ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2023. No. 3 (25)*

UDC 004.056.5+534.8 DOI: https://doi.org/10.30837/ITSSI.2023.25.052

O. MOZHAIEV, Y. GNUSOV, O. MANZHAI, V. STRUKOV, V. NOSOV, V. RADCHENKO, S. YENHALYCHEV

STEGANOGRAPHIC METHOD OF ACOUSTIC INFORMATION PROTECTION IN CRITICAL APPLICATIONS SYSTEMS

The subject of the study is the process of protecting acoustic information in critical computer systems to ensure the required level of system security. **The purpose of the article** is to study the method of protecting acoustic information in critical computer systems by means of masking to ensure the impossibility of unauthorized access to the system. The paper outlines the following **tasks:** to analyze the software and hardware masking of speech; to study the masking of speech messages in order to introduce unrecognizability; to consider the features of speech message compression; to investigate methods of covert transmission of acoustic information. **The results** of the work, which were obtained using mathematical methods of information transformation in computer systems, are potentially possible methods of masking speech messages to ensure the impossibility of unauthorized access to the system. The analysis of the functioning of the proposed methods made it possible to formulate specific **conclusions**. The research has shown that the use of direct expansion of the spectrum of discrete signals for steganographic purposes helps to covertly embed information messages in still images. The task of extracting a message on the receiving side of a steganography system is equivalent to the task of detecting information from a mixture of a useful signal and an interference in a broadband communication system. The research revealed certain disadvantages of steganographic systems with an expanded spectrum of discrete signals: the probability of correct extraction of embedded data depends on the amount of distortion introduced, which depends on the provided bandwidth of the steganographic channel. Further research is desirable to analyze the possible use of methods for synthesizing large ensembles of quasi-orthogonal discrete signals with improved ensemble, structural, and correlation properties to ensure higher security of acoustic channels in computer systems for critical applications.

Keywords: acoustic information; technical protection; cryptographic protection; steganographic (steganophonic) protection; modification; computer system languages.

Introduction

Protecting acoustic (speech) information is one of the most important tasks in the overall set of measures to ensure the information security of an object or institution.

The unique features of speech information (SI) circulating in closed rooms and outside them: a large volume and speed of exchange, high confidentiality of some messages, the ability to identify the person making the message, and even the ability to determine the personal attitude to the information being voiced and to draw up his or her psychological portrait determine the relevance and extreme importance of solving the problem of protecting confidential speech information (CSI). Despite the growing role of automated information systems, speech information still plays a key role in information traffic (up to 80% of the total information flow) [1, 2]. This is especially important now, in the context of Russia's military aggression. Therefore, in recent years, more and more attention has been paid to ensuring the security of acoustic information. On the one hand, this is due to the high polyinformativeness of acoustic information. On the other hand, it is due to the variety of information threats to acoustic (speech) information and the peculiarities of their development and implementation scenarios. All of this is reflected in a wide variety of modern methods, algorithms, software and hardware for protecting acoustic information from unauthorized access. The main directions of acoustic information protection are considered to be technical, cryptographic and steganographic (steganophonic) protection.

In a separate section, we consider the issue of protecting acoustic information by masking acoustic information based on modern computer technologies. In recent years, this area has been gaining more and more practical interest among software manufacturers. In order to provide basic security services for audio signals, complex software systems are being created, new methods for receiving, transmitting, processing, and presenting audio signals are being developed and used. Therefore, this article is devoted to the analysis of methods for protecting acoustic information existing in modern information systems of critical applications to ensure a higher level of security of such systems.

Literature review

Threats to speech information are usually realized by technical leakage channels, namely: acoustic, acoustic-vibration (vibroacoustic), acousto-optoelectronic

Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 3 (25)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

(laser acoustic), acoustoelectric, videoacoustic, high-frequency imposition. These channels can use a wide range of portable technical reconnaissance equipment [3, 4]:

– portable sound recording equipment (small-sized voice recorders, tape recorders and microphone-based recording devices)

– electronic stethoscopes;

– electronic devices for intercepting speech information (embedded devices) with microphone and contact type sensors with the transmission of intercepted information via radio, optical (in the infrared wavelength range) and ultrasonic channels, power supply network, telephone lines, connecting lines of auxiliary digital circuitry);

– technical means or special lines;

– optoelectronic acoustic systems, etc.

The main technical methods of protecting speech information today are:

– information concealment, which involves technical closure (frequency, time and combined analog scrambling);

– energy concealment, which is carried out by means of sound insulation, sound absorption, jamming in the premises (spatial jamming) and jamming of the functional communication channel with interference that masks speech signals (linear jamming);

– cryptographic concealment based on the discretization of speech information with subsequent encryption and reverse conversion to an analog signal or digital transmission over a communication channel;

– vocoder protection of speech information.

The study of steganographic concealment of speech information in data transmission channels, which can also be realized after cryptographic transformations, is of interest.

Recently, both developers and consumers of semantic protection of acoustic information have been observing an increasingly steady trend towards the use of new computer technologies for ensuring the security of speech communications without the use of classical cryptographic methods. In this regard, computer-based technologies for masking acoustic information are becoming increasingly attractive. However, one should not forget about cryptographic methods of protecting acoustic information, in particular: instantaneous cryptanalysis of GSM with only ciphertext [5]; real-time cryptanalysis of the assumed A5 stream cipher [6, 7]; cryptanalysis of anomalous behavior of a computer system [8]; crypto-resistant methods and random number generators in Internet of Things (IoT) devices [9].

The aim of the article is to analyze the methods of protecting acoustic information in computer systems of critical applications by means of masking to ensure the impossibility of unauthorized access to the system:

– to achieve this goal, the following tasks need to be performed:

– analyze software and hardware speech masking;

– to investigate the masking of speech messages in order to introduce unrecognizability;

– analyze the features of speech message compression;

– to investigate methods of covert transmission of acoustic information.

1. Spectrum expansion methods to improve the efficiency of discrete message transmission

In today's discrete message transmission systems, two methods of spectrum expansion are used:

– pseudo-random *Frequency Hopping Spread Spectrum* method (*FHSS*). Its essence lies in the periodic jump-like change of frequency, which is carried by a certain algorithm to a known receiver and transmitter. The advantage of this method is its simplicity of implementation; it is used in *Bluetooth*;

– *Direct Sequence Spread Spectrum (DSSS*) method. It is more efficient than the FHSS method, but more difficult to implement. The essence of the method is to increase the modulation clock frequency, in which case each symbol of the transmitted message corresponds to a sufficiently long pseudo-random sequence (PRS). The method is used in systems such as *CDMA* and *IEEE* 802.11.

Expanding the spectrum by pseudo-randomly tuning the operating frequency. In order to prevent radio communication from being intercepted or jammed by narrowband noise, it was proposed to transmit with a constant change of carrier within a wide frequency range. As a result, the signal power was distributed over the entire range, and listening to a particular frequency produced only a small amount of noise. The sequence of carrier frequencies was pseudo-random, known only to the transmitter and receiver. Attempting to jam the signal in a narrow range also did not degrade the signal too much, since only a small part of the information was jammed. The idea of this method is illustrated in Fig. 1.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 3 (25)

During a fixed time interval, transmission is carried out on a constant carrier frequency. At each carrier frequency, standard modulation techniques such as *FSK* or *PSK* are used to transmit discrete information. In order for the receiver to synchronize with the transmitter, synchronization tones are transmitted for a period of time to mark the beginning of each transmission period. Consequently, the useful rate of this coding method is lower due to the constant synchronization overhead.

The carrier frequency varies according to the frequency subchannel numbers produced by the pseudorandom number algorithm. The pseudorandom sequence depends on a certain parameter called the initial number. If the receiver and the transmitter know the algorithm and the value of the initial number, they change frequencies in the same sequence, which is called the pseudorandom frequency hopping sequence.

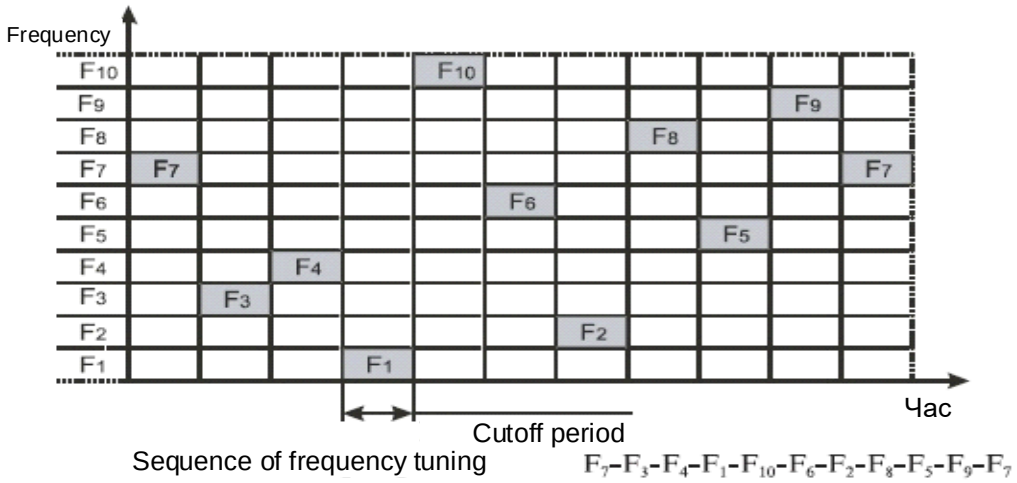

Fig. 1. Spectrum expansion by frequency hopping tuning

FHSS methods are used in *IEEE* 802.11 and *Bluetooth* wireless technologies. In *FHSS*, the approach to using the frequency range is not the same as in other coding methods – instead of economically using a narrow band, an attempt is made to occupy the entire available range. At first glance, this does not seem very efficient, since only one channel is operating in the band at any given time. However, the latter statement is not always true – spread spectrum codes can also be used to multiplex multiple channels over a wide range. In particular, *FHSS* methods make it possible to organize the simultaneous operation of several channels by selecting such pseudo-random sequences for each channel so that at any given time each channel operates at its own frequency (of course, this can only be done if the number of channels does not exceed the number of frequency subchannels).

Spectrum expansion using the direct sequence method. The direct sequential spread spectrum method also uses the entire frequency range allocated for one communication line. Unlike the *FHSS* method, the entire frequency range is occupied not by constantly switching from frequency to frequency, but by replacing each bit of information with N bits, so that the signal transmission rate increases by *N* times. This means that the signal spectrum is also expanded by a factor of *N*. It is enough to choose the appropriate data rate and N value so that the signal spectrum fills the entire range.

To transmit data in a broadband communication system, an information signal $x(t)=\begin{cases}+1\\-1\end{cases}$ is modulated by multiplying it by an expansion coded signal $g(t)=\Phi_i\in\Phi$ – a pseudo-random sequence of the above-mentioned ensembles of discrete signals. Since the code signal is similar to noise in its statistical properties, the resulting expanded signal

$$y'(t)=y(t)+e(t) \quad (1)$$

In the process of receiving in the demodulator, the received signal $y'(t)=y(t)+e(t)$ as a mixture of the transmitted sequence $y(t)$ and events in the error channel $e(t)$ is multiplied by a synchronized copy of the expanded signal $g(t)$. In other words, the correlation coefficient is calculated on the receiving side, the value of which determines the decision-making rule:

$$\rho\left(y'(t),g(t)\right)=\frac{1}{n}\sum_{z=0}^{n-1}x(t)\Phi_{i_z}\Phi_{i_z}+\frac{1}{n}\sum_{z=0}^{n-1}e(t)\Phi_{i_z}, \quad (2)$$

Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 3 (25)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

differ slightly from the noise in the communication channel, which makes it possible to carry out covert transmission.

Due to the pseudo-randomness of Φ_i, used as $g(t)$, he second terms in the right-hand side of the equation can be neglected (the number of "+1" is approximately equal to the number of "–1"), i.e.

$$\rho\left(y'(t),g(t)\right)\approx\rho\left(y(t),g(t)\right)=x(t)\frac{1}{n}\sum_{z=0}^{n-1}\left(\Phi_{i_z}\right)^2=x(t), \quad (3)$$

that is, the value of the information signal on the receiving side is determined according to the expression

$$x(t)=\begin{cases}+1, \text{if } \rho\left(y'(t),g(t)\right)\approx+1;\\ -1, \text{if } \rho\left(y'(t),g(t)\right)\approx-1,\end{cases} \quad (4)$$

where the "$\approx$" sign implies the presence of errors caused by natural or intentional interference in the communication channel.

The block diagram of the information transmission path using direct spectrum expansion is shown in Fig. 2.

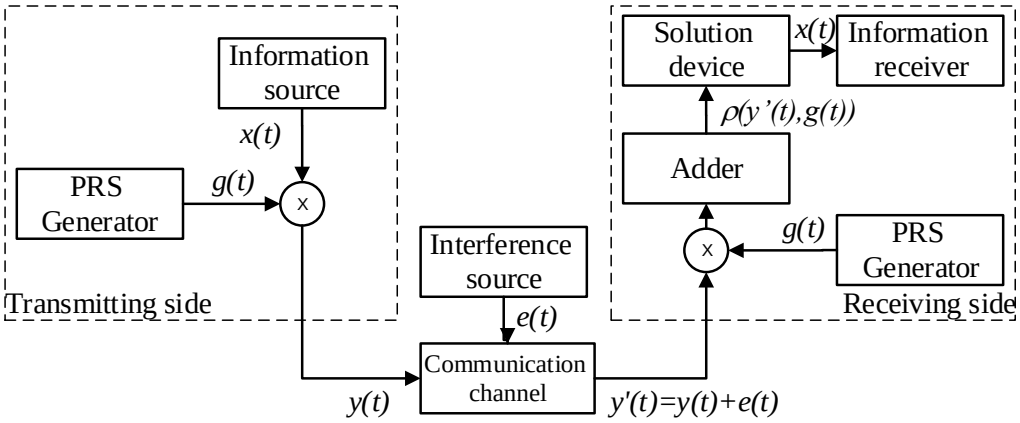

Fig. 2. Block diagram of the information transmission track using direct spectrum expansion

Suppose that the time interval of the unmodulated signal $x(t)$ is equal to T, and its frequency, respectively, is $F\left(x(t)\right)=1/T$. Transmission of a modulated signal $y(t)$ with the same time interval T will lead to a broadening of the frequency spectrum of the transmitted signal proportional to the number of elements of the pseudorandom sequence, i.e., proportional to the length n: $F\left(y(t)\right)=n\frac{1}{T}=nF\left(x(t)\right)$. However, the use of direct expansion of the transmitted signal spectrum ensures the simultaneous transmission of many other information signals in the same frequency band. This follows from the mutual orthogonality (quasi-orthogonality) of the used ensembles of discrete signals. Indeed, if an additive mixture $\sum_{\ell} y_l(t)$ of several modulated signals is received at the receiving end, then the calculation of the correlation coefficient will give the following:

$$\rho\left(\sum_{\ell} y_\ell(t),g(t)\right)=\frac{1}{n}\sum_{\ell}\sum_{z=0}^{n-1}x_\ell(t)\Phi_{\ell_z}\Phi_{i_z}. \quad (5)$$

But all the sequences in the set have a low value of mutual correlation, i.e., under the condition $\ell\neq i$ we have (for orthogonal signals we have the equality $\rho\left(\Phi_\ell,\Phi_i\right)=0$. So, all the terms if $\ell\neq i$, on the right side of equality (5) can be neglected. Hence, in the presence of a discrete signal in the additive mixture, we have expression (3) and the corresponding decision-making rule (4).

The purpose of *DSSS* coding is the same as that of *FHSS:* to increase immunity to interference. Narrowband interference will distort only certain frequencies of the signal spectrum, so that the receiver is more likely to correctly recognize the transmitted information.

A code that replaces a binary unit of the original information is called an expansion sequence, and each bit of such a sequence is called a chip (elementary signal). Accordingly, the transmission rate of the resulting code is called the chip rate. The binary zero is encoded by the inverse value of the expansion sequence. Receivers need to know the expansion sequence used by the transmitter to understand the information being transmitted.

The number of bits in the expansion sequence determines the expansion factor of the original code.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 3 (25)

As with *FHSS*, any type of modulation, such as *BFSK*, can be used to encode the bits of the resulting code.

The higher the expansion factor, the wider the spectrum of the resulting signal and the higher the degree of interference suppression. But in this case, the spectrum range occupied by the channel increases. Usually, the expansion factor has a value from 10 to 100.

Let's list some of the properties of signals with direct spectrum expansion that are most important from the point of view of organizing multiple access in communication systems with mobile objects.

1. *Multiple access.* If several subscribers use the transmission channel at the same time, then there are several signals with direct spectrum expansion in the channel at the same time. The receiver of a particular subscriber's signal performs the opposite operation – convolution of this subscriber's signal by using the same pseudo-random signal that was used in the transmitter of this subscriber. This operation concentrates the power of the received broadband signal back into a narrow frequency band equal to the spectral width of the information symbols. If the mutual correlation function between the pseudo-random signals of this subscriber and other subscribers is sufficiently small, then in the process of coherent reception, only a small fraction of the power of the signals of other subscribers will fall into the information band of the subscriber's receiver. The signal of a particular subscriber will be received correctly.

2. *Multiple beam interference.* If the pseudorandom signal used to expand the spectrum has a perfect autocorrelation function whose value outside the interval $[-t_0, +t_0]$ is zero, and if the received signal and a copy of this signal in another beam are shifted in time by more than $2t_0$, then, subject to signal convolution, its copy can be considered as interference that adds only a small fraction of power to the information band.

3. *Narrowband interference*. In the case of coherent reception, the received signal is multiplied in the receiver by a copy of the pseudorandom signal used to expand the spectrum in the transmitter. Thus, the receiver will perform a narrowband interference spectrum expansion operation similar to the one performed with the information signal in the transmitter. Consequently, the spectrum of the narrowband interference in the receiver will be expanded by a factor of B, where B is the expansion factor, so that only a small fraction of the interfering power, B times less than the original interfering power, will be transmitted to the information band.

4. *Interception probability.* Since a direct spread spectrum signal occupies the entire frequency band of the system during the entire transmission time, its radiated power per 1 Hz of the band will be very small. Therefore, detecting such a signal is a very difficult task.

Therefore, a promising direction in the development of modern broadband communication systems with direct spectrum expansion is the development and research of methods for synthesizing large ensembles of quasi-orthogonal discrete signals with improved ensemble, structural, and correlation properties.

The considered approach to the organization of digital jamming communication channels was applied in the construction of steganographic methods of information protection. For example, spectrum expansion by direct sequence was used to create a steganographic method for embedding information in still images. Let's consider one of the variants of this method implementation, authored by *J. Smith* and *W. Comiskey* [10]. We will study its effectiveness in terms of the provided throughput of the steganographic communication channel and the achieved resistance to unauthorized extraction of information messages.

2. Direct spectrum expansion in steganography

In the Smith-Comiskey method, as in the direct spread spectrum communication systems discussed above, an information message is bitwise modulated by multiplying it by an ensemble of orthogonal signals. The modulated message is then embedded in a container – a still image.

Let us introduce some conventions and mathematical relations, which, by analogy with the broadband digital communication systems discussed above, will allow us to study the features of construction and information exchange in a steganosystem [11–13].

Let us represent the information message m, to be embedded in a digital image container in the form of blocks m_i of equal length, i.e. $m = (m_0, m_1, ..., m_{N-1})$, where each block m_i is a sequence (vector) of n bits:

$$m_i = \left(m_{i_0}, m_{i_1}, ..., m_{i_{n-1}}\right).$$

We consider an image container as a set of data C of dimension $K \times L$ divided into subblocks of size $k \times l = n$. The elements of the array C can be, for example, raster data of the image used.

Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 3 (25)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

The secret key data is a set of basic functions

$$Key = \Phi = \{\Phi_0, \Phi_1, ..., \Phi_{M-1}\},$$

where all basic functions $\Phi_i = \left(\phi_{i_0}, \phi_{i_1}, ..., \phi_{i_{n-1}}\right)$ – mutually orthogonal discrete signals with a length equal to the message block n size, that is, for any $i, j \in [0, ..., M-1]$ equality m_i is fulfilled

$$\rho\left(\Phi_i, \Phi_j\right) = \frac{1}{n}\sum_{z=0}^{n-1} \Phi_{i_z} \Phi_{j_z} = \begin{cases} +1, & \text{if } i = j; \\ -1, & \text{if } i \neq j. \end{cases}$$

A formal graphical representation of the information message, image container, and key data is shown in Fig. 3.

The purpose of steganographic information transformation is to embed each individual message block m_i in the corresponding block of the image container.

The data block of a digital image with the dimension of $K \times L$ elements can contain $K \times \frac{L}{n}$ blocks of an information message, i.e., up to $K \times L$ bits.

The division of the container into blocks can be arbitrary, but as practice shows, the most appropriate (smaller numerical spread of values in a block, as opposed to a one-dimensional representation) is the two-dimensional division shown in Fig. 3. As the key data (an array of basis functions $Key = \Phi$), we use the above-mentioned ensembles of orthogonal discrete Walsh–Hadamard signals.

The embedding of the information message is carried out as follows. Each message block m_{i_j}, $j = 0, ..., n-1$ is mapped to a separate block of the image container. All information bits of the block m_{i_j}, $j = 0, ..., n-1$ are represented as an information signal

$$m_{i_j}(t) = \begin{cases} +1, & m_{i_j} = 1; \\ -1, & m_{i_j} = 0 \end{cases}$$ and modulated by an expansion code signal (basis functions), i.e. PRS $\Phi_j \in \Phi$.

Thus, a modulated information signal is generated for each information block:

$$E_i(t) = \sum_{j=0}^{n-1}\sum_{z=0}^{n-1} m_{i_j}(t)\Phi_{j_z}. \qquad (6)$$

The received message block E_i is pixel-by-pixel summed with the container subblock.

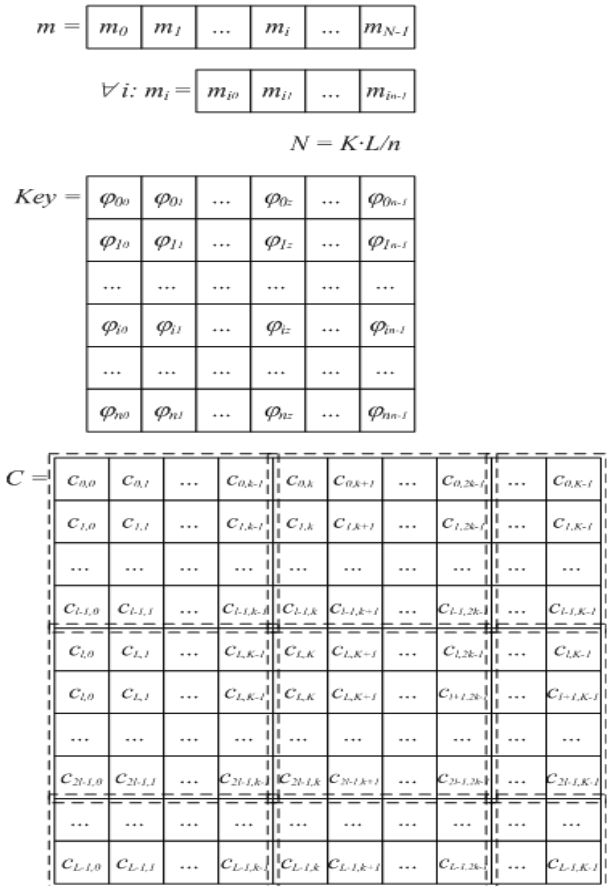

Fig. 3. Formal representation of the information message, image container, and key data

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Let's designate the container blocks as follows (see Figure 3):

$$C_0 = \begin{pmatrix} c_{0,0} & c_{0,1} & \dots & c_{0,k-1} \\ c_{1,0} & c_{1,1} & \dots & c_{1,k-1} \\ \dots & \dots & \dots & \dots \\ c_{\ell-1,0} & c_{\ell-1,1} & \dots & c_{\ell-1,k-1} \end{pmatrix}, \; C_1 = \begin{pmatrix} c_{0,k} & c_{0,k+1} & \dots & c_{0,2k-1} \\ c_{1,k} & c_{1,k+1} & \dots & c_{1,2k-1} \\ \dots & \dots & \dots & \dots \\ c_{\ell-1,k} & c_{\ell-1,k+1} & \dots & c_{\ell-1,2k-1} \end{pmatrix}, \dots, \; C_{N-1} = \begin{pmatrix} c_{L-l-1,K-k-1} & c_{L-l-1,K-k} & \dots & c_{L-l-1,K-1} \\ c_{L-l,K-k-1} & c_{L-l,K-k} & \dots & c_{L-l,K-1} \\ \dots & \dots & \dots & \dots \\ c_{L-1,K-k-1} & c_{l-1,k+1} & \dots & c_{L-1,K-1} \end{pmatrix}.$$

The corresponding modulated information signals $E_i(t)$ are presented in the form of a two-dimensional data array:

$$E_i = \begin{pmatrix} E_{i_0} & E_{i_1} & \dots & E_{i_{k-1}} \\ E_{i_k} & E_{i_{k+1}} & \dots & E_{i_{2k-1}} \\ \dots & \dots & \dots & \dots \\ E_{i_{(\ell-1)(k-1)-k+1=n-k+1}} & E_{i_{(\ell-1)(k-1)-k+2=n-k+2}} & \dots & E_{i_{(\ell-1)(k-1)=n-1}} \end{pmatrix}, i = 0,\dots,N-1.$$

Then the steganogram (filled container) is formed by combining data arrays S_i, $i = 0,\dots,N-1$:

$$S_i = C_i + E_i \times G, \qquad (7)$$

where $G > 0$ – gain of the expansion signal, which sets the "energy" of the embedded bits of the information sequence.

Thus, a filled container S is generated from the formed blocks S_i, $i = 0,\dots,N-1$ by combining them, as shown in Fig. 3, for the initial (empty) container C.

At the stage of data construction, it is not necessary to have information about the primary container C. The decoding operation consists in recovering the hidden message by projecting each block S_i, of the obtained steganoimage S onto all the basic functions $\Phi_j \in \Phi$, $i = 0,\dots,N-1$. To do this, each block S_i is represented as a vector $S_i = \left(S_{i_0}, S_{i_1}, \dots, S_{i_{n-1}}\right)$, $i = 0,\dots,N-1$.

To extract the j-th bit of the message from the i-th block of the steganomagnetic image, it is necessary to calculate the correlation coefficient between Φ_j and the received block S_i (represented as a vector):

$$\rho\left(S_i, \Phi_j\right) = \frac{1}{n}\sum_{z=0}^{n-1} S_{i_z}\Phi_{j_z} = G \cdot \frac{1}{n}\sum_{z=0}^{n-1} E_{i_z}\Phi_{j_z} + \frac{1}{n}\sum_{z=0}^{n-1} C_{i_z}\Phi_{j_z}, \qquad (8)$$

where C_i – is a one-dimensional array, i.e., the corresponding block of the container, represented as a vector.

Let's assume that the array has a random statistical structure, i.e., the second term on the right-hand side of expression (8) is close to zero and can be ignored.

Then we have:

$$\rho\left(S_i, \Phi_j\right) \approx G \cdot E_i \cdot \Phi_j = G \cdot \sum_{\ell=0}^{n-1}\sum_{z=0}^{n-1} m_{i_x}(t) \cdot \Phi_{l_z}\Phi_{j_z}. \qquad (9)$$

By analogy with (8), we note that all sequences from the set Φ are mutually orthogonal, i.e., provided $\ell \neq j$ we have $\rho\left(\Phi_i, \Phi_j\right) = 0$. Consequently, all terms on the right-hand side of equation (9) can be neglected if $\ell \neq j$. Hence, we have:

$$\rho\left(S_i, \Phi_j\right) \approx G \cdot m_{i_j}(t) \cdot \frac{1}{n}\sum_{z=0}^{n-1}\left(\Phi_{j_z}\right)^2 = G \cdot m_{i_j}(t). \qquad (10)$$

According to the rule of useful signal extraction:

$$x(t) = \begin{cases} \text{"1"}, & \text{if } \textit{polarity} > 0; \\ \text{"0"}, & \text{if } \textit{polarity} < 0; \\ \text{external signal, if } & \textit{polarity} = 0, \end{cases} \qquad (11)$$

values $m_{i_j}(t)$ can be easily recovered using the sign function (*polarity* – the polarity of the peak of the correlation function).

Since $G > 0$ and $n > 0$ the sign $\rho\left(S_i, \Phi_j\right)$ in (10) depends only on $m_{i_j}(t)$. Hence we have:

$$m_{i_j}(t) = sign\left(\rho\left(S_i, \Phi_j\right)\right) = \begin{cases} -1, & \text{if } \rho\left(S_i, \Phi_j\right) < 0; \\ +1, & \text{if } \rho\left(S_i, \Phi_j\right) > 0; \\ ?, & \text{if } \rho\left(S_i, \Phi_j\right) = 0. \end{cases} \qquad (12)$$

If $\rho\left(S_i, \Phi_j\right) = 0$ at (10) we assume that the embedded information has been lost.

A block diagram of embedding information in an image container using direct spectrum expansion for covert message transmission is shown in Fig. 4.

Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 3 (25)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Fig. 4 shows that the process of embedding information messages for covert transmission is very similar to the process of expanding the spectrum of discrete signals in communication systems (see Fig. 2). The element-by-element assembly of a modulated message $E(t)$ with an image container $C(t)$ should be interpreted as the imposition of errors $e(t)$ on the useful signal in the communication channel $y(t)$. The task of constructing a message $m(t)$ from $S(t)$ at the receiving side of the steganosystem is equivalent to the task of detecting $x(t)$ mixture of a useful signal and an interference $y'(t) = y(t) + e(t)$ in a broadband communication system. That is, the considered steganosystem inherits all the advantages of broadband communication systems: resistance to unauthorized extraction of embedded messages (analogous to concealment in a communication system), resistance to destruction or modification of embedded messages (analogous to interference protection), resistance to imposing false messages (analogous to imitation resistance in a communication system).

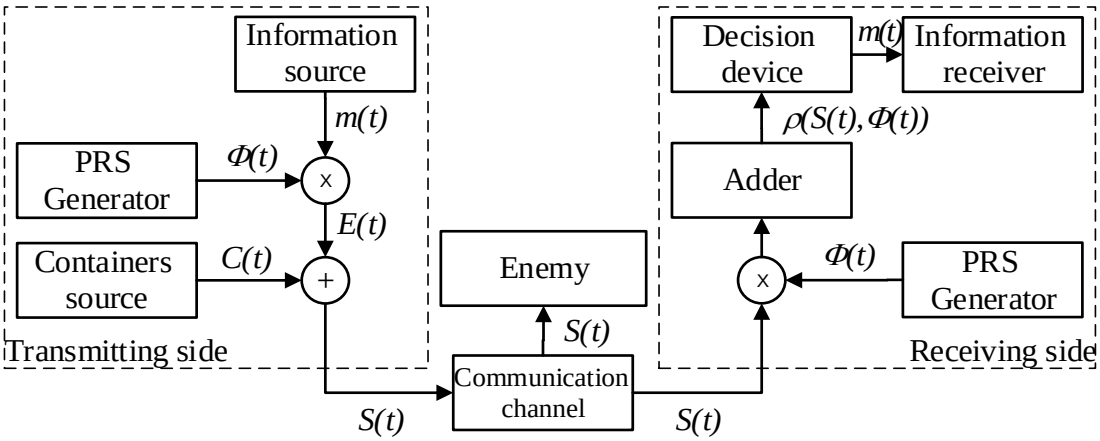

Fig. 4. Block diagram of embedding information in an image container for covert messaging

Thus, the use of direct expansion of the spectrum of discrete signals makes it possible to embed information in still images for covert transmission and thus implement steganographic information protection.

3. Evaluating the effectiveness of the steganosystem

The effectiveness of a technical system is broadly understood as the correspondence of the result of a certain operation to the required parameter. In this case, the technical system is a means of implementing the operation under study [14, 15].

In accordance with this process, a steganographic system is a technical means of implementing an operation aimed at hiding the fact of covert information transmission from the enemy. So, taking into account the functional purpose of the steganographic system, we will introduce performance indicators.

1. Bandwidth is the ratio of the volume V of information embedded in the container to the total volume of the container D

$$Q = V / D . \qquad (13)$$

2. Key data volume (in bits)

$$\ell_{Key} = \log_2 \left(|Key| \right), \qquad (14)$$

where $|Key|$ – power of the key data set.

3. The strength of a steganographic method will be evaluated as the inverse of the power of the set of secret key data. It can be interpreted as a probabilistic indicator of the selection of a secret key:

$$W = 1/|Key| = 2^{-l_{Key}} . \qquad (15)$$

4. The amount of distortion added as a percentage of the arithmetic mean of all absolute values of the container data Δ-changes to the maximum possible value $\Delta_{\max}$:

$$I = \frac{\Delta_{cp}}{\Delta_{\max}} \cdot 100 = \frac{100}{\Delta_{\max} \cdot D} \cdot \sum_{i=1}^{D} |\Delta_i| , \qquad (16)$$

where Δ_i – Δ-changes of the i-th container element.

5. Probability of erroneous construction of message information data

$$P_{ош} = \lim_{D \to \infty} \frac{V_{ош}}{D} = 1 - \lim_{D \to \infty} \frac{V - V_{ош}}{D} , \qquad (17)$$

where $V_{ош}$ – is the amount of falsely constructed data.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2023. No. 3 (25)

Using (13)–(17), let us evaluate the effectiveness of the considered steganographic method of information protection.

1. **Bandwidth capacity.** For each n-element block S_i of the filled container (steganogram), there is a n-bit vector of the embedded message m_i. Thus, $Q = 1/B$, where B is the amount of data per element of the container. To embed an image in raster data (color model *R*, *G*, *B*) with 8-bit encoding of each color, we have $B = 8$ and $Q = 1/8$.

2. **Key data volume.** The key data is an ensemble of discrete signals formed by the rows of the Hadamard matrix of order n. Thus, the set of key data should be understood as a set of different (non-isomorphic) Hadamard matrices, each of which represents an ensemble of discrete signals.

The given power estimates M_A give an estimate of the number of Walsh–Hadamard ensembles of discrete signals, i.e., an estimate of the power of non-equivalent keys of a quilted system. Thus, the amount of key data is estimated as $l_{key} = \log_2(M_A)$.

3. **Probability of selecting a secret key** $W = (M_A)^{-1}$.

4. To estimate the amount of **distortion being introduced**, let's use expression (16). The second term on the right-hand side of (16) determines the magnitude of the Δ-changes in the container data elements. The multiplier E_i is formed by summing the discrete signals (which take the value ±1) with the corresponding polarities (given by $m_{i_j}(t)$). Thus, all E_i elements will take values in the range $[-n,...,+n]$, and the corresponding Δ-changes of the container elements will not exceed $|\Delta_i| \le n \cdot G$.. Hence, we have an upper bound on the value of the added distortion:

$$I = \frac{\Delta_{cp}}{\Delta_{\max}} \cdot 100 \le \frac{n \cdot G}{\Delta_{\max}} \cdot 100. \qquad (18)$$

To embed into raster data an image (*R*, *G*, *B* color model) with 8-bit encoding of each color and using discrete signals $n = 256$, even with the added distortion $G = 1$, can reach 100%. It is possible to reduce the added distortion by decreasing the number of embedded data bits m_{i_j}, which will inevitably lead to a decrease in the bandwidth of the steganographic communication channel.

5. ***Probability of erroneous extraction***. The information message extraction, as well as in the case of the organization of anti-jamming communication (see (7)–(12)), is carried out by the correlation method (see (13)–(17)). Therefore, the extraction error will occur if the sign of the correlation coefficient $\rho(S_i, \Phi_j)$ in the expression (17) is changed.

The coefficient $\rho(S_i, \Phi_j)$ is expressed as:

$$\rho(S_i, \Phi_j) = \rho(C_i + E_i \cdot G, \Phi_j) = \rho(C_i, \Phi_j) + \rho(E_i \cdot G, \Phi_j).$$

The last term does not change the sign of $\rho(S_i, \Phi_j)$, event $\rho(S_i, \Phi_j) = \rho(E_i \cdot G, \Phi_j)$ corresponds to error-free message retrieval (see (11), (12)).

Thus, an error in extracting the message information bit m_{i_j} will occur if the event happens

$$|\rho(C_i, \Phi_j)| > \rho|E_i \cdot G, \Phi_j| = |G \cdot m_{i_j}| = G, \qquad (19)$$

that is, when the absolute value of the correlation coefficient used to embed a bit m_{i_j} of a discrete signal Φ_j in the block of the container C_i in which this bit is embedded exceeds the amplification coefficient G.

So, we write:

$$P_{er} = P(|\rho(C_i, \Phi_j)| > G),$$

where $P(x)$ – the probability of a random event x occurring.

In other words, the correct extraction of an embedded message is a random event, the probability $P_{er.fr}$ of which is directly related to the statistical properties of the image container used. To extract the message correctly

$$P_{er} = 0, P_{er.fr} = 1 - P_{er} = 1, \qquad (20)$$

for error-free message extraction, it is necessary to strive for mutual orthogonality of separate image fragments C_i and to use discrete signals Φ_j as secret keys.

In this case, the event

$$|\rho(C_i, \Phi_j)| = 0 < G$$

is valid for every $i = 0,..., N-1$ and is executed (20).

At the same time, experimental studies have shown that the correlation coefficient is usually much higher than zero $|\rho(C_i, \Phi_j)| >> 0$ and the event (19) occurs very often. The fact is that the elements of discrete signals $\Phi_j \in \Phi$ take the value of $\begin{cases} +1 \\ -1 \end{cases}$, and the corresponding normalized correlation coefficient $\rho(\Phi_i, \Phi_j)$ in absolute value does not exceed the

Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 3 (25)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

length n of the sequence and lies in the range of $[0,...,1]$, from which condition (20) actually follows.

However, the elements of the container take values from a numeric field $[0,...,Y]$, which dimensionality is set by the way the image data is encoded. For example, when embedding information in raster image data (*R*, *G*, *B* color model) with 8-bit encoding of each color, the corresponding C_i values take on the range of integers $[0,...,255]$. That is, the absolute value normalized with respect to the n correlation coefficient $\left|\rho\left(C_i,\Phi_j\right)\right|$ will lie in the range of $[0,...,Y]$, and for the error-free extraction of all bits of the message (20), the condition $G > Y$ must be met.

As studies have shown, an increase of G leads to an inevitable increase in the value of the added distortion (19). Under the condition $I > 2...3\%$ (the threshold of human visual sensitivity), they become noticeable to an outside observer, which compromises the steganochannel and makes it impossible to use the considered steganosystem.

Conclusions

Thus, in the course of research, the contradictions underlying the development and use of steganographic systems with an expanded range of discrete signals were revealed:

– the probability of correct extraction of embedded data $P_{er.fr}$ directly depends on the amount of added distortion I;

– the amount of added distortion I, directly depends on the amount of embedded data bits, i.e. on the bandwidth of steganochannel Q;

– probability of correct extraction of embedded data $P_{er.fr}$ directly depends on the statistical properties of the image container used.

The following empirical estimates were obtained as a result of the research:

– dependence of the added distortion value I, of the steganochannel Q bandwidth;

– dependence of the added distortion value I, and the frequency of extraction errors $P_{er}^{*} \approx P_{er}$ from the amplification coefficient G;

– dependence of the added distortion value I from the frequency of extraction errors $P_{er}^{*} \approx P_{er}$.

The research was conducted under the conditions of embedding information in raster image data (*R*, *G*, *B* color model) with 8-bit encoding of each color.

The analysis of the obtained dependencies confirms the conclusions made earlier, and the convergence of the experimental results with theoretical considerations indicates the reliability of the results.

The research has shown that the use of direct expansion of the spectrum of discrete signals for steganographic purposes makes it possible to covertly embed information messages in still images. The task of extracting a message on the receiving side of a steganography system is equivalent to the task of detecting information from a mixture of a useful signal and an interference in a broadband communication system.

The research has revealed the following disadvantages of steganographic systems with an expanded spectrum of discrete signals: the probability of correct extraction of embedded data depends on the amount of added distortion, which depends on the provided bandwidth of the steganographic channel. In other words, the practical construction of a steganosystem is associated with finding a compromise between the amount of added distortion, the probability of correct message retrieval on the receiving side, and the provided bandwidth. In addition, the research has established that the probability of correct extraction of embedded data directly depends on the statistical properties of the image container used.

References

1. Kosenko, V. (2017), "Principles and structure of the methodology of risk-adaptive management of parameters of information and telecommunication networks of critical application systems", *Innovative technologies and scientific solutions for industries*, No 1 (1), P. 75–81. DOI: https://doi.org/10.30837/2522-9818.2017.1.046

2. Kosenko, V. (2017), "Mathematical model of optimal distribution of applied problems of safety-critical systems over the nodes of the information and telecommunication network", *Advanced Information Systems*, Vol. 1, No. 2, P. 4–9. DOI: https://doi.org/10.20998/2522-9052.2017.2.01

3. Ivanchenko, S., Havrylenko, O., Lipskyi, O., Shevtsov, A. "Technical channels of information leakage. Procedure for creating complexes of technical information protection". ["Tekhnichni kanaly vytoku informatsii. Poriadok stvorennia

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2023. No. 3 (25)*

kompleksiv tekhnichnoho zakhystu informatsii"], Study guide K.: ISZZI NTUU "KPI", 2016. 104 p. available at: https://ela.kpi.ua/bitstream/123456789/15155/1/NP_Tekhnichni_kanaly_vytku_inf.pdf

4. Oleynikov, A. "Methods and means of information protection: Study guide for students of higher educational institutions". ["Metody ta zasoby zakhystu informatsii"]. Kharkiv. NTMT, 2014. 298 p. available at: https://ref.nure.ua/navchalna-laboratorija-tehnichnogo-zahistu-informacii

5. Nuzhny, S. M. (2018). "Improved technology for assessing the degree of protection of language information". Modern information protection. ["Udoskonalena tekhnolohiia otsinky stupenia zakhystu movnoi informatsii"]. Vol. 1 (33). P. 66–73. available at: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1796

6. Blintsov, V., Nuzhniy, S., Parkhuts, L., Kasianov, Y. (2018), "The objectified procedure and a technology for assessing the state of complex noise speech information protection". *Eastern-European Journal of Enterprise Technologies*, Vol. 5 (9 (95)). P. 26–34. DOI: https://doi.org/10.15587/1729-4061.2018.144146

7. Hrystak, A., Kinzeryavyy, V., Prysiazhnyi, D., Burmak, Y., Samoylik, Y. "High-speed and hash function for blockchain security mechanisms". Scientific and practical cyber security journal (SPCSJ). Vol. 4(1). 2020. P. 65–70. available at: https://journal.scsa.ge/ru/papers/high-speed-and-secure-hash-function-for-blockchain-security-mechanisms-3/

8. Mozhaiev, O., Semenov, S., Kuchuk, N., Mozhaiev, M., Tiulieniev, S., Gnusov, Y., Yevstrat, D., Chyrva, Y., Kuchuk, H. (2022), "Development of a method for determining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples". *Eastern-European Journal of Enterprise Technologies*, Vol. 6 (4 (120)), P. 40–49. DOI: https://doi.org/10.15587/1729-4061.2022.269128

9. Mozhaiev, O., Klimushyn, P., Solianyk, T., Gnusov, Y., Manzhai, O., Svitlychnyi, V. (2022), "Crypto-resistant methods and random number generators in internet of things (iot) devices". *Innovative technologies and scientific solutions for industries*. № 2 (20), P. 22–34 DOI: https://doi.org/10.30837/ITSSI.2022.20.022

10. Mozhaiev, O, Klimushyn, P., Solianyk, T., Kolisnyk, T. (2021), "Potential application of hardware protected symmetric authentication microcircuits to ensure the security of internet of things". *Advanced Information Systems*. Vol. 5, No 3 P. 103–111. DOI: https://doi.org/10.20998/2522-9052.2021.3.14

11. Smith, J., Comiskey, B., (1996), "Modulation and information hiding in images", *Lecture Notes in Computer Science*. 1996. P. 207–226. DOI:10.1007/3-540-61996-8_42.

12. Klimushyn, P., Solianyk, T., Mozhaev, O., Nosov, V., Kolisnyk, T., Yanov, V. (2021), "Hardware support procedures for asymmetric authentication of the internet of things". *Innovative Technologies and Scientific Solutions for Industries*, No. 4 (18). P. 31–39. DOI: 10.30837/ITSSI.2021.18.031

13. Friedrich, J., Miroslav, G., Du., R. (2021), "Reliable Detection of LSB Steganography in Color and Grayscale Images". *Binghampton*, New York: SUNY. P. 27-30. DOI:10.1145/1232454.1232466

14. Fridrich, J., Du., R. and Long, M. (2000), "Steganalysis of LSB Encoding in Color Images", *ICME 2000*, New York City. DOI:10.1109/ICME.2000.871000

15. Brock, W., Dechert. W., Scheinkman, J. "A test for independence based on the correlation dimension", Working Paper, University of Wisconsin, 1987. available at: https://www.academia.edu/5825079/A_test_for_independence_based_on_the_correlation_dimension

16. Wu, H.C., Wu, N.I., Tsai, C.S., Hwang, M.S. (2005), "Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods". *IEEE Transactions on Image and Signal Processing.* № 5. P. 611615. DOI:10.1049/ip-vis:20059022

Received 05.09.2023

Відомості про авторів / About the Authors

Можаєв Олександр Олександрович – доктор технічних наук, професор, Харківський національний університет внутрішніх справ, професор кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: mozhaev1957@gmail.com; ORCID ID: https://orcid.org/0000-0002-1412-2696

Гнусов Юрій Валерійович – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, завідувач кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: duke6969@i.ua; ORCID ID: https://orcid.org/0000-0002-9017-9635

Манжай Олександр Володимирович – кандидат юридичних наук, професор, Харківський національний університет внутрішніх справ, завідувач кафедри протидії кіберзлочинності факультету № 4, Харків, Україна; e-mail: E-maisofist@ukr.net; ORCID ID: http://orcid.org/0000-0001-5435-5921

Струков Володимир Михайлович – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, професор кафедри кібербезпеки та DATA-технологій, Харків, Україна; e-mail: struk_vm@ukr.net; ORCID ID: https://orcid.org/0000-0003-4722-3159

Носов Віталій Вікторович – кандидат технічних наук, доцент, Харківський національний університет внутрішніх справ, професор кафедри протидії кіберзлочинності факультету № 4, Харків, Україна; e-mail: vitnos@ukr.net; ORCID ID: https://orcid.org/0000-0002-7848-6448

Сучасний стан наукових досліджень та технологій в промисловості. 2023. № 3 (25)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Радченко Валерій Вікторович – кандидат фіз.-мат. наук, доцент, Харківський національний університет внутрішніх справ, доцент кафедри кібербезпеки та DATA-технологій, Харківський національний університет внутрішніх справ, Харків, Україна; e-mail: valeryradchenko2007@gmail.com; ORCID ID: https://orcid.org/0000-0003-1420-4832

Єнгаличев Сергій Олександрович – Харківський національний економічний університет ім. С. Кузнеця, аспірант кафедри кібербезпеки та інформаційних технологій, Харків, Україна; e-mail: engalichev.sergiy@hneu.net; ORCID ID: https://orcid.org/0000-0001-5298-2251

Mozhaiev Oleksandr – Doctor of Sciences (Engineering), Professor, Kharkiv National University of Internal Affairs, Professor at the Department of Cyber Security and DATA-Technologies, Kharkiv, Ukraine.

Gnusov Yurii – PhD (Engineering Sciences), Associate Professor, Kharkiv National University of Internal Affairs, Head at the Department of Cyber Security and DATA-Technologies, Kharkiv, Ukraine.

Manzhai Oleksandr – PhD (Juridical Sciences), Professor, Kharkiv National University of Internal Affairs, Head at the Department of Combating Cybercrime, Kharkiv, Ukraine.

Strukov Volodymyr – PhD (Engineering Sciences), Associate Professor, Kharkiv National University of Internal Affairs, Professor at the Department of Cyber Security and DATA-Technologies, Kharkiv, Ukraine.

Nosov Vitalii – PhD (Engineering Sciences), Associate Professor, Kharkiv National University of Internal Affairs, Professor at the Department of Combating Cybercrime, Kharkiv, Ukraine.

Radchenko Valery – PhD (Physical and Mathematical Sciences), Associate Professor, Kharkiv National University of Internal Affairs, Associate Professor at the Department of Cyber Security and DATA-Technologies, Kharkiv, Ukraine.

Yenhalychev Serhii – Simon Kuznets Kharkiv National University of Economics, Graduate Student at the Department of Cybersecurity and Information Technologies, Kharkiv, Ukraine.

СТЕГАНОГРАФІЧНИЙ МЕТОД ЗАХИСТУ АКУСТИЧНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ КРИТИЧНОГО ЗАСТОСУВАННЯ

Предмет дослідження – процес захисту акустичної інформації в комп'ютерних системах критичного застосування для забезпечення необхідного рівня безпеки системи. **Метою** статті є вивчення методу захисту акустичної інформації в комп'ютерних системах критичного застосування за допомогою маскування для забезпечення неможливості несанкційного доступу до системи. У роботі окреслено такі **завдання**: проаналізувати програмно-технічне маскування мови; дослідити маскування мовних повідомлень з метою введення невпізнання; розглянути особливості стиснення мовних повідомлень; дослідити методи прихованої передачі акустичної інформації. Застосовано математичні **методи** перетворення інформації у комп'ютерних системах. **Результатом роботи** є потенційно можливі методи маскування мовних повідомлень для унеможливлення несанкційного доступу до системи. Аналіз функціювання запропонованих методів дав змогу сформувати конкретні **висновки**. Дослідження показали, що використання в стеганографічних цілях прямого розширення спектра дискретних сигналів допомагає здійснити приховане вбудовування інформаційних повідомлень у нерухомі зображення. Завдання добування повідомлення на приймальній стороні стеганосистеми еквівалентне завданню виявлення інформації із суміші корисного сигналу й перешкоди в широкосмуговій системі зв'язку. У процесі досліджень виявлені певні недоліки стеганографічних систем із розширенням спектра дискретних сигналів: імовірність правильного добування вбудованих даних залежить від величини доданих спотворень, яка залежить від забезпечуваної пропускної спроможності стеганоканалу. Подальші дослідження бажано провести за результатами аналізу можливого використання методів синтезу великих ансамблів квазіортогональних дискретних сигналів із поліпшеними ансамблевими, структурними й кореляційними властивостями для забезпечення вищих показників захищеності акустичних каналів у комп'ютерних системах критичного застосування.

Ключові слова: акустична інформація; технічний захист; криптографічний захист; стеганографічний (стеганофонічний) захист; модифікація; мови комп'ютерної системи.

Бібліографічні описи / Bibliographic descriptions

Можаєв О.О., Гнусов Ю.В., Манжай О.В., Струков В.М., Носов В.В., Радченко В.В., Єнгаличев С.О. Стеганографічний метод захисту акустичної інформації у системах критичного застосування. *Сучасний стан наукових досліджень та технологій в промисловості*. 2023. № 3 (25). С. 52–63. DOI: https://doi.org/10.30837/ITSSI.2023.25.052

Mozhaiev, O., Gnusov, Y., Manzhai, O., Strukov, V., Nosov, V., Radchenko, V., Yenhalychev, S. (2023), "Steganographic method of acoustic information protection in critical applications systems", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (25), P. 52–63. DOI: https://doi.org/10.30837/ITSSI.2023.25.052