УДК 004.318

А. В. Ремизов, О. В. Рогозин,
М. В. Филиппов

АНАЛИЗ СТЕПЕНИ НЕОБНАРУЖИМОСТИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, СКРЫВАЕМОЙ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛЬНОЙ ФАЙЛОВОЙ СИСТЕМЫ

Рассмотрены методы сокрытия информации на уровне файловой системы. Показаны преимущества и недостатки современных методов. Предложен новый метод сокрытия с использованием специальной файловой системы. Приведены сравнительные результаты работы существующих методов сокрытия и предлагаемого метода по емкости, быстродействию и устойчивости к обнаружению.

E-mail: profitbig@rambler.ru

Ключевые слова: *стеганография, стеганографический анализ, стеганографический ключ, криптография, криптографическая схема, метаданные, карта занятых блоков, контрольная сумма, фрагментация, критерий согласия Пирсона.*

В связи с повсеместным использованием цифровых носителей и каналов связи актуальна проблема защиты передаваемой и хранимой информации от несанкционированного доступа. Большое количество криптографических алгоритмов [1] разработано для защиты собственно информации, однако они не позволяют скрыть от несанкционированного пользователя сам факт наличия информации. Поэтому в последнее время широкое распространение получили методы, скрывающие сам факт передачи конфиденциальной информации.

В данной работе дан сравнительный обзор существующих методов сокрытия информации и предложен новый метод — создание специальной файловой системы.

Обзор существующих методов. В настоящее время существует целый ряд методов сокрытия информации, применяющих программные и аппаратные подходы. В методах первой группы с этой целью используются свойства линий передачи информации. Для защиты беспроводных радиоканалов широко применяют средства передачи шумоподобных сигналов (ШПС) [2, 3]. Среди методов передачи ШПС наиболее распространенным является метод прямой последовательности [3].

Вся используемая “широкая” полоса частот делится на некоторое число подканалов: согласно стандарту 802.11 их должно быть 11 [4]. Каждый передаваемый бит информации превращается по заранее зафиксированному алгоритму в последовательность из 11 “чипов”, интенсивность сигнала одного чипа близка к фоновой. При приеме последовательность чипов декодируется по тому же алгоритму, что и

при передаче: таким образом полезный сигнал удается выделить на фоне шума. В другой паре приемник — передатчик может быть использован иной алгоритм кодировки-декодировки, причем количество алгоритмов практически неограниченно.

При передаче ШПС по методу частотных скачков вся отведенная для передач полоса частот разделяется на подканалы (по стандарту 802.11 их 79). В каждый момент времени каждый передатчик использует только один из подканалов, перескакивая с одного подканала на другой через определенные промежутки времени, не превышающие 20 мс. Эти скачки происходят синхронно на передатчике и приемнике в заранее зафиксированной псевдослучайной последовательности, известной на обоих постах; ясно, что, не зная последовательности переключений, принять сигнал нельзя. Другая пара передатчик — приемник должна использовать отличающуюся последовательность переключений частот, заданную независимо от первой.

Для скрытой передачи информации по оптическим линиям [5] связи сигнал от источника излучения модулируется не по амплитуде, как в обычных системах, а по фазе. Затем сигнал смешивается с самим собой, задержанным на некоторое время, которое превышает время когерентности источника излучения. При таком способе передачи информация не может быть перехвачена амплитудным приемником излучения, так как он зарегистрирует лишь сигнал постоянной интенсивности [6].

Другим направлением сокрытия информации является стеганография [7] — метод организации связи, при котором сообщение скрыто в другом, не подлежащем сокрытию, тексте. В отличие от криптографии, где неприятель может точно определить, является ли передаваемая информация зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить наличие тайного послания.

Существуют также методы сокрытия информации, использующие различные экзотические возможности системы передачи или хранения данных, например, сокрытие данных в потоках файловой системы NTFS. Такие методы не будут рассматриваться в силу их невысокой защиты и сложности для практического применения.

Стеганографическая система или стегосистема представляет собой совокупность средств и методов, которые используются для формирования скрытого канала передачи информации (рис. 1). При построении стегосистемы следует учитывать следующие положения:

— противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ:

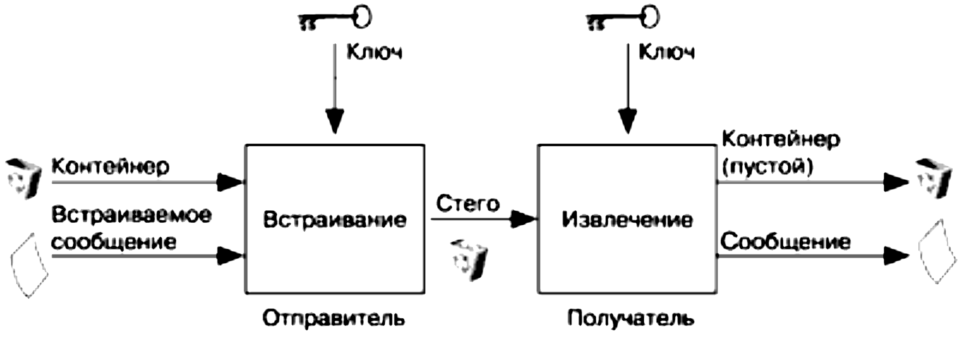

Рис. 1

только держатель его с помощью такого ключа может установить факт присутствия и содержание скрытого сообщения;

— если каким-либо образом противник узнает о факте существования скрытого сообщения, то он не должен иметь возможность извлечь подобное сообщение из других данных до тех пор, пока ключ хранится в тайне;

— потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

В настоящее время наиболее распространены стеганографические алгоритмы, использующие файлы цифровых изображений как контейнеры. Можно выделить две группы таких алгоритмов [7]:

1) скрывающие данные в неиспользуемых областях файла;

2) скрывающие данные в самом изображении.

Большинство коммерческих продуктов включают в первую группу: ввиду примитивности алгоритмов сокрытия данных в них нетрудно обнаружить конфиденциальную информацию.

Алгоритмы второй группы можно классифицировать как:

— LSB-алгоритмы, встраивающие данные в наименее значащий бит изображения;

— алгоритмы с сохранением статистики, которые аналогичны LSB, но используют часть коэффициентов изображения для сохранения исходной частотной статистики изображения [8];

— алгоритмы, в которых передаваемые скрытые данные [9] модулируют шум, прибавляемый к изображению;

— алгоритмы, скрывающие изображения, например, кодируя разность между блоками контейнера и исходного изображения [10];

— прочие алгоритмы [11].

Стеганография в изображении-контейнере основана на замещении незаметных человеческому зрению элементов изображения (фактически, шума сканирования и т.д.) скрываемыми данными, из-за чего невозможно использование искусственно созданных изображений.

Специальная файловая система. Стеганографические алгоритмы имеют ряд значительных недостатков:

— требуется контейнер, наличие которого не скрывается — контейнер может быть удален несанкционированным пользователем;

— сравнительно низкая пропускную способность — полезная информация занимает небольшую (порядка 1/20) часть контейнера;

— для работы хороших стеганографических алгоритмов необходимо значительное процессорное время.

Для практичного сокрытия значительных объемов информации предлагается специальная файловая система (SFS), лишенная подобных недостатков. В SFS файлы размещаются в неиспользуемых логических блоках основной файловой системы (ФС) носителя. В качестве такой системы поддерживаются ФС FAT и UDF.

Блоки выбираются случайным образом из числа незанятых основной или скрытой файловыми системами в данный момент. При случайном выборе, в отличие от характерного для обычных ФС последовательного выбора, затрудняется определение блоков SFS несанкционированным пользователем.

Следует понимать, что блоки SFS совпадают с логическими блоками ФС, существующей на носителе, например, кластерами FAT. Это упрощает работу с картой занятых блоков и не позволяет несанкционированному пользователю искать нетипичные части логических блоков видимой ФС.

Для ускорения открытия ФС в SFS хранится карта занятых блоков аналогично файлу, ссылка на ее начало находится в корневом блоке.

Файл размещается как связный список блоков — каждый блок содержит номер следующего блока или 0 (рис. 2). Кроме того, каждый блок содержит контрольную сумму. Размещение блоков списком позволяет избежать централизованного хранения метаданных, которое могло бы стать уязвимым местом файловой системы. Однако следует иметь в виду, что такое размещение значительно снижает скорость случайного доступа к файлам.

Рис. 2

При обнаружении в цепи блоков ошибки, цепь обрезается до последнего правильного блока, что позволяет считать данные даже при затирании ряда блоков.

Следует отметить, что такое затирание вполне вероятно при записи на диск в основную ФС, в которой отсутствует информация о существовании SFS. Однако можно изменить код, работающий с основной ФС данного конкретного устройства с тем, чтобы код содержал информацию о размещении секторов SFS и не использовал их при размещении данных. Иными словами, при использовании SFS, например, в цифровом фотоаппарате, совместная работа SFS и FAT будет возможна при условии изменения кода FAT в микропрограмме фотоаппарата, что не приведет к снижению безопасности — микропрограмма уже содержит код SFS.

Любая SFS начинается с корневой директории, начало которой вместе с паролем шифрования являются секретным ключом файловой системы.

Директория — это файл, состоящий из каталожных записей. Каждая каталожная запись содержит такую информацию, как тип записи (файл, каталог, пустая запись); атрибуты; размер (не определен для каталога); время модификации; первый и последний блок файла, или 0, если файл пуст; имя. Имена файлов размещаются на диске в кодировке cp866 (Русская OEM кодировка ОС Windows).

Первая каталожная запись корневой директории содержит информацию о начале карты занятых блоков и конце самой корневой директории. Все записываемые на диск блоки шифруются по описанному в ГОСТ 28147–89 алгоритму с использованием схемы LRW (рис. 3) [6]. Емкость блока шифрования составляет 16 байт; используется 256-битный ключ шифрования и 128-битный ключ схемы LRW. Для каждого блока шифрования в блоке данных рассчитываются 128-битный индекс как абсолютный адрес блока шифрования на диске и 128-битный вспомогательный ключ T как произведение I на 2-й ключ в поле GF(2 128). Блок шифрования складывается с T по модулю 2 и зашифровывается с помощью 1-го ключа; результат складывается с T по модулю 2 и записывается на диск.

Такая схема обеспечивает привязку каждого 16-байтного блока шифра к его месту в блоке и к месту блока на диске. В противном случае блоки одинаковых данных давали бы блоки одинаковых шифрованных данных, что позволило бы обнаружить их несанкционированному пользователю.

Ключи шифрования рассчитываются хешированием (SHA-256) введенного пользователем пароля. Затем хеш несколько тысяч раз зашифровывается самим собой. Из полученного 256-битного ключа

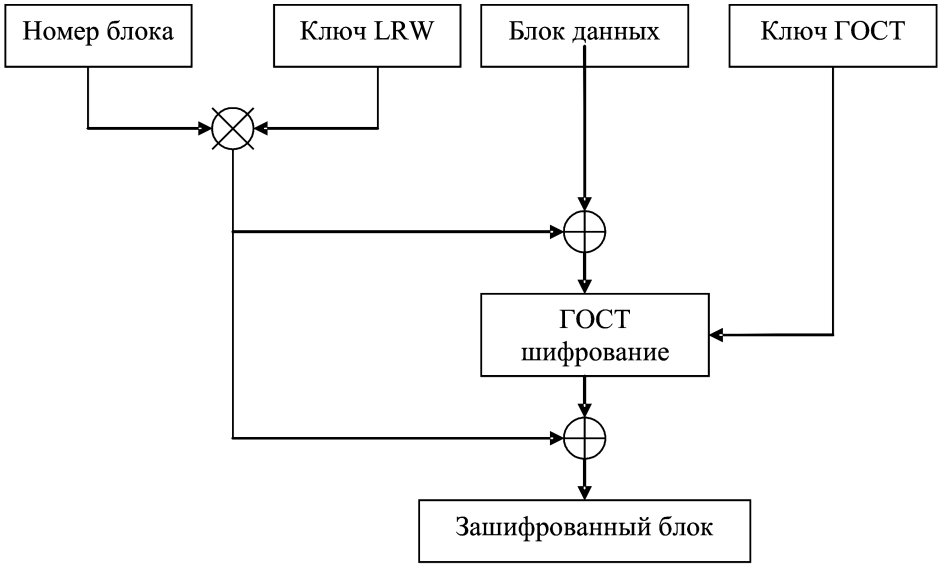

Рис. 3

выделяется 128-битный ключ схемы LRW. Данная схема позволяет значительно затруднить словарные атаки на шифр: атакующий вынужден повторить процедуру для каждого проверяемого слова. Кроме того, возможно использование алгоритма AES в качестве основного алгоритма шифрования.

Результаты тестирования специальной файловой системы. В процессе тестирования SFS определяли такие характеристики, как производительность и эффективность использования пространства носителя информации.

Производительность замеряли для реализации SFS на ПК с использованием алгоритма шифрования AES. Следует отметить, что данный алгоритм является достаточно ресурсоемким при реализации на вычислительных устройствах. В частности, при шифровании в значительной степени ограничивается быстродействие внутри цифрового фотоаппарата.

Время, затрачиваемое 16Mb Canon CF на выполнение типовых операций с файловой системой, приведено в табл. 1. Снижение скорости чтения/записи обусловлено тем, что блоки скрытой файловой системы записываются по одному в различные места носителя, в результате чего увеличивается число запросов к носителю.

Время, затрачиваемое на выполнение типовых операций с файловой системой TDK CD-RW 4x, приведено в табл. 2. Ряд операций для UDF не удалось замерить ввиду отсутствия возможности отключить кеширование InCD.

Таблица 1

Операция	SFS	FAT (Windows XP)
Создание файла, мс	63	94
Открытие файла, мс	16	16
Чтение, КБ/с	390	962
Запись, КБ/с	158	746
Удаление файла, мс	125	109

Таблица 2

Операция	SFS	UDF(InCD)
Создание файла, мс	2531	—
Открытие файла, мс	1125	—
Чтение, КБ/с	160	1169
Запись, КБ/с	54	28
Удаление файла, мс	5860	—

Резкое снижение скорости чтения вызвано разбросом блоков файловой системы по носителю: время поиска на оптических носителях значительно больше, чем у флеш.

Эффективность использования дискового пространства. Структуры SFS малы по размеру: в самом простом случае требуется всего по одному блоку для размещения корневой директории и для карты занятых блоков. Поэтому неэффективность использования дискового пространства в основном вытекает из фрагментации — последний блок каждого файла не используется полностью. Кроме того, SFS занимает 8 байт из каждого блока для размещения контрольной суммы и индекса следующего блока.

Блок данных SFS на 8 байт меньше блока видимой ФС, следовательно, и фрагментация приблизительно совпадает с видимой ФС.

В рамках проведенного исследования рассмотрено использование дискового пространства на 16 МБ носителе с 4 КБ блоками, заполняемом файлами размером около 200 КБ. Предполагаем, что количество данных в последнем секторе файла распределено равномерно, следовательно, потери на фрагментацию каждого файла в среднем равны половине размера блока.

В видимую ФС записываются данные размером 8192 КБ — в половину объема носителя, которые занимают реальный объем носителя 8304 КБ, так как 32 КБ занято самой FAT, 80КБ составляют потери фрагментации. Общие потери места составляют 1,37 % объема

полезных данных. Таким образом, 8080 Кб остаются для SFS. При заполнении этого пространства файлами имеем около 7978 КБ полезных данных — 48,7 % общего объема носителя. Около 16 КБ использовано под индексы и контрольные суммы, 4 КБ отведено корневой директории, 4 КБ — карте занятых блоков, 78 КБ — потери фрагментации. Потери места составляют 1,23 % объема полезных данных.

Таким образом, SFS несколько эффективнее использует дисковое пространство по сравнению с видимой ФС, но на практике это отличие незаметно.

СПИСОК ЛИТЕРАТУРЫ

1. Саломаа А. Криптография с открытым ключом. – М.: Мир, 1996. – 318 с.
2. Тельнов Ю. Ф., Рогозин О. В. Разработка инновационных образовательных технологий на основе модели с использованием scorm-спецификаций // Открытое образование: Науч.-практич. журнал. – 2009. – № 4. – С. 37.
3. Рогозин О. В. Выбор инструментальных средств анализа качественных характеристик программного обеспечения в области образования, как объекта инвестиций // Открытое образование: Науч.-практический журнал. – 2009. – № 2. – С. 48.
4. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. – М.: БИНОМ, 2003. – 294 с.
5. Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001. – 376 с.
6. Убайдуллаев Р. Р. Волоконно-оптические сети. – М.: Эко-Трендз, 2000. – 268 с.
7. Грибунин В. Г. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002. – 272 с.
8. FIPS publication: 197 Advanced Encryption Standard // Federal Information Processing Standards Publ., 2001. – 51 p.
9. Fridrich J. Digital image steganography using stochastic modulation // Proc. SPIE Electronic Imaging. Santa Clara, CA. – January, 2003. – P. 191–202.
10. Fridrich J., Miroslav G. New blind steganalysis and its implications // Proc. SPIE Electronic Imaging. – 2006. – Vol. 6072. – P. 1–13.
11. Hetlz S., Mutzel P. A graph-theoretic approach to steganography // Communications and multimedia security. – 2005. – Vol. 3677. – P. 119–128.

Статья поступила в редакцию 10.05.2012