УДК 004.056.55

ПРОЕКТИРОВАНИЕ СТЕГОСИСТЕМЫ, 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)

Рассматривается практический способ создания надежной стегосистемы с нестандартным способом скрытия информации. Построена система, основанная на скрытии текстовых сообщений в аудиофайлах. Выяснено, насколько пригодна такая система для практического применения.

В статье пойдет речь о сокрытии данных в аудиофайлах с помощью одного из методов стеганографии. Под цифровой стеганографией понимается скрытие одной информации в другой. Причем сокрытие это должно реализоваться таким образом, чтобы, во-первых, не были утрачены свойства и некоторая ценность скрываемой информации, а во-вторых, неизбежная модификация информационного носителя, не только не уничтожила смысловые функции, но и на определенном уровне абстракции даже не меняла их. Тем самым факт передачи одного сообщения внутри другого не выявляется традиционными методами.

Принцип построения стеганографической системы и описание алгоритма скрытия данных. Стандартная стеганографическая схема сохраняется вне зависимости от технологии, которой она реализуется. Задачу встраивания и выделения сообщений из другой информации выполняет стегосистема. Стегосистема состоит из следующих основных элементов, представленных на рисунке 1.

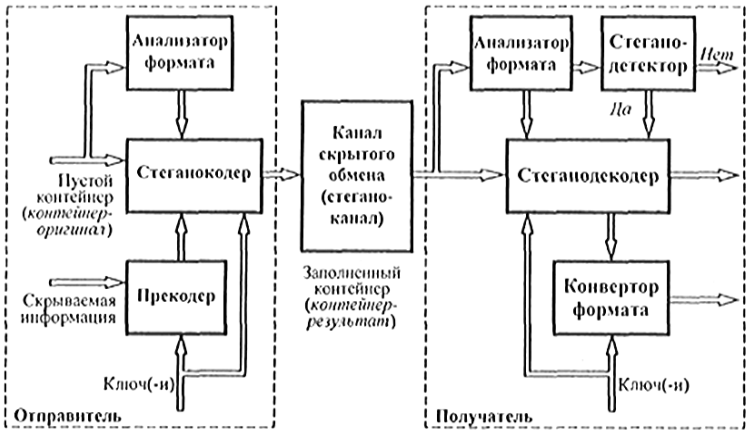

Рисунок 1. – Структурная схема типичной стегосистемы

Контейнер – любая информация, предназначенная для сокрытия тайных сообщений. Стегоключ, или просто ключ, – секретный ключ, необходимый для сокрытия информации. *Прекодер* – устройство, предназначенное для преобразования скрываемого сообщения к виду, удобному для встраивания в сигналконтейнер. *Стегокодер* – устройство, предназначенное для осуществления вложения скрытого сообщения в другие данные с учетом их модели; устройство выделения встроенного сообщения. *Стегодетектор* – устройство, предназначенное для определения наличия стегосообщения. *Декодер* – устройство, восстанавливающее скрытое сообщение. Этот узел может отсутствовать.

Данные, содержащие скрытое сообщение, могут подвергаться преднамеренным атакам или случайным помехам. Как показано на рисунке 1, в стегосистеме происходит объединение двух типов информации так, чтобы они могли быть различимы двумя принципиально разными детекторами. В качестве одного из детекторов выступает система выделения цифровых водяных знаков (ЦВЗ), в качестве другого – человек [1].

Для сокрытия данных использовался метод встраивания информации за счет изменения времени задержки эхо-сигнала. Этот метод позволяет внедрять данные в сигнал прикрытия, изменяя параметры эхо-сигнала. К параметрам эхо, несущим внедряемую информацию, относятся: начальная амплитуда, время спада и сдвиг (время задержки между исходным сигналом и его эхо). При уменьшении сдвига два сигнала смешиваются. В определенной точке человеческое ухо перестает различать два сигнала, и эхо воспринимается, как добавочный резонанс. Кодер использует два времени задержки: одно для кодирования нуля, другое для кодирования единицы. И то, и другое время задержки меньше того, на котором человеческое ухо может распознать эхо. Кроме уменьшения времени задержки необходимо добиться уста-

новлением начальной амплитуды и времени спада того, чтобы внедренная информация не могла быть воспринята системой слуха человека.

При кодировании информации были выбраны значения задержек эхо-сигналов, равные 0,0012 и 0,0008 секунды. Данные значения снижают эффективность алгоритма извлечения, уменьшая вероятность правильного извлечения бита, однако подходит практически для всех типов контейнеров. Значение амплитуды, равное 40%, выбрано в связи с тем, что оно помогает увеличить вероятность того, что факт наличия скрытой информации не будет раскрыт.

Декодирование внедренной информации представляет собой определение промежутка времени между сигналом и эхо. Для этого необходимо рассмотреть амплитуду (в двух точках) автокорреляционной функции дискретного косинусного преобразования логарифма спектра мощности (кепстра). Всплеск автокорреляционной функции будет наблюдаться через δ_1 или δ_0 секунд после исходного сигнала (рис. 2). Правило декодирования основано на определении промежутка времени между исходным сигналом и всплеском автокорреляции [2].

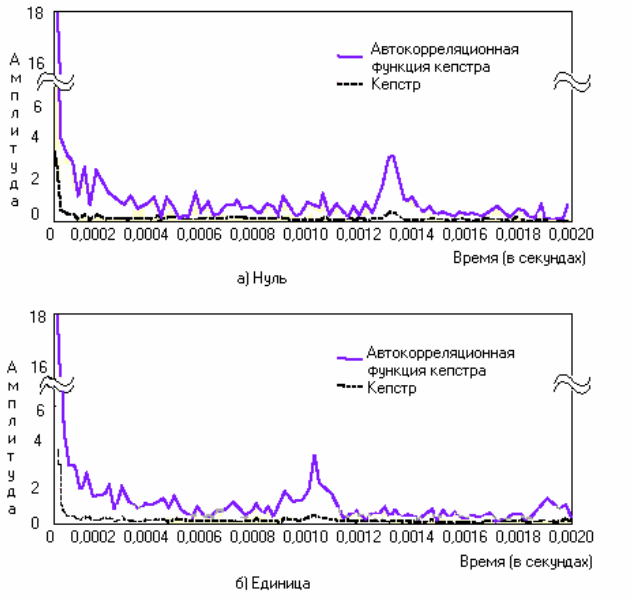

Рисунок 2. – Поведение автокорреляционной функции

По исследованиям В. Бендера и Н. Моримото, данная схема позволяет внедрять 16 бит в одну секунду аудиозаписи незаметно, без потери ее качества [3]. 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. При реализации метода стеганографической защиты информации посредством преобразования эхо-сигналов стало ясно, что основную трудность представляет реализация наиболее эффективного алгоритма извлечения встроенных бит. Некоторые исследования в этом направлении показали, что возможно достичь наибольшей эффективности только посредством индивидуального подхода к каждому контейнеру отдельно, меняя при этом время задержек накладываемого эхо-сигнала.

Заключение. Исследования в области стеганографии – перспективное направление защиты информации, так как в современном мире задача передачи секретной информации стоит наравне со скрытым общением, т.е. скрытия факта передачи сообщений. Поэтому необходимо продолжать исследованиями в этой области для поиска новых, эффективных, методов или улучшения существующих. В данной работе был 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. Программный продукт реализован и готов к использованию с возможностью доработки.

ЛИТЕРАТУРА

1. 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.
2. Садов, В.С. Компьютерная стеганография / В.С. Садов. – М. : МГВРК, 2012. – 289 с.
3. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин. – М. : СОЛОН-Пресс, 2002. – 272 с.