электронное научно-техническое издание
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 30569. Государственная регистрация №0421100025. ISSN 1994-0408

Как можно спрятать информацию?

 # 07, июль 2011

автор: Васина Т. С.

УДК 003.26.
05.13.00

МГТУ им. Н. Э. Баумана
tanka_best@mail.ru

Согласитесь, что не каждому из вас хотелось бы, чтобы его личные данные или какие-то секретные материалы были известны всем, но сейчас существует множество способов, с помощью которых можно узнать всю информацию, которая вас интересуют. А как же быть с тем, что не должно попасть другим на глаза, должно остаться в секрете от остальных. Вот тут на помощь приходит такая наука как стеганография, которая начала особенно активно развиваться в последнее десятилетие.

Слово «стеганография» пришло в русский язык из латинского: «Steganos» - «тайный», «grapho» - «пишу». Т.е. дословно получается «тайнопись». Основная суть ее заключается в том, чтобы скрыть не только саму информацию, но еще и факт ее передачи, замаскировав передаваемые данные в какую-нибудь обыденную информацию, факт передачи которой не вызывает никаких подозрений. В самых примитивных случаях может быть использовано несколько подходов. Если, в детстве, Вы когда-либо писали невидимое сообщение лимонным соком и давали друзьям, чтобы они прогревали его около лампочки для того, чтобы наблюдать, как чудесным образом появляется сообщение, Вы использовали стеганографию [1].

Для наглядности рассмотрим ещё один пример. Самый простой метод сокрытия информации - в тексте. Вот возьмём к примеру само слово "стеганография". Возьмём и скопируем в любое текстовое поле с проверкой орфографии. Редактор подчеркнёт его красным, слово не обнаружено в словаре. Потому что оно набрано на двух раскладках, русской и английской. Так можно скрыть текст от людей, ищущих через поисковые системы [1].

Стеганография является наукой, разрабатывающей приемы обмена информацией таким образом, что скрывается сам факт существования секретной связи. Она не заменяет криптографию (шифрование данных), а дополняет ее еще одним уровнем безопасности.

При обработке данных стеганографическими методами происходит скрытие передаваемой информации в других объектах (файлах, дисках и т. п.) таким образом, чтобы постороннее лицо даже не догадывалось о существовании скрытого секретного сообщения. При этом обнаружить такое сообщение довольно сложно, но если это и произойдет, то сообщение может быть к тому же еще и надежно зашифровано.

Впервые о стеганографии было упомянуто еще в 5-ом веке до н.э. Летописи Геродота донесли до нас любопытную историю. Тиран Гистий захваченный персидскими войсками в Сузах, захотел послать сообщение своему родственнику в Милиеет, что в Анатолии. Для этого он побрил наголо раба и вытатуировал сообщение на его голове план обороны Персов. После того, как волосы отрасли, раб доставил сообщение. Но это все стеганография в ее первобытном проявлении, по мере же внедрения научных достижений в повседневную жизнь, элементы стеганографии стали появляться в телеграфных сообщениях, радиограммах, наконец в носителях цифровой информации [2].

1. Методы компьютерной стеганографии

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям:

1. Методы, основанные на использовании специальных свойств компьютерных форматов;

2. Методы, основанные на избыточности аудио и визуальной информации.

1.1. Методы, основанные на использовании специальных свойств компьютерных форматов

Первое направление основано на использовании специальных свойств компьютерных форматов представления данных, а не на избыточности самих данных. Специальные свойства форматов выбираются с учетом защиты скрываемого сообщения от непосредственного прослушивания, просмотра или прочтения.

1.2. Методы, основанные на избыточности аудио и визуальной информации

В качестве носителя скрытой информации должен выступать объект (файл), допускающий искажения собственной информации, не нарушающие его функциональность. Внесенные искажения должны быть ниже уровня чувствительности средств распознавания.

В качестве носителя обычно используются файлы изображений или звуковые файлы. Такие файлы обладают большой избыточностью и, кроме того, обычно велики по размеру, обеспечивая достаточно места для сокрытия простого или форматированного текста. Скрываемое сообщение может быть простым набором чисел, изображением, простым или зашифрованным текстом.

Многие мультимедийные форматы имеют поля расширения, которые могут заполняться пользовательской информацией, а могут быть забиты нулями – в последнем случае их также можно использовать для хранения и передачи информации. Однако этот наивный способ не только не обеспечивает требуемого уровня секретности, но и не может прятать значительные объемы данных. Решение этих проблем нашлось в следующем подходе.

В графических файлах, аудио и видео файлах обычно содержится множество избыточной информации, которая совершенно не воспринимается органами чувств человека (следует, правда, заметить, что даже эта избыточная информация очень и очень далека от оригинала, поскольку, во-первых данные всегда разбиваются на конечное число элементов, каждый из которых описывается конечным двоичным числом. Аналоговый же сигнал содержит потенциально бесконечное число сведений, которые обрубаются при оцифровке). Поэтому при умеренной декрементации цифровых данных обычный человек, в силу своего анатомического строения не может заметить разницы между исходной и модифицированной информацией.

Предположим, что в качестве носителя используется 24-битовое изображение размером 800x600 (графика среднего разрешения). Оно занимает около полутора мегабайта памяти (800x600x3 = 1440000 байт). Каждая цветовая комбинация тона (пикселя – точки) – это комбинация трех основных цветов – красного, зеленого и синего, которые занимают каждый по 1 байту (итого по 3 на пиксел). Если для хранения секретной информации использовать наименьший значащий бит (Least Significant Bits – LSB) каждого байта, то получим по 3 бита на каждый пиксел. Емкость изображения носителя составит – 800x600x3/8=180000 байт. При этом биты в каких-то точках будут совпадать с битами реального изображения, в других – нет, но, главное, что на глаз определить такие искажения практически невозможно [3].

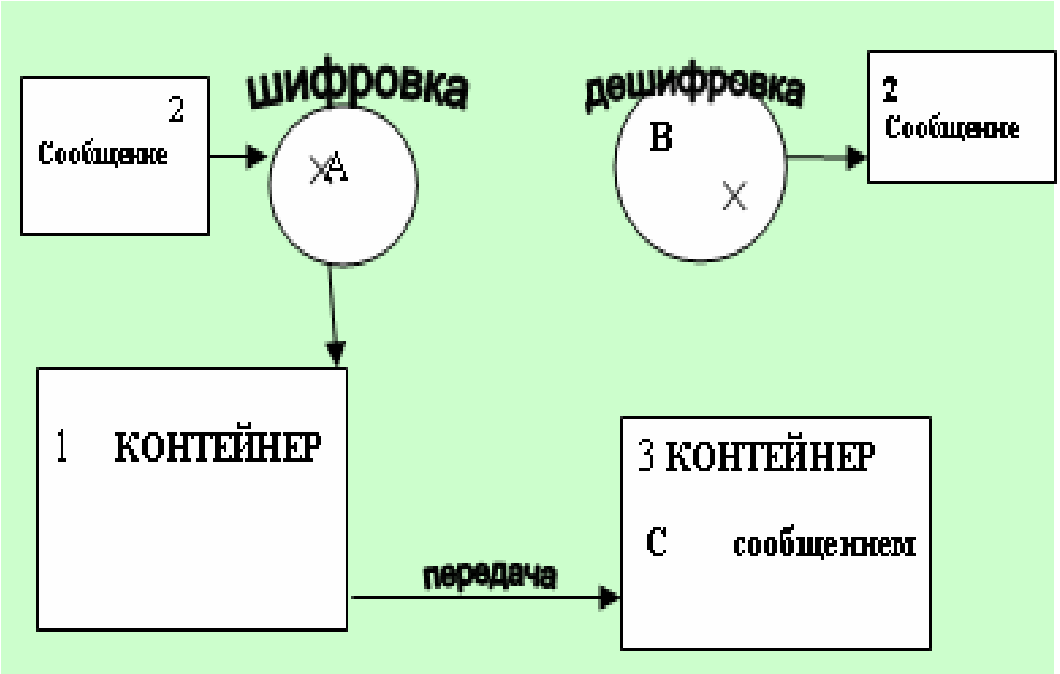

Рис. 1.

Цифровая стеганография реализуется следующим образом: имеется какой-то цифровой файл – контейнер (фото) (1) и сам файл-сообщение (2). Для обеспечения разрозненности и случайности значений зашифруем (А), так как шифровка обеспечивает большую степень защиты данных. Затем производится вставка сообщения в файл-контейнер. Затем можно свободно передавать файл, но пароль для расшифровки должен быть заранее передан по независимому каналу получателю информации.

Самой главной задачей является обеспечить наибольшее сходство файла контейнера с уже вложенным сообщением.

В младших битах изображений и других мультимедиа файлов имеются шумы – они распределены по всему файлу произвольным образом, и как правило представляют собой случайные числовые значения.

Для обеспечения псевдослучайности при вставке файла в контейнер используют алгоритмы шифрования. Для большей надежности и схожести оригинала следует использовать изображения с шумами в младших разрядах – это изображения, полученные при помощи цифровой фотокамеры или со сканера. Такие изображения уже содержат внутри себя случайный шум, который дополнительно маскирует факт внедрения посторонней информации внутрь файла.

Кроме скрытой передачи сообщений, стеганография является одним из самых перспективных направлений, применяемых для аутентификации и маркировки авторской продукции. При этом часто в качестве внедряемой информации используются дата и место создания продукта, данные об авторе, номер лицензии, серийный номер, дата

истечения срока работы (удобно для распространения shareware-программ) и др. Эта информация обычно внедряется как в графические и аудио- произведения так и в защищаемые программные продукты. Все внесенные сведения могут рассматриваться как веские доказательства при рассмотрении вопросов об авторстве или для доказательства факта нелегального копирования, и часто имеют решающее значение.

На первый взгляд заметить что информация была передана с использованием того или иного метода стеганографии невозможно. Но это не так. Обнаружить сам факт передачи информации и перехватить её вполне реально и именно поэтому для сейчас вместе со стеганографией неотъемлемо выступает понятие «криптография». Криптогра́фия— наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации. Ведь с использованием криптографии сложность распознавания передачи информации увеличивается почти в два раза, теперь перед «перехватчиком» стоит задача помимо того что ему надо заметить что файл был передан с использованием стеганографии, так ему ещё и нужно будет расшифровать информацию, что займет намного больше времени. Тем самым, когда информация будет перехвачена и расшифрована она уже потеряет свою актуальность [4].

Заключение

Вывод, который я бы хотела сделать, состоит в том, что в современном мире понятия криптография и стеганография не могут рассматриваться отдельно. В последнее время эти термины воспринимаются как одно целое, поскольку незащищенность методов стеганографии обречена на неудачу.

Список литературы

1. Boney L., Tewfic A.H., Hamdy A.K., Digital watermarks for audio signals, Department of Electrical engineering, University of Minnesota.
2. Marvel L. Image Steganography for hidden communication. PhD Thesis. Univ.of Delaware, 1999. 115p.
3. В. Г. Грибунин, И. Н. Оков, И. В. Туринцев Цифровая стеганография. // Солон-Пресс, 2002. – 272 с.
4. .Г. Ф. Конахович, А. Ю. Пузыренко . Компьютерная стеганография. Теория и практика.// МК-Пресс, 2006. – 288 с.