УДК 004.056.55

Анализ особенностей методов цифровой стеганографии для защиты информации, передаваемой по открытым каналам

Н.Е.Губенко канд. техн. наук, доцент каф. КСМ,
Д.С. Сипаков, магистрант
Донецкий национальный технический университет
negubenko@mail.ru, dimasipakov@gmail.com

Губенко Н.Е.,Сипаков Д.С. Анализ особенностей методов цифровой стеганографии для защиты информации, передаваемой по открытым каналам. *Рассмотрены и проанализированы методы цифровой стеганографии, которые используют в качестве контейнеров передаваемого сообщения аудио файлы и изображения. Приведены алгоритмы некоторых методов, выявлены их особенности, достоинства и недостатки.*

Введение

В настоящий момент представить нашу жизнь без интернета практически невозможно. На сегодня ежедневная аудитория всемирной паутины составляет более чем 3 млрд. человек. Глобальная сеть используется в каждом доме, в каждом устройстве, каждую секунду люди совершают миллиарды запросов внутри интернета, отсылают сообщения на огромные расстояния. В связи с таким быстрым и глобальным развитием данной технологии, логично ожидать появления ряда проблем. Одной из самых актуальных и важных из них является обеспечение безопасности этой самой глобальной сети. Данные, которые передаются между пользователями, должны оставаться конфиденциальными, а сам интернет не должен нарушать какие-либо права или свободы человека. Более того: интернет должен гарантировать защиту пользователя и его данных от всякого рода атак и угроз.

Учитывая тот факт, что глобальной сетью пользуются и спецслужбы стран, можно утверждать, что способы и методы защиты данных разрабатывались параллельно с развитием интернета. Логичным является появление термина и сферы науки — информационная безопасность. Информационная безопасность — это процесс обеспечения конфиденциальности, доступности и целостности информационных ресурсов, который поддерживается большим набором средств и методов для обеспечения защиты данных от разного вида угроз. Одной из важных отраслей информационной безопасности является стеганография. Стеганография — наука о скрытой передаче информации. В отличие от криптографии, задача которой состоит в шифровании сообщения, передаваемого по открытым каналам, задачей стеганографии является сокрытие самого факта передачи информации.

Особенности компьютерной стеганографии

Как уже было отмечено, стеганография является наукой о сокрытии самого факта передачи информации и может использоваться одновременно с криптографическими методами. Прогресс в области разработки компьютерных сетей, средств мультимедиа привел к появлению новых способов обеспечения безопасности данных при передаче их через интернет и другие каналы связи (телекоммуникации). Разрабатываемые методы компьютерной стеганографии направлены на использование избыточности в устройствах оцифровки или в аудио и видеосигналах (цифровая стеганография), а так же в сетевых каналах передачи данных (сетевая стеганография). Общая схема стеганографического процесса представлена на рис.1.

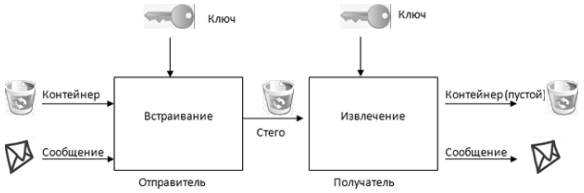

Рисунок 1 — Общая схема стеганографического процесса

В основе маскировки данных или стеганографического анализа лежит работа с физическими процессами. Аудио сигналы и изображения — это все физические процессы, мы получаем цифровые образы звука или изображения с помощью аналого-цифровых преобразователей. Стеганография, с точки зрения реализации – это процесс наложения слабого шума на реализацию цифрового процесса. Примерами могут служить дискретные косинусные и вейвлет-преобразования. Накладываемый шум, должен нести в себе маскируемую информацию и быть достаточно слаб для восприятия человеком.

Что касается сетевой стеганографии, то здесь носителем скрытой информации выступают сетевые протоколы модели OSI (сетевая модель взаимодействия открытых систем). В общем виде сетевая стеганография представляет собой совокупность методов изменений, вносимых в заголовки пакетов и в поля их полезной нагрузки, изменение структуры передачи данных и т.д. [2].

Области применения компьютерной стеганографии достаточно обширны и разнообразны:

- аутентификация;
- защита конфиденциальной информации от несанкционированного доступа - извлечения, изменения, копирования (противодействие системам мониторинга и управления сетевыми ресурсами промышленного шпионажа, сфера электронной коммерции, копирование мультимедийной информации и т.п.);
- скрытая аннотация документов для защиты авторского права на интеллектуальную собственность;
- скрытая связь (военные и разведывательные приложения, когда использовать криптографию нельзя).

Для проверки авторства и подлинности того или иного изображения, используют специальные стеганографические подписи, эти подписи называются цифровые водяные знаки (watermarking). Цифровой водяной знак (ЦВЗ) внедряется в изображение таким образом, чтобы его не было заметно для обычного пользователя (часто используют изменения яркости определенных пикселей изображения). ЦВЗ применяется также, когда стороны обмениваются секретными сообщениями, внедрёнными в цифровой сигнал, и как средство защиты документов с фотографиями (паспортов, водительских удостоверений и т.п.).

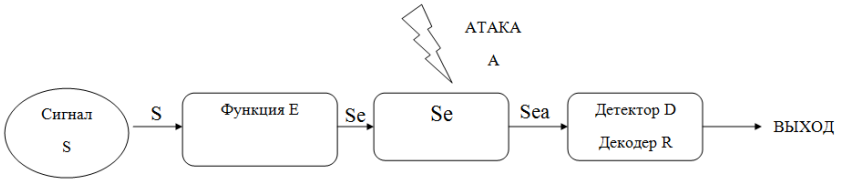

Рисунок 2 — Фазы жизненного цикла ЦВЗ

Для начала в сигнал-источник S внедряются цифровые водяные знаки при помощи функции E, получается S_E. Затем в процессе передачи на сигнал может совершиться атака, вследствие которой водяные знаки могут быть изменены. Во время приема данных, из полученного сигнала S_{EA} функция D вытаскивает внедренные водяные знаки, а функция R достает само сообщение. После этого, по полученным из функции D водяным знакам можно определить подлинность сообщения. В работе [11] рассмотрена задача генерации цифровых водяных знаков для внедрения в изображения. Отмечается, что методы нанесения ЦВЗ делятся на пространственные и частотные. К пространственным методам относится метод LSB. К частотным — методы расширения спектра. Такие ЦВЗ отличаются средней надёжностью, но очень маленькой

информационной ёмкостью. В работе [7] представлен метод встраивания в изображении цифровых водяных знаков путем изменения яркости синего, красного и зеленого цветов определенных пикселей изображения, так же в данной работе приведен сравнительный анализ данного метода и LSB.

На сегодняшний день большинство основных методов цифровой стеганографии базируется на использовании свойств компьютерных форматов данных и информационной избыточности аудио и видео файлов.

Анализ методов цифровой стеганографии в изображениях

Метод наименьшего значащего бита

Одним из наиболее распространенных методов цифровой стеганографии, является метод наименьшего значащего бита (Least Significant Bit, LSB). Чаще всего этот метод используют в тех случаях, когда информацию скрывают в изображении. Описание данного метода приведено в [14].

Алгоритм метода состоит в следующих шагах:

1. Имеется 8-битное изображение в градациях серого, 00h(00000000b) — черный цвет, FFh (11111111b) — белый цве, всего 256 градаций (2^8).
2. Допустим, скрываемое сообщение состоит из 1 байта, например: 01101011b.
3. Если использовать 2 младших бита, то потребуется 4 пикселя. Предположим, что они черного цвета, тогда пиксели, которые буду содержать скрытое сообщение, принимают следующий вид: 00000001 00000010 00000010 00000011.
4. Цвет этих пикселей изменится следующим образом: первого — 1/255, второго — 2/255 и т.д., такие градации не только не заметны для человека, но также не отображаются на низкокачественных устройствах вывода.

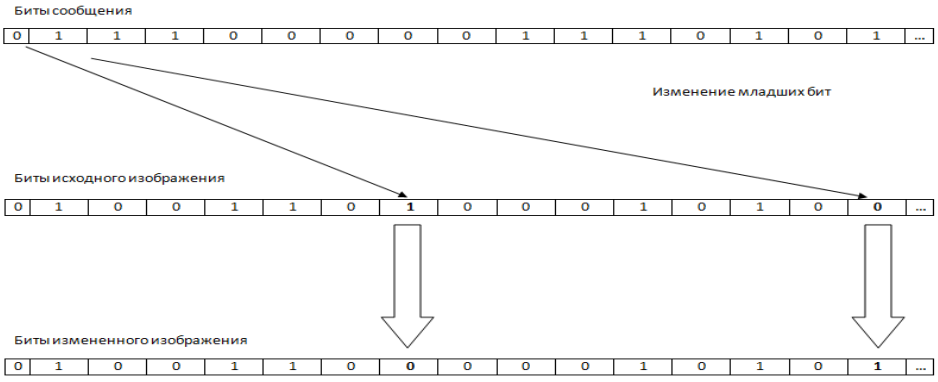

Рисунок 3 — Метод LSB

Метод LSB является аддитивными и крайне неустойчивым ко всем видам атак. Более того, при работе с форматами сжатия и потери данных (JPEG) данный метод не используется, так как анализ показал, что он не устойчив к геометрическим преобразованиям [4].

Алгоритм Куттера-Джордана-Боссена

Еще одним из стеганографических алгоритмов, используемых для скрытия информации в изображении, является алгоритм Куттера-Джордана-Боссена [5]. Он базируется на использовании одной из особенностей зрительной системы человека, которая менее всего восприимчива к изменению яркости синего цвета.

Исходя из этого, для встраивания информации используется синий цвет контейнера заданного изображения. Допустим, что встраивается 1 бит сообщения в 1 пиксель контейнера, секретный ключ задает координаты пикселя, в который будет встраиваться сообщение. Введем следующие обозначения:

- $Y_{x,y}$— яркость пикселя;
- $B_{x,y}$— яркость синего цвета пикселя;
- $B^*_{x,y}$ — яркость синего цвета измененного пикселя, m_i— бит сообщения;
- λ — коэффициент, задающий энергию встраиваемого бита данных (задаётся исходя из функционального назначения и особенности стеганосистемы);
- σ — размер области, по которой будет прогнозироваться яркость.

При встраивании битов скрываемой информации показатели яркости зеленого и красного цветов остаются без изменения, а вот яркость синего цвета изменяется по следующее формуле:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \lambda Y_{x,y}, \text{при } m_i = 1 \\ B_{x,y} - \lambda Y_{x,y}, \text{при } m_i = 0 \end{cases}, \quad (1)$$

где $\lambda = 0.1$; $Y_{x,y} = 0.3R_{x,y} + 0.59G_{x,y} + 0.11B_{x,y}$. Так как принимающая сторона не имеет оригинального изображения, то узнать в какую сторону изменилась яркость цвета не возможно, поэтому значение яркости синего цвета прогнозируется по следующей формуле:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma}(B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma}, \quad (2)$$

где σ = 1/3.

На рисунке 4 демонстрируется выборка пикселей при σ = 2.

	X-2	X-1	X	X+1	X+2
Y-2					
Y-1					
Y					
Y+1					
Y+2					

Рисунок 4 — Выборка пикселей для σ = 2

Пиксель в центре — это пиксель, для которого необходимо спрогнозировать яркость синего цвета, используя выделенные пиксели. Далее вычисляется скрытое сообщение, используя формулу:

$$m_i = \begin{cases} 1, \text{при } B^*_{x,y} > \overline{B_{x,y}} \\ 0, \text{при } B^*_{x,y} < \overline{B_{x,y}} \end{cases}. \quad (3)$$

К достоинствам данного метода можно отнести следующие факторы:

- высокая пропускная способность;
- высокая устойчивость к частотному детектированию;
- высокая устойчивость к разрушению младших бит контейнера;
- устойчивость к атаке сжатия.

А вот главным недостатком является вероятностный характер извлечения яркости цвета. Для уменьшения вероятности ошибки рекомендуется использовать помехоустойчивое кодирование.

Алгоритм Брайндокса

В отличие от метода Куттера-Джордана-Боссена алгоритм Брайндокса [21] использует фиксированную область пикселей (8*8), он содержит следующие шаги:

1. Классификация и разделение пикселей внутри блока на две группы с примерно одинаковой яркостью.
2. Разбиение каждой группы на категории.
3. Модификация яркости пикселей в каждой категории каждой группы.

Более подробно данный алгоритм приведен в работе [21], в работе [6] представлен сравнительный анализ данного метода и метода Куттера.

Файлы изображения не являются единственным хранилищем для помещения скрываемого сообщения, так же активно используются алгоритмы стеганографии, которые в качестве контейнера для скрываемого текста используют аудиофайлы.

Анализ методов цифровой стеганографии в аудио-файлах

Заголовки аудио и видео файлов представляются в виде последовательности битов, они содержат информацию о размере файла, данные о ширине и высоте, положение самого контента (видео и аудио потоков или матрицы пикселей), более того большинство форматов как аудио так и видео содержат блоки, называемые чанками (chunks), которые так же представлены последовательностью битов. Поскольку организации структур аудио и видео файлов в некотором смысле схожи, естественно использовать для внедрения в них скрываемой информации методы, применимые для сокрытия информации в видео изображениях. Например, можно внедрять информацию, замещая наименее значимые биты, или использовать некоторые особенности аудиосигналов и системы слуха человека (например, человек может слышать и распознавать сигналы в диапазоне 10 – 20000 Гц).

Самыми простыми, но и мало эффективными методами сокрытия информации в аудио-файлах являются эхо-методы. Они используют неравномерные промежутки между эхо-сигналами в аудио-файле для кодирования значений сообщения. Важно соблюдать требуемые ограничения при кодировании информации, чтобы гарантировать незаметность для человеческого восприятия. Все эхо-методы характеризуются тремя параметрами: начальной амплитудой, степенью затухания и задержкой. Сигнал и эхо смешиваются, при достижении некоего порога, в этой точке человеческое ухо уже не может отличить разницу в двух сигналах. Данную точку тяжело определить, так как это зависит от качества исходной записи слушателя.

Обычно используется задержка 1/1000, для обозначения логического нуля или единицы следует использовать две различных задержки. Отмечается, что данные методы стойки к атакам по амплитуде и частоте, однако они абсолютно не устойчивы к атакам по времени и не используются в аудио-форматах для сжатия [4].

Наиболее эффективным и распространенным методом сокрытия в аудио-файлах является метод фазового кодирования [9], смысл которого заключается в следующем:

1. Звуковая последовательность $S_i, (1 \le i \le L)$, разбивается на серию N коротких сегментов $S_n[i], (1 \le n \le N)$, рис. 5.

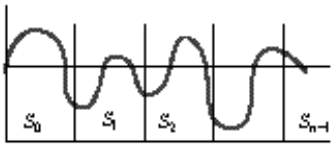

Рисунок 5 — Сигнал разбивается на сегменты

2. К n-тому сегменту сигнала применяется K-точечное дискретное преобразование Фурье (ДПФ), где K=L/N, создаются массивы фаз $\phi_n(\omega_k)$ и амплитуд $A_n(\omega_k)$, для $1 \le k \le K$, рис. 6

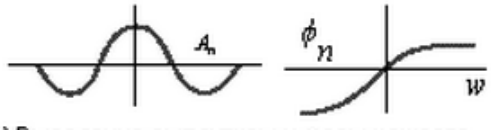

Рисунок 6 — Выделение амплитуды и фазы каждого сегмента

3. Запоминается разность фаз между каждыми соседними сегментами, для $1 \le n \le N$:

$$\Delta\phi_n(\omega_k) = \phi_n(\omega_k) - \phi_{n-1}(\omega_k);\ \Delta\phi_1(\omega_k) = 0. \quad (4)$$

Рисунок 7 — Вычисление разности фаз между соседними сегментами

4. Двоичная последовательность данных представляется как $\phi_{data} = \pi/2$ или $\phi_{data} = -\pi/2$, отображая «1» или «0», $\phi_1'(\omega_k) = \phi_{data}$

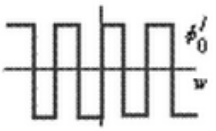

Рисунок 8 — Для сегмента S_0 создается новая фаза

5. С учетом разности фаз, воссоздается новый массив фаз для $n > 1$:

$$\left\| \begin{array}{c} \phi_1'(\omega_k) = \phi_{data} \\ \phi_2'(\omega_k) = \phi_1'(\omega_k) + \Delta\phi_2(\omega_k) \\ \dots \\ \phi_n'(\omega_k) = \phi_{n-1}'(\omega_k) + \Delta\phi_n(\omega_k) \\ \dots \\ \phi_N'(\omega_k) = \phi_{N-1}'(\omega_k) + \Delta\phi_N(\omega_k) \end{array} \right\|. \quad (5)$$

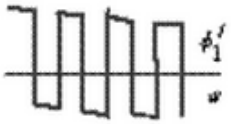

Рисунок 9 — Для всех других сегментов создаются новые фазы

6. Для восстановления звукового сигнала необходимо применить операцию обратного ДПФ к исходной матрице амплитуд и модифицированной матрице фаз.

Получателю должны быть известны длина сегмента, и точки ДПФ. Перед декодированием последовательность должна быть синхронизирована, недостатком данного метода является низкая пропускная способность.

Достаточно эффективными методами сокрытия сообщения в аудио-файлах являются методы, базирующиеся на встраивании в контейнер случайной последовательности битов с использованием согласованного фильтра для последующего ее детектирования. Данные методы позволяют встраивать большое количество сообщений в контейнер, и они не будут создавать помехи друг другу при условии ортогональности применяемых последовательностей. Преимуществом данных методов является противодействие геометрическим преобразованиям, удалению части файла и т.д. Данные методы основаны на расширении спектра сигнала. Изначально эти методы создавались для разведывательных и военных целей. Основная их идея состоит в распределении информационного сигнала по широкой полосе радиодиапазона, что в итоге позволяет значительно усложнить подавление или перехват сигнала.

Современной схемой расширенного спектра является метод прямого последовательного расширения (Direct Sequence Spread Spectrum - DSSS) [13]. Суть этого метода заключается в формировании широкополосного радиосигнала, при котором исходный двоичный сигнал преобразуется в псевдослучайную последовательность, используемую для модуляции несущей. Используется в сетях стандарта IEEE 802.11 и CDMA для преднамеренного расширения спектра передаваемого импульса. Вся используемая полоса частот делится на некоторое число

подканалов — по стандарту 802.11 этих подканалов 11. Каждый бит передаваемой информации преобразуется, по определенному алгоритму, в последовательность из 11 бит, и эти 11 бит передаются одновременно и параллельно, используя все 11 подканалов. При приеме, полученная последовательность бит декодируется с использованием того же алгоритма, что и при ее кодировке. Очень часто в качестве значения расширяющей последовательности берут последовательность Баркера, которая состоит из 11 бит: 10110111000. Если передатчик использует эту последовательность, то передача трех битов 110 ведет к передаче следующих битов: 10110111000 10110111000 01001000111.

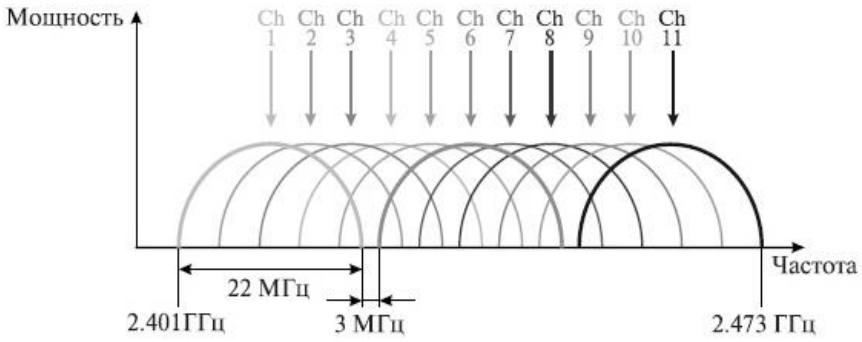

Рисунок 10 — Каналы, используемые в технологии DSSS

Очевидным достоинством данного метода является защита от прослушивания, благодаря 11-кратной избыточности передачи можно обойтись сигналом очень маленькой мощности, не увеличивая при этом мощность передатчика. Так же благодаря очень низкому уровню сигнала, DSSS-устройства не создают помех обычным радиоустройствам. Однако DSSS в меньшей степени защищен от помех, чем метод быстрого расширения спектра, так как мощная узкополосная помеха влияет на часть спектра, а значит, и на результат распознавания единиц или нулей.

Программы и утилиты для цифровой стеганографии

На сегодняшний день разработан и используется ряд готовых программных продуктов для шифрования и сокрытия разного вида информации. Данное программное обеспечение используется как спецслужбами, так и обычными пользователями, корпорациями и предприятиями, которые работают с важной информацией, к которой необходимо ограничить доступ. Эти программы разрабатываются либо отдельными разработчиками, либо отдельными компаниями по производству программного обеспечения. В таблице 1 представлена сравнительная характеристика некоторых шифрующих программ.

Таблица 1 — Сравнительная характеристика программ для шифрования информации

Название ПО	Описание	Достоинства	Недостатки
JSTEG	Одна из программ для встраивания сообщений в изображения формата JPEG. Алгоритм работы представляет собой замену наименее значимых бит (метод LSB). Программа устойчива к визуальным атакам и имеет высокую пропускную способность, скрытое	Полностью доступная программа для шифрования в JPEG; простота использования.	Не устойчива к анализу гистограмм; не устойчива к визуальным атакам; поддерживает только формат JPEG; только один алгоритм шифрования; мало возможностей.

	сообщение может занимать до 12% всего изображения [16].		
S-Tools	Данная программа позволяет скрывать любые файлы в GIF, BMP и WAV. Осуществляет регулируемое сжатие (архивирование) данных, кроме того,	Поддержка нескольких алгоритмов шифрования; без пароля невозможно установить факт работы S-Tools.	Поддерживает мало форматов; мало возможностей; в некоторых случаях наблюдалось искажение встраиваемой информации.

Продолжение таблицы 1

Название ПО	Описание	Достоинства	Недостатки
	производит шифрование с использованием алгоритмов MCD, DES, тройной-DES, IDEA. При шифровании использует пользовательский пароль [17].		
TrueCrypt	Компьютерная программа шифрования, для 32- и 64-разрядных операционных систем семейств Microsoft Windows NT 5 и новее (GUI-интерфейс), Linux и Mac OS X. Позволяет шифровать логические диски, разделы жесткого диска или usb-накопителя. Результат работы программы представляется файлом, содержащим всю зашифрованную информацию (каталоги, папки и т.д.) [18].	Программа умеет создавать виртуальный зашифрованный диск; присутствуют виды шифрования как для 32 битов так и для 64; при генерации ключей шифрования использует хэш-функции; наличие двух уровней защиты от выявления; не требует установки; возможность резервного копирования данных.	В мае 2014, в ходе проверки TrueCrypt, были обнаружены серьезные уязвимости и нарушения, вследствие чего проект был закрыт.
CyberSafe	Предоставляет широкий спектр услуг таких как: шифрование файлов, папок, каталогов и дисков, электронной почты и т.д. Программа является платной и необходимо приобрести лицензию на право использования [19].	Широкий спектр возможностей для шифрования абсолютно любых видов информации; неограниченная длина пароля для шифрования; использование новейших алгоритмов шифрования (Blowfish, AES, DES); простота использования.	Данное программное обеспечение является платным и требует специальной установки.
Folder Lock	Основные возможности: Aes-	Простой и понятный интерфейс;	Наличие только английского языка;

	шифрование (длина ключа 256 бит), сокрытие файлов и папок, шифрование файлов «на лету», резервное копирование-онлайн, создание защищенных usb/cd/dvd-дисков, шифрование вложений электронной почты [20].	прозрачное шифрование «на лету»; возможность резервного онлайн-копирования; возможность создания самораспаковывающихся контейнеров на USB/CD/DVD-дисках	отсутствует цифровая подпись на зашифрованных файлах; высокая стоимость.

Продолжение таблицы 1

Название ПО	Описание	Достоинства	Недостатки
PGP Desktop	Это комплекс программ для шифрования, обеспечивающий гибкое многоуровневое шифрование. Данная программа тесно интегрируется в системную оболочку, а доступ к ней осуществляется через «Проводник» [20].	Поддержка сервера ключей keyserver.pgp.com.; возможность создания самораспаковывающихся архивов; возможность шифрования системного жесткого диска; интеграция с «Проводником» ОС.	Нестабильная работа; низкая производительность.

Исходя из анализа характеристик, приведенных в таблице 1, можно сделать вывод, что наиболее эффективной программой с точки зрения безопасности является CyberSafe. Однако для использования CyberSafe необходимо приобрести лицензию на определенный срок (затем ее нужно продливать), в то время как остальные перечисленные продукты являются бесплатными или не требуют периодической оплаты. Это естественно объясняется тем, что информация сегодня является очень ценным ресурсом любой компании и за ее должную безопасность необходимо дорого платить.

Лингвистическая стеганография

Анализ предложений на рынке безопасности показывает, что методы стеганографии эволюционируют каждый год. Постоянно ведется поиск новых контейнеров для сокрытия информации, так как при передаче данных, злоумышленники в первую очередь концентрируют свои атаки на медиа и видео контенте. В последние годы популярность набирают методы, где в качестве контейнера скрываемого сообщения выступает другое сообщение, данное направление получило название — лингвистическая стеганография. Однако все известные на сегодня алгоритмы данного типа стеганографии обладают целым рядом недостатков. Из-за их примитивной реализации декодирования сообщения с помощью вычислительной техники не вызывает трудностей.

Рассмотрим некоторые методы данного направления:

- семаграммы — при использовании данного метода скрываемый текст заменяется последовательностью определенных знаков или символов, где каждый знак (символ) соответствует определенному слову;
- фонетика — способ, при котором слово транслитерируется на определенный язык;
- жаргоны — схожи с семаграммами, но вместо знаков используются другие (понятные только определенной группе лиц) слова;
- скрытое кодирование — наиболее распространенный метод, но и наиболее сложный в реализации.

Идея последнего метода состоит в том, чтобы превратить (закодировать) скрываемое сообщение в другой текст (стего-текст), который должен быть абсолютно лексически правилен и не вызывать подозрений. Зачастую в качестве стего-текста выступает разнообразная реклама.

Сравнительный анализ данных методов приведен в работе [15], в ней также отмечаются

главные преимущества и недостатки алгоритмов лингвистической стеганографии.

Заключение

Все вышеперечисленные методы стеганографии обеспечивают достаточно стойкую защиту передаваемых сообщений. Сравнительная таблица этих методов, приведеная в работе [3], позволяет сделать следующие выводы.

Методы, которые используют избыточность аудио и визуальной информации обладают целым рядом достоинств:

- относительная простота реализации;
  - возможность передачи больших объемов данных;
  - изменение младших разрядов информационных адиниц в форматах контейнеров никак не влияет на восприятие человека и даже некоторых мониторов и мультимедийных систем;
  - даже если факт сокрытия стал известен противнику через сообщника, извлечение самого файла-сообщения представляет сложную вычислительную задачу.

Но с изменением информации искажаются статистические характеристики цифровых потоков, более того данные способы плохо применимы к форматам со сжатием данных (JPEG), так как они не устойчивы к геометрическим преобразованиям, после которых внедренная информация сильно искажается и появляется проблема ее извлечения на принимающей стороне [3].

Методы цифровой стеганографии направленные на использование зарезервированных для расширения полей компьютерных форматов достаточно просты в реализации и использовании. Данные поля имеются во многих форматах и заполняются нулями, так что не учитываются программами, следовательно их изменение не будет заметно. Однако этот способ не позволяет встраивать в контейнер большие сообщения, более того при декодировании сразу же проверяются именно эти участки файлов.

В заключение можно сделать следующий вывод. При передаче сообщения, скрываемого в аудио файле или в файле изображения необходимо отдавать предпочтение методам кодирования и расширения спектра сигнала. Более того, само сообщение целесообразно зашифровать стойким криптоалгоритмом, тогда даже при обнаружении факта передачи, злоумышленнику будет достаточно проблематично достать исходное сообщение. И все же при передаче информации по открытым каналам, больше всего подозрений вызывают передаваемые аудио и видео файлы, в то время как обычный передаваемый текст зачастую не привлекает злоумышленников. По этой причине в последнее время активно развивается новое направление — лингвистическая стеганография.

Список литературы

1. Голубев Е.А., Емельянов Г.В. Стеганография как одно из направлений обеспечения информационной безопасности // Технологии информационного общества, Спецвыпуск T-Comm, 2009. — с. 185-186.
2. Стеганография [Электронный ресурс]. — Режим доступа: https://tpl-it.wikispaces.com/ Стеганография. — Заглавие с экрана
3. Классификация стеганографических методов [Электронный ресурс]. — Режим доступа: http://network-journal.mpei.ac.ru/cgi-bin/main.pl?l=ru&n=9&pa=13&ar=1. — Заглавие с экрана
4. Стеганография [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/Стеганография#.D0.9C.D0.B5.D1.82.D0.BE.D0.B4_LSB. — Заглавие с экрана
5. Метод Куттера-Джордана-Боссена [Электронный ресурс]. — Режим доступа: http://habrahabr.ru/post/115287/. — Заглавие с экрана
6. Г. И. Борзунов, А. С. Соловьев Сравнение алгоритмов Куттера и Брайндокса // Материалы XVIII всероссийской научно-практи ческой конференции БИТ, 2011. — с. 79-80.
7. Васина Т. С. Обзор современных алгоритмов стеганографии // Электронное научно-техническое издание "Наука и образование", МГТУ им. Н.Е. Баумана, 2012. — с. 1-8.
8. П.П. Кокорин О методах стегоанализа в аудиофайлах // Труды СПИИРАН. Вып. 4, 2007. — с. 239-246.
9. Внедрение информации в аудио сигнал [Электронный ресурс]. — Режим доступа: http://crypts.ru/vnedrenie-informacii-modifikaciej-fazy-audiosignala.html. — Заглавие с экрана
10. ЦВЗ [Электронный ресурс]. — Режим доступа:

https://ru.wikipedia.org/wiki/Цифровой_водяной_знак. — Заглавие с экрана
11. А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман, И.М. Кутузов Цифровые водяные знаки в графических файлах // Научно-технический вестник информационных технологий, механики и оптики, № 1, 2013. — с. 152-157.
12. Д.П. Рублёв, О.Б. Макаревич, В.М. Федоров Метод стеганографического встраивания сообщений в аудиоданные на основе вейвлет-преобразования // Известия ЮФУ. Технические науки. Раздел III. Методы и средства криптографии и стеганографии, 2009. — с. 199-205.
13. Технология расширенного спектра [Электронный ресурс]. — Режим доступа: http://www.intuit.ru/studies/courses/1004/202/lecture/5236?page=6. — Заглавие с экрана
14. О.Ю. Пескова, Г. Ю. Халабурда Применение сетевой стеганографии для защиты данных, передаваемых по открытым каналам Интернет // Технологический институт Южного федерального университета. Санкт-Петербург: Электронные библиотеки и развитие технологий информационного общества, 2012. — с. 348-354.
15. Д.С. Сипаков, Н.Е. Губенко Сравнительный анализ методов лингвистической стеганографии // VI международная научно-техническая конференция студентов, аспирантов и молодых ученых «Информационные управляющие системы и компьютерный мониторинг», 2015.
16. JSTEG [Электронный ресурс]. — Режим доступа: http://www.nestego.ru/2013/01/jpeg-jsteg.html. — Заглавие с экрана
17. S-Tools [Электронный ресурс]. — Режим доступа: http://www.myfreesoft.ru/s-tools.html. — Заглавие с экрана
18. TrueCrypt [Электронный ресурс]. — Режим доступа: https://ru.wikipedia.org/wiki/TrueCrypt. — Заглавие с экрана
19. CyberSafe [Электронный ресурс]. — Режим доступа: http://cybersafesoft.com/rus/. — Заглавие с экрана
20. Сравнение настольных программ для шифрования [Электронный ресурс]. — Режим доступа: http://habrahabr.ru/company/cybersafe/blog/252561/. — Заглавие с экрана
21. Е. В. Васильева Цифровая стеганография // Санкт-петербургский государственный университет информационных технологий, механики и оптики. Дискретная математика: алгоритмы, 2006. — с. 1-20.

Н.Є. ГУБЕНКО, Д.С. СИПАКОВ

Донецький національний технічний університет

Аналіз особливостей методів цифрової стеганографії для захисту інформації, що передається по відкритих каналах

Розглянуто та проаналізовано методи цифрової стеганографії, які використовують як контейнери для переданого повідомлення аудіо файли і файли зображення. Наведено алгоритми деяких методів, виявлено їх особливості, переваги та недоліки.

Ключові слова: стеганографія, контейнер, ЦВЗ, біт, інформація, зловмисник, аутентифікація, загроза, атака, безпека

N. Ye. GUBENKO, D.S. SIPAKOV

Donetsk National Technical University

Analysis of the features of digital steganography to protect information transmitted via open channels

We considered and analyzed digital steganography techniques, which are used as containers transmitted message audio files and images. The algorithms of some methods, revealed their features, advantages and disadvantages. The comparative analysis of some methods of a digital steganography is carried out. The considered finished software products for introduction of a steganography. The comparative analysis of programs which is presented in the table is realized. The short review of a linguistic steganography is carried out. Recommendations of use of algorithms are provided. A number of sources and works on concealment of information is considered.

Keywords: steganography, container, DW, bit, information, the attacker, the authentication, threat, attack, security

Статья поступила в редакцию 20.09.2015
Рекомендована к публикации д-ром техн. наук В.Н. Павлышом