Journal of Theoretical and Applied Information Technology
15th December 2022. Vol.100. No 23
© 2022 Little Lion Scientific
ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMAGE ENCRYPTION METHODOLOGY BASED ON CELLULAR AUTOMATA

NASHAT AL BDOUR

Department of Communications, Electronics, and Computer Engineering, College of Engineering, Tafila Technical University, Tafila 66110, Jordan

*Correspondence: *dr.nashat82@yahoo.com*

ABSTRACT

The paper considers a methodology for encrypting color images, in which the key is the initial state of an elementary cellular automata for the implementation of evolution based on a given rule. The research task is to improve the reliability of encryption of color images based on the encryption of the bit layers that make up the image. To solve this problem, the methodology of forming the evolution of an elementary cellular automata was used, which is a finite bit key array for each bit layer of the image. The encryption and decryption key consists of subkeys, the number of which corresponds to the number of bits that encode the color of each pixel. Each subkey consists of the initial states of an elementary cellular automata and the rules that shape its evolution. For the formation of each bit key array, different initial conditions and different Wolfram rules for elementary cellular automata were used. The size of each formed key bit array is equal to the size of the corresponding bit layer of the color image. Encryption is performed by using the XOR function for the generated key bit array and bit-slice of the image. As a result of the experiments, it was established that it is necessary to use different rules that form different geometric shapes in evolution. It is also established that it is necessary to form a key bit array for each bit layer starting not from the first lines of evolution. It was found that the quality of encryption of a color image is most influenced by the three most significant bits of each byte of the pixel code, encoding the corresponding red, blue and green colors.
Keywords:. *Encryption, Image, Cellular Automata, Evolution, Wolfram's Rule, Key Bit Array, Bit Layer.*

1. INTRODUCTION

In modern computer networks, images represented by various digital formats are transmitted as information. This is due to the high performance capabilities of such networks. Among all the transferred images, a significant number of them carry confidential or classified information. Such images and the information embedded in them, as a rule, are transmitted in encrypted form [1-5] or as containers when using steganographic information security methods. Secret images are transmitted either in a modified form (the same graphic format) or in another electronic format (another graphic format, text format, etc.). Nowadays, image encryption is increasingly used. The encryption method is implemented by simply encrypting the bytes that make up the electronic structure of the image. This method is especially effective in cases where there is a need to hide part of the image (for example, a person's face, license plate, various maps, etc.). Today, there are already a large number of image encryption methods that use various original approaches [1-6]. However, in many situations, such methods do not always give the desired result in terms of speed and complexity of encryption, as well as high resistance to attacks on the cipher.

2. PROBLEM STATEMENT

To encrypt an image, one of the main tasks is to present the encrypted image without the content of statistical relations with the original image. The most commonly used streaming encryption is based on representing the initial image as a sequence of bits and mixing these bits with bits generated by a pseudo-random number generator (PRNG). The effectiveness of this method is determined by the quality of the PRNG. In fact, a stream encryption method is used. There are also methods that use different image transformation operations, however these methods use additional algorithms and hardware to encrypt.

This work solves the problem of developing an image encryption method based on cellular automata (CA) technologies without using PRNG and other additional methods and means. The problem is solved by converting individual bit slices of a color image and transforming those using CA

technologies, which are aimed at generating an encryption key.

3. RELATIVE WORKS

The simplest and most popular method of encrypting images is a method based on the use of the electronic structure of an image, which consists of many bytes that encode its color and brightness characteristics. The characteristics of each pixel of the bitmap are represented by a binary code. A bit sequence is formed from these codes, which is further encrypted. The generated bit sequence is encrypted using a key gamut formed by the PRNG [1, 7. 8]. These methods also take into account the number of bits that form the code of each pixel in the image. Methods based on scrambling rows and columns of an image matrix are also used, the results of which are combined by the XOR function [1, 7, 8]. Implementation of this method can lead to confusion when choosing rows and columns, which leads to false results when decrypting.

There are image encryption methods that use various image transformations. Such transformations include: Fourier transform [9-11] and Wavelet transform [12]. The main disadvantage of such methods is distortion during digitalization of color images.

Many image encryption methods use systems that use chaos theory [8, 13-16]. These methods use a limited set of different general operations, which makes them vulnerable to external cipher attacks. In addition, chaos systems use complex algorithms that require large computational resources to encrypt images.

Since images are represented by arrays of pixels, 2D and 3D maps of different structures are used to encrypt them [17-21]. At the same time, the use of initially prepared forms can lead to their selection by an attacker, which leads to the vulnerability of the method to attacks.

There are also encryption methods that use various original approaches such as: Rubik's cube transformation [22], elliptic curves [23, 24], based on the calculation of DNA [25-27], etc.

In addition, there are methods based on the use of various architectures, such as artificial neural networks [28], CA [1, 29-31] and other architectures.

All described methods are investigated in terms of resistance to external attacks. However, the known methods cannot claim high reliability and resistance to hacking. In addition, the more reliable methods described require complex calculations, which reduces the performance of the methods. In this regard, the developers are looking for simpler and more reliable encryption methods without the use of additional computing facilities.

In paper [7], research was carried out to find bits in the code of each pixel, which would provide reliable encryption of the image. The RGB - images are used, in which each color was represented by one byte in the 24-bit code of each pixel of the image. As a result of the study, it was found that for effective image encryption, it is enough to encrypt the three most significant bits of each color byte in the code of each pixel. For such encryption, the PRNGs described in [32, 33] were used. In this case, the method uses additional means for encryption, on which the final result depends.

Any bitmap image can be represented as a three-dimensional bitmap image or a set of two-dimensional bitmaps images parallel to each other. Each two-dimensional array can represent a binary image. Real image pixels use depth coding (pixel color coding). In a two-dimensional bit array, each pixel can be defined as a cell of a two-dimensional CA (TDKA). The number of TDCAs used to form the image is determined by the width of the binary code of each cell. If a 24-bit color code is used (one byte encodes one color), then the number of TDCAs is 24.

Bits of all pixel codes with the same bit weight form each TDCA. For example, the first TDCA is formed from the least significant (zero) bits of the codes of all image pixels, the second TDCA is formed from the bits of the pixel codes that correspond to the bit weight equal to 1. In fig. 1 shows the initial real image with a size of 20 × 20, as well as the decimal and binary codes of each pixel. In addition, in Fig. 1 shows all TDCAs involved in the formation of the initial image.

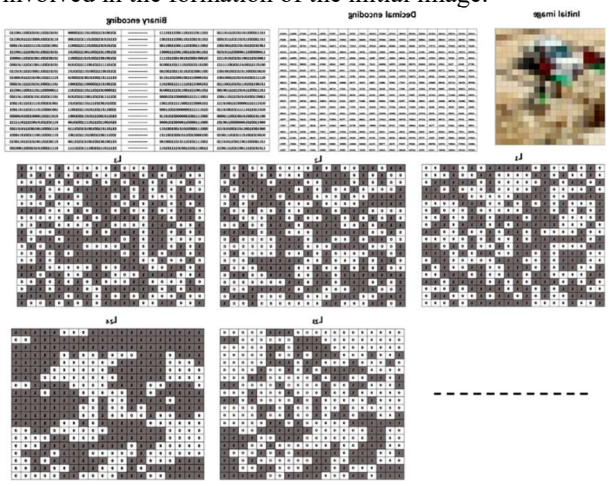

Fig. 1. An Example Of Dividing Of A Color Image Into 24 Tdcas

Each TDCA is also defined as a binary image slice. Depending on the coding method, TDCA images have a different structure. In complex color images, all TDCA differ from each other in the state of the cells.

Thus, the image can be represented both by one-dimensional codes for each pixel and by two-dimensional bitmaps, which are determined by the states of the cells.

4. IMAGE ENCRYPTION METHODOLOGY BASED ON ELEMENTARY CELLULAR AUTOMATA TECHNOLOGIES

The previous section shows the structure of a color raster image, the main elements of which are cellular binary layers. These layers can be considered as CA if their states are changed according to the selected rules [34]. Various rules for two-dimensional arrays can shift of image, select individual cells and transform their states, which allows you to change the states of all bit layers at any time. For such CA, the number of rules increases significantly.

To encrypt color images, a concept is used that contains the following main statements.

1. Encryption is carried out for each binary layer L_i of the image separately.
2. To encrypt each binary layer, a separate encryption key K_{encr_i} is used, which is the connection of the general encryption key K_{encr} of the entire binary image. Moreover, all subkeys should not have a large number of symbols.
3. Each subkey for encryption K_{encr_i} and decryption K_{decr_i} is a sequence of numbers that forms a final bit key array of image dimensions
   $K_{bit\_i} = f(K_{\text{encr\_i}}) = B_i$,
   were $f(\ldots)$ - function to convert a sequence of bits or decimal numbers to a two-dimensional bit array B_i.
4. Based on the generated key bit array B_i, the encrypted i-th bit layer is formed using the encryption function φ_s
   $I_{S,i} = \varphi_s(B_i, L_i)$.
5. The encryption and decryption system is symmetric
   $$K_{\text{encr}} = K_{decr}$$

The method for forming a binary array B_i is as follows.

The methodology of formation of evolution of elementary cellular automata (ECA), described by Stephen Wolfram, is used [35]. ECA is a line of cells, each of which is associated with the nearest neighboring cells that form a neighborhood. Each ECA cell can be in the state of logical "1" or logical "0".

The evolution of ECA is formed by a sequence of ECA (usually vertically), each of which changed its state at a given time step. In this case, the state of each subsequent ECA (at the next time step) is formed on the basis of the states of the cells of the previous ECA (at the previous time step). If an ECA consists of N cells, and evolution contains M ECA, then the formed two-dimensional bit array has a dimension of M × N cells. In this case, the evolution of ECA can be considered as a TDCA.

Each ECA changes its states at the next time step of evolution in accordance with the rules that have been studied and described in the works of S. Wolfram [35] and in many other works [36, 37]. Wolfram's rules are implemented based on coding from the states of the cell itself and from the cells that form the neighborhood. For example, rule 150_{10} is defined by code 10010110_2, and the formation of a new state is determined by Table 1. In this case, a classical neighborhood consisting of two cells is used. The formation of a new state at the next time step also involves its own cell, the state of which is assessed at the corresponding time step.

Table 1. Formation of new ECA states according to rule 150

Cell states at time t $a_{i-1}(t)$, $a_i(t)$, $a_{i+1}(t)$	1 1 1	1 1 0	1 0 1	1 0 0	0 1 1	0 1 0	0 0 1	0 0 0
Cell states at time t+1 $a_{i-1}(t+1)$, $a_i(t+1)$, $a_{i+1}(t+1)$	1	0	0	1	0	1	1	0

Thus, the binary key array is formed on the basis of the initial states of the cells of the first ECA and the corresponding Wolfram rule. Subkey is a bit array of cells of the initial ECA and Wolfram's rule. For each bit layer L_i of the image, different bit initial arrays and different Wolfram rules are used. In [38], various rules are considered for the formation of random states in the evolution of these rules. This and other works confirmed the effective use of separate rules for the formation of pseudo-random bit sequences.

Examples of ECA evolutions for rules 30, 90 and 111 in Fig. 2 are shown. The same initial cell states are used for all rules. The resulting bit arrays can act as subkeys for encrypting a given bit slice of a color image.

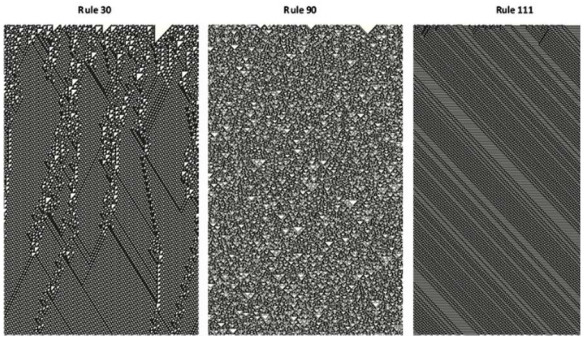

Fig. 2. Evolutions of ECA for rules 30, 90 and 111 with the same initial conditions

The initial states for the displayed (Fig. 1) evolutions in Fig. 3 are shown. In the image of evolutions, the initial states are the first line of the image.

Fig. 3. The initial states for the evolutions shown in Fig. 2.

Each subkey can be represented by a bit sequence and a rule or by a set of rules that are implemented in evolution. Each subsequent step in the evolution of ECA can be represented by a new rule. In this case, the resulting evolution will differ from the known classical ECA evolutions.

The final encrypted array of the new image is obtained using a bitwise XOR operation for each bit layer and given key bitmap image.

$E_i = B_i \oplus L_i$.

If you use a bit sequence, then you must use a special medium for storing subkeys. Therefore, this bit sequence is split into bytes and each byte is represented by a decimal number from 0 to 256. This conversion shortens the length of the subkey.

This paper discusses the methodology for applying one rule for each subkey, but different initial states of the cells of each ECA.

5. EXPERIMENTAL FINDING THE OPTIMAL KEY BIT ARRAY

Researches have shown that using the same Wolfram rule and the same initial states for each bitmap does not provide high encryption quality. It is possible to define the rules and contours of the image. To find the optimal bit key arrays, an experiment was carried out, the methodology of which is as follows.

At the first stage of the experiment, the same initial conditions and one Wolfram rule were used to encrypt all 24 bit layers $L_1,\ldots,L_{24}$. The results of such an experiment for rules 30, 90, and 111 in Fig. 4 are shown.

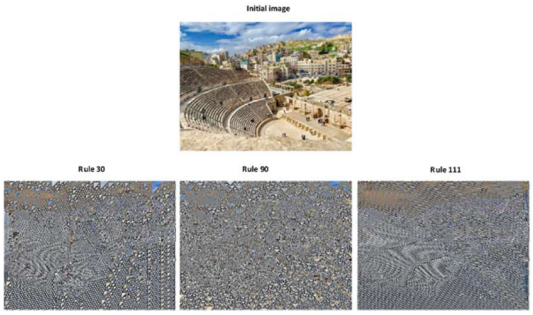

Fig. 4. Examples of images encrypted using rules 30, 90 and 111 with the same initial states of ECA cells

Analysis of Figure 4 showed that this approach generally preserves the structure of the initial image. Visual analysis also allows you to determine the rule that is used for encryption. This approach does not allow the image to be encrypted properly. For high efficiency of color image encryption, it is necessary to use different initial settings of ECA cells and rules for encrypting each bit layer.

At the second stage of the experiment, the same bit sequences and different rules were used for different layers of a color image. In fig. 5 shows an example of an encrypted image using rules 30, 45, 90, 105, 111, 150 and 180 with the same bit sequences for each L_i layer of the color image.

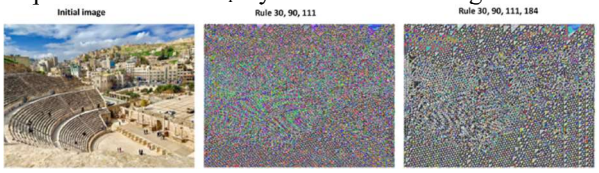

Fig. 5. Examples Of Image Encryption With The Same Bit Key Sequences And Different Rules

Using different rules with the same bit key sequences does not provide high quality encryption. The traces of the original image outlines on the encrypted image, as well as traces the geometric structures that are characterized by the use of a certain Wolfram rule. The second stage of the experiment showed that the main influence on the quality of encryption of a color image is exerted by the three most significant bits of each byte of the pixel, encoding blue, red and green colors, respectively.

In the third step, different key bit sequences and different Wolfram rules were used to form each subkey. Examples of color image encryption with different key bit sequences and different rules in Fig. 6 are shown.

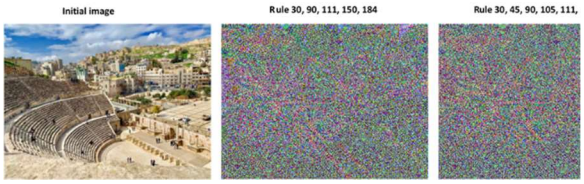

Fig. 6. Examples Of Image Encryption With Different Key Bit Sequences And Different Rules For ECA

Since the evolutions of the ECA for many rules contain the same geometric shapes (for example, triangles), the initial definition of the rule leads to significant difficulties. In addition, under the known rule (for an image with dimension M × N), 2^M variants of enumeration of initial states are required. For example, if M = 100 (100 pixels horizontally), then it is necessary to consider 1267650600228229401496703205376 combinations. In addition, since real images are much larger than 100 pixels, the number of possible combinations is very large. In this case, it is necessary to take into account the presence of a large number of bit layers of the image, as well as the use of different rules.

The third stage showed high quality encryption. However, it is possible to define encryption rules for the first few lines of the array. Therefore, an approach was used based on the analysis of geometric shapes formed by the used rules. As a result of the analysis, it was decided to use the generated key bit array shifted by the first 20 lines of the ECA evolution. The result of this encryption in Fig. 7 is shown.

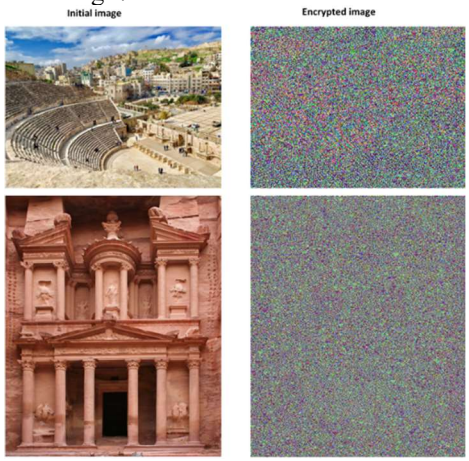

Fig. 7. Examples Of Encryption Of Color Images With Bit Arrays Starting With 21 Lines Of ECA Evolution

To encrypt the second (bottom) image, an additional rule 51 was used. Analysis of Figure 6 shows high quality color image encryption. In this case, you can use key bit arrays starting from any line of the evolution of the ECA. It is also recommended to use the rules of shaping evolution with different geometric shapes. It is also a recommendation to use evolution formed by using different rules at different time steps of evolution.

6. CONCLUSION

The paper considers the process of encrypting color images based on the evolution of elementary cellular automata. A methodology for the formation of a key bit array for encrypting bit layers of a color image has been developed. A methodology for conducting an experiment to find the optimal key bit array was developed and described, and recommendations for encrypting color images based on the theory of elementary cellular automata were formulated. As a result of experimental research, the bit layers (6, 7, 8, 14, 15, 16, 22, 23, 24) have been identified that most of all affect the encryption result. To obtain high quality encryption, it is recommended to use different Wolfram rules for each influencing bit layer of the image. In this case, the rules used should in their evolutions form different two-dimensional geometric shapes. The experiment also showed that the bit key array should not contain the first lines of evolution.

In further studies, for the formation of key bit arrays, the author plans to use various forms of neighborhoods, as well as to use elementary cellular automata with different paradigms of functioning.

REFERENCES

[1] Stepan Bilan, Andrii Demash. High performance encryption tools of visual information based on cellular automata. - Information Technology and Security. - 2016. - Vol. 4, № 1(6). - C. 62-75.

[2] Sung Won Kang, Un Sook Choi & Sung Jin Cho. Fast image encryption algorithm based on (n, m, k)-PCMLCA. *Multimedia Tools and Applications* (2021).

[3] Essaid M, Akharraz I, Saaidi A, Mouhib A (2018) A New Image Encryption Scheme Based on Confusion-Diffusion Using an Enhanced Skew Tent Map. Procedia Comp Sci 127:539–548.

[4] Ghadirl HM, Nodehi A, Enayatifar R (2019) An overview of encryption algorithms in color images. Signal Process 164:163–185

[5] Hasheminejad A, Rostami MJ (2019) A novel bit level multiphase algorithm for image

encryption based on PWLCM chaotic map. Optik 184:205–213. https://doi.org/10.1016/j.ijleo.2019.03.065

[6] Huang L, Cai S, Xiong X, Xiao M (2019) On symmetric color image encryption system with permutation-diffusion simultaneous operation. Opt Laser Eng 115:7–20. https://doi.org/10.1016/j.optlaseng.2018.11.015

[7] Optimal steganographic protection method based on image encryption (статья № 7).

[8] Lazaros Moysis, Aleksandra Tutueva, Christos Volos and Denis Butusov. A Chaos Based Pseudo-Random Bit Generator Using Multiple Digits Comparison.- CHAOS Theory and Applications. (2020). – V.2, N2, P. 58-68

[9] Juan M. Vilardy, Jorge E. Calderon, Cesar O. Torres, Lorenzo. Mattos, "Digital Images Phase Encryption using Fractional Fourier Transform", CERMA conference, Pages: 15–18, 2006.

[10] H Yoshimura, R Iwai," New encryption method of 2D image by use of the fractional Fourier transform", IEEE Conference on Signal Processing, Pages: 2182 – 2184, 2008

[11] L. Finkelstein, J. Kosmach and J. Smolinske. Method and apparatus for providing cryptographic protection of a data stream in a communication system. US Patent Appl. EP 0671092 A1, Sept. 13. 1995.

[12] Xianye, Xiangfeng, Xiulun, Yurong, Yongkai Yin, Xiang Peng, Wenqi, Guoyan, Hongyi, "Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme", Volume 102, Pages 106–111, March 2018.

[13] Chong Fu, Zhou-Feng Chen, Wei Zhao, Hui-yan Jiang, "A New Fast Color Image Encryption Scheme Using Chen Chaotic System", 18th IEEE conference, Pages: 121–126, 2017.

[14] Wenting Yuan, Xueiln Yang, Wei Guo, Weisheng Hu, "A double domain image encryption using hyperchaos", 19th ICTON conference, Pages: 1–4, 2017.

[15] Yaghoub Pourasad, Ramin Ranjbarzadeh and Abbas Mardani. A New Algorithm for Digital Image Encryption Based on Chaos Theory. Entropy 2021, 23, 341. P/ 1-16 https://doi.org/10.3390/e23030341

[16] XingyuanWang, NanaGuan, Hongyu Zhao, SiweiWang & YingqianZhang. A new image encryption scheme based on coupling map lattices with mixed multi-chaos. Scientific Reports, (2020) 10:9784, P. 1-15. https://www.nature.com/articles/s41598-020-66486-9.pdf

[17] Mao, Y.; Chen, G.; Lian, S. A novel fast image encryption scheme based on 3D chaotic baker maps. Int. J. Bifurcation Chaos 2004, 14, 3613–3624.

[18] Wu, Y. Image encryption using the two-dimensional logistic chaotic map. J.Electron. Imag. 2012, 21, 013014.

[19] Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals 2004, 21, 749–761

[20] Lian, S.; Sun, J.; Wang, Z. A block cipher based on a suitable use of the chaotic standard map. Chaos Solitons Fractals 2005, 26, 117–129.

[21] Ping, P.; Xu, F.; Mao, Y.; Wang, Z. Designing permutation substitution image encryption networks with Henon map. Neurocomputing 2018, 283, 53–63

[22] Govinda.K, Prasanna.S, "A Generic Image Cryptography Based on Rubik's Cube", ICSNS conference, Pages: 1–4, 2015.

[23] Shahryar Toughi, Mohammad H. Fathi, Yoones A. Sekhavat, " An image encryption scheme based on elliptic curve pseudo-random and Advanced Encryption System", Volume 141, December 2017, Pages 217–227

[24] Fathi, M.H.; Sekhavat, Y.A.; Toughi, S. An image encryption scheme based on elliptic curve pseudo random and Advanced Encryption System. Signal. Process. 2017, 141, 217–227.

[25] K.R.Radhika, M.K.Nalini, "Biometric Image Encryption using DNA sequences and Chaotic Systems", ICRAECT conference, Pages: 164–168, 2017.

[26] Enayatifar R., Abdullah A.H., Isnin I.F. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Opt. Lasers Eng. 2014;56:83–93. doi: 10.1016/j.optlaseng.2013.12.003.

[27] Chai X, Fu X, Gan Z, Lu Y, Chen Y (2019) A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process 155:44–62. https://doi.org/10.1016/j.sigpro.2018.09.029.

[28] S H Kamali, R Shakerian, M Hedayati, M Rahmani, "A New Modified Version of Advanced Encryption Standard Based Algorithm for Image Encryption", ICEIE

Conference, Year: 2010, Volume:1 Pages: 141–145.
[29] Nandi S, Chakraborty S, Roy S, Karaa WBA, Nath S, Dey N (2014) 1-D Group Cellular Automata Based Image Encryption Technique. in: Proceedings of the 2014 IEEE Intern Conf Control, Instrument, Commun, Computation Technol (ICCICCT). Kanyakumari India. https://doi.org/10.1109/ICCICCT.2014.6993017.
[30] Wang Y, Zhao Y, Zhou Q, Lin Z (2018) Image encryption using partitioned cellular automata. Neurocomputing 275(1), 1318–1332
[31] Zhang S, Luo H (2012) The Research of Image Encryption Algorithm Based on Chaos Cellular Automata. J Multimedia 7(1):66–73. https://doi.org/10.4304/jmm.7.1.66-73
[32] Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301.
[33] Stepan Bilan, Mykola Bilan, Sergii Bilan. Research of the method of pseudo-random number generation based on asynchronous cellular automata with several active cells.- MATEC Web of Conferences, - Vol. 125,- 02018 (2017), - P. 1-6.
[34] Stepan Bilan. Evolution of two-dimensional cellular automata. New forms of presentation, Ukrainian Journal of Information Technologies, т. 3, №1, (2021): 85-90.
[35] Wolfram, S. (2002). A new kind of science. Wolfram Media
[36] Adamatzky, A. (2018). Cellular automata. A volume in the Enciclopedia of cjmplexity and systems science. Second edition. Springer Science + business media LLC, part of springer Nature
[37] Mauri, Giancarlo, El Yacoubi, Samira, Dennunzio, Alberto, Nishinari, Katsuhiro, & Manzoni, Luca (Eds.). (2018). Lecture Notes in Computer Science. 13th International Conference on Cellular Automata for Research and Industry, ACRI 2018, Como, Italy. (September 17–21, 2018), Proceedings, 11115, Springer
[38] Wolfram, S. (1986). Random Sequence Generation by Cellular Automata. Advances in Applied Mathematics, 7(2), 429–432. doi:10.1016/0196- 8858(86)90028-X