Indian Journal of Science and Technology, *Vol 12(13), DOI: 10.17485/ijst/2019/v12i13/142823 April 2019*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Generating Recursive Sequence in Image Encryption using a New Method based on the Genetic Algorithm

Seyed Shahabeddin Moafimadani and Chunming Tang*

School of Mathematics and Information Science in Guangzhou University, Guangzhou, China;
madanishahab1368@yahoo.com, ctang@gzhu.edu.cn

Abstract

Objective: To present a new method for generating a recursive sequence in image encryption using the genetic algorithm. **Methods:** In order to accomplish these goals in this study, the coefficients of the recurrence relation are calculated by the genetic algorithm taking into account a generic form for the recurrence relation and the definition of a proper fitness function, so that the resulting sequence has the optimal efficiency for image encryption. **Findings:** With the implementation of the algorithm, the results obtained from values UACI, NPCR, MAE, the fitness function, and Correlation, it is seen that the proposed method in this paper is more effective than old methods. **Application:** In order to achieve these results, at each stage of the implementation of the genetic algorithm, using a chromosome gene, a 2D time sequence is generated, and this sequence is used to scramble the image.

Keywords: Chromosome Gene, Genetic Algorithm, Image Encryption, Recursive Sequence, 2D Time Sequence

1. Introduction

In recent years, the use of e-mail, video conferencing, and multimedia messages has been widely disseminated through the Internet through private and public information. Also, the development of computer networks and digital multimedia services has led to a comprehensive transmission of images, video and multimedia data. Considering the wide range of Visual Surveillance Systems in important areas such as airports, commercial centers, banks, schools and military strategic locations, videos and images with respect to security tips are stored and stored at destination after transfer. Therefore, providing a secure multimedia data for individuals, companies and governments is an urgent need. Encryption is an effective way of protecting multimedia data, which is done by transferring multimedia data into a non-identifiable format in the network context. Obviously, the encryption of multimedia data is done in such a way that unauthorized users do not gain access to the contents of the main data of the cached data. Due to the high volume of video and video data, as well as the specific features of the image, the use of classic encryption algorithms, such as RSA, DES is inefficient in cryptography because these algorithms are time-consuming and cannot be used in real-time systems. Therefore, for image data, special encryption methods have been developed with the title of Image Cryptography[1-6].

Image Cryptography is done with two techniques of substitution and Scrambling. In the technique of replacing image pixels, mathematical calculations are replaced with other reciprocating values, but in the Scrambling technique, the location of the pixels of the image is changed using mathematical relations[7].

It should be kept in mind that in ciphering the pixel displacement image should be made in such a way that the cached image does not convey any information from the original image to the unauthorized user. Image chaos is one of the most commonly used cryptographic methods for secure image transmission. Image Scrambling is also used as a preprocessor to hide the image[8].

*Author for correspondence

Image Scrambling is done in two areas of Spatial Domain and Frequency Domain. Scrambling in the field of location is performed by direct displacement of the brightness levels of the original image pixels. For image Scrambling in the frequency domain, the image is first transmitted with a proper conversion to the frequency domain, and then the encoding function is applied to the image conversion. In the end, calculating the inverse of the conversion, the image is transferred to the domain of the location[9].

In recent years, several methods have been proposed for image Scrambling, in which among these algorithms, chaos-based methods have been shown to be effective. Chaotic systems have nonlinear dynamic behavior. These systems are pseudo-random and non-symmetrical and sensitive to the initial state. The natural result of sensitivity to the initial condition is the diffusion feature that is appropriate for image encryption[9].

Also, because of the proper key space, chaos systems are resistant to a comprehensive attack[2]. It should be noted that chaos systems, in addition to encryption in communications, are also used for optimization, control and image processing[10-12].

In 1989, Matthews introduced a discrete dynamic system for image encryption[13]. He used one-dimensional chaos to produce a sequence of pseudo-accidental numbers. In 1994, Biance used the Logistic chaotic system to encrypt the image, which achieved good security[13].

In used two-dimensional chaos sequences to encrypt the image[9]. In used Lu's chaos sequence to encrypt the image. Their algorithm has a large key space and is resistant to attacks[14]. In used the chaos sequence to encrypt the image[15]. His cryptography algorithm was easy and secure. In 2010, Wang et. al. used the Hyper Chaoticto encrypt the image, which had an appropriate security and security algorithm[13].

In all references, the use of time sequences in mathematics is used to encrypt the image, and at the end of the performance of the algorithms provided by the standard similarity measures are evaluated. In the cryptography of the image due to the complexity of the present, the choice of the sequence type and the initial values for the appropriate criteria cannot be analyzed analytically. In this paper, using a genetic algorithm is a suitable sequence for image encryption. To find the sequence, a general form of recurrence relation is first considered and using the genetic algorithm, the coefficients are calculated for this relationship. By the proposed method, by defining a suitable fitness function, the important criteria of image encryption are optimally met at the same time.

The structure of the paper is as follows: In the second section, the two-dimensional time sequence is introduced; in the third section, the genetic algorithm is introduced, and in the fourth part the proposed method is expressed. The results of the tests and conclusions are presented in the final section.

2. 2D Time Sequence

The general form of a 2D time sequence is defined as equations (1) and (2):

$$x_{n+1} = a_1 + a_2 x_n + a_3 x_n^2 + a_4 y_n + a_5 y_n^2 + a_6 x_n y_n \quad (1)$$

$$y_{n+1} = a_7 + a_8 x_n + a_9 x_n^2 + a_{10} y_n + a_{11} y_n^2 + a_{12} x_n y_n \quad (2)$$

In these relationships, the sequence value at any moment depends on the values of the instantaneous moment and the first and second effects of the factor and the nonlinear factor multiplication of the two components are considered. In this sequence, other random values can be generated by specifying the coefficients of the sequence and the initial values of x_0 and y_0. Obviously, by selecting a_2. in the interval [0,4] and $a_3 = -a_2$ this sequence turns into a logistic sequence[16]. And by choice $a_4 = 1.55$, $a_5 = -1.3, a_8 = -1.1, a_{10} = 0.1$, this sequence transforms into a Hyper Chaotic 2D sequence.

3. Genetic Algorithm

The main idea of the genetic algorithm is derived from Darwinian evolutionary theory. Darwin's theory states that those natural traits that are more compatible with natural laws have a greater chance of survival. It is noteworthy that Darwin's evolutionary theory has no definitive and analytical proof, but has been empirically and statistically confirmed. New people of a community are born through fertility. The survival of a person in a new generation dependon the specific chromosomal composition. In reproductive stages, there may be mutations in the characteristics of a new generation person, resulting in an inventory of excellent characteristics and high adaptability. In reproductive processes, genera are allowed to be reproduced in each generation and undesir-

able species will gradually disappear and new generations evolve over time. The Genetic Algorithm was presented. This algorithm is in the category of randomization algorithms and is suitable for optimizing complex problems with unknown search space. The genetic algorithm is summarized.

- At the beginning of the algorithm, a random set of answer candidates, called primary populations, is generated and replaced by new candidates in each generation.
- In each replication, the population algorithm is evaluated by the fitness function. Then, some of the best candidates will be selected for the next generation and will form the new population.
- A number of these populations are being used by genetic operators such as Crossover and Mutation to produce new offspring.
- The steps above will continue to achieve an appropriate response. The steps proposed for implementing the genetic algorithm are presented in the form of a flowchart in Figure 1.

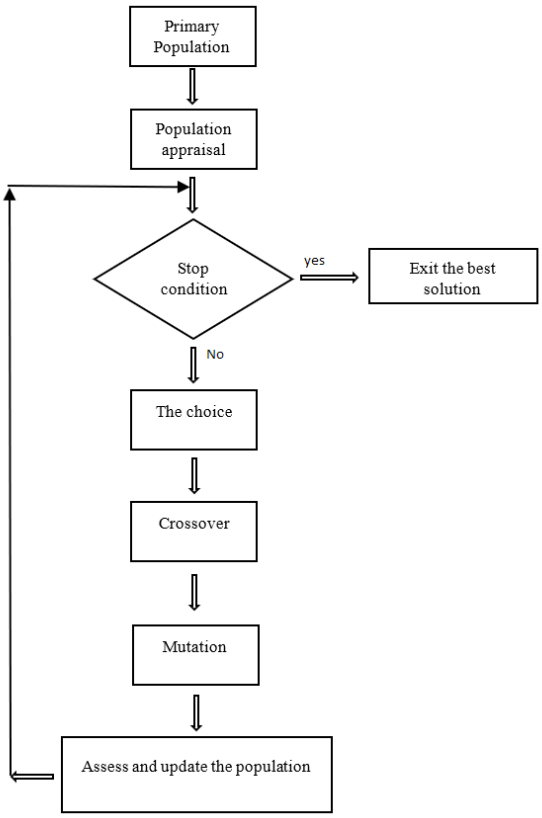


Figure 1. Flowchart of Genetic Algorithm.

4. Proposed Method

The proposed method in this study consists of two sections of the genetic algorithm for finding the proper sequence and image scrambling algorithm. First, the 2D time sequence coefficients are calculated and then they obtained coefficients are used to scrambling the image. In this section, some of the genetic algorithms and their allocation to the problem parameters are expressed. To the constructive elements of a chromosome, the gene is said to be called any 2D time sequence of a gene in this case.

In the genetic algorithm, a chromosome is a set of genes that is considered in the proposed method of twelve 2D time sequence coefficients of a chromosome. Each gene of the chromosome is replaced by the generic production of the bicameral time sequence, and then a two-dimensional sequence is generated. The image scrambling is performed using this sequence and the fitness function is calculated using equation (3).

Provides a new method for generating a recursive sequence in image cryptography using genetic algorithm

$$Fitness\_Function = \alpha_1 UACI + \alpha_2 NPCR + \alpha_3 MAE + \alpha_4 r_{xy}(horizontal) + \alpha_5 r_{xy}(vertical) + \alpha_6 r_{xy}(diameter) \quad (3)$$

In this regard, to measure the fitness functions of correlation functions, MAE (Mean Absolute Error), NPCR (Number of Pixel Change Rate), UACI (Unified Average Changing Intensity) used. Obviously, the functions mentioned are standard functions for calculating the similarity of two images[13]. The higher the values MAE, NPCR and UACI, the more efficient the encryption algorithm. Image pixels that are in the vicinity of each other have a certain correlation. By scrambling the image, the pixels that appear next to each other are different parts of the image, in which case the degree of correlation between neighboring pixels is sharply reduced. Therefore, in the proposed fitness function, the lower the correlation factor, the performance of the algorithm is preferable. Given that four criteria are not within a range, coefficients are used to map the criteria in a range. These coefficients can be increased or decreased according to the importance of each criterion.

The correlation criterion is expressed in equation (4). It should be noted that in the fitness function the correlation criterion is used in three horizontal, vertical and diagonal directions separately[17].

$$r_{xy} = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

$$Cov(x,y) = \frac{1}{M\times N}\sum_{j=1}^{M\times N}\left(\left(x_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}x_j\right)\left(y_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}y_j\right)\right). \quad (5)$$

$$D(x) = \frac{1}{M\times N}\sum_{j=1}^{M\times N}\left(x_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}x_j\right)^2 \quad (6)$$

$$D(y) = \frac{1}{M\times N}\sum_{j=1}^{M\times N}\left(y_j - \frac{1}{M\times N}\sum_{j=1}^{M\times N}y_j\right)^2 \quad (7)$$

In these equations, $x\,and\,y$ is the two-pixel brightness of the adcent in the image and $M\times N$ are pixels of the image.

Equation (8) is the MAE calculation, which is the mean absolute error[18].

$$MAE = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left|C_{ij} - P_{ij}\right| \quad (8)$$

Where, C_{ij}, P_{ij} are the pixel values of the original image and image. Equation (9) relates to the calculation of NPCR, which is the rate of changed pixels of the codec for a change bit in the original image[19].

$$NPCR = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}D(i,j)}{M\times N}\times 100\% \quad (9)$$

$$D(i,j) = \begin{cases} 0 & if \quad C(i,j) = \overline{c}(i,j) \\ 1 & if \quad C(i,j) \neq \overline{c}(i,j) \end{cases} \quad (10)$$

Where $C\,and\,\overline{c}$ are two encrypted images in which their respective original images are different in one pixel. The UACI is calculated from equation (11)[19]:

$$UACI = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[\frac{\left|C(i,j) - \overline{c}(i,j)\right|}{255}\right]\times 100\% \quad (11)$$

4.1 Image Scrambling Algorithm

As described in the previous section, to image encryption with the image scrambling technique, the image pixels of the image are replaced. In this article, the scrambling of the pixels of a row (column) is performed by another row (column) of the image[9]. The row (column) used for scrambling is selected using a 2D time sequence.

The scrambling algorithm is as follows:

Suppose A, B are vectors and vector B is supposed to be scramble by vector A. First, the vector A is arranged in ascending order and vector A' is obtained. Then each component from vector B is moved to a location in the vector A' in that location in vector A.

To clarify, the scrambling is described using an example. In the example below, vector A is torn with six elements by vector B.

$$A = (0.53, 0.99, 0.03, 0.42, 0.12, 0.97)$$

$$A' = (0.03, 0.12, 0.42, 0.53, 0.97, 0.99)$$

$$P = (354162)$$

$$B = (0.35, 0.91, 0.31, 0.85, 0.49, 0.99)$$

$$B' = (0.85, 0.99, 0.35, 0.31, 0.91, 0.49)$$

Vector P is the main place of vector components A' in vector A. And the vector B' is chaotic vector B.

4.2 Sequence Production Algorithm and Image Scrambling

At each stage of the implementation of the genetic algorithm, using a chromosome gene, a 2D time sequence is generated, and this sequence is used to scramble the image. The proposed algorithm is presented step-by-step in the following section.

- A 2D chaos system and initial values (x_0, y_0) are selected, which are used as the key to the encryption algorithm.
- In this algorithm, first the image of the row to the row and then the column to the column are scrambled. After producing the pair (x_1, y_1), the value x_1 is mapped to $0 \le x_1^{'} \le M$ and the value y_1 is mapped at distance of $0 \le y_1^{'} \le N$. It should be noted that if the value of $x_1^{'}$ is equal to one (equal to the line to be scramble now), or $y_1^{'}$ is equal to one. (Equal to the column that is now

to be scramble), the (x_1, y_1) pair is deleted and calculates the next pair of sequence is repeated.

Then, using the proposed algorithm, the x-the row is used to scramble the first row and the y-th column to scramble the first column.

- The next pairs of sequence are produced same as the previous stage and used to scrambling for next rows and columns.

It should be noted that the proposed algorithm can be repeated for more image scrambling. To do this, you must create the desired sequence to the desired number. The algorithm is repeated from the beginning of the image when it reaches the last row and the last column of the image.

After executing the above steps, the encrypted image is obtained. The encrypted image is sent from the sender to the receiver. The receiver receives the encrypted image and must retrieve the original image to use it. Recovering the original image from a cipher image is a reversal of the scramble process; with the exception that the chaos sequence should be used in reverse order.

To rebuild the original image of the encrypted image, the following steps are taken:

- First, the chaos sequence is generated to the required number, that the condition of the sequence is the same as the encryption step.
- The sequence is used from the end to the first; in other words, the last couple is used to scramble the row and the last column of the image, so that first the last column and then the last row return to their first state. This will continue to return to all pixels of the image.

5. Experiment Results

In this section, we will experiment the proposed algorithm for the gray Cat image. The parameters of the genetic algorithm including the number of primary populations, the probability of crossover, the probability of mutation, and the number of replications of the algorithm (stop condition) are considered respectively 55, 0.8, 0.02, and 4000 respectively. Also, in experiments, the fitness function coefficients were selected as values -8, -2, -3, +100, +100, and +100, respectively.

To investigate the convergence of the genetic algorithm, the fitness function curve has been used in terms of the number of replications. In Figure 2, the fitness function is represented by the number of repetitions. The vertical axis is the best cost per repetition and the horizontal axis is the number of replicas of the genetic algorithm. As can be seen, the genetic algorithm repeats this amount. This decrease indicates how the coefficients of the recurrence relation are changed in such a way that at each repetition of the algorithm it approaches a more appropriate answer.

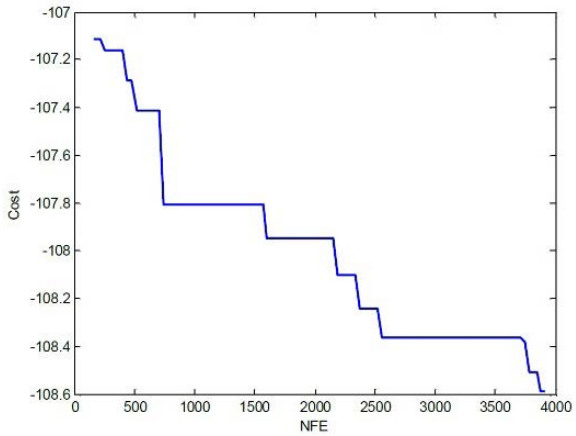
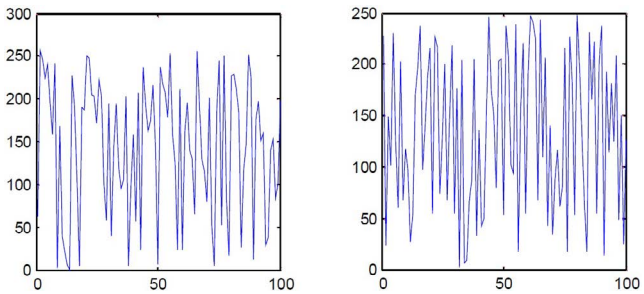


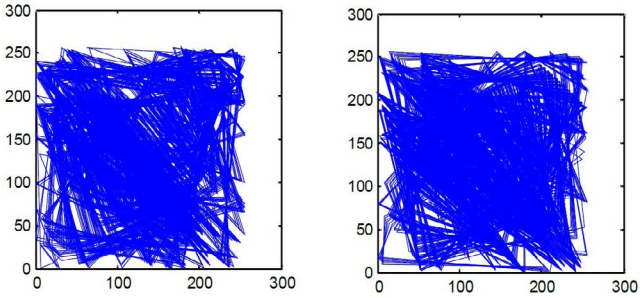
Figure 2. The best cost in terms of the performance of the fitness function.



(a) (b)

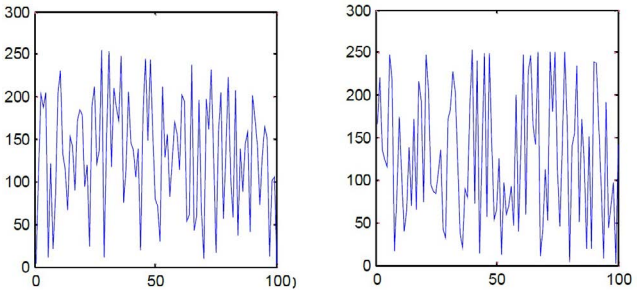
Figure 3. The genetic algorithm sequence values of the in terms of the number of repetitions; (a): Sequence values in x direction, (b): Sequence values in y direction.

To compare the 2D time sequence obtained from the genetic algorithm, three other sequences are used. These three sequences are: Hyper Chaotic Sequence[9], Logistic[16] and TD-ERCS[20]. In this section, the sequence diagram is represented by the number of repetitions and the chart of the number of sequence numbers irregularities. These two charts are plotted for each of the four sequences in Figures 3 to 10.



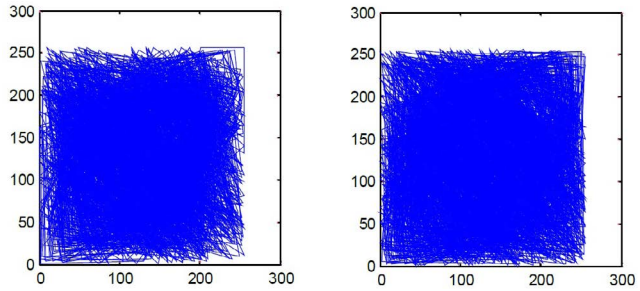
(a) (b)

Figure 4. Behavioral Pattern of Genetic Algorithm Sequence; (a): Behavioral pattern in x direction, (b): Behavioral pattern in y direction.



(a) (b)

Figure 5. Hyper chaotic sequence values in terms of the number of repetitions; (a): Sequence values in x direction, (b): Sequence values in y direction.



(a) (b)

Figure 6. Hyper chaotic sequence behavior pattern; (a): Behavioral pattern in x direction, (b): Behavioral pattern in y direction.

The generated sequence behavior by time-based genetic algorithm is shown in Figure 3. It can be seen that the behavior of the generated sequence is random, and this sequence does not have any periodic order.

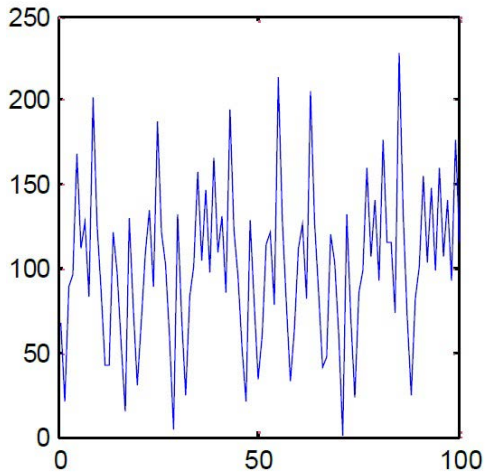


Figure 7. 1D Logistic sequence values in terms of the number of repetitions.

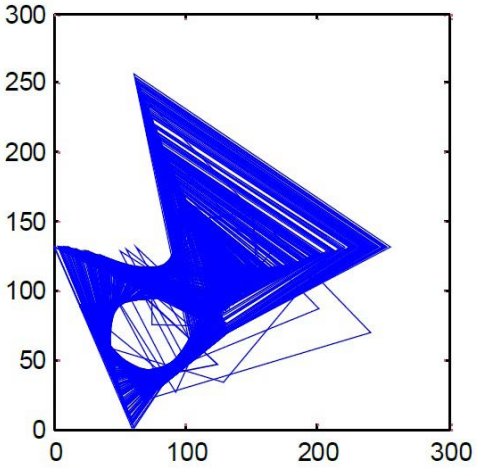
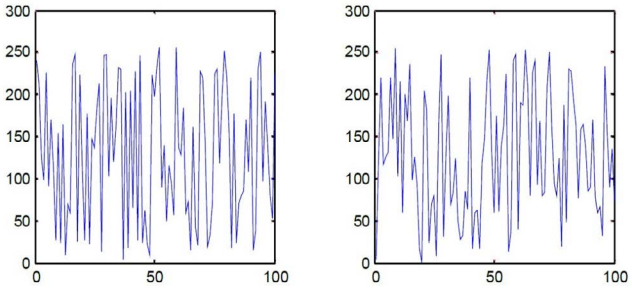


Figure 8. 1D logistics sequence behavioral pattern.



(a) (b)

Figure 9. The values of the sequence TD-ERCS in terms of the number of repetitions; (a): Sequence values in x direction, (b): Sequence values in y direction.

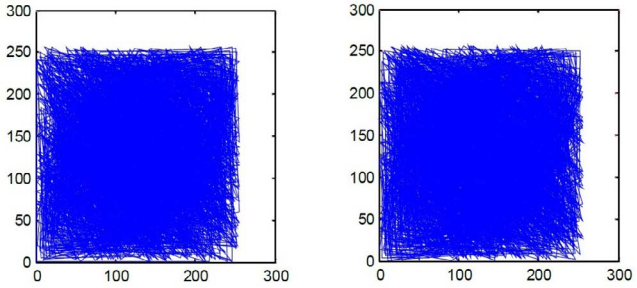


Figure 10. Behavioral pattern of TD-ERCS sequence; (a): Behavioral pattern in x direction, (b): Behavioral pattern in y direction.

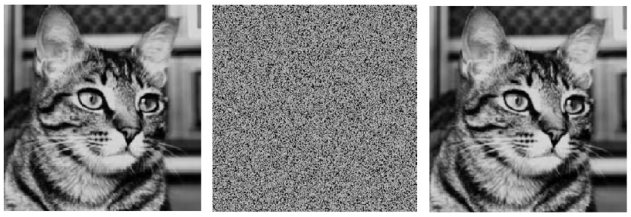


Figure 11. Encryption results with genetic algorithm sequence.

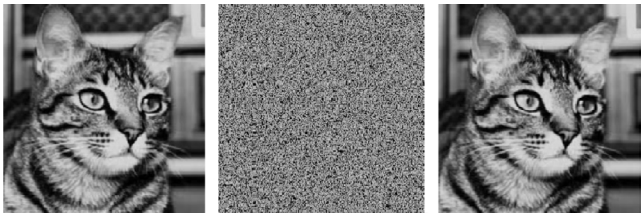


Figure 12. The results of encryption with hyper chaotic sequence.

Also, to illustrate the non-periodicity of production couples and the disorder of the 2D sequence, Figure 4 is used. This behavior is shown in the following figures for the other three sequences.

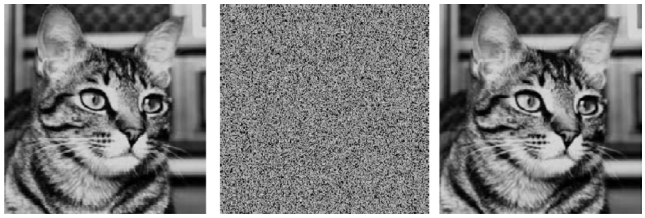


Figure 13. The results of encryption with the logistics sequence.

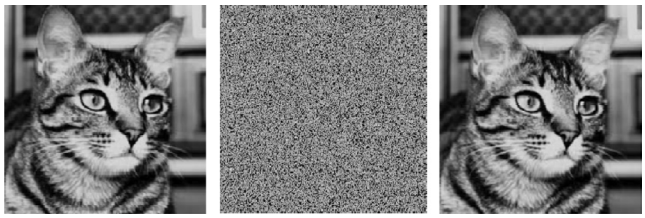


Figure 14. The results of encryption with TD-ERCS sequence.

In Figures 11 to 14, the results of image encryption with four sequences of genetic algorithms, hyper chaos, logistics and TD-ERCS are observation. As you can see, each sequence has been able to scramble the image well.

Comparing the encrypted image of these four sequences is not possible visually, and therefore numerical criteria for comparison are used. The value obtained from the evaluation functions and also the value of the fitness function for the four sequences is given in Table 1.

These criteria include UACI, NPCR, MAE and correlation in horizontal, vertical and diagonal directions. As seen from the table, the values of the evaluation criteria and the fitness function for the sequence of the genetic algorithm are better than the other sequences.

The values of the correlation function in three horizontal, vertical and diagonal directions for the plain image and cipher image with four different sequences are given in Table 2. These values indicate that the genetic algorithm performs better than other sequences.

Table 1. The values of the evaluation functions and the fitness function for the four desired sequences

The name of the evaluation function	UACI	NPCR	MAE	The value of the fitness function
Genetic algorithm sequence	13.2673	49.649	33.912	-107.4577
Hyper chaotic sequence[9]	13.2441	49.2416	33.6855	-104.7082
Logistics sequence[16]	13.2354	49.2874	33.6869	-105.651
TD-ERCS sequence[20]	13.2424	49.5926	33.705	106.4437

Table 2. Correlation values in horizontal, vertical and diagonal directions

Correlation function	Horizontal	Vertical	Diagonal
Plain image	0.9577	0.9574	0.9382
Cipher image (genetic algorithm sequence)	0.6648	0.6645	0.6648
Cipher image (hyper chaotic sequence)	0.6683	0.6714	0.671
Cipher image (Logistics sequence)	0.6667	0.6661	0.6672
Cipher image (TD-ERCS sequence)	0.6695	0.6678	0.6663

6. Conclusion

Digital images, due to their high dependence on neighboring pixel values and high data volumes, have special cryptographic algorithms. One of these algorithms is the scrambling of image pixels, which cannot be understood by the user as a result of the image content. In most of these methods, the intersection is performed by a time sequence. Each sequence is generated with a recursive relationship and predetermined coefficients and used to encrypt all images. Selection of the sequence coefficients so that the sequence is good for image encryption because of the lack of direct relation between the coefficients of the sequence and the encoded image. In this study, taking into account a recursive general sequence, using the genetic algorithm and defining a proper fitness function, the coefficients of the sequence were calculated in such a way that the generated sequence satisfies the criteria for the cryptographic evaluation of the image.

It is worth noting that the algorithm must be restarted in order to obtain the recursive sequence coefficients for the encryption of each image. This issue, as well as the timing of the genetic algorithm, can be counted from the limitations of the proposed method. The results of the experiments showed that the chaotic sequence obtained from the genetic algorithm was more efficient than some of the existing sequences.

7. Reference

1. Corron NJ, Reed BR, Blakely JN, Myneni K, Pethel SD. Chaotic scrambling for wireless analog video. IEEE Southeastcon. 2009; p. 38-43. https://doi.org/10.1109/SECON.2009.5174046
2. Pareek N, Patidar V, Sud K. Image encryption using chaotic logistic map. Image and Vision Computing. 2006; 24(9):934-9. https://doi.org/10.1016/j.imavis.2006.02.021
3. Kanso A, Ghebleh M. A novel image encryption algorithm based on a 3D chaotic map. Communications in Nonlinear Science and Numerical Simulation. 2012; 17(7):2943-59. https://doi.org/10.1016/j.cnsns.2011.11.030
4. Wang X, Zhao J. An improved key agreement protocol based on chaos. Communications in Nonlinear Science and Numerical Simulation. 2010; 15(12):4052-7. https://doi.org/10.1016/j.cnsns.2010.02.014
5. Hua Z, Zhou Y, Huang H. Cosine-transform-based chaotic system for image encryption. Information Sciences. 2019; 480:403-19. https://doi.org/10.1016/j.ins.2018.12.048
6. Cavusoglu U, Kacar S, Pehlivan I, Zengin A. Secure image encryption algorithm design using a novel chaos based S-Box. Chaos. Solitons & Fractals. 2017; 95:92-101. https://doi.org/10.1016/j.chaos.2016.12.018
7. Xiangdong L, Junxing Z, Jinhai Z, Xiqin H. Image scrambling algorithm based on chaos theory and sorting transformation. International Journal of Computer Science and Network Security. 2008; 8(1):64-8.
8. Zhang H. A new image scrambling algorithm. IEEE International Conference on Machine Learning and Cybernetics. 2008; 2(2):1088-99.
9. Gu G, Han G. The application of chaos and DWT in image scrambling. International Conference on Machine Learning and Cybernetics. 2006; p. 3729-33. https://doi.org/10.1109/ICMLC.2006.258635
10. Alatas B. Chaotic bee colony algorithms for global numerical optimization. Expert Systems with Applications. 2010; 37(8):5682-7. https://doi.org/10.1016/j.eswa.2010.02.042
11. Aghababa MP, Haghighi AR, Roohi M. Stabilisation of unknown fractional-order chaotic systems: an adaptive switching control strategy with application to power systems. IET Generation, Transmission & Distribution. 2015; 9(14):1883-93. https://doi.org/10.1049/iet-gtd.2015.0038
12. Roohi M, Mirjalily G, Sadeghi MT. Face Detection Using a Modified SVM-Based Classifier. International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007). 2007; 2:354-60. https://doi.org/10.1109/ICCIMA.2007.243
13. Wang P, Gao H, Cheng M, Ma X. A new image encryption algorithm based on hyper chaotic mapping. IEEE International Conference on Computer Application and System Modeling. 2010; 5:425-8.
14. Hong-E R, Jian Z, Xing-Jian W, Zhen-Wei S. Block sampling algorithm of image encryption based on chaotic scrambling. IEEE International Conference on Computational Intelligence and Security. 2007; p. 773-6. https://doi.org/10.1109/CISW.2007.4425609

15. Yanling W. Image scrambling method based on chaotic sequences and mapping. IEEE International Workshop Education Technology and Computer Science. 2010; 3:457.
16. Goldberg D, Holland J. Genetic algorithms and machine learning. Machine learning. 1998; 3(2):95-9.
17. Jolfaei A, Mirghadri A. Survey: image encryption using Salsa20. International Journal of Computer Science Issues. 2010; 7(5):213-20.
18. Ye R, Zhao H. An efficient chaos-based image encryption scheme using affine modular maps. International Journal of Computer Network and Information Security. 2012; 4(7):41-5. https://doi.org/10.5815/ijcnis.2012.07.05
19. Feng-Ying H, Cong-Xu Z. An novel chaotic image encryption algorithm based on tangent delay ellipse reflecting cavity map system. Procedia Engineering. 2011; 23:186-91. https://doi.org/10.1016/j.proeng.2011.11.2487
20. Wei X, Guo L, Zhang Q, Zhang J, Lian S. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. Journal of Systems and Software. 2012; 85(2):290-9. https://doi.org/10.1016/j.jss.2011.08.017