УДК 004.221

РАЗРАБОТКА СИСТЕМЫ ДЛЯ СКРЫТИЯ ИНФОРМАЦИИ В ЗВУКОВОЙ СРЕДЕ

И.С. АНДРЕЕВ
(***Представлено: канд. физ.-мат. наук, доц. Д.Ф. ПАСТУХОВ***)

В данной статье рассматриваются различные алгоритмы сокрытия информации в звуковой среде и их преимущества. В ходе исследований был выбран оптимальный вариант алгоритма.

Ключевые слова: стеганография, сокрытие информации, сигнал, музыкальная стегосистема.

Введение. Задача надежной защиты и сокрытия информации идет из далекой глубины веков. Еще в античные времена применяли различные методы защиты важной информации от “посторонних глаз». Это были скиталы, квадрат Полибия и первые сдвиговые шифры. Позже возникли шифры простой замены (рассказ Артура Конан Дойла “Пляшущие человечки”) и перестановочные шифры (решетка Кардано). В XVIII веке возник шифр “по книге”, который можно рассматривать как развитие шифра Цезаря (таким шифром пользуется герой Ю. Семенова - Штирлиц в романе “17 мгновений весны”).

Но все шифры обладают конечной стойкостью и могут быть расшифрованы за конечный промежуток времени. Решить эту проблему помогает стеганография, которая скрывает сам факт передачи секретного сообщения.

Основной раздел. В статье будет рассмотрены стеганографические методы сокрытия информации в звуковых файлах, как с точки зрения устойчивости к атакам, так и с точки зрения сохранения приемлемого качества звукового сигнала.

Метод наименьших значащих битов применяется при цифровом представлении аудиосигнала и пригоден для использования при любых скоростях связи. При преобразовании звукового сигнала в цифровую форму всегда присутствует шум дискретизации, который не вносит существенных искажений. “Шумовым” битам соответствуют младшие биты цифрового представления сигнала, которые можно заменить скрываемыми данными. Данный метод обладает чрезвычайно низкой стегостойкостью и простой реализацией. Изменение звукового сигнала можно обнаружить.

Методы широкополосного кодирования используют те же принципы, что методы сокрытия данных в изображениях. Их суть заключается в незначительной одновременной модификации целого ряда определенных битов контейнера при сокрытии одного бита информации. Данный метод имеет среднюю устойчивость к атакам и искажениям и сложную в реализацию. Звуковой сигнал практически не изменяется.

Метод сокрытия в эхо-сигнале скрывает данные путем внедрения эха в звуковой сигнал. Известно, что при небольших временных сдвигах эхо-сигнал практически неразличим на слух. Поэтому, если ввести определенные временные задержки, величина которых не превышает порог обнаружения, то, разбивая исходный звуковой сигнал на сегменты, в каждый из них можно ввести соответствующий эхо-сигнал, в зависимости от скрываемого бита. Данный метод стегоустойчив и сложен в реализации. Звуковой сигнал практически не изменяется.

Фазовые методы сокрытия применяются как для аналогового, так и для цифрового сигнала. Они используют тот факт, что плавное изменение фазы на слух определить нельзя. В таких методах защищаемые данные кодируются либо определенным значением фазы, либо изменением фаз в спектре. Изменения в звуковом файле при использовании данного метода невозможно обнаружить с помощью человеческого слуха, но чрезвычайно сложно извлечь информацию при малейшем повреждении сигнала.

Музыкальные стегосистемы. Музыкальная форма звуковой среды занимает большую часть информационного пространства Internet. Помимо этого, она широко используется в радиосетях общего назначения и распространяется на электронных носителях информации, которые, в связи с развитием компьютерной техники, получили широкое распространение. В связи с этим использование музыкальной среды для сокрытия информационных сообщений представляется достаточно перспективным. Для сокрытия данных можно применять методы, основанные на модификации тех параметров музыкальной среды, которые в теории музыки можно описать качественно. Музыкальная среда имеет свое текстовое отображение в виде нот и других знаков, которые позволяют достаточно адекватно отображать музыкальное произведение и его внутреннюю структуру такими элементами, как ноты, гаммы, периоды, такты, каденции, аккорды, мотивы, модуляции, тональности, различные виды развития, секвенции и пр. Построения музыкальных фрагментов подчиняются синтаксическим правилам, которые можно описать, что

позволяет строить логические взаимоотношения и, соответственно, описание структур музыкальных произведений.

Музыкальные стегосистемы обеспечивают сокрытие информации в музыкальной среде по аналогии с импровизацией музыкальных произведений. По существу, импровизация представляет собой такое изменение музыкального произведения или его фрагментов, которое сохраняет основные темы первоначального произведения в виде мелодий, но при этом расширяет образ музыкальной темы другими, дополняющими основной образ чертами, которых не было в основном музыкальном произведении. Основное отличие музыкальной стеганографии от импровизации состоит в том, что целью является не расширение образов базового музыкального произведения, а внесение изменений, которые сохраняют мелодию основного произведения, соответствуют всем правилам построения данного произведения и при этом кодируют скрываемое сообщение, не искажая главной темы произведения.

Фрагмент музыкального произведения может быть описан в виде некоторой логической структуры. Аналогом слова текстового предложения в музыкальном произведении будет один такт мелодии, а аналогом предложения в музыке будем считать фрагменты, разделяемые цензурами. Как правило, музыкальное произведение состоит из ряда фраз, которые состоят из тактов. Внедрение текста в музыкальное произведение осуществляется отдельными предложениями, каждое из которых может сопоставляться с отдельной мелодией. Далее формируется нотное отображение расширенного музыкального произведения с внедренным в него скрываемым сообщением. На основании нотного отображения расширения осуществляется его музыкальная реализация с помощью современных компьютерных систем, представляющих собой программно-аппаратные синтезаторы звука. Музыкальную стегосистема обладает высокой стойкостью к атакам и практически невозможностью обнаружения, однако для реализация этой системы необходимо потратить огромное количество ресурсов.

В ходе исследований было обнаружено преимущество фазового метода сокрытия перед другими методами.

Заключение. В данной статье были рассмотрены алгоритмы сокрытия данных в звуковых файлах, описана работа музыкальной стегосистемы и сделан вывод об оптимальном методе для реализации системы.

ЛИТЕРАТУРА

1. Мельников В.В. Защита информации в компьютерных системах. Электронинформ, 1997. – 368 с.
2. Барабаш А.В., Шанкин Г.П. История криптографии. Ч. l. – М.: Гелиос АРВ, 2002. – 240 с.
3. Домарев В.В. Защита информации и безопасность компьютерных систем. — К.: ДиаСофт, 1999. – 480 с.
4. Ярочкин В.И. Безопасность информационных систем. – М.: Ось-86, 1996. – 320с.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / под ред. В.Ф. Шаньгина. – 2-е изд., перераб. и доп. – М.: Радио и связь, 2001. – 376 с.
6. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МГИФИ, 1997. – 538 с.