УДК 378.1, 004
ББК 30

ВОПРОСЫ МАРКИРОВКИ МУЛЬТИМЕДИЙНЫХ ДАННЫХ В ОБУЧЕНИИ

Н.Н. Конобеева

Информатизация общества связана со значительными изменениями в образе жизни людей. Она требует серьезных усилий на многих направлениях, главным из которых является формирование культуры использования новейших информационных технологий. В данной работе предпринята попытка обосновать необходимость обучения студентов мультимедиа-технологиям, а также способам защиты авторских прав созданных мультимедийных продуктов.

Ключевые слова: *авторские права, мультимедиа-технологии, цифровой водяной знак, маркировка изображений, стеганография.*

Все большая информатизация общества как нельзя лучше характеризует современные тенденции в образовательном процессе, особенно это проявляется при подготовке специалистов, бакалавров и магистров по техническим направлениям, в частности, по направлению «Информационные системы и технологии». Предусмотрено множество дисциплин, позволяющих освоить студентам новые возможности информационных технологий. Одним из таких предметов является «Мультимедиатехнологии». В рамках данной дисциплины изучаются вопросы конфигурации технических средств мультимедиа, знакомство с программными средствами мультимедиа, а также этапами и технологией создания продуктов мультимедиа. Но немаловажной частью является и обучение студентов методам защиты разработанных мультимедийных файлов. Именно поэтому представляется достаточно актуальным введение в процесс обучения лабораторного практикума с использованием современных способов защиты авторских прав, в том числе на основе цифровых водяных знаков.

Цифровой водяной знак (ЦВЗ) – это технология, созданная для защиты авторских прав мультимедийных файлов [4]. Как правило, цифровые водяные знаки невидимы, однако существуют и видимые ЦВЗ на изображении или видео. Обычно эта информация представляет собой текст или логотип, который идентифицирует автора.

Основные отличия цифровых водяных знаков от обычных (бумажных) заключаются в том, что ЦВЗ невидимы (существует всего несколько случаев применения видимых ЦВЗ), а также в том, что задача злоумышленника состоит не в наиболее точной имитации водяного знака, а, напротив, в его полном уничтожении.

Требование невидимости необходимо прежде всего для того, чтобы злоумышленник не смог обнаружить цифровой водяной знак визуально (так как в этом случае его задача существенно упрощается). Лучшим способом борьбы с атаками является распределение ЦВЗ по всему цифровому контейнеру. Если речь идет об изображении (фотографии), основными атаками (методами уничтожения) на ЦВЗ являются: масштабирование, поворот на произвольный угол, вырезание каких-либо участков изображения, конвертирование в другой графический формат, печать и последующее сканирование [2]. (Смысл в этом имеется, если, конечно, после таких преобразований картинка похожа на первоначальный вариант.) Цифровой водяной знак должен успешно противостоять подобным атакам.

Цифровые водяные знаки по своей устойчивости можно разделить на три категории (рис. 1):

- робастные (англ. robust – прочно, крепко) – такие цифровые водяные знаки должны быть устойчивы к любым воздействиям на них;
- хрупкие – изменяются или разрушаются при незначительной модификации контейнера;
- полухрупкие – устойчивые ЦВЗ по отношению к одним воздействиям и неустойчивые к другим.

Робастные цифровые водяные знаки используются, когда автор хочет, чтобы идентификационный код, логотип компании и т. п. сохранились при максимальных искажениях контейнера. Хрупкие ЦВЗ, наряду с электронной цифровой подписью, используются для проверки целостности электронных документов. Алгоритмы внедрени хрупких ЦВЗ отличаются от остальных методов особой чувствительностью к любым искажениям. Они эффективны при защите от фальсификации и решении задачи контроля целостности. Изображение с полухрупкими цифровыми водяными знаками можно перевести в другой формат или подвергнуть сжатию, но вырезать или вставить в него фрагмент нельзя; для аудиотрека, например, можно изменить звучание частот, но нельзя убрать голос исполнителя.

В общем случае типичная схема жизненного цикла ЦВЗ имеет следующий вид (рис. 2).

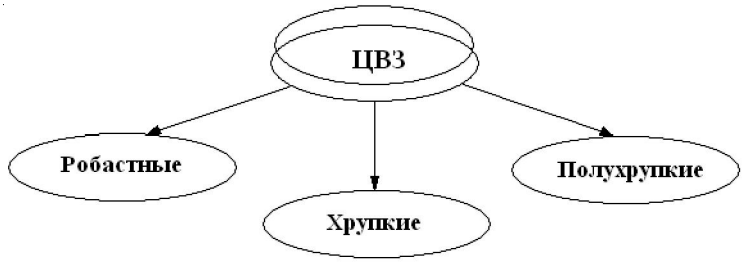

Рис. 1. Классификация ЦВЗ по устойчивости

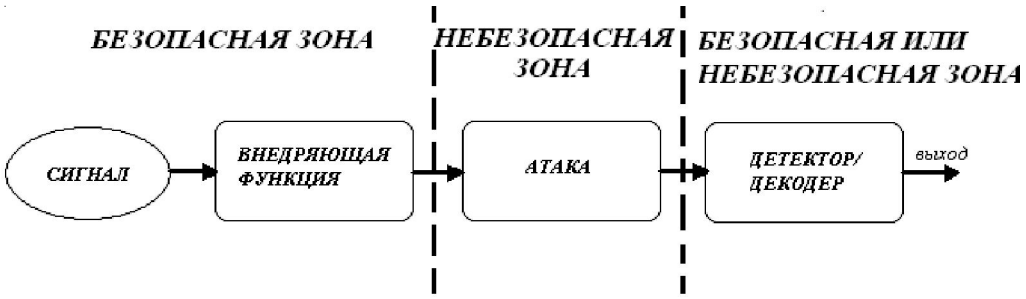

Рис. 2. Фазы жизненного цикла ЦВЗ *

* Составлено по: [1].

Существует множество алгоритмов встраивания цифровых водяных знаков в мультимедийные файлы, которые можно разделить на два больших класса: частотные и пространственные. К пространственным способам, например, относится метод LSB (наименьший значащий бит), к частотным – метод расширения спектра. Изучение студентами подобных алгоритмов очень важно для понимания общей методики маркировки мультимедийных данных. А постоянное обновление и расширение базы методов встраивания цифровых водяных знаков [3; 5] позволит подготовить их к работе с различными видами мультимедиа и стимулировать на разработку собственных алгоритмов, так широко востребованных в современном информационном мире.

СПИСОК ЛИТЕРАТУРЫ

1. Аграновский, А. В. Стеганография, цифровые водяные знаки и стеганоанализ / А. В. Аграновский. – М. : Вузовская книга, 2009. – 220 с.

2. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : Солон-Пресс, 2002. – 265 с.

3. Жарких, А. А. Новые методы внедрения водяного знака / А. А. Жарких, В. Ю. Пластунов // Вестник МГТУ. – 2009. – Т. 12, № 2. – С. 206–211.

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

5. Митенкин, А. В. Модифицированные методы статистического стегоанализа бинарных и полутоновых изображений / А. В. Митенкин // Компьютерная оптика. – 2005. – № 28. – С. 145–151.

ACTUAL QUESTIONS OF MULTIMEDIA DATA DIGITAL WATERMARKING IN EDUCATION

N.N. Konobeeva

Computer science and society associated with significant changes in the way people live. It requires a serious effort on many fronts, chief of which is the culture to use of advanced information technology. In this paper we attempt to justify the need for teaching students of multimedia technologies and ways of copyright protection created products.

Key words: *author rights, multimedia technologies, digital watermark, marking images, steganography.*