Information Encryption Method based on a Combination of Steganographic and Cryptographic Algorithm's Features

Vasyl Trysnyuk[1], Kirill Smetanin[2], Ihor Humeniuk[2], Oleksii Samchyshyn[2], and Taras Trysnyuk[1]

[1] *Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Chokolovskiy ave., 13, Kyiv, 02000*
[2] *Korolov Zhytomyr Military Institute, 22 Miru ave., Zhytomyr, 10004, Ukraine*

Abstract

At the present stage of development of science and technology, information security is becoming one of the most urgent tasks due to the extremely widespread use of automated information processing systems and the expansion of local and global computer networks, which transmit huge amounts of public, military, commercial, private information. character. An important task is the widespread introduction of information technology in various areas of human activity in Ukraine: the rapid growth of plastic cards, the introduction of electronic passports and medical cards, student tickets and record books. More and more public institutions and private enterprises are moving to electronic document management, which requires the legal validity of the signature of a natural or legal person. The protection of information has also become relevant with the armed aggression of the Russian Federation, which has recently significantly increased the number of cyberattacks, including attempts to intercept and steal confidential information. Therefore, there is a need to take additional measures to prevent attempts to intercept confidential information transmitted over insecure communication channels, such as the Internet. Information security in computer information and telecommunication systems is a priority. One of the most reliable methods of information protection is encryption. Cryptographic data transformations are the most effective way for a system to maintain the confidentiality of information when it is entered, output, transmitted, processed and stored, and to resist its destruction, theft or distortion. But the most effective way to ensure the confidentiality of information is the combined use of steganographic and cryptographic means. In order to ensure high stability of encrypted information when transmitting it through the network of information and telecommunications systems and reduce the threat of unauthorized access to it or attack on the cipher, it is proposed to change the approach to solving the problem of data encryption. A method of encrypting / decrypting digital text information based on the pixel alphabet of a monochrome image, which is based on hiding or distorting graphic data, is proposed. This approach allows you to ensure high stability of encrypted information and significantly reduce the risk of unauthorized access to confidential information or attack on the cipher by encrypting each character with a dynamic random number from the range of values of the corresponding character and hiding the encrypted text in the position of graphic data. only to sender and recipient

Keywords

Encryption, decryption, unauthorized access, cryptocurrency, information and telecommunication system, pixel alphabet, informational and cybersecurity.

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: trysnyuk@ukr.net (V. Trysnyuk); kiry221982@gmail.com (K. Smetanin); ig_hum@ukr.net (I. Humeniuk); samyj123@ukr.net (O. Samchyshyn); tryskTar@ukr.net (T. Trysnyuk)
ORCID: 0000-0001-9920-4879 (V. Trysnyuk); 0000-0002-6062-550X (K. Smetanin); 0000-0001-5853-3238 (I. Humeniuk); 0000-0002-1542-1065 (O. Samchyshyn); 0000-0002-3672-8242 (T. Trysnyuk)

1. Introduction

Formulation of the problem. The problem of protection of information resources is becoming increasingly important. This is due to the intensive scientific and technical development and, as a consequence, the development of information technology, which poses a threat to informational and cybersecurity of information transmitted, processed and stored in modern informational and telecommunications systems (ITS). At present, to ensure the appropriate level of informational and cybersecurity, various encryption and identification methods are used, which allow to reliably and effectively protect information from unauthorized access to it, violation of its integrity and leakage [1].

Issues of development and implementation of cryptographic methods of information security are relevant for all branches of science, given the high automation of various areas of human activity. The development of high-performance methods of encrypting (decrypting) data with high cryptographic stability is an important component in addressing informational and cybersecurity. The main task of the mathematical apparatus in cryptography is to ensure the cryptographic stability of developed and developed encryption algorithms, that's the ability to resist practical hacking. Cryptographic stability of cryptographic information protection methods is a property of cryptographic algorithms and cryptographic protocols, which characterizes their ability to resist decryption methods (the process of unauthorized restoration of the original message text) [2].

However, despite the large number of existing encryption algorithms, there are unauthorized access to information that lead to its leakage and violation of the basic criteria of the model that regulates its information security policy [3]. Thus, there is a need to develop a new crypto-resistant method of encryption to ensure the basic properties of information, which will combine the features of steganographic and cryptographic tools.

Analysis of recent research and publications. To date, a number of methods of protection against unauthorized access have been developed and implemented, but cryptographic methods occupy a special place among them. For example, [4] systematically outlines the problems of reliability and cryptographic stability of the steganographic system for different types of attacks, as well as assessing the bandwidth of the hidden data exchange channel, provides results of theoretical and practical studies of information concealment in case of active resistance; in [5] the basic concepts and definitions of information protection, security policy formation, criteria for assessing the security of computer systems, the basics of cryptographic information protection, information protection from unauthorized access in modern operating systems, and describes complex security systems in corporate information systems; in [6] the results of scientific researches on development of methods of increase of efficiency of components of safety of computer systems with use of masking elements of the text and biometric data based on application of cryptographic and identification systems of protection are presented; in [7] the results of researches of informational security in networks are resulted, methods of protection against hidden connection to information networks are offered, the approach to formation of schemes of blind signature is offered, kleptographic attacks are investigated and means of protection against them are offered, the algorithm of denied encryption is modified. on the CUDA platform; in [8] the solution of a scientific and technical problem of increase of efficiency of functioning of systems of computer cryptography by creation of methodology of synthesis of operations of transformation of the information and construction of cryptographic primitives on their basis is resulted; in [9] the results of the analysis of characteristic features of the method of increasing cryptographic stability of encryption algorithms by preliminary modification of input data with the method of optimal entropy non-uniform coding on the example of shift ciphers are presented. that can be used for mathematical modeling of procedures for algorithmic implementation of the combined method of encryption by the specified method; in [10] proposed a method of steganography of the image space,

An analysis of recent research and publications has shown that the most popular methods in computer steganography are those used as an image container. The closest method, which is considered as an analogue of the method developed by the authors, is a method of encrypting and decrypting digital data transmitted or stored using the method of transmitting priority pixels [11], which encrypts and decrypts digital data transmitted or stored using the preferred method of transmission pixels of information content to be encrypted or decrypted. Each pixel group contains a position value that is

used as a priority value, which is assigned at least one key by which the value of the pixel position or group of pixels on request are encrypted or decrypted.

The purpose of the article. The aim of the article is to ensure high cryptographic stability of encrypted information when transmitting it through the channels of the ITS network and reduce the level of threat of unauthorized access to it or attack on the cipher is proposed. To do this, it is necessary to develop a method of encrypting digital textual information, which is based on a combination of features of steganographic and cryptographic means, in particular on the concealment or deformation of graphic data.

2. Theoretical Fundamentals of Research

Terms used in the proposed Method. Message – the original text message. Length – the number of characters in the message. Normative alphabet – symbols Message (letters of the Ukrainian alphabet, numbers 0–9, special and punctuation characters), which is encrypted and transmitted through the network of the information and telecommunications system. Encryption alphabet – static ranges of brightness values of pixels of a monochrome image (0–255), which are assigned to each character of the Normative alphabet. Encryption – the process of replacing the Normative Alphabet Message in the elements of the Alphabet Encryption. Ciphertext is the result of encryption. Key – positions with a certain interval of placement of pixels on graphic data with brightness, corresponding to the Encryption Alphabet. Stegomessage is the result of hiding the Ciphertext. Sender – a user who encrypts a message and transmits ciphertext.

General Idea of the proposed Method. The problem is solved by the fact that in the method of data encryption / decryption based on the pixel alphabet of the monochrome image, which determines the key, assign to each element of the Normative alphabet a static range of brightness values of the pixels of the monochrome image. The Encryption Alphabet is formed, the Message is encrypted using the Encryption Alphabet, and the Ciphertext is hidden in the digital image by distorting it, in particular encoding the brightness values of the pixels corresponding to the Encryption Alphabet at the position with the defined Key. After sending the Recipient and receiving the Stegomessage, the Stegomessage is decrypted into a Message using the Encryption Alphabet according to the specified Key.

This approach allows to ensure high stability of encrypted information and significantly reduce the level of threat of unauthorized access to the Message or attack on the cipher by encrypting each character of the Message with a dynamic random number from the range of values of the corresponding character. A significant reduction in the level of unauthorized access threat to the Message or attack on the cipher is achieved by hiding the Ciphertext in the position of the graphic data, taking into account the Key, which is known to the Sender and the Recipient.

Algorithm of the proposed Method. Encryption / decryption of data based on the pixel alphabet of a monochrome image is performed in several stages:

1) Formation of the Encryption Alphabet, according to which each character of the Normative Alphabet is assigned a static range of values of the brightness of the pixels of the monochrome image (0–255) for:

- letters of the Ukrainian alphabet;
- letters of the English alphabet;
- digits 0–9;
- special characters.

2) Conversion of the Normative Alphabet of the Message into Ciphertext.

3) Formation of the Key (determination of the initial position of the first element of the Ciphertext and the interval of the following).

4) Formation of Stegomessage (hiding of the Ciphertext or deformation of graphic data by values of the Encryption Alphabet in the positions defined by the Key).

5) Transmission (reception) of Stegomessage.

6) Decryption of Stegomessage (determination of values of brightness of pixels in the positions set by the Key, their transformation into the Normative alphabet and formation of the Message).

The general scheme of operation of the proposed method is given in Fig. 1.

Consider in detail each of the stages.

The stage of formation of the Encryption Alphabet. For the set of all available characters used in the Message, static ranges of values within $[000; 255]$, namely:

- letters of the Ukrainian alphabet (Table 1): $B_1 = \{b_{"а"}, b_{"б"}, .., b_{"я"}\}, B_1 \in [000; 095]$;

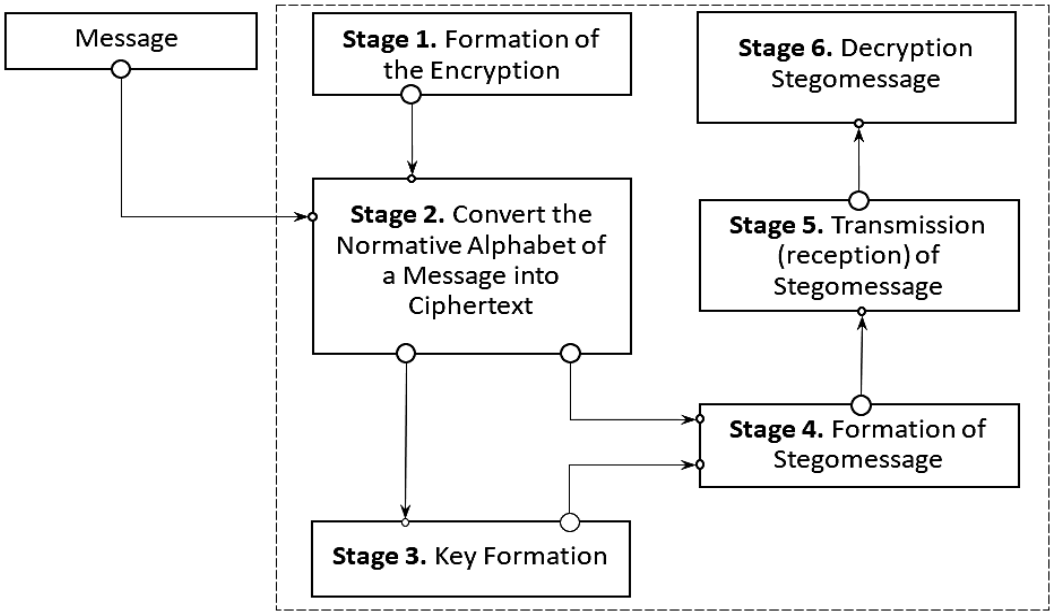

Figure 1. Scheme of encryption / decryption of data based on the pixel alphabet

Table 1

Alphabet of encryption of letters of the Ukrainian alphabet

Normative alphabet	Encryption alphabet	Normative alphabet	Encryption alphabet	Normative alphabet	Encryption alphabet	Normative alphabet	Encryption alphabet
А (а)	000–002	З (з)	024–026	Н (н)	048–050	Х (х)	072–074
Б (б)	003–005	И (и)	027–029	О (о)	051–053	Ц (ц)	075–077
В (в)	006–008	І (і)	030–032	П (п)	054–056	Ч (ч)	078–080
Г (г)	009–011	Ї (ї)	033–035	Р (р)	057–059	Ш (ш)	081–083
Д (д)	012–014	Й (й)	036–038	С (с)	060–062	Щ (щ)	084–086
Е (е)	015–017	К (к)	039–041	Т (т)	063–065	Ь (ь)	087–089
Є (є)	018–020	Л (л)	042–044	У (у)	066–068	Ю (ю)	090–092
Ж (ж)	021–023	М (м)	045–047	Ф (ф)	069–071	Я (я)	093–095

- letters of the English alphabet (Table 1): $B_1 = \{b_{"a"}, b_{"b"}, .., b_{"z"}\}, B_1 \in [096; 173]$;

Table 2

Alphabet encryption of letters of the English alphabet

Normative alphabet	Encryption alphabet	Normative alphabet	Encryption alphabet	Normative alphabet	Encryption alphabet
A (a)	096–098	I (i)	120–122	R (r)	147–149
B (b)	099–101	J (j)	123–125	S (s)	150–152
C (c)	102–104	K (k)	126–128	T (t)	153–155
D (d)	105–107	L (l)	129–131	U (u)	156–158
E (e)	108–110	M (m)	132–134	V (v)	159–161
F (f)	111–113	N (n)	135–137	W (w)	162–164

G (g)	114–116	O (o)	138–140	X (x)	165–167
H (h)	117–119	P (p)	141–143	Y (y)	168–170
		Q (q)	144–146	Z (z)	171–173

- numbers (Table 3): $B_3 = \{b_{"0"}, b_{"1"}, .., b_{"9"}\}$, $B_3 \in [174; 203]$;

Table 3

Number encryption alphabet

Normative alphabet	Encryption alphabet
0	174–176
1	177–179
2	180–182
3	183–185
4	186–188
5	189–191
6	192–194
7	195–197
8	198–200
9	201–203

- special characters (Table 4): $B_4 = \{b_{"?"}, b_{"!"}, .., b_{"пробіл"}\}$, $B_4 \in [204; 255]$.

Table 4

Alphabet of special characters

Normative alphabet	Encryption alphabet	Normative alphabet	Encryption alphabet
?	204–206	;	231–233
!	207–209	'	234–236
.	210–212	\	237–239
,	213–215	_	240–242
%	216–218	<	243–245
=	219–221	>	246–248
+	222–224	(	249–251
/	225–227	)	252–254
:	228–230	space	255

The peculiarity of the formation of the Encryption Alphabet is its representation in triad (three-digit) form, and each of its elements corresponds to the brightness of the pixel of the monochrome image, which will be hidden in (or distorted) graphic data, including RGB image model (12).

Stage of transformation of the Normative Alphabet of the Message into Ciphertext. For each separate Normative alphabet:

$$M = \{m_1, m_2, .., m_i\}; i = \overline{1, n},$$

where n – Length The message is replaced by a random value from the specified range of the Encryption Alphabet. Example $b_{"a"} = [000; 002]$ (The letter "A" of the Ukrainian alphabet can be replaced by the numbers: 000, 001 and 002), resulting in the formation of ciphertext:

$$G = \{rand(b_m)_i\},$$

where $rand$ – random number generation function.

The stage of formation of the Key. For Ciphertext the value of the initial position of its first element is chosen $k_1(x, y)$, which corresponds to the location of the first pixel of the monochrome image, and subsequent, taking into account certain intervals (horizontal – Δx, vertical – Δy). As a result, the Encryption Key is formed, the dimension of which must be not less than the Length of the Message:

$$K = \{k_i(x, y)\}; 1 \le x \le (w - 1), 1 \le y \le (h - 1),$$

where w – width, h – image height.

Formation of Stegomessage. Pixels with luminances that correspond to the values of the generated Ciphertext are placed in position (x_i, y_i) defined by the Key $K = \{k_i(x, y)\}$. Thus, the ciphertext is hidden in the graphic data or the raster image of the RGB model is distorted.

The result of this step is a Stegomessage of the form – $S = \{G, K\}$.

Stage of transmission (reception) of Stegomessage. Sending by the Sender and receiving by the Recipient of the Stegomessage is carried out using the existing network protocols of data transmission. At this stage, the availability of the Sender and the Recipient to the network is determined, the routing table is formed, the routes with the minimum connection cost are determined, along which the Stegomessage is transmitted directly.

Stage decryption stage. According to the received Stegomessage $S = \{G, K\}$ Recipient using the known Key $K = \{k_i(x, y)\}$ transmitted separately by alternative communication channels determines the positions of the pixels (x_i, y_i), evaluates the value of their brightness, forms the Ciphertext – $G = \{(b_m)_i\}$, according to a pre-known Alphabet, encryption sequentially transforms it into the Normative Alphabet and Message:

$$M = \{(b_{m_1} \to m_1), (b_{m_2} \to m_2), .., (b_{m_i} \to m_i)\}.$$

3. Research Results

The essence of the method of encrypting / decrypting data based on the pixel alphabet of a monochrome image is explained by illustration (see Figs. 2, 3), showing one of the possible options for encrypting the Message (see Fig. 2) and decrypting the Ciphertext (see Fig. 3).

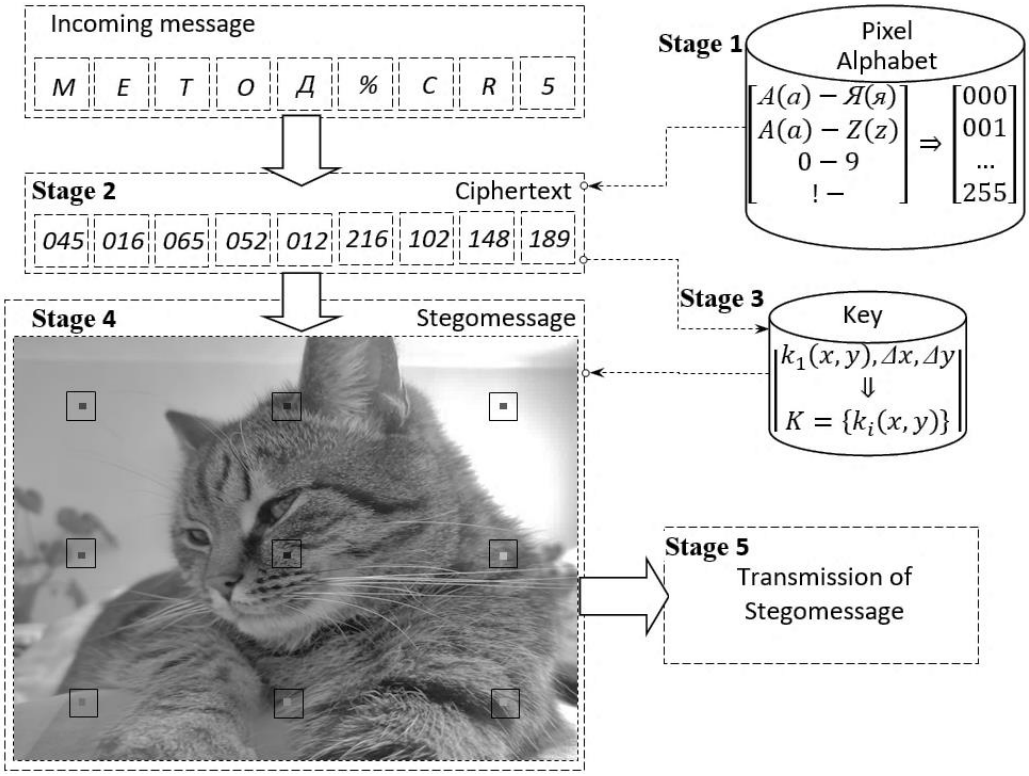

Figure 2. Message encryption

Thus, in this method is the encryption and decryption of digital data according to the following algorithm: determine the Key; assign to each element of the Normative alphabet a static range of values of brightness of pixels of the monochrome image; form the Encryption Alphabet; perform encryption of the Message using the Encryption Alphabet; form Stegomessages by setting the brightness value of the pixels corresponding to the Encryption Alphabet, at positions with a certain Key hide the Ciphertext in the digital image. For clarity, the pixel sizes of Stegomessages are presented in 10 times larger size while preserving the scale of the original image.

Thus, in this method is the encryption and decryption of digital data according to the following algorithm: determine the Key; assign to each element of the Normative alphabet a static range of values of brightness of pixels of the monochrome image; form the Encryption Alphabet; perform encryption of the Message using the Encryption Alphabet; form Stegomessages by setting the brightness value of the pixels corresponding to the Encryption Alphabet, at positions with a certain Key hide the Ciphertext in the digital image. For clarity, the pixel sizes of Stegomessages are presented in 10 times larger size while preserving the scale of the original image.

After transmission to the Recipient and receipt of the Stegomessage, the Stegomessage is decrypted into the Message using the Encryption Alphabet according to the specified Key.

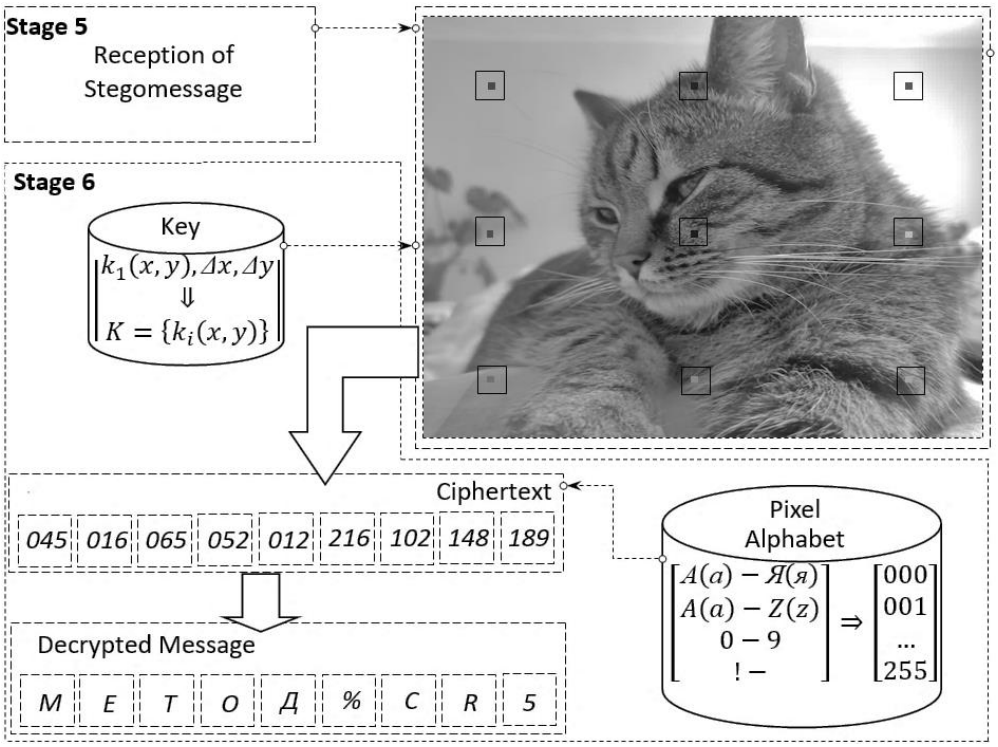

Figure 3. Decryption of Ciphertext

Evaluation of cryptographic stability of the proposed method by encryption is a multi-criteria task. During the solution of this problem there are problems with the choice of criteria that allow to build an adequate target function for the assessment of cryptographic stability. The problem with constructing an objective function is that the criteria that characterize the parameters and characteristics of the encryption process have their limitations. This means that when one of the criteria reaches its maximum value, the other criteria also increase sharply.

There are methods for solving a multicriteria problem [13], which reduce it to a problem with a single solution, which allows you to assess the cryptographic stability of the method by encryption. To do this, we use the objective function, which is a scalar convolution of partial criteria:

$$K_s^*(M) = f[I(M), P_s(S), \Theta(M)]$$

with the value of the entropy of the Message $I(M)$, the probability of a successful attack on the Stegomessage $P_s(S)$ and the computational complexity of the method itself $\Theta(M)$.

In the general case, the encryption method that is proposed must meet the following requirements:

$$\begin{cases} I(M) \to max, \\ P_s(S) \to min, \text{ if } (w,h) \to max, n \to min. \\ \Theta(M) \to min, \end{cases}$$

that's provides the maximum value of the entropy of the incoming message; has a low probability Successful attack on Stegomessages with maximum image resolution and minimum Length; has low computing power.

When finding the objective function, there is a problem of reduction to one method of extremization. Therefore, to ensure the finding of the optimal compromise between the partial criteria, a nonlinear scheme of compromises is used, which combines the conflicting nature of the quality criteria [14]:

$$K_s^*(M) = argmin\left\{\frac{1}{I(M)} + \frac{1}{1-P_S(S)} + \frac{1}{1-\Theta(M)}\right\}.$$

In the multi-criteria evaluation of alternatives there is a need to obtain not only analytical but also qualitative assessment. To do this, it is necessary to normalize the value of the scalar convolution and

compare the obtained value with the gradations of the interval normalized scale [15]. The formula of the normalized minimized scalar convolution has the form:

$$K_s(M) = 1 - (K_s{}^*(M,S)^{-1}).$$

In Fig. 4 shows the results of evaluating the cryptographic stability of the proposed method by encryption compared to a known analogue [11].

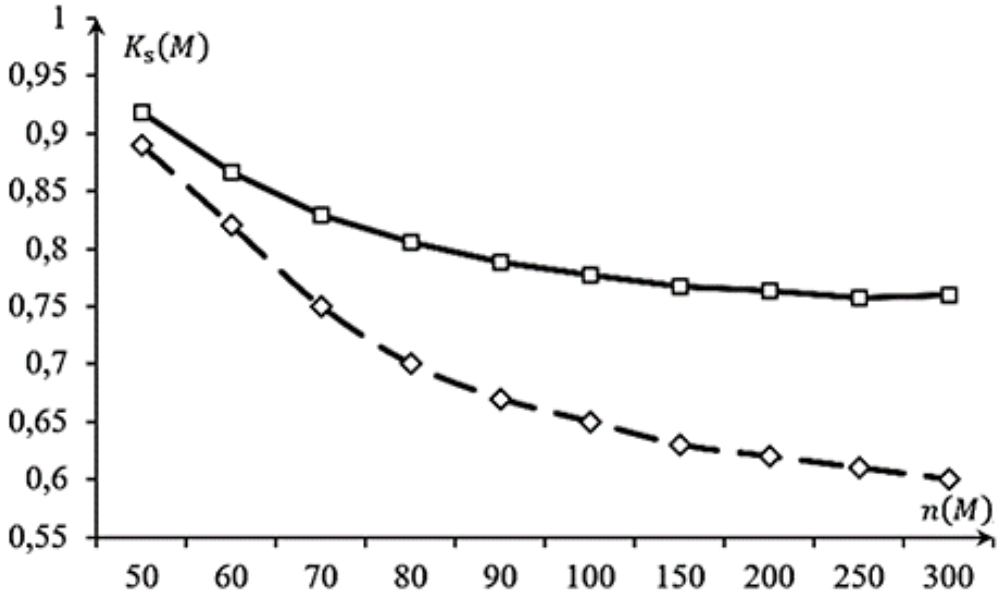

Figure 4 - Dependence of cryptographic encryption methods (1 – proposed method, 2 – analog)

From the analysis of the obtained results, it follows that the cryptographic stability of the proposed method is for the Length, which is much higher (20 – 30%) compared to the known analogue, while the value of the indicator for the second decreases exponentially. 0,9– 0,7550– 300

To automate encryption / decryption the message developed the appropriate software [16] with the possibility of implementing the proposed method, namely:

1) Formation of the Encryption Key and Alphabet, input of the Message, determination of its Length and formation of the Ciphertext.

2) Hiding of the Ciphertext or deformation of graphic data by values of the Ciphertext Encryption Alphabet in the positions determined by the Key.

3) Decryption of Ciphertext.

4. Conclusions and Prospects of Further Research

Thus, the proposed method provides: high stability of encrypted information; reducing the level of threat of unauthorized access to the Message or attack on the cipher by encrypting each character of the Message with a dynamic random number from the range of brightness values of the corresponding character; reducing the level of unauthorized access threat to the Message by hiding the Ciphertext in the position of graphic data, taking into account the Key, which is known only to the Sender and the Recipient.

The developed method of data encryption / decryption based on the pixel alphabet of monochrome image should be used for efficient operation of ITS networks when transmitting information through communication channels in the presence of a threat of unauthorized access to it or attack on the cipher in order to ensure high stability of encrypted information.

5. References

[1] A method for user authenticating to critical infrastructure objects based on voice message identification / Trysnyuk V., Nagornyi Ye., Smetanin K. And other // Advanced Information Systems, 2020. Vol. 4. No. 3. pp. 11–16.

[2] Korchenko O. G. Applied cryptology: encryption systems: a textbook / O. G. Korchenko, V. P Sidenko, Yu. O. Dreis. – Kyiv: DUT, 2014. 448 p.

[3] Pilkevych I. A., Boychenko O. S., Humeniuk I. V. Improving the method of developing a logical-probabilistic model of an internal violator // Electronic modeling. Electronic Modeling. Kyiv: G. E. Pukhov Institute of Modeling Problems in Energy NAS of Ukraine, 2020. Volume 42 (4). pp. 71–85.

[4] Konakhovich G. F. Computer steganography. Theory and practice / G. F. Konakhovich, A. Yu. Puzyrenko – Kyiv: MK-Press, 2006. 288 p.

[5] Ostapov S. E. Technologies of information protection: textbook / S. E. Ostapov, S. P. Evseev, O. G. Korol. – Kharkiv: Ed. KhNEU, 2013. 476 p.

[6] Ignatovych A. A. Methods of increasing the efficiency of security components of computer systems using masking elements of text and biometric data: dis. Cand. tech. Sciences: 05.13.05 / Anatoliy Oleksandrovych Ignatovych; Lviv Polytechnic National University. – Lviv, 2016. 145 p.

[7] Research and development of cryptographic and technical methods of information protection: report on research "04515" (final) / Karpukov L. M., Lizunov S. I., Voskoboynik V. O. and others. / Zaporozhye National Technical University / Zaporozhye: ZNTU, 2018. 91 p.

[8] Babenko V. G. Methodology of synthesis of information transformation operations for computer cryptography: dis. DR. Tech. Sciences: 05.13.05 / Vira Grigorivna Babenko; Cherkasy State Technological University. – Cherkasy, 2020. 200 p.

[9] Basic operations of the algorithm for the formation of shift ciphers using entropy Huffman coding / O. S. Androschuk, O. V. Nagrebetsky, V. S. Orlenko, A. I. Kataeva // Visnyk of Khmelnytsky National University. Technical Sciences Series. Khmelnytsky: KhNU, 2021. Volume 221. #6. pp. 7–14.

[10] Sulema E. S., Shirochin S. S. Method of steganography of images with fragmentation of stegodany and private key separation // Legal, regulatory and metrological support of the information protection system in Ukraine. Scientific and technical collection. Issue 1 (22), Kyiv: NTUU "KPI", 2012. pp. 64–68.

[11] Method for encrypting and decrypting digital data transmitted or stored using the priority pixel transmission method: German patent DE № 10229976a1, IPC H04 L9 / 14, H04 N7 / 24, application no. 03.07.2002, publ. 22.01.2004.

[12] Method of encrypting / decrypting data based on the pixel alphabet of a monochrome image: patent of Ukraine UA № 147950, IPC G 09C 1/00, G 09C 5/00, application no. 20.01.2021, publ. 06/24/2021.

[13] Voronin A. N. Nonlinear trade-off scheme in multicriteria estimation and optimization problems / Cybernetics and systems analysis, 2009, #4. C. 106–115

[14] Voronin A. N., Savchenko A. S. Multi-criteria optimization: a systems approach / Cybernetics and Systems Analysis, 2020, Volume 56, No. 6. pp. 160–174.1

[15] Varlamov I. D., Voronin A. N. Vector assessment of problematic situations // Problems of management and informatics, 2016. #3. pp. 7-16.

[16] Software for data encryption / decryption based on the pixel alphabet of the image, Certificate of registration of copyright to the work #101123, Date of registration 09.12.2020.