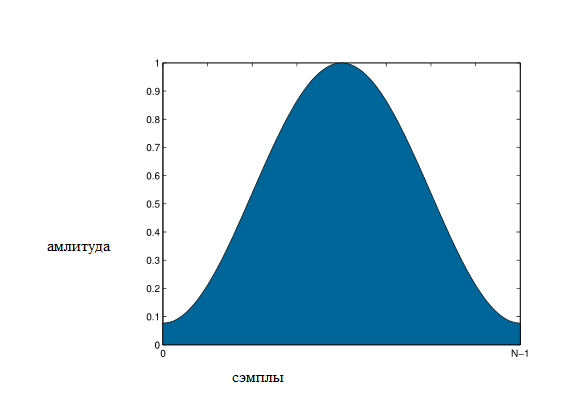


Рис. 14. Весовая функция Хэмминга

Ниже приведена полная схема алгоритма.

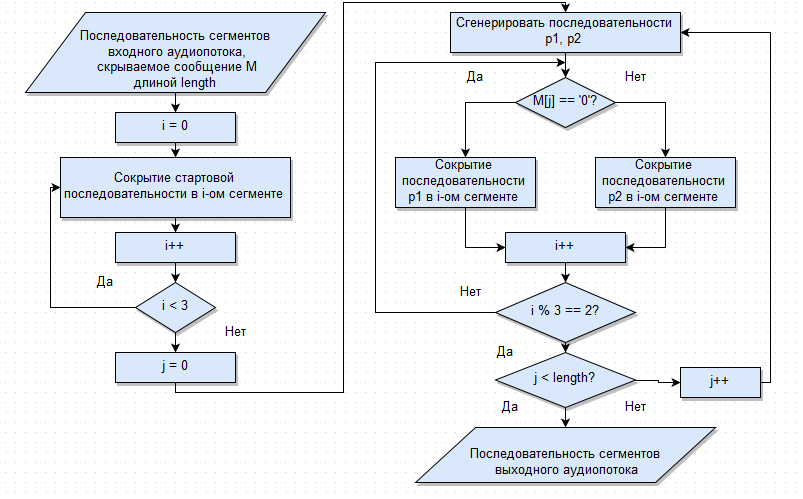


Рис. 15. Алгоритм сокрытия сообщения в аудиопотоке

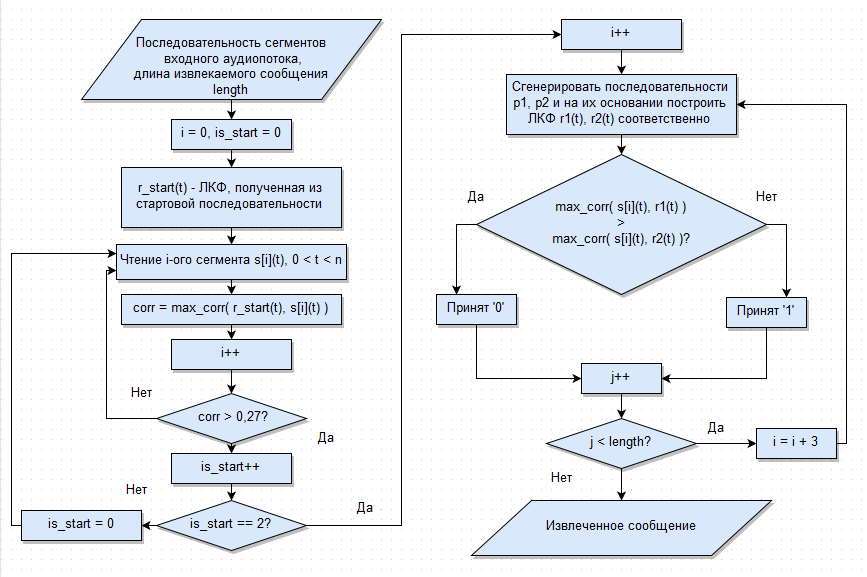


Рис. 16. Алгоритм извлечения сообщения из аудиопотока (max\_corr – функция “максимальной корреляции”, описанная на рис. 18)

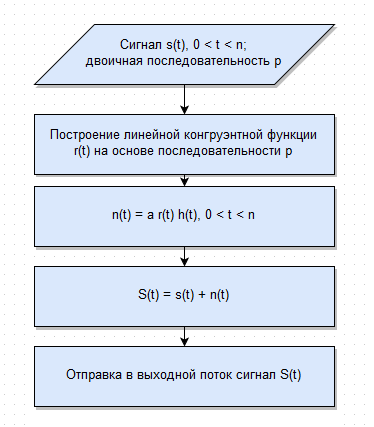


Рис. 17. Алгоритм сокрытия двоичной последовательности в одном сегменте

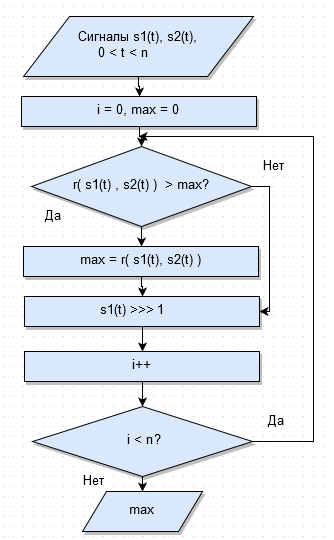


Рис. 18. Алгоритм вычисления функции “максимальной корреляции” (обозначаемой в работе max\_corr()) двух дискретных сигналов ( r( s1, s2) –коэффициент корреляции, >>> - оператор циклического сдвига вправо)

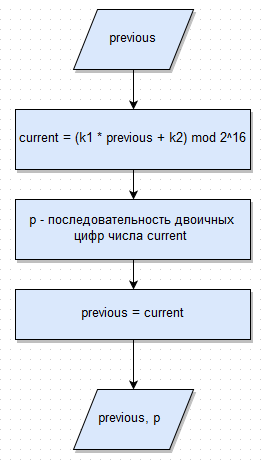


Рис. 19. Алгоритм генерации псевдослучайной двоичной последовательности (при первом проходе полагаем previous = k3), где числа k1, k2, k3 – ключ стегосистемы

Для программной реализации метода маркирования использовалась среда разработки Visual Studio 2013 с использованием интерфейса программирования приложений в среде Windows WinAPI. Информация по работе со звуковыми устройствами была получена из пособия [12]. В ходе разработки было написано два консольных приложения. Первое получает аудиоданные с устройства записи, скрывает сообщение, и передает их на заданное устройство. Второе приложение получает аудиоданные с заданного устройства, извлекает скрытое сообщение из аудиопотока и воспроизводит звук на устройстве воспроизведения. Полный исходный код приложений представлен на компакт-диске, прилагаемом к данной курсовой работе.

Глава 4. Тестирование метода сокрытия

Для проверки корректности алгоритма проведен ряд экспериментов с программным обеспечением Skype и реализованными приложениями. Целью этих экспериментов является оценка эффективности, робастности и скорости алгоритма и определение оптимального значения параметра (см. главу 3). Также с помощью экспериментов будет определено значение размера сегмента и пороговое значение детектирования стартовой последовательности .

Тестирование проводилось на персональном компьютере со следующими конфигурациями: процессор Intel Core i7 – 3610QM 2.3 GHz, ОЗУ - 8 Гб, ОС Windows 7 x64.

Ниже приводится схема тестового стенда в рамках исследования алгоритма внедрения и извлечения информации.

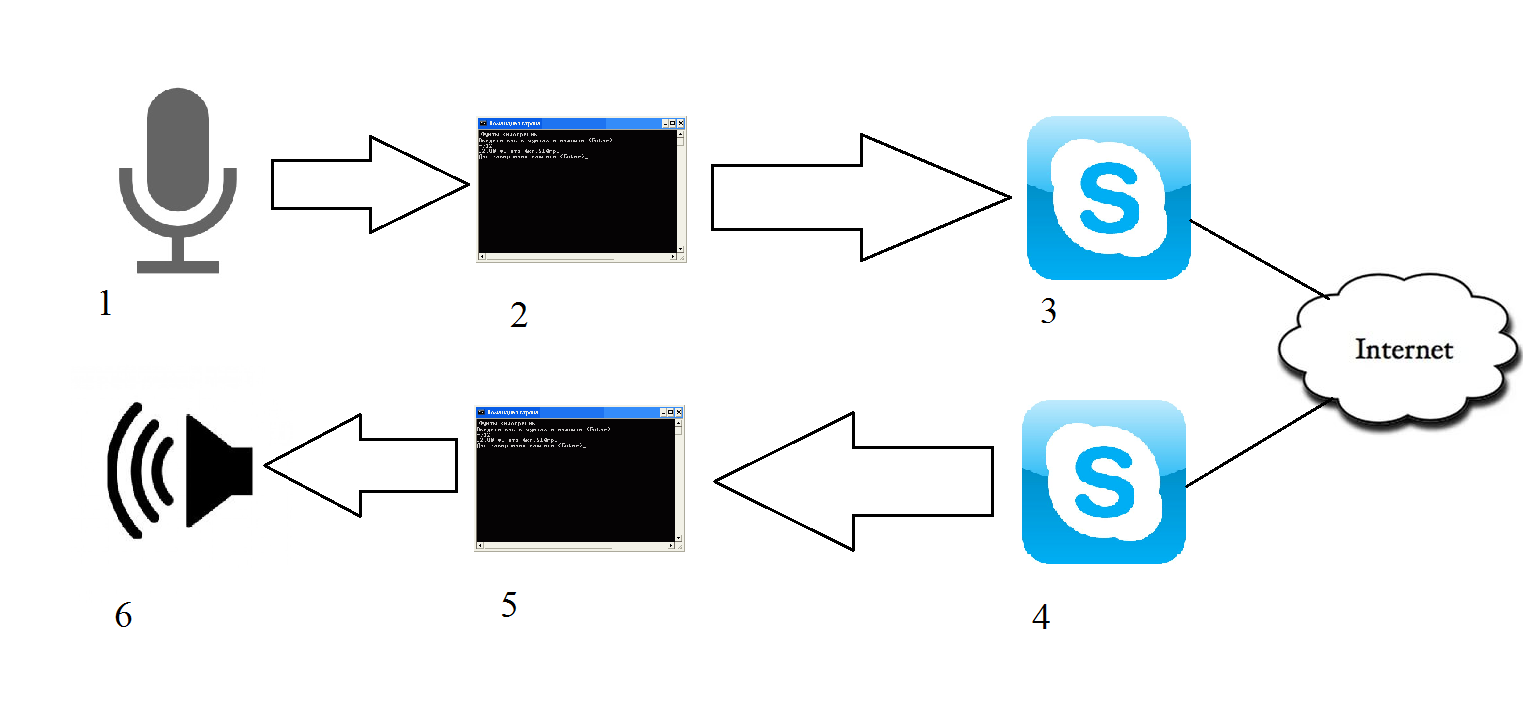


Рис. 20. Схема тестирования алгоритма. 1. Микрофон. 2. Программа внедрения Hide.exe 3. Первый экземпляр Skype 4. Второй экземпляр Skype, запущенный на том же ПК 5. Программа извлечения Extract.exe 6. Устройство воспроизведения. Стрелками показаны потоки аудиоданных

В программу сокрытия от микрофона приходит дискретизированные с частотой 44100 Hz, глубиной звучания 16 бит стерео аудиоданные. Далее они используются для сокрытия двоичного сообщения на ключе k1 = 35, k2 = 347, k3 = 121. Далее аудиоданные через виртуальный кабель попадают на первый экземпляр программы Skype, который используя сеть Интернет, соединяется со вторым экземпляром программы, находящийся на том же компьютере. Аудиоданные приходят от первого экземпляра ко второму. Далее также через виртуальный кабель данные попадают на программу извлечения информации и затем выводятся на динамики.

После ряда экспериментов с различными значениями установлено, что при значениях длины сегмента приблизительно меньших 1500 сэмплов в аудиосигнале появляются паузы связанные с тем, что сегмент обрабатывается дольше, чем он звучит. Значения большие приблизительно 8000 сэмплов вносят большую задержку при передаче аудиосигнала. Таким образом, размер сегмента был выбран в границе этих значений – 4096.

В следующем ряде экспериментов во все сегменты скрывается стартовая последовательность. Программа, извлекающая информацию, при вычислении значения функции “максимальной корреляции” с линейной конгруэнтной функцией, основанной на стартовой последовательности, дает среднее округленное значение 0,45. При отсутствии скрываемой последовательности среднее значение падает до 0,09. Таким образом, пороговое значение детектирования стартовой последовательности следует взять равным среднему арифметическому этих двух значений, а именно 0,27. При оценке вероятности ошибки первого рода, то есть отношения количества сокрытых стартовых последовательностей, но недетектированных при извлечении, к общему количеству сокрытых последовательностей, было внедрено 500 стартовых последовательностей на 1500 сегментах. Из них недектированными оказались 11. Таким образом, оценка вероятности первого рода составляет 0,022. При оценке вероятности ошибки второго рода, то есть отношения количества детектированных стартовых последовательностей в сегментах, где они изначально не скрывались, к общему числу этих сегментов, деленному на три (так как для сокрытия стартовой последовательности используется три сегмента), было взято 1500сегментов. Детектировано – две стартовые последовательности. Таким образом, оценка вероятности ошибки второго составляет 0,004.

При определении параметра , в работе проводится серия экспериментов по чтению битов из аудиопотока с закодированным несколько раз случайным 100 битным двоичным сообщением. Тестируется 5 значений параметра и измеряется процент ошибочно декодируемых бит при передаче разговора и при передаче тишины. Результаты тестирования занесены в таблицу 1.

Таблица №1

Результаты тестирования параметра

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Параметр | Процент ошибок при передаче тишины | Процент ошибок при передаче “тихого” разговора | Процент ошибок при передаче “громкого” разговора | Процент при передаче музыкального аудио |
| 1 | 30 | 8% | 20% | 30% | 24% |
| 2 | 50 | 8% | 16% | 30% | 18% |
| 3 | 70 | 6% | 16% | 24% | 13% |
| 4 | 100 | 2% | 10% | 19% | 10% |
| 5 | 150 | 0% | 8% | 18% | 8% |

Следует отметить, что по субъективной оценке качества аудиопотока, прослушиваемого с динамиков, в первых двух экспериментах по параметру , скрытые данные не заметны. В последних двух экспериментах слышимость помех, вызванная сокрытием данных практически очевидна. При третьем эксперименте, скрытые данные едва различимы. Таким образом, оптимальным параметром следует признать значение близкое к 70. Также при передаче сообщения возможно применить кодирование Хэмминга для большей надежности передачи данных.

Далее был проведен ряд экспериментов, связанных с тестированием разработанной программы в более реальных условиях, а именно использование двух компьютеров, связанных по сети интернет. Параметр принимается равным 70. Сообщение представляло случайную двоичную последовательность длины 1000, заполненной случайным образом. Процент ошибок при разговоре составил 12%.

При выборе размера сегмента равным 4096 и частоте дискретизации 44100 Hz, а также с учетом того факта, что один бит скрывается в трех сегментах, скорость передачи скрытой информации составляет 3,5 бит/с.

Заключение

В данной работе разработан и реализован стеганографический алгоритм внедрения информации в аудиопоток программного обеспечения Skype.

В процессе работы были решены следующие **задачи**:

1. Проанализирован кодек Opus программного обеспечения Skype. Этот кодек состоит из двух подкодеков – CELT, основанный на разложении сигнала в спектр с помощью МДКП, и SILK, основанный на технике линейного предсказания. Opus – кодек сжатия с потерями, и поэтому “простые” методы сокрытия в амплитудные или спектральные отсчеты не применимы.
2. Разработан и реализован алгоритм внедрения информации в аудиопоток программного обеспечения Skype. Алгоритм разработан на основе известных из теории радиосвязи шумоподобных последовательностей. Суть метода сокрытия информации заключается в аддитивном подмешивании различных в зависимости от внедряемого бита сигналов к сигналу-контейнеру.
3. Экспериментальным путем определены подходящие с точки зрения соотношения робастности и неотличимости параметры стегосистемы. Также реализованное программное средство было протестировано в условиях, близких к реальным условиям применения программы, а именно при соединении по Интернет-каналу двух компьютеров, с установленным на них программным обеспечением Skype. Оценено качество разработанного алгоритма, заключающегося в подсчете относительного числа ошибок при сокрытии-извлечении тестовой информации.

Литература

1. An Analysis of the Skype Peer-to-Peer Internet Telephony Protocol by Salman A. Baset and Henning Schulzrinne (Skype v1.4). – 2006.
2. IETF specifications. Official Opus codec RFC 6716. – 2012.
3. А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин, Основы компьютерной стеганографии. – 2003. – С. 64 – 65.
4. Thomas R. Fischer, A Pyramid Vector Quantizer. – 1986.
5. Martin G, Range encoding, An algorithm for removing redundancy from a digitised message. – 1979.
6. Нечипорук О.П., Одарченко Р.С.,Потапов В.Г., Тараненко А.Г., Ткалич О.П. Кодирование речи с комбинированным предсказанием. – 2005.
7. В. Г. Грибунин, Цифровая стеганография. – 2002. – С. 208.
8. Bender W., Gruhl D., Morimoto N., Lu A. Techniquies for Data Hiding. C. 313 – 331.
9. А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин, Основы компьютерной стеганографии. – 2003. – С. 76 – 78.
10. V. Habarchuk, G. Koziel, The Review of Soundbased Steganographic Techniques. 2008.
11. Ж. Макс, Методы и техника обработки сигналов при физических измерениях, Т.1. – 1983.
12. О. Гордеев, Программирование звука в Windows. – 1999.