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 перемешивания цветовой карты

Gif-изображение содержит цветовую карту с числом вхождений до 256, что обеспечивает максимальный объем хранимой информации в 1675 бит. Само изображение состоит из сжатого массива индексов на данную цветовую карту. Для сокрытия послания в изображении проделывается следующая последовательность шагов:

1. Сообщение указывается в командной строке либо файле. Опционально его можно сжать и/или зашифровать. Имеется последовательность нулей и единиц.
2. Добавляя спереди 1, получим двоичное число m.
3. Далее взгляните на изображение, в котором вы бы желали сокрыть сообщение. Посчитайте число уникальных цветов и обозначьте его n. Если m > (n!-1), то сообщение слишком велико для скрытия в исходном файле.
4. Цвета сначала сортируются в соответствии с их «естественным» порядком (если не применяется шифрование): каждому цвету в модели RGB присваивается значение (red \*65536 + green\*256 + blue), все дублирующиеся значения удаляются.
5. I изменяется от 1 до n. Каждый цвет (i-1) располагается в позиции (m mod i), после чего m делится на i.
6. Цвет, прежде занимавший позицию, и те, что находятся «выше», сдвигаются на 1 вверх.
7. В том случае, если размер цветовой карты превышает n, она будет «склеена» с последним цветом из исходной карты.
8. Далее изображение распаковывается, индексы изменяются в соответствие с новой цветовой картой, после чего изображение упаковывается вновь. Для файлов с анимацией данная процедура повторяется для каждого кадра.

Выделение спрятанного сообщения сопровождается сходной процедурой, только в обратной последовательности. Упорядочивание цветовой карты используется для конструирования двоичного числа, которое подается на выход после дешифрации и распаковывания.

Система представлена консольной утилитой, параметрами которой являются скрываемый файл или сообщение, исходное изображение и путь для итогового изображения (рисунок 1).



Рисунок 1 – Сокрытие текстового файла в изображении

Для обратного извлечения из контейнера необходимо указать пароль, путь к контейнеру и путь для извлекаемого содержимого (рисунок 2). Содержимое извлечённого файла доступно по указанному пути (рисунок 3).



Рисунок 2 – Извлечение сокрытого файла

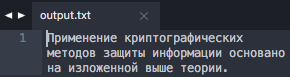


Рисунок 3 – Содержимое сокрытого файла

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 47145 байт.

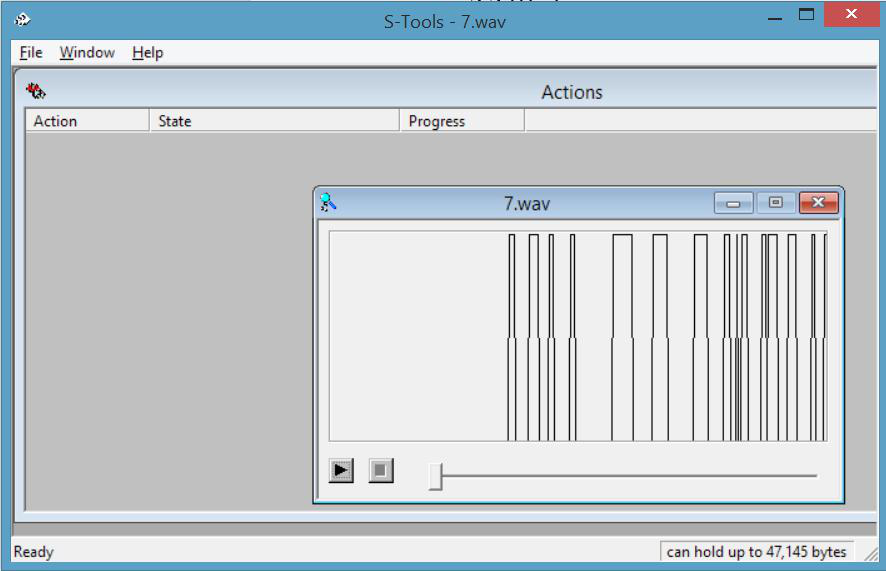


Рисунок 4 – Окно программы S-Tools с файлом-контейнером

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

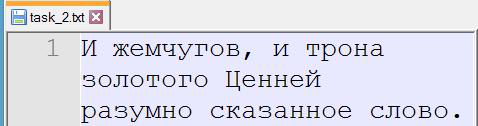


Рисунок 5 – Шифруемое сообщение

При перетаскивании текстового файла в окно программы появляется окошко для выбора пароля и типа шифрования. Выбранный пароль – 061097, выбранный тип шифрования – IDEA (рисунок 6).

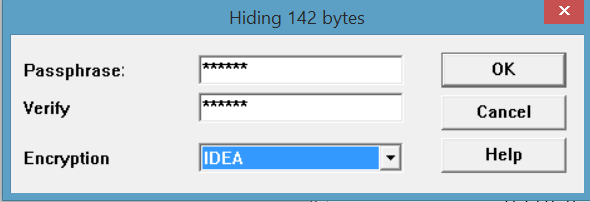


Рисунок 6 – Шифрование сообщения

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

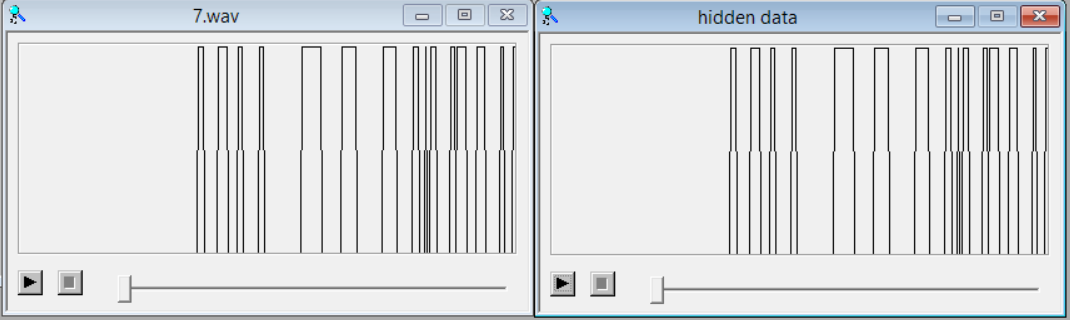


Рисунок 7 – Итог шифрования

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.

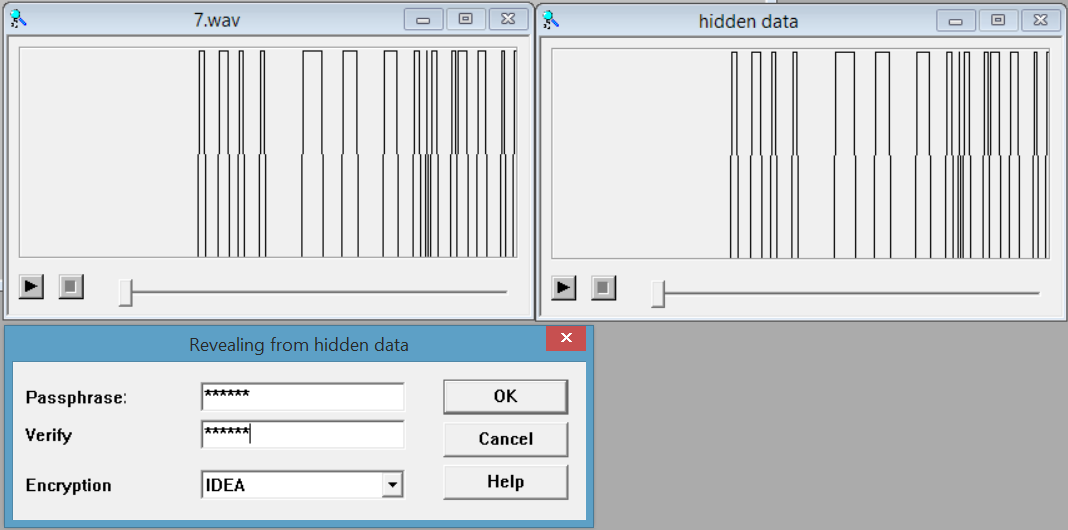


Рисунок 8. – Дешифрование сообщения.

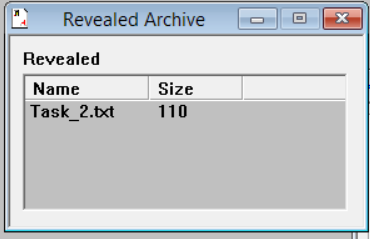


Рисунок 9 – Выделенное сообщение.

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.

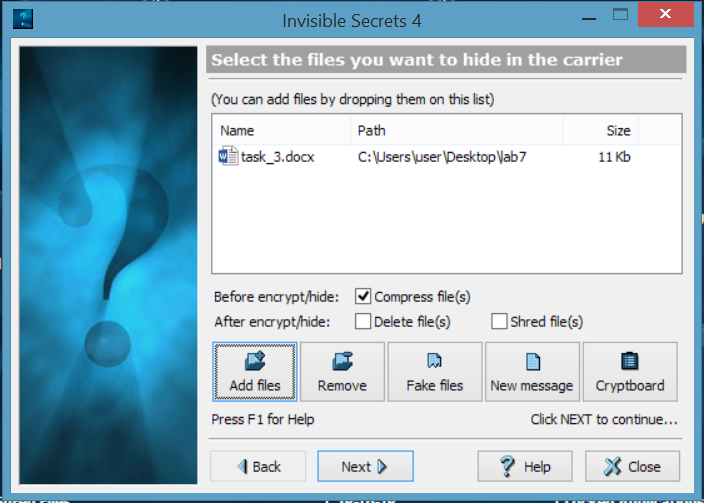


Рисунок 11 – Выбор файлов для шифрования

Контейнер – картинка формата .jpg, алгоритм шифрования – RS4, пароль – 06109.

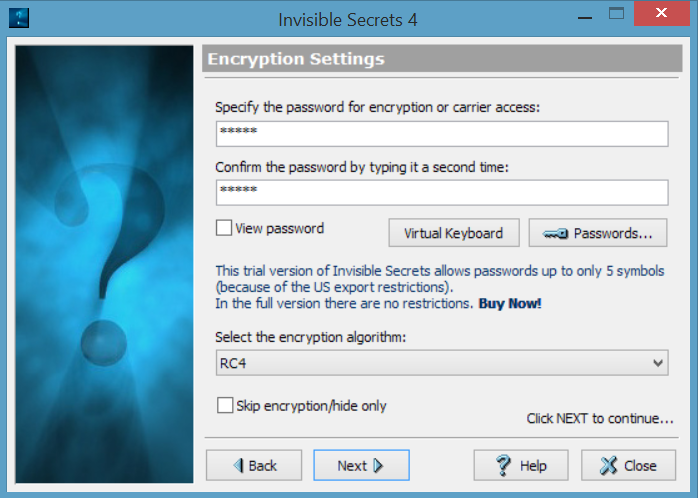


Рисунок 12 – Шифрование

Результат – картинка-контейнер с названием «task\_3\_stego.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).

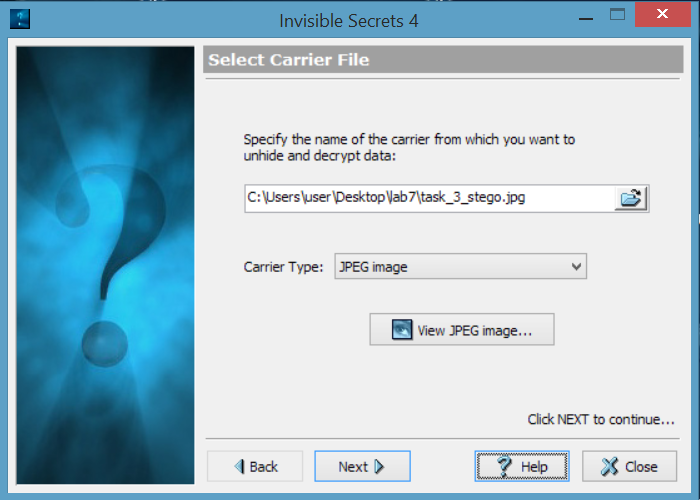


Рисунок 14 – Дешифрование сообщения

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

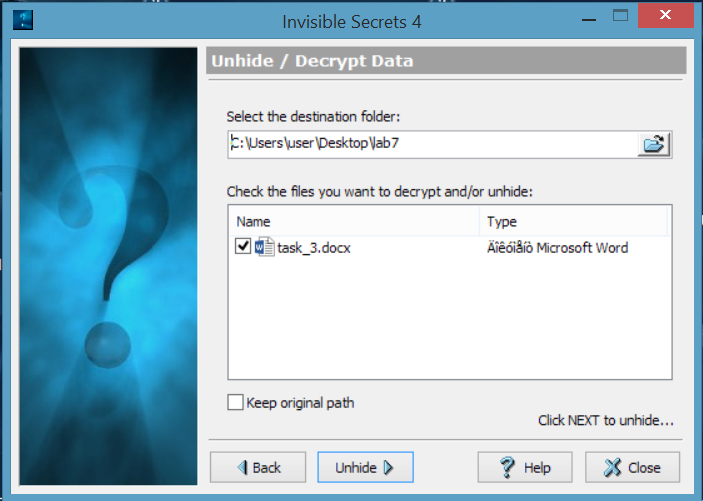


Рисунок 15 – Расшифрованный файл

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

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

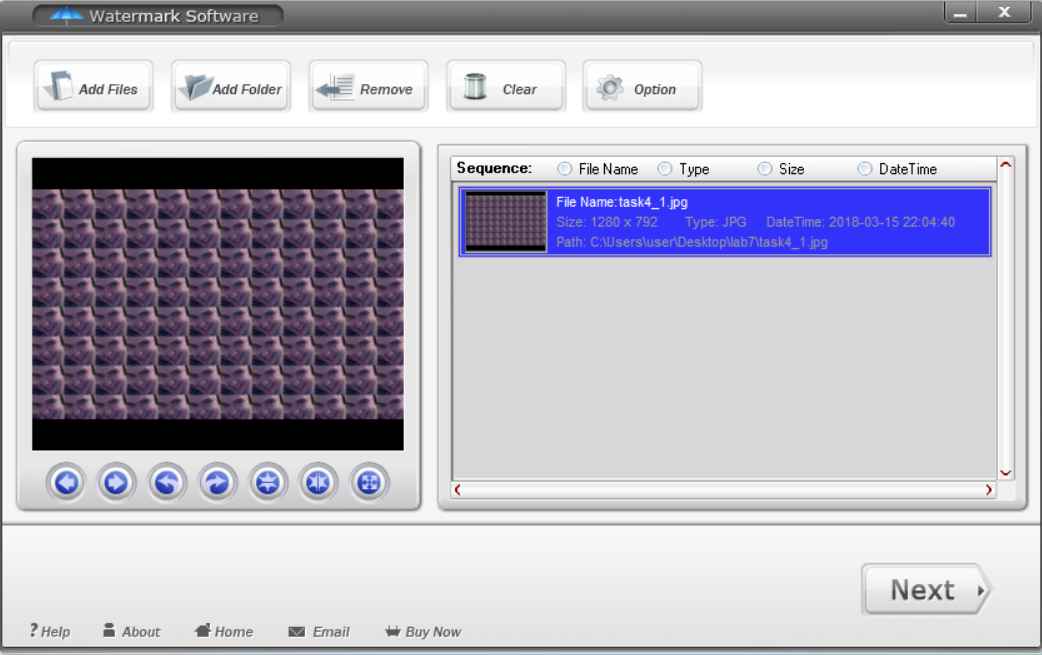


Рисунок 16 – Картинка для вставки ЦВЗ

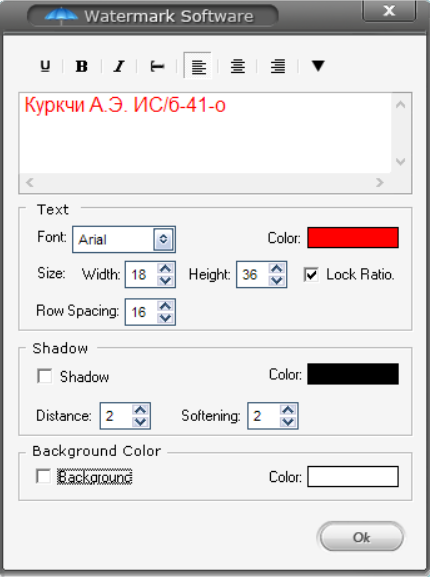


Рисунок 17 – Параметры ЦВЗ

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.

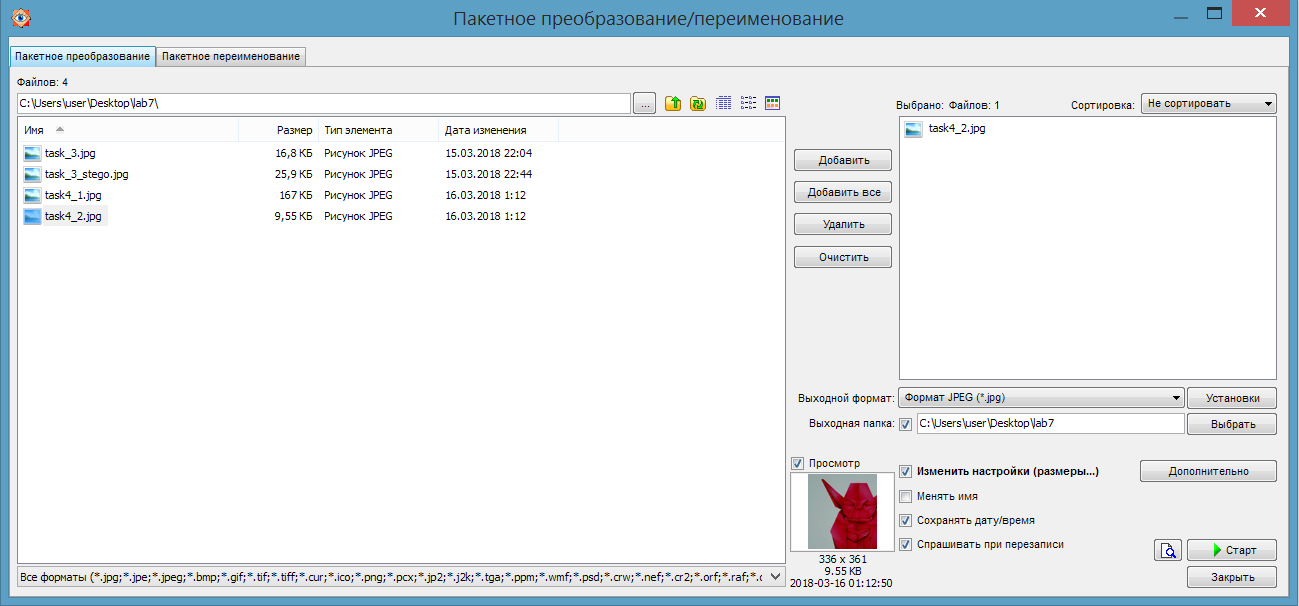


Рисунок 19 – Окно программы

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

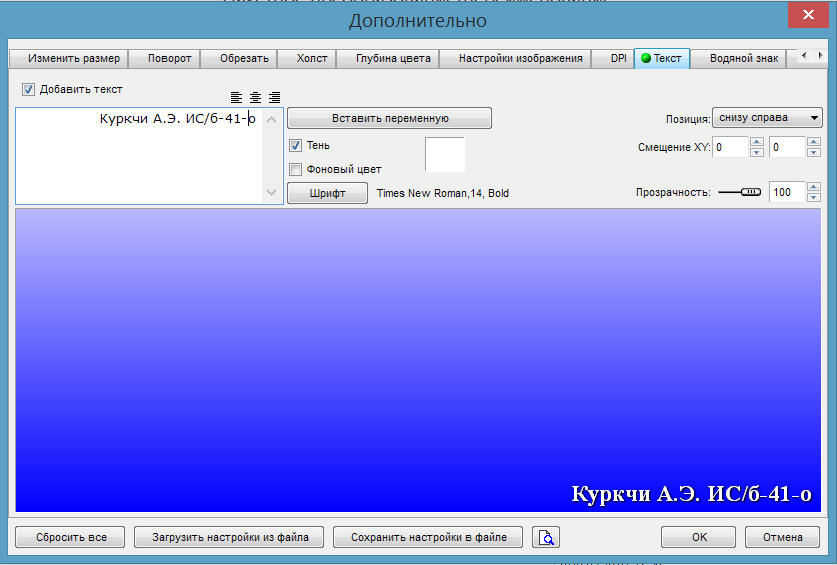


Рисунок 20 – Настройка водяного знака

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

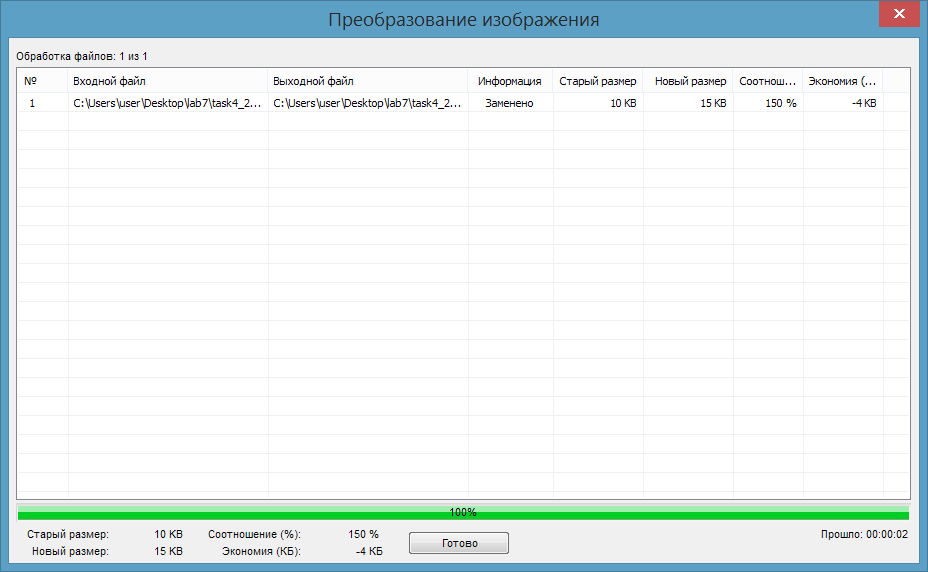


Рисунок 21. – Выполненные преобразования.



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.

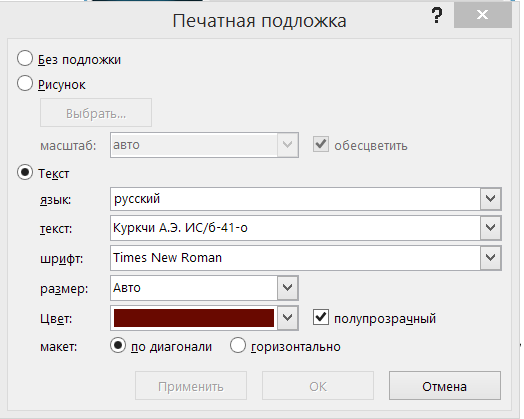


Рисунок 23 – Настройки подложки

**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.