УДК 004.056.55

ОПРЕДЕЛЕНИЕ СТЕПЕНИ ПРИГОДНОСТИ КОНТЕЙНЕРА ДЛЯ СТЕГАНОГРАФИЧЕСКОЙ МОДИФИКАЦИИ В СТЕГОСИСТЕМЕ, ОСНОВАННОЙ НА СОКРЫТИИ ТЕКСТОВЫХ ДАННЫХ В АУДИОФАЙЛАХ ЗА СЧЕТ ИЗМЕНЕНИЯ ВРЕМЕНИ ЗАДЕРЖКИ ЭХО-СИГНАЛА

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

Определяется степень пригодности контейнера для стеганографической модификации. Представлены некоторые виды атак на стегосистему. Построена система, основанная на скрытии текстовых сообщений в аудиофайлах, а также изучены атаки и выяснено, насколько пригодна такая система для практического применения.

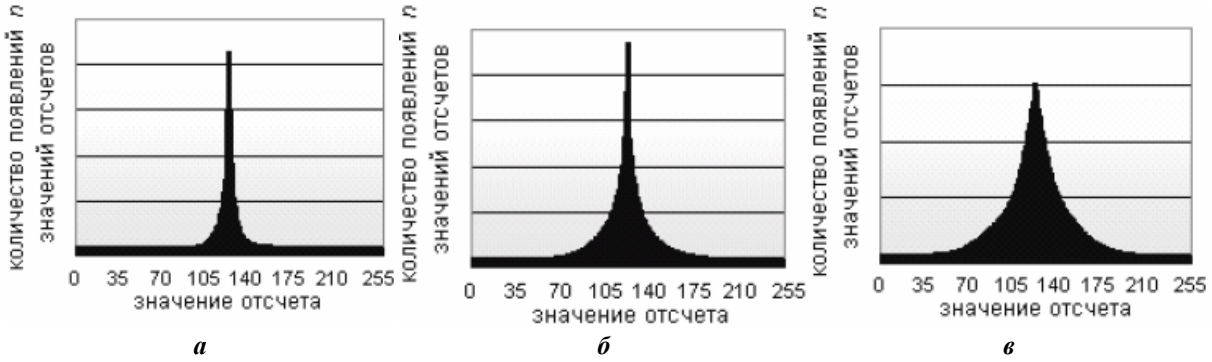
Основными параметрами аудиосигналов являются их амплитуда, частота и фаза. Для стеганографической модификации пригодны все эти параметры, но перед процедурой встраивания необходимо оценить пределы модификации параметров того или иного контейнера, а также вносимые при этом искажения. Пропускная способность, надежность, устойчивость стеганографической системы во многом будет определяться степенью модификации аудиоконтейнера [1].

Оценка стеганостойкости реализованной системы

Существует множество классификаций оцифрованных аудиосигналов по их техническим параметрам, таким как, частота дискретизации, количество каналов (моно или стерео), качество записи (количество кб в секунду) и т.д. В то же время, если аудиосигналы (контейнеры) принадлежат к одному формату представления данных (например, WAVE) имеют одну частоту дискретизации, одинаковое количество каналов, схожее качество звука и различаются только по музыкальному жанру, достаточно сложно оценить пригодность того или иного контейнера к стеганографической модификации.

Все аудиосигналы можно разбить на три группы (рис. 1):

- аудиофайлы, подобные речи, с большим количеством пауз: стихи, голос диктора, речь с негромкой фоновой музыкой и т.д. (рис. 1, *а*);
- аудиофайлы, не обладающие широким частотным диапазоном, подобные обычным музыкальным композициям: эстрадные песни, популярная музыка, блюз и т.д. (рис. 1, *б*);
- аудиофайлы, обладающие широким частотным диапазоном, прошедшие дополнительную компьютерную обработку: электронная музыка (trance, house, techno и др.), синтезированные звуки природы и т.д. (рис. 1, *в*).



а ***б*** ***в***

Рисунок 1. – Графики распределения отсчетов для трех групп аудиосигналов

Использование аудиофайлов из первой группы оказалось совсем неприемлемым для использования независимо от качества использованного контейнера. Вероятность правильного и полного изъятия сообщения из контейнера достаточно мала. При использовании аудиофайлов из второй группы, как и ожидалось, искажения едва различимы натренированным ухом, а вероятность правильного изъятия достаточно велика. Использование аудиофайлов из третьей группы показало, что вероятность правильного извлечения близка к 100%, при этом различить пустой контейнер и контейнер с данными на слух не удастся.

Из этого можно сделать вывод, что лучше всего для скрытия данных методом задержки эхосигнала подходят аудиофайлы, прошедшие дополнительную компьютерную обработку (электронная му-

зыка). Также следует учесть частоту дискретизации и количество каналов: чем их значения выше, тем больше вероятность правильного изъятия [2].

Основные виды атак на стегосистемы:

1. *Атака на основе известного заполненного контейнера*. Задача состоит в обнаружении факта наличия скрытого сообщения. Прослушивание аудиосигнала с целью обнаружить какие-либо помехи. Был выбран контейнер длительностью 60 секунд, с динамичной музыкой. И произведено скрытие сообщения длиной 20 символов. Результат – прослушивание заполненного контейнера на акустической системе показало, что никаких посторонних звуков, хрипов и тресков не обнаружено.

2. *Атака на основе известного пустого контейнера*. Если он известен, то путем сравнения его с предполагаемым контейнером, в котором есть скрытое сообщение, всегда можно установить факт наличия стегоканала. Это может быть сравнение по длине аудиосигнала, сравнение по размеру, а также прослушивание. Был выбран контейнер длительностью 60 секунд, с динамичной музыкой. И произведено скрытие сообщения длиной 20 символов. Результат – многократное прослушивание заполненного контейнера и контейнера оригинала на акустической системе без проигрывания низких частот (ноутбук) показало, что отличий между звучанием нет. Однако при прослушивании на акустической системе с устройством, проигрываемым низкие частоты, стали заметны некоторые отличия в глубине звучания заполненного контейнера и контейнера оригинала.

3. *Атаки против встроенного сообщения*, направленные на удаление или порчу встроенной информации путем манипулирования заполненным контейнером, а также направленные на затруднение или невозможность правильной работы детектора. При этом сообщение в аудиофайле остается, но теряется возможность его приема. Примерами являются: обрезка (изменение длины) аудиосигнала; изменение формата на другой; изменение параметров формата контейнера, ускорение или замедление; изменение тональности. Результат – метод скрытия данных с помощью задержки эхо-сигнала неустойчив к временным изменениям. При изменении длины аудиофайла нанесколько секунд извлечь какую-либо информацию уже невозможно. Изменение любых других параметров аудиофайла не повлияло на получение скрытой информации [3].

Заключение

Рассмотрен метод встраивания информации в звуковые файлы. Метод эхо-сигналов – самый перспективный, однако требует доработки в плане пропускной способности и вероятности правильного извлечения встроенных бит информации. Для оценки эффективности рассматривались такие параметры, как особые требования к контейнерам – звуковым файлам и сложность определения ее злоумышленником, влияние попытки уничтожения скрытой информации на сохранность контейнера. Выбор метода встраивания информации в звуковые файлы, используя преобразования эхо-сигналов, обусловлен тем, что этот метод имеет устойчивость к амплитудным и частотным атакам, что позволяет обойти остальные, неустойчивые к этим атакам, методы. Однако данный метод неустойчив к временным атакам, напрямую влияющим на длину аудиофайла и количество отсчетов в нем.

Программа реализована и готова к использованию с возможностью ее доработки.

ЛИТЕРАТУРА

1. Садов, В.С. Компьютерная стеганография / В.С. Садов. – М. : МГВРК, 2012. – 289 с.
2. Matsui, K. Digital signature on a facsimile document by recursive MH coding / K. Matsui, K. Tanaka and Y. Nakamura // Symposium On Cryptography and In-formation Security, 1989.
3. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин. – М. : СОЛОН-Пресс, 2002. – 272 с.