Реализация пакета программ для встраивания и извлечения скрытых сообщений в аудиофайлах

А. А. Жарких[1]***, А. В. Горбунов***[2]
zharkikh090107@mail.ru; lergex@gmail.com
[1]Мурманский государственный технический университет
Россия, г. Мурманск, ул. Спортивная, 13
[2]МФ ФГБУ «Центр системы мониторинга рыболовства и связи»
Россия, г. Мурманск, ул. Траловая, 43

Представлены результаты разработки пакета программ для встраивания, извлечения, обнаружения и прочтения сообщений в аудиофайлах. Методология работы и программная реализация относятся к стеганографии — одному из основных направлений защиты информации. Стегоконтейнер представляет собой аудиофайл, получаемый в результате модификации контейнера последовательностью бит сообщения. Контейнер и стегоконтейнер представляют собой последовательности отсчетов импульсно-кодовой модуляции (ИКМ), а встраивание осуществляется простым суммированием отсчетов контейнера с отсчетами сигнала сообщения. Сигнал сообщения модулируется методом двоичной дискретной частотной манипуляции (ЧМ; английский термин — frequency shift keying, FSK), а контейнер перед встраиванием подвергается режекторной фильтрации. И методология, и пакет программ являются основой построения стеганографических систем со скачками по частоте (СЧ) и с вариацией просодических параметров речи.

Ключевые слова: *защита информации; стеганография; аудиосигналы; обнаружение сигналов; различение сигналов*

DOI: 10.21469/22233792.2.4.02

1 Введение

Цель данной работы — описание стеганографического метода, алгоритмов его реализации и программных средств для встраивания и извлечения. Метод базируется на модификации вектора отсчетов аудиосигнала, представленного в формате ИКМ. Сообщение представляет собой вектор отсчетов сигнала, полученного путем двоичной ЧМ из вектора бит сообщения.

Стеганография отличается от криптографии. Криптография изучает методы защиты информации, при которых допускается модификация сообщений (шифрование), стеганография же изучает методы защиты информации, в которых сообщение не изменяется (не шифруется), зато скрывается сам факт ее наличия. В стеганографии можно отметить три следующих основных раздела: методы встраивания сообщений в контейнеры; методы извлечения сообщений из контейнера; стегоанализ.

Наименее проработанная область исследования стеганографии — стегоанализ. Стегоанализ — это раздел стеганографии, который представляет собой совокупность методов обнаружения, различения и прочтения сообщений в различных контейнерах любой природы [1–7].

Необходимость обнаружения скрытых вложений может быть вызвана различными причинами. Данные средств массовой информации указывают, что зачастую стегосистемы разрабатываются организованной преступностью и террористами для решения своих незаконных задач (создание скрытых каналов связи, каналов утечки конфиденциальной информации) [8, 9]. В этом случае стегоанализ таких систем решает задачи, позитивные для

общества. Стегоанализ проводится с целью обнаружения, различения, прочтения и определения скрытых сообщений для предотвращения противоправной деятельности. Также одним из направлений применения стегоанализа является стегоанализ разработчиков стегосистем. Важным показателем стегосистемы является устойчивость при различных атаках нелегальных пользователей, а также воздействия дефектов носителей и помех в каналах передачи. Данное направление используется разработчиками легальных стегосистем для оценки их устойчивости к обнаружению, различению, прочтению и определению смысла скрываемого сообщения.

В настоящее время в направлении науки, посвященном методам стеганографии работают многие отечественные и зарубежные ученые: В. Г. Грибунин, И. Н. Оков, Б. Я. Рябко, И. В. Туринцев, А. В. Аграновский, А. Н. Фионов, В. Бендер (W. Bender), Н. Моримото (N. Morimoto) и др. В данной работе авторы описывают опыт разработки пакета программ, реализующего алгоритмы встраивания, извлечения и обнаружения сообщений в аудиофайлах. Работа сдержит три основных раздела.

В первом разделе формулируются требования к программному средству, реализующему извлечение и обнаружение произвольной структуры в аудиофайлах. Обоснован формат сообщения и аудиофайла контейнера.

Во втором разделе описана структура аудиофайла контейнера, скрываемого сообщения, а также методы встраивания извлечения и обнаружения, лежащие в основе программного средства.

В третьем разделе описана архитектура программных средств и их функциональные возможности.

В заключении отмечены перспективы развития и использования как рассмотренных методов, так и созданного пакета программ.

2 Постановка задачи и требования к программному средству

Необходимо выбрать метод встраивания, и для выбранного метода встраивания должен быть реализован метод обнаружения. Для этого нужно разработать с помощью пакета MATLAB функцию, реализующую встраивание скрытых сообщений в аудиофайлы формата wav. Также должно быть разработано программное средство на языке высокого уровня, предназначенное для обнаружения скрытых вложений различного типа в аудиофайлы различной структуры.

Пользователю предлагается некоторый аудиофайл формата wav. Необходимо определить, содержится ли в аудиофайле некоторое скрытое сообщение. Обнаружение ведется «полуслепым» методом, т. е. предполагается, что известна некоторая дополнительная информация о стегосистеме:

1) метод встраивания;
2) параметры метода встраивания (все или несколько).

При всех известных ключевых параметрах программа должна позволить пользователю прочесть скрытое сообщение. Если содержание скрытого сообщения известно пользователю, программа должна, при заданных параметрах обнаружения, определять долю правильно обнаруженных и необнаруженных бит, а также неправильно обнаруженных и необнаруженных бит сообщения.

2.1 Требования к структуре и функционированию

Структура программного средства должна быть модульной. Функциональная структура средства должна включать следующие модули:

– модуль извлечения;
– модуль обнаружения;
– модуль воспроизведения. Позволяет проигрывать файл-контейнер как аудиофайл. Используется для субъективной оценки качества встраивания;
– модуль справки. Выводит справочную информацию;
– модуль обработки ошибок. Обрабатывает исключения.

Программное средство должно допускать наращивание функциональных возможностей. Пользовательский интерфейс должен быть графическим и обеспечивать удобную и простую навигацию в диалоге с пользователем. Необходимо наличие справки (помощи). Программа должна функционировать под операционной системой Windows Vista/7/8/10, так как данная операционная система является наиболее распространенной среди пользователей персональных компьютеров. Необходим установленный в системе Microsoft .NET Framework 4.5.

2.2 Требования к оборудованию

К оборудованию предъявляются следующие требования:

– процессор с тактовой частотой 1 ГГц или выше;
– опретивное запоминающее устройство объемом 512 МБ;
– 50 МБ доступного пространства на жестком диске;
– Наличие звуковой карты (необязательно).

Основным языком взаимодействия пользователей и системы является русский язык. Графический интерфейс пользователя должен быть создан на русском языке.

3 Метод встраивания сообщений в ИКМ — отсчеты аудиосигнала с использованием двухпозиционной частотной манипуляции

Цифровая запись аудиосигналов базируется на выполнении двух операций над аналоговыми сигналами: дискретизации и квантования. В реальных устройствах эти операции осуществляются одновременно. В результате дискретизации аналоговый аудиосигнал заменяется последовательностью отсчетов, а в результате квантования каждый отсчет заменяется последовательностью бит. В итоге исходный аналоговый сигнал заменяется массивом целых чисел, каждое из которых ограничено числом разрядов, равным числу бит квантования.

Для восстановления аналоговой формы сигнала кроме данного массива необходимо знать число уровней квантования и интервал дискретизации.

Часто цифровое представление аудиосигнала называют импульсно-кодовой модуляцией аудиосигнала [10–12]. Это связано с тем, что грубую копию аудиосигнала можно представить как последовательность прямоугольных импульсов одинаковой длительности равной интервалу дискретизации, при этом амплитуда текущего импульса равна текущему значению элемента массива цифровой записи.

Авторы предлагают использовать массив отсчетов аудиосигналов как контейнер для встраивания сообщений.

В следствие разнообразия приложений, скрываемые сообщения могут иметь различную природу и структуру, поэтому договоримся далее, что любое сообщение перед вложением в контейнер преобразуется просто в последовательность бит. Единственное ограничение, предъявляемое к данной последовательности, — это число ее элементов, которое ограничивается емкостью контейнера и для различных методов встраивания может оказаться различным.

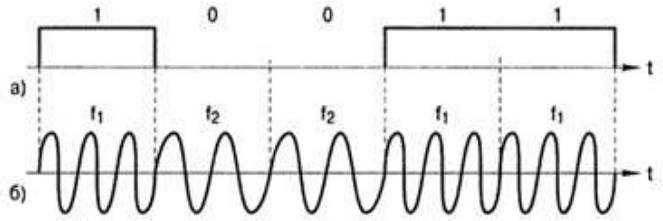

Рис. 1 Форма сигнала при ЧМ: (*а*) манипулирующий сигнал; (*б*) частотно-манипулирующий сигнал — радиосигнал ЧМ

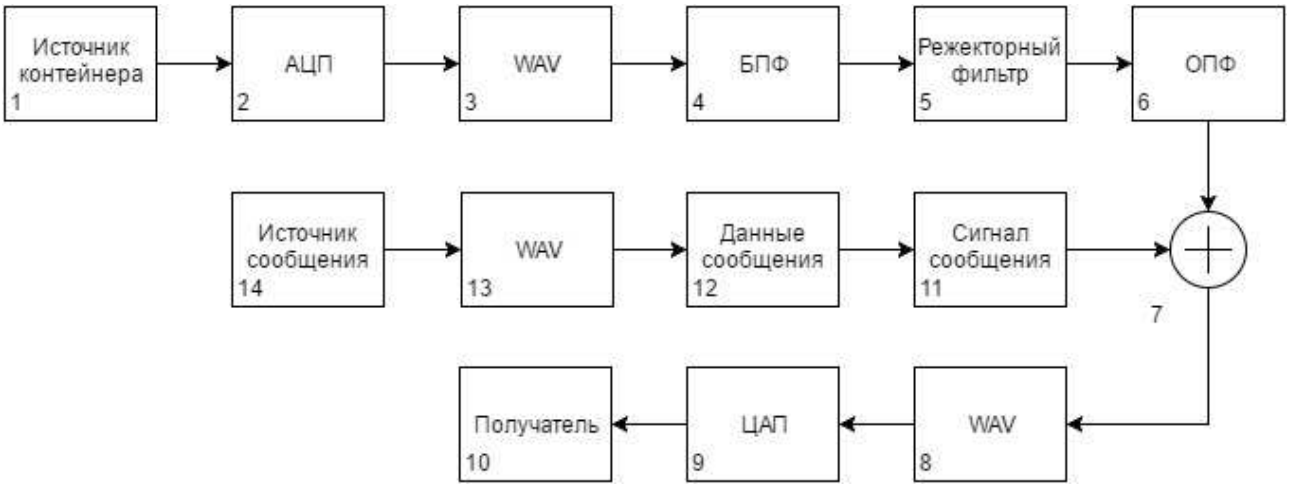

Рис. 2 Структурная схема алгоритма встраивания

При ЧМ каждому возможному значению передаваемого символа сопоставляется своя частота (рис. 1). В течение каждого символьного интервала передается гармоническое колебание с частотой, соответствующей текущему символу [13].

Алгоритм метода встраивания можно представить 14 блоками (рис. 2).

Структурная схема содержит следующие блоки:

1) источник контейнера;
2) аналого-цифровой преобразователь (АЦП);
3) формирователь wav файла контейнера;
4) блок быстрого преобразования Фурье (БПФ);
5) режекторный фильтр;
6) блок обратного преобразования Фурье (ОПФ);
7) сумматор;
8) формирователь wav файла стегоконтейнера;
9) цифроаналоговый преобразователь (ЦАП);
10) получатель данных;
11) сигнал сообщения;
12) данные сообщения;
13) отсчеты сообщения;
14) источник сообщения.

Блок 1 — источник контейнера, т. е. аудиосигнал, имеющий аналоговую форму. Из блока 1 сигнал поступает в блок 2, который представляет собой АЦП. На выходе бло-

ка 2 получается цифровой сигнал. Существует блок 3, который записывает выход из блока 2 в wav файл без сжатия. Из блока 3 данные поступают в блок 4, где осуществляется БПФ. Результат преобразования Фурье передается на блок 5, который представляет собой режекторный фильтр, вырезающий часть спектральной составляющей из спектра сигнала-контейнера. Результат преобразования контейнера подается на устройство 6 — ОПФ. Далее в сумматоре 7 осуществляется сложение контейнера и сообщения.

Формирование сигнала сообщения начинается в блоке 14. Блок 14 представляет собой источник битов сообщения. Источник битов сообщения преобразуется в некоторый набор отсчетов сигнала. Этот набор отсчетов объединяется в блоке 12 с данными о контейнере, полученными в блоке 5. Объединенные данные из блока 12 используются для формирования сигнала сообщения в блоке 11. Сигнал сообщения поступает на сумматор 7, где складывается с контейнером, поступающим с блока 5, как было сказано ранее. Результат суммирования подается в блок 8, где формируется файл стегоконтейнера с расширением wav. При необходимости воспроизведения стегоконтейнера в целом файл с устройства 8 преобразуется в ЦАП 9 и далее воспринимается получателем 10.

Сам алгоритм встраивания можно описать следующим образом. Аудиофайл-контейнер разбивается на отрезки, содержащие число отчетов, кратное степени двойки. Производится преобразование Фурье отрезка. Для встраивания данных используются узкие полосы частот вблизи выбранных частот. Для этих узких полос оценивается энергия, исходя из которой выбирается амплитуда модулированного скрываемого сообщения.

Модулированное сообщение формируется следующим образом:

1) выбираются две частоты, лежащие внутри полос встраивания;
2) оценивается длительность встраивания одного бита сообщения — в это время должно уложиться несколько периодов частоты встраивания;
3) формируется добавочное сообщение: встраиваемой единице соответствует колебание нижней частоты из полосы встраивания, а нулю — верхней частоты из полосы встраивания;
4) амплитуда модулированного сообщения выбирается такой, чтобы энергия встраиваемого сообщения соответствовала энергии контейнера в полосе встраивания.

После формирования сообщения полосы встраивания режектируются из спектра исходного отрезка и производится ОПФ. Далее полученные отсчеты суммируются с отсчетами модулированного сообщения. Ширина полос встраивания, а также частоты встраивания оцениваются исходя из требуемой скорости передачи бит скрываемого сообщения, а также из соображений незаметности встраивания.

На рис. 3 представлена структурная схема алгоритма метода, в котором происходит извлечения сообщения.

Структурная схема содержит следующие блоки:

1) источник стего;
2) АЦП;
3) формирователь wav файла стегоконтейнера;
4) блок БПФ;
5) полосовой фильтр;
6) блок ОПФ;
7) блок формирования сигнала сообщения;
8) данные о сообщении;
9) отсчеты файла сообщения;

Рис. 3 Структурная схема алгоритма извлечения

10) получатель отсчетов сообщения.

Для извлечения скрытого сообщения необходимо знать длину отрезка встраивания, частоту встраивания, а также ширину полос встраивания. Аудиофайл-стегоконтейнер также разбивается на отрезки известной длины и производится БПФ. Анализируются полосы частот вблизи полос встраивания. Полосы встраивания отфильтровываются, и производится ОПФ полученного узкополосного сигнала. Таким образом получаем модулированное сообщение. Далее оценивается длительность передачи одного бита сообщения. Модулированное сообщение разбивается на отрезки передачи одного бита, внутри каждого из которых оценивается частота и по этой частоте принимается решение о переданном бите. Таким образом принимается скрываемое сообщение.

Прием частотно-манипулированного сигнала осуществляется корреляционным методом. Корреляционный прием может быть когерентным или некогерентным. В данной работе используется когерентный прием. Он используется, если известны начальные фазы посылок. Его принцип состоит в вычислении взаимной корреляции между принимаемым сигналом и колебаниями-образцами (опорными сигналами), представляющими собой гармонические колебания с используемыми для манипуляции частотами.

Взаимная корреляция сигнала с k-м опорным сигналом для n-го по времени символа рассчитывается следующим образом:

$$u_k(n) = \int\limits_{nT}^{(n+1)T} s(t)\cos(\omega_k t + \varphi_{0k})\,dx,$$

где $s(t)$ — частотно-манипулированный сигнала; ω_k — частота манипуляции, соответствующая символу, равному k; φ_{0k} — начальная фаза посылки; T — длительность передачи символа.

Использованные пределы интегрирования задают обработку n-го символа. При программной реализации демодуляции частотно-манипулированного сигнала вместо интегрирования необходимо использовать суммирование дискретных отсчетов подынтегрального выражения [13].

Схема обнаружителя приведена на рис. 4. Сигнал сообщения $s(t)$ перемножается с опорными сигналами для нулевого $\cos(\omega_0 t + \varphi_0)$ и единичного $\cos(\omega_1 t + \varphi_1)$ битов. Затем результаты интегрируются (суммируются) и поступают в блок сравнения. В этом бло-

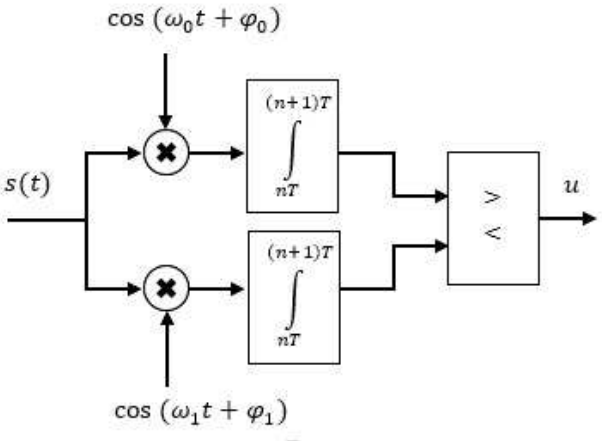

Рис. 4 Структурная схема обнаружения

ке полученные суммы сравниваются с пороговым значением. Порог выбирается с учетом энергии опорного сигнала и составляет его половину.

Энергия сигнала для нулевого бита:

$$E_{s_0} = \sum_{k=0}^{T} S_{0_k}^2 \Delta t = \frac{A_0^2 T}{2},$$

где S_{0_k} — значение сигнала нулевого бита в k-м отсчете; T — длительность одного бита; Δt — приращение отсчетов; A_0 — амплитуда сигнала.

Энергия сигнала для бита, равного единице:

$$E_{s_1} = \sum_{k=0}^{T} S_{1_k}^2 \Delta t = \frac{A_1^2 T}{2},$$

где S_{1_k} — значение сигнала бита равного единице в k-м отсчете; A_1 — амплитуда сигнала.

Пороговые значения, таким образом составляют $E_{s_0}/2$ и $E_{s_1}/2$ для бита «0» и бита «1» соответственно. Решение об обнаруженном бите в блоке сравнения принимается исходя из следующего алгоритма:

1) если сумма для бита 0 больше своего порогового значения, а сумма бита 1 меньше своего, то считается, что встроен бит 0;
2) если сумма для бита 1 больше своего порогового значения, а сумма бита 0 меньше своего, то считается, что встроен бит 1;
3) если суммы для обоих битов меньше их порогов, то делается вывод, что встраивания не было;
4) если суммы для обоих битов больше своих пороговых значений, то выбирается бит, сумма которого больше.

Таким образом на выходе обнаружителя формируется цепочка из нулей, единиц и символа «N» — отсутствия встраивания.

4 Архитектура программного средства

На основании изложенных в разд. 3 алгоритмов были разработаны функция в пакете MATLAB, осуществляющая встраивание, а также программное средство на языке C#,

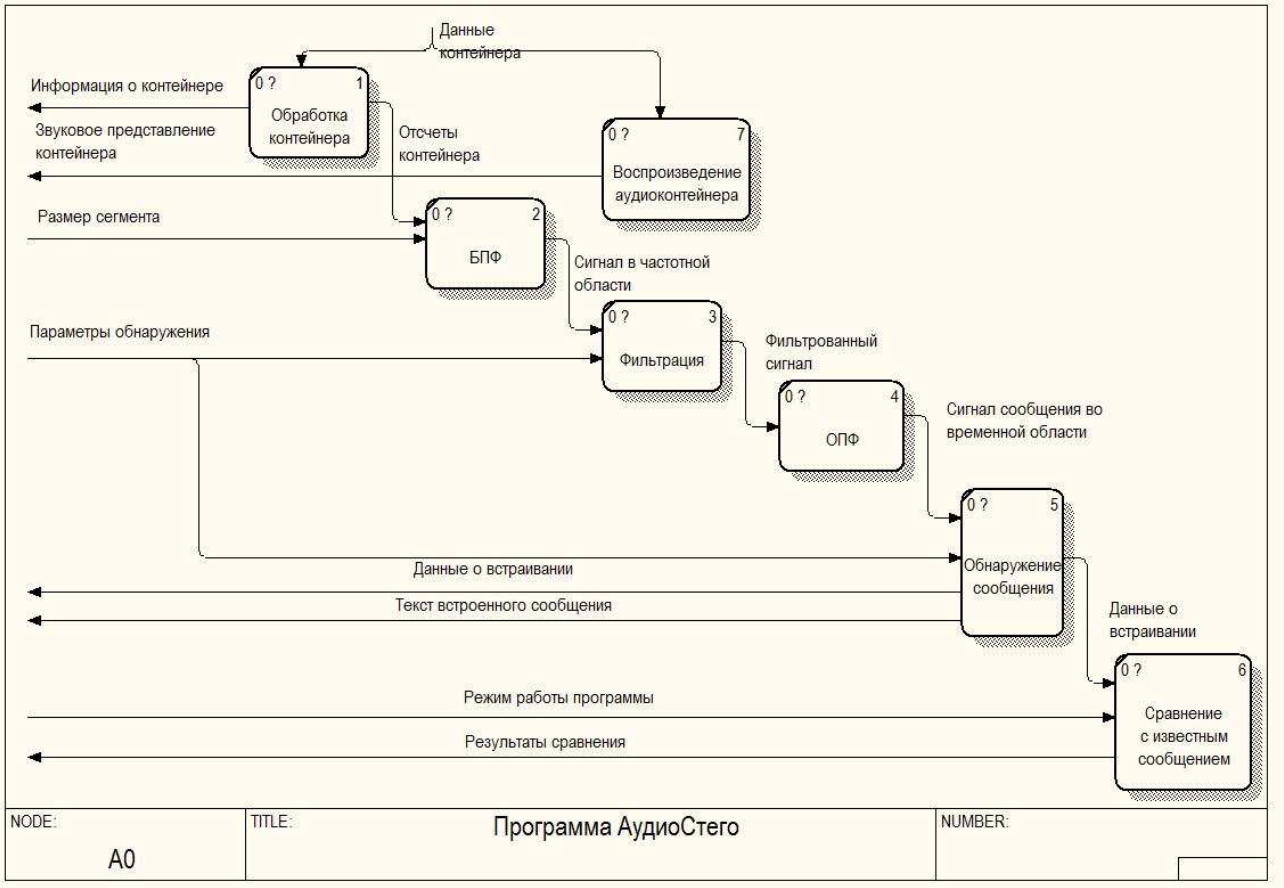

Рис. 5 Контекстная диаграмма потоков данных программы обнаружения

позволяющее обнаруживать скрытые методом на основе двухпозиционной ЧМ вложения в аудиофайле.

Функция встраивания позволяет осуществлять скрытие в контейнере произвольного (ограниченного емкостью контейнера) массива битов сообщения. Для этого задается аудиофайл-контейнер и выбираются параметры встраивания, такие как длина сегмента, частоты нулевого и единичного бита, длительность одного бита. На выходе получается стегоконтейнер в формате wav, содержащий сообщение.

Структурная схема программы для обнаружения в виде контекстной диаграммы потоков данных приведена на рис. 5.

Эта диаграмма содержит 7 процессов:

1) обработка контейнера — включает чтение с диска аудиофайла-контейнера, чтение и интерпретацию его заголовочной информации, определение формата хранения отсчетов сигнала, преобразование их в числа с плавающей точкой двойной точности;
2) БПФ — производит БПФ для последующей фильтрации сигнала в частотной области;
3) фильтрация — применяет к результату предыдущего процесса полосно-пропускающий фильтр, выделяя тем самым предполагаемый сигнал скрытого сообщения;
4) ОПФ — переводит сигнал сообщения из предыдущего процесса во временную область;
5) обнаружение сообщения — производит обнаружение битов скрытого сообщения в соответствии с заданными пользователем параметрами. Возвращает информацию о встраивании и, если возможно, текстовое представление полученного сообщения;

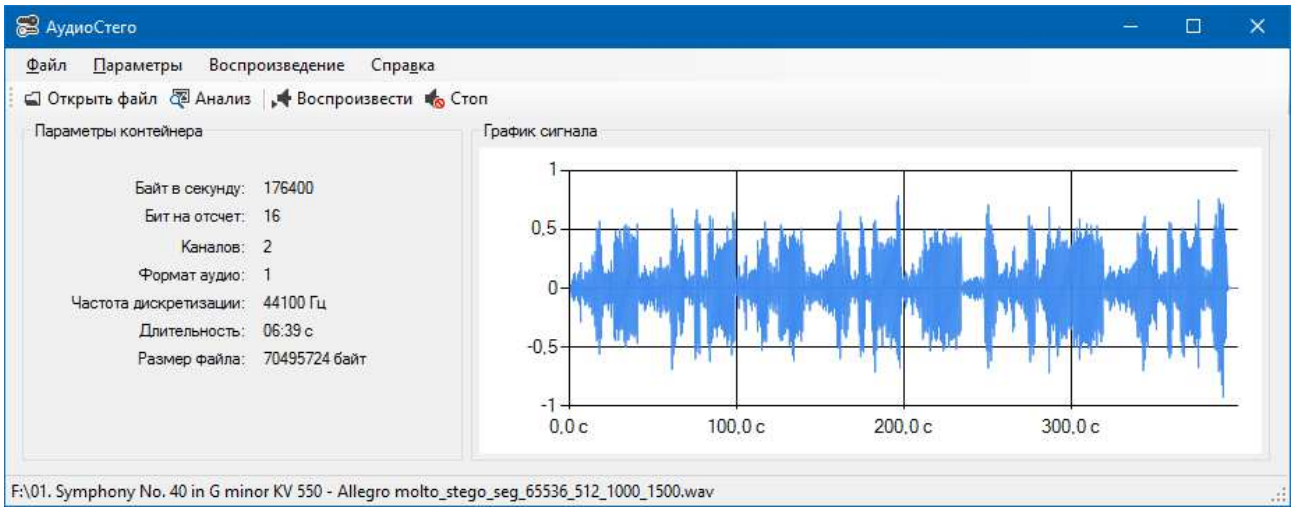

Рис. 6 Главное окно программы

6) сравнение с известным сообщением — сравнивает полученное сообщение с известным и выводит результаты оценки правильности обнаружения;
7) воспроизведение аудиоконтейнера — проигрывает аудиофайл.

К входной информации для программного средства относятся различные параметры, определяемые пользователем, а также аудиофайл — потенциальный стегоконтейнер. Параметры обнаружения включают в себя значения:

1) амплитуды;
2) частоты нуля;
3) частоты единицы;
4) длительности 1 бита;
5) порога обнаружения.

К выходной информации относятся информация о контейнере, результаты работы алгоритма обнаружения, текстовое представление обнаруженного сообщения. Для тестового режима работы программы дополнительно выводятся результаты сравнения с известным сообщением. Имеется возможность воспроизвести и прослушать открытый аудиофайл.

Текст встроенного сообщения представляет собой строковое представление полученного скрытого сообщения в кодировке windows-1251. Данные о встраивании состоят из информации по общему количеству бит, количеству встроенных бит, количеству бит без встраивания, а также числу нулевых и единичных битов.

Результаты сравнения содержат сравнительные оценки результатов обнаружения. К этим оценкам относятся количество правильно необнаруженных бит, правильно обнаруженных и различенных бит, правильно обнаруженных, но неправильно различенных бит, а также количество ложных обнаружений и ложных необнаружений.

Главное окно программы изображено на рис. 6. Здесь отображается основная информация о контейнере: количество каналов, частота дискретизации, продолжительность звучания, размер и другие параметры, а также графическое представление сигнала выбранного канала.

Окно «Стегоанализ» используется для анализа открытого контейнера (рис. 7).

В этом окне пользователем задаются основные параметры для обнаружения вложения. После выполнения процедуры обнаружения выводится статистика по общему количеству

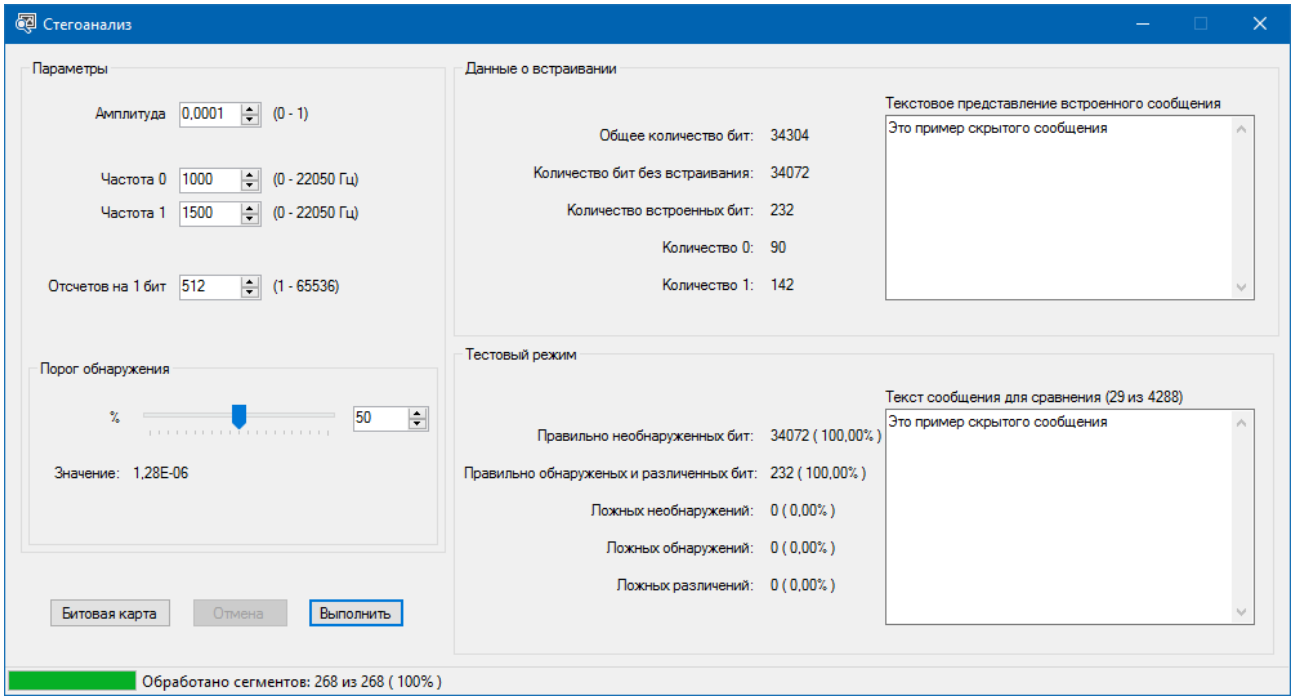

Рис. 7 Окно «Стегоанализ»

бит, количеству встроенных бит, количеству бит без встраивания, а также числу нулевых и единичных битов. В текстовое поле выводится строковое представление обнаруженного встроенного сообщения. При известном содержании скрытого сообщения после исполнения программа отобразит сравнительные оценки результатов обнаружения. К таким оценкам относятся количество правильно необнаруженных бит, правильно обнаруженных и различенных бит, правильно обнаруженных, но неправильно различенных бит, а также количество ложных обнаружений и ложных необнаружений.

5 Заключение

Завершая вышесказанное, отметим основные результаты работы.

Был создан пакет программ, который в широком диапазоне параметров аудиофайла и различных вариантов сообщений позволяет осуществлять встраивание, извлечение, обнаружение и прочтение сообщений в аудиофайлах.

Данный пакет по сути является виртуальной экспериментальной установкой для исследования различных характеристик стеганографических систем, использующих аудиофайлы-контейнеры. Он может быть использован по прямому назначению, т. е. для реализации всех четырех перечисленных функций, а также в учебном процессе по дисциплинам, связанным с защитой информации. Авторы полагают, что он также является весьма перспективным для научных направлений, таких как стеганография, интеллектуальный анализ данных и распознавание образов. По меньшей мере можно указать следующие перспективные области применения изложенных в работе методов и реализованного программного средства:

– методика стеганографии со скачками по частоте [14];
– методика стеганографии с модификацией просодических параметров речи [15];
– статистическая теория распознавания образов [16].

Литература

[1] *Bender W., Gruhl B., Morimoto N., Lu A.* Techniques for data hiding // IBM Syst. J., 1996. Vol. 35. № 3.

[2] *Чваркова И. Л.* Стеганографические методы скрытия информации в аудиоданных // Электроника, 2003. № 11. С. 54–56.

[3] *Романцов А. П., Бугаев В. С., Фролов М. А.* Комплекс лабораторных работ по стеганографии / Под ред. Заслуженного деятеля науки РФ д.т.н. проф. А. В. Петракова. — М.: РИО МТУСИ, 2005. 92 с.

[4] *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. — Киев: МК-Пресс, 2006. 288 с.

[5] *Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А.* Стеганография, цифровые водяные знаки и стеганоанализ. — М.: Вузовская книга, 2009. 220 с.

[6] *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. — М.: Солон-Пресс, 2009. 265 с.

[7] *Гурин А. В., Жарких А. А., Пластунов В. Ю.* Технологии встраивания цифровых водяных знаков в аудиосигнал / Под общ. ред. А. А. Жарких. — М.: Горячая линия — Телеком, 2015. 116 с.

[8] *Kelley J.* Terror groups hide behind Web encryption // USA Today, 2001. `http://usatoday30.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm`.

[9] *Fox S.* FBI: Russian spies hid codes in online photos // NBC News, 2010. `http://www.nbcnews.com/id/38028696/ns/technolog_and_science-science/t/fbi-russian-spies-hidcodes-online-photos`.

[10] *Евсеев А. И., Сорокин П. М., Кончаловский В. Ю.* Преобразование непрерывных сигналов в дискретные // Передача информации. `http://peredacha-informacii.ru`.

[11] *Котельников В. А.* О пропускной способности эфира и проволоки в электросвязи — Всесоюзный энергетический комитет // Мат-лы к I Всесоюзному съезду по вопросам технической реконструкции дела связи и развития слаботочной промышленности, 1933. Репринт. УФН, 2006. Т. 176. № 7. С. 762–770.

[12] *Радзишевский А. Ю.* Основы аналогового и цифрового звука. — М.: Вильямс, 2006. 288 с.

[13] *Сергиенко А. В.* Цифровая обработка сигналов. — СПб.: Питер, 2002. 608 с.

[14] *Torrieri D.* Principles of spread-spectrum communication systems. — Boston, MA, USA: Springer Science, 2005. 456 p.

[15] *Потапова Р. К.* Речь: коммуникация, информация, кибернетика. — 4-е изд., доп. — М.: ЛИБРИКОМ, 2010. 594 с.

[16] *Фукунага К.* Введение в статистическую теорию распознавания образов / Пер. с англ. — М.: Наука, 1979. 368 с. (*Fukunaga K.* Introduction to statistical pattern recognition. — New York, NY, USA: Academic Press, 1972. 250 p.)

Поступила в редакцию 29.08.2016

Implementation of the software package for embedding and extracting hidden messages in audiofiles

A. A. Zharkikh[1] ***and A. V. Gorbunov***[2]
zharkikh090107@mail.ru; lergex@gmail.com
[1]Murmansk State Technical University, 13 Sportivnaya Str., Murmansk, Russia
[2]Murmansk Branch SO CFMC, 43 Tralovaya Str., Murmansk, Russia

The results of development of a software for embedding, extraction, detection, and reading of messages in audiofiles are provided. The methodology of work and program implementation belong to a steganography — one of the main directions of information security. Stegocontainer represents the audiofile received as a result of modification of a container by the sequence of bits of the message. A container and a stegocontainer represent the sequences of counting of the pulse code modulation, and embedding is performed by simple summing of counting of a container with counting of a signal of the message. The signal of the message is modulated by the method of binary discrete frequency manipulation, and the container before embedding is exposed to rejection filtering. Both the methodology and the software are a basis for steganography systems with frequency hopping and with a variation of prosodic parameters of the speech creation.

Keywords: *information security; steganography; audio signals; signals detection; signals distinction*

DOI: 10.21469/22233792.2.4.02

References

[1] Bender, W., B. Gruhl, N. Morimoto, and A. Lu. 1996. Techniques for data hiding. *IBM Syst. J.* 35(3).

[2] Chvarkova, I. L. 2003. Steganograficheskie metody skrytiya informatsii v audiodannykh [Steganographic techniques to hide information in the audio data]. *Elektronika* [Electronics] 11:54–56.

[3] Romantsov, A. P., V. S. Bugaev, and M. A. Frolov. 2005. *Kompleks laboratornykh rabot po steganografii* [Complex laboratory works on steganography]. Moscow: RIO MTUSI. 92 p.

[4] Konakhovich, G. F., and A. Yu. Puzyrenko. 2006. *Komp'yuternaya steganografiya. Teoriya i praktika* [Computer steganography. Theory and practice]. Kiev: MK-Press. 288 p.

[5] Agranovskiy, A. V., A. V. Balakin, V. G. Gribunin, and S. A. Sapozhnikov. 2009. *Steganografiya, tsifrovye vodyanye znaki i steganoanaliz* [Steganography, digital watermarking, and steganalysis]. Moscow: Vuzovskaya kniga. 220 p.

[6] Gribunin, V. G., I. N. Okov, and I. V. Turintsev. 2009. *Tsifrovaya steganografiya* [Digital steganography]. Moscow: Solon-Press. 265 p.

[7] Gurin, A. V., A. A. Zharkikh, and V. Yu. Plastunov. 2015. *Tekhnologii vstraivaniya tsifrovykh vodyanykh znakov v audiosignal* [Technology of embedding digital watermarks into audiosignal]. Moscow: Goryachaya liniya — Telekom. 116 p.

[8] Kelley, J. 2001. Terror groups hide behind Web encryption. *USA Today*. Available at: `http://usatoday30.usatoday.com/life/cyber/tech/2001-02-05-binladen.htm` (accessed December 28, 2016).

[9] Fox, S. 2010. FBI: Russian spies hid codes in online photos. *NBC News*. Available at: `http://www.nbcnews.com/id/38028696/ns/technology_and_science-science/t/fbi-russian-spies-hidcodes-online-photos` (accessed December 28, 2016).

[10] Evseev, A. I., P. M. Sorokin, and V. Yu. Konchalovskiy. Preobrazovanie nepreryvnykh signalov v diskretnye [Convert continuous signals to discrete]. — Peredacha informatsii [Transmission of information]. Available at: `http://peredacha-informacii.ru` (accessed December 28, 2016).

[11] Kotel'nikov, V. A. 2006. O propusknoy sposobnosti efira i provoloki v elektrosvyazi [On the transmission capacity of "ether" and wire in electrocommunications]. *Mat-ly k I Vsesoyuznomu s"ezdu po voprosam tekhnicheskoy rekonstruktsii dela svyazi i razvitiya slabotochnoy promyshlennosti, 1933* [1st All-Union Conference on the Technological Reconstruction of the Communications Sector and the Development of Low-Current Engineering Proceedings]. Reprint. *UFN* 176(7):762–770.

[12] Radzishevskiy, A. Yu. *Osnovy analogovogo i tsifrovogo zvuka* [Foundations of analog and digital audio]. Moscow: Vil'yams. 288 p.

[13] Sergienko, A. V. 2002. *Tsifrovaya obrabotka signalov* [Digital signal processing]. SPb.: Piter. 608 p.

[14] Torrieri, D. 2005. *Principles of spread-spectrum communication systems*. Boston, MA: Springer Science. 456 p.

[15] Potapova, R. K. 2010. *Rech': Kommunikatsiya, informatsiya, kibernetika* [Speech: Communication, information, cybernetics]. Moscow: LIBRIKOM. 594 p.

[16] Fukunaga, K. 1972. *Introduction to statistical pattern recognition*. New York, NY: Academic Press. 250 p.

Received August 29, 2016