УДК 004.021

ПРОЕКТИРОВАНИЕ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА ПОЛЬЗОВАТЕЛЯ ДЛЯ ВСТРАИВАНИЯ ИНФОРМАЦИИ В АУДИОФАЙЛ НА ОСНОВЕ МОДИФИКАЦИИ СПЕКТРАЛЬНЫХ КОЭФФИЦИЕНТОВ. ОЦЕНКА СТЕГАНОСТОЙКОСТИ СИСТЕМЫ

А.С. ТАНАНА
(Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ)

В статье рассматриваются вопросы разработки и создания графического интерфейса пользователя для встраивания текстовой информации в звуковой файл. Выбор технологии разработки, определение основных функциональных возможностей. Оценка стеганостойкости разработанной системы.

Защита информации, в том числе конфиденциальных данных, становится актуальной задачей с развитием информационных технологий. Решение такой задачи даёт стеганография – наука, изучающая алгоритмы и методы сокрытия данных в мультимедийных объектах, которая должна оставаться не обнаружимой ни статистически, ни для человеческого восприятия. Среди возможностей стеганографии можно выделить встраивание цифровых водяных знаков, идентификационных номеров, заголовков.

Каждый стеганографический алгоритм должен удовлетворять ряду качественных характеристик. К ним можно отнести надёжность, устойчивость, объём встраиваемых данных. Большинство алгоритмов лишь частично соответствуют заданным требованиям, поэтому задача разработки стеганостойкого алгоритма встраивания данных остается актуальной задачей и в настоящее время.

Алгоритм встраивания данных на основе замены высокочастотных коэффициентов с применением генератора псевдослучайной последовательности является усовершенствованным методом существующих методов. Для оценки стеганостойкости алгоритма необходимо провести тестирование функциональности внедрения и извлечения сообщения, а также провести ряд модификаций и атак на стегоконтейнер.

В рамках данной статьи в качестве стегоконтейнера выберем звуковой файл формата WAVE. Данный формат содержит аудиоданные в несжатом виде, что позволяет хранить информацию в наилучшем качестве. В качестве встраиваемого сообщения будем использовать текстовые данные.

Для разработки программного обеспечения будем использовать возможности платформы .Net Framework: язык программирования C#, графический интерфейс пользователя Windows Forms, среду разработки Visual Studio 2015. Разработанная программа должна решать следующие задачи:

– встраивание текстовых данных в аудиофайл;

– извлечение данных из стегоконтейнера в целостном виде.

Дизайн пользовательского интерфейса должен быть удобным, интуитивно понятным и привлекательным.

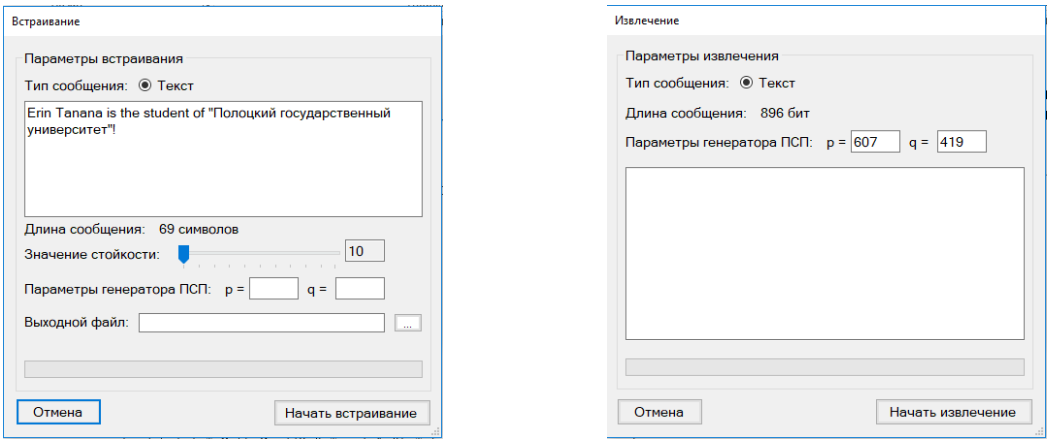
В основе алгоритма встраивания сообщения лежит дискретное косинусное преобразование. Рассмотрим программную реализацию преобразования на языке C#:

Листинг 1. Дискретное косинусное преобразование

```
1: public static void DCT(double[] data){
2: double[] result = new double[data.Length];
3: double c = Math.PI / (2.0 * data.Length);
4: double scale = Math.Sqrt(2.0 / data.Length);
5: for (int k = 0; k < data.Length; k++) {
6: double sum = 0;
7: for (int n = 0; n < data.Length; n++)
8: sum += data[n] * Math.Cos((2.0 * n + 1.0) * k * c);
9: result[k] = scale * sum;
10: }
11: data[0] = result[0] / Math.Sqrt(2.0);
12: for (int i = 1; i < data.Length; i++)
13: data[i] = result[i];
14: }
```

Интерфейс пользователя включает в себя следующие окна: главное окно приложения, окно встраивания сообщения, окно извлечения сообщения (рис. 1). На главном окне приложения пользователь выбирает файл и тип операции: встраивание или извлечение. Здесь же отображаются основные данные о выбранном аудиофайле. Перед встраиванием пользователь вводит сообщение, выбирает значение стойкости

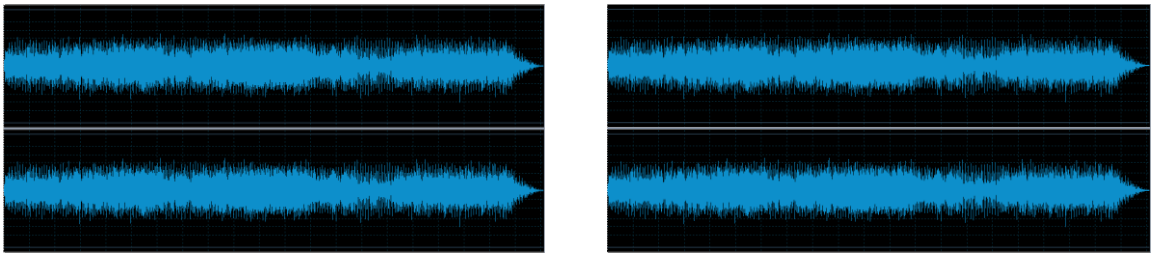
и начальные параметры генератора псевдослучайной последовательности. После указания пути выходного файла и при корректности введённых данных можно начать процесс встраивания сообщения. Для извлечения сообщения необходимо знать длину скрытого сообщения и начальные параметры генератора, а также исходный аудиофайл.



а *б*

Рисунок 1. – Интерфейс пользователя:
***а* – окно встраивания сообщения; *б* – окно извлечения сообщения**

Для демонстрации стеганографической модификации контейнера выберем аудиоконтейнер в формате WAVE. В нашем случае, это файл audiofile.wav (размер 35.5МБ). В качестве встраиваемого сообщения будем использовать текстовое сообщение «Erin Tanana is the student of “Полоцкий государственный университет”!» длиной 896 бит. Выберем значение стойкости s = 156, в качестве входных параметров генератора p = 607, q = 419. Зададим путь выходного файла и встроим сообщение. Сравним полученный стегоконтейнер с исходным контейнером:



а *б*

Рис. 2. Сравнение исходного и заполненного контейнера:
а – исходный контейнер; б – заполненный контейнер

Визуальных отличий волновой формы нет, при прослушивании файла заметных искажений нет, значит выбранный контейнер пригоден для стеганографической модификации. Визуальные отличия не были обнаружены и при выборе конейтнеров, содержащих монотонный звук. Таким образом, для встраивания сообщения пригоден любой контейнер. Отметим, что для встраивания сообщений большего объёма целесообразно использовать аудиофайлы большего размера, однако это приводит к увеличению вычислительного процесса.

Для определения стойкости разработанной стеганосистемы проведём несколько атак и модификаций: применение эффекта искажения звука, удаление 25% данных в конце файла, удаление 50% данных. В качестве исходного контейнера положим рассмотренный ранее контейнер audiofile.wav. Входные параметры также оставим неизменными. Как уже отмечалось, визуальных изменений волновой формы замечено не было, как и искажений звука при прослушивании. Результаты проведённых испытаний отображены в таблице.

Таблица 1. Результаты модификаций и атак

Название атаки	Результат
Эффект искажения звука	Сообщение успешно извлекается
Удаление 25% данных в конце файла	Сообщение успешно извлекается
Удаление 50% данных	Сообщение извлечь не удалось

Делаем вывод, что разработанный алгоритм обладает приемлемой надежностью и устойчивостью. В перспективе дальнейшей разработки планируется расширить функционал приложения и перевести приложение на веб-технологии.

ЛИТЕРАТУРА

1. Грибунин В.Г., Оков И.Н., Туринцев В.И. Цифровая стеганография. – М. : СОЛОН-Пресс 2002. 272 с.
2. Blackledge, J. Resilient Digital Image Watermarking for Document Authentication / J. Blackledge, O. Iakovenko // IAENG International Journal of Computer Science. – 2014. – № 41(1). – С. 1-17.
3. Горелкина Д.А., Дорошенко Н.С., Осипов Д.Л. Применение методов цифровой стеганографии для внедрения конфиденциальной информации в растровые изображения // Вестник Ставропольского государственного университета. – 2011. – №75. – С. 75-76.
4. Садов, В.С. Компьютерная стеганография / В.С. Садов – Минск: БГУ, 2010. – 211 с.