UDC 004

DESIGNING THE STEGOSYSTEM, BASED ON HIDING TEXT DATA IN AUDIO FILES BY MEANS OF CHANGING THE DELAY TIME OF THE ECHO SIGNAL

ALIAKSEI KAKHANOUSKI, YURIY PASTUKHOV
Polotsk State University, Belarus

The article presents a practical way of creating a reliable stegosystem with an unconventional way of hiding information. The purpose of this work is to build a system based on hiding text messages in audio files, as well as to study the attacks and to find out, whether such a system is suitable for practical usage. The task was being solved by splitting the main program into the library and sub-routines. The program is written in the Java programming language using JavaFX and the library for converting JAVE (Java Audio Video Encoder).

Introduction. The subject of the article deals with hiding data in audio files, using one of the steganography methods. Digital steganography is hiding one data in other data. Moreover, the concealment of this should be implemented in order not to lose the properties and value of hidden data and the inevitable modification of the digital storage medium wouldn't destroy the semantic functions and even wouldn't change them at the certain abstract level. Thereby the fact of one message transmission inside of another will not be revealed by the traditional approach.

The main audio signal settings are: amplitude, frequency and phase. All these setting are appropriate for steganographic modification, but before the integration it is necessary to estimate the limits of container modification settings as well as any distortions. The message rate, reliability, stability of the steganography system will largely depend on the degree of modification of the audio container [1].

The principle of a steganographic system designing and the description of the data hiding algorithm.

The standard steganographic scheme is maintained regardless of the technology used for its implementation. The task of embedding and separating messages from other data is performed by a stegosystem. Data, containing a hidden message, can be subjected to deliberate attacks or accidental interference. In the stegosystem two types of information are combined, so that they can be distinguished by two fundamentally different detectors. One of the detectors is the system of isolation of the CEH, another is a human [1]. To conceal the data, the method of embedding information was used by changing the delay time of the echo signal. This method allows to place data in the cover signal, changing the echo signal settings. The settings, carrying the embedded data are: initial amplitude, decay time and shift (delay time between the original signal and its echo). If the decline is reduced, two signals are mixed. At a certain point human ear ceases distinguishing two signals and the echo is perceived as additional resonance. The coder uses two time delays: one for coding zero, the other for coding unit. Both of them are less than the one a human ear is able to recognize. Besides the reduction of the delay time it is necessary to make the embedded information impossible for audio perception by a human listening system by means of setting the initial amplitude and the time of decline.

When encoding the information two values of echo signal delay were chosen: 0, 0012 & 0, 0008 seconds. These values reduce the efficiency of the extraction algorithm, reducing the probability of a correct extraction of the bit, but they are suitable for almost all types of containers. Amplitude value is 40%, because this value helps increase the probability that the fact of hidden data existence wouldn't be revealed.

Decoding of the embedded data means defining the time interval between signal and echo. For this it is necessary to consider the amplitude (at two points) of the autocorrelation function of the discrete cosine transformation of the logarithm of the power spectrum (cepstrum). The burst of the autocorrelation function will take place in δ_1 or δ_0 seconds after the original signal, shown in Figure 1. The decoding rule is based on defining the time interval between the original signal and autocorrelation burst.

According to the researches of V. Bender and N. Morimoto, such a scheme allows to imbed imperceptibly 16 bits in one second of audio, without losing its quality. The choice of the method of embedding data in sound files using echo conversion is determined by the fact that this method has resistance to amplitude and frequency attacks, which allows to bypass other methods that are unstable to these attacks. However, this method is unstable to temporary attacks that directly affect the length of the audio file and the number of samples in it. When it comes to implementing this method of steganographic protection of information through echo-signal conversion, it becomes clear that the main difficulty is the implementation of the most efficient algorithm for extracting embedded bits. Several researches in this field showed that it is possible to reach the highest efficien-

cy only by means of individual approach to each of the containers, changing the delay time of the overlaid echo signal.

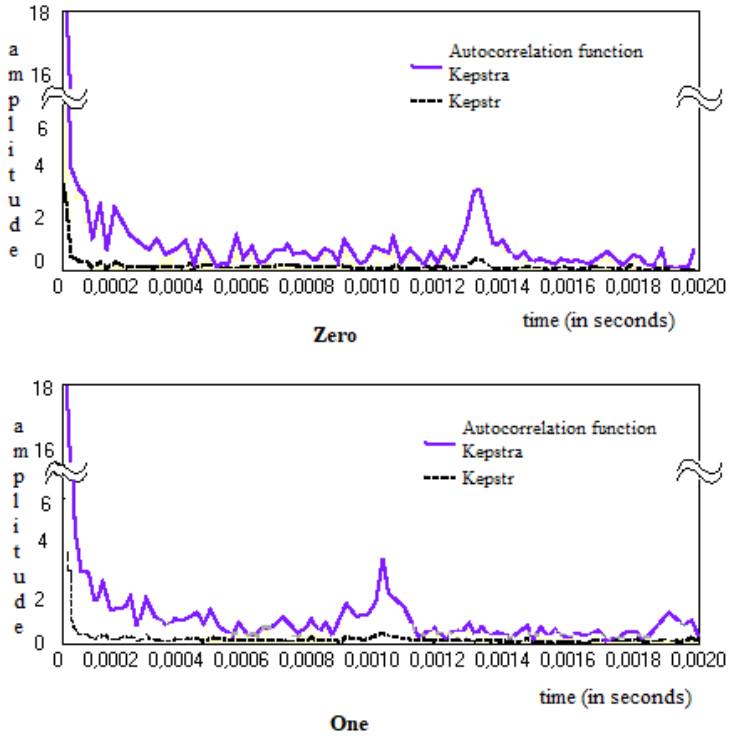

Fig. 1. Behavior of the autocorrelation function

Estimation of the implemented system stability.

There is a great variety of digitalized audio signals classifications according to their settings such as: sampling, the amount of channels (mono or stereo), recording quality (number of kbps), etc. At the same time, if the audio signals (containers) belong to the same data representation format (for example, WAVE), have the same sampling frequency, the same number of channels, the same sound quality and differ only in the music genre, it is difficult to assess the suitability of a container for steganography modification.

All audio files can be divided into three groups:

– audio files similar to speech, with a lot of pauses (poems, voice of the announcer, speech with low background music, etc.);

– audio files that do not have a wide frequency range, like ordinary musical compositions (pop songs, popular music, blues, etc.);

– audio files with a wide frequency range, passed additional computer processing (electronic music (trance, techno, etc.), synthesized sounds of nature, etc.).

The use of audio files from the first group was completely inappropriate for usage, regardless of the quality of the container used.

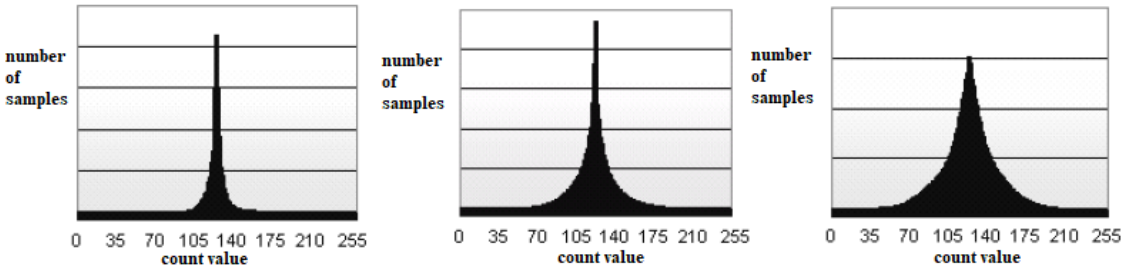

Fig. 2. Graphs of the distribution of samples for groups 1–3

When using audio files from the second group, the distortion is hardly discernible by a trained ear, and the probability of proper withdrawal is quite high. The use of audio files from group 3 showed that the probability of proper extraction is close to 100%, while distinguishing an empty container and a container with data by ear won't be possible.

From this we can make a conclusion, that the audio files that have been subjected to additional computer processing (electronic music) are the most suitable for the method of hiding data by means of echo-signal delay. The sampling rate and the number of channels should also be taken into account: the higher their values, the greater the probability of correct withdrawal is [2].

The main types of attacks on stegosystems are:

1. The attack on the basis of a known filled container. The task is to detect the presence of a hidden message. Listening to an audio signal in order to detect any interference. A container lasting 60 seconds, with the dynamic music was chosen, and a 20-character message was hidden. The result: after listening to the filled container using the speaker system extraneous sounds, wheezes and crackling were not detected.

2. An attack on the basis of a known empty container If it is known, then by comparing it with an assumed container in which there is a hidden message, it is always possible to establish the presence of a stego channel. This can be a comparison of the length of the audio signal, the comparison in size, as well as listening. A container lasting 60 seconds, with dynamic music was chosen, and a 20-character message was hidden. The result: repeated listening to a filled container and original container using the speaker system without playing low frequencies (laptop) showed that there is no difference between the sound. However, when listening to an acoustic system with a device playing low frequencies, some differences in the depth of sound of the filled container and the original container became apparent.

3. Attacks against the built-in message, aimed at removing or corrupting the built-in data by manipulating the filled container, and also, aimed at hindering or inability to operate the detector correctly. In this case, the message in the audio file remains, but the ability to receive it is lost. Examples are: trimming (changing the length) of the audio signal, changing the format to another, changing the container's format settings, accelerating or slowing down, changing the key. Result: the method of data concealment using echo delay is unstable to temporary changes. If you change the length of the audio file for a few seconds, you can't extract any data. Changing any other settings of the audio file did not affect the receipt of hidden data [3].

The conclusion. Research in the field of steganography is a very promising direction of data protection, since in the modern world the task of transferring sensitive data is in step with hidden communication, i.e. hiding the fact of message transmission. Therefore, it is necessary to continue researches in this area to find new, effective, methods or improve the existing ones. In this article the method of embedding data in audio files was considered. The method of echo signals is the most promising, however, it needs to be improved in terms of throughput, and the probability of correct extraction of embedded bits of data. The software product is implemented and ready for usage with the possibility of modification.

REFERENCES

1. Садов, В.С. Компьютерная стеганография / В.С. Садов. – М. : МГВРК, 2012. – 289 с.
2. Грибунин, В.Г. Цифровая стеганография / В.Г. Грибунин. – М. : СОЛОН-Пресс, 2002. – 272 с.
3. Matsui, K. Digital signature on a facsimile document by recursive MH coding / K. Matsui, K. Tanaka, Y. Nakamura // Symposium On Cryptography and In-formation Security. – 1989.