УДК 003.26

**РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ СОКРЫТИЯ ИНФОРМАЦИИ В ВИДЕОФАЙЛАХ**

Д.А. БАРАШКОВ

*Федеральное государственное бюджетное образовательное учреждение высшего образования «Московский технологический университет»*

*119454, Москва, Россия*

Интернет – это сеть с бесконечным количеством примеров мультимедийного контента. Здесь есть файлы самых разных форматов: звуковые записи, цифровые изображения, видеофайлы и т.д. Весь этот контент можно использовать в качестве контейнеров, чтобы скрыть информацию от восприятия внешних пользователей сети. Стеганография - это инструмент, который изучает различные методы встраивания скрытых данных в мультимедийные объекты [1]. Эта информация должна оставаться скрытой как статистически, так и для человеческого глаза.

Другими словами, реальность стеганографии – это сокрытие самого факта наличия любой информации, которая стремится скрыться от любопытных глаз.

В данной работе рассматривается проблема сокрытия информации методами стеганографии в видеофайле с использованием сжатия.

Актуальность этого вопроса, связанна с защитой данных. Методы стеганографии очень похожи на технологии, используемые для введения цифровых водяных знаков (CEH). CEH – это своего рода цифровая подпись, встроенная в контент для защиты прав автор [5]. Разница между CEH и стеганографией в том, что последняя ориентируется на незаметность данных, а в случае ЦВЕ концентрируют внимание на предоставлении вводимой информации. Использование подписей позволяет идентифицировать контент и обнаруживать его незаконное распространение [3].

Для решения поставленной задачи был использован метод дискретно-косинусного преобразования(ДКП) [5].

Метод делится на два этапа: алгоритм встраивания и алгоритм извлечения.

Встраивание данных в видео делиться на несколько шагов [2]:

- разбиение видеопоследовательности на отдельные кадры

- вычленение Y яркостной составляющей кадра каждого пикселя

- разбиение кадра на блоки 8\*8 пикселей

- объединение блоков в группы по 8 блоков для встраивания 1 байта скрываемой информации в конкретную область

- применение ДКП, на этапе которого и происходит сокрытие данных, путем обнуления высокочастотных коэффициентов ниже заданного порога.

Во избежание потери информации при обратной компоновке кадров в видеоряд с последующим сжатием, байт скрываемой информации несколько раз дублируется внутри кадра, что позволяет осуществлять проверку на правильность во время извлечения данных [4].

На выходе получаем файл в формате .mp4 со скрытыми данными без визуальных помех.

Алгоритм извлечения идентичен алгоритму встраивания [5].

В результате проведенного эксперимента получены следующие результаты:

- подтверждена результативность выбранного метода ДКП для решения задачи встраивания данных в видеоряд со сжатием

- подтвердилась теория об исправлении ошибок во время извлечения информации путем её многократного дублирования по всей области видеокадра.

- практическая значимость заключается в возможности применения разрабатываемого программного средства для подтверждения авторского права, путём нанесения водяного знака в видеозаписи.

Список использованных источников

1. Blackledge, J. Resilient Digital Image Watermarking for Document Authentication / J. Blackledge, O. Iakovenko // IAENG International Journal of Computer Science. – 2014. – № 41(1). – С. 1-17.

2. Hartung, F. Watermarking of Uncompressed and Compressed Video / F. Hartung, B. Girod // Signal Processing. – 1998. – № 66(3). – С. 283-301.

3. Swanson, M. D. Multimedia Data-Embedding and Watermarking Technologies / M. D. Swanson, M. Kobayashi, A. H. Tewfik // Proceedings of the IEEE. – 1998. – № 86(6). – С. 1064-1087.

4. Вернер, М. Основы кодирования: Учебник для ВУЗов / М. Вернер; пер. с нем. Д. К. Зигангирова. – Москва: Техносфера, 2004. – 288 с. – (Мир программирования).

5. Ричардсон, Я. Видеокодирование H.264 и MPEG-4 – стандарты нового поколения / Я. Ричардсон; пер. с англ. В. В. Чепыжова. – Москва: Техносфера, 2005. – 368 с. – (Мир цифровой обработки).