

Министерство образования и науки Российской Федерации

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

Азизовой Виктории Роберт

Научный руководитель

доцент, к.п.н.

А.С. Гераськин

18.01.2018 г.

Заведующий кафедрой

профессор, к.ф.-м.н.

В.Н. Салий

18.01.2018 г.

Саратов 2018

ВВЕДЕНИЕ

В современном информационном обществе проблема контроля использования прав собственности на цифровые ресурсы становится все более актуальной, поскольку использование цифровых форматов мультимедиа стало повсеместным. Одним из наиболее эффективных способов решения этой проблемы является использование методов стеганографии, т.е. встраивания в мультимедийные данные так называемых цифровых водяных знаков (ЦВЗ) – цифровых меток, не видимых без специального программного обеспечения и секретного ключа.

ЦВЗ применяется в кодировании, декодировании акустической информации, в уникализации и индивидуализации звуковых треков, в технологиях поиска и определения незаконных копий аудиоматериалов.

Целью работы является разработка программного продукта, осуществляющего внедрение цифровых водяных знаков в аудиофайл различными алгоритмами и оценка их эффективности. Для достижения этой цели необходимо поставить следующие задачи:

1. Проанализировать имеющиеся методы внедрения цифровых водяных знаков в аудиосигнал.
2. Выделить в результате анализа литературных источников наиболее эффективные из них.
3. Осуществить программную реализацию этих методов.

Дипломная работа состоит из введения, 5 разделов, заключения, списка использованных источников и приложения. Общий объем работы – 90 страниц, из них 40 страниц – основное содержание, включая 27 рисунков и таблицу, список использованных источников из 20 наименований.

КРАТКОЕ СОДЕРЖАНИЕ

Первая глава содержит основные понятия и определения, которые встречаются в работе, в том числе понятие цифрового водяного знака и основные его свойства. Вторая часть данной главы посвящена областям применения ЦВЗ, среди которых: защита авторских прав, доказательство обладания, аутентификация и обнаружение подделок, контроль копирования и доступа, создание отпечатка и мониторинг трансляций.

Во второй главе рассказывается об использовании преобразования Фурье, дискретного косинусного преобразования и вейвлет-преобразования для внедрения данных в аудиосигнал. У каждого из этих преобразований есть свои достоинства и недостатки. Преобразование Фурье заменяет коэффициенты высоких частот на информацию о водяном знаке. Высокие частоты не воспринимаются человеком, что гарантирует неразличимость ЦВЗ. Дискретное косинусное преобразование выражает энергию сигнала в небольшом количестве коэффициентов, что позволяет минимизировать искажения при внедрении водяного знака в контейнер. Оба эти преобразования имеют существенный недостаток – низкая устойчивость к атакам. Вейвлет-преобразование раскладывает сигнал на несколько частотных поддиапазонов. При вейвлет-преобразовании искажения, вносимые в аудиофайл, несколько выше, чем при других преобразованиях, но вычисляется за линейное время и хорошо противостоит атакам.

Далее рассматриваются методы, использующие перечисленные преобразования, а именно: метод внедрения ЦВЗ на основе статистических характеристик вейвлет-коэффициентов, метод расширения спектра и метод, основанный на добавлении эхо-сигналов. Для каждого из методов приводятся алгоритм внедрения и описывается общий принцип работы алгоритма.

Третья глава посвящена атакам на системы цифровых водяных знаков. Атаки разделены на категории и подробно описаны. Так же рассматривается устойчивость некоторых алгоритмов к конкретным типам атак.

В четвертой главе рассматривается интерфейс реализованной программы, доступные функции и возможные ошибки, возникающие при неправильном использовании программы. Так же указаны рекомендации по использованию программы и приведены результаты работы на тестовом примере для всех реализованных алгоритмов.

Пятая глава содержит исследование эффективности реализованных методов. Для оценки эффективности нами были выделены такие критерии, как отношение сигнал/шум, объективная оценка различия и вероятность ошибки на бит. В этой главе приводятся результаты оценки каждого из методов по указанным критериям в виде таблицы. Так же для наглядности приведено сравнение частотных и амплитудных характеристик пустого и заполненного контейнеров для каждого из методов. Для каждого из методов были посчитаны необходимые показатели стойкости и прозрачности водяного знака. Выбранные алгоритмы имеют отличные показатели скрытности и устойчивости к преобразованию. По результатам исследования, самым эффективным можно считать метод на основе вейвлет-преобразований. Данный алгоритм является не только самым стойким к атакам, но и вычисляется за линейное время. Однако, если главным критерием выбора метода внедрения водяного знака является минимизация искажений, то для такой задачи лучше всего подходит метод расширения спектра. Эхо-метод требует значительных вычислительных затрат, но если требуется извлечь водяной знак без контейнера-оригинала, то эти затраты вполне оправданны.

ЗАКЛЮЧЕНИЕ

В работе были изучены и проанализированы различные методы внедрения цифрового водяного знака в аудиосигнал. В результате анализа литературных источников были выбраны наиболее эффективные из методов для реализации программы, осуществляющей внедрение и извлечение цифровых водяных знаков в аудиосигнале.

В ходе производственной практики были реализованы три метода: внедрение цифровых водяных знаков на основе статистических характеристик вейвлет-коэффициентов, метод расширения спектра и метод, основанный на изменении задержки эхо-сигнала. Реализованные методы были протестированы и успешно прошли все тесты. По итогам исследования было установлено, что каждый из методов обладает как преимуществами, так и недостатками. Например, вейвлет и метод расширения спектра могут извлечь цифровой водяной знак только при наличии пустого контейнера, в отличие от эхо-метода. При извлечении из аудиосигнала лучше всех сохраняется водяной знак, внедренный методом расширения спектра, а хуже всех тот, что был внедрен эхо-методом. Главное преимущество методов встраивания данных с помощью вейвлет-преобразований – это скорость.

Результатом работы является программа, реализующая изученные методы внедрения цифровых водяных знаков, а так же анализ эффективности этих методов. Программа имеет графический интерфейс и позволяет пользователю самостоятельно выбирать метод внедрения. Таким образом все поставленные задачи были решены, цель работы достигнута.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Борисенко, Б.Б. Математические методы стеганографии [Электронный ресурс]/ Б.Б. Борисенко // Журнал института проблем информационной безопасности МГУ. 2010. №2(8). — 43 с. — URL: <http://journals.tsu.ru/uploads/import/437/files/08-042.pdf> (дата обращения: 3.09.2017).
2. Грибунин, В.Г. Цифровая стеганография [Электронный ресурс]/ В.Г. Грибунин, И.Н.Оков, И.В.Туринцев. — М.:Солон-Пресс, 2002. — 272 с. — URL:http://bezopasnik.org/article/book/gribunin_cifir_stenograf_2009.djvu (дата обращения: 3.09.2017).
3. Сергиенко, А. Б. Цифровая обработка сигналов [Электронный ресурс]/А. Б. Сергиенко — 2-е изд. — СПб.: Питер, 2006. — С. 751. — URL: http://www.rphf.spbstu.ru/dsp/lib/Sergijenko_2003.pdf (дата обращения: 8.10.2017).
4. Arnold, M. Audio watermarking: features, applications and algorithms [Электронный ресурс] // Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference — 2000. — URL: <http://ieeexplore.ieee.org/document/871531> (дата обращения 07.10.2017).
5. Дремин, И. М. Вейвлеты и их использование [Электронный ресурс] / И. М. Дремин, О. В. Иванов, В. А. Нечитайло. // Успехи физических наук. — май 2001. — том 171, №5. — с. 465-501. — URL: <http://mathnet.ru/links/7725ed065cab28add91f97b62da797e1/ufn1876.pdf> (дата обращения: 04.09.2017).
6. Поликар, Р. Введение в вейвлет-преобразование [Электронный ресурс] / Р. Поликар. — СПб.: АВТЭКС, 2006. — 59 с. — URL: http://files.libedu.ru/hjemj2jx83c188pkppo9c4ndd9cv8pgu/polikar_r__vvedenie_v_veivlet-preobrazovanie.pdf (дата обращения: 10.09.2017).
7. Fallahpour, M. High capacity audio watermarking using the high frequency band of the wavelet domain [Электронный ресурс] / M. Fallahpour, D. Megias // Multimedia Tools and Applications. — Volume 52, Issue 2-3, April 2011. — Pages

URL:http://in3.uoc.edu/opencms_in3/export/sites/in3/webs/grups_de_recerca/Kison/_resources/documents/J3.pdf (дата обращения: 11.10.2017).

8. Скляр, Б. Цифровая связь [Электронный ресурс] / Б. Скляр. – Теоретические основы и практическое применение. – 2-е изд., исправл. – М.: Вильямс, 2003. – 1104 с. – URL: http://www.rphf.spbstu.ru/dsp/lib/Sklar_Dig_Com_2003.pdf (дата обращения: 10.10.2017).

9. Коробейников, А.Г. Встраивание цифровых водяных знаков в аудиосигнал методом расширения спектра. [Электронный ресурс] / А.Г. Коробейников, А.Г. Даурских, Н. В. Павлова // Научно-технический вестник., 2009, №1(59), – URL: <http://ntv.ifmo.ru/file/article/52.pdf> (дата обращения: 17.09.2017).

10. Костина, А. В. Эхо-метод сокрытия информации в аудиофайле [Электронный ресурс] / А. В. Костина, А.Ю. Кунац, В.Г. Миснякин, М. А. Стельмах, СпбГЭУ– URL: <https://priem.etu.ru/api/open/nnb/stand-file?id=29363> (дата обращения: 30.10.2017)

11. Барсуков, В.С. Компьютерная стеганография вчера, сегодня, завтра [Электронный ресурс] / В.С. Барсуков, А.П. Романцов // Специальная техника. - 1998. - № 4,5. – 19-26с – URL: http://www.ess.ru/sites/default/files/files/articles/1998/0405/1998_0405_03.pdf (дата обращения 3.09.2017).

12. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика [Электронный ресурс]/ Г.Ф. Конахович, А.Ю. Пузыренко. – М.:МК-Пресс, 2006. – 288 с – URL: http://read.in.ua/pub2G_1/ftp1/pub3/2011.08_ihtik_nauka-tehnika/2011.08_ihtik_nauka-tehnika_1392.rar.

13. Аграновский, А. В. Стеганография, цифровые водяные знаки и стеганоанализ [Электронный ресурс] / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин, С. А. Сапожников. – М.: Вузовская книга, 2009. – 217 с. – URL: <http://nashol.com/2014072179059/steganografiya-cifrovie-vodyanie-znaki-i->

steganoanaliz-monografiya-agranovskii-a-v-balakin-a-v-gribunin-v-g-sapojnikov-s-a-2009.html (дата обращения: 07.10.2017).

14. Bender, W. Techniques for Data Hiding [Электронный ресурс] / W. Bender, D. Gruhl, N. Morimoto, // IBM Systems Journal. – 1996. – № 35 (3 & 4). – P. 313–336. – URL: <http://ieeexplore.ieee.org/document/5387237/> (дата обращения: 17.12.2017).

15. BER Bit Error Rate Tutorial and Definition [Электронный ресурс] : [сайт] URL: <http://www.radio-electronics.com/info/rf-technology-design/ber/bit-error-rate-tutorial-definition.php> (дата обращения: 10.01.2018). Загл. С экрана. Яз. англ.

16. Scholarpedia [Электронный ресурс] : [сайт] URL: http://www.scholarpedia.org/article/Signal-to-noise_ratio (дата обращения: 10.01.2018). Загл. С экрана. Яз. англ.

17. AudioWatermarking.info [Электронный ресурс] : [сайт] URL: http://audiowatermarking.info/awt1_main.php (дата обращения: 10.01.2018). Загл. С экрана. Яз. англ.

18. AudioWatermarking.info [Электронный ресурс] : [сайт] URL: http://audiowatermarking.info/awt2_main.php (дата обращения: 10.01.2018). Загл. С экрана. Яз. англ.

19. AG Watermark Generator [Электронный ресурс] : [сайт] URL: <https://watermark.agsoundtrax.com> (дата обращения: 5.01.2018) . Загл. С экрана. Яз. англ.

20. Watermark Embedding for Audio Signals [Электронный ресурс] : [сайт] URL: <http://www.musictrace.de/products/contentmark.en.htm> (дата обращения: 9.01.2018) . Загл. С экрана. Яз. англ.