УДК 004.056

ИССЛЕДОВАНИЕ И ВЫБОР ПРОГРАММНЫХ СРЕДСТВ КОМПЬЮТЕРНОЙ СТЕГАНОГРАФИИ ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ ПО ОТКРЫТЫМ КОММУНИКАЦИОННЫМ КАНАЛАМ

В.М. АЛЕФИРЕНКО

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 6 февраля 2018

Аннотация. Предложены критерии для сравнительного анализа программных средств компьютерной стеганографии. Проведено обоснование и выбор программных средств для исследований. Проведены экспериментальные исследования выбранных программных средств по предложенным критериям, и на основании анализа полученных результатов определено наиболее эффективное программное средство компьютерной стеганографии для скрытия информации.

Ключевые слова: защита информации, программное средство, компьютерная стеганография, выбор программных средств.

Abstract. Criteria for comparative analysis of a computer steganography software are offered. Substantiation and choice of software for researches are carried out. Pilot studies of the chosen software by the offered criteria are conducted and on the basis of the obtained results analysis of the most effective software of a computer steganography for concealment of information is defined.

Keywords: information security, software, computer steganography, software choice.

Doklady BGUIR. 2018, Vol. 118, No. 8, pp. 5-11
Research and choice of computer steganography software for concealment of information transferred through open communication channels
V.M. Alefirenko

Введение

В открытых коммуникационных каналах, таких как проводной телефон, сотовый телефон, радиотелефон, радиостанция, сеть Интернет, для скрытия передаваемой информации могут использоваться такие традиционные методы, как кодирование, скремблирование и шифрование информации. С появлением компьютерных технологий появилась возможность использования стеганографических методов скрытия информации, получивших название методов компьютерной стеганографии, которые базируются на двух основных принципах [1]. Первый принцип заключается в том, что файлы, представляющие собой оцифрованное изображение или звук, могут быть видоизменены до определенной степени без потери их функциональности. Второй принцип заключается в том, что органы чувств человека имеют ограниченные разрешающие характеристики (дифференциальные пороги различения) и не способны различать незначительные изменения в цвете изображения или качестве звука. Эти принципы особенно хорошо реализуются для файлов изображения или звука, которые несут некоторую избыточную информацию.

Существует большое число различных методов, реализующих принципы компьютерной стеганографии, для которых разработаны соответствующие программные

средства. Каждое программное средство характеризуется рядом количественных и качественных параметров, на основании которых пользователь выбирает его для решения своей задачи по скрытию информации. Состав, количество и численные значения этих параметров у каждого программного средства может быть свой. Поэтому выбор программного средства, которое эффективно может решить поставленную задачу по скрытию конкретного вида информации, представляет для пользователя определенные трудности. Немаловажным фактором является и правильный выбор контейнера, используемого для скрытия информации и подходящего по своим параметрам для выбранного программного средства.

Решение проблемы

На сегодняшний день для скрытия информации используется достаточно большое количество различных программных средств. Как показал обзор, количество таких программных средств превышает два десятка [2]. В большинстве случаев эти программные средства позволяют скрывать секретную информацию в графических, звуковых и видеофайлах. Многие из них являются бесплатными или условно бесплатными. Каждое имеет свои функциональные возможности, а также преимущества и недостатки в отношении скрытия того или иного вида информации. Однако для того, чтобы провести исследования их эффективности по скрытию информации, необходимо выбрать некоторое ограниченное число программных средств.

Вначале необходимо провести предварительный анализ имеющихся программных средств компьютерной стеганографии. Так как в большинстве случаев для скрытия информации используются стеганографические программы, работающие под управлением операционной системы Windows, то программы, работающие под управлением операционных систем «MS-DOS», «UNIX» и «Linux», в дальнейшем рассматриваться не будут.

Из остальных оставшихся программ для дальнейшего анализа были выбраны следующие: Steganos, Steganos for Windows, StegoWAV, MP3Stego, SecurEngine, InvisibleSecrets 2002, Masker, OpenStego, Hide4PGP, SteganographyTools 4, S-tools, DarkCryptTC.

Для дальнейшего выбора программных средств необходимо выбрать ряд параметров, по которым будут сравниваться оставшиеся программы. Как показал анализ выбранных программных средств, они характеризуются достаточно большим количеством различных параметров, влияющих на эффективность их использования. Эти параметры могут быть как количественными, так и качественными. К количественным параметрам относятся размер встраиваемого сообщения, количество алгоритмов шифрования, количество используемых форматов и др., а к качественным – возможность сжатия информации, виды используемых форматов, возможность шифрования информации и др. Количественные параметры, выраженные числовыми значениями, достаточно легко поддаются сравнению, и их можно использовать напрямую, применив, например, метод парных сравнений. Что касается качественных параметров, то при их сравнении возникают определенные трудности. Например, при равенстве количества видов форматов, используемых в нескольких программных средствах, одни из них могут иметь более широкое распространение, чем другие, что является положительным фактором. Но для более распространенных видов форматов, как правило, существует и более широкий набор различных программных средств, используемых для их стегоанализа, что является отрицательным фактором.

На основании проведенного анализа количественных и качественных параметров рассмотренных выше программных средств компьютерной стеганографии для исследования эффективности скрытия графической информации можно рекомендовать следующие параметры (критерии) их выбора:

– количество используемых графических форматов;

– возможность шифрования данных и количество алгоритмов шифрования;

– размер встраиваемого сообщения, который характеризуется отношением объема встраиваемого сообщения к объему контейнера;

– возможность сжатия информации, которая характеризует устойчивость заполненного контейнера к модификации;

– скрытность или стойкость к стегоанализу, которая связана с количественными или качественными изменениями (искажениями), вносимыми в контейнер при встраивании сообщения;

– возможность скрытия нескольких сообщений в одном контейнере.

Проведенный анализ оставшихся программных средств показал, что такие программы, как Steganos, Steganos for Windows, StegoWAV, MP3stego, SecurEngine, InvisibleSecrets 2002, Hide44PGP, SteganographyTools 4 и S-tools не подходят по предложенным критериям: одни из них имеют малое количество форматов или используют устаревшие форматы, другие имеют малый размер встраиваемого сообщения или у них отсутствует возможность шифрования информации. В итоге для дальнейших исследований были выбраны три программы – Masker, OpenStego и DarkCryptTC, которые подходят по всем предложенным критериям.

Большое влияние на надежность используемой стегосистемы и возможность обнаружения факта передачи скрытой информации оказывает выбор контейнера. От вида контейнера зависит не только объем скрываемого сообщения, но и его устойчивость к различным методам стегоанализа. Выбор контейнера должен проводиться с учетом используемого метода внедрения в него скрываемой информации. Также должен учитываться и факт существования методов анализа, позволяющих обнаружить скрываемую информацию [3].

Для проводимых исследований выбор контейнера был осуществлен для скрытия информации методом замены младших бит (LSB-метод), на основе которого и реализовано большинство программных средств компьютерной стеганографии. Учитывалась также возможность предварительного визуального стегоанализа контейнера, как первичного этапа анализа на наличие в нем скрытой информации.

При выборе контейнеров использовались следующие критерии:

– отказ от общеизвестных изображений в качестве контейнера, например, картины различных художников;

– отказ от использования изображений, которые конвертированы из *JPEG*-формата в *BMP*-формат;

– использование изображений, полученных с помощью фотокамеры или сканера;

– большой размер контейнера;

– наличие зашумленности контейнера;

– отсутствие полезной составляющей на младших битовых разрядах изображения;

– отсутствие плавных тоновых переходов и монотонных областей;

– наличие большого количества перепадов яркости;

– многоцветность;

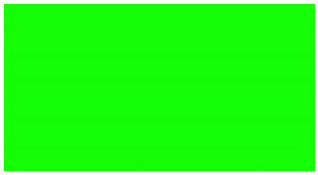
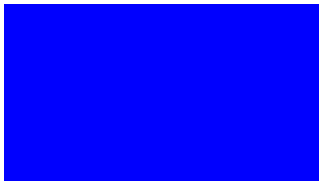
– наличие большого количества пикселей, у которых оттенки цветов плохо различаются зрительным анализатором человека.

Эти критерии в достаточной степени учитывают все особенности, которые необходимо принимать во внимание при выборе стегоконтейнера, устойчивого к визуальному стегоанализу и в котором для скрытия информации используется метод замены младших бит [4].

Так как в большинстве случаев обычно используются самые популярные форматы изображений, такие как jpeg, bmp, то в качестве контейнеров были выбраны изображения в форматах jpeg и bmp с глубиной цвета 24 бит. Чем больше размер изображения, тем сложнее обнаружить искажения. В итоге для проведения экспериментальных исследований в качестве контейнеров были выбраны картинки зеленого, красного, синего цвета и их сочетания, создающие полихромное изображение с последовательным плавным переходом цветов,

а также полихромные фотографии, которые представлены в табл. 1. В качестве скрываемой информации использовался аудиофайл с расширением wav и размером 55 кБ.

Таблица 1. **Виды контейнеров и их характеристики**

Изображение	Расширение	Размер файла, кБ	Размер, пикселей	Глубина цвета, бит
 Зеленый	jpeg	69	1920×1080	24
 Красный	jpeg	32,5	1920×1080	24
 Синий	jpeg	185	1920×1080	24
 RGB	jpeg	415	1200×941	24
 Тигр	jpeg	85	800×615	24
 Город	bmp	5930	610×460	24

Результаты и их обсуждение

Результаты экспериментальных исследований выбранных программных средств стеганографии представлены в табл. 2 и 3 (для программы DarkCryptTC).

Анализ полученных результатов исследований показывает:

– файлы одинаковых стегоконтейнеров для различных программ имеют разный размер, что обусловлено различной степенью сжатия исследуемых программ;

– как видно визуально, для всех программ зрительные отличия между контейнерами и стегоконтейнерами не наблюдались;

– программа OpenStego в меньшей степени подходит для скрытия информации, так как имеет худшие характеристики по сравнению с другими программами; кроме того, значительным минусом является то, что вне зависимости от формата исходного изображения (файла-контейнера), программа OpenStego сохраняет результат только в формате PNG;

– программа Masker хотя и имеет лучшие характеристики по сравнению с программой OpenStego и даже ряд дополнительных возможностей (возможность скрывать любые файлы и целые папки; шифрует и сжимает скрытые файлы; имеет защиту от посторонних пользователей), но тем не менее уступает программе DarkCryptTC;

– программа DarkCryptTC имеет лучшие на данный момент характеристики, а также более широкие дополнительные возможности, такие как:

– поддержка асимметричного шифрования RSA/Elgamal/ECC с использованием пары «публичный – секретный ключ»;

– поддержка шифрования одного файла в XDC и группы файлов/каталогов в Tar.XDC;

– возможность хранения информации о методе шифрования в заголовке файла;

– возможность хранения ключа шифрования в самом текстовом файле;

– определение шифрованного файла по содержимому;

– работа с фиксированным ключом шифрования и дешифрования;

– удобная и простая настройка параметров шифрования для каждого файла;

– встроенный генератор ключевых текстовых файлов произвольной длины ключа;

– возможность добавления комментария в архив;

– опциональная возможность использования мощной BWT компрессии алгоритмом ABC;

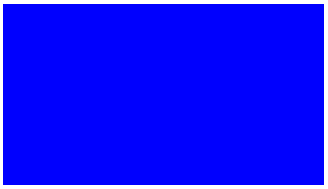
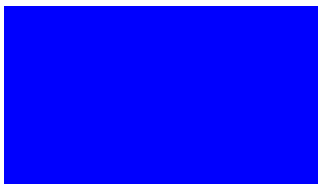
– повышение безопасности путем отключения подсчета контрольной суммы исходного файла и др.

Таким образом, по результатам проведенных экспериментальных исследований можно сделать заключение, что среди рассмотренных программ компьютерной стеганографии программа DarkCryptTC является наиболее эффективной для скрытия информации.

Таблица 2. **Результаты экспериментальных исследований программ стеганографии**

Параметры (критерии)	Программы стеганографии		
	Masker	OpenStego	DarkCryptTC
Количество форматов	12	6	12
Количество алгоритмов шифрования	7	1	40
Размер встраиваемого сообщения для графических/звуковых форматов, %	10/6,5	10/–	10/8
Возможность сжатия информации	+	+	+
Стеганографическая стойкость/скрытность	–	–	+
Возможность скрытия нескольких сообщений в одном контейнере	+	+	+

Таблица 3. **Результаты экспериментальных исследований программы DarkCryptTC**

DarkCryptTC		Размер контейнера, кБ	Размер стегоконтейнера, кБ
Контейнер	Стегоконтейнер		
 Зеленый	 Зеленый	69	310
 Красный	 Красный	32,5	219
 Синий	 Синий	185	600
 RGB	 RGB	415	1175
 Тигр	 Тигр	85	392
 Город	 Город	5930	14963

Заключение

Сравнительный анализ программных средств компьютерной стеганографии, проведенный по предложенным критериям, показал, что наибольшими возможностями по скрытию информации обладает программа DarkCryptTC. В качестве критериев были выбраны: количество используемых графических форматов; возможность и количество алгоритмов шифрования; размер встраиваемого сообщения; устойчивость заполненного контейнера к модификации (сжатию); скрытность или стойкость к стегоанализу; возможность скрытия нескольких сообщений в одном контейнере. Проведено обоснование выбора контейнеров для скрытия информации, в качестве которых выбраны картинки зеленого, красного, синего цвета и их сочетания, создающие полихромное изображение с последовательным плавным переходом цветов, а также полихромные фотографии.

Список литературы

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.
2. Савостьянчик В.В., Алефиренко В.М. Выбор программных средств компьютерной стеганографии для исследования эффективности скрытия графической информации // Science Time. 2017. № 11 (47). С. 37–42.
3. Основы компьютерной стеганографии / А.В. Аграновский [и др.]. М.: Радио и связь, 2003. 152 с.
4. Алиев А.Т., Балакин А.В., Колпаков Н.И. Основы построения стеганографической защиты мультимедиа-информации. Ростов-на-Дону: Изд-во СКНЦ ВШ, 2006. 204 с.

References

1. Gribunin V.G., Okov I.N., Turincev I.V. Cifrovaja steganografija. M.: Solon-Press, 2002. 272 s. (in Russ.)
2. Savost'janchik V.V., Alefirenko V.M. Vybor programmnyh sredstv komp'juternoj steganografii dlja issledovanija jeffektivnosti skrytija graficheskoj informacii // Science Time. 2017. № 11 (47). S. 37–42. (in Russ.)
3. Osnovy komp'juternoj steganografii / A.B. Agranovskij [i dr.]. M.: Radio i svjaz', 2003. 152 s. (in Russ.)
4. Aliev A.T., Balakin A.B., Kolpakov N.I. Osnovy postroenija steganograficheskoj zashhity mul'timedia-informacii. Rostov-na-Donu: Izd-vo SKNC VSh, 2006. 204 s. (in Russ.)

Сведения об авторах

Алефиренко В.М., к.т.н., доцент, доцент кафедры проектирования информационно-компьютерных средств Белорусского государственного университета информатики и радиоэлектроники.

Адрес для корреспонденции

220013, Республика Беларусь,
г. Минск, ул. П. Бровки, 6,
Белорусский государственный университет
информатики и радиоэлектроники
тел. +375-17-293-88-38;
e-mail: alefirenko@bsuir.by
Алефиренко Виктор Михайлович

Information about the authors

Alefirenko V.M., PhD, associate professor, associate professor of the information computer hardware design department of the Belarusian state university of informatics and radioelectronics.

Address for correspondence

220013, Republic of Belarus,
Minsk, P. Brovka st., 6,
Belarusian state university
of informatics and radioelectronics
tel. +375-17-293-88-69;
e-mail: alefirenko@bsuir.by
Alefirenko Viktor Mihajlovitch