

Алгоритмы сокрытия и извлечения информации в аудио-файлах

П.О. Волков
НИУ Высшая школа экономики
Москва, Россия
povolkov@miem.hse.ru

Аннотация—В работе рассмотрено два вида аудио-файлов, а именно: WAV, который является несжатым звуковым файлом, и MP3, полученный в результате сжатия аудиоинформации. В соответствии с их свойствами были разработаны алгоритмы сокрытия и извлечения информации.

Ключевые слова— цифровая стеганография, аудио-файлы, WAV-файлы, MP3-файлы.

1. ВВЕДЕНИЕ

Задача защиты информации от несанкционированного доступа решалась во все времена. С давних времен выделяется два пути решения данной задачи: криптография [1] и стеганография [2]. Целью криптографии является скрывание содержимого сообщений за счет их шифрования. В отличие от этого, при стеганографии (с греческого переводится как «тайнопись») скрывается сам факт существования тайного сообщения. Другими словами, скрываемое сообщение встраивается в некоторый не привлекающий внимание объект., а далее данный объект открыто отправляется адресату. Области применения стеганографии различны:

- защита от копирования;
- аутентификация;
- скрытая аннотация документов;
- скрытая связь.

Бурное развитие вычислительной техники и каналов передачи данных инициировало развитие нового направления сокрытия информации- цифровой стеганографии. В основе методов этого направления лежат особенности цифрового представления данных. Таким образом, цифровая стеганография – это наука о незаметном и надежном (или устойчивом к различного рода искажениям) скрывании одних битовых последовательностей в других, имеющих аналоговую природу.

Скрываемая информация внедряется в соответствии с ключом в те отсчеты, искажение которых не приводит к существенным искажениям контейнера. Эти биты образуют стегопуть.

В работе рассмотрен вопрос сокрытия информации в аудио-файлах. Данная проблема выбрана по той причине, что большинство контейнеров выбирают в качестве изображения. В данной работе рассмотрено 2 вида аудио-файла: WAV, который является несжатым звуковым файлом, и MP3, полученный в результате сжатия аудиоинформации. В соответствии с их свойствами был

разработан алгоритм сокрытия и извлечения информации.

2. СТРУКТУРА WAV-ФАЙЛА

Файлы WAV (или WAVE) были созданы компанией IBM и Microsoft [3]. Они содержат различные аудиоданные - звуки, звуковые эффекты, музыку, а также записи голоса. Файлы WAV значительно больше файлов MP3, поэтому они не пользуются популярностью. Отличительная черта файлов WAV - их технология сжатия звука без потерь. Полученные файлы отличаются высоким качеством. Отправка и загрузка таких файлов требует много времени и дискового пространства.

Отметим, что WAV-файлы используют универсальный RIFF формат (Resource Interchange File Format - формат файла для обмена ресурсами).

WAV-файл представляет собой две четко делящиеся области: заголовок файла и область данных. В заголовке файла хранится информация о:

- размере файла;
- количестве каналов;
- частоте дискретизации;
- количестве бит в сэмпле (глубине звучания), и т.д.

3. СТРУКТУРА MP3-ФАЙЛА

MP3 (или MPEG Layer3)- это один из потоковых форматов хранения и передачи аудио-сигнала в цифровой форме [4], [5]. В формате MP3 применяется алгоритм сжатия с потерями, разработанный для существенного уменьшения размера данных, необходимых для воспроизведения записи и обеспечения качества воспроизведения звука, близкого к оригинальному. В отличие от MP3-файла, WAV-файлу присуще несжатый объем данных.

MP3-файл, также как и WAV-файл, состоит из заголовка и области данных. Но заголовок MP3 не представляет такую важность, как заголовок WAV, вместо этого есть заголовок у каждого фрейма.

Фрейм- это условная часть аудио-данных. MP3-файл представляет последовательность фреймов, каждый из которых состоит из заголовка, служебной информации и данных. В 4-байтовом заголовке фрейма хранится информация о:

- частоте семплирования;
- битрейте;
- режиме стерео, и т.д.

4. АЛГОРИТМ СОКРЫТИЯ ИНФОРМАЦИИ В WAV-ФАЙЛАХ

Как было сказано ранее, область данных WAV-файла состоит из отсчетов. Изменив младший бит отсчета или даже удалив, человек не почувствует разницу между аудио-файлом с искаженным младшим битом и оригинальным аудио-файлом. В этом и состоит свойство каждого отсчета файла. Применяв данное свойство, можно будет незаметно и хитро скрыть информацию.

Алгоритм сокрытия информации в WAV-файлах представлен в следующих шагах:

1. Скрываемое сообщение посимвольно разделить.
2. Каждый символ, характеризующийся числовым значением в диапазоне 1-255, переводится в биты с помощью стандартного преобразования из десятичного числа в двоичное.
3. Каждый бит встроить в младший бит отсчета.

Этот алгоритм характеризуется следующими свойствами:

- незаметностью при прослушивании;
- сложностью обнаружения стегоаналитическими методами;
- высокой сложностью реализации и медленной работой.

Чтобы алгоритм сделать более надежным, можно биты скрываемого сообщения встраивать не в каждый младший бит отсчета аудио-сигнала, а в бит такого отсчета, номер которого подчиняется некоторому закону.

Извлечение информации происходит в обратном порядке. При этом учитывается количество символов скрываемого сообщения.

5. АЛГОРИТМ СОКРЫТИЯ ИНФОРМАЦИИ В MP3-ФАЙЛАХ

В силу того, что данные MP3-файла представляют сжатый вид (свободного места нет), алгоритм сокрытия информации в данном формате является затруднительной процедурой. Однако способы имеются: широкополосное кодирование, фазовое кодирование, замена шума [6], [7]. Общими характеристиками данных методов являются возможная заметность при прослушивании, пропускная способность порядка 40 бит в секунду и средняя скорость работы/сложность реализации. Так как методы вносят неестественные искажения в сигнал (белый шум определенной амплитуды, дискретные фазы сигнала и т.д.), вероятно создание надежных алгоритмов их обнаружения. Кроме того, указанные методы были разработаны применительно к процедурам обычного сжатия информации и не учитывали особенностей MP3 преобразований. Неопытные программисты кодируют сообщение в служебной информации MP3. Метод сокрытия информации, речь о котором пойдет далее, превосходит предыдущие способы сокрытия.

Как отмечалось, MP3-файл представляет последовательность фреймов. В заголовке файла содержится информация о скорости считывания данных (битрейт). Изменяя скорость считывания, можно увеличить размер области для аудио данных сверх

области, занимаемой полезной информацией контейнера (например, музыкой). Величина этой области данных файла-контейнера и ее смещение относительно заголовка определяется служебной информацией (СИ). Поскольку СИ не изменяется в процессе встраивания скрываемых данных, то эти данные не будут воспроизводиться в процессе проигрывания диска. Таким образом, MP3-файл будет выглядеть как на Рис. 1.



Рис. 1. MP3-файл со скрытыми данными

Алгоритм сокрытия информации в MP3 будет выглядеть следующим образом:

1. Увеличить параметр скорости (rate), находящийся в заголовке каждого фрейма. Вследствие чего увеличивается размер области данных.
2. В освободившееся место встроить сообщение.

Данный алгоритм обладает следующими преимуществами:

- абсолютной незаметностью при прослушивании;
- высокой пропускной способностью, порядка 20% от объема контейнера;
- высокой скоростью работы;
- простой схемной реализацией.

Процедура извлечения выполняется в обратном порядке.

6. ЗАКЛЮЧЕНИЕ

Информационная безопасность стала неотъемлемой частью современной системы связи. Основная задача информационной безопасности - защита целостности, доступности и конфиденциальности данных. Стеганография и криптография - это два направления цифровой безопасности, где стеганография скрывает сам факт существования сообщения, а криптография использует шифрование, чтобы сделать сообщение непонятным. Примером цифровой стеганографии является сокрытие и извлечение информации в аудио-файлах.

В данной работе представлено 2 алгоритма сокрытия информации в аудио-файлах. В первом алгоритме в качестве контейнера был выбран файл с разрешением WAV. Второй алгоритм реализует сокрытие данных в MP3. По итогу был разработан интерфейс пользователя на языке C++ в среде Visual Studio CLR Windows Forms, который позволяет выполнять работу по сокрытию

данных практически любому неподготовленному пользователю.

ЛИТЕРАТУРА

- [1] Введение в криптографию [Электронный ресурс]. – Режим доступа: https://www.rulit.me/data/programs/resources/pdf/Vvedenie-v-kriptografiyu_RuLit_Me_661516.pdf.
- [2] Гребенников, В.В. История Криптологии & Секретной Связи: глава 6.1, вступление в историю стеганографии / В.В. Гребенников, 2012 [Электронный ресурс]. – Режим доступа: <http://cryptohistory.ru/book/chast-6-istoriya-steganografii/61-vstuplenie/>.
- [3] Структура WAV-файла [Электронный ресурс]. – Режим доступа: <https://audiocoding.ru/articles/2008-05-22-wav-file-structure/>.
- [4] Структура MP3-файла [Электронный ресурс]. – Режим доступа: <https://audiocoding.ru/articles/2008-05-22-mp3-file-structure/>.
- [5] Структура MP3-файла [Электронный ресурс]. – Режим доступа: <https://ru.wikipedia.org/wiki/MP3>.
- [6] Кокорин, П.П. О методах стегоанализа в аудиофайлах / П.П. Кокорин // Труды СПИИРАН. – 2007. – № 4. – С. 239-246.
- [7] Забелин, М.А. Стегоанализ аудиоданных на основе методов сжатия / М.А. Забелин // Вестник СибГУТИ. – 2010. – № 1. – С. 41-46.