УДК 004.056

Стегоанализ аудиофайлов, базирующийся на алгоритмах сжатия

С. Ю. Очимов

Предлагается универсальный метод стегоанализа WAVE-файлов, базирующийся на алгоритмах сжатия. Приведены результаты работы предлагаемого метода на большой серии файлов, которые показывают, что эффективность метода выше, чем у ранее известных.

Ключевые слова: аудиостегоанализ, WAVE-файлы, LSB-методы, сжатие данных.

1. Введение

Предположим, что имеется открытый канал связи, по которому необходимо отправить секретное сообщение. Пусть Алиса и Боб – это отправитель и получатель некоторого сообщения, а Ева – это его перехватчик. Существует два сценария отправки сообщения. Первый – Алиса и Боб договариваются о секретном ключе. Алиса, предварительно зашифровав сообщение, посылает его. Боб принимает сообщение и, используя известный ключ, расшифровывает его. Ева перехватывает сообщение, но не может его расшифровать, т.к. не знает секретного ключа. Второй сценарий передачи информации следующий. Алиса отправляет не вызывающий подозрения файл, содержащий секретное сообщение, например аудиофайл с записью какой-нибудь известной композиции. Боб получает этот файл и, зная способ, извлекает секретное сообщение. При втором сценарии передачи данных скрывается сам факт пересылки секретного сообщения; в этом и заключается задача стеганографии.

Предполагается, что при помощи стеганографического алгоритма секретное сообщение встраивается в некий файл, называемый *контейнером*, так, чтобы не было заметных изменений этого файла. Контейнер пересылается по открытому каналу связи, не вызывая подозрений. Секретное сообщение извлекается получателем при помощи специального алгоритма. В качестве контейнеров могут быть использованы любые файлы, для которых придуманы такие алгоритмы. Наибольший интерес для использования в качестве контейнеров представляют файлы распространённого типа содержимого, например, фотографии или аудиофайлы. Действительно, если по сети передаётся альбом популярной группы, то маловероятно, что он вызовет подозрения. На сегодняшний день существует множество стеганографических алгоритмов[1, 2, 3], которые используют в качестве контейнеров звуковые и видеофайлы, фотографии, исполняемые программы, текстовые файлы и другие.

Звуковые и видеофайлы, как правило, довольно избыточны, поэтому незначительное изменение потока данных не приводит к заметным искажениям. Таким образом, например, изменяя специальным образом звуковую дорожку, можно внедрить секретное сообщение, не внося заметных изменений и тем самым скрыть факт его наличия. Наиболее распространённым алгоритмом встраивания информации является алгоритм LSB[1]. Данный алгоритм работает путём встраивания скрытой информации в наименее значимые биты. Такой способ встраивания применим, например, к цифровому изображению, где каждая точка описана тремя составляющими её цвета RGB (RGB – аббревиатура от трёх составляющих 24-битного

[1] От англ. Least-Significant Bit – наименее значимый бит.

способа хранения цвета: Red, Green, Blue). Наряду с этим алгоритм LSB применим и для внедрения скрытой информации в аудиоформат WAVE.

Файлы формата WAVE содержат так называемую простую импульсно-кодовую модуляцию сигнала. Звуковая волна преобразуется в набор целочисленных значений путём дискретизации сигнала. Таким образом, если исходный аналоговый уровень звука был 4.68, то при импульсно-кодовой модуляции уровень будет преобразован в 5. При проигрывании звука последовательность бит преобразуется в звуковую волну методом цифро-аналогового преобразования в зависимости от параметров дискретизации: размеров аудиообразца[2], частоты дискретизации и количества каналов. Таким образом, при преобразовании сигнала из вещественного значения в целое появляется погрешность, равная единице. Смена значения младшего значащего бита не приведёт к ощущаемым изменениям.

В сети интернет встречается множество программ для встраивания скрытой информации в различные мультимедиа форматы, такие как Bitmap, JPEG, WAVE, MPEG Layer 3, AIFF. Пример стеганографических программ: Gif-It-Up для файлов формата GIF; JPEG/JSteg, JP Hide-&-Seek (JPHS) by Allan Latham – для файлов формата JPEG; PGE, ScyTale, Out-Guess – в различные форматы изображения; S-Tools, Hide4PGP для файлов формата GIF, Bitmap, WAVE. Все вышеупомянутые программы находятся в свободном доступе в сети интернет и доступны для использования.

Целью данной работы является построение универсального алгоритма стегоанализа аудиоданных формата WAVE. Данный алгоритм также может быть применён и к другим форматам с подобным принципом хранения звука (AIFF, CD audio (CDDA)), либо к производным форматам, которые используют для уменьшения занимаемого объёма неискажающее сжатие. Разработанный алгоритм анализа основывается на применении методов универсального кодирования, которые используются для сжатия данных. Этот подход был предложен Б. Я. Рябко и был успешно реализован в ряде работ [1, 2, 4]. Основная его идея заключается в том, что после внедрения сообщения в контейнер нарушается статистическая структура контейнера, вследствие чего повышается его энтропия, поэтому заполненный контейнер будет сжиматься хуже, чем исходный (незаполненный).

Был построен универсальный, т.е. рассчитанный на обнаружение данных, встраиваемых различными методами, алгоритм стегоанализа аудиоданных формата WAVE. В алгоритм анализа были введены несколько параметров, которые позволили регулировать значения ошибок на пустых и заполненных контейнерах. Информация в контейнеры внедрялась при помощи общедоступных программ [3, 5]. В ходе проведённых испытаний подобраны параметры, при которых алгоритм показал наилучшее соотношение ошибок на пустых и заполненных контейнерах. Предлагается вариант алгоритма, для которого ошибка на пустом контейнере составила 5 %, при заполнении контейнера свыше 70 % все тестируемые файлы обнаруживались без ошибок. При сравнении полученных результатов с результатами подобных работ выяснилось, что данный метод обладает большей эффективностью.

Остановимся кратко на содержании статьи. В разд. 2 вводятся основные понятия, приводится описание стандарта WAVE и краткий исторический обзор. В разд. 3 приводится описание метода стегоанализа и алгоритма. В разд. 4 описаны экспериментальные исследования и показаны наилучшие результаты. В разд. 5 проведено сравнение данного метода с существующими методами стегоанализа.

[2] Размер аудиообразца может быть 8-бит, либо 16 бит в зависимости от необходимого качества звука.

2. Основные понятия и описание стандарта WAVE

Определим для краткости нижеследующие понятия ошибок. Ошибкой I рода назовём ситуацию, когда пустой контейнер принимается за заполненный. Ошибкой II рода назовём случай, когда заполненный контейнер принимается за пустой.

Остановимся на более детальном описании анализируемого стандарта. WAVE (Waveform Audio File Format) создан инженерами Microsoft и Intel в августе 1991 года. Он разрабатывался в качестве стандартного формата хранения звуковых данных в операционной системе Windows 3.1 [6].

Данные, имеющие отношение к мультимедиа (звук, видео и т. п.) хранятся в файлах в так называемом RIFF[3] формате. Как WAVE-файлы, содержащие звук, так и avi-файлы, содержащие видеоинформацию, имеют формат RIFF. Файл в формате RIFF содержит вложенные фрагменты. Внешний фрагмент состоит из заголовка и области данных (рис. 1). Первое двойное слово заголовка содержит четырехбайтный код FOURCC, который идентифицирует данные, хранящиеся во фрагменте. Второе двойное слово заголовка – размер области данных в байтах (без учёта размера самого заголовка). Заметим, что формат RIFF не описывает формат данных. Практически файл в формате RIFF может содержать любые данные для мультимедиа. Область, обозначенная на рис. 1 как "Данные", может содержать внутри себя другие фрагменты. Для файла, в котором хранятся звуковые данные (wav-файл), эта область содержит идентификатор данных "WAVE". Файл может дополнительно содержать фрагменты других типов, поэтому не следует думать, что заголовок wav-файла имеет фиксированный формат. Например, в файле может присутствовать фрагмент "LIST" или "INFO", содержащий информацию о правах копирования и другую дополнительную информацию.

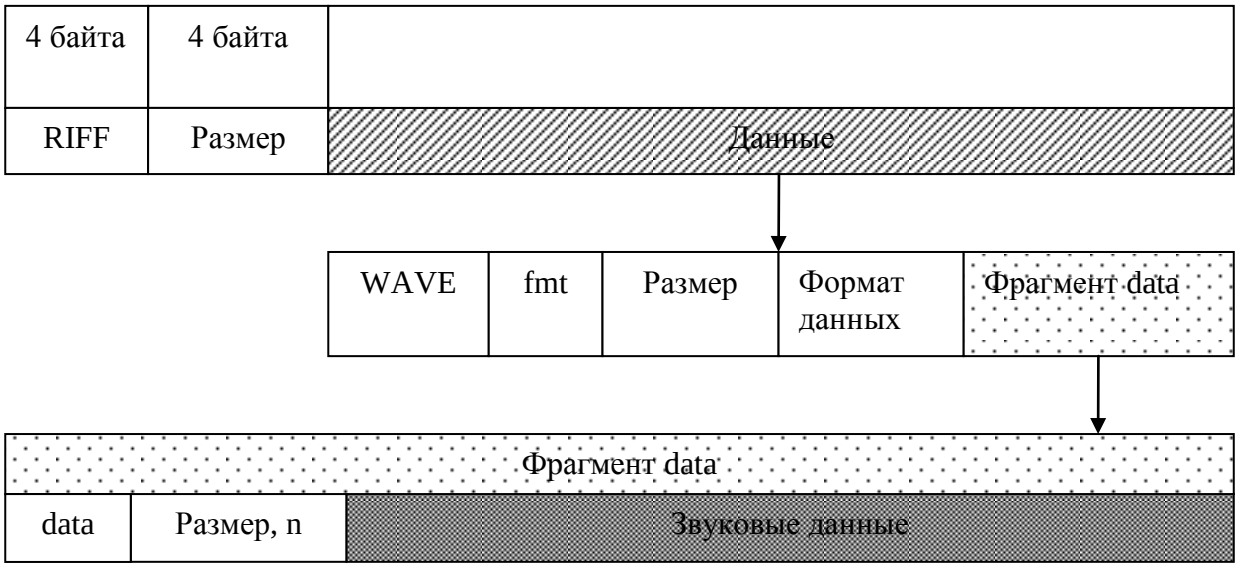

Рис. 1. Структура WAVE файла

Для задачи стегоанализа фрагмент data представляет наибольший интерес. Он состоит из определяющего поля «data», размера звуковых данных и дискретного набора значений. Звуковые данные содержат так называемую простую импульсно-кодовую модуляцию сигнала. Это означает, что звуковая волна преобразуется в набор целочисленных значений путём дискретизации аналогового сигнала. К набору значений фрагмента data и применяется внедрение сообщения методом LSB. Таким образом, ёмкость WAVE-контейнера составляет $P_{wav} = n/8$ байт, где n – размер звуковых данных фрагмента data в байтах.

[3] Resource Interchange File Format – от англ. формат файла обмена ресурсами

Первые программы по стеганографии wav появились в 1996 году, это S-Tools, Hide4PGP 2.0. Обе реализации добавляют скрытую информацию в аудиофайл методом LSB. Главное их отличие в следующем: программа S-TOOLS заполняет младшие биты контейнера последовательно, в то время как HIDE4PGP использует разбросанное по всему файлу изменение младших бит.

Однако работы по стегоанализу WAVE вышли только в 2005 [7] и в 2008 [8] годах. В работе [7] строится специальная статистическая модель, с помощью которой анализируются отклонения аудиоданных от этой модели, в результате чего выносится результат о наличии или отсутствии скрытой информации в файле. В работе [8] рассматривается метод, основанный на критерии хи-квадрат, и методы анализа пар фрагментов и дифференциальной гистограммы изображения.

3. Описание метода стегоанализа и алгоритма

Идея предлагаемого метода заключается в том, что файл, содержащий однородные данные, имеет свою статистическую структуру. Если использовать его в качестве контейнера для секретного сообщения, то после внедрения сообщения в контейнер нарушится статистическая структура контейнера и повысится его энтропия. Таким образом, при использовании алгоритмов сжатия исходный («пустой») контейнер сжимается, как правило, лучше, чем заполненный. Значит, если степень сжатия предполагаемого контейнера больше некоторого порогового значения, то с большой вероятностью можно сказать, что контейнер пуст, в противном случае с большой вероятностью можно судить о присутствии сообщения в контейнере.

Метод анализа заключается в сравнении коэффициентов сжатия исходного контейнера и его полностью заполненной копии. Полностью заполненная копия получается при помощи псевдослучайного изменения младших бит исходного («пустого») контейнера. К обоим файлам применяется метод сжатия данных и анализируются их коэффициенты сжатия. Если эти коэффициенты близки по значению, то весьма вероятно, что исходный файл содержал скрытое сообщение. И напротив, при большой разнице в коэффициентах сжатия выносится результат об отсутствии скрытой информации в файле.

При практической реализации этого метода контейнер и его заполненная копия рассматривается не целиком, а делятся на несколько равных частей. Это позволяет увеличить точность метода, кроме того, вводится дополнительный параметр, регулирующий соотношение ошибок I и II рода. Заметим, что метод анализа применяется не ко всему файлу, а именно к фрагменту файла, содержащему звуковые данные.

Формально разработанный алгоритм выглядит следующим образом. Пусть $X = \{x_1, \dots, x_n\}$ – последовательность байт звуковых данных (см. рис. 1), $|X| = N$ – длина последовательности. Последовательность X разобьем на k равных отрезков $X_i, i = \overline{1,k}$. Пусть $\Psi(X)$ – алгоритм сжатия, применённый к X. Введём величину $f(X,n) = |\Psi(X_n)|/|X_n|$ – коэффициент сжатия отрезка n последовательности X универсальным кодом Ψ.

Обозначим через $\varphi(X)$ псевдослучайное изменение младших бит последовательности X (алгоритм LSB). Тогда $Y = \varphi(X)$ – заполненный контейнер X. Введём величину

$$\delta(X,n) = |f(X,n) - f(Y,n)| \quad (1)$$

Для определения факта включения секретного сообщения выбирается пороговое значение для величины δ и производится оценка количества отрезков, на которых значение величины не превышает порог. Если таких отрезков больше, чем половина от их общего количества, то считается, что исходная последовательность X содержала скрытые данные; в противном случае последовательность X считается «пустой». Порог можно варьировать, тем са-

мым регулируя уровни ошибок программы на контейнерах с разной степенью наполнения, как будет показано в разд. 4.

Итак, параметры алгоритма:

1. *Пороговое значение δ (1).* Определяет положительный или отрицательный результат теста. Его увеличение приводит к большей чувствительности, т.е. увеличению ошибок на пустых контейнерах и уменьшению на заполненных;
2. *Размер блока.* В основном влияет на скорость анализа при использовании внешних архиваторов (в данной реализации);
3. *Архиватор.* Влияет как на скорость работы, так и на точность результата.

4. Экспериментальные исследования и результаты

В ходе экспериментальных исследований была подготовлена большая серия звуковых файлов формата WAVE Windows PCM. Звуковые файлы были получены частично из локальной сети, частично из интернет-источников [9]. Использовались только файлы формата PCM, тип формата[4] 1, частота дискретизации 8 кГц – 44 кГц, количество каналов 1 – 2, бит на отсчёт 8 – 16 бит, размер файла 5 – 300 Кб. Эти файлы использовались в качестве контейнеров для общедоступных программ внедрения скрытых сообщений в файлы формата WAVE. Для разбросанного заполнения использовалась программа `Hide4PGP 2.0` [3]. На вход программы подавались исходные контейнеры с различной степенью их наполнения: 0 %, 10 %, 20 %, …, 100 %. Для удобства анализа в программе реализована возможность сохранения всех собранных данных на листе Excel в виде таблицы. При проведении более детального анализа собранных данных такая таблица очень удобна, так как её можно без труда сортировать, искать в ней минимум, максимум, СКО[5] и т.д.

Назовём внешним архиватором архиватор, который вызывается из программы как консольное приложение, внутренним – архиватор, доступный в виде библиотеки подключаемой непосредственно к программе. В качестве архиваторов в программе возможно было использование как внешних архиваторов, так и внутренних. Итак, были использованы множество архиваторов, таких как RAR, ZIP, GZIP, библиотека zlib с реализацией на платформе .net [10] (ниже просто zlib), Slim, uda, bee. Подобрано значение размера блока, равное 5 %, и представляющие наибольший практический интерес значения δ (1).

Результат представлен на рис. 2. Здесь показана зависимость количества файлов (в процентах), в которых обнаружен факт сокрытия, от степени наполнения контейнера. Как видно из диаграммы, лучший результат показал архиватор zlib. По скорости анализа архиватор zlib также оказался самым предпочтительным: zlib – 147 килобайт/сек, RAR – 8.5 килобайт/сек, ZIP – 3.3 килобайт/сек. Стоит отметить, что при скорости 147 килобайт/сек при помощи данного метода можно проводить анализ потокового звука. Скорость потока, например, при высоком качестве стерео 44 кГц 16-бит равна 88 килобайт/сек.

[4] Тип формата в данном случае – это wFormatTag из поля формат данных заголовка RIFF.
[5] СКО – среднеквадратическое отклонение.

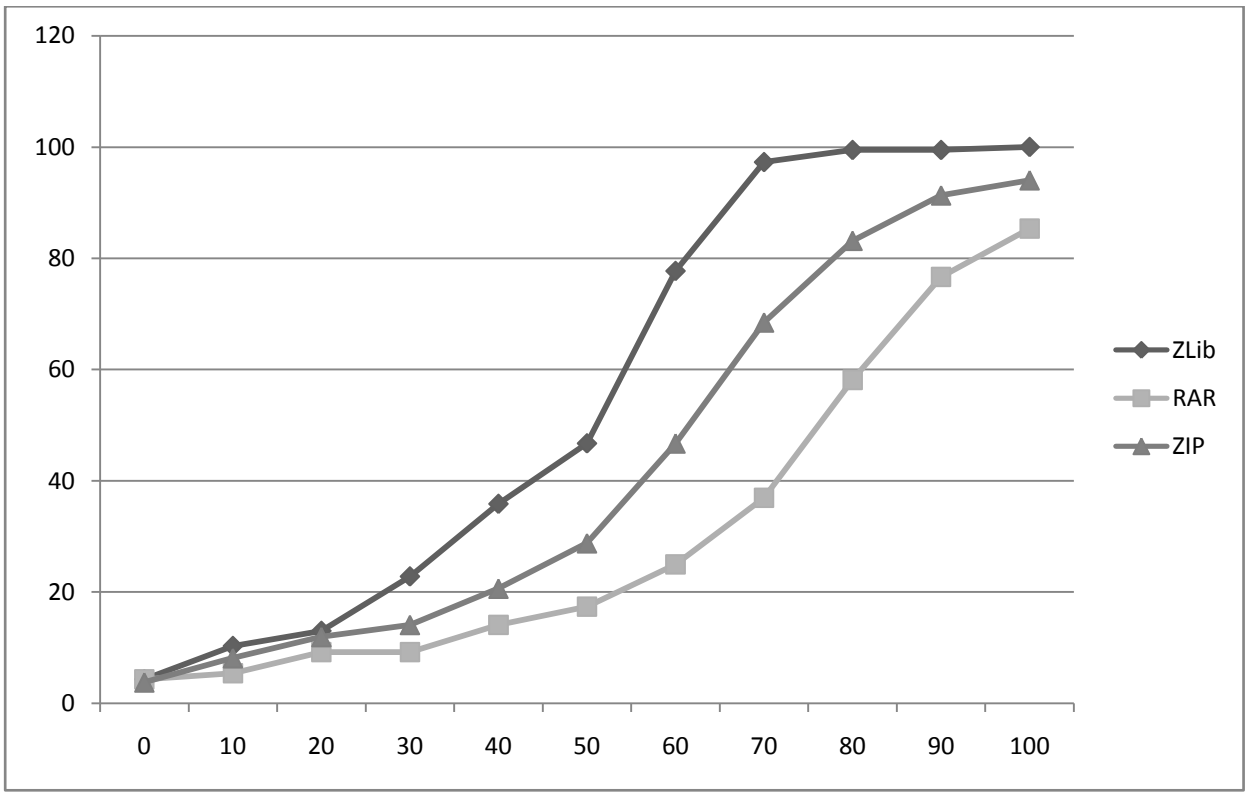

Рис. 2. Зависимость процента файлов, в которых обнаружен факт сокрытия информации на разных архиваторах (zlib, RAR, ZIP) в зависимости от наполнения контейнера. Уравнена ошибка на пустых контейнерах (4 %)

Изменение параметра δ позволяет регулировать соотношение ошибок I и II рода. Пример для архиватора zlib приведён в табл. 1. Первоначально была построена общая таблица с результатами тестов для δ от 0.15 до 10 с шагом 0.05. Табл. 1 была получена путём выбора такого набора значений δ из первоначальной таблицы, при котором ошибка первого рода изменялась от 0 до 10 с шагом в единицу.

Таблица 1. Количество файлов в процентах, определённых как содержащие скрытую информацию, в зависимости от порогового значения δ и процента наполнения контейнера. Архиватор zlib.

Пороговое значение δ, %	Процент наполнения контейнера, %										
	0	10	20	30	40	50	60	70	80	90	100
0.15	0	0	1	2	3	4	8	13	24	41	48
0.5	1	3	5	9	10	18	40	70	95	95	98
0.65	2	4	9	11	20	28	52	85	99	98	99
0.7	3	6	9	12	21	30	55	90	99	99	99
1.05	4	10	13	23	36	47	78	97	99	99	100
1.15	5	10	14	24	40	50	84	99	100	99	100
1.2	6	11	16	26	41	53	88	99	100	100	100
1.25	8	11	17	28	43	55	88	99	100	100	100
1.5	9	15	23	37	53	66	92	100	100	100	100
1.65	10	17	26	41	57	72	96	100	100	100	100

5. Сравнение с известными методами стегоанализа

Рассматриваемый в работе универсальный метод стегоанализа WAVE-файлов более эффективен в сравнении с известными аналогами. Так, наиболее близкий по принципу метод описывается в работе [7]. В данной работе приводится универсальный метод стегоанализа, который основан на анализе естественных закономерностей записанной речи. Статистическая модель основана на ошибках в представлении аудиоспектрограмм при использовании линейного базиса. Для заполнения контейнеров также используется программа Hide4PGP. Сравним разработанный метод с описанным в работе [7] (см. табл. 2).

Таблица 2. Сравнение эффективности разработанного метода стегоанализа с методом, описанным в [7]. Показано количество файлов в процентах, определённых как содержащие скрытую информацию

Название метода	Процент наполнения контейнера, %				
	0	25	50	75	100
Метод [10]	1.9	2.7	7.4	30.8	83.1
Разработанный	1	6	18	80	98

Как видно из табл. 2, предложенный метод стегоанализа выигрывает у метода, описанного в [7].

Работа [8] также посвящена стегоанализу WAVE файлов. В ней рассматриваются три метода стегоанализа: Chi-square detection[6], SPA (Sample pairs analysis[7]) и DIH (Differential Image Histogram[8]). Подробное описание методов можно найти в [8].

Для сравнения эффективности использовался результат тестирования методов, описанный в литературе [8], который применялся к 40 аудиофайлам. Согласно результату метода, основанного на критерии хи-квадрат [8], качественное определение вложений данным методом начинается при заполнении 50 % и выше от ёмкости контейнера. Эффективность разработанного метода стегоанализа превосходит данный результат.

Результаты сравнения методов приведены в табл. 3. Методы DIH и SPA имеют высокое значение ошибок I рода и не позволяют производить её регулировку, поэтому для сравнения с разработанным методом ошибки I рода были выровнены (по табл. 1).

Таблица 3. Сравнение разработанного метода стегоанализа с методами SPA и DIH. Показан процент правильно определённых файлов.

Метод стегоанализа	Процент наполнения контейнера, %									
	0	3	5	7	10	20	30	40	50	60
DIH	78	76	100	95	100	100	100	100	100	100
Разработанный	78	25	28	31	33	51	68	87	93	100
SPA	70	81	81	81	90	95	100	100	100	100
Разработанный	70	35	40	45	49	64	85	95	100	100

Авторы [8] не указывают конкретно, какой именно метод встраивания скрытой информации они использовали. Здесь важно отметить, что эффективность стеготеста существенно зависит от алгоритма включения скрытой информации.

[6] Chi-square detection – с англ. Обнаружение хи-квадрат.
[7] Sample pairs analysis – с англ. Анализ пробы пар.
[8] Differential Image Histogram – с англ. Дифференциальная гистограмма изображения.

Литература

1. Елтышева Е. Ю., Фионов А. Н. Построение стегосистемы на базе растровых изображений с учётом статистики младших бит // Вестник СибГУТИ. 2009. № 1. С. 67 – 84.
2. Нечта И. В. Стеганография в файлах формата Portable Executable // Вестник СибГУТИ. 2009. № 1. С. 85 – 89.
3. [Электронный ресурс]. Freeware program of steganography bmp, wav, voc. URL: http://www.heinz-repp.onlinehome.de/Hide4PGP.htm. (дата обращения: 13.02.2008).
4. Жилкин М. Ю. Стегоанализ графических данных на основе методов сжатия // Вестник СибГУТИ. 2008. № 2. С. 62 – 66.
5. Pulcini, G., 2005. Stegowav. [Электронный ресурс]. URL: http://www.jjtc.com/stegoarchive/stego/softwaredos.htm (дата обращения 10.10.2009).
6. Фролов А.В, Фролов Г.В Мультимедиа для Windows. М.: Диалог-МИФИ, 1995г.,204с.
7. M. Johnson, S. Lyu and H. Farid. Steganalysis of recorded speech. Proc. SPIE, 2005, vol. 5681, p.664 – 672.
8. CHEN Ming, ZHANG Ru, NIU Xin-xin, YANG Yi-xian. steganalysis of LSB Steganography in wav audio // Computer Engineering. February 2008. Vol.34. № 4.
9. The wav surfer. [Электронный ресурс]. URL: http://www.wavsurfer.com. (дата обращения: 10.09.2009).
10. zlib.net library. [Электронный ресурс]. URL: http://www.zlib.net. (дата обращения 10.11.2009).

Статья поступила в редакцию 25.01.2010

Очимов Сергей Юрьевич
Аспирант кафедры прикладной математики и кибернетики СибГУТИ,
e-mail: dlasvazi@ngs.ru

Steganalysis of audiodata based on data compression algorithms

S. Yu. Ochimov

Universal method of steganalysis of WAVE files based on compression algorithms is proposed. The results are obtained on a large series of files, which show that the effectiveness of the method is higher than that of previously known method.

Keywords: audio steganalysis, WAVE files, LSB-methods, data compression.