DOI: 10.5604/20830157.1130190

HARDWARE AND SOFTWARE REALIZATION OF THE TRANSMISSION OF AUDIO INFORMATION ENCRYPTED BY CHAOTIC SEQUENCES

Yuriy Bobalo[1], Zenon Hotra[2,3], Olexandr Hres[4], Ruslan Politans'kyy[1]
[1]Lviv Polytechnic National University, Department of Theoretical Radio Engineering and Radiometrics, [2]Rzeszow University of Technology, [3]Lviv Polytechnic National University, Department of Electronic Devices, [4]Yuriy Fedkovych Chernivtsi National University, Department of Radioengineering and Information Security

Abstract. *An audio information transmitting system, encrypted by chaotic sequences, which are generated on the base of discrete one-dimensional mappings is described in the article. The operation of the system is considered on the example of the information transmission between two computers.*

Keywords: audio information, chaotic sequences, generator, logistic mapping, synchronization

SPRZĘTOWO-PROGRAMOWA REALIZACJA SYSTEMU TRANSMISJI INFORMACJI AUDIO Z SZYFROWANIEM CHAOTYCZNYMI SEKWENCJAMI

Streszczenie. *W artykule opisano system transmisji informacji audio z szyfrowaniem chaotycznymi sekwencjami generowanymi na podstawie jednowymiarowych dyskretnych chaotycznych odwzorowań. Pracę systemu rozpatruje się na przykładzie transmisji informacji między dwoma komputerami.*

Słowa kluczowe: informacja audio, chaotyczne sekwencje, generator, odwzorowanie logistyczne, synchronizacja

Introduction

Along with the rapid development of telecommunication systems, internet technologies, in particular, IP-telephony the problem of the protection of audio information, which is transmitted by digital communication channels through Internet / Ethernet network, was raised. The modern telecommunication systems require a high confidentiality level of communications. The protection of the information, which is transmitted in telecommunication systems, can be realized by means of closing them by chaotic sequences. This approach resulted in the development of fundamentally new methods of encoding, encryption and transmission of information, in particular, cryptographic methods based on the theory of dynamical systems with their inherent chaotic properties. Nowadays, the cryptographic methods of information protection remain the most stable and secure methods of data transmission [3, 6].

One of the main problems of the design of secure communication systems is the synchronization between the receiving and transmitting components of the communication systems. The majority of the methods of secure data transmission with the synchronization by chaos are based on the total chaotic synchronization, which requires a high degree of identity of the generators of transmitting and receiving components of the information transmitting system. The improvement of the techniques of the secure data transmission, based on the systems with the chaotic synchronization is an important task for the research in the field of information and telecommunication systems based on chaos [3, 6].

The aim of our work is software and hardware realization of the audio information transmitting system with the encryption by pseudorandom sequences, which are generated on the basis of one-dimensional discrete chaotic mappings with the synchronization of transmitting and receiving components of the system.

1. Encryption algorithm

There are the following methods of the audio information protection: digital scrambling, streaming encryption and standard encryption. The most effective way for the protection of audio information from possible threats (the unauthorized access, the loss of the integrity and authenticity of information) is the cryptographic transformation. The aforementioned methods of information protection possess the following disadvantages: the digital scrambling results in the additional delays during the transmission of audio information that is caused by the scrambling algorithm itself; the standard cryptographic encryption, according to the known algorithms, provides satisfactory protection of audio information, but it is costly in terms of speed and complexity of computing [11]. The most preferred, in terms of speed and complexity of computing, is the bitwise addition on module 2 (XOR operation) of the digitized parts of the input sequence of audio information with an infinite or periodic key, which may be formed, for example, by a generator of pseudorandom sequences (PRS) [4, 11].

As the encryption sequence the pseudochaotic sequences can be used. Their generation algorithms can be realized on the basis of the dynamic chaos, which is sensitive to the initial conditions. The one-dimensional discreet mapping, called the logistic equation, is used for the generation of chaotic digital sequences [1, 4, 10]:

$$x_{n+1} = \lambda \cdot x_n (1 - x_n), \tag{1}$$

where λ is the parameter, x_0 is the initial condition for the generation process. The generation of a chaotic sequence, governed by the logistic equation (1), occurs if the value of the parameter $\lambda \in [3.65 \div 3.95]$.

The block diagrams of the proposed systems of the information transmission as well as the diagrams of the encoder and decoder are shown in Figures 1 and 2, respectively.

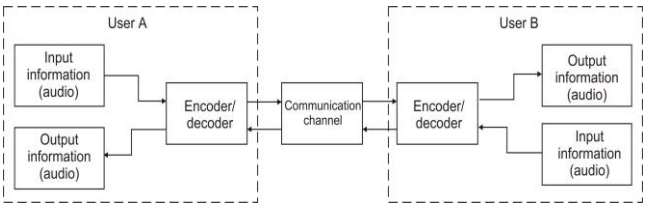

Fig. 1. The block diagram of the system for the transmission of audio information, encrypted by random sequences

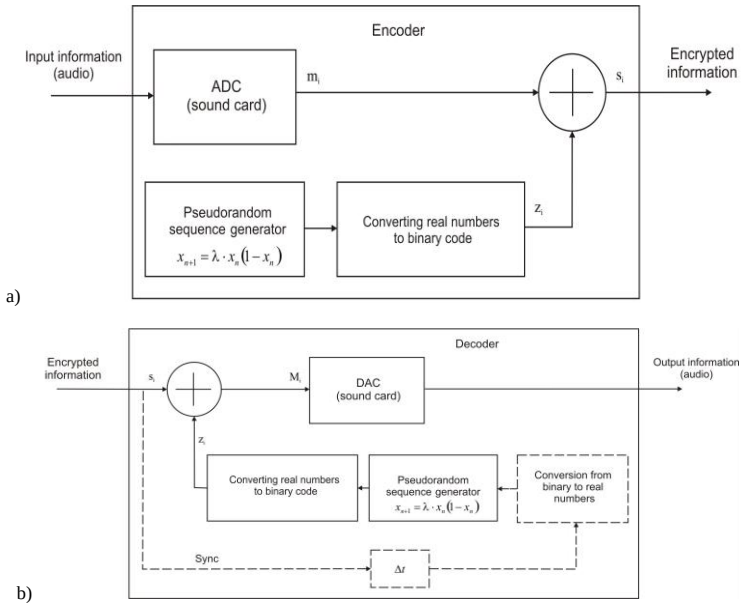

Fig. 2. The block diagram of the encoder a) and decoder b) of the proposed system

The input audio information (analogue signal) from a source of information is fed to the input of the analog-digital converter (ADC), which is a computer sound card, and is turned into a bit representation. The following one-dimensional discrete chaotic mapping (logistic mapping) is used in order to generate the pseudorandom sequences:

$$x_{n+1} = 3{,}94 \cdot x_n(1 - x_n). \tag{2}$$

The generated sequence of numbers is converted into the binary bit representation according to the following equation [9]:

$$z_n = 2^{-1}b_{n1} + 2^{-2}b_{n2} + ... + 2^{-L}b_{nL}, \tag{3}$$

where L is the digit capacity of the binary representation.

The digitized audio information m_i is added to the elements of the generated chaotic sequence, according to module 2 (using the XOR operation):

$$s_i = m_i \oplus z_i. \tag{4}$$

The decryption is performed by the adding, according to module 2, of the received encrypted information to the chaotic sequence, which is generated by the receiver using the same logistic equation and initial conditions [2, 5].

The reliability of the system is determined by the keyspace for the generation of the sequences that is the value of the parameter of the logistic mapping λ and the initial value of x_0. The amount of the keyspace can be calculated as follows:

$$N = (10^n)^2, \tag{5}$$

where n is the accuracy of the given parameters (the number decimal digits). In our case, the accuracy of the parameters is given by the program and is equal to 10. Thus, the keyspace is equal to $(10^{10})^2 = 10^{20}$ that is a satisfactory result for a two-parametric system.

The possibility of the faultless reproduction of information is realized by the application of one of the synchronization methods (complete, generalized, phase, etc.) in similar systems. In works [7, 8] the synchronization is carried out by means of the constant sync pulses by their shape and duration. A sync pulse is transmitted over a time interval, which consists of the duration of the informational signal and the synchronization sequence T_i and T_s, respectively. The time diagram of the transmission of the sync pulse and the informational signal is shown in Figure 3. In our system the synchronization is proposed to be realized by the transmission of the current value of x_n, which is generated by the logistic mapping, over some time intervals. The transmission period of the value x_n depends on the performance of a computer and on the distance between the system subscribers. The setting of the period is carried out at the program level. The maximum value of the transmission period of x_n was equal to 21 μs in the case of Intel P-IV 2.4 GHz computers. The synchronization was stable at the transmission period less than 21 μs that resulted in the almost faultless reproduction of the information.

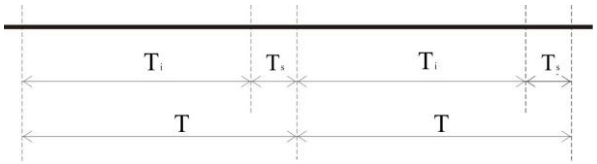

Fig 3. The time diagram of information transmission and synchronization

2. Implementation of the system

Modern computers usually allow to input/output audio signals by means of a standard sound card. The digitization, conversion and reproduction of audio signals are carried out by a computer and are controlled by the application of programming interface (API) of an operating system (Windows or other alternative operating systems). Modern programming environments C++ Builder, Delphi, Visual C + + and others can use the API interface and, thus, can be applied to create the programs of the input, conversion and reproduction of audio files.

The modern software, in particular, programming language Delphi 7.0, was used for the design of the system. The system operates in real-time in the full duplex mode at any hardware implementation of the Internet access. The system subscribers only need to enter the IP address.

The developed program allows:

1) to receive and reproduce the signal from a microphone connected to the built-in PC sound card, with the digital capacity of 8/16 bits and the sampling rate of 44100 Hz;
2) to encrypt/decrypt in real-time audio information (addition on module 2) by means of the periodic sequences obtained from the generator of pseudorandom sequences;
3) to set the parameters of the audio information processing (the digital capacity of 8/16 bits and the sampling rate of 44100 Hz);
4) to set the initial conditions for the generation of pseudorandom sequences.

The results of the program operation are shown in Figure 4.

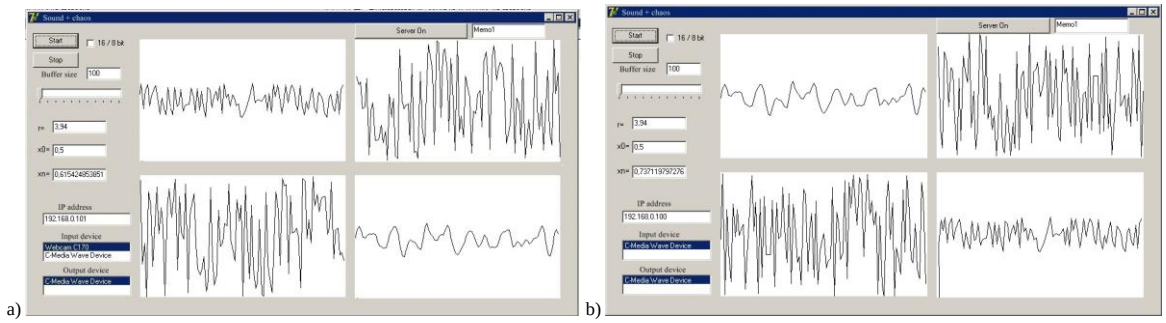

Fig. 4. The results of the operation of the proposed system: a) the window of the user A; b) the window of the user B

Figure 4a shows the window of the user A, who transmits audio information to the user B. The IP-address of the user B (192.168.0.101) is entered in the field of the name of the recipient. The value of the parameter of the encryption key λ is equal to 3.94 for the sender and recipient (Figure 4 a,b). The initial value x_0 is entered only at the beginning of the exchange of information. Afterward, the current value of x_n is shown in the program window. The left top window in Figure 4 a) shows the audio information, which comes from the microphone of the user A, the left bottom window in Figure 4 a) – the encrypted information, the right top window – the received encrypted information by user B, the bottom right window – the decoded information by user B. The user B can transmit audio information to the user A in the same manner (Figure 4 b).

3. Conclusions

We proposed the system for the transmission of audio information with its encryption by chaotic sequences, generated by the logistic equation. The value of the parameter λ of the logistic equation is given within the range from 3.65 to 3.95.

The synchronization of the audio information transmission is carried out by means of the transmission of the current value of x_n, generated by the logistic mapping, through the communication channel over some time intervals. The transmission period of the value x_n depends on the performance of a computer and on the distance between the system subscribers. The trouble free reproduction of the audio information by the recipient was achieved by setting the optimal transmission period of the current value of x_n.

The reliability of the system is determined by the keyspace for the generation of the sequences that is the value of the parameter of the logistic mapping λ and the initial value of x_0. In our case, the accuracy of the parameters is given by the program and is equal to 10 that results in the satisfactory keyspace $(10^{10})^2 = 10^{20}$ for a two-parametric system.

References

[1] Abd al-Karim, Maysa Abd al-Jalil, Iman Qays.: Speech Encryption Using Chaotic Map and Blowfish Algorithms, Journal of Basrah Researches (Sciences), Vol.(39), No.(2), 2013, 68-76.
[2] Cruz-Hernández C., Inzunza-González E., López-Gutiérrez R., Serrano-Guerrero H., García-Guerrero E.: Encrypted audio communication based on synchronized unified chaotic systems, World Academy of Science, Engineering & Technology, 42/2010, 475.
[3] Dmitriev A. S., Panas. A. I.: Dinamicheskij haos: novye nositeli informacii dlja sistem svjazi, Izdatel'stvo fiziko-matematicheskoj literatury, Moskva, 2002
[4] Gnanajeyaraman R., Prasadh K., Ramar Dr.: Audio encryption using higher dimensional chaotic map, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, 2009, 103-107.
[5] Pareek N. K., Patidar V., Sud K.: Cryptography using multiple one-dimensional chaotic maps, Commun. Nonlinear Sci. Numer. Simul., 10(7), 2005, 715-723.
[6] Pecora L. M., Carroll T. L.: Synchronization in chaotic systems, Phys. Rev. Lett. 64, 1990, 821-824.
[7] Politans'kyy L. F., Kushnir M. Ja., Politans'kyy R. L., Elijashiv O. M., Nevel's'kij O. O., Velichko S. V.: Bagatokoristuval'nic'ka sistema zv'jazku z vikoristannjam haotichnoï chastotnoï moduljaciï, Vostochno - Evropeyskiy Zhurnal peredovyh tehnologiy, 1/5(43), 2010, 44-47.
[8] PolItans'kyy R. L., PolItans'kyy L. F., Shpatar P. M., Ivanyuk P. V.: Koduvannya kanalu peredavannya danih, shifrovanih psevdovipadkovimi poslIdovnostyami, Vostochno - Evropeyskiy Zhurnal peredovyh tehnologiy, 1/9(61), 2013, 61-64.
[9] Politans'kyy R. L., Shpatar P. M., Gres' O. V., Ljashkevych V. Ja.: Shyfruvannja informacii' z vykorystannjam psevdovypadkovyh gausovyh poslidovnostej, Vostochno - Evropeyskiy Zhurnal peredovyh tehnologiy, 6/11(60), 2012, 8-10.
[10] Politans'kyy R. L., Shpatar P. M., Gres A. V., Veriga A. D.: Sistema peredachi dannyih s shifrovaniem haoticheskimi posledovatelnostyami, Tehnologiya i konstruirovanie v elektronnoy apparature, 2-3, 2014, 28-32.
[11] Shahov V. G., Nopin S. V.: Modelirovanie zashhity rechevoj informacii s pomoshh'ju personal'nogo komp'jutera, Omskij nauchnyj vestnik, 4(29), 2004, 124-126.

Prof. Yuriy Bobalo
e-mail: rector@lp.edu.ua

Rector of Lviv Polytechnic National University. D.Sc. (technical), Professor.
Research interests: theory of electronic circuits and methods to ensure their reliability. Author of nearly 150 publications in this research area.

Prof. Zenon Hotra
e-mail: zhotra@polynet.lviv.ua

Lviv Polytechnic National University. D.Sc. (technical), Professor, Head of the Department of Electronic Devices.
Research interests: physical processes in semiconductor devices, radio engineering devices and means of telecommunications. Author of nearly 800 publications in this research area.

M.Sc. Olexandr Hres
e-mail: alexgs85@ukr.net

Yuriy Fedkovych Chernivtsi National University. Postgraduate student, Department of Radio Engineering and Information Security.
Research interests: encryption algorithms and encoding information using pseudorandom sequences. Author of nearly 10 publications in this research area.

Ph.D. Ruslan Politans'kyy
e-mail: polrusl@i.ua

Lviv Polytechnic National University, Department of Theoretical Radio Engineering and Radiometrics PhD (Physical and Mathematical), Associate Professor, Department of Radio Engineering and Information Security.
Research interests: application of pseudorandom sequences and chaos in telecommunication systems. Author of nearly 30 publications in this research area.

otrzymano/received: 2014.09.23 *przyjęto do druku/accepted: 2014.09.30*