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

Анализ эффективности алгоритмов внедрения цифровых водяных знаков в аудиофайлы

АВТОРЕФЕРАТ
дипломной работы

студентки 6 курса 631 группы
специальности 10.05.01 Компьютерная безопасность
факультета компьютерных наук и информационных технологий
Громовой Наталии Викторовны

Научный руководитель
доцент _____ И. Ю. Юрин
23.01.2020 г.

Заведующий кафедрой
д. ф.-м. н., доцент _____ М. Б. Абросимов
23.01.2020 г.

Саратов 2020

ВВЕДЕНИЕ

Развитие информационных технологий привело к широкому распространению цифровых фотографий, музыки и видео в различных форматах. Такое массовое использование вызывает большую обеспокоенность в отношении таких вопросов, как защита интеллектуальной собственности, контроль копирования и подтверждением права на обладание, поскольку большинство из произведений мультимедиа используются в сети Интернет с грубыми нарушениями действующего законодательства. Решение этих проблем – сложный и пока еще далекий от полного завершения процесс, а достижение удовлетворительных результатов возможно лишь с помощью целого комплекса мер и средств, правовых и технических. Среди технических средств защиты авторских прав на медиаданные особый интерес как наиболее перспективные представляют технологии применения средств стеганографии, а именно встраивание в данные цифровых водяных знаков (далее ЦВЗ) – особых цифровых меток, содержащих в себе информацию о владельце или авторе цифровой информации, которые не могут быть обнаружены и извлечены без дополнительного программного обеспечения.

Цифровой знак не искажает и не вносит существенных изменений в файлы, при этом сами данные со встроенным в них ЦВЗ оказываются общедоступными. В отличие от криптографических средств защиты, целью которых является ограничение доступа к данным неавторизованных пользователей, ЦВЗ позволяют иметь доступ к информации всем желающим, при этом в случае необходимости встроенный ЦВЗ позволяет определить ее владельца.

В настоящее время наблюдаются тенденция к применению подходов, использующих информацию о зрительной системе человека для создания более надежных водяных знаков. Такие методы используют информацию об ограниченности диапазона человеческого глаза.

По сравнению с водяными знаками для видео и изображений, водяные знаки в аудио создают особую проблему, потому что слуховая система человека намного чувствительнее, чем зрительная.

Большинство методов встраивания ЦВЗ в аудиосигналы основываются на использовании особенностей слуховой системы человека, которая различает изменение фазы сигнала слабее, чем изменение его амплитуды и частоты, а также является чувствительной к аддитивному белому шуму.

На сегодняшний день существует большое количество способов внедрения водяных знаков в аудиофайлы. При этом каждый метод имеет отличные от других уровни надёжности, спецификации и недостатки.

Целью настоящей работы является разработка программы, реализующей алгоритмы внедрения водяных знаков в аудиофайлы, а также анализ эффективности этих методов.

В ходе работы необходимо решить следующие задачи:

1. ознакомиться с основными направлениями цифровой стеганографии;

2. изучить существующие методы внедрения ЦВЗ в аудиофайлы;

3. осуществить программную реализацию основных методов;

4. проанализировать данные, полученные с помощью программы, и оценить эффективность выбранных методов.

Дипломная работа состоит из введения, 6 разделов, заключения, списка использованных источников и 2 приложений. Общий объем работы – 70 страниц, из них 45 страниц – основное содержание, включая 28 рисунков и 2 таблицы, список использованных источников из 24 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первая глава содержит основные понятия, используемые в работе, такие как: стеганографическая система, контейнер, встраиваемое сообщение, стеганографическим преобразование, стеганографическая стойкость. Описываются основные положения и принципы компьютерной стеганографии. Во второй части описывается, какими могут быть ЦВЗ и в каких областях сейчас применяются водяные знаки, а именно: для защиты авторских прав, обнаружении подделок, мониторинга трансляций, передачи скрытых данных и контроля доступа. В третьей части первой главы описывается, почему аудиосигнал является удачным решением при выборе контейнера для встраивания ЦВЗ.

Вторая глава посвящена методам внедрения водяных знаков в аудио: методу внедрения сообщения в наименее значащие биты, методу внедрения с расширением спектра и с использованием эхо-сигнала. Для каждого из методов описывается основная идея и принцип работы алгоритма.

Третья глава посвящена возможным атакам на ЦВЗ: атаки направленные на удаление водяных знаков и используемые против текущего протокола, геометрические атаки и криптографические атаки. Также описаны возможные виды злоумышленников на основе знаний об используемой системе водяных знаков.

Четвертая глава описывает современное ПО, которое позволяет внедрять ЦВЗ в аудиофайлы. Проанализированы основные достоинства и недостатки каждой технологии.

Пятая глава содержит данные о разработанном программном продукте, который позволяет внедрять и извлекать ЦВЗ из аудиофайлов. Здесь же указаны рекомендации по использованию программы и приведены результаты работы для всех описанных алгоритмов.

Шестая глава содержит исследование эффективности реализованных методов. Для оценки эффективности использовались следующие метрики: отношение сигнал/шум, объективная и субъективные оценки качества звука и интенсивность битовых ошибок. В главе кратко описываются используемые метрики и приводятся результаты оценки каждого из методов по указанным критериям. Для каждого из методов приведено сравнение частотных и амплитудных характеристик пустого и заполненного контейнеров, посчитаны необходимые показатели робастности и прозрачности водяного знака. Выбранные алгоритмы имеют отличные показатели скрытности и устойчивости к преобразованию. Исходя из результатов исследования, самым эффективным можно считать метод расширения спектра. Этот алгоритм имеет хорошие показатели помехоустойчивости, прозрачности и минимизации искажения. Если же основным критерием выбора метода внедрения водяного знака является скорость внедрения, то для такой задачи лучше всего подходит метод наименее значащих битов. Метод внедрения с использованием эхо-сигнала работает дольше остальных методов, но если требуется внедрить небольшое по объему сообщение и к аудиосигналу не будет применяться сжатие, то этот метод лучше всего сохранит водяной знак.

ЗАКЛЮЧЕНИЕ

Технологии внедрения ЦВЗ активно используются в индустрии звукозаписи, в крупных онлайн платформах по продаже музыкальных альбомов и записи на blu-ray диски.

Круг задач защиты авторского права, решаемых с помощью ЦВЗ, постоянно расширяется. Так, появились алгоритмы встраивания ЦВЗ в Интернет-радиовещании. Крупные производители программного обеспечения начинают предоставлять свои продукты с возможностями встраивания в аудиофайлы ЦВЗ для решения проблем, связанных с пиратством.

Несмотря на появление новых способов внедрения, основные методы, которые были рассмотренные в работе, являются наиболее используемыми на сегодняшний день.

В ходе работы были рассмотрены три метода внедрения ЦВЗ в аудиофайлы – внедрение с помощью НЗБ, внедрения с помощью процедуры расширения спектра и внедрение с помощью эхо-сигналов. Методы были реализованы программно, дополнительно для каждого из алгоритмов отображается график аудиосигнала до и после внедрения ЦВЗ. В ходе процесса исследования полученных данных, для каждого из методов внедрения были выявлены свои плюсы и минусы.

Так, в методе расширения спектра для извлечения водяного знака необходимо иметь исходный контейнер, в отличие от метода НЗБ и эхо-метода. Внедрение с помощью эхо-сигнала показывает низкие показатели по прозрачности как при просмотре осциллограммы аудиофайла, так и при его прослушивании. Метод НЗБ является простым и удобным способом внедрить данные в аудио, но имеет слабую устойчивость к посторонним воздействиям на сигнал.

Для всех методов были подсчитаны требуемые оценки прозрачности и устойчивости к искажениям. Исходя из полученных результатов, внедрение с

помощью расширения спектра является наиболее результативным и эффективным методом внедрения. Однако стоит учитывать критерии выбора метода – если файл будет подвержен сжатию, то для этой задачи лучше использовать эхо-метод, если нужен быстрый способ передачи информации, при этом сам файл не будет подвержен искажениями, то можно использовать метод НЗБ.

Результатом практической работы является программный продукт, реализующий выбранные методы внедрения и извлечения ЦВЗ, а так же анализ эффективности этих методов. Таким образом, поставленные задачи выполнены полностью, цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Столов, Е. Л. Цифровая обработка сигналов. Водяные знаки в аудиофайлах. Учебное пособие / Е. Л. Столов. – Санкт-Петербург: Лань, 2018. — 176 с. — ISBN 978-5-8114-3014-7.
2. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н.Оков, И. В.Туринцев. – М.:Солон-Пресс, 2002. – 272 с.
3. Конахович, Г. Ф. Компьютерная стеганография Теория и практика / Г. Ф Конахович, А. Ю. Пузыренко. – К.: МК-Пресс, 2006 – 288 с.
4. Радзищевский, А. Ю. Основы аналогового и цифрового звука / А. Ю. Радзищевский. – М.: Издательский дом «Вильямс», 2006 – 298 с. – ISBN 5-8459-1002-1.
5. Коробейников, А. Г. Встраивание цифровых водяных знаков в аудиосигнал методом расширения спектра [Электронный ресурс] / А. Г. Коробейников Журнал «Научно-технический вестник» // [Электронный ресурс] – научно-популярный журнал, открытый доступ. URL: http://ntv.ifmo.ru/file/article/52.pdf (дата обращения: 17.08.2019).- Загл. с экрана.- Яз. рус.
6. Аграновский, А. В. Стеганография, ЦВЗ и стеганоанализ / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин, С. А. Сапожников. – М.: Вузовская книга, 2009. – 217 с.
7. Абазина, Е. С. Цифровая стеганография: состояние и перспективы [Электронный ресурс] – научно-популярная статья, открытый доступ. URL: https://cyberleninka.ru/article/v/tsifrovaya-steganografiya-sostoyanie-i-perspektivy (дата обращения 01.08.2019).- Загл. с экрана.- Яз. рус.
8. Генне, О. В. Основные положения стеганографии [Электронный ресурс] – научно-популярная статья, открытый доступ. URL: http://citforum.ru/internet /securities/stegano.shtml (дата обращения 01.08.2019).- Загл. с экрана.- Яз. рус.

9. Структурная схема и математическая модель типичной стеганосистемы [Электронный ресурс] – научно-популярная статья, открытый доступ. URL: https://helpiks.org/6-82903.html (дата обращения 01.08.2019).- Загл. с экрана.- Яз. рус.

10. Демидова, М. И. ЦВЗ как способ защиты произведений мультимедиа [Электронный ресурс] – научно-популярная статья, открытый доступ. URL: https://elibrary.ru/item.asp?id=17949326& (дата обращения 01.08.2019).- Загл. с экрана.- Яз. рус.

11. Волосатова, Т. М. Методика стеганоанализа аудиофайлов [Электронный ресурс] / Т.М. Волосатова, Н. В. Чичварин // Современные тенденции развития науки и технологий [Электронный ресурс] – научно-популярный журнал, открытый доступ.URL: https://elibrary.ru/item.asp?id=26600010 (дата обращения: 17.08.2019).- Загл. с экрана.- Яз. рус.

12. Федосеев, В. А. Компьютерная стеганография / В. А. Федосеев. Электрон. учеб.-метод. комплекс по дисциплине в LMS Moodle / Мин-во образования и науки РФ, Самар. гос. аэрокосм. ун-т им. С. П. Королева (нац. исслед. ун-т); авт.- сост. В. А. Федосеев. - Электрон. текстовые и граф. дан. - Самара, 2013 – 170 с.

13. AG Watermark Generator [Электронный ресурс] – сервис для внедрения водяных знаков. URL: https://watermark.agsoundtrax.com (дата обращения: 02.09.2019).- Загл. с экрана.- Яз. англ.

14. AudioWatermarking.info [Электронный ресурс] – сервис для внедрения водяных знаков. URL: http://audiowatermarking.info/awt2_main.php (дата обращения: 03.09.2019).- Загл. с экрана.- Яз. англ.

15. Watermark Embedding for Audio Signals. [Электронный ресурс] – сервис для внедрения водяных знаков. URL: http://www.musictrace.de/products/contentmark. en.htm (дата обращения: 03.09.2019).- Загл. с экрана.- Яз. англ.

16. Гончаренко, М.В. Проблема защиты авторских прав на аудио и видеоданные с помощью цифровых водяных знаков [Электронный ресурс] / М. В. Гончаренко, В. Г. Иваненко // Безопасность информационных технологий [Электронный ресурс] – научно-популярный журнал, открытый доступ. URL:https://bit.mephi.ru/index.php/bit/article/view/932/922 (дата обращения: 30.10.2019).- Загл. с экрана.- Яз. рус

17. Tanha, M. An overview of attacks against digital watermarking and their respective countermeasures [Электронный ресурс] – научно популярная статья, открытый доступ. URL: https://www.researchgate.net/publication/261160176_An_overview_of_attacks_against_digital_watermarking_and_their_respective_countermeasures (дата обращения: 15.10.2019).- Загл. с экрана.- Яз. англ.

18. Trustedaudio [Электронный ресурс] – онлайн сервис для внедрения водяных знаков. URL: https://www.trustedaudio.com (дата обращения: 15.10.2019).- Загл. с экрана.- Яз. англ.

19. Лутц, М. Изучаем Python / М. Лутц. – Пер. с англ. – Спб.: Символ-Плюс, 2011. –1280 с.

20. Dhar, P. Advances in Audio Watermarking Based on Singular Value Decomposition [Электронный ресурс] / P. K. Dhar, T. Shimamur // Online overwiew on the book [Электронный ресурс] – глава электронной книги, открытый доступ. URL: https://books.google.ru/books?id=E9a9BwAAQBAJ (дата обращения: 25.12.2019).- Загл. с экрана.- Яз. англ.

21. Аудио watermark для приложений Second Screen [Электронный ресурс] – научно-популярная статья, открытый доступ. URL: https://habr.com/ru/post/254379/ (дата обращения 23.12.2019).- Загл. с экрана.- Яз. рус.

22. Алексеев А.П. Скрытая передача данных в звуковых файлах формата WAV [Электронный ресурс] – научно-популярная статья, открытый доступ. URL: https://elibrary.ru/item.asp?id=15279844 (дата обращения 23.12.2019). - Загл. с экрана.- Яз. рус.

23. Dhar, P. Advances in Audio Watermarking Based on Matrix Decomposition [Электронный ресурс] / P. K. Dhar, T. Shimamur // Online overwiew on the book [Электронный ресурс] – глава электронной книги, открытый доступ. URL: https://books.google.ru/books?id=MXWUDwAAQBAJ (дата обращения: 12.01.2020).- Загл. с экрана.- Яз. англ.

24. Lu, C. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property [Электронный ресурс] / Chun-Shien Lu // Online book [Электронный ресурс] – электронная книга, открытый доступ. URL: https://books.google.ru/books?id=PF_U_x1TajUC&pg (дата обращения: 12.01.2020).- Загл. с экрана.- Яз. англ.