Informatics and Control Problems 43 Issue 1 (2023)
journal homepage: www.icp.az

Study performance indicators covert channels of steganographic systems in telecommunication networks

B.G. Ibrahimov[1,2*], A.G. Hasanov[3], S.R. Ismaylova[1], K.M. Tahirova[3]

[1]*Azerbaijan Technical University, Baku, Azerbaijan*
[2]*Institute of Control Systems, Baku, Azerbaijan*
[3]*National Defense University, Baku, Azerbaijan*

ARTICLE INFO

Article history:
Received 15.12.2022
Received in revised form 26.12.2022
Accepted 10.01.2023
Available online 05.04.2023

Keywords:
Performance
Covert channel
Steganographic system
Packet length
Counteraction method
Bandwidth

ABSTRACT

Composite performance indicators of steganographic systems are investigated, on the basis which a new approach to the construction covert channel models in telecommunication communication networks is proposed. Analytical expressions are obtained for estimating the maximum value covert channel bandwidth when introducing a counteraction method and when changing packet lengths, which allow determining the performance characteristics of the steganographic data hiding system.

1. Introduction

The global proliferation and continuous improvement computer and telecommunications systems and communication networks is accompanied by an increase in their bandwidth, the integration multimedia services and applications using promising technologies for building distributed communication networks, as well as the increasing information security challenges.

Problems of shared ensuring confidentiality, availability and integrity transmitted information are solved by using cryptographic and steganographic methods of its protection. Cryptography is aimed at keeping secret the semantics transmitted messages, while steganography is aimed at keeping secret the very fact transmission such message. Unlike cryptography, which hides the contents of a secret message, steganography hides its very existence. Steganography is usually used together with methods cryptography, thus supplementing it [1, p. 202; 2].

Steganography is the art sending secret messages or invisible messages of a mixed type, transmitted over overt communication channels. Steganography (from Greek $\sigma\tau\varepsilon\gamma\alpha\nu\sigma\sigma$ - hidden and γραφω - writing, literally "secret writing") is a special science covert transmission packets by keeping secret the very fact transmission [3, p.6]. Steganography is also a science about the ways transmission and storage of secret data in various files, such as text, audio, video, and service network packets [2, 4].

It is worth noting that steganography system hides not only the fact sending some secret mes-

*Corresponding author.
E-mail addresses: i.bayram@mail.ru (B.G. Ibrahimov), arifhasan2828@yandex.ru (A.G. Hasanov), sevinc_ism@hotmail.com (S.R. Ismaylova), konul_tahirova@yahoo.com (K.M. Tahirova).

www.icp.az/2023/1-03.pdf https://doi.org/10.54381/icp.2023.1.03

sage from Alice to Bob, but Eva does not even know that Alice communicates with Bob. Therefore, the construction of covert channels with increased bandwidth and information security using methods, algorithms and tools steganographic systems is an extremely relevant problem in telecommunication communication networks and critical infrastructure systems.

In [4-7], methods, algorithms and prospects of development steganographic systems for hiding mixed type information in text documents, audio signals and video images are analyzed. In addition, in [6; 8; 9, p.24-26] the effectiveness of transmission secret data through covert channels based on ways to counter information leakage through covert network channels is investigated.

However, the problem studying the composite indicators steganographic communication system bandwidth with the necessary parameters in telecommunication communication networks has not been solved at a sufficient level to this day.

We consider the solution to the above problem: the study and analysis composite performance indicators steganographic systems in hiding data transmitted through communication channels.

2. Problem statement

It is known [3, p.13; 10, p.412] that steganography is a technology about methods transmission hidden messages, where the covert channel is organized on the basis of and inside the overt channel of communication, using of specifics of perception of the information.

Steganographic systems widely use various methods and algorithms to hide information in text documents, in speech messages and in moving images [3, p.94-95]. Steganographic algorithms have two transforms: the direct steganographic transform: $F\ M \to B \to K \to N$, and the reverse steganographic transform: $F^{-1}\ N \to K \to M$, matching respectively the triple (message, empty container, key) container – result, and the pair (filled container, key) source message. To build a model steganographic data hiding system, we introduce the following indicators covert channel [11, p.28-31]:

- Steganographic field of signal units SE – covert channel spaces in steganographic systems, taking into account methods embedding, detection and extraction [3, p.15-16]:

$$SE = [SB, B, M, K, N, F, F^{-1}] , \tag{1}$$

where the objects of the steganographic field SE are: $b-$ container, the carrier of information and container, is the unrestricted data used to hide messages, $b \in B-$ set of all containers; m – message, $m \in M$ – set of all messages; k – key, $k \in K$ – set of all keys (with public and secret keys); $n-$ filled or modified container, $n \in N-$ set of all filled containers ($b, n \in B$).

- The method and algorithm data embedding $F-$ a set instructions implemented on a steganographic container to embed messages and retrieve a modified container ($b, n \in B$):

$$F : B \times M \times K \to N ; \quad n = F[b, m, k] , \tag{2}$$

- Detection method $F^{-1}-$ a set of instructions implemented on a modified container to detect and extract messages:

$$F^{-1} : N \times K \to M , \quad m = F^{-1}[n, k] , \quad b, n \in B \tag{3}$$

- Hidden channel steganographic system $SB-$ frequency, temporal and spatial area multimedia data suitable for steganographic message transmission:

$$E :\ B \to SB , \quad SB \subset B , \tag{4}$$

Expressions (1),...,(4) describe the essence of the new approach to the construction of the steganographic data hiding system model and are the basic parameters steganographic processes when

hiding messages transmitted via communication channels.

Studies show [2; 3, p.18; 9, p.36-37; 10] that steganographic processes can be conditionally broken into 3 stages:

1. At the first stage, objects of the steganographic field $b \in B, m \in M, k \in K$ are selected and any information can be used as hidden data: text, audio file, image, $K = 3$;

2. The second stage is selection of the method embedding, F, and detection, F^{-1};

3. At the third stage the stegano-key is generated. A stegano-key is some restricted information, known only to a legitimate user, necessary to hide the message [1, p.208-209; 11].

Thus, we propose models for assessing the performance of a covert channel when using methods to counteract information leakage, based on limiting the bandwidth of the communication channel by changing the length of service L_i^{cn} and useful packets L_i^{nn}.

To formalize the problem, we propose a mathematical model that will most accurately reflect the steganographic processes occurring in the steganographic communication network under study when embedding and extracting hidden data, and will allow obtaining analytical expressions to calculate their speed performance.

3. Schematic operation of the investigated steganographic communication network model

On the basis of the system-technical analysis steganographic communication network characteristics, a schematic operation of the investigated link model consisting of transmitting and receiving steganographic systems shown in Fig. 1 is proposed. On the basis of this schematic the covert channel is constructed. It is known [8] that transmission secret messages in steganographic systems is carried out through covert channels. In 1973, the term "covert channel" was firstly introduced by Simmons [3, p.93; 8], who established that the problem of information leakage is not limited to software. A covert channel is a communication channel, which was not intended for the transmission of mixed type messages in telecommunications systems [2].

Fig.1. shows a structural and functional schematic of a steganography system for data hiding, where there are three subjects: transmitting (Alice), receiving (Bob) and interfering (Eva), as well as the source (SM) and the recipient of the message (RM).

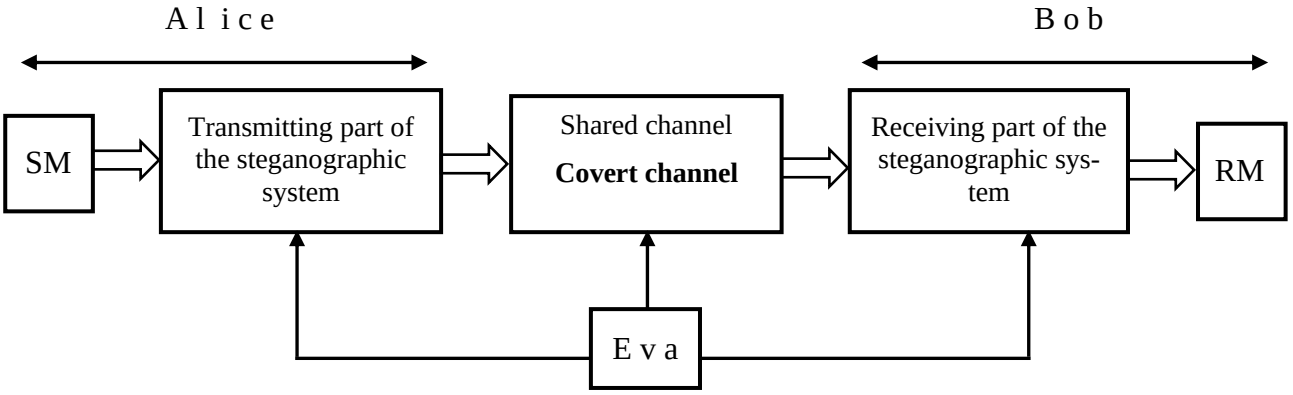

Fig.1. Structural and functional schematic diagram of the steganographic data hiding system

It follows from the schematic that a covert channel is a telecommunication channel that sends information in a different way and algorithm, which was not originally intended for it. Usually covert channels are divided into two groups according to transmission technique: covert channels by memory and by time. Here, the hidden data is called steganogram.

The conducted research shows [2; 3, p.94] that the efficiency steganographic systems with the intensity λ_i and packet length L_i, is characterized by the following functional dependence:

$$E_{эфф.}(\lambda_i, L_i) = W[Q_{cm.}(L_i), C_{ck}(\lambda_i, L_i), P_{об.}], \quad i = \overline{1,3}, \tag{5}$$

where $P_{об.}$ – probability detection of steganogram, transmitted packet with length $L_i = \psi(L_i^{nn}, L_i^{cn})$; $Q_{cm.}(L_i)$ – steganographic cost of a communication system with packet length L_i, which characterizes the degree carrier change after exposure to the steganographic method; $C_{ck}(\lambda_i, L_i)$ – bandwidth capacity of the covert channel, given the incoming flow rate λ_i when transmitting the i-th container traffic packet with message length L_i, $i = \overline{1, 3}$.

Expression (5) describes covert channel models in steganography system, based on changes in the lengths of service and useful packets, and takes into account their performance indicators.

4. Model description and performance analysis steganographic systems

Given the problem statement, a comprehensive approach is required in the study of the main characteristics of the covert channel communication systems with packet switching [12, p.120] using the protocol stack IP/MPLS (Internet Protocol/MultiProtocol Label Switching).

There is an important problem developing a mathematical model of steganographic system used for transmission of hidden messages. Te bandwidth of a covert channel is taken as the criterion efficiency of steganographic systems [2; 13-15].

The mathematical formulation of the problem proposed approach to building a steganographic systems efficiency model for estimating the covert channel bandwidth in the telecommunications system is described by the following objective functions:

$$E_{эфф.}(\lambda, L) = \mathrm{W}[Arg \max_i (C_{ck}(\lambda_i, L_i)], \qquad i = \overline{1, K} \tag{6}$$

with the following constraints

$$C_{окс}(\lambda_i, L_i) \geq C_{окс.доп.}(\lambda_i, L_i), \quad P_{обн.} \geq P_{обн.доп.}, \quad Q_{cm}(L_i) \leq Q_{cm.доп.}, \quad i = \overline{1, K}, \tag{7}$$

where $E_{эфф.}(\lambda_i, L_i)$ – functions that take into account the efficiency steganographic systems, taking into account the incoming flow rate λ_i when transmitting the flowof the *i*-th container traffic packet with the length L_i; $C_{окс}(\lambda_i, L_i)$ – total bandwidth of the communication channel with packet switching, taking into account the incoming flow rate λ_i when transmitting the flow of the *i*-th packet with the length L_i, $i = \overline{1, K}$.

Expressions (6) and (7) characterize the general essence of the new approach to building a mathematical model for assessing the efficiency steganographic system, taking into account the variation of packet lengths.

Among the investigated expressions (5), (6) and (7), the key indicator of steganographic systems efficiency is the covert channel bandwidth. The latter is determined by the volume of secret multimedia data that can be sent per unit time.

5. Study of the bandwidth capacity of the covert channel

One of the important indicators steganographic system is the maximum bandwidth capacity (MBC) of the covert channel, which is estimated with the help of informative characteristics as follows:

$$C_{ck}(\lambda_i, L_i) = \max_{p(u)} \{\frac{I_c(V,U)}{E[T_{nn}] + E[t]}\}, \text{ packet/s}, \qquad i = \overline{1, K}, \tag{8}$$

where $E[T_{nn}]-$ the average packet transmission time; $p(u)-$ the set of possible distributions probabilities hiding data transmitted through the communication channel; $E[t]-$ the average time required to move a packet in the communication channel; $I_c(V,U)-$ the mutual information random variables V,U .

Expression (8) determines the bandwidth of the covert channel with errors $H_c(U/V)\neq 0$, using informative and time characteristics of the steganographic system [10, p.151-152]. Besides, formula (8) is the threshold characteristic of the covert channel and can be expressed as

$$C_{ck}(\lambda_i,L_i)=\max_i[V_{ck}(\lambda_i,L_i)]=\lim_{n\to\infty}[H_{\max}/T_{nn}]=[V_{ck}(\lambda_i,L_i)/H_k]\cdot \log_2 m_k, \quad (9)$$

where H_k- encoder entropy, bits/packet.

It follows from (9) that the bandwidth of the covert channel is completely determined by the transmission speed $V_{ck}(\lambda_i,L_i)$ of the packet and the basis of the code used m_k .

The following formula [10, p. 150] is used to estimate the mutual information random variables V,U :

$$I_c(V,U)=H_c(V)-H_c(V/U)=H_c(U)-H_c(U/V), \quad (10)$$

Formula (10) describes informative input and output parameters of the covert channel.

To study of the MBC of a covert channel it is necessary to take into account the problem information leakage through covert network channels, which are characterized by a large scale due to the fact that the IP protocol stack is widely used in steganographic systems.

In this work, we use the highly efficient IP/MPLS protocol stack, which has many features that allow it to be used for covert transmission restricted-access data. Among the ways to counter information leakage over covert network channels, it is common to distinguish detection, elimination, and bandwidth limitation [13, 16-20]. The latter make it possible to manage the bandwidth the covert channel and control the residual bandwidth of the channel [7; 8; 14-16].

6. Evaluating the temporal characteristics steganographic systems

Suppose that we use a way to counteract information leakage through covert channels by changing the length of each packet transmitted through communication channels. Then the length transmitted packets increases by the number bits per packet, having uniform distribution on the set $N_d\bigcup\{0\}$, where *d* is the parameter counteraction method. To transmit the symbol "θ ", Alice sends via covert channels packets of length

$$L(\theta)=L_{cky}+\theta(d+1),\ N_{L_{yy}-1}\bigcup\{0\}, \quad (11)$$

where $L_{cky}-$ sum of header lengths network and channel levels of the model interaction of open systems $L_{cky}=L_{cy}+L_{ky}$ when using the IP/MPLS protocol stack; $L_{yy}-$ indicators of the covert channel, taking into account protocol units and the length of the service link packet with which the set of instructions F implemented for steganographic container ($b,n\in B$) by formula (2) for embedding secret messages.

The header length parameter L_{cky} identified in the IP/MPLS protocol stack for IPv4 is 34 bytes and $L_{yy}=140$ when using the Ethernet data link layer technology, and for IPv6 header length is $L_{cky}\geq 54$ bytes and $L_{yy}=204$ [12, p.224-227; 17; 18].

Given the specifics of the IP/MPLS protocol and the way to counter information leakage through covert channels, which is bandwidth limitation, the average packet transmission time is de-

termined by the expression:

$$E[T_{nn}] = \frac{L_{ckó}}{C_{okc}(\lambda_i, L_i)} + \frac{L_{óó}(d+1)-1}{2C_{okc}(\lambda_i, L_i)}, \quad (12)$$

From (12) we can see that $E[T_{nn}]$ significantly depends mainly on the parameter of the hidden L_{yy} channel and the bandwidth of the shared communication channel $C_{okc}(\lambda_i, L_i)$.

In this method of construction of the covert channel with the introduction of the proposed counteraction [13, 14; 19; 20], the parameter L_{yy} of the channel taking into account the mutual information of random variables is:

$$I(X,Y) = \ell og_2 L_{yy}, \;\; P_{ou}^{c\kappa} \to 0 \;, \; H(Y/X) = 0 \quad (13)$$

It follows from (13) that the covert channel parameter is determined using the counteraction method, the error probability $P_{ou}^{c\kappa}$ and the index mutual information of the random variables X, Y .

7. Study and evaluation performance efficiency of the steganographic system

Given the network and link layer header length function of the open systems interaction model L_{cky} and the parameter d , as well as the Lambert function [4, 5, 6], the covert channel parameter is determined as follows:

$$L_{yy} = (2L_{cky} - 1)/[(d+1) \cdot W(2L_{cky} - 1)/e \cdot (d+1)], \quad (14)$$

where $W(\cdot)-$ Lambert function [5], determined as the inverse function to $f(w) = we^w$, for complex w . In addition, the Lambert function for any complex z is determined by the functional equation $z = W(z)e^{W(z)}$.

In steganographic systems, the main characteristic is the MBC of the covert channel, which is determined as follows:

$$C_{\max.ck}(\lambda, L) = \frac{2\ell og_2 L_{yy}(d+1)}{N_{ck} \cdot [2L_{cky} + L_{yy}(d+1) - 1]} \cdot \frac{\lambda \cdot E[L_n]}{\rho_{ck}}, \quad (15)$$

where $N_{ck}-$ number of covert channels organized in steganography system; $E[L_{ck}]-$ average length of packets transmitted via covert channels; $\rho_{ck}-$ coefficient effective use of covert channel.

Expression (15) determines the maximum bandwidth capacity of the covert channel depending on the performance efficiency of steganographic systems.

8. Numerical results and interpretation

On the basis of the model, a numerical evaluation was made by modeling performance indicators of covert channels of steganographic systems using the Communications Toolbox package, an extension of the standard Matlab environment, R 2019b (9.7; 64 bit), designed for the calculation and modeling communication systems when using the IP/MPLS protocol stack. Based on the numerical values, a graphical dependence of the MBC of the covert channel on the total bandwidth of the packet-switched communication system with a given steganographic system performance indicator is plotted in Fig.2.

Analysis of graphical dependence $C_{\max ck}(\lambda, L) = W[\rho, C_{okc}(\lambda, L), L_{cky}, d]$ shows that an increase of the total bandwidth of communication channel $C_{okc}(\lambda, L)$ leads to an increase in the MBC

of the covert channel $C_{\max ck}(\lambda, L) \geq 15,...,100$ Kbps, meeting the requirements stability of network steganography for data hiding and construction high-speed steganographic communication systems using packet switching. Its noticeable change starts from values $C_{okc}(\lambda, L) \geq 4096$ Kbps with a given speed communication channel open systems and service parameters of packets hidden data. In this case, the MBC of the covert channel is $C_{\max .ck}(\lambda, L) \leq 45$ Kbps at $V_{ck}(\lambda, L) = 32$ Kbps.

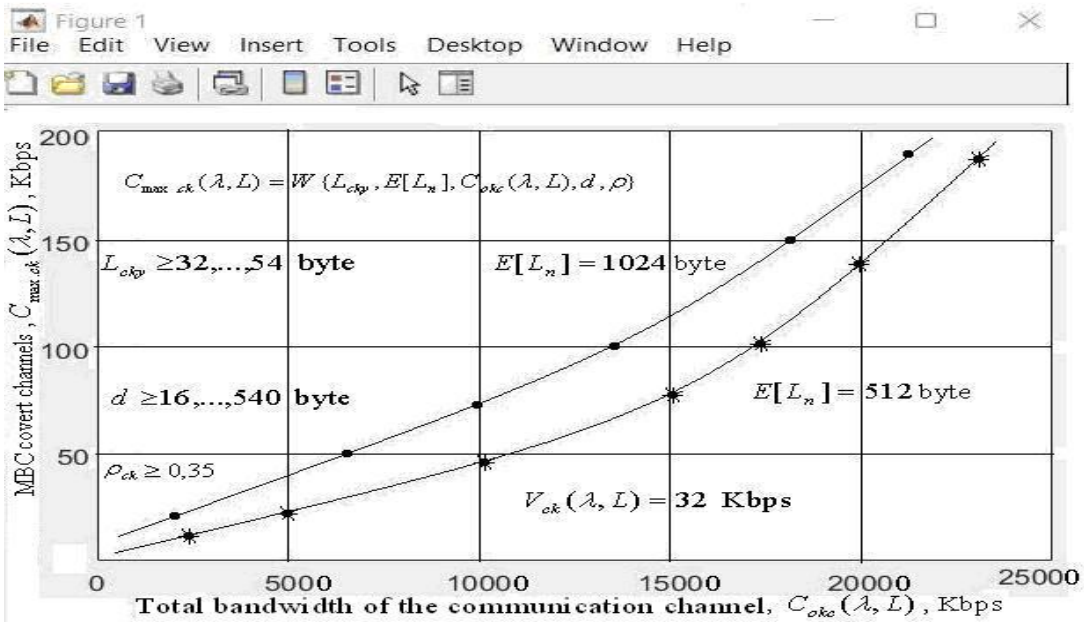

Fig.2. Graphical dependence of the maximum bandwidth capacity of a covert channel on the total bandwidth of the packet-switched communication system

Thus, the results of the study show that the MBC of the covert channel depends significantly on the parameter of the counteraction method, informative characteristics of the system and the parameter packet lengths of the network and link layers of the model.

9. Conclusion

As a result of the study efficiency of steganography systems in telecommunication networks, a new approach to the construction of a mathematical model of the covert channel bandwidth, taking into account the indicators both the input and output characteristics of the covert channel, the length of the service packet, steganographic processes for message embedding, and counteraction the method is proposed.

Based on the study of the model, which is based on information theory, analytical expressions are obtained for the evaluation composite performance indicators of steganographic systems in hiding data transmitted through communication channels.

References

[1] Б.Я. Рябко, А.Н. Фионов, Основы современной криптографии и стеганогрфии, 2-е изд, Москва, Горячая линия, Телеком, (2020), 232 p. [In Russian: B.Y. Ryabko, A.N. Fionov, Fundamentals of modern cryptography and steganography, 2nd edition, Moscow, Goryachyaya Liniya, Telecom].

[2] Б.Г. Ибрагимов, К.М. Тахирова, Исследования и анализ методов скрытия информации в пространственно-временной области с использованием стеганографических технологий, Проблемы инфокоммуникаций. No.2 (2022) pp.32-27. [In Russian: B.G. Ibrahimov, K.M. Tahirova, Research and analysis of methods of hiding information in the space-time domain using steganographic technologies, Problemi Infokommunikatsiy].

[3] О.И. Шелухин, С.Д. Канаев, Стеганография, Алгоритмы и программная реализация, Москва, Горячая линия, Телеком, (2018), 592 p. [In Russian: O.I. Shelukhin, S.D. Kanayev, Steganography, algorithms and software implementation, Moscow, Goryachyaya Liniya, Telecom].
[4] А.И. Белозубова, К.Г. Когос, Ф.В. Лебедев, Ограничение пропускной способности сетевых скрытых каналов по времени путем введения дополнительных случайных задержек перед отправкой пакета, Безопасность информационных технологий. 28 No.4 (2021) pp.74-89. [In Russian: A.I. Belozubova, K.G. Kogos, F.V. Lebedev, Time-based bandwidth limitation of network covert channels by introducing additional random delays before packet sending, Bezopasnost Informatsionnih Tehnologiy].
[5] B.W. Lampson, A Note on the confinement problem, Communications of the ACM. 16 No.10 (1973) pp.613-615.
[6] А.А. Грушо, Скрытые каналы и безопасность информации в компьютерных системах, Дискретная математика. 10 No.1 (1998) pp.3-9. [In Russian: A.A. Grusho, Covert channels and information security in computer systems, Diskretnaya Matematika].
[7] А.В. Епишкина, К.Г. Когос, Об оценке пропускной способности скрытых информационных каналов, основанных на изменении длин передаваемых пакетов, Информация и космос. No.4 (2015) pp.78-82. [In Russian: A.V. Epishkina, K.G. Kogos, On the estimation of the bandwidth of covert information channels based on changes in the lengths of transmitted packets, Informatsiya i Kosmos].
[8] G.J. Simmons, The prisoners' problem and the subliminal channel. In Chaum, D., ed., Crypto '83, Advances in Cryptography, Plenum Press. (1983) pp.51-67.
[9] В.С. Садов, Компьютерная стеганография, Минск, БГУ, (2010) 232 p. [In Russian: V. S. Sadov, Computer steganography, Minsk, Belarusian State University].
[10] Теория электрической связи, К.К. Васильев, В.А. Глушков, А.В. Дормидонтов, А.Г. Нестеренко; под общ. ред. К.К. Васильева, Ульяновск, УлГТУ, (2008) 452 p. [In Russian: Electrical communication theory, K.K. Vasilyev, V.A. Glushkov, A.V. Dormidontov, A.G. Nesterenko; eds. by K.K. Vasilyev, Ulyanovsk, Ulyanovsk State Technical University].
[11] Г.Ф. Конахович, А.Ю. Пузыренко, Компьютерная стеганография, Теория и практика, МК-Пресс, (2006) 288 p. [In Russian: G.F. Konakhovich, A.Yu. Puzyrenko, Computer steganography, theory and practice, MK-Press].
[12] А.Б. Гольдштейн , Б. С. Гольдштейн, Технология и протоколы MPLS, Санкт-Петербург, БХВ-Санкт-Петербург, (2014), 304 p. [In Russian: A.B. Goldstein , B. C. Goldstein, MPLS technology and protocols, St. Petersburg, BHV-St. Petersburg].
[13] Б.Г. Ибрагимов, К.М. Тахирова, Исследование эффективности стеганографических систем при встраивании или извлечении скрытых данных, Вестник компьютерных и информационных технологий. 19 No.11 (2022) pp.43-49. [In Russian: B.G. Ibrahimov, K.M. Takhirova, Study of efficiency of steganographic systems when embedding or extracting hidden data, Vestnik Komputernih i Informatsionnih Tekhnologiy].
[14] A. Ker, Steganalysis of LSB Matching in Grayscale Images, Signal Processing Letters.12 (2005) pp.441-444.
[15] M.T. Mustafa, B.A. Abdrahim, S.H. Rana, S.M. Siti, A literature review of various steganography metods, Journal of theoretical and applied information technology. 100 No.5 (2022) pp.1412-1427.
[16] Dhawan, Sachin, and Rashmi Gupta, Analysis of various data security techniques of steganography: A survey, Information security journal: A global perspective. 30 No.2 (2021) pp.63-87.
[17] Lei Tim, Jeremy Straub and Benjamin Bernard, Lightweight network steganography for distributed electronic warfare system communications, Advances in security, networks, and Internet of things, Springer, Cham. (2021) pp.437-447.
[18] Mondal, Bhaskar. A secure steganographic scheme based on chaotic map and DNA computing, MicroElectronics and telecommunication engineering, Springer, Singapore. (2020) pp.545-554.
[19] B.G. Ibrahimov, A.D. Tagiyev, Research of the performance multiservice telecommunication networks based on the architectural concept NGN and FN, Lecture notes in mechanical engineering, Engineering and photonic technologies, Vienna, Austria, Springer Nature Switzerland AG. (2023) pp.333-341.
[20] Wu, Zhijun, et al., Steganography and steganalysis in voice over IP: A Review, Sensors. 21 No.4 (2021) pp.10-32.