DOI 10.15276/imms.v13.no3-4.204
UDC 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 3-4, pp. 204-211

THE ALGORITHM FOR ENCRYPTION OF GRAPHIC INFORMATION BASED ON CHAOTIC MAP AND GALOIS FIELD TRANSFORM

O.O. Palagin, A.V. Sokolov

National Odesa Polytechnic University
1 Shevchenko Ave., Odesa, 65044, Ukraine
email: radiosquid@gmail.com

The current stage of development of information technologies is characterized by a significant increase in the use of graphic data, i.e., digital video and digital images combined with the widespread use of resource-constrained platforms, such as IoT and IoBT devices, mobile devices, as well as embedded devices. These circumstances condition the importance of the development of algorithms for encrypting graphic information, which would ensure high security for the least number of computational operations. Today, dynamic chaos theory is most often used for the development of such cryptographic algorithms. However, the optimal structure of the cryptographic algorithm for image encryption has not yet been found. In this paper, we propose a combination of the advantages of traditional SP networks and a gamma generator based on a Hyper-Chaotic Modified Robust Logistic Map to build an effective image encryption algorithm, capable of providing a high level of security. The proposed cryptographic algorithm uses high-quality S-boxes based on the Galois field transform, as well as P-boxes based on permutations generated using the Nyberg construction, while segmentation and further processing of three-dimensional image blocks are used, which allows for an increase in the diffusion effect. Numerous tests of the stochastic quality of cryptograms obtained using the developed cryptographic algorithm, as well as their comparison with the results obtained for the AES cryptographic algorithm, made it possible to establish that the developed cryptographic algorithm provides a sufficient level of information protection while requiring only two rounds. Therefore, the developed cryptographic algorithm for encrypting graphic information can be recommended for practical use, in particular, on resource-constrained platforms.

Keywords: cryptographic algorithm, image encryption, dynamic chaos, Hyper-Chaotic Modified Robust Logistic Map, Galois transform-based S-box, Nyberg construction.

Introduction and statement of the problem. Today, the development of information technologies adheres to increasing the amount of graphic information that is generated and transmitted. At the same time, the current state of computer technology involves the use of various devices for working with such information, including resource-constrained devices, such as mobile devices, IoT and IoBT devices, and embedded devices.

In modern information protection systems, cryptographic means are one of the most important tools that ensure confidentiality. At the same time, block symmetric ciphers, such as the AES cryptographic algorithm [1], are used to encrypt large volumes of information, including multimedia content. Nevertheless, today’s cryptographic algorithms, which are adapted specifically for the encryption of multimedia information and allow for a significant reduction in the level of computing costs required for the encryption of multimedia, are actively developed and increasingly used in practice.

One of the most promising areas of development of such cryptographic algorithms is chaotic maps. Chaos is the pseudo-random and unpredictable motion exhibited by a deterministic dynamical system due to its sensitivity to input values and parameters. The research of chaos theory began with the three-body problem, which was researched by A. Poincare [3]. Today, many papers [4 – 7] are devoted to the research of the problems of applying chaos theory to the encryption of multimedia information, however, the final optimal structure of cryptographic transformation based on chaotic maps has not been created yet.

The *purpose* of this paper is to improve the effectiveness of cryptographic protection of graphic information by developing a cryptographic algorithm based on chaotic map and Galois field transform.

Components of the proposed cryptographic algorithm. The proposed cryptographic algorithm uses a gamma block based on the theory of dynamic chaos, namely on the Hyper-Chaotic Modified Robust Logistic Map (HC-MRLM) [8]. For the completeness of the presentation of the material, we will briefly describe the algorithm of operation of this generator of pseudo-random key sequences.

Step 1. Set values $x_0 \in (0,1)$ and $\gamma \in [4,31]$.

Step 2. Calculate the values

$$\eta_1 = \left\lceil \frac{1}{2} - \sqrt{\frac{1}{4} - \frac{\lfloor \gamma/4 \rfloor}{\gamma}} \right\rceil, \eta_2 = \left\lceil \frac{1}{2} + \sqrt{\frac{1}{4} - \frac{\lfloor \gamma/4 \rfloor}{\gamma}} \right\rceil. \tag{1}$$

Step 3. Set the values of counters $i = 1$ and $j = 1$.

Step 4. If $\gamma \leq 4$, calculate

$$x_i = \gamma x_{i-1}(1 - x_{i-1}), \tag{2}$$

otherwise, calculate

$$x_i = \begin{cases} \dfrac{\gamma x_{i-1}(1 - x_{i-1})(\mathrm{mod}\,1)}{\gamma/4\,(\mathrm{mod}\,1)}, \text{if } x_{i-1} \geq \eta_1 \ i \ x_{i-1} \leq \eta_2 \\ \gamma x_{i-1}(1 - x_{i-1})(\mathrm{mod}\,1), \text{otherwise.} \end{cases} \tag{3}$$

Step 5. If $x_i \geq 0.1$ and $x_i \leq 0.6$ calculate the temporary value

$$t = x_i \cdot 10^{10}(\mathrm{mod}\,1), \tag{4}$$

otherwise, increase the counter value $i = i + 1$ and go to *Step 4*.

Step 6. Based on the temporary value, calculate the gamma element

$$y_j = \begin{cases} 1, \text{if } t \geq 0.5, \\ 0, \text{if } t < 0.5. \end{cases} \tag{5}$$

Increase the value of the counter $j = j + 1$.

Step 7. If all necessary gamma elements are generated, exit the algorithm, otherwise, increase the value of the counter $i = i + 1$ and go to *Step 4*.

In the paper [8] the high cryptographic quality of such a generator is proved, as well as the high stochastic quality of the sequences generated by it. At the same time, the number of protection levels of the specified generator is greater than 2^{100}, which is sufficient for its use in information encryption tasks.

In addition to the generator of pseudorandom key sequences based on the chaotic map, the proposed cryptographic algorithm uses the S-box based on the Galois field transform [9] and the P-box, for which it is proposed to use a permutation which is based on the Nyberg construction over non-binary Galois fields [10].

Thus, as a nonlinear transformation of the cryptographic algorithm, it is proposed to use promising constructions of non-binary Galois fields, which were first described in [9] and are characterized by a high level of cryptographic quality. As part of the experiments performed in this paper, the S-box was used, which is the third row of the direct matrix of the Galois field transform, constructed using arithmetic, defined by the irreducible polynomial $f(x)=x^8+x^4+x^3+x^2+1$

S	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	47	A7	D8	72	E0	3E	36	5F	92	4E	38	23	81	1A
1	83	A0	DE	90	AA	3D	9D	AD	0E	97	C1	13	67	16	88	30
2	E9	FB	28	D1	B9	C4	24	57	A4	C3	48	89	60	56	6C	ED
3	8D	52	EC	20	77	DB	CD	84	D0	70	8B	26	22	50	0C	AB
4	7D	85	F7	D2	0A	99	73	10	69	53	31	49	09	AC	DC	0B
5	29	71	F9	43	12	59	65	B8	18	DF	9B	BC	1B	54	7C	CC
6	64	C5	9A	95	3B	CE	08	9C	D4	42	FF	7F	74	FA	21	6D
7	34	C2	1C	82	EB	F2	87	E5	86	B1	14	3F	03	8F	E3	E7 .
8	58	C0	66	4C	F4	8E	BA	7A	8C	68	61	25	D5	F8	04	A6
9	5D	96	DD	98	4B	2A	55	80	45	93	2B	1E	37	41	CB	63
A	4D	17	5B	CA	79	DA	D9	11	8A	2C	51	39	5E	40	2E	6F
B	06	BB	FE	FC	EF	B3	2F	32	CF	A9	15	E1	1F	4A	33	6E
C	19	91	76	78	A8	3A	62	5A	C7	A2	BD	94	02	F5	27	2D
D	35	A5	9E	A3	F6	C8	D6	D7	1D	A1	B0	E4	4F	44	5C	0F
E	0D	3C	BE	B7	07	7B	AE	B6	F3	B4	B2	6A	E8	75	7E	FD
F	AF	BF	6B	EE	05	46	C6	9F	C9	D3	EA	B5	F1	E2	F0	E6

(6)

S-box (6) is characterized by a high level of nonlinearity, a small deviation from compliance with the strict avalanche criterion, uniform minimization of the elements of the correlation coefficients matrix, which makes it a promising choice for use in the proposed cryptographic algorithm.

Note that the inverse substitution to substitution (6) has the following form

S^{-1}	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	00	01	CC	7C	8E	F4	B0	E4	66	4C	44	4F	3E	E0	18	DF
1	47	A7	54	1B	7A	BA	1D	A1	58	C0	0F	5C	72	D8	9B	BC
2	33	6E	3C	0D	26	8B	3B	CE	22	50	95	9A	A9	CF	AE	B6
3	1F	4A	B7	BE	70	D0	08	9C	0C	AB	C5	64	E1	15	07	7B
4	AD	9D	69	53	DD	98	F5	02	2A	4B	BD	94	83	A0	0B	DC
5	3D	AA	31	49	5D	96	2D	27	80	55	C7	A2	DE	90	AC	09
6	2C	8A	C6	9F	60	56	82	1C	89	48	EB	F2	2E	6F	BF	AF
7	39	51	05	46	6C	ED	C2	34	C3	A4	87	E5	5E	40	EE	6B .
8	97	0E	73	10	37	41	78	76	1E	2B	A8	3A	88	30	85	7D
9	13	C1	0A	99	CB	63	91	19	93	45	62	5A	67	16	D2	F7
A	11	D9	C9	D3	28	D1	8F	03	C4	B9	14	3F	4D	17	E6	F0
B	DA	79	EA	B5	E9	FB	E7	E3	57	24	86	B1	5B	CA	E2	F1
C	81	1A	71	29	25	61	F6	C8	D5	F8	A3	9E	5F	36	65	B8
D	38	23	43	F9	68	8C	D6	D7	04	A6	A5	35	4E	92	12	59
E	06	BB	FD	7E	DB	77	FF	7F	EC	20	FA	74	32	2F	F3	B4
F	FE	FC	75	E8	84	CD	D4	42	8D	52	6D	21	B3	EF	B2	6A

(7)

As a P-box, it is proposed to use a permutation built on the basis of Nyberg construction [10], in which each element is defined as the multiplicative inversion of the given element by a double modulus

$$y_i = x_i^{-1}\mathrm{modd}(3,\psi(x)),\ x_i \in GF(3^5),\ i=0,1,...,242\,, \tag{8}$$

where the irreducible over $GF(3)$ polynomial $\psi(x)=x^5+2x+1$ is chosen.

The permutation itself has the following form

$$\begin{gathered}P=\{0,1,2,163,210,240,83,120,150,217,57,60,70,104,200,80,115,142,110,30,33,\\40,194,221,50,154,178,235,98,37,19,58,216,20,218,62,183,29,117,114,21,143,\\149,140,136,106,88,172,198,103,24,207,229,202,119,74,184,10,31,109,11,108,\\35,176,101,167,144,161,134,153,12,179,96,234,55,214,191,196,219,193,15,241,\\212,6,112,188,180,175,46,99,169,186,111,182,170,113,72,118,28,89,105,64,155,\\49,13,100,45,165,61,59,18,92,84,95,39,16,192,38,97,54,7,211,162,127,204,233,\\129,123,157,126,238,205,208,201,68,195,44,215,189,213,43,220,17,41,66,203,\\228,197,190,42,8,164,242,69,25,102,239,128,232,230,209,67,122,3,151,107,\\171,65,224,90,94,166,47,174,173,87,63,199,26,71,86,222,93,36,56,236,91,223,\\85,138,148,76,116,79,22,135,77,147,48,177,14,133,53,145,124,131,226,51,132,\\160,4,121,82,139,75,137,32,9,34,78,141,23,181,187,168,231,206,237,146,52,\\159,225,158,125,73,27,185,227,130,156,5,81,152\},\end{gathered}\tag{9}$$

while the inverse permutation for permutation (9) has the following form

$$\begin{gathered}P^{-1}=\{0,1,2,163,210,240,83,120,150,217,57,60,70,104,200,80,115,142,110,30,\\33,40,194,221,50,154,178,235,98,37,19,58,216,20,218,62,183,29,117,114,\\21,143,149,140,136,106,88,172,198,103,24,207,229,202,119,74,184,10,31,109,\\11,108,35,176,101,167,144,161,134,153,12,179,96,234,55,214,191,196,219,193,\\15,241,212,6,112,188,180,175,46,99,169,186,111,182,170,113,72,118,28,89,105,\\64,155,49,13,100,45,165,61,\ 59,18,92,84,95,39,16,192,38,97,54,7,211,162,127,\\204,233,129,123,157,126,238,205,208,201,68,195,44,215,189,213,43,220,17,41,\\66,203,228,197,190,42,8,164,242,69,25,102,239,128,232,230,209,67,122,3,151,\\107,171,65,224,90,94,166,47,174,173,87,63,199,26,71,86,222,93,36,56,236,91,\\223,85,138,148,76,116,79,22,135,77,147,48,177,14,133,53,145,124,131,226,51,\\132,160,4,121,82,139,75,137,32,9,34,78,141,23,181,187,168,231,206,237,146,\\52,159,225,158,125,73,27,185,227,130,156,5,81,152\}.\end{gathered}\tag{10}$$

The algorithms for information encryption and decryption. On the basis of mentioned cryptographic primitives, an effective algorithm for encrypting digital images consisting of two rounds was proposed.

In addition to the application of chaotic map, effective S-boxes based on Galois field transform and P-boxes based on permutations generated using the Nyberg construction, in the proposed information encryption algorithm an approach that involves working with three-dimensional image blocks is used, which allows a higher level of diffusion.

Information encryption algorithm:

Input data: a three-dimensional matrix of the input image P of size $m \times n \times 3$, the elements of which are integer numbers in the range $[0,255]$, initial data x_0 and γ for the chaotic map, a specific type of substitution S, a specific type of permutation P.

Output data: a three-dimensional encrypted image matrix C of size $m \times n \times 3$, the elements of which are integer numbers in the range $[0,255]$.

Encryption algorithm:

Step 1. Segment the image into three-dimensional blocks of size $9 \times 9 \times 3$. If the size of the image is not a multiple of the size of the block, the side blocks are supplemented with elements from the blocks lying on the opposite side of the image.

Step 2. The iteration counter of the rounds is set as $\alpha = 0$.

Step 3. Substitution within the block. Sequentially, in each block, the elements of the blocks are replaced according to the rule defined by substitution S.

Step 4. Permutation within the block. Each block of size $9 \times 9 \times 3$ is represented as a one-dimensional sequence $\{u_i\}$, $i = 0,1,...,242$ by sequential concatenation of columns taken sequentially from each matrix in the third dimension. Next, the permutation of elements is applied to the resulting sequence $\{u_i\}$ according to the rule defined by permutation P. After permuting the elements of the sequence $\{u_i\}$, the formation of an encrypted block is performed by successively filling it by columns, and then by filling each of the matrices of the third dimension with the elements of the sequence $\{u_i\}$.

Step 5. Gamming within the image. The image matrix is represented as a sequence $\{g_i\}, i = 0,1,...,m \cdot n \cdot 3 - 1$ by successive concatenation of columns that are taken sequentially from each matrix in the third dimension. The gamming result is determined in the following way

$$r_i = \begin{cases} g_i \oplus y_i, \text{if } i = 0, \\ g_i \oplus g_{i-1} \oplus y_i, \text{if } i \neq 0. \end{cases} \tag{11}$$

where y_i is the next bit of the gamma generated by the generator based on the Hyper-Chaotic Modified Robust Logistic Map, the notation $\oplus$ means the bitwise sum modulo 2, and $i = 0,1,...,m \cdot n \cdot 3 - 1$. After gamming, the resulting matrix of the image is formed from the sequence $\{r_i\}$ by sequentially filling it by columns, and then by filling each of the matrices of the third dimension, with elements of the sequence $\{r_i\}$.

Step 6. Increase the counter of the rounds $\alpha = \alpha + 1$. If $\alpha = 2$ the image encryption is complete, otherwise go to *Step 3*.

Information decryption algorithm:

Input data: a three-dimensional matrix of an encrypted image C of size $m \times n \times 3$, whose elements are integer numbers in the range $[0,255]$, initial data x_0 and γ for the chaotic map, a specific type of inverse substitution S^{-1}, a specific type of inverse permutation P^{-1}.

Output: a three-dimensional matrix of the output image P of size $m \times n \times 3$, whose elements are integer numbers in the range $[0,255]$.

Decryption algorithm:

Step 1. Segment the image into three-dimensional blocks of size $9 \times 9 \times 3$. If the size of the image is not a multiple of the size of the blocks, the blocks are supplemented with elements from the blocks lying on the opposite side of the image.

Step 2. The iteration counter of the rounds is set $\alpha = 0$.

Step 3. Gamming within the image. The image matrix is represented as a sequence $\{g_i\}, i = 0,1,...,m \cdot n \cdot 3 - 1$ by successive concatenation of columns that are taken sequentially from each matrix in the third dimension. After gamming, the resulting matrix of the image is formed from the sequence $\{r_i\}$ by sequentially filling it by columns, and then by filling each of the matrices of the third dimension, with elements of the sequence $\{r_i\}$.

Step 4. Reverse permutation within the block. Each block of size $9 \times 9 \times 3$ is represented as a one-dimensional sequence $\{u_i\}, i = 0,1,...,242$ by sequential concatenation of columns taken sequentially from each matrix in the third dimension. Next, permutation of elements is applied to the resulting sequence $\{u_i\}$ according to the rule defined by permutation P^{-1}. After permuting the elements of the sequence $\{u_i\}$, the decrypted block is formed by successively filling it by columns, and then by filling each of the matrices of the third dimension with elements of the sequence $\{u_i\}$.

Step 5. Reverse substitution within the block. Sequentially, in each block, the elements of the block are replaced according to the rule defined by inverse substitution S^{-1} .

Step 6. Increase the counter of the rounds $\alpha = \alpha + 1$. If $\alpha = 2$ the image decryption is complete, otherwise go to *Step 3*.

We show in Fig. 1 a schematic representation of the proposed cryptographic algorithm for encryption and decryption of digital images.

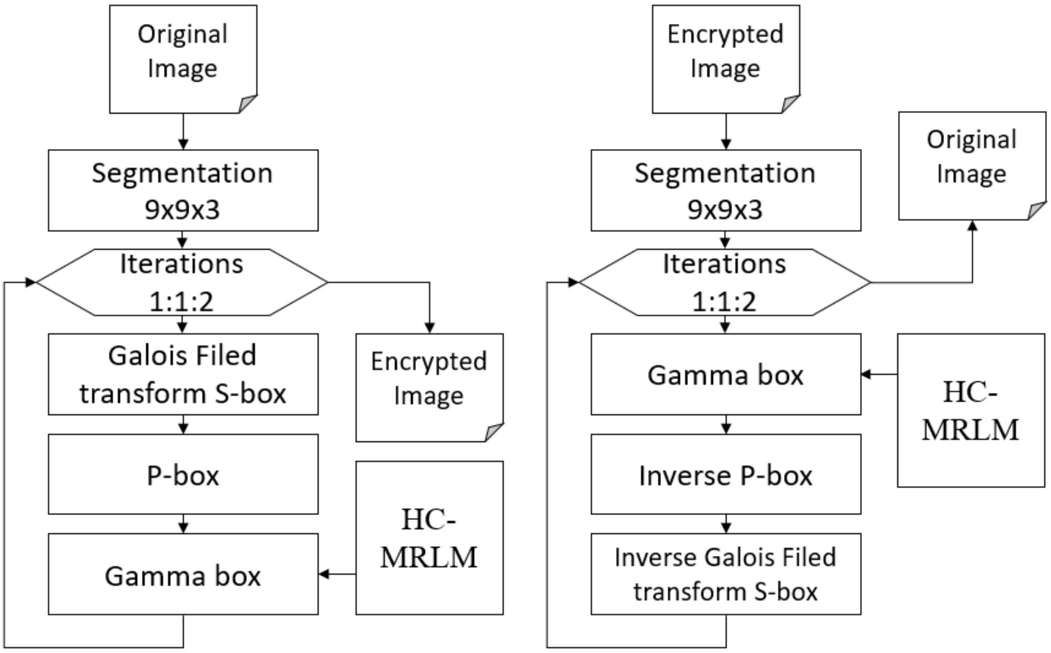

Fig. 1. Schematic presentation of the proposed cryptographic algorithm

Testing results of the proposed cryptographic algorithm. The proposed cryptographic algorithm for image encryption due to its optimal structure, which is adapted for the encryption of graphic information, as well as the high quality of the cryptographic primitives included into its composition, allows us to achieve sufficient results in the encryption of graphic information. In Fig. 2 we present an example of the original and encrypted digital image using the proposed cryptographic algorithm.

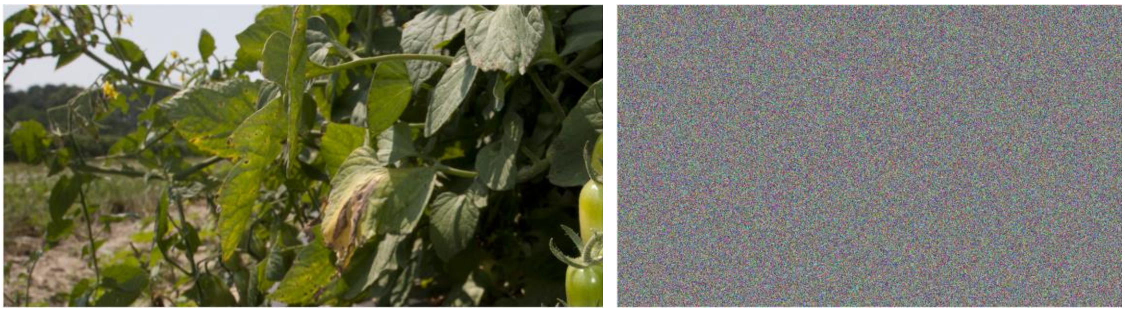

Fig. 2. An example of the original and encrypted image

For a deeper assessment of the quality of cryptograms obtained using the developed cryptographic algorithm, a NIST stochastic tests suite [11] can be used, which consists of 15 tests designed to determine the stochastic properties of binary sequences. A high-quality encryption algorithm should produce output sequences that are indistinguishable from truly random sequences.

To test the quality of the developed cryptographic algorithm, the following experiment was performed: 250 images from the NRCS database [12] were encrypted with the AES cryptographic algorithm (2 rounds), the AES cryptographic algorithm (14 rounds), and the proposed cryptographic algorithm. After encryption, the resulting cryptograms were truncated to a size of 1 MB and tested with the NIST stochastic test suite. A set of tests was considered passed if all tests from the set were passed. The results of the experiment are presented in the Table 1. In the Table 1, the information shown is interpreted as the number of cryptograms that did not pass the NIST test suite / the total number of cryptograms.

Table 1

Results of experimental testing of the developed graphic information encryption algorithm

The proposed cryptographic algorithm(2 rounds) *Failed / Total number*	AES(2 rounds) *Failed / Total number*	AES(14 rounds) *Failed / Total number*
56/250	61/250	47/250

Analysis of the data presented in the Table 1 allows us to conclude about the significant effectiveness of the proposed cryptographic algorithm for encrypting graphic information, which is sufficient for most practical applications. Although more cryptograms pass the NIST test suite when applying AES with 14 rounds, it should be noted that 14 rounds involve a large amount of computation, while the proposed cryptographic algorithm involves only 2 rounds of the SP network.

Conclusions. Let's note the main results of the research performed:

1. Common use of graphic information in modern cyberspace, combined with the widespread use of resource-constrained devices, in particular IoT devices, IoBT devices, mobile platforms, leads to the high importance of the issue of developing high-speed cryptographic algorithms for encrypting graphic information.

2. In this paper we propose an algorithm for encrypting graphic information based on a Hyper-Chaotic Modified Robust Logistic Map, as well as an SP network, which includes an S-box based on a Galois field transform, as well as a P-box based on a permutation, synthesized using the Nyberg construction.

3. Testing of cryptograms obtained using the developed cryptographic algorithm using a NIST stochastic tests suite shows that it allows to ensure a sufficient level of information protection while requiring only two rounds.

References

1. FIPS 197. Advanced encryption standard. 2001. URL: http://csrc.nist.gov/publications/
2. Kumari M., Gupta S., Sardana P. A survey of image encryption algorithms. *3D Research*. 2017. Vol. 8. P. 1-35.
3. Poincare H. J. Les methodes nouvelles de la mecanique celeste (Gauthiers-Villars, Paris, 1892, 1893, 1899). V. 1–3. [English translation edited by D. Goroff. New York: American Institute of Physics, 1993].
4. Zhang Y. The fast image encryption algorithm based on lifting scheme and chaos. *Information sciences*. 2020. V. 520. P. 177-194.
5. Pourasad Y., Ranjbarzadeh R., Mardani A. A new algorithm for digital image encryption based on chaos theory. *Entropy*. 2021. V. 23, No. 3. 341.
6. Luo Y. et al. A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*. 2019. V. 78. P. 22023-22043.
7. He Y. et al. A new image encryption algorithm based on the OF-LSTMS and chaotic sequences. *Scientific reports*. 2021. V. 11, 6398.
8. Irfan M. et al. Pseudorandom number generator (PRNG) design using hyper-chaotic modified robust logistic map (HC-MRLM*). Electronics*. 2020. V. 9. No. 1. 104.
9. Bakunina O.V., Balandina N.M., Sokolov A.V. Synthesis Method for S-boxes Based on Galois Field Transform Matrices. *Ukrainian Journal of Information Technology*. 2023. V.5, No 2. P. 41–48.

10. Zhdanov O.N., Sokolov A.V. Extending Nyberg construction on Galois fields of odd characteristic. *Radioelectronics and Communications Systems*. 2017. V. 60, No. 12. P. 538-544.
11. A statistical test suite for random and pseudorandom number generators for cryptographic applications. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology, 2000. 153 p.
12. NRCS Photo Gallery. United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/

АЛГОРИТМ ШИФРУВАННЯ ГРАФІЧНОЇ ІНФОРМАЦІЇ НА ОСНОВІ ХАОТИЧНОГО ПЕРЕТВОРЕННЯ І GF-ПЕРЕТВОРЕННЯ

О.О. Палагін, А.В. Соколов

Національний університет «Одеська політехніка»
1 Шевченка пр., Одеса, 65044, Україна
email: radiosquid@gmail.com

Сучасний етап розвитку інформаційних технологій характеризується суттєвим збільшенням обсягів мультимедійної інформації, зокрема, цифрових зображень при повсюдному впровадженні ресурсообмежених платформ, таких, як пристрої IoT, IoBT, мобільні пристрої та вбудовані системи. Зазначене обумовлює актуальність завдання розробки алгоритмів шифрування графічної інформації, які були б здатні забезпечити високу ефективність шифрування інформації за найменшу кількість обчислювальних операцій. На сьогодні для розробки таких криптографічних алгоритмів найчастіше застосовується теорія динамічного хаосу. Тим не менш остаточно оптимальної структури криптографічного алгоритму для шифрування зображень на сьогодні ще не створено. У даній роботі запропоновано комбінацію переваг традиційних SP мереж та генератора гами на основі гіперхаотичної модифікованої стійкої логістичної карти для побудови ефективного алгоритму шифрування зображень, що здатний забезпечити високий рівень стійкості. У запропонованому криптографічному алгоритмі застосовуються високоякісні S-блоки на основі GF-перетворення, а також P-блоки на основі перестановок, що згенеровані із застосуванням конструкції Ніберг, при цьому застосовується сегментація і подальша обробка тривимірних блоків зображень, що дозволяє збільшити ефект дифузії. Проведені в рамках роботи численні тести стохастичної якості криптограм, отриманих із застосуванням розробленого криптографічного алгоритму, а також їх порівняння із результатами, отриманими для криптографічного алгоритму AES дозволили встановити, що розроблений криптографічний алгоритм дозволяє забезпечити достатній рівень захисту інформації, при цьому вимагає всього два раунди основного кроку криптоперетворення. Отже, розроблений криптографічний алгоритм для шифрування графічної інформації може бути рекомендований для практичного застосування, зокрема, на ресурсообмежених платформах.

Ключові слова: криптографічний алгоритм, шифрування зображень, динамічний хаос, гіперхаотична модифікована стійка логістична карта, S-блок на основі GF-перетворення, конструкція Ніберг.