International Journal of Engineering

Journal Homepage: www.ije.ir

Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map

K. S. Khalaf, M. A. Sharif*, M. S. Wahhab

Electronic and Control Engineering Techniques Department, Technical Engineering College – Kirkuk, Northern Technical University, Iraq

P A P E R I N F O

Paper history:
Received 22 August 2021
Received in revised form 05 July 2022
Accepted 06 July 2022

Keywords:
Chaotic Map
Communication
Grasshopper Optimization
Image Encryption Optimization
Image Pixel Correlation
Security

A B S T R A C T

Encryption is very important to protect sensitive data, especially images, from any illegal access and infringement. This research is presented to provide an image encryption optimization method for communication based on image security. This method uses the grasshopper optimization algorithm to perform optimal encryption and irregular logical mapping. Initially, this approach creates multiple encrypted images and a chaotic map, in which the session key for the initial conditions of the map depends on a simple suspended image. After that, the encrypted images work as an initial and particles set for optimization through the grasshopper optimization algorithm. The optimized encoded image with the correlation coefficient of the continuous pixels is expressed as a function of proportion. The results from Matlab simulation of the proposed encoding method show that the encrypted images are the same, and the adjacent pixels are highly correlated with other outstanding encoding rows, such as planar histogram entropy and effective pixel rate of change average correction strength.

***doi**: 10.5829/ije.2022.35.10a.16*

NOMENCLATURE

DFT	Discrete Fourier Transform	DICOM	Digital Imaging and Communications in Medicine
WDICA	Discrete Weight Imperial Competitive Algorithm	DNA coding	Genetic coding
PSO	Particle Swarm Optimization	GOA	Grasshopper Optimization Algorithm

1. INTRODUCTION

With the expansion of the communication in the computer network technologies, it is easy to access digital images over the network process and use, produce and distribute them further. On the one hand, digital technology brings a lot of convenience to people, but on the other hand, due to the transmission of a lot of video data through non-standard and unreliable channels, issues of confidentiality and privacy are contradictory, and it poses a risk when communicating and gives attackers or illegal users a chance to abuse. Therefore, the security and protection of digital data storage and transfer is more important than ever [1].

In particular, image security helps the application layer protect data sent from unwanted leaks or changes during delivery. There are various ways to protect the personal information of the current image and prevent unauthorized access to the image content. It uses image encryption methods to convert simple images into undetectable hidden formats to ensure airtightness with authenticated end users [2]. In general, two main ways are available to protect digital image or multiple images. The first way by hiding information that includes display, steganography, anonymity, and channel range. In other cases, it is encryption that includes other items such as contract encryption and chaotic encryption [3].

Today, the need for image encryption to securely transmit images over the internet and wireless networks is increasing, with special features such as overloading of digital image data and strong correlation between adjacent pixels, desensitization (i.e. slight variations) to text data. .The characteristics of pixels of the image, it cannot significantly reduce the quality and bulk of the

*Corresponding Author Institutional Email: msharif@ntu.edu.iq
(M. A. Sharif)

Please cite this article as: K. S. Khalaf, M. A. Sharif, M. S. Wahhab, Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map, ***International Journal of Engineering, Transactions A: Basics***, Vol. 35 No. 10, (2022), 1981-1988

data). This is because encryption is slow for large amounts of data and stronger correlation between image pixel, so the implementations of these conventional image encryption algorithms are more complex when using commercial software's. For real-time video encryption, only encryption that does not compromise security and consumes less time at the same time is recommended. Although very slow cryptography sometimes provides improved security, real-time processes have few practical applications [2]. In various encryption algorithms, there are more advantages to chaos encryption technology, and these technologies are represented suitable for empirical use to provide an excellent combinations of high security, speed, complexity, and reasonable computational cost. However, the image encryption method using the chaos system still has many disadvantages, such as destruction of irregularities and low defense against simple text-based attacks. To get rid of these shortcomings and problems, the threats of the security and inefficiencies observed in image encryption can be enhanced by using optimization algorithms.

A chaotic algorithm is a well-defined nonlinear system with a variety of properties, including high-sensitivity self-assertion to initial conditions. The irregular order produced by the irregular map is a quasi-random sequence. Its structure is difficult to analyze, difficult to predict, and very complex. Chaos system can easily improve/ enhance the security of cryptographic systems. Based on the irregular map, the existing cryptographic algorithms can be siplitted into two types: permutation or modification and propagation. The first approach (permutation) algorithm depends on a random order or transformation of the matrix where the pixels positions in the original images. The encryption effect of the permutation algorithm is good, but if you don't change the pixels values, histogram of the encrypted images is created, and the original pictures are copied. So, security can threaten statistical analysis [3].

Irregularity theory is the part of mathematics that governs dynamic systems. In particular, it confirms a high sensitivity to the smallest changes in the initial conditions, thereby dramatically leading to large changes - a reaction commonly refer to the butterfly effects [4]. These minor changes produce the consequences of widespread distortion of such dynamic systems, making them unpredictable in the long run [5]. In addition to the advantages described in the previous section, these chaotic systems are easy to implement and exhibit confusing and spreading behavior in the iterative process of moving cryptosystems. The proposed approach in this paper for the optimal encoding of images due to the correlation of the pixels, using irregular mapping and grasshopper optimization algorithm is proposed. The irregularity function is utilized as the initial way of encryption to create the population, and then the locust optimization approach is utilized to guarantee the progress of the encryption process through the optimization operation. The results obtained in relation to the correlation coefficient of the image in comparisons with other recently introduced images encryption approaches show the optimal results of the proposed method.

2. RELATED WORKS

There are two main methods of chaotic cryptography: Block encryption and sequential encryption. Chaotic encryption methods provide a good balance between security, speed, and flexibility.

With the emergence of a new approach called chaos theory and the clarification of its scientific and theoretical dimensions, today chaos is no longer considered a concept of disorganization and disarray with the negative meaning concept, rather, it refers to the existence of unpredictable and accidental aspects in dynamic phenomena. One of the definitions of this theory states: "Chaos is a kind of regular irregularity or irregular in irregularity [6].

Logistic mapping is the most common and simple chaotic system that is widely used as an example of a low-dimensional chaotic mapping [7]. Logistic mapping involves a second order nonlinear differential equation. The dynamic relationship of this system was first introduced by Robert and defined as follows:

$$u_{n-1} = r \times u_n(1 - u_n) \quad (1)$$

where r is the logistic coefficient. The range of changes r is between zero to 4, but by changing r in this area it gives different properties to the function.

Chaotic tent mapping: Equation (2) represents the tent mapping equation:

$$f(x_n) = x_{n+1} = \begin{cases} \frac{x_n}{p} & 0 \le x_n \le p \\ \frac{1-x_n}{1-p} & p \le x_n \le 1 \end{cases} \quad (2)$$

So that $x_n \in [0,1]$, where p represents one of the control parameters that is very influential in the system behavior and x_0: the initial values. If the control parameters is in the range [0,1], the mapping of the tent becomes chaotic.

Hannon Mapping: A two-dimensional inverted chaotic mapping introduced by Hannon in 1976. Hannon mapping already introduced as a method for producing quasi-random sequence [8]. This mapping is defined as follows:

$$\begin{cases} x_{n+1} = 1 + y_n - \alpha x_n^2 \\ y_{n+1} = \beta x_n \end{cases} \quad (3)$$

Thus (X_0, Y_0) is the starting point and even (X, Y) represent a 2-dimension state of the proposed systems. Note that, $\alpha = 1.4$ and $\beta = 0.3$, this system will be in turbulence.

Conventional encryption requires that the encrypted text be the same size as the simple text. This is not a hindrance to similar images. Apart from the existing standards, the method used for encryption of images is to use affine transforms and bit performance. However, these methods cannot provide sufficient security for images as they cannot reduce the high correlation of pixels [7]. Another notable method utilized to encode images are based the random symmetry of the pixels in the images. The symmetric operation can significantly reduce the correlation, but it has little effects on the histograms of the encrypted images and other statistical attributes. Finally, you can expose a lot of information about simple images that are very vulnerable to histogram-based statistical attacks and other attacks [9-11].

Naskar et al. [12] presented a new approach that provides both purpose of encrypting both gray scale and binary images for harmless compression. Scanning methods are integrated to generate patterns utilized in encryption techniques and compression. Ravichandran et al. [13] have integrated irregular logical mappings to encrypt images and used them to meet the prerequisites for secure image transfer. Its cryptographic method involves the execution of two-irregular logical maps and a secret eighty-bit foreign key.

Talarposhti et al. [14] proposed in their paper an image encoding method using the differential evolution, discrete fourier transform (DFT), and differential evolution (DE). By utilizing differential evolution DE through crossover operations and mutations of chosen components whose selection indicators are generated by the linear feedback shift register (LFSR), this system manipulates the size and procedure of images from the DFT domain. Adleman [15] expressed that distortion within the 01 image extended using a single arch mapping generated arbitrary sequences, resetting the gray values of the image, and confusion. It demonstrates how to encode modern images to create the required release. Zhang et al. [16] reported a method of image encryption using irregular mapping and discrete weight imperial competitive algorithm (WDICA). They used arch mapping as a random source and WDICA as an evolutionary technique for designing cryptographic processes based on infiltration diffusion architecture. A method for encoding images using crystal particle optimization is introduced by Zhang et al. [17]. This method alters the ARNOLD image and then uses the key using the modified PSO to next transform the pixel position.

Özkaynak and Yavuz [18] have discussed symmetric image encoding using linear geometry. This approach involves consolidating alternatives with transfer techniques. The proposed image encryption scheme includes a combination of irregular arch mapping, sinusoidal mapping, and logical mapping to ensure further the safe transmission of medical DICOM images. Shiu et al. [19] achieved proper encoding, the dissemination of image pixels is achieved using cross-inspired biological mutations in the image encryption systems. Ravichandran et al. [20] also achieved image encryption by combining dynamic harmony search and irregular mapping.

Ravichandran et al. [20] showed that image encryption algorithms are easily selected by simple text attacks based on randomness and fixed encryption rules. Improved image encoding is provided using DNA coding and irregular mapping [21]. This is done by using a very irregular system to change positions and pixel values to do things like DNA using DNA coding rules and finally using images encoded by DNA. decoding. Ravihandran Pujari et al. [22] presented image encoding using a DNA encoding and irregularity system to encode medical images; DNA has a natural compatibility with the functions of DNA and genetic algorithms that determine the genetic properties of these organisms.

These approaches are utilized to encrypt images from an optimization point of view. In this work, images of genetic algorithms are shared and distributed by genetic operators.

Cryptographic algorithms using the randomness system provide a high level of security that can compensate for the shortcomings of traditional cryptographic algorithms. The proposed method in this work uses a combination of a chaos-based images encryption methods and a grasshopper optimization algorithm. The detail is explained in the following sections.

3. PROPOSED METHOD

The concept of optimization is to look for values between the parameters of a function that minimize or maximize the function. One of the optimization algorithms is meta-heuristic algorithms. Meta-heuristic algorithms have methods for getting out of local optimization and have high capability of development and scope. According to the studies, meta-heuristic algorithms have better results than accurate algorithms, which are able to find the optimal answer in a quantitative way, but are not suitable for complex and difficult problems. Meta-heuristic optimization algorithms are also known among engineering for four reasons: First, they are based on simple concepts and are easily implemented, second, they do not require much information, third, they can bypass the desired local state, and fourth they can cover different issues with different mechanisms.

One of the newest optimization algorithms introduced by grasshopper optimization algorithm [23]. The grasshopper algorithm is a nature-inspired meta-heuristic algorithm that simulates the behavior of grasshopper in

nature and the group movement of grasshoppers toward food sources.

The grasshopper algorithm was introduced by Coello [24]. The steps of the grasshopper algorithm are as follows:

$$X_i = S_i + 2G_i + A_i \quad (4)$$

X_i indicates the positions of the grasshoppers, S_i indicates social interactions, G_i the gravitational forces on the grasshopper, and A_i the horizontal force.

$$X_i = r_1 S_i + r_2 2G_i + r_3 A_i \quad (5)$$

r_1, r_2 and r_3 are random numbers. This is considered a black box.

The following equations are used to calculate S_i (social interactions).

$$d_{ij} = |x_j - x_i| \quad (6)$$

$$S_i = \sum_{j=1}^{N} s(d_{ij}) d_{ij} \quad (7)$$

The parameters i and j are grasshopper i and grasshopper j.

$$d_{ij} = x_j - x_i)/d_{ij} \quad (8)$$

That d_{ij} is a single vector from grasshoppers i to grasshoppers j, and the function s will be obtained as follows.

$$S(r) = fe^{\frac{-r}{l}} - e^{-r} \quad (9)$$

The parameter l indicates the scale of gravity and f indicates the intensity of gravity. Figure 1 shows the s function showing how it can affect the social interactions (gravity and repulsion) of the grasshopper.

Figure 2 shows a conceptual model of gravity and repulsion and comfort area.

Here are details of the steps of the proposed method. Its general flowchart is shown in Figure 3.

The steps that describe the proposed method are as follows:

- **Step 1:** In this step, we first give the parameters of the logistics mapping function, which includes two parameters r (the variable parameter of the logistics function) and u_0 (the initial value of the logistics function) as the initial population to the grasshopper algorithm to obtain the optimal value of each parameter. Of course, the value of r should be considered in the range of 3.57 to 4. However, in this study, we considered the value of r as a conformity so that the resulting encrypted image has the lowest correlation between pixels or the highest entropy. So each grasshopper is considered as x = [r, u_0].
- **Step 2:** In this step, the relevant image is entered into the system and the cost function is calculated. First, the relevant image must be encrypted using logistic mapping, which parameters are being optimized by the grasshopper algorithm; Then we get the cost function for each grasshopper.
- **Step 3:** After obtaining the cost function of the images or the same amount of grasshoppers, the best amount that has the highest value according to the cost function is selected as the superior grasshopper in the relevant iteration. During the implementation of the grasshopper optimization algorithm, the best grasshopper that attracts other grasshoppers is selected and then the best grasshopper with the values of parameters R and u_0 with the highest entropy in the encrypted image is selected.
- **Step 4:** In this step, after obtaining the optimal value for the parameters r and u_0 as the key, they must be converted to binary code. It should be noted that because the numbers are decimal, we used to convert decimal numbers to binary. The conversion is such that the integer parts of the numbers u_0 and r will remain and we will convert only the decimal part of them. In conversion, the size of the binary part is not fixed and is variable, so we choose the number so that it is a maximum of 64 bits for each of the parameters; As a result, the key length becomes 128 bits.
- **Step 5:** In this step, we encrypted the corresponding image using the optimized logistics function. The cryptographic method is performed in two steps. Change the parameter values of the pixels and the permutation of the pixels.

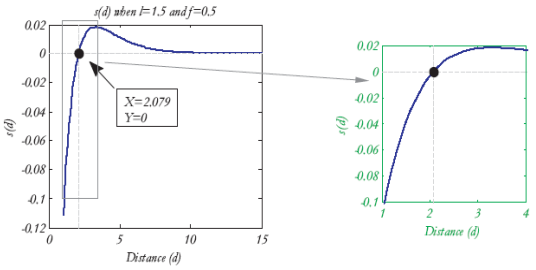

Figure 1. The function (s) (left); when l = 1.5; f = 0.5 (in the right Figure); The amplitude of the function (s), when x is in [1, 4]

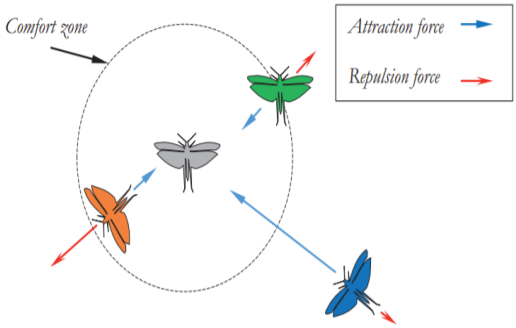

Figure 2. Conceptual model of the areas of gravity, repulsion and comfort [23]

❖ **Step 6:** In this step, the encrypted image will be generated as output.

Change the value of the pixels: First, according to Equations (3-11) the logistics function and the values of its optimized parameters to the number of pixels in the image; We produced the value of u_n, so the length of the matrix U is equal to M * N; and M is the length; N is the width of the corresponding image. Then multiply each element of the matrix by the number 255 (pixel color change area) and then XOR the corresponding pixel of the image to change its value. This process continues until all the pixels in the image are changed.

In Equation (11) U_i is any vector U and $\oplus$ means xor.

We changed the location of the pixels to increase the quality of the encryption and make the cryptographic system more secure, as well as to minimize the correlation between adjoining or adjacent pixels. For this purpose, we have used the Noth algorithm [25-28] to matrix permutation. Although the rand function is used to generate random numbers in this Note algorithm, but for cryptography and decryption that can reproduce the generated random number under certain conditions, we use functions that have quasi-random properties. Because in the decoding section to find the image, you must first change the location of the pixels to the original state. In this paper, we have used the logistic function instead of the rand function in the Noth algorithm.

$$u_{n+1} = r * u_n (1 - u_n) \quad (10)$$

$$newValue = round(U_i * 255) \oplus oldValue \quad (11)$$

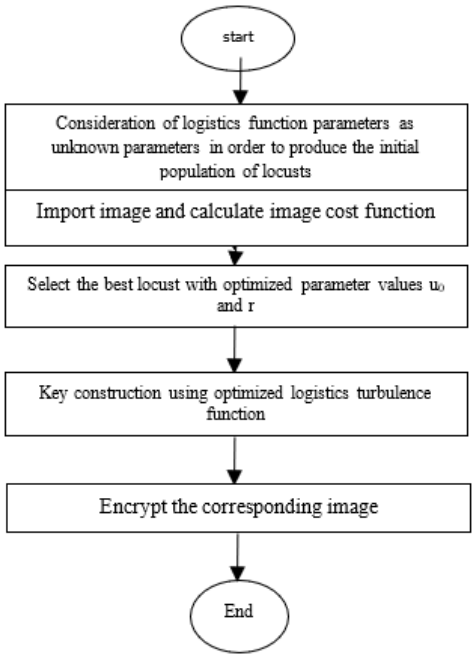

Figure 3. Flowchart of the proposed algorithm

4. EVALUATED THE PROPOSED METHOD

This section simulates the proposed method on standard images such as boat and Lena, peppers. We have also examined the proposed method with the methods available in literature [26, 29, 30].

To implement the method mentioned in this article, standard images with a size of 512 x 512 have been used. Also, the optimization operation has been done in 100 repetitions with MATLAB software. The encryption processes on the lena images is based on the correlation between adjoined pixels and the entropy-based optimization is performed. Of course, it should be noted that the diagrams shown are the average of the simulations during different iterations. Chaos-based image encryption is very sensitive to changes in specified parameters, so there is no single answer in optimizing this problem so that the set of answers converges to it, but the optimization operation can be terminated by determining the minimum value for correlation and the maximum value required for entropy or the maximum repetition.

In various articles, 1000 pairs of neighboring pixels are randomly selected for simplicity and speed of calculation, but in this study, we consider the value of N equal to all image pixels so that the correlation coefficient is constant each time the calculation covers the whole image. The original image and Lena: the encrypted image is shown in Figure 4.

The maximum correlation coefficient is one and refer to a high correlation between adjoining pixels. An excellent encryption algorithm must encrypt the image in such a way that the correlation coefficients between adjoining pixels in the encrypted image are pretty small and near to zero, here the attacker does not have access to any information through analysis.

The main images and the encrypted images and the histograms diagram of the original and encrypted images as well as the distribution of the correlations of the adjacent pixels in the horizontal direction in the main image and the encrypted images of Lena and the Boat image are shown in Figures 4 and 5. The original image histograms; and the encrypted image histograms is illustrated in Figure 6. In addition, the correlation of

Figure 4. Lena**:** The original image and Lena: the encrypted image

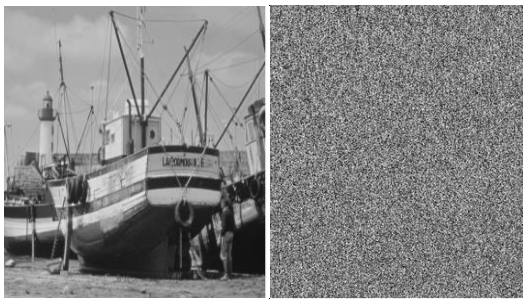

Figure 5. Boat: the original image and the encrypted image

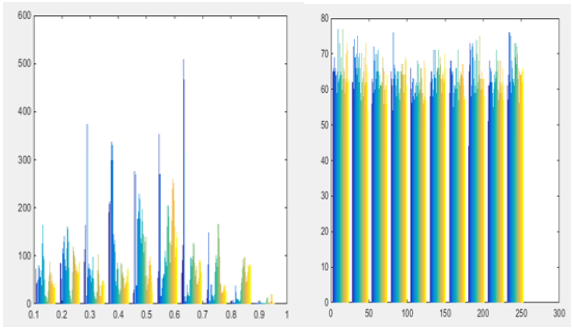

Figure 6. The original image histograms; and The Encrypted image histograms

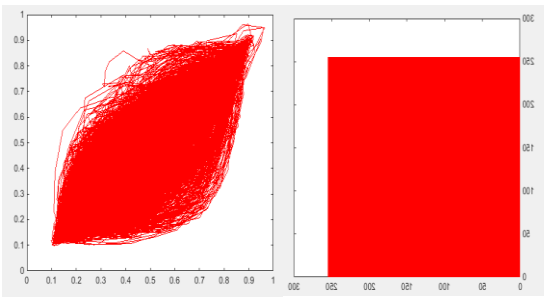

Figure 7. Correlation of adjoined pixels of the original images and encoded images

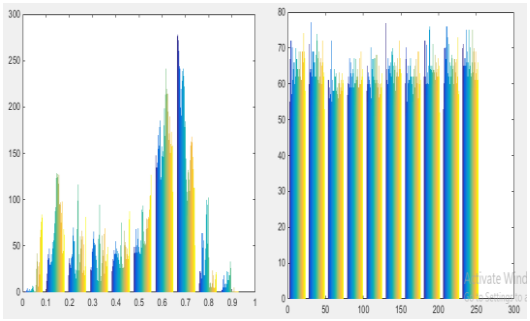

Figure 8. Boat main image histogram and encoded image histogram

adjoined pixels of the original images and encoded images are shown in Figure 7.

The boat main image histogram and encoded image histogram is also shown in Figure 8

Table 1 summarized the values obtained from the correlation coefficient between adjoined pixels in the images. From Table 2, the NPCR values are at the highest values and also the UACI values are better than the reference value reported in literature [27-29]. The results showed that the image encrypted by this work's approach has the lowest correlation between the available methods and the appropriate entropy.

TABLE 1. Correlation value of adjacent pixel

	Main image	Encrypted image with the proposed method	Encrypted image in reference [26]	Encrypted image in reference [29]	Encrypted image in reference [30]
Boat	0.9751	0.0000085	0.00000144	NA	NA
Lena	0.9718	0.000003226	0.00000682	NA	NA
Peppers	0.9732	0.0001017	0.00024591	0.0003	0.0114

TABLE 2. UACI and NPCR criteria

	NPCR proposed method	NPCR Reference [26]	UACI proposed method	UACI Reference [26]
Boat	99.65	99.191	42.152	31.159
Lena	99.43	99.22	58.12	30.147
Peppers	99.79	99.16	38.71	30.667

5. CONCLUSION

Today, image encryption represents as one of the important methods to achieve security. Conventional encryption methods cannot be utilized because of the correlations between adjoining pixels of large amounts of information and time-consuming processing. Among the proposed methods for image encryption, the turbulence functions have been used due to its properties like quasi-

randomness, sensitivity to and simplicity and initial conditions, reduction of computation time, and simple of implementations. Using the proposed method in this work, we were able to encode the images in a way that has the highest entropy and the lowest possible correlation by the logistic turbulence function using the grasshopper algorithm (GOA). The results show high accuracy, quality, and security against attacks, so that the correlation values of the encrypted images are significantly lower than the studied methods. For future solutions, we can point by fuzzy grasshopper parameters to improve the grasshopper algorithm and use it in image encryption.

5. REFERENCES

1. Nickel, S., Karimi, H. and Bashiri, M., "Capacitated single allocation p-hub covering problem in multi-modal network using tabu search", ***International Journal of Engineering, Transactions C: Aspects***, Vol. 29, No. 6, (2016), 797-808. doi: 10.5829/idosi.ije.2016.29.06c.09.
2. Su, Z., Zhang, G. and Jiang, J., "Multimedia security: A survey of chaos-based encryption technology", ***Multimedia-A Multidisciplinary Approach to Complex Issues***, (2012). doi: 10.5772/36036
3. Norouzi, B., Seyedzadeh ,S.M., Mirzakuchaki, S. and Mosavi, M.R., "A novel image encryption based on hash function with only two-round diffusion process", ***Multimedia Systems***, Vol. 20, No. 1, (2014), 45-64. doi: 10.1007/s00530-013-0314-4
4. Furht, B. and Kirovski, D., "Multimedia security handbook, CRC press.(2004)
5. Wu, Y., Zhou, Y., Noonan, J.P. and Agaian, S., "Design of image cipher using latin squares", ***Information Sciences***, Vol. 264, (2014), 317-339. doi: 10.1016/j.ins.2013.11.027.
6. Hua, Z. and Zhou, Y., "Image encryption using 2d logistic-adjusted-sine map", ***Information Sciences***, Vol. 339, (2016), 237-253. doi: 10.1016/j.ins.2016.01.017.
7. Hassan, M.A.S. and Abuhaiba, I.S.I., "Image encryption using differential evolution approach in frequency domain," arXiv preprint arXiv:1103.5783, (2011). doi: 10.48550/arXiv.1103.5783.
8. Schneier, B., "Applied cryptography: Protocols, algorithms, and source code in c, john wiley & sons, (2007).
9. Ye, R., Zeng, S., Lun, P., Ma, J. and Lai, C., "An image encryption scheme based on bit circular shift and bi-directional diffusion", ***Int J Inform Technol Comput Sci (IJITCS)***, Vol. 6, No. 1, (2014), 82-92. doi: 10.5815/ijitcs.2014.01.10.
10. Enayatifar, R., Abdullah, A.H. and Lee, M., "A weighted discrete imperialist competitive algorithm (wdica) combined with chaotic map for image encryption", ***Optics and Lasers in Engineering***, Vol. 51, No. 9, (2013), 1066-1077. doi: 10.1016/j.optlaseng.2013.03.010.
11. Sabarinath, R., Jegadeesan, S. and Venkatalakshmi ,K., "Image encryption using modified particle swarm optimization", ***IJRCCT***, Vol. 3, No. 2, (2014), 241-246. doi: 10.1007/s41870-018-0099-y
12. Naskar, P.K., Chaudhuri, A. and Chaudhuri, A., "A secure symmetric image encryption based on linear geometry ,"in 2014 Applications and Innovations in Mobile Computing (AIMoC), IEEE., (2014), 67-74.
13. Ravichandran, D., Praveenkumar, P., Rayappan, J.B.B. and Amirtharajan, R., "Chaos based crossover and mutation for securing dicom image", ***Computers in Biology and Medicine***, Vol. 72, (2016), 170-184. doi: 10.1016/j.compbiomed.2016.03.020
14. Talarposhti, K.M. and Jamei, M.K., "A secure image encryption method based on dynamic harmony search (dhs) combined with chaotic map", ***Optics and Lasers in Engineering***, Vol. 81, (2016), 21-34. doi: 10.1016/j.optlaseng.2016.01.006.
15. Adleman, L.M., "Molecular computation of solutions to combinatorial problems", ***Science***, Vol. 266, No. 5187, (1994), 1021-1024. doi: 10.1126/science.7973651.
16. Zhang, X., Zhou, Z. and Niu, Y., "An image encryption method based on the feistel network and dynamic DNA encoding", ***IEEE Photonics Journal***, Vol. 10, No. 4, (2018), 1-14.
17. Zhang, J., Fang, D. and Ren, H., "Image encryption algorithm based on DNA encoding and chaotic maps", ***Mathematical Problems in Engineering***, Vol. 2014, (2014). doi: 10.1155/2014/917147.
18. Özkaynak, F. and Yavuz, S., "Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system", ***Nonlinear Dynamics***, Vol. 78, No. 2, (2014), 1311-1320. doi: 10.1007/s11071-014-1517-8.
19. Shiu, H.-J., Ng, K.-L., Fang, J.-F., Lee, R.C. and Huang, C.-H., "Data hiding methods based upon DNA sequences", ***Information Sciences***, Vol. 180, No. 11, (2010), 2196-2208. doi: 10.1016/j.ins.2010.01.030
20. Ravichandran, D., Praveenkumar, P., Rayappan, J.B.B. and Amirtharajan, R., "DNA chaos blend to secure medical privacy", ***IEEE Transactions on Nanobioscience***, Vol. 16, No. 8, (2017), 85 .858-0doi: 10.1109/TNB.2017.2780881.
21. Wang, X. and Zhang, H.-l., "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems", ***Nonlinear Dynamics***, Vol. 83, No. 1, (2016), 333-346. doi: 10.1007/s11071-015-2330-8.
22. Pujari, S.K., Bhattacharjee, G. and Bhoi, S., "A hybridized model for image encryption through genetic algorithm and DNA sequence", ***Procedia Computer Science***, Vol. 125, (2018), 165-171. doi: 10.1016/j.procs.2017.12.023.
23. Sezavar, A., Farsi, H .and Mohamadzadeh, S., "A modified grasshopper optimization algorithm combined with cnn for content based image retrieval", ***International Journal of Engineering, Transactions A: Basics***, Vol. 32, No. 7, (2019), 924-930. doi: 10.5829/ije.2019.32.07a.04.
24. Coello, C.A.C., "Theoretical and numerical constraint-handling techniques used with evolutionary algorithms: A survey of the state of the art", ***Computer Methods in Applied Mechanics and Engineering***, Vol. 191, No. 11-12, (2002), 1245-1287. doi: 10.1016/S0045-7825(01)00323-1.
25. Knuth, D.E., *Theartofcomputerprogramming: Sortingandsearching*. 1973, Addison-Wesley, Reading, Massachusetts.
26. Hussain, I., Azam, N.A. and Shah, T., "Stego optical encryption based on chaotic s-box transformation", ***Optics & Laser Technology***, Vol. 61, (2014), 50-56. doi: 10.1016/j.optlastec.2014.01.018.
27. Ahmad, M., Alam, M.Z., Umayya, Z., Khan, S. and Ahmad, F., "An image encryption approach using particle swarm optimization and chaotic map", ***International Journal of Information Technology***, Vol. 10, No. 3, (2018), 247-255. doi: 10.1007/s41870-018-0099-y.
28. Jolfaei, A. and Mirghadri, A., "A new approach to measure quality of image encryption", ***International Journal of Computer and Network Security***, Vol. 2, No. 8, (2010), 38-44, doi: 10.12928/TELKOMNIKA.v17i6.10488.

29. Norouzi, B., Mirzakuchaki, S., Seyedzadeh, S.M. and Mosavi, M.R., "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process", ***Multimedia Tools and Applications***, Vol. 71, No. 3, (2014), 1469-1497. doi: 10.1007/s11042-012-1292-9.

30. Farwa, S., Muhammad, N., Shah, T. and Ahmad, S., "A novel image encryption based on algebraic s-box and arnold transform", ***3D Research***, Vol. 8, No. 3, (2017), 1-14, doi: 10.1007/s13319-017-0135-x

Persian Abstract

چکیده

رمزگذاری برای محافظت از داده های حساس، به ویژه تصاویر، در برابر هرگونه دسترسی غیرقانونی و نقض بسیار مهم است. این تحقیق به منظور ارائه یک روش بهینه سازی رمزگذاری تصویر برای ارتباطات مبتنی بر امنیت تصویر ارائه شده است. این روش از الگوریتم بهینه سازی ملخ برای انجام رمزگذاری بهینه و نگاشت منطقی نامنظم استفاده می کند. در ابتدا، این رویکرد چندین تصویر رمزگذاری شده و یک نقشه آشفته ایجاد می کند که در آن کلید جلسه برای شرایط اولیه نقشه به یک تصویر ساده معلق بستگی دارد. پس از آن، تصاویر رمزگذاری شده به عنوان یک اولیه و ذرات برای بهینه سازی از طریق الگوریتم بهینه سازی ملخ تنظیم می شوند. تصویر کدگذاری شده بهینه شده با ضریب همبستگی پیکسل های پیوسته به عنوان تابعی از نسبت بیان می شود. نتایج شبیه‌سازی متلب روش کدگذاری پیشنهادی نشان می‌دهد که تصاویر رمزگذاری‌شده یکسان هستند و پیکسل‌های مجاور با سایر ردیف‌های رمزگذاری برجسته، مانند آنتروپی هیستوگرام مسطح و نرخ پیکسل مؤثر تغییر میانگین قدرت تصحیح همبستگی بالایی دارند.