О МЕТОДАХ СТЕГОАНАЛИЗА В АУДИОФАЙЛАХ

П. П. Кокорин

Санкт-Петербургский институт информатики и автоматизации РАН

СПИИРАН, 14-я линия ВО, д. 39, Санкт-Петербург, 199178

<kokorin@list.ru>

УДК 004.9

Кокорин П. П. **О методах стегоанализа в аудиофайлах** // Труды СПИИРАН. Вып. 4. — СПб.: Наука, 2007.

Аннотация. *В работе рассматриваются основные подходы стеганографического встраивания информации в аудиофайлах. Предлагаются методы детектирования скрытых данных в служебных областях аудиофайлов, а также сокрытия в фазовой области аудиоданных.* — Библ. 4 назв.

UDC 004.9

Kokorin P. P. **About methods of stegoanalysis in audio files** // SPIIRAS Proceedings. Issue 4. — SPb.: Nauka, 2007.

Abstract. *The article says about the main approaches of embedding data in audio files. Moreover, methods for detection of embedding in audio files' headers and in phase scope are proposed.* — Bibl. 4 items.

1. Введение

Методы стеганографии были известны человечеству еще задолго до появления компьютеров. Как полагают историки, еще в Древнем Египте для секретной передачи послания брили голову раба, писали на ней сообщение, после чего, когда волосы отрастали, отправляли раба получателю сообщения. С появлением фотографии стали доступны новые способы — например, в ничего не значащие снимки добавлялись микроточки. Подобные методы передачи секретных сообщений активно использовались во время Второй мировой войны. Можно найти еще массу примеров использования стеганографии в прошлом [1].

Во многих странах существуют законы, запрещающие применение стойких алгоритмов криптографии. На применение стеганографии подобных ограничений пока нет, что делает привлекательным ее использование как дополнительного способа защиты информации.

В отличие от криптографии, основной задачей стеганографии является сокрытие самого факта передачи сообщения. Сообщение, факт передачи которого мы хотим скрыть, назовем секретным сообщением. Файл, не содержащий секретного сообщения, называется пустым контейнером, а файл с включенным сообщением – заполненным контейнером. Обозначим несколько важных требований, которым должны отвечать стеганографические методы:

- Осведомленность злоумышленника обо всех методах работы алгоритма, а также знание статистических характеристик контейнера не должны помочь ему в обнаружении секретного сообщения.
- Информация о том, что контейнер заполнен, не должна способствовать извлечению секретного сообщения.
- Заполненный контейнер должен быть неотличим от пустого контейнера.
- В качестве контейнера могут служить разнообразные данные: текстовый документ, музыка, изображения, видео и др.

Значительный размер музыкальных файлов, их информационная избыточность, а также возросшая популярность передачи их через сеть делают звуковые файлы особенно привлекательными для использования в качестве стегоконтейнера.

Существует несколько основных подходов стеганографического сокрытия информации в аудиоданных, приведем одну из возможных классификаций:

— сокрытие в служебных областях аудиофайла;
— сокрытие в области звуковых данных:
  - в частотно-фазовой области;
  - во временной области.

2. Методы стеганографии в аудиофайлах

2.1. Сокрытие данных в служебных областях аудио файлов

Формат WAV PCM основан на стандартном формате IFF (Interchange File Format). Файл WAV содержит заголовок и непосредственно следующий за ним блок данных. В заголовке содержится информация о количестве каналов, способе кодирования отсчетов и количестве отсчетов в секунду. Блок данных содержит импульсно-кодовое представление сигнала.

Файл формата MP3 состоит из множества фреймов, каждый из которых содержит свой собственный заголовок. В заголовке фрейма хранится информация о способе кодирования текущего фрейма, использовании контрольных сумм заголовка, режиме стерео и другая техническая информация. Заголовок содержит также область синхронизации, необходимую для идентификации фрейма в потоке байтов. Важной особенностью формата является то, что фреймы могут следовать друг за другом с промежутками.

Структура файлов MP3 позволяет легко прятать информацию в служебных областях. Возможными местами вставки являются: промежутки между фреймами, поле контрольной суммы фрейма, поля специальных информационных заголовков — ID3 теги. Возможна вставка информации вместо аудиоданных (при этом заголовок фрейма остается неизменным). Такие методы являются самыми простыми в реализации. В настоящее время существует большое количество программ, основанных на данных методах [2]; примером могут служить: Rohos (<http://www.rohos.com>) скрывает информацию в промежутках между фреймами, Camouflage (<http://scifi.pages.at/yoda9k/cf>) помещает вставку после последнего фрейма в файле, MP3Stego (<http://www.petitcolas.net/fabien/steganography/mp3stego>) манипулирует битом четности размера фрейма данных, Steganos Security Suite (<https://www.steganos.com>) оставляет заголовок фрейма без изменения, внедряя данные вместо аудиоинформации и др.

Применяя такие методы, можно скрыть в контейнере значительно больше информации по сравнению с любыми другими подходами. С другой стороны, их стойкость к атакам низкая. Кроме того, существуют вариации метода, которые вставляют данные не между фреймами, а под видом поврежденного фрейма или в блок аудиоданных фрейма. В последнем случае модифицируются аудиоданные, что влияет на качество звука.

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Методы сокрытия в заголовках файла в основном могут быть легко детектированы проверкой значений полей в соответствии со спецификацией формата файла. Приведем пример еще одного интересного варианта вставки данных в служебные области файла — это использование бита четности размера аудиоданных фрейма, как это сделано в программе MP3Stego. Особенность этого метода заключается в том, что места модификации битов, выбираются нерегулярным методом, основанным на наложении маски рекурсивно получаемого значения хеш-функции пароля. Существуют объективные трудности в детектировании данного метода. Данный метод является необратимым, т.е. не существует эффективного способа выделения внедренного сообщения из контейнера. Любая попытка уничтожения скрытого сообщения сильно искажает аудиоданные.

Детектирование методов, основанных на сокрытии данных в промежутках между фреймами, сводится к анализу последних. Наличие таких промежутков может свидетельствовать о наличии стеговставки либо о том, что звуковой файл поврежден. Необходимо определить и проанализировать суммарный размер таких промежутков, места их обнаружения и сами данные.

2.2. Сокрытие информации в области аудиоданных

Методы, которые будут рассмотрены в следующем пункте, значительно боле сложны в реализации, но и более эффективны.

Хронологически одним из первых методов встраивания информации в аудиофайлы был метод изменения малозначащих битов (LSB). Чаще всего он применяется для сокрытия в аудиофайлах формата WAV благодаря простоте осуществления вставки. Скрываемая информация встраивается в несколько младших битов отчетов сигнала [2, 4]. В результате сокрытия сигнал практически неотличим на слух от исходного файла. Такой подход неустойчив к сжатию с потерями, поэтому практически неприменим для формата MP3.

Модификация частотно-фазовой области является достаточно популярной темой для исследователей. Было предложено несколько способов сокрытия данных в частотной и фазовой областях [3, 4]. Места закладки скрываемого сообщения могут выбираться в соответствии с психоакустической моделью восприятия звука. В этом случае заполненный контейнер практически неотличим на слух от пустого контейнера. Данные методы более стойки к атакам. С другой стороны, они в некоторой степени снижают субъективное качество звука.

Методы, основанные на изменении фазовой области, как правило, изменяют абсолютное значение фазы некоторых гармоник. Существуют вариации, в которых восстанавливаются значения разностей фаз смежных фреймов. Делается это исходя из предположения, что человеческое восприятие звука чувствительно не к абсолютному значению фазы сигнала, а к разности фаз смежных фрагментов. В других методах фаза выбранной гармоники изменяется либо на фиксированное значение, либо изменением знака действительной и мнимой частей комплексного спектра [3]. В простейших случаях эти методы неустойчивы к модификациям данных.

Более сложные методы могут комбинировать несколько подходов, например использование модели психоакустического восприятия звука, различных методов модуляции и др., что оправдано увеличением стойкости таких методов.

Детектирование стеговставок в частотно-фазовой, а также во временной областях представляет гораздо больший интерес для исследования. Основной подход заключается: в установлении возможных мест закладки, в извлечении данных из этих мест для анализа, в проверке полученных данных по критериям отклонения от ожидаемых значений.

Нам не удалось найти действующих программ сокрытия информации в фазовой области аудиоданных. Поэтому было принято решение реализовать некоторые варианты данного подхода. Для этого были реализованы два метода с изменением абсолютного значения фазы гармоник фрейма, а также вариант с изменением знака действительной и мнимой частей гармоник комплексного спектра [3].

Для реализации методов были использованы свободно распространяемые исходные коды MP3 компрессора 8Hz, а также методы формирования псевдослучайной последовательности из программы MP3Stego.

Исходный файл MP3 распаковывался, модифицировалась фазовая область сигнала, затем сигнал упаковывался обратно в формат MP3. Для встраивания использовался каждый 20й фрейм потока. Решение об использовании фрейма для сокрытия информации принималось на основе случайной последовательности, единичный бит которой значил, что в соответствующий фрейм будет встроен один бит сообщения. Метод получения этой последовательности состоит в вычислении значения хеш-функции SHA-1 от введенной ключевой фразы. После того как были использованы все биты последовательности, тем же способом вычислялось хеш-значение для конкатенации строкового представления предыдущего значения и ключевой фразы.

Из 1156 отсчетов, содержащихся во фрейме, для встраивания использовались 512 отсчетов. Для этих значений вычислялось 512 точечное быстрое преобразование Фурье.

Для метода изменения фазы на фиксированное значение фазы $\phi(S)$ и амплитуды $A(S)$ компонент спектра вычислялись по формулам:

$$\phi(S) = \operatorname{arctg}\left(\frac{\mathrm{Im}_S}{\mathrm{Re}_S}\right), \tag{1}$$

$$A(S) = \sqrt{\mathrm{Im}_S^2 + \mathrm{Re}_S^2}, \tag{2}$$

где S — вектор значений комплексного спектра; Im_S и Re_S — мнимая и действительная части спектра сигнала; arctg — четырехквадрантный арктангенс.

Значения фазы гармоник модифицировались в соответствии с формулой

$$\phi'(S) = \begin{cases} \dfrac{\pi}{6}, & b = 0; \\ \dfrac{\pi}{3}, & b = 1, \end{cases} \tag{3}$$

где b — текущий встраиваемый бит данных.

Затем восстанавливались значения спектра

$$S = A(S) \cdot e^{j\phi'(s)}, \tag{4}$$

где j — мнимая единица.

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

В методе с инвертированием знаков компонент спектра вектор фаз не вычислялся, а непосредственно изменялись компоненты спектра по формулам:

$$\mathrm{Re}_S = \begin{cases} -|\mathrm{Re}_S|, & b = 0 \\ |\mathrm{Re}_S|, & b = 1 \end{cases}, \quad (5)$$

$$\mathrm{Im}_S = \begin{cases} -|\mathrm{Im}_S|, & b = 0 \\ |\mathrm{Im}_S|, & b = 1 \end{cases}, \quad (6)$$

где b — текущий встраиваемый бит данных; Im_S и Re_S — мнимая и действительная части спектра фрейма сигнала.

Обратным преобразованием Фурье восстанавливается поток данных. Полученный модифицированный сигнал далее подвергался компрессии в формат MP3.

В зависимости от выбранного метода для восстановления сообщения необходимо проанализировать значения фаз компонент спектра либо знаки действительной и мнимой частей компонент спектра.

3. Детектирование стеговставок в файлах MP3

Предлагаемый в данной работе метод детектирования стеговставок в аудиофайлах состоит из двух независимых частей:

– поиск стеговставок в служебные области файла MP3;
– детектирование изменения фазовой области сигнала.

3.1. Поиск в служебных областях файла MP3

На предмет наличия вложений проверяются следующие места в структуре формата файла MP3:

— промежутки между фреймами;
— контрольные суммы заголовков фреймов;
— анализ «подозрительных» фреймов.

Для начала пропускаются заголовки информационных тегов ID3v1, ID3v2. Далее ищется заголовок первого фрейма, из которого извлекается информация о наличии битов заполнения (padding bits), контрольная сумма; определяется используемый стандарт сжатия MPEG, количество каналов, битрейт и прочие параметры сжатия. Полученная на данном этапе информация используется для последующей распаковки сигнала. После того как вся необходимая информация извлечена из фрейма и он считается обработанным, переходим к поиску следующего фрейма. При этом подсчитывается количество битов, находящихся в промежутке между фреймами сигнала. На основе этой информации делается предположение о наличии стеговставки между фреймами сигнала.

Если заголовок защищен контрольной суммой, то выполняется проверка этой контрольной суммы.

Последним этапом идет поиск «подозрительных» фреймов. Условимся называть «подозрительным» тот фрейм, который, обладая правильным заголовком, не мог быть создан MP3кодером. К признакам подозрительности фрейма можно отнести изменение параметров сжатия фрейма относительно предыдущих фреймов:

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

— стандарт сжатия (например, с MPEG-1 layer 3 (MP3) на MPEG-1 layer 2);
— битрейт фрейма (для сжатия с постоянным битрейтом);
— режим стерео;
— частота дискретизации;
— защита заголовков контрольными суммами и пр.

Это предположение основано на том факте, что стандарт MPEG-1 позволяет фреймам иметь различные параметры сжатия, на практике же это не встречается и может быть расценено как попытка встраивания информации.

Таким образом, полученная информация о промежутках между фреймами, результат проверки контрольных сумм, а также наличие «подозрительных» фреймов анализируются и делается заключение о присутствии в файле стеговставки.

Испытания работы алгоритма проводились на 52 различных аудиофайлах формата MP3 со стеговставками. Сокрытие информации осуществлялось программами Rohos, Camouflage, MP3Stego и Steganos Security Suite. Метод эффективно обнаружил все вложения в файлы MP3, кроме вложений программы MP3Stego. Нам не удалось найти эффективного способа ее детектирования.

Метод был также испытан на большом количестве файлов без вложений. В результате чего было выявлено большое количество ложных срабатываний метода. Причиной этого явилось наличие повреждений структуры MP3 файлов (поврежденные фреймы принимались за возможные стеговставки).

3.1. Поиск в фазовой области аудиоданных

Анализ методов встраивания информации в фазовую область, рассмотренных выше, позволяет сделать вывод, что для их детектирования необходимо проанализировать распределение значений квадрантов фаз гармоник. В случае если во фрейм было встроено сообщение, будет заметно преобладание некоторых квадрантов. Для пустого фрейма такого преобладания не будет (рис. 1).

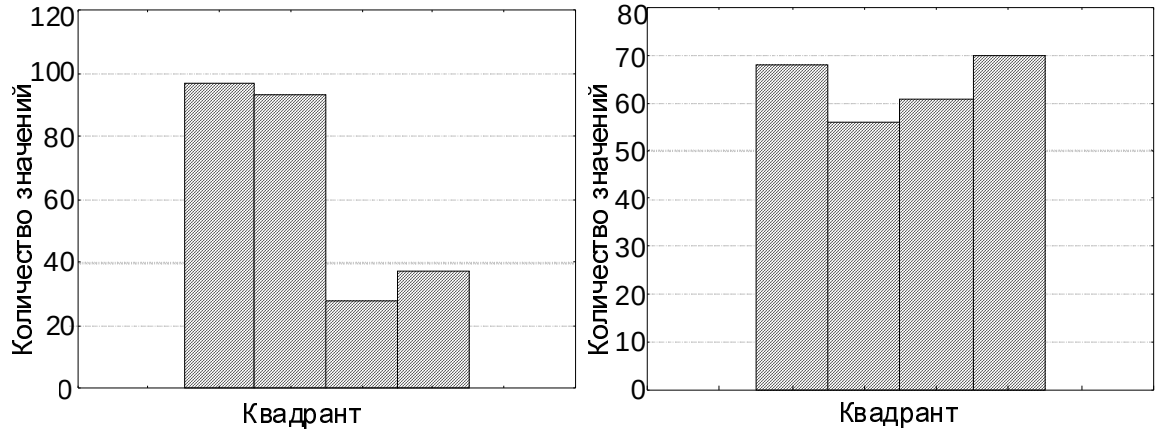

Рис. 1. Гистограммы распределений значений фаз по квадрантам для фреймов со вставкой (слева) и без вставки (справа).

Как видно на рисунке слева, значительное преобладание 1 и 2 квадрантов свидетельствует о том, что во фрейм был встроен единичный бит.

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Алгоритм поиска вставок в фазовую область заключается в следующем. При обработке каждого фрейма данных аудиосигнал извлекался и декодировался. В зависимости от параметров сжатия фрейм мог содержать 578 или 1156 отсчетов на канал. Таким образом, полученные данные разбиваются на фрагменты по 512 отсчетов. Для полученных фрагментов вычисляется 512 точечное быстрое преобразование Фурье. Далее по знаку мнимой части комплексного спектра определяются квадранты фаз гармоник и проводится частотный анализ этих значений. Затем отыскиваются преобладающие значения. Для этого вычисляются рейтинги пар квадрантов 1–2 и 3–4 по формуле

$$R_{i,j} = \frac{N_i + N_j}{N}, i \neq j, \quad (7)$$

где $R_{i,j}$ — рейтинг пары квадрантов i j; N_i — частота встречаемости i-го квадранта; N — количество компонент в векторе фаз.

Значение порога наличия преобладания для рейтинга пары выбиралось опытным путем.

Для испытания предложенного метода детектирования в 52 музыкальных файла формата MP3 были встроены сообщения длиной 32 бита двумя описанными выше методами сокрытия информации в фазовой области. Файлы содержали современную музыку различных стилей. Средний размер файла составил 3 Мб при битрейте 128 кБ/с и частоте дискретизации 44,1 кГц.

В ходе испытаний был подобран порог рейтинга для пар квадрантов. При значении порога равного 0,8 обнаруживались все вложения. Для исключения случаев ложного срабатывания был введен параметр минимального количества модифицированных фреймов. Оказалось, что даже в файлах, не содержащих вложений, может встречаться незначительное количество фреймов с признаками вложений. Опытным путем было установлено, что при минимальном количестве модифицированных фреймов равном 8 исключались все случаи ложного срабатывания. Необходимо заметить, что при этом минимальная длина детектируемого вложения составляет один байт.

4. Заключение

Информационная избыточность форматов хранения аудиоданных предоставляет большое количество мест для сокрытия информации как в служебных областях файлов, так и непосредственно в области аудиоинформации. Появление большого количества различных методов и алгоритмов стеганографии в аудиофайлах порождает трудности для стегоанализа, т.к. требуется учитывать особенности работы каждого из этих методов.

Предложенный метод поиска вложений в служебных областях файлов эффективно обнаруживает факт внедрения сообщения, созданного большинством существующих программ. В то же время его недостатком является ложное срабатывание на поврежденные файлы. Для предотвращения этого необходимо анализировать сами подозрительные данные, что является, несомненно, не менее трудной задачей, выходящей за рамки данной работы. Предложенный метод не применим для автономного функционирования, тем не менее целесообразно его использование для выявления «подозрительных» файлов MP3, которые затем тщательно исследуются экспертом.

Труды СПИИРАН. 2007. Вып. 4. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2007. Issue 4. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Метод детектирования модификации фазовой области аудиосигнала показал достаточно хорошие результаты при обнаружении стеговставок, созданных методами модификации фазовой области [3]. Недоступность реализации методов встраивания в фазовую область создает некоторые трудности в испытании предложенного способа стегоанализа. Тем не менее метод может быть использован в задачах стегоанализа в фазовой области аудиофайлов формата WAV и MP3.

Литература

1. *Кузнецов А. И.* Двоичная тайнопись (по материалам открытой печати) // КомпьютерПресс. 2004. № 4. С. 38–41.
2. *Барсуков В. С., Романцов А. П.* Компьютерная стеганография вчера, сегодня, завтра [Электронный ресурс] // Специальная Техника. 1998. № 4–5. // <http://st.ess.ru/publications/articles/steganos/steganos.htm> (по состоянию на 12.03.2007).
3. *Рублёв Д. П., Федоров В. М., Макаревич О. Б., Бабенко Л. К.* Метод встраивания данных в аудиопоток на основе преобразования фазовых составляющих // Информационное противодействие угрозам терроризма. 2005. № 4. С. 169–174.
4. *Чваркова И. Л.* Стеганографические методы скрытия информации в аудиоданных // Электроника. 2003. № 11. С. 54–56.