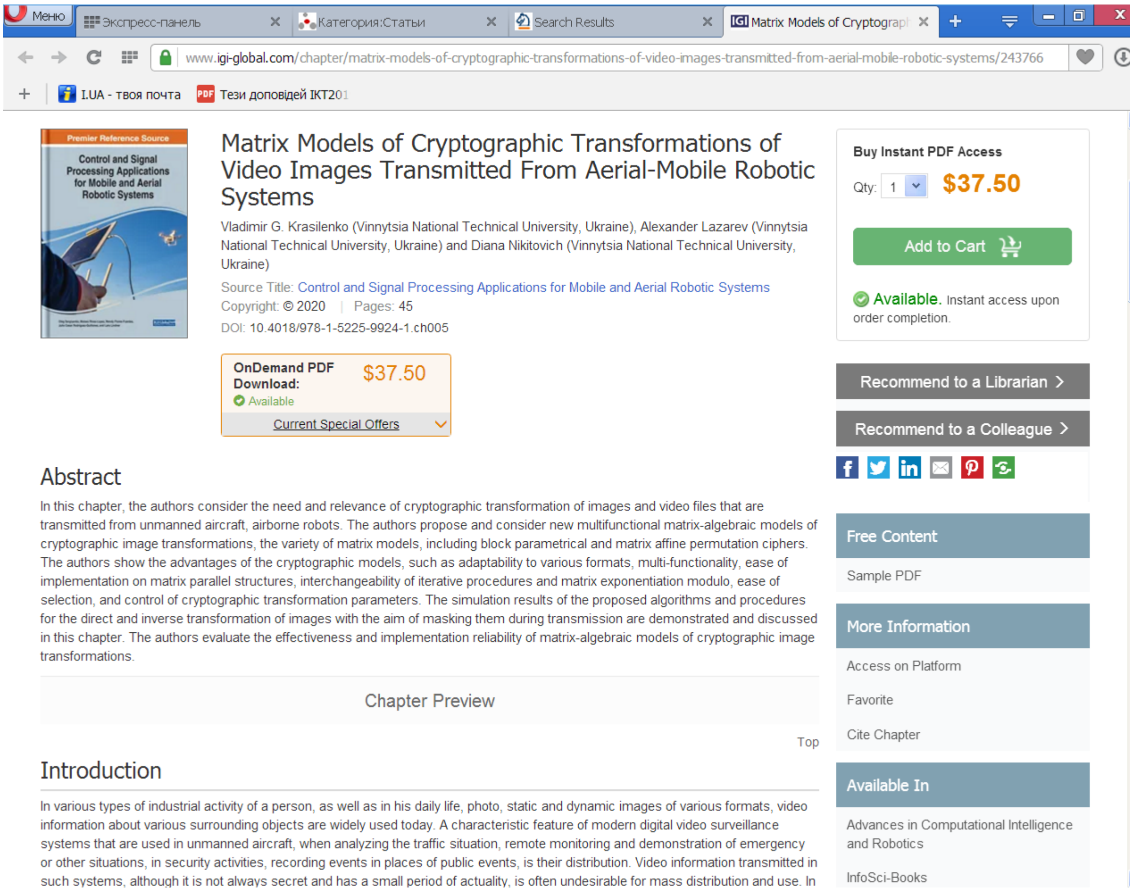
Krasilenko, Vladimir G. and Alexander Lazarev, and Diana Nikitovich. "Matrix Models of Cryptographic Transformations of Video Images Transmitted From Aerial-Mobile Robotic Systems." In Control and Signal Processing Applications for Mobile and Aerial Robotic Systems. edited by Oleg Sergiyenko , Moises Rivas-Lopez , Wendy Flores-Fuentes , Julio Cesar Rodríguez-Quiñonez , and Lars Lindner, 170-214. Hershey, PA: IGI Global, 2020. http://doi:10.4018/978-1-5225-9924-1.ch005


Меню
Экспресс-панель
Категория:Статьи
Search Results
Matrix Models of Cryptograph
www.igi-global.com/chapter/matrix-models-of-cryptographic-transformations-of-video-images-transmitted-from-aerial-mobile-robotic-systems/243766
I.UA - твоя почта
Тези доповідей ІКТ201
Premier Reference Source
Control and Signal Processing Applications for Mobile and Aerial Robotic Systems

Matrix Models of Cryptographic Transformations of Video Images Transmitted From Aerial-Mobile Robotic Systems

Vladimir G. Krasilenko (Vinnytsia National Technical University, Ukraine), Alexander Lazarev (Vinnytsia National Technical University, Ukraine) and Diana Nikitovich (Vinnytsia National Technical University, Ukraine)

Source Title: Control and Signal Processing Applications for Mobile and Aerial Robotic Systems
Copyright: © 2020 | Pages: 45
DOI: 10.4018/978-1-5225-9924-1.ch005

Abstract

In this chapter, the authors consider the need and relevance of cryptographic transformation of images and video files that are transmitted from unmanned aircraft, airborne robots. The authors propose and consider new multifunctional matrix-algebraic models of cryptographic image transformations, the variety of matrix models, including block parametrical and matrix affine permutation ciphers. The authors show the advantages of the cryptographic models, such as adaptability to various formats, multi-functionality, ease of implementation on matrix parallel structures, interchangeability of iterative procedures and matrix exponentiation modulo, ease of selection, and control of cryptographic transformation parameters. The simulation results of the proposed algorithms and procedures for the direct and inverse transformation of images with the aim of masking them during transmission are demonstrated and discussed in this chapter. The authors evaluate the effectiveness and implementation reliability of matrix-algebraic models of cryptographic image transformations.

Chapter Preview

Top

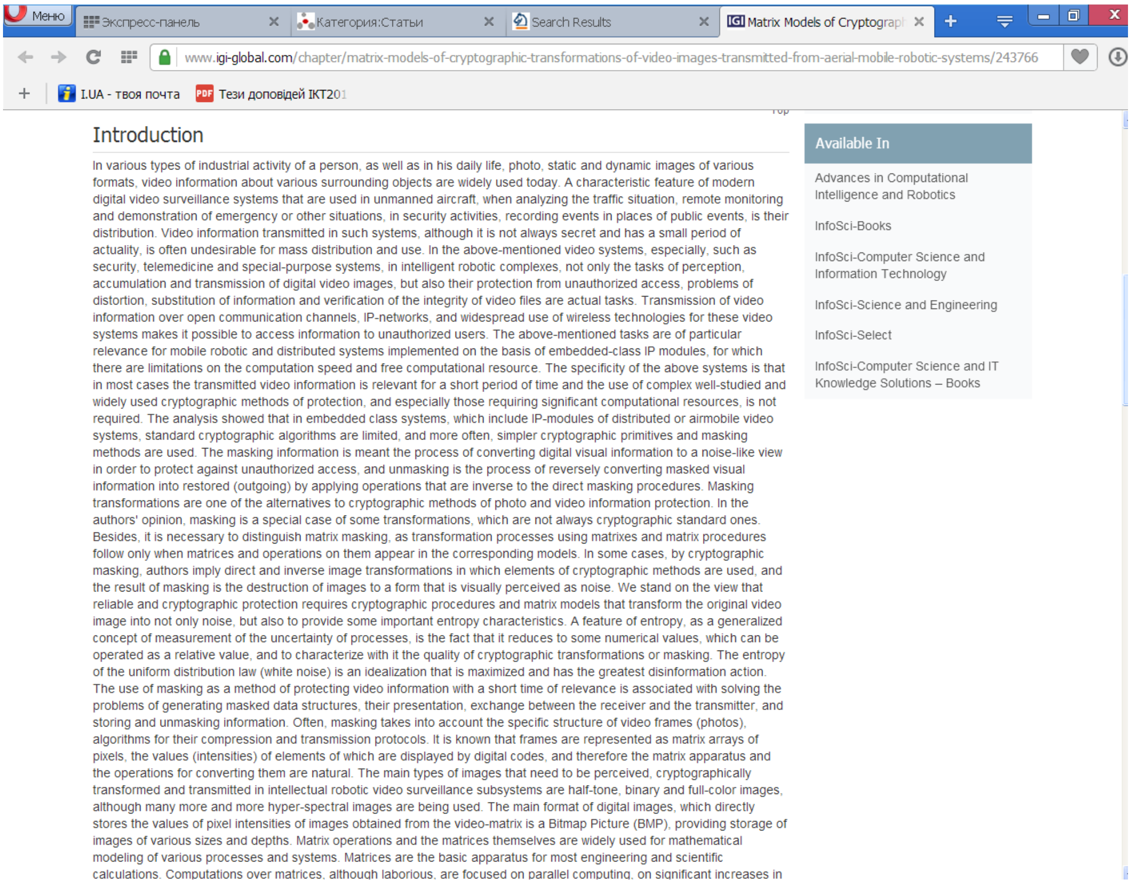
Introduction

In various types of industrial activity of a person, as well as in his daily life, photo, static and dynamic images of various formats, video information about various surrounding objects are widely used today. A characteristic feature of modern digital video surveillance systems that are used in unmanned aircraft, when analyzing the traffic situation, remote monitoring and demonstration of emergency or other situations, in security activities, recording events in places of public events, is their distribution. Video information transmitted in such systems, although it is not always secret and has a small period of actuality, is often undesirable for mass distribution and use. In

Free Content
Sample PDF

More Information
Access on Platform
Favorite
Cite Chapter

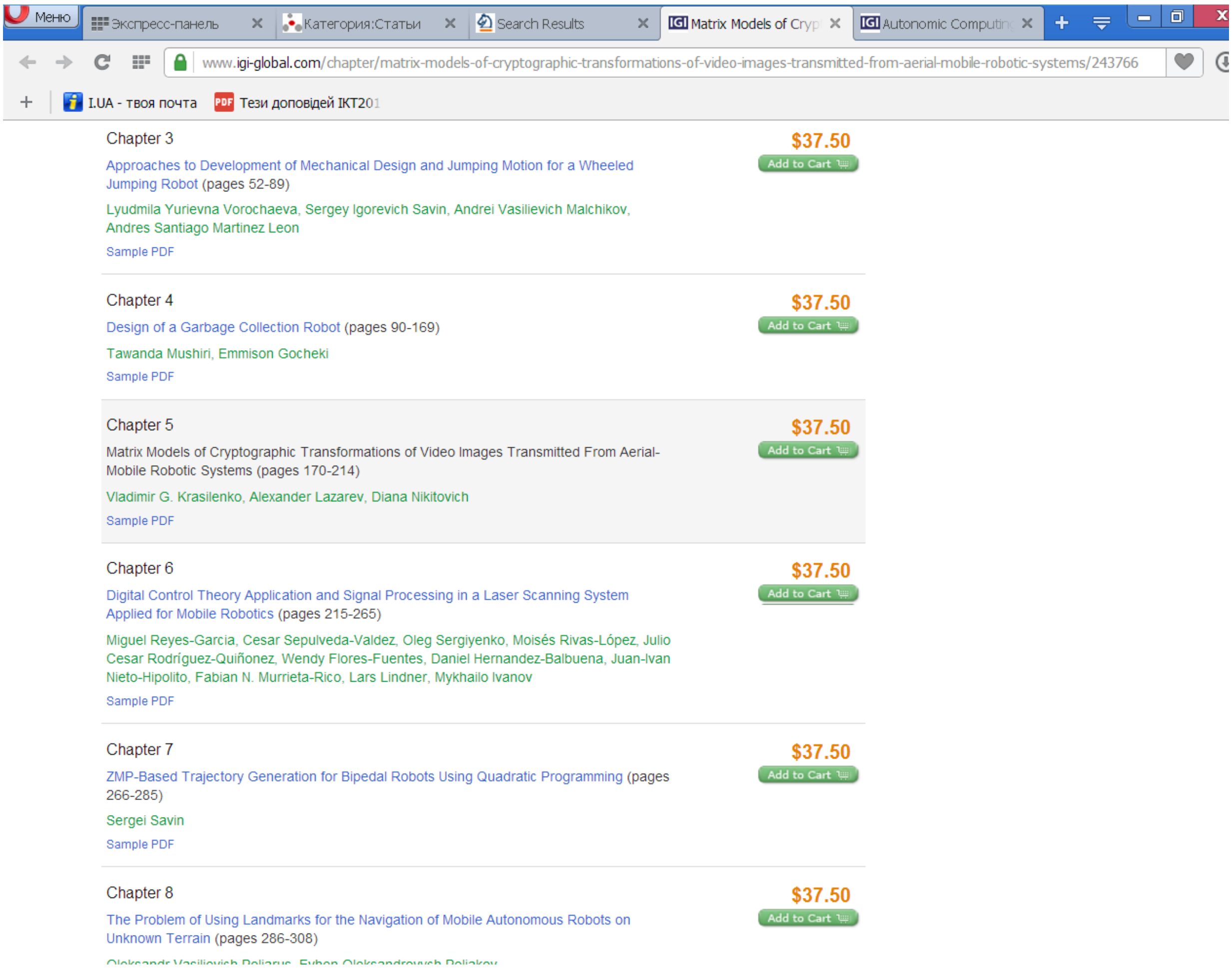
Available In
Advances in Computational Intelligence and Robotics
InfoSci-Books


Меню
Экспресс-панель
Категория:Статьи
Search Results
Matrix Models of Cryptograph
www.igi-global.com/chapter/matrix-models-of-cryptographic-transformations-of-video-images-transmitted-from-aerial-mobile-robotic-systems/243766
I.UA - твоя почта
Тези доповідей ІКТ201

Introduction

In various types of industrial activity of a person, as well as in his daily life, photo, static and dynamic images of various formats, video information about various surrounding objects are widely used today. A characteristic feature of modern digital video surveillance systems that are used in unmanned aircraft, when analyzing the traffic situation, remote monitoring and demonstration of emergency or other situations, in security activities, recording events in places of public events, is their distribution. Video information transmitted in such systems, although it is not always secret and has a small period of actuality, is often undesirable for mass distribution and use. In the above-mentioned video systems, especially, such as security, telemedicine and special-purpose systems, in intelligent robotic complexes, not only the tasks of perception, accumulation and transmission of digital video images, but also their protection from unauthorized access, problems of distortion, substitution of information and verification of the integrity of video files are actual tasks. Transmission of video information over open communication channels, IP-networks, and widespread use of wireless technologies for these video systems makes it possible to access information to unauthorized users. The above-mentioned tasks are of particular relevance for mobile robotic and distributed systems implemented on the basis of embedded-class IP modules, for which there are limitations on the computation speed and free computational resource. The specificity of the above systems is that in most cases the transmitted video information is relevant for a short period of time and the use of complex well-studied and widely used cryptographic methods of protection, and especially those requiring significant computational resources, is not required. The analysis showed that in embedded class systems, which include IP-modules of distributed or airmobile video systems, standard cryptographic algorithms are limited, and more often, simpler cryptographic primitives and masking methods are used. The masking information is meant the process of converting digital visual information to a noise-like view in order to protect against unauthorized access, and unmasking is the process of reversely converting masked visual information into restored (outgoing) by applying operations that are inverse to the direct masking procedures. Masking transformations are one of the alternatives to cryptographic methods of photo and video information protection. In the authors' opinion, masking is a special case of some transformations, which are not always cryptographic standard ones. Besides, it is necessary to distinguish matrix masking, as transformation processes using matrixes and matrix procedures follow only when matrices and operations on them appear in the corresponding models. In some cases, by cryptographic masking, authors imply direct and inverse image transformations in which elements of cryptographic methods are used, and the result of masking is the destruction of images to a form that is visually perceived as noise. We stand on the view that reliable and cryptographic protection requires cryptographic procedures and matrix models that transform the original video image into not only noise, but also to provide some important entropy characteristics. A feature of entropy, as a generalized concept of measurement of the uncertainty of processes, is the fact that it reduces to some numerical values, which can be operated as a relative value, and to characterize with it the quality of cryptographic transformations or masking. The entropy of the uniform distribution law (white noise) is an idealization that is maximized and has the greatest disinformation action. The use of masking as a method of protecting video information with a short time of relevance is associated with solving the problems of generating masked data structures, their presentation, exchange between the receiver and the transmitter, and storing and unmasking information. Often, masking takes into account the specific structure of video frames (photos), algorithms for their compression and transmission protocols. It is known that frames are represented as matrix arrays of pixels, the values (intensities) of elements of which are displayed by digital codes, and therefore the matrix apparatus and the operations for converting them are natural. The main types of images that need to be perceived, cryptographically transformed and transmitted in intellectual robotic video surveillance subsystems are half-tone, binary and full-color images, although many more and more hyper-spectral images are being used. The main format of digital images, which directly stores the values of pixel intensities of images obtained from the video-matrix is a Bitmap Picture (BMP), providing storage of images of various sizes and depths. Matrix operations and the matrices themselves are widely used for mathematical modeling of various processes and systems. Matrices are the basic apparatus for most engineering and scientific calculations. Computations over matrices, although laborious, are focused on parallel computing, on significant increases in

Available In
Advances in Computational Intelligence and Robotics
InfoSci-Books
InfoSci-Computer Science and Information Technology
InfoSci-Science and Engineering
InfoSci-Select
InfoSci-Computer Science and IT Knowledge Solutions – Books


Меню
Экспресс-панель
Категория:Статьи
Search Results
Matrix Models of Cryp
Autonomic Computin
www.igi-global.com/chapter/matrix-models-of-cryptographic-transformations-of-video-images-transmitted-from-aerial-mobile-robotic-systems/243766
I.UA - твоя почта
Тези доповідей ІКТ201

Chapter 3 $37.50 Add to Cart

Approaches to Development of Mechanical Design and Jumping Motion for a Wheeled Jumping Robot (pages 52-89)

Lyudmila Yurievna Vorochaeva, Sergey Igorevich Savin, Andrei Vasilievich Malchikov, Andres Santiago Martinez Leon

Sample PDF

Chapter 4 $37.50 Add to Cart

Design of a Garbage Collection Robot (pages 90-169)

Tawanda Mushiri, Emmison Gocheki

Sample PDF

Chapter 5 $37.50 Add to Cart

Matrix Models of Cryptographic Transformations of Video Images Transmitted From Aerial-Mobile Robotic Systems (pages 170-214)

Vladimir G. Krasilenko, Alexander Lazarev, Diana Nikitovich

Sample PDF

Chapter 6 $37.50 Add to Cart

Digital Control Theory Application and Signal Processing in a Laser Scanning System Applied for Mobile Robotics (pages 215-265)

Miguel Reyes-Garcia, Cesar Sepulveda-Valdez, Oleg Sergiyenko, Moisés Rivas-López, Julio Cesar Rodríguez-Quiñonez, Wendy Flores-Fuentes, Daniel Hernandez-Balbuena, Juan-Ivan Nieto-Hipolito, Fabian N. Murrieta-Rico, Lars Lindner, Mykhailo Ivanov

Sample PDF

Chapter 7 $37.50 Add to Cart

ZMP-Based Trajectory Generation for Bipedal Robots Using Quadratic Programming (pages 266-285)

Sergei Savin

Sample PDF

Chapter 8 $37.50 Add to Cart

The Problem of Using Landmarks for the Navigation of Mobile Autonomous Robots on Unknown Terrain (pages 286-308)

Oleksandr Vasilievich Poliarus, Evhen Oleksandrovych Poliakov

MLA

Krasilenko, Vladimir G.,et al. "Matrix Models of Cryptographic Transformations of Video Images Transmitted From Aerial-Mobile Robotic Systems." Control and Signal Processing Applications for Mobile and Aerial Robotic Systems,edited by Oleg Sergiyenko, et al., IGI Global, 2020, pp. 170-214. http://doi:10.4018/978-1-5225-9924-1.ch005

APA

Krasilenko, V. G., Lazarev, A., & Nikitovich, D. (2020). Matrix Models of Cryptographic Transformations of Video Images Transmitted From Aerial-Mobile Robotic Systems. In Sergiyenko, O., Rivas-Lopez, M., Flores-Fuentes, W., Rodríguez-Quiñonez, J. C., & Lindner, L. (Ed.), Control and Signal Processing Applications for Mobile and Aerial Robotic Systems (pp. 170-214). IGI Global. http://doi:10.4018/978-1-5225-9924-1.ch005

Chapter 5
Matrix Models of Cryptographic Transformations of Video Images Transmitted From Aerial-Mobile Robotic Systems

Vladimir G. Krasilenko
Vinnytsia National Technical University, Ukraine

Alexander Lazarev
Vinnytsia National Technical University, Ukraine

Diana Nikitovich
Vinnytsia National Technical University, Ukraine

ABSTRACT

In this chapter, the authors consider the need and relevance of cryptographic transformation of images and video files that are transmitted from unmanned aircraft, airborne robots. The authors propose and consider new multifunctional matrix-algebraic models of cryptographic image transformations, the variety of matrix models, including block parametrical and matrix affine permutation ciphers. The authors show the advantages of the cryptographic models, such as adaptability to various formats, multi-functionality, ease of implementation on matrix parallel structures, interchangeability of iterative procedures and matrix exponentiation modulo, ease of selection, and control of cryptographic transformation parameters. The simulation results of the proposed algorithms and procedures for the direct and inverse transformation of images with the aim of masking them during transmission are demonstrated and discussed in this chapter. The authors evaluate the effectiveness and implementation reliability of matrix-algebraic models of cryptographic image transformations.

DOI: 10.4018/978-1-5225-9924-1.ch005

INTRODUCTION

In various types of industrial activity of a person, as well as in his daily life, photo, static and dynamic images of various formats, video information about various surrounding objects are widely used today. A characteristic feature of modern digital video surveillance systems that are used in unmanned aircraft, when analyzing the traffic situation, remote monitoring and demonstration of emergency or other situations, in security activities, recording events in places of public events, is their distribution. Video information transmitted in such systems, although it is not always secret and has a small period of actuality, is often undesirable for mass distribution and use. In the above-mentioned video systems, especially, such as security, telemedicine and special-purpose systems, in intelligent robotic complexes, not only the tasks of perception, accumulation and transmission of digital video images, but also their protection from unauthorized access, problems of distortion, substitution of information and verification of the integrity of video files are actual tasks. Transmission of video information over open communication channels, IP-networks, and widespread use of wireless technologies for these video systems makes it possible to access information to unauthorized users. The above-mentioned tasks are of particular relevance for mobile robotic and distributed systems implemented on the basis of embedded-class IP modules, for which there are limitations on the computation speed and free computational resource. The specificity of the above systems is that in most cases the transmitted video information is relevant for a short period of time and the use of complex well-studied and widely used cryptographic methods of protection, and especially those requiring significant computational resources, is not required. The analysis showed that in embedded class systems, which include IP-modules of distributed or airmobile video systems, standard cryptographic algorithms are limited, and more often, simpler cryptographic primitives and masking methods are used. The masking information is meant the process of converting digital visual information to a noise-like view in order to protect against unauthorized access, and unmasking is the process of reversely converting masked visual information into restored (outgoing) by applying operations that are inverse to the direct masking procedures. Masking transformations are one of the alternatives to cryptographic methods of photo and video information protection. In the authors' opinion, masking is a special case of some transformations, which are not always cryptographic standard ones. Besides, it is necessary to distinguish matrix masking, as transformation processes using matrixes and matrix procedures follow only when matrices and operations on them appear in the corresponding models. In some cases, by cryptographic masking, authors imply direct and inverse image transformations in which elements of cryptographic methods are used, and the result of masking is the destruction of images to a form that is visually perceived as noise. We stand on the view that reliable and cryptographic protection requires cryptographic procedures and matrix models that transform the original video image into not only noise, but also to provide some important entropy characteristics. A feature of entropy, as a generalized concept of measurement of the uncertainty of processes, is the fact that it reduces to some numerical values, which can be operated as a relative value, and to characterize with it the quality of cryptographic transformations or masking. The entropy of the uniform distribution law (white noise) is an idealization that is maximized and has the greatest disinformation action. The use of masking as a method of protecting video information with a short time of relevance is associated with solving the problems of generating masked data structures, their presentation, exchange between the receiver and the transmitter, and storing and unmasking information. Often, masking takes into account the specific structure of video frames (photos), algorithms for their compression and transmission protocols. It is known that frames are represented as matrix arrays of pixels, the values (intensities) of elements of which are displayed by digital codes, and therefore the matrix apparatus and the operations for converting them are natural. The main types of images that need to be perceived, cryptographically transformed and transmitted in intellectual robotic video surveillance subsystems are half-tone, binary and full-color images, although many more and more hyper-spectral images are being used. The main format of digital images, which directly stores the values of pixel intensities of images obtained from the video-matrix is a Bitmap Picture (BMP), providing storage of images of various sizes and depths. Matrix operations and the matrices themselves are widely used for mathematical modeling of various processes and systems. Matrices are the basic apparatus for most engineering and scientific calculations. Computations over matrices, although laborious, are focused on parallel computing, on significant increases in computational performance, and are a classic example and direction for the further development of more intelligent computer architectures of parallel action. The emerged multi-core processors, graphics accelerators, digital signal processing (DSP) processors, structures on the FPGA, essentially support vector and matrix calculations and increase the speed and performance of the latters. Therefore, it is precisely for more modern hardware implementations that matrix models are ideally suited for implementations of cryptographic or similar methods for transforming and masking information objects in order to protect them during transmission. Matrix algebra and its operations are well studied, they are structured, regular, and easily mapped to hardware matrix structures that provide parallelization of computations, increasing computational performance and efficiency. In addition, such structures are more efficiently implemented using DSP or FPGA, which is important for systems of embedded classes, especially small and mobile ones. The actual task is to create such cryptographic procedures for direct and inverse transformation of video information, which use fully matrix models and procedures that are easily mapped to the corresponding matrix equipment. At the same time ensuring their simplicity, meeting the requirements of speed and computation performance while ensuring the best entropy characteristics .

Review and Analysis of Publications and Formulation of Problems and Challenges

The necessity of solving theoretical and practical tasks of information security and achieving the necessary level of information protection for state, military, commercial and private content caused the corresponding accelerated development of cryptography and related new scientific disciplines. In the era of electronic communications, the need to process and transmit specific text and graphic documents (TGDs) in the form of digital, table data, drawings, charts, diagrams, signatures, visas, resolutions, etc., has essentially increased, and the data are essentially 2D arrays (images) of significant dimension. In addition, the sharing of new tasks in which cryptographic transformations over multidimensional signals is required, among which a variety of semi-tones, color multispectral images, 2-D, 3-D, and even 4-D arrays (Yemets, 2003; Khoroshko, 2003; Korkishko, 2003; Kovalchuk, 2009; Rashkevich, 2009; Deergha, 2011; Han Shuihua, 2005; Chin-Chen, 2001) occupy an important place. In recognition, identification, biometric, navigation monitoring systems, robotics, intelligent management, when deciding, it is necessary to process and transmit a large number of various images in encrypted form, for example, fingerprints, photographs of persons, images of moving objects, iris eye retina, etc. Expansion of the spectral range that is perceived by modern multisensory remote sensing and monitoring systems has necessitated the processing of large arrays of large-scale multi-spectral images. Since this information is often confidential, there is an urgent need for cryptographic transformations to protect against unauthorized access. Many TGDs contain restricted access information that should be reported to tax and other government agencies, in a timely manner and in encrypted form, transmitting over communication channels and providing only authorized access, to certify their digital signatures. Authorized access many information resources such as library, archival and book funds, scientific publications, patent documents, which are formed in the process of activities of information actors, can be provided with appropriate technologies of cryptography and measures with the issuance of permits, certificates and access keys.

For such information security purposes, methods and tools for cryptographic transformations (CTs) of information arrays or images (Yemets, 2003; Khoroshko, 2003; Korkishko, 2003; Kovalchuk, 2009; Rashkevich, 2009; Deergha, 2011; Han Shuihua, 2005; Chin-Chen, 2001; Krasilenko, 2004; Krasilenko, 2006), procedures and protocols for the formation of keys and their exchange (Yemets, 2003; Krasilenko, 2012; Krasilenko, 2008) are used. Among their great variety (Yemets, 2003; Khoroshko, 2003; Korkishko, 2003; Kovalchuk, 2009; Rashkevich, 2009; Deergha, 2011; Han Shuihua, 2005; Chin-Chen, 2001; Krasilenko, 2004; Krasilenko, 2006) most of them focused on sequential scalar processing of TGD blocks transformed into digital formats, and only a small part is devoted to methods and algorithms oriented on matrix models (Krasilenko, 2012; Krasilenko, 2012; Krasilenko, 2011; Krasilenko, 2009; Krasilenko, 2012; Krasilenko, 2013; Krasilenko, 2013; Krasilenko, 2014; Krasilenko, 2010) and matrix specialized algorithms and tools. At the same time, the emergence of parallel algorithms, and especially matrix multiprocessor, matrix linear-algebraic, specialized multi-core, parallel and matrix (image-type) processors (Korkishko, 2003; Krasilenko, 2004) contributed to the reorientation in the study of image CTs on these new tools and the creation and corresponding models of matrix type (MT) (Krasilenko, 2012; Krasilenko, 2012; Krasilenko, 2011; Krasilenko, 2009). In addition, the urgency of the problem of creating new high-performance models, algorithms, protocols for processing and cryptographic transformations of images is confirmed by the significant increase in the number of works devoted to encryption and decoding of images in recent years (Kovalchuk, 2009; Rashkevich, 2009; Deergha, 2011; Han Shuihua, 2005; Chin-Chen Chang, 2001; Krasilenko, 2012; Krasilenko, 2009; Krasilenko, 2012; Krasilenko, 2013; Krasilenko, 2013; Krasilenko, 2014; Krasilenko, 2010; Krasilenko, 2016; Krasilenko, 2016; Krasilenko, 2016). 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.

Analysis of recent research and publications. The results of modeling the processes of cryptographic transformations of images on the basis of the proposed work by V.G. Krasilenko and the investigated matrix algorithms and models of cryptographic protection show their advantages. For example in (Krasilenko, 2006; Krasilenko, 2006) matrix algorithms and the implementation on the Delphi language in CryptoFax program were considered. It has been shown that the developed methods of permutations are resistant to the effects of disturbances and various distortions. The disadvantage of the CryptoFax program was that the transformations did not change the histogram of converted ciphered images. Therefore, in order to eliminate this disadvantage and improve the stability of the algorithms of cryptographic transformations of images, generalization of affine ciphers and their expansion into matrix cases (Krasilenko, 2009) were proposed. Experiments in the MathCad environment partially demonstrated the possibilities and advantages for practical applications of matrix algorithms for cryptographic protection on the basis of more generalized matrix affinity ciphers (MACs). In Krasilenko (2012) and Krasilenko (2011) more generalized matrix algorithms for cryptographic transformations of images and so-called matrix affine-permutation algorithms (MAPA) (Krasilenko,

2012) based on modifications of known affine ciphers were proposed and modified. The results of simulation (Krasilenko, 2012; Krasilenko, 2012; Krasilenko, 2011; Krasilenko, 2009) of processes of cryptographic transformations of multi-gradation and color images (Krasilenko, 2010) on the basis of such models and algorithms have shown their significant advantages over traditional scalar affine asymmetric ciphers such as: greater stability, increase in speed, the possibility of parallel computing procedures and processes and implement them using parallel problem-specific tools, matrix processors. In work (Krasilenko, 2011) 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 of a developed and practically verified program for the formation and verification of such DBS are presented. Such matrix cryptographic models, algorithms and cryptographic systems based on them are better and more effectively based on completely parallel matrix computing devices, since they are described purely by mathematical matrix models, which significantly increase the processing efficiency during transformations and reduces the time for their execution.

The results of modeling algorithms for creating a 2D key are also known (Krasilenko, 2012; Krasilenko, 2008), the essence of which is the synthesis of known protocols for creating and generating keys on the matrix case, and the formation and description of these protocols using matrix models. Paper (Krasilenko, 2012) is devoted to creation of DBS on TGD, but on the basis of other models of matrix type. One of the main components of the most generalized matrix affine-permutation ciphers or MAPA, proposed and investigated in paper (Krasilenko, 2012), 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 (Krasilenko, 2013; Krasilenko, 2013; Krasilenko, 2014; Krasilenko, 2016; Krasilenko, 2016). However, as shown in papers (Krasilenko, 2013; Krasilenko, 2014), the CPs on their basis, without additional operations, do not modify histograms of images or TGDs, and the proposed modified MM_Ps with decomposition of bit sections eliminate this defect, although in some cases they require two vector keys (VK) in addition to two matrix keys (MK). At the same time, for most of the above-mentioned works, there is a common significant disadvantage, especially for work related to MAC (Krasilenko, 2009; Krasilenko, 2010), MAPA (Krasilenko, 2009) and the like (Krasilenko, 2012; Krasilenko, 2012; Krasilenko, 2011; Krasilenko, 2014; Krasilenko, 2016; Krasilenko, 2016; Krasilenko, 2016), which requires the use of at least two MK, if implemented in models MAC, MAPA, MT and multiplicative and additive matrix components. But the kind of MK that is used is of two types: in the form of random images (basically black and white 8-bit) for MAC and square matrix of permutations for the implementation of MM_P and algorithms on them (Krasilenko, 2013; Krasilenko, 2013; Krasilenko, 2014). The first kind is less investigated. Therefore, the search for ways to improve the MAC and especially the multi-step MAC, MAPA (Krasilenko, 2012) in order to reduce the number of MKs to one, while maintaining stability and other characteristics of the matrix models (MM), their experimental verification on various images is a necessary task and which is justified by the above survey of publications.

Formulation of the problem. It is necessary to further modify and improve the well-known MACs with spectral decomposition for the CT over color images in order to simplify, improve and to study the models that implement MAC in different environments, to identify their specific features of specific applications and expansion their functional capabilities. Testing the created models, carrying out experiments with real images of different formats and dimensionalities allow assessing their adequacy, characteristics, indicators and features.

Therefore, the purpose of this work is to study and modify such modifications and enhancements of the MACs in the Mathcad software environment for the purpose of their use in the CT over black-and-white and color images, including large-scale and multi-spectral, in which the number of necessary matrix keys for these transformations would be reduced to one, so-called main or basic, while retaining the same functionality. One of the sub-tasks is an experimental verification of the correctness and quality of the work of such MAC in their work with different types and formats, image sizes to study their impact on indicators, characteristics of ciphers, models and algorithms for their implementation.

PRESENTATION OF THE MAIN MATERIAL AND RESEARCH RESULTS

Theoretical Foundations of Matrix Affine Ciphers

Let's recall some of the simplest theoretical foundations of the matrix affine ciphers (MAC). The encryption and decryption processes on the basis of the MAC for the message of an arbitrary form and size of the matrix **M** and for the created corresponding cryptogram **C** using cryptographic transformations (CT) described by the matrix model (MM), which are expressed by the following matrix formulas (Krasilenko, 2009):

$$\mathbf{C} = \left(\mathbf{M} \underset{N}{\otimes} \mathbf{A} \underset{N}{+} \mathbf{S}\right); \quad \mathbf{M} = (\mathbf{C} \underset{N}{\otimes} \mathbf{AD} \underset{N}{+} \mathbf{SD});$$

where **A** and **S** – two keys (multiplicative and additive components) for encryption in the form of matrices, **AD** and **SD** – decryption keys, moreover, **AD** – respectively, the multiplicative component of the matrix affine cipher, and **SD** – additive component of the matrix affine cipher, **N** – matrix, all elements of which are equal to n (simple large number), and components of all matrices are selected from the range 1÷(n-1), in addition, symbols $\underset{N}{\otimes}$ and $\underset{N}{+}$ denote element-wise matrix multiplication and matrix addition by modulo N.

To reduce the number of matrix keys, you can use the following formulas for one-key MAC:

$$\mathbf{C}=\left(\mathbf{M}\underset{N}{\otimes}\mathbf{A}\underset{N}{+}\mathbf{AD}\right);\quad \mathbf{M}=(\mathbf{C}\underset{N}{\otimes}\mathbf{AD}\underset{N}{+}(\text{-}\mathbf{AD}\underset{N}{\otimes}\mathbf{AD}));$$

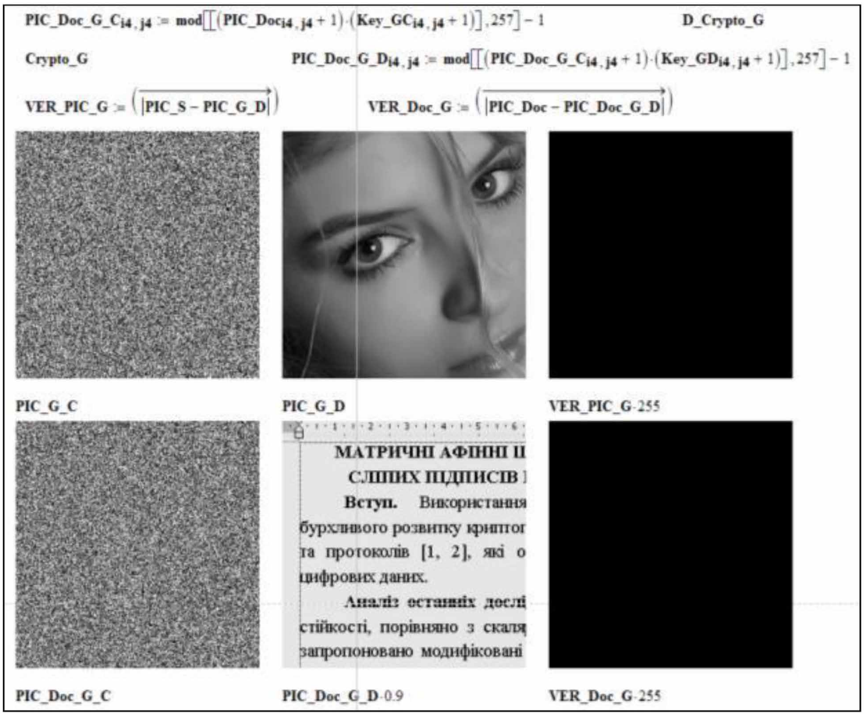
in this case **S= AD, SD=** $(\text{-}\mathbf{AD}\underset{N}{\otimes}\mathbf{AD})$.

Simulation Results of Matrix Affine Ciphers

Let's consider the essence of MAC algorithms on the MM with spectral decomposition basis. The offered modification of the MM MAC is essentially one matrix key (MK) for the corresponding both multiplicative and additive direct and inverse transformations that are components of one or multi-step MAC and implement cryptographic procedures for black and white or for all spectral components of color images. The idea is that the secret MK, which is selected or generated by known methods in the form of pseudo-random black and white or multi-level image with dimensions equal to the size of the input image. There is always, under the fulfillment of some simple additional conditions, the inverse matrix key that we denote as MK, and its elements are reversed by the corresponding modulo to the MK elements. This idea and its explanation were proposed by Krasilenko V.G. and are covered in our previous works (Krasilenko, 2009; Krasilenko, 2012), so here we note only the fact that when using a simple number 257 as the modulo, the entire range of 0-255 graduations of the 8-bit image which are displaced in the range 1-256, will have unambiguous inverse values in the same range of 1-256, and hence with their inverse shift and in the range of 0-255, that is, have a similar 8-bit representation. Before moving to some the new suggestions and improvements, let's consider the simulation results of the simplest MAC with only one multiplicative component, which is a generalization of the scalar linear cipher to the matrix case. In the first of a series MAC simulation experiments conducted with the Mathcad software, we recreated the direct and inverse cryptographic processes over two different images (C) (256x256) using the MK Key_GC and its associated inverse MKi Key_GD. The Experimental results are shown in Fig. 1 and testify the correct and adequate work of the models. The formulas used for transformations are shown in Fig. 1, especially in the scalar form, and those used for verification in the matrix form (left in the 1st and 2nd rows - cryptograms, in the center are decoded images, they are initial, in the right there are differences (zero) matrix). The inscriptions in the Figure 1 are fuzzy and blurry.

Our second idea is to use the inverse MKi for the second step, namely the additive component, for the direct transformation of the MAC, since the use of the direct MK is primitive. Since the matrix **SD** is a matrix, all elements of which are equal to (-1). And since, in essence, the MK and MKi are secret and interconnected, this leads to the need for the two parties to coordinate or formally create only one MK in the process of creating and transmitting encrypted data. At the same time, it is not desirable to apply the same MK when applying MAC for cryptographic transformations of color images. Let's move on to the application of the second idea and its verification by encrypting and deciphering a color image, using each of its components R, G, B of its MK, that is three random R, G, B components, equivalent

Figure 1. The simulation results of the processes of direct and inverse cryptographic transformations over two images by the matrix affinity cipher: the formulas used for the multiplicative component of the MAC, encrypted, decrypted and difference matrixes



$PIC\_Doc\_G\_C_{i4,j4} := \mathrm{mod}\left[\left[(PIC\_Doc_{i4,j4}+1)\cdot(Key\_GC_{i4,j4}+1)\right],257\right]-1$ D_Crypto_G

Crypto_G $PIC\_Doc\_G\_D_{i4,j4} := \mathrm{mod}\left[\left[(PIC\_Doc\_G\_C_{i4,j4}+1)\cdot(Key\_GD_{i4,j4}+1)\right],257\right]-1$

$VER\_PIC\_G := \left(\overrightarrow{|PIC\_S - PIC\_G\_D|}\right)$ $VER\_Doc\_G := \left(\overrightarrow{|PIC\_Doc - PIC\_Doc\_G\_D|}\right)$

PIC_G_C PIC_G_D VER_PIC_G·255

МАТРИЧНІ АФІННІ Ш

СЛІПИХ ПІДПИСІВ І

Вступ. Використання

бурхливого розвитку криптог

та протоколів [1, 2], які о

цифрових даних.

Аналіз останніх дослі

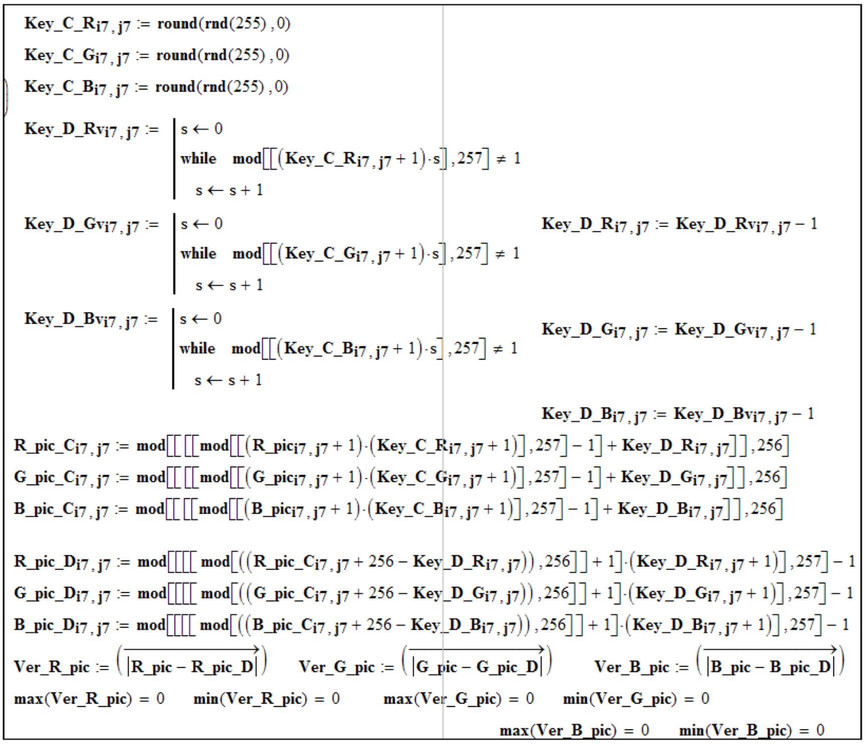
стійкості, порівняно з скаля

запропоновано модифіковані

PIC_Doc_G_C PIC_Doc_G_D·0.9 VER_Doc_G·255 to one MK in color format. Figure 2 shows one of the windows with the formulas that were used to generate keys, direct and inverse to them in modulo 257, encrypt and decrypt each R, G, B_pic component of C (600 x 549), three MK Key_C_ (R, G, B) and Key_D_ (R, G, B) respectively.

Fig. 3 shows the results of a MAC-based CT with only one MK for each component: a color output image, MK (1 row, right), a cryptogram (2 rows, left) and a decoded image. They testify to the correct operation of models for such modification of MAC. We note here that the components of the CT are executed in elementary matrix procedures of multiplication and addition, respectively, by modulo 257 and 256, using practically one corresponding MK, since the inverse key MKi is essentially an additive component of the MAC.

Figure 2. The Mathcad window with formulas for the CT over color image MAC when using spectral components, but only one MK, which performs a multiplicative direct transformation, and the inverse MKi - multiplicative, direct and inverse additive transformations.



$$\text{Key\_C\_R}_{i7,j7} := \text{round}(\text{rnd}(255),0)$$

$$\text{Key\_C\_G}_{i7,j7} := \text{round}(\text{rnd}(255),0)$$

$$\text{Key\_C\_B}_{i7,j7} := \text{round}(\text{rnd}(255),0)$$

```
Key_D_Rv_{i7,j7} :=
    $s \leftarrow 0$
    while  $\text{mod}[[(\text{Key\_C\_R}_{i7,j7} + 1)\cdot s],257] \neq 1$
        $s \leftarrow s + 1$
```

```
Key_D_Gv_{i7,j7} :=
    $s \leftarrow 0$
    while  $\text{mod}[[(\text{Key\_C\_G}_{i7,j7} + 1)\cdot s],257] \neq 1$
        $s \leftarrow s + 1$
```

$$\text{Key\_D\_R}_{i7,j7} := \text{Key\_D\_Rv}_{i7,j7} - 1$$

```
Key_D_Bv_{i7,j7} :=
    $s \leftarrow 0$
    while  $\text{mod}[[(\text{Key\_C\_B}_{i7,j7} + 1)\cdot s],257] \neq 1$
        $s \leftarrow s + 1$
```

$$\text{Key\_D\_G}_{i7,j7} := \text{Key\_D\_Gv}_{i7,j7} - 1$$

$$\text{Key\_D\_B}_{i7,j7} := \text{Key\_D\_Bv}_{i7,j7} - 1$$

$$\text{R\_pic\_C}_{i7,j7} := \text{mod}[[[[\text{mod}[[(\text{R\_pic}_{i7,j7} + 1)\cdot(\text{Key\_C\_R}_{i7,j7} + 1)],257] - 1] + \text{Key\_D\_R}_{i7,j7}]],256]$$

$$\text{G\_pic\_C}_{i7,j7} := \text{mod}[[[[\text{mod}[[(\text{G\_pic}_{i7,j7} + 1)\cdot(\text{Key\_C\_G}_{i7,j7} + 1)],257] - 1] + \text{Key\_D\_G}_{i7,j7}]],256]$$

$$\text{B\_pic\_C}_{i7,j7} := \text{mod}[[[[\text{mod}[[(\text{B\_pic}_{i7,j7} + 1)\cdot(\text{Key\_C\_B}_{i7,j7} + 1)],257] - 1] + \text{Key\_D\_B}_{i7,j7}]],256]$$

$$\text{R\_pic\_D}_{i7,j7} := \text{mod}[[[[\text{mod}[((\text{R\_pic\_C}_{i7,j7} + 256 - \text{Key\_D\_R}_{i7,j7})),256]] + 1]\cdot(\text{Key\_D\_R}_{i7,j7} + 1)],257] - 1$$

$$\text{G\_pic\_D}_{i7,j7} := \text{mod}[[[[\text{mod}[((\text{G\_pic\_C}_{i7,j7} + 256 - \text{Key\_D\_G}_{i7,j7})),256]] + 1]\cdot(\text{Key\_D\_G}_{i7,j7} + 1)],257] - 1$$

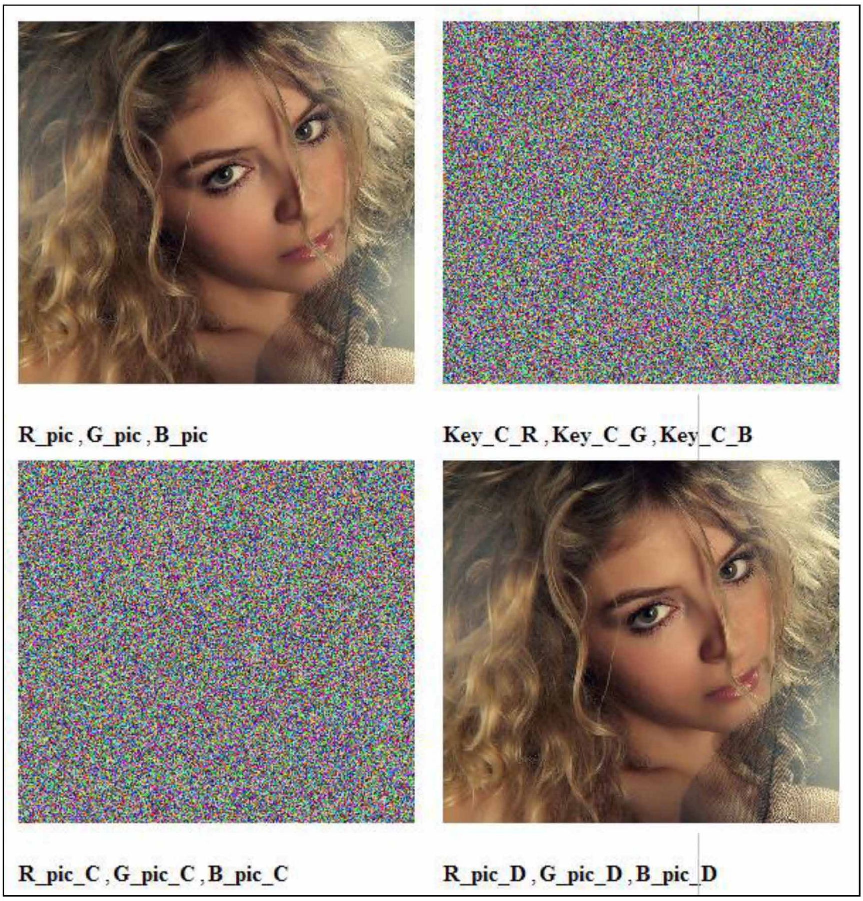
$$\text{B\_pic\_D}_{i7,j7} := \text{mod}[[[[\text{mod}[((\text{B\_pic\_C}_{i7,j7} + 256 - \text{Key\_D\_B}_{i7,j7})),256]] + 1]\cdot(\text{Key\_D\_B}_{i7,j7} + 1)],257] - 1$$

$$\text{Ver\_R\_pic} := \left(\overrightarrow{|\text{R\_pic} - \text{R\_pic\_D}|}\right) \qquad \text{Ver\_G\_pic} := \left(\overrightarrow{|\text{G\_pic} - \text{G\_pic\_D}|}\right) \qquad \text{Ver\_B\_pic} := \left(\overrightarrow{|\text{B\_pic} - \text{B\_pic\_D}|}\right)$$

$$\max(\text{Ver\_R\_pic}) = 0 \qquad \min(\text{Ver\_R\_pic}) = 0 \qquad \max(\text{Ver\_G\_pic}) = 0 \qquad \min(\text{Ver\_G\_pic}) = 0$$

$$\max(\text{Ver\_B\_pic}) = 0 \qquad \min(\text{Ver\_B\_pic}) = 0$$

Figure 3. Simulation results (fragment of interface window from Mathcad) of processes of direct and inverse cryptographic transformations by matrix affinity cipher: encryption image, matrix key (three-key set), crypto graph and decoded image in color formats.

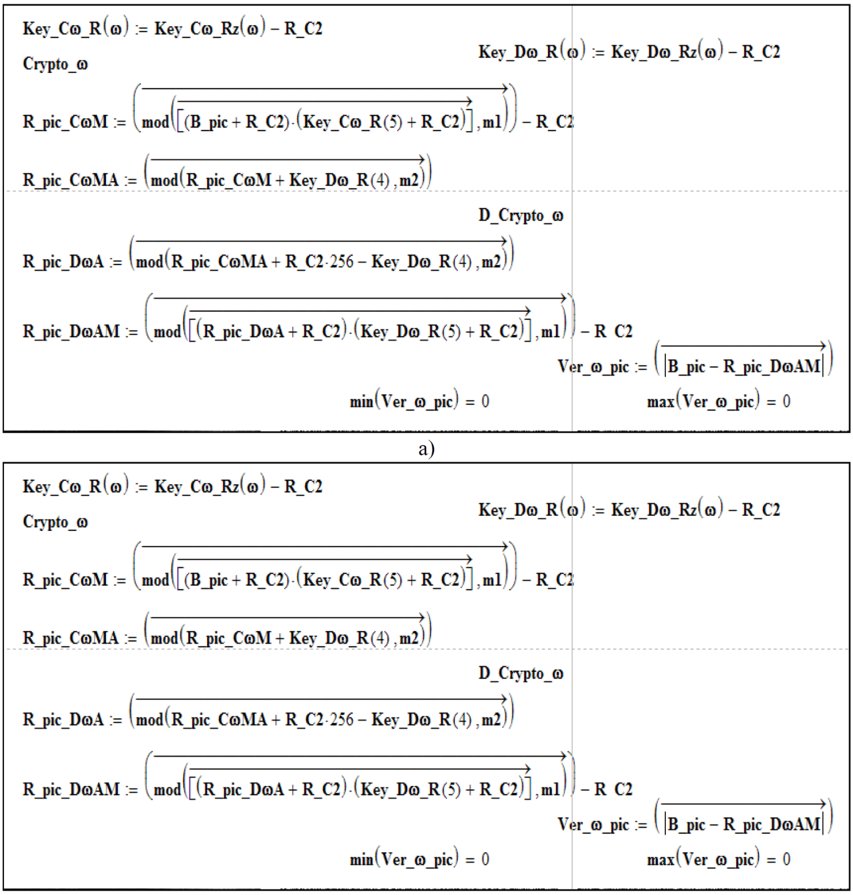

R_pic , G_pic , B_pic
Key_C_R , Key_C_G , Key_C_B
R_pic_C , G_pic_C , B_pic_C
R_pic_D , G_pic_D , B_pic_D

Our third suggestion is that it is possible to create matrix keys from one main or basic key for other or all spectral components, not even for color, but for multispectral images or 3-D arrays. The use of scalar keys and procedures of elemental powering by modulo each MK (even one agreed key!) gives the realization of one and multi-step MAC (Krasilenko, 2011; Krasilenko, 2009; Krasilenko, 2012) with only one secret MK, from which other MK are formed. Thus, our third experiment was to develop models and create a procedure for generating a series of MKs, as derivatives from one base in accordance with an agreed sequence of the numerical values that will be taken as degrees in elemental powering by modulo and in an attempt to implement them on the basis of MAC images of different formats. The vector of scalar keys with the dimension equal to the required number of matrix keys taking into account the number of spectral components. This model experiment was performed on the basis of formulas in a matrix form, some of which for sufficient understanding and with allowance for restrictions are shown in Fig. 4. It shows a copy of the fragment of the Mathcad window with formulas, procedures for forming a number of auxiliary lines and matrix keys turned to them, and formulas for the multiplicative and additive components of direct and inverse cryptographic transformations. As can be seen from Fig. 4 a), the keys Key_Cw_Rz (w) are created by a recursive procedure of elemental powering according to the modulus of the previous MK, starting from the base, and the degree of these MK and their corresponding matrix of values depend on the parameter w. If w = 0, then the matrix Key_Cw_Rz (0) is formed that equal to matrix R_C2, all elements of which is "1".

Some copies of the Mathcad windows of these MKs with dimensions of 600x549 corresponding to the sizes of one of a series of images for the CT are shown in Fig. 5 in digital format and correspond exactly to those MKs having the value w such as 1, 2, 7. The agreed secret key is marked as Key_C_R. To display the MK in the format of 8-bit images, the displacement of the values of matrices MK by subtracting from them the matrix R_C2. Note that the check shows the correctness of getting all values of the elements of all matrix keys to the required range. The results of this experiment using the prevailing and shown in Fig. 5 keys at the CT of the color image and its spectral components with such an improved MAC are shown in Fig. 6, 7, 8, 9. They testify to the qualitative correct operation of MAC models when using the correct keys and the impossibility of deciphering without the knowledge of keys and the base (not shown for the wrong keys!).

We have also created and experimentally tested the subroutine, which allows in accordance with the automatically determined sizes of input arrays or images, to form the basis of the Diffie-Helman protocol, generalized on the matrix case, as agreed upon by the parties of the secured data transmission MK (MKi), made on the basis of the results considered in papers (Krasilenko, 2012; Krasilenko, 2008), to verify them and generate keys derived from it. The Created keys are shown in Fig. 10, and the results of the direct and inverse CT of these MKs of a specific color image of the natural scene with fragments of the same intensity values using the improved MAC are shown in Fig. 11, 12. Similar studies performed in (Krasilenko, 2012; Krasilenko, 2009; Krasilenko, 2012; Krasilenko, 2014) histogram and entropy analyzes also showed good indexes of formed cryptograms and increase their entropy to almost 90-95% of the maximum possible. In more detail, we discuss these issues below and show some histograms.

Figure 4. A fragment of Mathcad window with formulas, procedures of forming a number of auxiliary direct and inverse matrix keys and formulas for the multiplicative and additive components of direct and inverse cryptographic transformations: a) the R-spectral component and b) the B-spectral component of the color image



$\mathrm{Key\_C\omega\_R}(\omega) := \mathrm{Key\_C\omega\_Rz}(\omega) - \mathrm{R\_C2}$

Crypto_ω

$\mathrm{Key\_D\omega\_R}(\omega) := \mathrm{Key\_D\omega\_Rz}(\omega) - \mathrm{R\_C2}$

$\mathrm{R\_pic\_C\omega M} := \left(\overrightarrow{\mathrm{mod}\left(\overrightarrow{\left[(\mathrm{B\_pic} + \mathrm{R\_C2})\cdot(\mathrm{Key\_C\omega\_R}(5) + \mathrm{R\_C2})\right]}, \mathrm{m1}\right)}\right) - \mathrm{R\_C2}$

$\mathrm{R\_pic\_C\omega MA} := \left(\overrightarrow{\mathrm{mod}(\mathrm{R\_pic\_C\omega M} + \mathrm{Key\_D\omega\_R}(4), \mathrm{m2})}\right)$

D_Crypto_ω

$\mathrm{R\_pic\_D\omega A} := \left(\overrightarrow{\mathrm{mod}(\mathrm{R\_pic\_C\omega MA} + \mathrm{R\_C2}\cdot 256 - \mathrm{Key\_D\omega\_R}(4), \mathrm{m2})}\right)$

$\mathrm{R\_pic\_D\omega AM} := \left(\overrightarrow{\mathrm{mod}\left(\overrightarrow{\left[(\mathrm{R\_pic\_D\omega A} + \mathrm{R\_C2})\cdot(\mathrm{Key\_D\omega\_R}(5) + \mathrm{R\_C2})\right]}, \mathrm{m1}\right)}\right) - \mathrm{R\ C2}$

$\mathrm{Ver\_\omega\_pic} := \left(\overrightarrow{|\mathrm{B\_pic} - \mathrm{R\_pic\_D\omega AM}|}\right)$

$\mathrm{min}(\mathrm{Ver\_\omega\_pic}) = 0$ $\mathrm{max}(\mathrm{Ver\_\omega\_pic}) = 0$

a)

$\mathrm{Key\_C\omega\_R}(\omega) := \mathrm{Key\_C\omega\_Rz}(\omega) - \mathrm{R\_C2}$

Crypto_ω

$\mathrm{Key\_D\omega\_R}(\omega) := \mathrm{Key\_D\omega\_Rz}(\omega) - \mathrm{R\_C2}$

$\mathrm{R\_pic\_C\omega M} := \left(\overrightarrow{\mathrm{mod}\left(\overrightarrow{\left[(\mathrm{B\_pic} + \mathrm{R\_C2})\cdot(\mathrm{Key\_C\omega\_R}(5) + \mathrm{R\_C2})\right]}, \mathrm{m1}\right)}\right) - \mathrm{R\_C2}$

$\mathrm{R\_pic\_C\omega MA} := \left(\overrightarrow{\mathrm{mod}(\mathrm{R\_pic\_C\omega M} + \mathrm{Key\_D\omega\_R}(4), \mathrm{m2})}\right)$

D_Crypto_ω

$\mathrm{R\_pic\_D\omega A} := \left(\overrightarrow{\mathrm{mod}(\mathrm{R\_pic\_C\omega MA} + \mathrm{R\_C2}\cdot 256 - \mathrm{Key\_D\omega\_R}(4), \mathrm{m2})}\right)$

$\mathrm{R\_pic\_D\omega AM} := \left(\overrightarrow{\mathrm{mod}\left(\overrightarrow{\left[(\mathrm{R\_pic\_D\omega A} + \mathrm{R\_C2})\cdot(\mathrm{Key\_D\omega\_R}(5) + \mathrm{R\_C2})\right]}, \mathrm{m1}\right)}\right) - \mathrm{R\ C2}$

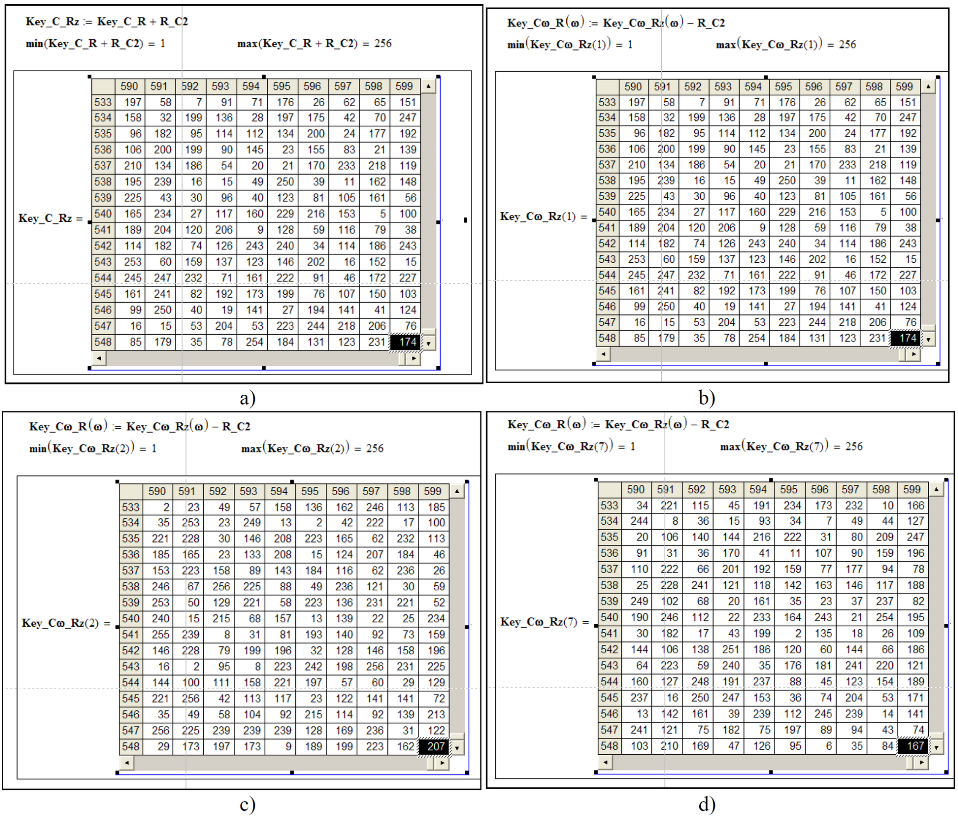
$\mathrm{Ver\_\omega\_pic} := \left(\overrightarrow{|\mathrm{B\_pic} - \mathrm{R\_pic\_D\omega AM}|}\right)$

$\mathrm{min}(\mathrm{Ver\_\omega\_pic}) = 0$ $\mathrm{max}(\mathrm{Ver\_\omega\_pic}) = 0$

b)

To test the influence of sizes, number of spectral components, statistical characteristics, structural and texture peculiarities of images subject to cryptographic transformations on some of the performance indicators of the proposed improved MAC, and especially on the histogram-entropy and visual characteristics of the obtained cryptograms, we have performed a group of other experiments. The results of these model experiments with other images, including video streams, large-scale (640x1024) multispectral (100 spectral channels) images and their constituents, text documents in color format, etc., are shown in Fig. 13-17 and also confirm the correct functioning of the MAC with a reduced number of keys. They showed

Figure 5. Results (Mathcad window interface) of the the base MK formation and its elemental powers modulus as auxiliary keys with scalar keys



Key_C_Rz := Key_C_R + R_C2

min(Key_C_R + R_C2) = 1 max(Key_C_R + R_C2) = 256

Key_C_Rz =

	590	591	592	593	594	595	596	597	598	599
533	197	58	7	91	71	176	26	62	65	151
534	158	32	199	136	28	197	175	42	70	247
535	96	182	95	114	112	134	200	24	177	192
536	106	200	199	90	145	23	155	83	21	139
537	210	134	186	54	20	21	170	233	218	119
538	195	239	16	15	49	250	39	11	162	148
539	225	43	30	96	40	123	81	105	161	56
540	165	234	27	117	160	229	216	153	5	100
541	189	204	120	206	9	128	59	116	79	38
542	114	182	74	126	243	240	34	114	186	243
543	253	60	159	137	123	146	202	16	152	15
544	245	247	232	71	161	222	91	46	172	227
545	161	241	82	192	173	199	76	107	150	103
546	99	250	40	19	141	27	194	141	41	124
547	16	15	53	204	53	223	244	218	206	76
548	85	179	35	78	254	184	131	123	231	174

a)

Key_Cω_R(ω) := Key_Cω_Rz(ω) − R_C2

min(Key_Cω_Rz(1)) = 1 max(Key_Cω_Rz(1)) = 256

Key_Cω_Rz(1) =

	590	591	592	593	594	595	596	597	598	599
533	197	58	7	91	71	176	26	62	65	151
534	158	32	199	136	28	197	175	42	70	247
535	96	182	95	114	112	134	200	24	177	192
536	106	200	199	90	145	23	155	83	21	139
537	210	134	186	54	20	21	170	233	218	119
538	195	239	16	15	49	250	39	11	162	148
539	225	43	30	96	40	123	81	105	161	56
540	165	234	27	117	160	229	216	153	5	100
541	189	204	120	206	9	128	59	116	79	38
542	114	182	74	126	243	240	34	114	186	243
543	253	60	159	137	123	146	202	16	152	15
544	245	247	232	71	161	222	91	46	172	227
545	161	241	82	192	173	199	76	107	150	103
546	99	250	40	19	141	27	194	141	41	124
547	16	15	53	204	53	223	244	218	206	76
548	85	179	35	78	254	184	131	123	231	174

b)

Key_Cω_R(ω) := Key_Cω_Rz(ω) − R_C2

min(Key_Cω_Rz(2)) = 1 max(Key_Cω_Rz(2)) = 256

Key_Cω_Rz(2) =

	590	591	592	593	594	595	596	597	598	599
533	2	23	49	57	158	136	162	246	113	185
534	35	253	23	249	13	2	42	222	17	100
535	221	228	30	146	208	223	165	62	232	113
536	185	165	23	133	208	15	124	207	184	46
537	153	223	158	89	143	184	116	62	236	26
538	246	67	256	225	88	49	236	121	30	59
539	253	50	129	221	58	223	136	231	221	52
540	240	15	215	68	157	13	139	22	25	234
541	255	239	8	31	81	193	140	92	73	159
542	146	228	79	199	196	32	128	146	158	196
543	16	2	95	8	223	242	198	256	231	225
544	144	100	111	158	221	197	57	60	29	129
545	221	256	42	113	117	23	122	141	141	72
546	35	49	58	104	92	215	114	92	139	213
547	256	225	239	239	239	128	169	236	31	122
548	29	173	197	173	9	189	199	223	162	207

c)

Key_Cω_R(ω) := Key_Cω_Rz(ω) − R_C2

min(Key_Cω_Rz(7)) = 1 max(Key_Cω_Rz(7)) = 256

Key_Cω_Rz(7) =

	590	591	592	593	594	595	596	597	598	599
533	34	221	115	45	191	234	173	232	10	166
534	244	8	36	15	93	34	7	49	44	127
535	20	106	140	144	216	222	31	80	209	247
536	91	31	36	170	41	11	107	90	159	196
537	110	222	66	201	192	159	77	177	94	78
538	25	228	241	121	118	142	163	146	117	188
539	249	102	68	20	161	35	23	37	237	82
540	190	246	112	22	233	164	243	21	254	195
541	30	182	17	43	199	2	135	18	26	109
542	144	106	138	251	186	120	60	144	66	186
543	64	223	59	240	35	176	181	241	220	121
544	160	127	248	191	237	88	45	123	154	189
545	237	16	250	247	153	36	74	204	53	171
546	13	142	161	39	239	112	245	239	14	141
547	241	121	75	182	75	197	89	94	43	74
548	103	210	169	47	126	95	6	35	84	167

d)

that the duration of CT procedures does not exceed a few seconds, even for large-scale (640x1024) color images when they are modeled in the Mathcad and the use of medium-class PCs. Of course, the total duration of the required procedures is influenced by both the number of spectral channels, the way of writing software modules when emulating models, and the use of vector parallel computing, and therefore making more detailed estimates inappropriate, and here we note only the fact that our matrix models MAC with decomposition, have internal parallelism, are more easily structurally reflected on hardware matrix means.

The visual analysis of the obtained cryptograms in the simulation and shown in Fig. 13 - 17 shows the qualitative encryption and the correct operation of the MM of direct and inverse cryptographic transformations on the basis of MAC in all cases. For a more accurate analysis, we determined the entropy of images, keys and cryptogram and their histograms were constructed using the Mathcad tools.

Figure 6. The results of the direct and inverse CT MAC of R component of color image with using the multiplicative and additive components of the MAC with only one MK Key_Cw_R (2).

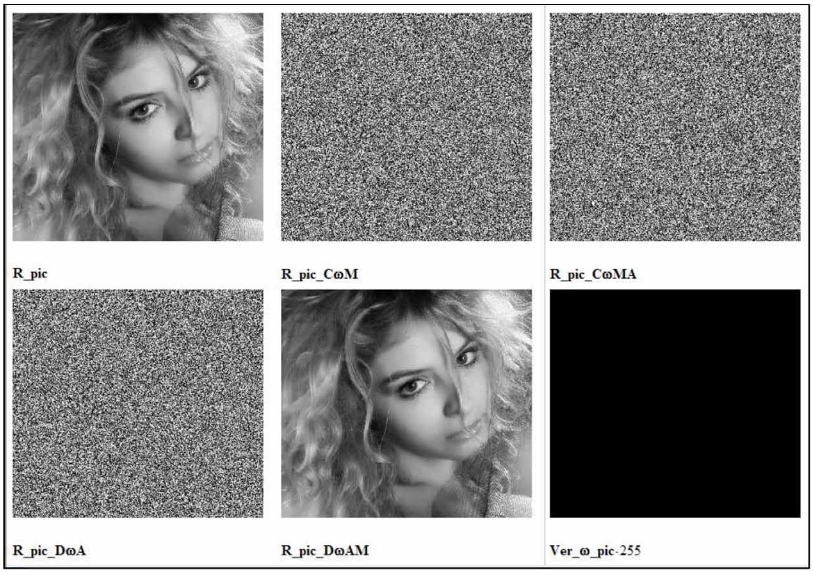


Figure 7. The results of the direct and inverse CT MAC of G component of color image with using the multiplicative and additive components of the MAC with only one MK Key_Cw_R (7).

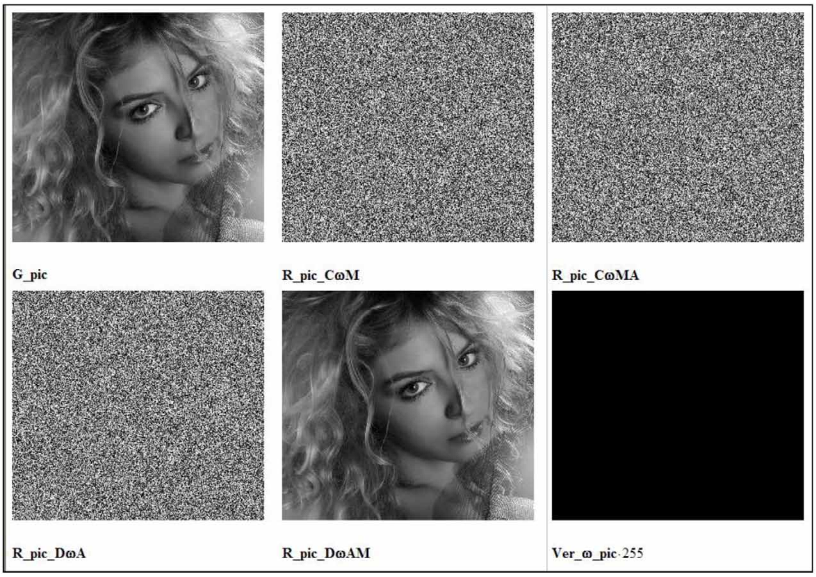
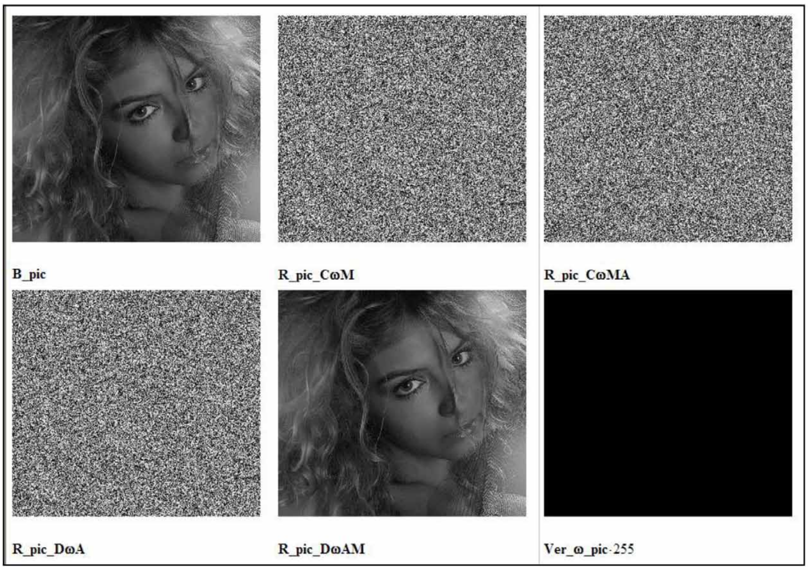


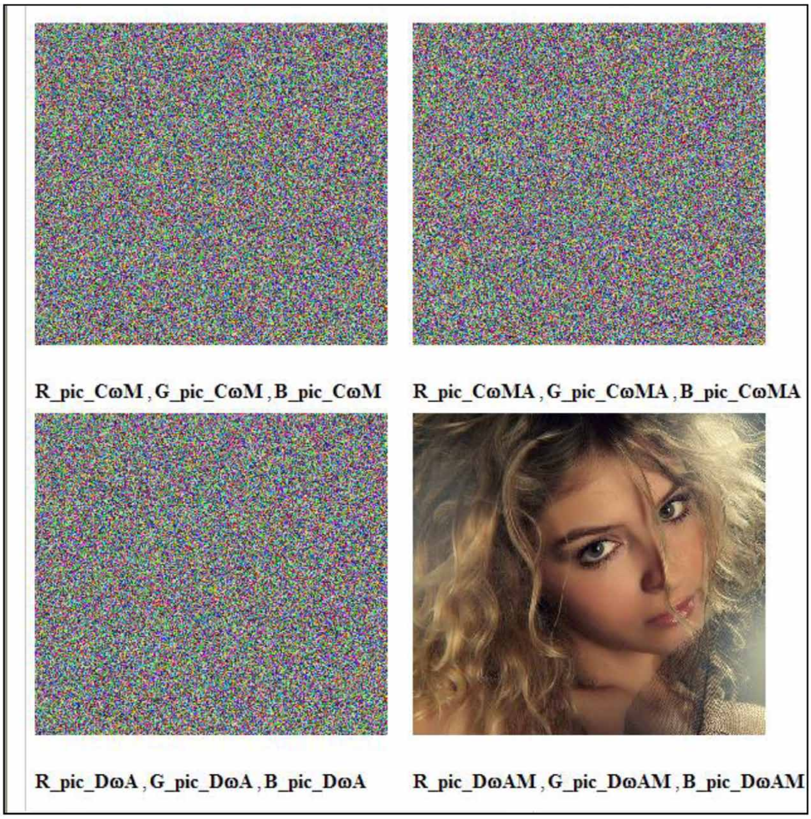
Figure 8. The results of the direct and inverse CT MAC of B component of color image with using the multiplicative and additive components of the MAC with only one MK Key_Cw_R (5).



They are shown in Fig. 18-19. From the drawings it can be seen that despite the very specific histograms of the composite images, the histograms of the components of the cryptogram have changed significantly, and do not allow them to guess, as they are, to recognize the possible appearance of the image or read the message or understand the TGD.

To evaluate the quality of encrypted images or documents, we also used, developed and covered in paper (Krasilenko, 2011) a subroutine in MathCad, which allows to calculate the average entropy by 1 pixel of specific images. As shown in Fig. 18-19 and with histogram distributions R, G, B components of explicit color image and confirmed by the definition of entropy, the entropy of the initial explicit image, namely its 8-bit components, is within 3-4 bits per pixel, and the entropy of the cryptogram (its components) for various experiments fluctuated within 7.5-7.8 bits per pixel, which is very close to the maximum possible value of 8. Similar values of entropy also have 8-bit components of MK, see Fig. 18. Note, that the comparison (from Figure 19) of histograms and entropy of the components of cryptograms obtained after **multiplicative and multiplicative** with subsequent additive transformations, allows us to conclude that they are insignificant. We also found that the multichannel MAC-based CT practically improves the histogram-entropy characteristics if the base agreed key is correctly selected or generated, meets the necessary requirements, and is

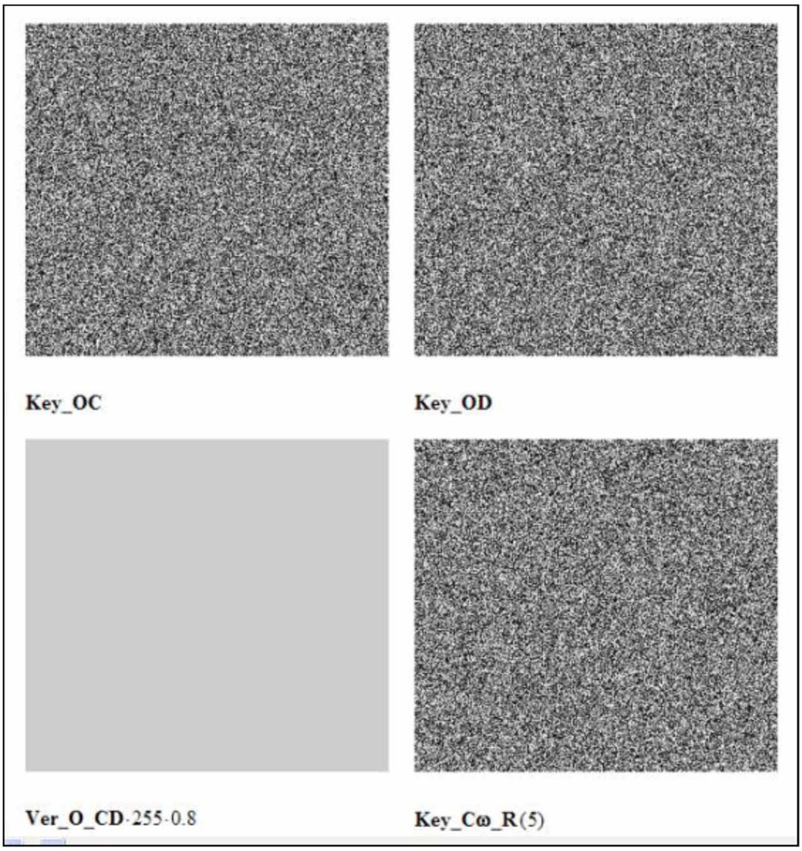
Figure 9. Results of the direct and inverse CT MAC of color image with using the multiplicative and additive components of the cipher for spectral components transformation with only derivatives from the base MK and parametric scalar keys


R_pic_CωM , G_pic_CωM , B_pic_CωM
R_pic_CωMA , G_pic_CωMA , B_pic_CωMA
R_pic_DωA , G_pic_DωA , B_pic_DωA
R_pic_DωAM , G_pic_DωAM , B_pic_DωAM

also close to the maximum possible entropy. The greater the entropy of cryptograms, the greater the degree of uncertainty of the corresponding image and the more difficult it is to attack this algorithm. The modeling established by the fact that all derivative keys have the required histogram distribution, which is practically close to the uniform distribution, and therefore they are close to the maximum entropy. This allows even by the visual appearance of the histogram to evaluate the quality of both keys and cryptogram.

We note that the use of spectral decomposition and recursive procedures for forming a set of MK, the consistency between the sizes of matrices, displacements of the ranges of values of matrix elements make possible to use for the CT on the basis of the improved MAC single secret matrix key, which can be easily represented as image. And having only one such MK it is possible to implement all the necessary procedures for specific applications and for different types of data, reliable CT

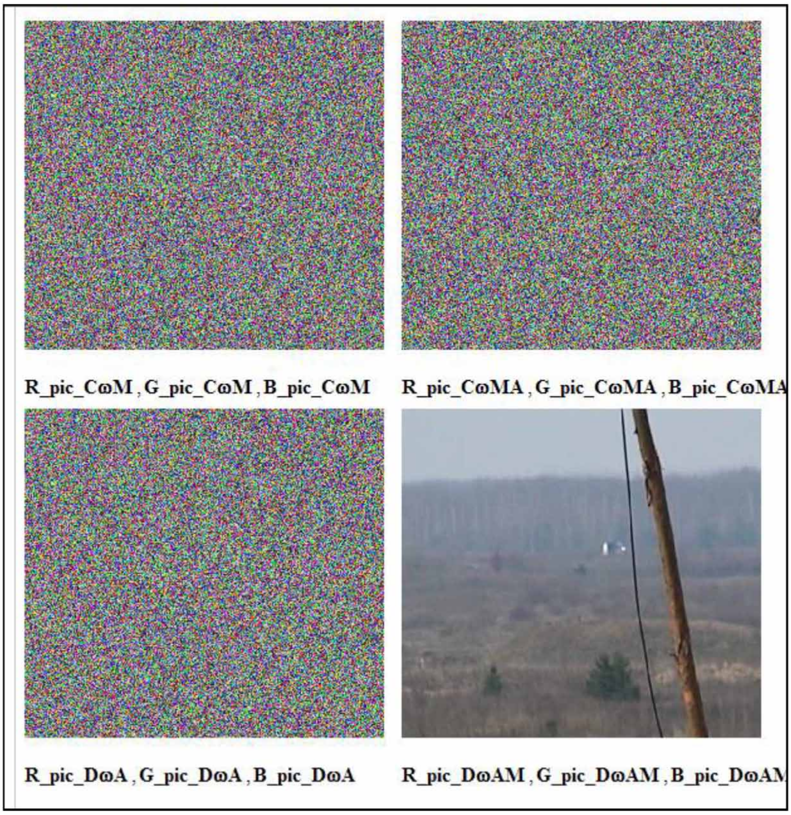
Figure 10. View of one of the basic matrix keys (Key_OC), the inverse MKi (Key_OD), auxiliary (Key_Cw_R (5)) with parameter 5 and the verifying matrix (Ver_O_CD) formed in accordance with the selected parameters and the dimension of the encrypted images.



procedures of MAC. All the experiments performed and the results presented here have confirmed the correct work of the proposed models and their modifications, the convenience of their adaptation to the size of the images or their fragments-blocks for cryptographic transformations, the convenience and ease of choosing the necessary keys. Some effective procedures, secret key negotiation protocols and their exchange, updates, were partly considered in papers (Krasilenko, 2012; Krasilenko, 2008) for some more general types.

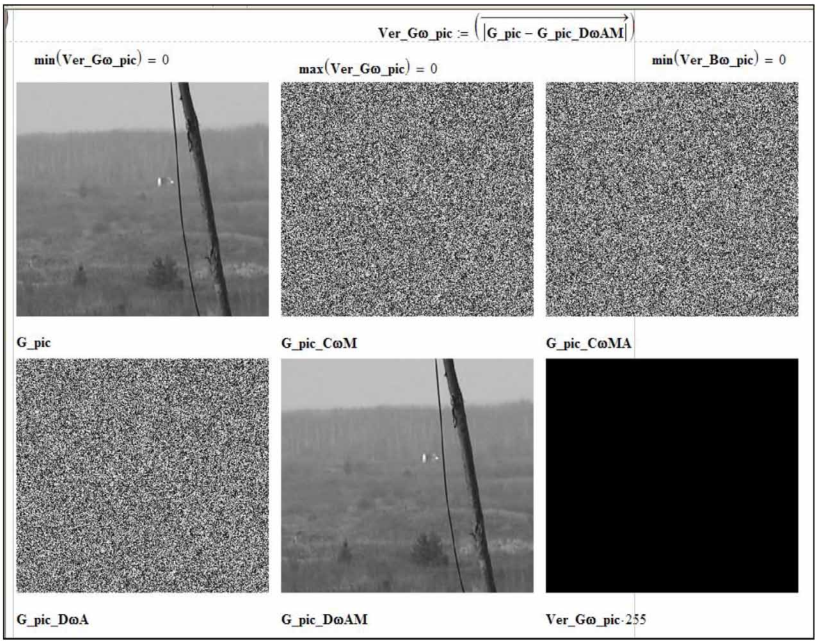
The section conclusions: Based on the review and analysis of publications, the prospects and necessity of further research and improvement of matrix affine ciphers and their derivatives have been substantiated. The ways of perfection are proposed and the results of the simulation of the matrix affine advanced ciphers for

Figure 11. Colored cryptograms obtained after multiplicative (left upper row), multiplicative and additive (right in the upper row) of direct (encryption) and inverse transformations (decoding): additive (on the left in the bottom row) and multiplicative (decoded on the right in bottom row).


R_pic_CωM , G_pic_CωM , B_pic_CωM
R_pic_CωMA , G_pic_CωMA , B_pic_CωMA
R_pic_DωA , G_pic_DωA , B_pic_DωA
R_pic_DωAM , G_pic_DωAM , B_pic_DωAM

cryptographic transformations of black-and-white and color images with a reduced number of matrix keys are given. Modified models and algorithmic procedures of keys formation, direct and inverse cryptographic transformations, reduced to matrix-matrix elemental operations by modulo, are developed. It was shown that the use of decomposition of color and multispectral images on their black and white components allowed unifying the transformation procedures, using only one agreed matrix key and expanding the types, data formats and the range of the cipher applications. It is suggested and confirmed experimentally that as an auxiliary derivative key you can use the power of the master key by modulo. Based on a series of experiments in Mathcad with different multi-gradation and color images to encrypt and decrypt them with proposed models, it is shown that the proposed improvements to such ciphers are correct, adequate, easy to use, have advantages and even allow to increase their

Figure 12. A fragment of the interface window that shows the process of direct and inverse cryptographic transformations of one, namely G, of the spectral component of the color image



$$\text{Ver\_G}\omega\text{\_pic} := \left(\overrightarrow{\left|\text{G\_pic} - \text{G\_pic\_D}\omega\text{AM}\right|}\right)$$

min(Ver_Gω_pic) = 0

max(Ver_Gω_pic) = 0

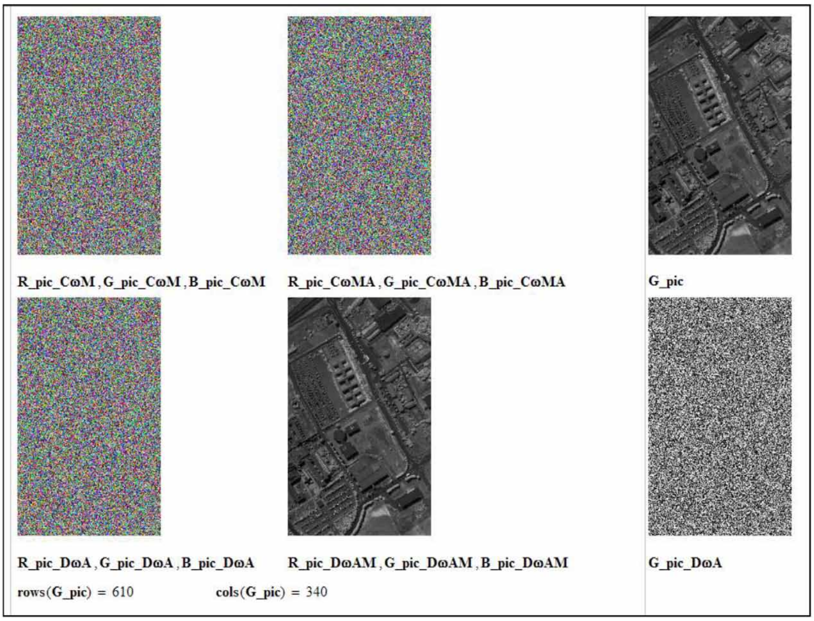
min(Ver_Bω_pic) = 0

functionality. The histogram-entropy characteristics of the cryptograms obtained with MAC are determined and evaluated, which also testify to their cryptographic properties and stability.

Multi-Functional Parametric Matrix-Algebraic Models (MAM) of Cryptographic Transformations (CT) with Operations by Modulo and Their Modeling

Modifications of the above mentioned models allow the CT to check the integrity of the cryptogram and their distortions, as shown in paper (Krasilenko, 2016; Krasilenko, 2016), for both black and white and color images. However, as experiments have shown, some specific TGDs, for example scanned documents, have a sizeable area of almost the same intensity of pixels, a small number of graduations and very characteristic histograms, which requires their CT to increase cryptostability by seeking improvements to MAM, including and by expanding their functionality while maintaining unified matrix operations and procedures ((Krasilenko, 2016). Thus, the purpose of this section is development and further modification, universalization

Figure 13. A fragment of a window with cryptograms and decoded images demonstrating the process of direct and inverse cryptographic transformations of components of a large-scale multispectral image obtained from a remote monitoring aircraft and used for model experiments

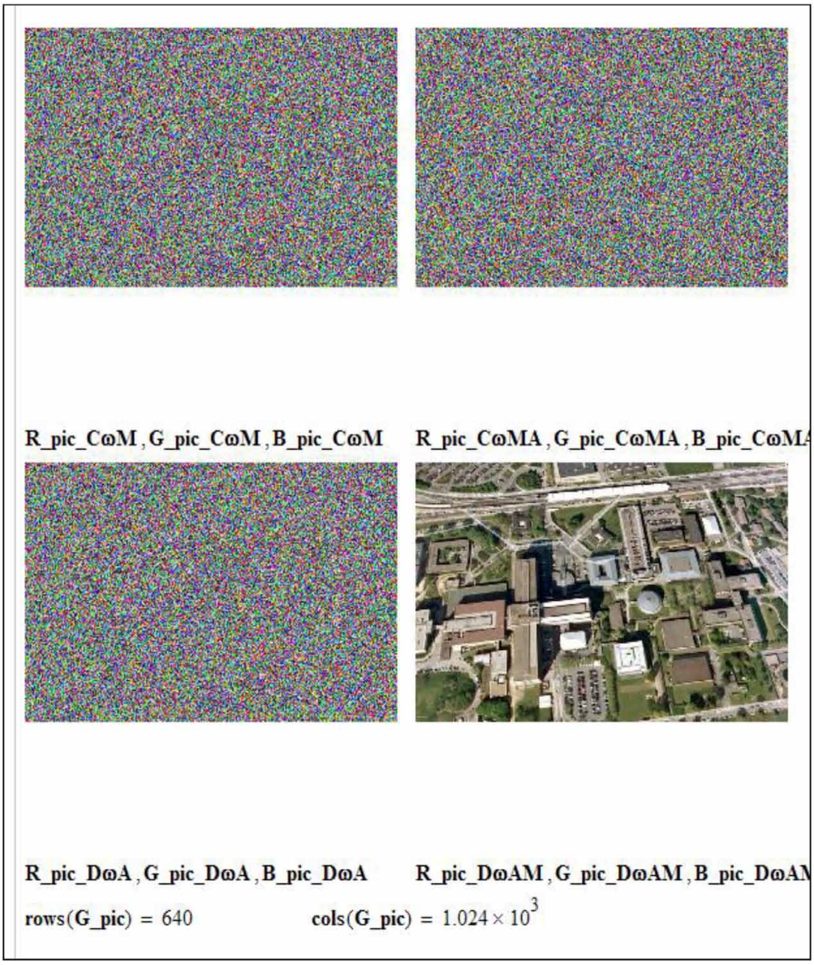

R_pic_CωM , G_pic_CωM , B_pic_CωM
R_pic_CωMA , G_pic_CωMA , B_pic_CωMA
G_pic
R_pic_DωA , G_pic_DωA , B_pic_DωA
R_pic_DωAM , G_pic_DωAM , B_pic_DωAM
G_pic_DωA

```
rows(G_pic) = 610          cols(G_pic) = 340
```

and generalization of MAM for the CT in order to improve their characteristics, sustainability, simulation **and** testing the created models on real information objects (IO) that will allow evaluating their parameters, possibilities and application features.

The essence of the proposed MAM for CT is to apply matrix multiplication procedures to the corresponding 8-bit MK of the same dimension (KLC256, KLD256) for matrix size NxN, as sets of bytes or 8-bit images (PIC_S, PIC_Doc, see Fig. 20) using multiplication and add operations by modulo. As can be seen from Fig. 20 - 24, the simulation results of the processes of direct and inverse CT TGD with a dimension of 256x256 confirmed the correct operation of models when applying the correct (Fig. 23) and wrong (Fig. 24) keys. MK had a hierarchical structure, the dimension of 256x256 consisted of a block matrix of 16x16 units with each unit size of 16x16, and each of the blocks (KLC16, KLD16) had 4 sub-blocks of 4x4 elements. Using matrices of permutations **P** of types K, KP16V1, KP16V2, allow arbitrary permutations of blocks and sub-blocks, as shown in Fig. 20. Blocks KLC, KLD and full keys are mutually inverse matrices when multiplying them by the corresponding modulo.

Figure 14. A fragment of the window with cryptograms and decoded images (all color!) that demonstrates the process of direct and inverse cryptographic transformations based on the improved MAC of a large-scale image (640x1024 elements) that was used for experiments



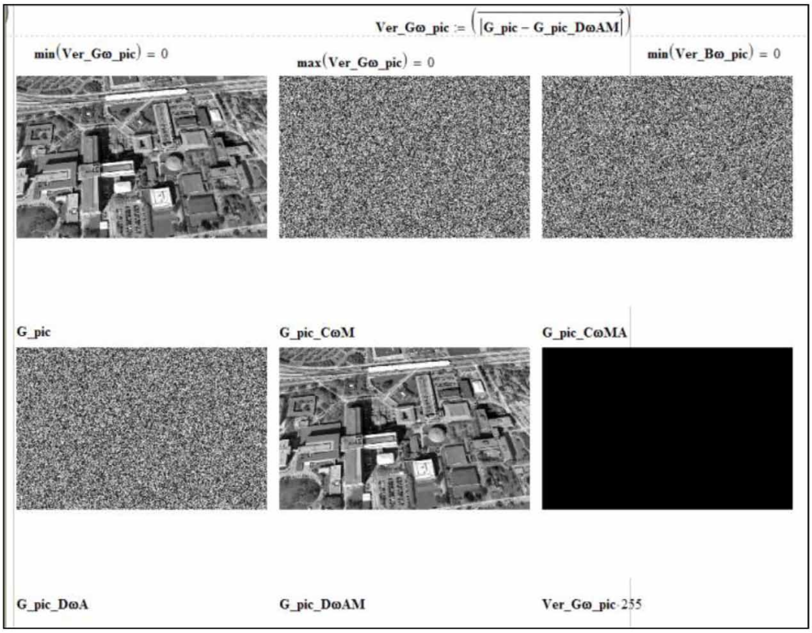
R_pic_CωM , G_pic_CωM , B_pic_CωM   R_pic_CωMA , G_pic_CωMA , B_pic_CωM

R_pic_DωA , G_pic_DωA , B_pic_DωA   R_pic_DωAM , G_pic_DωAM , B_pic_DωA

rows(G_pic) = 640   cols(G_pic) = 1.024×10^3

The essential difference between the proposed MKs is that both the blocks themselves in the entire matrix and sub-blocks, and elements in them can be mixed, and their structures are similar to the permutations matrix. Thus, the cryptographic block processing is accompanied by simultaneous mixing blocks and sub-blocks, as well as their elements (Fig. 21 - 23). But the analysis of entropy, histograms of TGD and their cryptogram (Fig. 20) **shows** that for TGD, in contrast to an image of a person, even several iterative multiplications of the data matrix (DM) by the MK may not be sufficient, more when applying the same MK.

Figure 15.A Fragment of the interface window, which shows the details of the processes of direct and inverse cryptographic transformations and their verification of one, namely G, of the spectral component of the color image shown in Fig. 14 and was used to simulate the improved MAC with a reduced number (one base!) of MK



Ver_Gω_pic := $\overrightarrow{\left(|G\_pic - G\_pic\_D\omega AM|\right)}$

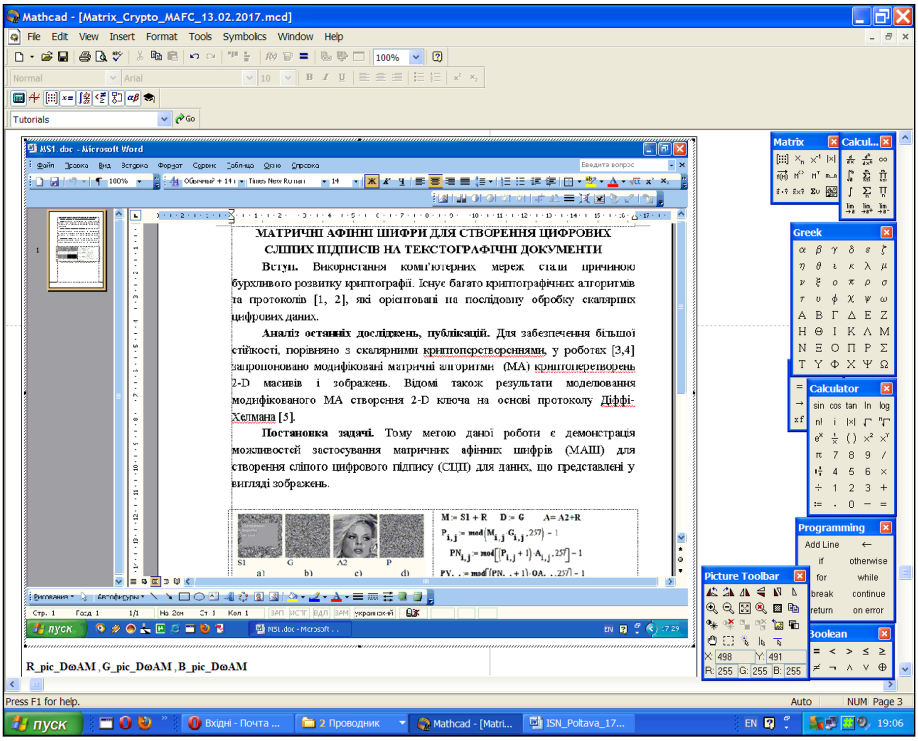
min(Ver_Gω_pic) = 0

max(Ver_Gω_pic) = 0

min(Ver_Bω_pic) = 0

Therefore, we proposed two new multifunctional parametric MAM CTs, the main conceptual idea of which is based on the use of additional scalar or vector keys (VK) as parameters influencing the power of matrices of MD and MK by modulus in their matrix multiplication models and the degree and form of permutation matrices blocks or elements. At each iterative step, depending on the VK, different MKs are formed. Fragments of the simulation of the processes of formation of matrices P, cyclic MK and their components, as well as the MAM formula for direct and inverse CT and verification using parametric MK are **shown** in Fig. 21. Fig. 22 **shows** the appearance of some parametric MK, and Fig. 23 and 24 **show** the results of modeling the CT TGD on the basis of parametric MAM and MK for cases of correct and accordingly, incorrect MK. The appearance of the initial histograms and after the CT confirms that even for the selected TGD-specific histogram, the proposed models give better results. The power of the set of possible keys has increased by an order of magnitude (more than 10^{300}), and as the estimates show, only the power of a plurality of mini-blocks (8x8 8-bit) is of the order of more than 10^{150}. Thus, the stability of the models has increased significantly.

Figure 16. Mathcad interface window (fully) with tools and a text-graphical document (TGD) displayed in its window that was used to simulate advanced MACs



МАТРИЧНІ АФІННІ ШИФРИ ДЛЯ СТВОРЕННЯ ЦИФРОВИХ СЛІПИХ ПІДПИСІВ НА ТЕКСТОГРАФІЧНІ ДОКУМЕНТИ

Вступ. Використання комп'ютерних мереж стали причиною бурхливого розвитку криптографії. Існує багато криптографічних алгоритмів та протоколів [1, 2], які орієнтовані на послідовну обробку скалярних цифрових даних.

Аналіз останніх досліджень, публікацій. Для забезпечення більшої стійкості, порівняно з скалярними криптоперетвореннями, у роботах [3,4] запропоновано модифіковані матричні алгоритми (МА) криптоперетворень 2-D масивів і зображень. Відомі також результати моделювання модифікованого МА створення 2-D ключа на основі протоколу Діффі-Хелмана [5].

Постановка задачі. Тому метою даної роботи є демонстрація можливостей застосування матричних афінних шифрів (МАШ) для створення сліпого цифрового підпису (СЦП) для даних, що представлені у вигляді зображень.

$M := S1 + R \quad D := G \quad A = A2+R$

$P_{i,j} := \mathrm{mod}(M_{i,j} \cdot G_{i,j}, 257) - 1$

$PN_{i,j} := \mathrm{mod}[(P_{i,j} + 1) \cdot A_{i,j}, 257] - 1$

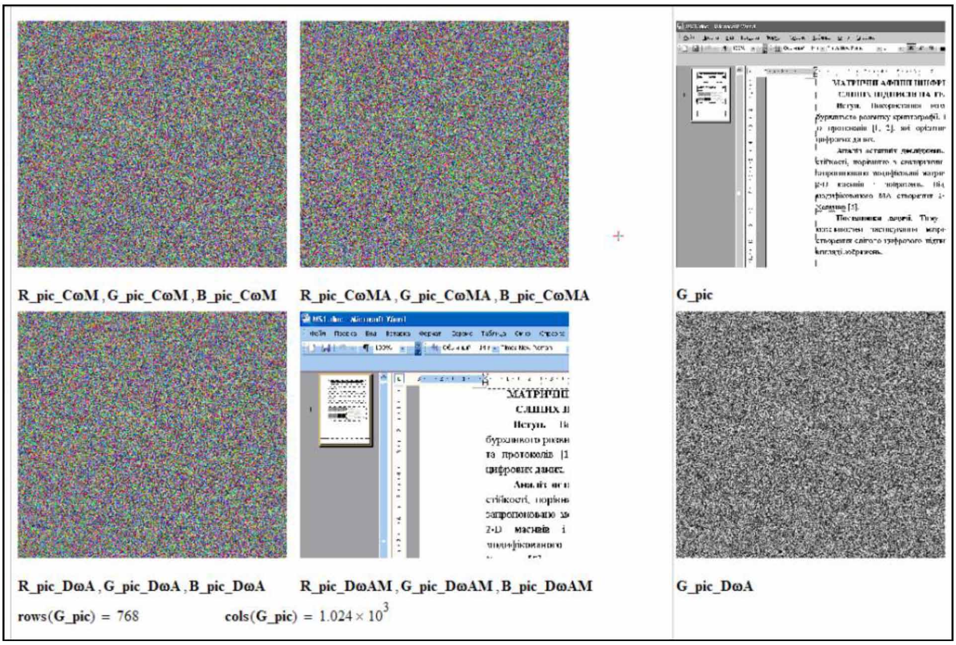
$PY_{.\,.} := \mathrm{mod}[(PN_{.\,.} + 1) \cdot OA_{.\,.}, 257] - 1$

R_pic_DωAM , G_pic_DωAM , B_pic_DωAM

Without the knowledge of keys, it is impossible to restore MD and, as shown in papers (Krasilenko, 2011; Krasilenko, 2012), even with the dimension of MK, equal to 32x32, the stability of models is ensured and we have the keys of 256x256 8-bit elements, which gives a substantial strength!

The section conclusions: New models with modular operations for MD, including images, are proposed and considered. The results of their simulation are presented on the example of direct and inverse CT over images, which testify to their correct work, convenience (only 1 matrix procedure and one in essence MK!), adaptability to formats, multi-functionality (combination of operations of matrix block replacements with permutations, interchangeability of cyclic iterations procedures and matrix substitutions in modulus with convenient choice of parameters and management of transformations and key shapes) and efficiency (orientation to matrix processors). The aspects of matrix algebraic procedures and operations by modulo and creation of MK are considered. The results of simulation of direct and inverse CT, their verification confirmed the adequacy of parametric generalized MAM, their convenience, multi-functionality, efficiency for use. They both are

Figure 17. A Fragment of the window with fragments of cryptogram and decoded images of TGD from Fig. 16 (both colored in the center and left, and black and white corresponding spectral components!), which demonstrates the correctness of the processes of direct and inverse cryptographic transformations of TGD with the improved MAC



R_pic_CωM , G_pic_CωM , B_pic_CωM   R_pic_CωMA , G_pic_CωMA , B_pic_CωMA   G_pic

R_pic_DωA , G_pic_DωA , B_pic_DωA   R_pic_DωAM , G_pic_DωAM , B_pic_DωAM   G_pic_DωA

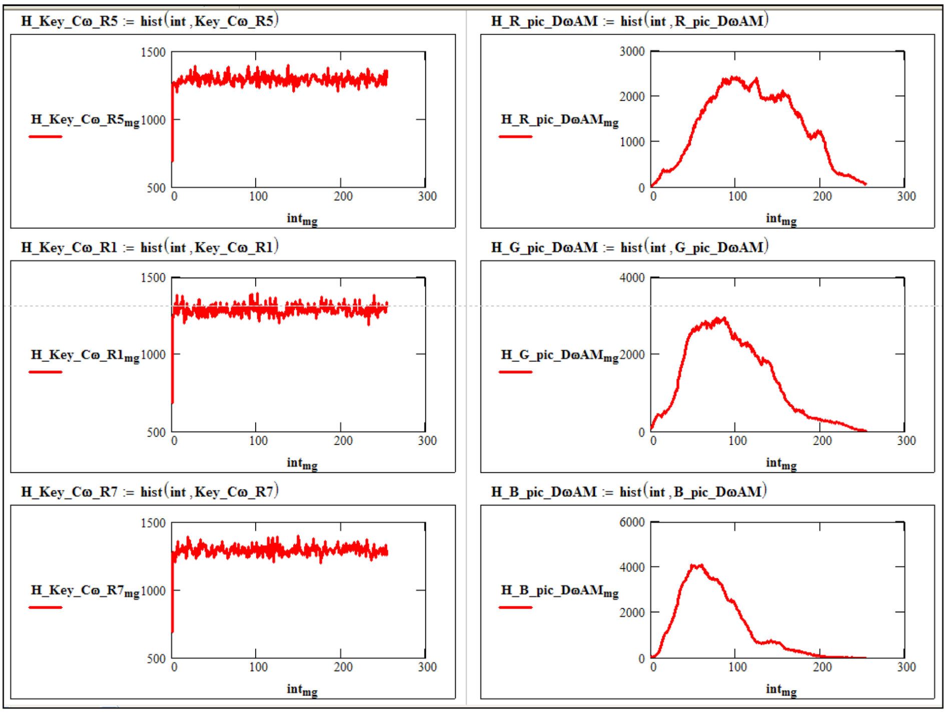
rows(G_pic) = 768   cols(G_pic) = 1.024×10^3

implemented programmatically and with matrix processors, have high speed and stability of transformations and adapt to the CT over image of different formats.

Models of Block Matrix Affine-Permutation Ciphers (MAPCs) for Cryptographic Transformations and Their Research

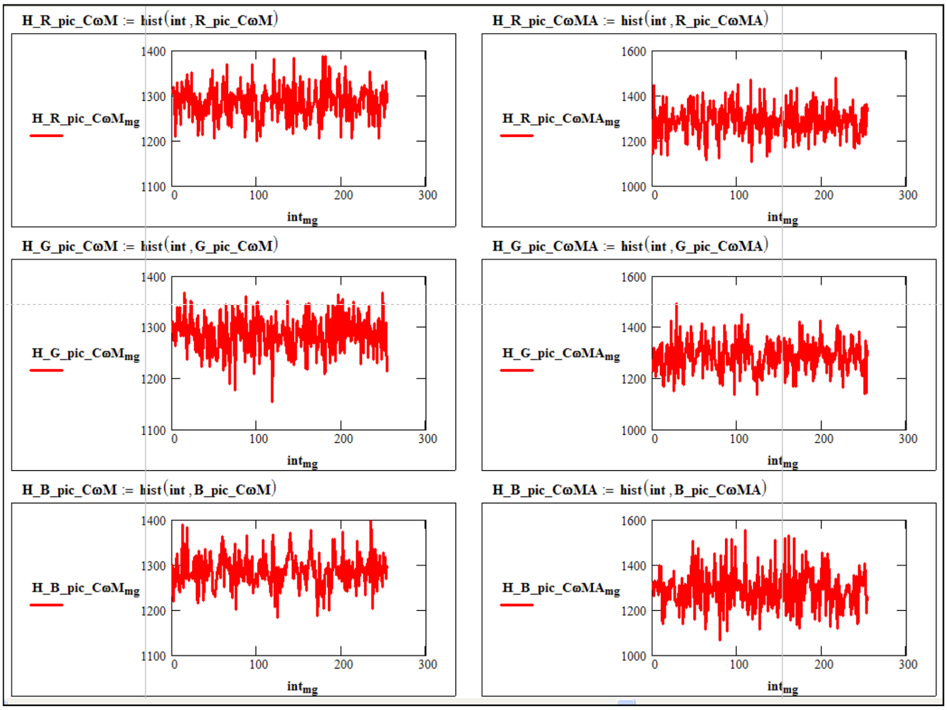
The emergence of parallel algorithms and especially the matrices of multiprocessor means, requires the creation of appropriate matrix-algebraic models (MAM), matrix-type systems (MT) for CT. Advantages of the TGD, black and white, color images by generalized matrix affine and affine-permutation ciphers (MAPCs), including the creation of blind digital signatures, were demonstrated in works (Krasilenko, 2011; Krasilenko, 2009; Krasilenko, 2012) . 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

Figure 18. Histograms of three formed from the main matrix keys (left) and corresponding R, G, B spectral components (right) of the color image over **which** *the CT based on the MAC* **which** *is shown in Fig. 9 on the right in the bottom row*



blocks in the form of matrices, which split multi-page data. Some MAMs based on MM_P require decomposition of bit-sections and in addition to the 2 MKs, there are two vector keys (VK) for increasing entropy and the change of histograms with the CT (Krasilenko, 2014; Krasilenko, 2010; Krasilenko, 2016). The promise of the MAM and its modifications for the CT is evidenced by the ability to check the integrity of the cryptogram of the images and the presence of distortions in them, see papers (Krasilenko, 2016; Krasilenko, 2016), increasing the crypto-stability and expanding their functionality while maintaining unified matrix operations, procedures, even for very specific characteristic histograms) of scanned TGDs, as experimentally shown in paper (Krasilenko, 2016). The generalization of the AM to a matrix-block view is necessary in terms of the versatility of block algorithms and independence on data volumes. Therefore, the improvement of the MAPCs, aimed at reducing the number of MK while maintaining the stability and other characteristics of the matrix models (MMs), their experimental testing on various images is also an urgent task. Thus, the actual purpose of this section is the development of block

Figure 19. Histograms of three R, G, B spectral components (left) of the received cryptogram after the multiplicative CT and the corresponding spectral components R, G, B of the obtained cryptogram after the second additive CT over the color image with the CT based on the MAC which is shown in Fig. 9 on the right in the bottom row

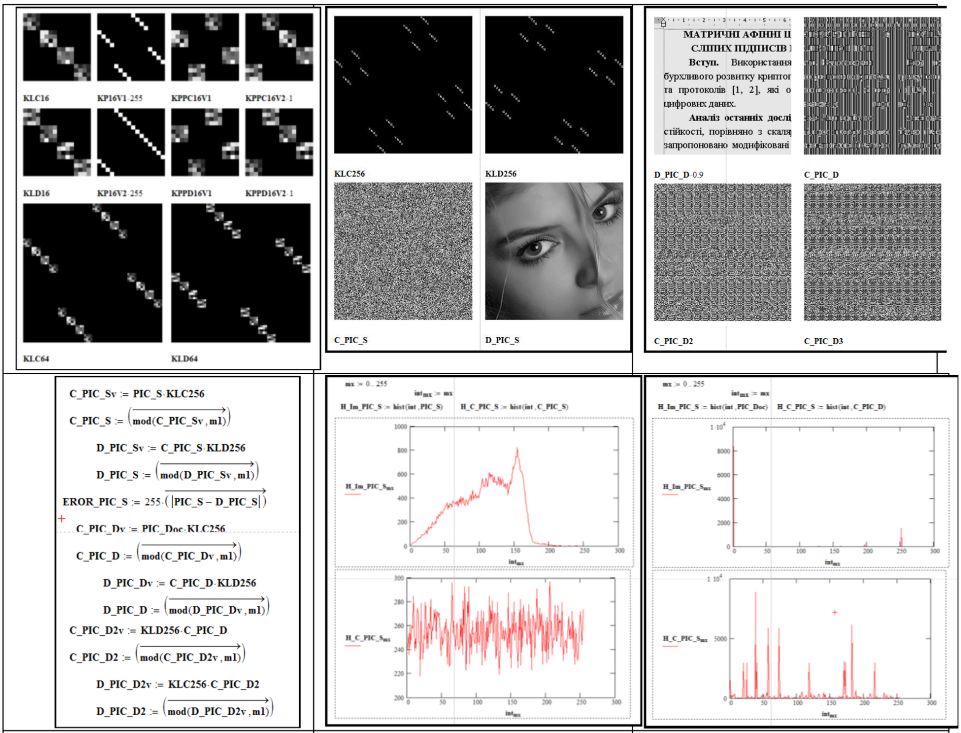


```
H_R_pic_CωM := hist(int, R_pic_CωM)        H_R_pic_CωMA := hist(int, R_pic_CωMA)
H_G_pic_CωM := hist(int, G_pic_CωM)        H_G_pic_CωMA := hist(int, G_pic_CωMA)
H_B_pic_CωM := hist(int, B_pic_CωM)        H_B_pic_CωMA := hist(int, B_pic_CωMA)
```

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.

Presentation of section material and research results. The proposed CT algorithm for encryption consists of the following steps: 1) the partition of IO into blocks in the form of matrices with a dimension 2^mx2^m, where m = 4, 5, 6, ... and with element-bytes in a digital format that 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 as the power of the main according to the parametric model, the argument of which is index block, 3) matrix affine or affine-permutation transformations (MAPTs) of matrix of bytes of current keys, the same as on stage 2 or similar, but according to another parametric model, 4) concatenation of the received blocks for the formation of cryptogram of IO. The decryption process

Figure 20. Fragments of Mathcad windows with the results of MK formation and simulation of MAM CT



C_PIC_Sv := PIC_S·KLC256

$C\_PIC\_S := \left(\overrightarrow{mod(C\_PIC\_Sv, m1)}\right)$

D_PIC_Sv := C_PIC_S·KLD256

$D\_PIC\_S := \left(\overrightarrow{mod(D\_PIC\_Sv, m1)}\right)$

$EROR\_PIC\_S := 255\cdot\overrightarrow{(|PIC\_S - D\_PIC\_S|)}$

C_PIC_Dv := PIC_Doc·KLC256

$C\_PIC\_D := \left(\overrightarrow{mod(C\_PIC\_Dv, m1)}\right)$

D_PIC_Dv := C_PIC_D·KLD256

$D\_PIC\_D := \left(\overrightarrow{mod(D\_PIC\_Dv, m1)}\right)$

C_PIC_D2v := KLD256·C_PIC_D

$C\_PIC\_D2 := \left(\overrightarrow{mod(C\_PIC\_D2v, m1)}\right)$

D_PIC_D2v := KLC256·C_PIC_D2

$D\_PIC\_D2 := \left(\overrightarrow{mod(D\_PIC\_D2v, m1)}\right)$

mx := 0 .. 255

$int_{mx} := mx$

H_Im_PIC_S := hist(int, PIC_S) H_C_PIC_S := hist(int, C_PIC_S)

mx := 0 .. 255

$int_{mx} := mx$

H_Im_PIC_S := hist(int, PIC_Doc) H_C_PIC_S := hist(int, C_PIC_D)

a) The MKs in their hierarchical formation and the formula of MAM

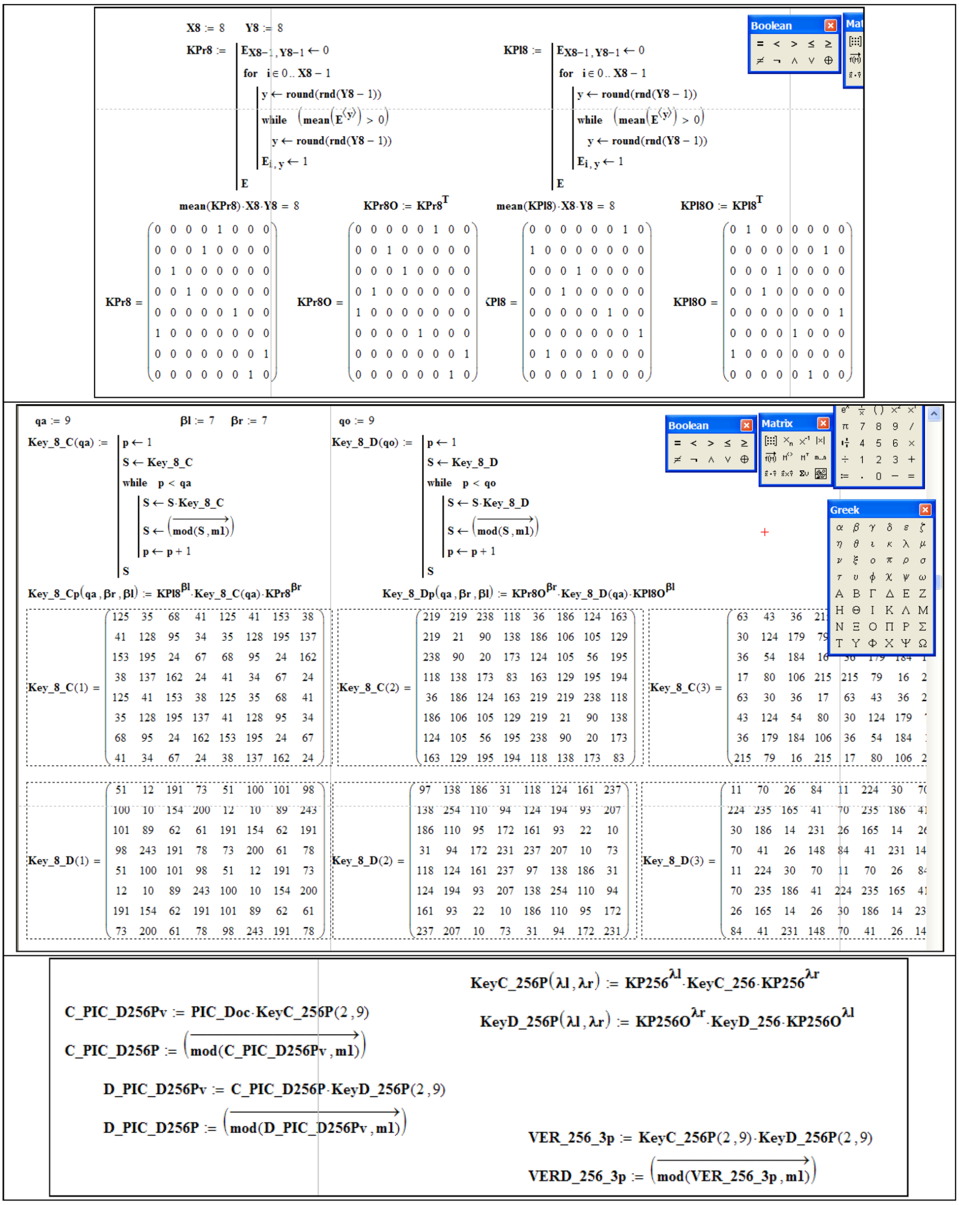
b) The keys (256x256x8), cryptogram, decoded image, and their histograms

c) The TGD, its cryptograms for steps 1-3, histogram for the 1-st cryptogram

has the following steps: 1) decomposing the cryptograms on blocks, 2) reversing the MAPT blocks based on the reversed current keys; 3) reversing bytes of blocks by current keys (vectors); 4) concatenating the transformed blocks into the restored IO. Blocking MAPS modeling was done with Mathcad using black and white and color images of different dimensions for visual demonstration. Mathcad windows with formulas for modeling the CT of the image by the algorithm of block MAPTs for two black and white images (256x256 elements) with the M-key M_V are shown in Fig. 25. Fig. 26 shows the results of the CT and the form of keys, blocks before and after the CT, the difference verification matrix blocks. Fragments of Mathcad windows with modules for the MK formation and the CT formulas are shown in Fig. 27, 28. Results of these CT are shown in Fig. 29.

The random bitmap KPX (256x256x1) of permutations formed in any way is used for permutations of bytes in each kp-th block (256 component vector VID (C_VID) or matrix C_M_V (16x16) with 8-bit numbers). It can be uniquely represented in

Figure 21. Fragments of modeling of the processes of forming matrices ***P****, cyclic parametric* ***MK****, their constituents, as well as MAM formulas for encryption, decryption and verification*



```
X8 := 8    Y8 := 8

KPr8 := | E_{X8-1, Y8-1} ← 0
        | for  i ∈ 0 .. X8 − 1
        |     | y ← round(rnd(Y8 − 1))
        |     | while  (mean(E^<y>) > 0)
        |     |     y ← round(rnd(Y8 − 1))
        |     | E_{i, y} ← 1
        | E

KPl8 := | E_{X8-1, Y8-1} ← 0
        | for  i ∈ 0 .. X8 − 1
        |     | y ← round(rnd(Y8 − 1))
        |     | while  (mean(E^<y>) > 0)
        |     |     y ← round(rnd(Y8 − 1))
        |     | E_{i, y} ← 1
        | E
```

mean(KPr8)·X8·Y8 = 8   KPr8O := $KPr8^T$ mean(KPl8)·X8·Y8 = 8   KPl8O := $KPl8^T$

$$KPr8 = \begin{pmatrix} 0&0&0&0&1&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{pmatrix} \quad KPr8O = \begin{pmatrix} 0&0&0&0&0&1&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{pmatrix}$$

$$KPl8 = \begin{pmatrix} 0&0&0&0&0&0&1&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&1&0&0&0&0&0&0\\ 0&0&0&0&1&0&0&0 \end{pmatrix} \quad KPl8O = \begin{pmatrix} 0&1&0&0&0&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&1&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&1&0&0&0\\ 1&0&0&0&0&0&0&0\\ 0&0&0&0&0&1&0&0 \end{pmatrix}$$

```
qa := 9                      βl := 7    βr := 7

Key_8_C(qa) := | p ← 1
               | S ← Key_8_C
               | while  p < qa
               |     | S ← S·Key_8_C
               |     | S ← (vectorize mod(S, m1))
               |     | p ← p + 1
               | S

qo := 9

Key_8_D(qo) := | p ← 1
               | S ← Key_8_D
               | while  p < qo
               |     | S ← S·Key_8_D
               |     | S ← (vectorize mod(S, m1))
               |     | p ← p + 1
               | S
```

$$Key\_8\_Cp(qa, \beta r, \beta l) := KPl8^{\beta l} \cdot Key\_8\_C(qa) \cdot KPr8^{\beta r}$$

$$Key\_8\_Dp(qa, \beta r, \beta l) := KPr8O^{\beta r} \cdot Key\_8\_D(qa) \cdot KPl8O^{\beta l}$$

$$Key\_8\_C(1) = \begin{pmatrix} 125&35&68&41&125&41&153&38\\ 41&128&95&34&35&128&195&137\\ 153&195&24&67&68&95&24&162\\ 38&137&162&24&41&34&67&24\\ 125&41&153&38&125&35&68&41\\ 35&128&195&137&41&128&95&34\\ 68&95&24&162&153&195&24&67\\ 41&34&67&24&38&137&162&24 \end{pmatrix}$$

$$Key\_8\_C(2) = \begin{pmatrix} 219&219&238&118&36&186&124&163\\ 219&21&90&138&186&106&105&129\\ 238&90&20&173&124&105&56&195\\ 118&138&173&83&163&129&195&194\\ 36&186&124&163&219&219&238&118\\ 186&106&105&129&219&21&90&138\\ 124&105&56&195&238&90&20&173\\ 163&129&195&194&118&138&173&83 \end{pmatrix}$$

$$Key\_8\_C(3) = \begin{pmatrix} 63&43&36&21\\ 30&124&179&79\\ 36&54&184&16\\ 17&80&106&215&215&79&16&2\\ 63&30&36&17&63&43&36&2\\ 43&124&54&80&30&124&179\\ 36&179&184&106&36&54&184\\ 215&79&16&215&17&80&106&2 \end{pmatrix}$$

$$Key\_8\_D(1) = \begin{pmatrix} 51&12&191&73&51&100&101&98\\ 100&10&154&200&12&10&89&243\\ 101&89&62&61&191&154&62&191\\ 98&243&191&78&73&200&61&78\\ 51&100&101&98&51&12&191&73\\ 12&10&89&243&100&10&154&200\\ 191&154&62&191&101&89&62&61\\ 73&200&61&78&98&243&191&78 \end{pmatrix}$$

$$Key\_8\_D(2) = \begin{pmatrix} 97&138&186&31&118&124&161&237\\ 138&254&110&94&124&194&93&207\\ 186&110&95&172&161&93&22&10\\ 31&94&172&231&237&207&10&73\\ 118&124&161&237&97&138&186&31\\ 124&194&93&207&138&254&110&94\\ 161&93&22&10&186&110&95&172\\ 237&207&10&73&31&94&172&231 \end{pmatrix}$$

$$Key\_8\_D(3) = \begin{pmatrix} 11&70&26&84&11&224&30&70\\ 224&235&165&41&70&235&186&41\\ 30&186&14&231&26&165&14&26\\ 70&41&26&148&84&41&231&14\\ 11&224&30&70&11&70&26&84\\ 70&235&186&41&224&235&165&41\\ 26&165&14&26&30&186&14&23\\ 84&41&231&148&70&41&26&14 \end{pmatrix}$$

$$KeyC\_256P(\lambda l, \lambda r) := KP256^{\lambda l} \cdot KeyC\_256 \cdot KP256^{\lambda r}$$

$$KeyD\_256P(\lambda l, \lambda r) := KP256O^{\lambda r} \cdot KeyD\_256 \cdot KP256O^{\lambda l}$$

$$C\_PIC\_D256Pv := PIC\_Doc \cdot KeyC\_256P(2, 9)$$

$$C\_PIC\_D256P := \left(\overrightarrow{mod(C\_PIC\_D256Pv, m1)}\right)$$

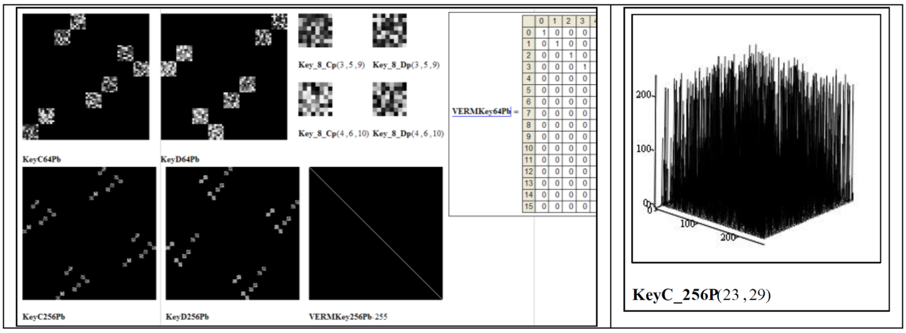
$$D\_PIC\_D256Pv := C\_PIC\_D256P \cdot KeyD\_256P(2, 9)$$

$$D\_PIC\_D256P := \left(\overrightarrow{mod(D\_PIC\_D256Pv, m1)}\right)$$

$$VER\_256\_3p := KeyC\_256P(2, 9) \cdot KeyD\_256P(2, 9)$$

$$VERD\_256\_3p := \left(\overrightarrow{mod(VER\_256\_3p, m1)}\right)$$

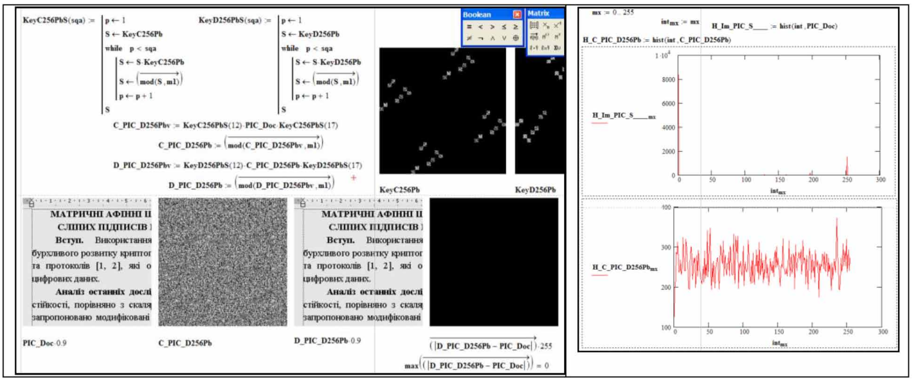
Figure 22. The appearance of some parametric MKs, their component hierarchical blocks, and the unity- matrix (at checking) in different formats (2D, 3D, and digital)



VERMKey64Pb =

	0	1	2	3	4
0	1	0	0	0	
1	0	1	0	0	
2	0	0	1	0	
3	0	0	0	1	
4	0	0	0	0	
5	0	0	0	0	
6	0	0	0	0	
7	0	0	0	0	
8	0	0	0	0	
9	0	0	0	0	
10	0	0	0	0	
11	0	0	0	0	
12	0	0	0	0	
13	0	0	0	0	
14	0	0	0	0	
15	0	0	0	0	

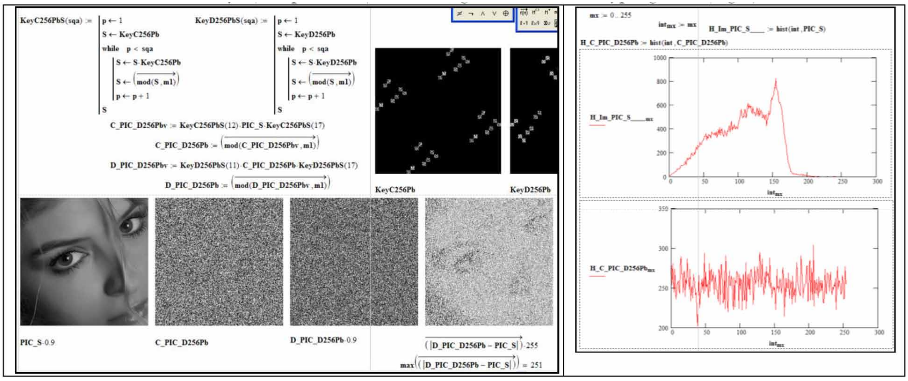
Figure 23. Results of simulation of CT TGD on the basis of parametric MAM and MK with the correct keys (1 experiment) and histogram TGD and cryptograms (right)



```
KeyC256PbS(sqa) := | p ← 1                      KeyD256PbS(sqa) := | p ← 1
                   | S ← KeyC256Pb                                 | S ← KeyD256Pb
                   | while  p < sqa                                | while  p < sqa
                   |    | S ← S·KeyC256Pb                          |    | S ← S·KeyD256Pb
                   |    | S ← (mod(S, m1)→)                        |    | S ← (mod(S, m1)→)
                   |    | p ← p + 1                                |    | p ← p + 1
                   | S                                             | S

C_PIC_D256Pbv := KeyC256PbS(12)·PIC_Doc·KeyC256PbS(17)
     C_PIC_D256Pb := (mod(C_PIC_D256Pbv, m1)→)
D_PIC_D256Pbv := KeyD256PbS(12)·C_PIC_D256Pb·KeyD256PbS(17)
     D_PIC_D256Pb := (mod(D_PIC_D256Pbv, m1)→)

mx := 0..255
int_mx := mx          H_Im_PIC_S____ := hist(int, PIC_Doc)
H_C_PIC_D256Pb := hist(int, C_PIC_D256Pb)

((|D_PIC_D256Pb − PIC_Doc|)→)·255
max(((|D_PIC_D256Pb − PIC_Doc|)→)) = 0
```

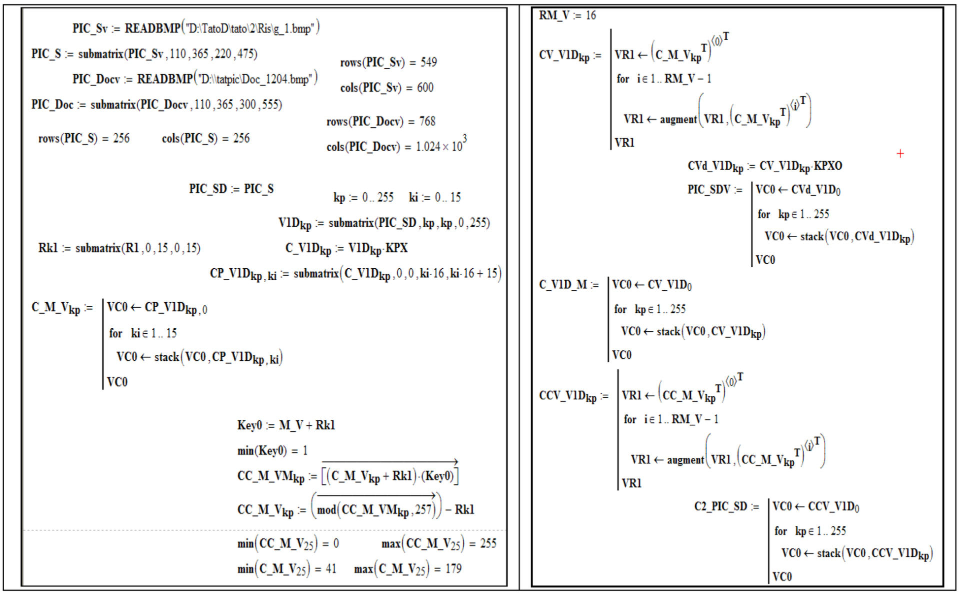
МАТРИЧНІ АФІННІ П
СЛІПИХ ПІДПИСІВ
Вступ. Використання
бурхливого розвитку криптог
та протоколів [1, 2], які о
цифрових даних.
Аналіз останніх дослі
стійкості, порівняно з скаля
запропоновано модифіковані

Figure 24. Results of simulation of CT TGD on the basis of parametric MAM and MK with wrong keys (2 experiments) and TGD histograms and cryptograms (right)



```
KeyC256PbS(sqa) := | p ← 1                      KeyD256PbS(sqa) := | p ← 1
                   | S ← KeyC256Pb                                 | S ← KeyD256Pb
                   | while  p < sqa                                | while  p < sqa
                   |    | S ← S·KeyC256Pb                          |    | S ← S·KeyD256Pb
                   |    | S ← (mod(S, m1)→)                        |    | S ← (mod(S, m1)→)
                   |    | p ← p + 1                                |    | p ← p + 1
                   | S                                             | S

C_PIC_D256Pbv := KeyC256PbS(12)·PIC_S·KeyC256PbS(17)
     C_PIC_D256Pb := (mod(C_PIC_D256Pbv, m1)→)
D_PIC_D256Pbv := KeyD256PbS(11)·C_PIC_D256Pb·KeyD256PbS(17)
     D_PIC_D256Pb := (mod(D_PIC_D256Pbv, m1)→)

mx := 0..255
int_mx := mx          H_Im_PIC_S____ := hist(int, PIC_S)
H_C_PIC_D256Pb := hist(int, C_PIC_D256Pb)

((|D_PIC_D256Pb − PIC_S|)→)·255
max(((|D_PIC_D256Pb − PIC_S|)→)) = 251
```

Figure 25. Fragments of Mathcad windows with formulas for forming (concatenate) blocks, encrypting, decoding images with block algorithm MAPTs and verification



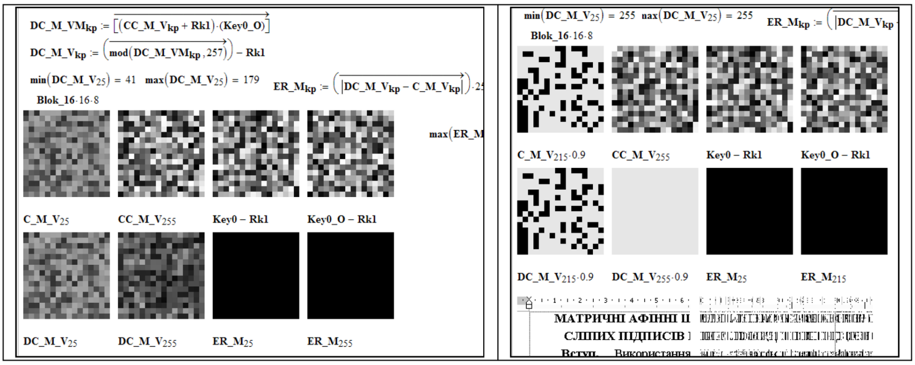
```
PIC_Sv := READBMP("D:\TatoD\tato\2\Ris\g_1.bmp")
PIC_S := submatrix(PIC_Sv, 110, 365, 220, 475)
PIC_Docv := READBMP("D:\\tatpic\Doc_1204.bmp")
PIC_Doc := submatrix(PIC_Docv, 110, 365, 300, 555)
rows(PIC_Sv) = 549
cols(PIC_Sv) = 600
rows(PIC_Docv) = 768
cols(PIC_Docv) = $1.024 \times 10^3$
rows(PIC_S) = 256        cols(PIC_S) = 256

PIC_SD := PIC_S
kp := 0 .. 255     ki := 0 .. 15
$V1D_{kp}$ := submatrix(PIC_SD, kp, kp, 0, 255)
Rk1 := submatrix(R1, 0, 15, 0, 15)
$C\_V1D_{kp}$ := $V1D_{kp}$·KPX
$CP\_V1D_{kp,ki}$ := submatrix($C\_V1D_{kp}$, 0, 0, ki·16, ki·16 + 15)

$C\_M\_V_{kp}$ := | VC0 ← $CP\_V1D_{kp,0}$
                  | for ki ∈ 1 .. 15
                  |   VC0 ← stack(VC0, $CP\_V1D_{kp,ki}$)
                  | VC0

Key0 := M_V + Rk1
min(Key0) = 1
$CC\_M\_VM_{kp} := \overrightarrow{[(C\_M\_V_{kp} + Rk1)\cdot(Key0)]}$
$CC\_M\_V_{kp} := \left(\overrightarrow{mod(CC\_M\_VM_{kp}, 257)}\right) - Rk1$

$min(CC\_M\_V_{25}) = 0$      $max(CC\_M\_V_{25}) = 255$
$min(C\_M\_V_{25}) = 41$      $max(C\_M\_V_{25}) = 179$
```

```
RM_V := 16
$CV\_V1D_{kp}$ := | VR1 ← $\left((C\_M\_V_{kp})^T\right)^{\langle 0 \rangle T}$
                 | for i ∈ 1 .. RM_V − 1
                 |   VR1 ← augment(VR1, $\left((C\_M\_V_{kp})^T\right)^{\langle i \rangle T}$)
                 | VR1

$CVd\_V1D_{kp}$ := $CV\_V1D_{kp}$·KPXO
PIC_SDV := | VC0 ← $CVd\_V1D_0$
           | for kp ∈ 1 .. 255
           |   VC0 ← stack(VC0, $CVd\_V1D_{kp}$)
           | VC0

C_V1D_M := | VC0 ← $CV\_V1D_0$
           | for kp ∈ 1 .. 255
           |   VC0 ← stack(VC0, $CV\_V1D_{kp}$)
           | VC0

$CCV\_V1D_{kp}$ := | VR1 ← $\left((CC\_M\_V_{kp})^T\right)^{\langle 0 \rangle T}$
                  | for i ∈ 1 .. RM_V − 1
                  |   VR1 ← augment(VR1, $\left((CC\_M\_V_{kp})^T\right)^{\langle i \rangle T}$)
                  | VR1

C2_PIC_SD := | VC0 ← $CCV\_V1D_0$
             | for kp ∈ 1 .. 255
             |   VC0 ← stack(VC0, $CCV\_V1D_{kp}$)
             | VC0
```

the form of a matrix of M_V (16x16) bytes, which is either a parametric (power) model and is used for MAPTs in the next stage. The essence of MAPT is to apply to matrices-B, as a collection of bytes (8-bit images (PIC_S, PIC_Doc, see Fig. 25), procedures on-element matrix multiplication by the corresponding 8-bit MKs (direct and inverse) of the same dimensions (Key0, Key0_O or Key_C (qa), Key_C (qo), Key_CN (qs), depending on the parameters and the formation modules of which are shown in Fig. 27, 28) using the multiplication and modulo operations. As can be seen from Fig. 29 and 30, the simulation results of the processes of direct and reverse CT TGDs and images with the dimension of 256x256 elements are confirmed the correct work of the models.

The cryptographic blocks processing is accompanied by the simultaneous mixing of their elements and their subsequent replacements of the MAPT, but, as it was shown by our researches with the entropy analysis, histograms of images, TGDs and their cryptogram, shown in Figure 29, in contrast to the image of a person, several iterative multiplications of the data matrix (MD) on the MK to the left or right may not be sufficient, especially with the application of the same MK. Therefore, in order to improve the algorithm, we propose to apply different current MKs to the blocks, as the process of their generation can be reduced to simple parametric models.

Figure 26. The results of the CT and the form of the current keys and blocks before and after the CT, the difference verification matrix-blocks: left - for the 1-st image, right - for the TGD



$DC\_M\_VM_{kp} := \overrightarrow{[(CC\_M\_V_{kp} + Rk1)\cdot(Key0\_O)]}$

$DC\_M\_V_{kp} := \left(\overrightarrow{mod(DC\_M\_VM_{kp}, 257)}\right) - Rk1$

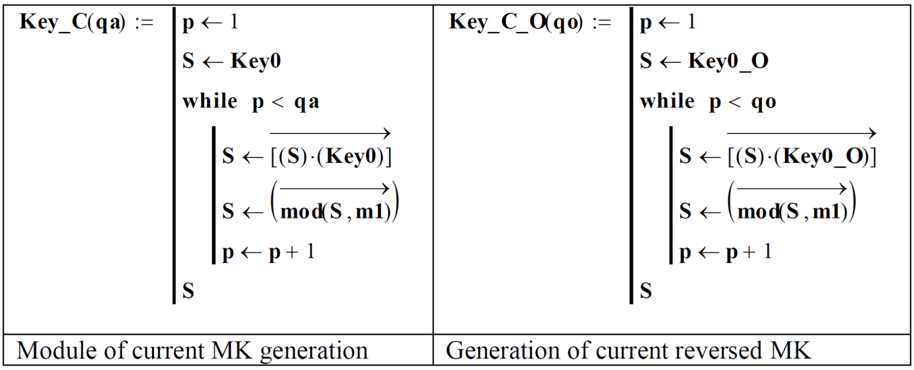
$min(DC\_M\_V_{25}) = 41 \quad max(DC\_M\_V_{25}) = 179$

$ER\_M_{kp} := \left(\overrightarrow{|DC\_M\_V_{kp} - C\_M\_V_{kp}|}\right)\cdot 2$

$min(DC\_M\_V_{25}) = 255 \quad nax(DC\_M\_V_{25}) = 255$

$ER\_M_{kp} := (|DC\_M\_V_{kp}$

Figure 27. Fragments of Mathcad windows with modules of MK formation



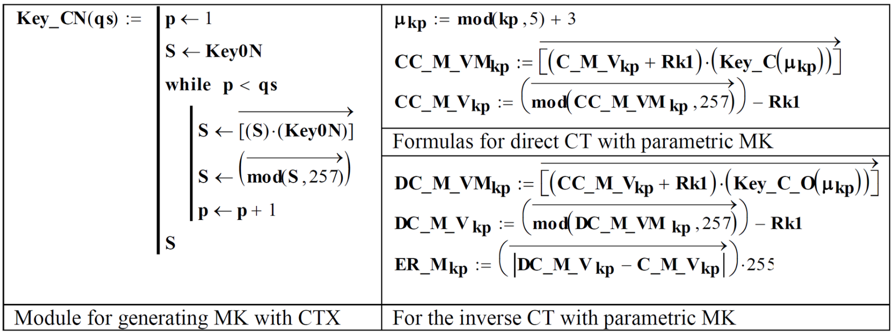
```
Key_C(qa) :=  p ← 1
              S ← Key0
              while  p < qa
                  S ← [(S)·(Key0)]→
                  S ← (mod(S, m1)→)
                  p ← p + 1
              S
```

Module of current MK generation

```
Key_C_O(qo) :=  p ← 1
                S ← Key0_O
                while  p < qo
                    S ← [(S)·(Key0_O)]→
                    S ← (mod(S, m1)→)
                    p ← p + 1
                S
```

Generation of current reversed MK

Figure 28. Fragments of Mathcad windows with modules for the MK formation and the CT formulas



```
Key_CN(qs) :=  p ← 1
               S ← Key0N
               while  p < qs
                   S ← [(S)·(Key0N)]→
                   S ← (mod(S, 257)→)
                   p ← p + 1
               S
```

Module for generating MK with CTX

$\mu_{kp} := mod(kp, 5) + 3$

$CC\_M\_VM_{kp} := \overrightarrow{[(C\_M\_V_{kp} + Rk1)\cdot(Key\_C(\mu_{kp}))]}$

$CC\_M\_V_{kp} := \left(\overrightarrow{mod(CC\_M\_VM_{kp}, 257)}\right) - Rk1$

Formulas for direct CT with parametric MK

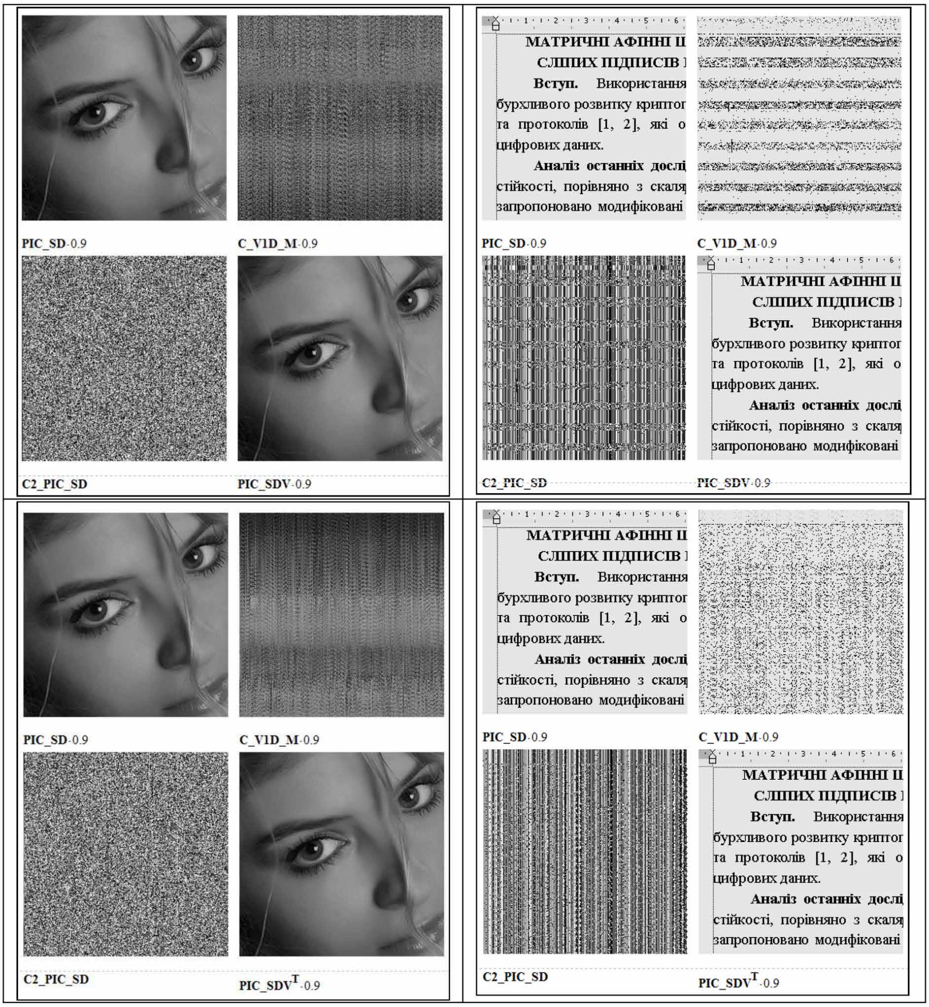
$DC\_M\_VM_{kp} := \overrightarrow{[(CC\_M\_V_{kp} + Rk1)\cdot(Key\_C\_O(\mu_{kp}))]}$

$DC\_M\_V_{kp} := \left(\overrightarrow{mod(DC\_M\_VM_{kp}, 257)}\right) - Rk1$

$ER\_M_{kp} := \left(\overrightarrow{|DC\_M\_V_{kp} - C\_M\_V_{kp}|}\right)\cdot 255$

For the inverse CT with parametric MK

Figure 29. Fragments of Mathcad windows with the results of CT modeling the block MAPC

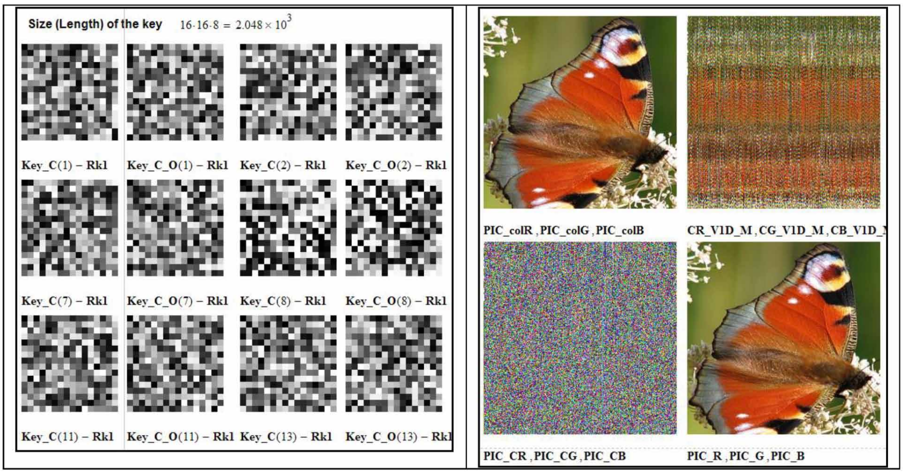


МАТРИЧНІ АФІННІ Ц
СЛІПИХ ПІДПИСІВ І
Вступ. Використання
бурхливого розвитку криптог
та протоколів [1, 2], які о
цифрових даних.
Аналіз останніх дослі
стійкості, порівняно з скаля
запропоновано модифіковані

Parametric block MAPC CT, the idea of which is based on the use of dependencies on the indexes of blocks and additional scalar-vector keys (VK) and as parameters influencing the power of matrices MD and MK by modulus in models of their matrix multiplication and the degree and form of permutation matrices. For different blocks and iterative steps different MKs are taken.

The analysis of histograms before and after the KT confirms that the proposed models give better results. The entropy of the TGD was 0.738, and the entropy of the cryptogram of the TGD increased 10.62 times and became equal to 7.837. The

Figure 30. The form of the parametric current MK (right) and the CT of a color image (left)



entropy of the image cryptogram has become almost equal to 8 bits per element: 7,997 (-0.04%!). Without knowledge of MK it is impossible to restore MD and, as was shown in (Krasilenko, 2011; Krasilenko, 2012), already with a dimension of 32x32 MK of type **P** The stability of models is ensured and with keys 16x16 8-bit elements, gives a substantial strength. The power of the set of possible keys has increased by an order of magnitude more than 10^{300} . Therefore, the stability of the models has increased significantly.

The section conclusions: New parametric matrix-algebraic models (MAMs) of block MAPC for CT are proposed and modulated. The results of their simulation are presented on the example of direct and inverse CT over images, which testify to their correct performance and efficiency. Considered aspects of creating current MK, models can be implemented with software or hardware matrix processors, and have high speed and stability of transformations.

Modeling and Study of the Generation Method of the Matrix Keys Flow and Their Quality

For the MAM there is an urgent need to form a whole range of permutation matrixes (MPs) from the main MK, which would satisfy a number of requirements. Since in papers (Krasilenko, 2017; Krasilenko, 2017) only the main MK of the general type, but not the series (flow) of the MP was considered, the purpose of this section is to model and study the processes for forming the flow of MP for MAM CT, checking the statistical and correlation properties of a series of generated MP.

Presentation of the main material of the section. Consider the situation for blocks of 256x256 bytes long representing a black-and-white image matrix or 256 bytes (2048 bits) length vector blocks that use MPs with size of 256x256 (Krasilenko, 2012; Krasilenko, 2014; Krasilenko, 2016). Since it is desirable for each block to have a number of MKs generated from the master key, taking into account the requirements for the cryptographic and statistical characteristics of MK, the urgent task of studying the processes of rapid reliable generation of the MK sequence in the form of MP is established, assuming that their number is also equal to 256. The results of modeling the processes of generating a series of MPs for such a situation with the Mathcad formulas and matrices of MP are shown in Fig 31. If the main MK is a random MP of KPX (Fig. 31), then it is unambiguously represented by a 256-component permutation (vector) of V_KPX and also in the form of an image or matrix of bytes (MB) of 16× 16 size with the peculiarity that all 256 grades of intensity are different.

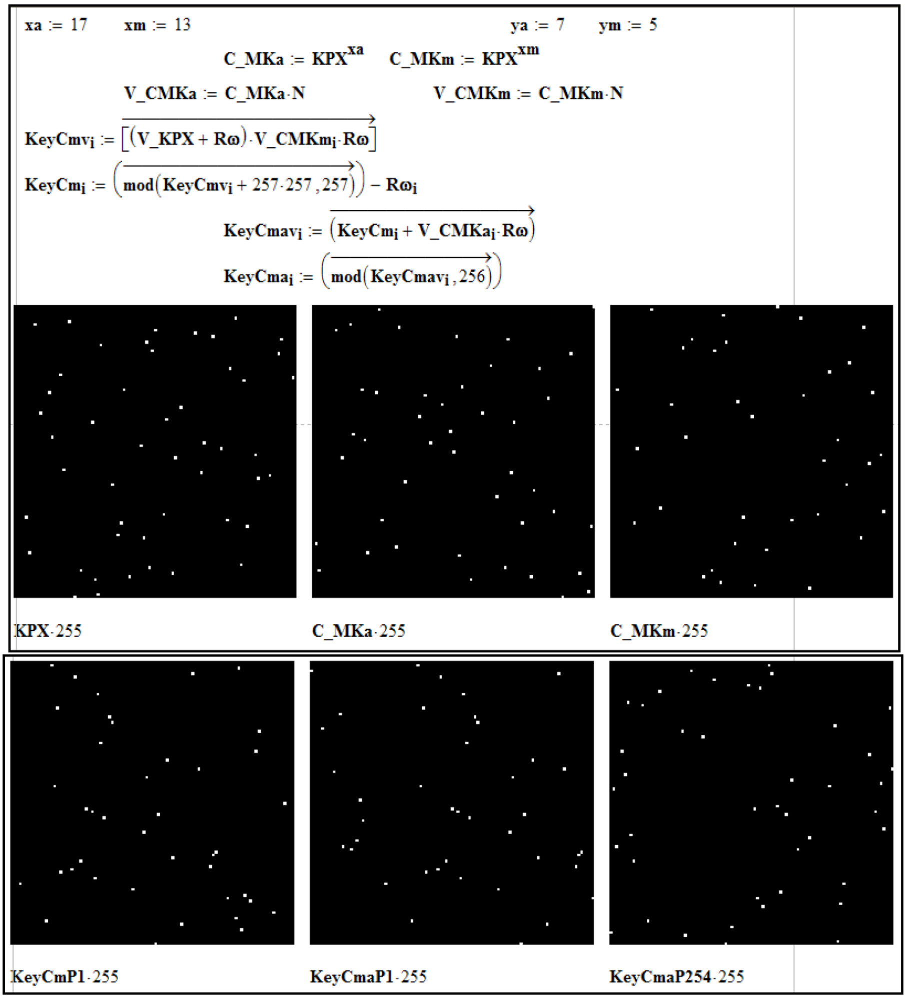
Using the coordinated scalars xa and xm, as KPX degrees, we form two additional matrices C_MKa, C_MKm, see Fig. 31, and the corresponding vectors V_CMKa, V_CMKm, which together with the vector V_KPX (vector representation KPX) are shown in Fig. 32. The histograms of all these vectors are horizontal lines, see Fig. 33, as well as all vector representations of generated permutations that are formed from V_KPX, as its i-th cryptograms, using the affine cipher and the pair of their components of vectors V_CMKa, V_CMKm (additive and multiplicative components). These cryptograms are i-th current permutations (vectors) of KeyCma, which can be uniquely represented in the form of bit matrices KeyCmaR dimension (256x256), for example, KeyCmaP1-254, Fig. 31. Fragments of Mathcad windows are shown in Fig. 34.

Since the histograms of all MPs (their vectors) are horizontal lines, and their entropy is 8 bits, then cryptanalysis on their basis is impossible. In addition, the main and two subsidiary MKs are secret, which allows only the CT parties to create or have this series of MK (MP). In principle, only the main and aforementioned xa and xm scalar keys can be secret or negotiated.

To study the quality of MK (MP), their properties **were investigated**, we calculated all of their possible correlation and equivalent normalized functions, which are represented as fragments of Mathcad windows (Fig. 35-37) and confirm the achievements of surprisingly beautiful properties. We note that the obtained results and their comparison also show that the mutually-equivalently normalized functions are better than mutually correlated ones.

For better perception and more efficient transmission of basic MK (MP) and sequence of created MP, the latter using software modules are converted to colored or black and white images, shown in Fig. 38 and can go as video stream frames (colored images corresponds to three basic MK).

Figure 31. Results of modeling processes for generating an array of MK (MP)



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

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

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

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

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

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

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

As can be seen from Fig. 36-37, for one MP (in the 200-th experiment) there is a similarity to another key, but this is due to the fact that xm is equal to “1”. This can easily be eliminated if the number of MPs in a sequence decreases from 256 to 255 for the one selected in the simulation and the situation described here.

The section conclusions. A method for generating a series of MK (MP) for multipage, block, matrix affine-permutation algorithms and MAM CT is proposed and modulated with Mathcad. The properties of a series of MK (MP) with the mutually equivalent normed functions that are more effective than correlations are investigated, and the adequacy and stability of the method is confirmed.

Figure 32. Vector representations of base MK for generating an array of MK (MP)

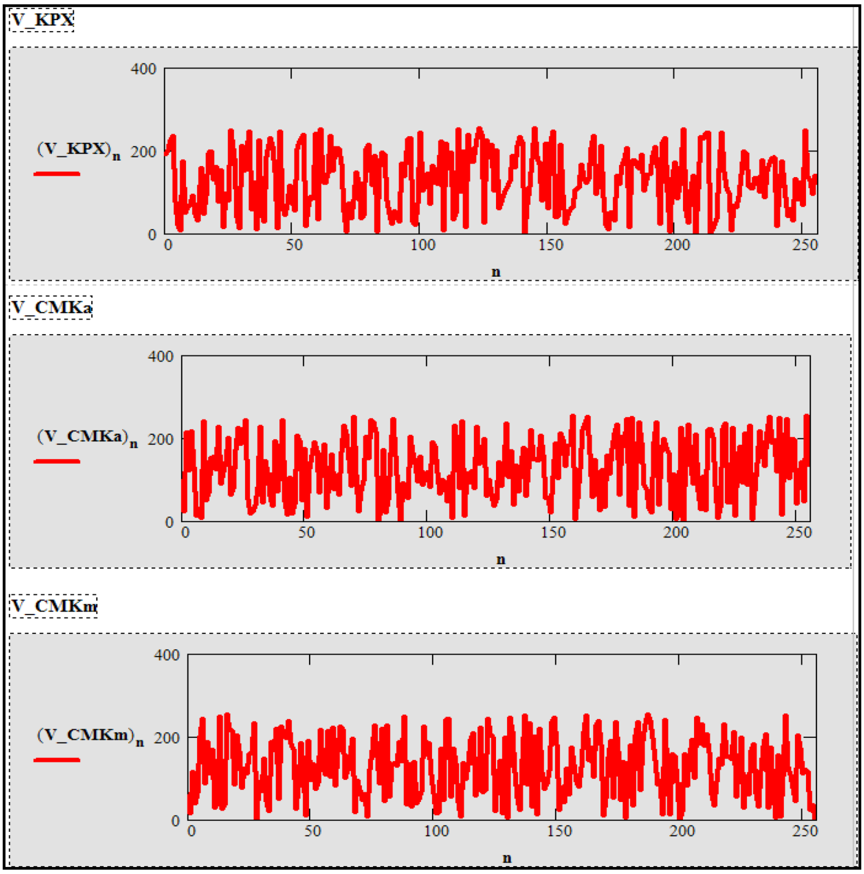
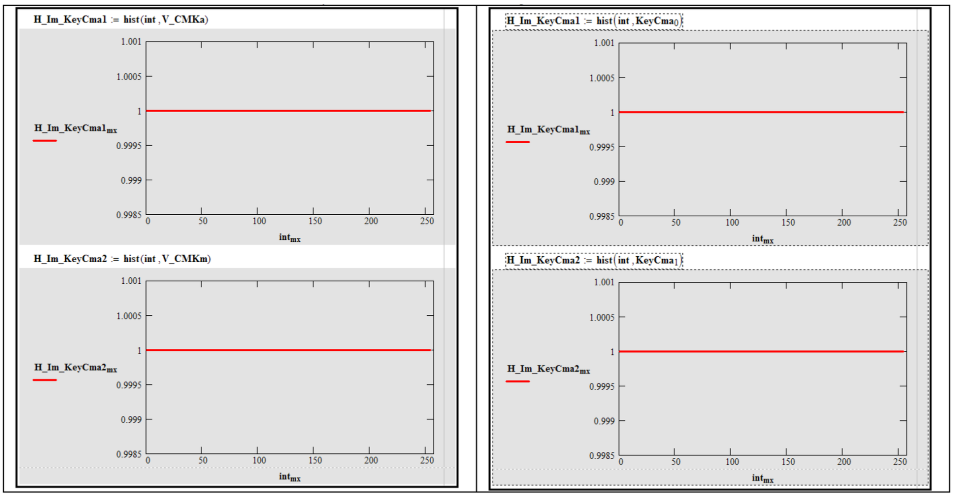


Figure 33. Histograms of vector representations of the base (left) and some (first, second) generated (right) MK (MP)



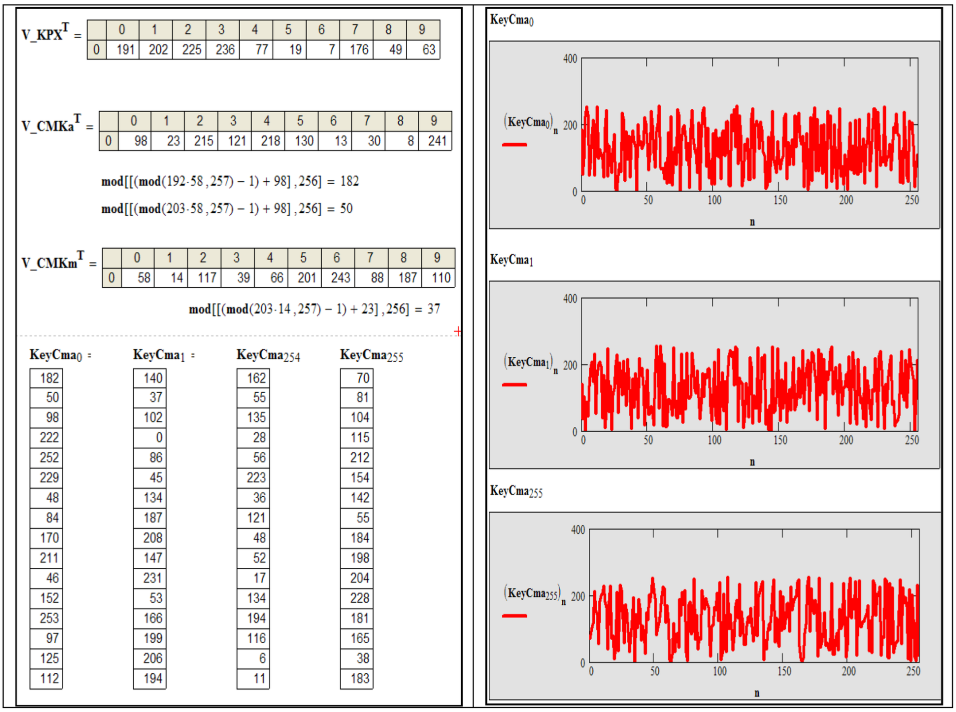
H_Im_KeyCma1 := hist(int, V_CMKa)

H_Im_KeyCma2 := hist(int, V_CMKm)

H_Im_KeyCma1 := hist(int, $KeyCma_0$)

H_Im_KeyCma2 := hist(int, $KeyCma_1$)

Figure 34. Fragments of Mathcad windows: one of the keys forming procedures (left) and vector representations of some (zero, first, 255th) generated (right) 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

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

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

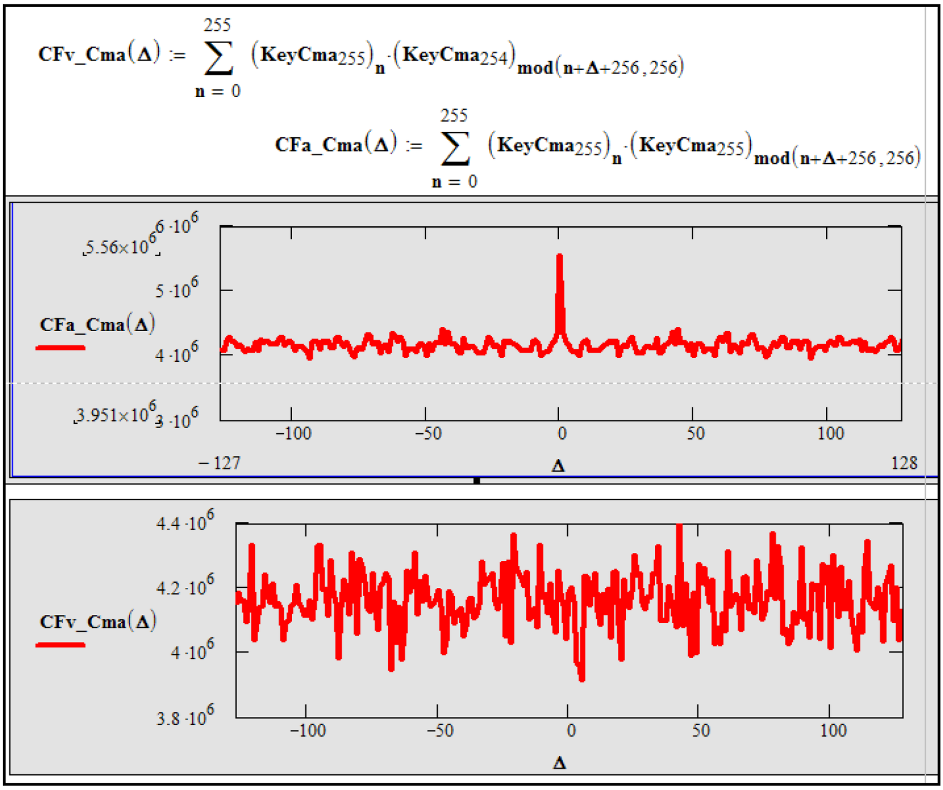
$V\_CMKm^T =$

	0	1	2	3	4	5	6	7	8	9
0	58	14	117	39	66	201	243	88	187	110

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

$KeyCma_0$ =	$KeyCma_1$ =	$KeyCma_{254}$	$KeyCma_{255}$
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

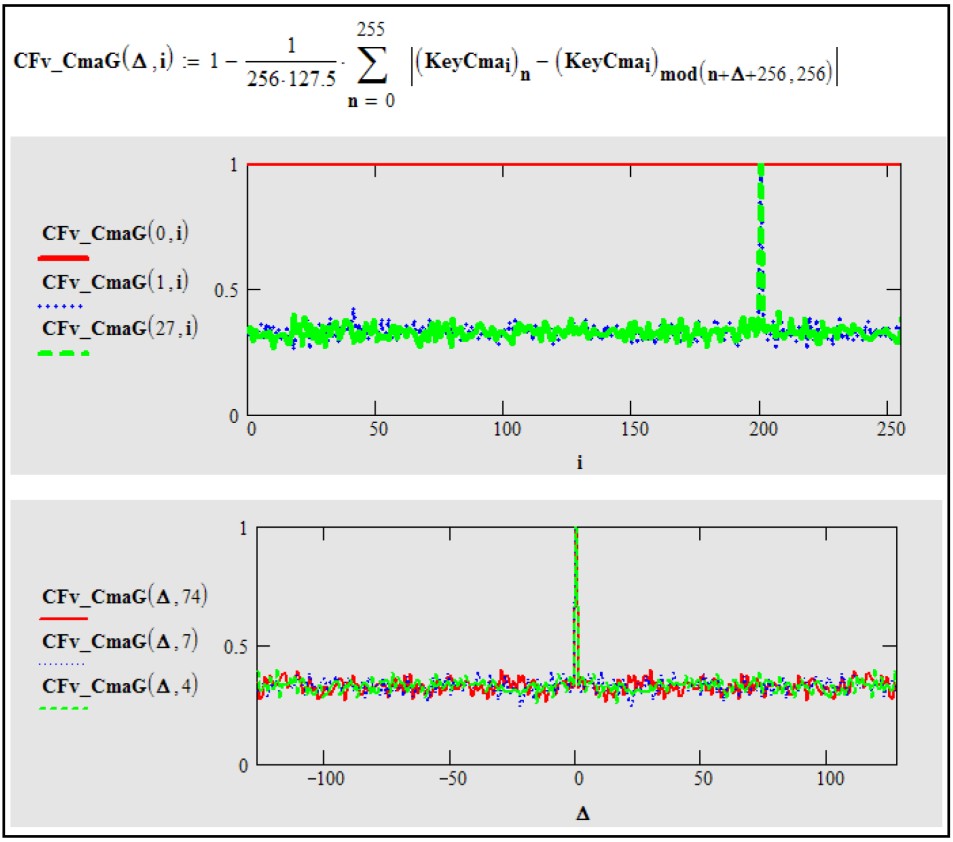
Figure 35. Formulas and the auto-correlation CFa_Cma and mutual-correlation CFv_Cma functions, depending on cyclic shift, displacement of elements of vectors MP



$$\mathrm{CFv\_Cma}(\Delta) := \sum_{n=0}^{255} \left(\mathrm{KeyCma}_{255}\right)_n \cdot \left(\mathrm{KeyCma}_{254}\right)_{\mathrm{mod}(n+\Delta+256,256)}$$

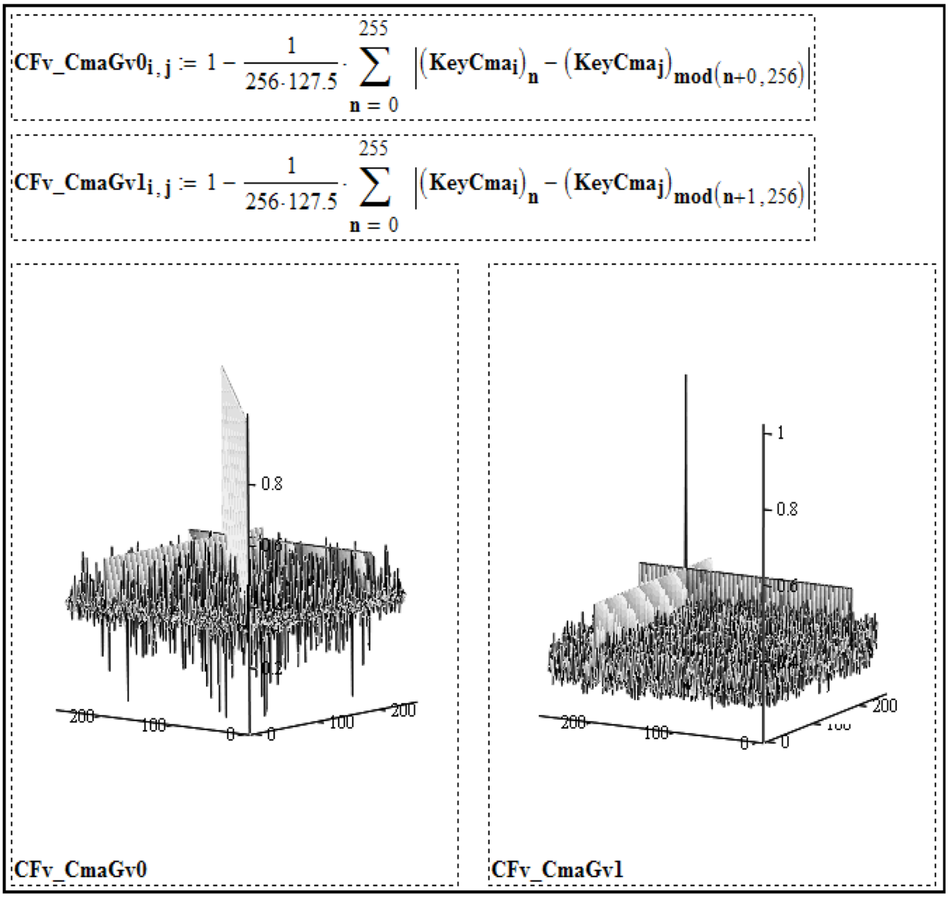
$$\mathrm{CFa\_Cma}(\Delta) := \sum_{n=0}^{255} \left(\mathrm{KeyCma}_{255}\right)_n \cdot \left(\mathrm{KeyCma}_{255}\right)_{\mathrm{mod}(n+\Delta+256,256)}$$

Figure 36. Formulas and the mutually-equivalent CFv_CmaG functions depending on the number of MP (i) and cyclic shift, bias of the elements of t vectors MP



$$\mathrm{CFv\_CmaG}(\Delta,i) := 1-\frac{1}{256\cdot 127.5}\cdot\sum_{n=0}^{255}\left|\left(\mathrm{KeyCma}_i\right)_n-\left(\mathrm{KeyCma}_i\right)_{\mathrm{mod}(n+\Delta+256,256)}\right|$$

Figure 37. Formulas and appearance (3D) of the mutually-equivalent CFv_CmaG functions depending on the numbers of the MP (i, j) for the "0" and "1st" displacements of the elements of the vectors



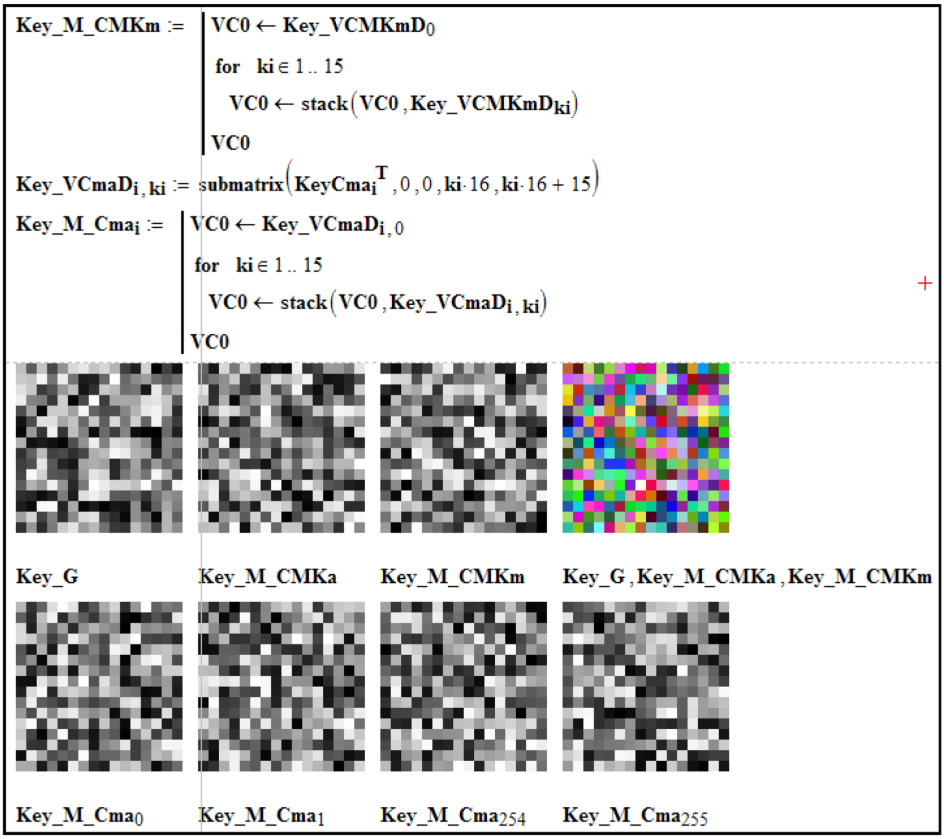
$$\mathbf{CFv\_CmaGv0}_{\mathbf{i},\mathbf{j}} := 1 - \frac{1}{256\cdot 127.5}\cdot\sum_{\mathbf{n}=0}^{255}\left|\left(\mathbf{KeyCma}_{\mathbf{i}}\right)_{\mathbf{n}} - \left(\mathbf{KeyCma}_{\mathbf{j}}\right)_{\mathbf{mod}(\mathbf{n}+0,256)}\right|$$

$$\mathbf{CFv\_CmaGv1}_{\mathbf{i},\mathbf{j}} := 1 - \frac{1}{256\cdot 127.5}\cdot\sum_{\mathbf{n}=0}^{255}\left|\left(\mathbf{KeyCma}_{\mathbf{i}}\right)_{\mathbf{n}} - \left(\mathbf{KeyCma}_{\mathbf{j}}\right)_{\mathbf{mod}(\mathbf{n}+1,256)}\right|$$

CFv_CmaGv0

CFv_CmaGv1

Figure 38. Matrix representation of the basic MK and a number of MPs.



```
$Key\_M\_CMKm :=$ | $VC0 \leftarrow Key\_VCMKmD_0$
                  | for $ki \in 1..15$
                  |     $VC0 \leftarrow stack(VC0, Key\_VCMKmD_{ki})$
                  | $VC0$
$Key\_VCmaD_{i,ki} := submatrix(KeyCma_i^T, 0, 0, ki \cdot 16, ki \cdot 16 + 15)$
$Key\_M\_Cma_i :=$ | $VC0 \leftarrow Key\_VCmaD_{i,0}$
                   | for $ki \in 1..15$
                   |     $VC0 \leftarrow stack(VC0, Key\_VCmaD_{i,ki})$
                   | $VC0$
```

CONCLUSION

In the four sections of the chapter, the authors propose and consider new multifunctional matrix-algebraic models of cryptographic image transformations, the variety of matrix models, including matrix affine ciphers, block parametrical and matrix affine permutation ciphers. The algorithms and protocols for generating the necessary matrix keys are discussed in the chapter. The authors show the advantages of the cryptographic models, such as: adaptability to various formats, multi-functionality, ease of implementation on matrix parallel structures, interchangeability of iterative procedures and matrix exponentiation modulo, ease of selection and control of cryptographic transformation parameters. The simulation results of the proposed algorithms and procedures for the direct and inverse transformation of images, with the aim of masking them during transmission, are demonstrated and discussed in this chapter. The authors evaluate the effectiveness and implementation reliability of matrix-algebraic models of cryptographic image transformations. The results of model experiments on encryption and decryption of text-graphic documents, images and video files using the software products Mathcad and LabVIEW are shown by the authors.

REFERENCES

Chang. (2001). A new encycle algorithm for image cryptosystems. *Journal of Systems and Software, 58*, 83-91.

Deergha Rao, K. (2011). A New and Secure Cryptosyce for Image Encryption and Decryption. *IETE Journal of research, 57*(2), 165-171.

Han. (2005). An Asymmetric Image Encryption Based on Matrix Transformation. *Ecti Transactions on Computer and Information Technology, 1*(2), 126-133.

Khoroshko, V. O. (2003). *Methods and means of information protection: Teaching. Academic Press.*

Korkishko, T. A. (2003). *Algorithms and Processors of Symmetric Block Encryption: Scientific Edition*. Baku: V.A. Melnik. - Lviv.

Kovalchuk A. (2009). *Increasing the stability of the RSA system when encrypting images*. Academic Press.

Krasilenko, V. G. (2013). *Matrix models of permutations with matrix-bit decomposition for cryptographic transformations of images and their modeling. In Science and educational process: a scientific and methodical collection of materials of the NPC of all the Universities "Ukraine"* (pp. 90–92). Vinnytsya: Vinnytsia Socio-Economic Institute of the University of Ukraine.

Krasilenko, V. G. (2006). A noise-immune crptographis information protection method for facsimile information transmission and the realization algorithms. *Proc. SIEE, 6241*, 316-322.

Krasilenko, V.G. (2004). Algorithms and architecture for high-precision matrix-matrix multipliers based on optical four-digit alternating arithmetic. *Measuring and computing engineering in technological processes, 1*, 13-26.

Krasilenko, V.G. (2012). Algorithms for the formation of two-dimensional keys for matrix algorithms of cryptographic transformations of images and their modeling. *Systems of information processing, 8*, 107-110.

Krasilenko, V. G. (2008). Simulation of the modified algorithm for creating 2-D keys in cryptographic applications. *Scientific-methodical collection of the scientific-practical conference "Science and educational process"*, 107-109.

Krasilenko, V. G. (2006). Development of the method of cryptographic protection of information text-graphic type. Science and educational process: a scientific and methodical collection of scientific and practical conference, 73-74.

Krasilenko, V. G. (2012). Simulation of Blind Electronic Digital Signatures of Matrix Type on Confidential Text-Graphic Documentation. *International Scientific-Methodical Conference*, 103-107.

Krasilenko, V. G. (2012). Modifications of the RSA system for creation of matrix models and algorithms for encryption and decryption of images on its basis. Systems of information processing, 8, 102-106.

Krasilenko, V.G. (2011). Matrix Affine Ciphers for the Creation of Digital Blind Signatures for Text-Graphic Documents. *Systems of information processing, 7*(97), 60 - 63.

Krasilenko, V.G. (2009). Modeling of Matrix Cryptographic Protection Algorithms. *Bulletin of the National University of Lviv Polytechnic "Computer Systems and Networks", 658*, 59-63.

Krasilenko, V.G. (2012). Matrix affine and permutation ciphers for encryption and decryption of images. *Systems of information processing, 3*(101), 53-62.

Krasilenko, V. G. (2013). Matrix models of cryptographic transformations of images with matrix-bit-map decomposition and mixing and their modeling. Materials of 68 NTC "Modern Information Systems and Technologies. Informational security", 139-143.

Krasilenko, V. G. (2014). Cryptographic transformations of images based on matrix models of permutations with matrix-bit-map decomposition and their modeling. *Bulletin of Khmelnitsky National University. Technical sciences, 1*, 74-79.

Krasilenko, V. G. (2010). Modeling of Matrix Affine Algorithms for the Encryption of Color Images. Computer technologies: science and education: abstracts of reports v VseUkr. sci. conf., 120-124.

Krasilenko, V. G. (2016). Modeling and research of cryptographic transformations of images based on their matrix-bit-map decomposition and matrix models of permutations with verification of integrity. In *Electronics and Information Technologies: a collection of scientific works*. Lviv: Lviv Ivan Franko National University. Retrieved from http://elit.lnu.edu.ua/pdf/6_12.pdf

Krasilenko, V. G. (2016). Simulation of cryptographic transformations of color images based on matrix models of permutations with spectral and bit-map decompositions. *Computer-integrated technologies: education, science, 23*, 31-36. Retrieved from http://ki.lutsk-ntu.com.ua/node/132/section/9

Krasilenko, V. G. (2016). Modeling cryptographic transformations of color images with verification of the integrity of cryptograms based on matrix permutation models. *Materials of the scientific and practical Internet conference "Problems of modeling and development of information systems",* 128-136. Retrieved from http://ddpu.drohobych.net/wp-content/uploads/2016/04/material_konf.pdf37

Krasilenko, V. G. (2016). Cryptographic transformations (CTs) of color images based on matrix models with operations on modules. In *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*. Lutsk: RVB of Lutsk National Technical University.

Krasilenko, V. G. (2017). Modeling Protocols for Matching a Secret Matrix Key for Cryptographic Transformations and Matrix-type Systems. *Systems of information processing, 3*(149), 151-157.

Krasilenko, V. G. (2017). Modeling of multi-stage and multi-protocol protocols for the harmonization of secret matrix keys. *Computer-integrated technologies: education, science, production: scientific journal, 26*, 111-120. Retrieved from http://ki.lutsk-ntu.com.ua/node/134/section/27

Rashkevich, Y.M. (2009). Affine transformations in modifications of the RSA image encryption algorithm. *Automation. Electrotechnical complexes and systems, 2*(24), 59-66.

Yemets, V. (2003). Modern cryptography. Lviv: Baku.

About the Contributors

Oleg Sergiyenko received the B.S., and M.S., degrees in Kharkiv National University of Automobiles and Highways, Kharkiv, Ukraine, in 1991, 1993, respectively. He received the Ph.D. degree in Kharkiv National Polytechnic University on specialty "Tools and methods of non-destructive control" in 1997. He has editor of 1 book, written 8 book chapters, 87 papers and holds 1 patent of Ukraine. Since 1994 till the present time he was represented by his research works in several International Congresses of IEEE, ICROS, SICE, IMEKO in USA, England, Japan, Italy, Austria, Ukraine, and Mexico. Dr.Sergiyenko in December 2004 was invited by Engineering Institute of Baja California Autonomous University for researcher position. He is currently Head of Applied Physics Department of Engineering Institute of Baja California Autonomous University, Mexico, director of several Master's and Doctorate thesis. He was a member of Program Committees of various international and local conferences. He is member of Scientific Council on Electric specialties in Engineering Faculty of Autonomous University of Baja California and Academy of Engineering. Included in the 2010-2015 Edition of Marquis' Who's Who in the World.

Moisés Rivas-López was born in June, 1, 1960. He received the B.S. and M.S. degrees in Autonomous University of Baja California, México, in 1985 and 1991, respectively and the PhD degree in Applied Physics, in the same university, in 2010. He is editor of a book, has written 38 papers and 6 book chapters in optical scanning, 3D coordinates measurement, and structural health monitoring applications. He holds a patent and has presented different works in several international congresses, of IEEE, ICROS, SICE, AMMAC in America and Europe. He was Dean of Engineering Institute of Autonomous University Baja California (1997-2005) and Rector of Polytechnic University of Baja California (2006 -2010). He is member of National Researcher System Dr. Rivas was Head of Engineering Institute of Baja California Autonomous University Since 1997 to 2005; was Rector of Baja California Polytechnic University Since 2006 to 2010 and now is full researcher and the head of physic engineering department, of Engineering Institute of UABC, Mexico.

Wendy Flores-Fuentes received the master's degree in engineering from Technological Institute of Mexicali in 2010, and the Ph.D. degree in science, applied physics, with emphasis on Optoelectronic Scanning Systems for SHM, from Autonomous University of Baja California in June 2014. Until now she is the author of 24 journal articles in Elsevier, IEEE Emerald and Springer, 13 book chapters and 5 books in Intech, IGI global and Springer, 27 proceedings articles in IEEE ISIE 2017-2017, 2019, IECON 2018-2019, the World Congress on Engineering and Computer Science (IAENG 2013), IEEE Section Mexico IEEE ROCC2011, and the VII International Conference on Industrial Engineering ARGOS 2014. Recently, she has organized and participated as Chair of Special Session on ''Machine Vision, Control and Navigation'' at IEEE ISIE 2015, 2017 and 2019. She has been a reviewer of several articles in Taylor and Francis, IEEE, Elsevier, and EEMJ (Gh. Asachi Technical University of Iasi. Currently, she is a full-time professor-researcher at Universidad Autónoma de Baja California, at the Faculty of Engineering.

Julio C. Rodríguez-Quiñonez received the Ph.D. degree from Baja California Autonomous University, México, in 2013. He is currently Professor of Electronic Topics with the Engineering Faculty, Autonomous University of Baja California. His current research interests include automated metrology, stereo vision systems, control systems, robot navigation and 3D laser scanners. He has written over 50 papers, 3 Book Chapters, has been guest editor of Journal of sensors, book editor, and has been reviewer for IEEE Sensors Journal, Optics and Lasers in Engineering, IEEE Transaction on Mechatronics and Neural Computing and Applications of Springer, he participated as a reviewer and Section Chair of IEEE conferences in 2014, 2015, 2016 and 2017. He is involved in the development of optical scanning prototype in the Applied Physics Department and is currently research head in the development of a new stereo vision system prototype.

Lars Lindner was born on July 20th 1981 in Dresden, Germany. He received his M.S. degree in mechatronics engineering from the TU Dresden University in January 2009. He was working as graduate assistant during his studies at the Fraunhofer Institute for Integrated Circuits EAS in Dresden and also made his master thesis there. After finishing his career, he moved to Mexico and started teaching engineering classes at different universities in Mexicali. Since August 2013 he began his PhD studies at the Engineering Institute of Autonomous University of Baja California in Mexicali with the topic "Theoretical Method to Increase the Speed of Continuous Mapping of a Three-dimensional Laser Scanner using Servomotor Control", in which he worked in the development of an optoelectronic prototype for the measurement of 3D coordinates, using laser dynamic triangulation. Its academic products include 13 original research articles, 3 articles in national congresses, 20 articles in international congresses and 9 book chapters. In September 2017, he was appointed as a Level 1 National Researcher by the National System of Researchers CONACYT for the period 2018-2020. Right now he is working as a technician assistant at the Engineering Institute of Autonomous University of Baja California for the department of applied physics.

* * *

Roman Antoshchenkov was born on September 14, 1982 in Kharkov, Ukraine. In 2006, he graduated from the Kharkiv Petro Vasylenko National Technical University of Agriculture (Kharkov, Ukraine) and obtained the qualification of an agricultural mechanical engineer. The degree of Candidate of Technical Sciences at the Kharkiv Petro Vasylenko National Technical University of Agriculture (Kharkov, Ukraine) in the specialty “Machines and means of agricultural mechanization” in 2010 The degree of doctor of (technical) sciences was received at the Kharkiv Petro Vasylenko National Technical University of Agriculture (Kharkov, Ukraine) with a degree in Machinery and Means of Agricultural Production Mechanization in 2018. He is the author of a monograph, 2 textbooks, 75 articles, 5 patents of Ukraine. Since 2006, he has participated in international scientific conferences in Bulgaria, Belarus, Russia and Ukraine. He began his scientific activity in 2006 as a junior researcher at the Kharkiv Petro Vasylenko National Technical University of Agriculture (Kharkiv, Ukraine). Currently, he is the head of the department of mechatronics and machine parts of the Kharkiv Petro Vasylenko National Technical University of Agriculture. Under his leadership, defended dozens of master’s works. He leads the work of a graduate student.

Viktor Antoshchenkov was born on March 24, 1957. In 1985 he graduated from the Kharkov Institute of Mechanization and Electrification of Agriculture (Kharkov, Ukraine) and received the qualification of an engineer-mechanic. He obtained the degree of PhD at the Kharkov Institute of Mechanization and Electrification of Agriculture (Kharkov, Ukraine) in the specialty “Mechanization of Agricultural Production” in 1991. He is the author of 5 textbooks, 53 articles, 3 copyright certificates of the USSR and 5 patents of Ukraine. He is a member of the organizing committee of the International Youth Forum “Youth and Agricultural Machinery in the XXI Century”; scientific and practical workshop; scientific-practical conference “Technical progress in the agricultural sector”; scientific-practical conference “Mechanization of Agriculture”; Interuniversity student seminar “Tractor Energy”. He began his scientific activity in 1978 as a senior technician in the department of tractors and automobiles, as an engineer, junior researcher, assistant, associate professor, and from 2014 a professor in this department. From 2007 to 2015, he held the position of Deputy Director, and from 2015 to 2017, Acting Director of the Educational and Scientific Institute of Mechatronics and Management Systems. Since 2017, he holds the position of Professor at the Department of Tractors and Automobiles of the Kharkiv Petro Vasylenko National Technical University of Agriculture. Under his leadership several dozens of master's works and one dissertation of the candidate of technical sciences were defended.

Joel Antúnez-García was born in Ensenada B. C., México, in 1975. He received the B. Sc. degree in Physics from Universidad Autónoma de Baja California (UABC), México, in 1999. The M. Sc. from Centro de Investigación Científica y de Educación Superior de Ensenada (CICESE), México, in 2004. The Ph. D. in Physical-Industrial Engineering from Universidad Autónoma de Nuevo Léon (UANL), Méxio, in 2010. From 2012 to 2013 he did a postdoctoral stay at Centro de Nanociencias y Nanotecnología at UNAM working on DFT calculations to obtain the electronic properties of different zeolites. From 2013-2015 he was working as professor at Centro de Enseñanza Técnica y Superior (CETYS university). From 2016 to date, he has been involved in the theoretical study of bi-and tri-metallic catalysts based on MoS2 compounds.

Danilo Cáceres Hernández received the Bachelor's degree in electrical and electronic engineering from the Universidad Tecnológica de Panamá, Panamá City, Panama, the Master of Science in electrical engineering, and the Ph.D. in electrical engineering from the University of Ulsan, Ulsan, South Korea, in 2004, 2011, and 2017, respectively. He is currently a Full-Time Professor in the Electrical Department at the Universidad Tecnológica de Panamá.

Wilmar Hernandez graduated in 1992 with an Electronics Engineering degree from the Instituto Superior Politécnico Jose Antonio Echeverria (ISPJAE), Havana, Cuba, and received a Specialist degree in Microelectronics from the ISPJAE in 1994. Also, he received a M.S. degree in Signal Treatment and a Ph.D. degree in Electronic Engineering from Enginyeria La Salle at the Universitat Ramon Llull, Barcelona, Spain, in 1997 and 1999, respectively. From 1992 to 1995, he was a lecturer in the Electrical Engineering Faculty at the ISPJAE and a researcher in the Microelectronic Research Center at the same university. From 1999 to 2003, he was with the Department of Electronics and Instrumentation in the University Institute for the Automobile Research at the Universidad Politécnica de Madrid (UPM), Spain, where he was the Technical Director of such a department from January 2003 to January 2004. From January 2004 to March 2013 he was an Associate Professor of Circuits and Systems in the Department of Circuits and Systems in the EUIT de Telecomunicación at the UPM. From September 2014 to September 2015 he was a researcher of SENESCYT, Ecuador, under the Prometeo fellowship program. From December 2015 to November 2017 he was a professor at the Universidad Técnica Particular de Loja, Ecuador, and currently he is a professor at the Universidad de Las Américas, Ecuador.

Juan Ivan Nieto Hipólito received his M.Sc. degree from CICESE Research Center in 1994 (México). His PhD degree from Computer Architecture Department at Polytechnic University of Catalonia (UPC, Spain) in 2005. Since august 1994 he is full professor at the Autonomous University of Baja California (UABC, México), where he was the leader of the Telematic research group from 2007 to 2012. His research interest is in applications of ICT, mainly wireless, mac and routing protocols for e-health.

Kang-Hyun Jo received the Ph.D. degree in Computer Controlled Machinery from Osaka University, Japan, in 1997. After a year of experience at ETRI as a postdoctoral research fellow, he joined the School of Electrical Engineering, University of Ulsan, Ulsan, Korea. He has served as a director or an AdCom member of Institute of Control, Robotics and Systems, The Society of Instrument and Control Engineers, and IEEE IES Technical Committee on Human Factors Chair. Currently, he is serving as AdCom member, and from 2018, as the Secretary, of the IEEE IES. He has also been involved in organizing many international conferences such as International Workshop on Frontiers of Computer Vision, International Conference on Intelligent Computation, International Conference on Industrial Technology, International Conference on Human System Interactions, and Annual Conference of the IEEE Industrial Electronics Society. At present, he is an Editorial Board Member for international journals, such as the International Journal of Control, Automation, and Systems and the Transactions on Computational Collective Intelligence. His research interests include computer vision, robotics, autonomous vehicle, and ambient intelligence.

Vladimir Krasilenko was born 20 July 1953, Vinnitsa Region, Ukraine. Education: Radio Engineers Diploma, 1975, Candidate of Sciences Degree (PhD), 1988, Information systems, Vinnitsa State Technical University. Engineering positions and head of the department of research institutes and enterprises -1975-1982; PhD student and Lecturer Assistant, 1982-88; Senior, Leading Scientific Researcher, Head of Special Design and Technology Bureau of Vinnitsa National Technical University, Leading Scientist, Enterprise «Injector», Science Research Institute of Videotechnic, 1988-2001; Associated Professor, Professor of Information Technology Department, Vinnitsa Social Economy Institute of Univ. “Ukraine”, 2001-2015. He has authored/ co-authored more 400 scientific works, including 188 inventions, about 80 articles in scientific journals and Proc. SPIE, 2 chapter published by InTech, 5 tutorial books. Krasilenko named best Young Inventor of Ukraine in 1985, Member of SPIE with 1995 and Senior Member of SPIE with 2012. Research interests: optoelectronic devices and multifunctional logic elements for parallel image processing and for computing, neural networks, multi-valued, continuous matrix logic, recognition, cryptography, information protection, analog-to-digital transformations.

Laksono Kurnianggoro received his bachelor of engineering from the University of Gadjah Mada, Indonesia, in 2010. He is currently a Ph.D. student at the Graduate School of Electrical Engineering, University of Ulsan, Ulsan, Korea. He is actively participating as a member of societies such as IEEE. His research interest include stereo vision, 3D image processing, computer vision, and machine learning. He has scientific publications in some publishers such as IEEE, Springer, and Elsevier. He also involved in several projects including development of autonomous vehicle system, advanced car washer system, low-cost 3D scanner, autonomous robot, and many mores. He is also an active contributor of the popular computer vision library, like OpenCV.

Alexander Lazarev is an assistant professor at the Vinnytsia National Technical University (VNTU), Ukraine. He completed his graduate studies with a PhD from the VNTU in 2003 and his undergraduate studies at the VNTU with a MSc in Electronics Engineering in 1998. He has authored/co-authored more than 250 publications.

Andrei Malchikov is a candidate of technical sciences Academic title: assistant Professor From 2004 to 2010 studied mechatronics and robotics at Southwest State University and graduated with degrees at bachelors and masters level. In 2013 he defended his candidate thesis: “Dynamics of controlled motion of a six-link in-pipe robot”. He published more than 50 publications and has more than 10 patents on inventions.

Andres Santiago Martinez Leon, 26 years, born in Ecuador, received a B.Sc. (with honors) in 2015 and a M.Sc. (with honors) in 2017 in Mechatronic and Robotic Engineering at Southwest State University, Kursk, Russian Federation. At present, pursuing a Ph.D. in Mechanical Engineering at Southwest State University, Kursk, Russian Federation. Since 2017 Associated Teacher at Escuela Politécnica Nacional, Quito, Ecuador and Universidad Estatal Amazónica, Puyo, Ecuador. Author and coauthor of several international scientific papers and also 1 RU patent and 2 pending patents. The current research involves the development of Unmanned Aerial Vehicles (UAV).

Viktor I. Melnyk was born January 8, 1958. In 1980 was graduated from Poltava Agricultural Institute (Poltava, Ukraine) and was qualified as a mechanical engineer in agriculture. PhD degree obtained at the Kharkov State Technical University of Radio Electronics (Kharkiv, Ukraine) on specialty "Technology, equipment and production of electronic devices" in 2000. He get the Degree of Doctor of Sciences (in Technics) at the Kharkov National Technical University of Agriculture named after Peter Vasilenko (Kharkiv, Ukraine) on specialty "Machinery and mechanization of agricultural production" in 2011. He is the author of 4 books, 261 articles, 39 patents of the Russian Federation and 19 patents of Ukraine. Since 1986 participated in the international scientific conferences in the United States, Belarus, Russia and Ukraine. He is currently a professor in the Department of technologic systems optimization, the Head of the research laboratory «Engineering of nature management», as well as the deputy director for scientific activities in Institute of Mechatronics and management systems at the Kharkov National Technical University of Agriculture. He was tutor of several masters' and two PhD thesis. He is deputy chairman of the specialized scientific council for doctoral dissertations on specialty "Machinery and mechanization of agricultural production" at the Kharkov National Technical University of Agriculture. Since 2014 he is the Editor-in-Chief of the scientific journal "Engineering of nature management".

Alfredo Méndez Alonso was born in Madrid, Spain, in June 6, 1958. He graduated with a degree in Mathematical Sciences (Section of Fundamental Mathematics) in 1981, from the Universidad Complutense de Madrid (UCM). Also, he received a M.S. degree in Mathematical Sciences in 1987 and a Ph.D. degree in Mathematical Sciences (Section of Statistics and Operational Research) in 1995 from the UCM. From 1983 to 1993, he was a lecturer at the EUIT Agrícola at the Universidad Politécnica de Madrid (UPM), Spain. Since 1993 he has been professor of Mathematics in the Department of Applied Mathematics to Information and Communication Technologies, of the ETS Ingeniería y Sistemas de Telecomunicación at the UPM, where he was the director of the department from May 2004 to May 2012.

Fabian N. Murrieta-Rico was born in September the 7th of 1986. He received the B.Eng. and M.Eng. degrees from Instituto Tecnológico de Mexicali (ITM) in 2004, and 2013 respectively. In 2017 he received his Ph. D. in Materials Physics from Centro de Investigación Científica y Educación Superior de Ensenada (CICESE). He has worked as automation engineer, systems designer, and as a university professor. His research has been published in different journals, and presented in international conferences since 2009. His research interests are in the field of time and frequency metrology, wireless sensor networks design, automated systems, and highly sensitive chemical detectors. Currently he is involved in development of new frequency measurement systems, and highly sensitive sensors for detection of chemical compounds.

Tawanda Mushiri is a holder of BSc Mechanical Engineering (UZ), Master of Science in Manufacturing Systems and Operations Management (MSOM) (UZ) a PhD in Automation, Robotics and Artificial Intelligence (U.J) of machinery monitoring systems. He is currently a Senior Lecturer at the University of Zimbabwe teaching Machine Dynamics, Robotics, Solid Mechanics and Finite Element Analysis. He is also the coordinator of Undergraduate projects and Master of Science in Manufacturing Systems and Operations Management (MSOM). Tawanda has supervised more than 100 students' undergraduate projects and 1 Masters Student to completion. He has published 2 Academic Textbooks, 3 Chapters in a book, 14 Journals and 84 Conference Papers plus a Patents in highly accredited publishers. He has done a lot of commercial projects at the University of Zimbabwe. He is a reviewer of 4 journals highly accredited. He has been invited as a keynote speaker in workshops and seminars. Beyond work and at a personal level, Tawanda enjoys spending time with family, travelling and watching soccer.

Diana V. Nikitovich i an dispatcher of Faculty for Radio Engineering, Telecommunication and Electronic Instrument Engineering at the Vinnytsia National Technical University (VNTU), Ukraine. She graduated from the magistracy from Vinnitsa Social and Economic Institute in 2012 and its MSc and his bachelor in document management and information activities. She is the author / coauthor of about 50 publications. Research interests: neural networks, devices and logic elements for image processing, continuous matrix logic, recognition, information protection, cryptography, analog-to-digital transformations.

Vitalii Petranovskii received his PhD in Physical chemistry from Moscow Institute of Crystallography in 1988. In 1993-1994 he worked as invited scientist at National Institute of Materials and Chemical Research, Japan. Since 1995, he is working at "Centro de Nanociencias y Nanotecnología, Universidad Nacional Autónoma de México" (2006-2014 – as the Nanocatalysis department chair). His research interests include synthesis and properties of nanoparticles supported over zeolite matrices. He is a member of Mexican Academy of Sciences, International Zeolite Association, and Mendeleev Russian Chemical Society. He has published over 140 papers in peer-reviewed journals and 5 invited book chapters. Also he is co-author of monograph "Clusters and matrix isolated cluster superstructures", SPb, 1995.

Oleksandr Poliarus was born on February 18, 1950 in Gadyach town of Poltava region (Ukraine). From 1967 to 1973 he studied at the Moscow Higher Technical School named after M. E. Bauman, after which he worked as an engineer at a research institute for one year. From 1974 to 1999 he served in the Armed Forces of the USSR and Ukraine. In 1980 graduated from the Military Radio Engineering Academy of Air Defense in Kharkiv. He was in teaching positions of Academy, and since 1996 - the head of the department of antenna-feeder devices. In 1994 he defended the doctoral thesis. Since September 2007 he is the head of the Department of Metrology and Life Safety of the Kharkiv National Automobile and Highway University.

Yevhen Polyakov was born in 1985 in Pavlograd, Dnipropetrovsk region. In 2008 he graduated from Kharkiv National Automobile and Highway University and received a full higher education in the specialty “Automated Control of Technological Processes”. From 2008 to 2012, graduate student of the Department of Metrology and Life Safety of Kharkiv National Automobile and Highway University. From 2012 he works at the Kharkiv National Automobile and Highway University as Associate Professor of the Department of Metrology and Life Safety. In 2014 he defended his Ph.D. thesis on the theme “Improvement of methods of sensors dynamic errors decrease”.

Miguel Reyes-Garcia was born in Hidalgo state, Mexico, September, 29, 1989. He is a graduated mechatronics engineer of the Universidad Politécnica de Baja California (UPBC) in 2014. Currently, He is studying his Master degree with his thesis named: Theoretical method to reduce the positioning error in a scanning laser system, using an embedded digital controller and direct current motors. Working in the Optoelectronics and Automated Measurement Laboratory, Engineering Institute of the Universidad Autónoma of Baja California (UABC), Mexicali, B.C., Mexico.

Juan de Dios Sanchez Lopez received the B. Eng. (Electrical engineering) degree from the Mechanical and Electrical Department of the Technological Institute of Madero City in 1988. He received his M.Sc. and Ph.D. degrees from the CICESE Research Center in 1999 and 2009 respectively. His research interest include wireless communications, optical communications, analog-digital signal processing, electronic instrumentation and bio-optical signals.

Sergei Savin graduated from Southwest State University (SWSU) in 2011, and received PhD in 2014. From 2013 worked at the department of Mechanics, Mechatronics and Robotics at SWSU (senior researcher and docent), from 2018 is a senior research at the Innopolis University. Research interests include application of optimal control, convex optimization and computational geometry to mobile robotics. The areas of research include legged locomotion in general, bipedal walking robots, exoskeletons, in-pipe robots and multi-link mobile robots, machine learning in robotics. He is author of 4 books, more than 50 scientific papers and over 20 patents.

Cesar Sepúlveda-Valdez was born in Mexico in 1994, he obtained his degree in mechatronical engineering from the Autonomous University of Baja California in 2016. He is currently in the master and doctorate program of the UABC Engineering Institute to acquire his master degree in engineering in the applied physics department to which he joined in 2018. He participated in ISIE Vancouver 2019 Congress, obtaining a certificate for the best session presentation. He has written articles in the machine vision area which is the topic of his thesis degree.

Vera (Vira) V. Tyrsa was born on July 26, 1971. She received the B. S. and M. S. degrees in Kharkov National University of Automobiles and Highways, Kharkov, Ukraine, in 1991, 1993, respectively (Honoris Causa). She received the Ph.D. degree in Kharkov National Polytechnic University on specialty ''Electric machines, systems and networks, elements and devices of computer technics'' in 1996. She has written 1 book, 7 book chapters, and more than 50 papers. She holds one patent of Ukraine and one patent of Mexico. From 1994 till the present time, she is represented by her research works in international congresses in USA, England, Italy, Japan, Ukraine, and Mexico. In April 1996, she joined the Kharkov National University of Automobiles and Highways, where she holds the position of associated professor of Electrical Engineering Department (1998–2006). In 2006–2011, she was invited by Polytechnic University of Baja California, Mexico for professor and researcher position. Currently, she is a professor of electronic topics with the Engineering Faculty, Autonomous University of Baja California. Her current research interests include automated metrology, machine vision systems, fast electrical measurements, control systems, robot navigation and 3D laser scanners. Now she works at the Autonomous University of Baja California.

Mabel Vazquez-Briseño received her Ph.D in Computer Science from Telecom SudParis (ex INT) and Pierre et Marie Curie University, France in 2008. She received the M.Sc degree in Electronics and Telecommunications from CICESE Research Center, Mexico, in 2001. She is now researcher-professor at the Autonomous University of Baja California (UABC), where she is a member of the Telematics research group. Her research interests include computer networks, mobile computing, sensor networks and protocols.

Rosario Isidro Yocupicio Gaxiola was born in Los Mochis, Sinaloa, Mexico. He studied at the Instituto Tecnológico de Los Mochis and completed a PhD at Centro de Nanociencias y Nanotecnología of Universidad Nacional Autónoma de México (CNyN.UNAM) in 2017. Actually, he is a posdoctoral researcher at CNyN-UNAM. His research interests lie in the synthesis, analysis and applications of porous solids, particularly the study of zeolites as microporous and mesoporous systems. His research is focused in the use of microporous materials as catalysts, supports of catalysts, sorbents and opticals devices.