DOI 10.31891/2307-5732-2023-321-3-339-347
UDC 681.3.05

VLADIMIR KRASILENKO
Vinnytsia National Agrarian University
ORCID ID: 0000-0001-6528-3150
e-mail: krasvg@i.ua
PIDLUBNYI VLADISLAV
Vinnytsia National Agrarian University
ORCID ID: 0000-0002-4676-4271
e-mail: vladpodlubny@gmail.com
DIANA NIKITOVICH
Vinnytsia National Technical University
ORCID ID: 0000-0002-8907-1221
e-mail: diananikitovych@gmail.com

RESEARCH AND SIMULATION OF THE METHOD OF GENERATION OF THE FLOW OF MATRIX KEYS OF PERMUTATIONS AND THEIR CHARACTERISTICS FOR ENCRYPTION-MASKING OF VIDEO FRAMES

Abstract *- The article proposes and considers a method of generating and forming a stream of secret matrix keys (MK) in the form of permutation matrices. Based on consideration of the advantages of matrix models and algorithms for cryptographic transformations (CT) of images (I), textographic documents, aspects of the application of these matrix-type cryptosystems for creating blind electronic digital signatures (BEDS), masking of video frames, etc., the urgent need to form a set or a consistent series of secret keys. It is shown that, taking into account the peculiarities of crypto-transformations in multi-page, block ciphers, in matrix affine-permutation ciphers, a series of keys in the form of permutation matrices (PM) is necessary. To solve this problem, the article proposes a new approach and method of generating a series of MK (PM), based on the use of a series of sequential cryptotransformations of the base key using affine encryption when changing the keys of this cipher in accordance with the generated random digital sequence. Functionality and advantages of the method of generating a series of secret keys in the form of permutation matrices (PM) are demonstrated by model experiments in the Mathcad Professional software environment, screenshots from the created software modules. The properties of a series of MK PM were investigated using correlation and mutually equivalent normalized functions, which are more effective than correlation functions, and the adequacy and stability of the method were confirmed. The advantage of the proposed method and its matrix models and computational procedures is the consideration of the specificity of images and the ease of adaptation to different types and formats of images, the clarity and isomorphism of the visualization of both the components of the MK PM and the entire flow of keys. Formulas and algorithmic steps of procedures for creating a set of secret matrix keys and intermediate steps of closing, encrypting and decrypting images are given. The obtained results of modeling the method and the processes of creating a series of secret keys of matrix permutations in the Mathcad software environment confirmed the correct functioning and advantages of the proposed method.*

Keywords*: cryptography, matrix models of cryptographic transformations, keys stream generation method, secret matrix key, permutation matrix, text-graphic document, electronic digital signature, modeling, Mathcad Professional, image encryption-decryption, video frame masking, affine cipher, cryptographic nonlinear transformations of image pixel intensities, correlation function, spatial equivalence function.*

КРАСИЛЕНКО ВОЛОДИМИР
ПІДЛУБНИЙ ВЛАДИСЛАВ
НІКІТОВИЧ ДІАНА
Вінницький національний технічний університет

ДОСЛІДЖЕННЯ ТА МОДЕЛЮВАННЯ МЕТОДУ ГЕНЕРУВАННЯ ПОТОКУ МАТРИЧНИХ КЛЮЧІВ ПЕРЕСТАНОВОК ТА ЇХ ХАРАКТЕРИСТИК ДЛЯ ЗАШИФРУВАННЯ-МАСКУВАННЯ ВІДЕОКАДРІВ

Анотація *- У статті запропоновано та розглянуто метод генерації та формування потоку секретних матричних ключів у вигляді матриць перестановок. На основі розгляду переваг матричних моделей та алгоритмів криптоперетворень (КП) зображень (З), текстографічних документів, аспектів застосування цих криптосистем матричного типу для створення сліпих електронних цифрових підписів (СЕЦП), маскування відеокадрів, тощо, обгрунтовано гостру необхідність формування набору чи послідовної серії секретних ключів. Показано, що з урахуванням особливостей криптоперетворень у багатосторінкових, блокових шифрах, у матричних афінно-перестановочних шифрах, необхідна в тому числі низка ключів у вигляді матриць перестановок (МП). Для вирішення цієї проблеми у статті пропонується новий підхід і метод генерації низки МК (МП), що базується на використанні серії послідовних криптоперетворень базового ключа за допомогою афінного шифрування при зміні ключів цього шифру у відповідності до згенерованої випадкової цифрової послідовності. Модельними експериментами у програмному середовищі Mathcad Professional, скрінами зі створених програмних модулів продемонстровані функціональні можливості та переваги методу генерації послідовної серії секретних ключів у вигляді матриць перестановок (МП). Досліджені властивості низки МК (МП) за допомогою кореляційних та взаємно еквівалентністних нормованих функцій, що є ефективнішими за кореляційні, та підтверджено адекватність, стійкість методу. Перевагою запропонованого методу та його матричних моделей, обчислювальних процедур є враховування специфіки зображень та простота адаптації до різних типів та форматів зображень, наочність та ізоморфність візуалізації, як складових МК МП, так і всього потоку ключів. Наведені формули та алгоритмічні кроки процедур створення набору секретних матричних ключів та проміжних кроків закриття, зашифрування та розшифрування зображень. Отримані результати моделювання методу та процесів створення послідовної серії секретних ключів матричних перестановок у програмному середовищі Mathcad підтвердили правильність функціонування та переваги запропонованого методу.*

***Ключові слова**: криптографія, матричні моделі криптографічних перетворень, метод генерування потоку ключів, секретний матричний ключ, матриця перестановок, текстографічний документ, електронний цифровий підпис, моделювання, Mathcad Professional, зашифрування-розшифрування зображень, маскування відеокадрів, афінний шифр, криптографічні нелінійні перетворення інтенсивностей пікселів зображення, кореляційна функція, просторова функція еквівалентності.*

Introduction

Actuality of theme. Digital visual information in the form of images of various formats and streams of video frames is the most common type of data used today in the most diverse areas of industrial, scientific and technical activity, as well as in everyday life. A large number of scientific, scientific and technical, regulatory, educational and other documentation contain a significant amount of visual information in the form of halftone, color images of various objects, diagrams, schemes, drawings, photographs, etc. Regardless of the diversity of such documentation and the options and formats of its digital representation and encoding, all such text-graphic documents (TGD) are visualized as a set of images of pages or fragments of these TGD, stored and displayed using display devices, including monitors, displays personal computers. The constant increase in the bandwidth of information transmission channels and the speed of its processing in distributed communication systems, in hardware and software tools and built-in accelerators of new classes and computer architectures is compensated, firstly, by the constant growth of the volume of both public and confidential visual digital information transmitted in real time, and secondly, the increasing requirements for the dimensionality and resolution of such information. This leads to the necessity improving, and often, revising the foundations of building methods and means of transforming such information in objects of distributed systems based on heterogeneous networks, including on the basis of a radio channel. The main transformations of images are reduced to compression, protection in the channel from unauthorized access, from obstacles of natural and artificial origin, which are based on matrix transformations, for example, orthogonal, affine, etc. In this regard, the interest of researchers in discrete matrix transformations of information in general, as well as in the cryptographic aspect for the purpose of its encryption, today is connected with the fact that the expansion of the set of basic matrix operations and matrix transformation procedures allows choosing the most rational operation or their a set to solve a specific task, and the achievement of great success in the field of digital signal processing processors and programmable logic with the possibility of structural implementation of algorithms of any complexity contributes to the emergence of new, more effective representations of the proposed matrix models and transformations into hardware high-performance implementations and digital processing devices.

And this will make it possible to process large data sets, TGD or whole streams of video frames at an accelerated pace, to solve new and more complex tasks. At the same time, the main aspect of relevance is the improvement of the basic characteristics of transmission processes, protection against unauthorized access and information hiding in telecommunication systems based on matrix models, their new basic operations and necessary transformation procedures. One of the urgent issues is the study and assessment of the prospects for the application of an extended family of matrix models and transformations, taking into account their properties and features, in algorithms for compression, masking of images and video frames, which requires separate research. Solving this issue will significantly increase the security of transmission of digital visual information in telecommunication channels. Development of a method of frame-by-frame masking matrix transformation of visual data to protect against unauthorized access when storing images or video files and transferring them in open communications is a very urgent task, which has already been studied at the level of cryptotransformation models of individual images, including color ones, or individual frames. However, for the direct or reverse crypto-transformation of the entire flow of frames or image matrices based on new, specifically matrix models and procedures, additional research and solving of such a task as forming a series of frame-by-frame masking or encryption-decryption keys is required. Advantages of cryptographic transformations (CT) of textual documents (TGD) with visas, signatures, images (I), tables, diagrams, etc., in cryptosystems of the matrix type (MT) [1-4] based on algorithms and matrix-algebraic models (MAM) , including generalized matrix affine and affine-permutation ciphers were demonstrated in works [5-10]. Modifications of MAM were used in the creation of blind and other digital signatures [11-17], they allow checking the presence of distortions in cryptograms of black and white and color images, their integrity [5,7], creating block [6], multifunctional parametric models [8] , multi-page [9] and investigate their stability characteristics [10]. The basic operations of MAM are element-by-element multiplication, addition modulo matrices, and matrix permutation models (MP_M) with matrix multiplication procedures.

To implement CT, it is necessary to multiply byte matrices on the left and right by permutation matrices (PM), a matrix of rows, columns, vectors that display symbols, codes, bytes in unitary codes, can also be replaced and rearranged using such permutations. In order to change and equalize the histograms of all spectral components of the image with equal probability, to increase the entropy of the cryptogram of the image during its cryptographic transformations based on MP_M, the decomposition of R, G, B components and their bit slices and several matrix keys (MKs) and vector keys (VKs) are necessary [3-5]. That is, for MAM there is an urgent need to form a whole series of MPs from the main MK, which would satisfy a number of requirements.

Formulation of the problem

Since in [18,19, 20, 21] the issue of coordination of only the main matrix key of a general type was considered, and not a number (flow) of PMs, the aim of the work is to model and study the processes of formation of the permutation matrices (PMs) flow for MAM CT in MT systems, to check the statistical and correlation properties of a number of generated PMs .

Presentation of the main material, research results

Let us consider the situation when PMs of size 256*256, described in [2-5], are used for the cryptographic transformations of blocks 256*256 bytes long, presented in the form of a black-and-white image matrix, or vectors 256 bytes long (2048 bits), described in [2-5], where the processes are given their generation, MAM of their transformations and cryptographic transformations based on them. Since for each block, several round, cyclic cryptographic transformations it is desirable to have a number of matrix keys generated from the master key, for example, the same MK, then, taking into account the requirements for the crypto-statistical characteristics of MKs, the task of researching the processes of fast and reliable generation of MK sequences in the form of MKs becomes very relevant. Let's assume that their number is also equal to 256. The results of modeling the processes of generating a number of PMs for such a situation in Mathcad with formulas and matrices of PMs are shown in Fig. 1. If the main MK is the generated random PM KPX (Fig. 1), then it is uniquely displayed by a 256-component permutation (vector) V_KPX and also in the form of image or a byte matrix (BM) of size 16*16 with the peculiarity that all 256 of its gradations of intensity are different.

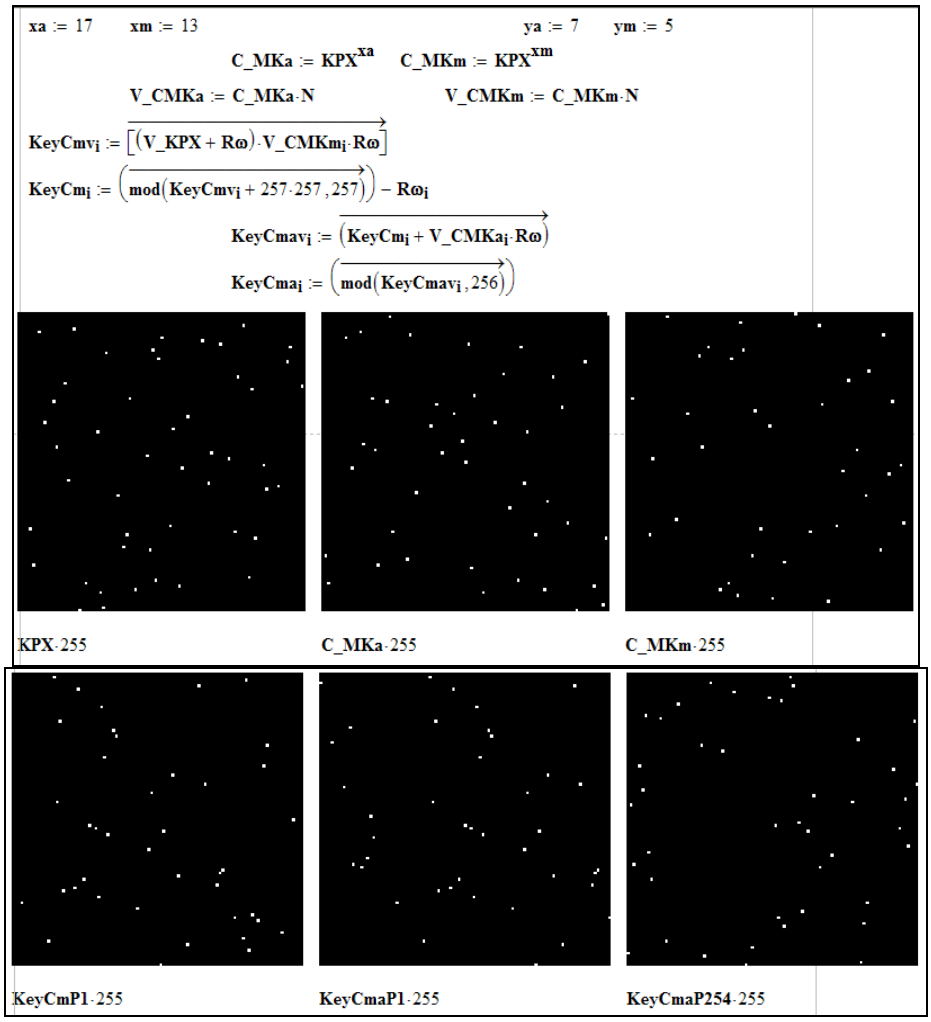

Fig. 1. Results of simulation of MKs (PMs) array generation processes

Using the scalars xa and xm agreed by the parties, as powers of KPX, we form from KPX two additional matrices C_MKa, C_MKm, see Fig. 1, and their corresponding vectors V_CMKa, V_CMKm, which together with the vector V_KPX (vector representation of KPX) are shown in Fig. 2. Histograms of all these vectors (basic!) are horizontal lines, see Fig. 3, as well as all vector representations of generated permutations formed from V_KPX, as its i-th cryptograms, using an affine cipher and a pair of i-th components of vectors V_CMKa, V_CMKm (additive and multiplicative components). These cryptograms are the i-th current permutations (vectors) of KeyCma, which can also be unambiguously represented in the form of KeyCmaP bit matrices with dimensions (256*256), for example, KeyCmaP1-KeyCmaP254, Fig. 1. Fragments from Mathcad windows are shown in Fig. 4.

Since the histograms of all PMs (their vectors) are horizontal lines, and their entropy is equal to 8 bits, crypto-analysis based on them is impossible. In addition, the main and 2 auxiliary MKs are secret, allowing only parties to the CT to create or have this series of MKs (PMs). In principle, only the master and the aforementioned xa and xm scalar keys can be secret or negotiated parties.

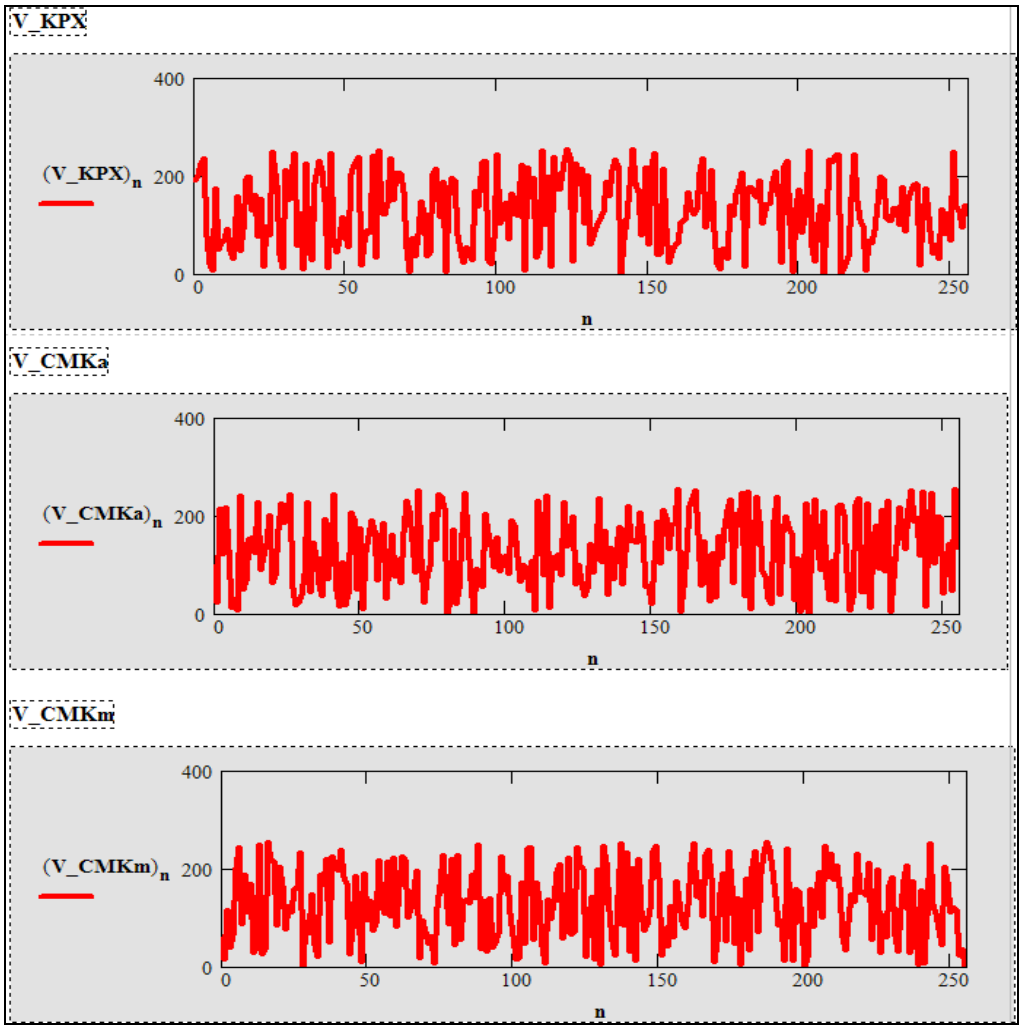

Fig. 2 Vector representations of basic MKs for generating an array of MKs (PMs) from them

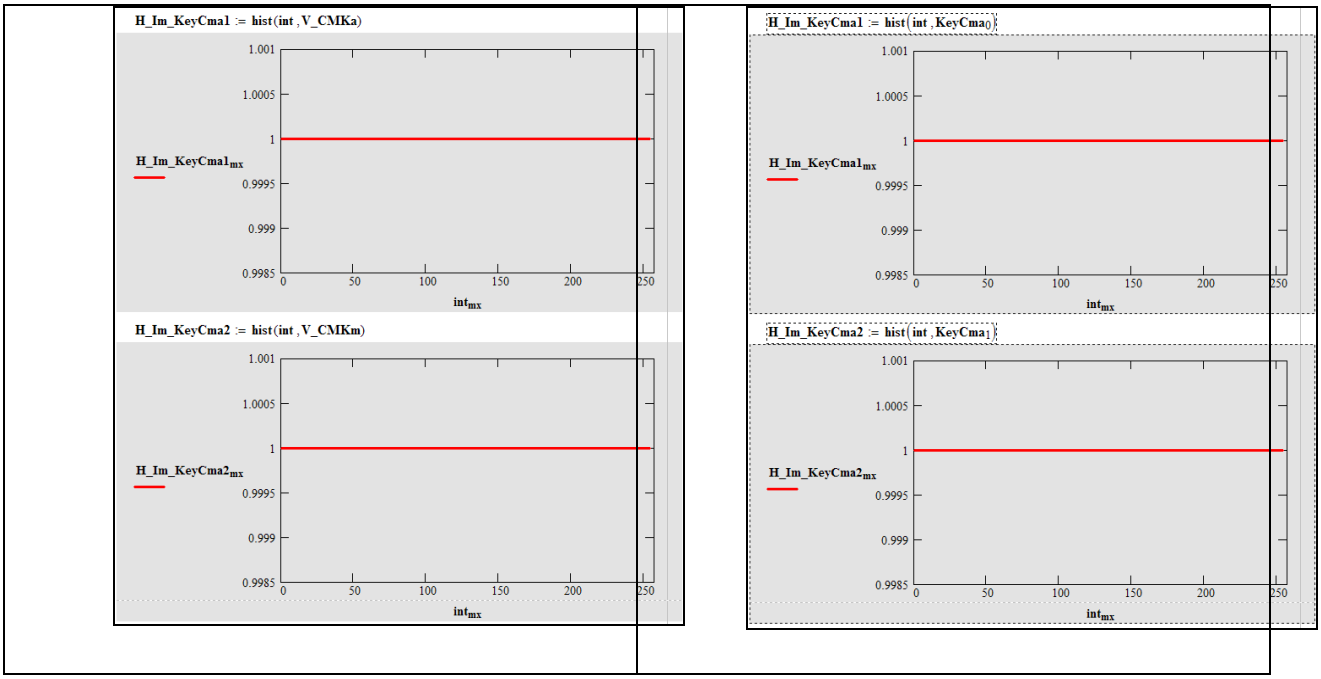

Fig. 3 Histograms of vector representations of basic (left) and some (first, second) generated (right) MKs (PMs)

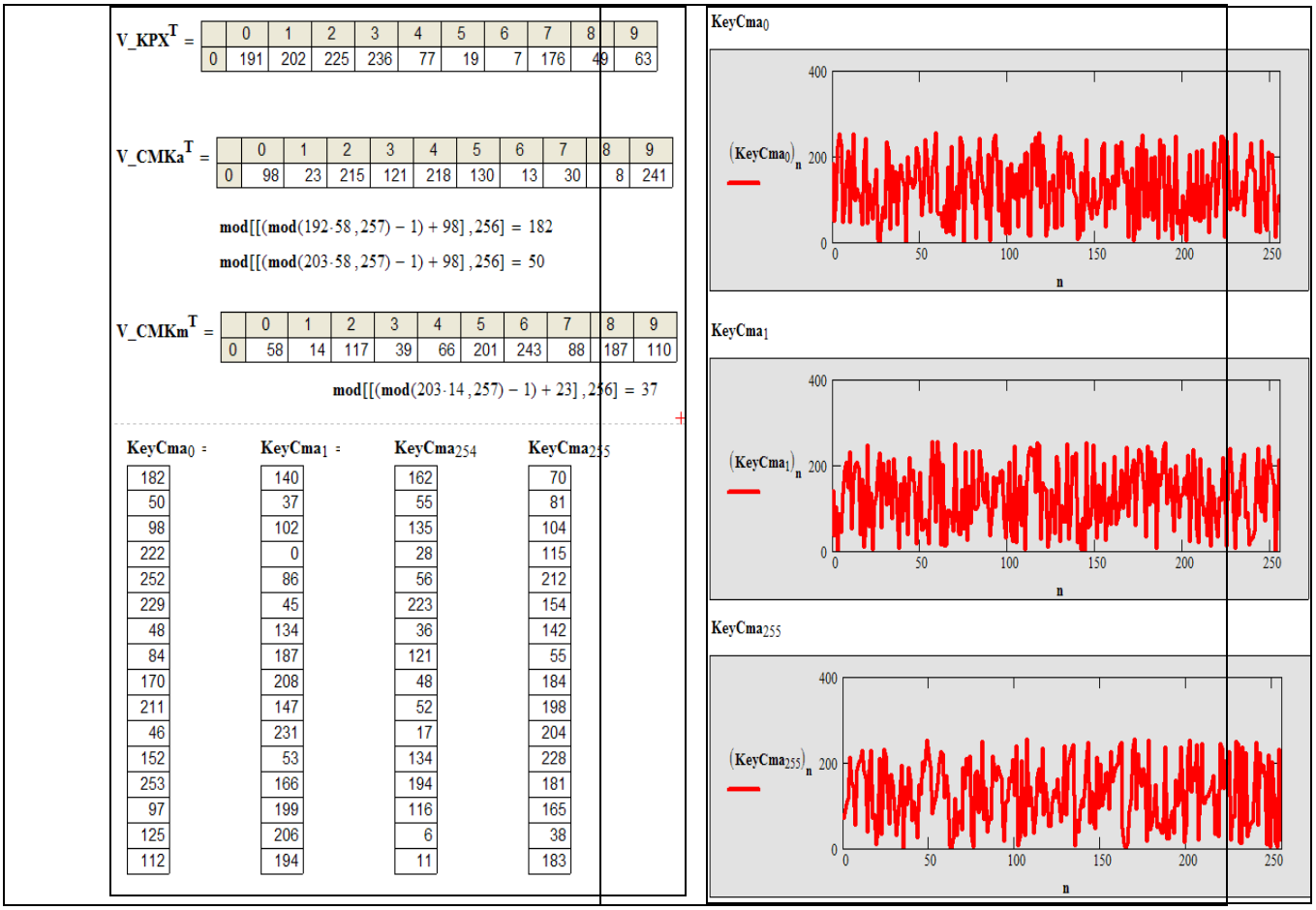

Fig. 4 Fragments from Mathcad windows: one of the key formation procedures (left) and vector representations of some (zero, first, 255-th) generated (right) MKs (PMs)

To study the quality of MKs (PMs) of the created series, to study their properties, we calculated all their possible mutual-correlation and equivalence normalized functions, which are displayed in the form of fragments of Mathcad windows in fig. 5-7 and confirm the achievement of surprisingly good properties. Note that the obtained results and their comparison also indicate that mutual-equivalence normalized functions are better than mutual-correlation functions.

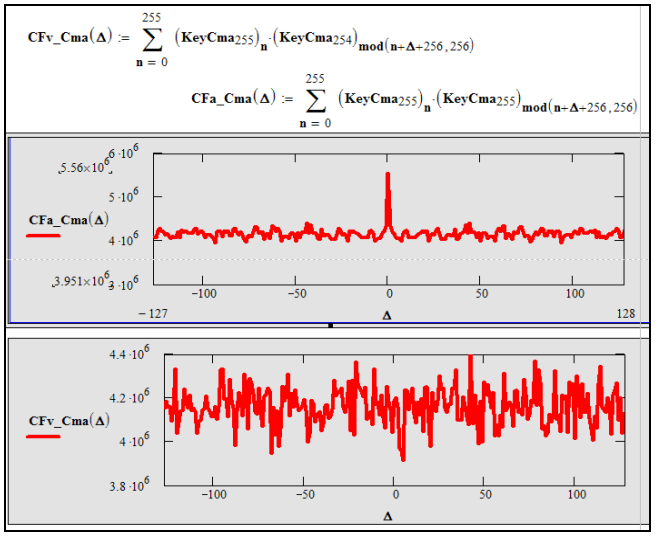

Fig. 5 Formulas and form of auto-correlation CFa_Cma and cross-correlation CFv_Cma functions depending on cyclic shift, displacement of elements of PM vectors

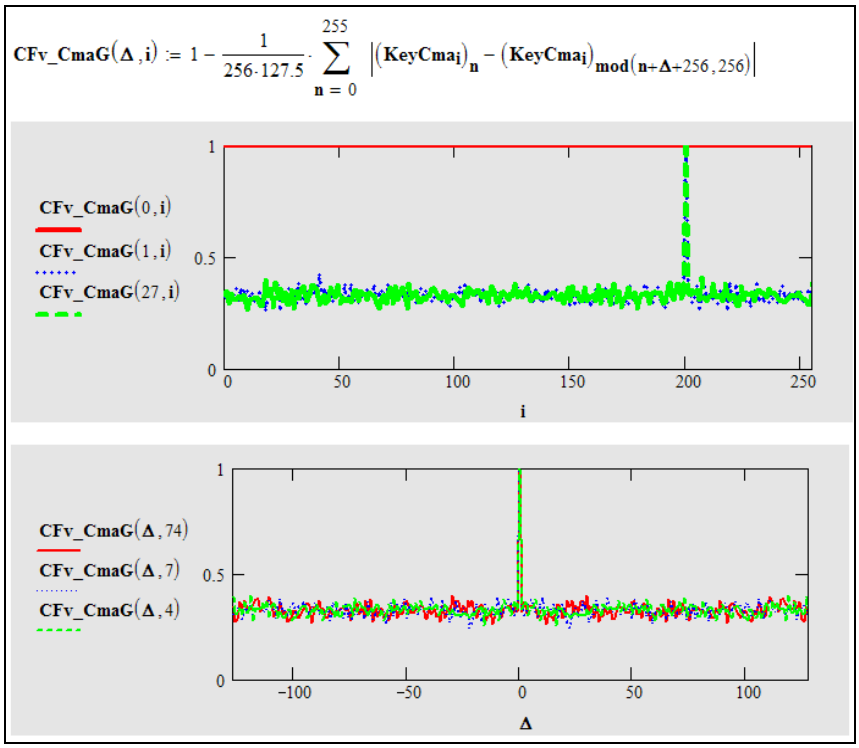

Fig. 6 Formulas and form of mutual-equivalence CFv_CmaG functions depending on the MP number (i) and cyclic shift, displacement of elements of the PM vectors

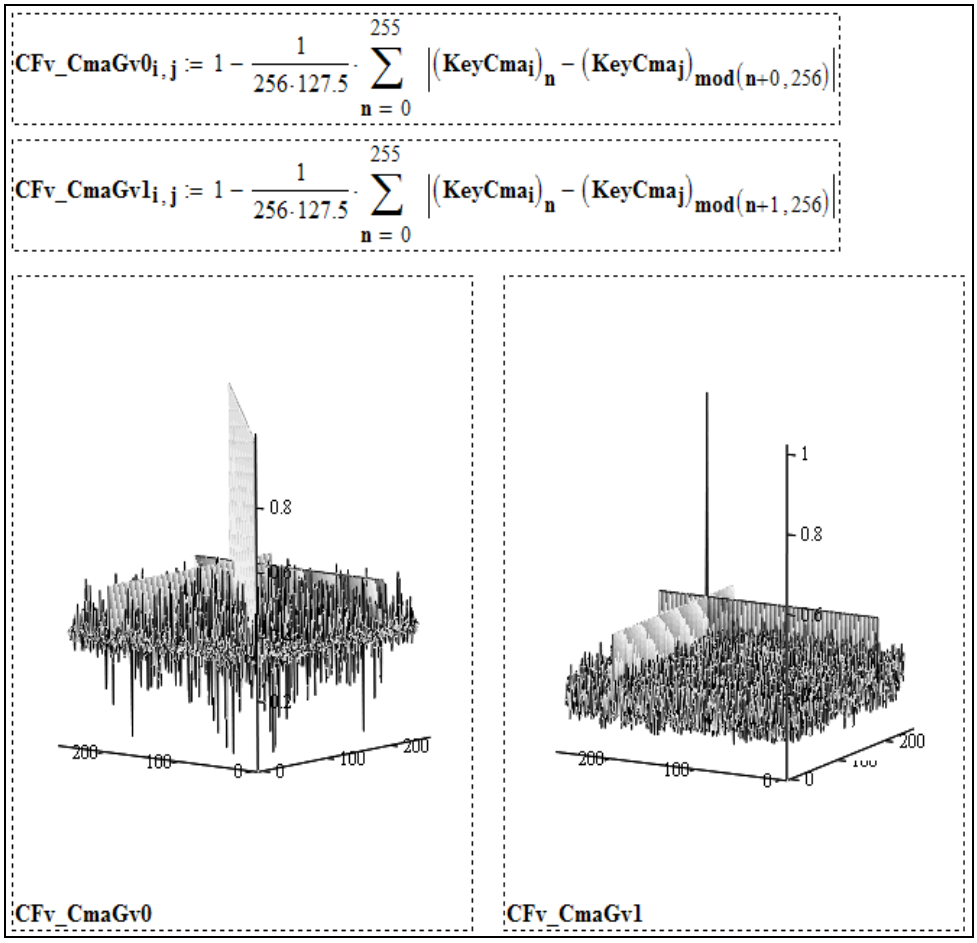

Fig. 7 Formulas and form (3D) of mutual equivalence CFv_CmaG functions depending on the PM numbers (i,j) for the "0-th" and "1-th" displacements of the elements of the PM vectors

For better perception and more effective transmission of basic MK (PM) and the sequence of created PMs, the latter are converted with the help of software modules into color or black and white image, shown in fig.8 and can go as frames of a video stream (colored image corresponds to three basic MKs).

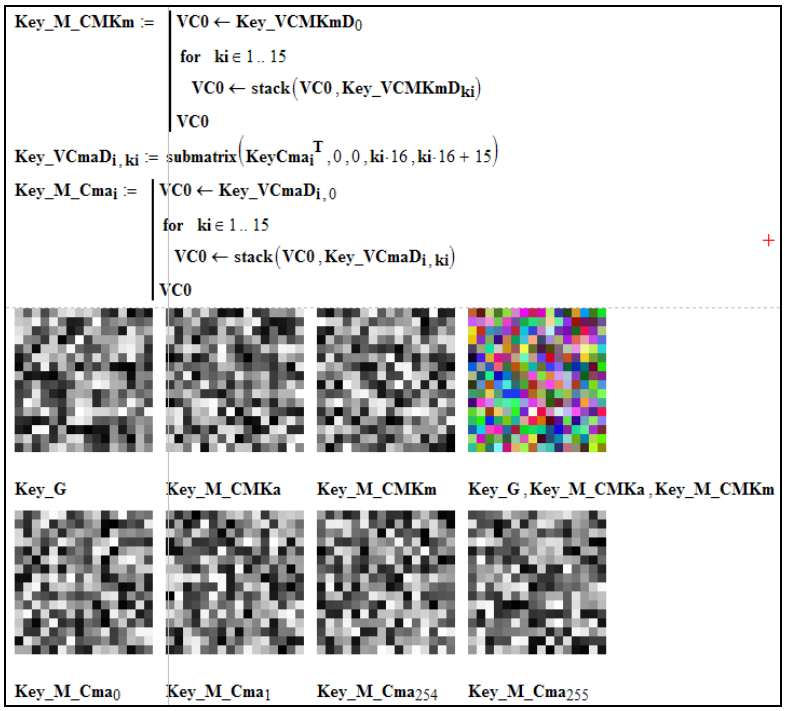

Fig. 8 Matrix representation of basic MK and a number of MPs

As can be seen from fig. 6-7, for one PM (in the 200-th experiment) there is a similarity with another key, but this is explained by the fact that for it xm is equal to "1". This is easily eliminated if the number of PMs in the sequence is reduced from 256 to 255 for the situation chosen in the simulation and described here

Conclusion

The proposed and modeled in Mathcad method of generating a series of MKs (PMs) for multi-page, block, matrix affine-permutation algorithms and matrix-algebraic models of cryptographic transformations. The properties of a series of MKs (PMs) were investigated using mutually equivalent normalized functions, which are more effective than correlation functions, and the adequacy and stability of the method were confirmed.

References

1. Красиленко В.Г. Моделювання матричних алгоритмів криптографічного захисту / В.Г. Красиленко, Ю.А. Флавицька // Вісн. НУ "Львів. політехніка".- 2009. - № 658. - С. 59-63.

2. Красиленко В. Г. Матричні афінно-перестановочні алгоритми для шифрування та дешифрування зображень / В. Г. Красиленко, С. К. Грабовляк // Системи обробки інформації. - 2012. - Вип. 3(2). - С. 53-61. - Режим доступу: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

3. Красиленко В.Г. Криптографічні перетворення зображень на основі матричних моделей перестановок з матрично-бітовозрізовою декомпозицією та їх моделювання / В. Г. Красиленко, В. М. Дубчак // Вісник Хмельн. НУ. Технічні науки. - 2014. - № 1. - С. 74-79.

4. Красиленко В.Г. Моделювання криптографічних перетворень кольорових зображень на основі матричних моделей перестановок зі спектральною та бітово-зрізовою декомпозиціями / В.Г. Красиленко, Д.В. Нікітович // Комп'ютерно-інтегровані технології: освіта, наука, виробництво : наук. журн. – Луцьк: Видавництво Луц. нац. техн. ун-т., - 2016. - № 23. - С. 31-36. – Режим доступу: http://ki.lutsk-ntu.com.ua/node/132/section/9

5. Красиленко В.Г. Моделювання та дослідження криптографічних перетворень зображень на основі їхньої матрично-бітовозрізової декомпозиції та матричних моделей перестановок з верифікацією цілісності / В.Г. Красиленко, Д.В. Нікітович // Електроніка та інформаційні технології. – Львів: ЛНУ імені Івана Франка, 2016. – Вип. 6. – С 111-127. – Режим доступу: http://elit.lnu.edu.ua/pdf/6_12.pdf

6. Красиленко В.Г. Моделі блокових матричних афінно-перестановочних шифрів (МАПШ) для криптографічних перетворень та їх дослідження / В.Г. Красиленко, Д.В. Нікітович // 72 НТК: матеріали конференції (13-15 грудня 2017 р.). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.117-122.

7. Красиленко, В.Г. Моделювання матричних афінних алгоритмів для шифрування кольорових зображень / В. Г. Красиленко, К. В. Огородник, Ю.А.Флавицька // Комп'ютерні технології: наука і освіта: тези доповідей V Всеукр. НПК– К., 2010. – С.120-124.

8. Красиленко В.Г. Багатофункціональні параметричні матрично-алгебраїчні моделі (МАМ) криптографічних перетворень (КП) з операціями за модулем та їх моделювання. / В.Г. Красиленко, Д.В. Нікітович. // 72 НПК: матеріали конференції (13-15 грудня 2017 року). – Одеса: ОНАЗ ім. О.С. Попова, 2017. – Частина 1. – С.123-128.

9. Красиленко В.Г. Моделювання сторінкових криптографічних перетворень масивів кольорових зображень на основі матричних моделей та перестановок / В.Г. Красиленко, Д.В. Нікітович // «Інформаційно-комп'ютерні технології – 2018»: Збірник тез доповідей IX Міжнародної НТК, 20-21 квітня 2018 року. – Житомир: Вид. О. О. Євенок, 2018. – С. 73-77.

10. Красиленко В.Г. Дослідження покращеного багатокрокового 2D RSA шифру та його гістограмно-ентропійних характеристик / В.Г. Красиленко, Д.В. Нікітович // «Інформаційна безпека та комп'ютерні технології»: Збірник тез доповідей III Міжнародної НПК, 19-20 квітня 2018 року. – Кропивницький: ЦНТУ, 2018. – С. 78-82. Режим доступу: http://it-kntu.kr.ua/wp-content/uploads/2015/01/Zbirnyk-tez-InfoSecCompTech-2018.pdf

11. Красиленко В.Г. Матричні афінні шифри для створення цифрових сліпих підписів на текстографічні документи / В.Г. Красиленко, С.К. Грабовляк // Системи обробки інформації. – Х.: ХУПС, 2011. – Вип. 7(97). – С. 60 – 63.

12. Красиленко В.Г. Демонстрація процесів створення сліпих електронних цифрових підписів на текстографічну документацію на основі моделей матричного типу / В.Г. Красиленко, Р.О. Яцковська, Ю.М. Тріфонова, // Системи обробки інформації. – 2013. – Вип. 3(110). – Т. 2. – С. 18 – 22.

13. Красиленко В.Г. Вдосконалення та моделювання електронних цифрових підписів матричного типу для текстографічних документів / В.Г. Красиленко, Д.В. Нікітович // Матеріали VI міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ-Одеса-2017), Одеський національний морський університет, 20-22 вересня 2017р. – Одеса: «ВидавІнформ НУ «ОМА», 2017. - С. 312 -318.

14. Krasilenko V.G., Lazarev A.A, Nikitovich D.V. The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research. Actual problems of information systems and technologies. 2020. P. 270-282..

15. Krasilenko V.G., Lazarev A.A., Nikitovich D.V. Models of matrix block affine-permutation ciphers (mbapcs) for cryptographic transformations and their research. Problems of cyber security of information and telecommunication systems: Collection of reports and articles. 2020. P. 314–321.

16. Krasilenko V.G., Lazarev A.A, Nikitovich D.V. Matrix Models of Cryptographic Transformations of Video Images Transmitted from Aerial-Mobile Robotic Systems. In Control and Signal Processing Applications for Mobile and Aerial Robotic Systems. Hershey, PA: IGI Global, 2020. P. 170-214. http://doi:10.4018/978-1-5225-9924-1.ch005 ISBN13: 9781522599241 ISBN10: 152259924X EISBN13: 9781522599265 ISBN13 Softcover: 9781522599258 (eBook)

17. Красиленко В. Г., Нікітович Д. В. Моделювання покращених сліпих електронних цифрових підписів 2D типу для систем захисту інформації. Вісник Хмельницького національного університету. Технічні науки. 2022. №1 (305). С. 72-77.

18. Красиленко В.Г. Моделювання протоколів узгодження секретного матричного ключа для криптографічних перетворень та систем матричного типу / В.Г. Красиленко, Д.В. Нікітович // Системи обробки інформації. – 2017. – Вип. 3 (149). – С 151-157.

19. Красиленко В.Г. "Моделювання багатокрокових та багатоступеневих протоколів узгодження секретних матричних ключів" / В.Г. Красиленко, Д.В. Нікітович // Комп`ютерно-інтегровані технології: освіта, наука, виробництво: науковий журнал. – Луцьк: ЛНТУ, 2017. – Вип. 26. – С 111-120. - Режим доступу: http://ki.lutsk-ntu.com.ua/node/134/section/27

20. Красиленко В. Г., Нікітович Д. В. Криптографічний кооперативний протокол узгодження ізоморфно представленого спільного секретного матричного ключа-перестановки великої розмірності: матеріали IX Міжнародної науково-практичної конференції «Інформаційні управляючі системи та технології» (ІУСТ), 24– 26 вересня 2020 р. Одеса, 2020. С. 45-50. URL: http://ir.lib.vntu.edu.ua//handle/123456789/30698

21. Красиленко В. Г., Юрчук Н. П, Нікітович Д. В. Застосування ізоморфних матричних представлень для моделювання протоколу узгодження секретних ключів-перестановок значної розмірності. Вісник Хмельницького національного університету. Технічні науки. Хмельницький, 2021, Вип. № 2. С. 78-88. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/32827/83207.pdf?sequence=2&isAllowed=y

References

1. Krasilenko V.G. Modeliuvannia matrychnykh alhorytmiv kryptohrafichnoho zakhystu / V.G. Krasilenko, Yu.A. Flavytska // Visn. NU "Lviv. politekhnika".- 2009. - № 658. - S. 59-63.

2. Krasilenko V. G. Matrychni afinno-perestanovochni alhorytmy dlia shyfruvannia ta deshyfruvannia zobrazhen / V. G. Krasilenko, S. K. Hrabovliak // Systemy obrobky informatsii. - 2012. - Vyp. 3(2). - S. 53-61. - Rezhym dostupu: http://nbuv.gov.ua/UJRN/soi_2012_2_3_15

3. Krasylenko V.H. Kryptohrafichni peretvorennia zobrazhen na osnovi matrychnykh modelei perestanovok z matrychno-bitovozrizovoiu dekompozytsiieiu ta yikh modeliuvannia / V. H. Krasylenko, V. M. Dubchak // Visnyk Khmeln. NU. Tekhnichni nauky. - 2014. - № 1. - S. 74-79.

4. Krasilenko V.G. Modeliuvannia kryptohrafichnykh peretvoren kolorovykh zobrazhen na osnovi matrychnykh modelei perestanovok zi spektralnoiu ta bitovo-zrizovoiu dekompozytsiiamy / V.G. Krasilenko, D.V. Nikitovich // Kompiuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo : nauk. zhurn. – Lutsk: Vydavnytstvo Luts. nats. tekhn. un-t., - 2016. - № 23.

- S. 31-36. – Rezhym dostupu: http://ki.lutsk-ntu.com.ua/node/132/section/9

5. Krasilenko V.G. Modeliuvannia ta doslidzhennia kryptohrafichnykh peretvoren zobrazhen na osnovi yikhnoi matrychno-bitovozrizovoi dekompozytsii ta matrychnykh modelei perestanovok z veryfikatsiieiu tsilisnosti / V.G. Krasilenko, D.V. Nikitovich // Elektronika ta informatsiini tekhnolohii. – Lviv: LNU imeni Ivana Franka, 2016. – Vyp. 6. – S 111-127. – Rezhym dostupu: http://elit.lnu.edu.ua/pdf/6_12.pdf

6. Krasilenko V.G. Modeli blokovykh matrychnykh afinno-perestanovochnykh shyfriv (MAPSh) dlia kryptohrafichnykh peretvoren ta yikh doslidzhennia / V.G. Krasilenko, D.V. Nikitovich // 72 NTK: materialy konferentsii (13-15 hrudnia 2017 r.). – Odesa: ONAZ im. O.S. Popova, 2017. – Chastyna 1. – S.117-122.

7. Krasilenko V.G. Modeliuvannia matrychnykh afinnykh alhorytmiv dlia shyfruvannia kolorovykh zobrazhen / V.G. Krasilenko, K.V. Ohorodnyk, Yu.A. Flavytska // Kompiuterni tekhnolohii: nauka i osvita: tezy dopovidei V Vseukr. NPK– K., 2010. – S.120-124.

8. Krasilenko V.G. Bahatofunktsionalni parametrychni matrychno-alhebraichni modeli (MAM) kryptohrafichnykh peretvoren (KP) z operatsiiamy za modulem ta yikh modeliuvannia. / V.G. Krasilenko, D.V. Nikitovich. // 72 NPK: materialy konferentsii (13-15 hrudnia 2017 roku). – Odesa: ONAZ im. O.S. Popova, 2017. – Chastyna 1. – S.123-128.

9. Krasilenko V.G. Modeliuvannia storinkovykh kryptohrafichnykh peretvoren masyviv kolorovykh zobrazhen na osnovi matrychnykh modelei ta perestanovok / V.G. Krasilenko, D.V. Nikitovich // «Informatsiino-kompiuterni tekhnolohii – 2018»: Zbirnyk tez dopovidei IX Mizhnarodnoi NTK, 20-21 kvitnia 2018 roku. – Zhytomyr: Vyd. O. O. Yevenok, 2018. – S. 73-77.

10. Krasilenko V.G. Doslidzhennia pokrashchenoho bahatokrokovoho 2D RSA shyfru ta yoho histohramno-entropiinykh kharakterystyk / V.G. Krasilenko, D.V. Nikitovich // «Informatsiina bezpeka ta kompiuterni tekhnolohii»: Zbirnyk tez dopovidei III Mizhnarodnoi NPK, 19-20 kvitnia 2018 roku. – Kropyvnytskyi: TsNTU, 2018. – S. 78-82. Rezhym dostupu: http://it-kntu.kr.ua/wp-content/uploads/2015/01/Zbirnyk-tez-InfoSecCompTech-2018.pdf

11. Krasilenko V.G. Matrychni afinni shyfry dlia stvorennia tsyfrovykh slipykh pidpysiv na tekstohrafichni dokumenty / V.G. Krasilenko, S.K. Hrabovliak // Systemy obrobky informatsii. – Kh.: KhUPS, 2011. – Vyp. 7(97). – S. 60 – 63.

12. Krasilenko V.G. Demonstratsiia protsesiv stvorennia slipykh elektronnykh tsyfrovykh pidpysiv na tekstohrafichnu dokumentatsiiu na osnovi modelei matrychnoho typu / V.G. Krasilenko, R.O. Yatskovska, Yu.M. Trifonova, // Systemy obrobky informatsii. – 2013. – Vyp. 3(110). – T. 2. – S. 18 – 22.

13. Krasilenko V.G. Vdoskonalennia ta modeliuvannia elektronnykh tsyfrovykh pidpysiv matrychnoho typu dlia tekstohrafichnykh dokumentiv / V.G. Krasilenko, D.V. Nikitovich // Materialy VI mizhnarodnoi naukovo-praktychnoi konferentsii «Informatsiini upravliaiuchi systemy ta tekhnolohii» (IUST-Odesa-2017), Odeskyi natsionalnyi morskyi universytet, 20-22 veresnia 2017r. – Odesa: «VydavInform NU «OMA», 2017. - S. 312 -318.

14. Krasilenko V.G., Lazarev A.A, Nikitovich D.V. The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research. Actual problems of information systems and technologies. 2020. P. 270-282.

15. Krasilenko V.G., Lazarev A.A., Nikitovich D.V. Models of matrix block affine-permutation ciphers (mbapcs) for cryptographic transformations and their research. Problems of cyber security of information and telecommunication systems: Collection of reports and articles. 2020. P. 314–321.

16. Krasilenko V.G., Lazarev A.A, Nikitovich D.V. Matrix Models of Cryptographic Transformations of Video Images Transmitted from Aerial-Mobile Robotic Systems. In Control and Signal Processing Applications for Mobile and Aerial Robotic Systems. Hershey, PA: IGI Global, 2020. P. 170-214. http://doi:10.4018/978-1-5225-9924-1.ch005 ISBN13: 9781522599241 ISBN10: 152259924X EISBN13: 9781522599265 ISBN13 Softcover: 9781522599258 (eBook)

17. Krasylenko V. H., Nikitovych D. V. Modelyuvannya pokrashchenykh slipykh elektronnykh tsyfrovykh pidpysiv 2D typu dlya system zakhystu informatsiyi. Visnyk Khmel′nyts′koho natsional′noho universytetu. Tekhnichni nauky. 2022. №1 (305). S. 72-77.

18. Krasilenko V.G. Modeliuvannia protokoliv uzghodzhennia sekretnoho matrychnoho kliucha dlia kryptohrafichnykh peretvoren ta system matrychnoho typu / V.G. Krasilenko, D.V. Nikitovich // Systemy obrobky informatsii. – 2017. – Vyp. 3 (149). – S 151-157.

19. Krasilenko V.G. "Modeliuvannia bahatokrokovykh ta bahatostupenevykh protokoliv uzghodzhennia sekretnykh matrychnykh kliuchiv" / V.G. Krasilenko, D.V. Nikitovich // Komp`iuterno-intehrovani tekhnolohii: osvita, nauka, vyrobnytstvo: naukovyi zhurnal. – Lutsk: LNTU, 2017. – Vyp. 26. – S 111-120. - Rezhym dostupu: http://ki.lutsk-ntu.com.ua/node/134/section/27

20. Krasilenko V.G., Yurchuk N.P, Nikitovich D.V. Zastosuvannia izomorfnykh matrychnykh predstavlen dlia modeliuvannia protokolu uzghodzhennia sekretnykh kliuchiv-perestanovok znachnoi rozmirnosti. Visnyk Khmelnytskoho natsionalnoho universytetu. Tekhnichni nauky. Khmelnytskyi, 2021, Vyp. № 2. S. 78-88. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/32827/83207.pdf?sequence=2&isAllowed=y

21. Krasilenko V.G, Nikitovych D.V. Kryptohrafichnyi kooperatyvnyi protokol uzghodzhennia izomorfno predstavlenoho spilnoho sekretnoho matrychnoho kliucha-perestanovky velykoi rozmirnosti: materialy IX Mizhnarodnoi naukovo-praktychnoi konferentsii «Informatsiini upravliaiuchi systemy ta tekhnolohii» (IUST), 24– 26 veresnia 2020 r. Odesa, 2020. S. 45-50. URL: http://ir.lib.vntu.edu.ua//handle/123456789/30698