Int. J. Nonlinear Anal. Appl.
10 (2019) Special Issue (Nonlinear Analysis in Engineering and Sciences), No. 15, 169-177
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2019.4429

Digital Color Image Encryption Using Cellular Automata and Chaotic Map

Hamed Ghazanfaripour[a], Ali Broumandnia[b*]

[a] *Department of Computer Engineering, Kerman Branch, Islamic Azad University, Kerman Iran.*
[b] *Islamic Azad University-South Tehran Branch, Iran.*

Abstract

Today, with the expansion of multimedia communications, computer networks, and the distribution of information on the Internet, maintaining the security of information exchanged through insecure channels has become an important and essential issue in data communication. One way to protect the information in passive defense is to encrypt data so that people can communicate securely on a secure channel while maintaining their privacy and data authenticity. Because color image data has certain features compared to traditional data such as text and binary data, special algorithms are needed to encrypt digital images to maintain the efficiency, security, and speed of encryption. The present study provides a way to encrypt digital images using reversible cell automation and chaotic mapping. The basis for encrypting the proposed method is the use of the concepts of Shannon's confusion and diffusion technique, which takes place in two main stages. In the first step, the plain image is received as input, then it is permuted using the 3D chaotic map by using suitable key. In the second step, the cipher image from the previous step are extracted to 24 one-bit plates image and XOR by suitable 2D reversible cell automata. The proposed method will be compared with several cryptographic methods and has good outperform results.

Keywords: Color image encryption, reversible cellular automata, permutation, diffusion, confusion, chaotic map.
2010 MSC: 76T20

1. Introduction

Today, with the spread of computer networks for a variety of purposes, extensive changes have taken place in the way we work and live. This means that individuals and organizations make their

*Corresponding Author: Hamed Ghazanfaripour
Email address: Broumandnia@gmail.com (Hamed Ghazanfaripour[a], Ali Broumandnia[b*])

Received: June 2019 *Revised:* August 2019

data available to others by connecting to the World Wide Web. That's why information security is so important. Ensuring that people do not access information is one of the most important pillars of information security on the Internet. So far, various solutions have been proposed for information security, including restrictions on the use of the Internet, the use of security tools, and data encryption. In the meantime, cryptography is very important and has been used for various purposes. One of the most common ways to protect information is to encrypt it. Encryption is the knowledge of changing the information sent using the password key and a password algorithm so that only the person who knows the key and the algorithm can extract the original information from the password information and the person who does not know one or both of them, Cannot access information. The use of cryptography has a long and historical history. Before the information age, most information encryption users were governments, especially military users. The history of information encryption dates back to the Roman Empire. Today, most computer encryption methods and models are used in connection with computers. Access to information that does not have any scientific cryptographic methods and is normally stored or exchanged through computer networks will be easily done by unauthorized persons and without the need for special expertise, so data encryption Due to recent developments, new developments, and algorithms have been designed for this purpose. Recently, with the growth of digital image transmission over the Internet, communication channels need to be secure enough and not attacked by hackers, so maintaining security and verifying images is becoming increasingly important. But implementing cryptographic methods for visual data is a challenge compared to text messaging. Image data is not securely encrypted by classic text encryption algorithms such as RSA and DES due to features such as bulk, large additions, and high correlation between image points, especially in real-time applications, especially in real-time applications [1, 10, 13]. Another of these algorithms is their key length, which due to the volume of encrypted data, the use of limited length keys makes the method vulnerable to encrypted text attacks. To overcome these problems, many people have come up with new ways to encrypt images.

Recently, various image encryption techniques have been proposed that use the concepts of displacement and propagation to provide resistance to the known functions of the image. Extremely high parallelism is used as a tool for rapid computations in system simulation as well as computational tasks such as image processing and image encryption. Today, cellular automation is considered to be a structure that has the potential to perform complex tasks and performs these calculations very efficiently.

In this research, we examine the cryptography of images by proposing a method based on the concept of confusion, diffusion, and the use of cellular automata. In the second section of this study, the theory of cellular automata is presented. In the third section, the concepts of the 3D modular chaotic map are described. In the fourth section, the proposed method is described. The results of the evaluation of the proposed method will be reviewed in Chapter fifth. The final section of the dissertation outlines future conclusions and suggestions.

2. Cellular automata

Cellular automata (CA) [14] is a useful mathematic model for physical, biological, and computational systems. The discrete characteristic of CA is that simple fundamental rules of it can effort very proficiently by composite activities which can be used to develop CA-based encryptions. Cellular automata is a mathematical model of a scheme, with an open system by discrete inputs and outputs. It represents the sequential behavior of several interconnected cells which are organized consistently, each with a finite set of likely values. A CA evolves in discrete time steps and the value engaged by a specific cell (local state) is affected by the cell values in its nearest neighbors on the previous time step, affording to a function known as the CA rule. Elementary CA is the simplest case, which is a linear array of cells, with three neighborhood dependencies, and the state of each the cell is 0 or 1. S_i^t denotes the state of the ith cell at time t, and f is a Boolean state function that specifies the local rule, a new state is produced as [6]:

$$S_i^{t+1} = f(S_{i-1}^t, S_i^t, S_{i+1}^t) \tag{2.1}$$

The set of local rules for the time evolution of a 1D CA has been coded by Wolfram [14]. An example of Wolfram's notation for CA rules is given in Table 1. The neighborhood is composed of 3 cells. This makes $n = 2^3$ possible configurations of that neighborhood. This means that the total number of rules of ECA is 256 [6].

Table 1: Elementary rule 90 [14]

Neighborhood	111	110	101	100	011	010	001	000	No.
Next state	0	1	0	1	1	0	1	0	90

3. The 3D chaotic map

To overcome security attacks challenges on the transmission of digital images through network and internet, from the past few years, image encryption schemes are widely used the chaos to perform encryption and decryption operation [9]. Chaotic maps have certain prominent features like "sensitivity to initial conditions", "ergodicity", "pseudo-random property", "non-periodicity", etc. [4, 5]. In terms of speed, security, and complexity, the chaotic map based encryption methods provide excellent performance as compared to the standard encryption techniques [9]. Chaotic maps for encryption are divided into reversible and non-reversible. For example, the logistic map and Arnold cat map are non-reversible and reversible respectively. Usually reversible chaotic maps are used for permutation operations in cryptography. In encryption, some chaotic maps extend from continuous-time to discrete-time. In this study, reversible and discrete chaotic maps are used to permutation operations in the image cryptography. This reversible and discrete chaotic map is defined by equation (3.1) and it's called 3D modular chaotic map (3DMCM)[2, 3].

$$\begin{bmatrix} x_{m+1} \\ y_{m+1} \\ z_{m+1} \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \times \begin{bmatrix} x_m \\ y_m \\ z_m \end{bmatrix} \bmod n \tag{3.1}$$

In equation (3.1) A is a residue matrix of 3×3 that its elements belong to Z_n. 3DMCM is reversible if $gcd(|A|, n) = 1$ and its multiplicative inverse is defined by

$$\begin{bmatrix} x_m \\ y_m \\ z_m \end{bmatrix} = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}^{-1} \times \begin{bmatrix} x_{m+1} \\ y_{m+1} \\ z_{m+1} \end{bmatrix} \bmod n \tag{3.2}$$

Where A^{-1} is the inverse of the residue matrix A. The residue matrix A is reversible if it satisfies in the equation $gcd(|A|, n) = 1$. In this case, the inverse matrix A^{-1} is calculated using equation $A^{-1} = (|A|^{-1} \times C^T) \bmod n$ and the extended Euclidean algorithm [2, 3].

4. The proposed encryption method

The proposed method for encrypting digital color images is based on the concepts of the 3D chaotic map, and the use of cellular automation. The general procedure in chaotic systems is based on permutated the pixels and changing the values of the pixels, which also uses the concepts of confusion and diffusion in image encryption. Displacement or permutation using the 3D chaotic map is the important type of confusion property that only changes the location of the image pixels in each sub-image, and substitution is a specific mode of propagation that changes the gray level values of the RGB pixels CA rules. In the proposed method, image encryption is performed during two stages or the main process of permutation and diffusion, according to the block diagram presented in Figure 1. Each encryption operation has a reverse encryption process, i.e. decryption.

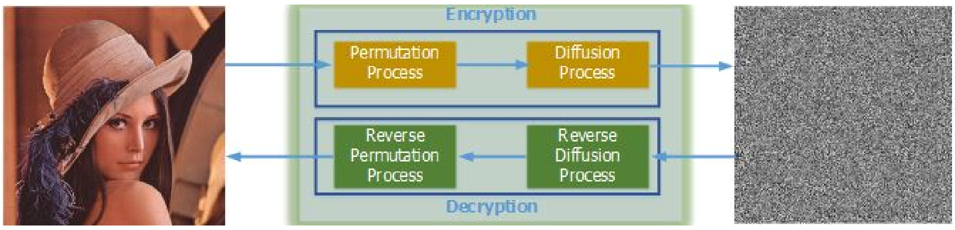

Figure 1: The general proposed color image encryption and decryption

4.1. Permutation process

The first step in the proposed method is the permutation process. The goal of this step is to eliminate the strong correlation between adjacent pixels in the plain or unencrypted image, while the level (intensity) of the histogram remains at the same level as the plain image, and at the end of this stage, the original image becomes an incomprehensible or randomize like image. In this step, according to Figure 2, a color digital image is selected as the input of the permutation process without any limitation on its size. First, the image is divided into three red, green, and blue components, next to the 3D chaotic map based on equation (3.1), which is based on the discrete chaotic map, is applied to the red, green, and blue components to permute the pixels.

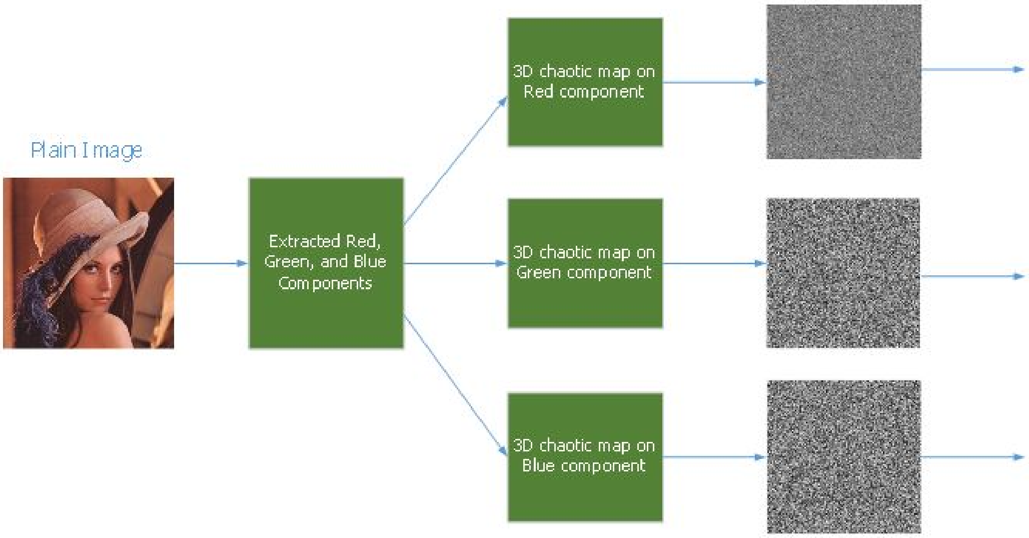
Plain Image
Extracted Red, Green, and Blue Components
3D chaotic map on Red component
3D chaotic map on Green component
3D chaotic map on Blue component

Figure 2: The permutation process using the 3D chaotic map

4.2. Diffusion Process

The second step of the proposed method is the diffusion process, in which the gray level of the image pixels is altered. As shown in Figure 3, in this step, the input color image is first broken down into three separate components, red or R, green or G, and blue or B components, and each component is converted into 8 one-bit binary images. Each RGB component is broken down into 8 1-bit plate images. Due to the operation of separating the bit surface, this method, while simple, has high complexity.

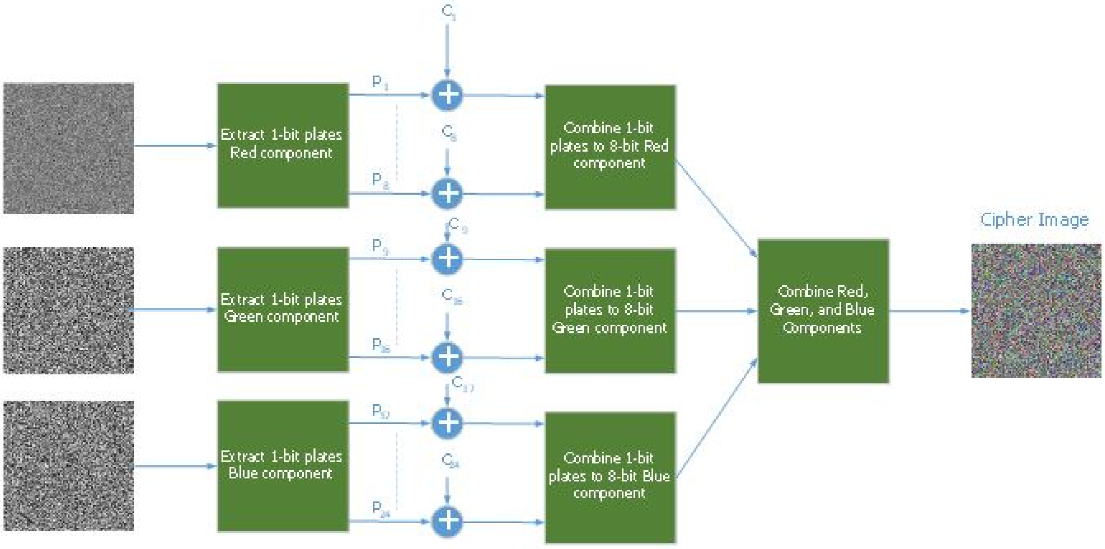
C1
P1
C8
P8
C9
P9
C16
P16
C17
P17
C24
P24
Extract 1-bit plates Red component
Extract 1-bit plates Green component
Extract 1-bit plates Blue component
Combine 1-bit plates to 8-bit Red component
Combine 1-bit plates to 8-bit Green component
Combine 1-bit plates to 8-bit Blue component
Combine Red, Green, and Blue Components
Cipher Image

Figure 3: The diffusion process using cellular automata

On the other hand, using the rules of Wolfram cellular automata, binary images of cellular automata are available, which are used as special keys generated by Wolfram cellular automatics for diffusion on 24 binary image plates, and each binary plate image is XOR by 2D Wolfram key and result combat to give the encrypted color image. After performing the XOR operation on the binary plate images, first the binary image plates will be combining to obtained three red, green, and blue components, then these components will be combined, and then the cipher color image will be obtained. Figure 4 shows some 2D Wolfram cellular automata used in the diffusion process.

5. Experimental results

In the present study, MATLAB software has been used to run the proposed encryption and decryption process on the digital color image by the system with 2.60GHz CPU specifications, 16GB of RAM, and Windows 10 operating system.

5.1. Histogram analysis

The histogram shows how the pixels are distributed on the gray level [16].The histogram shows how many pixels of the image are on each gray level from 0 to 255. Gray level distribution is one of the most important features of any image encryption system [11].Histogram analysis of the original and encrypted images is a test method for the encrypted image. A good encryption algorithm should mixture the image so that its visual features are not easily recognizable. Also, by comparing the cipher image with the plain image, no information should be observed in the cipher image, even after extreme changes in the brightness of the pixels of the plain image, the plain image, and the

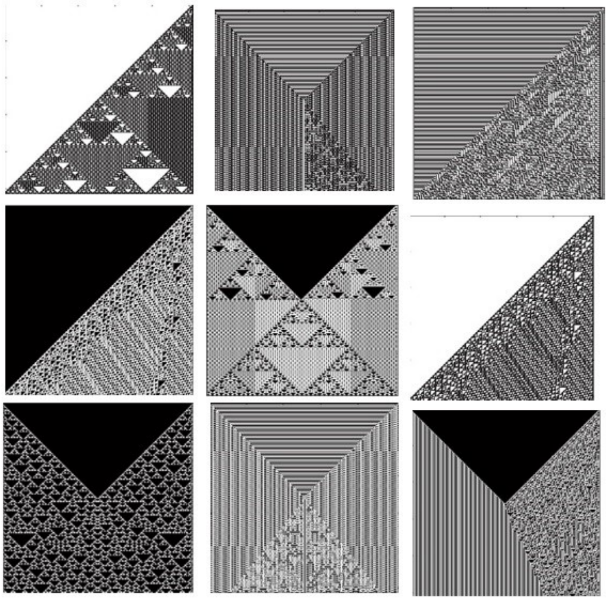

Figure 4: 2D Wolfram cellular automata [14]

cipher image should be visually distinct. It is worth noting that since the result of the visual test is different for different viewers, it cannot be considered scientifically valid, so histogram analysis is used. Histogram analysis describes how the pixels in the image are distributed using the number of observations of each light intensity, and to prevent information leakage and statistical attacks, it is important to ensure that the original image and the encrypted image have no statistical similarity. The image encryption algorithm should be such that it does not provide any pieces of evidence for the statistical attack. The histogram shows the number of pixels on each gray level for an image. In general, the more uniform the hand-held histogram in the proposed algorithm, the less likely it is that statistical attacks will occur on it. In other words, the relatively uniform distribution of image histograms can indicate the good quality of the encryption method. The main image histogram of the Lena is shown in 512 × 512 grayscale and the cryptogram of its encrypted image is shown using the proposed method in Figure 5. The examination of the results shows that the histogram of the cipher image has an almost uniform distribution, which indicates that encryption in the proposed method has good security.

5.2. Entropy information

The information entropy was first introduced by Shannon in 1949. Shannon identified entropy as a measure of the amount of information in a source. The concept of entropy is related to the degree of disorder and uncertainty in a physical system. The entropy of an image's information can indicate the distribution of the gray level of that image. For a color image with 256 gray level in the RGB components, assuming that all gray values are equal, the entropy should be equal to 8. It can be completely resistant to entropy attacks [15].The entropy of an image is an estimate of its randomness, which is commonly used to measure the sharpness of histogram peaks. Information entropy is an important indicator of randomness that is calculated by Equation (5.1).

$$H(s) = \sum_{i=0}^{2^{N-1}} p(s_i) \log_2 \frac{1}{p(s_i)} \tag{5.1}$$

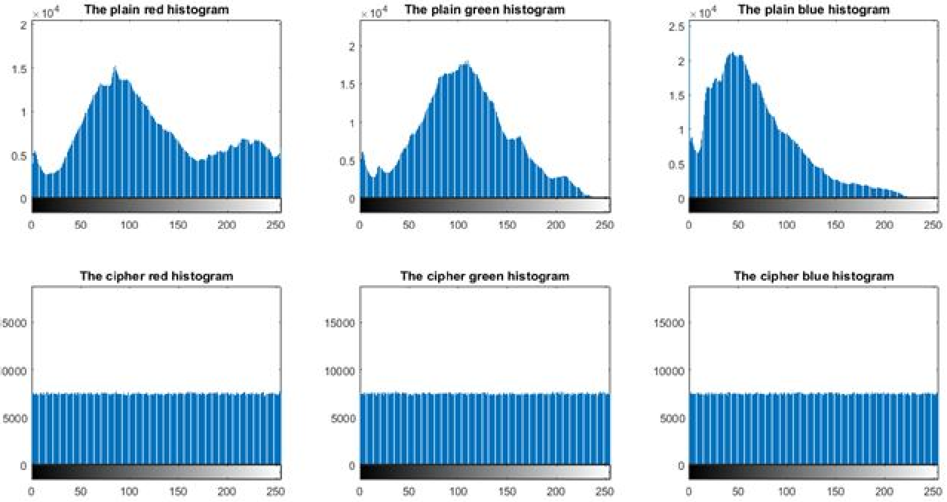

Figure 5: Histogram of the plain and the cipher images

Where $p(s_i)$ specifies the probability of the symbol s_i. For a random source of the 2^L symbol, the entropy must be L. Consider the plain or cipher image with 256 gray level in each component, in the other word, the pixel data has 2^8 possible values, the desired entropy of the cipher image should be 8. The entropy information of proposed RGB cipher components are equal to 7.994, 7.993, 7.992.

5.3. Sensitivity analysis

A good encryption system must be sensitive to the key and image. So in this section, we test the sensitivity to the key using two indicators: NPCR, or the rate of change in the number of pixels, and UACI, or the intensity of change by the unit. UACI and NCPR evaluation criteria are standard expectations for calculating the similarity of the two images. The more these two, the better the encryption algorithm. These two indicators are defined according to the following equations [7, 8, 12]

$$NCPR = \frac{\sum_{ij} D(i,j)}{WH} \times 100 \tag{5.2}$$

$$UACI == \frac{1}{WH} \times \left[\sum_{ij} |c_1(i,j) - c_2(i,j)| \right] \times 100 \tag{5.3}$$

Where c_1 and c_2 are two cipher images with same size $W \times H$. $D(i,j)$ is a binary image if $c_1(i,j) \neq c_2(i,j)$ then $D(i,j) = 1$ else $D(i,j) = 0$ The NCPR and UACI of the proposed method are equal to 99.56% and 34.45% respectively.

5.4. Adjacency pixels correlation analysis

The adjacency pixels correlation coefficient is one of the evaluation criteria in statistical analysis. The lower the correlation of neighboring pixels in the encrypted image, the better the performance of the algorithm. The following equation is used to study the correlation of pixels in horizontal, vertical, and diagonal directions.

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5.4}$$

$$Cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \tag{5.5}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad E(y) = \frac{1}{N}\sum_{i=1}^{N} y_i \tag{5.6}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x)) \quad D(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - E(y)) \tag{5.7}$$

Figure 6 shows the pixels adjacency correlation of red, green and blue spectrums of plain and cipher images

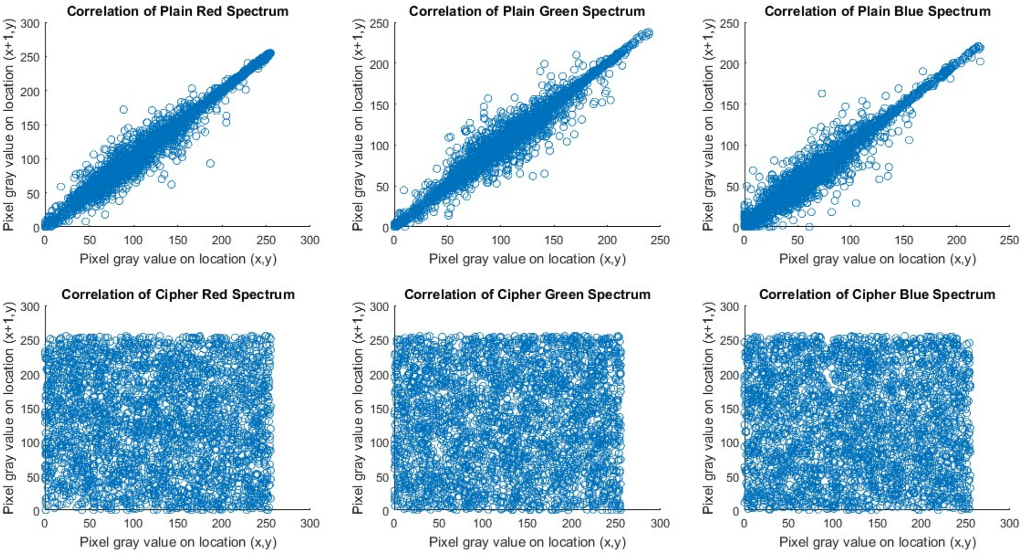

Figure 6: The pixels adjacency correlation of red, green and blue spectrums of plain and cipher images

6. Conclusion

Maintaining security and ensuring the accuracy of images in the computer world is essential, because the images that are transmitted may have military, commercial, medical, and other uses. Encryption can be a way to prevent unauthorized access to images. But video data has a large volume and high correlation between high points, and their encryption with traditional methods is inefficient and time-consuming. Sometimes, images such as colorlessness, image uniformity, and data compression are required for image transfer. It is very difficult to meet these needs when combined with security needs. The present study examines digital color image encryption using cellular automation and the 3D modular chaotic map, which also uses permutation and diffusion to improve standard metrics. The general process of the proposed method includes permutation and diffusion steps. Due to the intrinsic properties of cellular automata such as simple structure, random operation, complex behavior, and highly ambiguous parallelization, it can be used as a useful tool for encrypting digital images well and with high quality by combining other tests.

References

[1] B.A. Forouzan, Cryptography & Network Security, McGraw-Hill, Inc., 2007.

[2] A. Broumandnia, Designing digital image encryption using 2D and 3D reversible modular chaotic maps, Journal of Information Security and Applications 47 (2019): 188-198. https://doi.org/10.1016/j.jisa.2019.05.004

[3] A. Broumandnia, The 3D modular chaotic map to digital color image encryption. Future Generation Computer Systems 99 (2019): 489-499. https://doi.org/10.1016/j.future.2019.04.005

[4] R. Guesmi, M.A.B. Farah, A. Kachouri, and M. Samet, A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2, Nonlinear Dynamics 83.3 (2016): 1123-1136. https://doi.org/10.1007/s11071-015-2392-7

[5] R. Guesmi, M.A.B. Farah, A. Kachouri, and M. Samet, Hash key-based image encryption using crossover operator and chaos Multimedia tools and applications 75.8 (2016): 4753-4769. https://doi.org/10.1007/s11042-015-2501-0

[6] J. Jun, An image encryption based on elementary cellular automata, Optics and Lasers in Engineering 50.12 (2012): 1836-1843. https://doi.org/http://dx.doi.org/10.1016/j.optlaseng.2012.06.002

[7] M. Kumar, A. Iqbal, and P. Kumar, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie-Hellman cryptography, Signal Processing 125 (2016): 187-202. https://doi.org/10.1016/j.sigpro.2016.01.017

[8] M. Kumar, G. Sathish, M. Alphonse, and R.A.M. Lahcen, A new RGB image encryption using generalized heat equation associated with generalized Vigen è re-type table over symmetric group, Multimedia Tools and Applications 78.19 (2019): 28025-28061. https://doi.org/10.1007/s11042-019-07893-7

[9] K.A.K. Patro, and B. Acharya, An efficient colour image encryption scheme based on 1-D chaotic maps, Journal of Information Security and Applications 46 (2019): 23-41. https://doi.org/10.1016/j.jisa.2019.02.006

[10] M. Kumari, S. Gupta, and P. Sardana, A Survey of Image Encryption Algorithms, 3D Research 8.4 (2017): 37. https://doi.org/10.1007/s13319-017-0148-5

[11] H. Liu, A. Kadir, and J. Liu, Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system, Optics and Lasers in Engineering 122 (2019): 123-133. https://doi.org/10.1016/j.optlaseng.2019.05.027

[12] M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez, and O.A. Del Campo, A RGB image encryption algorithm based on total plain image characteristics and chaos, Signal Processing 109 (2015): 119-131. https://doi.org/10.1016/j.sigpro.2014.10.033

[13] W. Stalling, Cryptography and Network Security: Principles and Practice 7th Edition, Pearson press, 2018.

[14] S. Wolfram, Statistical mechanics of cellular automata, Reviews of modern physics 55.3 (1983): 601. https://doi.org/https://doi.org/10.1103/RevModPhys.55.601

[15] A. Vaish, and M. Kumar, Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain, Optik 145 (2017): 273-283. https://doi.org/10.1016/j.ijleo.2017.07.041

[16] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan, and P. Natarajan, Local Shannon entropy measure with statistical tests for image randomness, Information Sciences 222 (2013): 323-342. https://doi.org/10.1016/j.ins.2012.07.049