ЛАБОРАТОРНАЯ РАБОТА № 7

Тема: Изучение базовых принципов стеганографии.

1. ЗАДАНИЕ К ЛАБАРОТОРНОЙ РАБОТЕ

1.1 Скрыть сообщение различными стеганографическими способами (способ выбирается самостоятельно). В отчете описать алгоритм сокрытия текста.

1.2 В соответствии со своим вариантом скрыть и извлечь заданный текст с помощью программы S-Tools. Контейнеры-оригиналы следует выбрать из выданной папки в соответствии со своим вариантом. Текст рекомендуется набирать в текстовом редакторе Notepad (Блокнот) или MS Word. Пароль и метод шифрования нужно выбрать самостоятельно. Зашифрованный файл (начиненный контейнер) следует сохранить в собственной папке. В отчете необходимо привести максимально допустимый объем скрываемой информации в данном звуковом файле, описать порядок сокрытия и извлечения текстового файла в звуковом контейнере (с скриншотами) с помощью программы S-Tools, а также указать выбранный алгоритм шифрования и пароль.

1.3 Скрыть и извлечь в графическом файле заданный текст с помощью программы Invisible Secrets-4. Текст рекомендуется набирать в текстовом редакторе MS Word. Формат файла контейнера, алгоритм шифрования и пароль выбрать самостоятельно. В отчете описать порядок сокрытия и извлечения текстового файла, а также указать выбранный алгоритм шифрования и пароль.

1.4 С помощью программ Watermark Software, FastStone Image Viewer 4.6. встройте ЦВЗ в произвольно выбранное сообщение. ЦВЗ должен содержать ФИО. В отчете необходимо описать порядок встраивания ЦВЗ (в виде скриншотов с пояснениями) в изображение при помощи этих программ.

1.5 Добавьте в отчет о практической работе водяной знак в виде своей фамилии и номера группы.

1. ПРАКТИЧЕСКАЯ ЧАСТЬ

2.1 Шифрование методом DarkJPEG

Данный метод базируется на известном LSB, в котором младшие разряды значений цветовой палитры заменяются на информационные. Недостатком такого метода является сопутствующая простоте в реализации низкая стойкость. Обнаружить такой вид стега достаточно просто, достаточно склеить необходимые биты и сообщение будет восстановлено.

Для устранения этого недостатка прибегнем к шифрованию AES-256 скрываемого содержимого. Для того, что бы использовать пароли любой длины воспользуемся хеш-функцией SHA3, результатом которой является 256 бит хеша. А для усложнения раскрытия пароля добавим к нему случайно сгенерированную соль перед получением хеша. Эту соль в дальнейшем мы запишем в начале нашего сообщения.

Сообщение в такой стегосистеме представляет собой последовательно идущие заголовок и содержимое прикрепляемого файла. В заголовке содержатся имя и размер вкладываемого файла. В качестве маркера конца сообщения воспользуемся значением 0xFFD9, которое является маркером конца JPEG изображения.

Цвета контейнера переводятся из RGB в YCbCr. Над каждым блоком 8х8 пикселей производится дискретное косинусное преобразование, после чего данные записываются в последние 2 бита каждого не нулевого коэффициента. Сами коэффициенты сжимаются с использованием кодирования серией и кодов Хаффмана.

Для работы с системой первым действием необходимо выбрать скрываемый файл или картинку, его содержащую. После этого необходимо выбрать метод скрытия (рисунок 1). Rand следует заменить на image и выбрать картинку-контейнер в предложенном окне. Нажав на знак равно файл будет скрыт в картинке

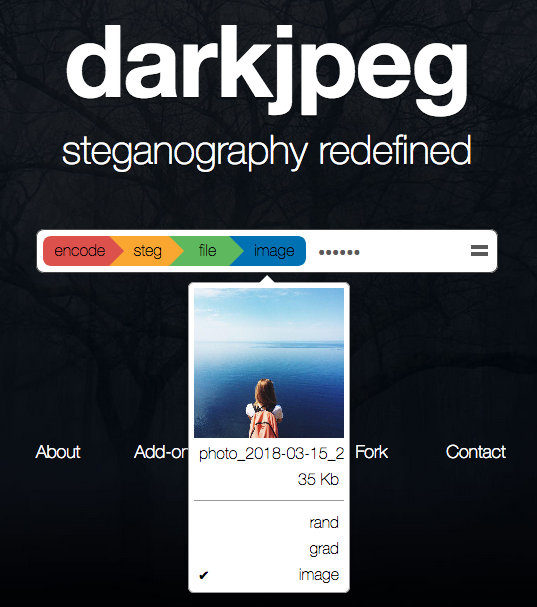


Рисунок 1 – Сокрытие текстового файла в изображении

Для обратного извлечения из контейнера поместим полученное изображение в начальное поле на странице и выберем последовательность шагов decode-steg-file (рисунок 2). Введя пароль и нажав на знак равно получим файл с изначальным названием и содержимым (рисунок 3).

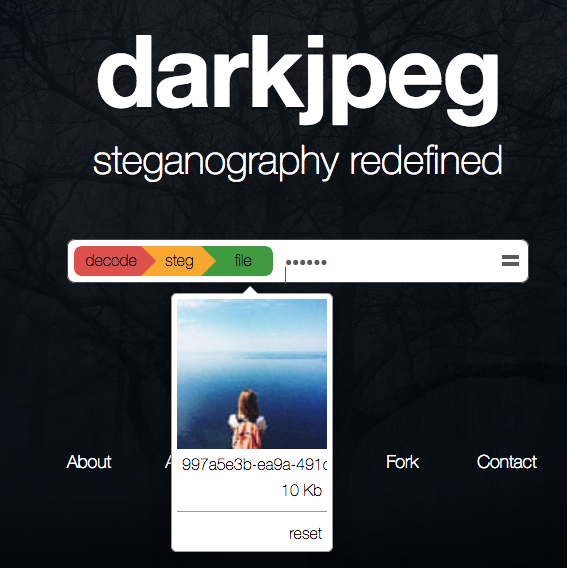


Рисунок 2 – Извлечение сокрытого файла

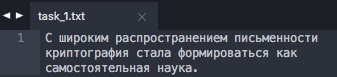


Рисунок 3 – Содержимое сокрытого файла

2.2 Шифрование с помощью программы S-Tools.

Для шифрования информации необходимо, прежде всего, внести файл-контейнер в программное окно. На рисунке 4 видно, что максимально допустимый объем скрываемой информации в этом файле равен 63848 байт.

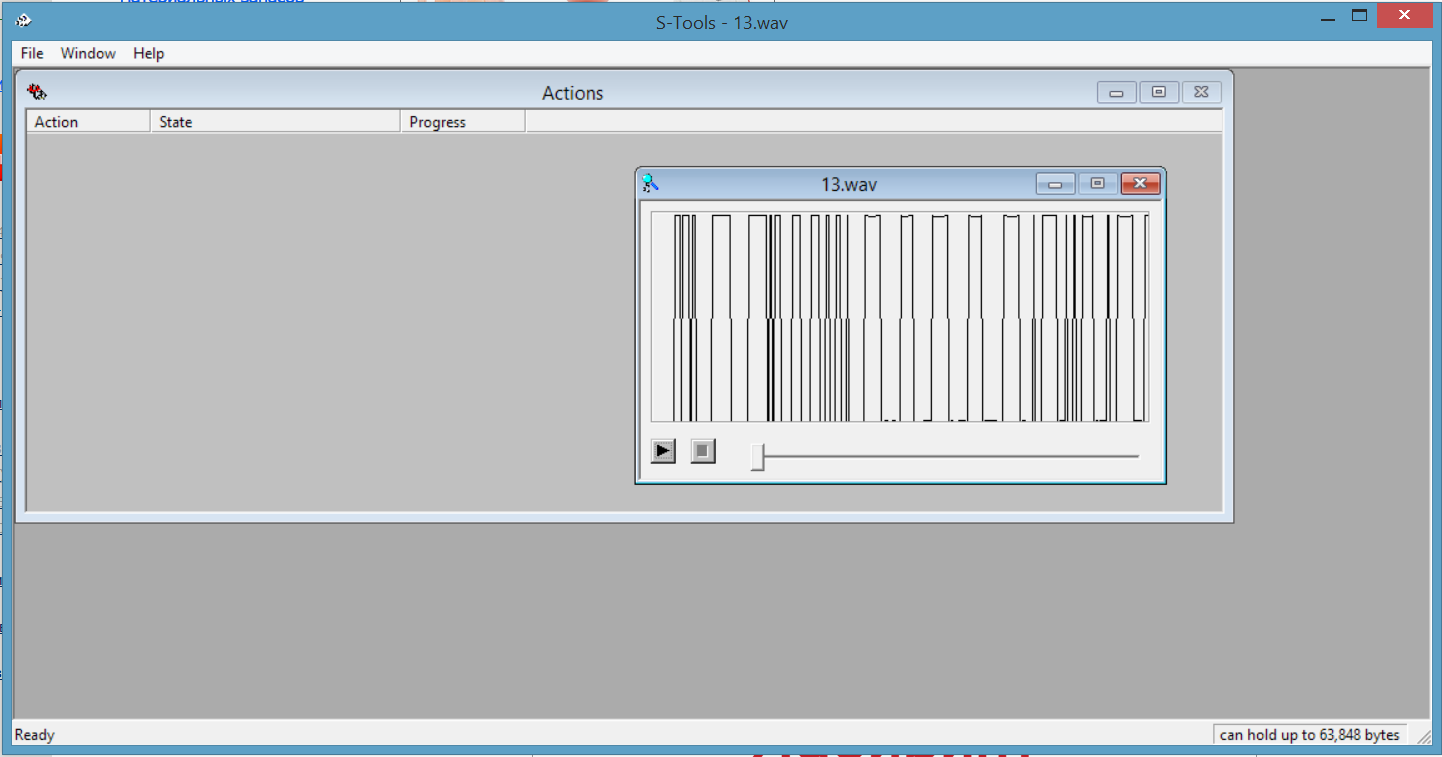


Рисунок 4 – Окно программы S-Tools с файлом-контейнером.

Файл с названием «задание\_2.txt» содержит в себе текст по варианту 13, который будет зашифрован, что отображено на рисунке 5.

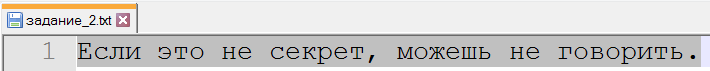


Рисунок 5 – Шифруемое сообщение.

При перетаскивании текстового файла в окно программы появляется окошко для выбора пароля и типа шифрования. Выбранный пароль – 220996, выбранный тип шифрования – DES (рисунок 6).

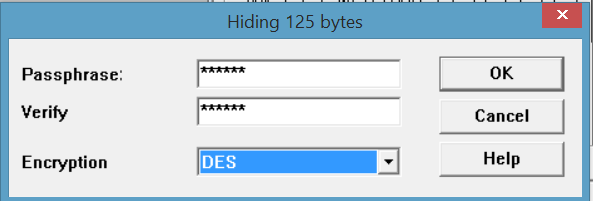


Рисунок 6. – Шифрование сообщения.

Итог – новый аудиофайл, названный “hidden data” (рисунок 7).

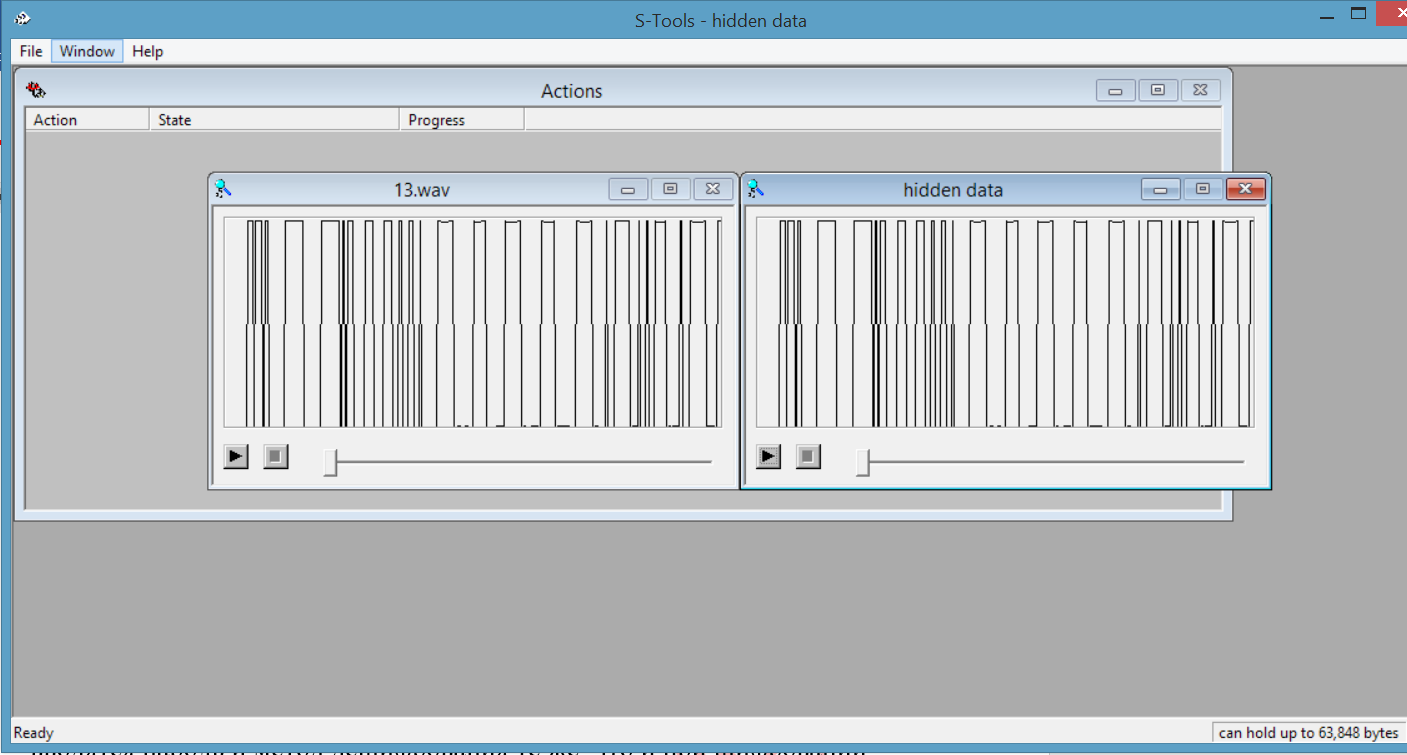


Рисунок 7. – Итог шифрования.

Для дешифрования сообщения щелчком правой кнопки мыши по шифрованному файлу вызывается подпункт «Reveal», в открывшемся окне вводятся пароль и метод дешифрования те же, что и при шифровании.

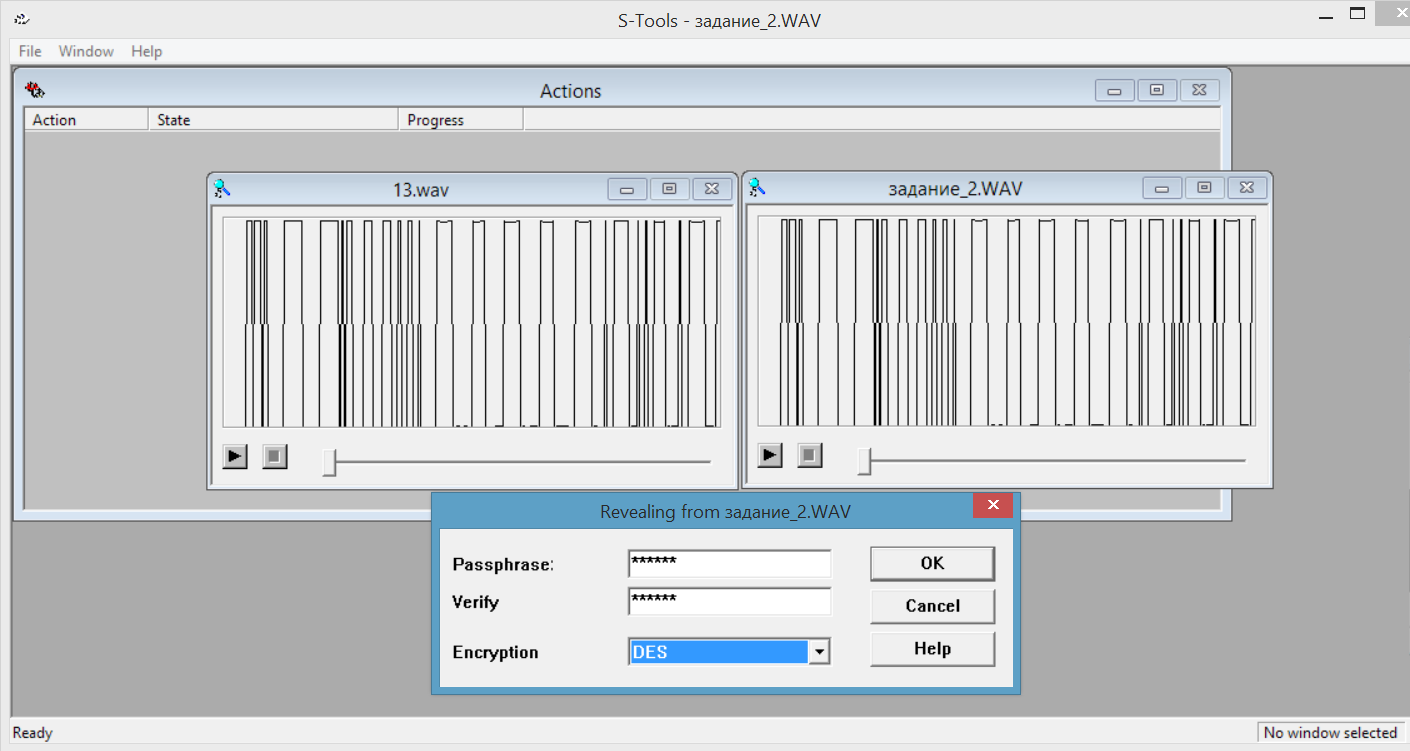


Рисунок 8. – Дешифрование сообщения.

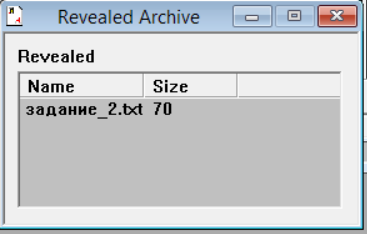


Рисунок 9. – Выделенное сообщение.

2.3 Шифрование сообщения в графическом файле с помощью программы Invisible Secrets 4.

Для шифрования выбирается то же сообщение, что и при шифровании в программе S-Tools, картинка для шифрования показана в рисунке 10.



Рисунок 10. – Картинка для шифрования.

Интерфейс программы показан на рисунке 11. В главном окне программы выбирается подпункт «Hide Files», в открывшемся окне предлагается выбрать файлы для шифрования.

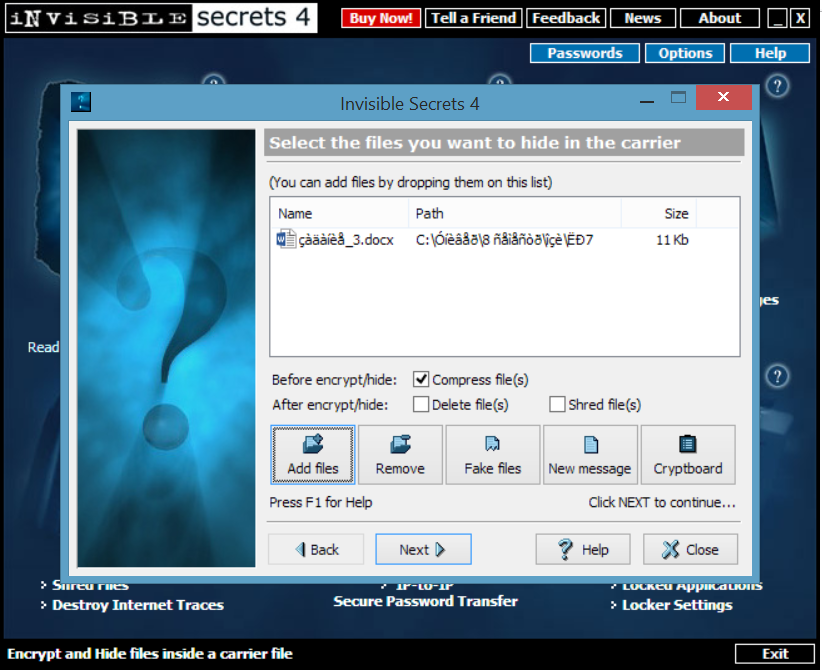


Рисунок 11. – Выбор файлов для шифрования.

Контейнер – картинка формата .jpg, алгоритм шифрования – GOST, пароль – 22099.



Рисунок 12. – Шифрование.

Результат – картинка-контейнер с названием «лаба8.jpg» (рисунок 13).



Рисунок 13. – Контейнеры.

Для дешифрования в главном окне программы выбирается подпункт «Unhide Files», в открывшемся подпункте выбирается файл-контейнер с зашифрованным сообщением (рисунок 14).

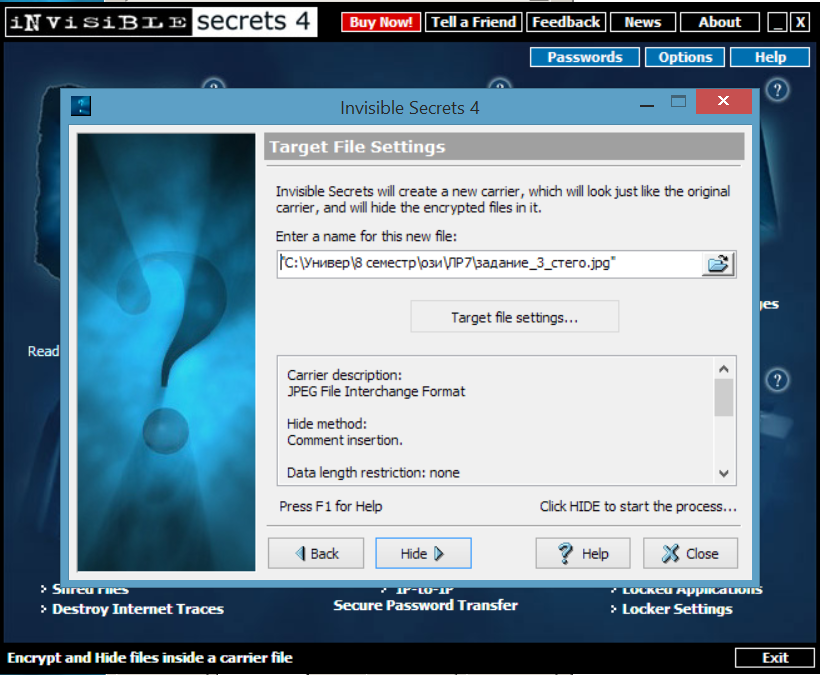


Рисунок 14. – Дешифрование сообщения.

После вводится пароль. Итог – дешифрованное сообщение (рисунок 15).

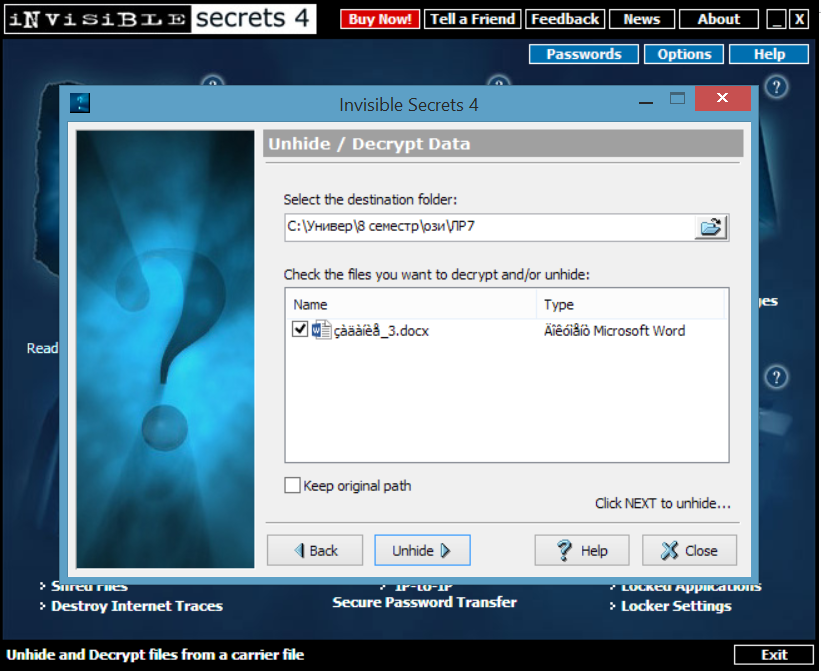


Рисунок 15. – Расшифрованный файл.

2.4 Встраивание ЦВЗ с помощью Watermark Software, FastStone Image Viewer 4.6

В открывшемся окне программы Watermark Software выбирается файл для вставки ЦВЗ.

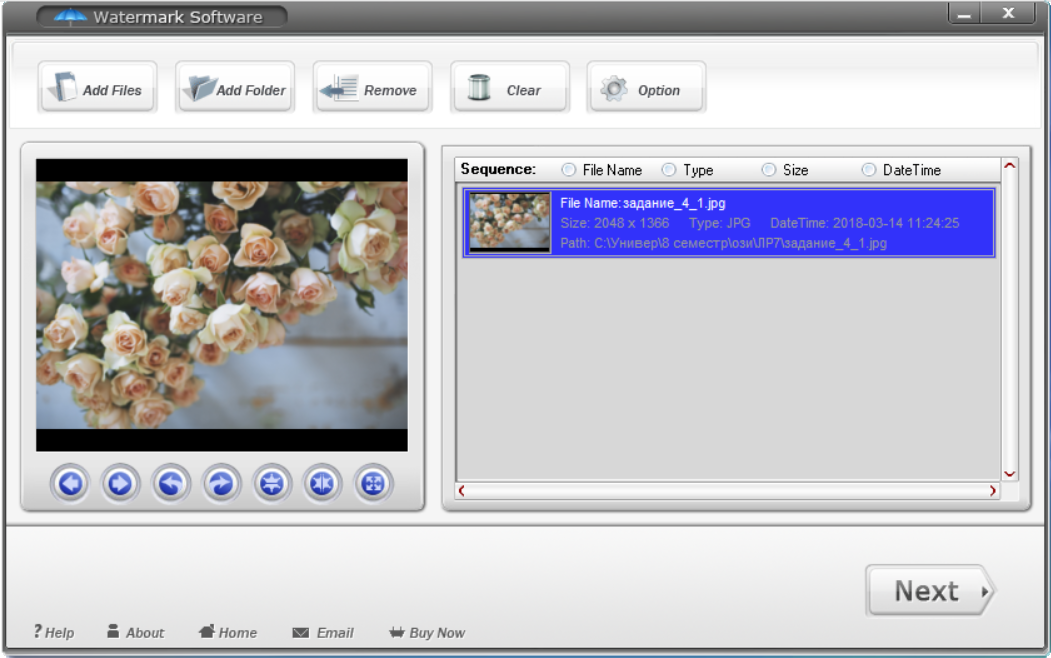


Рисунок 16. – Картинка для вставки ЦВЗ.

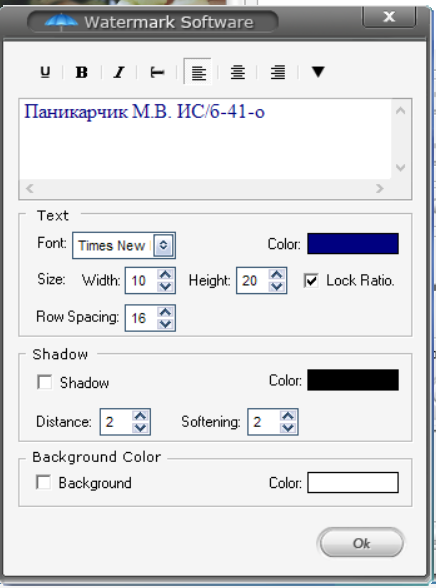


Рисунок 17. – Параметры ЦВЗ.

Итог – на рисунке 18.



Рисунок 18. – Рисунок с ЦВЗ.

В программе FastStone Image Viewer 4.6 выбирается картинка, открывается вкладка «Сервис-Пакетное преобразование/переименование», добавляется файл и выходная папка, во вкладке «Установки» выбирается формат JPEG.

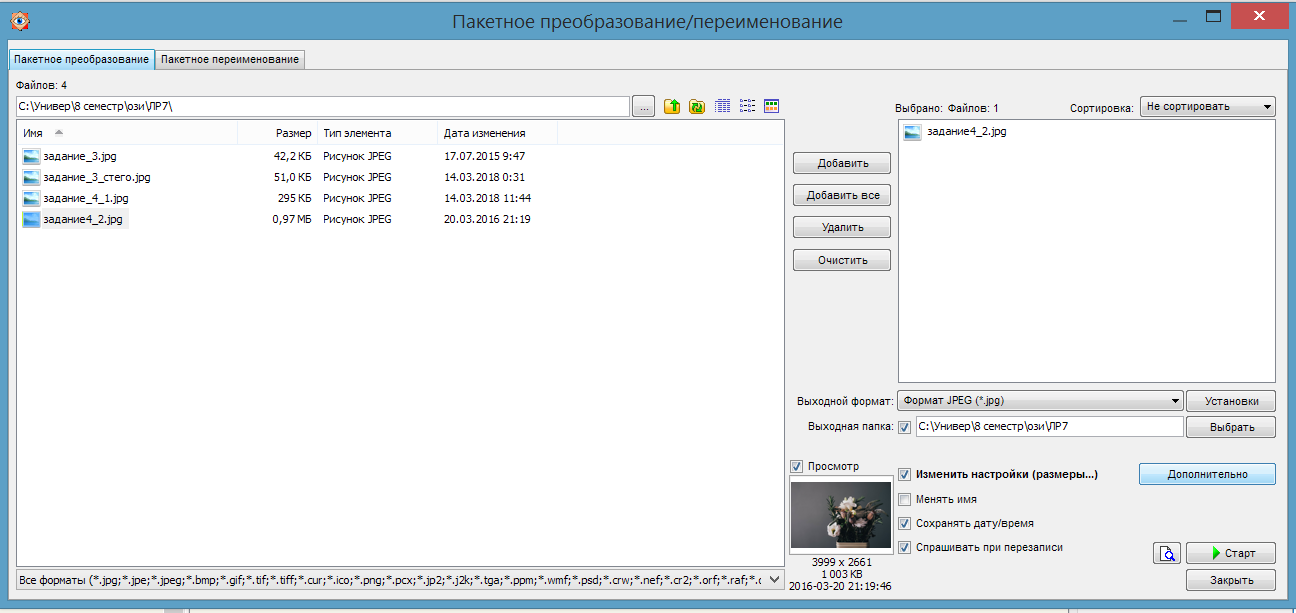


Рисунок 19. – Окно программы.

Для вставки водяного знака при нажатии кнопки «Дополнительно» выбирается вкладка «Текст», ставится галочка на пункте «Добавить текст», вводится некоторый текст и выставляются его параметры.

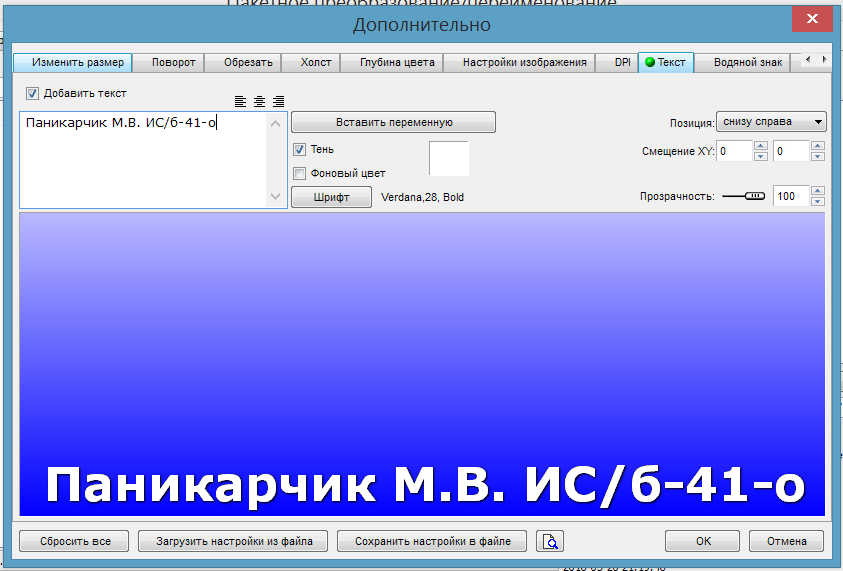


Рисунок 20. – Настройка водяного знака.

После всех преобразований при нажатии кнопки «Старт» производятся преобразования.

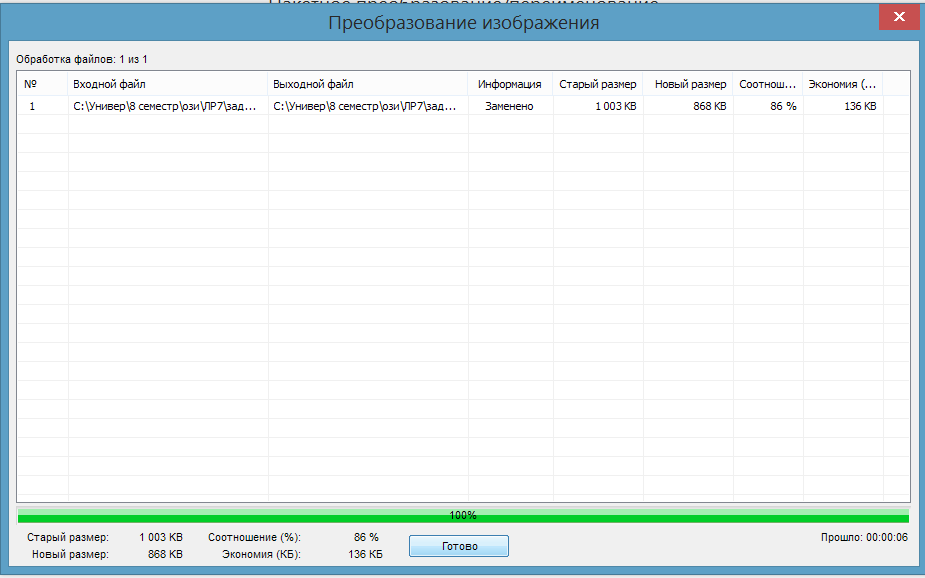


Рисунок 21. – Выполненные преобразования.



Рисунок 22. – Итоговое изображение.

2.5 Вставка ЦВЗ с помощью MS Word.

Во вкладке Дизайн выберем пункт «Подложка-Настраиваемая подложка». Настройки представлены на рисунке 23.

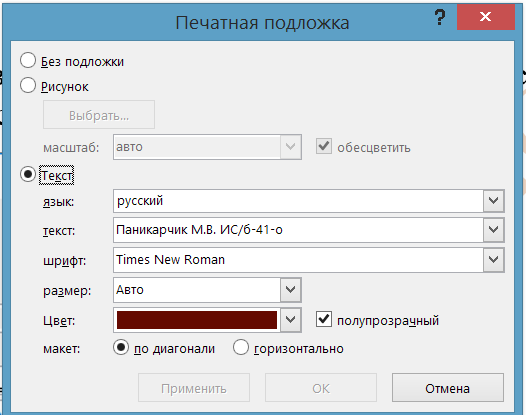


Рисунок 23. – Настройки подложки.

**ВЫВОДЫ**

В ходе проведения лабораторной работы были изучены методы стеганографии, в частности, шифрование сообщений в изображениях, звуковых файлах, без применения специальных программ для шифрования и с ними.