УДК 004.056.5

ОПРЕДЕЛЕНИЕ СТЕПЕНИ ПРИГОДНОСТИ КОНТЕЙНЕРА ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ МОДИФИКАЦИИ В СТЕГОСИСТЕМЕ, ОСНОВАННОЙ НА СОКРЫТИИ ТЕКСТОВЫХ ДАННЫХ В ИЗОБРАЖЕНИЯХ ПРИ ПОМОЩИ ДИСКРЕТНЫХ ПРЕОБРАЗОВАНИЙ

А.В. КОХАНОВСКИЙ
(***Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ***)

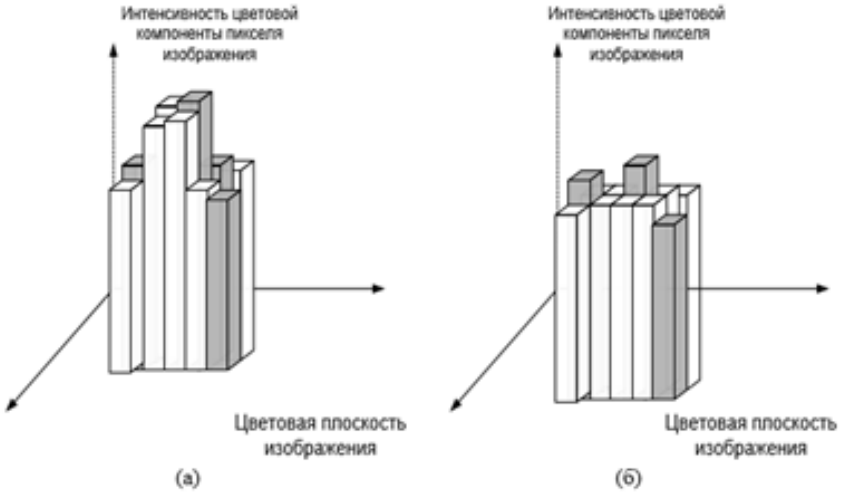
В статье определена степень пригодности контейнера для стеганографической модификации и представлены некоторые виды атак на стегосистему. Цель данной работы – построить систему, основанную на скрытии текстовых сообщений в изображениях, а также изучить атаки и выяснить, насколько пригодна такая система для практического применения. Задача решалась путём разбиения основной программы на библиотеки и вспомогательные подпрограммы. Программа написана на языке программирования C#.

Введение. Стеганографической модификации могут подвергаться как пространственные, так и частотные параметры контейнера-изображения. Для стеганографической модификации пригодны все эти параметры, но перед процедурой встраивания необходимо оценить пределы модификации параметров того или иного контейнера, а также вносимые при этом искажения. Пропускная способность, надежность, устойчивость стеганографической системы во многом будет определяться степенью модификации контейнера-изображения [1].

Оценка стеганостойкости реализованной системы. Каждое изображение обладает уникальными свойствами, которые можно положить в основу их разделения на классы.

1. Изображения с небольшим количеством цветов (4-16) и большими областями, заполненными одним цветом.
2. Изображения, построенные на компьютере, с плавными переходами цветов.
3. Фотореалистичные изображения.
4. Фотореалистичные изображения с наложением деловой графики.
5. Картографические изображения.
6. Космические изображения.

Для обеспечения незаметности факта скрытия данных в контейнерах-изображениях необходимо выбирать изображения, содержащие области с резкими переходами цветов, границы объектов, так как в них можно в больше степени скрыть небольшие изменения интенсивностей цветовых компонент пикселя контейнера по отношению к соседним пикселям (рис.). Модифицированные пиксели на рисунке выделены серым цветом. Видно, что даже незначительное изменение интенсивности какой-нибудь цветовой компоненты отдельных пикселей, в областях, заполненных одним цветом (рис. 1, *б*), увеличивает возможность визуального или компьютерного детектирования факта стеганографического скрытия данных.



***а* – область резкого перехода цветов; *б* – область, заполненная одним цветом**

Рисунок. – Цветовые плоскости модифицированных областей изображения

Анализ содержимого контейнеров-изображений целесообразно проводить при помощи математического преобразования, позволяющего выделить его частотные параметры и оценить вклад отдельных частот в состав изображения. Одним из таких преобразований является дискретное косинусное преобразование [2], применяемое к изображениям посредством окон размеров n×n пикселей. Дискретное косинусное преобразование позволяет получить информацию о резких и плавных границах цветов изображения, областях, заполненных одним цветом или с градиентным изменением цвета и др.

Оценку степени пригодности изображения для стеганографической модификации целесообразно проводить в два этапа.

На первом этапе изображения делятся на классы согласно относительному весу их пространственных частот. Положительные результаты получены при использовании спектральной классификации изображений, позволяющей провести их разбиение на 8 классов [3]. Классы с 1-го по 3-й описывают изображения с наибольшим относительным весом низких частот; классы с 4-ого по 7-ой разграничивают изображения по спектральным составляющим, сосредоточенным в областях близких к низкочастотному и/или высокочастотному диапазонам; восьмой класс отделяет изображения, имеющие равномерный спектр в пределах всего рассматриваемого диапазона.

На втором этапе оценивается пропускная способность изображения-контейнера путем исключения непригодных для модификации областей, например, заполненных одним цветом или градиентным изменением цвета. Обнаружить такие области на изображении возможно при анализе его спектрального состава (наличие границ на изображении приводит к увеличению вклада средних и высоких частот), так и при оценке изменения интенсивности пикселя по отношению к соседним пикселям.

В методе Коха-Жао для обеспечения незаметности факта скрытия данных в контейнерах-изображениях нежелательно использовать изображения с небольшим количеством цветов и большими областями, заполненными одним цветом (в частности, белым). Так как при этом, после шифрования на изображении будет наглядно виден факт скрытия информации.

Выделяются следующие типы атак для метода Коха-Жао:

1. Атаки против встроенного сообщения, направленные на удаление или порчу встроенной информации путем манипулирования заполненным контейнером. Входящие в эту категорию методы атак не нацелены на оценку и выделение сообщения. Примерами таких атак в данной работе является сжатие изображений.
2. Атака против встроенного сообщения, направленная на использование фильтров. При этом сообщение в изображении остается, но теряется возможность его приема. В эту категорию входят такие атаки, как атака с использованием эффектов в различных фоторедакторах.
3. Атака против встроенного сообщения, направленная на использование геометрических преобразований. Данная категория атак связана с усечением и изменением размерности нашего изображения.
4. Атака, направленные на изменении яркости и контрастности изображения. Данный вид атак связан с существенным изменением изображения.

Заключение. При выполнении данного проекта были выделены основные результаты и выводы:

1. Произведен анализ метода Коха-Жао, используемый для встраивания данных в изображения.
2. В работе были произведены многочисленные эксперименты, которые позволили дать определенные рекомендации по выбору атак для данного метода.
3. Метод Коха-Жао является достаточно устойчивым к существенному изменению изображений (контрастность, яркость и т.д.) и к геометрическим преобразованиям (размерность, повороты изображений и т.д.), связанных с ними.
4. При использовании в качестве атак фильтров и сжатия в формате JPEG зашифрованного изображения гарантировано разрушается встроенное сообщение.
5. Эффективность применения ДКП в данном методе для сжатия изображений объясняется тем, что оно хорошо моделируют процесс обработки изображения в системе человеческого зрения (СЧЗ), отделяет «значимые» детали от «незначимых». Значит, его более целесообразно применять в случае активного нарушителя.
6. В ходе тестирования программы при изменении разности коэффициентов (Р) и сравнении полученных результатов скрытия и извлечения информации, можно сделать вывод, что чем больше значение Р, тем стеганосистема, созданная на основе данного метода, является более стойкой к компрессии, однако качество изображения при этом значительно ухудшается.
7. Программа реализована и готова к использованию с возможностью ее доработки.

ЛИТЕРАТУРА

1. Садов, В. С. Компьютерная стеганография / В. С. Садов. – М: МГВРК, 2012. – 289 с.
2. Тихоненко, С.Г. Формирование критерия качества фильтрованных изображений / С. Г. Тихоненко // Тезисы докладов IX республиканской научной конференции студентов и аспирантов РБ, Гродно, 26-27 мая 2004 г. В 8-ми частях / Гродненский гос. университет; редкол.: А. И. Жук. – Гродно, 2004. – Ч.6. – С. 241– 243. 40.
3. Чернявский, А.Ф. Оценка информационных потерь при фильтрации изображений / А.Ф. Чернявский, С.Г. Тихоненко, В.С. Садов // Информатика. – 2005. – № 3(7). – С. 52–59.