СОКРЫТИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СПЕЦИАЛЬНОЙ ФАЙЛОВОЙ СИСТЕМЫ

УДК 004.318

Александр Владимирович Ремизов,
аспирант МГТУ им. Н.Э. Баумана, ведущий инженер-программист ЗАО «НТЦ ФОМОС»
Тел.: 8 (499) 975-34-18
Эл. почта: profitbig@rambler.ru

Олег Викторович Рогозин,
К.т.н., доц. кафедры «ПО ЭВМ и ИТ», МГТУ им. Н.Э.Баумана
Тел.: 8 (495) 442-80-98
Эл. почта: logic00@mail.ru

Михаил Владимирович Филиппов,
к.т.н., доц. кафедры «ПО ЭВМ и ИТ», МГТУ им. Н.Э.Баумана
Тел.: 8 (499) 732-97-95
Эл. почта: profitbig@rambler.ru

В статье рассматриваются методы сокрытия информации на уровне файловой системы. Показаны преимущества и недостатки существующих методов. Предлагается новый метод сокрытия с использованием специальной файловой системы. Приводятся сравнительные результаты работы существующих и предлагаемого метода с точки зрения емкости, быстродействия и устойчивости к обнаружению.

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

Alexander V. Remizov,
Post-graduate student, the Department of Computer Software and Information Technology, Baumann Moscow State Technical University, Principal Software Engineer of ZAO «NTC FOMOS», JSC
Tel.: 8 (499) 975-3418
E-mail: profitbig@rambler.ru

Oleg V.Rogozin,
PhD in Technical Sciences, Associate Professor, the Department of Computer Software and Information Technology, Baumann Moscow State Technical University
Tel.: 8 (495) 442-80-98
E-mail:logic00@mail.ru

Mikhail V. Filippov,
PhD in Technical Sciences, Associate Professor, the Department of Computer Software and Information Technology, Baumann Moscow State Technical University
Tel.: 8 (499) 732 97 95
E-mail:profitbig@rambler.ru

CONCEALMENT OF PRIVATE INFORMATION USING THE SPECIAL FILE SYSTEM

The article deals with methods of information hiding at the level of file system. Advantages and disadvantages of existing methods are given. The new method of information hiding with the use of specific file system is offered. Comparative results of existing works and offered method connected with capacity, speedwork and stability to detection are given.

Keywords: stenography, cryption, cryptographic scheme, metadata, the map of busy blocks, checksum, fragmentation, Pirson's fittion criterion.

1. Введение

В связи с повсеместным использованием цифровых носителей и каналов связи актуальна проблема защиты передаваемой и хранимой информации от несанкционированного доступа. Для защиты собственно информации было разработано большое количество криптографических алгоритмов. Однако эти алгоритмы не позволяют скрыть от несанкционированного пользователя сам факт наличия информации.

В данной работе дается сравнительный обзор существующих методов сокрытия информации и предлагается новый метод – создание специальной файловой системы.

2. Обзор существующих методов

Методы сокрытия информации были разработаны для различных уровней передачи и хранения данных. Методы защиты на физическом уровне могут использовать беспроводные радиоканалы и волоконно-оптические линии связи. Для защиты беспроводных радиоканалов широко используется средства передачи шумоподобных сигналов (ШПС) [1,2].

Одним из наиболее часто используемых методов передачи ШПС является метод прямой последовательности [3]. Вся используемая «широкая» полоса частот делится на некоторое число подканалов — по стандарту 802.11 их должно быть 11. Каждый передаваемый бит информации превращается по заранее зафиксированному алгоритму в последовательность из 11 «чипов»; интенсивность сигнала одного чипа близка к фоновой, однако при приеме последовательность чипов декодируется по тому же алгоритму, что и при кодировке, и таким образом полезный сигнал удается выделить на фоне шума. Другая пара приемник – передатчик может использовать другой алгоритм кодировки – декодировки, причем количество алгоритмов практически неограниченно. Передаваемые сигналы, как отражено в названии, схожи с фоновым шумом, что затрудняет их обнаружение атакующим.

Другой способ – передача 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 обоим; ясно, что не зная последовательности переключений принять сигнал нельзя. Другая пара передатчик-приемник должна использовать и другую последовательность переключений частот, заданную независимо от первой.

Для скрытой передачи информации по оптическим линиям [4] 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, большее, чем время когерентности источника излучения.

При таком способе передачи информация не может быть перехвачена амплитудным приемником излучения, так как он зарегистрирует лишь сигнал постоянной интенсивности. Для обнаружения перехватываемого сигнала понадобится перестраиваемый интерферометр Майкельсона специальной конструкции. Причем, видность интерференционной картины может быть ослаблена как $1:2N$, где N – количество сигналов, одновременно передаваемых по оптической системе связи. Можно распределить передаваемую информацию по множеству сигналов или передавать несколько шумовых сигналов, ухудшая этим условия перехвата информации. Потребуется значительный отбор мощности из волокна, чтобы несанкционированно принять оптический сигнал, а это вмешательство легко зарегистрировать системами мониторинга. Методы сокрытия информации на физическом уровне, при их эффективности, не позволяют использовать распространенные системы передачи и хранения информации. Таким образом,

многие практические задачи требуют сокрытия информации на логическом уровне.

Наиболее исследованным направлением сокрытия информации на логическом уровне является стеганография [7] – метод организации связи, который скрывает сообщение в другом, не требующем сокрытия, сообщении. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

Существуют так же методы сокрытия информации, использующие различные экзотические возможности системы передачи или хранения данных, например сокрытие данных в потоках файловой системы NTFS. Данные методы не будут рассматриваться в силу их невысокой защиты и сложности для практических применений.

Стеганографическая система или стегосистема – совокупность средств и методов, которые используются для формирования скрытого канала передачи информации.

При построении стегосистемы должны учитываться следующие положения:

– противник имеет полное представление о стеганографической системе и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения;
– если противник каким-то образом узнает о факте существования скрытого сообщения, это не должно позволить ему извлечь подобные сообщения в 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.

Стеганографические алгоритмы, использующие файлы цифровых изображений как контейнеры, являются наиболее распространенными в настоящее время. Их можно разбить на две группы:

– скрывающие данные в неиспользуемых областях файла;
– скрывающие данные в самом изображении.

Первая группа включает в себя большинство коммерческих продуктов, но ввиду своей примитивности элементарно обнаруживается.

Алгоритмы второй группы можно классифицировать как:

– LSB алгоритмы, встраивающие данные в наименьший значащий бит изображения.
– Алгоритмы с сохранением статистики, аналогичны LSB, но используют часть коэффициентов изображения для сохранения исходной частотной статистики изображения.
– Алгоритмы, модулирующие прибавляемый к изображению шум передаваемыми скрытыми данными.
– Алгоритмы, скрывающие изображения, например, кодируя разность между блоками контейнера и исходного изображения.
– Прочие алгоритмы.

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

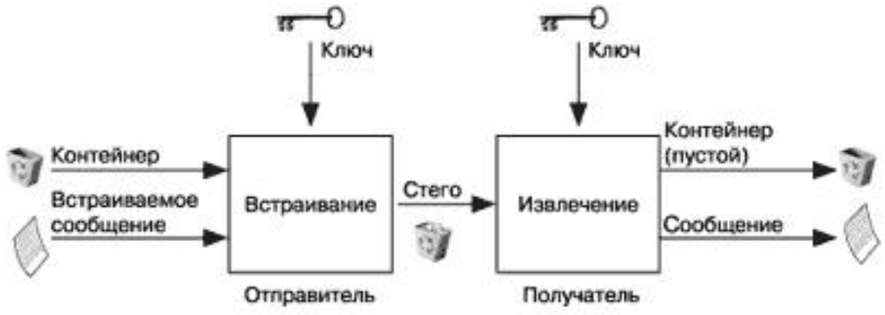

Рис. 1

3. Специальная файловая система

Стеганографические алгоритмы имеют ряд значительных недостатков:

– требуется контейнер, чье наличие 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 требуется значительное процессорное время.

В качестве лишенного этого недостатков решения, предназначенного для практичного сокрытия значительных объемов информации, предлагается специальная файловая система.

Специальная файловая система (далее SFS) размещает файлы в неиспользуемых логических блоках основной файловой системы носителя.

В качестве основной файловой системы поддерживаются файловые системы FAT и UDF.

Блоки выбираются случайным образом из числа незанятых основной или скрытой файловыми системами в данный момент. Случайный выбор, в отличии от характерного для обычных файловых систем последовательного выбора, затрудняет определение несанкционированным пользователем блоков SFS.

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

Для ускорения открытия файловой системы, SFS хранит карту занятых блоков. Карта хранится аналогично файлу, ссылка на ее начало размещена в корневом блоке.

Файл размещается как связный список блоков – каждый блок содержит номер следующего блока или 0 (см. 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 это значительно снижает скорость случайного доступа к файлам. При обнаружении в цепи блоков ошибки, цепь

Рис. 2

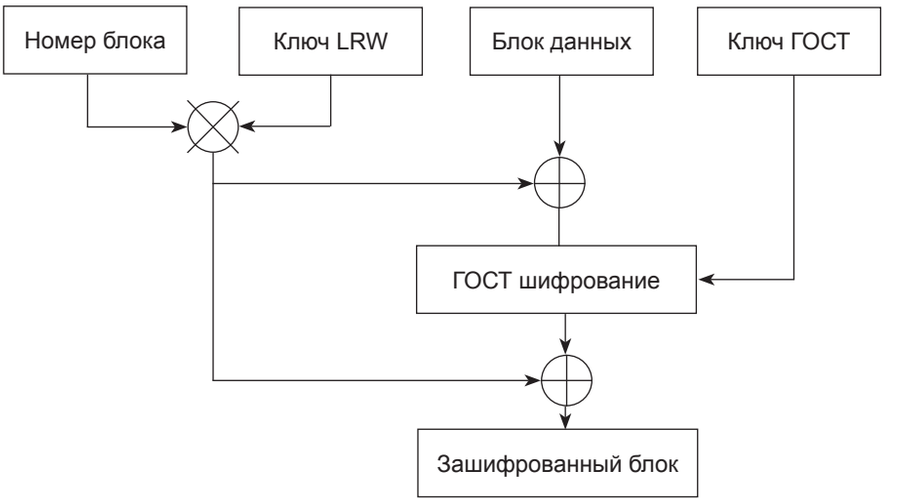

Рис. 3

обрезается до последнего правильного блока. Это позволяет считать данные даже при затирании ряда блоков.

Следует отметить, что такое затирание вполне возможно при записи на диск в основную файловую систему, которая не знает о существовании SFS. Однако возможно изменить код, работающий с основной файловой системой данного конкретного устройства с тем, чтобы он знал о размещении секторов SFS и не использовал их при размещении данных. Т.е. при использовании SFS в, например, цифровом фотоаппарате, совместная работа SFS и FAT будет возможна при условии изменения кода FAT в микропрограмме фотоаппарата, и не приведет к снижению безопасности – микропрограмма уже содержит код SFS.

Директория – это файл, состоящий из каталожных записей. Каталожная запись содержит следующую информацию: 1) тип записи (файл, каталог, пустая запись), 2) атрибуты, 3) размер (не определен для каталога), 4) время модификации, 5) первый и последний блок файла, или 0, если файл пуст, 6) имя файла. Имена файлов размещаются на диске в кодировке cp866 (Русская OEM кодировка ОС Windows). SFS начинается с корневой директории. Начало корневой директории вместе с паролем шифрования являются секретным ключом файловой системы.

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 шифрования с использованием схемы LRW(см. рис. 3) [6]:

- блок шифрования – 16 байт;
- используется 256-битный ключ шифрования и 128-битный ключ схемы LRW;
- для каждого блока шифрования в блоке данных:
  - рассчитывается 128-битный индекс как абсолютный адрес блока шифрования на диске;
  - рассчитывается 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;
  - блок шифрования зашифровывается 1-м ключом;
  - 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 несанкционированному пользователю обнаружить их. Ключи шифрования рассчитываются хешированием (SHA-256) введенного пользователем пароля. Затем хеш несколько тысяч раз зашифровывается самим собой. Из полученного 256-битного ключа выделяется 128-битный ключ схемы LRW. Такая 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. В процессе тестирования SFS определялись следующие характеристики: производительность, эффективность использования пространства носителя информации.

4. Заключение

Производительность замерялась для реализации на ПК с использованием алгоритма шифрования AES. Следует отметить, что используемый алгоритм шифрования достаточно требователен к вычислительным ресурсам системы. В частности, шифрование в значительной степени ограничивает быстродействие реализации внутри цифрового фотоаппарата. Время, затрачиваемое на выполнение типовых операций с файловой системой, 16Mb Canon CF, приведено в Таблице 1.

Снижение скорости чтения/записи обусловлено тем, что блоки скрытой файловой системы записываются по

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	–

одному в различные места носителя. Это увеличивает число запросов к носителю.

Время, затрачиваемое на выполнение типовых операций с файловой системой TDK CD-RW 4x, приведено в Таблице 2.

Ряд операций для UDF не удалось замерить из-за неотключаемого кеширования InCD.

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

Структуры специальной ФС малы по размеру (в самом простом случае требуется всего 1 блок для размещения корневой директории и 1 блок для карты занятых блоков). Таким образом, неэффективность использования дискового пространства в основном вытекает из фрагментации – неиспользовании полностью последнего блока каждого файла. Кроме того, специальная ФС использует 8 байт из каждого блока для размещения контрольной суммы и индекса следующего блока. Блок данных специальной ФС на 8 байт меньше блока видимой ФС, следовательно, фрагментация так же приблизительно совпадает с видимой ФС.

В рамках проведенного исследования было рассмотрено использование дискового пространства на 16Мб носителе с 4Кб блоками, заполняемом файлами размером около 200Кб. Предполагаем, что кол-во 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 в половину объема носителя, 8192Кб. Эти данные занимают реальный объем носителя 8304Кб. 32Кб занято самой ФАТ, 80Кб – потери фрагментации. Общие потери места составляют 1.37% от объема полезных данных. Таким образом, 8080Кб остаются специальной ФС. Заполняя это пространство файлами, имеем около 7978Кб полезных данных, 48.7% от общего объема носителя. Около 16Кб использовано под индексы и контрольные суммы, 4Кб занимает корневая директория, 4Кб – карта занятых блоков, 78Кб – потери фрагментации. Потери места составляют 1.23% от объема полезных данных.

Таким образом, специальная ФС несколько более эффективно использует дисковое пространство, чем видимая, но это отличие на практике незаметно.

Литература

1. Грибунин В.Г. Цифровая стеганография. – М.: СОЛОН-Пресс, 2002.

2. Мосягин Г. М., Немтинов В. Б., Лебедев Е. Н. Теория оптико-электронных систем. Учебник для студентов ВУЗов по оптическим специальностям. – М.: Машиностроение, 1990.

3. Саломаа А. Криптография с открытым ключом. – М.: МИР, 1996.

4. Рошан П., Лиэри Дж. Основы построения беспроводных локальных сетей стандарта 802.11. – М.: БИНОМ, 2003.

5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 2001.

6. Убайдуллаев Р. Р. Волоконно-оптические сети. – М.: Эко-Трендз, 2000.

7. FIPS publication 197 Advanced Encryption Standard // Federal Information Processing Standards Publ. 2001.

8. Fridrich J., Miroslav G. New blind steganalysis and its implications // Proc. SPIE Electronic Imaging 2006.

9. Hetlz S., Mutzel P. A graph-theoretic approach to steganography // Communications and multimedia security 2005, pp. 119-128.

References

1. Gribunin V.G. Digital steganography. – M.: SOLON-Press, 2002.

2. Mosyagin G.M., Nemtinov V.B., Lebedev E.N., Theory of electro-optical systems. Textbook for university students in optical fields. – M.: Engineering, 1990.

3. Salomaa A. Public-key cryptography. – Academic Press, 1996.

4. Roshan P. Lieri J. Fundamentals of Wireless LAN 802.11. – Moscow: BINOM, 2003.

5. Romanet Y.V., Timofeev P.A., Shangin V.F. Protection of information in computer systems and networks. – M.: Radio and communication, 2001.

6. Ubaydullaev R.R. Fiber Optic network. – M.: Eco-Trendz, 2000.

7. FIPS publication 197 Advanced Encryption Standard // Federal Information Processing Standards Publ. 2001.

8. Fridrich J., Miroslav G. New blind steganalysis and its implications // Proc. SPIE Electronic Imaging 2006.

9. Hetlz S., Mutzel P. A graph-theoretic approach to steganography // Communications and multimedia security 2005, pp. 119-128.