Отличительной особенности разработанного оптоэлектронного метода по сравнению с другими подобными методами является то что шумоподобный сигнал подается не со стороны передатчика вололоконно оптической линии связи а со стороны приемника информации который позволяет выделит информационный сигнал при зашумлении даже при очень сложных законов изменении .

Литература

1. В.В. Гришачев, В.Н. Кабашкин А.Д. Фролов. Физические принципы формирования каналов утечки информации в волоконно-оптической линии связи. //Информационное противодействие угрозам терроризма: научн-практ. Журн. /ФГПУ НТЦ , Москва. 2004, №3. С. 74 – 76.

М.А. Кудрина, И.Е. Дулимова

СКРЫТИЕ ИНФОРМАЦИИ В АУДИОФАЙЛАХ МЕТОДАМИ СТЕГАНОГРАФИИ.

(Самарский национальный исследовательский университет имени академика С.П. Королева)

Стеганография – это метод организации связи, который скрывает само наличие связи. Общей чертой различных способов стеганографии является то, что скрываемое сообщение встраивается в обычный, не вызывающий подозрение объект. После чего данный объект открыто доставляется адресату. В криптографии наличие шифрованного сообщения само по себе создает угрозу целостности информации, при стеганографии наличие скрытого сообщения остается незаметным[1].

Сообщение, факт передачи которого хотят скрыть, называют секретным сообщением. Файл, не содержащий секретного сообщения, называется пустым контейнером, а файл с включенным сообщением – заполненным контейнером. В данной работе рассмотрена возможность встраивания информации методом стеганографии. В качестве контейнера выбраны аудиофайлы в формате WAV.

Одним из первых методов встраивания информации в аудиофайлы, затрагивающих область аудиоданных, является метод изменения малозначащих битов (LSB). Чаще всего он применяется для сокрытия в аудиофайлах формата WAV благодаря простоте осуществления вставки [2]. Метод заключается в использовании погрешности дискретизации, которая всегда существует в оцифрованных изображениях или аудио- и видеофайлах. Данная погрешность равна наименьшему значащему разряду числа, определяющего величину элемента файла. Поэтому модификация младших битов в большинстве случаев не вызывает значительной трансформации файла и не обнаруживается визуально [3].

В рамках данной работы реализован метод изменения малозначащих битов, разработана автоматизированная система встраивания текстовых данных в контейнер аудиофайла, реализована обратная операция по извлечению встро-

енных данных из контейнера и произведено исследование возможностей использования данного метода. На рисунке 1 представлен интерфейс системы.

Большое влияние на эффективность алгоритма оказывает отношение размера файла, используемого в качестве контейнера, к объему встраиваемых данных. Исследования показывают, что, если объем встраиваемых данных составляет не менее 10% от объема файла контейнера, то при первичном анализе можно обнаружить факт встраивания. При наиболее оптимальных параметрах (менее 10% от объема файла контейнера) искажения исходного аудифайла незначительны и вероятность обнаружения факта встраивания ниже. Популярность данного метода обусловлена тем, что он позволяет скрывать в относительно небольших файлах достаточно большие объемы информации. Основной недостаток метода – высокая чувствительность к малейшим искажениям контейнера, слабая устойчивость к посторонним воздействиям на сигнал (сжатие, воздействие шумов).

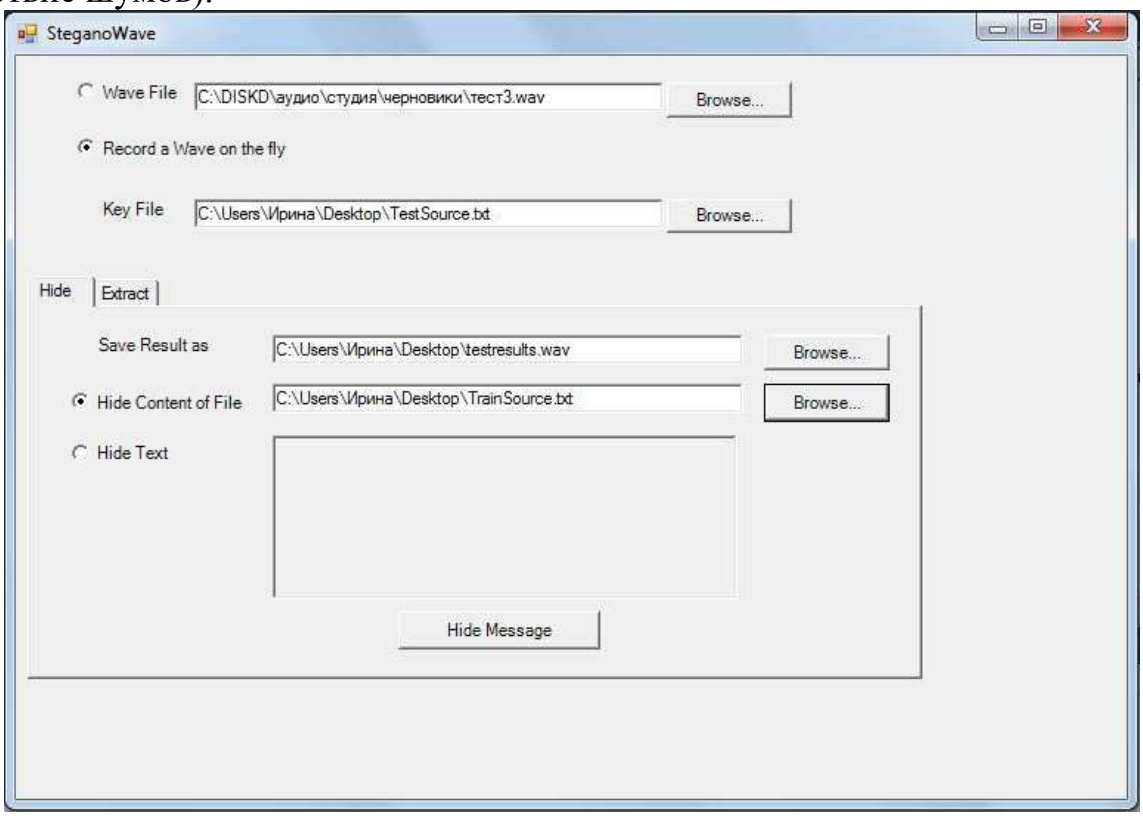

Рисунок 1 – Интерфейс системы

Литература

1. Генне О. В. ОСНОВНЫЕ ПОЛОЖЕНИЯ СТЕГАНОГРАФИИ // журнал "Защита информации. Конфидент", №3, 2000.

2. Нечта И. В. Стеганография в файлах формата Portable Executable // Вестник СибГУТИ. 2009. № 1. С. 85 – 89.

3. Freeware program of steganography bmp, wav, voc. [Электронный ресурс] http://www.heinz-repp.onlinehome.de/Hide4PGP.htm.