5. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Д.В. Богданов, В.Ю. Швачко, М.Б. Атманских

Тюменский государственный университет, г. Тюмень

УДК 004.056, 347.78

ПРОЕКТИРОВАНИЕ КОНЦЕПЦИИ СИСТЕМЫ ПО ВНЕДРЕНИЮ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ В ВИДЕОКОНТЕНТ, ЗАЩИЩЕННЫЙ АВТОРСКИМ ПРАВОМ

Аннотация. В статье обсуждаются проблема нарушения авторского права в сфере киноиндустрии и методы по предотвращению и пресечению нарушений. Приведена концепция системы по внедрению цифровых водяных знаков в материалы, демонстрируемые в цифровых кинозалах.

Ключевые слова: стеганография, цифровые водяные знаки, кинопиратство, цифровые метки, видеоконтейнеры, авторские права.

Введение

Большую часть кинофильмов, демонстрируемых в кинотеатрах, можно найти в сети в свободном доступе несмотря на то, что это не предусмотрено автором. Основываясь на аналитике британской компании MUSO, на 2020 год в России было произведено около 727 миллионов переходов по пиратским ресурсам. Спрос на пиратские фильмы вырос почти на треть, по сравнению с предыдущим годом. В 2019 году мировые потери правообладателей от интернет-пиратства оцениваются более чем в 9 миллиардов долларов, к 2024 году сумма может возрасти до 12 миллиардов [1]. Финансовые потери, связанные с кинопиратством сказывается в целом на развитии кинематографической отрасли. Таким образом, проблема нарушения и защиты авторских прав кинематографических продуктов является актуальной. Одним из решений этой проблемы является создание системы по защите авторских прав для фильмов, находящихся в прокате.

Существует ряд методов по защите видеоряда и определению его принадлежности, например алгоритм Куттера или алгоритм Patchwork, в основе которых заложен принцип внедрения цифровых водяных знаков (далее – ЦВЗ) [2].

Этот метод защиты авторского права и определения принадлежности файла является наиболее эффективным и распространенным из-за того, что сложно (или невозможно) увидеть ЦВЗ при просмотре видеоряда без применения специального программного обеспечения, а так же удалить эти метки без причинения ущерба целостности кинофильма.

Проанализировав области применения ЦВЗ, нами была подмечена актуальность данного метода стеганографии в сфере кинопроката.

На данный момент в сфере кинопроката уже существуют решения для идентификации сеанса, на котором велась несанкционированная видеозапись по меткам, которые наносятся на видеоряд. Однако, данные решения имеют один существенный недостаток – искажение зрительского опыта во время просмотра фильма. Согласно комментариям, опубликованным на тематических форумах, существует процент людей, которым данные метки бросаются в глаза, а, следовательно, отвлекают фокус внимания от повествования картины [3].

В связи с выявленными проблемами, нами был разработан собственный метод, по внедрению цифровых водяных знаков или меток для контейнеров формата DCP, который используется для демонстрации материалов в цифровых кинозалах.

Формат DCP

Формат DCP – цифровой кино пакет, разработанный консорциумом ведущих мировых киностудий DCI (англ. Digital Cinema Initiatives). Важной особенностью является то, что для полноценной работы, цифровой пакет DCP должен соответствовать требованиям DCI – это необходимо для совместимости со всеми цифровыми кинозалами. Согласно этому стандарту, каждый кадр при сохранении сжимается по стандарту JPEG 2000, используя цветовое пространство CIE XYZ с глубиной цвета 12 бит на канал. Звук сохраняется в

формате WAV. Все компоненты вносятся в пакет DCP, который предполагает использование контейнера MXF с ограничением максимального потока в 250 мегабит в секунду и при необходимости шифруется. Ключ, в котором содержится номер кино сервера и период времени, в который кинотеатр сможет запустить данный пакет, высылается по электронной почте для воспроизведения зашифрованного контента [4].

Пакет DCP всегда включает в себя следующие составляющие: контейнер с изображением формата MXF, контейнер MXF со звуком, файл списка воспроизведения компонентов фильма, файл описания содержимого DCP и файл, содержащий контрольные суммы контейнеров [4].

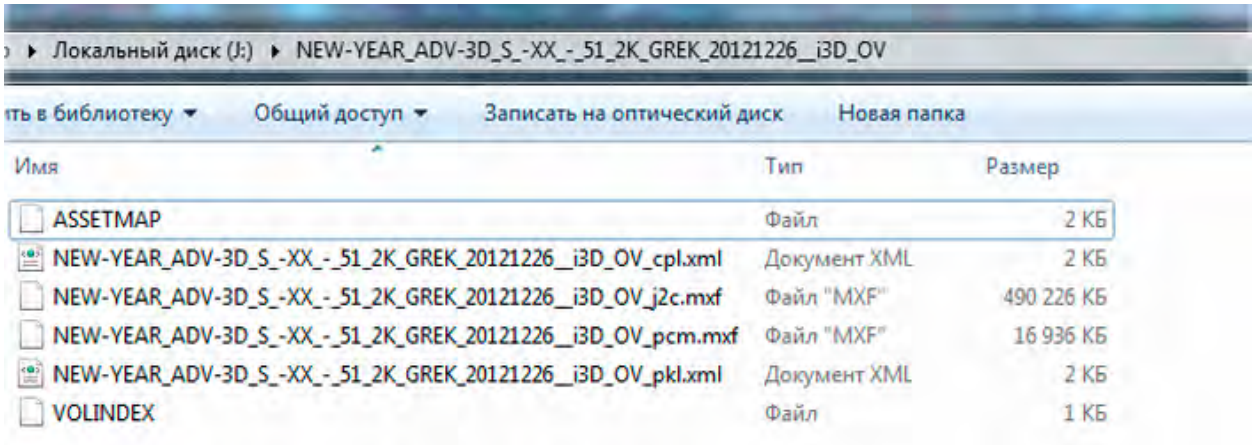

Рис. 1. Пример содержимого видеоконтейнера формата DCP

Водяные знаки

Цифровой водяной знак – технология, созданная для защиты авторских прав мультимедийных файлов. Различают видимые и невидимые ЦВЗ. Невидимые ЦВЗ внедряются непосредственно в цифровые данные, но их невозможно обнаружить без вспомогательных инструментов. Эту информацию можно представить в виде надписи или логотипа [5].

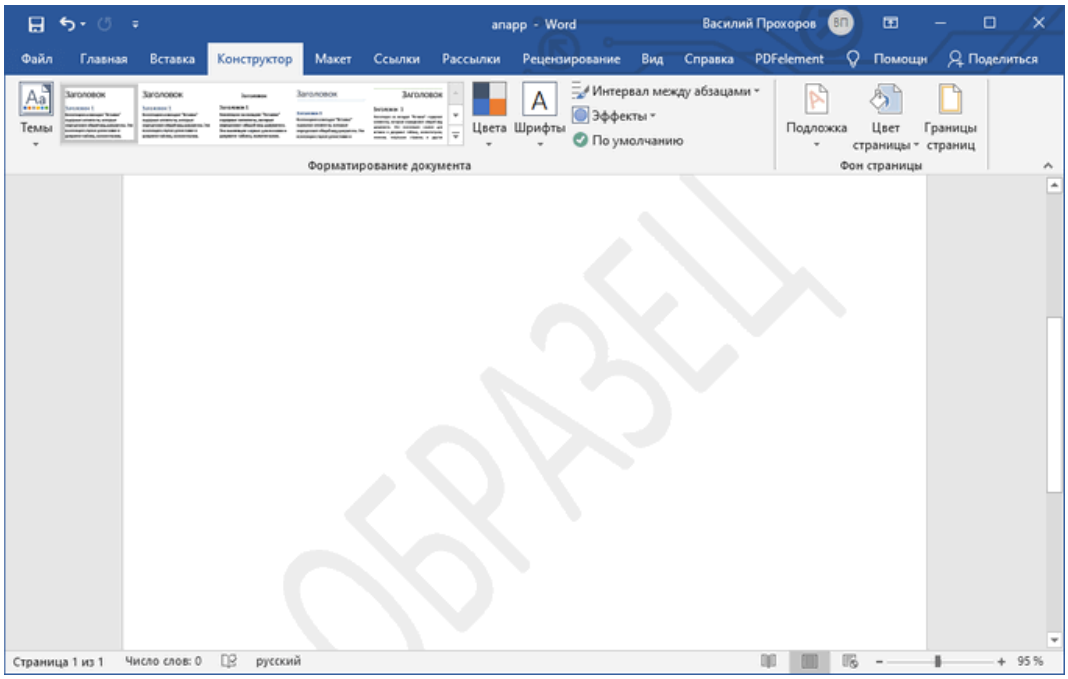

Рис. 2. Пример видимого ЦВЗ

Жизненный цикл ЦВЗ можно описать следующими шагами:

1. В источник сигнала в некоторой доверительной среде при помощи вспомогательной функции внедряется ЦВЗ;
2. Полученный в результате внедрения ЦВЗ защищенный сигнал распространяется (передается получателю каким-либо способом);
3. Во время распространения сигнала, на него может быть совершена атака, в результате которой ЦВЗ могут быть уничтожены или изменены;
4. Заключительным этапом является обнаружение ЦВЗ и идентификация подлинности данных с помощью вспомогательных функций [6].

Рис. 3. Жизненный цикл ЦВЗ

ЦВЗ обладают рядом важных свойств, которые нужно учитывать при работе с ними. Первым таким свойством является внедряемый объем. Это размер сообщения, которое возможно записать. Вторым свойством является извлекаемый объем. Это свойство связано с размером сообщения, которое было извлечено при получении сигнала. В нашем случае это свойство для нас не важно, так как целью внедрения ЦВЗ не является передача сообщения по незащищенному каналу. Далее можно отметить такое свойство как сложность. Сложность ЦВЗ – совокупность таких факторов как: усилия на внедрение, атаку, детектирование или расшифровку. В зависимости от реализации сложность описывает затрачиваемое время, кол-во операций ввода-вывода, количество строк кода и так далее. Заключительным важным свойством ЦВЗ является надежность. Для измерения надежности используются понятия числа ошибочных байтов и частоты ошибочных битов. Измеряется расстояние между строками извлеченного и внедренного сообщений или процент совпадений для побитового сравнения. Если строки совпадают, то метод надежен. Существует три вида надежности ЦВЗ:

- Хрупкий – при малейшей модификации уже нельзя обнаружить. Используется для проверки целостности;
- Полухрупкий – выдерживает незначительные модификации сигнала, но вредоносные преобразования не выдерживает. Используется для обнаружения атаки;

- Надежный – противостоит всем известным видам атак. Используется в системах защиты от копирования и идентификации [7].

Система по внедрению цифровых водяных знаков

Система, концепцию которой мы разработали, предоставляет собой аналогичный набор возможностей по идентификации, однако, в отличие от существующих, она разработана, в том числе, чтобы минимизировать акцентирование внимания на нанесенных цифровых метках и не портить зрительский опыт.

В соответствии с жизненным циклом ЦВЗ (рис.3), система по внедрению цифровых водяных знаков должна состоять из двух приложений:

1) Приложение, внедряющее идентификационные метки в видеоряд;
2) Приложение, выполняющее анализ меток по загруженному файлу и дальнейшее информирование правообладателя об утечке.

Алгоритм работы приложения, внедряющего идентификационные метки в видеоряд:

1) Запускается покадровая обработка видео;
2) Из потока берется целевой кадр/набор кадров для размещения меток согласно алгоритму;
3) Метки помещаются на целевые кадры;
4) Кадры возвращаются в поток.

Разработанный нами алгоритм работает следующим образом. Из видеопотока берется целевой кадр и кадр, идущий в потоке перед ним. Далее, на целевой кадр помещается определенный фрагмент предыдущего кадра (выбранный согласно обозначениям разделения кадра на фрагменты). На рисунке 4, в качестве условного обозначения фрагментов, мы берем разделение кадра по горизонтали на N фрагментов. К примеру, размещение на целевом кадре 7-го по счету сверху фрагмента из предыдущего кадра обозначает цифру 7.

Ознакомиться со схематичным изображением алгоритма можно на рисунке 4.

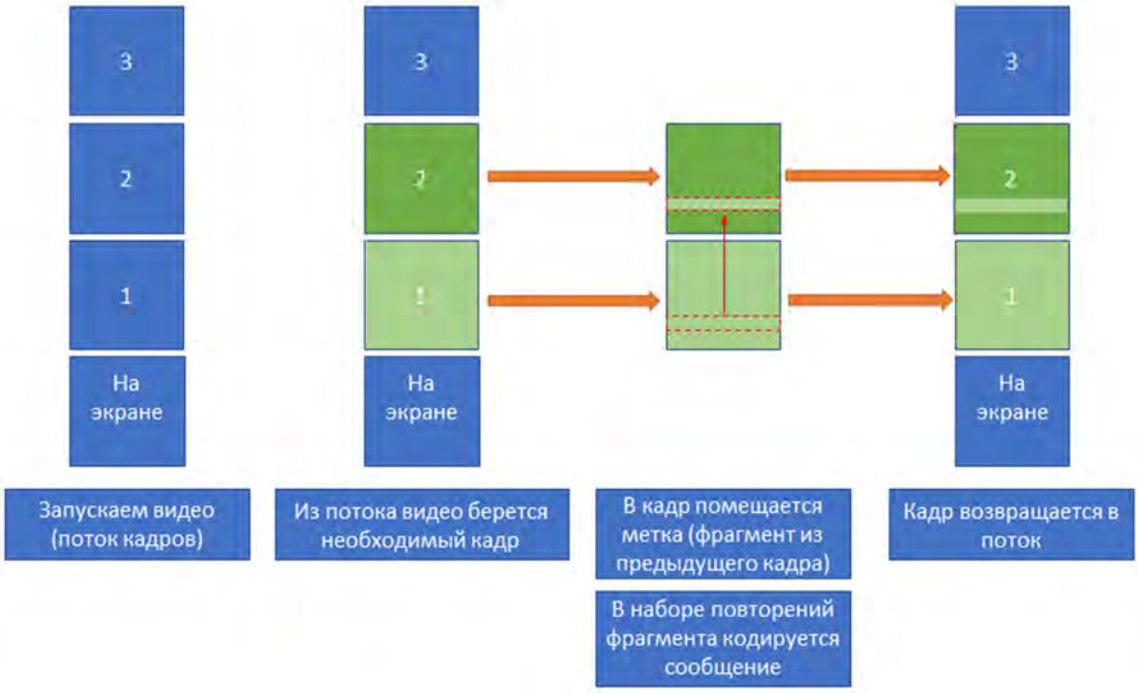

Рис. 4. Алгоритм размещения цифровых меток

Однако, помимо разработки алгоритма размещения меток, перед нами также стоит задача разработки системы обозначений для меток. Поскольку, при разработке системы мы ориентируемся на кинопрокат, предполагается, что информация об идентификаторе кинозала, дате и времени сеанса будет кодироваться для достижения минимальной длины послания, и, далее, помещаться на кадр(ы) в виде метки, соответствуя системе обозначения.

Алгоритм работы приложения для автоматического анализа меток:

1) в приложение загружается запись экрана, на котором демонстрируется видеоряд со внедренными метками;

2) при помощи компьютерного зрения на видеоряде опознаются метки;

3) опознанные метки проходят процесс раскодирования;

4) выясненная информация о кинозале, дате и времени сеанса отправляется на электронную почту компании-прокатчика с целью дальнейших разбирательств и взыскания штрафа с администрации кинотеатра.

Заключение

Используя изученную информацию о контейнерах DCP и сведения о ЦВЗ, была предложена концепция системы по внедрению цифровых меток в видеоконтент, состоящей из приложения, внедряющего ЦВЗ, и приложения для автоматического анализа меток.

Дальнейшей задачей для нас стоит выбор подходящих библиотек и API для разработки и проектирования прототипа системы. Разработка первого прототипа планируется для работы с массовыми видеоконтейнерами (такими как mp4, avi, mkv).

СПИСОК ЛИТЕРАТУРЫ

1. Статья о пиратстве. URL: https://lenta.ru/articles/2020/05/20/pirates/ (дата обращения: 20.04.2021).
2. Методы защиты видеоинформации. URL: https://ru.bmstu.wiki/Методы_защиты_видеоинформации (дата обращения: 27.04.2021).
3. ADSLclub – сообщество пользователей Ростелеком Новосибирск, форум. URL: https://www.adslclub.ru/forum/topic43960 (дата обращения: 27.04.2021).
4. DCP формат. URL: https://clck.ru/VB9WM (дата обращения: 20.04.2021).
5. Цифровые водяные знаки. URL: http://fkn.ktu10.com/?q=node/4439 (дата обращения: 20.04.2021).
6. Жизненный цикл цифровых водяных знаков. URL: http://chinapads.ru/c/s/tsifrovoy_vodyanoy_znak_-_jiznennyiy_tsikl_tsifrovyih_ vodyanyih_ znakov (дата обращения: 25.04.2021).
7. Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А. Стеганография, цифровые водяные знаки и стеганоанализ. М.: Вузовская книга, 2009. 220 с.