УДК 004.021

ПРОЕКТИРОВАНИЕ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА СИСТЕМЫ ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ НА ОСНОВЕ ДИСКРЕТНЫХ ПРЕОБРАЗОВАНИЙ С ПОМОЩЬЮ АЛГОРИТМА КОХА И ЖАО

К.В. СТАНКЕВИЧ
(Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ)

Рассматривается проектирование графического интерфейса системы для скрытия информации на основе дискретных преобразований с помощью алгоритма Коха и Жао. Проведён анализ степени пригодности контейнера для модификации, моделирование атак и определение устойчивости к ним.

Введение. Развитие средств вычислительной техники в последнее десятилетие дало новый толчок для развития компьютерной стеганографии. Появилось много новых областей применения. Сообщения встраивают теперь в цифровые данные, как правило, имеющие аналоговую природу.

Интерфейс программы должен обладать целым рядом свойств: естественность, согласованность, дружественность, принцип «обратной связи», простота, гибкость, эстетическая привлекательность.

Основная часть. Любое приложение должно быть грамотно спроектировано и разделено на отдельные модули, которые должны быть относительно независимыми друг от друга. Подобное разделение значительно облегчает не только реализацию приложения, но и возможную его модификацию. В этом заключается принцип модульности объектно-ориентированного программирования.

Приложение «KochZhao» представляет собой приложение для скрытия информации в изображениях. Для скрытия сообщения необходимо будет выбрать контейнер (поддерживаемые форматы: bmp и png), выбрать скрываемый файл и указать настройки: P и размер сегментов (блоков). Для дальнейшего извлечения сообщения необходимо запомнить ключ, который будет выведен в соответствующем поле, и размер сегментов (блоков).

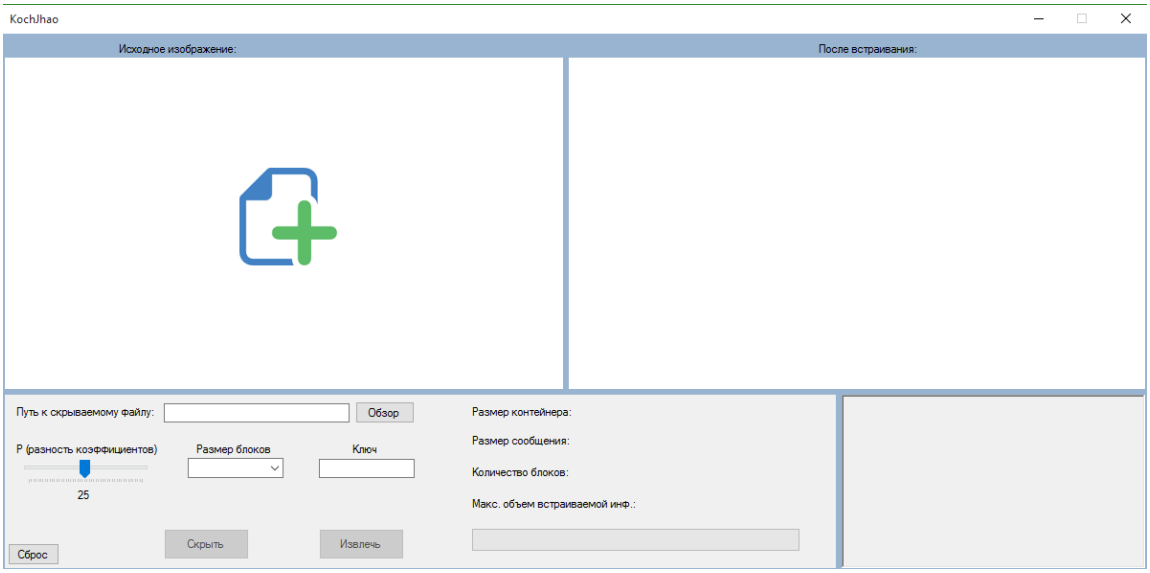

Рисунок 1. – Интерфейс программы

Для определения оптимального контейнера будем использовать различные изображения с преобладанием какой-то одной цветовой компоненты RGB.

В результате исследований было выявлено, что наиболее подходящими под контейнер являются изображения с преобладанием синей и зеленой компонентов.

Для определения устойчивости стеганосистемы проведены несколько видов атак: пассивного нарушителя, активного нарушителя.

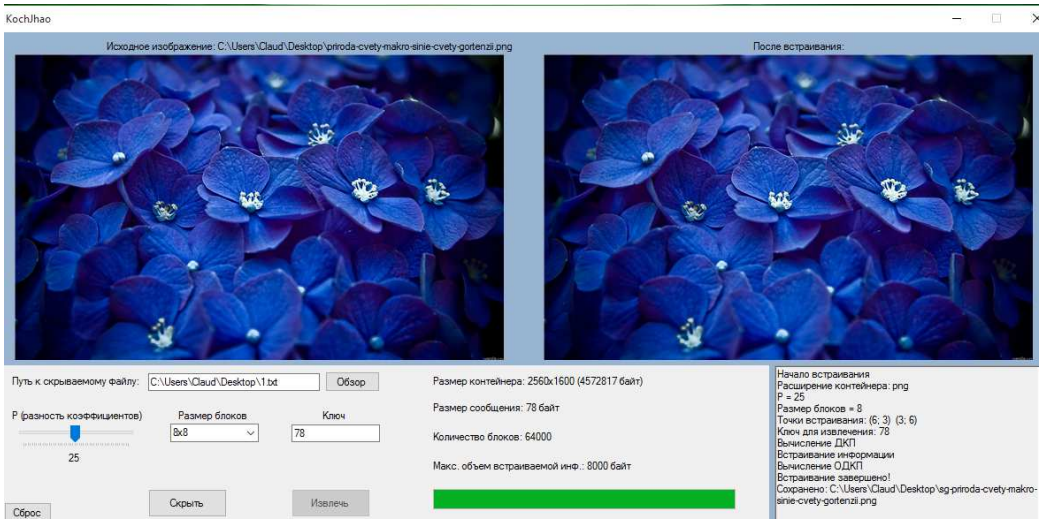

Рисунок 2. – Интерфейс шифрования

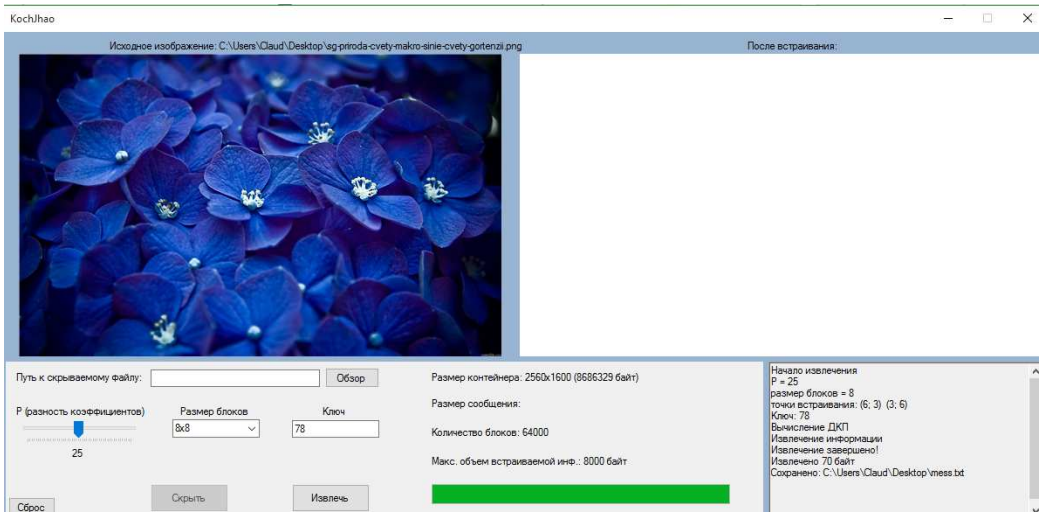

Рисунок 3. – Интерфейс дешифрования

Пассивной называется атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

Активной называется атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы активных атак:

1. отказ в обслуживании – DoS-атака (Denial of Service);
2. модификация потока данных;
3. создание ложного потока (фальсификация);
4. Повторное использование.

При попытках определить наличие в контейнере скрытого сообщения, при помощи функции программы Adobe Photoshop уровни каналов, было заметно выделение синего канала у некоторых пикселей, что свидетельствует о наличии скрытого сообщения.

При атаках активного нарушителя было выявлено, что алгоритм имеет устойчивость к большинству известных стеганоатак, в том числе к атаке сжатием, к аффинным преобразованиям, геометрическим атакам.

В результате, проведенных тестов выяснила следующее:

– изменение цветовой модели перед ДКП значительно ухудшило результат отношения сигнал/шум;

– встраивание в высокочастотную область спектра незначительно улучшило результат;

– встраивание в низкочастотную область спектра значительно ухудшило результат, уменьшится устойчивость к компрессии;

– уменьшение блока до размерности 4x4 незначительно улучшило результат, уменьшится устойчивость к компрессии;

– встраивание 2 бит в блок в среднечастотную и высокочастотную область улучшило результат.

Заключение. В данной статье рассмотрен способ построения графического интерфейса системы скрытия информации на основе дискретных преобразований, проведён анализ степени пригодности контейнера для модификации, моделирование атак и определение устойчивости к ним.

ЛИТЕРАТУРА

1. Матюшик, В.Н. Методы и средства стеганографии для защиты графических образов / В.Н. Матюшик. – Минск : Белорусский государственный университет информатики и радиоэлектроники.
2. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М. : СОЛОН-Пресс, 2002.
3. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев : МК-Пресс, 2006.