Advanced data encryption method based on the monochrome pixel alphabet

Vasyl Trysnyuk[1,†], Kyrylo Smetanin[2,*,†], Ihor Humeniuk[2,†], Oleksandr Lahodnyi[2,†] and Volodymyr Okhrimchuk[2,†]

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

Abstract

Results of the encryption methods analysis showed, that modern approaches only consider the cryptographic and steganographic properties of data protection algorithms and do not provide the proper level of information confidentiality. An advanced data encryption method based on a monochrome image alphabet, which takes into account cryptographic and steganographic properties of information security, has been proposed in the article. The method utilizes mathematical techniques to conceal the content of the original message, specifically by transforming its characters into an alphabet-like form and applying mathematical operations to convert the result into ciphertext. In combination with steganographic techniques, a monochrome image serves as the container, forming the basis for constructing a pixel matrix. It is shown that the cryptographic resilience of the method and information confidence exhibit functional dependency on the number of blocks into which the original image is divided, as well as its key system and the dynamic nature of pixel alphabet formation. The results of the experiment confirm that the method possesses the combination of cryptographic and steganographic properties exhibits, high efficiency, and provides an adequate and necessary level of information confidentiality. The conducted experiments have confirmed the functionality and adequacy of the proposed data encryption method based on a monochrome image alphabet. This allows us to recommend its practical use for information protection systems in institutions and organizations.

Keywords

data encryption, monochrome pixel alphabet, steganographic and cryptographic properties, cryptographic strength.

1.Introduction and Literature Review

In the current stage of information technology development, the issue of safeguarding the confidentiality of information resources is becoming increasingly relevant, timely, and

ITTAP'2024: 4th International Workshop on Information Technologies: Theoretical and Applied Problems, October 23-25, 2024, Ternopil, Ukraine, Opole, Poland
* Corresponding author.
† These authors contributed equally. trysnyuk@ukr.net (V. Trysnyuk); kiry221982@gmail.com (K. Smetanin); ig_gum@ukr.net (I. Humeniuk); lov.82@ukr.net (O. Lahodnyi); okhrimchuk84@ukr.net (V. Okhrimchuk)
0000-0001-9920-4879 (V. Trysnyuk); 0000-0002-6062-550X (K. Smetanin); 0000-0001-5853-3238 (I. Humeniuk); 0000-0002-0812-939X (O. Lahodnyi); 0000-0001-7518-9993 (V. Okhrimchuk)

important. This is primarily due to the intensive scientific and technical progress in the field of information security, information, and cybersecurity, and, as a result, the advancement of hardware and software information technologies. These advancements pose a threat to important information that is transmitted, processed, and stored by ICS. At the present time, various cryptographic protection algorithms are employed to ensure an adequate level of information and cybersecurity (achieving the fundamental properties of information). These include encryption for confidentiality, hashing for integrity control, and electronic digital signatures for availability (authentication) [1].

However, statistical data from global government response teams to cyber incidents indicate an increase in the number of attacks in the global and national cyberspace. This includes cyberattacks of the access type, whose purpose is to gain unauthorized access to important confidential and/or personal information of citizens and government officials of Ukraine, among others. The development of highly effective methods for cryptographic data protection is an important component in addressing information and cybersecurity concerns. The primary goal is to ensure a high level of cryptographic security in the developed encryption algorithms. Cryptographic security in methods of cryptographic data protection refers to the property of cryptographic algorithms and cryptographic protocols that characterizes their ability to resist cryptographic analysis methods [2].

Therefore, despite the existence of a lot of the number of known encryption algorithms, unauthorized access to information and access-based cyberattacks leading to data leaks and violations of the fundamental properties of information, which regulated by information security policies, are still prevalent [3]. Thus, there is a need for the development of a new cryptographic method that combines the mathematical properties of steganographic and cryptographic systems to provide robust information protection.

The known methods [4–7] only consider either the cryptographic or steganographic properties of data protection algorithms and, therefore, are incapable of resisting cryptographic attacks or attacks on the cipher. Let is analyse these methods. In scientific project [4] authors have proposed the new technic of steganography, based on the use of LSB method, for raster images of different colorful models for higher security and reliability level achievement.

The article [5] presents a method of data concealment in Portable Document Format (PDF) files that utilizes dereferenced objects and secret splitting or combining algorithms. It has been demonstrated that the hidden pages are not visible during regular use of the software. In [6], the authors focus on the development of Public-Key Encryption with Keyword Search (PEKS) in cloud technologies through comprehensive research. They also propose certain potential applications for this method.

In the scientific project [7], a mechanism for one-to-one information exchange with individual persons by concealing it from the rest of the group is developed. Given their availability, digital images are the most suitable components for use as containers compared to other objects available on the internet. The technique proposed encrypts the message within an image. In the scientific project [8–12], the authors propose approaches to combining cryptographic and steganographic properties for information protection. Their solutions are based on methods such as LSB, DWT, and well-known symmetric and asymmetric cryptographic data encryption algorithms. Therefore, in the scientific project [8], the authors propose an advanced steganographic-cryptographic system that combines the features of

cryptography and steganography. In [9], various combinations of cryptographic and steganographic methods are explored, highlighting that steganography based on DWT with Advanced Encryption Standard (AES) provides a higher level of security while preserving image quality. Additionally, a combination of the Data Encryption Standard (DES) cryptographic algorithm and LSB steganography for ensuring information confidentiality is suggested in [10].

The authors [11] have implemented a combination of the encryption method Cipher Block Chaining (CBC) and steganography method LSB-Sobel. This combination allows for achieving a relatively high quality of stego-images by using the Sobel edge detection method. In the scientific project [12] an increase in the level of information resistance of unauthorized access (UAA) was implemented using cryptographic and steganographic algorithm of its protection based on LSB-method, AES-algorithm and exchange opened keys protocol Diffie-Hellman. The analysis of scientific achievements indicates a large number of possible promising and implemented combinations of steganographic and cryptographic methods for information security. However, all of them are based on the use of known and outdated algorithms, the study of cryptographic stability of which indicates the imperfection of these cryptographic systems. This is due to the possibility of successful implementation by the violator of the UAA and attacks on the cipher. And it is carried out in order to violate the integrity and confidentiality of information that circulates in information systems or systems such as “sender-recipient”.

To achieve goal it’s necessary to: form pixel alphabet $B = \{B_1, B_2, B_3, B_4\}$ for Ukrainian and English alphabet symbols, numbers and punctuation symbols; synthesize and detail method stages, which takes into account cryptographic and steganographic algorithm properties of information security. After that for outgoing message $Mes = \{M_1, \ldots, M_m\}$ conduct verification of suggested method; conduct research of studying the impact of the parameters of a graphical container on the effectiveness of the proposed method.

2.Materials and methods

The proposed data encryption method, which combines the mathematical properties of steganographic and cryptographic systems and is based on the use of a pixel alphabet of a monochrome image, consists of five main stages: forming the pixel alphabet, creating the pixel matrix, key pair generation, encryption (forming ciphertext), and decryption.
A detailed scheme of the functioning of the developed method is presented in Fig. 1.

Let's describe each of the method's stages in detail. In the first stage, a specific static range of values [000;255] is assigned to every possible character of the output message that can be used in the message. This range corresponds to the brightness range of pixels in a digital raster image:

$$B = \{B_1, B_2, B_3, B_4\},$$

where B_1 – for letters in Ukrainian alphabet,

B_2 – for letters in English alphabet,

B_3 – for numbers,

B_4 – for special symbols and punctuation.

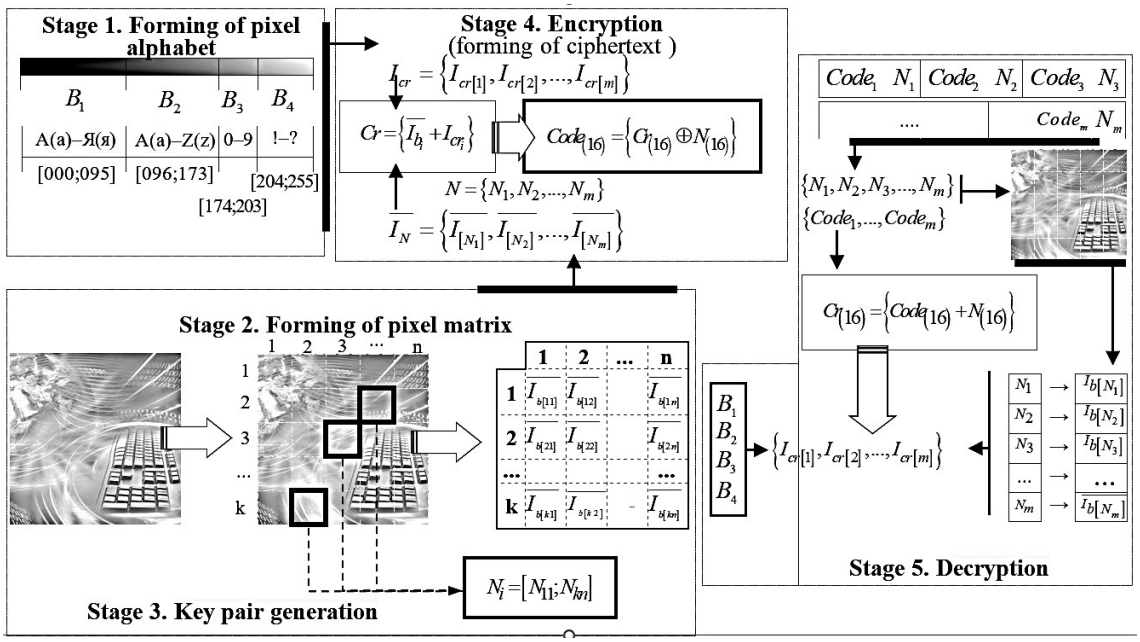

Figure 1: Block diagram of the proposed method.

The possible variant of pixel alphabet can be presented as follows: for letters in Ukrainian alphabet:

$$B_1 = \{B_{"а"}, B_{"б"}, \ldots, B_{"я"}\}, \quad (1)$$

where $B_1 \in [000; 095]$ and for example $B_{"а"} \in [000; 003]$; for letters in English alphabet:

$$B_2 = \{B_{"a"}, B_{"b"}, \ldots, B_{"z"}\}, \quad (2)$$

where $B_2 \in [096;173]$ and for example $B_{"a"} \in [096; 098]$; for numbers:

$$B_3 = \{B_{"0"}, B_{"1"}, \ldots, B_{"9"}\}, \quad (3)$$

where $B_3 \in [174; 203]$ and for example $B_{"0"} \in [174;176]$; for special symbols and punctuation:

$$B_4 = \{B_{"?"}, B_{"!"}, \ldots, B_{"\_"}\}, \quad (4)$$

where $B_4 \in [204; 255]$ and for example $B_{"?"} \in [204; 206]$.

The example for numbers of synthesized pixel alphabet is presented in Table 1.

Table 1

Pixel alphabet of numbers

Numbers	Value of brightness	Numbers	Value of brightness
0	174–176	5	189–191
1	177–179	6	192–194

2	180–182	7	195–197
3	183–185	8	198–200
4	186–188	9	201–203

It is worth mentioning, that symbols for message, choose out of the static range, that increases, which, in turn, increases the level of cryptographically resistant of such an algorithm. The pixel alphabet is synthesized on one side of the information exchange and transmitted to the other side through secure data transmission channels or is coordinated without any third party. That is, the pixel alphabet is generated or agreed upon only between the recipient and sender. Besides this, advisable to change the pixel alphabet periodically.

The next step is the formation of a pixel matrix. At this stage, an image with a consistent color model (usually monochrome) is arbitrarily selected, and the number of blocks into which it will be divided and numbered is determined. For each block, the average brightness values of the pixels are calculated $\overline{I_{[N_i]}}$, where $[N_i]$ – the block numbers, which are then recorded or mapped into the pixel matrix.

Similarly, to the alphabet, it is advisable to periodically change either the image itself or the number of blocks into which it is divided. It's worth noting that the choice of a raster image and the number of blocks are coordinated by both sides of the exchange, and for algorithm usage, only the pixel matrix is retained.

During the generation of a set of encryption keys, the sender arbitrarily selects block numbers from the pixel matrix and their corresponding average brightness values, which determine the encryption key.

The main step of the method is the process of encrypting information: each character in the original message is replaced using the synthesized alphabet with a corresponding value from its assigned range. Then, a set of sums is calculated between the transformed message into the pixel alphabet and the corresponding values of the pixel matrix $I_{cr[i]}$ using the encryption key set:

$$Cr_i = \left\{\overline{I_{[N_i]}} + I_{cr[i]}\right\}. \quad (5)$$

Afterwards, the ciphertext is calculated as:

$$Code_{(16)} = \{Cr_{(16)} \oplus N_{(16)}\}. \quad (6)$$

It's worth mentioning that to obtain the ciphertext, the corresponding values are used in the hexadecimal system. This rule also applies to transmitting the ciphertext. As a result, the ciphertext appears as a sequence of pairs of ciphertext values $Code_{(16)}$ and block numbers $N_{(16)}$ each character of the message. A notable feature of the method is that multiple characters can be assigned to the same block, which further enhances the algorithm's cryptographic resistance.

On the recipient's side, the reverse process of encryption, decryption, is performed. The result of this stage is the retrieval of the original message.

3.Experiment, Results and Discussions

In order to confirm the functionality of the proposed enhanced data encryption method based on the monochrome image alphabet, an experiment was conducted using the verification method selected in reference [13].

To conduct the experiment in the Python programming language, the method proposed in the article was implemented. During the experiment, encryption of the open-text message was performed based on the developed method, followed by the transmission of the ciphertext over a network, and then the decryption of the received ciphertext on another host. So, for conducting the experiment, the following original message was chosen: Cybersecurity.

According to the first stage of the method, all characters of the input message were transformed based on the proposed technique outlined in [14] Alphabet encryption of letters of the English alphabet.

Table 2
Message transformation to pixel alphabet

Outgoing message symbol	The transformation result
C	102
Y	169
B	100
E	108
R	147
S	150
E	109
C	104
U	156
R	147
I	120
T	153
Y	168

In this way, the input message takes the following form:

$$I_{cr} = \{102; 169; 100;108; 147; 150;109; 104; 156; 147;120; 153; 168\}. \quad (7)$$

In the next stage, a test image with dimensions of 264x192 pixels was selected and divided into 25 blocks (5 by 5). Using the Python Imaging Library (PIL) library, the average brightness values of the pixels in each block were calculated, and a pixel matrix was generated as follows in Table 3.

Table 3
Formation of pixel matrix

Columns of matrix	Rows of matrix				
-	1	2	3	4	5
1	219	216	203	188	225
2	213	210	234	232	223
3	210	193	96	198	170
4	198	204	212	226	224

5	198	204	215	185	209

After the formation of the pixel matrix, the encryption process of the message takes place. To encrypt the characters of the message, a set of keys was generated by randomly selecting block numbers from the pixel matrix and their corresponding average brightness values using the "random" module. The number of keys corresponds to the number of characters in the message being encrypted. Therefore, during the experiment, a set of block numbers from the image was formed (Table 4).

Table 4
The set of encryption keys

Block numbers	Hexadecimal representation
12	0C
54	36
33	21
22	16
12	0C
25	19
12	0C
51	33
31	1F
51	33
52	34
35	23
53	35

Mathematically, the set of keys has the following form:

$$N = \{12;54;\ 33;\ 22;\ 12;\ 25;\ 12;\ 51;\ 31;\ 51;\ 52;\ 35;\ 53\}. \quad (8)$$

In the next stage, the sum is calculated according to expression (5), transformed into the pixel alphabet message (7), and the corresponding values of the pixel matrix (Table 3) are used with the encryption key set (8). As a result, the following values are obtained:

$$Cr = \{318;\ 354;\ 196;318;\ 363;\ 373;\ 325;302;\ 366;\ 345;324;\ 323;\ 383\}. \quad (9)$$

In the final stage, before sending the message to the recipient, it is transformed into ciphertext according to expression (6). As a result of this transformation, obtained message has the following form:

$$Code_{(16)} = \{132;154;\ E5;\ 128;\ 167;\ 16C;\ 149;\ 11D;\ 171;\ 16A;\ 170;160;\ 14A\}. \quad (10)$$

Therefore, by using the proposed method, the encrypted message (Table 5) is presented in the hexadecimal numbering system.

Table 5
Components of ciphertext

Key	Ciphertext

0C	132
36	154
21	0E5
16	128
0C	167
19	16C
0C	149
33	11D
1F	171
33	16A
34	170
23	160
35	14A

The recipient receives tuples of pairs consisting of ciphertext values (10) and block numbers (8) for each character of the message:

$$\{(132,0C);\ (154,36);\ \ldots;\ (160,23);(14A,\ 35)\}. \tag{11}$$

After receiving the encrypted message, the recipient performs decryption (the reverse execution of the steps).

When analysing the effectiveness of the proposed method, we used incoming messages with different numbers of characters are provided in Table 6.

Applying the mathematical apparatus proposed in this paper, we obtained results, the analysis of which confirms the adequacy of the method of data encryption and decryption.

In addition to testing the functionality of the proposed data encryption method based on the monochrome image alphabet, the experiment also investigated the influence of factors such as image size, the number of blocks into which the image is divided, and/or the number of characters in the encrypted message on the data encryption speed. As a result of the study, the time indicators depending on the selected parameters (Table 6).

Table 6
Experimental results of research

Size of the image in pixels	Number of blocks	Number of symbols in the message	Time of encrypting, sec
264x191	5x5	13	0:00:00.025991
		331 13	0:00:00.030206
1200x675		331	0:00:00.384151
			0:00:00.389754
264x191	10x10	13	0:00:00.026113
		331 13	0:00:00.030313
1200x675		331	0:00:00.384858
			0:00:00.391086

As a result of the conducted experiment to assess the functionality and adequacy of the proposed method, the following conclusions were made:

1. The method possesses cryptographic properties, utilizing mathematical techniques to conceal the content of the original message (transforming its characters into an alphabetlike format and performing a mathematical operation to convert the result into ciphertext). It also combines steganographic properties, using a monochrome image as a container, which forms the basis for constructing the pixel matrix.

The computational complexity of the mathematical apparatus in the proposed method is relatively low, yet it demonstrates high efficiency and is capable of resisting cryptographic analysis methods.

2. As a container for constructing the pixel matrix, it is indeed possible to use monochromatic raster images with varying resolutions and different geometric dimensions. This flexibility in choosing the container makes the method adaptable to various scenarios and use cases.

If a color raster image is chosen as the container, the pixel alphabet range increases threefold due to the use of all three color channels. (R, G and B). As a result, the number of possible variations in synthesizing the alphabet increases. For example, values for English language characters can be chosen from the [0; 255] range in the R channel, punctuation marks and special characters from the G channel, and digits from the B channel, and so on. This expanded range of possibilities in a color image allows for more diverse and robust encryption. The size of the image has the most significant impact on the speed of the data encryption procedure, particularly increasing the size of the image results in an increase in the duration of the encryption process. However, the encryption time of the message is almost independent of the number of blocks into which the image is divided and the number of characters in the message itself. This suggests that the primary factor affecting encryption speed is the image size.

3. The number of blocks into which the original image (container) is divided and its color system indeed have a direct impact on the set of possible variations in forming the ciphertext. This, in turn, increases the level of cryptographic resistance of the method.

4. The set of variations in the pixel alphabet depends directly on the characters in the original message (including the alphabet used, punctuation marks, digits, etc.) and the color system of the raster image. The degree of periodicity in changing the pixel alphabet is directly proportional to the level of confidentiality of the information that needs to be encrypted. In essence, greater diversity and complexity in the formation of the pixel alphabet contribute to higher information security.

The analysis of the results in Table 5 indicates that all encryption stages have been completed for the initial values of the original message (Table 2), resulting in the corresponding ciphertext (11). It is important to note that this is one of the possible variants of the encrypted message, based on the specific choices of pixel alphabet range values for each individual character of the original message. Furthermore, the set of possible ciphertexts also depends on the formation of the pixel matrix, including the number of blocks into which the raster image is divided. This is because the same block or different blocks can be used to select the encryption key for the characters of the original message. Taking into account the image size and the number of blocks (Table 6) into which it is divided allows for an evaluation of the set of possible ciphertexts as well as the time required for the encryption procedure.

The data encryption method based on a monochrome image alphabet is suitable for secure transmission of confidential or important information in conditions where there may be threats like cyberattacks, UAA, or other fraudulent actions, , even when the data network is secured using a cluster approach [15]. Consideration of encryption parameters (such as the periodicity of pixel alphabet changes, increasing the number of blocks in the pixel matrix, and so on) significantly enhances the cryptographic resilience of the proposed method. It also enhances the level of information confidentiality protection and resistance against UAA.

4.Conclusions

The scientific novelty of obtained results involves improving the data encryption method based on a pixel alphabet by changing the order and mathematical apparatus. The proposed method, unlike known and existing ones, does not utilize the functionality of cryptographic and steganographic encryption systems but rather their structural properties. It provides an adequate level of information confidentiality and possesses a sufficient and necessary level of cryptographic resilience. The mathematical apparatus of the data encryption method implements the concealment of the message content, while the pixel matrix and its usage represent the very existence of such a message. By using the blocks into which it is divided as mathematical components of encryption, namely their average pixel brightness values obtained at the stage of pixel matrix formation.

The practical orientation of the study lies in the ability to apply the proposed data encryption method to ensure secure and confidential exchange of important information between organizations and institutions.

Prospects for further research include improving the mathematical apparatus of the encryption method, considering pseudorandomness and the dynamic formation of the pixel alphabet, and utilizing various color systems for raster images.

References

[1] Analysis of the Cryptographic Algorithms in IoT Communications / [Catarina Silva, Vitor A. Cunha, João P. Barraca, Rui L. Aguiar] // Information Systems Frontiers. – 2023. –P. 18. DOI: doi.org/10.1007/s10796-023-10383-9.

[2] Cryptographic Strength Evaluation of Key Schedule Algorithms / [S. Afzal, M. Yousaf, H. Afzal, N. Alharbe, M. Rafiq Mufti] // Security and Communication Networks. – Volume 2020. – P. 1–9. URL: https://doi.org/10.1155/2020/3189601

[3] Development of a modified UMAC algorithm based on crypto-code constructions / [A. Gavrilova, I. Volkov, Y. Kozhedub, R. Korolyov, O. Lezik, V. Medvediev, O. Milov, B. Tomashevsky, A. Trystan, O. Chekunova] // Eastern-European Journal of Enterprise Technologies. – 2020. – Vol. 4/9. – Issue 106. P. 45–63. URL: https://journals.uran.ua/eejet/article/view/210683.

[4] A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method [S. Rahman, J. Uddin, H. Ullah Khan, H. Hussain, A. Ali Khan, M. Zakarya] // IEEE Access. – 2022. – Vol. 10. P. 124053–124075. URL: http://dx.doi.org/10.1109/ACCESS.2022.3224745.

[5] Koptyra K., Ogiela M. R. Distributed Steganography in PDF Files–Secrets Hidden in Modified Pages / [K.Koptyra, M. R. Ogiela] // Entropy (Basel). – 2020. – Volume 22 (6). – Issue 600. P. 12. URL: https://doi.org/10.3390/e22060600.

[6] Public Key Encryption with Keyword Search in Cloud: A Survey / [Y. Zhou, N. Li, Y. Tian, D. An, L. Wang] // Entropy. – 2020. – Volume 22. Issue 421. P. 24. URL: https://www.mdpi.com/1099-4300/22/4/421.

[7] An efficient and secure technique for image steganography using a hash function / [Z. Nezami, Ali H., M. Asif, H. Aljuaid, I. Hamid, Z. Ali] // PeerJ Comput Sci. – 2022. Volume 8. – Issue 1157. P. 18. DOI: 10.7717/peerj-cs.1157.

[8] Cryptographic steganography / V. Yadav, V. Ingale, A. Sapkal, G. Patil // Sundarapandian et al. (Eds) : CCSEIT, DMDB, ICBB, MoWiN, AIAP – 2014. P. 17–23. DOI: 10.5121/csit.2014.4803.

[9] A study on combined cryptography and steganography / V. S. Babu, K. J. Helen // International Journal of Research Studies in Computer Science and Engineering (IJRSCSE). – 2015. – Volume 2. Issue 5. ISSN 2349-4840. P. 45–49.

[10] Image security using steganography and cryptographic techniques / R. Nivedhitha, T. Meyyappan // International Journal of Engineering Trends and Technology. – 2012. Volume 3. Issue 3. ISSN: 2231-5381. P. 366–371.

[11] Kombinasi Least Significant Bit (LSB-1) Dan Rivest Shamir Adleman (RSA) Dalam Kriptografi Citra Warna / C. A. Sari, W. S. Sari // Jurnal masyarakat informatika. – 2022. – Volume 13. Issue 1. ISSN: 2086-4930. P. 45–58. URL: https://doi.org/10.14710/jmasif.13.1.43314.

[12] Crypto-steganographic LSB-based system for AES-encrypted data / M. Abu-Alhaija // (IJACSA) International Journal of Advanced Computer Science and Applications. – 2019. – Volume 10. Issue 10. P. 55–60.

[13] Hryshchuk R. V., Hryshchuk O. M., Okhrimchuk V. V. Verification of a generalized differential game model of a potentially dangerous cyber attack template. Telecommunications and information technology. 2020, № 1 (66). С.53 - 67.

[14] Information Encryption Method based on a Combination of Steganographic and Cryptographic Algorithm's Features / [V. Trysnyuk, K. Smetanin, I. Humeniuk, O. Samchyshyn, T. Trysnyuk] // Cybersecurity Providing in Information and Telecommunication Systems II, Kyiv, Ukraine, October 26, 2021. – P. 150–159.

[15] Smetanin K. Cluster approach of building networks as a way of ensuring the appropriate level of cyber security of the information and telecommunication system // Vol. 29 No. 1 (2023): Ukrainian Scientific Journal of Information Security. URL: https://doi.org/10.18372/2225-5036.29.17547.