Лабораторная работа № 5

Стеганография

Цель работы: Изучение основных принципов скрытой передачи информации, получение навыков работы с программой стенографического сокрытия информации S-Tools.

Теоретическая часть

Слово “стеганография” происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и, таким образом, означает буквально “тайнопись”, хотя методы стеганографии появились, вероятно, раньше, чем появилась сама письменность (первоначально использовались условные знаки и обозначения). По возрасту она существенно старше криптографии.

Цель криптографии состоит в сокрытии содержания секретных сообщений.

Правда, в этом случае противник знает, что вы передаете некоторое секретное сообщение, но не может его прочитать. Но даже факта передачи шифрованных сообщений вполне достаточно, чтобы вами заинтересовались компетентные органы.

Стеганография идет принципиально дальше: ее цель скрыть от непосвященных лиц сам факт существования сообщений. Такие скрытые сообщения могут включаться в различные внешне безобидные данные и передаваться вместе с ними вне какого-либо подозрения со стороны. "КОМПАНИЯ "ЛЮЦИФЕР" ИСПОЛЬЗУЕТ ЕДКИЙ НАТР, ТЯЖЕЛЫЕ ГРУЗИЛА, ОСТРОГУ ТРЕХЗУБУЮ, ОБВЕТШАЛЫЙ ВАТНИК".

Обратите внимание на первые буквы, они складываются в предложение: "Клиент готов". Этот пример хотя и тривиален, но он позволяет проиллюстрировать способ скрытия информации, называемый *стеганографией*.

Стеганография известна еще со времен Геродота. 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. Еще один, весьма неожиданный способ сокрытия информации или условных знаков - татуировка на голове бритого посланца. После отрастания волос послание становится невидимым. Для прочтения требуется побрить голову гонца. Вот только уничтожать секретное сообщение, похоже, придется вместе с головой носителя.

К стеганографии также относится написание текстов невидимыми чернилами, проявляющимися при нагревании. Помните дедушку Ленина, который в тюрьме писал статьи в "Искру" молоком между строк книги? Еще "чернильница" у него была из хлеба, и он ее быстро съедал, когда надзиратель подходил к двери камеры. Прямо детективная была история! По мере совершенствования техники обнаружения тайнописи появились и специальные химические соединения. Но это было до компьютеров.

По сути компьютерная стеганография базируется на двух принципах. Первый заключается в том, что файлы, в первую очередь содержащие оцифрованное изображение или звук, могут быть до некоторой степени видоизменены без потери функциональности, в отличие от других типов данных, требующих абсолютной точности. Второй принцип состоит в неспособности органов чувств человека различить незначительные изменения в цвете изображения или качестве звука, что особенно легко использовать применительно к объекту, несущему избыточную информацию, будь то 16-битный звук или 24-битное изображение.

Для целей стеганографии обычно используется 24 - битный BMP формат (на пиксел отводится три байта). Полезная (передаваемая)

информация записывается в качестве младшего бита каждого цвета (RGB). Изменения не уловимы для человеческого глаза.

Рассмотрим пример:

Пусть имеется число 180, в двоичном коде оно выглядит так: 10110100.

Давайте спрячем его в последовательности из восьми байт, приведенной в первой колонке таблицы. Для этого заменим в двоичном представлении чисел последовательности (вторая колонка) младшие биты (подчеркнуты) битами нашего числа. Получим третью колонку таблицы, десятичное представление чисел которой запишем в четвертой колонке.

Исходные значения (десятичные)	Двоичное представление	Последовательность после замены	Десятичные значения после замены
135	10000111	10000111	135
121	01111001	01111000	120
120	01111000	01111001	121
107	01101011	01101011	107
143	10001111	10001110	142
98	01100010	01100011	99
103	01100111	01100110	102
102	01100110	01100110	102

Плотность упаковки 1:8, т.е. для скрытия какого-либо файла необходим контейнер, имеющий объем в 8 раз больше.

В качестве контейнеров целесообразно использовать звуковые файлы плохого качества, но громкие. Изображения лучше использовать пестрые, без четких геометрических фигур и без обширных однотонных участков. Черно-белые полутоновые изображения предпочтительнее высококачественных цветных. Не стоит прятать сообщения в популярные заставки; всегда лучше, чтобы это был уникальный (в смысле – не виденный ранее никем из потенциальных "перехватчиков") рисунок. Плохая идея – использовать известную картину, например, «Джоконду» Леонардо де Винчи, так как все знают, как она выглядит, и, кроме того, она содержит большие зоны одного цвета. А вот фотография вашего песика вполне подойдет.

На практике компьютерная стеганография может принимать самые разные формы. Например, можно пойти путем Ульянова-Ленина, и написать письмо невидимыми чернилами, то есть шрифтом.

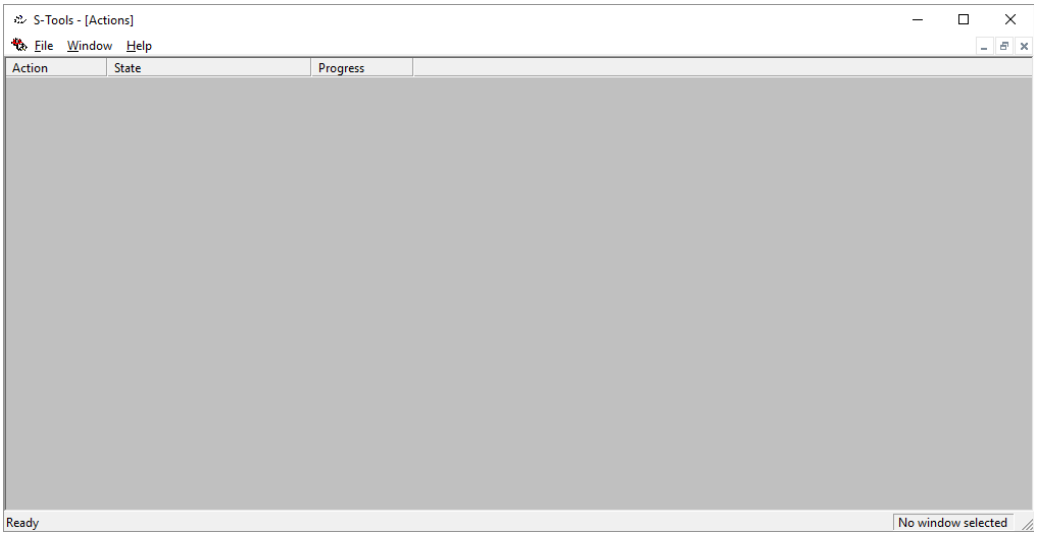
Для этого достаточно в обычном редакторе "Microsoft Word" написать какое-нибудь обыкновенное письмо, например, рекламу очередного способа заработать миллион за месяц. В конце этого письма можно дописать несколько строчек с той информацией, которую нужно скрытно переслать, а затем двумя нажатиями мыши сделать цвет этих строчек одинаковым с фоном письма. Белые буквы на белом фоне будут не видны, и письмо может пройти простейшую проверку.

Разумеется, эта маскировка очень ненадежна, но она предельно проста, не требует никаких дополнительных программ, и хорошо иллюстрирует, как находчивый человек может прятать данные с помощью элементарных приёмов.

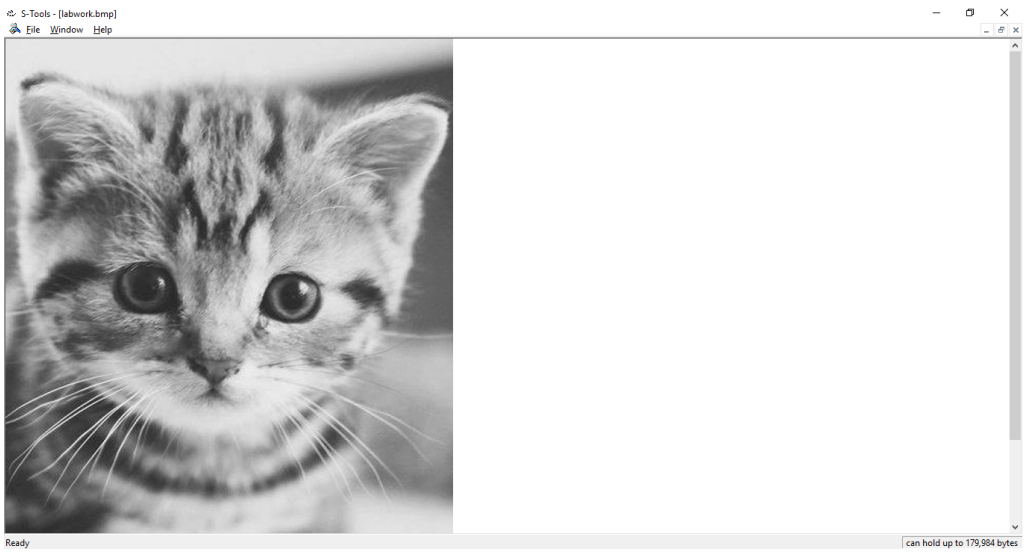
В большинстве стенографических программ, в качестве файлов-контейнеров используются графические и звуковые файлы. По многим показателям это наилучший выбор. Рисунки или фотографии легко доступны, могут иметь самый разный размер, и пересылка их по почте не вызывает больших подозрений.

Наиболее известной утилитой, умеющей прятать информацию в рисунках и звуках, является программа Энди Брауна S-Tools. Она умеет работать с графическими файлами с расширением gif и bmp, и со звуковыми в формате wav. Во все три формата S-Tools может прятать абсолютно любые файлы, главное только, чтобы они были не слишком большими. Размер сообщения обычно должен быть в десять раз меньше файла-контейнера, а лучше еще меньше. При этом S-Tools - это стеганография и криптография "в одном флаконе", потому что файл, подлежащий сокрытию, еще и шифруется с помощью одного из криптографических алгоритмов с симметричным ключом: DES, тройной DES или IDEA.

При запуске программы мы видим следующую картинку:

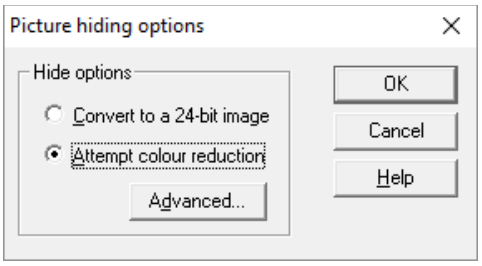


Программа поддерживает функцию drag’&’drop. При этом есть только одно неудобство - кроме окна программы необходимо держать открытым окно Проводника для поиска нужных файлов. Файл-контейнер перетаскивается в окно программы, он отображается в окне либо как есть (для картинки), либо в виде линии, изображающей уровни сигнала (для звука).



После этого необходимо перетащить в окно с картинкой либо уровнем сигнала любой файл, предназначенный для скрытия, размером не более указанного. После проверки размера данных программа запросит пароль, и попросит выбрать алгоритм шифрования.

Программа позволяет упрятать информацию внутрь изображения в формате GIF или BMP. К сожалению, GIF-картинки она предлагает либо преобразовать в True Color (24 бит), либо уменьшить количество цветов изображения для того, чтобы больше места оставить для хранения данных.

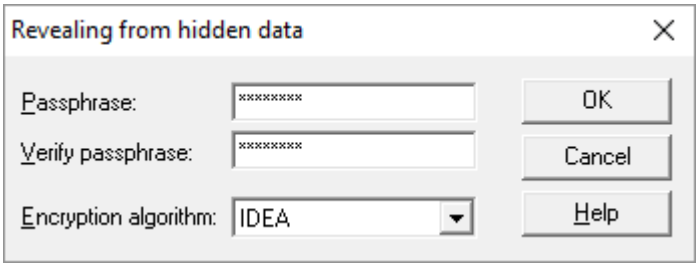


S-tools работает следующим образом: скрываемые данные сначала сжимаются (степень сжатия можно программно регулировать из меню File/Properties), затем шифруются по алгоритму (IDEA, DES) с ключом необходимой длины, полученным из введенного пароля, после чего распределяются по графическому или звуковому файлу в последовательности, определяемой генератором псевдослучайных чисел, начальное значение которого также связано с тем же паролем.

Время скрытия информации зависит от размера данных. Наблюдать за процессом можно в окне «Action». Когда все будет готово, появится окно «Hidden data». После этого вы можете сравнить исходный файл и оригинал.

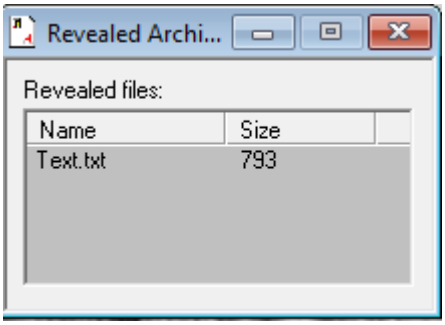
Сохранить результат можно, щелкнув в окне правой кнопкой мыши и выбрав пункт "Save as...", введя имя файла и нажав ОК. При сохранении графической информации качество обеспечивается лишь при сохранении результата в формате BMP.

Для восстановления послания необходимо перетащить картинку либо звук в окно S-tools, щелкнуть на изображении правой кнопкой и выбрать пункт "Reveal...". Программа запросит пароль и информацию о виде шифрования:



Если введенная информация удовлетворит программу, то при наличии спрятанных данных начнется их восстановление, за процессом которого можно наблюдать в окне Action.

Вложенный файл вынимается из рисунка и расшифровывается. Откроется окно с информацией о файле:



Программа также позволяет узнать свойства файла, выведя при запросе сообщение:

Как уже упоминалось выше, для большей безопасности следует использовать неизвестные широкой публике изображения, изменения в которых не бросятся в глаза с первого взгляда, а также изображения с большим количеством полутонов и оттенков.

Также можно использовать самодельные звуковые оцифровки, чтобы информацию в звуковом файле, если кому вздумается анализировать его, проще было принять за шум.

Задание

Изучить теоретическую часть.

Рассмотреть работу стенографического сокрытия информации на основе программы S-Tools:

1. Выполнить внедрение некоторой информации в один из поддерживаемых контейнеров.
1. Сравнить полученный результат с исходным файлом.
2. Извлечь информацию из контейнера.
3. Сделать выводы.
4. Оформить отчет. Отчет должен содержать подробную инструкцию о проделанной работе.

Контрольные вопросы

1. Что такое стеганография?
2. Каковы базовые принципы компьютерной стеганографии?
3. Что такое контейнер? Какие контейнеры поддерживает программа S-tools.
4. Какие можно дать рекомендации по выбору контейнера – картинки?
5. Какие можно дать рекомендации по выбору звукового файла контейнера?
6. Каковы достоинства и недостатки рассмотренной программы.