

Анализ эффективности встраивания информации методом WF5 в BMP-изображения при использовании помехоустойчивых кодов разной длины

Т. А. Минаева (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург)

Н. В. Волошина (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Санкт-Петербург) – научный руководитель

На сегодняшний день в связи с возросшей возможностью быстрого распространения мультимедийных объектов в интернете становится актуальной задача защиты таких объектов от незаконного копирования и распространения, которое может нарушить авторские права. Для защиты мультимедиа данных различного типа используют методы встраивания авторской информации. Одним из наиболее эффективных методов защиты таких данных являются цифровые водяные знаки. Основная задача при встраивании цифрового водяного знака заключается в добавлении информации об авторе в исходные данные (контейнер) таким образом, чтобы встраиваемая информация полностью помещалась в контейнер и не влияла на качество защищаемого объекта.

Одним из наиболее распространяемых типов мультимедийных объектов является статические изображения. Существуют два типа методов встраивания цифровых водяных знаков в изображения: встраивание во временную и в частотную область [1], [2]. Эти методы имеют ограничения на объем встроенной информации. В данной работе исследовались методы встраивания во временную область, в связи с высокой локализацией вносимых при встраивании искажений.

Цель исследования заключается в оценке и анализе эффективности встраивания различной авторской информации во временную область тестовых BMP-изображений, основанного на стеганографическом методе встраивания цифровых водяных знаков WF5 [3], [4], в котором применяется специальный класс помехоустойчивых кодов Хэмминга с разной длиной кодового слова: 7, 9 и 15 бит.

Для сравнения эффективности метода WF5 был рассмотрен самый распространенный стеганографический метод встраивания – метод замены LSB (Least Significant Bit) [5]. Данный метод позволяет встраивать существенный объем путем простой замены наименее значимых бит при расширении зоны встраивания на старшие битовые плоскости. Однако, при увеличении объема встраивания необходимо обеспечивать визуальную необнаруживаемость самого факта добавления информации, т.е. не должно происходить сильного искажения (потери качества) контейнера. В данном исследовании метод WF5 также проверялся по наличию визуальных искажений. Рабочая область контейнера в исследованном методе формировалась из наименее значимых бит цветовых компонентов пикселей изображения. Для анализа визуального качества (уровня искажений) контейнера рассчитывались следующие показатели: PSNR [6], SSIM, MAD и корреляция Пирсона.

Для исследования метода WF5 с разной длиной кодового слова был разработан комплекс программ для встраивания и извлечения различной информации в BMP-изображение и последующего анализа. В ходе исследования стеганографического метода были выявлены его основные свойства. При встраивании исследуемым методом максимального возможного объема информации невозможно было визуально обнаружить факт встраивания или изменения изображения. Значения исследуемых показателей визуального качества свидетельствуют о незначительных искажениях контейнера, обеспечивающих их незаметность, т.е. визуальную необнаруживаемость. При увеличении кодового слова с 7 до 9 стало возможным увеличить объем встраиваемой информации на 15% не увеличивая уровень искажения контейнера. Исследование проводилось на тестовых изображениях различных типов: текст, портрет, пейзаж и т.п. Реализованный метод также позволяет комбинировать

наименее значимые биты для лучшего распределения встраиваемой информации в контейнере, тем самым также уменьшая уровень искажения изображения.

Исследуемый метод WF5, использующий помехоустойчивый код Хэмминга, позволяет оптимально встроить различного вида информацию в изображение так, чтобы при увеличении объема встраивания факт самого встраивания визуально не обнаруживался. Работа выполнена при финансовой поддержке Российского Фонда Фундаментальных Исследований в 2018-2019 годах (грант 17-07-00849-А).

Список используемых источников

1. D. Neeta, K. Snehal, D. Jacobs, Implementation of lsb steganography and its evaluation for various bits, Digital Information Management: 1st International Conference, 2006, pp. 173–178.
2. A. Westfeld, High Capacity Despite Better Steganalysis (F5-A Steganographic Algorithm) Information Hiding. 4-th International Workshop. Lecture Notes Computer Science, Berlin; Heidelberg; New-York: Springer-Verlag, 2001. Vol. 2137, pp. 289–302.
3. Беззатеев С.В. Специальные классы кодов для стеганографических систем/С.В. Беззатеев, Н.В. Волошина, К.А. Жиданов, Труды ТУСУР, 1(25), ч.2, Новосибирск, 2012, с. 112-118.
4. Minaeva T.A., Voloshina N.V., Bezzateev S. MLSB optimal effective weighted container construction for WF5 embedding algorithm // Ultra-Modern Telecommunications and Control Systems and Workshops (ICUMT), 2018 10th International Congress on - 2018, pp. 22-27
5. Fridrich J., Du R., Meng L. Steganalysis of LSB Encoding in Color Images, ICME 2000, New York City, July 31 — August 2, New York.
6. Минаева Т.А., Волошина Н.В., Беззатеев С.В. Анализ методов обнаружения многоуровневых стегановставок в bmp-изображениях // Региональная информатика и информационная безопасность. Сборник трудов СПОИСУ - 2017. - № 4. - С. 230-234