Selection of Intelligent Rules for the Evolution of Elementary Cellular Automata for Image Encryption

NASHAT AL BDOUR
Computer and Communication Engineering,
Tafila Technical University,
Tafila,
JORDAN

Abstract: - The paper is devoted to the search for new approaches to the formation of key arrays for encryption of color images. Emphasis is placed on using the initial key sequence of the smallest length. In this case, the key is the initial state of an elementary cellular automaton for implementing evolution based on a given rule. The use of an evolutionary approach on cellular automata to the formation of large key arrays made it possible to achieve unpredictable image encryption based on a single rule of an elementary cellular automata. The task of the research is to search for the rules of elementary cellular automata, which, based on a small initial key bit sequence, allow one to form a reliable key array of large dimensions for encrypting the bit layers that make up the image. To solve this problem, an experiment was carried out, on the basis of which the search for the necessary rules and options for choosing the elements of each bit array was carried out to encrypt the bit layers of the image. To form each bit key array, different initial conditions were used for elementary cellular automata. It is shown that for different initial conditions and for the chosen rules, the encryption quality is preserved. The most reliable encryption is the use of two key arrays formed on the basis of the evolution of one rule for different initial conditions. As a result of the experiments, the rules were determined (rules 90, 105, 150 and XOR function based on the two previous steps of evolution), which can be used without additional rules. Each bit layer of the image is encrypted using different subarrays of each generated one key array of the same dimension. It has been established that the most effective for encryption is the rule 105 and the XOR function based on the two previous steps of evolution. The resulting histograms of the distribution of brightness for each color of the encrypted image confirm the high quality of encryption based on the proposed method.

Key-Words: - Encryption, Cellular automata, Key array, Image bit layers, Evolution, Wolfram's rule.

Received: August 28, 2021. Revised: August 29, 2022. Accepted: September 27, 2022. Published: October 25, 2022.

1 Introduction

Modern society is characterized by a high degree of digitalization, which is being implemented at a rapid pace in all spheres of human activity. On this basis, digital information transmission systems have received great development, which, like tentacles, have come to every apartment and to every person, to every desktop. Almost every person who has a modern smartphone has its own access point, which allows the user to communicate with anywhere in the world. Modern smartphones contain high-performance processors and large amounts of memory, which allows high-speed transfer of large amounts of data from point to point.

Images presented in digital form take up significant amounts of memory. At the same time, many methods and tools for image compression have been developed, [1], [2], which allow to reduce the occupied volumes, but at the same time, in most methods, part of the information about the image itself is lost. In most digital systems, images are represented in raster form.

In most cases, users do not want the images they represented or send to be viewable by other network users. Therefore, images are converted or encrypted so that visual information is not available for viewing.

There are a large number of image encryption methods that take into account its digital structure. The most ideal encrypted image is an image in which all the colors of the pixels are distributed evenly and do not make it possible to reveal any statistical relationships with the original image. Also, the ideal method for encrypting an image is a method that is based on using any encryption key with the smallest possible length.

Existing methods often provide high quality image encryption. However, these methods cannot boast of the simplicity and versatility of the method itself, since they use various additional computing

tools. In this regard, the search and development of new methods for encrypting images that are close to ideal are carried out. Increasingly, there are publications that describe image encryption methods implemented using cellular automata (CA) technologies [3], [4], [5], [6], [7], [8], [9], [10]. In these works, CA proved to be promising in solving encryption problems.

2 Problem Statement

One of the main problems in solving the problem of image encryption is the use of a long key gamma, which can be generated by the user himself, or can also generate a pseudo-random number generator (PRNG) based on the established initial conditions. Forming a key gamma for encrypting large amounts of data (images) does not seem realistic. Therefore, PRNG is most often used. However, PRNG cannot always form the highest quality sequence of numbers. In addition, the structure of the generator may be known to other users. Such shortcomings force developers to search for new more effective methods.

A promising direction in solving such a problem is the use of CA, on the basis of which PRNGs are built, which showed a high quality of the generated bit sequences, [3], [11], [12], [13], [14]. Elementary CA (ECA) and two-dimensional CA are used, as well as their states obtained during the formation of evolution.

Despite the byte structure, bitmaps can be considered as a sequence of two-dimensional bit layers that can be encrypted both in parallel and sequentially. To encrypt one two-dimensional N×M bit array, it is necessary to use N×M key bits. If a binary code of length K bits is used to encode the visual characteristics of one pixel of a raster image, then K × N × M key bits must be used to encrypt the entire image. The use of PRNG based on CA complicates the implementation of the encryption method.

The paper solves the problem of implementing a method for encrypting raster images using a key of small length. To solve this problem, one ECA rule is used, determined on the basis of experimental studies.

Since a bitmap image is represented in a computer system by a sequence of bytes or, more precisely, a binary sequence, it is easiest to encrypt images using the streaming encryption method [3], [4], [5], [11], which consists in applying a bit key gamma to a bitmap image [3], [4], [5], [6], [7], [8], [9], [10], [11]. To implement this method, a device for generating a key gamut is used, which, as a rule, is a PRNG [12]. To date, a large number of PRNGs have been developed [12], [13], [14], [15]. which have different configurations. Almost all existing PRNGs (mathematical, hardware, etc.) can be simulated on a PC and implemented in software. Using such a program model, you can encrypt any graphic file. In papers [3], [10], [11], [15], methods using this method are considered. In [11], experimental studies were carried out and it was shown that it is enough to encrypt the three most significant bits of each color byte. In this case, a pseudo-random bit sequence was used, generated by a PRNG implemented on a CA with active cells, [13], [14]. The obtained experimental results showed a high quality of encryption. However, this method takes time to form the key gamma and complete enumeration of all bits that encode the image.

There are image encryption methods based on the Fourier transform, [16], [17], [18], and Wavelet transform, [19]. In recent years, a direction based on quantum image encryption has been developing [21], [22], [23], [24]. Papers on these topics describe complex encryption schemes that do not always provide high quality encryption. In addition, such approaches can lead to partial loss of information about the original image at the decryption stage.

A large number of methods use various methods based on chaos theory, [25], [26], [27], [28], [29], [30]. However, these methods require complex calculations and can lead to partial loss of information.

There are methods using genetic algorithms, [31]. [32], [33] [34], [35], DNA calculations, [36], [37], [38], based on elliptic curves, [39], [40], Rubik's cube, [41], and artificial neural networks, [42]. All these methods require special calculations to be performed to transform the information array and form a key array, which limits these methods, since they are not resistant to attacks and cannot guarantee high reliability.

Image encryption methods using CA technologies have been greatly developed [3], [4], [5], [6], [7], [8], [9], [10]. Many of these works use additional means for encryption. Often an additional tool is chaos theory , [25], [26], [27], [28], [29], [30]. There are also works that use separate ECA rules with additional methods [7], [43]. Thus, in [43], rules for an ECA with a length of 8 cells were considered and studied. Rules that give a good result are defined. However, the limited length of the ECA does not give full grounds for asserting effective encryption of color images. In [7], rule 30 is considered, which does not provide high quality image encryption. This is proven in paper [10]. In

this paper, a good encryption result is obtained. However, this uses multiple rules to encrypt each bit layer of the image, and also uses different initial states for each rule. This approach requires the formation of a large encryption key, which limits this method. At the same time, paper [10] has valuable material that shows which ECA rules are the most effective for encrypting color bitmaps.

3 The Structure of a Bitmap Color Image

In a computer system, a color image is stored as a graphic file, consisting of bytes that encode the structure of the image and the colors for each pixel. Color depth is encoded by the number of bits allocated for each pixel (4, 8, 16, 24, etc. bits). The more bits per pixel color code, the more color gradations can be displayed by one pixel of the image and the more realistic the visual picture can be presented.

The paper [14] presents the structure of a color image, which displays it as a sequence of bit layers. Each bit layer is a matrix (two-dimensional array), each element of which represents the bit value of the corresponding bit, which occupies a position in the binary code corresponding to the binary layer number. Each i-th bit layer contains the i-th bits of the codes of all pixels. The number of bit layers is equal to the number of bits in the code of each image pixel.

Since each bit layer contains only logical "0" and logical "1", they are considered as two-dimensional cellular automata or as arrays formed as ECA evolution in one of four directions.

4 Color Image Encryption Methodology

The image encryption method uses the representation of an image as a matrix of codes that encode the color and brightness of each pixel. The pixel code consists of three parts (3 bytes). The first high byte of the code encodes the blue color and its shades, the second and third code bytes encode the green and red colors and their shades, respectively. A color image can be represented as a sequence consisting of a sequence of 24 bit layers forming an image matrix in depth.

The paper [10] describes the encryption methodology for color images based on the technology of cellular automata with different rules. Each bit layer is encrypted separately with a key array of the same dimension. Key arrays are formed based on the use of ECA evolution construction technology. The structure of the encryption method on Fig. 1 is shown.

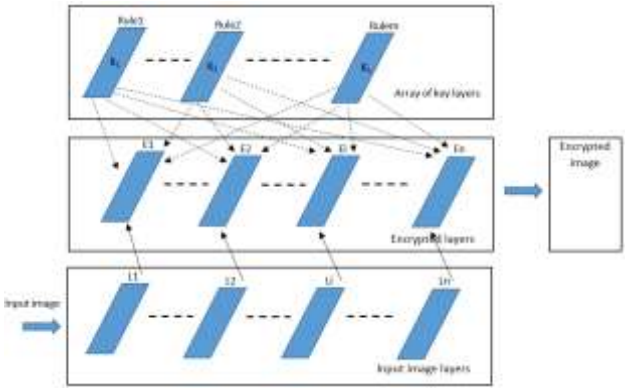

Fig. 1: Structure of the color image encryption method

Each binary layer of the image is encrypted using one of the key layers formed according to the selected ECA rule. The initial state of the ECA is set and the evolution is formed. The resulting evolution is commensurate with the dimension of the bit layer of the image and is a key array. Each key array as a key gamma is superimposed on each binary bit layer of the image. As a result, we get encrypted binary layers, which form an array of binary layers E_i of the encrypted image. The binary encrypted array E is formed by applying the XOR operation

$E = K \oplus L.$

In this case, the key layers K are formed on the basis of different rules and are used for encryption for different binary layers of the initial image. If the same rules are often used, then an offset on key layers is applied for different initial layers. To implement this approach, evolutions form two-dimensional arrays of a larger dimension than the dimension of the bit layer of the image.

Using the same initial conditions to form key layers with different rules requires a large number of rules with different forms of evolution. In this case, there is a need to select the initial conditions, as well as the rules for each layer of the initial image. Different initial conditions (initial keys) for each rule improve the picture of encryption. However, for images of large dimensions, it is necessary to use key bit sequences of large length. As the number of rules increases, the number of large length encryption keys increases.

In this method, encrypted images contain some geometric shapes that are inherent in the ECA evolution forms for some rules. Therefore, image encryption requires careful selection and placement

of rules before encryption, which partially limits the method.

5 Experimental Selection of One Rule for Image Encryption

The main task of the experiment is to analyze the ECA evolutions for different rules and the rules selection that can be used to form a key array. In this case, only one rule should be used and a combination of several rules should not be used, since this circumstance complicates the encryption system. The rules were selected both visually by the user and possible rules without visual analysis that could be effective.

To search for optimal rules, the following rules were studied: 30, 45, 51, 90, 105, 111, 150, and 184. These rules were selected from the analysis of evolutions described earlier in various works [44], as well as visual analysis of these evolutions. On fig. 2 is shows the evolutions for these rules. A visual analysis was carried out for the predictability of states at each step of the iteration.

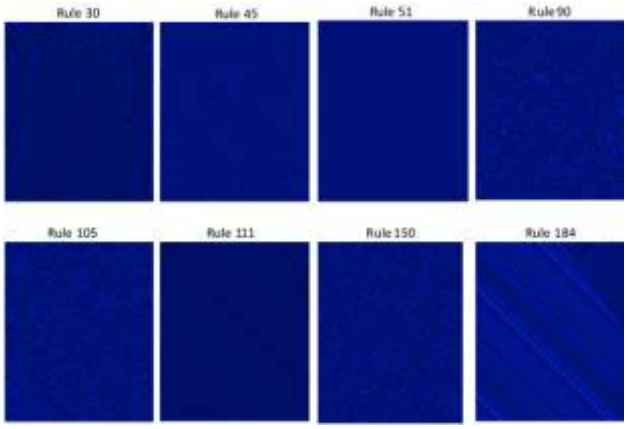

Fig. 2: ECA evolutions for rules: 30, 45, 51, 90, 105, 111, 150 and 184.

Visual analysis of the obtained evolutions showed that the most suitable rules are the rules: 90, 105 and 150. Rules 111 and 184 can only be used in addition to other rules and cannot be used as separate rules. Evolutions show constant state changes throughout the field of the formed two-dimensional array. If rules 90 and 150 form evolutions with triangular shapes, then rule 105 is the most attractive. However, encryption was carried out for all the described rules.

The first step of the experiment was to use only one key array, which, using the XOR function, encrypted all the bit layers into which the images were divided. Lighter colors barely changed the color characteristics of the corresponding pixel. The encryption results at this stage did not show high quality. You can see the outlines of differences in brightness and colors, which can be used to restore the original image.

At the second stage of the experiment, one rule was used, but each bit layer of the image was encrypted with the received key array, the beginning of which was shifted for each bit layer (Fig. 3). The initial key array was formed with a larger dimension along one coordinate. The value of the generated array is determined by the number of shifts of the initial key array and the number of pixels by which the shift is performed.

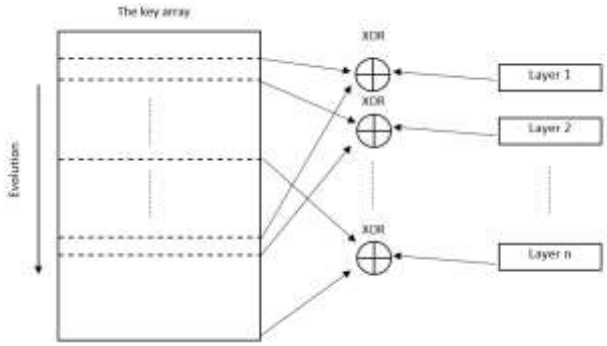

Fig. 3: Selection of key arrays at the second stage of the experiment

In many cases (for many rules), this approach gives a sufficiently high quality of encryption. It depends on the used initial states of the initial CA, which is used to form the initial keys. However, the outlines of the original image are often traced on the obtained images (Fig. 4).

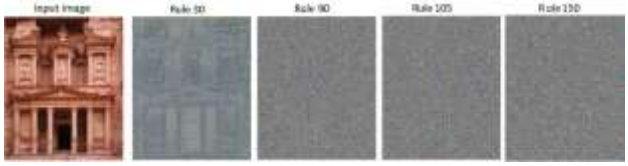

Fig. 4: Results of image encryption obtained at the second stage of the experiment

To improve the quality of encryption, key arrays obtained as a result of using the XOR function were used at two adjacent previous steps of evolution (Fig. 5). In this case, the initial key bit sequence is doubled, but the number of rules does not change. Changes start from the third line of evolution and then form unpredictable states if the previous ones are not known to the user.

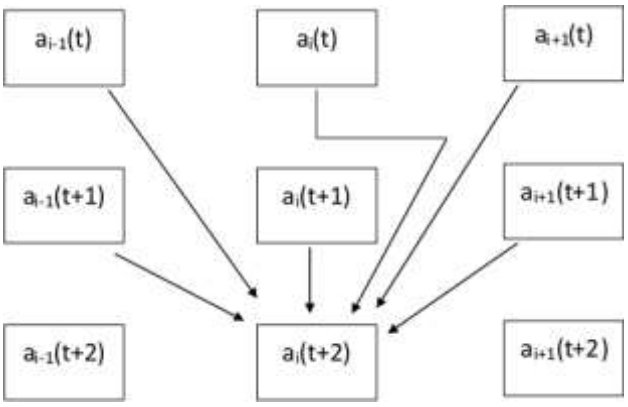

Fig. 5: Formation of the next step of evolution based on the two previous steps

To form the state of the cell, the XOR function of six arguments was used. The arguments are the states of the six cells in the previous steps. These cells are shown in Fig. 4 and are indicated by the beginnings of outgoing arrows. The state of the cell at the time (t + 2) is determined by the following formula.

$$a_i(t+2) = XOR(a_{i-1}(t), a_i(t), a_{i+1}(t), a_{i-1}(t+1), a_i(t+1), a_{i+1}(t+1))$$

An example of CA evolution for this variant is shown in Fig. 6.


Fig. 6: An example of CA evolution based on the two previous steps of evolution

On fig. 4 is shows the result of image encryption, which also does not give the desired quality. In some places of the encrypted image, the outlines of the original image are visible, which, after a detailed analysis, can lead to a complete restoration of the original image.

For more reliable encryption, several key arrays were used, which were obtained using the same rule, but with different initial states of the ECA. In this case, an additional shift in each key array was used to encrypt individual bit layers of a color image. The results of such encryption in Fig. 7 are shown. To be sure, are used a test image (presented first), which contains different solid color zones.

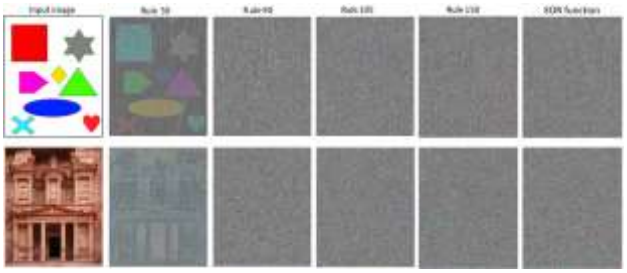
Fig. 7: Results of image encryption based on one rule and several key arrays

Encryption results (Fig. 7) showed high quality for rules 90, 105, 150 and XOR functions based on two evolution steps for both test images. The high quality of encryption for these rules is confirmed by the obtained histograms of the distribution of brightness for each color (Fig. 8). On fig. 8 color distribution histograms are presented for the initial image (leftmost) and encrypted images for each rule.

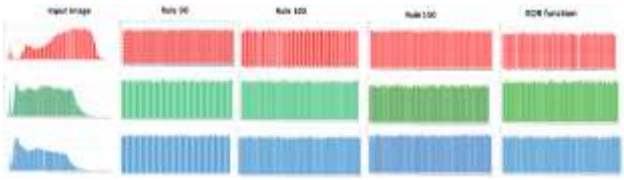
Fig. 8: Color distribution histograms for each encryption rule

The first row describes the distribution for red, the second for green, and the third for blue. The resulting histograms show a uniform distribution of colors over the entire field of the encrypted image. Such a distribution does not allow the adversary to determine and restore the original image. Histograms are shown for the second image shown in Fig. 7.

If the images obtained using rules 90 and 150 contain many triangular shapes, then the encrypted images obtained using the remaining two rules do not have any geometric shapes that could prompt the opponent to determine the structure of the key array. The analysis of the obtained images made it possible to assert that the rule 105 and the XOR function are the most effective based on the two previous steps in the ECA evolution.

6 Conclusion

The paper considers the process of experimental search for the rules of elementary cellular automata, with the help of which a key array is formed for

encrypting color images. As a result of the experiment, rules were defined that give high quality encryption (90, 105, 150 and XOR function based on the two previous steps of evolution). It has been proven that to encrypt an image, it is sufficient to use only one of these rules, which gives two key arrays based on different initial conditions. The use of these rules made it possible to reduce the length of the initial key, as well as to simplify the image encryption scheme. These rules can also be used together. At the same time, the quality of encryption remains high.

In further research, the author plans to use cellular automata that implement other paradigms that give unpredictable evolutions. Research will also focus on the use of two-dimensional cellular automata.

References:

[1] William A. Pearlman. Wavelet Image Compression (Synthesis Lectures on Image, Video, and Multimedia Processin). Morgan & Claypool Publishers; 1st edition (January 22, 2013).

[2] Yuxin Peng, Shi-Min Hu, Moncef Gabbouj, Kun Zhou, Michael Elad, Kun Xu. Image and Graphics: 11th International Conference, ICIG 2021, Haikou, China, August 6–8, 2021, Proceedings, Part I (Lecture Notes in Computer Science Book 12888). Springer (September 30, 2021)

[3] 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.

[4] Xingyuan Wang, Dapeng Luan. (2013). A novel image encryption algorithm using chaos and reversible cellular automata. Communications in Nonlinear Science and Numerical Simulation 18(11):3075–3085

[5] A.L.A. Dalhoum, A. Madain, H. Hiary, Digital image scrambling based on elementary cellular automata, Multimedia Tools Appl. 75 (24) (2016) 17019–17034.

[6] T.H. Chen, M. Zhang, J.H. Wu, C. Yuen, Y. Tong, Image encryption and compression based on kronecker compressed sensing and elementary cellular automata scrambling, Opt. Laser Technol. 84 (2016) 118–133.

[7] Wassim Alexan, Mohamed khaled Elbeltagy. (2021). Lightweight Image Encryption: Cellular Automata and the Lorenz System. Conference: 2021 International Conference on Microelectronics (ICM): 34-39.

[8] Juan Contreras, Marco Ramírez, Jesús Aboytes. Image Encryption System Based on Cellular Automata and S-Box. Research in Computing Science 148(10), 2019. pp. 153–161

[9] Wang Y, Zhao Y, Zhou Q, et al. (2018) Image encryption using partitioned cellular automata. Neurocomputing 275:1318–1332

[10] Paper9/ Image encryption methodology based on cellular automata

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

[12] Stepan Bilan. Formation Methods, Models, and Hardware Implementation of Pseudorandom Number Generators: Emerging Research and Opportunities.- (2017).- IGI Global, USA.- P. 301.

[13] 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.

[14] Stepan Bilan. Evolution of two-dimensional cellular automata. New forms of presentation, Ukrainian Journal of Information Technologies, т. 3, №1, (2021): 85-90.

[15] 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

[16] 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.

[17] 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

[18] 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

[19] 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.

[20] Xingbin Liu, Di Xiao, Cong Liu. (2018). Double Quantum Image Encryption Based on Arnold Transform and Qubit Random Rotation. *Entropy* 2018, *20*(11), 867

[21] Li, C.-L.; Li, H.-M.; Li, F.-D.; Wei, D.-Q.; Yang, X.-B.; Zhang, J. Multiple-image encryption by using robust chaotic map in wavelet transform domain. *Optik* 2018, *171*, 277–286.

[22] Wang, Jian & Geng, Ya-Cong & Han, Lei & Liu, Ji-Qiang. (2019). Quantum Image Encryption Algorithm Based on Quantum Key Image. International Journal of Theoretical Physics. 58.

[23] Yang, Yu-Guang & Xia, Juan & Jia, Xin & Zhang, Hua. (2013). Novel image encryption/decryption based on quantum Fourier transform and double phase encoding. Quantum Information Processing. 12.

[24] Tan, R.-C.; Lei, T.; Zhao, Q.-M.; Gong, L.-H.; Zhou, Z.-H. Quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform. *Int. J. Theor. Phys.* 2016, *55*, 5368–5384

[25] Y. Xie, J. Yu, S. Guo, Q. Ding, and E. Wang, "Image encryption scheme with compressed sensing based on new three-dimensional chaotic system," *Entropy*, vol. 21, no. 9, p. 819, 2019.

[26] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[27] M. Kaur and V. Kumar, "Adaptive differential evolution-based lorenz chaotic system for image encryption," *Arabian Journal for Science and Engineering*, vol. 43, no. 12, pp. 8127–8144, 2018.

[28] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1d chaotic maps," *Entropy*, vol. 20, no. 11, p. 843, 2018.

[29] Hua, Z., Zhou, Y. & Huang, H. Cosine-transform-based chaotic system for image encryption. *Information Sciences* 480, 403–419. https://doi.org/10.1016/j.ins.2018.12.048 (2019).

[30] Yaghoub Pourasad, Ramin Ranjbarzadeh, Abbas Mardani. A New Algorithm for Digital Image Encryption Based on Chaos Theory. *Entropy* 2021, *23*(3), 341

[31] Chai, X. *et al.* Combining improved genetic algorithm and matrix semi-tensor product (stp) in color image encryption. *Signal Processing* 183, 108041. https://doi.org/10.1016/j.sigpro.2021.108041 (2021).

[32] Wang, X.; Zhang, H.-L. A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems. *Nonlinear Dyn.* 2016, *83*, 333–346.

[33] Nematzadeh, H.; Enayatifar, R.; Motameni, H.; Guimarães, F.G.; Coelho, V.N. Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. *Opt. Lasers Eng.* 2018, *110*, 24–32.

[34] Kaur, M.; Kumar, V. Beta Chaotic Map Based Image Encryption Using Genetic Algorithm. *Int. J. Bifurc. Chaos* 2018, *28*

[35] Nematzadeh H, Enayatifar R, Motameni H, et al. (2018) Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt Lasers Eng 110:24–32

[36] Zhen, P., Zhao, G., Min, L., Jin, X. Chaos-based image encryption scheme combining DNA coding and entropy. *Multimed. Tools Appl.* 2016, *75*, 6303–6319

[37] T. Hu, Y. Liu, L.H. Gong, S.F. Guo, H.M. Yuan, Chaotic image cryptosystem using DNA deletion and DNA insertion, Signal Process. 134 (2017) 234–243.

[38] R. Guesmi, M.A.B. Farah, A. Kachouri, M. Samet, A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2, Nonlinear Dyn. 83 (3) (2015) 1123–1136.

[39] Ikram Ullah, Umar Hayat, and Miguel D. Bustamante. Image Encryption Using Elliptic Curves and Rossby. Drift Wave Triadsıo Entropy 2020, 22, 454. https://arxiv.org/pdf/2003.03394.pdf

[40] Wu J, Liao X, Yang B (2017) Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. Signal Process 141:109–124

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

[42] Dridi M, Hajjaji MA, Bouallegue B, et al. (2016) Cryptography of medical images based on a combination between chaotic and neural network. IET Image Process 10(11):830–839

[43] Jun Jin. An image encryption based on elementary cellular automata. Optics and Lasers in Engineering Volume 50, Issue 12, December 2012, Pages 1836-1843

[44] Wolfram, S. (2002). A new kind of science. Wolfram Media

.