UDC 004.221

DEVELOPMENT OF A SYSTEM FOR HIDDEN INFORMATION IN A SOUND ENVIRONMENT

I. ANDREYEU, D. PASTUKHOV
Polotsk State University, Belarus

This article discusses various algorithms for hiding information in a sound environment and their advantages. In the course of research, the optimal version of the algorithm has been chosen.

Introduction. The task of reliable protection and concealment of information comes since the earliest times. Even in ancient times, various methods were used to protect important information from prying eyes of wanderers, the Polybius square and the first shift ciphers. Later ciphers of simple replacement (Arthur Conan Doyle's story "Dancing Men") and permutation ciphers (Cardan grille) appeared. In the XVIII century, the code "according to the book" arose, which can be considered as the development of Caesar's cipher (used by the hero Yu. Semenov - Stirlitz in the novel "17 Moments of Spring").

But all ciphers have finite strength and can be decrypted in a finite period of time. Steganography, which hides the very fact of transmitting a secret message, helps to solve this problem.

The main section. The article will examine the steganographic methods of hiding information in sound files, both from the point of view of resistance to attacks, and from the point of view of maintaining an acceptable quality of the sound signal.

The least significant bits method is used for digital representation of the audio signal and is suitable for use at any communication speeds. When converting an audio signal into digital form, there is always a sampling noise that does not introduce significant distortion. The "noise" bits correspond to the lower bits of the digital representation of the signal, which can be replaced by hidden data. This method has extremely low stegosity and simple implementation. A change in the sound signal can be detected.

Broadband coding methods use the same principles as the methods of hiding data in images. Their essence lies in the slight simultaneous modification of a number of certain bits of the container while hiding one bit of information. This method has medium resistance to attacks and distortions and is difficult to implement. The sound signal is practically unchanged.

The echo hiding method hides data by incorporating the echo into the audio signal. It is known that at small time shifts the echo signal is almost indistinguishable by ear. Therefore, if certain time delays are introduced, the value of which does not exceed the detection threshold, then, dividing the initial sound signal into segments, you can enter the corresponding echo signal in each of them, depending on the hidden bit. This method is stego-proof and difficult to implement. The sound signal is practically unchanged.

Phase hiding methods are used for both analog and digital signals. They use the fact that a smooth phase change cannot be determined by ear. In such methods, the protected data is encoded either by a specific phase value or by a phase change in the spectrum. Changes in the sound file using this method cannot be detected using human hearing, but it is extremely difficult to extract information at the slightest damage to the signal.

As for musical stegosystems, the musical form of the sound environment occupies most of the information space of the Internet. In addition, it is widely used in general purpose radio networks and is distributed on electronic information carriers, which, due to the development of computer technology, have become widespread. In this regard, the use of the music environment to conceal information messages seems quite promising. To conceal data, methods based on the modification of those parameters of the musical environment that can be qualitatively described in music theory can be used. The musical environment has its own textual display in the form of notes and other signs that allow adequately to reflect the musical work and its internal structure with such elements as notes, scales, periods, measures, cadences, chords, motives, modulations, tones, various types of development, sequences, etc. The construction of musical fragments obeys syntactic rules that can be described, which allows you to build logical relationships and, accordingly, a description of the structures of musical works.

Musical stegosystems provide information hiding in the musical environment by analogy with the improvisation of musical works. Essentially, improvisation is such a change in a musical work or its fragments that preserves the main themes of the original work in the form of melodies, but at the same time expands the image of the musical theme with other features that complement the main image that were not in the main musical work. The main difference between musical steganography and improvisation is that the goal is not to expand the im-

ages of the basic musical work, but to make changes that preserve the melody of the main work, comply with all the rules for constructing this work, and at the same time encode the message to be hidden without distorting the main theme of the work.

A fragment of a musical work can be described as a logical structure. An analogue of a text sentence word in a musical work will be one beat of a melody, and fragments shared by censorship will be considered an analogue of a sentence in music. Typically, a piece of music consists of a series of phrases that consist of measures. The introduction of the text into a musical work is carried out in separate sentences, each of which can be compared with a separate melody. Next, a musical display of the expanded musical composition with a hidden message embedded in it is formed. Based on the musical representation of the extension, its musical realization is carried out using modern computer systems, which are software and hardware sound synthesizers. The musical stegosystem is highly resistant to attacks and almost impossible to detect, however, to implement this system, you need to spend a huge amount of resources.

Conclusion. In this article, algorithms for hiding data in sound files have been considered, the operation of the musical stegosystem has been described, and the conclusion has been drawn on the optimal method for implementing the system.

REFERENCES

1. Мельников В.В. Защита информации в компьютерных системах. Электронинформ, 1997. — 368 с.
2. Барабаш А.В., Шанкин г.п. История криптографии. Ч.l. — М.: Гелиос АРВ, 2002.—240 с.
3. Домарев В.В. Защита информации и безопасность компьютерных систем. — К.: Издательство ДиаСофт, 1999. — 480 с.
4. Ярочкин В.И. Безопасность информационных систем. — М.: Ось-86, 1996. — 320с.
5. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях/Под ред. В.Ф. Шаньгина; 2-е изд., перераб. и доп. — М.: Радио и связь, 2001. — 376 с.
6. Герасименко В.А., Малюк А.А. Основы защиты информации. — М.: МГИФИ, 1997. — 538 с.