УДК 681.3

ИССЛЕДОВАНИЕ АНАЛИЗА СТОЙКОСТИ СТЕГАНОГРАФИЧЕСКИХ АЛГОРИТМОВ

А.Н. Михайлов, З.Б. Холодная
(Национальный аэрокосмический университет им. М.Е. Жуковского «ХАИ», Харьков)

Представлена структура программы для исследования робастности стегоинформации в неподвижных изображениях и реализован ее прототип.

стойкость, стеганографические алгоритмы, стегоинформация

Постановка проблемы и анализ литературы. Повышенный интерес к стеганографии, которая занимается разработкой средств и методов скрытия факта передачи сообщений [1], основан на двух факторах. Актуальность проблемы защиты авторских прав и ее использование как альтернативы криптографии, давно укоренившейся в области защиты информации. В отличие от криптографии, стеганография не шифрует, а укрывает данные от постороннего пользователя. Такое скрытие информации находит свое применение в традиционных «военных» организациях [2, 3].

Как следствие разделения направлений в использовании информационного скрытия, в современной литературе выделяют направление, занимающееся проблемами устойчивых маркеров авторских прав, называемое ЦВЗ (цифровой водяной знак – digital watermark) и цифровую стеганографию, как развитие традиционной стеганографии. В этих направлениях для скрытия информации применяются, главным образом, мультимедийные данные, простейшим видом которых является изображение.

Стегосистемой называется структура, внутри которой выполняется полный цикл обмена сообщениями средствами стеганографии. С одной стороны такой системы обязательно будет находиться устройство (стегокодер), скрывающее информацию в соответствии с определенным алгоритмом, который может учитывать или не учитывать характеристики встраиваемой информации и предполагаемого носителя (контейнера). Для изображения примерами таких характеристик могут быть: цветовые системы, используемые в контейнере и в исходном изображении, например, RGB, YCbCr, Grayscale, особенности человеческого зрения, изменение статистических характеристик изображения при внедрении

в него информации, в том числе в частотных областях изображения, интерпретируемого, как сигнал.

Со стороны получателя скрытой информации в стегосистеме должно находиться устройство (стегодекодер), выполняющее извлечение информации из контейнера. Это устройство, в зависимости от алгоритма, может использовать или не использовать пустой контейнер для выполнения своей задачи. В состав декодера может входить устройство, называемое детектором, которое выполняет задачу определения содержания в контейнере встроенной информации. Такой детектор, как правило, рассчитан на используемый в кодере алгоритм.

Информацию в стегосистеме передают по каналу, на концах которого и находятся кодер и декодер. К открытому каналу может подключаться устройство, используемое злоумышленником для атаки на контейнер. Пассивная атака – обнаружение информации в контейнере с определенной долей вероятности и, возможно, извлечение информации. В случае активной атаки злоумышленник изменяет содержание внедренной информации или удаляет её. Детекторы и декодеры злоумышленника обычно содержат несколько возможных алгоритмов встраивания.

К наиболее распространенным алгоритмам внедрения информации в изображение можно отнести метод наименее значащих бит [3, 4], его модификации [5, 6, 7] и скрытие данных в коэффициентах дискретного косинусного преобразования [3, 5, 8] при котором изображение обычно разбивается на блоки размером 8 × 8 пикселей, и ДКП применяется к каждому блоку.

Из атак, обнаруживающих содержание встроенной информации в изображении, отметим следующие:

– статистическая атака по критерию согласия χ^2;

– тест длины серий, основанный на том, что в случайной последовательности серии большой длины встречаются значительно реже, чем в незначащих битах реальных сигналов;

– визуальная атака, при которой исследуются признаки дисгармонии изображения в общем и в отдельных битовых слоях.

– Существующие в настоящее время утилиты стегосистем, можно разделить на три группы:

– утилиты-тестеры, обнаруживающие и извлекающие информацию. Лучше других зарекомендовала себя в этой области программа комплексных тестов StirMark [3];

– утилиты, встраивающие информацию. Примером может служить утилита Steganos File Manager коммерческого пакета Steganos Security Suite 6 [9], выполняющая внедрение информации в BMP и WAV-файлы;

– комплексные утилиты, выполняющие все описанные выше действия. Характерными представителями этого класса являются утилиты Hide and Seek, S-Tools, Ez-Stego, рассмотренные в работе [10].

Опишем характеристики упомянутых и некоторых других утилит.

StirMark – программа использует комплексный тест, включающий аффинные преобразования медианный (для встроенной информации, имеющей распределение Лапласа) и усредняющий (для гауссовского распределения) фильтры и др. Авторы программы заявляют, что на данный момент не существует открытого алгоритма, устойчивого к их комплексному тесту.

Steganos Security Suite 6 – коммерческий пакет, объединивший множество утилит и почему-то имеющий к криптографии отношение большее, чем к стеганографии, несмотря на название. В пакет входит всего одна стеганографическая утилита (из имеющихся семи), работающая только с одним графическим файловым форматом – BMP.

Hide and Seek v4.1b – скрывает информацию и выполняет ее поиск в GIF файлах.

S-Tools – стеганографическая программа для Windows; скрывает данные в файлах формата BMP, GIF, WAV и на свободном пространстве дискет.

Hide4PGP v1.0 – внедряет метки в 8- или 24-битные файлы BMP, 8- или 16-битные файлы WAV и 8-битные VOC-файлы.

Wnstorm (White Noise Storm) – криптографическая и стеганографическая программа для введения водяных цифровых знаков в PCX-файлы.

Jpeg-Jsteg v4 – утилита предназначена специально для работы с файлами формата JFIF JPEG. Использует как стеганографические, так и криптографические методы.

Все рассмотренные популярные программы имеют ряд недостатков. Так, большинство из них не имеют удобного для пользователя графического интерфейса. Только некоторые программы имеют приемлемую контекстную справку, хотя все программы снабжены документацией. Кроме того, ни одна из этих программ не является автоматически расширяемой.

Целью данной работы является описание прикладной программы, которая может быть использована как инструмент скрытия информации и обнаружения стегоинформации, свободный от указанных недостатков.

Для решения задач стеганографии разработана программа-прототип: система анализа стегоалгоритмов «CAC Duul». Программное изделие представляет собой приложение ОС Windows, выполняющее анализ робастности изображений по отношению к атакам. При разработ-

ке структуры приложения были выделены две основные части: расчетная и интерфейсная.

Общая схема архитектуры приложения приведена на рис. 1.

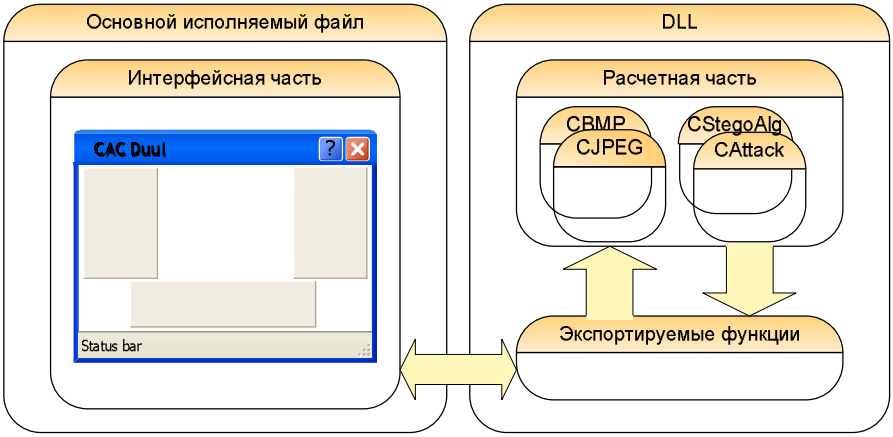

Рис. 1. Архитектуры приложения

В расчетной части реализованы основные алгоритмы внедрения информации (метод наименее значащих бит и алгоритм встраивания в коэффициенты ДКП), основные стегоатаки (визуальная, с гистограммой, атака сжатием JPEG, аффинные преобразования, субполосная фильтрация), а также возможность автоматического подгружения скомпилированных библиотек, содержащих сторонние стегоалгоритмы и стегоатаки. Расчетная часть выполнена на языке C++.

В интерфейсной части разработан удобный пользовательский интерфейс на основе полнофункционального оконного приложения, соответствующего современным требованиям эргономичности (реализация «плавающих» панелей, настройка пользовательского меню и пиктограмм инструментальных панелей), а также подробная контекстная справка, основанная на структурированных файлах формата chm, обработка которых встроена в Windows и поддерживается Delphi 7.

При разработке структур данных создана иерархия классов, в соответствии с разделением на расчетную и интерфейсную части. Так, например, иерархия расчетных классов содержит классы изображений, в том числе со встроенными данными; классы-коллекции изображений; классы стегоалгоритмов внедрения информации в изображение; классы атак на изображения; вспомогательные классы и типы данных.

Общий алгоритм работы приложения приведен на рис. 2.

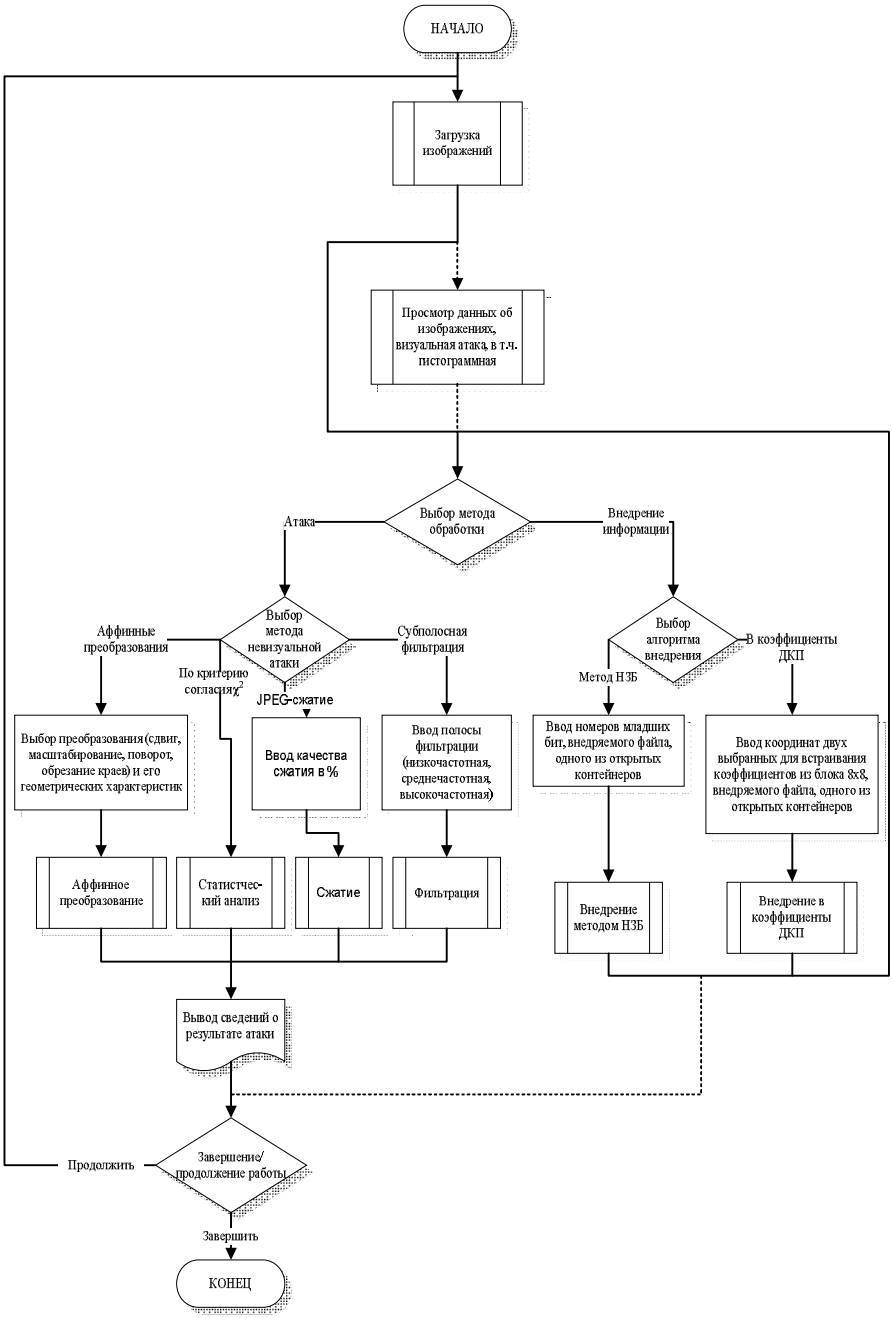

Рис. 2. Алгоритм работы приложения

Вывод. Разработанное приложение может быть использовано для встраивания информации различной природы (изображение, текст) в неподвижные изображения, а также как инструмент предварительного апробирования качества такого встраивания. Приложение можно также применять как детектор информации в изображениях-контейнерах, созданных без его помощи.

ЛИТЕРАТУРА

1. *Введение в криптографию / Под общ. ред. В.В. Ященко. – СПб.: Питер, 2001. – 288 с.*
2. *Kessler Gary C. Steganography: Implications for the Prosecutor and Computer Forensics Examiner // National District Attorney's Association Newsletter, April 2004. – [Электрон. ресурс]. – Режим доступа: http://www.fbi.gov/hq/lab/fsc/backissu/july2004/researc/ 2004 03 research01.htm, 2004.*
3. *Petitcolas F.A.P., Anderson Ross J., Kuhn Markus G. Attacks on Copyright Marking Systems // Second workshop on information hiding, in vol. 1525 of Lecture Notes in Computer Science, Portland, Oregon, USA, 14-17 April, 1998. – P. 218-238.*
4. *Celik Mehmet U., Sharma Gaurav, Tekalp A. M. Universal Image Steganalysis Using Rate-Distortion curves // SPIE: Security, Steganography, and Watermarking of Multimedia Contents VI, San Jose – Jan 2004. – Vol. 5306. – P. 19-22*
5. *Грибунин В.Г., Оков В.Г., Туринцев И.В. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.*
6. *Алиев А.Т. О применении стеганографического метода LSB к графическим файлам с большими областями монотонной заливки // Вестник ДГТУ. – 2004. – Т. 4. – № 4 (22). – С. 45-51.*
7. *Fridrich J., Goljan M. Digital image steganography using stochastic modulation // Department of Electrical and Computer Engineering; SUNY Binghamton, Binghamton, NY, USA.*
8. *Wang Y., Moulin P. Steganalysis of block-DCT image steganography // University of Illinois at Urbana-Champaign; Beckman Institute, CSL&ECE Dept., Urbana, USA.*
9. *Кучук Г.А. Моделирование трафика изолированного пульсирующего источника // Системи обробки інформації. – Х.: ХВУ, 2004. – Вип. 1. – С. 168-173.*
10. *Johnson Neil F. Steganography. – [Электрон. ресурс]. – Режим доступа: http://www.gmu.edu, 2003.*

Поступила 22.06.2006

Рецензент: доктор технических наук, профессор В.С. Харченко,
Национальный аэрокосмический университет
им. Н.Е. Жуковского «ХАИ», Харьков.