УДК [004.56+003.26] (075.8)

Студ. Е.В. Дурко, Е.П. Шестовец
Науч. рук. профессор П.П. Урбанович
(кафедра информационных систем и технологий, БГТУ)

МЕТОДЫ ЗАЩИТЫ АВТОРСКОГО ПРАВА НА МУЗЫКАЛЬНЫЕ ПРОИЗВЕДЕНИЯ

Стороны, стремящиеся к несанкционированному распространению и копированию защищенного коммерческого музыкального или видеоконтента, должны обойти ее защиту, чтобы получить расшифрованную копию. После получения такой копии технология защиты перестает быть эффективной при управлении доступом к файлу, и дешифрованный контент может подлежать неограниченному использованию, копированию и распространению.

Для защиты аудиофайлов от несанкционированного копирования и распространения, а также доказательства авторства можно использовать следующие способы идентификации файлов:

вставка идентификационной метки (маркер); при этом пользователь не сможет на слух уловить какие-либо изменения после наложения метки, но с помощью специальных устройств эту метку легко обнаружить;

вычисление “цифрового отпечатка” звукового файла и хранения его в базе данных [1].

Использование водяных знаков относится к методам стеганографии, а именно: к одному из направлений стеганографии – цифровым водяным знакам (ЦВЗ). Цель стеганографии – скрыть факт передачи защищенной информации [2]. Отправитель встраивает секретное сообщение в некоторый объект (контейнер), и только принимающая сторона, знающая о факте передачи, может получить это сообщение. Учитывая, что злоумышленник знает или может догадаться о наличии ЦВЗ и предпринимает попытки изменить защищенный файл. Существует ряд требований при внесении информации в аудиосигналы:

- скрытая информация должна быть устойчивой к наличию различных шумов, сжатию с потерями, фильтрации, аналого-цифровому и цифро-аналоговому преобразованию;
- скрытая информация не должна вносить искажения в сигнал, воспринимаемый человеческим слуховым аппаратом;
- попытка удалить скрытую информацию должна привести к заметному повреждению контейнера (для ЦВЗ) или его непригодности для восприятия;

– ЦВЗ должен однозначно идентифицировать автора произведения;

– скрытая информация не должна вносить заметных изменений в статистику контейнера.

ЦВЗ имеют небольшие размеры, но для их внедрения необходимо использовать сложные методы встраивания. Для встраивания скрытой информации в аудиосигналы можно использовать методы, применимые в других видах стеганографии [3]. Или вы можете построить стегосистемы, основанные на особенностях звуковых сигналов и человеческого слуха.

ЦВЗ обеспечивают дополнительный уровень безопасности в цепочке защиты контента для предотвращения несанкционированного использования контента путем встраивания водяных знаков, которые идентифицируют разрешенное использование контента в музыку или саундтрек к фильму, до театральных, упакованных носителей (диски Blu-ray, DVD) и цифровое распространение в Интернете. В настоящее время имеются также приложения, с помощью которых каждый пользователь может самостоятельно зашифровать собственные произведения. Например, такие как *Free Audios Copy Protection* – уникальное программное обеспечение для защиты от копирования данных, которое позволяет предотвратить кражу изображений, позволяя защитить ваши изображения, фотографии и цифровые произведения искусства от копирования. В основе зашифровки файлов лежит шифр Advanced Encryption Standard (AES), который является одним из наиболее часто используемых алгоритмов шифрования.

Лицензионная защита основана на том, что только пользователь, купивший лицензию, может запускать файлы. Лицензия включает в себя:

– серийный номер для активации 4

– оптический диск с защищенными файлами;

– USB-накопитель с защищенными файлами [4].

Настройка плеера – это метод защиты, который позволяет изменять интерфейс плеера в соответствии с вашими потребностями. Вы можете использовать логотип вашей компании, дизайн и т. д. Для этого вам необходимо изменить исходный код проигрывателя (требуются навыки программирования). Сам плеер защищен вместе с видео- и аудиофайлами и затем предоставляется конечным пользователям.

Защищенное видео или аудио можно привязать к:

– компьютеру конечного пользователя (активация по серийному номеру, как при защите на сайте);

– удаленному серверу (привязка к конечному пользователю; лицензия проверяется каждый раз при запуске файла);
– CD/DVD диску;
– USB-накопителю;

Рассмотренные методы позволяют защитить музыкальные произведения от несанкционированного доступа. Метка должна быть устойчива к наличию различных шумов, сжатию с потерями, фильтрации, аналого-цифровому и цифро-аналоговому преобразованию, а также удалению.

В методе цифровых отпечатков стоит учитывать тот факт, что отпечатки, хранящиеся в базе данных, могут занимать место, значительно превышающее размер самого аудиофайла. Этот метод будет иметь смысл, если будет создана единая база данных для всех аудиофайлов. Если же будет создано множество баз данных, это может привести к конфликтным ситуациям между авторами произведений.

Программный метод защиты отлично подходит не только для авторов произведений, но и обычных пользователей, которые хотят защитить свои аудиофайлы от несанкционированного доступа.

ЛИТЕРАТУРА

1. Методы защиты аудиофайлов от несанкционированного копирования и распространения [Электронный ресурс]. – 2015. – Режим доступа: https://www.fundamental-research.ru/ru/article/ view?id=38286. – Дата доступа: 30.03.2021.

2. Урбанович, П. П. Защита информации методами криптографии, стеганографии и обфускации: учеб.-метод. пособие для студ./ П. П. Урбанович. – Минск: БГТУ, 2016. – 220 с.

3. Берников, В. О. Модификация метода LSB для многоключевой стеганографической системы [Электронный ресурс] / В. О. Берников, П. П. Урбанович // Доклады VII Международной научно-технической интернет-конференции «Информационные технологии в образовании, науке и производстве», Минск,16–17.11.2019.

4. How to protect video files from copying [Электронный ресурс]. – 2018. – Режим доступа: https://www.star-force.com/blog/index.php ?blog=2802. – Дата доступа: 03.04.2021.