Computers, Materials & Continua
DOI: 10.32604/cmc.2022.030267
Article

Tech Science Press

Wind Driven Optimization-Based Medical Image Encryption for Blockchain-Enabled Internet of Things Environment

C. S. S. Anupama[1], Raed Alsini[2], N. Supriya[3], E. Laxmi Lydia[4], Seifedine Kadry[5], Sang-Soo Yeo[6] and Yongsung Kim[7,*]

[1]Department of Electronics & Instrumentation Engineering, V. R. Siddhartha Engineering College, Vijayawada, 520007, India
[2]Department of Information Systems, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
[3]Department of Computer Science and Engineering, Malla Reddy Engineering College(A), Hyderabad, 500100, India
[4]Department of Computer Science and Engineering, Vignan's Institute of Information Technology, Visakhapatnam, 530049, India
[5]Department of Applied Data Science, Noroff University College, 4612, Kristiansand, Norway
[6]Department of Computer Engineering, Mokwon University, Daejeon, 35349, Korea
[7]Department of Technology Education, Chungnam National University 99, Daehak-ro, Yuseong-gu, Daejeon, 34134, Korea
*Corresponding Author: Yongsung Kim. Email: kys1001@cnu.ac.kr

Received: 22 March 2022; Accepted: 04 May 2022

Abstract: Internet of Things (IoT) and blockchain receive significant interest owing to their applicability in different application areas such as healthcare, finance, transportation, etc. Medical image security and privacy become a critical part of the healthcare sector where digital images and related patient details are communicated over the public networks. This paper presents a new wind driven optimization algorithm based medical image encryption (WDOA-MIE) technique for blockchain enabled IoT environments. The WDOA-MIE model involves three major processes namely data collection, image encryption, optimal key generation, and data transmission. Initially, the medical images were captured from the patient using IoT devices. Then, the captured images are encrypted using signcryption technique. In addition, for improving the performance of the signcryption technique, the optimal key generation procedure was applied by WDOA algorithm. The goal of the WDOA-MIE algorithm is to derive a fitness function dependent upon peak signal to noise ratio (PSNR). Upon successful encryption of images, the IoT devices transmit to the closest server for storing it in the blockchain securely. The performance of the presented method was analyzed utilizing the benchmark medical image dataset. The security and the performance analysis determine that the presented technique offers better security with maximum PSNR of 60.7036 dB.

Keywords: Internet of things; image security; medical images; encryption; optimal key generation; blockchain

1 Introduction

With the fast advancement in medical innovation, it became normal to analyze different sicknesses utilizing medical images. Medical images are communicated through various organizations; hence, getting these images turned into a fundamental theme lately [1]. Safe transmission of medical images requires secrecy, trustworthiness, and validation. Unapproved use of such images might prompt loss of security of patients' information [2]. The Internet of Things (IoT) characterizes the idea of associated gadgets and objects of numerous types over the web, remote, or wired. For example, the most recent movements from 1G to 5G organizations assume a significant part in the IoT applications and frameworks. This idea draws in scientists' interest and consideration about the conceivable protection and security chances, especially with high transmission capacity and recurrence [3]. The short frequency is probably going to change the framework, making a requirement for more base stations serving a similar area covered by the other remote system [4]. The absence of gadget refreshes, oblivious utilization of the gadgets without understanding the related outcomes, and change of passwords have expanded the cybersecurity access and dangers to malignant uses of touchy information on IoT frameworks [5]. The unseemly security components increment the chance of an information break, among different dangers. Additional, one of the security specialists consider that IoT gadgets give weak focus to digital assaults due to powerless security strategies and conventions [6]. Notwithstanding the few security systems that have been created and set up to safeguard IoT gadgets from digital assaults, rules on arising security challenges are satisfactorily recorded. This implies that the end-client can't utilize defensive measures to turn away the assaults on information. Overseeing IoT-empowered security thinks about three contemplations.

To start with, perceive the gadgets as associated with an organization. Second, decide and uphold what different frameworks, applications, and devices convey [7]. In conclusion, guarantee that these IoT gadgets have disrupted different gadgets in the organization or the associations assuming something turns out badly. The openness of IoT applications permits to make a finding, make duplicates, information, and recover an enormous number of advanced images all over the planet. It regularly brings about the creation of ill-conceived duplicates or unapproved use in concern [8]. In this manner, to safeguard images, numerous scientists have zeroed in on creating procedures for image security in IoT applications [9]. To get each kind of image, for instance, medical images, numerous innovations have been grown up until this point. Encryption is among these innovations the most unconstrained and proficient method for changing images into unnoticed examples. Just with the upholding right (secret) key, would the first image be able to be recuperated productively [10]. A few image encryptions plans have as of late been proposed which can be utilized to safeguard high-security medical images.

This paper presents a new wind driven optimization algorithm based medical image encryption (WDOA-MIE) technique for blockchain enabled IoT environments. The WDOA-MIE model involves three major processes namely data collection, image encryption, optimal key generation, and data transmission. Initially, the medical images are captured from the patient using IoT devices. Then, the captured images are encrypted using signcryption technique. Moreover, for improving the performance of the signcryption technique, the optimal key generation process was applied by WDOA algorithm. The performance of the presented algorithm was examined using the benchmark medical image dataset.

2 Related Works

Alqaralleh et al. [11] designed deep learning (DL) using blockchain-aided secured image communication and diagnoses method for the IoT setting. Mainly, elliptic curve cryptography (ECC) is exploited, also the optimum key generation of ECC occurs by hybridizing grasshopper using fruit-fly optimization (GO-FFO) approach. Next, the neighborhood indexing sequence (NIS) using burrow wheeler transform (BWT), named NIS-BWT was applied for encrypting the hash value. In conclusion, a DBN was employed as the classifier method for diagnosing the presence of disease. Khasawneh et al. [12] examine the parallel technique of image encryption on a massive amount of remotely sensed image from Hadoop. The Hadoop file visit technique is improved thus it could process the whole Tiff files as an individual unit. Moreover, the file setup is expanded to support Hadoop for supporting GeoTiff in Hadoop. The outcomes of the experiment show that the presented approach is scalable and effective to a massive amount of images in comparison with other familiar techniques.

Bharadwaj et al. [13] presented a simple security architecture for ensuring the secrecy of medicinal information in the transmission among IoT hops. The presented architecture employs the idea of encryption to guarantee safety. In [14], presented a V-net convolution neural network (CNN) based 4D hyperchaotic scheme for medicinal image encryption. Initially, the plaintext medicinal image is processed into 4D hyperchaotic sequential image, involving pseudorandom sequence generation, image segmentation, and chaotic system processing. Jan et al. [15] proposed an Image Encryption architecture based on Hessenberg transform and Chaotic encryption (IEFHAC), for reducing computation time and enlightening privacy when encrypting patient information. IEFHAC employs 2 1D-chaotic maps: Sine and Logistic maps for the data confusion, whereas diffusion was accomplished by employing the Hessenberg household transform. The Logistic and Sin maps were utilized for regeneration affecting output, as dynamically changes the primary parameter. Some other models are available in the literature [16–25].

3 The Proposed Model

In this article, a new WDOA-MIE technique has been developed for blockchain enabled IoT environment. The WDOA-MIE model enables the acquisition of medical images from the patient via IoT devices. Followed by, the acquired images are coded by the use of signcryption technique. For enhancing the efficacy of the signcryption technique, the optimal key generation process was applied by WDOA algorithm.

3.1 Level I: Image Encryption

At this stage, the acquired images are coded by the use of signcryption technique [26]. Signcryption is determined by a public-key primitive that performs the use of encryption and digital signature. The digital signature and encryption are considered important cryptographic tool that ensures redundancy, privacy, and reliability. However, it can be constraint with two potential objectives namely maximum processing cost and minimum efficiency. The signcryption is determined by an expanded method of cryptographic framework that is applied for implementing encryption and digital signature in a single logical stage and to limit the transmission overhead and assessment cost. A signcryption includes digital signature and encryption methods which are appropriate rather than encryption and individual signature. Assume the hybrid encryption was employed rather than utilizing easier encryption, the single session-key was treated in various encryption for achieving optimal signature-encryption in comparison to signcryption method.

The signcryption indicates the public-key primitive that constituted 2 indispensable cryptographic tool that is capable of ensuring honesty, non-repudiation, and privacy. The initialized technique initialized the prime number, hash function (HF) with key. It develops the public and private keys to the sender and receiver. To increase the information security, the presented method uses the perfect private key by enhanced method.

Initialization:- L_P denotes the massive prime numbers, L_f denotes the prime factor, I signifies the integer with order L_f modulo L_P, some randomly in $[1, \ldots ; L_P - 1]$, Hash One way HF, that result is a minimal 128 bit, L_P Keyed one way HF D Value, arbitrarily selected $\left[1, \ldots ; L_f - 1\right]$.

Sender Key pair $((M_{k1}, N_{k1}))$

$$M_{k1} = Q^{A_{k1}} \mathrm{mod}\ L_P \tag{1}$$

Receiver key pairs (M_{k2}, N_{k2})

$$N_{k2} = Q^{A_{k2}} \mathrm{mod}\ L_P \tag{2}$$

3.2 Level II: Optimal Key Generation Using WDOA

For enhancing the efficacy of the signcryption technique, the optimal key generation procedure is carried out by WDOA algorithm [27]. The stimulus of the presented WDOA develops in the atmosphere. During the atmosphere, wind blows from try for balancing the imbalance of pressures. It flows in maximal pressure regions for minimal regions at a velocity. The initial point of WDOA technique was Newton's second law of motion that was utilized for providing accurate outcomes for investigation of atmospheric motion from the Lagrangian description

$$\rho \vec{\alpha} = \sum \vec{F}_i, \tag{3}$$

whereas $\vec{\alpha}$ implies the acceleration, ρ refers the air density to infinitesimal air parcel, and $\vec{F}$ are every force performing on the air parcel. For assuming air pressure introduce the formula connection with air parcel density and temperature, the ideal gas law was provided as:

$$P = \rho RT, \tag{4}$$

In which P refers to the pressures, R signifies the universal gas constants, and T denotes the temperature. The reason for air movements are because of the integration of several forces mostly containing gravitational force ($\vec{F}_G$), pressure gradient force ($\vec{F}_{PG}$), Coriolis force ($\vec{F}_C$), and friction force ($\vec{F}_F$). The physical formulas of aforementioned force are as follows:

$$\begin{aligned} \vec{F}_G &= \rho \delta V \vec{g}, \\ \vec{F}_{PG} &= -\nabla P \delta V, \\ \vec{F}_C &= -2\Omega \times \vec{u}, \\ \vec{F}_F &= -\rho \alpha \vec{u}, \end{aligned} \tag{5}$$

In which δV refers the finite volume of air, $\vec{g}$ stands for the gravitational acceleration, ∇P denotes the pressure gradients, Ω refers the rotation of Earth, $\vec{u}$ signifies the velocity vector of winds, and α refers the friction co-efficient. The force aforementioned was added to (3). The formula is explained as

$$\rho \frac{\Delta \vec{u}}{\Delta t} = \left(\rho \delta V \vec{g}\right) + \left(-\nabla P \delta V\right) + \left(-2\Omega \times \vec{u}\right) + \left(-\rho \alpha \vec{u}\right), \tag{6}$$

whereas the acceleration $\vec{\alpha}$ in (3) is modified as $\vec{\alpha} = \vec{u}/t$; to simplicity set $\Delta t = 1$; to an infinitesimal air parcel, set $\delta V = 1$ that make simpler (6) to

$$\rho \Delta \vec{u} = \left(\rho \vec{g}\right) + \left(-\nabla P\right) + \left(-2\Omega \times \vec{u}\right) + \left(-\rho \alpha \vec{u}\right). \tag{7}$$

At the beginning of (2), the density ρ is expressed with respect to the pressure; therefore (7) is modified as;

$$\Delta \vec{u} = \vec{g} + \left(-\nabla P \frac{RT}{P_{cur}}\right) + \left(\frac{-2\Omega \times \vec{u}RT}{P_{cur}}\right) + \left(-\alpha \vec{u}\right), \tag{8}$$

In which P_{cur} refers the pressure of existing place. It can be considered in the WDOA technique which velocity as well as position of air parcels were altered at all the iterations. Therefore, $\Delta \vec{u}$ is formulated as $\Delta \vec{u} = \vec{u}_{new} - \vec{u}_{cur}$, whereas $\vec{u}$ signifies the velocity in next iterations and $\vec{u}$ refers the velocity at existing iterations. $\vec{g}$ and ∇P are vectors, it could be broken down from direction and magnitude as $\vec{g} = |g|(0 - x_{cur})$, $-\nabla P = \left|P_{opt} - P_{cur}\right| \left(x_{opt} - x_{cur}\right)$, P_{opt} refers the optimal pressure point which is establish so far, x_{opt} signifies the optimal place which is established so far, and x_{cur} refers the existing place; update (8) with the novel formula, (8) is altered as:

$$\vec{u}_{new} = (1 - \alpha)\, \vec{u}_{cur} - g x_{cur} + \left(\frac{RT}{P_{cur}} \left|P_{opt} - P_{cur}\right| \left(x_{opt} - x_{cur}\right)\right) + \left(\frac{-2\Omega \times \vec{u}RT}{P_{cur}}\right). \tag{9}$$

The formula of updating the place was explained as in (11):

$$\vec{u}_{new} = (1 - \alpha)\, \vec{u}_{cur} - g x_{cur} + \left(RT \left|1 - \frac{1}{i}\right| \left(x_{opt} - x_{cur}\right)\right) + \left(\frac{c\vec{u}_{cur}^{other\ dim}}{i}\right) \tag{10}$$

$$\vec{x}_{new} = \vec{x}_{cur} + \left(\vec{u}_{new} \times \Delta t\right), \tag{11}$$

whereas i refers the ranking amongst every air parcel and $\vec{x}_{new}$ signifies the novel place to the next iterations. WDOA is related to other nature-inspired optimized techniques, however, related to other optimized techniques, the code of WDOA is very easy and simple for implementing; it is lesser some control variables which require change.

The WDOA derived a fitness function for optimum key generation procedure, as follows.

$$fitness\,function = \max\left\{PSNR\right\} \tag{12}$$

The purpose of the WDOA is to choose the optimum key for the signcryption method that the peak signal to noise ratio (PSNR) is increased. Fig. 1 depicts the flowchart of WDOA.

3.3 Level III: Blockchain Enabled Secure Transmission

The recognized field of Blockchain is a Bitcoin Blockchain that can be determined as a ledger established to provide economic transactions via Bitcoin cryptocurrency [28]. The miners are appropriate in confirming the operation and gathering into block; miners are appropriate in solving exclusive cryptographic puzzles termed "proof-of-work," wherein a determined hash value is associated with concluding blocks. In recent times, alternative class of Blockchain model has been organized.

For example, Ethereum Blockchain Buterin provides a standardized technique by using "smart contracts" which allows the program to implement the Blockchain and implements retrieval and storage operation. Furthermore, the information is stored in inner state parameter and describes the convention procedure to alter the real state. The procedure implemented in current contracts is transmitted in transaction that is universally progressive. Such techniques are validated and measurable by miners in Ethereum Blockchain and guarantee legitimacy. This feature develops Blockchain model in healthcare field and thus, developer enhances the healthcare prediction. Fig. 2 depicts the framework of blockchain.

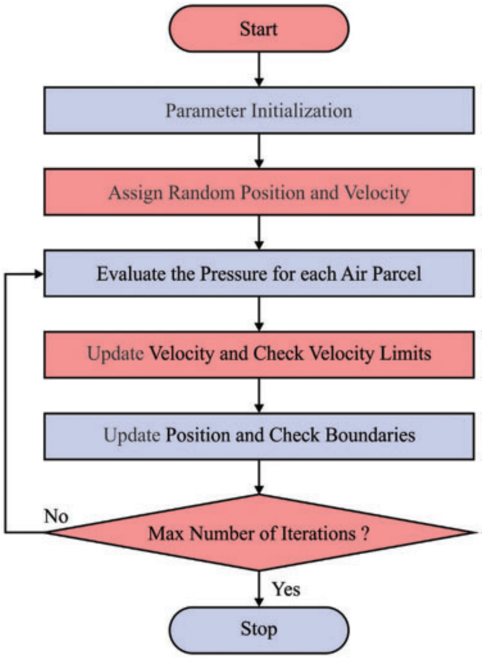
Start
Parameter Initialization
Assign Random Position and Velocity
Evaluate the Pressure for each Air Parcel
Update Velocity and Check Velocity Limits
Update Position and Check Boundaries
No
Max Number of Iterations ?
Yes
Stop

Figure 1: Flowchart of WDO algorithm

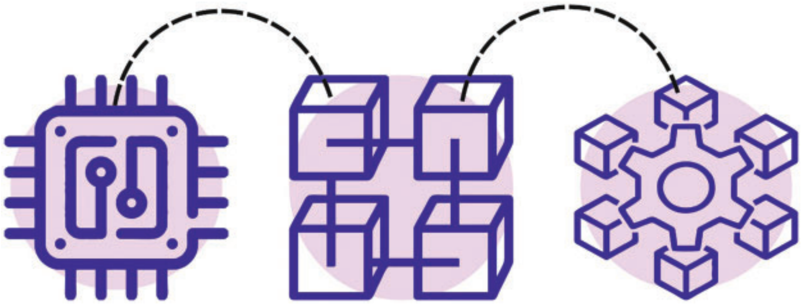

Figure 2: Structure of blockchain

4 Experimental Validation

This section portrays the results offered by the WDOA-MIE model on benchmark medical images. Fig. 3 shows the sample set of test medical images. Besides, Fig. 4 illustrates the histogram of the input and encrypted images.

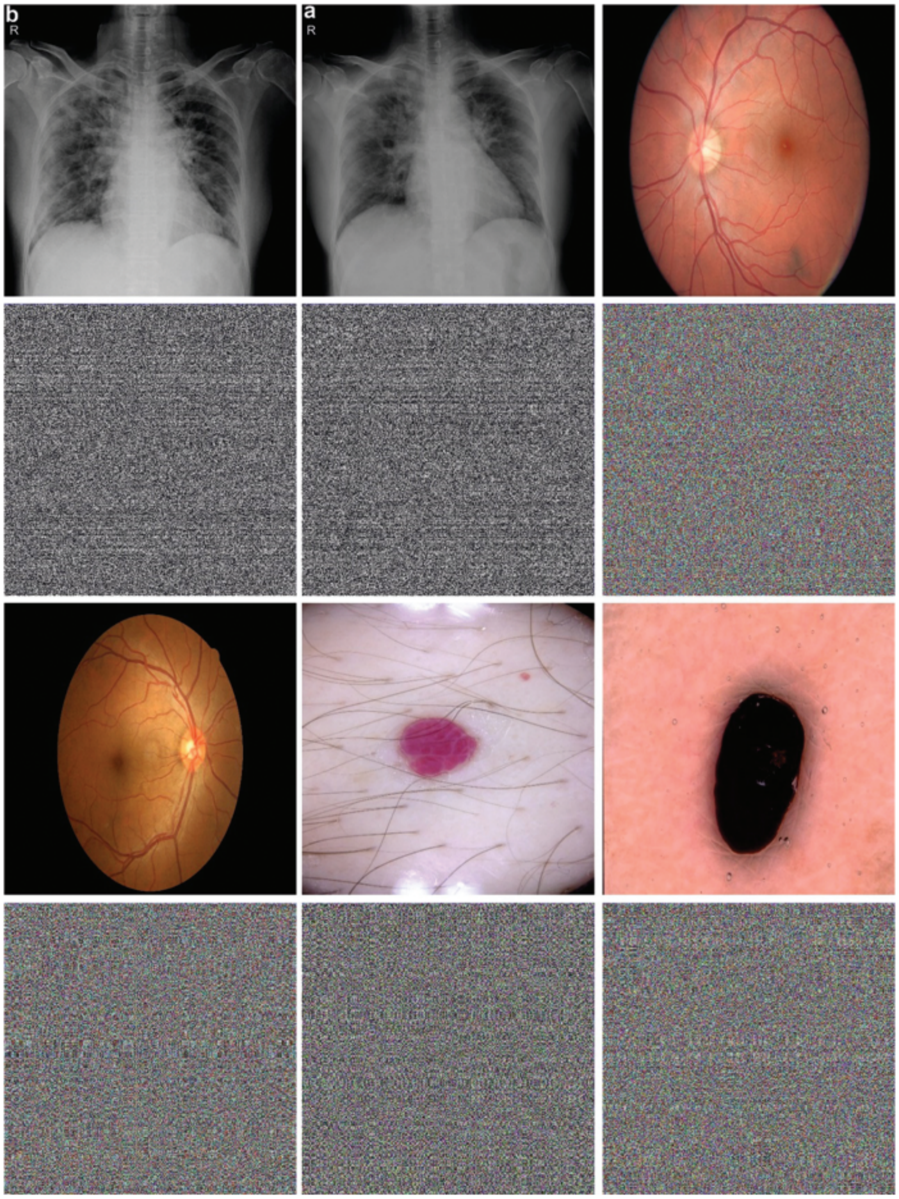

Figure 3: Sample medical images

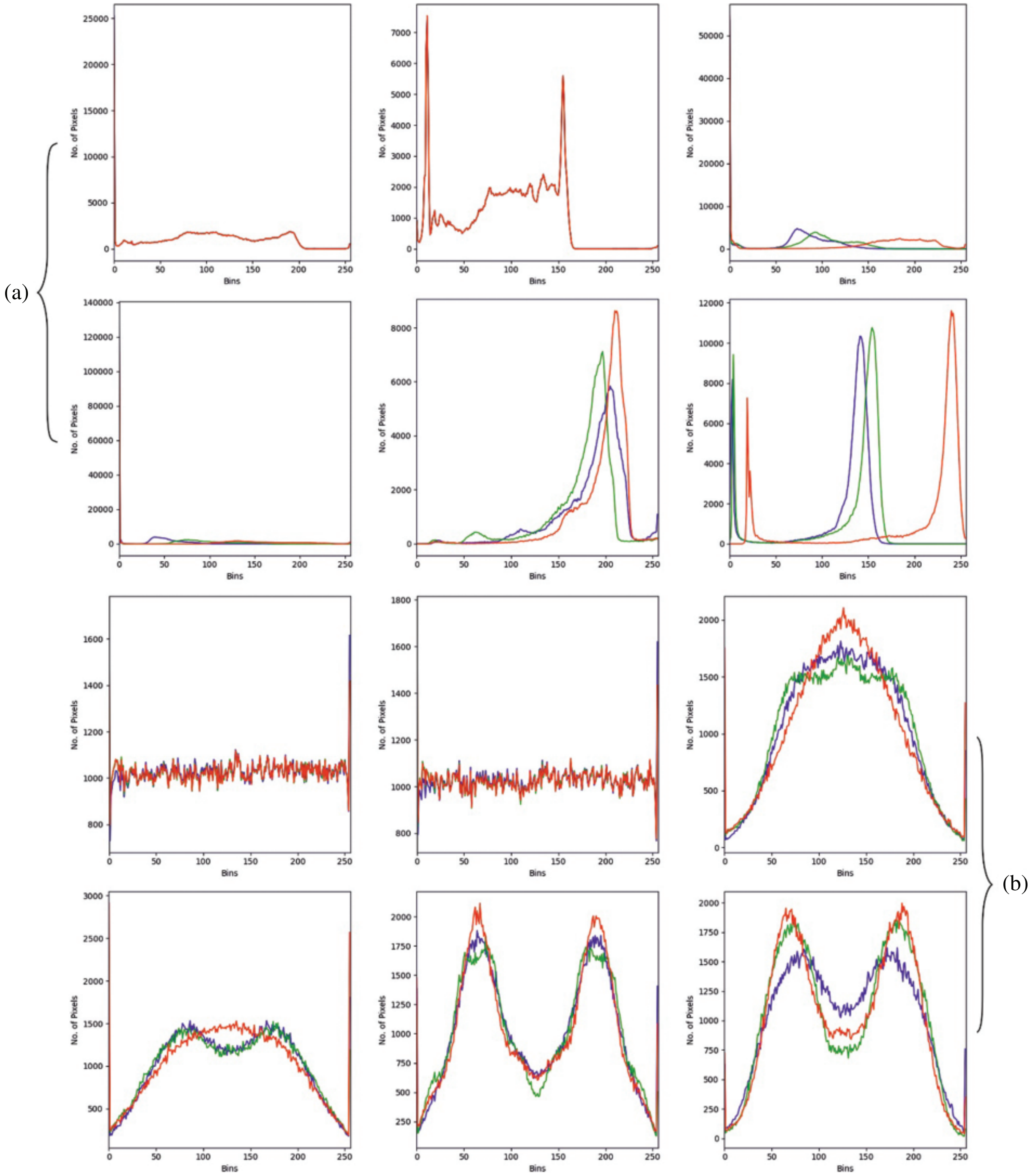

Figure 4: Histogram analysis (a) histogram of original images (b) histogram of encrypted images

Tab. 1 reports the overall results offered by the WDOA-MIE model on six test images. The experimental values implied that the WDOA-MIE model has obtained minimal values of MSE and RMSE with maximum values of PSNR and structural similarity (SSIM). For instance, on image-1, the WDOA-MIE method has gained mean square error (MSE) of 0.0713, root mean square error (RMSE) of 0.2670, PSNR of 59.5999 dB, and SSIM of 0.9999. Besides, on image-2, the WDOA-MIE model has obtained MSE of 0.1021, RMSE of 0.3195, PSNR of 58.0405 dB, and SSIM of 0.9992. At last, on image-6, the WDOA-MIE model has resulted in MSE of 0.0553, RMSE of 0.2352, PSNR of 60.7036 dB, and SSIM of 0.9993.

Table 1: Result analysis of WDOA-MIE model under distinct test images

Image No.	MSE	RMSE	PSNR (dB)	SSIM
Image-1	0.0713	0.2670	59.5999	0.9999
Image-2	0.1021	0.3195	58.0405	0.9992
Image-3	0.1060	0.3256	57.8777	1.0000
Image-4	0.0748	0.2735	59.3918	0.9994
Image-5	0.1075	0.3279	57.8167	0.9999
Image-6	0.0553	0.2352	60.7036	0.9993

Tab. 2 and Fig. 5 illustrate a comparative MSE examination of the WDOA-MIE model with other encryption models. The results signified the betterment of the WDOA-MIE model with least values of MSE. For instance, with Image-1, the WDOA-MIE model has gained lower MSE of 0.0713 while the RSA, ECC, cuckoo search (CS), and particle swarm optimization (PSO) approaches have achieved superior MSE of 0.3379, 0.2446, 0.1792, and 0.1680 respectively. Moreover, with Image-4, the WDOA-MIE model has gained lower MSE of 0.0748 while the RSA, ECC, CS, and PSO models have reached increased MSE of 0.3449, 0.2140, 0.1865, and 0.1747 respectively. Furthermore, with Image-5, the WDOA-MIE model has resulted in least MSE of 0.0553 but the RSA, ECC, CS, and PSO models have accomplished increased MSE of 0.3225, 0.2398, 0.1744, and 0.1245 respectively.

Table 2: MSE examination of WDOA-MIE with existing models

Mean Square Error					
Image No.	RSA	ECC	CS	PSO	WDOA-MIE
Image-1	0.3379	0.2446	0.1792	0.1680	0.0713
Image-2	0.3364	0.2419	0.1751	0.1450	0.1021
Image-3	0.3418	0.2438	0.1987	0.1409	0.1060
Image-4	0.3449	0.2140	0.1865	0.1747	0.0748
Image-5	0.3258	0.2151	0.1681	0.1440	0.1075
Image-6	0.3225	0.2398	0.1744	0.1245	0.0553

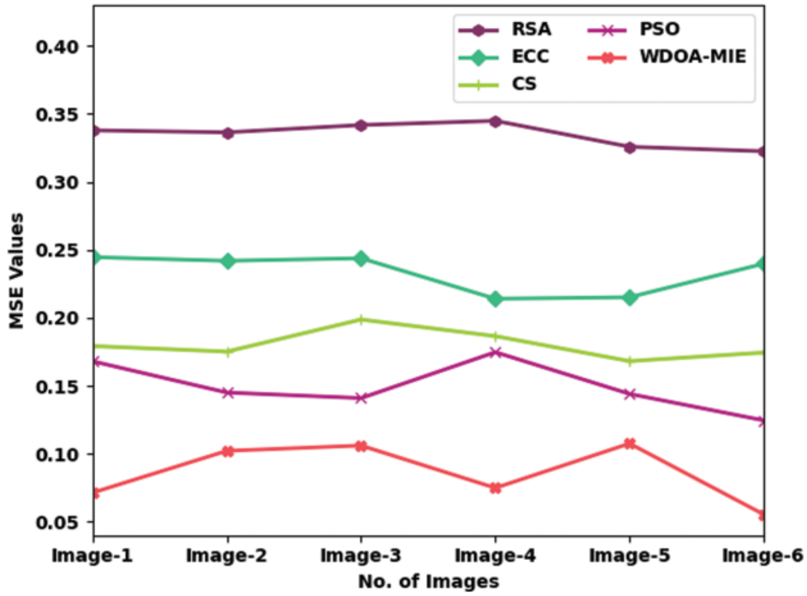

Figure 5: Comparative MSE examination of WDOA-MIE with existing models

A comprehensive PSNR investigation of the WDOA-MIE model with recent models is made in Tab. 3 and Fig. 6. The obtained values implied that the WDOAMIE model has accomplished effectual outcomes with increased PSNR values under all images. For instance, with image1, the WDOAMIE approach has provided maximum PSNR of 59.60 dB but the RSA, ECC, CS, and PSO models have resulted to lower PSNR of 52.84, 54.25, 55.60, and 55.88 dB respectively. Simultaneously, with image5, the WDOAMIE model has delivered enhanced PSNR of 57.82 dB whereas the RSA, ECC, CS, and PSO models have accomplished reduced PSNR of 53, 54.80, 55.88, and 56.55 dB respectively.

Table 3: PSNR examination of WDOA-MIE with existing models

PSNR (dB)					
Image No.	RSA	ECC	CS	PSO	WDOA-MIE
Image-1	52.84	54.25	55.60	55.88	59.60
Image-2	52.86	54.29	55.70	56.52	58.04
Image-3	52.79	54.26	55.15	56.64	57.88
Image-4	52.75	54.83	55.42	55.71	59.39
Image-5	53.00	54.80	55.88	56.55	57.82
Image-6	53.05	54.33	55.72	57.18	60.70

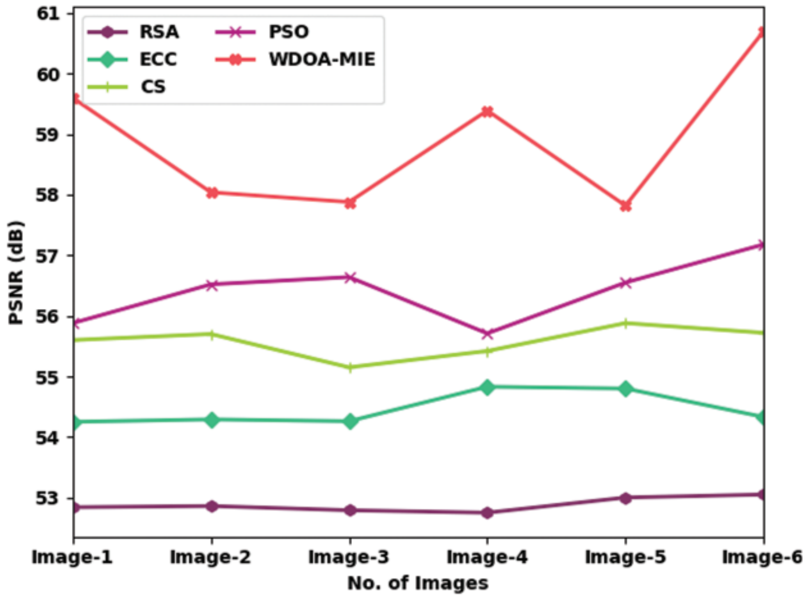

Figure 6: Comparative PSNR examination of WDOA-MIE with existing models

A comprehensive SSIM investigation of the WDOAMIE model with existing models is made in Tab. 4 and Fig. 7. The achieved values implied that the WDOAMIE model has accomplished effectual outcomes with increased SSIM values under all images. For instance, with Image-1, the WDOAMIE method has provided superior SSIM of 0.9989 while the RSA, ECC, CS, and PSO models have resulted to lower SSIM 0.9600, 0.9706, 0.9782, and 0.9836 respectively. Simultaneously, with Image-5, the WDOAMIE model has delivered enhanced SSIM of 0.9949 whereas the RSA, ECC, CS, and PSO models have accomplished reduced SSIM of 0.9260, 0.9700, 0.9707, and 0.9825 respectively.

Table 4: SSIM examination of WDOA-MIE with existing models

SSIM					
Image No.	RSA	ECC	CS	PSO	WDOA-MIE
Image-1	0.9600	0.9706	0.9782	0.9836	0.9989
Image-2	0.9364	0.9673	0.9857	0.9931	0.9968
Image-3	0.9209	0.9675	0.9855	0.9953	0.9991
Image-4	0.9007	0.9707	0.9763	0.9952	0.9994
Image-5	0.9260	0.9700	0.9707	0.9825	0.9949
Image-6	0.9551	0.9622	0.9851	0.9944	0.9983

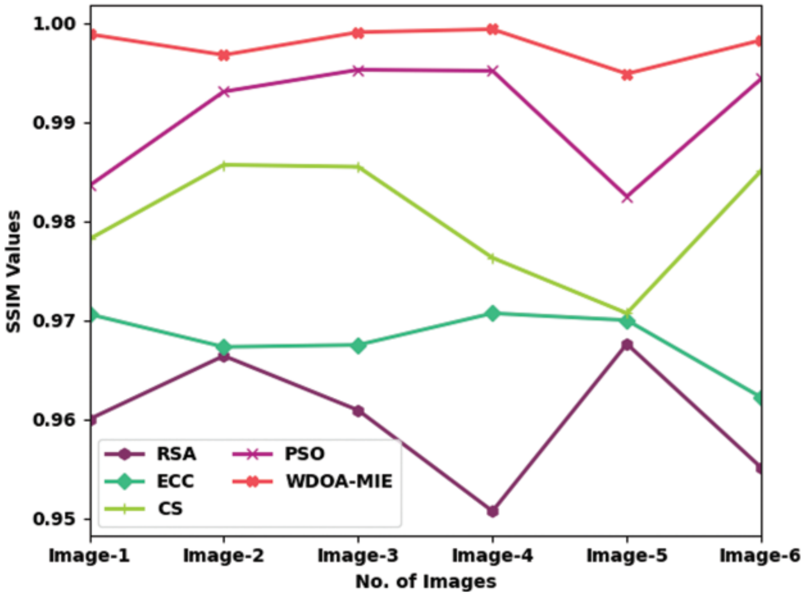

Figure 7: Comparative SSIM examination of WDOA-MIE with existing models

Tab. 5 and Fig. 8 exemplify a comparative computation time (CT) investigation of the WDOA-MIE model with other encryption models [29]. The results indicated the improvement of the WDOA-MIE model with minimum values of CT. For instance, with Image-1, the WDOA-MIE model has gained lower CT of 72.60 s whereas the RSA, ECC, CS, and PSO models have obtained higher CT 106.56, 122.76, 110.22, and 104.10 s respectively. Also, with Image-4, the WDOA-MIE model has gained lower CT of 66.90 s whereas the RSA, ECC, CS, and PSO models have obtained higher CT of 124.62, 80.88, 81.78, 132 s, respectively. In addition, with Image-6, the WDOA-MIE model has resulted in least CT of 42.60 s whereas the RSA, ECC, CS, and PSO models have accomplished increased CT of 128.04, 113.88, 52.38, and 54.66 s respectively.

Table 5: CT examination of WDOA-MIE with existing models

Computation Time (s)					
Image No.	RSA	ECC	CS	PSO	WDOA-MIE
Image-1	106.56	122.76	110.22	104.10	72.60
Image-2	142.62	99.06	107.16	96.00	70.20
Image-3	111.78	108.18	108.36	80.10	60.00
Image-4	124.62	80.88	81.78	132.00	66.90
Image-5	77.88	52.02	109.74	95.46	41.34
Image-6	128.04	113.88	52.38	54.66	42.60

From the comprehensive results and discussion, it can be evident that the WDOA-MIE model has gained effectual encryption performance over the other methods.

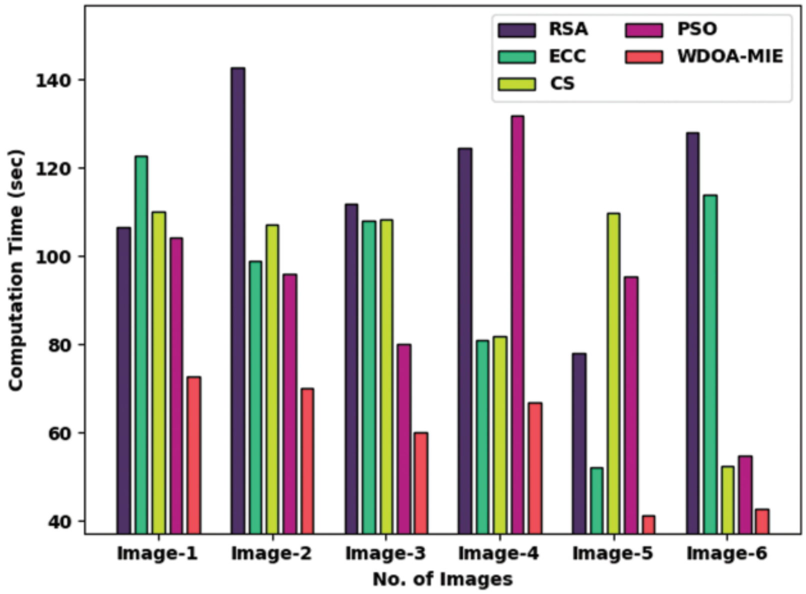

Figure 8: Comparative CT examination of WDOA-MIE with existing models

5 Conclusion

In this article, a new WDOA-MIE technique was established for blockchain enabled IoT environment. The WDOA-MIE model enables the acquisition of medical images from the patient via IoT devices. Followed by, the acquired images are coded by the use of signcryption technique. For enhancing the efficacy of the signcryption technique, the optimal key generation procedure was executed by WDOA algorithm. The goal of the WDOA-MIE algorithm is to derive a fitness function based on PSNR. Upon successful encryption of images, the IoT devices transmit to the closest server for storing it in the blockchain securely. The performance of the presented approach was analyzed utilizing the benchmark medical image dataset. The security and the performance analysis establish that the presented method offers better security with increased PSNR of 60.7036 dB. In future, hybrid metaheuristic optimization algorithms can be designed to further enhance security performance. In addition, lightweight cryptographic techniques can be involved to ensure security.

Acknowledgement: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1G1A1099559).

Funding Statement: The authors received no specific funding for this study.

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

References

[1] M. K. Hasan, S. Islam, R. Sulaimanm, 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.

[2] M. H. Kashani, M. Madanipour, M. Nikravan, P. Asghari and E. Mahdipour, "A systematic review of IoT in healthcare: Applications, techniques, and trends," *Journal of Network and Computer Applications*, vol. 192, p. 103164, 2021.

[3] 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.

[4] J. Jain and A. Jain, "Securing e-healthcare images using an efficient image encryption model," *Scientific Programming*, vol. 2022, pp. 1–11, 2022.

[5] 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, pp. 1–17, 2021.

[6] P. Sarosh, S. A. Parah and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 7253–7270, 2022.

[7] M. Gupta, K. K. Gupta, M. R. Khosravi, P. K. Shukla, S. Kautish *et al.,* "An intelligent session key-based hybrid lightweight image encryption algorithm using logistic-tent map and crossover operator for internet of multimedia things," *Wireless Personal Communications*, vol. 121, no. 3, pp. 1857–1878, 2021.

[8] W. E. Shafai, F. Khallaf, E. E. Rabaie and F. E. Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9007–9035, 2021.

[9] 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.

[10] S. Jeevitha and N. A. Prabha, "Novel medical image encryption using DWT block-based scrambling and edge maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3373–3388, 2021.

[11] B. A. Y. Alqaralleh, T. Vaiyapuri, V. S. Parvathy, D. Gupta, A. Khanna *et al.,* "Blockchain-assisted secure image transmission and diagnosis model on internet of medical things environment," *Personal and Ubiquitous Computing*, vol. 19, no. 2, p. 326, 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. Bharadwaj, A. Lakshman, G. Bhatnagar and C. Chattopadhyay, "A novel security framework for medical data in IoT ecosystem," *IEEE MultiMedia*, pp. 1–1, 2022.

[14] X. Wang, S. Yin, M. Shafiq, A. A. Laghari, S. Karim *et al.,* "A new V-net convolutional neural network based on four-dimensional hyperchaotic system for medical image encryption," *Security and Communication Networks*, vol. 2022, no. 1, pp. 1–14, 2022.

[15] A. Jan, S. Parah and B. Malik, "IEFHAC: Image encryption framework based on Hessenberg transform and chaotic theory for smart health," *Multimedia Tools and Applications*, vol. 78, no. 1, pp. 27569, 2022.

[16] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir *et al.,* "A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966–12982, 2022.

[17] F. Masood, J. Masood, L. Zhang, S. S. Jamal, W. Boulila *et al.,* "A new color image encryption technique using DNA computing and chaos-based substitution box," *Soft Computing*, vol. 266, no. 5187, pp. 1021, 2021.

[18] F. Masood, J. Ahmad, S. A. Shah, S. S. Jamal and I. Hussain, "A novel hybrid secure image encryption based on Julia set of fractals and 3D Lorenz chaotic map," *Entropy*, vol. 22, no. 3, p. 274, 2020.

[19] F. A. Khan, J. Ahmed, J. S. Khan, J. Ahmad and M. A. Khan, "A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S8 permutation," *Journal of Intelligent & Fuzzy Systems*, vol. 33, no. 6, pp. 3753–3765, 2017.

[20] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 2, pp. 943–961, 2019.

[21] J. Ahmad and S. O. Hwang, "Chaos-based diffusion for highly autocorrelated data in encryption algorithms," *Nonlinear Dynamics*, vol. 82, no. 4, pp. 1839–1850, 2015.

[22] X. R. Zhang, X. Chen, W. Sun and X. Z. He, "Vehicle re-identification model based on optimized densenet121 with joint loss," *Computers, Materials & Continua*, vol. 67, no. 3, pp. 3933–3948, 2021.

[23] M. Wang, Z. Zhou and C. Ding, "Blockchain-based decentralized reputation management system for internet of everything in 6G-enabled cybertwin architecture," *Journal of New Media*, vol. 3, no. 4, pp. 137–150, 2021.

[24] H. M. Waseem, M. Khan and T. Shah, "Image privacy scheme using quantum spinning and rotation," *Journal of Electronic Imaging*, vol. 27, no. 6, p. 1, 2018.

[25] M. Khan, F. Masood, A. Alghafis, M. Amin and S. I. Batool Naqvi, "A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion," *PLoS ONE*, vol. 14, no. 12, p. e0225031, 2019.

[26] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using TLTS and Henon chaotic map," *IEEE Access*, vol. 8, pp. 71974–71992, 2020.

[27] O. Abdalla, H. Rezk and E. M. Ahmed, "Wind driven optimization algorithm based global MPPT for PV system under non-uniform solar irradiance," *Solar Energy*, vol. 180, no. 5, pp. 429–444, 2019.

[28] D. Berdik, S. Otoum, N. Schmidt, D. Porter and Y. Jararweh, "A survey on blockchain for information systems management and security," *Information Processing & Management*, vol. 58, no. 1, p. 102397, 2021.

[29] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno 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, 2018.