http://doi.org/10.35784/iapgos.907

STUDYING THE PROPERTIES OF PIXELS PERMUTATIONS BASED ON DISCRETIZED STANDARD MAP

Serhii Haliuk, Oleh Krulikovskyi, Vitalii Vlasenko
Chernivtsi National University, Department of radio engineering and information security, Chernivtsi, Ukraine

Abstract. *In this article, we described specifics of pixels permutations based on the discretized, two-dimensional Chirikov standard map. Some properties of the discretized Chirikov map can be used by an attacker to recover the original images that are studied. For images with dimensions $N \times N$ the vulnerability of permutations allows for brute force attacks, and shown is the ability of an intruder to restore the original image without setting the value of keys permutations. Presented is also~~,~~ successful cryptographic attack on the encrypted image through permutation of pixels. It is found that for images with dimension $N \times N$ the maximum number of combinations is equal to N^{N-1}. A modified Chirikov map was proposed with improved permutation properties, due to the use of two nonlinearities, that increase the keys space to $N^2!$.*

Keywords: discretized standard map, permutation of pixels, key space, precision of computing

BADANIE WŁAŚCIWOŚCI PERMUTACJI PIKSELI W OPARCIU O ZDYSKRETYZOWANĄ MAPĘ STANDARDOWĄ

Streszczenie. *W tym artykule opisana została specyfika permutacji pikseli w oparciu o zdyskretyzowaną, dwuwymiarową mapę standardową Czirikowa. Niektóre właściwości tej mapy mogą zostać użyte przez napastnika, aby odzyskać oryginalne obrazy, które są badane. Jeśli chodzi o obrazy o wymiarach $N \times N$, permutacje są podatne na agresywne ataki. Pokazana jest również możliwość odzyskania przez intruza oryginalnego obrazu bez ustawienia wartości permutacyjnych. Przedstawiony został również udany atak kryptograficzny na zaszyfrowany obraz za pomocą permutacji pikseli. Stwierdzono, że w przypadku obrazów o wymiarach $N \times N$, maksymalna liczba kombinacji jest równa N^{N-1}. Zaproponowano zmodyfikowaną mapę Czirikowa z ulepszonymi właściwościami permutacji, dzięki wprowadzeniu dwóch nieliniowości, które zwiększyły zestaw możliwych kombinacji do $N^2!$.*

Slowa kluczowe: zdyskretyzowana mapa standardowa, permutacja pikselowa, możliwe kombinacje, precyzja obliczeń

Introduction

Over the last two decades the application of deterministic chaos for information security became an active field of research [2, 6, 8]. Among chaos–based cryptography algorithms, a significant part is designed for image encryption. The most commonly used design is cipher with two mean stages: pixels permutation and diffusion which can be repeated several times [5]. Permutations of pixels are needed to break relations between adjacent pixels and prevent correlation attacks. The goal of diffusion is to transform the uneven distribution of color pixels into uniform, thereby concealing the statistical properties of the original image. Typically for pixels permutations, used are discretized versions of Standard, Baker or Cat map [5] or their modifications. For the diffusion step typically is used PRNG based on one, two or multi-dimensional maps. Along with the new encryption algorithms based on deterministic chaos, the works dedicated to cryptanalysis have been presented [1, 3, 10, 12]. In [10] was proposed one of the earliest chaotic image encryption algorithms which uses discretized version of Chirikov standard map for pixels permutations [4]. It was later shown in [9] that in this map, the first pixel does not change its position after any number of permutation cycles. To eliminate this vulnerability, it was suggested to use mechanism, which essence is to shift first pixel into any position in the image. Also, there were given [9] recommendations for minimum size images for encryption and minimum number of permutation cycles.

In this paper we focus on cryptographic security of pixels permutations based on the discretized two-dimensional Chirikov standard map considering its geometric properties. We explore the resistance of permutations to brute force attack and we find property that greatly reduces the key space of permutations compared to the known assessment of key space made in [9]. To eliminate the identified vulnerabilities, we propose to modify the discretized standard map by entering additional nonlinearity. Also, we estimate the key space of permutations for double-precision arithmetic and we show that the key space is very small compared to the theoretically possible maximum. Please note that we consider changes as only one stage of the chaotic algorithms.

In section 1 specifics of pixels permutations based on discretized standard map and power of key space are described. In section 2 shown is a cryptographic attack on the encrypted image by permutation of pixels and reduced key space.

1. Specifics of permutations based on discretized standard map

As noted above, in [5] was introduced discretized standard map for pixels permutations, that is given by the following iterative equations:

$$\begin{aligned} x_{i+1} &= (x_i + \mathrm{y}_i)\bmod N \\ y_{i+1} &= \left(y_i + K\sin\left(\frac{x_{i+1}N}{2\pi}\right)\right)\bmod N \end{aligned} \tag{1}$$

where x_i and y_i are coordinates, $i \in [0;\ N-1]$, K – a control parameter which is a positive integer, N is the number of pixels in width or height of the original image. As we can see, (1) is suitable only for bitmaps with $N \times N$ dimensions.

Properties of the discretized map (1) are not as perfect as the original [3], but it can be implemented in the integer x_i and y_i values of intervals, which reduce the computational complexity and are more convenient to encryption data applications [5].

The procedure of one cycle of pixels permutation for bitmap with dimension $N \times N$ in RGB format is as follows:

a) For each pixel x_i and y_i there is a calculation of (1) made to form its new coordinates x_{i+1} and y_{i+1} in encrypted image.
b) Coordinates x_{i+1} and y_{i+1} in encrypted image record pixel color values (RGB) of the original image.
c) These operations (1 and 2) are carried out sequentially for each pixel.

Let's analyze features of pixels permutations based on map (1), considering its geometric properties for bitmaps with $N \times N$ dimensions.

1.1. Features of permutations

Any picture with dimension $N \times N$ has $2N-1$ diagonals (see Fig. 1). The first and the last diagonals are composed of one element. Number of elements in the diagonal varies from 1 to N. The first element of the diagonal is the pixel with the lowest x_i. Permutations based on discretized standard map have following properties:

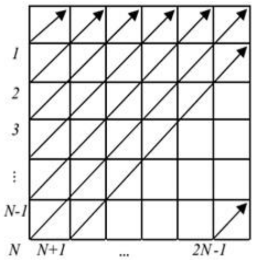

Fig. 1. Diagonals of any image with N × N dimensions

a) The first pixel in coordinates $(0;\ 0)$ does not change its position at any number of permutation cycles, it can be used by cryptanalyst to crack the encrypted images [9]. When $x_i = 0$, $y_i = 0$ we use (1) and calculate that $x_{i+1} = 0$, $y_{i+1} = 0$.

b) Each column after one cycle of permutation consists of two diagonals with numbers n and $N + n$, $n \in [2; N-1]$ except the diagonal *N*. It is because the diagonal *N* consists of *N* elements. This property of the permutation is shown in Fig. 2b, where each column of the image after one permutation cycle contains pixels with two colors. Each square is a pixel in an image sized 10×10 (see Fig. 2a). All pixels in the diagonal after the permutation will always be placed in one column. Consistently placed diagonal elements (see Fig. 2b) for which the original image:

$$(x_i + y_i) \bmod N = C = const \tag{2}$$

where $C \in 0 \ldots N-1$ corresponding column element of the encrypted image (Fig. 2*b*), according to (1) $x_{i+1} = C = const$. When the equation for calculation of coordinate line y_{i+1} can be written as:

$$y_{i+1} = (y_i + KC) \bmod N \tag{3}$$

where

$$C_1 = \sin\left(\frac{x_{i+1} N}{2\pi}\right) = \sin\left(\frac{CN}{2\pi}\right) = const$$

it means that after permutation, pixels coordinates which satisfy (2) are placed in one column consecutively, but are shifted in relation to the initial position, which depends on the parameters *K* and *C*$_1$.

c) Pixels for which coordinates the equation is true:

$$x_{i+1} = (x_i + y_i) \bmod N = 0 \tag{4}$$

always after the permutation will be in the first column. By doing so, the coordinates of the rows will not change because of (1). Let's take into account (4) $x_{i+1} = 0$, $y_{i+1} = y_i$ (Fig. 2b).

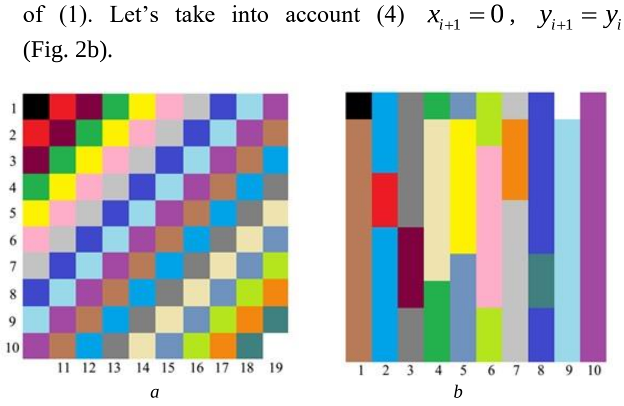

Fig. 2. Image (10×10) – original (a), after one cycle of permutation by K = 123 (b)

Each pixel diagonal can be uniquely identified by a column number that forms this diagonal. Using properties (2–4), a cryptanalyst can try to reproduce the original image by moving the pixels in columns to the place of pixels in diagonals.

1.2. Analysis of key space

The row number where a pixel may be moved after the permutation by $x_i + y_i \neq N$, $x_i + y_i \neq 0$ depends on the value of the parameter *K* and term KC_1 in (3). Thus, for pixels that are in the first column, their position in the original image is uniquely known. Two consecutive columns contain the pixels of two neighboring diagonals.

Therefore, there are possible only *N* variants to shift elements of the second column in relation to the first. Given the fact that the pixels of adjacent diagonals slightly differ among themselves, shift between them can be determined by the maximum of the correlation function.

Given the map properties (2) and (3), the number of combinations of a brute force attack that is needed to restore the original image after one permutation cycle equals to N^{N-1} which is much less than $N^2!$ as was considered in the evaluated key space for this map in [9, 12].

1.3. Subkeys properties

Let's consider another property of the standard map (1) that can be used to break pixels permutations. Let's assume that:

$$K_i = K \sin\left(\frac{x_{i+1} N}{2\pi}\right).$$

Then, if $x_{i+1} = const$ then number K_i is a key of permutation in the diagonal in a column. In total, there are *N* subkeys, while some of them may be the same.

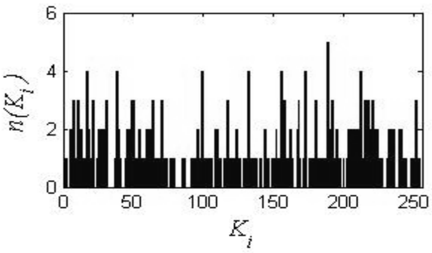

Fig. 3. Histogram of subkeys distribution for image sized 256×256 pixels at K = 1000003

From Fig. 3 one can understand that each subkey was found a limited number of times $m \leq N$, which reduces the key space of permutation in comparison with N^{N-1}. Setting a limit on the number of appearances of permutation subkeys is possible to estimate the key space for a brute force attack as the number of permutations of *N* different elements of *N*, provided that each element of it occurred fewer than *m* times [11]:

$$K = \sum_{\substack{n_1+n_2+\ldots+n_N=N \\ n_i \leq m,\ i=1\ldots N}} \frac{N!}{n_1!n_2!\ldots n_N!} = \\ = \sum_{r_1=N-m}^{N} \sum_{r_2=r_1-m}^{r_1} \sum_{r_3=r_2-m}^{r_2} \ldots \sum_{r_k=r_{k-1}-m}^{r_{k-1}} C_N^{r_1} C_{r_1}^{r_2} C_{r_2}^{r_3} \ldots C_{r_{k-1}}^{r_1} \tag{5}$$

However, these properties of subkeys can be used by an attacker to select the most likely key at the beginning of attacks, and thus increase their chances of success. Reducing key space of (1) through dependence between the *N* and *m* according to (5) is shown in Table 1.

Table 1. Reducing the key space, %

N	*m* = 3	*m* = 5	*m* = 7
64	72.6	3.2	0.046
128	93.1	6.81	0.11
256	99.6	13.7	0.11

In Tab. 1 it can be seen that at $m \leq 5$ the key space is greatly reduced. For $m \geq 5$ the key space is weakly reduced.

1.4. The effect of limiting precision of calculations

As it is known, a set of different states of chaotic system is defined by precision of calculations [9] and increases with increased precision. For permutations using (1), this effect is also true. We estimate the key space using system (1), provided that the parameter K is a positive integer. In calculations of double precision, the mantissa is 52 bits. The range of integers that can be accurately represented in the form of double precision is $1...2^{53}$ [14]. Given the possible steps 2, the number of different positive integer values of K is $2^{61.9}$. In [9] it is recommended to use for permutations an image which size is of at least $N \geq 128$. Thus we can say that the most appropriate break permutations based on the standard map are the brute force of a possible key values, because:

$$N^{N-1} = 128^{127} \cong 2^{894.6} \gg 2^{61.9} \qquad (6)$$

The real key space for modern computing systems is small compared to theoretically possible. Please note that we have established a number of options of the brute force in various possible methods of attack, without considering time complexity of their implementation.

2. Cryptographic attack based on the correlation between adjacent pixels

Considering the facts that there are possible only N variants of shifting elements of the second column in relation to the first and that pixels in adjacent diagonals differ slightly from each other, we can find a shift between pixels of adjacent columns by the maximum of the correlation function.

2.1. Cryptographic attack based on the correlation between adjacent pixels

We organized our cryptographic attack on permutations based on (1) as follows:

a) For two adjacent columns we calculated the value of cross-correlation function:

$$c_k = \sum_{k=0}^{N-1} \left(x_{i,n} - m_i\right)\left(x_{i+1,n+k} - m_{i+1}\right) \qquad (7)$$

where $m_i = \dfrac{1}{N} \sum_{N=0}^{N-1} x_{i,n}$.

b) Defined k for which

$$c_k = \max\left\{c_0, c_1, ..., c_{n-1}\right\} \qquad (8)$$

c) Column $i+1$ shifted to the K positions down, i.e.

$$x_{i+1,n} = x_{i+1,n+K} \bmod N \qquad (9)$$

d) Repeated steps a, b and c for remaining columns in the image. The algorithm has been tested on the image in Fig. 4.

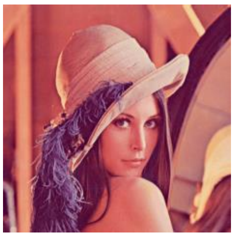

Fig. 4. Original test image

After the first and second permutation cycles, the original image is successfully restored (see Fig. 5). However, there is a slight distortion. After three permutation cycles, the correlation between adjacent pixels is lost and the restoration of the original image by this method is impossible. Thus, considering the correlation, image properties can be broken by 2 cycles of permutations.

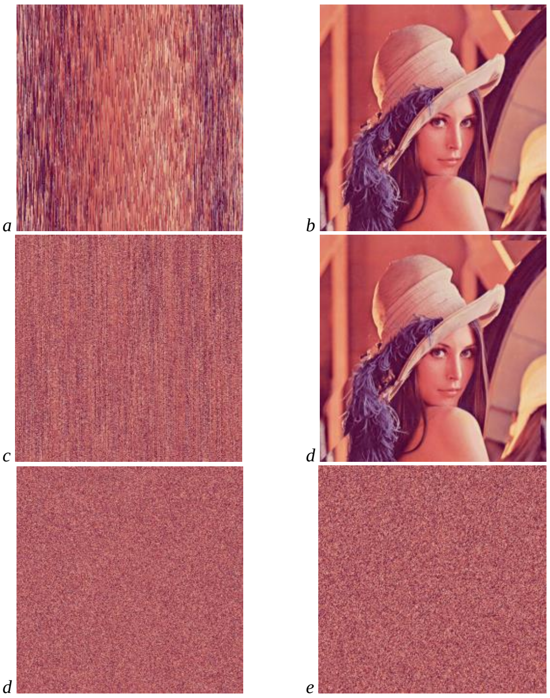

Fig. 5 a; c; e – encrypted test image after one, two and three cycles of permutation, respectively; b; d; f – recovered image

2.2. Modified standard map with a maximum key space for permutations

In order to get the maximum size of the key space of permutation for the system (1), it is necessary to introduce non-linearity in the variable x_{i+1}. Our proposed map in the discretized form is described by the following recurrent system of equations:

$$\begin{cases} x_{i+1} = \left(x_i + K_x \sin\left(\dfrac{y_i N}{2\pi}\right)\right) \bmod N \\ y_{i+1} = \left(y_i + K_y \sin\left(\dfrac{x_{i+1} N}{2\pi}\right)\right) \bmod N \end{cases} \qquad (10)$$

where K_x, K_y – parameters (keys). Jacobian system (10):

$$D = \begin{vmatrix} \dfrac{\partial x}{\partial x} & \dfrac{\partial x}{\partial y} \\ \dfrac{\partial y}{\partial x} & \dfrac{\partial y}{\partial y} \end{vmatrix} = \begin{vmatrix} 1 & \dfrac{K_x N}{2\pi} \cos\left(\dfrac{yN}{2\pi}\right) \\ \dfrac{K_y N}{2\pi} a & 1 + \dfrac{K_y K_x N^2}{(2\pi)^2} a \cos\left(\dfrac{yN}{2\pi}\right) \end{vmatrix} = 1 \qquad (11)$$

where $a = \cos\left(\left(x + K_x \sin\left(\dfrac{yN}{2\pi}\right)\right) N / 2\pi\right)$, i.e., map saves the area and is potentially useful for permutations in encryption algorithms. The drawback of the map (10) is the need to have two sinus functions computed. Considering that value of trigonometric functions in digital means are calculated using the Taylor series of desired functions, the number of mathematical operations in system (1) is less complex in comparison to (10).

Let us consider the effectiveness of permutations based on (10). The encrypted image after one cycle of permutations is shown in Fig. 6.

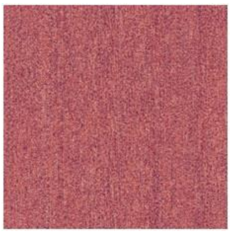

Fig. 6. Permutation of pixels of a test image using (10)

In the encrypted image contours are not observed and pixels of different colors are uniformly distributed within its size. To evaluate the similarity of two images, we use the correlation coefficient [7]. Correlation coefficient close to zero means that two images are independent and use the map characterized by good mixing properties.

The calculation results for different number of permutation cycles using (1) and (10) are presented in the Table 2.

Table 2. Correlation of image pixels depending on the number of cycles n in permutations N = 512, K = K_x = K_y = 10000

n	Correlation of pixels	Standard map	
		with one nonlinearity (1)	with two nonlinearity (10)
0	horizontal	0.9753	0.9753
	vertical	0.9853	0.9853
1	horizontal	0.0972	-0.0011
	vertical	0.9699	0.0375
2	horizontal	-0.0040	0.00006
	vertical	0.0969	0.00063
3	horizontal	-0.00075	-0.0015
	vertical	-0.0070	-0.0034
4	horizontal	0.0011	-0.0026
	vertical	-0.00025	-0.0029

Systems (1) and (10) are explored with the parameters $K = K_x = K_y = 10000$ For the original image (Fig. 4) the correlation coefficient between the adjacent pixels in columns and rows equals to 0.9759 and 0.9857 respectively. One cycle of permutations with a standard map does not lead to uniform dissemination of pixels (Fig. 5 a), because preserved was a strong correlation between pixels in columns.

From Tab. 2 it can be deduced that system (10) compared to (1) has better correlation properties. Efficiency of permutations with (1) and (10) is seen in Fig 7.

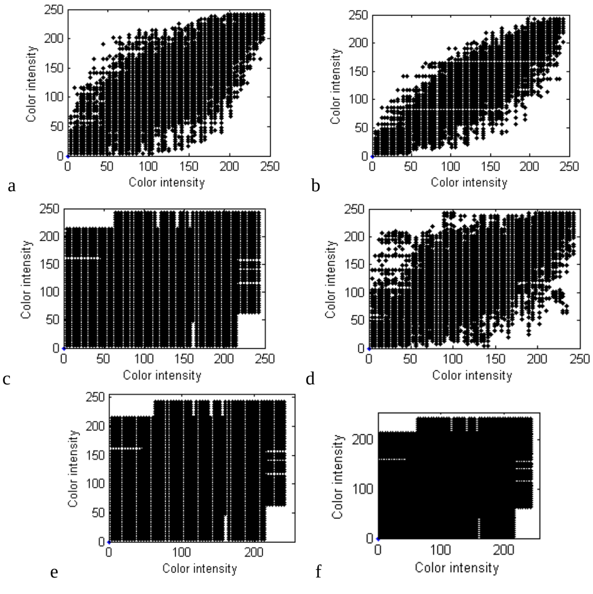

Fig. 7. The relationship between the adjacent pixels: a; b – in the horizontal and vertical for test image (Fig. 4); c; d – after one cycle of permutations using the map (1); e; f – after one cycle of permutations using the map (10)

For one cycle permutations performed by system (1), pixels are grouped along the diagonal (see Fig. 7 c, d). After one cycle permutations (10), relationships between adjacent pixels in rows (Fig. 7 e) and columns (Fig. 7 f) have the form of a square, which means no statistical relationship between them.

3. Conclusion

We analyzed permutations of pixels based on discretized Chirikov standard map considering its geometric features. We discovered specific properties of a map that can be used by an attacker to recover the original image. It is shown that the permutations are much weaker before brute force attacks, and it is possible to recover the original image without setting the key value (key) permutations. For images with dimension $N \times N$ the number of combinations is N^{N-1} for one permutation cycle instead of $N^2!$ as was previously thought. In order to get the maximum size of key space of permutation for the discretized standard map, we proposed to introduce additional nonlinearity. Please note that the evaluation of key space of permutations is received on the condition that calculations are made with absolute precision.

References

[1] Alvarez, G., Li, S. J.: Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. Inter. Journal of Bif. and Chaos 16(8)/2006, 2129–2151.

[2] Argyris A., Syvridis D., Larger L., Annovazzi-Lodi V., Colet P., Fischer I., García-Ojalvo J., Mirasso C.R., Pesquera L., Shore K.A.: Chaos-based communications at high bit rates using commercial fibre-optic links. Nature 438(7066)/2005, 343–346.

[3] Arroyo D., Alvarez G., Fernandez V.: A basic framework for the cryptanalysis of digital chaos-based cryptography. Proc. of the 6th International Multi-Conference on Systems, Signals and Devices, Djerba 2009, 58–63.

[4] Chirikov B. V.: Research concerning the theory of nonlinear resonance and stochasticity Preprint 267, Institute of Nuclear Physics, Novosibirsk, 1969, (Engl. Trans., CERN Trans. 1971, 71–40).

[5] Fridrich J.: Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. Inter. Journal of Bif. and Chaos 8(6)/1998, 1259–284.

[6] Hussain I., Shah T.: Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. Nonlinear Dynamics 74/2013, 869–904.

[7] Jolfaei A., Mirghadri A.: An image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology 19(2)/2010, 117–125.

[8] Kocarev L., Lian S. (Eds.): Chaos-Based Cryptography Theory, Algorithms and Applications. Springer-Verlag Berlin Heidelberg, 2011.

[9] Lian S. G., Sun J., Wang Z.: A block cipher based on a suitable use of chaotic standard map. Chaos, Solitons and Fractals 26(1)/2005, 117–29.

[10] Lian S., Sun J., Wang Z.: Security analysis of a chaos-based image encryption algorithm. Phisyca A 351(2)/2005, 645–661.

[11] National Institute of Standards and Technology (May 11, 2010). NIST Digital Library of Mathematical Functions. Section 26.4. Retrieved August 30, 2010.

[12] Solak, E., Cokal, C., Yildiz, O.T., Biyikoglu, T.: Cryptanalysis of fridrich's chaotic image encryption. Int. J. Bifurcation Chaos 20(5), 1405–1413.

[13] von Bremen H. F., Udwadia F. E., Proskurowski W.: An efficient QR based method for the computation of Lyapunov exponents. Physica D 101/1997, 1–16.

[14] Warren H. S. .: Hacker's Delight. Addison-Wesley Professional. 2012.

[15] Yuan G., Yorke J. A.: Collapsing of chaos in one dimensional maps. Physica D: Nonlinear Phenomena 136/2000, 18–30.

Ph.D. Serhii Haliuk
e-mail: s.haliuk@chnu.edu.ua

Assistant of professor at Radio Engineering and Information Security Department of Yuriy Fedkovych Chernivtsi National University. His research field covers the development of the different components of hidden communication systems. Author of more than 20 publications.

http://orcid.org/0000-0003-3836-2675

Ph.D. Oleh Krulikovskyi
e-mail: o.krulikovskyi@chnu.edu.ua

Assistant of professor at Radio Engineering and Information Security Department of Yuriy Fedkovych Chernivtsi National University. His research field covers digital signal processing, FPGA and cryptography. Author of more than 20 publications.

http://orcid.org/0000-0001-5995-6857

Vitalii Vlasenko
e-mail: vetalvlasenko98@gmail.com

A graduate student. Winner of Ukrainian national student contests on the topic of cybersecurity in 2017 and 2019.

http://orcid.org/0000-0002-9085-5787

otrzymano/received: 15.11.2019 *przyjęto do druku/accepted: 15.02.2020*