Modeling a method for generating a stream of secret keys in the form of permutation matrices for encryption-masking of video frames and studying its characteristics

Vladimir Krasilenko, Vladislav Podlubnyi, Diana Nikitovich

Department of Computer Science and Economic Cybernetics
Vinnytsia National Agrarian University
Vinnytsia, Ukraine

Abstract

The article considers a method of forming a stream of secret matrix keys in the form of permutation matrices. On the basis of consideration of the advantages of matrix models and cryptosystems for masking video frames, the urgent need to form a stream of secret matrix keys (MKs) is stressed. It is shown that, taking into account of crypto-transformations in matrix affine-permutation ciphers, a number of keys in the form of permutation matrices (MPs) are required for the successful use of the latter in frame masking tasks. To solve this problem the article proposes a approach of generating a series of MKs (MPs). The method is based on the use of a series of crypto-transformations of the base key using affine encryption while changing the keys of this cipher in accordance with the generated random sequence. Functionality and advantages of the proposed method are demonstrated by model experiments in the Mathcad, screenshots from the created modules. The properties of a set of generated MKs (MPs) were investigated using mutual correlation and equivalence normalized functions. Adequacy and stability of the method were confirmed. The advantage of the method is the focus on parallel processing, ease of adaptation to different formats of images, isomorphism of visualization of keys

Keywords

Cryptography transformations, Secret matrix key, Permutation matrix, Keys stream, Matrix model, Encryption-decryption, Masking of video frames, Cipher, Spatial equivalence function

I. INTRODUCTION

Review of the publication

Problem Statement

II. PRESENTATION OF THE MAIN MATERIAL AND RESEARCH RESULTS

V. CONCLUSION

Introduction

A Review of the publication

- Today, the most prevalent type of data used in various fields, including industry, science, technical development, and everyday life, is digital visual information in the form of images and video frames. A vast number of documents containing scientific, technical, educational, and other data include diverse images of objects, diagrams, schematics, drawings, and photographs, both halftone and color [1-6].

Introduction

A Review of the publication

- Cryptographic methods for protecting information must be used today in a significant number of information technologies and areas of their application. These areas include the Internet of Things (IoT), intelligent sensors and devices for collecting, processing and transmitting information, microcontrollers and devices for diagnostics and monitoring in medicine, military equipment, RFID tags, network information and communication technologies, geo-information systems for remote monitoring

Introduction

A Review of the publication

- Taking into account the diversity and specificity of these areas, different requirements are placed on cryptographic algorithms, models and systems. But there are also general requirements, such as stability and sustainability. The latter in most known cryptosystems significantly depend on the quality of the generated keys, for example, the gamma in stream ciphers [4, 6-9]. Determining the randomness and characteristics of the generated sequences is one of the priority tasks. A good generation of a pseudo-random sequence is one for which it is impossible to predict the next values without knowledge of the seed, knowing the entire history of previous values.

Introduction

A Review of the publication

- Independent testing by the authors of the properties of such algorithms and generators in identical universal conditions made it possible to obtain objective and independent results of a comparative analysis and substantiate the principles of creating a new stream cryptographic algorithm, which can be the basis of the national standard of Ukraine [8, 9]. This is explained by the fact that the study of the “Strumok” algorithm, developed by Ukrainian scientists, showed that its statistical and other characteristics correspond to the best algorithms in the world [8. 9]. And therefore, in our work, we will show how to build new pseudo-random streams based on such generators, but not simple bit or numerical values, but secret keys of a special format

A Review of the publication

Despite the diversity of such information and the formats in which it is presented, all these text-graphic documents (TGD) are represented as sets of page images or their fragments, which are stored and displayed using various devices, including computer monitors and displays.

And this will make it possible to process large data sets or whole streams of video frames at an accelerated pace, to solve new and more complex tasks. 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 transformation procedures. One of the urgent issues is the study of the prospects for the application of matrix models and transformations 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.

A Review of the publication

The constant increase in the bandwidth of information transmission channels and the speed of its processing in communication systems, in hardware and software accelerators and computer architectures is compensated, firstly, by the constant growth of the volume of both public and confidential visual digital information, 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.

The fundamental image processing operations include compression and protection against unauthorized access and the influence of natural and artificial factors, and for this purpose, matrix transformations such as orthogonal and affine transformations are used.

A Review of the publication

Today, researchers are showing significant interest in discrete matrix transformations of information, both in a general context and in the realm of cryptography, for information encryption and protection. Expanding the set of basic matrix operations allows for selecting the most suitable operation for a specific task, and modern processors and programmable logic contribute to the implementation of these operations at the hardware level, enabling more efficient processing of large volumes of data, TGD, and video streams.

However, the primary challenge lies in enhancing the transmission, protection, and concealment of information in telecommunication systems using matrix models, their operations, and transformations. One of the urgent problems is the research and assessment of the possibilities of using an extended family of matrix models and transformations in algorithms for compression, hiding and protection of visual data, taking into account their features and properties. This requires additional research. Solving this problem will help to significantly increase the security of transmission of digital visual information through telecommunication channels.

A Review of the publication

- 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 crypto-transformation models of individual images or individual frames. However, for the direct or reverse crypto-transformation of the entire flow of frames or image matrices based on new matrix models, additional research is required.
- The solving of such a task, as forming a series of frame-by-frame masking encryption-decryption keys is required.

A Review of the publication

- Advantages of cryptographic transformations (CT) of textographic documents (TGD) with visas, signatures, images (I), tables, diagrams, etc., in cryptosystems of the matrix type (MT) [7-11] based on algorithms and matrix-algebraic models (MAMs), including generalized matrix affine and affine-permutation ciphers were demonstrated in works [12-17]. Modifications of MAM were used in the creation of blind and other digital signatures [11], they allow checking the presence of distortions in cryptograms of black and white and color images, their integrity [12], creating block [13-14], multifunctional parametric models [15], multi-page [16] and investigate their stability characteristics.

A Review of the publication

The basic operations of MAM are element-by-element multiplication, addition modulo matrices, and matrix permutation models (MP_M) with matrix multiplication procedures. For security purposes technologies of cryptography, tools for CTs and protocols for the formation of keys and their exchange [17-19] are used, but only small part is devoted to methods oriented on matrix models (MMs) [8-10] and tools. In work [8] generalized algorithms for CTs, so-called matrix affine-permutation ciphers (MAPCs) based matrix affinity ciphers (MACs), were proposed. The results of simulation [7-10] of CTs used such MMs have shown their significant advantages: greater stability, increase in speed. In work [15, 16] based on of MACs the algorithm for creating digital blind signature (DBS) is proposed.

To implement cryptographic transformations, it is necessary to produce byte matrices, permutation matrices, and image matrices representing characters, codes, and bytes through permutations. To achieve uniform alignment of histograms of image spectral components and increase the entropy of the image cryptogram using matrix-algebraic model transformations, the decomposition of R, G, B channels and their bit components is required [10, 20, 21]. This necessitates the generation of numerous matrix keys and vectors. In other words, there is a need to develop a series of matrix transformations and keys to address these tasks.

B Problem Statement

Creation of generators of sequences of random numbers evenly distributed in a given interval is one of the main problems of developing information protection systems. Generating long random sequences is one of the important problems of classical cryptography [18-19]. Pseudorandom sequence generators (PSGs) are widely used to solve this problem. Generators of pseudo-random sequences must meet certain conditions [18, 19, 22, 23]. Sequences obtained with their help should have a uniform distribution (or at least close to uniform). This means that the number of zeros in the generated binary sequence should be approximately equal to the number of ones contained in the sequence. The gamma must be unpredictable, which means that it is impossible to predict the next bits of the sequence (gamma) by the previous segments of its bits, even if the type of the generator or the algorithm of its operation are known. To create an almost unpredictable gamut, it must, at a minimum have a very large period and a uniform law of distribution of bits or possible values of numbers or code words from the alphabet, in general, over the entire length of the gamut. In addition, the random values that make up the generated sequence must be statistically independent. This requirement means that there should be no correlation between individual bits and between groups of bits.

B Problem Statement

- These requirements are provided by the application of one-sided and computationally complex mathematical problems, for example, quadratic remainders modulo, the complexity of solving the problem of factorization of numbers. In order for the generator to be efficient, it must generate a very long sequence in the shortest possible time. For real-time systems, this requirement is particularly important. At the same time, for the use of generators in cryptography, they must be resistant to various attacks and non-standard situations and have a sufficiently long sequence period.
- Protocols for creating keys in the form of a bit sequence and the mathematical foundations of such protocols are considered in works [23-25], but they only partially consider the creation of permutation matrices, or simple bit sequences.
- At the same time, in this paper, we solve the problem of generating a sequence of permutations in their various isomorphic representations, not numbers or bits, as in traditional and well-known HPPs.

B Problem Statement

- We can use the latter only as arguments or seeds, based on of which a tuple-flow of vectors is formed, which are essentially permutations, or matrices of permutations, which are an isomorphic representation of permutations.
- Since in [17, 19], the issues of coordinating only the main matrix permutation of the general type were considered, and not a sequence (stream) of matrix permutations, the aim of this work is to model and study the processes of creating a sequence of matrix permutations for matrix-algebraic methods of cryptographic transformation in matrix-based systems, as well as to analyze the statistical and correlation characteristics of this sequence.

II. Presentation of the main material and research results

- Let's consider a situation where we use matrix permutations (MP) for cryptographic transformation of data blocks of size 256x256 bytes, which can be represented as either grayscale images or vectors of length 256 bytes (2048 bits). These matrix permutations and the processes of their creation are described in references [8-11], which also provide detailed instructions on their generation and use for cryptographic transformations.
- Since each data block undergoing multiple rounds of cyclic cryptographic transformations requires its own sequence of matrix keys (MK), there is a need to investigate the process of efficient and reliable generation of such a sequence of MK in the form of MP. Let the number of these MK also be equal to 256.
- In Fig.1 the results of modeling the process of generating a sequence of MK for such a case, performed in Mathcad using formulas and MP matrices are shown. If the main MK is a randomly generated matrix permutation KPX (Fig. 1), it is uniquely mapped to a vector permutation V_KPX with 256 components, as well as in the form of an image or a matrix of bytes of size 16x16. An important feature is that all 256 intensity levels in this image are unique.

$xa := 17 \quad xm := 13 \qquad ya := 7 \quad ym := 5$

$$C\_MKa := KPX^{xa} \quad C\_MKm := KPX^{xm}$$

$$V\_CMKa := C\_MKa \cdot N \qquad V\_CMKm := C\_MKm \cdot N$$

$$KeyCmv_i := \overrightarrow{\left[(V\_KPX + R\omega) \cdot V\_CMKm_i \cdot R\omega \right]}$$

$$KeyCm_i := \left(\overrightarrow{mod(KeyCmv_i + 257 \cdot 257, 257)} \right) - R\omega_i$$

$$KeyCmav_i := \overrightarrow{(KeyCm_i + V\_CMKa_i \cdot R\omega)}$$

$$KeyCma_i := \left(\overrightarrow{mod(KeyCmav_i, 256)} \right)$$

KPX·255 C_MKa·255 C_MKm·255

Fig. 1. Results of modeling the processes of generating an array of MK (MP).

II. Presentation of the main material and research results

- By utilizing the coordinated scalars xa and xm, raised to the power, we obtain two additional matrices, denoted as C_MKa and C_MKm (see Fig. 1), along with corresponding vectors denoted as V_CMKa and V_CMKm. These matrices and vectors, together with the vector V_KPX (which is the vector representation of KPX), are depicted in Fig. 2. Histograms of all these vectors (primary ones!) are horizontal lines, just like the vector representations of the created permutations, which are formed from V_KPX using an affine cipher and a pair of their vector components from vectors V_CMKa and V_CMKm (additional and multiplicative components).

II. Presentation of the main material and research results

These generated permutations are also represented as binary matrices, for example, KeyCmaP with a size of 256x256 (see Fig. 1), and labeled as KeyCmaP1-254.

In Fig. 3 Fragments from Mathcad windows are shown. 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 two 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. To study the quality of MKs (PMs) of the created series, to study their properties, we calculated all their possible mutual-correlation and normalized equivalence functions, which in Fig. 4 the Fragments from Mathcad windows are shown.

Note that the obtained results and their comparison also indicate that mutual-equivalence normalized functions are better than mutual-correlation functions. 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.5 and can go as frames of a video stream (colored image corresponds to three basic MKs).

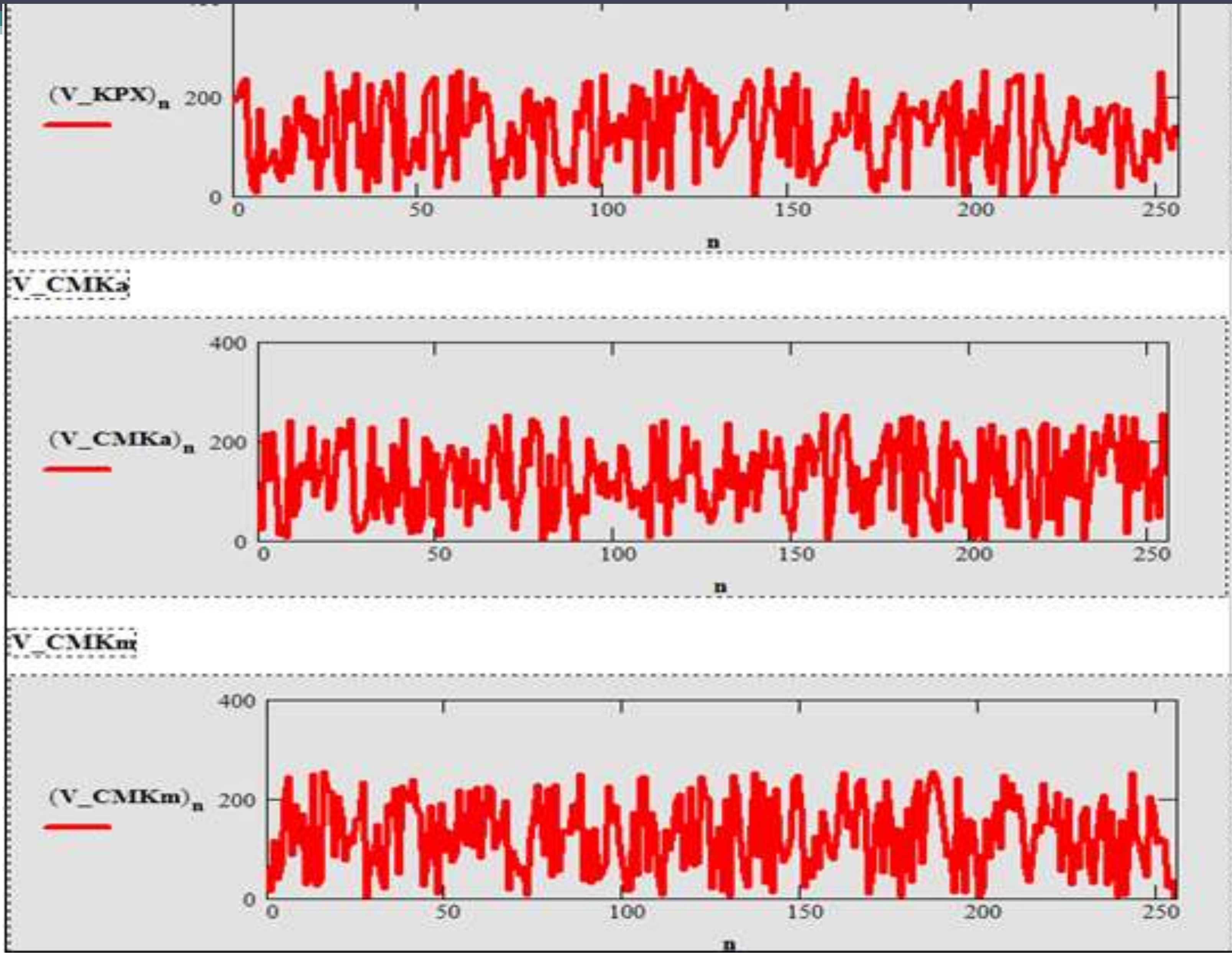

Fig. 2. Basic MKs for forming an array of MKs (MPs) in vector representations

II. Presentation of the main material and research results

- Since the histograms of all permutation matrix (their vectors) are horizontal lines, and their entropy is 8 bits, this means that cryptanalysis based on them becomes practically impossible. Furthermore, the main key and the two auxiliary keys are strictly confidential, allowing only authorized parties to create or have access to this sequence of matrix keys (MP). In general, only the main key and the aforementioned scalar keys xa and xm can be secret or agreed upon parties.

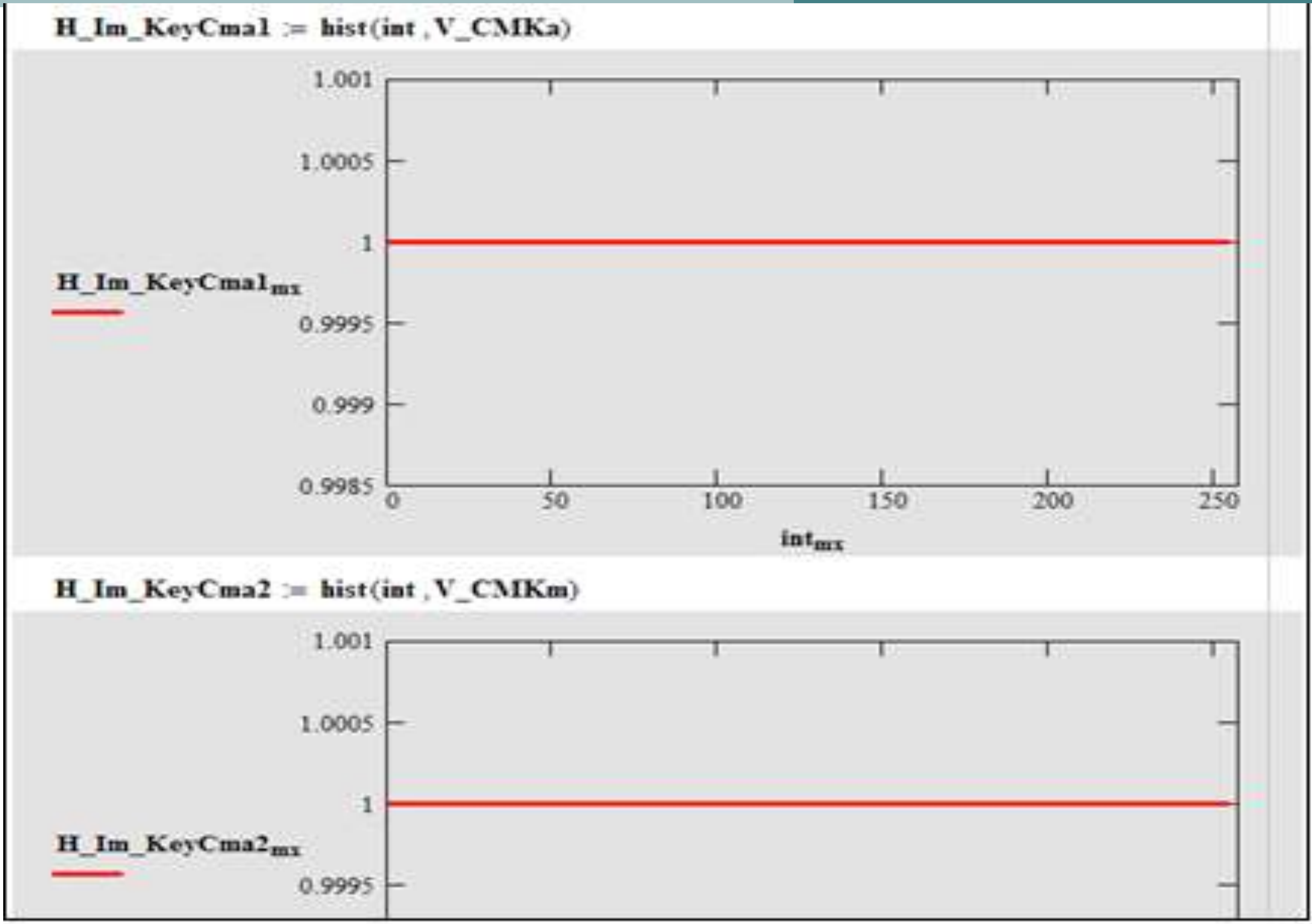

Fig. 3. Histograms of vector representations of basic and some generated MK (MP).

$V\_KPX^T =$

	0	1	2	3	4	5	6	7	8	9
0	191	202	225	236	77	19	7	176	49	63

$V\_CMKa^T =$

	0	1	2	3	4	5	6	7	8	9
0	98	23	215	121	218	130	13	30	8	241

$$\mathrm{mod}[[(\mathrm{mod}(192 \cdot 58, 257) - 1) + 98], 256] = 182$$

$$\mathrm{mod}[[(\mathrm{mod}(203 \cdot 58, 257) - 1) + 98], 256] = 50$$

$V\_CMKm^T =$

	0	1	2	3	4	5	6	7	8	9
0	58	14	117	39	68	201	243	88	187	110

$$\mathrm{mod}[[(\mathrm{mod}(203 \cdot 14, 257) - 1) + 23], 256] = 37$$

$KeyCma_0$	$KeyCma_1$	$KeyCma_{254}$	$KeyCma_{255}$
182	140	162	70
50	37	55	81
98	102	135	104
222	0	28	115
252	86	56	212
229	45	223	154
48	134	36	142
84	187	121	55
170	208	48	184
211	147	52	198
46	231	17	204
152	53	134	228
253	166	194	181
97	199	116	165
125	206	6	38
112	194	11	183

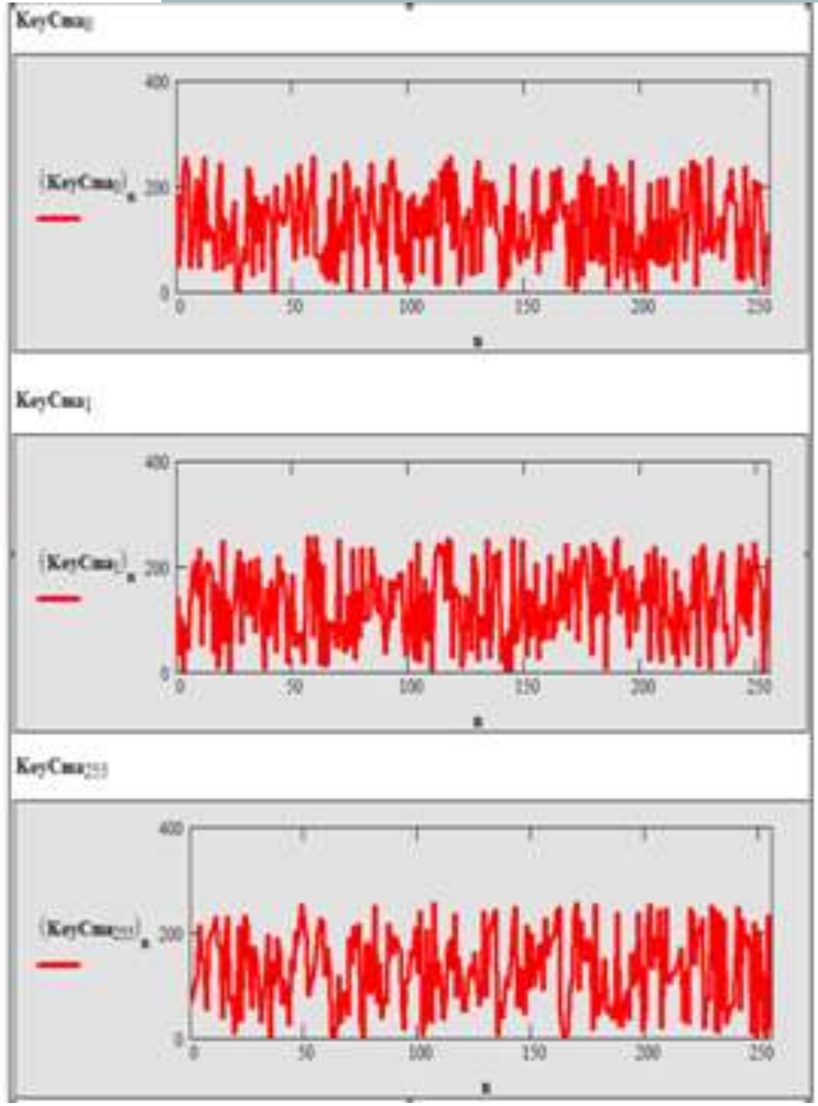

Fig. 4. Mathcad window fragments: one of the key generation procedures (left) and vector representations of some (zero-th, first, 255-th) generated (right) MK (MP).

II. Presentation of the main material and research results

- To assess the quality of the created sequences of matrix keys (MK) or matrix permutations (MP), we calculated all possible normalized cross-correlation and equivalence functions. These results are presented in fragments from the Mathcad program in Fig. 5-6 and confirm the high quality of these sequences. It should be noted that the comparison of the obtained results indicates the superiority of normalized equivalence functions over cross-correlation functions.
- Observing Fig.s 6-7, one can notice that one of the matrix keys (in this experiment, the 200th) has a similar appearance to another key. However, this can be explained by the fact that in this case, xm equals "1." This similarity can be easily eliminated by reducing the number of matrix keys in the sequence from 256 to 255, as specified in the chosen modeling and described in this context.

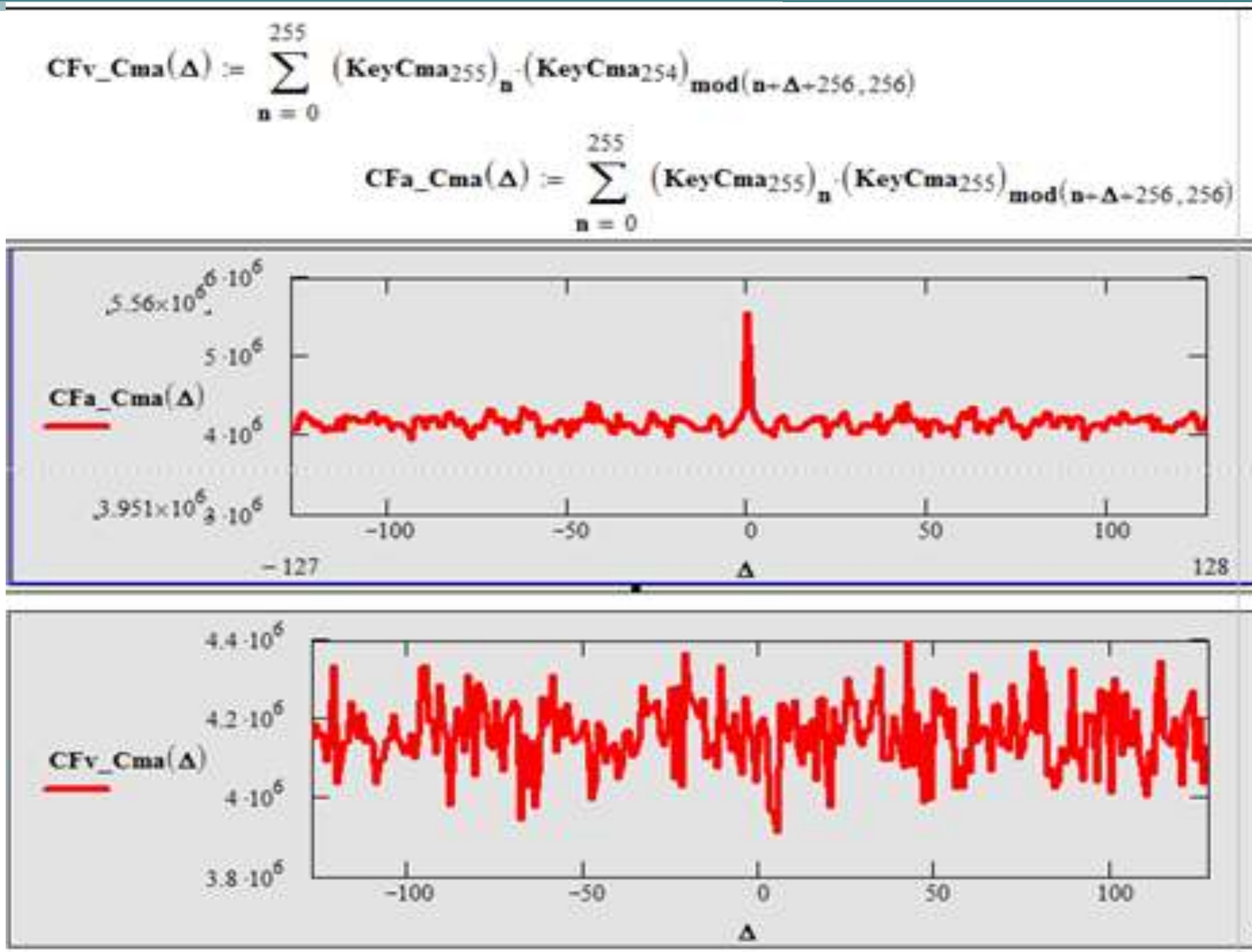

Fig. 5. Formulas from Mathcad window and representation of auto-correlation function CFa_Cma and cross-correlation function CFv_Cma depending on cyclic shift, displacement of elements in the MP vectors.

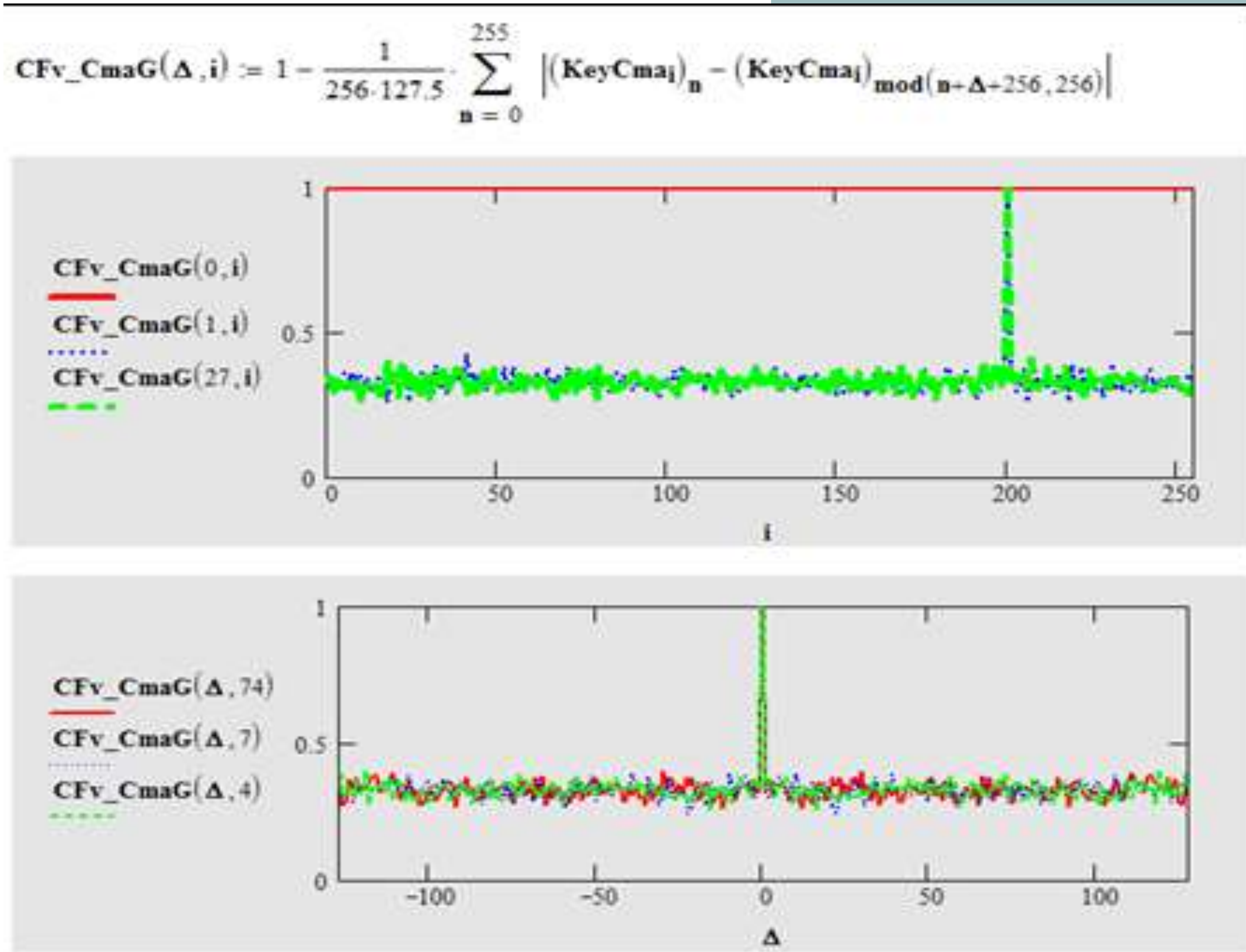

Fig. 6. Formulas from Mathcad window and form of cross-equivalence functions CFv_CmaG depending on the MP number (i) and cyclic shift, displacement of elements in the MP vectors.

II. Presentation of the main material and research results

- For ease of comprehension and more efficient transmission of the main matrix keys (MK) and sequences of created matrix permutations (MP), the latter are transformed into color or grayscale images using software modules, as shown in Fig. 7. These images can be transmitted as frames of a video stream (color image corresponds to the three main matrix keys). The BP_MAPC simulation with the generated keyset was done using Mathcad. Windows for GT simulation will be presented in the report. The essence of BP_MAPC is to apply to blocks, as a set of bytes (PIC_S), procedures for pixel-by-pixel multiplication / addition modulo with MK (direct / inverse). Simulation of the processes of direct / reverse CT TGD, images confirm the correctness of the models

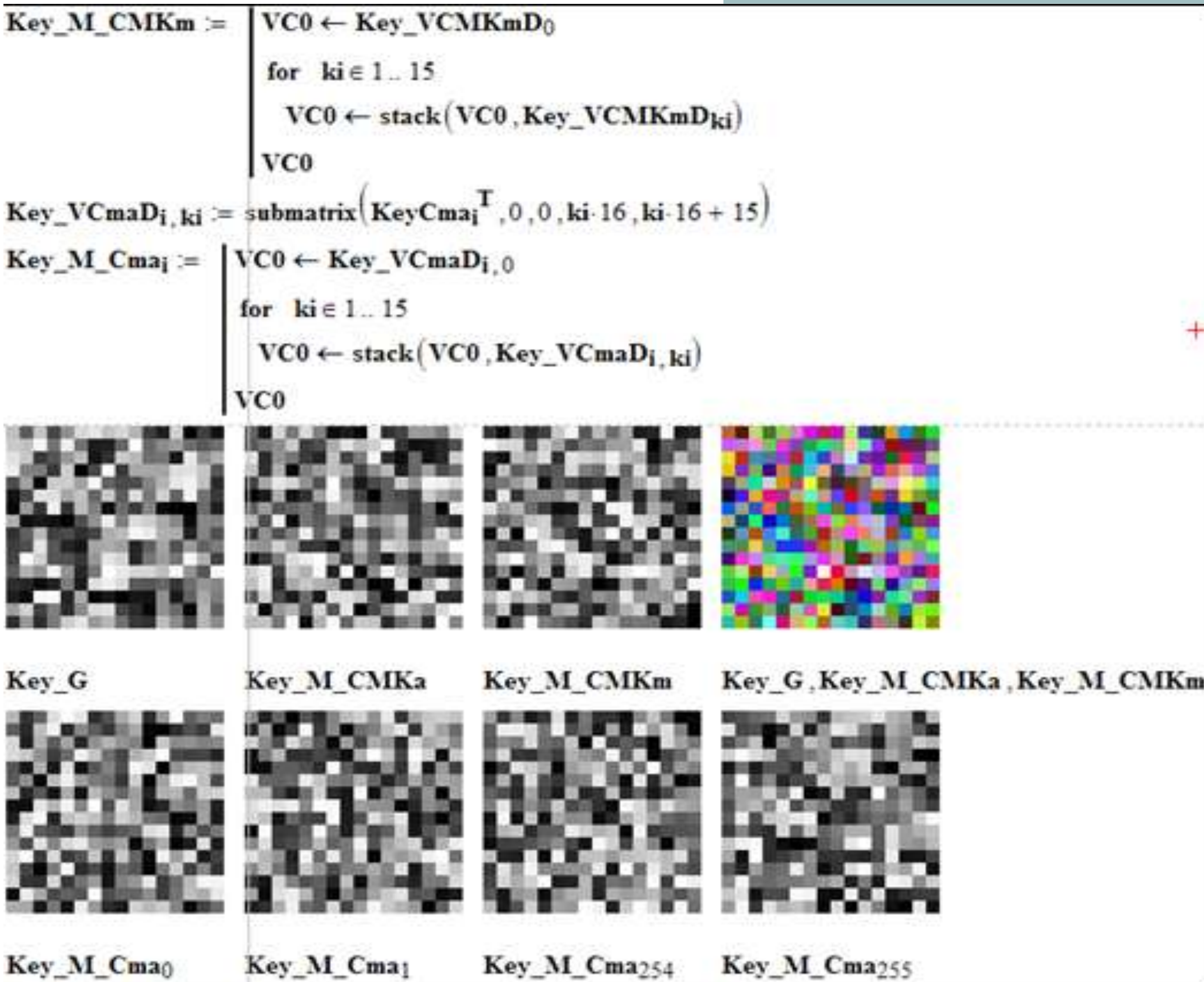

Fig. 7. Mathcad window fragments: Matrix representation of basic MK and a series of MP.

II. Presentation of the main material and research results

- In order to improve the algorithm, we propose to apply various current MKs to blocks and increase the size of MKs, blocks up to 256x256 bytes. Thus, the idea of BP_MAP ciphers of CT is to use the functional dependencies of their parameters on block indices and additional vector keys (VC). MP in the generally accepted form should be square with elements N x N ("0" or "1"), where $N = 2^{16}$. The power of the set of MPs, that is, their number, is estimated as N!, which gives huge values. Each block address can be represented by two bytes denoting two block coordinates. In [26, 27] questions were considered of creating by the parties a secret MMK of type P with isomorphic representations and the synthesis of set number of sub-keys of a similar type from it (will be covered in the report).

III. Conclusion

- A method of generating a series of matrix keys in the form of permutation matrices and their isomorphic representations, which are necessary for multi-page, block, matrix affine-permutation algorithms and matrix-algebraic models of cryptographic transformations, is proposed. The method is modeled in Mathcad. The properties of the pseudo-random sequence of generated matrix keys in the form of permutation matrices are investigated using mutual correlation and equivalence normalized functions, and the advantages of equivalence versus correlation are shown. The obtained results confirm the adequacy and reliability of this method.

REFERENCES

- [1] Ferguson N. and Schneier B. Practical Cryptography. John Wiley & Sons.2003.432 p..
- [2] Horbenko I.D., Horbenko Yu.I. Prykladna kryptolohiya. Teoriya. Praktyka. Zastosuvannya. Monohrafiya I.D. Horbenko. – Kharkiv: Fort, 2012. – 878 s.
- [3] Yemets′ V. Suchasna kryptohrafiya: Osnovni ponyattya / V. Yemets′, A. Mel′nyk, R. Popovych. – L′viv: BaK, 2003. – 144 s.: il.
- [4] Gorbenko I. D., Dolgov V.I., Rublinetskii V.I., Korovkin K.V. Methods of Information Protection in Communications Systems and Methods of Their Cryptoanalysis //Telecommunications and Radio Engineering. 1998. Volume 52, Issue 4, pp. 89-96.
- [5] Hu, Z., Gnatyuk, S., Okhrimenko, T., Tynymbayev, S., & Iavich, M. (2020). High-Speed and secure PRNG for cryptographic applications. International Journal of Computer Network and Information Security, 12(3), 1–10. https://doi.org/10.5815/ijcnis.2020.03.01
- [6] Security Comparison Between Wi-Fi 6 and 5G. https://forum.huawei.com/ enterprise/en/securitycomparison-between-wi-fi-6-and-5g/thread/615836-869
- [7] Mcginthy, J. M., & Michaels, A. J. (2019). Further analysis of prng-based key derivation functions. IEEE Access, 7, 95978–95986. https://doi.org/10.1109/access.2019.2928768

References

- [8] Gorbenko I., Kuznetsov A., Lutsenko M. and Ivanenko D. The research of modern stream ciphers //4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 207-210.
- [9] KuznetsovO., M. Lutsenko and D. Ivanenko, "Strumok stream cipher: Specification and basic properties, "2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 59-62
- [10] V.G. Krasilenko, V.M. Dubchak, "Cryptographic Transformations of Images based on Matrix Models of Permutations with Matrix-Bit-Map Decomposition and their Modeling," Bulletin of Khm. National University. Technical sciences, 2014, no. 1, pp. 74-79
- [11] V.G. Krasilenko, D.V. Nikitovich, "Modeling and Research of Cryptographic Transformations of Images based on their Matrix-Bit-Map Decomposition and Matrix Models of Permutations with Verification of Integrity," Electronics and Information Technologies, Lviv: National University, 2016, vol. 6, pp. 111-127.
- [12] A.Ya. Bilets′kyy, A.A. Bilets′kyy, D.A. Stetsenko, "Modyfikovanyy matrychnyy asymetrychnyy kryptohrafichnyy alhorytm Diffi-Khellmana," Shtuchnyy intelekt, 2010, № 3, s. 697-705
- [13] V.G. Krasilenko, A.A. Lazarev, D.V. Nikitovich, "The Block Parametric Matrix Affine-Permutation Ciphers (BP_MAPCs) with Isomorphic Representations and their Research," Actual Problems of Information Systems and Technologies, 2020, pp. 270-282.

References

- [14] V.G. Krasilenko, D.V. Nikitovich, "Modelyuvannya storinkovykh kryptohrafichnykh peretvoren′ masyviv kol′orovykh zobrazhen′ na osnovi matrychnykh modeley ta perestanovok," «Informatsiyno-komp″yuterni tekhnolohiyi – 2018»: Zbirnyk tez dopovidey IX Mizhnarodnoyi NTK, 20-21 kvitnya 2018 roku, Zhytomyr: Vyd. O. O. Yevenok, 2018, s. 73-77.
- [15] V. G. Krasilenko, A. A. Lazarev, and D. V. Nikitovich, "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, pp. 170-214.
- [16] Yu. I. Horbenko ta I. D. Horbenko, "Infrastruktury vidkrytykh klyuchiv. Systemy ETSP. Teoriya ta praktyka. Monohrafiya." Kharkiv: Fort, 2010, 593 p.
- [17] V. G. Krasilenko and D. V. Nikitovich, "Modeling of multi-step and multi-stage secret matrix key matching protocols," in "Computer-integrated technologies: education, science, production": scientific journal. Lutsk: LNTU, 2017, vol. 26, pp. 111-120. [Online]. Available: [http://ki.lutsk-ntu.com.ua/node/134/section/27]
- [18] M. A. Dabbah, W. L. Woo, and S. S. Dlay, "Secure Authentication for Face Recognition," presented at Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on, 2007.
- [19] M. Kutter, F. Jordan, and F. Bossen, "Digital Signature Of Color Images Using Amplitude Modulation," in Proc. Of the SPIE Storage and Retrieval for Image and Video Databases, 1997, vol. 3022, pp. 518-526

References

- [20] R. N. Kvyetnyy, Ye. O. Tytarchuk, and A. A. Hurzhiy, "Metod ta alhorytm obminu klyuchamy sered hrup korystuvachiv na osnovi asymetrychnykh shyfriv ECC ta RSA," in "Informatsiyni tekhnolohiyi ta komp'yuterna inzheneriya," 2016, no. 3, pp. 38-43.
- [21] V. Luzhets′kyy and I. Horbenko, "Metody shyfruvannya na osnovi perestanovky blokiv zminnoyi dovzhyny," in "Zakhyst informatsiyi," 2015, vol. 17, no. 2, pp. 169-175.
- [22] Yu. I. Hrytsyuk and P. Yu. Hrytsyuk, "Matematychni osnovy protsesu heneruvannya klyuchiv perestavlyannya z vykorystannyam shyfru Kardano," in "Naukovyy visnyk NLTU Ukrayiny," 2015, vol. 25.10, pp. 311-323.
- [23] Yu. I. Hrytsyuk and P. Yu. Hrytsyuk, "Metody i zasoby heneruvannya QP-matryts′ Fibonachchi-klyuchiv dlya realizatsiyi kryptohrafichnykh peretvoren′," in "Naukovyy visnyk NLTU Ukrayiny," 2015, vol. 25.6, pp. 334-351.
- [24]] V. G. Krasilenko, N. P. Yurchuk, and D. V. Nikitovich, "Zastosuvannya izomorfnykh matrychnykh predstavlen′ dlya modelyuvannya protokolu uz•hodzhennya sekretnykh klyuchiv-perestanovok znachnoyi rozmirnosti," in "Visnyk Khmel′nyts′koho natsional′noho universytetu. Tekhnichni nauky," Khmel′nyts′kyy, 2021, vol. № 2, pp. 78-88.
- [25] V. G. Krasilenko and D. V. Nikitovich, "Modeling of methods for generating flows of matrix permutations of significant dimension for cryptographic transformations of images," in Abstracts of the II All-Ukrainian STC Computer Technologies: Innovations, Problems, Solutions. Zhytomyr: Zhytomyr Polytechnic, 2019, pp. 67-77.

Thank you for attention!