

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение  
высшего образования

**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ  
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теоретических основ  
компьютерной безопасности и  
криптографии

**Исследование устойчивости ЦВЗ, встроенных методом вейвлет-  
преобразования, в аудиофайлах**

АВТОРЕФЕРАТ

дипломной работы

студентки 6 курса 631 группы

специальности 10.05.01 Компьютерная безопасность

факультета компьютерных наук и информационных технологий

Никитиной Александры Сергеевны

Научный руководитель

к. п. н., доцент

\_\_\_\_\_

А. С. Гераськин

22.01.2024 г.

Заведующий кафедрой

д. ф.-м. н., доцент

\_\_\_\_\_

М. Б. Абросимов

22.01.2024 г.

Саратов 2024

## ВВЕДЕНИЕ

Все более актуальной становится проблема защиты информации. Интерес к стеганографии можно объяснить широким распространением мультимедийных технологий. Методы стеганографии позволяют не только скрытно передавать данные, но и решать задачи помехоустойчивой аутентификации, защиты информации от несанкционированного копирования, отслеживания распространения информации по сетям связи, поиска информации в мультимедийных базах данных.

Компьютерную стеганографию можно разделить на два основных направления: первое направление, связанное с цифровой обработкой сигналов, второе – не связано, то есть сообщения могут быть встроены в заголовки файлов или заголовки пакетов данных. Этот способ достаточно ограничен в своем применении, так как легко вскрываем. В большей степени разработки ведутся именно в направлении обработки сигналов.

Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты прав собственности на информацию, представленную в цифровом виде.

Цифровой водяной знак (ЦВЗ) – специальная метка, незаметно внедряемая в изображение или другой сигнал с целью тем или иным образом контролировать его использование.

Целью данной работы является реализация метода внедрения цифрового водяного знака в аудиофайл с помощью вейвлет-преобразования, а также анализ эффективности данного метода относительно других распространенных методов и устойчивости к атакам на аудиофайл.

Для достижения поставленной цели были сформулированы следующие задачи:

1. изучить теоретический материал о стеганографии и цифровых водяных знаках;

2. получить представление о процессе внедрения цифрового водяного знака в аудиофайл с помощью вейвлет-преобразования;
3. разработать программу, внедряющую и извлекающую ЦВЗ выбранным методом;
4. проанализировать данные, полученные с помощью программы, и оценить эффективность внедрения ЦВЗ;
5. рассмотреть аналоги, существующие на рынке;
6. проанализировать реакцию ЦВЗ на применяемые атаки.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 1 приложения. Общий объем работы – 66 страниц, из них 44 страницы – основное содержание, включая 40 рисунков и 1 таблицу, список использованных источников из 18 наименований.

## КРАТКОЕ СОДЕРЖАНИЕ

Первый раздел работы содержит теоретические понятия, необходимые для дальнейшего изучения темы. Делится на два подраздела, в первом приводятся общие сведения о стеганографии, во втором описывается аудиостеганография.

Стеганография – это метод организации связи (передачи сообщений), при котором скрывается само наличие связи. В отличие от криптографии, где противник точно может определить, является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в открытые послания таким образом, чтобы было невозможным заподозрить существование самого встроенного послания.

Компьютерная стеганография базируется на двух основных принципах.

Первый принцип заключается в том, что файлы, содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери их функциональности в отличие от других типов данных, требующих абсолютной точности.

Второй принцип заключается в неспособности органов чувств человека различать незначительные изменения в цвете изображения или качестве звука. Этот принцип особенно легко применять к изображению или звуку, несущему избыточную информацию.

Структурная схема стegosистемы представлена на рисунке 1. Сообщение – это любая информация, подлежащая скрытой передаче.



Рисунок 1 – Структурная схема стegosистемы

Аудиостенография – один из способов сокрытия информации применимый только к аудиофайлам. При шифровании данных в аудио, также как и с изображениями можно изменять младшие биты, так же можно построить алгоритм шифрования, упираясь на особенности системы слуха человека. Человеческое ухо воспринимает сигналы в диапазоне 10 – 20000 Гц, также, изменение фазы сигнала улавливается человеком слабее, чем изменение частоты или амплитуды. Следовательно, существуют пять основных методов встраивания информации в аудиосигналы:

- встраивание с расширением спектра (незначительно изменяются амплитуды отсчетов);
- встраивание за счет модификации фазы аудиосигнала (фаза исходного сегмента сигнала изменяется согласно помещенных данных, фаза последующих сегментов согласовывается с фазой начального сегмента для сохранения разности фаз);
- встраивание за счет изменения времени задержки эхо-сигнала;
- методы маскирования ЦВЗ;
- методы кодирования наименее значащих бит.

Во втором разделе рассматриваются основные методы внедрения цифровых водяных знаков в аудиофайлы.

Один из распространенных методов внедрения – модификация наименее значащих бит (LSB). Идея метода заключается в следующем: исходный водяной знак переводится в битовую последовательность. Полученные биты замещают наименее значащие биты в отдельных отсчетах аудиофайла. Для извлечения ЦВЗ достаточно собрать биты из нужных отсчетов и поместить их в одну строку.

Метод кодирования с расширением спектра описывается следующим образом. Пусть аудиосигнал состоит из  $N$  отсчетов  $x(i)$ ,  $i = 1, \dots, N$ , 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  $[-\alpha; \alpha]$ ,  $\alpha$  – некоторая константа. Функция  $f$  должна принимать во внимание особенности системы слуха человека во избежание ощутимых искажений исходного сигнала. Отсчет результирующего сигнала получается следующим образом, как показано в формуле 1.

$$y(i) = x(i) + f(x(i), w(i)) \quad (1)$$

В следующем подразделе рассматривается метод, основанный на изменениях времени задержки эхо-сигнала. 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, 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.

В завершающем подразделе описывается метод, использующий вейвлет преобразования. Вейвлет-преобразование по своей сути является математической функцией, которая позволяет разложить сигнал на несколько частотных областей, что обеспечивает ЦВЗ большей устойчивостью к атакам относительно других преобразований, например, Фурье или дискретного косинусного преобразования.

Основная идея метода заключается в том, что в зависимости от значений вейвлет-коэффициентов определяется, в какие из них можно внести большие изменения, а в какие – меньшие.

В вейвлет-преобразовании участвуют два множества функций: масштабирующие функции и вейвлеты, играющие роль низкочастотных и высокочастотных фильтров, соответственно. Один уровень преобразований можно записать с помощью формул 2 и 3:

$$y_{high}[k] = \sum_n x[n] * g[2k - n]; \quad (2)$$

$$y_{low}[k] = \sum_n x[n] * h[2k - n], \quad (3)$$

где  $y_{high}[k]$  и  $y_{low}[k]$  есть прореженные в два раза выходы высокочастотного и низкочастотного фильтров,  $x$  – вектор значений сигнала,  $g$  – вектор коэффициентов масштабирующей функции,  $h$  – вектор коэффициентов вейвлета.

В третьем разделе рассматриваются метрики, с помощью которых можно оценить требования к ЦВЗ аудиофайла и судить о его эффективности:

- 1) простой количественной характеристикой прозрачности является параметр SNR (Signal-to-Noise Ratio), определяющий отношение мощности исходного сигнала к мощности искажений, вызванных ЦВЗ;
- 2) параметр SDG (Subjective Difference Grade) является одним из наиболее используемых методов для выражения субъективной оценки качества звука при сравнении исследуемого сигнала с исходным. Этот тест необходим для оценки качества восприятия, поскольку окончательное решение принимается человеком и его системой восприятия;
- 3) устойчивость к атакам оценивают количеством ошибочно декодированных бит в единицу времени.

В последнем – четвертом подразделе были вычислены приведенные характеристики реализованных за научную работу по данной теме методов. Результаты представлены в таблице 1.

Таблица 1. Результаты исследования.

	Методы внедрения ЦВЗ						
	LSB	Изменение времени задержки эхосигнала	Метод расширения спектра	Хаара, простой метод	Хаара, сингулярный метод	Добеши, простой метод	Добеши, сингулярный метод
SNR	25,09	46,91	40,84	61,46	70,97	66,61	73,91
SDG	4,8	3,9	4,1	4,2	4,3	4,1	4,4
BER	12%	19%	16%	14%	12%	11%	13%

В четвертом разделе приводится пример работы программы, главное окно которой представлено на рисунке 2.

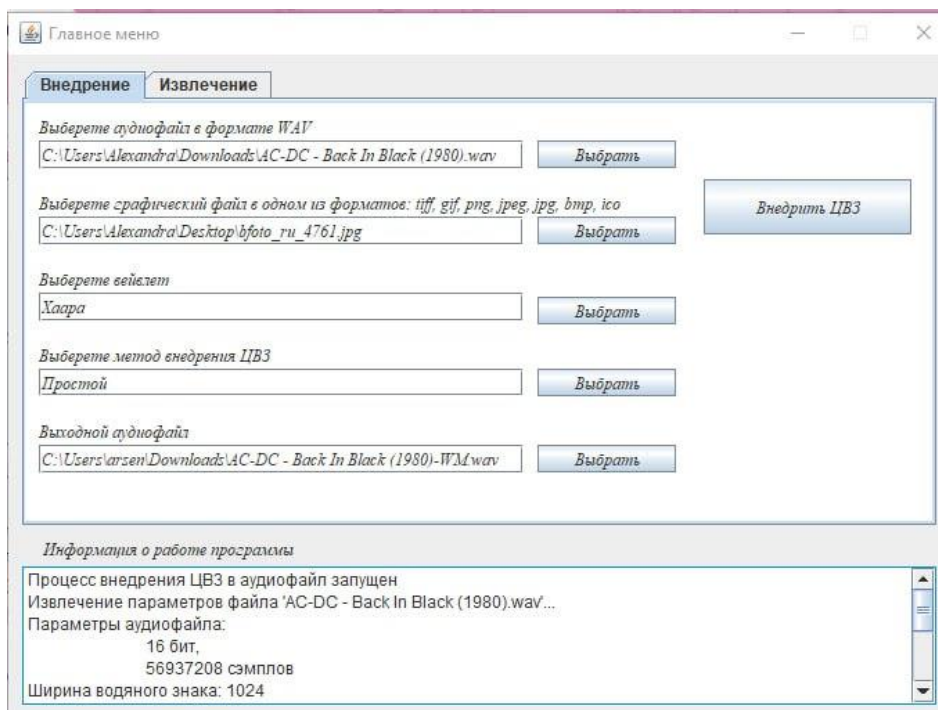


Рисунок 2 – Пример запуска программы в режиме внедрения

Показаны возможности программы внедрять, извлекать цифровой водяной знак, обрабатывать ошибки, логировать процесс выполнения.

В пятом разделе приведен обзор аналогов, описаны основные возможности, рассмотрены преимущества и недостатки, а также приведен пример работы различных плагинов программы FL Studio 20.

В шестой главе были рассмотрены типы атак на ЦВЗ, а также проведен анализ устойчивости ЦВЗ к воздействиям на контейнер.

Первая атака, направленная на уничтожение ЦВЗ: обрезка аудиофайла – это процесс изменения длительности аудиозаписи путем удаления ее части. Метод, использующий вейвлет-преобразования, не устойчив к данной атаке. Объяснением может служить то, что встраивание бит изображения в аудиодорожку происходит не последовательно и пропорционально (как в методе наименее значащих бит), а с разделением дорожки на поддиапазоны, как бы «перемешивая» последовательности бит. А также при извлечении необходимо знать ширину и высоту ЦВЗ, поэтому при обрезке видео эти



параметры становятся некорректными, так как часть изображения удалена. Поэтому восстановить изображение не представляется возможным.

Далее производили атаки с помощью фильтров низких и высоких частот. При небольших значениях ЦВЗ все еще различим, особенно в местах, где присутствует большое скопление пикселей черного цвета, а также на контрасте с более светлыми участками. При увеличении удаляемых частот ЦВЗ становится трудноразличимым, просматриваются очертания контрастных элементов на исходном изображении, но большая часть данных уничтожена.

Можно сделать вывод, что при атаке на аудиофайл с ЦВЗ частотными фильтрами, ЦВЗ может быть распознано в зависимости от величины отбрасываемых частот.

Следующая атака, которая была нанесена на контейнер: mp3-сжатие. Так как разработанная программа работает только с аудиофайлами формата WAV, проверить извлекаемость после mp3-сжатия нет возможности. Проведем следующий эксперимент: применим к аудиофайлу mp3-сжатие, затем переведем полученный файл вновь к формату WAV и попробуем извлечь ЦВЗ. По результатам исследования выяснили, что изображение извлекается с большим количеством шумов и маленькой детализацией, mp3-сжатие сильно воздействует на встроенный цифровой знак, но не разрушает его полностью.

## ЗАКЛЮЧЕНИЕ

Дипломная работа была посвящена теме цифровых водяных знаков, в которой были рассмотрены основные методы внедрения ЦВЗ в аудиофайлы. Был реализован метод, использующий вейвлет-преобразования Хаара и Добеши с простым подходом, а также с подходом, использующим сингулярное разложение.

Конечным результатом стала программа с пользовательским интерфейсом, позволяющая внедрять и извлекать графические файлы, используемые в роли ЦВЗ.

Также был проведен сравнительный анализ методов, используя как новые исследования и реализации, так и прошлые личные наработки по данной теме, что позволило широко охватить методы аудиостеганографии и сделать выводы относительно эффективности и устойчивости каждого из них.

Далее рассмотрели доступные на рынке аналоги разработанного ПО, привели примеры их работ, а также выделили преимущества личной разработки.

Провели анализ устойчивости ЦВЗ, внедренного с использованием вейвлетов, к популярным атакам.

Таким образом, задачи работы были выполнены, и цель достигнута.