

## Improved Multileader Optimization with Shadow Encryption for Medical Images in IoT Environment

Mesfer Al Duhayyim<sup>1,\*</sup>, Mohammed Maray<sup>2</sup>, Ayman Qahmash<sup>2</sup>, Fatma S. Alrayes<sup>3</sup>,  
Nuha Alshuqayran<sup>4</sup>, Jaber S. Alzahrani<sup>5</sup>, Mohammed Alghamdi<sup>2,6</sup> and Abdullah Mohamed<sup>7</sup>

<sup>1</sup>Department of Computer Science, College of Sciences and Humanities-Aflaj, Prince Sattam Bin Abdulaziz University, Saudi Arabia

<sup>2</sup>Department of Information Systems, College of Computer Science, King Khalid University, Abha, Saudi Arabia

<sup>3</sup>Department of Information Systems, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, P.O. Box 84428, Riyadh 11671, Saudi Arabia

<sup>4</sup>Department of Information Systems, College of Computer and Information Sciences, Imam Mohammad Ibn Saud Islamic University, Saudi Arabia

<sup>5</sup>Department of Industrial Engineering, College of Engineering at Alqunfudah, Umm Al-Qura University, Saudi Arabia

<sup>6</sup>Department of Information and Technology Systems, College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia

<sup>7</sup>Research Centre, Future University in Egypt, New Cairo, 11845, Egypt

\*Corresponding Author: Mesfer Al Duhayyim. Email: m.alduhayyim@psau.edu.sa

Received: 28 May 2022; Accepted: 05 July 2022

**Abstract:** Nowadays, security plays an important role in Internet of Things (IoT) environment especially in medical services' domains like disease prediction and medical data storage. In healthcare sector, huge volumes of data are generated on a daily basis, owing to the involvement of advanced health care devices. In general terms, health care images are highly sensitive to alterations due to which any modifications in its content can result in faulty diagnosis. At the same time, it is also significant to maintain the delicate contents of health care images during reconstruction stage. Therefore, an encryption system is required in order to raise the privacy and security of healthcare data by not leaking any sensitive data. The current study introduces Improved Multileader Optimization with Shadow Image Encryption for Medical Image Security (IMLOSIE-MIS) technique for IoT environment. The aim of the proposed IMLOSIE-MIS model is to accomplish security by generating shadows and encrypting them effectively. To do so, the presented IMLOSIE-MIS model initially generates a set of shadows for every input medical image. Besides, shadow image encryption process takes place with the help of Multileader Optimization (MLO) with Homomorphic Encryption (IMLO-HE) technique, where the optimal keys are generated with the help of MLO algorithm. On the receiver side, decryption process is initially carried out and shadow image reconstruction process is conducted. The experimentation analysis was carried out on medical images and the results inferred that the proposed IMLOSIE-MIS model is an excellent performer compared to other models.



This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The comparison study outcomes demonstrate that IMLOSIE-MIS model is robust and offers high security in IoT-enabled healthcare environment.

**Keywords:** Medical image security; image encryption; shadow images; homomorphic encryption; optimal key generation

## 1 Introduction

The current technological advancements and development in Internet of Things (IoT) alleviate the individuals to employ resources across the globe. This rapid advancement in IoT technology facilitates the patients to get consulted by clinicians worldwide. Patient information like X-rays, scan report, clinical test reports etc., can be forwarded via internet while most of the clinical data remain in image format [1]. In general, information communicated via internet is prone to attacks and vulnerabilities. Any misinterpretation or corruption of medical data, due to transitional assaults is non-tolerable. At times, it might threaten the lives of humans as well. This mandates the scheme for safe remote monitoring of medical data [2]. Various image encoding structures have been proposed earlier for ordinary images. However, in case of medical images, such techniques are incapable of preserving the patient's information. This is because of the strong correlative nature of pixels in healthcare images which tend to have adjacent pixels and other numerous modalities [3]. This complication motivated the authors to develop highly advanced strong encoding schemes [4].

Particularly, medical images such as X-rays, Magnetic Resonance Imaging (MRI), and Computed Tomography (CT) consume huge memory and have high pixel correlation. In case of no security for these images, it can be easily tampered with and attacked through illicit access. Thus, it is essential to develop highly effective health care image encoding techniques [5,6]. The demand for efficient cryptographic solutions for healthcare images need highly advanced system and its seamless application. In order to protect the image from new generations of attacks, encoding solutions must guarantee image confidentiality. Confidentiality can be achieved by encoding the data so that the data becomes unusable and unintelligible, when it is hacked or lost [7–9]. Among the available encoding schemes, symmetric encoding is the best cryptographic solution that provides heavy security for huge volumes of data [10]. In this creative ideology, chaos is considered as an efficient axis of latest cryptographic difficulties that prevail in conventional symmetric encoding systems like Advanced Encryption System (AES) [11,12]. Medical images usually contain confidential information about the patients and it is vulnerable to cyber-attacks when it is transmitted via public networks [13]. Therefore, it is mandatory to secure such images prior to transmission over public networks. The existing encoding approaches cannot provide the highest possible security since healthcare images have varied properties redundancy, higher correlation among pixels, and huge size [14]. In such case, these techniques are incapable of resisting numerous security assaults. In this background, the primary goal of this study is to design an effective image encoding method that can advance the development of complicated secret keys.

The current article introduces Improved Multileader Optimization with Shadow Image Encryption for Medical Image Security (IMLOSIE-MIS) technique for IoT environment. The proposed IMLOSIE-MIS initially generates a set of shadows for every input medical image. Besides, shadow image encryption process takes place with the help of MLO with Homomorphic Encryption (IMLO-HE) technique. Here, the optimal keys are generated using MLO algorithm. On the receiver side, decryption process is initially carried out and shadow image reconstruction process is fulfilled. The

experimentation analysis was conducted upon medical images and the results infer the superior performance of IMLOSIE-MIS model over other existing models.

## 2 Related Works

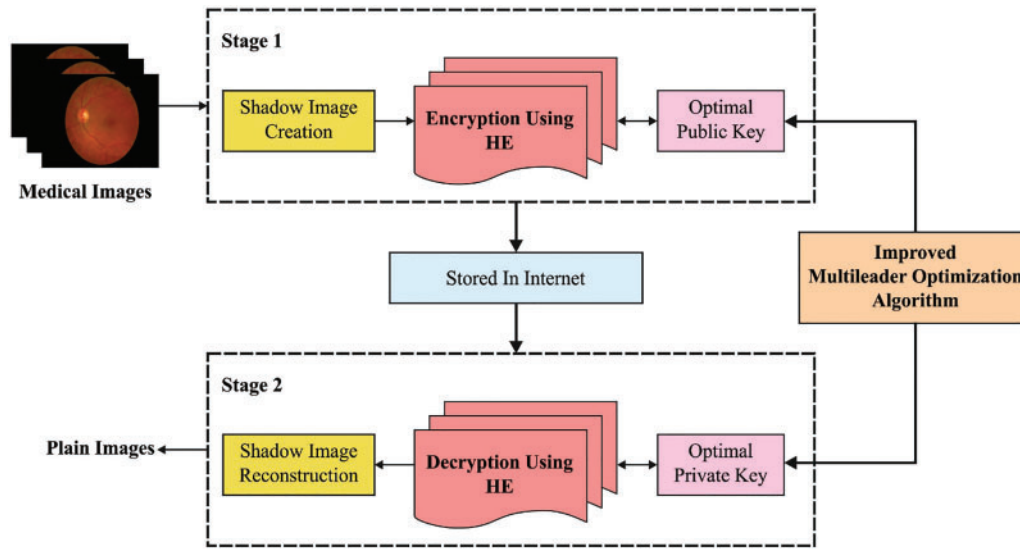
In literature [15], low-area and high-speed architectures were suggested for Secure IoT (SIT) systems under resource-limited applications. The presented pipeline infrastructure was highly helpful for high-frequency applications whereas the suggested serial architecture is advantageous for low-area necessities that result in hardware cost reduction. The dynamic size of block selection approach rescues a substantial volume of clock cycles during image encryption. Elhoseny et al. [16] inspected the safety of health care images in IoT by using a new cryptographic method with optimization strategies. Most of the times, a patient's data is saved in hospital cloud server due to security purposes. To increase the security level of decryption and encryption procedures, an optimal key has to be selected with the help of hybrid swarm optimization i.e., Particle Swarm Optimization (PSO), Elliptic Curve Cryptography (ECC) and grasshopper optimization.

In the study conducted earlier [17], a server-client authentic medical image transmission model was suggested. Previously, AES-encoded health care image is secured by embedding One Time Password (OTP) that can be generated via Tent map. Once an OTP is received via Global System for Mobile communication (GSM), the official user confirms the similarity of OTP received on their mobile, and accesses the encoded health care image. The researchers in literature [18] concentrated on disease classification using image processing method. In this study, a secure cloud computing environment was used in which a prolonged zigzag image encoded scheme was tested. This scheme showed high tolerance towards distinct data attacks. Then, a fuzzy Convolutional Neural Network (CNN) system was suggested in this study for potential image classification. The decoded images were utilized for the classification of cancer stages with distinct layers of training. Shafai et al. [19] provided a medical image cryptosystem in which Stacked Autoencoder (SAE) network is used for the generation of two sets of chaotic random matrices. Another set produces a separate series which is used for removal of association between original image and the permuted encoded medical image.

Kamal et al. [20] provided a novel encoding system for encoding both color and grey medical images. The potentiality of the suggested technique to encode medical images was assessed with the help of time complexity and security analysis. In literature [21], an Evolutionary system such as memetic system was utilized for encoding the text messages. The encoded data was inserted in medical images with the help of Discrete Wavelet Transform 1 level and 2 levels.

## 3 The Proposed Model

In current study, a new IMLOSIE-MIS model has been developed to accomplish security in IoT-enabled medical image transmission process. The proposed IMLOSIE-MIS model primarily generates a set of shadow images for the applied medical images. Followed by, IMLO-HE technique is derived to encrypt the shadow images in an effective manner. At the same time, the optimal generation of the keys, involved in HE technique, is performed by MLO algorithm in such a way that the PSNR value gets maximized. Fig. 1 is the block diagram of the proposed IMLOSIE-MIS approach.



**Figure 1:** Block diagram of IMLOSIE-MIS approach

### 3.1 Shadow Image Creation Process

In initial stage, the presented IMLOSIE-MIS model primarily generates a set of shadow images for the applied medical images. During shadow creation process, binary secret images are encrypted to 'n' shadows from wavelet sub-bands [22]. Each shadow encompasses white and black pixels in the state of clamor and is particularly larger in measurement compared to secret images. Each original pixel of the secret image appears in 'n' attuned version and is labelled as 'shadows'. Fig. 2 illustrates the structure of shadow creation process. Thus, each shadow is a collection of subpixels of RGB images as shown below.

$$R_p = \int_1^k \lim_{k \rightarrow 1, \text{to, no. of pixel}} R_{mn-Subband} \quad (1)$$

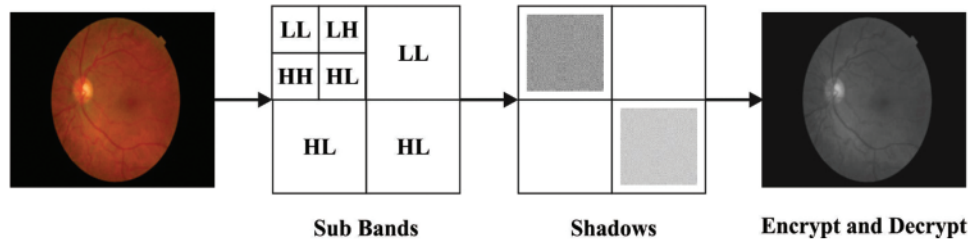
$$G_p = \int_1^k \lim_{k \rightarrow 1, \text{to, no. of pixel}} G_{mn-Subband} \quad (2)$$

$$B_p = \int_1^k \lim_{k \rightarrow 1, \text{to, no. of pixel}} B_{mn-Subband} \quad (3)$$

In the abovementioned conditions, the matrix location of every band and  $k$  denotes the overall number of pixels. At last, two shadow images are attained by shadow creation condition; visual secret share generation process is employed in the production of two shadows in all the images. The individual shadow does not reveal the secret except its size. The original secret is recreated by integrating all the shadows. In encryption technique, each secret pixel becomes two shadows whereas all the shadows belong to respective shadow images.

1. Choose the secret input images with recompense width and tallness that spread from RGB in order to gray scale the image.
2. Use wavelet transformation on luminance so as to produce four sub-bands namely  $HL$ ,  $LL$ ,  $HH$ , and  $LH$ , which are determined by high pass, low pass, fat and vertical measurements.

3. Considering the sub-bands, make two lattices to offer white mystery pixels to the same as black mystery pixels.
4. Replace the sub-bands by offer. Considering that the ultimate objective is to implement supplant tasks, it should be equal to the size of the sub-bands.
5. A reverse Discrete Wavelet Transform (DWT) is transported to restore the image.
6. Initialize variable text style shading and record values.



**Figure 2:** Shadow creation process

Visual Secret Sharing system is an effective approach to hide an image. It is completed by segregating the images into meaningless shadows. The secret can be recovered by superposing a thresholding number of shadows without unpredicted computation. The individual shadow does not reveals the secret, except their size while the shadows are transferred to a participant number.

### 3.2 Shadow Image Encryption Process

Once the shadows are created, IMLO-HE technique is implemented to encrypt the shadow images in an effective manner. In order to encrypt the image or data, Homomorphic Encryption plays a further operation that is represented as a public key cryptosystem. This process contains four functions such as encryption, key generation, decryption, and evaluation, in addition to decryption of the data for evaluation; the evaluation process offers a corresponding result which should be validated to check whether the task is performed appropriately on initial messages. The decision of the plan is subjected to the kind of processes done in the applications, detached from the variable which is used to select the encryption strategy.

In encoding and decoding processes, the related images use a symmetric key while trustworthy security and secrecy are offered in key generation process. Now, key generation technique is continued to choose further parameters for registering both public and private keys.

$$H_{pk} \text{ and } H_{sk}$$

$$K = cd \text{ and } \omega = lcm (r - 1, s - 1)$$

For this process, the keys are generated for both decryption and encryption processes in a random manner. These keys should be optimized using IMLO approach. While rest of the process in image security system involves the generation of ideal ideal public and private keys.

### 3.3 Optimal Key Generation Process

MLO technique is arithmetically modelled for the implementation of optimization problems [23]. The key objective is to exploit information from a member of the population. In such cases, a member

of the population exploits the information of diverse leaders to assess the problem-solving space as given herewith.

$$X_i = [\chi_i^1, \dots, \chi_i^d, \chi_i^m] \tag{4}$$

In Eq. (19),  $X_i$  refers to i-th member of the population and  $\chi_i^d$  specifies the d-th variable of optimization problem.

$$X^{sort} = \left[ \begin{array}{c|c|c} X_1^{sort} & X_{r_1} & \min(fit) \\ \vdots & \vdots & \vdots \\ X_N^{sort} & X_{r_N} & \max(fit) \end{array} \right] \tag{5}$$

In Eq. (20),  $X_N^{sort}$  denotes the member with worst fitness value,  $X^{sort}$  specifies the matrix of population,  $X_1^{sort}$  represents the member with optimum fitness value,  $X_{r_N}$  signifies the member of the population with worst rank-related fitness value,  $X_{r_1}$  indicates the member of population with best rank-based fitness value,  $N$  characterizes the number of members in the population, and  $fit$  shows the fitness value. After arranging the population matrix, certain members of the ranked population are selected as leaders.

$$L = \{X_l^{sort}, X_l^{sort} \in X^{sort}, l = 1 : n_L\} \tag{6}$$

$$x^{sort} = \left[ \begin{array}{c} X_1^{sort} \\ \vdots \\ X_{n_L}^{sort} \\ \vdots \\ X_N^{sort} \end{array} \right]_{N \times m} \rightarrow L = \left[ \begin{array}{c} X_1^{sort} \\ \vdots \\ X_l^{sort} \\ \vdots \\ X_{n_L}^{sort} \end{array} \right]_{n_l \times m} \tag{7}$$

In this expression,  $L$  denotes the designated leader member matrix whereas  $n_L$  indicates the leader numbers. The population in MLO is upgraded. At first, every member of the population is moved into search space based on the location of the leader. Then the leader is determined based on roulette wheel. Every leader is selected for upgrading various parameters.

$$fit_i^n = \frac{fit_i - \max(fit)}{\sum_{j=1}^N (fit_j - \max(fit))} \tag{8}$$

$$P_l = \frac{fit_l^n}{\sum_{j=1}^{n_l} fit_j^n} \tag{9}$$

$$C_l = P_l + C_{l-1}, C_0 = 0 \ \& \ l = 1 : n_l \tag{10}$$

$$L_{i,c}^d = \begin{cases} L_1 = X_1^{sort}, & 0 \leq r \leq C_1 \\ \vdots & \vdots \\ L_c = X_c^{sort}, & C_{c-1} < r \leq C_c \\ \vdots & \vdots \\ L_{n_l} = X_{n_L}^{sort}, & C_{n_l-1} \leq r \leq C_{n_l} \end{cases} \tag{11}$$

$$\chi_{i,new}^d = \chi_i^d + rand (L_{i,c}^d - 2 \times x_i^d) \tag{12}$$

$$X_i = \begin{cases} X_{i,new}, & fit_{i,new} \leq fit_i \\ X_i, & else \end{cases} \tag{13}$$

Here,  $fit_i^n$  specifies the standardized fitness function for  $i$ -th population member,  $P_l$  represents the possibility of selecting  $l$ -th leader to guide the variable,  $C_l$  indicates the cumulative possibility of  $l$ -th leader,  $x_{i,new}^d$  indicates the updated value for  $d$ -th parameter of  $i$ -th dimension,  $L_{i,c}^d$  symbolizes the  $d$ -th parameter of the selected  $c$ -th leader to guide  $d$ -th variable of  $i$ -th population member, and  $r$  indicates the arbitrary integer that lies in the interval of  $[0,1]$ . Once the updated position is highly pertinent, the member upgrades their position to current status or otherwise they return to their prior position.

$$x_{i,new}^d = x_i^d + 2 \times (1 - \frac{\tau}{T}) \times (-0.2 + rand \times 0.4) \times x_i^d \tag{14}$$

$$X_i = \begin{cases} X_{i,new'} & fit_{i,new'} \leq fit_i \\ X_i, & else \end{cases} \tag{15}$$

In this expression,  $t$  represents the  $t^{th}$  iteration and  $T$  indicates the maximum number of iterations. MLO algorithm is extended to the design of IMLO algorithm based on Nelder Mead (NM) concept [24]. NM model is a simple search methodology for multi-dimensional unrestricted minimization. It consists of expansion, reflection, shrinkage, and contraction. Initially,  $(n + 1)$  point  $x_1, x_2, \dots, x_{n+1}$  is initialized in  $D$ -dimensional searching space. Such points are arranged in ascending sequence based on the fitness value. The centroid point  $\bar{X}$  is comprised of initial  $n$  point which is evaluated as follows.

$$\bar{x} = \sum_{i=1}^n \frac{\chi_i}{n} \tag{16}$$

Next, the reflection point  $\chi_r$  is shown below.

$$x_r = \bar{x} + \rho (\bar{x} - x_{n+1}) \tag{17}$$

In Eq. (17)  $\rho > 0$  refers to reflection coefficient, and  $x_{n+1}$  denotes the worst point. Then, the expansion point  $x_e$  is evaluated by the following expression.

$$x_e = \bar{x} + \chi (x_r - \bar{x}) \tag{18}$$

In Eq. (18),  $\chi > \max\{1, \rho\}$  indicates the expansion coefficient. When the fitness of reflection point  $x_r$  is worst than the secondary worst  $x_n$ , it is essential to implement inside or outside contraction. Now, the fitness of point represents the function value. Once the fitness of reflection point  $x_r$  is superior to the worst point  $x_{n+1}$ , the outside contraction operation is implemented as given below.

$$x_{0c} = \bar{x} + \gamma (x_r - \bar{x}) \tag{19}$$

Or else, the inside contraction process gets implemented.

$$x_{ic} = \bar{x} - \gamma (\bar{x} - x_{n+1}) \tag{20}$$

where  $0 < \gamma < 1$  indicates the contraction coefficient. When the fitness of outside contraction point  $x_{0c}$  is worst compared to reflection point  $x_\gamma$ , then the fitness of inside contraction point  $x_{ic}$  is worst than  $x_{n+1}$ . In such case, the shrink operation for  $i$ -th point  $x_i$  is implemented as given below.

$$v_i = x + \sigma (x - x) \quad (21)$$

If  $0 < \sigma < 1$  represents the shrink coefficient, then the comprehensive data is applicable for the four abovementioned coefficients.

IMLO algorithm defines a fitness function for optimal key generation process which defines the maximization of PSNR. PSNR defines the proportion between the possible assessment of signal and the energy of mutilating clamor that influences its nature of portrayal. Both reference and original images should be of similar class and size.

$$Fitness = Max (PSNR) \quad (22)$$

$$PSNR = \frac{1}{s} \sum_{i=1}^{shares} 10 \log_{10} (255^2 / MSE) \quad (23)$$

The PSNR condition 's', as a number in DWT, is used as shadows. In Peak Signal to Noise Ratio (PSNR), the square of peak values in the images should be assumed (in case of 8-bit images, the peak value is 255) and divided by Mean Square Error.

### 3.4 Encryption and Decryption Process

During encryption procedure analysis, an ideal public key is used for encoding all the pixels of the images. It is regarded as message bit  $m$  while the figure should be computed to notify cipher data action. With the help of confidential key  $H_{sk}$ , the client encrypts the original image  $I_p$  and create  $H_{k-opt}(I_p)$  together with public key,  $K_{pk}$ . This ciphered image  $I_c$  is sent to the server.  $H_{pk} = (k, i)$  and  $K_{sk} = (c, d)$   $Enc(I, H_{sk})$  select the arbitrary variables and cipher data  $c = I.r^k \text{mod} k^2$  is calculated. During decryption process, the ciphered image is reviewed since it contains the encryption pixel addressed by  $(c, d)$  and the secret vector,  $s$ . Decryption method consumes two veils, particularly, the confidential mask  $\langle as \rangle$  while even the masks from steady progression. The message bit (pixel esteem)  $m$  in cipher image and another confidential parameter should be decoded. The generated  $dec(f(H_{sk-opt}))$  is decrypted by the used based on  $K_s$  and the following primary result is obtained.

$$Dec Image = \frac{L(c^a \text{mod} k_{opt}^2)}{L(i^a \text{mod} k_{opt}^2)} \text{mod } k \quad (24)$$

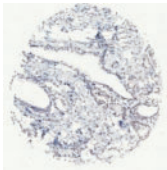
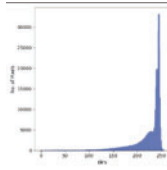
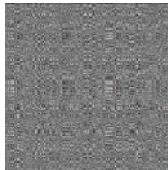

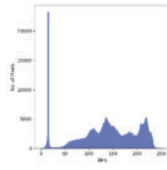
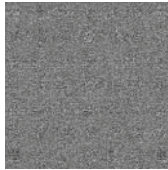
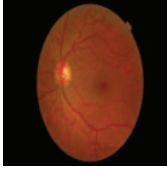
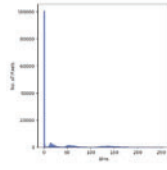
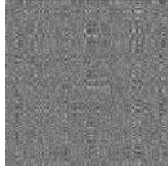
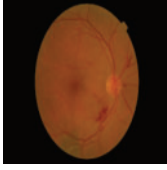
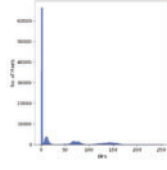
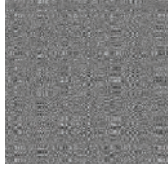

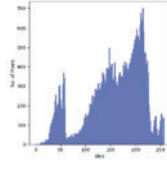

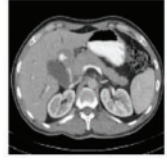
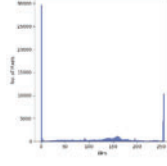

## 4 Experimental Validation

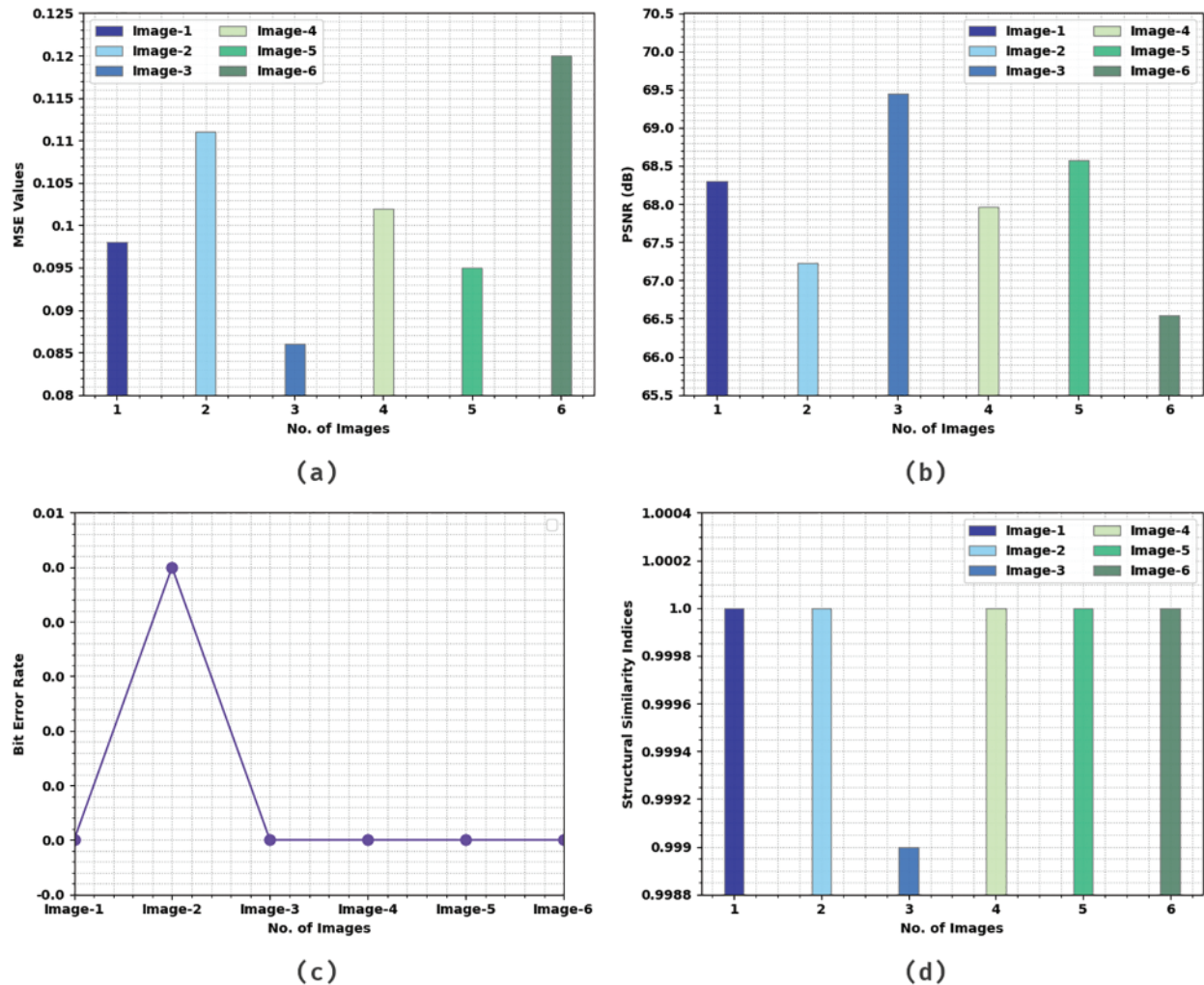
The current section validates security performances of the proposed IMLOSIE-MIS method utilizing a set of benchmark medical images. The outcomes were assessed under both presence and absence of attacks. Tab. 1 and Fig. 3 is a brief overview on the results achieved by IMLOSIE-MIS model without attacks under different measures such as Mean Square Error (MSE), PSNR, Bit Error Rate (BER), and Structural Similarity Index (SSI). The table indicates that the proposed IMLOSIE-MIS model effectively encrypted the input images. Besides, IMLOSIE-MIS model attained high PSNR and low MSE values. For instance, in image 1, the proposed IMLOSIE-MIS model achieved a high PSNR of 68.306 dB and a low MSE of 0.098. Also, in image 3, IMLOSIE-MIS technique accomplished



a high PSNR of 69.441 dB and a low MSE of 0.086. Besides, on image 6, the proposed IMLOSIE-MIS method attained a high PSNR of 66.547dB and a low MSE of 0.120.

**Table 1:** Results of the analysis of IMLOSIE-MIS technique under distinct measures without attacks

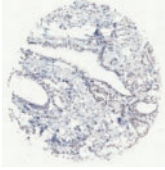

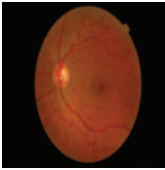
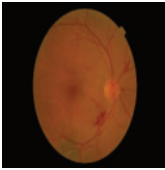
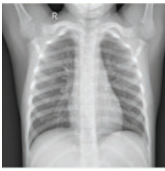

Images	Histogram	Encrypted	MSE	PSNR	BER	SSI
			0.098	68.306	0.000	1.000
			0.111	67.224	0.005	1.000
			0.086	69.441	0.000	0.999
			0.102	67.959	0.000	1.000
			0.095	68.576	0.000	1.000
			0.120	66.547	0.000	1.000

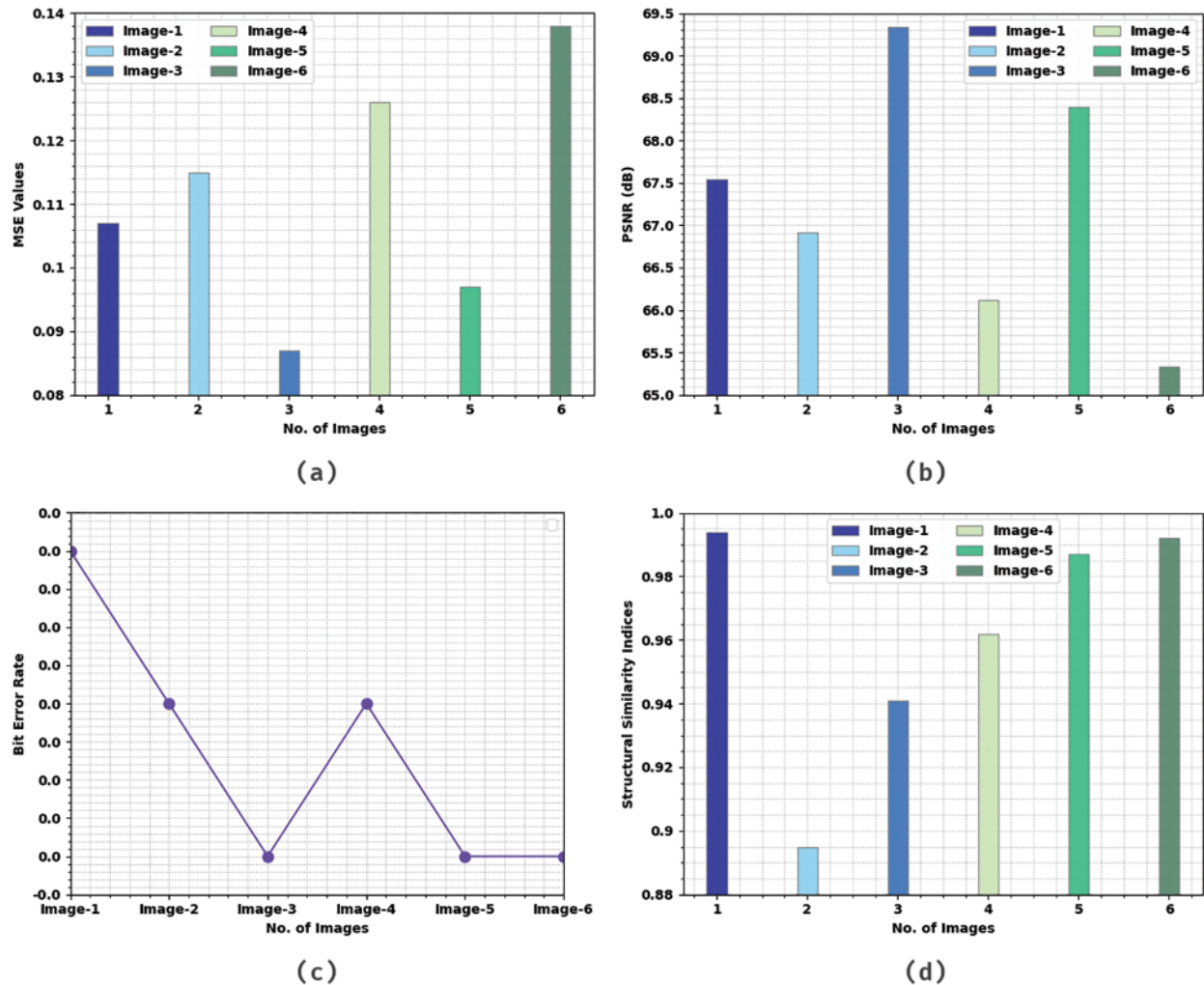


**Figure 3:** Results of the analysis of IMLOSIE-MIS technique without attacks (a) MSE, (b) PSNR, (c) BER, and (d) SSI

Tab. 2 and Fig. 4 details about the results accomplished by IMLOSIE-MIS method in the presence of attacks. The table denotes that the proposed IMLOSIE-MIS technique effectively encrypted the input images. Also, IMLOSIE-MIS methodology acquired high PSNR and low MSE values. For example, in image 1, IMLOSIE-MIS approach attained a high PSNR of 67.543 dB and a low MSE of 0.107. Additionally, in image 3, the proposed IMLOSIE-MIS algorithm achieved a high PSNR of 69.340 dB and a low MSE of 0.087. Moreover, in image 6, the proposed IMLOSIE-MIS technique achieved a high PSNR of 65.333 dB and a low MSE of 0.138.

**Table 2:** Results of the analysis of IMLOSIE-MIS technique under distinct measures with attacks

Images-attack	MSE	PSNR	BER	SSI
	0.107	67.543	0.002	0.994
	0.115	66.917	0.001	0.895
	0.087	69.340	0.000	0.941
	0.126	66.123	0.001	0.962
	0.097	68.395	0.000	0.987
	0.138	65.333	0.000	0.992

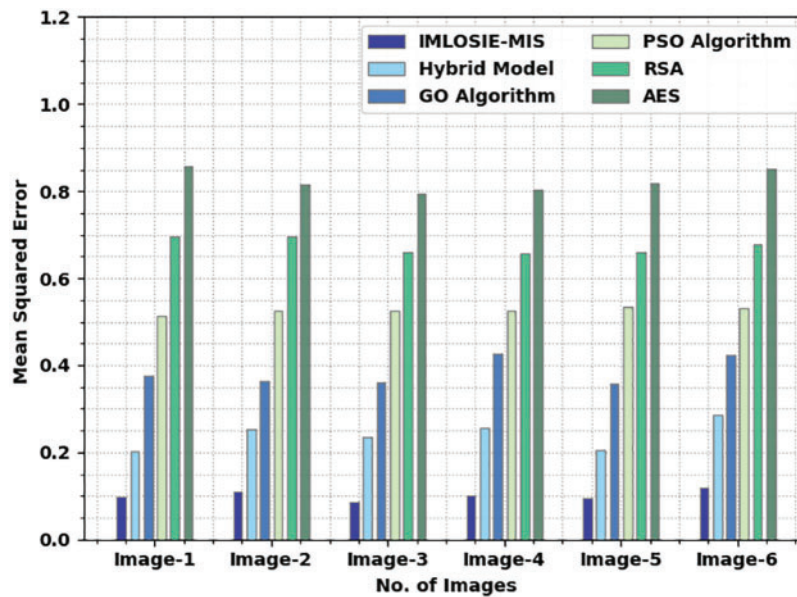


**Figure 4:** Results of the analysis of IMLOSIE-MIS technique under attacks (a) MSE, (b) PSNR, (c) BER, and (d) SSI

Tab. 3 and Fig. 5 shows the comparative MSE inspection results achieved by IMLOSIE-MIS method and other existing models. The results infer that the proposed IMLOSIE-MIS methodology produced less MSE values under all the images. For instance, on image 1, IMLOSIE-MIS technique obtained a minimal MSE of 0.098, whereas hybrid, Grasshopper Optimization (GO), PSO, Rivest, Shamir, Adleman (RSA), and AES models produced maximum MSE values such as 0.203, 0.375, 0.515, 0.695, and 0.857 respectively. Also, in image 3, the proposed IMLOSIE-MIS approach reached a minimal MSE of 0.086, whereas the hybrid, GO, PSO, RSA, and AES methodologies produced the highest MSE values such as 0.234, 0.361, 0.526, 0.66, and 0.795 correspondingly. In addition, on image 6, IMLOSIE-MIS technique attained a minimal MSE of 0.120, whereas hybrid, GO, PSO, RSA, and AES methods resulted in maximal MSE values such as 0.287, 0.425, 0.533, 0.679, and 0.853 correspondingly.

**Table 3:** MSE analysis results of IMLOSIE-MIS approach and other existing methods under distinct images

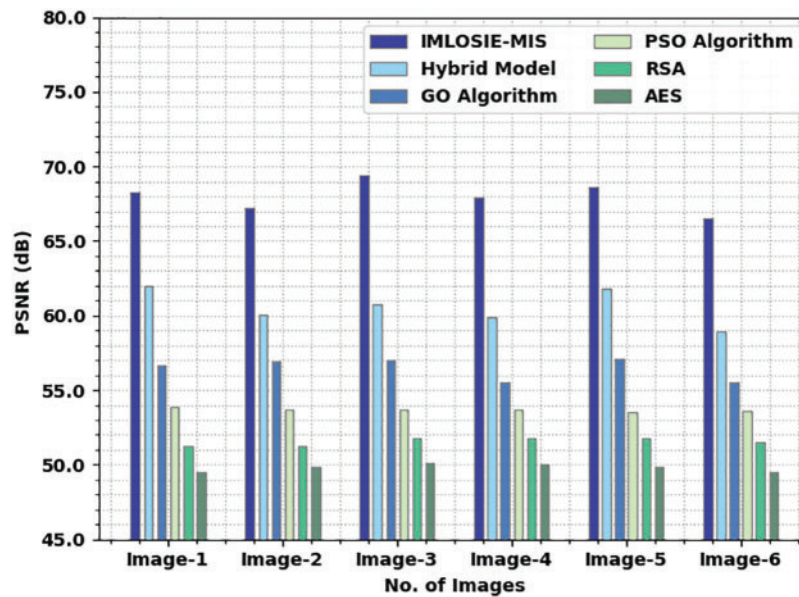
Mean squared error						
No. of images	IMLOSIE-MIS	Hybrid model	GO algorithm	PSO algorithm	RSA	AES
Image-1	0.098	0.203	0.375	0.515	0.695	0.857
Image-2	0.111	0.254	0.364	0.525	0.696	0.816
Image-3	0.086	0.234	0.361	0.526	0.66	0.795
Image-4	0.102	0.257	0.426	0.527	0.658	0.803
Image-5	0.095	0.207	0.357	0.536	0.659	0.819
Image-6	0.120	0.287	0.425	0.533	0.679	0.853

**Figure 5:** MSE analysis of IMLOSIE-MIS approach under distinct images

A comparative PSNR inspection was conducted between IMLOSIE-MIS model and other models under distinct images and the results are shown in [Tab. 4](#) and [Fig. 6](#). The experimental values indicate that the proposed IMLOSIE-MIS model achieved a superior performance with maximum PSNR values. For instance, in image 1, the proposed IMLOSIE-MIS model achieved a high PSNR of 68.306 dB, whereas the hybrid, GO, PSO, RSA, and AES models gained low PSNR values such as 61.981, 56.650, 53.895, 51.291, and 49.471 dB respectively. Concurrently, in image 3, the proposed IMLOSIE-MIS technique produced an improved PSNR of 69.441 dB, whereas the hybrid, GO, PSO, RSA, and AES methods accomplished low PSNR values such as 60.746, 56.981, 53.711, 51.740, and 50.123 dB correspondingly. Eventually, on image 6, the proposed IMLOSIE-MIS method resulted in improved PSNR of 68.306 dB, whereas the hybrid, GO, PSO, RSA, and AES approaches reached low PSNR values such as 58.973, 55.563, 53.596, 51.493, and 49.512 dB correspondingly.

**Table 4:** PSNR analysis results of IMLOSIE-MIS approach and other existing methods under distinct images

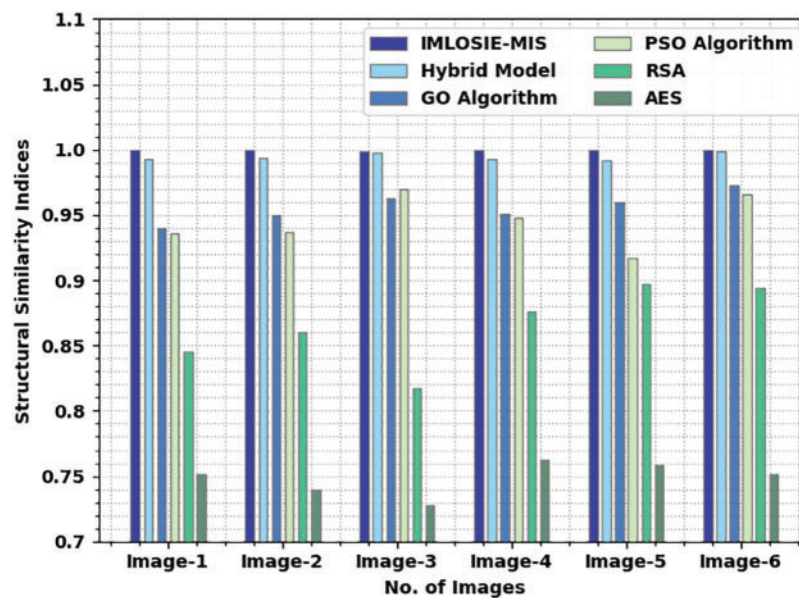
PSNR (dB)						
No. of images	IMLOSIE-MIS	Hybrid model	GO algorithm	PSO algorithm	RSA	AES
Image-1	68.306	61.981	56.650	53.895	51.291	49.471
Image-2	67.224	60.034	56.909	53.728	51.279	49.897
Image-3	69.441	60.746	56.981	53.711	51.740	50.123
Image-4	67.959	59.932	55.543	53.695	51.766	50.036
Image-5	68.576	61.811	57.077	53.548	51.753	49.865
Image-6	66.547	58.973	55.563	53.596	51.493	49.512

**Figure 6:** PSNR analysis results of IMLOSIE-MIS approach under distinct images

A comparative SSI investigation was conducted between the proposed IMLOSIE-MIS approach and other existing methodologies under distinct images and the results are shown in [Tab. 5](#) and [Fig. 7](#). The experimental values denote that the proposed IMLOSIE-MIS technique outperformed all other methods and achieved a superior performance with maximal SSI values. For instance, on image 1, IMLOSIE-MIS method resulted in improved SSI of 1.000, whereas the hybrid, GO, PSO, RSA, and AES models gained low SSI values such as 0.993, 0.940, 0.936, 0.845, and 0.752 correspondingly.

**Table 5:** SSI analysis results of IMLOSIE-MIS approach and other existing methods under distinct images

SSI						
No. of images	IMLOSIE-MIS	Hybrid model	GO algorithm	PSO algorithm	RSA	AES
Image-1	1.000	0.993	0.940	0.936	0.845	0.752
Image-2	1.000	0.994	0.950	0.937	0.860	0.740
Image-3	0.999	0.998	0.963	0.970	0.817	0.728
Image-4	1.000	0.993	0.951	0.948	0.876	0.763
Image-5	1.000	0.992	0.960	0.917	0.897	0.759
Image-6	1.000	0.999	0.973	0.966	0.894	0.752

**Figure 7:** SSI analysis results of IMLOSIE-MIS approach under distinct images

Simultaneously, on image 3, the proposed IMLOSIE-MIS methodology achieved an improved SSI of 0.999, whereas hybrid, GO, PSO, RSA, and AES techniques accomplished low SSI values such as 0.998, 0.963, 0.970, 0.817, and 0.728 correspondingly. Finally, on image 6, IMLOSIE-MIS method resulted in enhanced SSI of 1.000, whereas the hybrid, GO, PSO, RSA, and AES models attained low SSI values such as 0.999, 0.973, 0.966 B, 0.894, and 0.752 correspondingly.

## 5 Conclusion

In this study, a new IMLOSIE-MIS technique has been developed to accomplish security in IoT-enabled medical image transmission process. The proposed IMLOSIE-MIS model primarily generates a set of shadow images for the applied medical images. Then, IMLO-HE technique is implemented to encode the shadow images in an effective manner. At the same time, the optimal generation of the keys

involved in HE technique is accomplished by MLO algorithm in such a way that the PSNR values get maximized. At the receiver point, decryption process is initially carried out along with shadow image reconstruction process. The experimentation analysis was carried out on the medical images and the results exhibit that the proposed IMLOSIE-MIS model achieved better results than the existing techniques. The comparison analysis results demonstrate that IMLOSIE-MIS model is robust and offers high security in IoT-enabled healthcare environment. In future, disease diagnosis module can be included in the proposed model to enable medical image classification process.

**Funding Statement:** The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work through Small Groups Project under Grant Number (241/43). Princess Nourah Bint Abdulrahman University Researchers Supporting Project number (PNURSP2022R319), Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4340237DSR30).

**Conflicts of Interest:** The authors declare that they have no conflicts of interest to report regarding the present study.

## References

- [1] J. Khan, J. Li, A. U. Haq, S. Parveen, G. A. Khan *et al.*, “Medical image encryption into smart healthcare IoT system,” in *2019 16th Int. Computer Conf. on Wavelet Active Media Technology and Information Processing*, Chengdu, China, pp. 378–382, 2019.
- [2] M. K. Hasan, S. Islam, R. Sulaiman, S. Khan, A. H. A. Hashim *et al.*, “Lightweight encryption technique to enhance medical image security on internet of medical things applications,” *IEEE Access*, vol. 9, pp. 47731–47742, 2021.
- [3] T. K. A. Shayea, C. X. Mavromoustakis, J. M. Batalla and G. Mastorakis, “A hybridized methodology of different wavelet transformations targeting medical images in IoT infrastructure,” *Measurement*, vol. 148, pp. 106813, 2019.
- [4] M. Shen, Y. Deng, L. Zhu, X. Du and N. Guizani, “Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach,” *IEEE Network*, vol. 33, no. 5, pp. 27–33, 2019.
- [5] V. Sangavi and P. Thangavel, “An exotic multi-dimensional conceptualization for medical image encryption exerting Rossler system and Sine map,” *Journal of Information Security and Applications*, vol. 55, no. 8, pp. 102626, 2020.
- [6] A. A. Malibari, F. N. Al-Wesabi, M. Obayya, M. A. Alkhonaini, A. A. Hamza *et al.*, “Arithmetic optimization with RetinaNet model for motor imagery classification on brain computer interface,” *Journal of Healthcare Engineering*, vol. 2022, no. 1, pp. 1–11, 2022.
- [7] M. V. Narayana, C. S. Lakshmi and R. Sayal, “Medical image cryptanalysis using adaptive, lightweight neural network based algorithm for IoT based secured cloud storage,” *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, pp. 167–173, 2022.
- [8] M. A. Hamza, S. B. Haj Hassine, I. Abunadi, F. N. Al-Wesabi, H. Alsolai *et al.*, “Feature selection with optimal stacked sparse autoencoder for data mining,” *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2581–2596, 2022.
- [9] A. A. Albraikan, S. B. H. Hassine, S. M. Fati, F. N. A. Wesabi, A. M. Hilal *et al.*, “Optimal deep learning-based cyberattack detection and classification technique on social networks,” *Computers, Materials & Continua*, vol. 72, no. 1, pp. 907–923, 2022.
- [10] M. A. Alohal, F. N. Al-Wesabi, A. M. Hilal, S. Goel, D. Gupta *et al.*, “Artificial intelligence enabled intrusion detection systems for cognitive cyber-physical systems in industry 4.0 environment,” *Cognitive Neurodynamics*, vol. 42, no. 3, pp. 16, 2022. <https://doi.org/10.1007/s11571-022-09780-8>.



- [11] K. Shankar, D. Taniar, E. Yang and O. Yi, "Secure and optimal secret sharing scheme for color images," *Mathematics*, vol. 9, no. 19, pp. 1–20, 2021.
- [12] M. A. A. Khasawneh, I. Uddin, S. A. A. Shah, A. M. Khasawneh, L. Abualigah *et al.*, "An improved chaotic image encryption algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications," *Cluster Computing*, vol. 25, no. 2, pp. 999–1013, 2022.
- [13] V. K. Reshma, I. R. Khan, M. Niranjnamurthy, P. K. Aggarwal, S. Hemalatha *et al.*, "Hybrid block-based lightweight machine learning-based predictive models for quality preserving in the internet of things- (IoT-) based medical images with diagnostic applications," *Computational Intelligence and Neuroscience*, vol. 2022, no. 8, pp. 1–14, 2022.
- [14] A. F. S. Devaraj, G. Murugaboopathi, M. Elhoseny, K. Shankar, K. Min *et al.*, "An efficient framework for secure image archival and retrieval system using multiple secret share creation scheme," *IEEE Access*, vol. 8, pp. 144310–144320, 2020.
- [15] Z. Mishra and B. Acharya, "High throughput and low area architectures of secure IoT algorithm for medical image encryption," *Journal of Information Security and Applications*, vol. 53, pp. 102533, 2022.
- [16] M. Elhoseny, K. Shankar, S. K. Lakshmanaprabu, A. Maselena and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things," *Neural Computing and Applications*, vol. 32, no. 15, pp. 10979–10993, 2020.
- [17] S. Rajagopalan, S. Janakiraman, A. Rengarajan, S. Rethinam, S. Arumugham *et al.*, "IoT framework for secure medical image transmission," in *2018 Int. Conf. on Computer Communication and Informatics (ICCCI)*, Coimbatore, pp. 1–5, 2018.
- [18] J. Deepika, C. Rajan and T. Senthil, "Security and privacy of cloud- and IoT-based medical image diagnosis using fuzzy convolutional neural network," *Computational Intelligence and Neuroscience*, vol. 2021, no. 7, pp. 1–17, 2021.
- [19] W. E. Shafai, F. Khallaf, E. S. M. E. Rabaie and F. E. Abd El-Samie, "Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications," *Neural Computing and Applications*, 2022. <https://doi.org/10.1007/s00521-022-06994-z>.
- [20] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855–37865, 2021.
- [21] S. Doss, J. Paranthaman, S. Gopalakrishnan, A. Duraisamy, S. Pal *et al.*, "Memetic optimization with cryptographic encryption for secure medical data transmission in IoT-based distributed systems," *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1577–1594, 2021.
- [22] K. Shankar, M. Elhoseny, R. S. Kumar, S. K. Lakshmanaprabu and X. Yuan, "Secret image sharing scheme with encrypted shadow images using optimal homomorphic encryption technique," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 5, pp. 1821–1833, 2020.
- [23] T. Vaiyapuri, A. K. Dutta, I. H. Punithavathi, P. Duraipandy, S. S. Alotaibi *et al.*, "Intelligent deep-learning-enabled decision-making medical system for pancreatic tumor classification on CT images," *Healthcare*, vol. 10, no. 4, pp. 677, 2022.
- [24] A. Ebrahimzadeh and R. Khanduzi, "A directed tabu search method for solving controlled Volterra integral equations," *Mathematical Sciences*, vol. 10, no. 3, pp. 115–122, 2016.