Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

Стеганография.

Сунчугашев Иван

4 апреля 2008г

г. Долгопрудный.

Вступление

Стеганогра́фия (*пер. с греч*, «тайнопись») — это наука о скрытой передаче информации путём сохранения в тайне самого факта передачи. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает само его существование.

Стеганография не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты.

Необходимость скрыть какую-либо информацию от чужих глаз возникла очень и очень давно. Спрятать информацию можно разными способами, например, зашифровать ее. Правда, в этом случае противник знает, что вы передаете некоторое секретное сообщение, но не может его прочитать (криптография). А ведь иногда достаточно и самого факта передачи для получения информации о каком-то событии, особенно если рассматривать и сопоставлять все факты вместе -- на этом основана разведка по материалам из открытых источников. Так вот другой способ состоит в том, чтобы скрыть не только сообщение, но и сам факт его передачи, при этом секретная информация может содержаться во вполне безобидной фразе, например:

"КОМПАНИЯ "ЛЮЦИФЕР" ИСПОЛЬЗУЕТ ЕДКИЙ НАТР, ТЯЖЕЛЫЕ ГРУЗИЛА, ОСТРОГУ ТРЕХЗУБУЮ, ОБВЕТШАЛЫЙ ВАТНИК".

В настоящее время, когда объемы различной информации все растут, соответственно растет доля сведений, которые необходимо держать в тайне от посторонних глаз. Применение компьютеров позволило усовершенствовать известные идеи скрытия информации и дало возможность так прятать текст и любые другие данные, что их дешифровка без знания ключей и паролей стала практически невозможной.

История стеганографии.

Известно, что стеганография применяется с древнейших времен:

- В Древней Греции послания писались острыми палочками на дощечках, покрытых воском. В одной из историй Демерат хотел послать в Спарту сообщение об угрозе нападения Ксерксов. Тогда он соскоблил воск с дощечки, написал послание непосредственно на дереве, затем вновь покрыл ее воском. В результате доска выглядела неиспользованной и без проблем прошла досмотр центурионов.

- В V веке до н.э. тиран Гистий, находясь под надзором царя Дария в Сузах, должен был послать секретное сообщение своему родственнику в анатолийский город Милет, он побрил наголо своего раба и вытатуировал послание на его голове. Когда волосы снова отросли, раб отправился в путь. Так Геродот описывает один из первых случаев применения в древнем мире стеганографии - искусства скрытого письма

- Вождь Мирового Пролетариата В.И.Ленин, находясь в ссылке писал молоком между строк, при нагревании этот тексты выделялся (симпатические чернила).

- Во время второй мировой войны немцами применялась **"микроточка"**, представлявшая из себя микрофотографию размером с типографскую точку, которая при увеличении давала четкое изображение печатной страницы стандартного размера. Такая точка или несколько точек вклеивались в обыкновенное письмо, и, помимо сложности обнаружения, обладали способностью передавать большие объемы информации, включая чертежи.

Принципы стеганографии

Стеганографию можно разделить на 3 раздела

- **Классическая стеганография** – включает в себя все «некомпьютерные методы».
- **Компьютерная стеганография** — направление классической стеганографии, основанное на особенностях компьютерной платформы и использования специальных свойств компьютерных форматов данных
- **Цифровая стеганография** — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов. Используется избыточность аудио- и визуальной информации.

Классическая стеганография
Например: см. историческую справку, запись на боковой стороне колоды карт, расположенных в условленном порядке, акростихи, трафареты, которые, будучи положенными на текст, оставляют видимыми только значащие буквы и прочее.

Компьютерная стеганография

Использование регистра букв - пускай нам необходимо спрятать букву "A" в тексте "stenography". Для этого берем двоичное представление кода символа "A" - "01000001". Пускай для обозначения бита содержащего единицу используется символ нижнего регистра, а для нуля - верхнего. Поэтому после накладывания маски "01000001" на текст "stenography", результат будет

"sTenogrAphy". Окончание "phy" нами не использовано поскольку для сокрытия одного символа используется 8 байт (по биту на каждый символ), а длинна строки 11 символов, вот и получилось, что последние 3 символа "лишние". Исспользуя такую технологию можно спрятать в текст длинной N, сообщение из N/8 символов.)

Использование пробелов - пробел обозначен символом с кодом 32, но в тексте его можно заменить также символом имеющим код 255 или TAB'ом на худой конец. Также как и в прошлом примере, передаем биты шифруемого сообщения используя обычный текст. Но на этот раз 1 - это пробел, а 0 - это пробел с кодом 255.

Использование специфики файловых систем - при хранении файл всегда занимает целое число блоков - это сделано из соображений удобства адресации. Из-за этого хранение маленьких файлов реализуется крайне нерационально - в системе Fat32 файл размером 1 байт занимает на диске 4 Кб! При этом очевидно, что все 4 Кб, за вычетом 1 байта, забиты мусором и никак не используются. А ведь могут быть заняты полезными данными! Такой метод широко используется для долговременного скрытого хранения небольших объемов информации - однако он довольно легко обнаруживается и крайне небезопасен. Также существует возможность записи данных просто на неиспользуемые области накопителей (например, нулевую дорожку).

Использование зарезервированных полей компьютерных форматов данных - Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой.

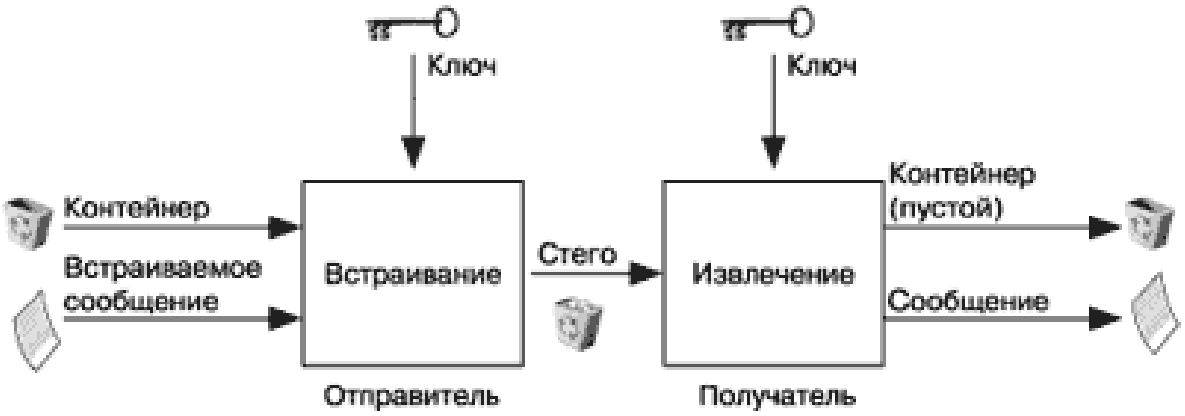
Цифровая стеганография

Именно цифровая стеганография представляет собой наибольший интерес , с точки зрения защиты информации, как наиболее перспективное направление. Ее мы рассмотрим подробнее.

Основные положения стеганографии:

1. Методы скрытия должны обеспечивать аутентичность и целостность файла.
2. Предполагается, что криптографу полностью известны возможные стеганографические методы.
3. Безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации — ключа.
4. Даже если факт скрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения представляет сложную вычислительную задачу.

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



В качестве данных может использоваться любая информация: текст, сообщение, изображение и т. п.

В общем же случае целесообразно использовать слово "сообщение", так как сообщением может быть как текст или изображение, так и, например, аудиоданные. Далее для обозначения скрываемой информации, будем использовать именно термин сообщение.

Принятые Термины

Контейнер - любая информация, предназначенная для сокрытия тайных сообщений.

Пустой контейнер - контейнер без встроенного сообщения; заполненный контейнер или стего - контейнер, содержащий встроенную информацию.

Встроенное (скрытое) сообщение - сообщение, встраиваемое в контейнер.

Стеганографический канал или просто стегоканал - канал передачи стего.

Стегоключ или просто ключ - секретный ключ, необходимый для сокрытия информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей.

По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два типа:

- с секретным ключом;
- с открытым ключом.

В стегосистеме с секретным ключом используется один ключ, который должен быть определен либо до начала обмена секретными сообщениями, либо передан по защищенному каналу.

В стегосистеме с открытым ключом для встраивания и извлечения сообщения используются разные ключи, которые различаются таким образом, что с помощью вычислений невозможно вывести один ключ из другого. Поэтому один ключ (открытый) может передаваться свободно по незащищенному каналу связи. Кроме того, данная схема хорошо работает и при взаимном недоверии отправителя и получателя.

В общем случае встраиваемое сообщение может быть зашифровано другими методами криптографии.

Атаки на стегосистемы

Субъективная атака.

Анатлитик внимательно рассматривает изображение (слушает аудиозапись), пытаясь определить “на глаз”, имеется ли в нем скрытое сообщение. Ясно, что подобная атака может быть проведена лишь против совершенно незащищенных стегосистем. Тем не менее, она, наверное, наиболее распространена на практике, по крайней мере, на начальном этапе вскрытия стегосистемы.

Атака на основе известного заполненного контейнера.

В этом случае у нарушителя есть одно или несколько стего. В последнем случае предполагается, что встраивание скрытой информации осуществлялось отправителем одним и тем же способом. Задача аналитика может состоять в обнаружении факта наличия стегоканала (основная), а также в его извлечении или определения ключа. Зная ключ, нарушитель получит возможность анализа других стегосообщений.

Атака на основе известного встроенного сообщения.

Этот тип атаки в большей степени характерен для систем защиты интеллектуальной собственности, когда в качестве водяного знака используется известный логотип фирмы. Задачей анализа является получение ключа. Если соответствующий скрытому сообщению заполненный контейнер неизвестен, то задача крайне трудно решаема.

Атака на основе выбранного скрытого сообщения.

В этом случае аналитик имеет возможность предлагать отправителю для передачи свои сообщения и анализировать получающиеся стего.

Адаптивная атака на основе выбранного скрытого сообщения.

Эта атака является частным случаем предыдущей. В данном случае аналитик имеет возможность выбирать сообщения для навязывания отправителю адаптивно, в зависимости от результатов анализа предыдущих стего.

Атака на основе выбранного заполненного контейнера.

Этот тип атаки больше характерен для систем ЦВЗ. Стегоаналитик имеет детектор стего в виде «черного ящика» и несколько стего. Анализируя детектируемые скрытые сообщения, нарушитель пытается вскрыть ключ.

Также стегоаналитик может применить еще три атаки, не имеющие аналогов в криптографии

Атака на основе известного пустого контейнера.

Если он известен аналитику, то путем сравнения его с предполагаемым стего он всегда может установить факт наличия стегоканала. Несмотря на тривиальность этого случая, в ряде работ приводится его информационно-теоретическое обоснование. Гораздо интереснее сценарий, когда контейнер известен приблизительно, с некоторой погрешностью (как это может иметь место при добавлении к нему шума). В главе 4 показано, что в этом случае имеется возможность построения стойкой стегосистемы.

Атака на основе выбранного пустого контейнера.

В этом случае аналитик способен заставить отправителя пользоваться предложенным ему контейнером. Например, предложенный контейнер может иметь большие однородные области (однотонные изображения), и тогда будет трудно обеспечить секретность внедрения.

Атака на основе известной математической модели контейнера или его части.

При этом атакующий пытается определить отличие подозрительного сообщения от известной ему модели. Например допустим, что биты внутри отсчета изображения коррелированы. Тогда отсутствие такой корреляции может служить сигналом об имеющемся скрытом сообщении. Задача внедряющего сообщение заключается в том, чтобы не нарушить статистики контейнера. Внедряющий и атакующий могут располагать различными моделями сигналов, тогда в информационно-скрывающем противоборстве победит имеющий лучшую модель.

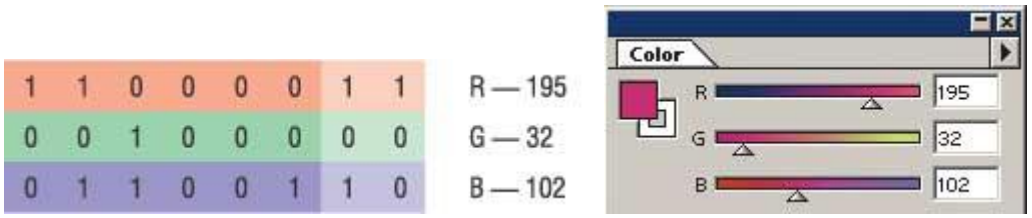
Методы

Метод наименее значащих битов (Least Significant Bit, LSB)

Является наиболее распространенным в электронной стеганографии. Основывается на ограниченных способностях органов чувств, вследствие чего людям очень тяжело различать незначительные вариации звука или цвета. Рассмотрим этот метод на примере 24 битного растрового RGB изображения. Каждая точка кодируется 3мя байтами, каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цвета. Совокупность интенсивностей цвета в каждом из 3х каналов определяет оттенок пиксела.

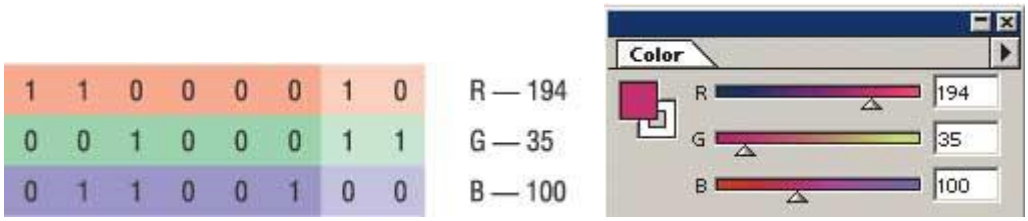
Для наглядности рассмотрим пример:

Представим пиксел тремя байтами в битовом виде:



Младшие биты (выделены бледным, справа) дают незначительный вклад в изображение по сравнению со старшими. Замена одного или двух младших бит для человеческого глаза будет почти незаметна.

Пусть необходимо в этом пикселе скрыть 6 бит – 101100. Разделим их на 3 пары и заместим этими парами младшие биты в каждом канале.



Получили новый цвет, очень похожий на первоначальный:

На этом рисунке слева – оригинальный цвет, справа – модифицированный.

Оценим эффективность такого метода: используя 2 бита на канал мы сможем прятать три байта информации на 4 пиксела изображения. А это уже где-то 25% картинки. Например, в мегабайтовом файле можно спрятать 250 Кбайт информации, причем для невооруженного глаза этот факт останется незаметен.

Недостатки метода:

1. Скрытое сообщение легко разрушить, например при сжатии или отображении.
2. Не обеспечена секретность встраивания информации. Точно известно местоположение зашифрованной информации. Для преодоления этого недостатка можно встраивать информацию не во все пикселы изображения, а лишь в некоторые из них, определяемые по псевдослучайному закону в соответствии с ключом, известному только законному пользователю. Пропускная способность при этом уменьшается.

Рассмотрим подробнее вопрос выбора пикселов изображения для встраивания в них скрытого сообщения.

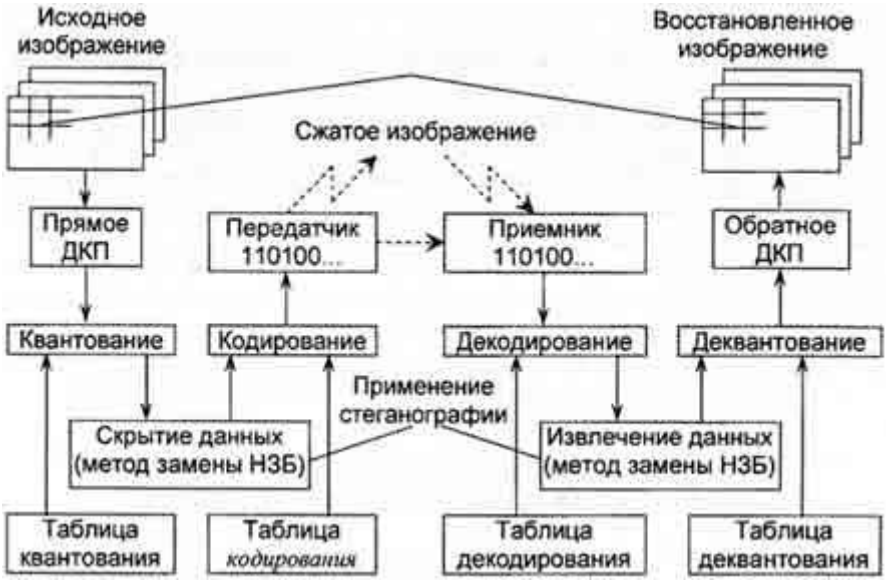
Характер поведения младшего бита неслучаен. Скрываемое сообщение не должно изменять статистики изображения. Для этого, в принципе возможно, располагая достаточно большим количеством незаполненных контейнеров, подыскать наиболее подходящий. Теоретически возможно найти контейнер, уже содержащий в себе наше сообщение при данном ключе. Тогда изменять вообще ничего не надо, и вскрыть факт передачи будет невозможно. Метод выбора подходящего контейнера требует выполнения большого количества вычислений и обладает малой пропускной способностью.

Альтернативным подходом является моделирование характеристик поведения LSB. Встраиваемое сообщение будет в этом случае частично или полностью зависеть от контейнера. Процесс моделирования является вычислительно трудоемким, кроме того, его надо повторять для каждого контейнера. Главным недостатком этого метода является то, что процесс моделирования может быть повторен нарушителем, возможно обладающим большим вычислительным ресурсом, создающим лучшие модели, что приведет к обнаружению скрытого сообщения. Это противоречит требованию о независимости безопасности стегосистемы от вычислительной мощности сторон. Кроме того, для обеспечения скрытности, необходимо держать используемую модель шума в тайне. А как нам уже известно, нарушителю неизвестен должен быть лишь ключ.

В силу указанных трудностей на практике обычно ограничиваются поиском пикселов, модификация которых не вносит заметных искажений в изображение. Затем из этих пикселов в соответствии с ключом выбираются те, которые будут модифицироваться. Скрываемое сообщение шифруется с применением другого ключа. Этот этап может быть дополнен предварительной компрессией для уменьшения объема сообщения.

Алгоритм преобразования графического изображения JPEG

При сжатии алгоритм состоит из нескольких последовательных операций, выполняемых одна за другой: преобразования цветового пространства; поддискретизации; прямого дискретного косинусного преобразования (ДКП); квантования; скрытия данных методом замены LSB; кодирования. А при восстановлении изображения эти операции выполняются в обратном порядке.
Метод замены наименее значимых бит в спектре изображения использует психофизиологические особенности зрения человека. Он основан на использовании того факта, что замена LSB частот блоков изображения после их квантования (перед этапом кодирования) заменит изображение на зрительно неотличимое от оригинального.



Этот метод позволяет скрывать большое число бит, и его стойкость к атаке пассивного противника значительна. Предварительное кодирование скрываемых данных, а также замена LSB в псевдослучайной последовательности дополнительно повышают стойкость этого метода. При использовании этого метода объем скрываемых данных пропорционален объему сжатого изображения, при этом увеличение объема внедряемой информации может приводить к изменениям исходного изображения и снижению эффективности последующего этапа кодирования. Однако возможность варьировать качество сжатого изображения в широком диапазоне не позволяет определить, являются ли возникающие в результате сжатия погрешности следствием скрытия данных или использования больших коэффициентов квантования.

Применение

В настоящее время можно выделить три тесно связанных между собой и имеющих одни корни направления приложения стеганографии: сокрытие данных (сообщений), цифровые водяные знаки и заголовки.

Сокрытие внедряемых данных, которые в большинстве случаев имеют большой объем, предъявляет серьезные требования к контейнеру: размер контейнера в несколько раз должен превышать размер встраиваемых данных.

Цифровые водяные знаки - используются для защиты авторских или имущественных прав на цифровые изображения, фотографии или другие оцифрованные произведения искусства. Основными требованиями, которые предъявляются к таким встроенным данным, являются надежность и устойчивость к искажениям.

Цифровые водяные знаки имеют небольшой объем, однако, с учетом указанных выше требований, для их встраивания используются более сложные методы, чем для встраивания просто сообщений или заголовков.

Заголовки - используются в основном для маркирования изображений в больших электронных хранилищах (библиотеках) цифровых изображений, аудио- и видеофайлов.

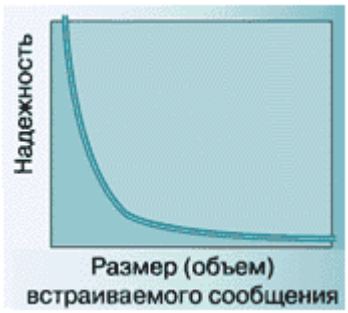
В данном случае стеганографические методы используются не только для внедрения идентифицирующего заголовка, но и иных индивидуальных признаков файла.

Внедряемые заголовки имеют небольшой объем, а предъявляемые к ним требования минимальны: заголовки должны вносить незначительные искажения и быть устойчивы к основным геометрическим преобразованиям.

Ограничения

Каждое из перечисленных выше приложений требует определенного соотношения между устойчивостью встроенного сообщения к внешним воздействиям (в том числе и стегоанализу) и размером самого встраиваемого сообщения.

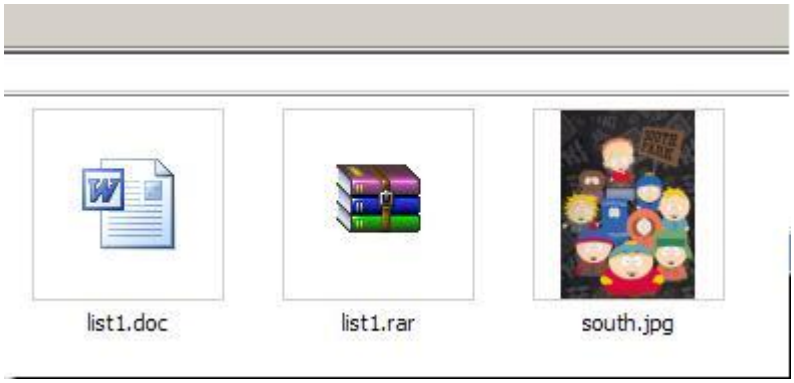
Для большинства современных методов, используемых для сокрытия сообщения в цифровых контейнерах, имеет место следующая зависимость надежности системы от объема встраиваемых данных (рис. 2).



Данная зависимость показывает, что при увеличении объема встраиваемых данных снижается надежность системы (при неизменности размера контейнера). Таким образом, используемый в стегосистеме контейнер накладывает ограничения на размер встраиваемых данных.

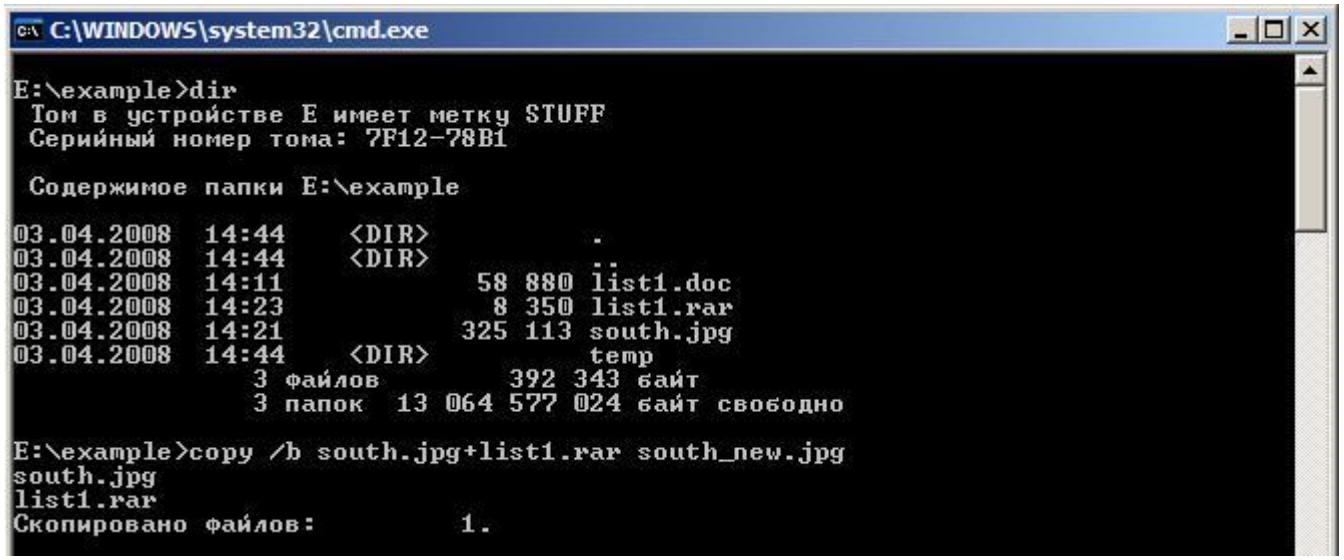
Примеры

Возьмем сверхсекретный файл list1.doc с результатами второго quiz. Зарарим его. Для надежности при архивации его можно запаролить. Будем прятать его в изображении.



Далее: открываем командную строку и вбиваем туда

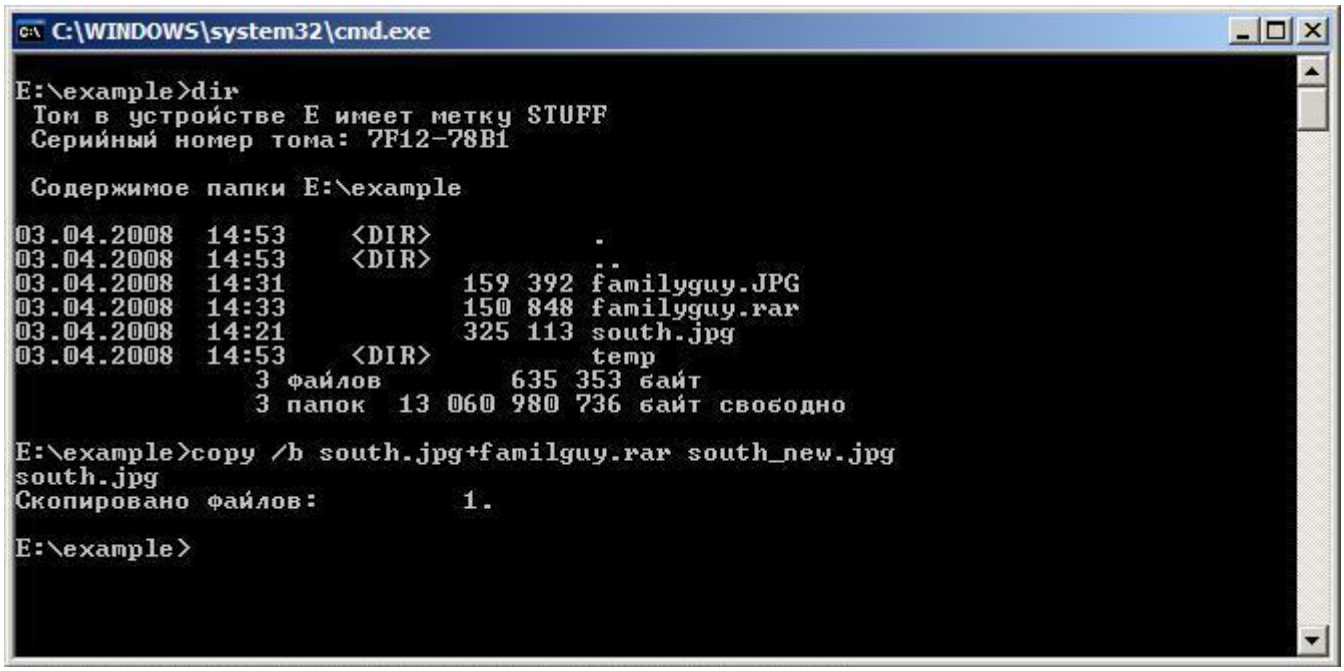
copy /b south.jpg+list1.rar south_new.jpg



Сравним 2 изображения до и после добавления файла

ДО ПОСЛЕ

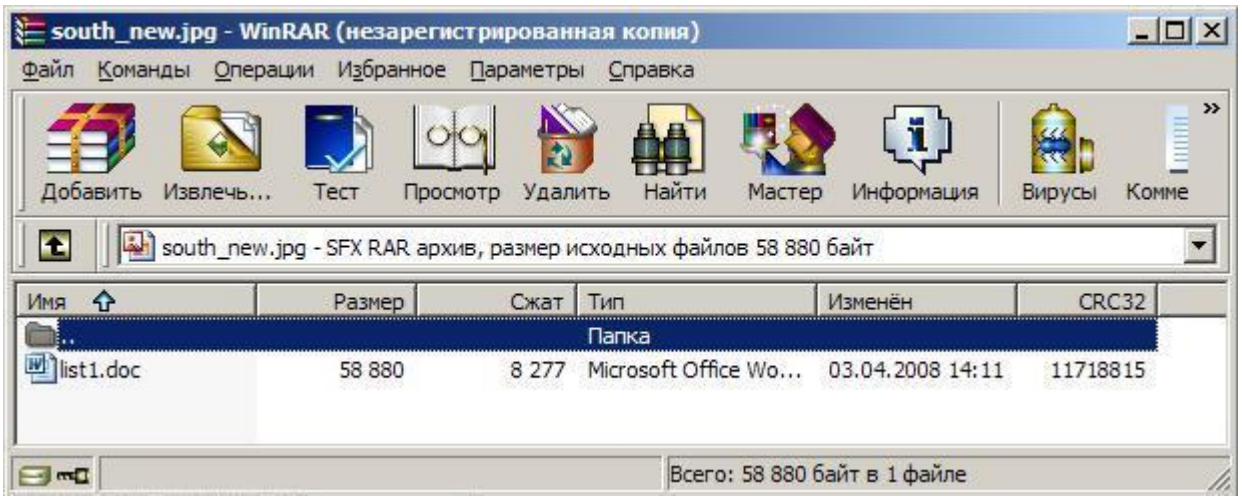
Теперь попробуем вложить одно изображение в другое:

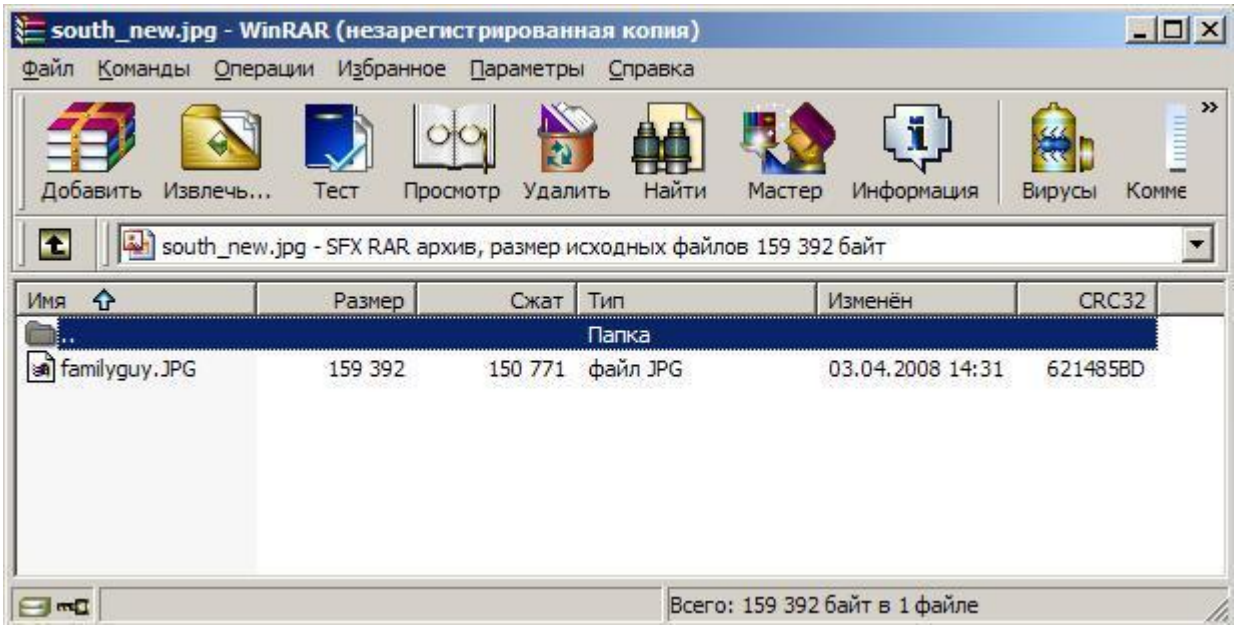


Снова сравним результаты:

ДО ПОСЛЕ

Как потом извлечь секретную информацию из изображения? Открыть ее архиватором и извлечь в нужную папку.





Заключение

В настоящее время компьютерная стеганография продолжает развиваться: формируется теоретическая база, ведется разработка новых, более стойких методов встраивания сообщений. Среди основных причин наблюдающегося всплеска интереса к стеганографии можно выделить принятые в ряде стран ограничения на использование сильной криптографии, а также проблему защиты авторских прав на художественные произведения в цифровых глобальных сетях.