An Optimal Teaching and Learning based Optimization with Multi-Key Homomorphic Encryption for Image Security

Mustafa s Khalifa[1], Ahmed N. Al-Masri[2,*]

[1] Computer Science Department, Faculty of Education Pure Science, Basra University, Iraq

[2]American University in the Emirates, Dubai, UAE

Emails: Mustafa.khalefa@uobasrah.edu.iq ; ahmed.almasri@aue.ae

Abstract

Due to the drastic rise in multimedia content, digital images have become a major carrier of data. Generally, images are communicated or archived via wireless communication changes, and the significance of data security gets increased. In order to accomplish security, encryption is an effective technique which is used to encrypt the images using secret keys in such a way that it is not readable by the hacker. In this view, this study focuses on the design of Teaching and Learning based Optimization (TLBO) with Multi-Key Homomorphic Encryption (MHE) technique, called MHE-TLBO algorithm. The goal of the MHE-TLBO algorithm is to optimally select multiple keys using TLBO algorithm for encryption and decryption processes. In addition, the MHE-TLBO algorithm has derived a fitness function involving peak signal to noise ratio (PSNR) and thereby ensures the superior quality of the reconstructed image. For validating the security performance of the MHE-TLBO algorithm, a comprehensive result analysis is made and the simulation results ensured the betterment of the MHE-TLBO algorithm interms of different aspects.

Keywords: Image encryption, Security, Key generation, Homomorphic encryption, TLBO algorithm, Optimization process.

1. Introduction

Recently, with the rapid popularization and promotion of digital communication and network technologies across the globe, digital video based digital images became a significant means for data transmission and storage in the computer network under the fields of military and civil [1, 2]. But network security problems have been a significant factor which restricted and plagued the growth of network technologies [3, 4]. Particularly, in the data resource of the government department and public, to comprehend the information security in the computer networks are the significant direction and content of the study fields in information security and network security. Amongst other, digital video and digital image became the significant contents of broadcast information in the network with the virtues of its convenience and intuitiveness [5, 6]. Hence, the security protections of digital images have attained more interest from each party. Particularly, in the background of increasing serious network security situations over the past few years, data sharing and transmission depending on digital image frequently facing the problem of information tampering, theft, attack, and deletion that have created huge losses to the publishers/owners of digital image [7-9]. In the security method of digital data, encryption technique is a more popular method and technique. Encryption techniques can be encrypted by encrypting the new information. When the reliability and security of the encryption technique are relatively large, the security of digital data could be secured [10]. Hence, the study on digital image encryption methods and technology is a significant direction for digital image security. But, encryption system/encryption

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021

technology is based largely on the requirement of text encryption. Now, the most popular encryption scheme could not attain better results in the encryption quality and compatibility of digital image encryptions. Even though digital images could be treated as 2D datasets, cryptographic systems which straightforward utilize text encryption methods frequently facing the problem of inefficacy in decryption and encryption, low security, and low practicability [11, 12]. Studying an encryption method/cryptographic system appropriate for digital image encryptions is a certain technique for protecting the security of digital images in network environments.

Khan et al. [13] proposed an effective method of making high nonlinear cryptographic substitution boxes as an alternative to algebraic/chaotic construction method. The PSO method is used in the construction of high nonlinear S-box, in the proposed method the first populations are arbitrarily generated, and the location vectors of particles are employed in producing S-box. A hyperchaotic image encryption scheme [14] is presented according to PSO and CA models. First of all, to increase the capability for resisting plaintext attack, the early condition of the hyperchaotic scheme is produced by the hash function values i.e., nearly associated with the plaintext images to be encrypted. Furthermore, the fitness of PSO is the relation coefficients among nearby pixels of images.

Farah et al. [15] proposed a novel image cipher on the basis of diffusion or confusion Shannon property. The presented approach is based on novel enhanced substitution boxes, has been performed using chaotic Jaya optimization approach for generating S-box based on their non-linearity scores. The aim of the optimization method is to contain a bijective matrix using higher non-linearity scores. [16] studied an image encryption method according to MOPSO method, 1D Logistic maps, and DNA encoding sequences. Initially, the primary objective of this work includes the subkey sequences elected with PSO method, hash values of the shuffle mark bit, and plaintext images. Generate arbitrary DNA mask image by DNA encoding and Logistic map. Later, utilize the block shuffling plaintext DNA encoding sequences for operating an encryption method.

In [17], hyperchaotic maps are enhanced by a multi-objective evolution optimization method. The DLS-MO method is employed for obtaining the optimum variables of an encryption factor and hyperchaotic map. Next, with an optimum parameter, a hyperchaotic map develops the secret key. This secret key is later employed for performing diffusion and permutation on a plain image for developing the encrypted image. In [18], a novel medicinal image encryption method integrating GSAPSO and MQC systems is presented for obtaining improved security performances. First, an enhanced MQC method is employed for generating is used key streams. Later, the cross operation and election of GA method are employed for processing the plaintext images. The optimum sequence created using SA method is applied for scrambling. While the PSO method is presented for the SA method. The early temperature is fixed based on the best fitness values of the primary population.

In [19], a hybrid image encryption technique was presented depends on chaos and GA. The encryption method includes 3 major phases: improvement, confusion, and diffusion stages with a GA method. Initially, Chen's chaotic map is employed in the confusion stage to make scrambled images with shuffling plain image pixels, and in diffusion phase, Logistic Sine map alters this pixel's gray level value. It creates few encrypted images that are deliberated as the primary population for the GA method. Later, with GA method, the encrypted image is enhanced.

This study focuses on the design of Teaching and Learning based Optimization (TLBO) with Multi-Key Homomorphic Encryption (MHE) technique, called MHE-TLBO algorithm. The goal of the MHE-TLBO algorithm is to optimally select multiple keys using TLBO algorithm for encryption and decryption processes. In addition, the MHE-TLBO algorithm has derived a fitness function involving peak signal to noise ratio (PSNR) and thereby ensures the superior quality of the reconstructed image. For validating the security performance of the MHE-TLBO algorithm, a comprehensive result analysis is made interms of different measures.

2. The Proposed Image Encryption Scheme

Fig. 1 illustrates the overall block diagram of MHE-TLBO model. Image encryption techniques are turned into a basic part of an image conveyance procedure, in case if they point near productivity and meanwhile, maintain the maximum security level. The presented method utilizes MHE with ideal keys to image

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021

security procedures. Semantically secured homomorphic public key encrypted techniques were focal cryptographic apparatus to any protected multiparty computation problems. The property of homomorphic has been valuable for building a secure model with high-security data recovery plan. These encryption structures are employed for performing tasks utilizing encoder data without significant the private key (with no decryption), for instance, the customer is a vital holder of the confidential key [20]. The homomorphic assessment technique produces as to account the polynomial many cipher images that are encrypted in N keys, composed of the connecting assessment key, and deliver the cipher images. In multiple encryptions were the only manner near altering on a unique message as to confused shape with carrying out encrypted to the number of times, also with implementing similar or distinctive technique processes. It could be demonstrated as cascade encryption, cascade ciphering, together with several encryptions. To examine model, encrypt as well as decrypt are carried out with several keys. The presented MHE considers 3 stages like multiple key generations, optimum key determination, and encrypt/decrypt approach [21].

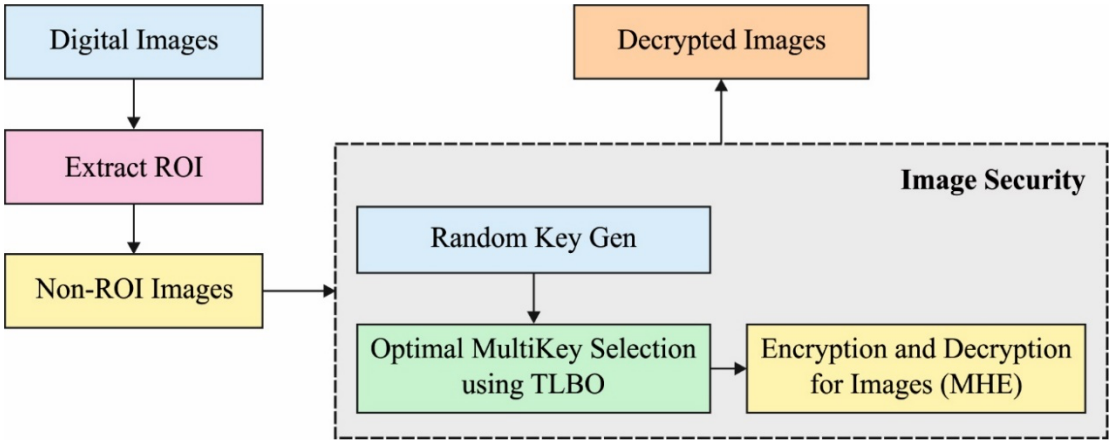

Fig. 1. Block diagram of MHE-TLBO model

A key has been employed for encrypting/decrypting whatever data has been encrypted or decrypted. This technique was utilized to encoded as well as decoded keys and the compared images utilizing symmetric keys; both privacy and trust value security are provided. The private key (pr_k) and relative public key(pu_k) are in several key sets. The key equal was employed with asymmetric key technique; at this point, several keys K = {K_1, K_2, ..… K_n} was created to MHE. In specific cases, the keys are arbitrarily created utilizing a Random Number Generator. In order to select the optimum key in several keys, TLBO technique was implemented.

The TLBO technique was simulated in the knowledge transmission amongst the teacher as well as students from the educational periods [22]. Assume that 2 teachers, T1 and T2, teach a subject with similar data to an identical merit level learner from 2 dissimilar classes. Curves 1 and 2 demonstrate the marks reached as the learner taught by teacher T1 and T2 correspondingly. The normal distribution has been regarded as to obtained marks, however, it should be skewness. Normal distribution was demonstrated in Eq. (1).

$$f(X) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-(x-\mu)^2}{2\sigma^2}} \quad (1)$$

where σ2 implies the variance, μ refers the mean and x is some value to that the normal distribution function was required. Curve 2 referred to optimum efficiency related to curve 1 and so it can be stated that T2 is higher than T1 with respect to teaching. An important difference amongst the efficiency was measured by calculating the mean amongst them (M2 for Curve-2 and M1 for Curve-1), for instance, an excellent teacher attains optimum mean to the outcomes of learner. The learner also learns to interface among themselves and it also supports improving its outcomes. In the above teaching procedure, the mathematical process was complete for optimizing the unconstrained non-linear continuous function, and so planning an effectual optimized manner called as TLBO technique. There are 2 essential levels from

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021

TLBO technique such as 'Teacher Phase' (learned from teacher) and 'Learner Phase' (learned through its interaction).

During the teacher phase, the mean of class improves in MA to MB dependent upon the optimum teacher. The teacher was supposed to an optimum if his/her learner up to his/her level dependent upon knowledge. However, it can be challenging and the teacher is only changing the mean of class up for particular level dependent upon capability of class. Let Mi implies the mean and Ti represent the teacher at some iteration i. Ti attempts to change the mean Mi near their individual level, thus the novel means is Ti called Mn. The solution takes upgraded dependent upon difference amongst the present and novel mean compared as

$$\text{Difference\_Mean}_i = r_i(M_n - T_F M_i) \quad (2)$$

Where TF signifies the teaching issue that calculates the value of mean to be changed, and ri implies the arbitrary number from range of 0 and 1. The value of TF is one/two that is yet over a heuristic step and obvious in an arbitrary approach with similar probabilities as TF= round[1 + rand(0, 1) {2 − 1}]. These variance alterations the existing solution dependent on Eq. (3) as demonstrated under.

$$X_{n,\ i} = X_{o,\ i} + \text{Difference\_Mean}_i \quad (3)$$

The learners enhance the knowledge utilizing 2 manners: input in the teacher and interaction among themselves. The learner ensures communication with rest of learners with utilizes group discussion, presentation, etc. The learner learns novel things if the other learners are further knowledge related to them and learner modification is associated as:

$For i = 1 : P$n

Arbitrarily elect 2 learners Xi and Xj, where i≠j

$If f(X_i) < f(X_j)$

Xn,i= Xo,i+ ri(Xi − Xj)

Else

Xn,i= Xo,i+ ri(Xj− Xi)

End If

End For

Accept Xn if an optimum function value has reached.

3. Experimental Validation

Table 1 and Fig. 2 depict the result analysis of the MHE-TLBO model with other existing techniques. The figure demonstrated that the MHE-TLBO technique has gained maximum PSNR under the applied test images. For instance, with Lena image, the MHE-TLBO technique has accomplished a higher PSNR of 65.12dB whereas the HE, MHE, and MHE-AWO techniques have attained a lower PSNR of 51.60dB, 52.95dB, and 63.36dB respectively. In addition, with House image, the MHE-TLBO approach has accomplished a superior PSNR of 57.34dB whereas the HE, MHE, and MHE-AWO methods have reached a minimum PSNR of 56.37dB, 53.98dB, and 56.37dB correspondingly. Moreover, with Pepper image, the MHE-TLBO manner has accomplished a maximum PSNR of 59.10dB whereas the HE, MHE, and MHE-AWO techniques have gained a reduced PSNR of 55.58dB, 53.36dB, and 58.13dB respectively. Furthermore, with Baboon image, the MHE-TLBO technique has accomplished a higher PSNR of 56.67dB whereas the HE, MHE, and MHE-AWO approaches have achieved a minimum PSNR of 52.69dB, 52.82dB, and 55.83dB correspondingly.

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021

Table 1 PSNR analysis of MHE-TLBO model on different test images

PSNR (dB)				
Methods	**Lena**	**House**	**Pepper**	**Baboon**
HE	51.60	56.37	55.58	52.69
MHE	52.95	53.98	53.36	52.82
MHE-AWO	63.36	56.37	58.13	55.83
MHE-TLBO	65.12	57.34	59.10	56.67

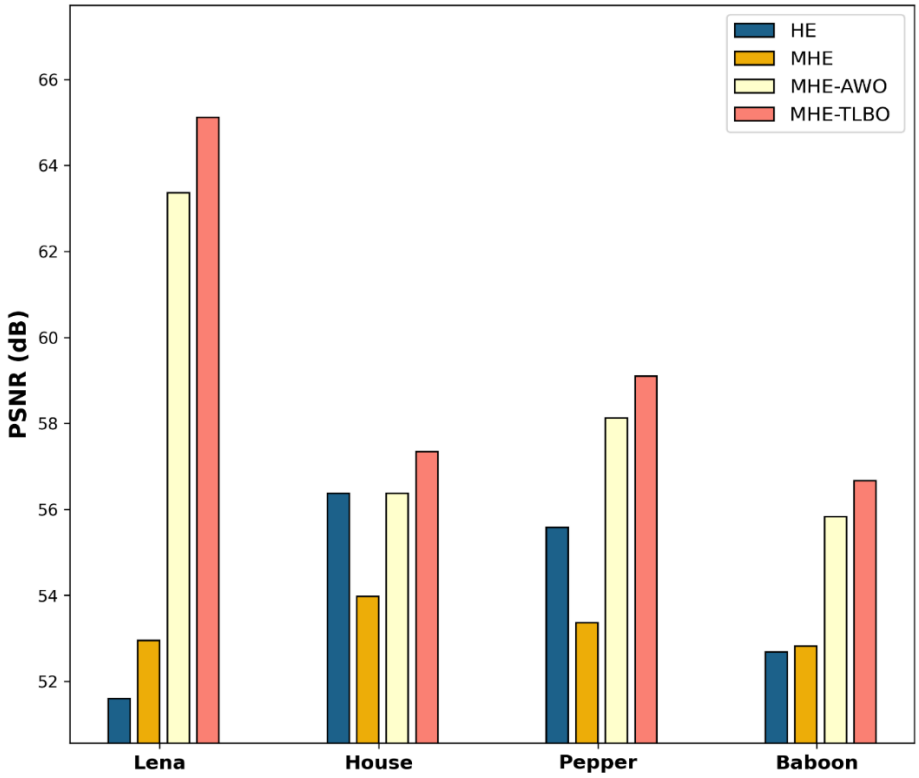

Fig. 2. Comparative PSNR analysis of MHE-TLBO model

Table 2 and Fig. 3 showcases the MSE analysis of the MHE-TLBO model with other existing techniques. The figure depicted that the MHE-TLBO technique has accomplished a higher PSNR under the applied test images. For instance, with Lena image, the MHE-TLBO technique has accomplished a higher PSNR of 0.02 whereas the HE, MHE, and MHE-AWO techniques have attained a lower PSNR of 0.45, 0.33, and 0.03 respectively. Followed by, with House image, the MHE-TLBO method has accomplished a superior PSNR of 0.12 whereas the HE, MHE, and MHE-AWO algorithms have reached a minimal PSNR of 0.15, 0.26, and 0.15 correspondingly. Along, with Pepper image, the MHE-TLBO method has accomplished an increased PSNR of 0.08 whereas the HE, MHE, and MHE-AWO algorithms have attained a lower PSNR of 0.18, 0.3, and 0.1 correspondingly. In line with, with Baboon image, the MHE-TLBO technique has accomplished an improved PSNR of 0.14 whereas the HE, MHE, and MHE-AWO methodologies have gained a lesser PSNR of 0.35, 0.34, and 0.17 correspondingly.

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021

Table 2 MSE analysis of MHE-TLBO model on different test images

MSE				
Methods	**Lena**	**House**	**Pepper**	**Baboon**
HE	0.45	0.15	0.18	0.35
MHE	0.33	0.26	0.3	0.34
MHE-AWO	0.03	0.15	0.1	0.17
MHE-TLBO	0.02	0.12	0.08	0.14

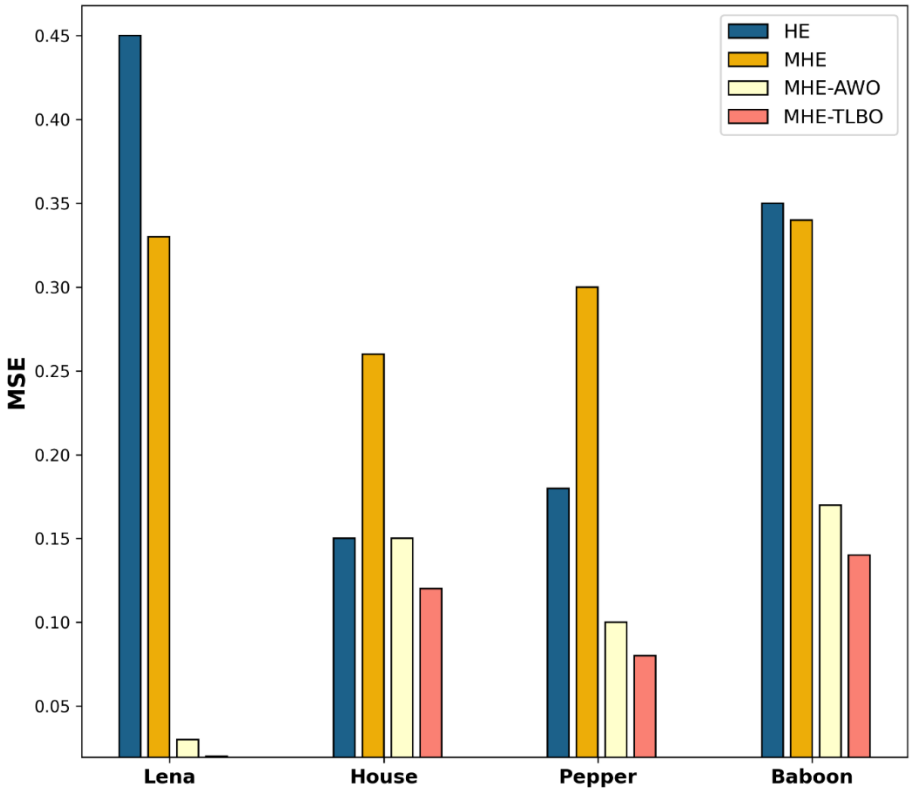

Fig. 3. Comparative MSE analysis of MHE-TLBO model on different test images

Table 3 portrays the outcome analysis of the MHE-TLBO manner with other existing algorithms. The figure demonstrated that the MHE-TLBO technique has gained maximum CC under the applied test images. For sample, with Lena image, the MHE-TLBO manner has accomplished an increased CC of 0.98 whereas the HE, MHE, and MHE-AWO techniques have reached a least CC of 0.93, 0.79, and 0.95 correspondingly. Then, with House image, the MHE-TLBO technique has accomplished a higher CC of 0.96 whereas the HE, MHE, and MHE-AWO methodologies have attained a decreased CC of 0.92, 0.90, and 0.94 respectively. Followed by Pepper image, the MHE-TLBO algorithm has accomplished a higher CC of 0.98 whereas the HE, MHE, and MHE-AWO techniques have attained a lower CC of 0.92, 0.95, and 0.96 correspondingly. Besides, with Baboon image, the MHE-TLBO manner has accomplished a superior CC of 0.99 whereas the HE, MHE, and MHE-AWO techniques have reached a minimum CC of 0.90, 0.96, and 0.97 correspondingly.

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021

Table 3 CC analysis of MHE-TLBO model on different test images

CC				
Methods	**Lena**	**House**	**Pepper**	**Baboon**
HE	0.93	0.92	0.92	0.90
MHE	0.79	0.90	0.95	0.96
MHE-AWO	0.95	0.94	0.96	0.97
MHE-TLBO	0.98	0.96	0.98	0.99

4. Conclusion

This study has designed a new MHE-TLBO algorithm to ensure security in image transmission. The goal of the MHE-TLBO algorithm is to optimally select multiple keys using TLBO algorithm for encryption and decryption processes. In addition, the MHE-TLBO algorithm has derived a fitness function involving peak signal to noise ratio (PSNR) and thereby ensures the superior quality of the reconstructed image. For validating the security performance of the MHE-TLBO algorithm, a comprehensive result analysis is made and the results are investigated interms of diverse aspects. The simulation results highlighted the improved security performance of the MHE-TLBO algorithm over the recent image encryption approaches. In future, the MHE-TLBO algorithm can be extended to secure video transmission in IoT environment.

References

[1] Noshadian, S., Ebrahimzade, A. and Kazemitabar, S.J., 2018. Optimizing chaos based image encryption. Multimedia Tools and Applications, 77(19), pp.25569-25590.

[2] Li, G.D., 2019. Double chaotic image encryption algorithm based on optimal sequence solution and fractional transform. The Visual Computer, 35(9), pp.1267-1277.

[3] Abdullah, A.H., Enayatifar, R. and Lee, M., 2012. A hybrid genetic algorithm and chaotic function model for image encryption. AEU-International Journal of Electronics and Communications, 66(10), pp.806-816.

[4] Enayatifar, R., Abdullah, A.H. and Isnin, I.F., 2014. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. Optics and Lasers in Engineering, 56, pp.83-93.

[5] An, F.P. and Liu, J.E., 2019. Image encryption algorithm based on adaptive wavelet chaos. Journal of Sensors, 2019.

[6] Shankar, K. and Eswaran, P., 2016. An efficient image encryption technique based on optimized key generation in ECC using genetic algorithm. In Artificial intelligence and evolutionary computations in engineering systems (pp. 705-714). Springer, New Delhi.

[7] Soni, A. and Agrawal, S., 2012. Using genetic algorithm for symmetric key generation in image encryption. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(10), pp.137-140.

[8] Niu, Y., Zhou, Z. and Zhang, X., 2020. An image encryption approach based on chaotic maps and genetic operations. Multimedia Tools and Applications, 79(35), pp.25613-25633.

[9] Noshadian, S., Ebrahimzade, A. and Kazemitabar, S.J., 2020. Breaking a chaotic image encryption algorithm. Multimedia Tools and Applications, 79(35), pp.25635-25655.

[10] Pashakolaee, P.G., Shahhoseini, H.S. and Mollajafari, M., 2018. Hyper-chaotic Feeded GA (HFGA): a reversible optimization technique for robust and sensitive image encryption. Multimedia Tools and Applications, 77(16), pp.20385-20414.

[11] Kaur, M. and Kumar, V., 2018. Adaptive differential evolution-based lorenz chaotic system for image encryption. Arabian Journal for Science and Engineering, 43(12), pp.8127-8144.

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021

[12] Enayatifar, R., Abdullah, A.H. and Lee, M., 2013. A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption. Optics and Lasers in Engineering, 51(9), pp.1066-1077.
[13] Khan, L.S., Hazzazi, M.M., Khan, M. and Jamal, S.S., 2021. A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes. Chinese Journal of Physics.
[14] Zeng, J. and Wang, C., 2021. A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata. Security and Communication Networks, 2021.
[15] Farah, M.A., Farah, A. and Farah, T., 2020. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 99(4), pp.3041-3064.
[16] Wang, X. and Li, Y., 2021. Chaotic image encryption algorithm based on hybrid multi-objective particle swarm optimization and DNA sequence. Optics and Lasers in Engineering, 137, p.106393.
[17] Kaur, M. and Singh, D., 2021. Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption. Multidimensional Systems and Signal Processing, 32(1), pp.281-301.
[18] Yin, S. and Li, H., 2020. GSAPSO-MQC: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system. Evolutionary Intelligence, pp.1-13.
[19] Ghazvini, M., Mirzadi, M. and Parvar, N., 2020. A modified method for image encryption based on chaotic map and genetic algorithm. Multimedia Tools and Applications, 79(37), pp.26927-26950.
[20] Shankar, K. and Lakshmanaprabu, S.K., 2018. Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology, 7(9), pp.22-27.
[21] Shankar, K., Lakshmanaprabu, S.K., Gupta, D., Khanna, A. and de Albuquerque, V.H.C., 2020. Adaptive optimal multi key based encryption for digital image security. Concurrency and Computation: Practice and Experience, 32(4), p.e5122.
[22] Singh, M., Panigrahi, B.K. and Abhyankar, A.R., 2013. Optimal coordination of directional over-current relays using Teaching Learning-Based Optimization (TLBO) algorithm. International Journal of Electrical Power & Energy Systems, 50, pp.33-41.

DOI: 10.5281/zenodo.5497654
Received: April 15, 2021 Accepted: August 02, 2021