ЗАЩИТА АВТОРСКИХ ПРАВ НА ИЗОБРАЖЕНИЕ И АУДИОФАЙЛЫ НА ОСНОВЕ ВСТРАИВАНИЯ ЦИФРОВОГО ВОДЯНОГО ЗНАКА

Габутдинова К.С., Тихонова В.В., Усманов Р.И.

Научный руководитель: Инюшкин А.А.

Россия, г. Самара,
Самарский национальный исследовательский университет
имени академика С.П. Королева

Аннотация. *Цифровой водяной знак – технология, созданная для защиты авторских прав мультимедийных файлов. Её суть заключается в встраивании какого-либо текста или логотипа, идентифицирующего автора. Наличие встраиваемой метки невозможности определить без специального ПО или оборудования. С помощью цифрового водяного знака правообладатели могут защитить свои аудио и фото от несанкционированного копирования, изменения или распространения. Существует большое количество алгоритмов встраивания и каждый алгоритм решает разные задачи. Одни способы встраивания защищают от незаконного копирования, другие препятствуют изменению, третьи защищают от несанкционированного распространения.*

Ключевые слова: *защита авторских прав, информационная безопасность, цифровой водяной знак, стеганография, интеллектуальная собственность, изображение, аудиофайл, несанкционированное копирование.*

В эпоху быстро развивающихся интернет-технологий защита прав интеллектуальной собственности стала жизненно важным вопросом. Это актуально и для изображений, и для аудио- и видеоинформации. Широкое распространение глобальных сетей и повсеместное использование электронных средств массовой информации дает авторам возможность делиться своими работами со всем миром. Эти произведения должны быть доступны любым пользователям. Но такая свобода делает информацию уязвимой для угроз несанкционированного копирования и распространения от чужого имени. Многие правообладатели обеспокоены защитой своих произведений от незаконного копирования. Существует достаточно много способов доказательства авторства. Мы рассмотрим метод встраивания в изображения и аудиофайлы цифрового водяного знака, некой идентификационной метки. Такие метки невозможно обнаружить без использования специальных детекторов.

Из статьи 1255 Гражданского кодекса Российской Федерации (далее ГК РФ) известно, что авторскими правами являются интеллектуальные права на произведения науки, литературы и искусства. Автор произведения наделен следующими правами:

1) исключительное право на произведение;
2) право авторства;
3) право автора на имя;

4) право на неприкосновенность произведения;

5) право на обнародование произведения. [2]

В соответствии со статьей 1257 ГК РФ автором любого произведения считается гражданин, творческим трудом которого оно создано. Автором произведения признается лицо, которое указано на оригинале или экземпляре произведения в качестве автора, в случае если не доказано иное.

Согласно статье 1300 ГК РФ любая информация, с помощью которой можно идентифицировать произведение, автора или иного правообладателя, а также информация об условиях использования произведения, любые числа и коды, содержащие такую информацию, считается информацией об авторском праве. В отношении произведений запрещено:

1) искажение или уничтожение информации об авторских правах без позволения автора или другого правообладателя;

2) любая публикация работ, в отношении которых информация об авторских правах была искажена или уничтожена без разрешения автора или другого правообладателя. [2]

При нарушении положений, предусмотренных пунктом 2 статьи 1300 ГК РФ, правообладатель вправе требовать от нарушителя возмещения убытков или выплаты компенсации в соответствии со статьей 1301 ГК РФ. [2]

Любая фотография вне зависимости от того, на какое устройство она снята, защищается авторским правом на основании статьи 1265 ГК РФ. Автор фотографии обладает всеми имущественными и неимущественными правами на этот объект.

Автор вправе проводить со своим произведением любые действия. Другие же лица при попытке размещения фотографии и любого другого использования должны оформить письменное разрешение автора на совершение этих действий.

Главная сложность фотографа состоит в доказательстве авторства. Проще доказать свое авторство тем фотографам, чьи работы под их именами были впервые обнародованы в периодических СМИ, альбомах, книгах, описаны в каталогах выставок.

Для упрощения процесса доказательства авторства при съемке следует включать опцию автоматической записи своего имени в EXIF и сохранять RAW фотографии в архиве фотоаппарата. Кроме того, при публикации снимка в Интернет прямо на самих фотографиях желательно указывать свое имя.

Иначе дело обстоит с музыкальными и кинопроизведениями, представленными в цифровом виде. Собственники не публикуют их в открытом доступе с целью заработка. В то же время многие правообладатели обеспокоены защитой от всякого незаконного копирования своих работ. В Российской Федерации существует закон об авторском праве и смежных правах, который регулирует отношения, связанные с созданием и использованием научных, литературных и художественных произведений, фонограмм, исполнений, постановок, передач эфирного или кабельного вещания, а также устанавливает ответственность за их неразрешенное использование и плагиат. Тем не менее этот закон не всегда помогает правообладателям защищать свои произведения. И, как показывает

практика, на различных веб-страницах можно отыскать множество дубликатов аудио- и видеофайлов. Притом названия музыкальных файлов и фильмов часто меняются во время несанкционированного распространения, что осложняет их идентификацию правообладателем. Ввиду этого автору нужно не только найти все существующие в сети копии, но и по закону доказать приоритет своего авторства.

Для предупреждения неразрешенного распространения и копирования, а также для подтверждения первоочередности своего авторства можно предложить различные методы идентификации файлов.

1. Встраивать идентификационную метку в аудиофайлы. Такие метки незаметны для человеческого слуха, но легко распознаются специальными детекторами.

2. Получить «цифровой отпечаток» аудиофайла в качестве идентификатора и хранить его в базе данных (БД). Такой идентификатор будет занимать гораздо меньше места в БД, чем сам файл, это позволит хранить значительное количество отпечатков.

Метод, основанный на встраивании цифрового водяного знака (ЦВЗ), относится к методам стеганографии. Цифровой водяной знак – это технология, созданная для защиты авторских прав и контроля целостности мультимедийных файлов. [1] Одним из наиболее важных применений водяных знаков для изображений и аудиофайлов является предотвращение распространения, незаконного копирования, защищенного авторским правом аудио и фото. С распространением портативных смартфонов, планшетных компьютеров и диктофонов обычные пользователи могут легко перезаписать защищенный авторским правом звук.

Контейнер – это защищаемый мультимедийный файл, а скрываемые данные – различная информация, идентифицирующая автора объекта. Принимая во внимание тот факт, что злоумышленник может знать или предполагать о присутствии ЦВЗ и попробовать изменить файл, существует несколько требований, предъявляемых к ЦВЗ:

– необходимо, чтобы ЦВЗ был устойчив к воздействию разного рода окрашенных шумов, фильтрации, сжатию с потерями, аналогово-цифровому и цифро-аналоговому преобразованиям;

– необходимо, чтобы ЦВЗ не вызывал искажение сигнала, воспринимаемого слуховой системой человека;

– необходимо, чтобы попытка удалить ЦВЗ вызывала заметное искажение контейнера или форму, не подходящую для восприятия;

– посредством ЦВЗ необходимо иметь возможность однозначного установления авторства защищаемого файла;

– необходимо, чтобы ЦВЗ не вызывал ощутимых искажений в статистике контейнера.

При встраивании ЦВЗ должны использоваться сложные методы. При встраивании ЦВЗ в аудиосигналы можно строить стегосистемы, основываясь на особенностях аудиосигналов и системы слуха человека, а при встраивании в

изображение следует основываться на особенностях самого изображения и зрительной системы человека. [1]

В наше время популярны следующие методы генерации ЦВЗ для аудиофайлов:

1. Метод замены наименее значащих бит – это самый просто способ внедрить конфиденциальные данные. Недостатком данного метода является низкая устойчивость к внешним воздействиям на сигнал.

2. Метод внедрения информации с использованием эхо-сигнала. Метод слабо устойчив к сжатию.

3. Метод фазового кодирования. Метод фазового кодирования является одним из методов, который устойчив к сжатию и воздействию шумов.

4. Метод растяжения спектра. Метод является устойчивым к некоторым посторонним воздействиям.

5. Time base modulation (изменение масштаба временной оси). Метод устойчив к сжатию, искажениям. [6]

По методу противостояния атакам ЦВЗ делятся на робастные, полухрупкие и хрупкие.

Робастные ЦВЗ устойчивы при любых видах атак. Такие виды ЦВЗ используются, когда автор хочет, чтобы идентификационная метка (подпись, логотип компании) сохранились при максимальных искажениях контейнера.

Полухрупкие ЦВЗ устойчивы только к одному виду воздействий. Такие методы встраивания ЦВЗ специально проектируются так, чтобы быть неустойчивыми к определенным операциям. Например, они могут позволять выполнять сжатие изображения, но запрещать его кадрирование.

Хрупкие ЦВЗ изменяются или разрушаются при незначительных модификациях. Они применяются для проверки целостности полученной информации. [5]

На данный момент существует множество различных вариантов выбора области встраивания ЦВЗ. Классификация алгоритмов по области встраивания приведена на рисунке 1.

Методы сокрытия данных в пространственной области изображения являются нестойкими к большинству из известных видов искажений, например сжатие с потерями. Они отличаются набором изменяемого подмножества и алгоритмом смены значений пикселей. Встраивание ЦВЗ происходит в области первичного изображения [4]. Достоинство данных алгоритмов заключается в том, что нет необходимости выполнять громоздкие с точки зрения вычислений линейные преобразования изображений для реализации цифрового водяного знака. ЦВЗ встраиваются путем управления компонентами яркости или цвета.

Наибольший интерес в области цифровых изображений представляют методы встраивания информации в изображения, где происходит сжатие с потерями (такие популярные форматы как JPEG) [3]. Для таких форматов нет смысла встраивать в пространственную область, потому как после определённых преобразований данные будут отличаться от исходных, и поэтому многие внедряемые сообщения попросту невозможно извлечь, и, таким образом, теряется

смысл системы. Для встраивания информации используется область изменяемого разрешения или частотная область.

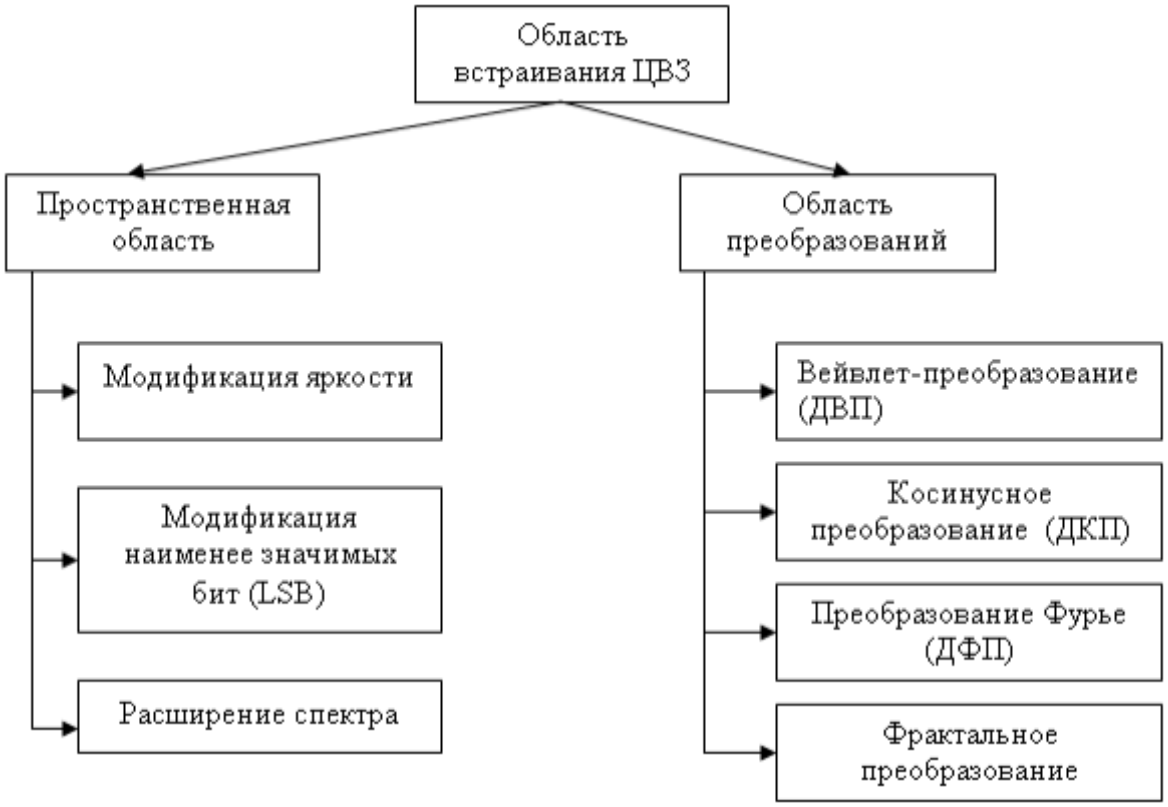

Рисунок 1 – Классификация алгоритмов встраивания ЦВЗ по области, используемой в процессе внедрения

Методы, использующие для скрытия данных частотную область, являются более стойкими к различным возможным внешним воздействиям на изображение-контейнер. Такие методы имеют хорошие характеристики робастности [4].

Данные преобразования можно использовать как по отношению к отдельным фрагментам изображения, как и ко всему изображению в целом. Чтобы скрыть данные, рекомендуется применять именно то преобразование изображения, которое оно будет претерпевать с течением времени с возможным сжатием. Для алгоритмов встраивания информации в видеопоследовательности используют более простые алгоритмы встраивания информации в цифровые изображения.

Patchwork – это перспективный алгоритм встраивания водяных знаков, который имеет высокую устойчивость ко многим популярным атакам, таким, как добавление шума, фильтрация, сжатие, повторное квантование и повторная выборка. Метод состоит из нескольких действий, которые обеспечивают его простую реализацию и в то же время хорошую устойчивость ко многим атакам. Реализация алгоритма patchwork:

- выбор двух псевдослучайных значений;

- добавление небольшой константы к выборке одного значения и вычитание этой же константы из выборки другого значения;

- процесс обнаружения начинается с нахождения остатка от вычитания этих значений [1].

Цифровые водяные знаки являются очень важным как в области информационной безопасности, так и в области юридический защиты авторских прав. В результате исследования была определена и обоснована актуальность выбранной темы, определены объект и предмет исследования. Подводя итоги, отметим, что ЦВЗ, как и любая система защиты, должен быть надежным и устойчивым к искажениям информации.

Стеганография быстро развивается: формируется теоретическая база, ведется разработка новых, устойчивых методов встраивания сообщений. Одной из причин популярности стеганографии является принятый в некоторых странах закон на ограничение использования сильной криптографии. И пока на данный момент он остается одним из лучших способов защиты авторских прав. Также нами был изучен метод встраивания устойчивого к десинхронизации и перезаписи цифрового водяного знака на основе patchwork.

Метод patchwork основан на изменении функции FDLM путём увеличения или уменьшения его на некоторое значение в зависимости от встраиваемого ЦВЗ. Алгоритм прост в реализации и в то же время обеспечивает необходимую устойчивость ЦВЗ ко многим атакам. Вопросом дальнейшего исследования является программная реализация рассмотренного выше метода встраивания ЦВЗ и проведение экспериментов с целью выявить все достоинства и недостатки при практическом использовании алгоритма в области защиты авторских прав.

Библиографический список

1. Liu Z. Huang Y., Huang J. Patchwork-Based Audio Watermarking Robust-DAgainst De-Synchronization and Recapturing Attacks // IEEE Transactions on Information Forensics and Security, vol. 14, no. 5, pp. 1171-1180, May 2019.

2. ГК РФ Глава 70. Авторское право [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_64629/0b3181 26c43879a845405f1fb1f4342f473a1eda/ (дата обращения: 15.10.2020).

3. Стеганография [Электронный ресурс]. URL: https://habr.com/ru/post/114 597/ (дата обращения: 01.11.2020).

4. Стеганография. Метод LSB. Призрак Бассенджи [Электронный ресурс]. URL: https://ghostbasenji.blogspot.com (дата обращения: 18.10.2020).

5. Федосеев В.А. Цифровые водяные знаки. Самара: Изд-во Самарского университета, 2019. 144 с.

6. Цифровая стеганография. Полезная информация из книг [Электронный ресурс]. URL: https://tech.wikireading.ru/13223 (дата обращения: 30.10.2020).

IMAGE AND AUDIO COPYRIGHT PROTECTION BASED ON EMBEDDING DIGITAL WATERMARK

Gabutdinova K.S., Tikhonova V.V., Usmanov R.I.

Scientific adviser: Inyushkin A.A.

Samara National Research University, Samara, Russia

Abstract. *Digital watermark is a technology designed to protect the copyright of multimedia files. Its essence lies in the embedding of any text or logo that identifies the author. The presence of an embedded tag cannot be determined without special software or hardware. With the help of a digital watermark, copyright holders can protect their audio and photos from unauthorized copying, modification or distribution. There are many embedding algorithms, and each algorithm solves different problems. Some embedding methods protect against illegal copying, others prevent modification, and still others protect against unauthorized distribution.*

Keywords: *copyright protection, information security, digital watermark, steganography, intellectual property, image, audio file, unauthorized copying.*