УДК 004.056

Стегоанализ аудиоданных на основе методов сжатия

М. А. Забелин

На примере формата WAVE предлагается метод определения наличия скрытых данных, размещённых в аудиофайлах путём изменения младших бит. Экспериментально показана высокая эффективность алгоритма.

Ключевые слова: стеганография в аудиофайлах, стегоанализ, формат WAVE.

1. Введение

Сегодня мы живём в мире информационных технологий. Информация стала неотъемлемой частью нашей жизни. С появлением современных средств копирования и тиражирования данных остро встаёт проблема сохранения авторских прав и защита от несанкционированного тиражирования. Соответственно возникает потребность в шифровании данных, скрытой их передаче и во внедрении специальных меток в электронные представления данных для однозначной идентификации владельца.

Способы и методы скрытия секретных сообщений известны с давних времён. Вместе с их появлением возникла и наука, изучающая данную сферу человеческой деятельности. Она получила название стеганография. Это слово происходит от греческих слов «steganos», что означает секрет или тайна, и «graphy» – запись. Буквально – «тайнопись». Исторически это направление появилось первым, но затем во многом было вытеснено криптографией. В отличие от криптографии, где неприятель точно может определить, является ли передаваемое сообщение зашифрованным текстом или нет, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания. Таким образом, под словом «стеганография» принято понимать метод передачи сообщения, который скрывает факт передачи сообщения. Отметим, что сегодня стеганография и криптография существуют в тандеме, взаимно дополняя друг друга. Стеганографические методы позволяют уменьшить вероятность выявления факта передачи некоторого сообщения. Криптографические методы – увеличить степень защищённости встроенного сообщения [1, 2].

Местом зарождения стеганографии многие называют Египет, хотя первыми «стеганографическими» сообщениями можно назвать и наскальные рисунки древних людей. Первое упоминание о стеганографических методах в литературе приписывается Геродоту, который описал случай передачи сообщения Демартом. Общеизвестно, что в Древней Греции тексты писались на дощечках, покрытых воском. Во избежание попадания сообщения к противнику Демарт использовал следующее ухищрение. Соскабливал воск с дощечек, писал сообщение прямо на поверхности дерева, а потом снова покрывал дощечку воском. Таблички выглядели без изменений и потому не вызывали подозрений. Другой эпизод, который относят к тем же временам – передача послания с использованием головы раба. Для передачи тайного сообщения голову раба обривали, наносили на кожу татуировку, и когда волосы отрастали, отправляли с посланием.

В XVII – XVIII веках были хорошо известны различные способы скрытого письма между строк обычного незащищённого письма: от применения молока до использования сложных химических реакций с последующей обработкой при чтении [3].

Сегодня, благодаря научным достижениям в области компьютерной техники и технологий появлению новых способов передачи информации, появились новые стеганографические методы, в основе которых лежат особенности представления информации в оцифрованном виде. К примеру, существуют методы, которые позволяют скрывать сообщения в компьютерных файлах (контейнерах) за счёт учёта естественных неточностей устройств оцифровки и избыточности аналогового видео- или аудиосигнала. Таким образом, можно говорить о новом витке развития – эре компьютерной стеганографии.

Наряду с развитием стеганографии идёт бурное развитие стегоанализа. Основной задачей стегоанализа является определение факта наличия скрытого сообщения в предположительном контейнере (речи, видео, изображении). Решить эту задачу возможно путём изучения статистических свойств сигнала. Например, распределение младших битов сигналов имеет, как правило, шумовой характер (ошибки квантования). Они несут наименьшее количество информации о сигнале и могут использоваться для внедрения скрытого сообщения. При этом, возможно, изменится их статистика, что и послужит для аналитика признаком наличия скрытого сообщения [4].

Целью данной работы является разработка эффективной методики автоматического выявления скрытой информации в аудиоданных (на примере WAVE). В основе данной методики лежит сжатие данных [5]. Заметим, что скорость метода напрямую будет зависеть от выбранного метода сжатия.

За основную идею разрабатываемой методики был взят алгоритм, предлагаемый в [6]. В оригинале данный метод применялся для исследования графических изображений в форматах BMP и JPEG. Для исследования аудиофайлов предлагается использовать более общий подход. При этом суть метода остаётся неизменной: включение данных повлечёт за собой изменение статистических закономерностей внутри контейнера, а значит, можно отследить такое включение.

Теперь несколько слов о целесообразности проводимых исследований. Известно, что в 1998 году Кашен (Cachin) предложил теоретико-информационный подход к стеганографии, в рамках которого, в частности, была определена так называемая совершенная стегосистема, у которой сообщения, несущие и не несущие скрытую информацию, статистически неразличимы. Там же была описана и универсальная стеганографическая система, для которой это свойство выполнялось асимптотически, при увеличении длины сообщения. При этом сложность кодирования и декодирования возрастала экспоненциально. В [7] приводится улучшенная универсальная стеганографическая система, обладающая описанным выше свойством и скоростью передачи «скрытой» информации, стремящейся к пределу – энтропии Шеннона источника, используемого для «внедрения» скрытой информации.

Таким образом, возникает вопрос: а есть ли смысл проведения стегоанализа при наличии подобных систем? Ввиду особенностей реализации, подобные системы применимы непосредственно к вероятностным источникам, но не к сообщениям. А как уже отмечалось ранее, данные исследования базируются на изучении аудиофайлов, которые представляют собой сообщения, порождённые некоторым источником. Помимо этого, нельзя упускать из виду, что при внедрении одного сообщения внутрь другого некоторым образом меняется статистика сообщения-контейнера, что в свою очередь является опорной точкой для проведения анализа. Итог: проведение анализа при определённых условиях имеет смысл.

В заключение отметим, что разработанная методика, как и оригинал, приводимый в [6], позволяет достаточно эффективно выявлять скрытые данные, обладает высокой степенью автоматизации и широкой областью применимости.

2. Основные методы добавления скрытой информации

Как известно, любой файл на жёстком диске представляется последовательностью байт, такое представление удобно при рассмотрении методов включения инородных данных внутрь контейнера, так как любая программа, реализующая данную функцию, переходит именно к такому представлению. Помимо этого для скрытия данных могут быть использованы и так называемые служебные заголовки файлов.

Рассмотрим общую классификацию:

1. *Методы, основанные на использовании специальных свойств компьютерных форматов данных.*
   a. Методы, базирующиеся на использовании зарезервированных для расширения полей компьютерных форматов данных. Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программами. Таким образом, они могут быть использованы для скрытия некоторой информации. Данная схема проста в использовании. Но при этом она обладает существенными недостатками: низкая степень скрытности, передача лишь небольших объёмов информации.
   b. Методы специального форматирования текстовых файлов. В эту группу методов можно отнести методы, основанные на изменении положения строк и расстановки слов в предложении. Сюда относятся и методы, базирующиеся на выборе определённых позиций букв в тексте, например, начальные буквы каждой строки образуют сообщение. Наконец, в эту группу входят методы, основанные на использовании специальных «невидимых», скрытых полей для организации сносок и ссылок. Например, использование чёрного шрифта на чёрном фоне. Отметим положительные и отрицательные стороны подобных методов. К плюсам относятся: простота использования и наличие доступного программного обеспечения. К минусам: слабая производительность, передача небольших объёмов информации, а также низкая степень скрытности.
   c. Методы скрытия в неиспользуемых местах гибких и компакт-дисков. Например, запись на нулевую дорожку. Отрицательные и положительные стороны метода аналогичны предыдущей группе методов.
   d. Методы использования имитирующих функций. Данные методы основываются на генерации осмысленных текстов, скрывающих некоторое сообщение. Как и две предыдущие группы методов, данная группа обладает слабой производительностью, небольшими объёмами скрываемой информации и низкой степенью скрытности. Данные методы обладают более высокой степенью сложности. Достоинством же является то, что результирующий текст не является подозрительным для систем мониторинга.

2. *Методы использования избыточности файлов цифрового видеоряда, фотографий или цифрового звука.* Как известно, младшие разряды цифровых отсчётов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия, что и обеспечивает возможность скрытия. У данной группы методов имеется ряд отличительных особенностей. Сначала рассмотрим негативные особенности. С изменением информации искажаются статистические характеристики цифровых потоков. Ввиду этого для снижения компрометирующих признаков требуется коррекция статистических характеристик. К достоинствам можно отнести: возможность скрытой передачи большого объёма информации, возможность защиты авторского права, скрытого изображения, товарной марки, регистрационных номеров и т.п.

3. Краткое описание формата WAVE

WAVE – это формат хранения оцифрованных аудиоданных. Этот формат поддерживает данные различной разрядности, с различной частотой выборки и числом каналов. Он весьма популярен на платформах стандарта IBM PC (и совместимых с ним). Использование данного формата подразумевает хранение аудиоданных в особых блоках (chunks). В проводимых исследованиях в качестве контейнеров использовались WAVE-файлы в PCM-формате. То есть, для создания подобного файла использовалась импульсно-кодовая модуляция, сохраняющая последовательно записанные значения амплитуды звука (по принципу работы АЦП). Также в этом формате отсутствует сжатие. Частота выборки определяет качество оцифрованного звука (8000 Гц, 11025 Гц, 22050 Гц, 44100 Гц). Величина амплитуды в момент оцифровки может быть закодирована либо при помощи 8-разрядного числа (256 значений), либо 16-разрядного (65536 значений). Помимо этого встречаются 24- и 32-разрядные варианты реализаций. Каждое такое значение принято называть отсчётом (sample).

Как говорилось ранее, WAVE-файл представляет собой набор из многочисленных блоков разного типа. Первым следует RIFF-заголовок, который содержит информацию о типе файла, и его размер без размера RIFF-заголовка. Одним из основных блоков является блок формата, который содержит основные параметры звуковых данных, например, частоту выборки. Другим важным блоком является блок данных, который непосредственно хранит форму аудиосигнала. В WAVE-файле могут быть и другие дополнительные блоки, наличие которых необязательно.

Порядок следования блоков разного типа может быть произвольным. Исключение составляет блок формата, который должен предшествовать блоку данных. Заметим, что первый блок (после RIFF-заголовка) не обязательно должен быть блоком формата, он может быть и дополнительным.

Для наглядности рассмотрим схему простейшего WAVE файла:

Рис 1. Схема простейшего WAVE-файла

4. Методы добавления данных в WAVE

Основными требованиями, предъявляемым к таким методам, являются:

1. сохранность целостности контейнера;
2. неразличимость на слух файлов со встроенным сообщением и без оного;
3. маскировка проводимых действий с целью препятствия стегоанализу.

Большинство программ, находящихся в свободном доступе и позволяющих встраивать одни данные внутрь других, зачастую удовлетворяют первым двум пунктам требований.

Рассмотрим принцип скрытия данных внутри аудиофайла. WAVE-формат хранит значения амплитуд в чистом виде, значит, для скрытия сообщения необходимо специальным образом модифицировать младшие биты отсчётов, причём нет надобности в каких-либо дополнительных преобразованиях. Не будем исключать возможность включения скрытых данных в заголовочную часть файла, так как формат WAVE не стандартизирован.

Для исследования возьмём WAVE-файлы со следующими характеристиками:

1. файл состоит из RIFF-заголовка, блока формата и блока данных;
2. формат файла – PCM;
3. частота выборки (дискретизации) – 44100 Гц;
4. число каналов – 1;
5. разрядность отсчёта (sample) – 16 бит.

5. Описание алгоритма анализа

Как говорилось ранее, за основу выбранного способа исследования аудиоданных был взят метод, приведённый в [6]. Предлагается внести в него некоторые изменения и обобщения.

Во-первых, предлагается не отделять блок данных от остальных блоков, поскольку в общем случае при внедрении информации внутрь контейнера (именно блок данных и служит таковым) остальные блоки остаются неизменными, а значит, статистические характеристики информации, хранимой в этих блоках, также остаются постоянным. В частном случае это позволит отследить как попытку изменения дополнительных полей, так и изменение заголовков, а непосредственное выделение блока данных (к примеру, запись его в отдельный файл) несущественно, но всё же замедлит процесс анализа. Помимо этого, ввиду небольших размеров остальных блоков, их обработка слабо скажется на скорости анализа.

Во-вторых, предлагается анализировать аудиофайлы целиком, не разделяя их на части. На ранних этапах разработки метода анализа были исследованы два подхода: с разделением на части и без разделения. Сравнение результатов работы алгоритма при использовании этих подходов показало, что использование разделения несколько увеличивает процент обнаружения файлов со стегосообщением, но незначительно. С другой стороны, за это незначительное увеличение приходится расплачиваться производительностью, так как, к примеру, число обращений к жёсткому диску (операции чтения/записи) увеличивает в число раз, равное количеству частей, на которые делится исследуемый аудиофайл. В общем случае производительность подхода с разделением на части была не лучше, чем без разделения.

В-третьих, ввиду отказа от разделения, предлагаемого в [6], критерий обнаружения требует пересмотра. Аналогично [6] предлагается использование порогового значения δ, но сравнивать его необходимо с абсолютным значением разницы коэффициентов сжатия исходного и модифицированного файлов.

Учитывая вышеописанные обобщения, перейдём к формальному описанию алгоритма.

Пусть $X = \{x_1, ..., x_n\}$ – последовательность байт, представляющая собой исследуемый файл. Через $N = |X|$ обозначим длину этой последовательности, иными словами N – размер исследуемого файла. Пусть даны два алгоритма ξ и ψ – алгоритм внедрения стегосообщения и алгоритм сжатия данных соответственно.

Последовательность действий:

1. Применим алгоритм ξ к последовательности X, получим $\tilde{X} = \xi(X)$.
2. Применим алгоритм ψ к последовательностям X и $\tilde{X}$, получим $Y = \psi(X)$ и $\tilde{Y} = \psi(\tilde{X})$. Обозначим через $M = |Y|$ и $\tilde{M} = |\tilde{Y}|$ длины полученных последовательностей Y и $\tilde{Y}$.

3. Вычислим коэффициенты сжатия. Получим $\gamma = \frac{M}{N} \cdot 100\%$ и $\tilde{\gamma} = \frac{\tilde{M}}{N} \cdot 100\%$.
4. Вычислим модуль разности коэффициентов сжатия $\Delta = |\gamma - \tilde{\gamma}|$ и сравним его значение с заранее выбранным значением δ. В случае если $\Delta < \delta$, считаем, что файл содержит стегосообщение. Иначе полагаем, что файл не содержит скрытых данных.

6. Экспериментальный анализ

Для экспериментального настроечного тестирования был подготовлен набор серий аудиофайлов, рассортированных по видам аудиоданных (речь, классическая музыка, песни).

Обработка осуществлялась следующим образом:

1. при помощи средств визуальной настройки задавался список исследуемых пустых аудиофайлов и параметры программы-анализатора: пороговое значение δ и процент наполнения ν исследуемого файла;
2. каждый файл из списка пропускался через программу-анализатор, работающую по указанному ранее алгоритму;
3. на выходе программы получался список файлов, содержащих скрытые данные, и их количество;
4. в случае неудовлетворительно результата выполнялась подстройка, и исследование повторялось заново.

При тестировании могут возникать следующие ошибки. Ошибка 1-го рода – ситуация, в которой анализатор считает пустой файл заполненным. Соответственно, при ошибке 2-го рода – заполненный файл считается пустым.

После проведения ряда экспериментов были получены следующие величины порогового значения δ и процента наполнения ν исследуемого файла:

Таблица 1. Значения δ и ν при использовании WinRAR® 3.80

Содержимое аудиофайла	**δ, %**	**ν, %**
Русская речь	0.2	25
Английская речь	0.2	25
Немецкая речь	0.1	25
Классическая музыка	0.1	25

Таблица 2. Значения δ и ν при использовании WinZIP® 11

Содержимое аудиофайла	**δ, %**	**ν, %**
Русская речь	0.80	25
Английская речь	0.80	25
Немецкая речь	0.60	25
Классическая музыка	0.50	25
Шансон	0.05	25
Динамичная музыка	0.05	75

Полученные значения были использованы для проведения тестирования на независимых данных. Обратим внимание, что пороговое значение δ падает с уменьшением корреляции внутри аудиофайла. Иными словами, отдельные звуки в файлах с речью более взаимосвязаны между собой, нежели в файлах с музыкой. А смешение речи и музыки приводит к значительному ослаблению таких связей. Этим и объясняется падение порогового значения δ и увеличение процента наполнения ν.

7. Результаты тестирования на независимых данных

На рис. 2 приведены данные по работе алгоритма с архиватором WinRAR® 3.80 и WinZIP® 11 на WAVE-файлах, содержащих русскую речь.

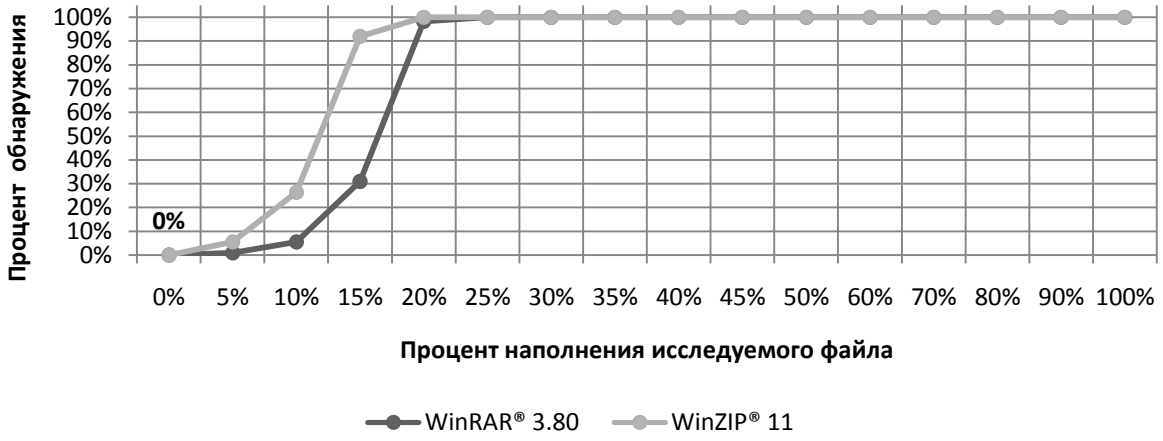

Рис 2. Сравнительные характеристики работы алгоритма для разных архиваторов

Из рисунка видно, что для дальнейших исследований предпочтительнее использовать архиватор WinZIP® 11. Далее предлагаются результаты работы алгоритма с архиватором WinZIP® 11 на WAVE-файлах, содержащих классическую музыку и шансон (см. рис. 3, 4).

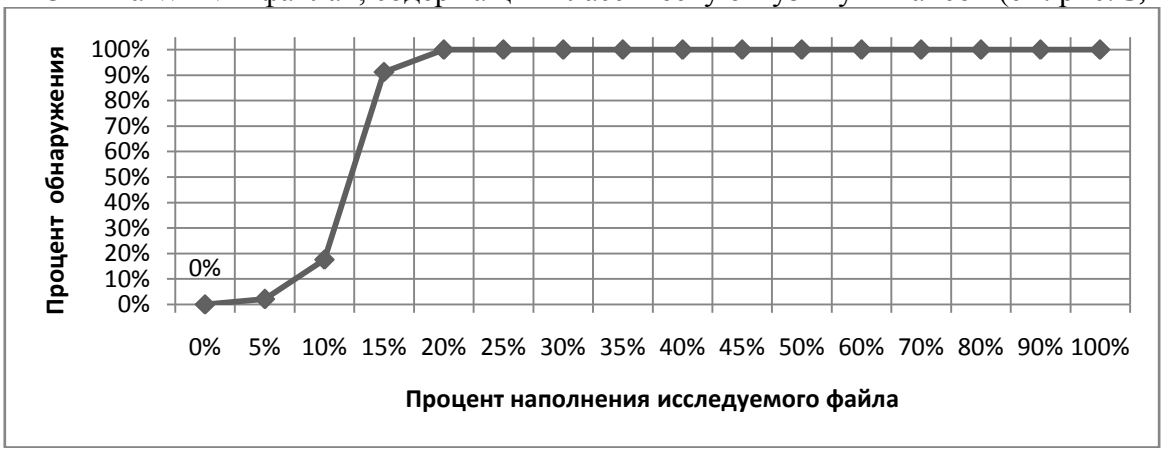

Рис 3. Результат работы алгоритма на WAVE-файлах, содержащих классическую музыку

Рис 4. Результат работы алгоритма на WAVE-файлах, содержащих шансон

Обратим внимание на следующий график зависимостей (см. рис.5). На нём представлен результат работы алгоритма с архиватором WinZIP® 11 на WAVE-файлах, содержащих динамичную музыку, который наглядно подтверждает ранее сделанные выводы. Ввиду достаточно слабой корреляции внутри аудиофайла достаточно сложно отделить файл со стегосообщением от не содержащего такового данным методом.

Рис 5. Результат работы алгоритма на WAVE-файлах, содержащих динамичную музыку

8. Выводы

Таким образом, данный метод позволяет в автоматическом режиме выявлять факт наличия скрытых данных внутри аудиофайла. Заметим, что в зависимости от выбранного метода сжатия варьируется и процент выявленных файлов. Как видно из графиков, WinZIP® 11 имеет явное преимущество перед WinRAR® 3.80, и в общем случае ошибка при заполнении контейнера на 25 % и более не превышает 1.5 % для отдельных типов аудиофайлов. С уменьшением корреляции внутри аудиофайла происходит резкое снижение порогового значения δ и увеличение процента наполнения ν.

Литература

1. Стеганография [Электронный ресурс]. URL: http://www.kriptolog.net/blog/steganografija (дата сообщения: 29.05.2007).
2. Барсуков В. С., Романцов А. П. Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века. [Электронный ресурс]. URL: http://st.ess.ru/publications/articles/steganos/steganos.htm (дата сообщения: 29.05.2007).
3. Стеганография – Энциклопедический Фонд России [Электронный ресурс]. URL: http://www.russika.ru/termin.asp?ter=3474 (дата сообщения: 29.05.2007).
4. В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. Цифровая стеганография. – Солон-Пресс, 2002. – 272 с.
5. Boris Ryabko and Jaakko Astola. Universal codes as a basis for time series testing statistical methodology. 2009. v. 3. p.375 – 397.
6. Жилкин М.Ю. Стегоанализ графических данных на основе методов сжатия // Сборник научных трудов «Вестник СибГУТИ». - 2008. - №2. – стр. 62 – 66.
7. B. Ryabko, D.Ryabko. Asymptotically optimal perfect steganographic systems. Problems of Information Transmission. 2009. v. 45, No.2. p. 184 – 190.

Статья поступила в редакцию 21.02.2010

Забелин Максим Александрович
магистрант кафедры прикладной математики и кибернетики СибГУТИ,
тел. (383) 3-55-44-54, e-mail: sibsuti_ivt_prog@mail.ru

Audio-data steganalysis based on compression method

M.A. Zabelin

A method of detecting data hidden in the least significant bits of audio files in WAVE format is suggested. High effectiveness of the method is experimentally demonstrated.

Keywords: audio-files steganography, steganalisis, WAVE format.