ПОРТФЕЛЬ РЕДАКЦИИ

БИТ

А. А. Аленин, А. П. Алексеев

ИССЛЕДОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ ВЛОЖЕНИЙ В ЗВУКОВЫХ ФАЙЛАХ ФОРМАТА WAV

1. Постановка задачи

В настоящее время нередко наблюдаются случаи несанкционированного использования мультимедийной продукции (фотографий, аудио- и видеофайлов). Одним из приемов защиты авторских прав является скрытое внедрение меток (маркеров, водяных знаков) в защищаемые мультимедийные файлы. Обнаружение этих меток позволяет нарушителю удалить водяные знаки из контейнера. Очевидно, что внедрение скрываемой информации в мультимедийные файлы следует осуществлять таким образом, чтобы нарушитель не смог обнаружить и удалить сделанные изменения в контейнере.

В статье рассматриваются методы обнаружения вложений в звуковых файлах формата WAV и алгоритм работы программ, которые построены на базе результатов исследований.

2. Экспертная оценка слышимости искажений контейнера

Файл формата WAV содержит в себе квантованные цифровые значения амплитуды сигнала, измеренные в дискретные моменты времени (так называемые отсчеты). Для файла формата WAV наиболее известным и распространенным методом сокрытия секретной информации является метод замены наименьшего значащего бита (НЗБ) [1].

При внедрении информации в звуковые файлы формата WAV методом НЗБ приходится решать задачу выбора номера разряда отсчета, в который можно поместить скрываемую информацию, с учетом двух конфликтующих требований. С одной стороны, необходимо увеличивать объем скрываемой информации в одном файле (увеличивать пропускную способность канала), а с другой стороны, нужно обеспечить высокую степень скрытности вложенной информации.

Для решения этой задачи была проведена экспертная оценка слышимости искажений в зависимости от номера разряда отсчета, в который происходило внедрение скрываемой информации. Очевидно, что заметные искажения звукового сигнала позволяют обнаружить вложение, а затем его удалить.

При проведении экспериментальных исследований учитывались требования, перечисленные в [2]. Для исследования были подготовлены 15 файлов с записью информации в различные разряды отсчетов (от младшего разряда до предпоследнего старшего разряда). Исходный файл содержал запись «полной тишины» (фрагмент mn на рисунке 1), и он искажался поочередной записью информации в различные разряды.

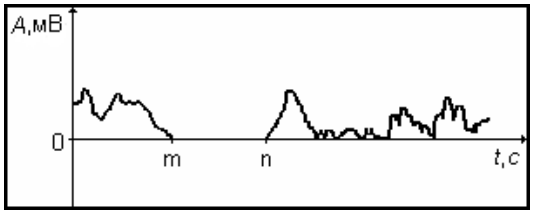


Рис. 1. Звуковой сигнал с участком «полной тишины»

Запись внедряемой информации в каждый файл производилась следующим образом: в четные отсчеты записывался логический нуль, а в нечетные отсчеты записывалась логическая единица.

Восемнадцать экспертов (в возрасте 18–19 лет) оценивали громкость звучания предъявленных файлов по пятибалльной шкале (от 0 до 4). Наибольшей громкости звучания соответствовал балл 4, а файлу без вложения («полная тишина») соответствовал балл 0. При прослушивании (тестировании) каждого файла для сравнения воспроизводились файл с записью «полной тишины» и файл с записью битов, скрытых в младшем разряде.

При обработке экспериментальных данных вычислялись среднее арифметическое значение громкости звучания для каждого файла и дисперсия. Значение дисперсии находилось в пределах 3–12 % от среднего арифметического значения громкости звучания и позволяло контролировать наличие промахов при проведении исследований. При этом одну запись (с использованием правил статистической обработки данных) пришлось удалить, определив ее как промах (ошибку) эксперта.

Результаты экспертной оценки громкости звучания указанных файлов приведены на рисунке 2. По горизонтали отложены номера разрядов отсчетов, в которые производилось внедрение информации, а по вертикали — громкость звучания, выраженная в баллах.

На рисунке 2 младшему разряду отсчета соответствует номер $n = 16$.

Экспериментально полученные данные были аппроксимированы логистической функцией:

$$g = a + \frac{b}{1 + \left(\frac{n}{c}\right)^d},$$

где g — громкость звучания, выраженная в баллах; n — номер разряда, в который происходило внедрение скрываемой информации; коэффициенты аппроксимации:

$a = -0{,}165$; $b = 5{,}504$; $c = 3{,}25$; $d = 2{,}325$.

Исследования показали, что для скрытой передачи информации можно использовать 2 младших разряда отсчетов звукового контейнера. При этом уловить на слух наличие внедренной информации невозможно.

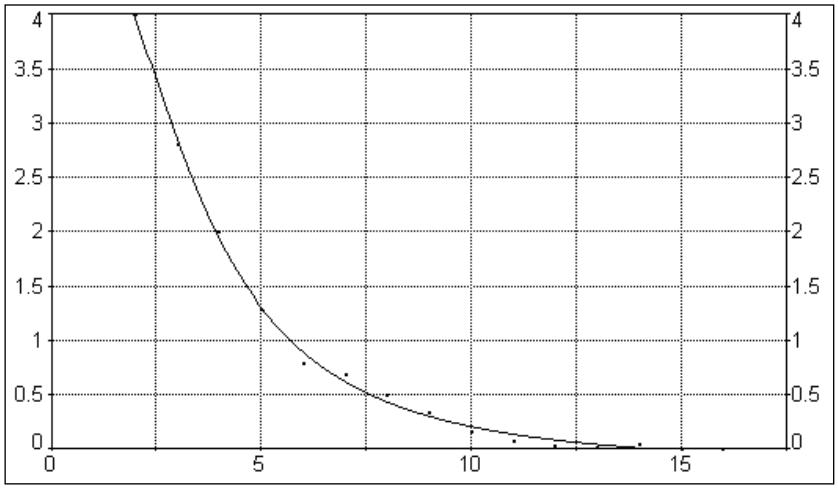


Рис. 2. Результаты экспертной оценки слышимости вложений

3. Визуальная оценка искажения синусоидального сигнала

Проверка полученной выше оценки слышимости искажений (другими словами, возможности обнаружения вложений) была проведена визуально с помощью звукового редактора Audacity 1.3. Для этого исследовались искажения спектра синусоидального сигнала в зависимости от номера разряда, выбранного для внедрения.

Синусоидальный сигнал был сформирован с помощью программы MATLAB R2008a.

Временной интервал длительностью 10 секунд с шагом 1/44100 задавался в следующем виде:

t = 0:1/44100:10.

Для генерации синусоидального сигнала с частотой 1350 Гц была использована функция:

x = 0.5**sin*(1350**t*).

Частота 1350 Гц была выбрана потому, что на этой частоте чувствительность слуха человека наивысшая.

Генерация звукового файла формата WAV с частотой дискретизации 44100 Гц и уровнем квантования 16 бит осуществлялась с помощью функции:

wavwrite(x,44100,16,'c:\sin.wav').

Частота дискретизации 44100 Гц была выбрана по той причине, что она обеспечивает качество звучания фонограммы, сопоставимое с качеством звучания музыкальных произведений, записанных на CD-дисках.

Информация внедрялась в звуковой файл с помощью математической системы Mathcad 14 путем замены очередного бита и с учетом знака отсчета. Отсчеты представляют собой значения амплитуды в определенные моменты времени, значения которых могут быть как положительными, так и отрицательными. Положительные значения в WAV-файле представлялись в прямом коде, а отрицательные значения — в дополнительном коде.

При проведении экспериментальных исследований информация сначала внедрялась в шестнадцатые (младшие) разряды отсчетов. В нечетные отсчеты внедрялась логическая единица, а в четные отсчеты — логический нуль. В следующем файле внедрение осуществлялось в пятнадцатые разряды и так далее до второго разряда. Форма внедряемых сигналов показана на рисунке 3.

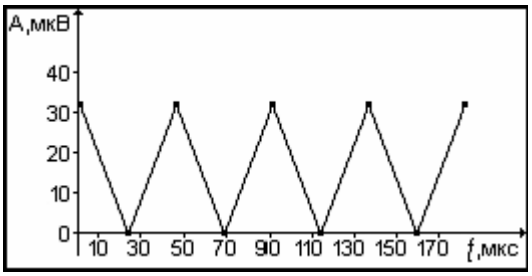


Рис. 3. Форма внедряемого сигнала

Экспериментально установлено, что визуально можно обнаружить наличие вложения в сигнале при изменении девятого разряда в отсчете. Внедрение информации в разряды 10…16 путем визуального анализа спектров сигналов обнаружить практически невозможно. Данные оценки иллюстрирует рисунок 4.

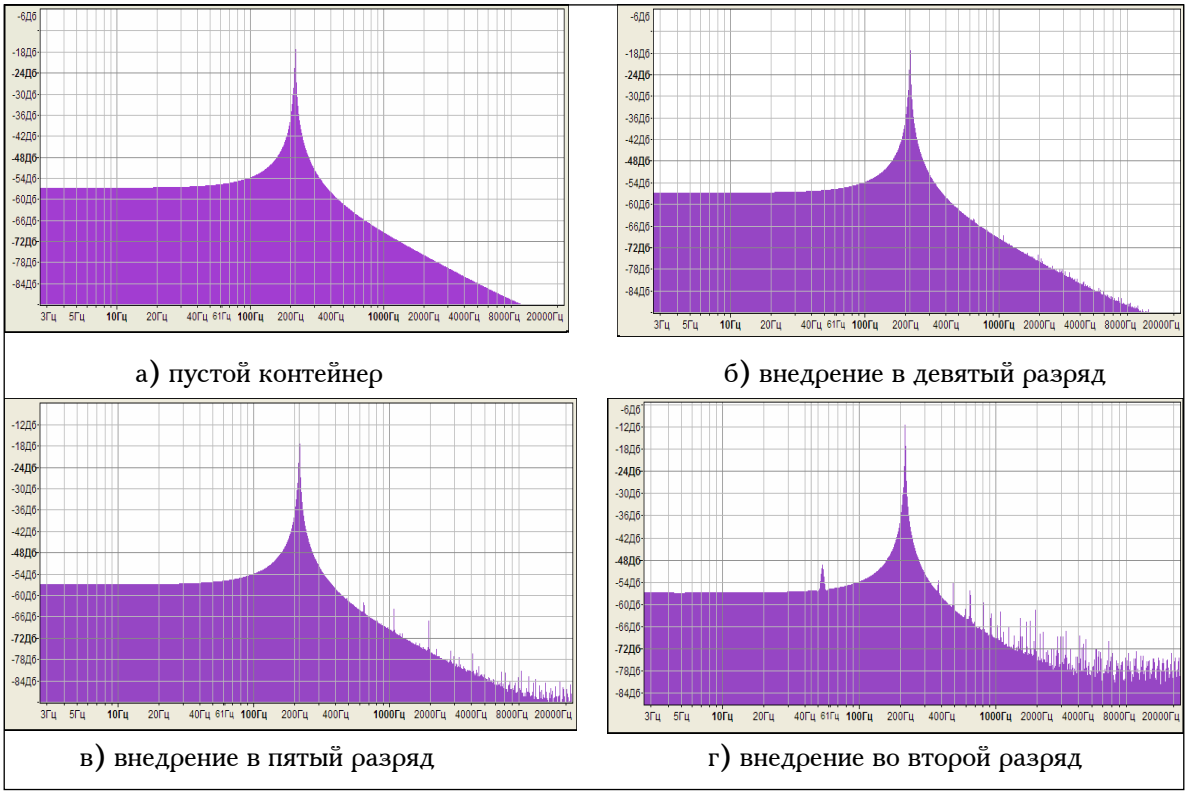


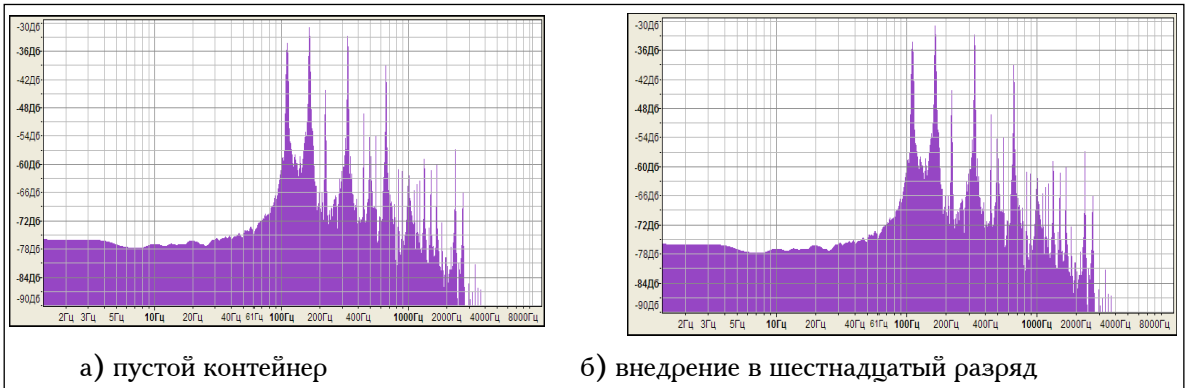
Рис. 4. Осциллограммы синусоидального сигнала с модифицированными битами

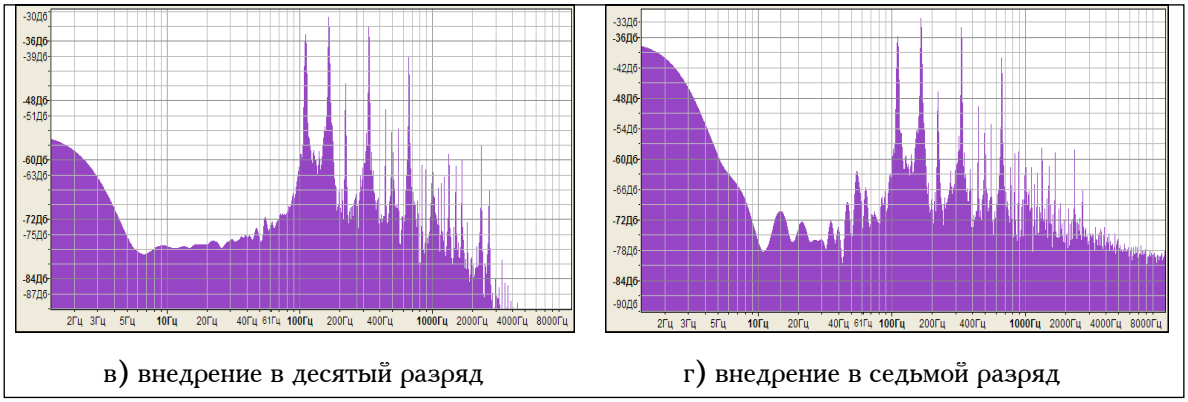
4. Визуальная оценка искажений звукового сигнала

Искажения, вносимые методом замены наименьшего значащего бита в реальном звуковом сигнале, можно также визуально обнаружить путем анализа спектра сигнала.

В качестве контейнера использовался звуковой файл с уровнем квантования 16 бит, который содержал запись инструментального симфонического произведения. На рисунке 5а изображен спектр пустого контейнера.

Внедрение в шестнадцатые разряды (самые младшие) каждого отсчета не вносило заметных искажений (рисунок 5б). Изменения в десятом разряде надежно выявлялись путем анализа спектра (рисунок 5в), но плохо различались на слух. При внедрении информации в седьмой разряд искажения были различимыми даже на слух (рисунок 5г). Наиболее заметные искажения обнаруживались на участках с низким уровнем звукового сигнала («полная тишина»). Если исключить внедрение информации на участках с низким уровнем громкости, то для внедрения можно использовать разряды с 14 по 16. При этом изменения спектра с помощью звукового редактора Audacity 1.3 визуально зарегистрировать нельзя.





в) внедрение в десятый разряд г) внедрение в седьмой разряд

Рис. 5. Спектр звукового сигнала

5. Программы Crypto и WaveCrypto

Результаты экспериментальных исследований были учтены при разработке программ Crypto и WaveCrypto (последняя программа разработана совместно со студентом Димитровградского института технологии, управления и дизайна (ДИТУД) Сомковым С. А.).

Программа Crypto предназначена для скрытой передачи информации в аудиофайлах, с использованием принципов стеганографии [1, 3].

Для повышения скрытности внедренной информации в программе использован модифицированный метод замены наименьшего значащего бита. Информация разделяется на фрагменты и распределяется по нескольким звуковым файлам. На рисунке 6 показан интерфейс главного окна приложения. Программа позволяет распределять информацию по десяти звуковым файлам. Такой подход позволяет осуществить защиту авторских прав не только на отдельный музыкальный файл, но и на весь альбом. В качестве контейнеров используются звуковые файлы формата WAV. Ключом для извлечения сообщения служит последовательность файлов, в которых были скрыты фрагменты сообщения. Для повышения степени защиты информации скрываемое сообщение можно предварительно зашифровать с использованием различных симметричных алгоритмов, которые реализованы в данной программе: шифр Цезаря, шифр Атбаш, квадрат Полибия, прямоугольник Плейфейра, метод перестановок, метод гаммирования, аффинные преобразования, шифр Виженера.

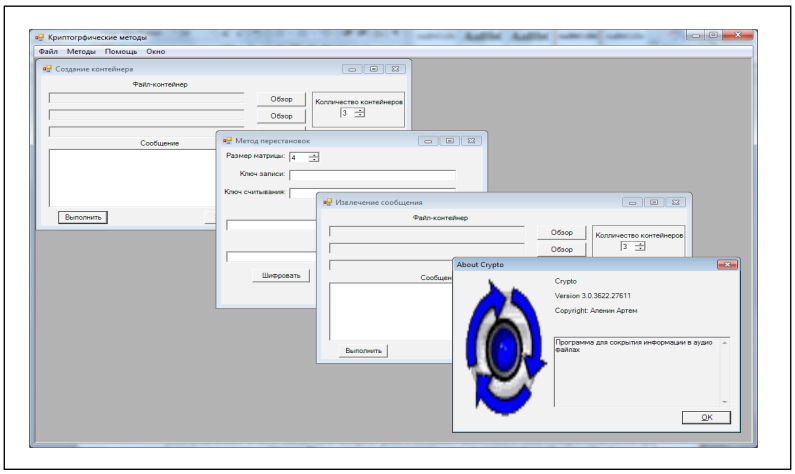


Рис. 6. Главное окно программы Crypto

Программа WaveCrypto позволяет внедрять информацию в один звуковой файл с использованием ключа, распределяющего внедряемую информацию по всему контейнеру. Ключ распределения генерируется в зависимости от размера файла и требующегося соотношения между

наполняемостью и скрытностью. Если в контейнере содержится «полная тишина» (т. е. отсчеты с малой амплитудой), то программа пропускает их, внедряя информацию на других участках фонограммы. Для пропуска участков фонограммы с низким уровнем звука файл-контейнер разбивается на серии (блоки) от «полной тишины» до «полной тишины».

Ключ распределения информации генерируется в следующем виде: количество бит, заменяемых в одном отсчете, количество модифицируемых отсчетов в серии, количество серий, в которых сохранена информация. Например, если ключ 2:2:3, то контейнер будет заполнен следующим образом: файл разбивается на серии, количество которых не менее трех, в каждой серии содержится как минимум два отсчета, в которых два последних бита заменяются значимой информацией. Данный пример иллюстрирует рисунок 7. Серым цветом на рисунке 7 выделены отсчеты, в которых сохранена информация.

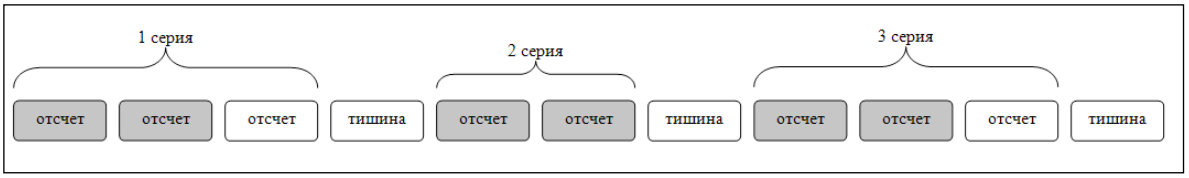


Рис. 7. Распределение информации в контейнере

Естественно, что используемый ключ может быть сложнее.

Указанный подход может быть применен для формирования скрытых меток в музыкальном альбоме, состоящем из нескольких музыкальных произведений.

Разработанные программы Crypto и WaveCrypto создают несколько уровней защиты информации: шифруют открытый текст одним из криптографических методов, внедряют зашифрованный текст в звуковые файлы, распыляя скрываемые биты не только внутри одного файла, но и среди нескольких звуковых файлов. В отличие от известных программ здесь исключаются участки фонограммы с низким уровнем громкости и распыление скрываемой информации осуществляется по множеству файлов.

Выводы

При выборе номера разряда, в который осуществляется внедрение скрываемой информации, следует ориентироваться на наиболее уязвимые с точки зрения криптоанализа случаи. Наиболее уязвимыми являются участки звуковой фонограммы с низким уровнем громкости звучания.

СПИСОК ЛИТЕРАТУРЫ:

1. *Алексеев А. П., Орлов В. В.* Стеганографические и криптографические методы защиты информации: учебное пособие. Самара: ИУНЛ ПГУТИ, 2010. – 330 с.
2. *И. А. Алдошина, Э. И. Вологдин, А. П. Ефимов и др.* Электроакустика и звуковое вещание: Учебное пособие для вузов. М.: Горячая линия — Телеком, Радио и связь, 2007. – 872 с.
3. *Аленин А. А., Алексеев А. П.* Пространственное распределение информации в звуковых файлах // XVI Российская научная конференция проф.-преп. состава, научных сотрудников и аспирантов. Самара: ПГУТИ, 2009 . С. 171–172.