

Министерство образования Республики
Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.056.5

Шахмуть Андрей Михайлович

Модифицирование частотных и временных характеристик речевого
сигнала для скрытой передачи сообщений

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты
информации. Информационная безопасность»

Научный руководитель

Петров Сергей Николаевич
кандидат технических наук,
доцент

Минск 2020

ВВЕДЕНИЕ

Целью магистерской диссертации является повышение эффективности методов скрытого внедрения информации в звуковые файлы посредством алгоритмов скрытой передачи информации и методов выявления несанкционированного скрытого вложения в звуковом файле.

С развитием интернет-сообщества мультимедийная передача подвергается различным типам атак, потому что эта передача произошла в общественных системах связи. Ежедневно тысячи мультимедийных файлов загружаются многими пользователями. Мультимедийные данные, такие как аудио, занимают огромное количество места для хранения, аудиофайлы считаются наиболее важным типом мультимедийных файлов, содержащих конфиденциальные данные. Одним из привлекательных решений для обеспечения безопасной передачи звука является стеганография, которая означает скрытие секретных данных в других данных без того, чтобы посторонние пользователи знали о существовании сообщения. Несколько типов исследований предложили различные алгоритмы для встраивания и извлечения сообщения в аудиофайл. Цифровая стеганография может использоваться и для криминальных целей. В связи с этим большую актуальность приобретает стегоанализ.

В настоящее время разрабатываются новые методы компьютерной стеганографии, основанные на особенностях представления информации в цифровом виде. Часть этих методов использует модификацию палитры, неточность устройств оцифровки, избыточность аудио и видео файлов и др. подходы.

Первый раздел данной работы посвящен основным понятиям и положениям стеганографии, а также дана классификация стеганографических атак. Второй раздел содержит подробный анализ существующих методов встраивания информации в пространственные области цифровых файлов. Третий раздел представляет обоснование выбора формата аудио файла. В четвертом разделе разработано приложение для стеганографического сокрытия данных в аудио файлах.

В результате проверки магистерской диссертации в системе «Антиплагиат» был получен результат в 75,56% оригинальности и 24,4% заимствований из различных источников, что эквивалентно использованию общепринятых определений, терминов и другой информации.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цели и задачи исследования

Цель магистерской диссертации - повышение эффективности методов скрытого внедрения информации в звуковые файлы с использованием алгоритмов скрытой передачи информации, а также выявление несанкционированного скрытого вложения в звуковом файле.

В соответствии с поставленной целью, в работе сформулированы и решены следующие основные задачи:

- изучить, проанализировать и систематизировать основные методы и положения цифровой стеганографии;
- рассмотреть особенности файловых форматов WAV;
- сформулировать стеганографический алгоритм, обеспечить его надежное функционирование;
- разработать программную реализацию разработанного алгоритма, с возможностью использования функций встраивания и извлечение данных через удобный пользовательский интерфейс.

Положения, выносимые на защиту

- метод внедрения информации в старшие разряды отсчета звукового файла формата WAV, позволяющий извлекать информацию из звукового файла при воздействии на него различных искажающих действий.
- программное обеспечение для сравнительного корреляционного анализа аудио-файлов и реализации метода LSB (наименьшего значащего бита).

Связь с приоритетными направлениями научных исследований и запросами реального сектора экономики

Тема диссертационной работы соответствует:

- п. 3.8 «Обеспечение цифрового доверия, защита информационных ресурсов и информационно-коммуникационной инфраструктуры» Стратегии развития информатизации в Республике Беларусь на 2016 – 2022 годы утвержденной на заседании Президиума Совета Министров от 03.11.2015 №26.

В диссертации исследована и решена актуальная задача по выбору оптимального стеганографического алгоритма и оценке его эффективности. Научную новизну содержат результаты исследования эффективности алгоритмов стеганографических преобразований. Практическая ценность

работы состоит в разработке приложения для анализа аудио-файлов на предмет наличия встроенной записи, а также реализующего стего-метод LSB.

Личный вклад соискателя

Содержание диссертации отображает личный вклад автора. Он заключается в разработке метода внедрения информации в старшие разряды отсчетов звукового файла, позволяющий извлекать информацию из звукового файла при воздействии на него различных искажений. Скрытность внедренной информации обеспечивается записью информации через определенный интервал отсчетов, который определяется с учетом психофизических особенностей слуховой системы человека.

Определение целей и задач исследований, интерпретация и обобщение полученных результатов проводились с научным руководителем, кандидатом технических наук, доцентом С.Н. Петровым.

Апробация результатов диссертации

Теоретические результаты диссертационных исследований представлены в виде тезисов на следующей научной конференции: XVIII Белорусско-российской научно – технической конференции «Технические средства защиты информации», Минск, 9 июня 2020 г.(стр. 83-84).

Практические результаты диссертационных исследований представлены в виде тезисов на следующей научной конференции: 56-ой конференции аспирантов, магистрантов и студентов БГУИР, Минск, 18 – 20 мая 2020 г.

Опубликованность результатов диссертации

По результатам исследований, представленных в диссертации, опубликованы 2 печатные работы в сборниках «Инфокоммуникации: 56-я конференция аспирантов, магистрантов и студентов», «ТСЗИ 2020».

Структура и объём диссертации

Диссертационная работа состоит из введения, общей характеристики работы, основной части из четырех разделов, заключения, списка использованных источников, списка собственных источников, трех приложений, графического материала. Полный объём диссертационной

работы составляет 54 страниц, включая 16 иллюстраций, 1 таблицу, список использованных источников из 26 наименований, список собственных источников из 2 наименований, три приложения объемом 11 страниц, графический материал из 17 слайдов презентации в формате А4.

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Введение содержит краткое описание работы и обоснование необходимости исследований.

В первом разделе рассмотрены основные понятия и положения стеганографии, исследованы принципы построения цифровых стеганосистем. Дана классификация применяемых методов стеганографических атак. Определена наиболее вероятная атака на методы используемые в данной работе.

Второй раздел содержит подробный анализ существующих методов встраивания информации в пространственные области цифровых файлов. Определен наиболее часто используемый метод встраивания информации в аудиофайлы является метод замены наименее значащих бит (LSB) цифровых файлов, который в дальнейшем использован в качестве используемого метода встраивания информации.

В третьем разделе представлено обоснование выбора формата аудио файла. Формат WAVE был выбран из тех соображений, что он идеально подходит для реализации алгоритма LSB в силу своей избыточности. Представлена структура WAVE файла.

В четвертом разделе представлены общие требования к реализации стеганографических методов для аудио файлов. Проведено тестирование существующего ПО, которое показало, что ни одно из них не соответствует изложенным выше требованиям к стеганографическим пакетам. Разработано программное обеспечение, назначением которого является внесение сокрытого сообщения в аудиофайл переменного размера методом LSB.

В заключении разработано приложение для стеганографического сокрытия данных в аудио файлах, которое отвечает всем требованиям, поставленным к стеганографическому программному обеспечению и может использоваться для сокрытия данных в аудио файлах.

ЗАКЛЮЧЕНИЕ

Рассмотрена проблема стеганографии и стегоанализа на аудио файлах и получены следующие результаты.

В ходе исследования разработано программное обеспечение, назначением которого является внесение сокрытого сообщения в аудиофайл переменного размера методом LSB. Также продукт должен проводить корреляционный анализ стего-файла и контейнера. Вышеуказанные функции реализованы с помощью пакета MATLAB R2018b с представлением данных в оконных формах Visual Studio.

На первом этапе были рассмотрены основные принципы работы стеганографической системы, детально рассмотрены особенности структуры аудио-файлов WAV, на предмет потенциальных мест для встраивания секретной информации, были описаны основные стеганографические методы, а также продемонстрированы общие принципы стеганографического анализа, сформулирован наиболее удачный стеганографический алгоритм. На основе выбранного метода были сформированы основные требования и ограничения к работе разрабатываемого приложения и составлен список предоставляемых функций, нарисован макет будущего приложения.

Разработано приложение для стеганографического сокрытия данных в аудио файлах формата WAVE с помощью метода LSB (Least Significant Bit, Наименьший Значащий Бит). Приложение поддерживает WAVE файлы любой битности, частоты дискретизации, определяет объем контейнера и реазует многотомность. Также реализован алгоритм извлечения скрытых данных. Шифрование данных перед сокрытием производится с помощью алгоритма XOR. Приложение отвечает всем требованиям, поставленным к стеганографическому программному обеспечению и может использоваться для сокрытия данных в аудио файлах формата WAVE.

СПИСОК СОБСТВЕННЫХ ПУБЛИКАЦИЙ

1–А. Шахмуть, А. М. Особенности применения аудиостеганографии для скрытой передачи информации / А. М. Шахмуть // Технические средства защиты информации : тезисы докладов XVIII Белорусско-российской научно – технической конференции, Минск, 9 июня 2020 г. / Белорусский государственный университет информатики и радиоэлектроники; редкол. : Т. В. Борботько [и др.]. – Минск, 2020.

2–А. Шахмуть, А. М. Приложение для сокрытия информации в аудиофайле методом замены наименьшего значащего бита (LSB) / А. М. Шахмуть, С. Н. Петров // Инфокоммуникации: 56-я конференция аспирантов, магистрантов и студентов, Минск, 18 – 20 мая 2020 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск, 2020.