Computers, Materials & Continua
DOI:10.32604/cmc.2022.021873
Article

Tech Science Press

Novel Image Encryption and Compression Scheme for IoT Environment

Mesfer Al Duhayyim[1], Fahd N. Al-Wesabi[2], Radwa Marzouk[3], Manar Ahmed Hamza[4], Anwer Mustafa Hilal[4,*] and Majdy M. Eltahir[2]

[1]Department of Natural and Applied Sciences, College of Community-Aflaj, Prince Sattam bin Abdulaziz University, Saudi Arabia
[2]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Saudi Arabia
[3]Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Saudi Arabia
[4]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
[*]Corresponding Author: Anwer Mustafa Hilal. Email: a.hilal@psau.edu.sa
Received: 18 July 2021; Accepted: 30 August 2021

Abstract: Latest advancements made in the processing abilities of smart devices have resulted in the designing of Intelligent Internet of Things (IoT) environment. This advanced environment enables the nodes to connect, collect, perceive, and examine useful data from its surroundings. Wireless Multimedia Surveillance Networks (WMSNs) form a vital part in IoT-assisted environment since it contains visual sensors that examine the surroundings from a number of overlapping views by capturing the images incessantly. Since IoT devices generate a massive quantity of digital media, it is therefore required to save the media, especially images, in a secure way. In order to achieve security, encryption techniques as well as compression techniques are employed to reduce the amount of digital data, being communicated over the network. Encryption Then Compression (ETC) techniques pave a way for secure and compact transmission of the available data to prevent unauthorized access. With this background, the current research paper presents a new ETC technique to accomplish image security in IoT environment. The proposed model involves three major processes namely, IoT-based image acquisition, encryption, and compression. The presented model involves optimal Signcryption Technique with Whale Optimization Algorithm (NMWOA) abbreviated as ST-NMWOA. The optimal key generation of signcryption technique takes place with the help of NMWOA. Besides, the presented model also uses Discrete Fourier Transform (DFT) and Matrix Minimization (MM) algorithm-based compression technique. Extensive set of experimental analysis was conducted to validate the effective performance of the proposed model. The obtained values infer that the presented model is superior in terms of both compression efficiency and data secrecy in resource-limited IoT environment.

Keywords: Data compression; image security; encryption; signcryption; optimal key generation

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.

1 Introduction

The emergence of new technologies in Internet of Things (IoT) without considering security concerns may expose the users to threats and make them vulnerable. The incorporation of IoT with security approaches is a challenging process. The security aspects of IoT have received significant attention among the researchers in recent years. In addition, the transmission of confidential data over wireless networks is an ineffective process. At the same time, the use of digital media, captured by IoT devices, is also increasing. In general, the transmission of private information (like images, videos, etc.) through social media and networks is non-advisable due to improper security features and fear of data loss. It is essential to ensure data security at the time of sending data through unauthorized channels. Therefore, image encryption techniques have become essential to accomplish secure image communication in IoT environment. Most of the issues arise when transmitting the data through currently available networks [1]. At the beginning, the image size should be enlarged to maximize the quality of image. Besides, the vulnerability for security of the images interrupts the supremacy of image quality as well.

Security risks can be resolved under the application of encryption model, in which the private data is masked with legal properties. Compression and Encryption methodologies are extremely interconnected with each other and interact at most of the times. At the initial stage, compression is applied to limit the redundant data. Data encryption, on the other hand, provides a brief security when the repetition is low in image data. Therefore, both compression and encryption are carried out together to accomplish precise, supreme, robust, and maximum confidentiality. Various methods have been presented by combining compression and encryption methodologies namely, [2] Encryption-Compression, Compression-Encryption [3–5] as well as Hybrid Compression-Encryption. Thus, the former approaches have exhibited symmetric cryptography to compute the encoding for image data. Symmetric encryption is highly efficient in comparison with asymmetric encryption. Although symmetric encryption is a better performing candidate, still massive security problems are experienced in this entity which degrades the efficiency of data transmission [6–8].

In literature [9], the developers have focused on improving the security and compression tasks. The projected model was used to reduce the size of image data whereas the average of key sensitivity measures was enhanced and protected from statistical and entropy attacks [10]. However, this study did not define how the quality of reformed images is predicted. The model developed in the literature [11] aimed at resolving the problems related to key management by applying session key generator approach. Furthermore, it aspired at resolving the threats involved in session key distribution using Elliptic Curve Cryptosystem (ECC) before the transmission of data via secured channel. Therefore, the newly deployed approach was considered to be ineffective as ciphered images and ciphered keys were shared. As a result, the model is prone to several attacks since the UACI measures are limited.

In the study conducted earlier [12], a 256-bit flow generator was applied to protect the data of color image. Actually, a session key contains symmetric keys since a key is comprised of 8-bits. In literature [13], a dynamic session key generator was employed to study the properties of gray-scale images. So, primary symmetric key was generated through convolution model and new chaotic mapping. Encryption approach is highly effective in resisting different intrusions and is simply applied in diminishing the size of image content. A symmetric key is required for the agreement between transmitter and receiver. Afterwards, hybrid compression-encryption methods are applied to protect private details with minimum processing time. Moreover, compression as well as encryption techniques are used for sub-classified images.

A technique employed in [14] utilized different keys to enhance the security of image data. The researchers have estimated the effect of enhancing external keys in encryption process. Followed by, a scheme applied in [15] made use of three session keys under the application of Chirikov standard map to maximize the integrity of data. Moreover, dynamic session keys was applied in [16]. This method employed S-box as a combination of chaotic systems and Linear Fractional Transform (LFT). Therefore, the major objective of this study was to enlarge the security of replacement phase.

Different types of compression-encryption methods have been employed by developers to offer better security and effective data exchange operations. These methods are categorized under three levels as described in [4,5]. Initially, it is termed as encryption-compression [6,7] and made use of lossless compression mechanism to ensure data reconstruction. This approach is applied to protect both text data and medical images that focus on data accuracy as well as image integrity, with regards to reduction in data size [8]. Then, compression-encryption is applied to enhance the integrity of image data. Moreover, it reduces the efficacy of frequency analysis attacks. This in turn increases the duration of brute force attacks, limits the redundancy of plaintext and finally eliminates the cryptanalytic attacks. The implementation of chaos models for maximum symmetric encryption assures that the approach provides maximum security. Therefore, the performance of compression technology has not been implemented by researchers.

The current research paper presents a new Encryption Then Compression (ETC) technique for securing colored images in IoT environment. The proposed model operates on two main stages such as encryption and compression. The presented model involves optimal signcryption technique with Whale Optimization Algorithm (NMWOA) abbreviated as ST-NMWOA. The optimal key generation of signcryption technique takes place with the help of NMWOA. Furthermore, the presented model makes use of Discrete Fourier Transform (DFT) and Matrix Minimization (MM) algorithm-based compression technique. A comprehensive simulation analysis was conducted to validate the superiority of the presented model.

In short, the key contributions of current paper are as follows.

- A new ETC technique is proposed in this study using metaheuristics to accomplish secure communication in IoT environment.
- An effective encryption technique is designed using ST-NMWOA technique in which NWOA technique is implemented for optimal key generation process.
- A compression technique is presented using DFT and MM techniques
- Both security and compression performance of the proposed model was validated against benchmark images under several aspects.

Rest of the sections in the study is as follows. Section 2 discusses the proposed ETC technique developed for IoT environment. Then, Section 3 offers a detailed note on performance validation of the ETC model. Finally, Section 4 highlights the concluding remarks of ETC technique and derives possible future enhancements of the approach.

2 The Proposed Model

The overall process, involved in the proposed model, is defined here. An input color image is initially encrypted with the help of optimal signcryption technique. Next, the encrypted image is compressed by DFT-MM model. Then, the compressed image is transmitted to the receiver side. Finally, decompression and decryption processes are executed on the compressed image to reconstruct the original image without losing its quality.

2.1 Image Encryption

To achieve image compression, a public key cryptographic technique called 'Signcryption' is applied as it concurrently fulfills the components of digital signature and open key encryption at a minimal cost. The features of signcryption are as follows; confidentiality, unforgeability, integrity, and non-repudiation. In the presented encryption model, there involves three processes namely, key generation, signcryption, and unsigncryption process [17]. An extreme level of protection is given for 'message forwarding process' of the previously encoded image by the presented NM-WOA signcryption with optimum choice of keys.

Generation of Keys

Signcryption denotes the primitive of a public key that establishes two important cryptographic gadgets to ensure privacy, honesty, and non-repudiation. At the same time, it is implemented to obtain both digital signature as well as encryption. In light of these, it obtains a private as well as public key for both sender as well as the receiver. In order to enhance medical image security, the presented method employs single private keys by optimization procedure.

L_P-Larger prime number

L_f-Larger prime factor

I-Integer with order L_f modulo L_P, selected arbitrarily from $[1, \ldots L_P - 1]$

L_P-Keyed one-way hash function

D-Value, selected arbitrarily $[1, \ldots L_f - 1]$

Transmitter key pair $((M_{k1}, N_{k1}))$

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

Receiver key pair $((M_{k2}, N_{k2}))$

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

2.2 Optimal Key Generation Using NMWOA Model

For optimal selection of keys, NMWOA model is applied. In general, WOA is a metaheuristic approach developed in literature [18]. Alike spotted hyena model and grasshopper search models, WOA is a population-based scheme and is used in resolving the optimization issues. WOA model was developed on the basis of a social hierarchy of humpback whales which are assumed as the largest mammals globally. The length of a matured adult whale ranges from 12 to 16 m while few whales tend to grow up to 30 m too. It weights more than 30 metric tonnes. With a stocky body and large hump, it has extended pectoral fins as well as black dorsal coloring. It is an established and interesting mammal known for its intelligence, especially in food collection. Though its social architecture is not effective, it often lives in groups. However, it is for a limited time and it gets dispersed as usual. While targeting prey, it swims over the sea and makes different bubbles in circular fashion. Similar to swarm-based heuristics, WOA heuristic is also initialized from the random development of Np possible solutions as given herewith.

$$X_{i,j}^{t=0} = x_{\mathrm{i,min}} + rand_{i,j}\,(0 \times 1) \times \left(x_{i,\mathrm{mix}} - x_{i,\,\mathrm{min}}\right) \tag{3}$$

Here, t denotes the generation value, $j = 1, \ldots, NP, i = 1D$ (D refers to problem dimension), x_i, min and x_i, max denote the lower as well as higher measures of i^{th} design parameter,

correspondingly. Additionally, WOA is composed of the following objectives namely, surrounding the prey, developing a bubble net to trap the prey, and using a principle to search the prey.

2.2.1 Encircling Preys

Initially, hunting is invoked by surrounding the prey [19]. Followed by, the position has to be upgraded iteratively and the global optimal solution is found. This hierarchy is represented by Eqs. (4) and (5):

$$D = \left| C \cdot x^{*}(z) - x \geq (z) \right| \tag{4}$$

$$x(z+1) = x^{*}(z) - A \cdot D \tag{5}$$

where z denotes the present iteration, x^{*} implies the optimal solution, and x shows the original solution. Here, the coefficients vectors A and C are projected by Eqs. (6) and (7):

$$A = 2 \times a \cdot r - a \tag{6}$$

$$C = 2 \times r \tag{7}$$

where a indicates the linearly reduced values from 2 to 0, and r defines the arbitrarily dispersed value from [0, 1]. Fig. 1 shows the flowchart of WOA process.

2.2.2 Bubblenet Attacking Strategy

Humpback whales use a model in which the prey is assigned with a value and a shrinking bubble net is developed spirally. The basic principle is developed numerically by reducing the measure of a while Eq. (6) provides the information herewith.

$$a = 2 - \frac{2z}{z_{\max}} \tag{8}$$

where z refers to the present iteration value and $z_{\max}$ indicates the value by applied criterion.

Likewise, the spiral updating location is depicted herewith.

$$D' = \left| x^{*}(z) - x(z) \right| \tag{9}$$

$$x(z+1) = D' \cdot e^{bl} \cdot \cos(2\pi l) + x^{*}(z) \tag{10}$$

where b refers to the constant defining shape of logarithmic spiral and l indicates an arbitrary value from $[-1, 1]$.

In case of optimization, the maximum opportunity is applied to shrink the encircling values whereas the remaining ones are deployed in the development of spiral-shaped path as depicted in the mathematical equation given below.

$$x(z+1) = \begin{cases} x^{A*}(t) - A \cdot D & if \ p < 0.5 \\ D' \cdot e^{bl} \cdot \cos(2\pi l) + x^{*}(z) & otherwise \end{cases} \tag{11}$$

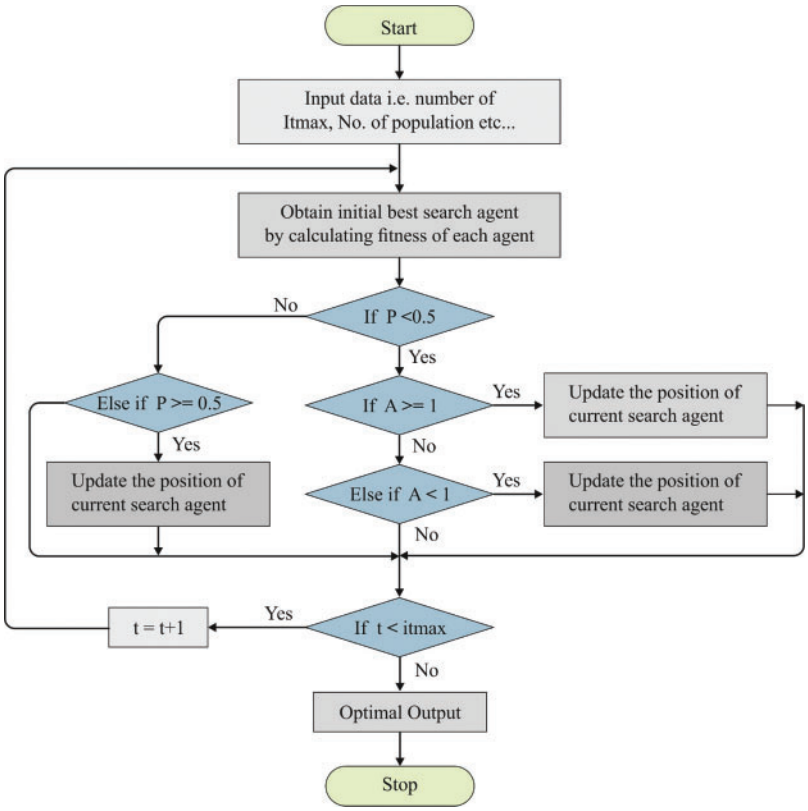


Figure 1: Process involved in WOA

2.2.3 Searching for Preys

This stage is referred to as exploration stage. In this module, vector A with random measures in the range of $[-1,\ 1]$ is employed to promote the solution from well-known searching agent and is expressed numerically as given below.

$$D' = |C \cdot x_{rand} - x| \tag{12}$$

$$x(z+1) = x_{rand} - A \cdot D \tag{13}$$

where x_{rand} defines a random whale which was selected from recent population.

Algorithm 1: Pseudocode of WOA

Population initialization Xi (i = 1, 2, 3, …, n)
Determine fitness value (FV) all whales
Assume X∗ as the optimum whale
while (t < max_no.of_iterations) do
For (all hunting whales) do
Upgrade a, A, C, l and p
If (p < 0.5) then
If (|A| < 1) then
Whale location gets updated by moving in the direction of optimal agent

(Continued)

Else
If (|A| ≥ 1) then
Select the arbitrary whale Xrand
Update the location of the whale position
End If
End If
Else
If (p ≥ 0.5) then
Modify the whale locations
End If
End If
End For
Compute the FV of all searching agents.
Upgrade X ∗ if there is an optimal solution
Increment t
End while

2.2.4 Nelder–Mead Algorithm (NM)

A newly-presented direct search model i.e., NM manages to resolve different sorts of issues and accomplish the challenging outcome. It is composed of five processes namely, sorting, reflection, expansion, contraction, and shrinkage. Here, the basic points are emitted $(x^1, x^2, \ldots, x^{n+1})$ and the objective function measures $f\left(x^i\right)$ are processed.

Step 1: Sorting

It is applied at different points and are estimated as best (x^b), worst (x^h), next worst (x^{nw}) and centroid x^0 of the points whereas no worst expression has been determined.

Step 2: Reflection

Here, a reflection point x^r is depicted by the function as expressed herewith.

$$x^r = x^0 + \alpha\left(x^0 - x^h\right) \tag{14}$$

Step 3: Expansion

Likewise, the expansion point x^e is processed under the application of the given function:

$$x^e = x^0 + \gamma\left(x^r - x^0\right) \tag{15}$$

where γ implies the coefficient of expansion. While the objective function values for x^e is better than x^l, w is exchanged by x^e. Otherwise, x^h is substituted by x^r and the iterations are concluded.

Step 4: Contraction

When the expression $f(x^r) > f(x^{nw})$ is identified, then the contraction is also employed.

a. Outside contraction. While the derivation $f(x^r)$ is maximum than $x^h f\left(x^h\right)$, then outside contraction is utilized by the Eq. (8) and $f(x^{oc})$ is attained.

$$x^{oc} = x^0 + \beta\left(x^r - x^0\right) \tag{16}$$

where β denotes a contraction coefficient. When $f(x^{oc})$ is supreme than (x^r) , x^h is interchanged by x^{oc} which concludes the iteration. Otherwise, the consecutive step shrinkage is applied.

b. Inside contraction. When $f\left(x^h\right)$ is optimal than (x^r), then inside contraction is recommended by applying Eq. (9) and $f\left(x^{ic}\right)$ is determined under the application of the given function:

$$x^{ic} = x^0 + \beta\left(x^h - x^0\right) \tag{17}$$

If $\left(x^{ic}\right) \leq f\left(x^h\right)$, x^h is interchanged with x^{ic}, and iteration is ended. Otherwise, the next step shrinkage is followed.

Step 5: Shrinkage

It is the final task and is determined based on the function given below.

$$x^i = x^i + \gamma\left(x^b - x^i\right) \tag{18}$$

where δ denotes the shrink coefficient.

2.3 Image Compression

Next to image encryption process, the encrypted images are compressed with the help of DFT-MM model. In general, an actual image is sub-classified as non-overlapping blocks sized at M × N pixels that begins from top left corner of an image. Then, DFT is employed at every M × N block autonomously to illustrate the image in a frequency domain and this scenario provides real as well as imaginary units. Matrix Minimization approach is employed for all the components whereas zeros are eliminated by this approach [20]. Equal quantization is utilized for these portions and it contributes to the classification of elements by a factor named 'quantization factor Q. This surrounds the simulation results that enhance the possibility of frequency coefficients and reduces the count of bits that are essential for demonstrating the coefficients. Finally, the compression ratio gets maximized. Fig. 2 demonstrates the compression model.

In order to acquire maximum details, uniform quantization (Qr and Qi) is performed in a heuristic fashion. Thus, two matrices (Qr and Qi) are presented in a block which shows both real as well as imaginary portions correspondingly. Based on the real portion, low coefficient measures (such as Discrete Cosine (DC) values) are detached and are secured with novel matrix named 'Low Frequency Coefficients (LFC-Matrix)'. This gets replaced with zero value in the quantized matrix. It is significant to know that the DC measures can be identified in real portions where significant information as well as features of images are involved. Followed by, the attained LFC-Matrix size is composed of minimum DC measures in comparison with High Frequency Coefficients (HFC-Matrix) and is illustrated in the form of bytes. Hence, the model is named after Matrix-Minimization and is employed in current study. This mechanism is employed to reduce the size of HFC matrices by contracting three coefficients to corresponding measures that monitors the actual values in decompression state.

Here, contraction is carried out on all three subsequent coefficients by applying Random-Weight-Values. A value is multiplied by different random values (Ki) and a summation is determined. The value, thus attained, is assumed to be a contracted value of input measures. It is apparent to point out that during decompression phase, search technology is essential to identify three actual values which are applied in the identification of the contracted value. Hence, minimum as well as maximum values of m × n block are recorded. The strategy used in this method is to reduce the grade of measures that are essential to win back the actual three values, to enlarge the contracted value and improve the efficiency of searching method. Therefore, it

is feasible that the complicated images might exhibit maximum arrays during the degradation of compression process. For this purpose, the developers have recommended the application of alternate model in which DFT is applied while at the same time the search regions (search region is composed of two measures like [MIN, MAX]) are mitigated. This kind of bounding intends to make searching process, a fast, simple and a reliable one.

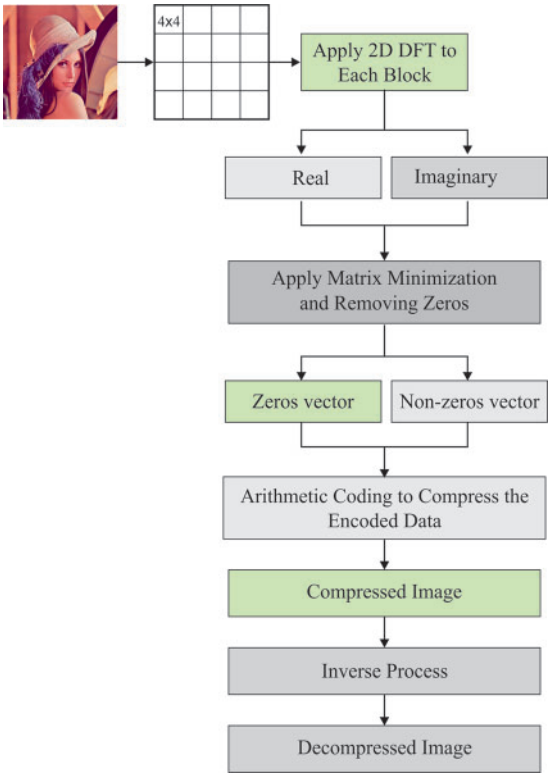


Figure 2: Compression model

Once Matrix-Minimization approach is employed, the HFC-Matrix developed for real as well as imaginary portions are investigated. This analysis is viable to measure the probability in zero values in comparison with alternate measures of the matrix. Hence, the isolation of zero from non-zero values eliminates the repeated data and maximizes the efficacy of arithmetic coding compression. Moreover, a novel array named 'Zero Matrix' is developed and a zero value is appended in non-zero value. The actual HFC-Matrix is indexed by applying integer which implies the overall count of zeros from two non-zero measures. Next, the zero values present in zero-matrix mimics the original non-zero measures in series of actual matrices. At last, two matrices are applied in compression process with the application of coding model called arithmetic coding. It is clear that the newly developed approach can also be employed for LFC-Matrix with low-frequency coefficient measures of real part. Therefore, value-matrix as well as zero-matrix are assumed to be headers and are utilized in decompression tasks to reproduce actual HFC as well as LFC matrices.

2.4 Image Decompression

Decompression method is defined as a counter compression task in which the act of compression is performed in inverse order. Decompression procedures are initialized by decoding LFC-matrix, value-matrix, and zero-matrix under the application of arithmetic decoding. However, the reconstruction of unified array is executed based on value and zero matrices, while HFC Matrix undergoes reformation. A new framework termed Sequential Search Algorithm is presented based on frequent processing of three pointers to generate three measures with contracted measures and guidance of MIN and MAX values preserved during compression. Therefore, MIN and MAX values are represented in minimum space search values and are applied in the restoration of original HFC for real and imaginary portions. At last, inverse quantization as well as DFT are employed for every portion to regenerate the compressed digital images.

3 Experimental Validation

This section details about the experimental validation of the presented model against benchmark color images and some sample test images as shown in Fig. 3. To verify the superiority of the presented method, a detailed comparative analysis was conducted against existing techniques. For comparative analysis of the compression performance, LZW and LZMA models were used. In addition, encryption results were compared with ST-AEHO, Chaotic Map, and Rubik's Cube models.

Figure 3: Sample images

Tab. 1 visualizes the encrypted and decrypted versions of the images created by the presented ST-NMWOA model. The table shows that the presented model generated both encrypted and decrypted images proficiently for the applied input image. From the decrypted image, it is apparent that the proposed ST-NMWOA model effectively reconstructed the image with no loss of image quality.

Tab. 2 shows the results of compression performance analysis of the presented image. The table lists MSE, PSNR, and compressed file size values obtained from the compression of the encrypted image. The presented model compressed the first Lena image sized 768 KB into 319 KB size image with a minimum MSE of 0.062 and maximum PSNR of 60.21 dB. Also, on the applied Mandrill image, the presented technique compressed the image file size from 768 to 387 KB size with a low MSE of 0.076 and high PSNR of 59.32 dB. Finally, on the applied Diabetic Retinopathy (DR) image, the presented model compressed the image size from 1024 to 592 KB with a minimum MSE of 0.051 and a maximum PSNR of 61.06 dB.

Table 1: Visualization of encrypted and decrypted images of the proposed ST-NMWOA model

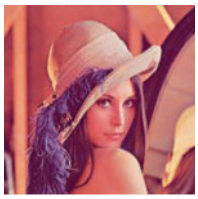
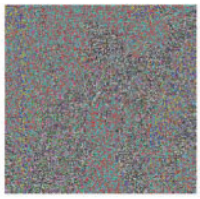
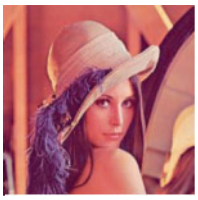
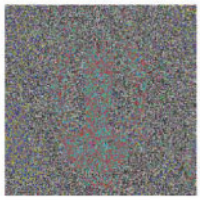
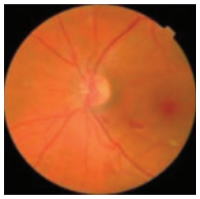
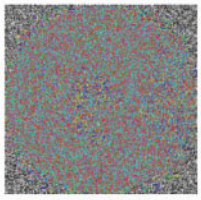
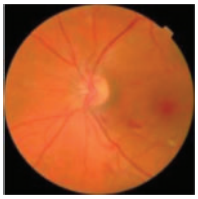
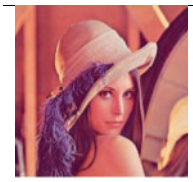
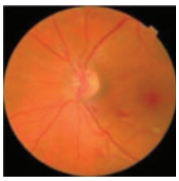
Original image	Encrypted image	Decrypted image
		
		
		

Table 2: Result analysis of proposed method

Decrypted image	MSE	PSNR	Orig. size (KB)	Comp. size (KB)
	0.062	60.21	768	319
	0.076	59.32	768	387
	0.051	61.06	1024	592

Tab. 3 and Fig. 4 illustrate the results of SS analysis of the presented DFT-MMA technique on test images. The resultant values exhibit that the proposed DFT-MMA model obtained a high

SS on the employed images. For sample, on test 'Lena' image, the DFT-MMA method reached a high SS of 58.46%, whereas LZW and LZMA models achieved least SS values such as 40.76% and 42.87%. Simultaneously, on test 'Mandrill' image, DFT-MMA algorithm gained an increased SS of 49.61%, whereas a minimum SS of 37.98% was obtained by LZW model and 39.15% was attained by LZMA model. Concurrently, on test 'DR' image, the presented DFT-MMA method reached an improved SS of 42.19% while low SS values such as 30.16% and 32.89% were attained by LZW and LZMA models.

Table 3: Results of the analysis of different methods on compression scheme in terms of space savings (%)

Test images	DFT-MMA	LZW	LZMA
Lena image	58.46	40.76	42.87
Mandrill image	49.61	37.98	39.15
DR image	42.19	30.16	32.89

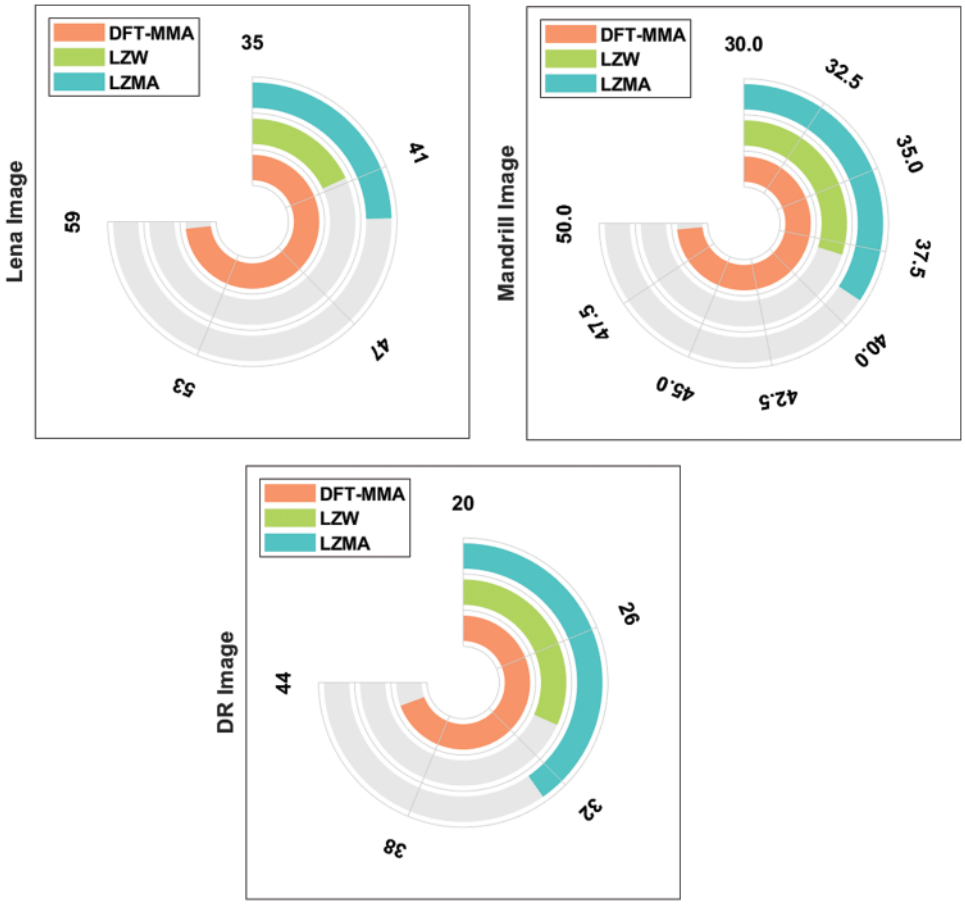


Figure 4: SS analysis of DFT-MMA model

Tab. 4 and Fig. 5 showcase the results of PSNR analysis of the presented technique on test images. The resultant values demonstrate that the presented ST-NMWOA model attained a superior PSNR on the employed images. For instance, on test 'Lena' image, ST-NMWOA model achieved a superior PSNR of 60.21 dB, whereas low PSNR values such as 59.52, 54.92, and 52.91 dB were attained by ST-AEHO, Chaotic map, and Rubik's cube models respectively. At the same time, on test 'Mandrill' image, ST-NMWOA approach obtained a maximal PSNR of 59.32 dB, but minimum PSNR values such as 56.22, 51.02, and 50.54 dB were achieved by ST-AEHO, Chaotic map, and Rubik's cube models respectively. Along with these, on test 'DR' image, ST-NMWOA technique gained a high PSNR of 61.06 dB, whereas low PSNR values such as 58.54, 53.78, and 49.87 dB were attained by ST-AEHO, Chaotic map, and Rubik's cube models correspondingly.

Table 4: Results of the proposed method against existing methods in terms of PSNR (dB)

Test images	ST-NMWOA	ST-AEHO	Chaotic map	Rubik's cube
Lena image	60.21	59.52	54.92	52.91
Mandrill image	59.32	56.22	51.02	50.54
DR image	61.06	58.54	53.78	49.87

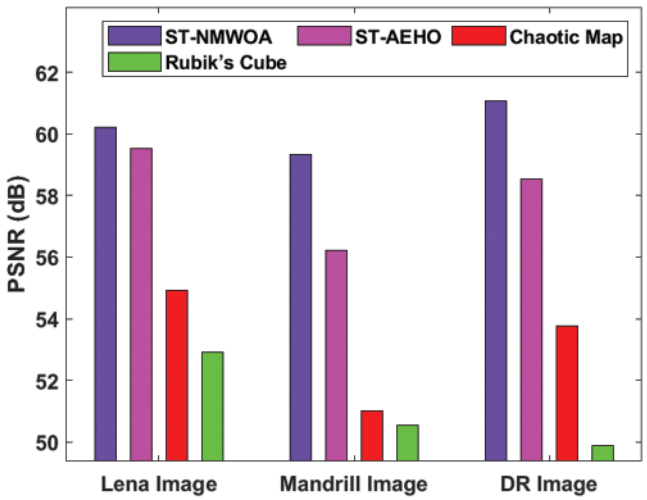


Figure 5: PSNR analysis of ST-NMWOA model

From the above discussed results of the analyses, the effective performance of the proposed model is understood compared to other techniques. The obtained values establish that the presented model is superior in terms of both compression efficiency and data security in resource-limited IoT environment. In addition, the presented model has proficiently generated both encrypted and decrypted images for the applied input image. From the decrypted image, it is apparent that the proposed ST-NMWOA model has effectively reconstructed the image without losing the quality of image. The comparison study results demonstrate that the proposed model outperformed the compression performance of LZW and LZMA models. Besides, the

proposed model shows enhanced encryption results over ST-AEHO, Chaotic Map, and Rubik's Cube models.

4 Conclusion

The current research paper presented an efficient ETC technique to secure the color images. The input color image is initially encrypted with the help of optimal signcryption technique. Next, the encrypted image is compressed by DFT-MM model. Then, the compressed image is transmitted to the receiver end. Finally, decompression and decryption processes are executed on the compressed image to reconstruct the original image without losing the quality. A comprehensive simulation analysis was carried out to validate the superiority of the presented model and a maximum PSNR of 61.06 dB was achieved. The obtained values infer that the presented model is superior in terms of both compression efficiency as well as data secrecy. In future, advanced lightweight compression techniques can be developed to increase the compression performance of DFT-MM model.

Funding Statement: The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under Grant Number (RGP 2/209/42). www.kku.edu.sa. This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-Track Path of Research Funding Program.

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

References

[1] 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, no. 3, pp. 102533, 2020.

[2] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang *et al.,* "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679–3689, 2018.

[3] E. Yang, V. S. Parvathy, P. P. Selvi, K. Shankar, C. Seo *et al.,* "Privacy preservation in edge consumer electronics by combining anomaly detection with dynamic attribute-based re-encryption," *Mathematics*, vol. 8, no. 11, pp. 1871, 2020.

[4] X. Kang, A. Peng, X. Xu and X. Cao, "Performing scalable lossy compression on pixel encrypted images," *EURASIP Journal on Image and Video Processing*, vol. 2013, no. 1, pp. 32, 2013.

[5] 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.

[6] M. Kumar and A. Vaish, "An efficient encryption-then-compression technique for encrypted images using SVD," *Digital Signal Processing*, vol. 60, no. 1, pp. 81–89, 2017.

[7] M. Zhang and X. Tong, "Joint image encryption and compression scheme based on IWT and SPIHT," *Optics and Lasers in Engineering*, vol. 90, no. 4, pp. 254–274, 2017.

[8] M. Elhoseny, K. Shankar, S. K. 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, 2020.

[9] X. J. Tong, P. Chen and M. Zhang, "A joint image lossless compression and encryption method based on chaotic map," *Multimedia Tools and Applications*, vol. 76, no. 12, pp. 13995–14020, 2017.

[10] T. Avudaiappan, R. Balasubramanian, S. S. Pandiyan, M. Saravanan, S. K. Lakshmanaprabu *et al.,* "Medical image security using dual encryption with oppositional based optimization algorithm," *Journal of Medical Systems*, vol. 42, no. 11, pp. 208, 2018.

[11] K. Gupta and S. Silakari, "Novel approach for fast compressed hybrid color image cryptosystem," *Advances in Engineering Software*, vol. 49, no. 3, pp. 29–42, 2012.

[12] M. Zhang and X. Tong, "A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system," *Multimedia Tools and Applications*, vol. 74, no. 24, pp. 11255–11279, 2015.

[13] S. Hanis and R. Amutha, "Double image compression and encryption scheme using logistic mapped convolution and cellular automata," *Multimedia Tools and Applications*, vol. 77, no. 6, pp. 6897–6912, 2018.

[14] S. A. Maadeed, A. A. Ali and T. Abdalla, "A new chaos-based image-encryption and compression algorithm," *Journal of Electrical and Computer Engineering*, vol. 2012, pp. 1–11, 2012.

[15] M. Hamdi, R. Rhouma and S. Belghith, "A selective compression-encryption of images based on spiht coding and chirikov standard map," *Signal Processing*, vol. 131, no. 4, pp. 514–526, 2017.

[16] A. Belazi, A. A. A. E. Latif, A. V. Diaconu, R. Rhouma and S. Belghith, "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Optics and Lasers in Engineering*, vol. 88, no. 11–12, pp. 37–50, 2017.

[17] K. Shankar, M. Elhoseny, E. Perumal, M. Ilayaraja and K. S. Kumar, "An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization," in *Cybersecurity and Secure Information Systems*. Berlin: Springer, pp. 31–42, 2019.

[18] S. Mirjalili and A. Lewis, "The whale optimization algorithm," *Advances in Engineering Software*, vol. 95, no. 12, pp. 51–67, 2016.

[19] A. R. Yildiz, "A novel hybrid whale-nelder–mead algorithm for optimization of design and manufacturing problems," *The International Journal of Advanced Manufacturing Technology*, vol. 105, no. 12, pp. 5091–5104, 2019.

[20] M. H. Rasheed, O. M. Salih, M. M. Siddeq and M. A. Rodrigues, "Image compression based on 2d discrete fourier transform and matrix minimization algorithm," *Water*, vol. 6, pp. 100024, 2020.