MSC 62M45 **DOI: 10.14529/jcem160302**

COPYRIGHT PROTECTION OF MUSIC IN DIGITAL FORM

R.R. Dautov[1]**,** drr793@yandex.ru,
N.D. Zulyarkina[1]**,** toddeath@yandex.ru,
[1] South Ural State University, Chelyabinsk, Russian Federation.

The work is devoted to consideration of audio data protection against unauthorized copying and distribution from others name, and also identification of audio files for authorship definition. The characteristics of audio files resistant to distortions are investigated. The review of digital watermarks, the digital prints applied as protection methods is carried out.

Keywords: audio file, copyright, digital watermark, digital print, spectrogram.

Introduction

Today the protection of intellectual property rights is topical issue. In particular, it is true for multimedia information. The use of the Internet allows creative people to self-express by publication of results of their creativity in network. On the one hand, these data shall be available to view, because it is their basic purpose. On the other hand, the open entry to information makes it vulnerable against threats of unauthorized copying and distribution from others name. Somewhat different is the case with the musical works presented in a digital form. Owners of such works – labels of sound recording, as a rule, want to get a benefit from their sales and don't publish them in open access. However, musicians as copyright owners are interested in protection of the works against any illegal copying. Therefore recently serious work on tracking of unauthorized distribution of similar information is carried out. As practice shows, it is possible to find thousands of audio file copies on various web pages. Besides, names of musical files in case of unauthorized distribution often change that makes difficult their identification by owners. So the author need to prove a first priority of the authorship.

To protect audio files against unauthorized copying and distribution, and also to prove a first priority of the authorship one can use the following methods, which allow to identify files.

1. To build an identification tag in audio files. These tags are imperceptible for human hearing, but are easily found by special detectors, programs.

2. To calculate "a digital print" of the sound file and to store it in the database (DB). The digital print takes much less place of DB than the file. It allows to create big base of prints.

1. Digital Watermarks

The first method is one of the steganography methods. It is called digital watermarks (DW). The purpose of steganography is to hide the fact of transfer of the protected information. The sender implements a confidential message in any object (container) and only the host party aware of the transfer fact can take this message. Unlike an usual steganography, DW don't need to hide the embedding fact, it is rather on the contrary.

In DW the multimedia files (images, video and audiofiles) are used as containers, and the hidden data is various information (as a rule, text or image), which identify the author of an object. Note that a violator knows or can guess existence of DW and makes attempts of modification of the protected file. Therefore for implementation of information in audio-signals there is a certain number of requirements [2]:

– hidden information should be resistant to availability of various painted noise, to compression with losses, to filtering, to analog digital and digital-to-analog transformations;

– hidden information should not contribute a distortion to the signal, which is perceived by the human auditory system;

– an attempt to remove the hidden information should lead to noticeable damage of a container (for DW) or its unsuitability for perception;

– DW should clearly identify the author of the protected file;

– hidden information should not make any significant changes in the container statistics. Digital watermarks have small size, however difficult methods are used for their

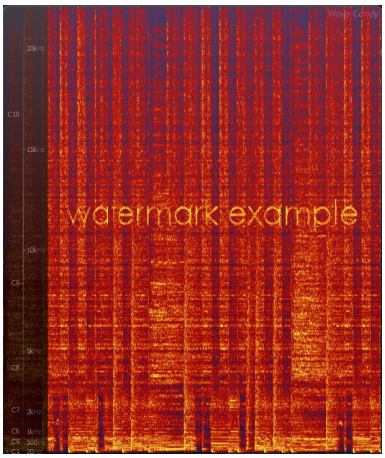

Fig. 1. An example of DW in frequency area

embedding. To embed the hidden information in audio signals it is possible to use the methods, which are applied in other types of steganography [1, 2]. For example, one can embed an information by replacing of the least significant bits (all or some).

Several methods of creation of DW for audio files [1, 2, 3, 5] are currently popular, however for DW it is preferable to use the methods making embedding to the frequency area of a signal [7].

2. Embedding of Information in Metadata

The use of metadata is another method to hide the information. The ID3 format is a bright example of the sound file metadata. It is called by "**Id**entify" and "MP**3**". ID3 signature contains data about title of a track and an album, an artist name etc. They are used by media players and other programs, and also hardware players to display an information about the file. The second version of this format assumes use of "frames which are the sites of memory located at the beginning or the end of the file and designated by the keyword. Each frame contains any metadata. For example, the frame with "TIT2"

keyword contains the name of the work. Among standard ones, there are frames for storage of information about author's rights and the license. Fig. 2 shows an information which contains in the file from the online store called "Amazon.com".

Fig. 2. An embedding of metadata on Amazon.com

This example contains the following metadata:
– C2br1vaR – the random numbers of Amazon assigned to the order,
– Amazon.com – the name of Amazon.com shop,
– 2011-12-08T03:10:50Z – date and time of purchase of the song,
– 00011805301110 – identifier of an album (Universal Product Code),
– USAG21130102 – the international standard number of audio/video of record,
– KRXaw+vu1wr8bB2cCNxJScKWcFKk7fDg – number of sale transaction, which in the database of shop is connected with a credit card number, the address and other data of the buyer,
– user-name – the identifier of the buyer (an initial part of the e-mail address of the buyer).

Further there are some more parameters. Among them there is a digital signature, which allows to determine the fact of the file modification.

Using this information it is possible to identify who from whom and when bought this composition.

In this case of an information hiding there is the steganography, which does not destroy audio data. That is the embedding data don't influence on audio data in any way, and hide in the official fields, which aren't displayed in the most widespread ID3 Tag scanners.

3. Digital Prints of Files

The second method of sound files protection against unauthorized copying and distribution is the use of digital prints of files. Today the technology of digital prints is used for different protection of information, mostly for protection of text documents against leaks. However this technology can be extended also to other types of files, for example to images, audio-and video files. To form digital prints it is necessary to consider 3 important points. First, the print shall be the most compact. Second, the print shall take into account the characteristics of files (sound or visual). Third, to use prints it is necessary to create a base of prints of all protected files.

The sound print (signature) represents the short description of an audio file considering its sound characteristics. Note that one need takes into account such characteristics which are not only resistant to different modifications of the sound file (to compression, analog-to-digital and to digital-to-analog conversion, filtering, etc.), but also are relevant to his perception. That is function of computation of an audio file signature must be constructed such that the perceived equally sound objects lead to identical prints [7]. The second problem of digital prints use is a choice of an effective algorithm of prints comparing and an algorithm of false operations splitting. At the same time receiving and search of prints shall be fast and simple.

The analysis of English literature on the selected topic allowed to suggest to use two effective algorithms for tracing of illegal audio content of web pages.

In paper [6] the music is considered as the time-and-frequency diagram called a spectrogram. One axis is time, another is frequency, the third one is an intensity of spectrogram peaks, which are points of a local maximum of amplitude. Each point of the diagram represents intensity of a specific frequency at a given time. The location of these points on a grid "frequency вГУ time" changes little in case of a noise. In order to improve the search, a neighboring point forward on a time axis is found for each pica of the spectrogram. Such neighboring point is called reference point. Then these points are associated in pairs, which are called constellations. The digital print is a hash table. The key of this table is a frequency rate for the peak of intensity and for its reference point opposite to which time in seconds from the beginning of a track is set. Process of formation of one element of the hash table is shown in Fig. 3.

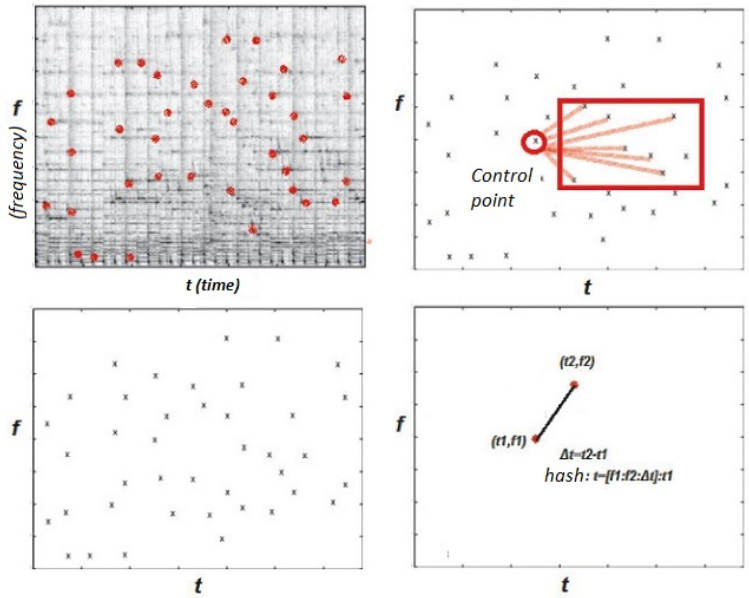

Fig. 3. Formation of a digital print of the sound file by its spectrogram

In work [3] well-known characteristics of a sound, which are resistant to distortions, are used to form prints of the sound file. They are Fourier's coefficients, coefficients of cosine transformation of Fourier, spectral flatness, coefficients of linear coding with a prediction and others. The proposed scheme for producing prints is based on this approach of a stream processing. The review of the scheme is shown in Fig. 4. At first the sound signal is

divided into frames. A set of characteristics of the sound file is calculated for each frame, where the coefficients of the Fourier transformation (FT) are chosen as characteristics. In order to calculate FT parameters, only the absolute value of a spectrum (that is the power spectral density) is remained. A sub-print of 32 bits is formed for each frame.

In order to receive a sub-print, 33 not superimposed ranges of frequencies from 300 to 2000 Hz are selected for each frame. Each bit m of sub-print for a frame n is determined by the formula

$$F(n,m) = \begin{cases} 1, & if\ E(n,m) - E(n,m+1) - (E(n-1,m) - E(n-1,m+1)) > 0, \\ 0, & if\ E(n,m) - E(n,m+1) - (E(n-1,m) - E(n-1,m+1)) \leq 0, \end{cases}$$

where $E(n,m)$ is an energy of range of frequencies m for the n-th frame. Bit "1" encodes a white pixel, bit "0" – a black pixel. The energy difference (on both time and frequency axes) is a property that is very resistant to many types of processing.

Sub-prints are combined in blocks of 256 elements (Fig. 4). Such way of prints formation describes only 3 seconds of the sound file. The authors of the method claim that it is sufficient for exact identification of the sound file.

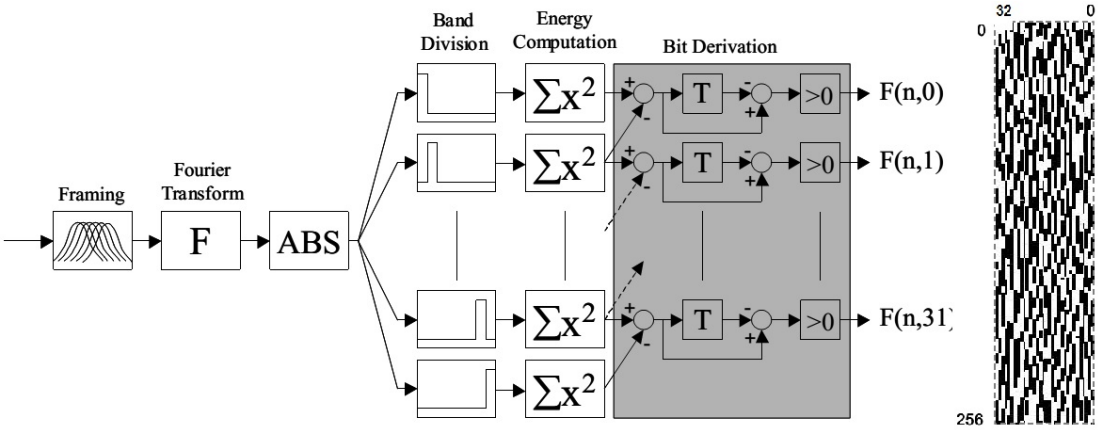

Fig. 4. Formation of a print of the sound file

4. Possible Ways to Circumvent the System of Sound Print

Popular social network "VK" began a campaign to combat piracy on its pages in the middle of June, 2014. By the request of owners, it removed illegally placed audio recordings. Users were indignant and found a method to circumvent the system: massively they began to rename audio files (to change names of artists, titles of songs).

It pushed developers to toughen measures in order to make an acceptance of "masking" useless. Their answer was "a digital print". As a result already existing records and their disguised copies are removed in case of the owner request, or the new attempt of their loading is blocked (Fig. 5). On the server of VK the list of songs with "digital prints which owners prohibit to post them online, is created.

Despite this fact, there are several methods to circumvent this protection. The first of them is adjustment of the medium frequencies range, namely weakening of a section of frequencies around 300 Hz approximately on 3 dB (Fig. 6). It means that the system of

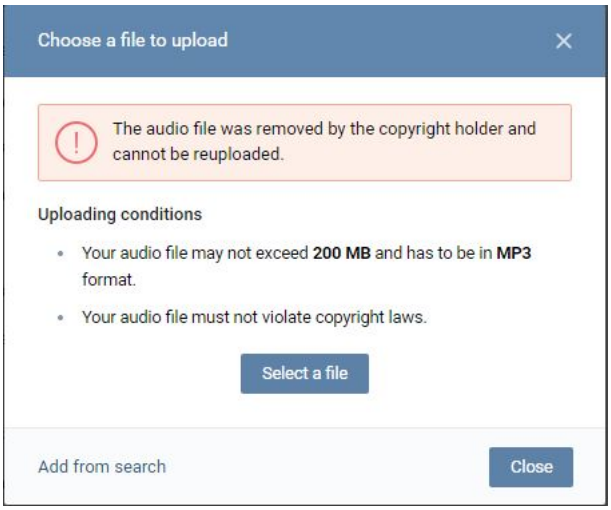

Fig. 5. An attempt to upload copyright of protected record

digital prints obtaining, which is applied in social network "VK analyzes medium frequency area of the file. Thus, weakening of these frequencies led to change of peaks of frequencies intensity. It resulted in obtaining a completely different print. As a result, record was successfully loaded.

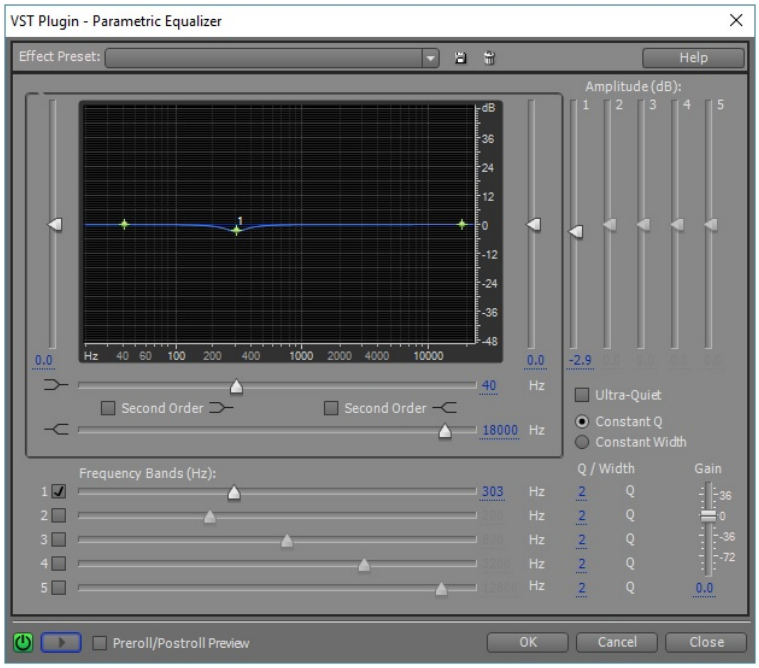

Fig. 6. Adjustment of medium frequencies using parametric equalizer

Another way to circumvent the above-mentioned system is a duplication of the loaded file (Fig. 7). A copy of the original file "is pasted" in the end of it. And this procedure can be performed using the mp3DirectCut program which allows to edit mp3 files without re-encoding. It is very important in order to save a quality of the initial file.

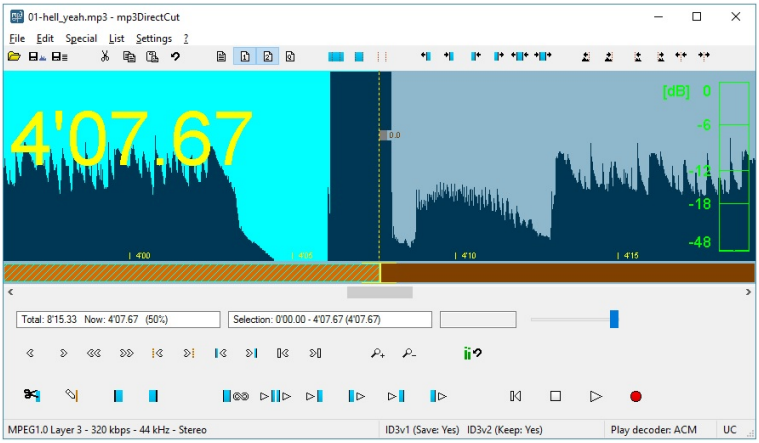

Fig. 7. Duplication of the sound file

As a result of duplication, record was also successfully loaded. It explains the fact that the system analyzes a certain site of the file (most likely, around the middle). The procedure of duplication displaces the previous location of the middle, therefore record is identified as a new one.

Conclusion

As a result of the ideas of this work it is possible to conclude that the offered methods of audio files protection against unauthorized copying and distribution can be quite used. However, to track sound files by the built-in identification tag, it is necessary to be sure that this tag is present there initially. But it is impossible to build an identification tag in all copies of files. Using the second way to track the audio file by its digital print, one can to track arbitrarily modified copies of the original file. The feature of use of digital prints to identify files is that the decision on similarity or distinction of audio files is given with some share of probability. That is the result of files recognition is evaluated by two errors: an error of the first type (the file is not found, but it is exist) and an error of the second type (another file is mistakenly found). The error of the second type for a method of spectrograms is about 2,5 times higher, than for a method of single-frame calculation of prints. An introduction of some redundancy is supposed to improve the probability of detection. It can increase the search time. Their practical realization is necessary for the proof of the assumptions given above and obtaining more detailed characteristics of algorithms work. It is a subject for a further research.

References

1. Gribunin V.G., Okov I.N., Turintsev I.V. [*Digital steganography*]. Moscow, Solon–Press, 2002. – 272 p. (in Russian)

2. Konakhovich G.F, Puzyrenko A.Y. [*Computer steganography. Theory and practice*]. Kiev, MK–Press, 2006. – 288 p. (in Russian)

3. Avery Li-chun Wang. An Industrial-Strength Audio Search Algorithm. http://www.ee.columbia.edu/ dpwe/papers/Wang03-shazam.pdf (Date: 11.09.2016)

4. Bender W., Gruhl D., Morimoto N., Lu A. Techniques or Data Hiding. *IBM Systems Journal*, 1996, vol. 35, no. 3&4, pp. 313–336.

5. Foote J., Adco J. and Girgensohn A. Time base modulation: a new approach to watermarking audio. http://www.fxpal.com/publications/FXPAL-PR-03-212.pdf (Date: 11.09.2016)

6. Borisova S.N. [Methods of protection of audiofiles against unauthorized copying and distribution]. *Fundamental research*, 2015, no. 5-3, pp. 481–487. (in Russian)

Rustam R. Dautov, Undergraduate, Faculty of Mathematics, Mechanics and Computer Science, South Ural State University (Chelyabinsk, Russian Federation), drr793@yandex.ru.

Natalya D. Zulyarkina, Doctor of Physics and Mathematics, Faculty of Mathematics, Mechanics and Computer Science, South Ural State University (Chelyabinsk, Russian Federation), toddeath@yandex.ru.

Received June 27, 2016

УДК 004.056 **DOI: 10.14529/jcem160302**

ЗАЩИТА АВТОРСКИХ ПРАВ МУЗЫКАЛЬНЫХ ПРОИЗВЕДЕНИЙ В ЦИФРОВОМ ВИДЕ

Р.Р. Даутов, Н.Д. Зюляркина

Работа посвящена рассмотрению защиты аудиоданных от несанкционированного копирования и распространения от чужого имени, а также идентификации аудиофайлов для определения авторства. Исследованы характерные особенности аудиофайлов, устойчивые к искажениям. Проведен детальный обзор цифровых водяных знаков, цифровых отпечатков, применяемых в качестве методов защиты.

Ключевые слова: аудиофайл, авторское право, цифровой водяной знак, цифровой отпечаток, спектрограмма.

Литература

1. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин, И.Н. Оков, И.В. Туринцев. – М.: Солон–Пресс, 2002. – 272 с.

2. Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. – Киев: МК–Пресс, 2006. – 288 с.

3. Avery Li-chun Wang. An Industrial-Strength Audio Search Algorithm. [Электронный ресурс] – Режим доступа: http://www.ee.columbia.edu/ dpwe/papers/Wang03-shazam.pdf (дата обращения 8.06.2016).

4. Bender, W. Techniques or Data Hiding / W. Bender, D. Gruhl, N. Morimoto, A. Lu // IBM Systems Journal. – 1996. – V. 35, № 3&4. – P. 313–336

5. Foote, J. Time base modulation: a new approach to watermarking audio / J. Foote, J. Adco, and A. Girgensohn. [Электронный ресурс] – Режим доступа: http://www.fxpal.com/publications/FXPAL-PR-03-212.pdf (дата обращения 8.06.2016).

6. Haitsma, J. A Highly Robust Audio Fingerprinting System / J. Haitsma, T. Kalker. [Электронный ресурс] – Режим доступа: http://ismir2002.ismir.net/proceedings/02-FP042.pdf (дата обращения 8.06.2016).

7. Борисова, С.Н. Методы защиты аудиофайлов от несанкционированного копирования и распространения / С.Н. Борисова // Фундаментальные исследования. – 2015. – № 5-3. – С. 481–487. URL: http://fundamental-research.ru/ru/article/view?id=38286 (дата обращения: 25.08.2016).

Даутов Рустам Рамисович, магистрант, факультет Математики, механики и компьютерных наук, Южно-Уральский государственный университет (г. Челябинск, Российская Федерация), drr793@yandex.ru.

Зюляркина Наталья Дмитриевна, доктор физико-математических наук, факультет Математики, механики и компьютерных наук, Южно-Уральский государственный университет (г. Челябинск, Российская Федерация), toddeath@yandex.ru.

Поступила в редакцию 27 июня 2016 г.