УДК 004.056.5

ПРОЕКТИРОВАНИЕ СТЕГОСИСТЕМЫ, 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 представлен практический способ создания надёжной стегосистемы с нестандартным способом сокрытия информации. Цель данной работы – построить систему, основанную на скрытии текстовых сообщений в изображениях, 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. В статье пойдёт речь о сокрытии данных в изображениях с помощью одного из методов стеганографии. Под цифровой стеганографией понимается скрытие одной информации в другой. Причем сокрытие это должно реализоваться таким образом, чтобы, во-первых, не были утрачены свойства и некоторая ценность скрываемой информации, а во-вторых, неизбежная модификация информационного носителя не только не уничтожила смысловые функции, но и на определенном уровне абстракции даже не меняла их. Тем самым факт передачи одного сообщения внутри другого не выявляется традиционными методами.

Принцип построения стеганографической системы и описание алгоритма скрытия данных. Стандартная стеганографическая схема сохраняется вне зависимости от технологии, которой она реализуется. Задачу встраивания и выделения сообщений из другой информации выполняет стегосистема. Стегосистема состоит из следующих основных элементов (рис.).

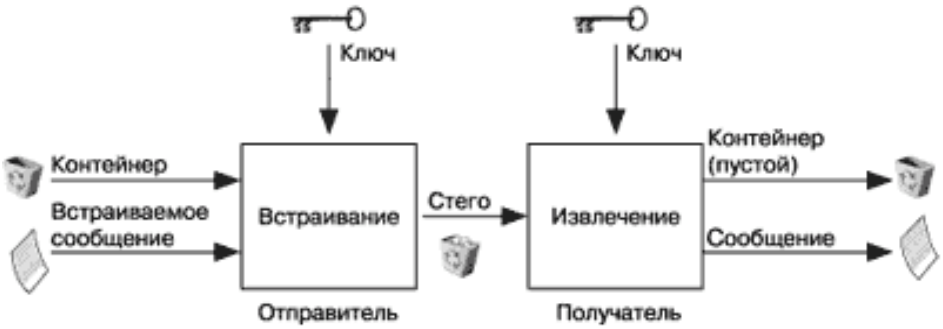

Рисунок. – Структурная схема типичной стегосистемы

В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п. Контейнер - любая информация, предназначенная для сокрытия тайных сообщений. Пустой контейнер - контейнер без встроенного сообщения; заполненный контейнер или стегоконтейнер, содержащий встроенную информацию. Встроенное (скрытое) сообщение - сообщение, встраиваемое в контейнер. Стеганографический канал или просто стегоканал - канал передачи стего. Стегоключ или просто ключ - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

Данные, содержащие скрытое сообщение, могут подвергаться преднамеренным атакам или случайным помехам. Как показано на рисунке 1, в стегосистеме происходит объединение двух типов информации так, чтобы они могли быть различимы двумя принципиально разными детекторами. В качестве одного из детекторов выступает система выделения ЦВЗ, в качестве другого – человек [1].

Стеганографические методы замены неустойчивы к любым искажениям, а применение операции сжатия с потерями приводит к полному уничтожению всей секретной информации, скрытой методом НЗБ в изображении. Более устойчивыми к различным искажениям, в том числе сжатию, являются методы, которые используют для сокрытия данных не временную область, а частотную [2].

Подавляющее большинство методов компьютерной стеганографии базируется на двух ключевых принципах:

– файлы, которые не требуют абсолютной точности (в данном случае файлы с изображением), могут быть видоизменены без потери своей функциональности;

– органы чувств человека неспособны надежно различать незначительные изменения в модифицированных таким образом файлах и/или отсутствует специальный инструментарий, который был бы способен выполнять данную задачу.

В основе базовых подходов к реализации методов компьютерной стеганографии в рамках той или иной информационной среды лежит выделение малозначительных фрагментов этой среды и замена существующей в них информации информацией, которую необходимо скрыть.

Рассматриваемый в данной работе, алгоритм Коха-Жао для встраивания информации использует частотную область контейнера и заключается в относительной замене величин коэффициентов дискретного косинусного преобразования (ДКП) [3].

Изображение разбивается на блоки размерностью 8×8 (в нашем случае на блоки размером 2×2, 3×3 и 4×4) пикселей и к каждому блоку применяется ДКП. Каждый блок пригоден для записи одного бита информации.

Алгоритм скрытия будет заключаться в следующем:

– итерируем изображение двойным массивом с шагом в 8;

– на каждой итерации создаем временный массив 8x8 пикселей, каждым элементом которого будет набор трех цветов пикселя;

– применяем ДКП к этому массиву, и получаем массив коэффициентов размером 8x8;

– выбираем 2 коэффициента и высчитываем их разность по модулю;

– если разность меньше или равна 25, то присваиваем первому коэффициенту положительное значение второго + константа, либо тоже самое, но со знаком минус (это называется передача бита);

– если разность меньше либо равна -25, то выполняем те же действия только для второго коэффициента;

– далее применяется обратное ДКП чтобы перевести наши коэффициенты обратно в пространственную область;

– после чего копируем новые значения цветов в изображение.

Достоинства метода:

– устойчивость к JPEG-компрессии с малым коэффициентом сжатия

Недостатки:

– заметное визуальное искажение изображения-контейнера при большом пороговом значении разницы между коэффициентами ДКП блоков;

– малый объем сообщения, который можно встроить.

Заключение. Исследования в области стеганографии очень перспективное направление защиты информации, так как в современном мире задача передачи секретной информации стоит наравне со скрытым общением, т.е. скрытия факта передачи сообщений. Поэтому, необходимо продолжать исследованиями в этой области для поиска новых, эффективных, методов или улучшения существующих. В данной работе был рассмотрен метод встраивания информации в изображения. Метод самый перспективный, однако, требует доработки в плане пропускной способности, и вероятности правильного извлечения встроенных бит информации. 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. Программный продукт реализован и готов к использованию с возможностью доработки.

ЛИТЕРАТУРА

1. Matsui K., Tanaka K., and Nakamura Y. Digital signature on a facsimile document by recursive MH coding / Symposium On Cryptography and In-formation Security, 1989.
2. Садов, В. С. Компьютерная стеганография / В. С. Садов. – М: МГВРК, 2012. – 289 с.
3. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин. – М.: СОЛОН-Пресс, 2002. – 272 с.