Ярославский государственный университет им. П. Г. Демидова

Кафедра компьютерной безопасности и математических

методов обработки информации

«10.05.01 Компьютерная безопасность»

Исследование методов внедрения цифровых водяных знаков на основе вейвлет-преобразований

Выполнила: студент группы КБ61-СО Шарунцова Анна Александровна, 6 курс

Научный руководитель: канд. физ.-мат. наук, доцент кафедры КБиММОИ Мурин Дмитрий Михайлович

В современном мире, благодаря активному развитию технологий, передача и дублирование данных осуществляется достаточно просто. В связи с этим остро стоит вопрос о защите интеллектуальной собственности. Нередко возникают ситуации незаконного копирования и использования произведений интеллектуальной собственности. В таких случаях автор вынужден обращаться в суд и доказывать свое исключительное право на собственное произведение. Многие интернет-магазины по продаже стоковых фотографий во избежание копирования и незаконного использования накладывают поверх полупрозрачную надпись с названием магазина размером почти во всю фотографию. Это эффективно, но визуально портит продукт.

Что если «подписывать» фотографию таким образом, чтобы это не было заметно глазу, но при этом было очень сложно удалить, не прибегая к сильным искажениям фотографии? Эту проблему решает один из способов современной цифровой стеганографии – цифровой водяной знак (ЦВЗ).

Объектом исследования являются методы внедрения цифровых водяных знаков в изображения с помощью вейвлет-преобразований.

Цель работы – исследование различных схем по встраиванию ЦВЗ, реализация и оптимизация алгоритма встраивания ЦВЗ в изображение с помощью вейвлет-преобразований.

Работа состоит из трех глав. В главе 1 даны определения некоторых понятий стеганографии, а также рассказано о возможностях применения цифровой стеганографии в современном мире.

Стеганография — способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения).

В отличие от криптографии, которая скрывает содержимое тайного сообщения, стеганография скрывает сам факт его существования. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её.

В настоящее время разделяют три вида стеганографии: классическая, компьютерная и цифровая. Классическая берет свое начало в глубокой древности и представляют собой сокрытие информации «вручную». Например, использование симпатических чернил, запись на боковой стороне колоды карт, расположенных в условленном порядке, трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы и т.д. Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы. Например, использование зарезервированных полей компьютерных форматов файлов, сокрытие информации в неиспользуемых местах гибких дисков, использование особых свойств полей форматов, которые не отображаются на экране и использование особенностей файловых систем. Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Цифровая стеганография находит применение в защите конфиденциальной информации от несанкционированного доступа, преодолении систем мониторинга и управления сетевыми ресурсами, камуфлировании программного обеспечения и защите авторских прав.

Глава 2 представляет собой теоретическую сводку о вейвлет-преобразованиях, в частности, преобразованиях Хаара.

Вейвлет-преобразование в настоящее время имеет большую популярность при обработке различных данных, так как оно устраняет те недостатки, которые присущи преобразованию Фурье. Преобразование Фурье даёт информацию о частотах исследуемого сигнала, но не даёт сведенья о локальных особенностях сигнала. Поэтому при использовании преобразования Фурье можно получать информацию либо во временной области, либо в частотной. Вейвлет-преобразование справляется с этой задачей.

Основы вейвлет-анализа были разработаны в середине 80-х годов Гроссманом и Морле как альтернатива преобразованию Фурье для исследования временных (пространственных) рядов с выраженной неоднородностью. В отличие от преобразования Фурье, локализующего частоты, но не дающего временного разрешения процесса, вейвлет-преобразование, обладающее самонастраивающимся подвижным частотно-временным окном, одинаково хорошо выявляет как низкочастотные, так и высокочастотные характеристики сигнала на разных временных масштабах. По этой причине вейвлет-анализ часто сравнивают с "математическим микроскопом", вскрывающим внутреннюю структуру существенно неоднородных объектов.

Вейвлет-преобразования применяются в таких областях как обработка экспериментальных данных, обработка изображений, сжатие данных.

Глава 3 описывает алгоритм И. Р. Ким по встраиванию цифрового водяного знака в изображение с помощью вейвлет-преобразований. Также в ней проведен анализ указанного алгоритма и предложены способы оптимизации исходя из основных выявленных недостатков алгоритма.

В алгоритме И.Р. Кима используется трехуровневое разложение с использованием вейвлет-преобразования Хаара. ЦВЗ встраивается в коэффициенты всех уровней разложения последовательно, начиная с третьего и заканчивая первым. Для встраивания выбираются коэффициенты, превышающие значение определенного порога. Для извлечения ЦВЗ необходимо исходное изображение. Количество встраиваемой информации относительно невелико. В среднем оно составляет примерно 1/120 от размера исходного изображения, однако при расчете возможного количества встраиваемой информации следует учитывать не только размер изображения, но и насыщенность цвета определенных составляющих.

Алгоритм предназначен для незаметного встраивания информации в изображения в целях защиты авторских прав.

В ходе анализа эффективности работы алгоритма и его устойчивости к различным преобразованиям, было выяснено, что он соответствует заявленной цели, но требует доработки для использования в реальной жизни. В связи с этим были предложены и реализованы некоторые способы оптимизации существующего алгоритма для расширения его функционала.