ICST
Information Control Systems
and Technologies

Монография

# Актуальные проблемы информационных систем и технологии

Информационные системы управления

Интеллектуальные системы и анализ данных

Моделирование и разработка программ

ОДЕССКИЙ НАЦИОНАЛЬНЫЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

# АКТУАЛЬНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

МОНОГРАФИЯ

ОДЕССА 2020

УДК 681.518.54
А43

***Авторский коллектив*:**

Борисова Н., Васянин В., Волошин В., Волошинов С., Вольская О., Востров Г., Вычужанин В., Гобов Д., Гоменюк С. І., Гришин С., Дрозд А., Дрозд Ю., Журиленко Б., Защелкин К., Заяц Ю., Кораблев Н., Красиленоко В., Кузнецов Н., Лазарев А., Лисецкий Ю., Мартынюк А., Межуєв В. І., Мельник К., Мироненко Д. Ю., Михайлов С., Николаев К., Опиата Р., Петров И., Поворознюк А., Поворознюк О., Постан М., Рудниченко Н., Ситников В., Стрельцов О., Ступень П., Теплечук А., Трофимчук А., Ухіна Г., Ушакова Л., Федосова И., Филатова А., Фомичев А., Чуприна А., Чупринка В., Чупринка Н., Шибаев Д., Шибаева Н., Шинкевич Е.

***Рецензенты*:**

*ГОВОРУЩЕНКО Татьяна,* доктор технических наук, профессор, Хмельницкий национальный университет (Украина);

*ПАКСТАС Альгирдас,* доктор технических наук, профессор, институт математики и информатики (Великобритания);

*ЦАРЕВ Александр*, доктор технических наук, профессор, Западно-Поморский технологический университет (Польша).

*Рекомендовано в печать ученым советом*
*Одесского национального политехнического университета*
*(протокол № 1 от 30.09.2020 г.)*

А43 **Актуальные** проблемы информационных систем и технологий: монография / Н. Борисова, В. Васянин и др.; под науч. ред. проф. В. Вычужанина. – Одесса: НУ «ОМА», 2020. – 296 с.:ил., табл. (укр., рус., англ. языками).
ISBN 978-617-7857-03-6

В монографии отражены результаты научных исследований в области информацйионных систем управления, интеллектуальных систем и анализа данных, моделирования и разработки программ. Материалы монографии будут полезными для аспирантов, магистрантов, преподавателей высших учебных заведений, специализирующихся в области IT-технологий.

УДК 681.518.54

ISBN 978-617-7857-03-6

UDC 004.056.55: 004.032: 004.93

# THE BLOCK PARAMETRIC MATRIX AFFINE-PERMUTATION CIPHERS (BP_MAPCs) WITH ISOMORPHIC REPRESENTATIONS AND THEIR RESEARCH

**Ph.D. Krasilenko V.G.**[0000-0001-6528-3150]**, Ph.D. Lazarev A.A.**[ 0000-0003-1176-5650]**, Nikitovich D.V.**[0000-0002-8907-1221]

*Vinnytsia National Technical University, Khmelnytske shoes, 95, Vinnytsia, 21021,* Ukraine

*krasvg@i.ua*

**Abstract.** First, we will give a brief overview of the proposed multifunctional block parametric MAPSs, their subspecies of vector affine permutation ciphers (VAPSs), and show that to achieve the goal it is advisable to use the isomorphism of various representations of permutations (matrices or vectors), which act as the main and block-wise, vector matrix keys. Modeling confirms the adequacy of the proposed block parametric ciphers (MAPS) with isomorphic representations of the MP of significant dimensions and blocks and their good characteristics, their advantages, including increased stability and enhanced functionality. The processes of crypto-transformations, generation of MP, main MP and turn-key processes, their advantages are clearly shown by a number of model experiments. The models are simple, convenient, adapted for multi-format and color images, implemented by matrix processors, have high efficiency, stability, and speed.

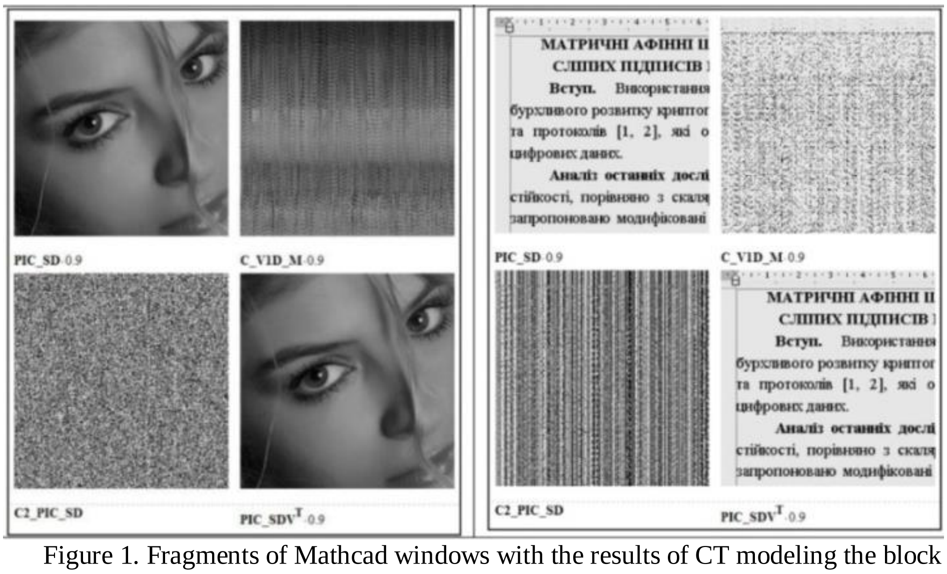
**Keywords**: block parametric matrix affine permutation cipher, vector affine permutation cipher, isomorphism of various representations, simulation, matrix processor, matrix key, encrypted, decrypted, methods of image crypto-processing.

## 1. Introduction, analysis of recent publications, formulation of the problems

In the era of electronic communications, the need to transmit and cryptographic transformations (CTs) specific text and graphic documents (TGDs) in the form of table data, 2-D, 3-D, 4-D arrays, drawings, diagrams, resolutions has essentially increased [1-7]. In identification, biometric systems, intelligent management it is necessary to transmit in encrypted form a large number of various images. Many TGDs contain restricted access information that should be reported to government agencies, in a timely manner and in encrypted form, to transmit over communication channels, providing only authorized access, to certify their digital signatures. Authorized access many resources can be provided with appropriate technologies of cryptography and measures with the issuance of certificates and access keys. For such security purposes, methods and tools for CTs of images [1-22] and procedures and protocols for the formation of keys and their exchange [1, 8, 19, 23-24] are used, but among their variety [1-7, 22] only a small part is devoted to methods and algorithms oriented on matrix models [24-31] and tools. At the same time, the emergence of parallel matrix (image-type) processors [3, 21] contributed to the reorientation in the study of image CTs and the creation and models of matrix type (MT) [24-34]. That is why the search and research of new matrix models (MM) of CT, improvement of existing matrix ciphers and means for their realization are an actual strategic task. In works [25, 26] more generalized matrix algorithms for CTs of images and so-called matrix affine-permutation ciphers (MAPCs) [28] based on of more generalized matrix affinity ciphers (MACs), as modifications of known affine ciphers [27], were proposed. The results of simulation [24-27] of processes of CTs of color images [31] on the basis of such models have shown their significant advantages such as: greater stability, increase in speed. In work [26] on the basis of MACs the algorithm and the procedure for creating a digital blind signature (DBS) is proposed on the TGD, and the results of simulation. The results of modeling algorithms for creating a 2D key are also known [23]. Paper [24] is devoted to creation of DBS on TGD, but on the basis of other models of matrix type. One of the main components of MAPCs [28], is matrix permutation model (MM_P), which has obvious simplicity. Further application and improvement of matrix-type ciphers based on such MM_P is highlighted in papers [29, 30, 32, 33]. Their basic operations are elemental multiplication, matrix addition and matrix permutation models (MM_P) with multiplication matrices. But the disadvantage of these works is the large size of the matrix keys (MK) and the lack of demonstration of their effective work with blocks in the form of matrices, which split multi-page data. However, as shown in papers [29, 30], the CTs on their basis, without additional operations, do not modify histograms of TGDs. At the same time, for most of the above-mentioned works, there is a common significant disadvantage, especially for work related to MAC [27, 31], MAPCs [28] and the like [24-26, 30, 32-34], which requires the use of at least two MK, if implemented in models multiplicative and additive matrix components. Therefore, the search to improve especially the multi-step MAC, MAPCs [28] while maintaining stability and other characteristics, in order to reduce the number of MKs to one, and their experimental verification is a necessary urgent task. The emergence of parallel algorithms, and especially the matrices of multiprocessor means, requires the creation of appropriate matrix-algebraic models (MAM), matrix-type systems (MT) for CT. The promise of the MAM, its modifications for the CT is evidenced by the ability to check the integrity of the cryptograms and the presence of distortions in them [32, 34], increasing the crypto-stability and expanding their functionality for very specific characteristic histograms of scanned TGDs, as experimentally shown in [35]. The generalization of the MAM to a matrix-block view is necessary in terms of the versatility of block algorithms and independence on data volumes. Thus, the actual purpose of this section is the development of block modifications of the MAPCs with a minimum length of 2048 bits, with the possibility of choosing its parameters and cyclic or block keys of similar length, their simulation on real information objects (IO) and demonstration, evaluation of their advantages, characteristics and durability, application possibilities.

## 2. Presentation of research results

The CT algorithm for encryption based on BP_MAPCs consists of the following steps: 1) the partition of IO into blocks in the form of matrices with a dimension $2^m x 2^m$, where m = 4, 5, 6, ... and with element-bytes in a digital format that at m = 4 is equivalent to the length of the block 256x8 = 2024 bits; 2) the permutation of the bytes of each current block using the current key, which is formed synchronously from the main key by the selected procedure according to the parametric model, the argument of which is index of block, 3) matrix affine/affine-permutation transformations (MAPTs) of bytes in block using the current key, the same as on stage 2 or similar, but according to another parametric model, 4) concatenation of received blocks for formation of cryptogram of IO. The decryption process has the following steps: 1) decomposing the cryptograms on blocks, 2)  using MAPT for reversing of blocks based on the reversed current keys; 3) reversing the permutation of the bytes of blocks by current keys (vectors); 4) concatenating the transformed blocks into the restored IO. The steps of permutations and affine transformations can change and repeat in different sequences. Modeling of block parametric MAPC was done with Mathcad. Windows with formulas for modeling the CT of the image by the algorithm of block MAPTs are shown in Fig. 1-14. In the first experiment, a random permutation bitmap KPX (256x256x1) generated in any way is used to rearrange bytes in each kp-th block. The block is represented by 256 component VID vectors (C_VID) or C_M_V (16x16) with 8-bit levels matrices, and KPX cards are also isomorphically represented by vectors or matrices in the same format. This allows you to use them as keys for affine conversions. Current MK can be uniquely represented in the form of a matrix of M_V (16x16) bytes, which is either its parametric model and is used in the next stage. The essence of MAPT is to apply to blocks, as a collection of bytes (PIC_S, PIC_Doc images), procedures pixel by pixel modulo multiplication or additions by the corresponding 8-bit MKs (direct or inverse) of the same dimensions (KeyA, KeyAO or KeyM (qa), KeyMO(qo)), depending on the parameters and formation modules, which are shown in Fig. 2, 7, 9. As can be seen from Fig. 1, the simulation results of the processes of direct and reverse CT TGDs and images elements are confirmed the correct work of the models.

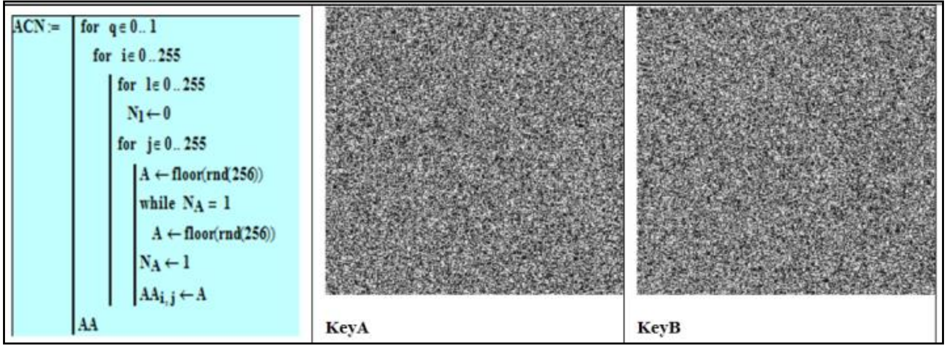


МАТРИЧНІ АФІННІ П
СЛІПИХ ПІДПИСІВ
**Вступ.** Використання
бурхливого розвитку криптог
та протоколів [1, 2], які о
цифрових даних.
**Аналіз останніх дослі**
стійкості, порівняно з скаля
запропоновано модифіковані

МАТРИЧНІ АФІННІ П
СЛІПИХ ПІДПИСІВ
**Вступ.** Використання
бурхливого розвитку криптог
та протоколів [1, 2], які о
цифрових даних.
**Аналіз останніх дослі**
стійкості, порівняно з скаля
запропоновано модифіковані

Figure 1. Fragments of Mathcad windows with the results of CT modeling the block MAPC for block wich16x16 bytes.

The cryptographic blocks processing is accompanied by the simultaneous mixing of their elements and their subsequent replacements, but, as it was shown by researches with histograms of images, TGDs and their cryptogram, shown in Fig. 1, for TGDs, in contrast to the image of a person, several iterative multiplications of the data (MD) on the MK P or permutations to may not be sufficient, especially with the application of the same MK. Therefore, in order to improve the algorithm, we propose applying various current MKs to blocks and increasing the dimension of MK and blocks do 256x256 bytes. Thus, the idea and essence of parametric block MAP-ciphers of CTs consists in using the functional dependencies of their parameters on block indices and additional scalar-vector keys (VK). In this case, the MP in the generally accepted form should be square with N x N elements ("0" or "1"), where N = $2^{16}$. The power of the set of possible such MPs, that is, their number is estimated as N!, which gives huge values. But each byte address of a block can be represented using two bytes, indicate two coordinates (row and column) of the block. This enables us to represent any permutation with two blocks (256 x 256 elements) of bytes, putting in each identical address of these blocks the corresponding high byte (in the first block) and the least significant byte (in the second block) the coordinates of the new address of the byte selected for permutation. Show The Mathcad software module for generating the base (main) MK (MP) and the type of its components KeyA and KeyB in the format of two gray images is shown in Fig. 2. The histograms of images, keys, its cryptograms after each CT affine components of this MP are shown in Fig. 3.



```
ACN := for $q \in 0..1$
         for $i \in 0..255$
           for $l \in 0..255$
             $N_l \leftarrow 0$
           for $j \in 0..255$
             $A \leftarrow floor(rnd(256))$
             while $N_A = 1$
               $A \leftarrow floor(rnd(256))$
             $N_A \leftarrow 1$
             $AA_{i,j} \leftarrow A$
       AA
```

Fig. 2. The program module for the generation of the basic (head) MK (MP) and KeyA and KeyB warehouse views in the format of two black-and-white images (Mathcad window).

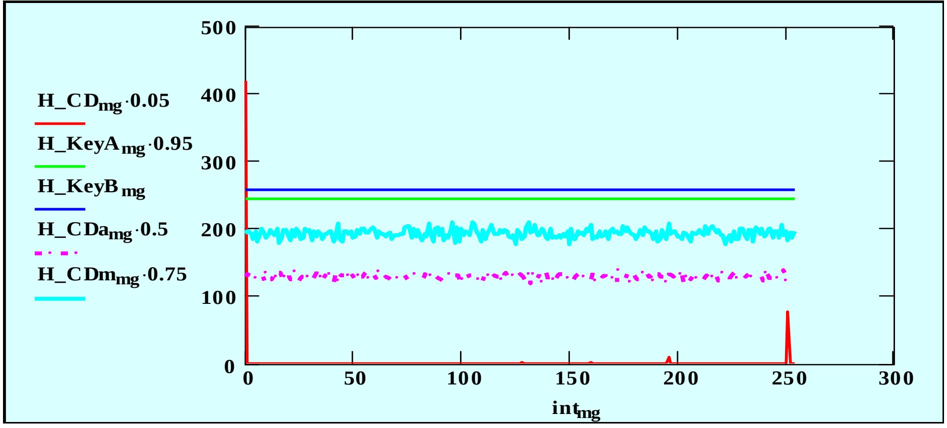
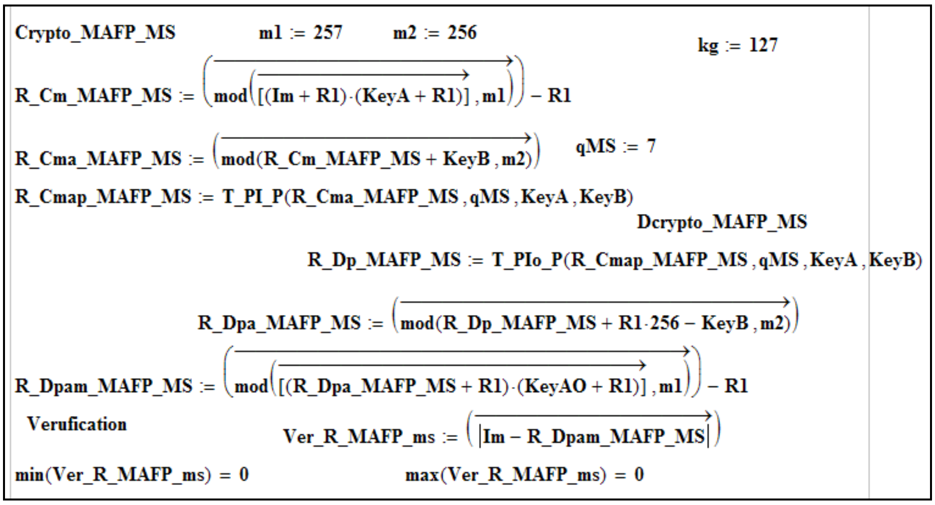


Fig. 3. Histograms H_KeyA and H_KeyB respectively components KeyA and KeyB MP, histogram H_CD after only permutation cryptogram explicit Im after only permutation (coincides with histogram Im), corresponding histograms H_CDa and H_CDm cryptograms after additive and multiplicative affine CT using the same KeyA and KeyB.



Crypto_MAFP_MS $\quad m1 := 257 \quad m2 := 256 \quad kg := 127$

$$\text{R\_Cm\_MAFP\_MS} := \left(\overrightarrow{\text{mod}\left(\overrightarrow{[(\text{Im}+\text{R1})\cdot(\text{KeyA}+\text{R1})]}, \text{m1}\right)}\right) - \text{R1}$$

$$\text{R\_Cma\_MAFP\_MS} := \left(\overrightarrow{\text{mod}(\text{R\_Cm\_MAFP\_MS}+\text{KeyB}, \text{m2})}\right) \qquad \text{qMS} := 7$$

$$\text{R\_Cmap\_MAFP\_MS} := \text{T\_PI\_P}(\text{R\_Cma\_MAFP\_MS}, \text{qMS}, \text{KeyA}, \text{KeyB})$$

Dcrypto_MAFP_MS

$$\text{R\_Dp\_MAFP\_MS} := \text{T\_PIo\_P}(\text{R\_Cmap\_MAFP\_MS}, \text{qMS}, \text{KeyA}, \text{KeyB})$$

$$\text{R\_Dpa\_MAFP\_MS} := \left(\overrightarrow{\text{mod}(\text{R\_Dp\_MAFP\_MS}+\text{R1}\cdot 256-\text{KeyB}, \text{m2})}\right)$$

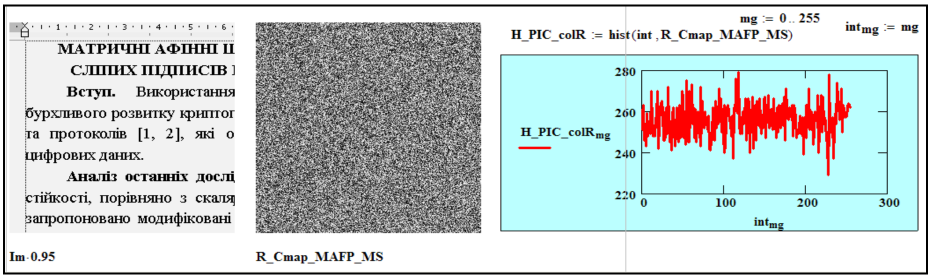
$$\text{R\_Dpam\_MAFP\_MS} := \left(\overrightarrow{\text{mod}\left(\overrightarrow{[(\text{R\_Dpa\_MAFP\_MS}+\text{R1})\cdot(\text{KeyAO}+\text{R1})]}, \text{m1}\right)}\right) - \text{R1}$$

Verufication

$$\text{Ver\_R\_MAFP\_ms} := \left(\overrightarrow{|\text{Im}-\text{R\_Dpam\_MAFP\_MS}|}\right)$$

$$\min(\text{Ver\_R\_MAFP\_ms}) = 0 \qquad \max(\text{Ver\_R\_MAFP\_ms}) = 0$$

Figure 4. A fragment of the Mathcad window with parametric models (formulas) of forward and reverse cryptographic transformations (pixel-by-pixel affine encryption / decryption and multiple permutations of block byte-pixels) and model verification formulas.



**МАТРИЧНІ АФІННІ П**
**СЛІПИХ ПІДПИСІВ І**
**Вступ.** Використання
бурхливого розвитку криптог
та протоколів [1, 2], які о
цифрових даних.
**Аналіз останніх дослі**
стійкості, порівняно з скаля
запропоновано модифіковані

Figure 5. Fragments of Mathcad windows with the results of the simulation of cryptographic image Im conversion using BP_MAPC: the original image (block), its cryptogram, and histogram of cryptogram.

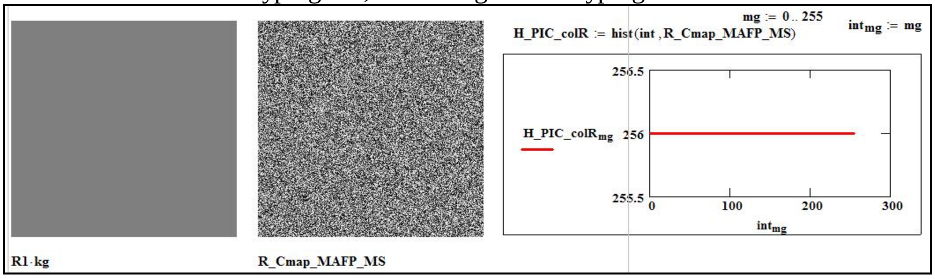
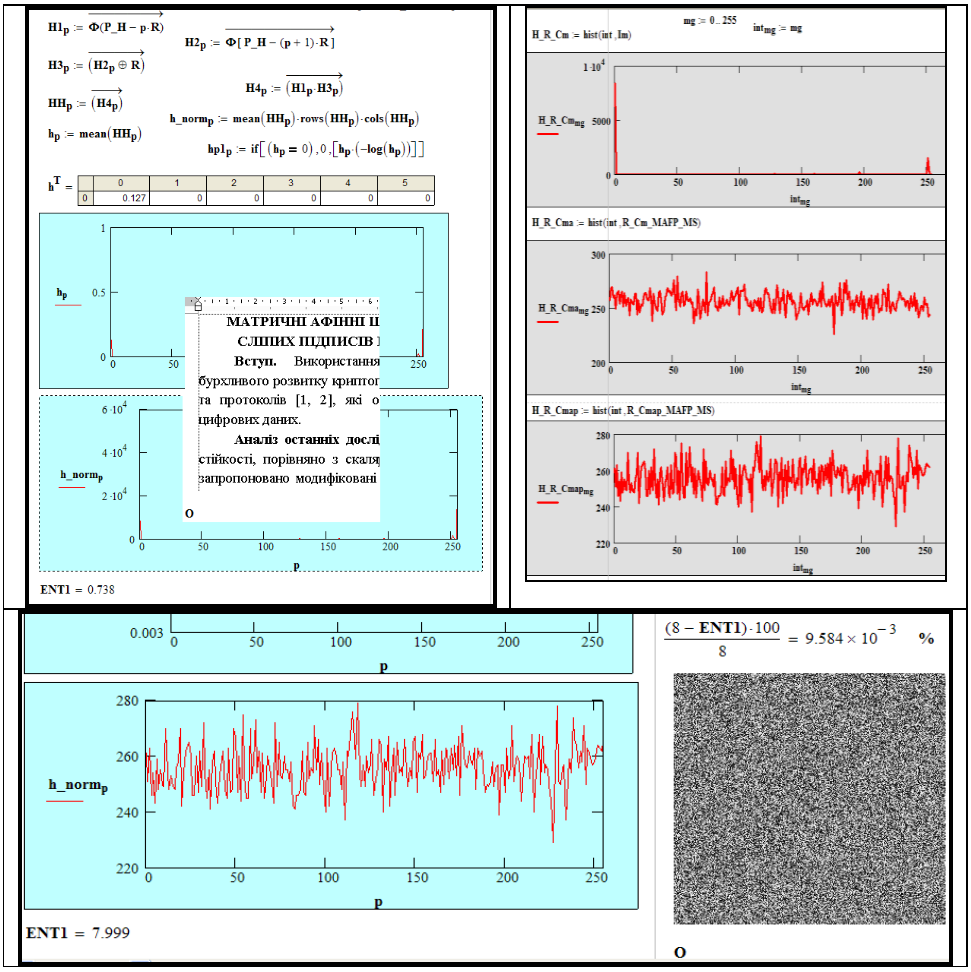


Figure 6. Fragments of Mathcad windows with the results of the simulation of cryptographic single-level image R1 conversion using BP_MAPC: the original image (block), its cryptogram, and histogram of cryptogram.



$H1_p := \overrightarrow{\Phi(P\_H - p \cdot R)}$

$H2_p := \overrightarrow{\Phi[P\_H - (p+1) \cdot R]}$

$H3_p := \overrightarrow{(H2_p \oplus R)}$

$H4_p := \overrightarrow{(H1_p \cdot H3_p)}$

$HH_p := \overrightarrow{(H4_p)}$

$h\_norm_p := mean(HH_p) \cdot rows(HH_p) \cdot cols(HH_p)$

$h_p := mean(HH_p)$

$hp1_p := if[(h_p = 0), 0, [h_p \cdot (-log(h_p))]]$

$h^T =$

|   | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0.127 | 0 | 0 | 0 | 0 | 0 |

МАТРИЧНІ АФІННІ П

СЛІПИХ ПІДПИСІВ І

**Вступ.** Використання бурхливого розвитку криптог та протоколів [1, 2], які о цифрових даних.

**Аналіз останніх дослі** стійкості, порівняно з скаля запропоновано модифіковані

ENT1 = 0.738

$mg := 0..255$ $\quad int_{mg} := mg$

H_R_Cm := hist(int , Im)

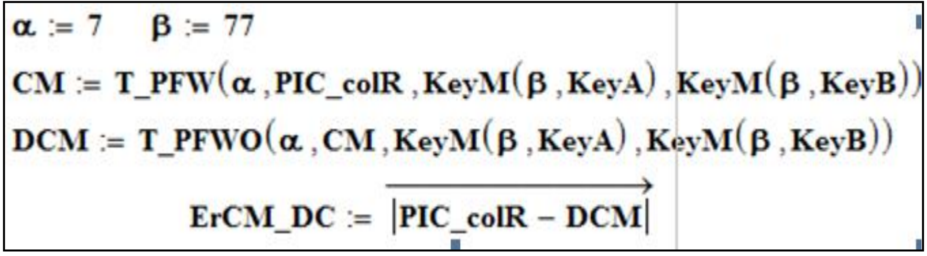
H_R_Cma := hist(int , R_Cm_MAFP_MS)

H_R_Cmap := hist(int , R_Cmap_MAFP_MS)

ENT1 = 7.999

$\frac{(8 - ENT1) \cdot 100}{8} = 9.584 \times 10^{-3}$ %

Figure 7. Fragments of Mathcad windows with modules and formulas for calculating the entropy of image pixels and plotting a histogram



$\alpha := 7 \quad \beta := 77$

$CM := T\_PFW(\alpha, PIC\_colR, KeyM(\beta, KeyA), KeyM(\beta, KeyB))$

$DCM := T\_PFWO(\alpha, CM, KeyM(\beta, KeyA), KeyM(\beta, KeyB))$

$ErCM\_DC := \overrightarrow{|PIC\_colR - DCM|}$

Figure 8. Fragment of a Mathcad window with parametric models (formulas) of forward and reverse cryptographic transformations (multiple permutations of block bytes and pixels) and the formation of a stream-MK (larger-dimensional permutation) in an isomorphic representation, and model verification formula.

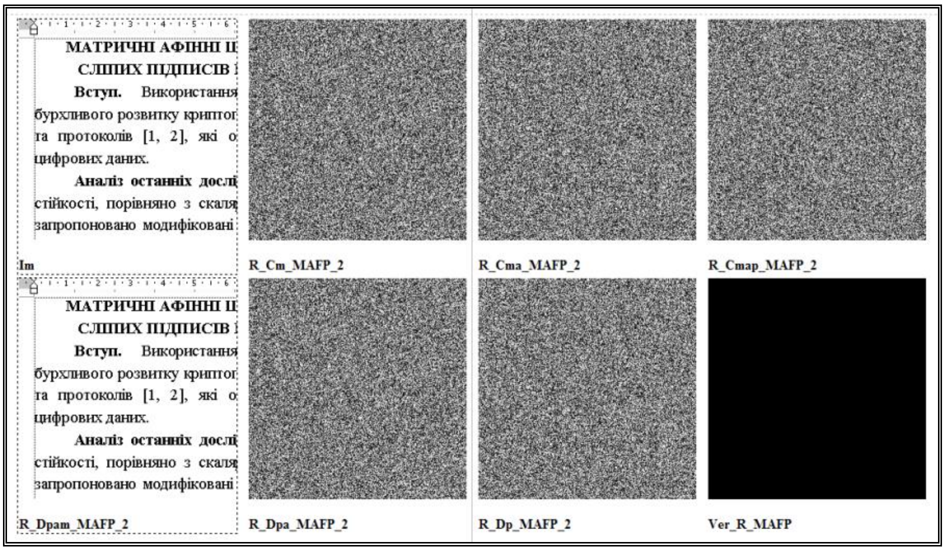
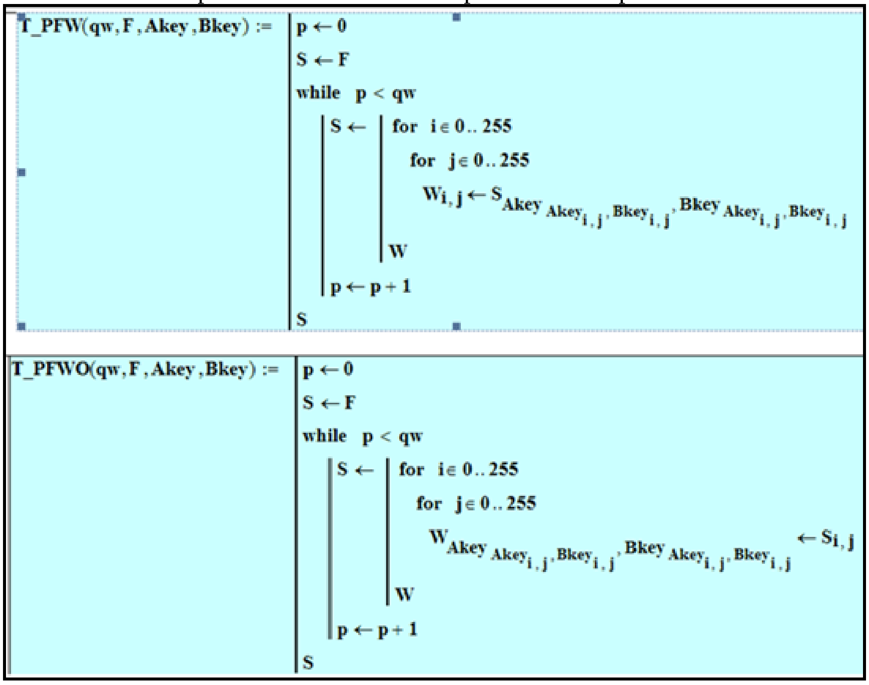


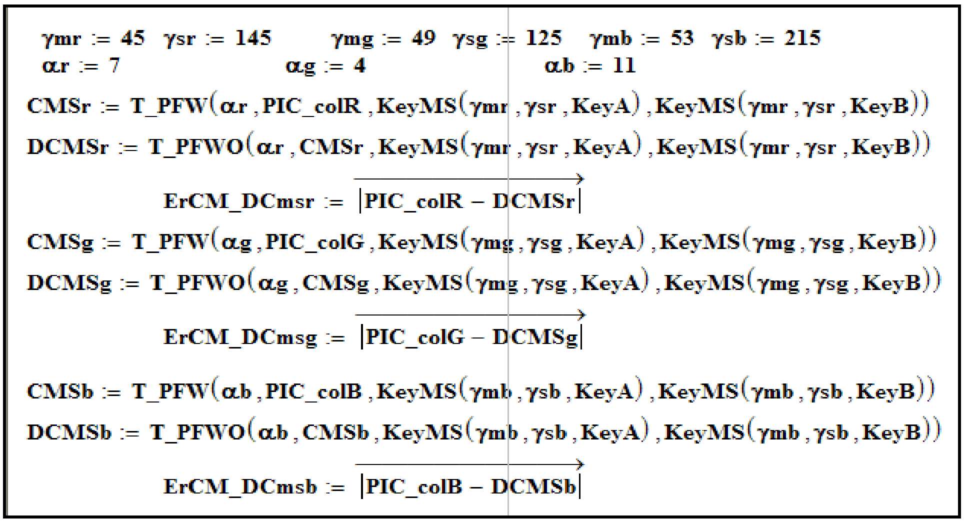
Figure 9. Fragment of a Mathcad window with the results of simulation of direct and reverse cryptographic transformations of a block in the form of a gray image with a block parametric matrix affine permutation cipher.



```
T_PFW(qw, F, Akey, Bkey) :=  p ← 0
                             S ← F
                             while  p < qw
                                S ←  for  i ∈ 0..255
                                        for  j ∈ 0..255
                                           $W_{i,j} \leftarrow S_{Akey_{Akey_{i,j},Bkey_{i,j}},\,Bkey_{Akey_{i,j},Bkey_{i,j}}}$
                                     W
                                p ← p + 1
                             S
```

```
T_PFWO(qw, F, Akey, Bkey) :=  p ← 0
                              S ← F
                              while  p < qw
                                 S ←  for  i ∈ 0..255
                                         for  j ∈ 0..255
                                            $W_{Akey_{Akey_{i,j},Bkey_{i,j}},\,Bkey_{Akey_{i,j},Bkey_{i,j}}} \leftarrow S_{i,j}$
                                      W
                                 p ← p + 1
                              S
```

Figure 10. Fragment of a Mathcad window with parametric program modules of forward and reverse cryptographic transformations (qw-multiple permutations of block F bytes and pixels) and stream-MKs (larger-dimensional permutation) Akey, Bkey in an isomorphic representation.



$$\gamma mr := 45 \quad \gamma sr := 145 \qquad \gamma mg := 49 \quad \gamma sg := 125 \qquad \gamma mb := 53 \quad \gamma sb := 215$$

$$\alpha r := 7 \qquad \alpha g := 4 \qquad \alpha b := 11$$

$$CMSr := T\_PFW(\alpha r, PIC\_colR, KeyMS(\gamma mr, \gamma sr, KeyA), KeyMS(\gamma mr, \gamma sr, KeyB))$$

$$DCMSr := T\_PFWO(\alpha r, CMSr, KeyMS(\gamma mr, \gamma sr, KeyA), KeyMS(\gamma mr, \gamma sr, KeyB))$$

$$ErCM\_DCmsr := \overrightarrow{|PIC\_colR - DCMSr|}$$

$$CMSg := T\_PFW(\alpha g, PIC\_colG, KeyMS(\gamma mg, \gamma sg, KeyA), KeyMS(\gamma mg, \gamma sg, KeyB))$$

$$DCMSg := T\_PFWO(\alpha g, CMSg, KeyMS(\gamma mg, \gamma sg, KeyA), KeyMS(\gamma mg, \gamma sg, KeyB))$$

$$ErCM\_DCmsg := \overrightarrow{|PIC\_colG - DCMSg|}$$

$$CMSb := T\_PFW(\alpha b, PIC\_colB, KeyMS(\gamma mb, \gamma sb, KeyA), KeyMS(\gamma mb, \gamma sb, KeyB))$$

$$DCMSb := T\_PFWO(\alpha b, CMSb, KeyMS(\gamma mb, \gamma sb, KeyA), KeyMS(\gamma mb, \gamma sb, KeyB))$$

$$ErCM\_DCmsb := \overrightarrow{|PIC\_colB - DCMSb|}$$

Figure 11. Window with parametric models of forward and reverse CTs of color image (multiple permutations) and of stream-MKs formation in an isomorphic representation and with parameters and verification formulas.

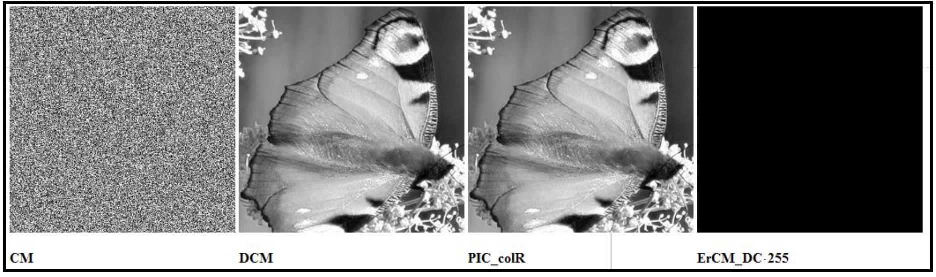


Figure 12. The result of direct and reverse CT of block, in form of gray image PIC_colR, using models of multiple permutations in Fig.7.

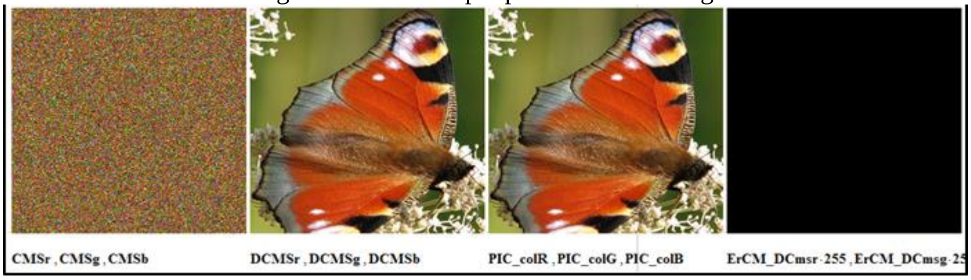

CMSr , CMSg , CMSb
DCMSr , DCMSg , DCMSb
PIC_colR , PIC_colG , PIC_colB
ErCM_DCmsr·255 , ErCM_DCmsg·25

Figure 13. The simulation results of direct and reverse CTs of color image, using parametric models of multiple permutations in Fig.10.

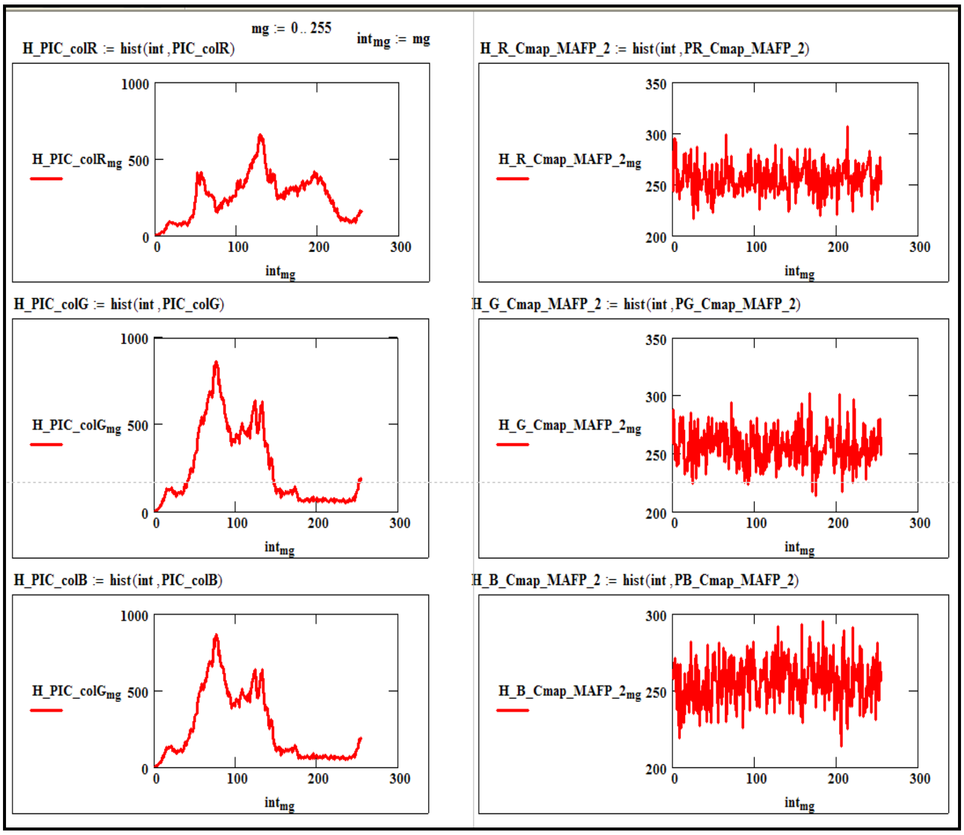


Figure 14. Histograms of components of color image (left) and histograms their cryptograms, obtained using the BP_MAPC models in Fig.3.

The analysis of histograms before and after the CT confirms that the proposed models give better results. The TGD entropy was 0.738, and the cryptogram entropy increased 10.6–10.8 times and became equal to 7.82-7.999. The entropy of cryptogram has become almost equal to 8 bits per element: 7,999 (- 0.009 %!). Without knowledge of MK it is impossible to restore MD and, as was shown in [26, 28], already with a dimension of 32x32 MK of type **P**, the stability is ensured, and with dimension 256x256 8-bit elements of key, gives a substantial gain (the power of keys set is estimated $256^2$ !!). The power of the set of possible keys has increased by many orders of magnitude!! Therefore, stability has increased significantly. For MAM, it is urgently necessary to form a whole series of permutation matrices (MP) from the main MK, which would satisfy a number of requirements. In works [36, 37], only the main MK of the general type was considered, but not the MP series, the aim of the work is to study the processes of formation of the MP flow for CTs of images, and to check their properties. And in [38], questions were considered of creating by the parties a secret main MK of type P with isomorphic representations and the synthesis of a number of sub-keys of a similar type from it, therefore they are not considered in detail here, but will be covered in the report.

## 3. Conclusion

New block parametric matrix-algebraic models and matrix affine-permutation ciphers for CTs are proposed and modulated. The results of their modeling are presented using direct and inverse CT scans over images as an example, which indicates their correct operation and effectiveness. The entropy-histogram analysis of the obtained cryptograms, the advantages of the proposed modifications of ciphers with an increased permutation matrix are shown. The aspects of creating existing MKs are considered. Models can be implemented on matrix processors and have high speed, stability of transformations, and are more resistant to attacks.

## References

1. Yemets V. Modern cryptography. Basic concepts / V. Yemets, A. Melnyk, R. Popovich. - Lviv: Baku, 2003. - 144 p.
2. Khoroshko V.O. Methods and means of information protection: Teaching. manual / V.O. Khoroshko, A.O. Chetkov - K .: Junior, 2003. - 502 p.
3. Korkishko T.A. Algorithms and Processors of Symmetric Block Encryption: Scientific Edition / T.A. Korkishko, A.O. Melnik, V.A. Melnik. - Lviv: Baku, 2003. - 168 p.
4. Rashkevich Yu.M. Affine transformations in modifications of the RSA image encryption algorithm / Yu.M. Rashkevich, A.M. Kovalchuk, D.D. Peleshko // Automatics. Electrotechnical complexes and systems. - 2009. - No. 2 (24). - pp. 59-66.
5. Deergha Rao K. A New and Secure Cryptosyce for Image Encryption and Decryption / K. Deergha Rao, K. Praveen Kumar, P.V. Murali Krishna // IETE Journal of research. - 2011. - Vol. 57. - Issue 2. - pp. 165-171.
6. Han Shuihua. An Asymmetric Image Encryption Based on Matrix Transformation / Han Shuihua, Yang Shuangyuan // Ecti Transactions on Computer and Information Technology. - 2005 - Vol.1, No.2. - pp. 126-133.
7. Chin-Chen Chang. A new encycle algorithm for image cryptosystems / Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen // Journal of Systems and Software. - 2001. - No. 58. - pp. 83-91.
8. Diffie, W., Hellman, M.E.: New Directions in Cryptography. IEEE Transactions on Information Theory. Volume IT-22, Issue 6: 644 - 654 (1976).
9. Alvarez, G., Encinas, L.H., de-Rey, A. M.: A multi-secret sharing scheme for color images based on cellular automata. Inf. Sci. **178**, 4382–4395 (2008).
10. Muñoz-Rodríguez, J.A., Rodríguez-Vera R.: Image encryption based on moiré pattern performed by computational algorithms. Optics Communication 236 (4–6), 295–301 (2004).
11. Muñoz-Rodríguez, J.A., Rodríguez-Vera R.: Image encryption based on a grating generated by a reflection intensity map. J. Mod. Opt. 52, 1385–1395 (2005).
12. Zhang, Y., Xiao D.: An image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Commun. Nonlinear Sci. Numer. Simul. 19 (1), 74–82 (2014).
13. Laiphrakpam, D.S., Khumanthem, M.S.: A robust image encryption scheme based on chaotic system and elliptic curve over finite field. Multimedia Tools Appl. 77(7), 1–24 (2017).
14. Zhang, W., Yu, H., Zhao, Yl, Zhu, Zl: Image encryption based on three-dimensional bit matrix permutation. Sig. Process. 118, 36–50 (2016).

15. Pak, C., Huang L.: A new color image encryption using combination of the 1-D chaotic map. Signal Process. 138, 129–137 (2017).

16. Wu, J., Liao, X., Yang, B.: Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation. Signal Process. 142, 292–300 (2018).

17. Wang, H., Xiao, D, Chen, X, Huang, H.: Cryptanalysis and enhancements of image encryption using combination of the 1-D chaotic map. Signal Process. 144, 444–452 (2018).

18. Li, C.: Cracking a hierarchical chaotic image encryption algorithm based on permutation. Signal Process. 118, 203–210 (2016).

19. Sava, D., Vlad, A., Tataru, R.: A new type of keystream generator based on chaotic maps: illustration on a Hénon generalized map. IEEE Int. Conf. on Communications (COMM 2014), 551–557 (2014).

20. Wang, Y., Lei, P., Yang, H.Q., Cao, H.Y.: Security analysis on a color image encryption based on DNA encoding and chaos map. Comput. Electr. Eng. **46**, 433–446 (2015).

21. Krasilenko V.G. Algorithms and architecture for high-precision matrix-matrix multipliers based on optical four-digit alternating arithmetic / V.G. Krasilenko // Measuring and computing engineering in technological processes. - 2004. - №1. - pp. 13-26.

22. Krasilenko V.G. A noise-immune crptographis information protection method for facsimile information transmission and the realization algorithms / V.G. Krasilenko, A.I. Nikolsky, V. F. Bardaschenko // Proc. SPIE, 2006. - Vol. 6241. - pp. 316-322.

23. Krasilenko V.G. Algorithms for the formation of two-dimensional keys for matrix algorithms of cryptographic transformations of images and their modeling / V.G. Krasilenko, V. I. Yatskovsky, R. A. Yatskovskaya // Systems of information processing. - 2012. - Exp. 8. - pp. 107-110.

24. Krasilenko V.G. Simulation of Blind Electronic Digital Signatures of Matrix Type on Confidential Text-Graphic Documentation / V.G. Krasilenko, R. O. Yatskovskaya, S. K. Grabovlyak, // I ISMC: VNAU, 2012. - pp. 103-107.

25. Krasilenko V.G. Modifications of the RSA system for creation of matrix models and algorithms for encryption and decryption of images on its basis / V.G. Krasilenko, S.K. Grabovliak // Systems of information processing. - Kh.: KhUPPS, 2012. - Vol. 8. - pp. 102-106.

26. Krasilenko V.G., Matrix Affine Ciphers for the Creation of Digital Blind Signatures for Text-Graphic Documents / V.G. Krasilenko, S.K. Grabovlyak // Systems of information processing. - Kh.: KhUPPS, 2011. - Vol. 7 (97). - pp. 60 - 63.

27. Krasilenko V.G. Modeling of Matrix Cryptographic Protection Algorithms / V.G. Krasilenko, Yu.A. Flavitskaya // Bulletin of the National University of Lviv Polytechnic "Computer Systems and Networks". - 2009. - No. 658. - pp. 59-63.

28. Krasilenko V.G. Matrix affine and permutation ciphers for encryption and decryption of images / V.G Krasilenko, S.K. Grabovlyak // Systems of information processing. - Kh.: KhUPPS, 2012. - Vol. 3 (101).- t. 2. - pp. 53-62.

29. Krasilenko V.G. Matrix models of cryptographic transformations of images with matrix-bit-map decomposition and mixing and their modeling / V.G. Krasilenko, D.V.

Nikitovich // Materials of 68 NTC "Modern Information Systems and Technologies. Informational security". - Odessa, ONAT them O.P.Popova, 2013. - pp. 139-143.

30. Krasilenko V.G. Cryptographic transformations of images based on matrix models of permutations with matrix-bit-map decomposition and their modeling / V.G. Krasilenko, V.M. Dubchak // Bulletin of Khmelnitsky National University. Technical sciences. - 2014. - No. 1. - pp. 74-79.
31. Krasilenko, V.G. Modeling of Matrix Affine Algorithms for the Encryption of Color Images / V.G. Krasilenko, K.V. Ogorodnik, Yu.A. Flavitskaya // Computer technologies: science and education: abstracts of reports v VseUkr. sci. conf. - K., 2010. - pp. 120-124.
32. Krasilenko V.G. Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity / V.G. Krasilenko, D.V. Nikitovich // Electronics and Information Technologies: a collection of scientific works. - Lviv: Lviv Ivan Franko National University, 2016. - Vol. 6. – pp. 111-127.
33. Krasilenko V.G. Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-map decompositions / V.G. Krasilenko, D.V. Nikitovich // Computer-integrated technologies: education, science, production: sciences. journ - Lutsk: Lutsk Publishing House. nats tech Un., - 2016. - No. 23. - pp. 31-36.
34. Krasilenko V.G. Modeling cryptographic transformations of color images with verification of the integrity of cryptograms based on matrix permutation models / V.G. Krasilenko, D.V. Nikitovich // Materials of the scientific and practical Internet conference "Problems of modeling and development of information systems". - Drohobych: DDPU them. I. Franko, 2016. - pp. 128-136.
35. Krasilenko V.G. Cryptographic transformations (CTs) of color images based on matrix models with operations on modules / V.G. Krasilenko, D.V. Nikitovich // Modern methods, information and software management systems for organizational and technical complexes: a collection of abstracts of reports of the All-Ukrainian scientific and practical Internet conference (May 11, 2016). - Lutsk: RVB of Lutsk National Technical University, 2016. - pp. 41-43.
36. Krasilenko V.G. Modeling Protocols for Matching a Secret Matrix Key for Cryptographic Transformations and Matrix-type Systems / V.G. Krasilenko, D.V. Nikitovich // Systems of information processing. - 2017 - Vol. 3 (149). – pp. 151-157.
37. Krasilenko V.G. Modeling of multi-stage and multi-protocol protocols for the harmonization of secret matrix keys / V.G. Krasilenko, D.V. Nikitovich // Computer-integrated technologies: education, science, production: scientific journal. - Lutsk: LNTU, 2017. - Vol. 26. – pp. 111-120. - Access mode: http://ki.lutsk-ntu.com.ua/node/134/section/27
38. Krasilenko VG Modeling of methods for generating flows of matrix permutations of significant dimension for cryptographic transformations of images // V.G. Красиленко, D.V. Nikitovych // Abstracts of the II All-Ukrainian Scientific and Technical Conference Computer Technologies: Innovations, Problems, Solutions (November 14 - 15, 2019). - Zhytomyr: Zhytomyr Polytechnic, 2019. - pp. 67-77. - Access mode: https://conf.ztu.edu.ua/wp-content/uploads/2019/12/67-1.pdf