УДК 004.056.55+681.8

Н.В. Попеня, асп.; Д.М. Романенко, зав. кафедрой
(БГТУ, г. Минск)

ВНЕДРЕНИЕ ИНФОРМАЦИИ В АУДИОПОТОК ДЛЯ ЗАЩИТЫ АВТОРСКИХ ПРАВ

Нелегальное копирование аудиозаписей – серьезная проблема, наносящая значительный ущерб музыкальной индустрии. Она лишает правообладателей заслуженных доходов и сдерживает развитие творчества. Традиционные методы защиты, например, DRM (Digital Rights Management), часто оказываются неэффективными, создавая неудобства для пользователей и легко обходясь при наличии определенных навыков. В этой связи, стеганография представляет собой перспективный инструмент защиты авторских прав, отличающийся надержностью. Стеганография, в отличие от криптографии, которая стремится сделать информацию нечитаемой для посторонних, фокусируется на сокрытии самого факта передачи секретного сообщения [1]. Её основная цель – обеспечить незаметную передачу данных, не привлекая внимания и не вызывая подозрений.

Среди множества методов стеганографии, LSB-стеганография (Least Significant Bit – метод наименее значимых битов) выделяется своей эффективностью [2]. Этот метод основан на изменении наименее значимых битов в цифровых данных, будь то изображения, аудио или видеофайлы. Простота реализации и относительная незаметность для человеческого восприятия являются ключевыми преимуществами LSB-стеганографии. Особенно эффективно данный метод проявляет себя при работе с аудиоданными. Человеческое ухо обладает ограниченной чувствительностью к незначительным изменениям, особенно в тихих участках аудиозаписи [3]. Этот факт активно используется в алгоритмах стеганографии, основанных на анализе аудиосигнала и скрытой передаче данных в малозаметных фрагментах.

Рассмотрим подробнее принцип работы алгоритма стеганографии, использующего LSB-метод и анализ тихих участков аудио. Процесс начинается с загрузки аудиофайла, как правило, в формате MP4, который является распространенным контейнером для хранения аудиоданных. В целях упрощения, стереофонический звук преобразуется в монофонический путем усреднения значений сэмплов из левого и правого каналов. Затем формируется массив сэмплов, представляющих собой числовые значения амплитуды звуковой волны в дискретные моменты времени. Извлекаются такие важные параметры аудиофайла, как частота дискретизации, количество каналов (в нашем случае – один,

после преобразования в моно) и разрядность (ширина) сэмпла.

Следующий этап – разбиение аудиосигнала на короткие временные отрезки, называемые фреймами. Это необходимо для проведения покадрового анализа и выявления участков, пригодных для скрытого встраивания информации. Размер фрейма определяет продолжительность каждого анализируемого отрезка, а шаг – величину перекрытия между соседними фреймами. Частичное перекрытие фреймов способствует более плавному и точному анализу аудиосигнала.

Далее, для каждого фрейма выполняется преобразование Фурье, в результате чего получается спектрограмма аудиосигнала. Спектрограмма дает визуальное представление распределения энергии сигнала по различным частотам во времени. Для минимизации искажений, возникающих при преобразовании Фурье, применяется так называемое окно Хэмминга, которое сглаживает края каждого фрейма.

Центральным этапом алгоритма является анализ энергетических характеристик звука в различных частотных диапазонах: низких, средних и высоких. Фреймы, в которых энергия сигнала во всех трех диапазонах оказывается ниже заданного порогового значения, классифицируются как “тихие” [4]. Именно эти малозаметные фрагменты и будут использованы для встраивания секретного сообщения.

Само секретное сообщение предварительно преобразуется в последовательность битов – нулей и единиц. Затем эти биты последовательно встраиваются в младшие (наименее значащие) биты сэмплов аудио, принадлежащих “тихим” фреймам. Модификация младших битов вносит лишь незначительные изменения в звучание, которые, как правило, остаются незамеченными для человеческого слуха.

Процесс извлечения скрытого сообщения является обратным. Из тех же самых “тихих” фреймов считываются младшие биты сэмплов, которые затем объединяются в битовую строку. Эта строка преобразуется обратно в исходное сообщение.

Надежность и устойчивость стеганографической системы могут быть существенно повышены за счет применения дополнительных мер. Например, перед встраиванием секретное сообщение может быть зашифровано с использованием надежного алгоритма шифрования. Это гарантирует, что даже в случае обнаружения факта скрытой передачи, злоумышленник не сможет получить доступ к содержимому сообщения без знания ключа дешифрования. Другой способ повышения безопасности – случайный выбор позиций для встраивания битов внутри "тихих" фреймов. Добавление контрольной суммы к извлеченному сообщению позволяет проверить его целостность и убедиться в отсутствии искажений.

Важно понимать, что LSB-стеганография не является единственным способом скрытия информации в аудио. Существуют и другие методы, такие как фазовое кодирование (изменение фазы аудиосигнала), расширение спектра (распределение скрываемой информации по широкому диапазону частот), эхо-скрытие (внесение в сигнал искусственного эха с малой задержкой) и частотная маскировка (использование эффекта маскировки более громкими звуками). Каждый из этих подходов имеет свои сильные и слабые стороны, и выбор конкретного метода зависит от требований к незаметности, устойчивости к искажениям и объему скрываемых данных.

Стеганография в аудио находит широкое применение в различных областях. Она может использоваться для защиты авторских прав на музыкальные произведения путем внедрения в них невидимых (неслышимых) цифровых водяных знаков. Стеганография обеспечивает конфиденциальность при передаче секретной информации, такой как пароли, личные сообщения или любые другие данные, которые необходимо скрыть от посторонних глаз.

ЛИТЕРАТУРА

1. Грибунин, В.Г. Стеганография: учебное пособие / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: СОЛОН-ПРЕСС, 2016. – 304 с.

2. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006. – 288 с.

3. Кузнецов, А.А. Исследование устойчивости методов стеганографии в аудио к атакам / А.А. Кузнецов, Д.С. Лавров, Е.С. Григорьева // Вестник компьютерных и информационных технологий. – 2021. – № 7(205). – С. 3-10.

4. Пташкина, А.С. Обзор и анализ методов стеганографии / А.С. Пташкина // Наука и образование сегодня. – 2021. – №2 (61). – С. 14-16.

УДК 621.396.98

А.А. Дятко, доц. (БГТУ, г. Минск)

МОДЕЛИРОАНИЕ РАБОТЫ АВТОКОМПЕНСАТОРА ПОМЕХ

Одним из важнейших элементов современных радиоэлектронных систем является автокомпенсатор помех. Он представляет собой адаптивную антенную решетку [1] – антенную решетку, осуществляющую автоматическую подстройку своих характеристик в соответствии с из-