МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра защиты информации и систем связи

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
«__» _____ 2015 г.

СТЕГАНОГРАФИЧЕСКИЕ СИСТЕМЫ СКРЫТИЯ ДАННЫХ. ИЗУЧЕНИЕ ПРОГРАММНЫХ ПРОДУКТОВ MASKER И S-TOOLS

Методические указания по выполнению лабораторной работы
по дисциплине «Криптографические методы защиты информации»
для студентов специальностей 10.05.03, 10.05.02, 10.03.01

Курск 2015

УДК 004.056 (076.5)

Составитель: М.А. Ефремов, А.Л. Ханис

Рецензент
Кандидат технических наук, доцент *И.В. Калуцкий*

Стеганографические системы скрытия данных. Изучение программных продуктов masker и s-tools: методические указания по выполнению лабораторной работы по дисциплине «Криптографические методы защиты информации» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов, А.Л. Ханис. Курск, 2015. 18 с.: ил. 14. Библиогр.: с. 18.

Содержат сведения о применении стеганографических систем скрытия данных. Рассматриваются основные этапы по настройке и установке программных продуктов Masker и S-Tools. Указывается порядок выполнения лабораторной работы, правила оформления и содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по образованию в области информационной безопасности (УМО ИБ).

Предназначены для студентов специальностей 10.05.03, 10.05.02, 10.03.01 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. . Уч.-изд.л. . Тираж 30 экз. Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

1. ЦЕЛЬ РАБОТЫ

Цель лабораторной работы - ознакомление с работой стеганографического скрытия информации на примере программных продуктов Masker и S-Tools.

2. ЗАДАНИЕ

Изучить теоретический материал. Установить программы, настроить требуемые параметры, изучить применение программных продуктов в области криптографической защиты информации. Скрыть информацию с помощью программ Masker и S-Tools. Восстановить исходную информацию.

3. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Получить задание.
2. Изучить теоретическую часть.
3. Произвести установку программы Masker.
4. Скрыть исходную информацию с помощью программы Masker.
5. Скрыть информацию с помощью программы S-Tools.
6. Восстановить исходную информацию.
7. Составить отчет.

4. СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист.
2. Краткая теория.
3. Описание процесса выполнения работы со скриншотами.
4. Вывод.

5. ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

5.1. Введение

Задача надежной защиты информации от несанкционированного доступа является одной из древнейших и не решенных до настоящего времени проблем. Способы и методы скрытия секретных сообщений известны с давних времен. Стеганография – с греческого steganos (секрет, тайна) и graphy (запись), буквально “тайнопись”.

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.

Когда 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.

В дальнейшем для защиты информации стали использоваться более эффективные методы кодирования и криптографии. От криптографии стеганография отличается тем, что с помощью криптографии можно скрыть содержание сообщения, а, пользуясь стеганографией, можно скрыть само существование сообщения.

5.2. Компьютерная стеганография

Компьютерные технологии придали новый импульс развитию и совершенствованию стеганографии, появилось новое направление в области защиты информации – *компьютерная стеганография*.

Компьютерная стеганография – это сокрытие сообщения или файла в другом сообщении или файле. Например, стеганографы могут спрятать аудио- или видеофайл в другом информационном или даже в большом графическом файле.

Процесс стеганографии можно разделить на несколько этапов.

1. Выбор информационного файла.

Первым этапом в процессе стеганографии является выбор файла, который необходимо скрыть. Его ещё называют информационным файлом.

2. Выбор файла-контейнера.

Вторым этапом в процессе стеганографии является выбор файла, используемый для сокрытия информации. Его ещё называют файлом-контейнером. В большинстве известных программ по стеганографии говорится, что для сокрытия информации, объём памяти файла-контейнера должен где-то не меньше чем в восемь раз превышать объём памяти информационного файла. Следовательно, чтобы спрятать файл размером 710КБ, понадобится файл объёмом не меньше чем 5600КБ.

3. Выбор стеганографической программы.

Третьим этапом в процессе стеганографии является выбор стеганографической программы.

Один из лучших и самых распространенных продуктов в этой области для платформы Windows – это S-Tools (имеет статус freeware). Программа позволяет прятать любые файлы как в изображениях формата gif и bmp, так и в аудиофайлах 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 (времена которого прошли), тройной DES или IDEA – два последних на сегодня вполне заслуживают доверия.

Программа S-Tools прячет информацию в графических файлах форматов BMP и GIF, а также в звуковых файлах формата WAV. Внешне работа с программой выглядит так. После распаковки архива запускаем файл s-tools.exe, затем Windows

Explorer (Проводник). Последний понадобится, так как S-tools использует технологию drag and drop, соответственно окна не должны полностью перекрываться. Перетаскиваем мышью файл в окно программы S-tools, 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. Перетаскиваем в окно с картинкой, либо уровнем сигнала любой файл, предназначенный для скрытия, размером, не более указанного. После проверки размера данных программа запросит пароль, набрав который можно будет восстановить информацию. Затем начнется скрытие, время которого зависит от размера данных (наблюдать за процессом можно в окне Action). Когда все будет готово, появится окно Hidden data. Сохранить результат можно, щелкнув в окне правой кнопкой мыши и выбрав пункт "Save as...", введя имя файла и нажав ОК. Для восстановления послания необходимо перетащить картинку либо звук в окно S-tools, щелкнуть на изображении правой кнопкой и выбрать пункт "Reveal...". После ввода пароля, если спрятанные данные есть, начнется их восстановление, за процессом которого можно наблюдать в окне Action, либо если данных нет, то ничего и не произойдет.

Другая распространенная стеганографическая программа – Masker – программа для защиты любых объёмов данных, использующая стеганографию – скрытие зашифрованных данных во внешне безобидных файлах-носителях: графических (bmp, gif, jpg, tif), музыкальных (wav, mid, snd, mp3), видео (avi, mov, mpg). При этом файлы-носители, в которых прячутся зашифрованные сведения, остаются полностью функциональны. Например, картинка, в которой спрятаны конфиденциальные сведения, при просмотре будет ничем не отличаться от такой же, но без внедренных в нее зашифрованных данных, разве что размером – она будет побольше.

Зашифрованные таким способом данные можно не только хранить на своем компьютере, но и пересылать в виде приложения к письму – даже в случае его перехвата в нем будет обнаружена всего-навсего, к примеру, картинка с красивым пейзажем.

4. Кодирование файла.

После того, как выбран информационный файл, файл-контейнер и программное обеспечение по стеганографии, необходимо установить защиту нового файла по паролю.

5. Отправление сокрытого сообщения по электронной почте и его декодирование.

Пятым и последним этапом в процессе стеганографии является отправление спрятанного файла по электронной почте и его последующая расшифровка.

После краткой технической характеристики использования методов компьютерной стеганографии возникает вопрос: насколько лёгким или сложным является этот процесс? Степень лёгкости и сложности этого процесса попытались проанализировать в Центре исследования проблем компьютерной преступности и представили свои соображения по этому поводу.

В Интернете можно найти большое количество платных и бесплатных стеганографических программ. Фактический процесс по сокрытию одного файла в другом относительно лёгкий. Сжатие видео, увеличение графического изображения, анализ программ по стеганографии – под силу даже неподготовленному пользователю.

К сожалению, методы компьютерной стеганографии уже используются в преступных целях. В то время как стеганография может помочь в решении проблем защиты конфиденциальной информации. Анализ тенденций развития компьютерной стеганографии показывает, что в ближайшие годы интерес к развитию ее методов будет усиливаться все больше и больше. Предпосылки к этому уже сформировались сегодня. В частности, общеизвестно, что актуальность проблемы информационной безопасности постоянно растет и стимулирует поиск новых методов защиты информации. С другой стороны, бурное развитие информационных технологий обеспечивает возможность реализации этих новых методов защиты. И конечно, сильным катализатором этого процесса является лавинообразное развитие Internet, в том числе, такие нерешенные противоречивые проблемы Internet, как защита авторского права, защита прав на личную тайну, организация электронной торговли, компьютерная преступность и кибертерроризм.

5.3. Установка программы

Запустим исполняемый файл msksetup.exe. Появится окно приветствия (рис.1). Нажимаем кнопку Next.

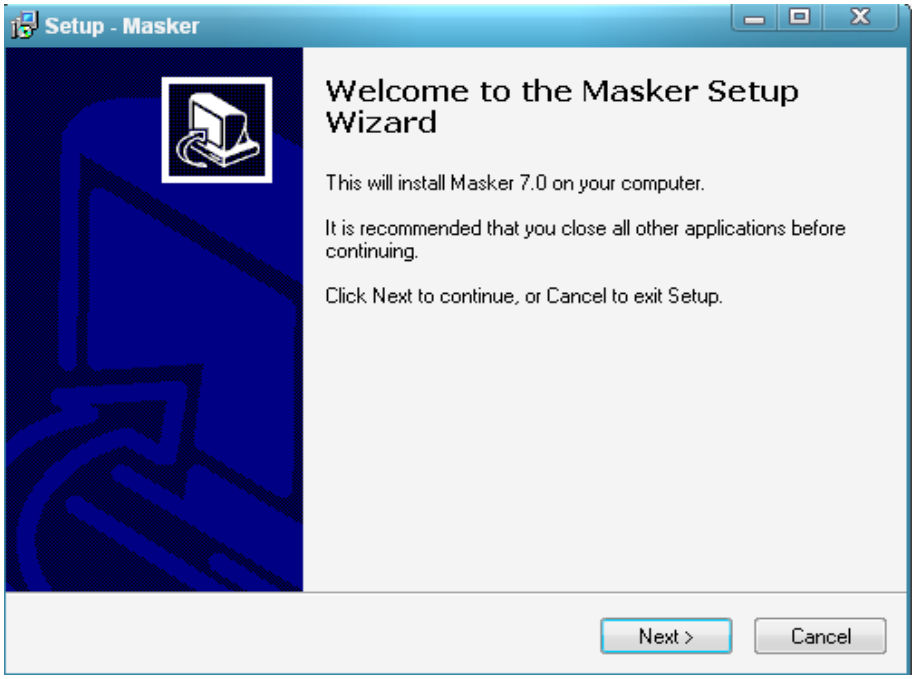

Рисунок 1 – Окно приветствия программы

Затем принимаем лицензионное соглашение (рис.2).

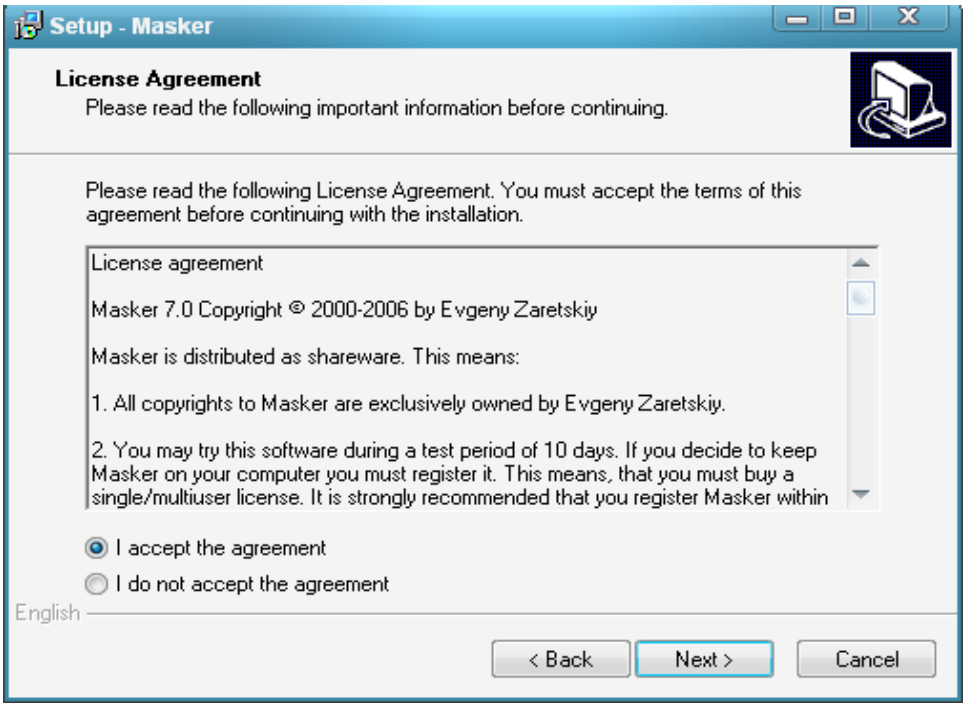

Рисунок 2 – Принимаем лицензионное сообщение

Выбираем директорию, в которую следует установить программу (рис. 3).

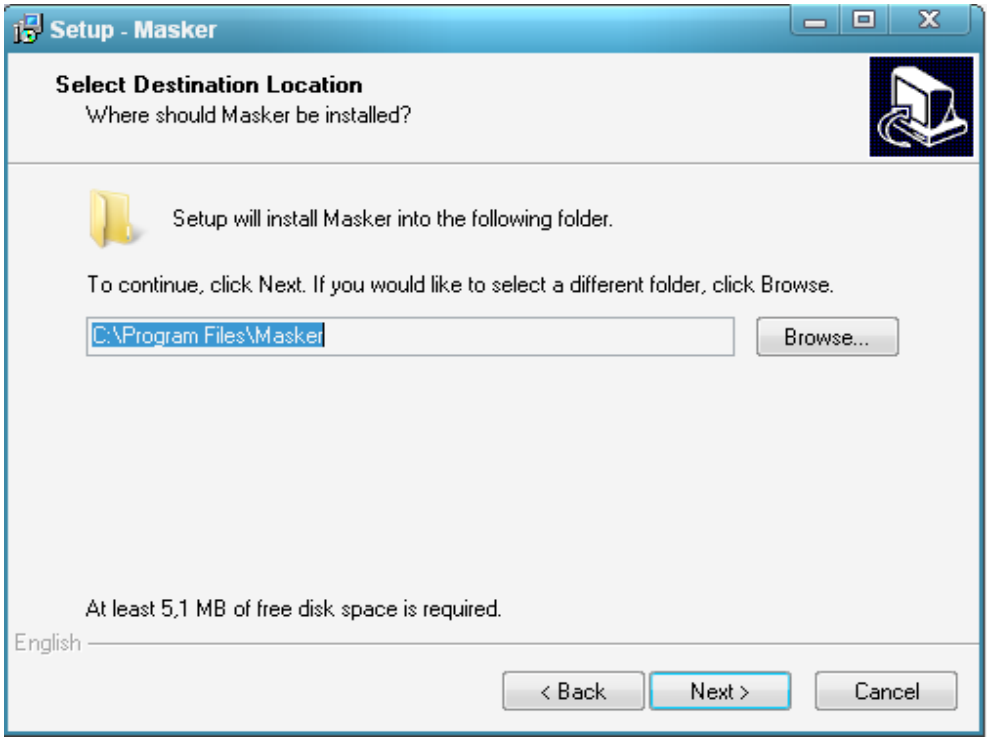

Рисунок 3 – Выбор директории

Для завершения установки программы требуется нажать кнопку Next. Данная программа будет установлена по выбранному адресу. Далее приступаем к непосредственной работе с программой Masker.

6. ВЫПОЛНЕНИЕ РАБОТЫ

6.1. Скрытие информации с помощью программы Masker

Чтобы начать работать, нужно либо на панели, либо в меню выбрать пункт "Open Carrier File", и в появившемся окне указать файл-контейнер (рис.4).

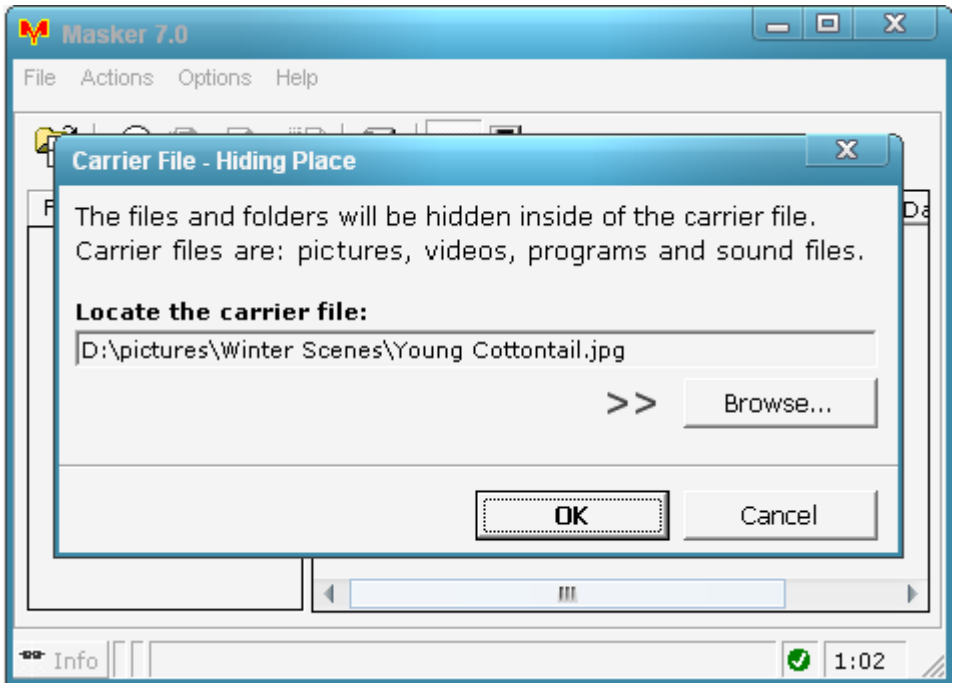

Рисунок 4 – Выбор файла-контейнера

После этого нужно в следующем окне перейти на "Create New Hideout", где можно указать пароль и алгоритм шифрования для новой порции скрываемых данных (рис. 5). Шифрование – один из "коньков" программы: поддерживаются 7 алгоритмов, среди которых есть BLOWFISH и TripleDES.

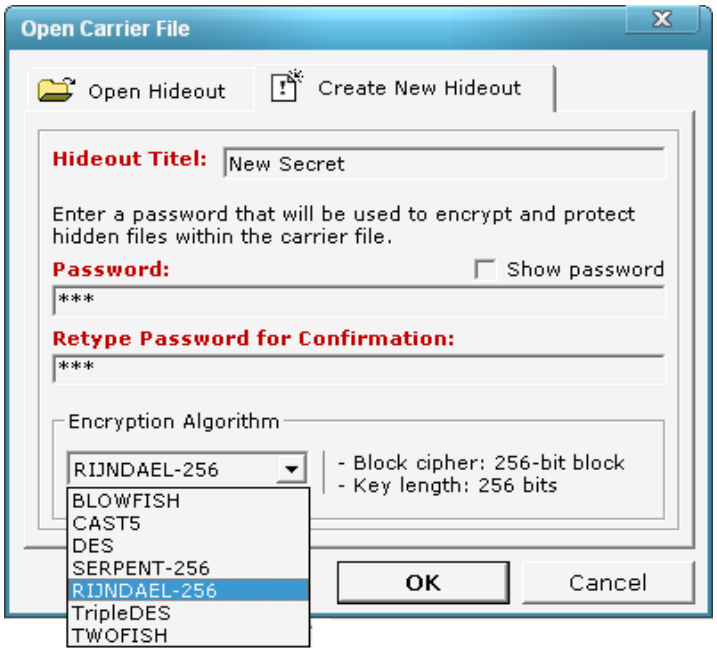

Рисунок 5 – Выбор пароля и алгоритма шифрования

После указания всех параметров в основной части окна будут отображаться скрытые файлы. Чтобы добавить туда файлы, нужно щёлкнуть правой кнопкой и выбрать "Hide/Add Files". Появится окно, в котором нужно будет выбрать эти файлы, а затем и указать параметры их сохранения (рис. 6). Например, можно добавить целую папку, сохранив её структуру, или дать файлу-контейнеру статус "read-only", чтобы сохранить скрытые файлы более надёжно.

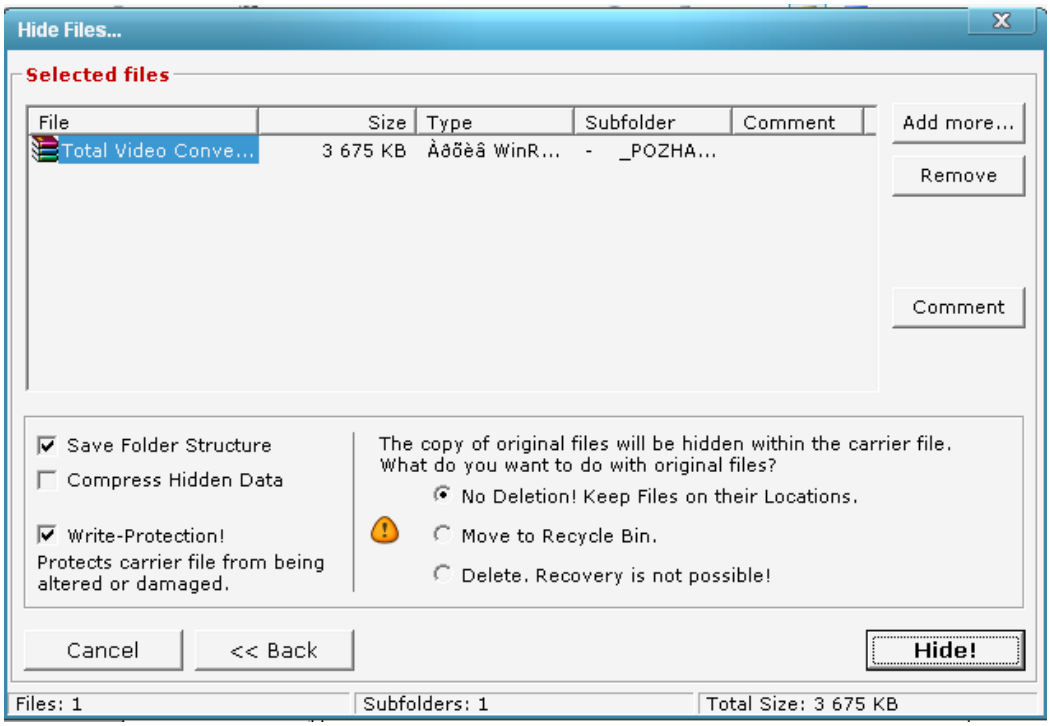

Рисунок 6 – Добавление файлов

6.2. Восстановление информации

Извлечение файлов не вызовет затруднений – при открытии файла-контейнера нужно зайти на вкладку "Open Hideout", указать пароль (рис. 7), и перед вами появится список спрятанных файлов.

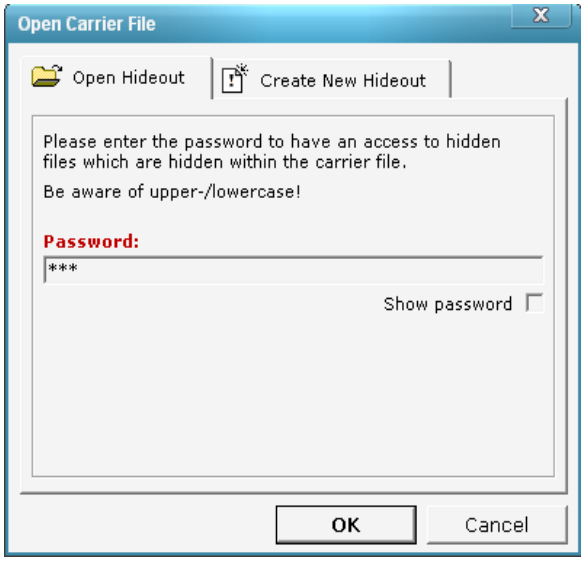

Рисунок 7 – Ввод пароля

Извлеченные файлы можно сохранить, выбрав «Extract» в контекстном меню извлеченного файла.

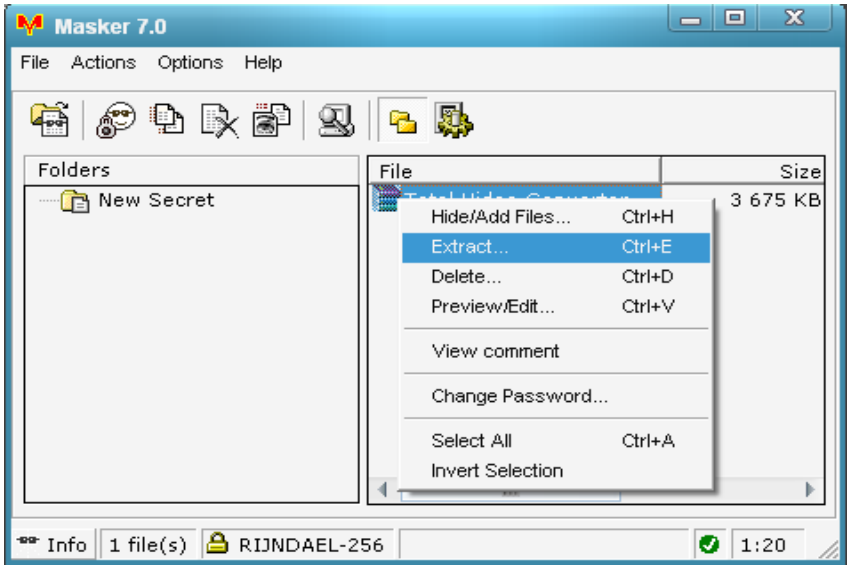

Рисунок 8 – Сохранение извлеченного файла

Объем файла-контейнера увеличился: до скрытия информации его размер составлял 270 Кб, а после – 4,01 Мб.

6.3. Скрытие информации с помощью программы S-Tools

Спрячем текстовый документ «Скороговорки.doc» и графический «Птичка.jpg» в музыкальном файле «September-Cry for you.wav». Нужно запустить файл S-Tools.exe и перетащить мышкой в окно программы файл-контейнер «September-Cry for you.wav» (рис. 10).

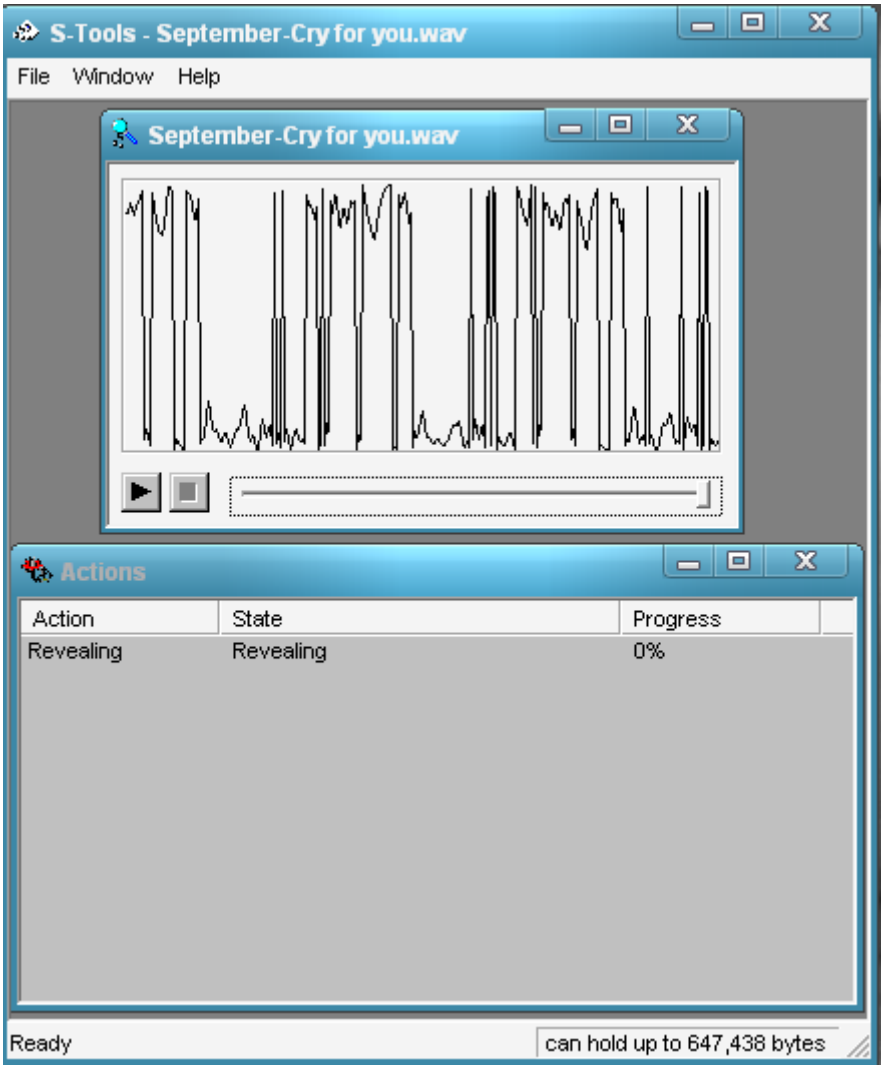

Рисунок 9 – Выбор файла-контейнера

Далее в файл-контейнер перетащить мышкой то, что мы хотим спрятать («Скороговорки.doc», «Птичка.jpg»). Появится окно «Hiding» («скрытие»), в котором нужно ввести пароль и выбрать алгоритм шифрования. Нажать кнопку OK (Рис. 11).

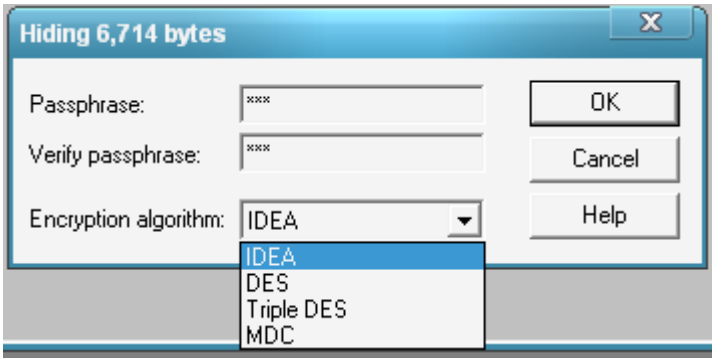

Рисунок 10 – Ввод пароля и выбор алгоритма шифрования

В главном окне программы откроется файл-контейнер с содержимым – фалом, который мы спрятали. Заполненный файл-контейнер нужно сохранить, выбрав «Save as» в его контекстном меню (рис. 12).

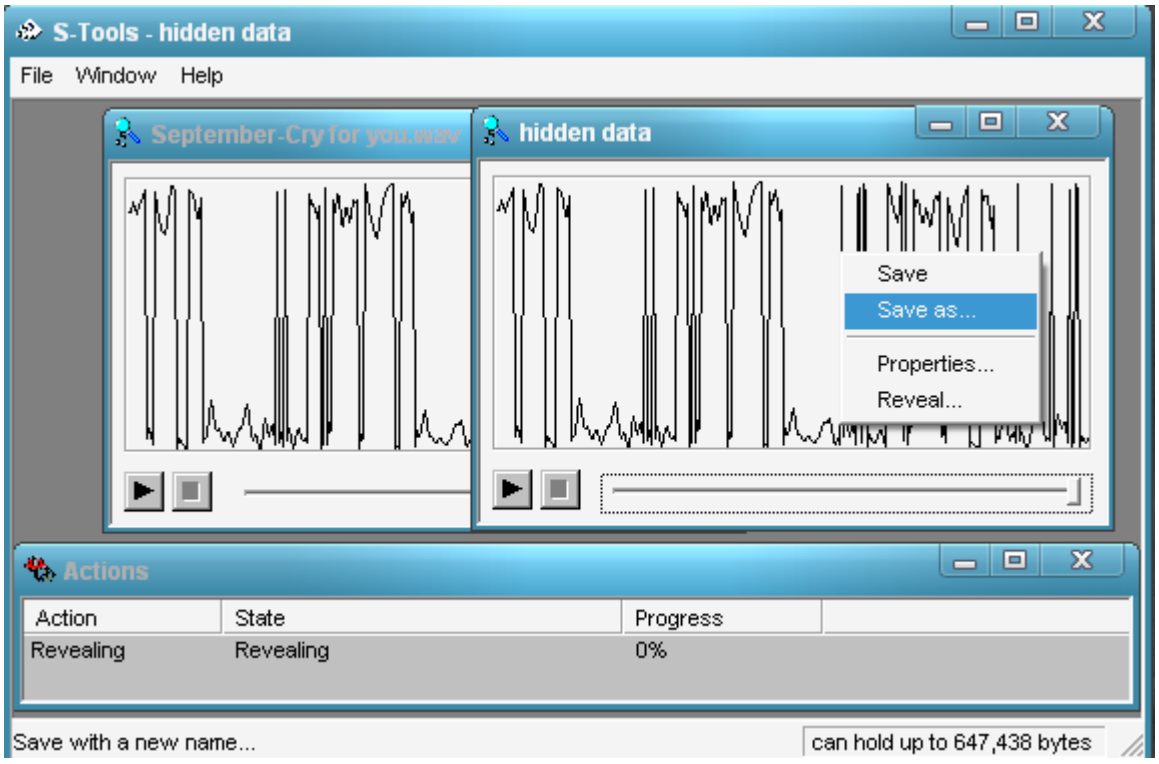

Рисунок 11 – Сохранение файла-контейнера

6.4. Восстановление исходной информации

Чтобы извлечь скрытую информацию из файл-контейнера «шифр-September-Cry for you.wav» теперь перетащим мышкой последний в окно программы и выберем в контекстном меню «Reveal» («обнаружение») (рис. 13).

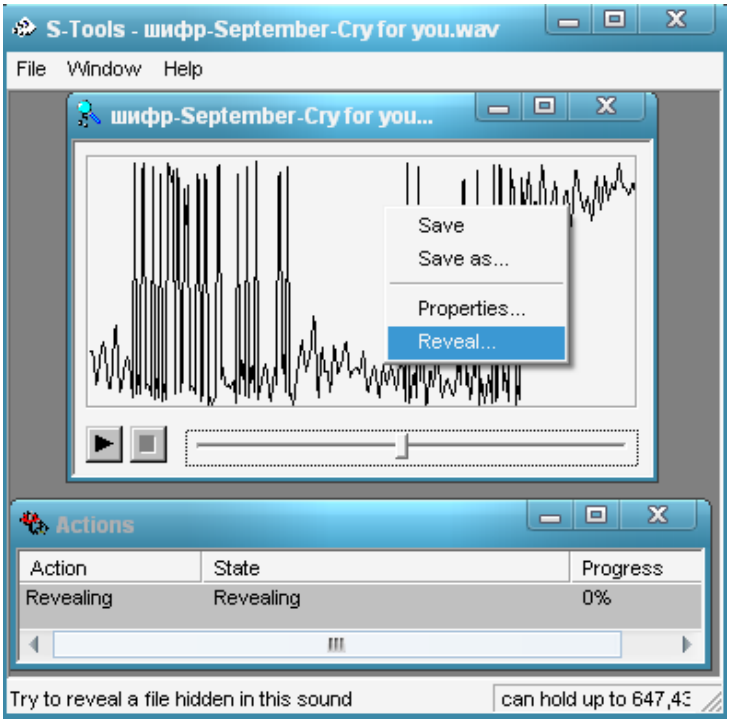

Рисунок 12 – Извлечение скрытой информации

Появится окно «Revealing from шифр-September-Cry for you.wav», в котором нужно ввести пароль для расшифровки файла и выбрать алгоритм, которым этот файл был зашифрован (рис. 14).

Рисунок 13 – Ввод пароля и выбор алгоритма

В окне «Revealed Ar…» («Обнаруженные файлы») отобразятся спрятанные в файл-контейнере файлы и их размеры (рис. 14).

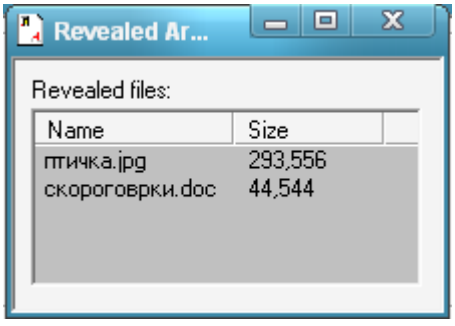

Рисунок 14 – Отображение скрытых файлов

7. КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что такое стеганография?
2. Что такое компьютерная стеганография?
3. Какие виды компьютерной стеганографии вы знаете?
4. Что такое файл-контейнер?
5. Какие файлы можно скрывать с помощью компьютерной стеганографии?
6. Какие программные продукты для реализации методов стеганографии вы знаете?
7. С какими файлами работает программа S-Tools? Назовите преимущества и недостатки программы.
8. С какими файлами работает программа Masker 7.0? Назовите преимущества и недостатки программы.

8. СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

1. Компьютерная стеганография [Электронный ресурс] http://www.crime-research.ru/

2. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века. [Электронный ресурс] http://www.bnti.ru/