ПРИЛОЖЕНИЕ ДЛЯ СОКРЫТИЯ ИНФОРМАЦИИ В АУДИОФАЙЛЕ МЕТОДОМ ЗАМЕНЫ НАИМЕНЬШЕГО ЗНАЧАЩЕГО БИТА (LSB)

Шахмуть А.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петров С.Н. – к.т.н., доцент

Слово стеганография происходит от греческих слов: «steganos», что дословно означает «скрывать» или «секрет» и «graphy», что означает «письмо» или «рисование». Отсюда, стеганография – это искусство сокрытия секретной информации в файле таким образом, что только отправитель и получатель могут знать о ее наличии. Конфиденциальная информация закодирована так, что само существование сообщения утаивается. Преимущество стеганографии над чистой криптографией состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

Одним из самых распространённых методов является LSB (Least Significant Bit, наименьший значащий бит) алгоритм, который заменяет наименьший значащий бит в нескольких байтах файла-носителя, чтобы скрыть последовательность байтов, содержащих скрытые данные. Это, как правило, эффективно тогда, когда замена младшего бита не влечет за собой значительное ухудшение качества. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека. Небольшая модификация этой стеганографической техники позволяет использовать для встраивания сообщения два или более младших битов на байт. Это увеличивает объем скрытой информации в объекте-контейнере, но скрытность сильно снижается, что облегчает обнаружение стеганографии.

Преимущества метода:

– размер файла-контейнера остается неизменным;

– при замене одного бита в канале синего цвета внедрение невозможно заметить визуально;

– возможность варьировать пропускную способность, изменяя количество заменяемых бит.

Недостатки метода:

– скрытое сообщение легко разрушить, например, при сжатии или отображении;

– не обеспечена секретность встраивания информации, так как точно известно местоположение скрываемой информации.

В ходе исследования разработано программное обеспечение, назначением которого является внесение сокрытого сообщения в аудиофайл переменного размера методом LSB. Также продукт должен проводить корреляционный анализ стего-файла и контейнера. Вышеуказанные функции реализованы с помощью пакета MATLAB R2018b с представлением данных в оконных формах Visual Studio. На рисунках 1 и 2 представлены графики сигналов исходного аудиофайла и содержащего стегоконтейнер.

Основными возможностями программы являются:

– безопасное сокрытие информации в контейнере;

– извлечение информации из контейнера, с использованием ключа;

– графическое отображение информации, необходимой для сравнительного корреляционного анализа метода стеганографии – LSB.

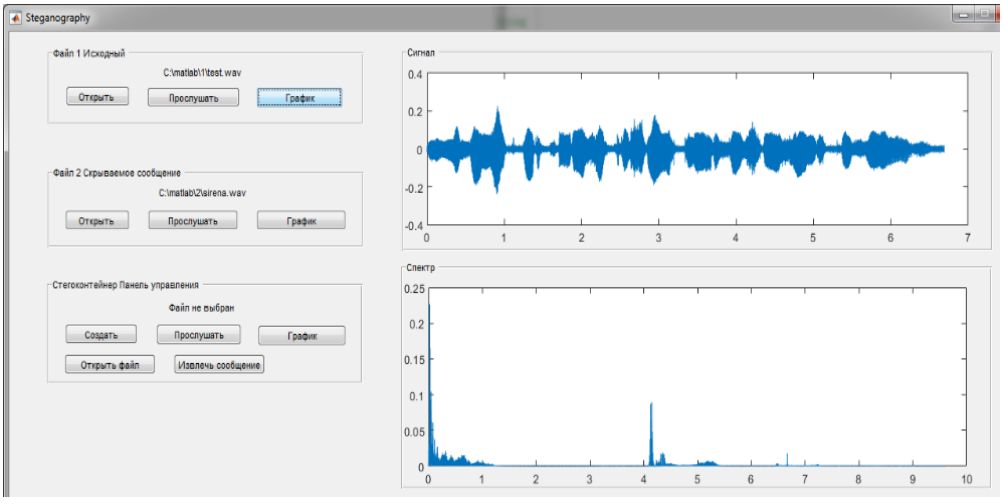

Рисунок 1 – Графики исходного (скрываемого) файла

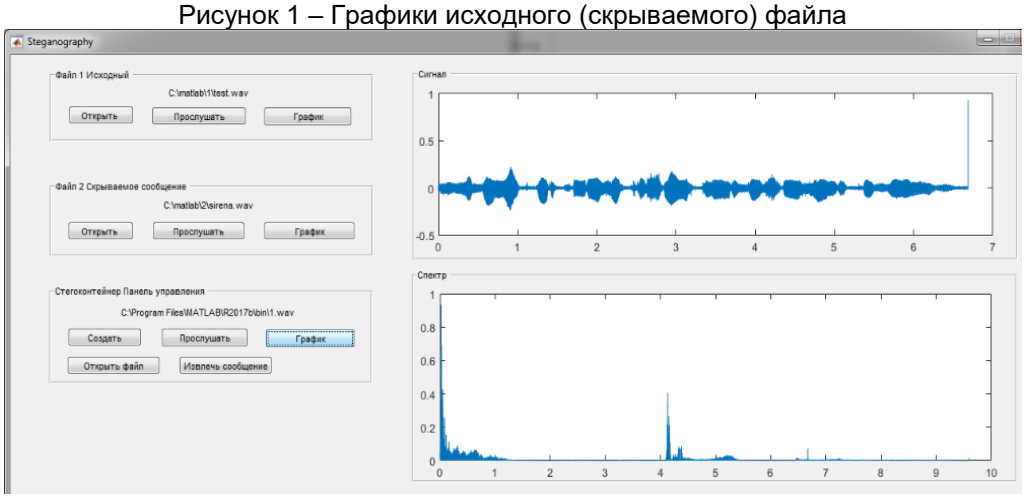

Рисунок 2 – Графики стегоконтейнера

По результатам исследования можно уверенно говорить, что человеческое ухо неспособно различить «чистый» контейнер от стего. В частотной области наибольшие расхождения между стего и контейнером находятся в области низких частот (инфразвук). Методы LSB являются неустойчивыми ко всем видам атак и могут быть использованы только при отсутствии шума в канале передачи данных.

Список использованных источников:

1 Коржик В. И. Лекции по основам стеганографии [Электронный ресурс]. – Режим доступа : www.ibts-sut.ru.

2 Конахович Г. Ф., Пузыренко А. Ю. Основы современной криптографии и стеганографии [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Стеганография#Ссылки.

3 В. Шрайбман, Стеганография аудиофайла методом LSB [Электронный ресурс]. – Режим доступа https://ru.bmstu.wiki/Стеганография_аудиофайла_методом_LSB.

4 Завьялов С. В., Ветров Ю. В, Стеганографические методы защиты информации [Электронный ресурс]. – Режим доступа : https://ghostbasenji.blogspot.com/2018/08/steganography-method-LSB.html.