ВЫБОР ПРОГРАММНЫХ СРЕДСТВ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ ДЛЯ ИССЛЕДОВАНИЯ ЭФФЕКТИВНОСТИ СКРЫТИЯ ГРАФИЧЕСКОЙ ИНФОРМАЦИИ

Савостьянчик Вадим Вячеславович,
Алефиренко Виктор Михайлович,
УО «Белорусский государственный университет информатики и радиоэлектроники», г. Минск

E-mail: magistrsavostyanchik@gmail.com,
E-mail: alefirenko@bsuir.by

Аннотация. Проведен анализ программных средств компьютерной стеганографии и предложены критерии их выбора для исследования эффективности скрытия графической информации.

Ключевые слова: программные средства, стеганография, критерии, эффективность.

На сегодняшний день существует достаточно много программных средств, которые применяются для целей стеганографии и реализующих, как правило, функции внедрения секретных данных в графические, звуковые и видео файлы. Многие из них бесплатны или условно бесплатны (shareware). Каждое из таких программных средств имеет свои возможности, принцип работы, а также преимущества и недостатки (таблица 1) [1-3].

Таблица 1

Программные средства стеганографического скрытия данных

Наименование	Возможности	Принцип работы	Преимущества	Недостатки	Операционная система
Outguess Rebirth steganography 1.1	Позволяет пользователю вставлять скрытые данные внутри изображения JPEG	Скрытие данных в младших битах, отличных от нуля, квантованных коэффициентов блоков изображения	Возможность контроля вносимых статических искажений, большая стойкость к атакам	-	UNIX
Steganos	Сокрытие в графических файлах BMP, DIB, VOC, WAV, ASCII	Скрытие информации путем замены младших битов элементов изображения	Заполнение неиспользованного пространства контейнера шумоподобным сигналом	Использование устаревших форматов контейнеров	MS-DOS и Windows

Продолжение таблицы 1

Наименование	Возможности	Принцип работы	Преимущества	Недостатки	Операционная система
Gifshuffle		Скрытие информации посредством изменения порядка цветов в палитре	Возможность предварительного сжатия или шифрования скрываемого сообщения	Малый объем скрываемого сообщения, не зависящий от размера контейнера	MS-DOS
DC-Stegano	Сокрытие данных в графических файлах в формате PCX	Скрытие посредством замены младших битов цветовых индексов точек изображения		Отсутствие стего-ключа, строго заданный размер изображения-контейнера	MS-DOS
Steganography Tools 4	Предварительно кодирует данные с помощью алгоритмов шифрования IDEA, MPJ2, DES TripleDES и NSEA, а затем прячет их в графических файлах, звуковых (WAV) файлах или свободных секторах флоппи-дисков				Windows
StegoWAV	Внедрение данных в аудиоданные в формате PCM(WAV)	Сокрытие информации путем замены младших битов элементов контейнера	Шифрование скрываемого сообщения, распределение скрываемой информации по контейнеру	Неразвивающийся продукт, использование устаревших форматов контейнеров	Windows
Stegahan	Сокрытие данных в графических BMP- и звуковых WAV файлах			Неразвивающийся продукт, использование устаревших форматов контейнеров	UNIX
JSTEG	Одна из программ стеганографии для встраивания данных в изображения JPEG	По принципу реализации похожа на LSB для формата BMP, иными словами на замену наименее значащего бита в цветовом пространстве	Первая общедоступная программа для стеганографии в JPEG Простота использования	Похожа на LSB для BITMAP изображений Для выявления факта скрытия эффективен анализ гистограмм. Эффективна визуальная атака на изображение, модифицированное программой JSTEG	MS-DOS
Steghide	Сокрытие данных в графических BMP- и звуковых WAV- и AU-файлах	Скрытие информации путем замены младших битов элементов изображения	Возможность предварительного шифрования скрываемого сообщения		MS-DOS

Продолжение таблицы 1

Наименование	Возможности	Принцип работы	Преимущества	Недостатки	Операционная система
Invisible Secrets 2002	Внедрение данных в аудиоданные в формате PCM, WAV, BMP, DIB, VOC, HTML, ASCII	Скрытие информации путем замены младших битов элементов контейнера, а также путем добавления пробелов в конце строки для формата ASCII	-	Отсутствие распределения скрываемой информации по контейнеру, отсутствие предварительного анализа контейнера на пригодность	Windows
Steganos for Windows		-	Заполнение неиспользованного пространства контейнера шумоподобным сигналом	Использование устаревших форматов контейнеров	Windows
Hide4PGP		-	Распределение скрываемой информации по контейнеру	Отсутствие предварительного анализа контейнера на пригодность	Windows
Наименование	Возможности	Принцип работы	Преимущества	Недостатки	Операционная система
MP3Stego	Внедрение данных в аудиоданные в формате PCM (WAV)	Скрытие информации на основе изменения четности при квантовании частотных коэффициентов на этапе сжатия аудиопотока	Сжатие и шифрование скрываемого сообщения, зашумление неиспользуемого пространства контейнера	Нестойкость к атакам активного противника (к уничтожению данных)	Windows и Unix
UnderMP3 Cover		Скрытие информации путем встраивания в контейнер некорректных MP3 кадров	-	Низкая стойкость к пассивному стегоанализу.	UNIX
WNS (белый шумовой шторм)	Универсальная программа стеганографии	Предварительно скрываемый файл шифруется алгоритмом PGP и затем скрывается в контейнер	Хорошее качество сопровождающей документации	Завышенные требования к размерам контейнера за счет выбранного метода шифрования	DOS

Продолжение таблицы 1

Covert_TCP	Программа управляет TCP_IP заголовком и передает с каждым файлом один скрытый байт	Передача скрытых данных осуществляется как с пакетами данных, так и со служебными пакетами	Большие возможности передачи скрытых данных. Программа может работать как станция и как пользователь	Инструмент полезен для обхода систем сетевой защиты и для экспорта данных с безвредными пакетами, которые не содержат никаких данных для анализа	Linux, Solaris, UNIX
SecurEngine	Внедрение данных в текстовые файлы, графические файлы (BMP, JPG) и аудиофайлы (WAV)	-	Сжатие и шифрование скрываемого сообщения	Все скрываемые данные предварительно шифруются	Windows
Masker	Позволяет скрывать сообщения среди исполняемых, видео- и аудиофайлов, а также в изображениях. Поддерживает огромное число форматов, среди которых есть как форматы прямого кодирования, так и сжимающие (JPEG, MP3, MPEG)			Прячет любые файлы и целые папки. Раскрывает файлы-носители и извлекает спрятанные файлы	Windows
ImageSpyer G2	Утилита для сокрытия информации в графических файлах с использованием криптографии При этом поддерживается около 30 алгоритмов шифрования В качестве исходных графических файлов могут использоваться форматы BMP, JPEG, WMF, EMF, TIFF	Скрывает объем, равный числу пикселей изображения. Опционально доступна компрессия скрываемых данных		Безопасность обеспечивается целым рядом параметров секретности, не зная которые злоумышленник не сможет определить наличие скрытой информации	Windows
RedJPEG	Предназначена для сокрытия любых данных в JPEG в изображении	Использует открытые алгоритмы шифрования, поточный шифр AMPRNG и Cartman II DDP4 в режиме хеш-функции, LZMA-компрессию		Поддерживает режим случайного секретного распределения	Windows
DarkCryptTC	Эту программу можно назвать наиболее мощным стеганографическим решением. Она поддерживает более сотни различных симметричных и асимметричных криптоалгоритмов. Включает в себя поддержку собственной системы плагинов, предназначенной для блочных шифров (BlockAPI), текстовую, аудио и графическую стеганографию (включая реальную стеганографию JPEG), мощный генератор паролей и систему уничтожения информации и ключей. Поддерживает следующие форматы: *.txt, *.html, *.xml, *.docx, *. odt, *.bmp, *jpg, *.tiff, *.png, *.jp2, *.psd, tga, *.mng, *.wav, *.exe, *.dll.			Определение шифрованного файла по содержимому. Хранение информации о методе шифрования и режиме в заголовке файла. Возможность хранения ключа шифрования в текстовом файле каждого файла	Windows

Однако для исследования эффективности скрытия графической информации необходимо выбрать ограниченное количество программных средств. Для этого необходимо определить критерии, по которым необходимо осуществлять выбор.

Вначале проведем предварительный анализ программных средств. Программы, работающие на операционной системе «UNIX», «MS-DOS» и «Linux» рассматриваться не будут, так как в большинстве случаев используются программы с операционной системой Windows.

Из всех перечисленных программ остаются следующие:

- Steganos;
- Invisible secrets 2002;
- Steganos for windows;
- Masker;
- Hide4pgp;
- Stegowav;
- Steganography tools 4;
- S-tools;
- Mp3stego;
- Securengine;
- Darkcrypttc.

Для дальнейшего выбора необходимо выбрать параметры, по которым будут сравниваться оставшиеся программы. Существует достаточно большое число параметров, влияющих на эффективность использования программ компьютерной стеганографии, которые носят как количественный, так и качественный характер. В качестве примера количественных параметров можно привести отношение максимального размера встраиваемого сообщения, не приводящего к искажению изображения, к размеру самого контейнера, количество используемых форматов, а качественных – виды используемых форматов, возможность шифрования информации. Однако, если количественные параметры легко поддаются сравнению, то с количественными параметрами дело обстоит сложнее. Например, одни виды форматов имеют большее распространение (в том числе и в сети Интернет), чем остальные, что является положительным фактором. Однако для некоторых из этих форматов разработан широкий спектр методов и инструментов стеганоанализа. С этой точки зрения эти форматы являются более уязвимыми, а значит и менее эффективными с точки зрения стеганографии.

Проанализировав параметры рассмотренных программных средств компьютерной стеганографии и с учетом вышеизложенного, можно рекомендовать следующие параметры (критерии) их выбора для исследования эффективности скрытия графической информации [4]:

- скрытность или стеганографическая стойкость, которая связана с

изменениями (искажениями), вносимыми в исходное изображение при встраивании сообщения;

- размер встраиваемого сообщения, который характеризуется процентным соотношением между объемом встраиваемого сообщения и исходным объемом контейнера;

- устойчивость к модификации заполненного контейнера (сжатию), которая характеризует вероятность восстановления сообщения;

– объем вычислений, необходимый для встраивания сообщения в цифровое изображение;

– количество используемых графических форматов;

– возможность шифрования и их количество.

Таким образом, программы Steganos; Invisible secrets 2002; Steganos for Windows; Hide4pgp; Stegowav; Steganography tools 4; S-tools; Mp3stego и Securengine не подходят по предложенным критериям, так как у одних из них либо недостаточное количество форматов, либо они используют устаревшие форматы, а у других – размер встраиваемого сообщения слишком мал, либо количество алгоритмов шифрования слишком мало, либо их вовсе нет. В итоге наиболее подходящими остаются лишь две программы – Darkcrypttc и Masker, которые подходят по всем предложенным критериям.

Литература:

1. Стеганография [Электронный ресурс]. - Режим доступа: http://ru-steganography.narod.ru/

2. Программные средства стеганографического сокрытия данных [Электронный ресурс]. - Режим доступа: http://www.bnti.ru/showart.asp?aid=643&lvl=04.03.07.

3. Darkcrypttc [Электронный ресурс]. - Режим доступа: http://wincmd.ru/plugring/darkcrypttc.html

4. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. - М.: Солон-Пресс, 2002. - 272 с.