*Corresponding Author Email: musa.dogan@selcuk.edu.tr
Proceedings of the International Conference on Academic Research in Science, Technology and Engineering, Vol. 1, Issue. 1, 2022, pp. 12-20
DOI: https://doi.org/10.33422/icarste.v1i1.13

ISSN: 2783-7742 online

Diamond Scientific Publishing

Enhanced Diffusion and Confusion Based Encryption Algorithm Using Differential Evolution and Chaotic Mapping

Musa Doğan[1*], and Nurettin Doğan[2]
Selcuk University, Türkiye

Abstract

Encryption is critical to protecting sensitive data, especially images, against potential illegal access and breaches. The use of chaotic maps for image encryption is widespread among researchers. However, it is necessary to set up initial parameters for chaotic maps to generate random sequences. These parameters need to be selected with care. To determine the optimal initial parameters for image encryption, evolutionary optimization techniques have been used. In this paper, we propose a secure image-based communication system based on an optimized image encryption algorithm. This approach uses differential evolution optimization, which is an ideal solution for reducing convergence time when optimizing chaotic map parameters. Furthermore, the security parameters of these techniques are evaluated, including entropy, Number of Pixel Change Rate (NPCR), Unified Average Changed Intensity (UACI), and correlation coefficients. The simulation results of the proposed encryption approach by combining Arnold's cat map, chaotic logistic map and optimization method show that the encrypted image is safe against attacks.

Keywords: Arnold transform, chaotic encryption, differential evolution, logistic map function, metaheuristic optimization

1. Introduction

In today's world, digital data transfer has become possible with developing technologies. However, in order to ensure security in the transfer of data from the sender to the receiver, the data must be sent in an encrypted manner. Therefore, there is a growing demand for technologies and methods for encrypting information so that information is understandably accessible only to authorized users.

Block ciphers that were initially developed to encrypt textual data, such as the highly computationally secure Data Encryption Standard (DES), Advanced Encryption Standard (AES), and International Data Encryption Algorithm (IDEA), are not suitable for digital images because of their high pixel correlation and slow speeds in large data volumes. (Li et al., 2006; Salleh et al., 2003; Usama & Khan, 2008). The two main techniques for hiding strong correlations are confusion and diffusion (Shannon, 1949). Confusion increases the complexity between the key and ciphertext, while diffusion spreads the association of the plain text to the entire ciphertext, thus reducing correlation.

Chaotic maps are well-suited for various data encryption methods due to their satisfactory ergodicity characteristics and strong sensitivity to initial conditions and parameters. In particular, it is possible to apply them to microprocessors and personal computers. Therefore, they are a better candidate for data encryption than many traditional encryption methods (Lian et al., 2005).

There are many studies conducted with chaotic mapping methods in the literature. In their study, Salleh et al. (2003) proposed a Secure Image Protection (SIP) algorithm based on Baker's chaotic map. With this algorithm, they solve the weak key problem and increase the security power of the algorithm. Lian et al. (2005) has proposed some methods to improve the performance of maps. Based on the improved standard map consisting of confusion, diffusion and key generation, a block cipher was designed and presented to encrypt large volumes of data sets. Gao and Chen (2008) proposed a new image encryption algorithm based on the hyper-chaos method, which uses an image blending matrix to confuse the pixel positions of an original image. Jolfaei and Mirghadri (2010), an encryption scheme based on the combination of a chaotic map and the W7 flow cipher to create a permutation matrix in two directions to form shuffler is presented. Liu and Wang (2010), designed a flow encryption algorithm based on one-time keys and piecewise linear chaotic map to ensure high security and improve dynamic distortion, achieving satisfactory values in metrics such as number of pixel change rate (NPCR) and unified average changed intensity (UACI). Chen et al. (2013) has shown that the orbital variables of the chaotic map are continuously triggered by the previously processed pixel value in both permutation and diffusion procedures when a minor change in the original image propagates and creates a diffusion effect during confusion. Fu et al. (2013) in their encryption study on medical images made pixel-level displacements in classical permutation stages at the bit level and provided the same level of security with fewer laps in the substitution phase. Chen et al. (2014) proposed a method in which permutation-diffusion-based picture encryption algorithms are not fast enough and the parameter of the chaotic map is changed with the image they obtain after the diffusion stage to increase the speed. With the proposed method, the diffusion effect is increased and effective against known plain text attacks.

There are also studies in the literature with metaheuristic optimization techniques to securely encrypt the image. These methods have the advantage of optimizing the fixed parameters

needed for encryption. Due to the fact that they are based on population behavior, evolutionary algorithms (EAs) have the ability to generate several potential outcomes in a single evolution. (Kaur & Kumar, 2018). In, Abdullah et al. (2012) firstly, the initial population consists of an original image created using the chaotic function. After that, the correlation coefficient is used to select half of the superior generations and recombination is carried out on these generations. Sreelaja and Pai (2012), in their study using Ant Colony Optimization (ACO), used a table of character codes to encode plain text representing keys and binary images. With this approach, they have shown in their experimental study that the number of keys to be stored and distributed decreases.

In the proposed method in this study, a 2D Arnold's cat map is used to scramble the image, a chaotic logistic map function to encrypt it, and a random key obtained from the original image is used. The initial parameter of the chaotic logistic map is optimized using the metaheuristic optimization algorithm until the optimal value is obtained. In the following sections, the metaheuristic approach and the chaotic functions used are introduced, the proposed method and the experimental results are presented.

2. Preliminaries

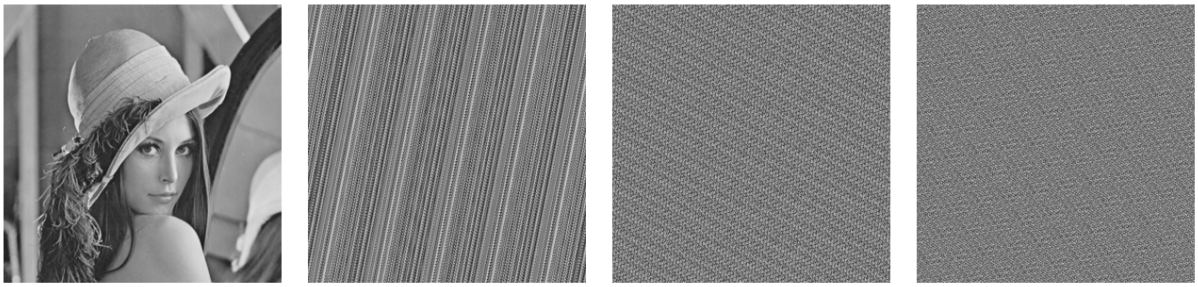
2.1. Arnold's Cat Map

Arnold's cat map transform is used to confuse the pixels of the image and provide the additional security of the encryption system (Abbas, 2016). This 2D map does not change the intensity value of the image, it just messes up the image data and given in Eq. 1.

$$\begin{aligned} x' &= (x + p * y) \quad mod256 \\ y' &= (q * x + (b * q + 1) * y) \quad mod256 \end{aligned} \tag{1}$$

Here, p and q are the positive secret keys, x and y are the original position information before the image is mixed, and x' and y' are the position information after the image has been mixed. After several rounds of the Arnold cat map transformation, the relationship between neighboring pixels is destroyed and the original image appears distorted and meaningless. In Figure 1, an example image where pixel locations were changed with Arnold cat map is given.

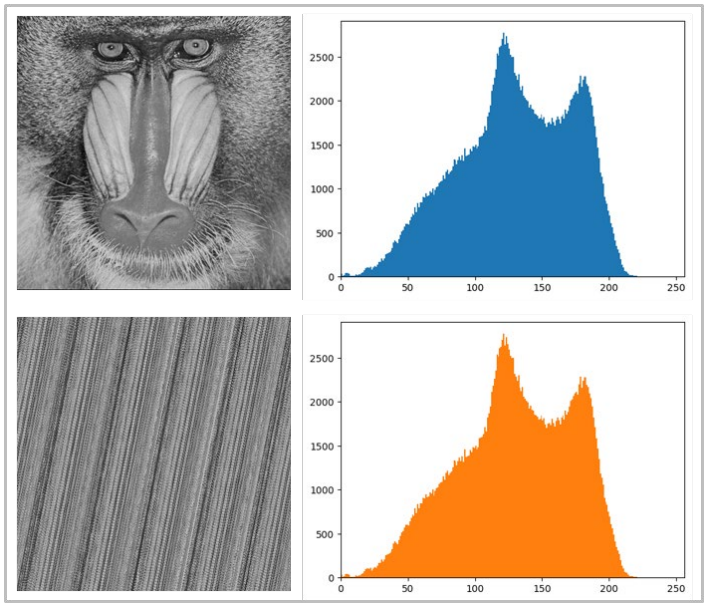
Figure 1: (a) plain image of lena (b) 1 round cat's transform (c) 2 round cat's transform (d) 3 round cat's transform



a b c d

Replacing the pixels of the image with Arnold cat map does not affect the histogram. It is shown in Figure 2.

Figure 2: Plain image of baboon, histogram of original image and transformed image with Arnold map, histogram of transformed image



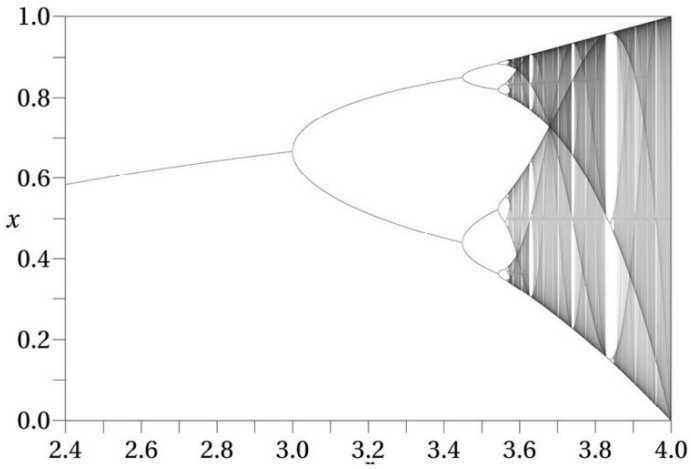
2.2. Chaotic Logistic Map

The chaotic logistic map was chosen among the chaotic maps used for encryption because of its high performance. (Pareek et al., 2006) A logistic map can be expressed as:

$$x_{n+1} = \mu x_n(1 - x_n), x_n \in [0,1], \mu \in [0,4] \quad (2)$$

Here, the values μ and x_n specify the parameter and the state variable. In the case of $\mu \in [3.57, 4]$ the system becomes chaotic. Figure 3 illustrates this situation. In this map, μ ve x_0 values can be considered as secret keys in the diffusion step.

Figure 3: Chaotic logistic map diagram

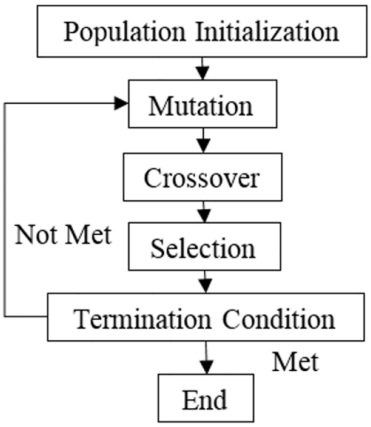


Source: (Almazrooie et al., 2015)

2.3. Differential Evolution

K. Price first introduced the differential evolution algorithm (Storn & Price, 1997). This algorithm is a recently popular population-based algorithm that utilizes similar operators found in genetic algorithms such as crossover, mutation, and selection. This evolutionary process will continue until a predetermined stopping condition is satisfied. The chaotic logistic map's initial parameter is optimized using the metaheuristic optimization technique until the optimal value is reached.

Figure 4: Differential Evolution Flowchart

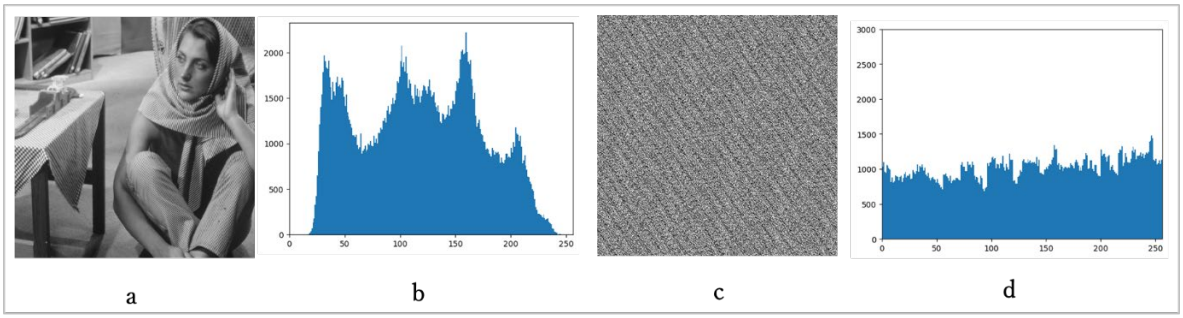


Source: (Kok & Rajendran, 2016)

3. Experimental Results and Analysis

In this study, a secure method with chaotic maps, which is one of the image encryption techniques, is proposed. Five gray-scale images (baboon, lena, barbara, boat and goldhill), which are often used in image processing studies, were tested. This experimental study was carried out on a computer with an i7 6700HQ processor in a Windows environment using the Python 3.8 programming language. In this section, simulation results and security analysis details are given to show the validity and effectiveness of the proposed encryption. The original and encrypted histogram values of a sample image selected as a result of our work are given in Figure 5.

Figure 5: (a) plain image of barbara (b) original image histogram (c) encrypted image (d) encrypted image histogram



3.1. Information Entropy Analysis

Entropy is a probability distribution-based measure of information or uncertainty (Stinson, 2005). If the information source specified as x, and the formula for calculating information entropy:

$$H(x) = \sum_{i=1}^{2^n} p(x_i) \log_2 \frac{1}{p(x_i)} \tag{3}$$

where $p(x)$, represents the probability of the expression x. For a truly random source emitting 2^n symbols, the entropy is $H(x)$=8. As the images selected are 256 greyscales, the encrypted image should have an entropy of close to 8 after (Liu & Wang, 2010). The closer to 8, the less likely it is that the encryption system will disclose information. It means that the encryption process is secure against entropy attacks, and information leakage is negligible.

In our scheme, since the use of the chaotic map increases the randomness of the encrypted images, the information entropy values are quite high. In Table 1, the entropy values for the original and encrypted images are given.

Table 1: Original and ciphered images entropy values

Image	Original Image	Ciphered Image
Goldhill	7.44552	7.92234
Baboon	7.35831	7.97781
Barbara	7.63211	7.97407
Boat	7.19137	7.90163
Lena	7.47782	7.96953

3.2. Correlation Coefficient Analysis

The adjacent pixel values of an original image are clearly related in three ways: horizontally, vertically, and diagonally. The correlation coefficient (CC) is used to determine the relationship between pixels in an original and cipher image (Sreelaja and Pai (2012). It is preferable to minimize the correlation coefficient of the ciphertext picture in an image encryption algorithm. The formula for this analysis is below.

$$r_{x,y} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x) * D(y)}} \tag{4}$$

where $r_{x,y}$ represents the CC. $\mathrm{cov}(x, y)$ represent the correlation between x and y. $D(x)$ and $D(y)$ represent the variances of x and y. The CC of the original and encrypted images is given in Table 2.

Table 2: CC of two adjacent pixels in original and encrypted images

Image	Original Image	Ciphered Image
Goldhill	0.96757	0.08750
Baboon	0.86277	0.01197
Barbara	0.89175	-0.03592
Boat	0.93408	-0.04071
Lena	0.96411	0.01821

3.3. Differential Attack

NPCR refers to the rate at which the pixel values of two cipher images change and a pixel of an original image is modified (Pareek et al., 2006). The high NPCR rating demonstrates the algorithm's effectiveness against various forms of blocking attacks and given in Eq. 5.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\% \tag{5}$$

$$D(i,j) = \begin{cases} 0, & \text{if } C^1(i,j) = C^2(i,j) \\ 1, & \text{if } C^1(i,j) \neq C^2(i,j) \end{cases} \tag{6}$$

UACI computes the standard deviation difference between two encrypted pictures, which corresponds to a one-pixel change in the original image (Kaur & Kumar, 2018). This method is given in Eq. 7.

$$UACI = \frac{1}{m \times n}\left[\sum_{i,j} \frac{|C^1(i,j) - C^2(i,j)|}{255}\right] \times 100\% \tag{7}$$

The test results that we have carried out to measure the resistance of the study to attacks are given in Table 3.

Table 3: NPCR and UACI values in encrypted images

Image	NPCR	UACI
Goldhill	99.65057 %	31.30890 %
Baboon	99.64065 %	29.25064 %
Barbara	99.61318 %	30.58657 %
Boat	99.68605 %	28.89640 %
Lena	99.61700 %	29.25105 %

4. Conclusion

Our study proposes a secure image encryption system that employs a differential evolution (DE) algorithm to optimize the initial values of the chaotic logistic map used in the encryption process. In order to enhance security, both confusion and diffusion are used. Traditionally, the chaotic logistic map initial parameter is set to 3.999999, but the proposed optimization process finds that this is not the most appropriate value. The evaluation results demonstrate that this encryption approach shows significant improvements in terms of security, as confirmed by various tests such as entropy, NPCR, UACI, and correlation coefficients. Additionally, future work will aim to extend the encryption technique to RGB images, which can potentially improve the system's versatility.

Acknowledgment

The authors thank to Selcuk University Scientific Research Projects (BAP) financial supporting this study (Project No: 22701185).

References

Abbas, N. A. (2016). Image encryption based on Independent Component Analysis and Arnold's Cat Map. *Egyptian informatics journal*, *17*(1), 139-146. https://doi.org/10.1016/j.eij.2015.10.001

Abdullah, A. H., Enayatifar, R., & Lee, M. (2012). A hybrid genetic algorithm and chaotic function model for image encryption. *Aeu-International Journal of Electronics and Communications*, *66*(10), 806-816. https://doi.org/10.1016/j.aeue.2012.01.015

Almazrooie, M., Samsudin, A., & Singh, M. M. (2015). Improving the Diffusion of the Stream Cipher Salsa20 by Employing a Chaotic Logistic Map. *Journal of Information Processing Systems*, *11*(2), 310-324. https://doi.org/10.3745/Jips.02.0024

Chen, J. X., Zhu, Z. L., Fu, C., & Yu, H. (2013). An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism. *Opt Express*, *21*(23), 27873-27890. https://doi.org/10.1364/OE.21.027873

Chen, J. X., Zhu, Z. L., Zhang, L. B., Fu, C., & Yu, H. (2014). An Efficient Diffusion Scheme for Chaos-Based Digital Image Encryption. *Mathematical Problems in Engineering*, *2014*, 1-13. https://doi.org/10.1155/2014/427349

Fu, C., Meng, W. H., Zhan, Y. F., Zhu, Z. L., Lau, F. C., Tse, C. K., & Ma, H. F. (2013). An efficient and secure medical image protection scheme based on chaotic maps. *Comput Biol Med*, *43*(8), 1000-1010. https://doi.org/10.1016/j.compbiomed.2013.05.005

Gao, T. G., & Chen, Z. Q. (2008). A new image encryption algorithm based on hyper-chaos. *Physics Letters A*, *372*(4), 394-400. https://doi.org/10.1016/j.physleta.2007.07.040

Jolfaei, A., & Mirghadri, A. (2010). An image encryption approach using chaos and stream cipher. *Journal of Theoretical and Applied Information Technology*, *19*(2), 117-125.

Kaur, M., & Kumar, V. (2018). A Comprehensive Review on Image Encryption Techniques. *Archives of Computational Methods in Engineering*, *27*(1), 15-43. https://doi.org/10.1007/s11831-018-9298-8

Kok, K. Y., & Rajendran, P. (2016). Differential-Evolution Control Parameter Optimization for Unmanned Aerial Vehicle Path Planning. *PloS one*, *11*(3), e0150558. https://doi.org/10.1371/journal.pone.0150558

Li, S., Chen, G., & Zheng, X. (2006). Chaos-based encryption for digital image and video. *Multimedia Encryption and Authentication Techniques and Applications*, 129.

Lian, S. G., Sun, J. S., & Wang, Z. Q. (2005). A block cipher based on a suitable use of the chaotic standard map. *Chaos Solitons & Fractals*, *26*(1), 117-129. https://doi.org/10.1016/j.chaos.2004.11.096

Liu, H. J., & Wang, X. Y. (2010). Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications*, *59*(10), 3320-3327. https://doi.org/10.1016/j.camwa.2010.03.017

Pareek, N. K., Patidar, V., & Sud, K. K. (2006). Image encryption using chaotic logistic map. *Image and vision computing*, *24*(9), 926-934. https://doi.org/10.1016/j.imavis.2006.02.021

Salleh, M., Ibrahim, S., & Isnin, I. F. (2003). Enhanced chaotic image encryption algorithm based on Baker's map. *Proceedings of the 2003 Ieee International Symposium on Circuits and Systems, Vol Ii*, 508-511.

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal*, *28*(4), 656-715.

Sreelaja, N. K., & Pai, G. A. V. (2012). Stream cipher for binary image encryption using Ant Colony Optimization based key generation. *Applied Soft Computing*, *12*(9), 2879-2895. https://doi.org/10.1016/j.asoc.2012.04.002

Stinson, D. R. (2005). *Cryptography: theory and practice*. Chapman and Hall/CRC.

Storn, R., & Price, K. (1997). Differential evolution - A simple and efficient heuristic for global optimization over continuous spaces. *Journal of global optimization*, *11*(4), 341-359. https://doi.org/10.1023/A:1008202821328

Usama, M., & Khan, M. K. (2008). Classical and chaotic encryption techniques for the security of satellite images. 2008 International Symposium on Biometrics and Security Technologies,