УДК 003.26.09 + 004.056 Вестник УрФО № 4(30) / 2018, с. 5–10

Сидоркина И. Г., Кубашева Е. С., Соловьев М. Г., Галанина Н. А.

DOI: 10.14529/secur180401

ПОДХОД К РЕАЛИЗАЦИИ АЛГОРИТМОВ РАБОТЫ С ЦИФРОВЫМ ВОДЯНЫМ ЗНАКОМ В АУДИОФАЙЛАХ ДЛЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Методы стеганографии получили активное развитие только в последние годы. Одно из направлений стеганографии – встраивание цифровых водяных знаков (ЦВЗ) в контейнеры, представляющие собой файлы разнородных данных. ЦВЗ – это информация, которая внедряется в файл, с целью контроля правомерного использования информационного объекта. ЦВЗ бывают видимые и скрытые. Видимые ЦВЗ легко обнаружить и удалить. Невидимые ЦВЗ встраиваются в компьютерный файл, не меняя основной функциональности файла. Актуальность вопроса применения ЦВЗ связана с необходимостью обеспечения безопасности и достоверности информации, которой владеет пользователь. Предложенные алгоритмы реализации ЦВЗ в аудиофайле демонстрируют обеспечение эффективной защиты прав автора.

Ключевые слова: *стеганография, цифровой водяной знак, файловый контейнер, формат данных, аудиофайл, преобразование Фурье, автокорреляционная функция (АКФ), АКФ кепстра, алгоритм встраивания ЦВЗ, алгоритм извлечения ЦВЗ.*

APPROACH TO REALIZING WORKING ALGORITHMS WITH DIGITAL WATER SIGN IN AUDIO FILES FOR INFORMATION SECURITY SYSTEMS

The methods of steganography have been actively developed only in recent years. One of the directions of steganography is the embedding of digital watermarks (DWs) into containers, which are files of heterogeneous data. CEH is information that is embedded in a file, in order to control the legitimate use of the information object. CEHs are visible and hidden. Visible CEHs are easy to detect and remove. Invisible CEHs are built into the computer file without changing the main functionality of the file. The relevance of the application of CEH is related to the need to ensure the security and reliability of information that the user owns. The proposed algorithms for implementing the CEH in the audio file demonstrate the effective protection of the author's rights.

Keywords: *steganography, digital watermark, file container, data format, audio file, Fourier transform, autocorrelation function (ACF), AKF cepstrum, embedding algorithm, CEV extraction algorithm.*

Для эффективного применения технологий ЦВЗ [1], необходимо обеспечить аудио и визуальную незаметность сообщений, сохранить исходное качество исходного контейнера и, одновременно, обеспечить высокую достоверность извлечения сообщения с учетом возможных непреднамеренных и преднамеренных воздействий в канале передачи информации.

Так как информация представляет собой передаваемое знание, то приведем пример абстрактной модели канала скрытной передачи информации (Рис. 1). Имеется отправитель, получатель и противник, который хочет завладеть этой информацией. Но противником может быть не один человек, а группа, и они могут ставить себе различные цели: например, уничтожение скрытой информации, обнаружение факта передачи, подделка или искажение информации, навязывание ложной. Поэтому для различных случаев методы противодействия различаются. Например, это попытки скрыть факт передачи информации, попытки в открытом канале связи создать трудности для перехвата. И таких вариантов много, и на каждом этапе решается задача обеспечения надежности [2].

Цифровое изображение представляет собой матрицу пикселей. Изменение младшего бита LSB изображения обычно не заметно для глаза человека, поэтому его можно использовать для встраивания информации. Таким образом, графические файлы позволяют передавать большое количество данных. Так для картинки 1024x768 можно в закрытом виде передать 294912 байт, используя метод наименее значимого бита – LSB.

Реализация методов цифровой стеганографии включает в себя следующую последовательность:

1) встраивание ЦВЗ(watermarking);

2) встраивание заголовков;

3) встраивание номеров идентификации;

4) встраивание информации для скрытой передачи.

Выделим следующие два принципа компьютерной стеганографии: файлы, не требующие особой аутентичности (например, медиафайлы), могут видоизменяться до определенной степени без потери функциональности и человеческие органы неспособны идентично различать изменения в таких данных.

ЦВЗ — это специальная метка, идентифи-

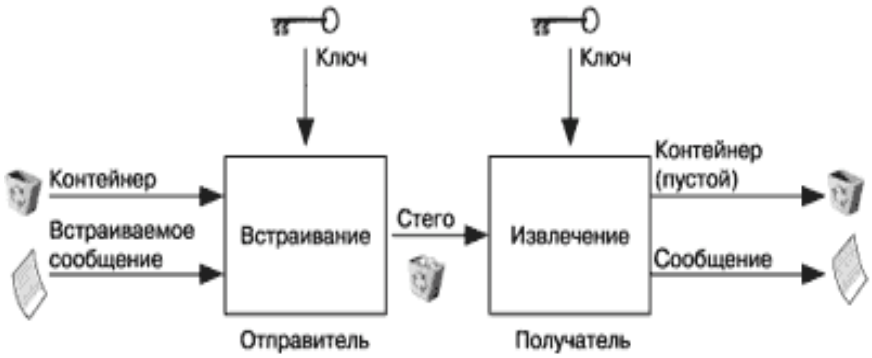

Рис. 1. Обобщенная модель стегосистемы

цированная и внедренная для защиты авторских прав мультимедийных файлов. Как правило, они (метки) встроены в цифровые данные, с целью иметь возможность контролировать файлы. Но, как известно, система защиты информации должна выполнять свои функции даже при полной информативности злоумышленника о структуре и алгоритмах ее функционирования [3]. Невидимые ЦВЗ внедряются в цифровые объекты таким образом, чтобы пользователю было крайне сложно выявить добавленную метку. Например, если ЦВЗ внести на графическое изображение, то мы можем изменить яркость определенных точек, тем самым при просмотре рисунка человек может не заметить следов искусственного изменения.

1) человек, использующий мультимедийный файл, визуально не должен заметить встроенную метку;

2) возможность для автора обнаружить несанкционированное использование файла;

3) невозможность удаления метки сторонними лицами, не имеющими на то право;

4) устойчивость к изменениям файла носителя.

Атаки, предназначенные для систем ЦВЗ [4], можно классифицировать, например, следующим образом:

1) Атаки, которые служат для удаления ЦВЗ или его порчи. В задачу таких атак не входит извлечение стегосообщения. В качестве

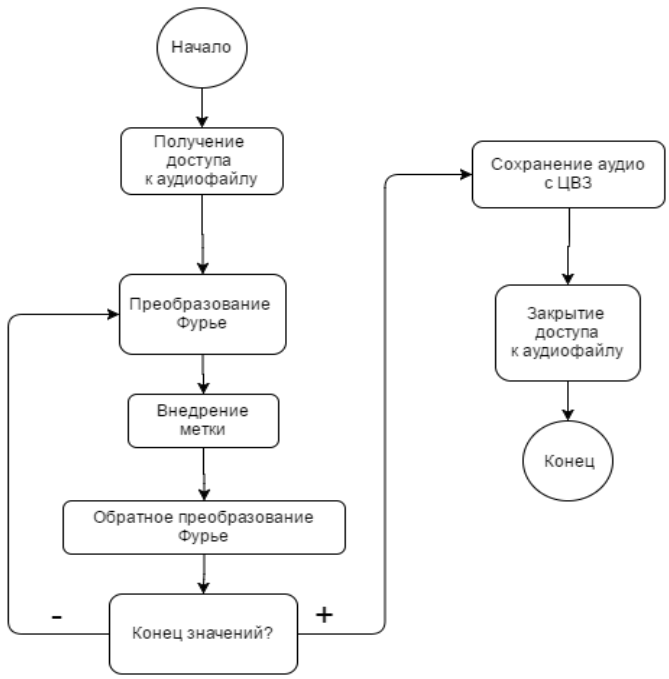

Рис. 2. Общая схема внедрения ЦВЗ

ЦВЗ должны отвечать ряду требований, таких как:

примера можно привести линейную фильтрацию, добавление шума;

2) атаки, направленные на извлечение цифровой метки. Например, статистическое усреднение;

3) атаки, предназначенные для затруднения извлечения ЦВЗ. В данном случае, как правило, происходит искажение самого контейнера. Сюда относятся различные сдвиги, повороты, то есть приемы, связанные с масштабированием;

4) атаки, главная задача которых состоит в создании ложных ЦВЗ.

Это один из вариантов классификации, в других источниках атаки могут классифицироваться по другим параметрам.

Продемонстрируем схемы внедрения ЦВЗ (Рис.2) и извлечения ЦВЗ (Рис.3) в аудиофайл.

Аудио файл представляет собой последовательность бит, в которых представлен частотный спектр звука. Для получения доступа

Для встраивания и извлечения цифрового водяного знака на основе предложенных схем в аудио файл разработаны и исследуются следующие алгоритмы.

Алгоритм встраивания.

1) переводится встраиваемое сообщение в двоичный код;

2) определяется вместительность контейнера и размер встраиваемого сообщения. В случае если сообщение не помещается в контейнер, завершить выполнение с ошибкой;

3) в зависимости от частоты дискретизации, осуществляется разделение контейнера на равные части, для того, чтобы обеспечить пропускаемую способность 16 бит в секунду;

4) рассматривается первая часть контейнера;

5) создается эхо-сигнал путем смещения оригинального сигнала на значение задержки соответствующее текущему биту;

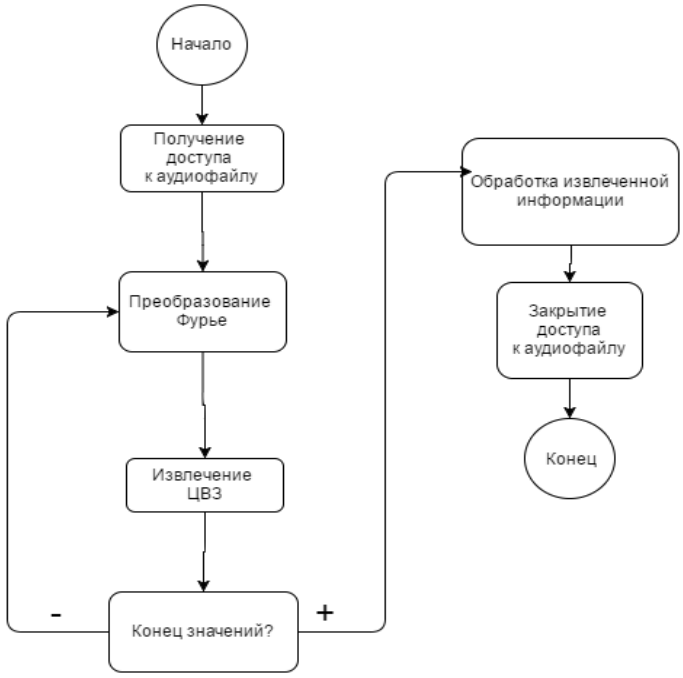

Рис. 3. Общая схема извлечения ЦВЗ

к этим числовым данным, а также возможность воспроизводить аудио использована библиотека OpenAl, которая содержит в себе необходимые функции для работы с аудио.

Далее внедряем данные в аудио файл. После того, как получили значения частотного спектра звука, формируем их для дальнейшего внедрения с помощью преобразования Фурье. Само внедрение происходит методом Хола-Тиркеля [5], после чего мы сохраняем наш аудио файл с внедренным ЦВЗ.

6) уменьшается амплитуда эхо-сигнала. Так же требуется создать спадающий и возрастающий фронты в конце и начале эхо-сигнала соответственно для предотвращения появления резких переходов;

7) наложение эхо-сигнала на оригинальный сигнал.

Алгоритм извлечения.

1) перевести проверяемое сообщение в двоичный код;

2) сверить вместительность контейнера и

размер проверяемого сообщения. В случае если сообщение не помещается в контейнер, завершить выполнение с ошибкой.

В зависимости от частоты дискретизации, разделить контейнер на равные части, для того, чтобы обеспечить пропускаемую способность 16 бит в секунду.

1) Берем первую часть контейнера;

2) Посчитать АКФ кепстра для текущего фрагмента контейнера;

3) Сравнить значения АКФ кепстра соответствующие времени равному значению смещения эхо-сигналов. Если значение на уровне смещения равного «1» больше, чем «0», то встраивался бит 1;

4) Сравнить полученный бит с соответствующим битом проверяемого сообщения;

5) При условии, что все биты совпали (возможен вариант проверять процент совпадения, т.к. метод эхо-сигналов обладает не 100% вероятностью правильного извлечения бит), делаем вывод о том, что аудио файл защищен.

Алгоритмы по области встраивания относятся к частотным, они достаточно сложны в плане вычислений и затрачиваемых ресурсов. Большинство известных алгоритмов создания ЦВЗ [6,7] имеет общий недостаток, а именно все алгоритмы встраивания информации в объекты образуют конечное множество вариантов, вследствие чего они могут быть идентифицированы и вскрыты. Необходимо отметить, что большинство алгоритмов зависимы от формата, трудоемкости вычисления. Кроме того, например, для извлечения ЦВЗ в некоторых случаях необходимо иметь исходный немаркированный файл.

Таким образом, предложенное решение не требует создания дополнительных сигналов, вследствие чего не нужно сравнивать объем контейнера и сообщение, чтобы записать информацию, и что, следовательно, более эффективно.

Литература

1. Грибунин В.Г. Цифровая стеганография // СПб.: Солон-Пресс, 2002. — 272 С.

2. Рябко Б.Я. Основы современной криптографии и стеганографии. / Б.Я. Рябко, А.Н. Фионов – М.: Горячая линия – Телеком, 2010. – 232 С.

3. Kerckhoffs, La Cryptographie Militare. Journal des sciences militaires, pp:5-83, Jan. 1883, pp:161-191, Feb. 1883.

4. Charbon E., Torunoglu I.H. On Intellectual Property Protection. In proceedings of Custom Integrated Circuits Conference, 2000, pp. 517-523.

5. New Matrices with Good Auto and Cross-Correlation - A. TIRKEL and T. HALL - IEICE TRANS. FUNDAMENTALS, VOL.E89–A, NO.9 SEPTEMBER 2006.

6. А.Г. Коробейников, С.С. Кувшинов, С.Ю. Блинов, А.В. Лейман, И.М. Кутузов. ЦИФРОВЫЕ ВОДЯНЫЕ ЗНАКИ В ГРАФИЧЕСКИХ ФАЙЛАХ. / Научно-технический вестник информационных технологий, механики и оптики,

7. 2013, № 1 (83), С. 152-156.

8. 7. Сидоркина И.Г. Метод аутентификации по биометрическим параметрам// Изд.: «Южный федеральный университет» в г. Таганроге (Таганрог) Информационное противодействие угрозам терроризма. 2015. № 24. С. 202-205.

References

1. Gribunin V.G. Tsifrovaya steganografiya // SPb.: Solon-Press, 2002. — 272 S.

2. Ryabko B.YA. Osnovy sovremennoy kriptografii i steganografii. / B.YA. Ryabko, A.N. Fionov – M.: Goryachaya liniya – Telekom, 2010. – 232 S.

3. Kerckhoffs, La Cryptographie Militare. Journal des sciences militaires, pp:5-83, Jan. 1883, pp:161-191, Feb. 1883.

4. Charbon E., Torunoglu I.H. On Intellectual Property Protection. In proceedings of Custom Integrated Circuits Conference, 2000, pp. 517-523.

5. New Matrices with Good Auto and Cross-Correlation - A. TIRKEL and T. HALL - IEICE TRANS. FUNDAMENTALS, VOL.E89–A, NO.9 SEPTEMBER 2006.

6. A.G. Korobeynikov, S.S. Kuvshinov, S.YU. Blinov, A.V. Leyman, I.M. Kutuzov. TSIFROVYYe VODYANYYe ZNAKI V GRAFICHESKIKH FAYLAKH. / Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki,

7. 2013, № 1 (83), S. 152-156.

8. 7. Sidorkina I.G. Metod autentifikatsii po biometricheskim parametram// Izd.: "Yuzhnyy federal'nyy universitet" v g. Taganroge (Taganrog) Informatsionnoye protivodeystviye ugrozam terrorizma. 2015. № 24. S. 202-205.

СИДОРКИНА Ирина Геннадьевна, доктор технических наук, профессор, декан Факультета информатики и вычислительной техники ФГБОУ ВО «Поволжский государственный технологический университет». 424000, Республика Марий Эл, г. Йошкар-Ола, пл. Ленина, дом 3. E-mail: igs592000@mail.ru

КУБАШЕВА Елена Сергеевна, кандидат технических наук, доцент кафедры ИВС ФГБОУ ВО «Поволжский государственный технологический университет». 424000, Республика Марий Эл, г. Йошкар-Ола, пл. Ленина, д. 3. E-mail: e.kubasheva@mail.ru

СОЛОВЬЕВ Максим Геннадьевич, студент кафедры Информационной безопасности ФГБОУ ВО «Поволжский государственный технологический университет». 424000, Марий Эл, г. Йошкар-Ола, пл. Ленина, д. 3. E-mail: fivt@volgatech.net

ГАЛАНИНА Наталия Андреевна, доктор технических наук., профессор, г.Чебоксары ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова». 428010, Чувашская Республика г. Чебоксары, Московский просп., 15. E-mail: galaninacheb@mail.ru

SIDORKINA Irina, Doctor of Technical Sciences, Professor, Dean of the Faculty of Informatics and Computer Engineering of Volga State University of Technology. 424000, Republic of Mari El, Yoshkar-Ola, pl. Lenin, 3. E-mail: igs592000@mail.ru

KUBASHEVA Helena, Candidate of Technical Sciences, Associate Professor of the Department of IVS FSBEI HE "Volga State University of Technology". 424000, Republic of Mari El, Yoshkar-Ola, pl. Lenin, 3. E-mail: e.kubasheva@mail.ru

SOLOVIEV Maksim, student of the Department of Information Security FSBEI of HE "Volga State University of Technology". 424000, Republic of Mari El, Yoshkar-Ola, pl. Lenin, 3. E-mail: fivt@volgatech.net

GALANINA Nataliya, Doctor of Technical Sciences., Professor, Cheboksary FSBEI of HE "I. Chuvash State University". Ulyanova. 428010, Chuvash Republic, Cheboksary, Moskovsky Prospect, 15. E-mail: galaninacheb@mail.ru