Лабораторная работа № 4

Цель работы: Ознакомление с понятием стеганографии, ее базовыми принципами, используемыми форматами контейнеров, способами упаковки скрываемой информации, наиболее популярными программами стеганографии.

1. 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 (криптография). 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, позволяет проиллюстрировать способ скрытия информации, называемый стеганографией.

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.

Пусть имеется число 180, в двоичном коде оно выглядит так: 101101 - 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	1000011<u>1</u>	10000111	135
121	0111100<u>1</u>	01111000	120
120	0111100<u>0</u>	01111001	121
107	0110101<u>1</u>	01101011	107
143	1000111<u>1</u>	10001110	142
98	0110001<u>0</u>	01100011	99
103	0110011<u>1</u>	01100110	102
102	0110011<u>0</u>	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 «Джаконду» Леонардо де

Винчи, так как все знают, как она выглядит, и, кроме того, она содержит большие зоны одного цвета. А вот фотография вашей кошки вполне подойдет.

2. Наиболее распространенные стеганографические программы

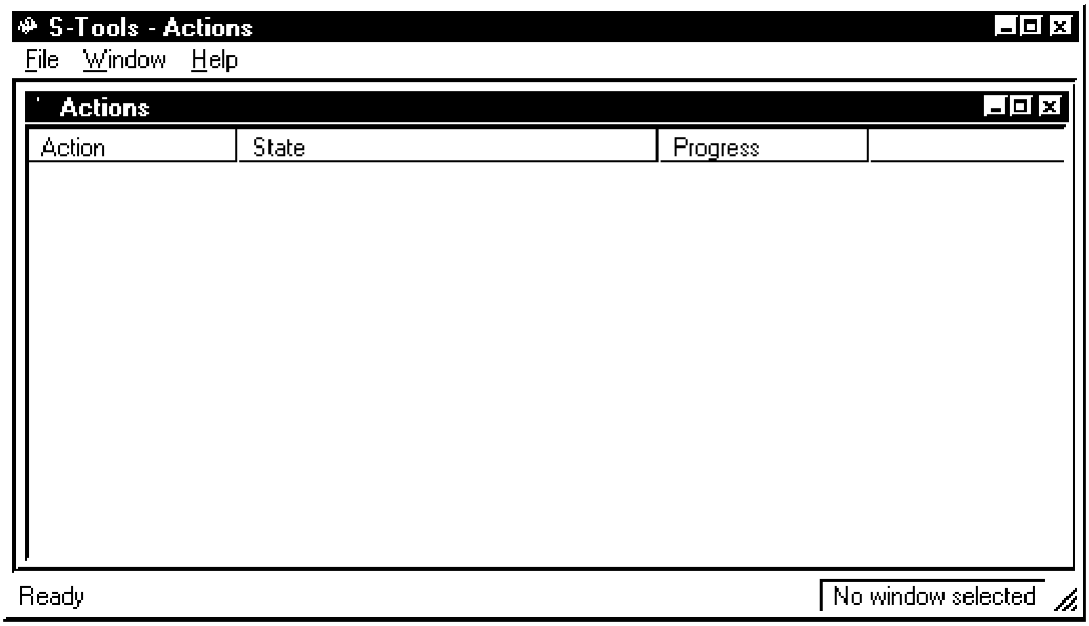
2.1. S-Tools

Один из лучших и самых распространенных продуктов в этой области для платформы Windows это S-Tools. Имеется коммерческая версия и версия freeware. Ее автор Andrew Brown. Программа позволяет прятать любые файлы как в изображениях формата gif и bmp, так и в аудио файлах формата wav.

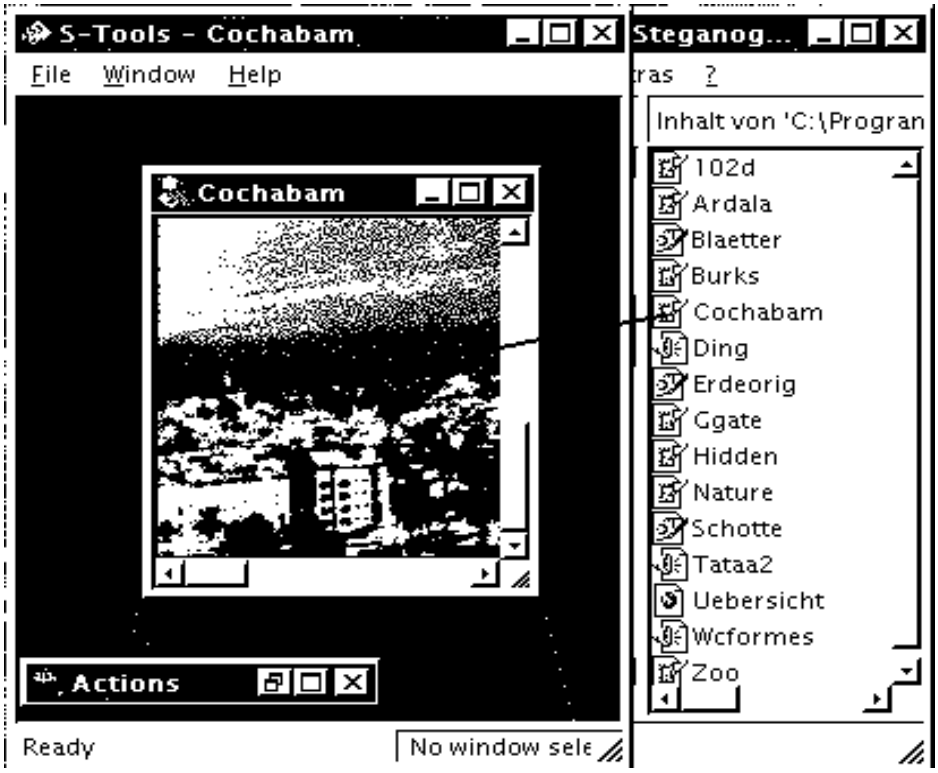
При этом S-Tools - это стеганография и криптография «в одном флаконе», потому что файл, подлежащий сокрытию, еще и шифруется с помощью одного из криптографических алгоритмов с симметричным ключом:

- DES,
- тройной DES,
- IDEA,

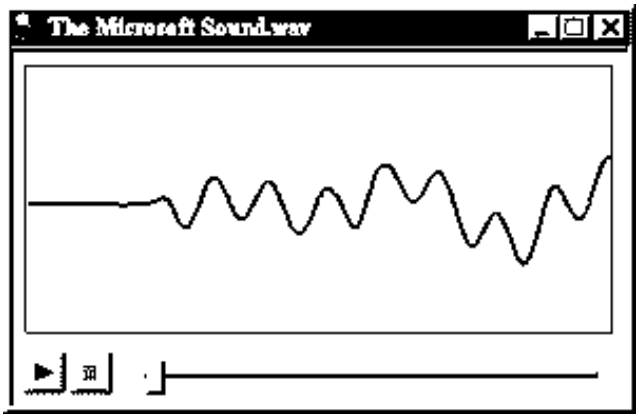
При запуске программы мы видим следующую картинку:



Догадаться, что же делать дальше, не прочитав помощь, невозможно. Обратившись же к помощи, становится все предельно ясно и просто программа поддерживает функцию drag&drop. При этом есть только одно неудобство кроме окна программы необходимо держать открытыми окна Проводника для поиска нужных файлов. Файл-контейнер перетаскивается в окно программы, он отображается в окне либо как есть (для картинки),

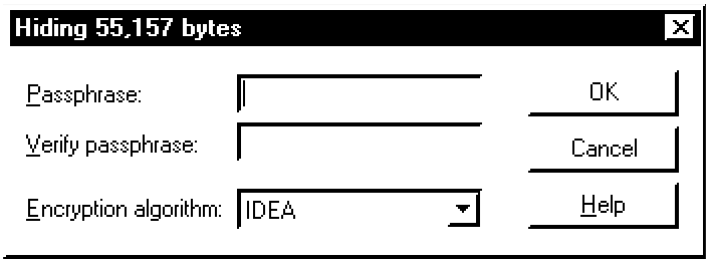


либо в виде линии, изображающей уровни сигнала (для звука).



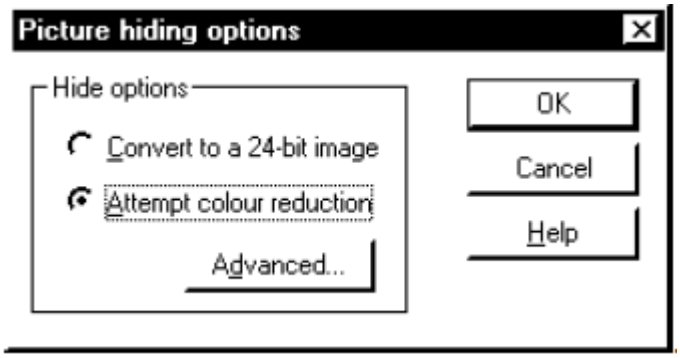
В правом нижнем углу окна S-tools появится информация о размере данных, которые можно спрятать в этом файле.

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.

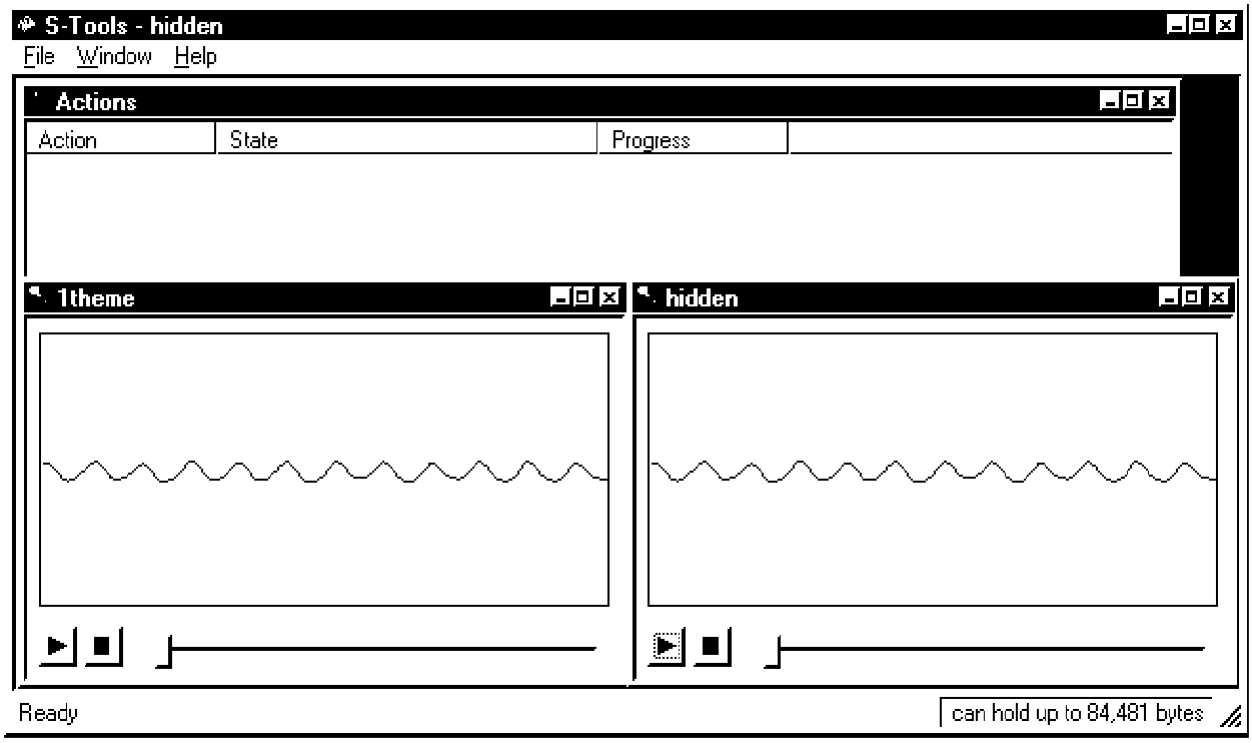


В первом случае сохранить результат удастся только в формате BMP, файл которого имеет значительный размер. Во втором случае конечный результат может иметь настолько убогий вид, что сам факт пересылки такого изображения может вызвать подозрение, так как в настоящее время использование полноцветных изображений режима True Color становится общепринятым.

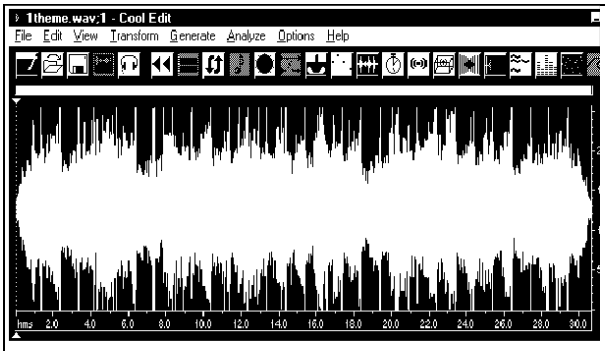
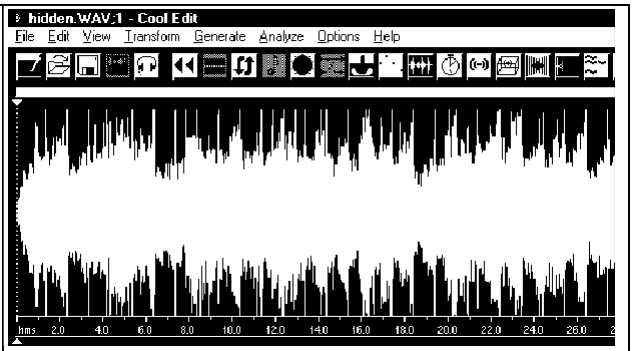
S-tools работает следующим образом: скрываемые данные сначала сжимаются (степень сжатия можно программно регулировать из меню File/Properties), затем шифруются по алгоритму (IDEA, DES) с ключом необходимой длины, полученным из введенного пароля, после чего распределяются по графическому или звуковому 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». Вы можете сравнить исходный файл и оригинал. Внешне при использовании BMP формата графический файл остается практически неизменным, практически неуловимо меняются лишь кое-где оттенки цвета.

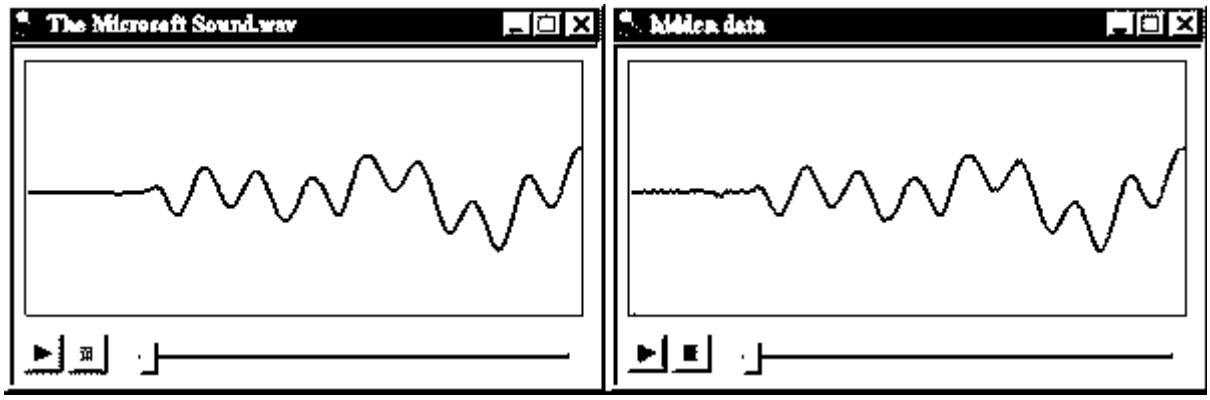
Звуковой файл также не претерпевает заметных изменений.



Если сравнить волновые картины обоих звуковых файлов файла-контейнера и файла со спрятанной информацией, то оказывается, что они практически неразличимы, также как и спектральные.

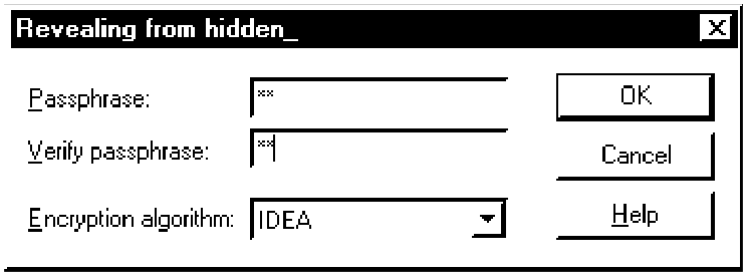
	
Контейнер	А здесь уже спрятано сообщение

Анализ файлов по значениям сигнал/шум (Signal to Noise Ratio) и Общее Гармоническое Отклонение + Шум (Total Harmonic Distortion+Noise) показывает разницу, хотя обычно практически мало уловимую. При работе со звуком (возможно, это заметно на рис.) выдать наличие посторонней информации может малозаметная «рябь» там, где уровень сигнала был нулевым.



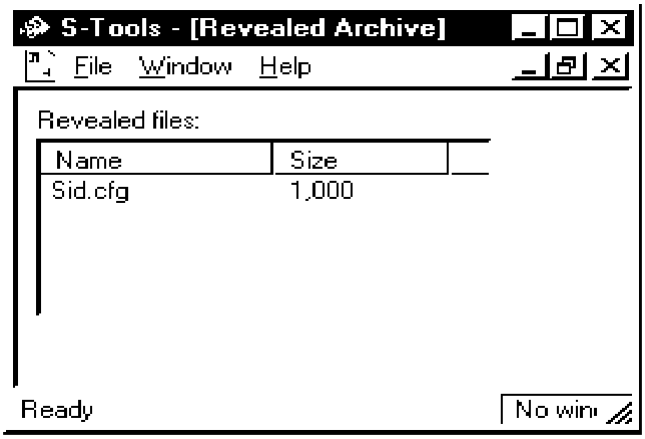
Сохранить результат можно, щелкнув в окне правой кнопкой мыши и выбрав пункт "Save as...", введя имя файла и нажав OK. При сохранении графической информации качество обеспечивается лишь при сохранении результата в формате BMP.

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:

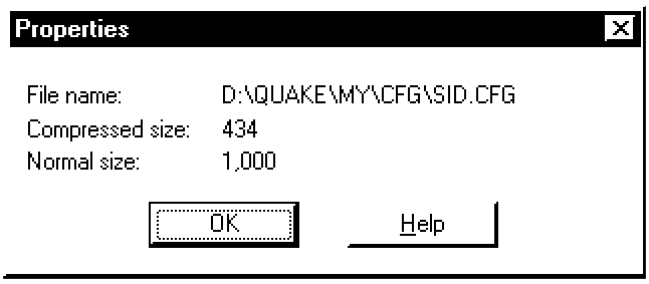


Если введенная информация удовлетворит программу, то при наличии спрятанных данных начнется их восстановление, за процессом которого можно наблюдать в окне Action.

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



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



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.

2.2. Steganos for Windows

Программа Steganos for Windows обладает практически теми же возможностями, что и S-Tools. Созданная в середине 1996 г. программа немецкого программиста Фабиана Хансманна Steganos также объединяет обе защитные технологии: криптографию и стеганографию. Появившись как утилита командной строки **(Steganos v. 1.4**), в настоящее время работает в среде Windows. В разработке Windows версии наряду с Хансманном участвовали Sascha Wildgrube и Gabriel Yoran.

Программа отличается большой номенклатурой форматов файлов, которые могут использоваться в качестве контейнера. В этом качестве могут использоваться :

- графические файлы формата .DIB, BMP;
- звуковые файлы форматов WAV, VOC;
- текстовые файлы формата TXT, HTML.

При использовании 24 битного BMP формата Steganos сохраняет вашу информацию побитно в самом младшем бите каждого байта, соответствующего отдельному цвету (RGB) пиксела изображения. Этот "шум" распределяется по всему файлу.

Чтобы сэкономить место и замести следы, можно преобразовывать BMP-файлы "с начинкой" в другие графические форматы, например gif. Когда при получении адресат преобразует такой файл обратно в формат BMP, программа Steganos все равно сумеет извлечь спрятанное сообщение. Правда, это не относится к сжимающим

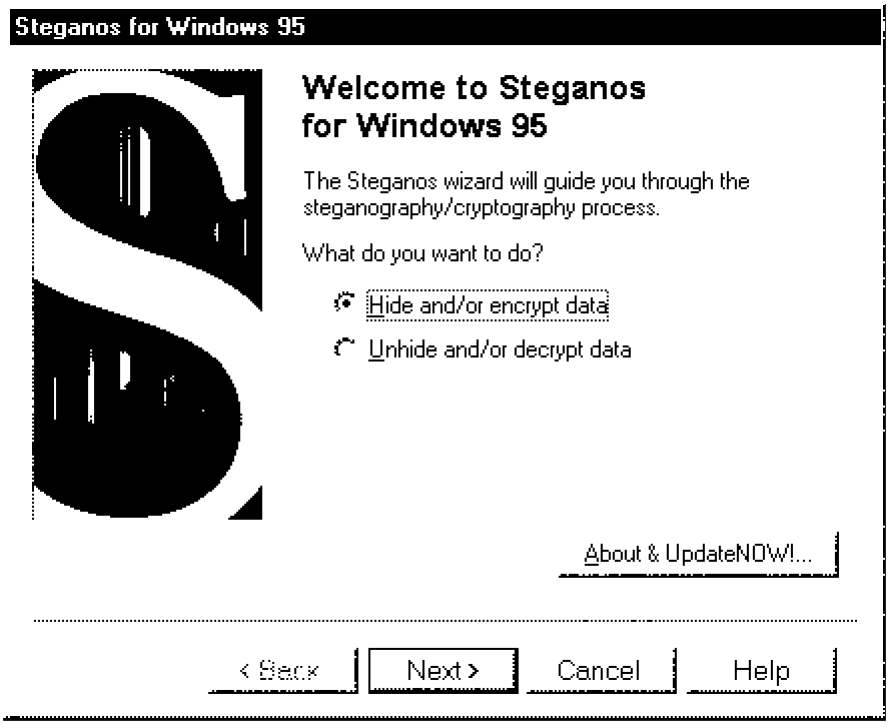
преобразованиям с частичной потерей информации, например, применение формата JPEG, использующего метод DCT (Discrete Cosinus Transformation), разрушит сообщение, спрятанное в картинке.

В обычных текстовых и HTML файлах информация прячется оригинальным способом - в конце каждой строки добавляется определенное число пробелов. Для шифрования используется криптографический алгоритм HWY1.

Программа позволяет удалять после сокрытия секретный файл, создавать резервную копию файла «контейнера», не изменять дату и время создания файла «контейнера».

Работа с программой Steganos for Windows очень проста. Программа общается с пользователем в пошаговом режиме, выдавая и запрашивая информацию, необходимую на данный момент, что делает ее простой и доступной для всех. Начинать работу с ней, можно не читая сопроводительную документацию.

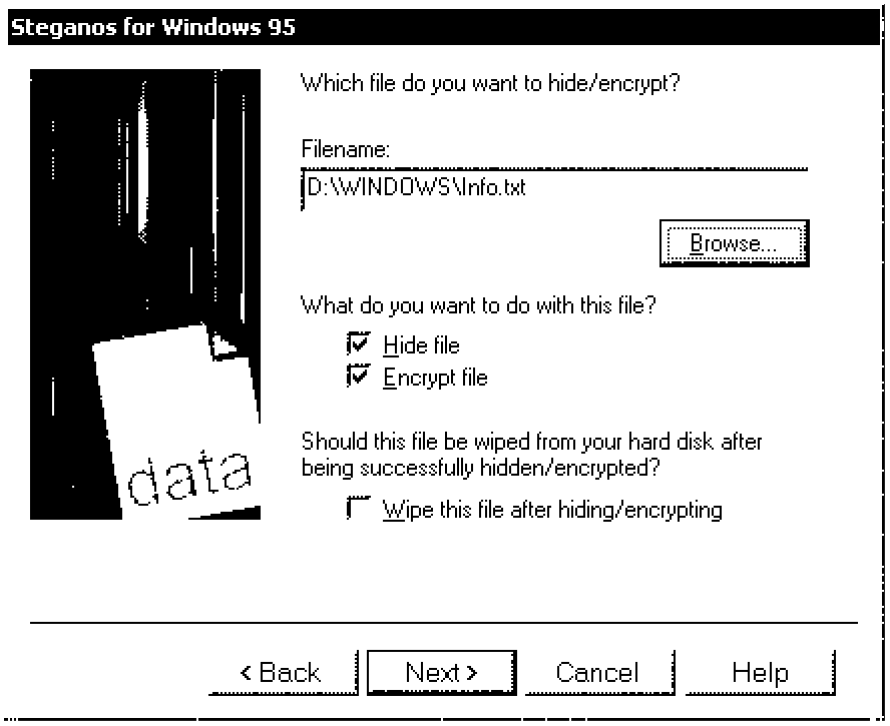
Первое окно программы предлагает определиться: вы хотите спрятать информацию или извлечь спрятанные данные.



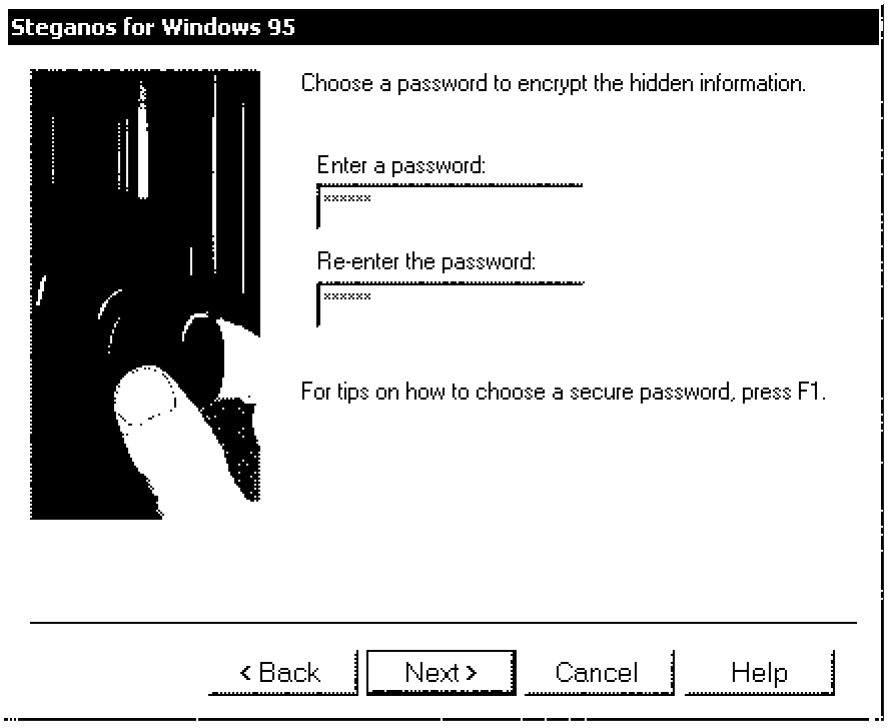
Рассмотрим порядок действий при сокрытии информации:

а) сначала программа запрашивает имя(filename) секретного файла, который необходимо скрыть(hide) и зашифровать (encrypt) в рисунке. Можно

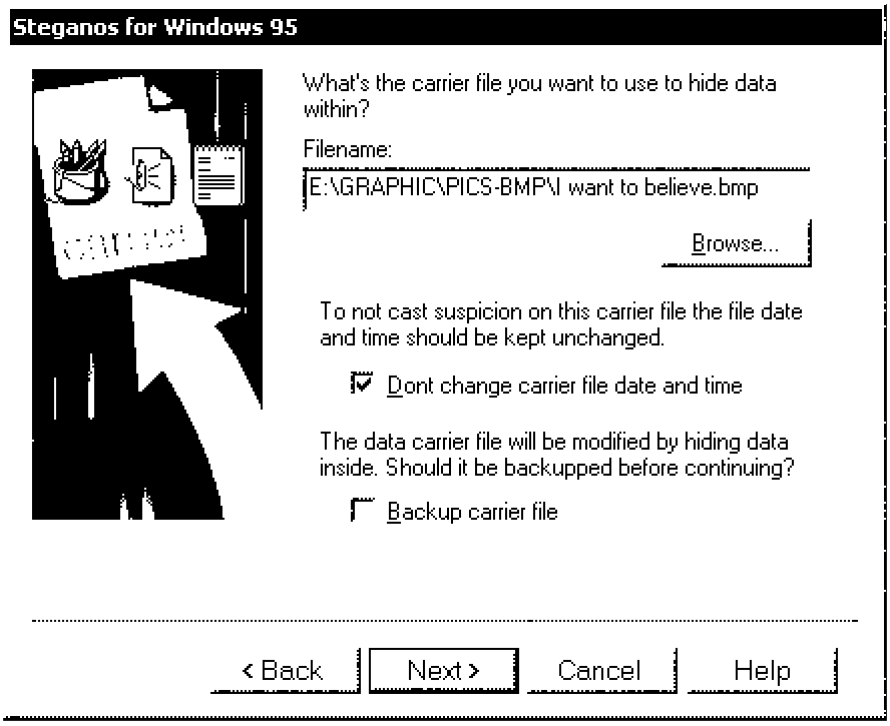
обеспечить стирание исходного секретного файла после его сокрытия, включив опцию «Wipe this file after hiding / encryption»;



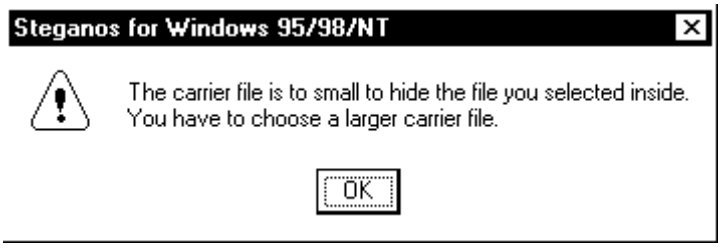
б) затем предлагается ввести 2 раза пароль;



в) далее необходимо определить имя файла (filename), который вы будете использовать в качестве контейнера. Вы можете сделать его архивную копию, включив опцию «Backup carrier file» и сохранить после сокрытия информации старую дату создания контейнера (опция Don□t change file date and time);

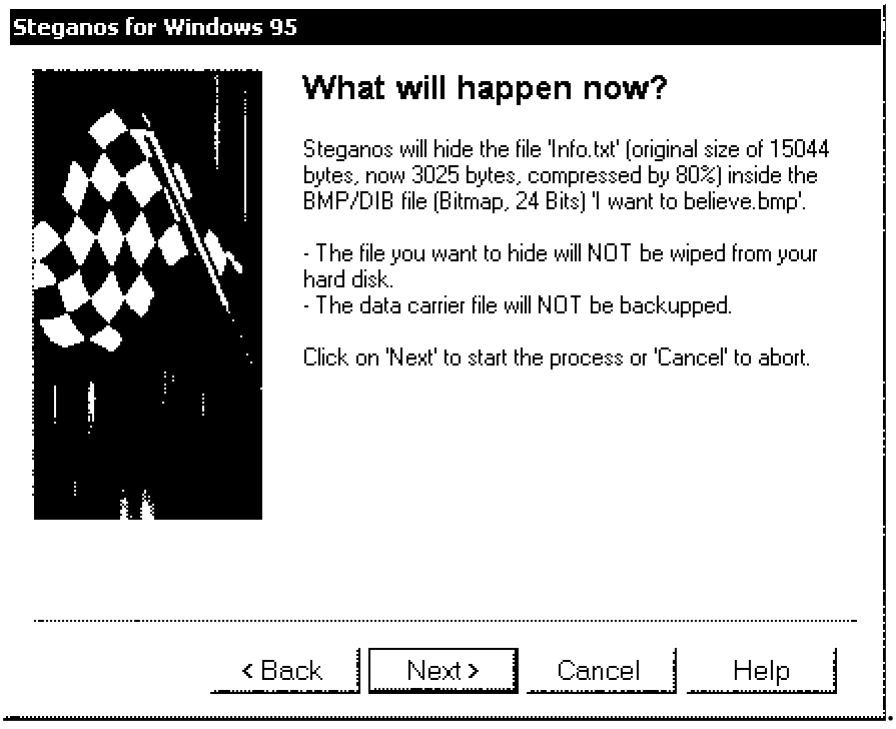


г) если выбранный пользователем контейнер окажется слишком маленьким появится сообщение;



и процедуру ввода имени файла-контейнера придется повторить;

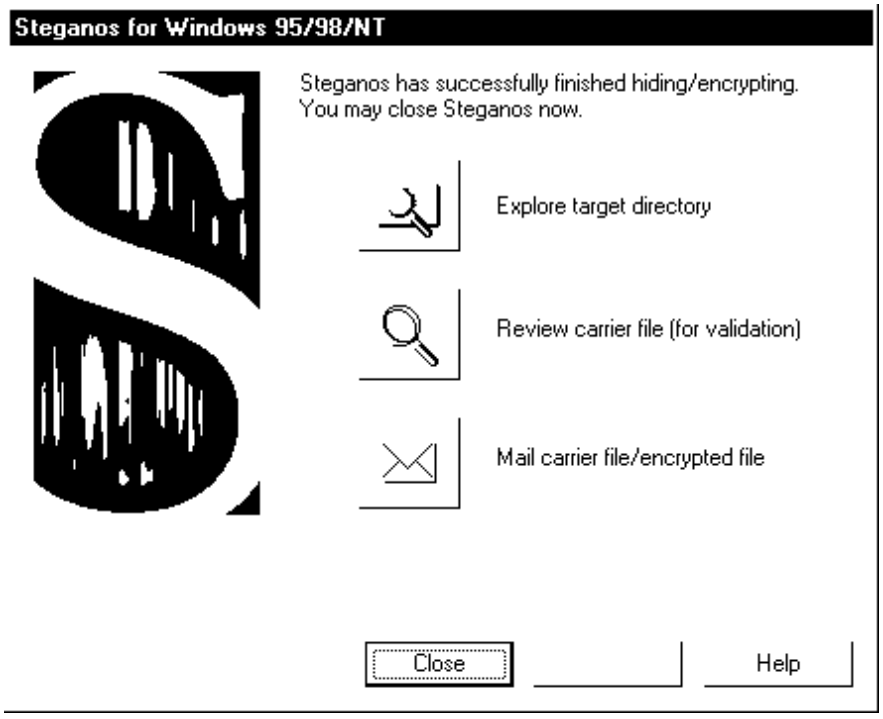
д) следующее сообщение сообщает о начале при нажатии на кнопку NEXT процесса сокрытия информации.



При нажатии кнопки NEXT происходит отображение процесса стеганографии в виде процентной линии, продвигающейся к 100% со скоростью, пропорциональной тактовой частоте компьютера.

Следующее окно информирует пользователя о том, что процесс сокрытия секретного файла прошел успешно (или не успешно) и предлагает ему одно из действий:

- закрыть программу (кнопка Cancel);
- просмотреть измененный графический файл (Review carrrrier file);
- отправить измененный графический файл по почте (Mail carrier file/encrypted);
- просмотреть директорию, куда помещаются полученные файлы.



Процесс изъятия секретного файла (при знании пароля) происходит аналогичным образом.

2.3. Программа JSTEG (JPEG + STEG = JSTEG)

Алгоритм скрытия информации в JPEG реализует пакет программ для DOS - JSTEG , состоящий из 2 программ. Первая программа cjpeg.exe позволяет создать файл в формате JPEG и добавить туда секретное послание, а вторая djpeg.exe извлечь это послание, попутно распаковав JPEG в какой-либо простой формат (по умолчанию - .PPM).

Для создания изображения наберите в командной строке:

CJPEG.EXE -steg secret.txt img.ppm img.jpg.

Здесь

secret.txt имя файла, который необходимо спрятать (необязательно текстовый),

img.ppm имя исходного файла с картинкой,

img.jpg имя конечного файла в формате JPG.

Для восстановления информации наберите в командной строке:

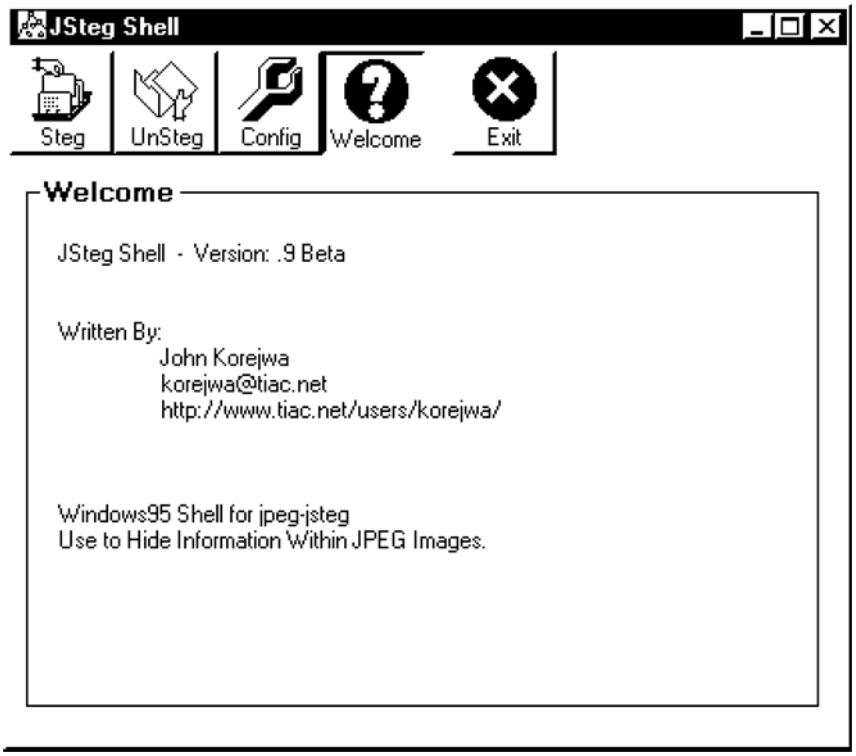
DJPEG.EXE -steg secret.txt img.jpg img.ppm.

Автор программы Derek Upham.

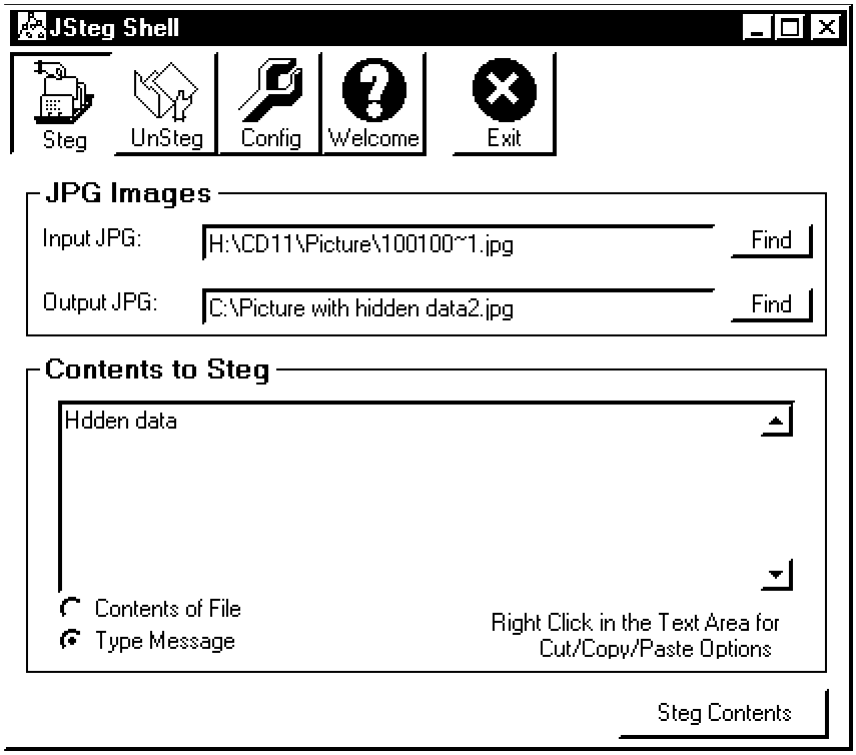
Качество стеганографического сокрытия информации очевидно из сравнения файла-контейнера до и после сокрытия в нем информации.

Программа JSTEG Shell представляет Windows интерфейс для пакета Jsteg.

Интерфейс JSTEG Shell разработан максимально простым и интуитивно понятным для пользователя. Инструментальная панель состоит только из четырех кнопок, обеспечивающих переход к четырем функциональным экранам, и одной кнопки для выхода из программы. При запуске JSTEG активна кнопка Welcome.



Для скрытия информации внутри изображения JPG, нажмите кнопку "Steg".

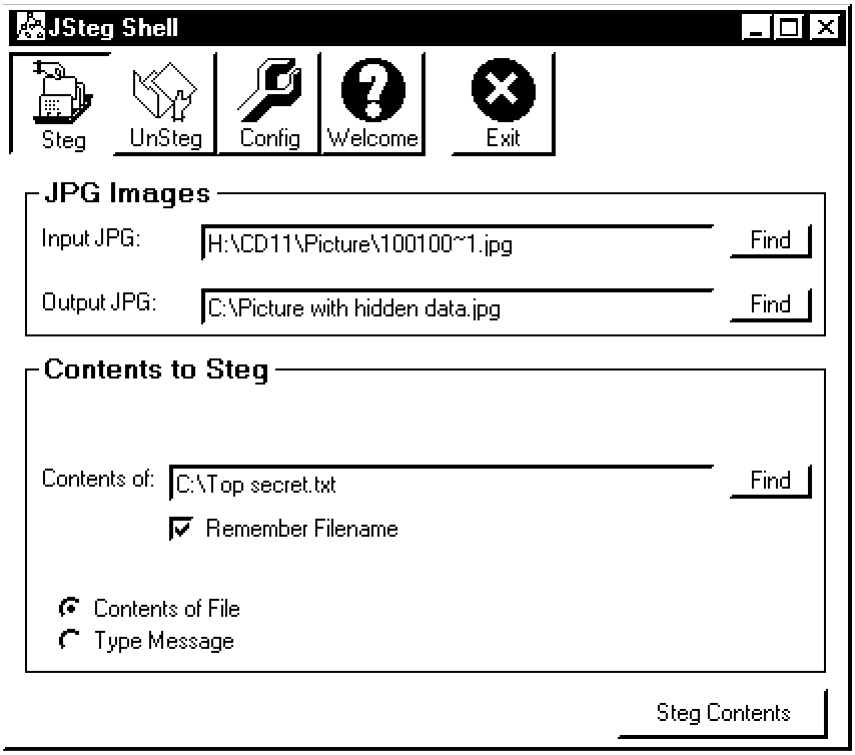


В поле «Input JPG» указывается имя файла контейнера.

В поле «Output JPG» имя нового JPG файла, который будет содержать скрытую информацию.

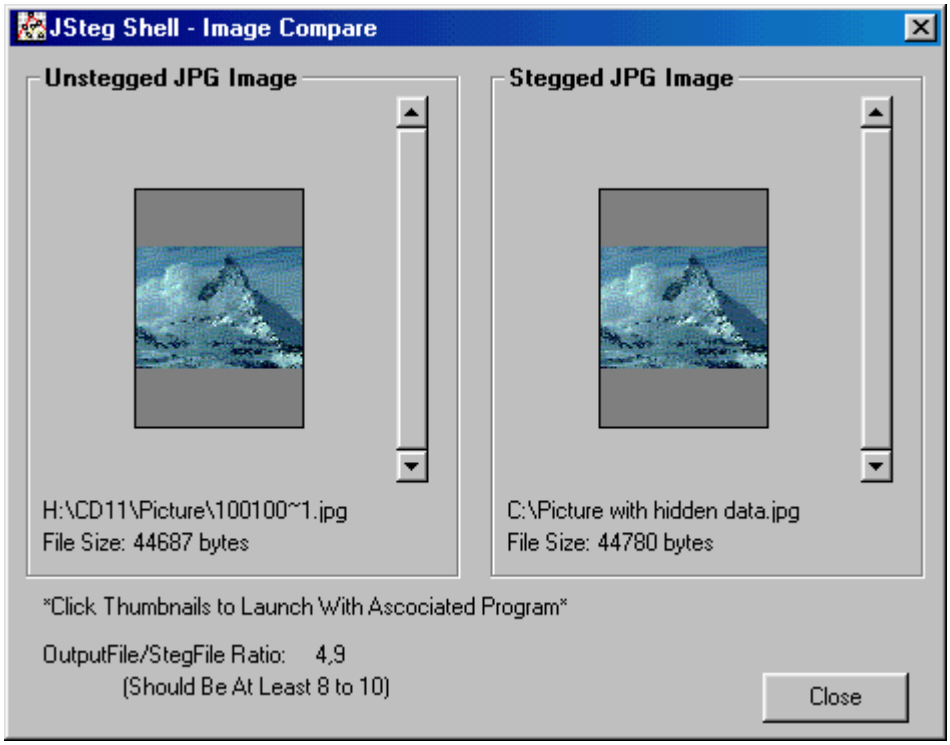
При необходимости скрыть текстовое сообщение в JPG файле, выберите опцию «Type Message» и наберите сообщение в области «Content to Steg». Можно вставить текст из буфера обмена с помощью контекстного меню путем правого щелчка в текстовом блоке.

Для скрытия содержимого файла, включите переключатель «Contents of File». Появится поле для ввода имени файла.



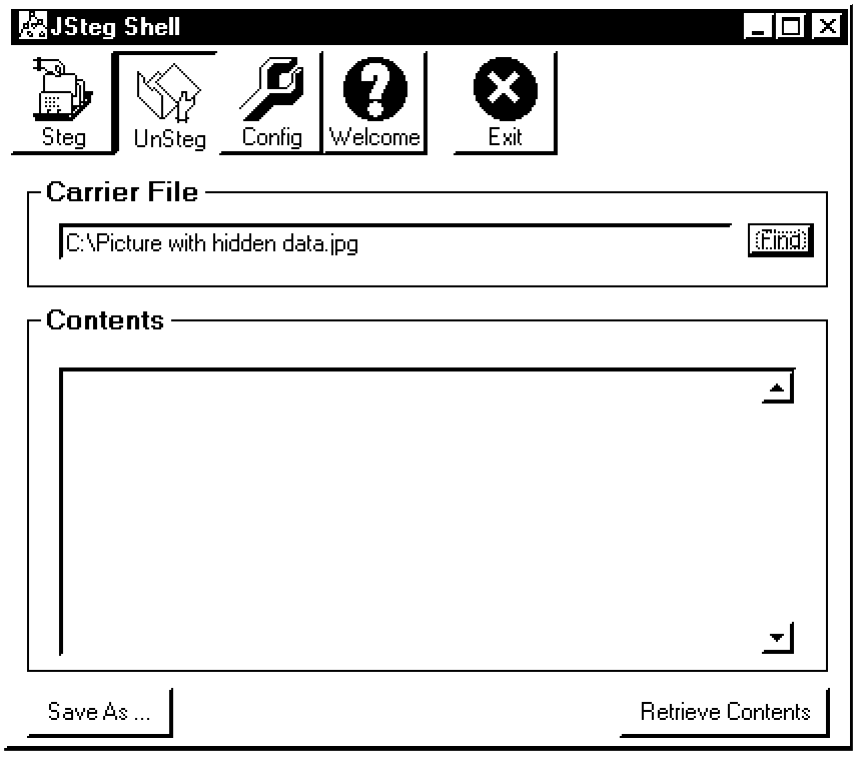
JSTEG (DOS) скроет только содержание файла. При включении переключателя «Remember Filename», JSTEG Shell дополнительно сохранит имя файла, которое будет восстановлено при извлечении скрытой информации.

Для скрытия информации нажмите кнопку «Steg Contents».



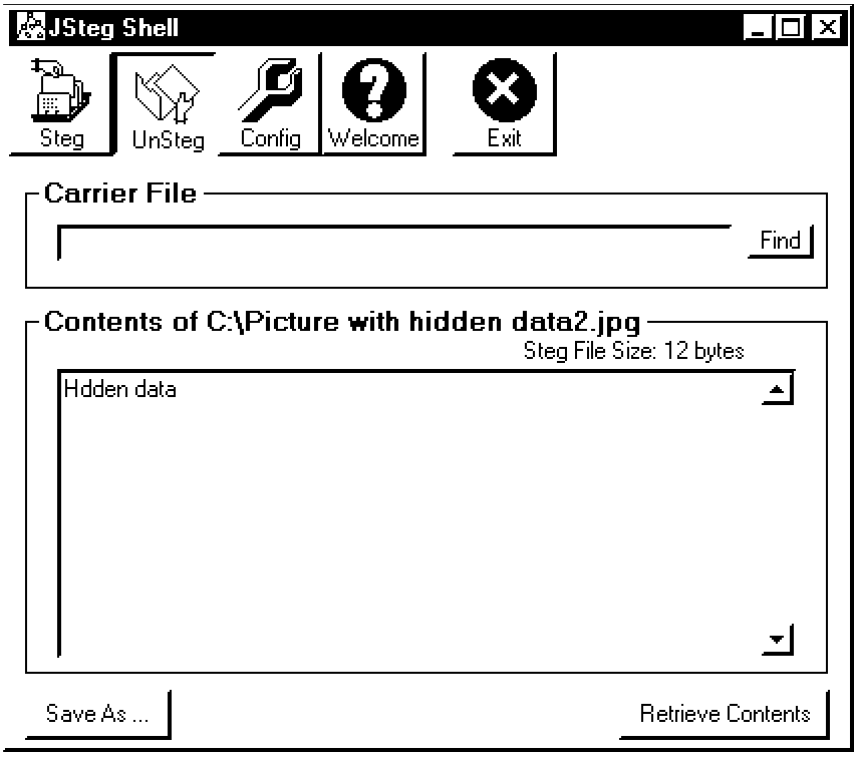
По окончанию упаковки рядом будут показаны оригинальный JPG и новый JPG со скрытой информацией. Вы можете щелкнуть на них и получить полное изображение. Это окно также сообщает отношение размера выходного JPG файла к размеру скрываемого Steg файла (Output File/- StegFile Ratio).

Для извлечения информации из JPG изображения необходимо нажать кнопку UnSteg,



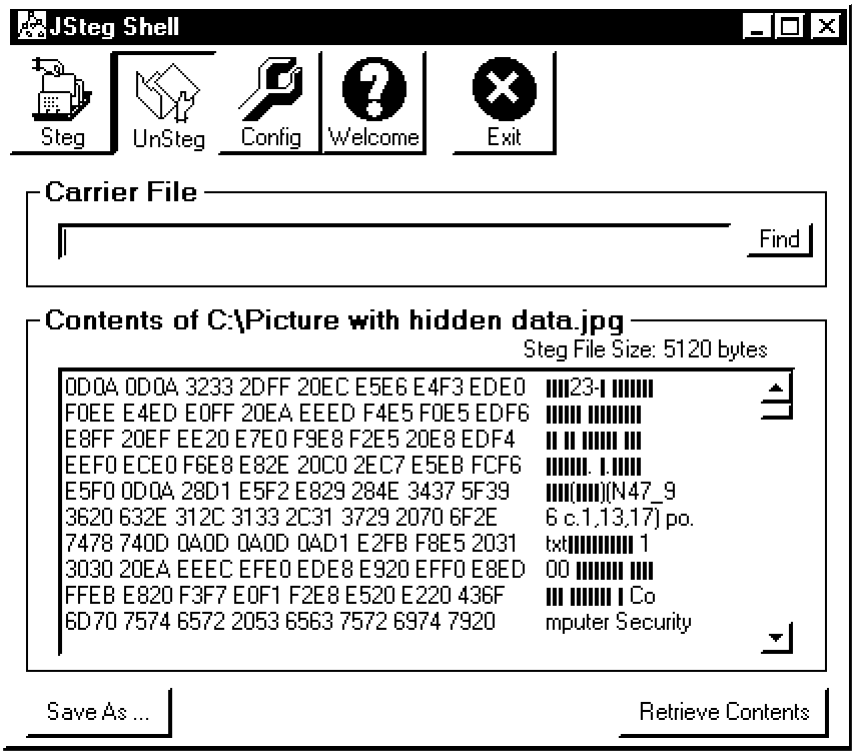
указать имя файла со скрытой в нем информацией (carrier файла) и нажмите кнопку «Retrieve Contents» для запуска JSTEG(DOS). Если для сокрытия информации использовалась оболочка JSTEG Shell и была выбрана опция «Remember Filename», то JSTEG Shell восстановит и имя файла.

Если скрытая информация текст, то появится как простой текст в текстовом блоке.



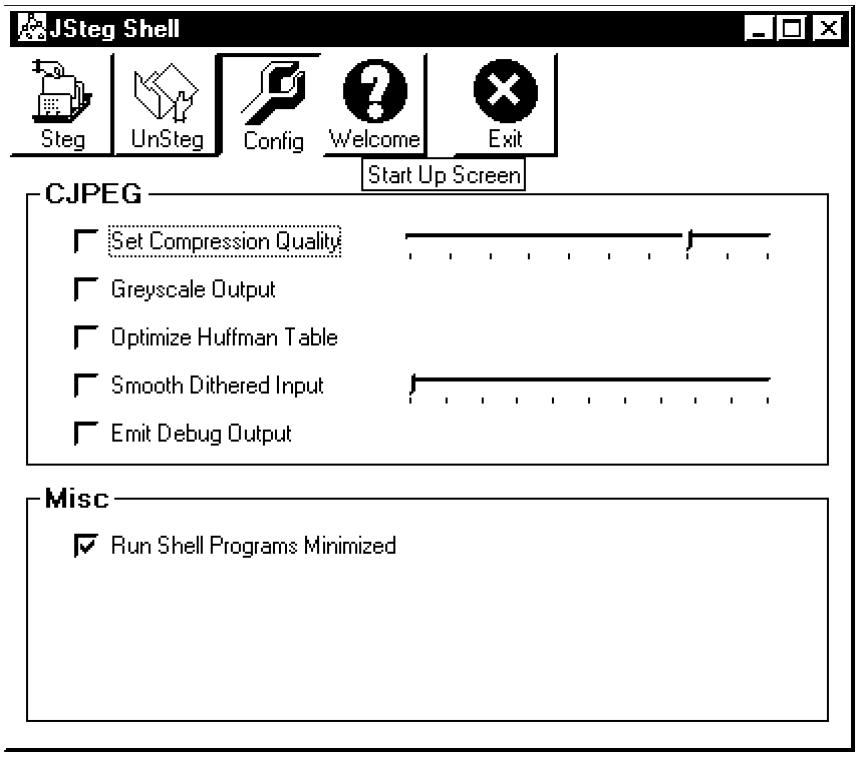
Русский текст нормально отображаться не будет.

Если информация не простой текст, она будет отображаться в шестнадцатеричном формате.



Нажатие кнопки «Save As» в левой нижней части сохранит восстановленную информацию как файл. При щелчке правой клавиши мыши, область текста помещается в буфер обмена.

Конфигурирование JSTEG Shell производится при нажатии кнопки «Config».



Опция «Set Compression Quality» определяет степень сжатия JPG.

Значение по умолчанию - 75.

Опция «Greyscale output» формирует черно-белый JPG.

Опция «Optimize Huffman Table» обеспечивает уменьшение размера JPG файла при том же качестве.

Smooth Dithered Output степень сглаживания резкости изображения.

Опция «Emit Debug Output» обеспечивает выдачу сообщений программой CJPEG.

При установленной опции «Run ShellProgram Minimized» JSTEG (DOS) будет показываться как значок на панели задач.

3. Порядок выполнения работы

Ход работы:

1. Выбрать стеганографическую программу;
2. Определите поддерживаемые форматы файлов контейнеров;
3. Изучите возможность и качество упаковки файлов в файлы разного формата (если формат имеет несколько разновидностей, как например bmp, то для всех возможных вариантов);
4. Определите плотность упаковки скрываемой информации в разные типы контейнеров;
5. Приведите в отчете исходные файлы контейнеров и контейнеры с упакованной информацией;
6. Оцените изменение размеров файлов контейнеров после их наполнения в случае использования и не использования шифрования.

4. Требования к отчету

Отчет должен оформляться в текстовом редакторе Word на листах формата А4 в соответствии с требованиями ЕСКД и содержать полученные результаты и выводы. В отчете должны быть рассмотрены использованные в изученных программах алгоритмы и способы упаковки, приведены контейнеры до и после сокрытия в них информации, отражены достоинства и недостатки программ стеганографии.

5. Контрольные вопросы

1. Что такое стеганография?
2. Каковы базовые принципы компьютерной стеганографии?
3. Что такое скрывающие биты?

4. Что такое суррогатная стеганография?
5. Что такое селектирующая стеганография?
6. Что такое конструирующая стеганография? Ее достоинства и недостатки.
7. Что такое контейнер?
8. Каковы особенности потоковых контейнеров?
9. Что такое контейнеры случайного доступа? Каковы их достоинства и недостатки?
10. Какие из рассмотренных Вами программ обеспечивают дополнительное шифрование скрываемой информации? Какие используются алгоритмы шифрования?
11. Какие форматы файлов контейнеров поддерживают рассмотренные Вами программы?
12. Какие можно дать рекомендации по выбору контейнера картинки?
13. Какие можно дать рекомендации по выбору звукового файла контейнера?
14. Назовите особенности упаковки информации в файлы формата JPEG.
15. Что такое цифровые водяные знаки?
16. Какие требования предъявляются к водяным знакам?
17. Какие разновидности водяных знаков Вы знаете?
18. Какова плотность упаковки скрываемой информации для различных форматов контейнеров для рассмотренных программ?
19. Какие из рассмотренных вами программ обеспечивают сжатие упаковываемой информации?
20. Изменяются ли размеры файлов контейнеров разных типов после скрытия в них информации?
21. Какие алгоритмы и способы упаковки используются в рассмотренных вами программах?
22. Каковы достоинства и недостатки рассмотренных программ?
23. Как происходит сокрытие информации в текстовых и html файлах?
24. Какие стеганографические программы поддерживают подобную возможность?

6. Список литературы