Computers, Materials & Continua
DOI: 10.32604/cmc.2022.025763
Article

Tech Science Press

Metaheuristic Lightweight Cryptography for Security Enhancement in Internet of Things

Mahmoud Ragab[1,2,3,*] and Ehab Bahaudien Ashary[4]

[1]Information Technology Department, Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[2]Centre of Artificial Intelligence for Precision Medicines, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
[3]Mathematics Department, Faculty of Science, Al-Azhar University, Naser City, 11884, Cairo, Egypt
[4]Electrical and Computer Engineering Department, Faculty of Engineering, King Abdulaziz University, Jeddah, 21589, Saudi Arabia
*Corresponding Author: Mahmoud Ragab. Email: mragab@kau.edu.sa

Received: 03 December 2021; Accepted: 09 February 2022

Abstract: The advancements made in Internet of Things (IoT) is projected to alter the functioning of healthcare industry in addition to increased penetration of different applications. However, data security and private are challenging tasks to accomplish in IoT and necessary measures to be taken to ensure secure operation. With this background, the current paper proposes a novel lightweight cryptography method for enhance the security in IoT. The proposed encryption algorithm is a blend of Cross Correlation Coefficient (CCC) and Black Widow Optimization (BWO) algorithm. In the presented encryption technique, CCC operation is utilized to optimize the encryption process of cryptography method. The projected encryption algorithm works in line with encryption and decryption processes. Optimal key selection is performed with the help of Artificial Intelligence (AI) tool named BWO algorithm. With the combination of AI technique and CCC operation, optimal security operation is improved in IoT. Using different sets of images collected from databases, the projected technique was validated in MATLAB on the basis of few performance metrics such as encryption time, decryption time, Peak Signal to Noise Ratio (PSNR), CC, Error, encryption time and decryption time. The results were compared with existing methods such as Elliptical Curve cryptography (ECC) and Rivest-Shamir-Adleman (RSA) and the supremacy of the projected method is established.

Keywords: Security; images; encryption time; correlation coefficient; black widow optimization; artificial intelligence; decryption time

1 Introduction

Internet of Things (IoT) is a novel phenomenon that connects the devices and things through remote or wired internet for seamless communication and functioning of devices. IoT has been extensively applied in a wide range of domains such as transportation, communication [1], business, technology, manufacturing and so on. The concept of IoT hyperlink enables people and organizations to point out the problems remotely without talking to each other [2–4]. Currently, about 26.66 billion IoT gadgets are in use worldwide. IoT was first introduced as a trial and error technology in 2011 to be applied in home automation, smart-energy meters and wearable gadgets. The developments made in IoT has helped corporates to categorize the way how their business practices can be developed, track their transactions, resource tracking and conduct statistical survey. IoT has optimized the way people live by proposing computerized administrations [5]. However, this high penetration of IoT in today's world has also a drawback to address i.e., security and safety challenges [6].

Lack of gadget updates, slow functioning of the gadgets and changing passwords without understanding the associated consequences have increased cyber security risks while it also made the usage of sensitive information, a vulnerable activity in IoT framework [7]. Such extraordinary risk attempts improve the probability of loss of privacy and information breakdown among different types of risks. Furthermore, most of the security experts acknowledge that IoT gadgets do not pay the much-needed attention to cyberattacks, as a result of weak security arrangements and traditions. Several security measures have been taken to secure IoT gadgets from cyberattacks whereas the rules for increasing the security challenges have not yet been satisfactorily achieved [8]. In other words, the security efforts taken by the end user may not necessarily protect their information from cyberattacks. Since 2008, hackers have developed different malware configurations to attack the IoT architecture [9]. These cyber attackers have chosen various phishing components to encourage people or representatives to share significant data and information. Therefore, personal gadgets and corporate workstations face security breaches in light of attacks on high-level corporate connections. While security professionals and gadget developers can accurately assess such cyberattacks, they can frame compelling security strategies for war and prevent the digital risks [10]. It is important for the specialists manage different risk concerns. Further, they should also plan at far-sighted security strategies and measures to ensure the security of business resources by enforcing better management and coordination [11].

Existing encryption techniques such as Information Encryption Standard, Advanced Encryption Standard [12] and Rivest-Shamir-Adleman calculations [13] have been used earlier to address the difficulties in terms of low-performance scenarios, low levels of information and high thought process. Subsequently, these techniques were sufficient enough to overcome the hurdles and an appropriate encryption technique can be recognized for clinical images within the IoT system [14]. Unique image encryption Dion calculations or techniques to change the images are calculated by different dialog techniques. In trading tool, a clear image is used to apply irregular correction. Pixels and its thickness can be converted into squares in any case [15]. The other option is to map every element in the clear image to digital image with some other trademarks since key methods are being explored.

The main contributions of the current study are as follows.

- Novel lightweight cryptography method has been proposed to enhance the security in IoT. The projected encryption algorithm is a blend of Cross Correlation Coefficient (CCC) and Black Widow Optimization (BWO).
- In the proposed encryption algorithm, CCC process is exploited to enhance the encryption process of cryptography. The proposed encryption algorithm works in line with encryption and decryption processes.
- Optimal key selection is executed with the help of Artificial Intelligence (AI) technique named BWO algorithm. Due to the combination of AI technique and CCC operation, the optimal security operation gets improved in IoT.

- Using different sets of images collected from databases, the projected technique was validated in MATLAB on the basis of few performance metrics such as encryption time, decryption time, Peak Signal to Noise Ratio (PSNR), CC, Error, encryption time and decryption time.
- The results were compared with existing methods such as Elliptical Curve cryptography (ECC) and Rivest-Shamir-Adleman (RSA) and the supremacy of the projected method is established.

Rest of the article is developed as briefed herewith. Section 2 reviews the studies conducted earlier in the same domain. Section 3 describes the proposed encryption and decryption procedure model. A detailed description of key generation process is explained in Section 4. Section 5 concludes the manuscript.

2 Literature Review

A number of methods has been developed earlier to enhance the security of images in IoT framework. Archana et al. [16] introduced a different attack calculation method for unadulterated poor optical cryptosystems. Furthermore, a safe asymmetric crypto-wound was introduced with respect to limited modulus rot that was stacked in Fresnel field. Fresnel misappropriation and asymmetric modulus scandal are exceptionally gentle in their limits. An informative grayscale film was first twisted with an arbitrary stage cover, at which point the Fresnel got disintegrated followed by rotting of the bad modulus. This is a two-layered cycle to get the milling image and it resembles an exceptionally irregular and white image. The project was recognized in the classification of grayscale and pair images. However, the parallel focus demonstrated reproduction for boat, stream flight, medicine and vegetable films. The outcomes demonstrated that the projected crypto-ulcer image reduces the issues and withstood both real and exceptional attacks. The proposed crypto-season was a real attack related on histogram, entropy, and contact allocation investigation in adjacent pixels. The results were shown depending on correlation coefficient whereas the true estimates exist such as normal square error between the blank content and encryption. The proposed plan works against the confusing attack.

Khatavkar et al. [17] validated the performance of an image encryption process using a single key method. This model was tested on some images which yielded excellent results. Less Significant-Bit (LSP)-based techniques are highly popular for steganography in spatial field. Simple LSP technique converts the LSP in cover image with bits from confidential information. Further, the advanced techniques can be used to identify the pixels that can transform LSPs with bits of confidential information using certain criteria. The insertion of confidential information into carrier in Discrete Cosine Transform (DCT)-based technique, depends on its coefficients. Any DCT coefficient, above the correct threshold, is a potential location for the insertion of confidential information.

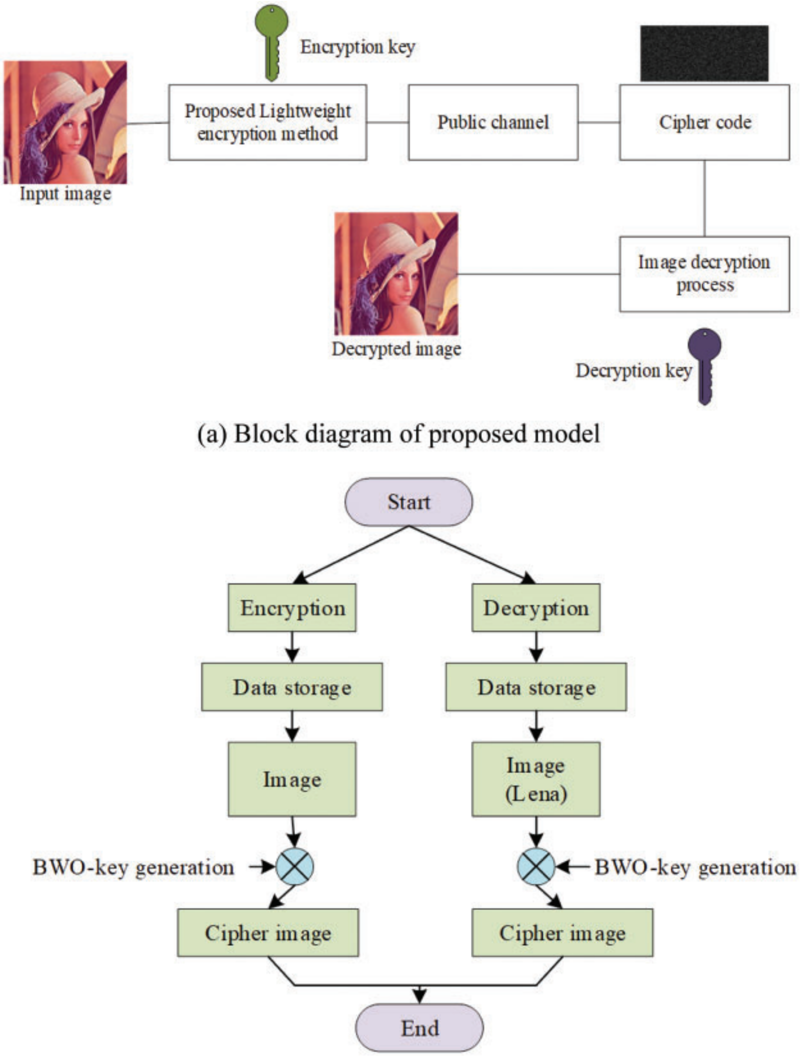
Xian et al. [18] presented a type of matrix as a recalculation technique with fractal characteristics named ‘Fractal Sorting Matrix’ (FSM). FSM is normal, self-similar and markedly repetitive. It is significant to note that clearing images or information related to this cluster of matrices efficiently improves the security of encryption technique. The study presented global pixel diffusion technique with two confusing displays to provide better security and high encryption performance. In addition to global confusing pixel distribution, in line with FSM, this study developed an efficient safe confusing image encryption algorithm too which was efficient than conventional approaches. According to comparison results, the presented technique was faster and a high pass rate was associated with local Shannon entropy. The data for ant differential attack test was close to theoretical values and the data fluctuations were found to be small. Further, the images obtained from crop and noise attacks were clear. Therefore, the presented method showed better protection and resistance to different types of attacks.

Hua et al. [19] developed a Two-dimensional Logistic Tent Modular Map (2D-LTMM) to create Color Image Encoding Algorithm (CIEA), otherwise known as LTMM-. CIEA. In contrast to current false maps, utilized for image encryption, 2D-LTMM can be leveraged to maximum extent in a more comprehensive manner. Further, it shows consistent confusing access and more consistently possess diffused paths. LTMM-CIEA uses cross-plane shift and uniform scattering to achieve diffusion in addition to confusing properties. The cross-plane level converts the demand and segment the pixels into three shadow planes. The subsequent scattering pattern scales the pixels in a mysterious and irregular request. The primary aim of this investigation is to integrate LDMM-CIEA2D-LDMM so as to overcome the inadequacies found in conventional confusing maps and clear the three shadow planes of images simultaneously. The evaluation outcomes in security ratings show that 2D-LTMM surpasses the confusing guidelines of late generation, and outperforms advanced image encryption techniques in terms of LTMM-CIEA security.

Wu et al. [20] introduced a crypto-developed image encryption process with two-dimensional partial unwinding decomposition (2D-PUD) method. Among three levels, stream ensemble (initial section of the security key) was created in the first level through a pseudo-arbitrary number. In second level, a clear image was distorted by 2D-PUD into three sections such as 2D rot section, two 1D rot parts and normal power value of the image. For a long time, 2D rot section is replaced through a common Arnold transition, where the normal power value is designated as the second fragment of wellness key. Scatter method is used to process the controlled or capable image with irregular 1D decay components (third part of the security key) in addition to segments through which the digital image is acquired. Due to the versatility of 2D-PUD, the 1D decomposition parameters can be uniquely created to different images. Also, they can be basically separated by changing the rot times for a similar film. Accordingly, the introduced computation is an image content-versatile encryption program that can successfully balance the cryptographic attacks. The evaluation outcomes reveal the technique with better encryption processing and can overcome the drawbacks found in the classification of conventional attacks including rebel force, scalable, entropy and various attacks.

3 The Proposed System Model

Security enhancement is an essential factor to achieve in digital era while security computations are one of the methods to assure this security. Image encryption process is an important step to protect the images communicated through IoT platforms. The entropy of images gets enhanced with efficient encryption processes and the relationship between two pixels gets reduced with an equivalent one. Both entropy and correlation are considered to empower the security of the system. The proposed technique has been designed to optimize the security of images. The complete diagram of the proposed methodology is shown in Fig. 1.



(a) Block diagram of proposed model

(b) Flowchart of proposed model

Figure 1: Proposed architecture

The proposed calculation method is used for both decryption and encryption processes which empowers the security. The proposed algorithm proceeds with entropy in addition to correlation measure and is named as cryptographic algorithm. The projected lightweight encryption is largely dependent upon the security and accuracy of images in IoT submission. The projected method primarily measures the entropy and correlation factors. The following subsections discuss about the proposed algorithm in detail.

3.1 Proposed Encryption and Decryption Procedures

The proposed procedure considers both entropy and correlation and is explained in this section.

3.1.1 Entropy

Entropy is the calculation of similarity between the encrypted images and unique images. The results are encrypted in a coded image and a separate image edge. The image is considered to have an acceptable visual quality [21] whereas blank image has a border of zero entropy. In addition, such a system undoubtedly turns it into a more modest document size. Further, a high entropy image with high pixel thickness cannot be converted into a moderate image. This makes the image a different one into a zero image. As a result, entropy can be defined as an integer as given herewith.

$$E = -\sum_{n=0}^{s-1} P\left(N\right) logP\left(N\right) \tag{1}$$

where, s denotes the possibility symbol and E denotes the entropy. The input image is denoted by $S(0, 255)$. This possibility parameter is utilized to analyze the original image in addition to the encrypted image. The entropy value is utilized to analyze the security level of the image. Higher the value of entropy, closer the image to the absolute value and the scenario is deemed to be a safe condition.

3.1.2 Correlation

In recent years, Digital Image Correlation (DIC) method has evolved in detail with updated versions. DIC is related to CC and can be described as an examiner of pixel asset during subset selection on different images. Further, it also plays a role during the removal of distortion charting function associated with images [22]. This CC is utilized to enable the efficient method for empowering the system performance. Cross correlation can be mathematically formulated as follows.

$$\eta = \frac{N\sum AB - \sum a \sum b}{\sqrt{\frac{N\sum\left(A^2\right) - \sum\left(A^2\right)}{N\sum\left(B^2\right) - \sum\left(B^2\right)}}} \tag{2}$$

where, $\sum\left(B^2\right)$ denotes the aggregate of squared b data, $\sum(B)$ denotes the amount of squared data, $\sum(A)$ denotes the sum of data, $\sum(AB)$ denotes the addition of products of objective information series, η denotes the correlation value and N denotes the number of data pairs. In CC, some of the key performance is decided by few factors such as execution time, memory requirement, crypto analysis and encryption quality.

3.1.3 Encryption and Decryption Processes

The proposed encryption procedure is developed as a three-stage procedure. In first stage, the transition mechanisms are initialized with input image. Here, shuffling mechanism is utilized with 256-bit key for encryption process. The complete process is given below.

- Initially, the images are designated.
- Pixel blocks are generated from optimal images by distributing the procedure.
- The pixel block = image width/10 is computed at horizontal range.
- The pixel block = Image height/10 is computed at vertical range. The computation of pixel block is mathematically formulated as follows.

$$Pixel\,blocks = horizontal\,pixel\,block * vertical\,pixel\,block) \tag{3}$$

- After that, the number of pixels is checked using the formula given below.

$$If\,pixel\frac{blocks}{2!} = 0 \tag{4}$$

$$Then\ set\ number\ of\ pixel\ blocks = number\ of\ pixel\ blocks\ +\ extra\ pixel\ block \tag{5}$$

- Divided the pixel blocks into deputize blocks (SB1, SB2)
- Then choice variables $I = 0$ and $R = 0$

($R =>$ *random variable*)

While ($I < SBI.R = random\ number\ among(o, subblock - I)$

- Set the novel position of block R <= pixel block

$I = I + 1$

- End while
- Similarly, for SB2.I = 0 and R = 0

While (I < SB2.R = random values among (0, SB2-I) R <= pixel block)

I = I + 1

End while.

- At last, get the novel position of pixels blocks in SBI and SB2.

Initially, the parameters are configured. Then, the key is selected with the help of BWO. The block-based image is encrypted and decrypted using reverse process. Finally, the proposed method is utilized to enhance the security of image. A detailed description of the proposed key generation method is presented in the upcoming section.

3.2 Proposed Algorithm for Key Generation

The proposed BWO methodology is utilized to find the optimal key parameters so as to enhance the image security. With an objective to enhance the security, it becomes important to meet the security parameters of images, which are also checked in the proposed algorithm. This section details about the proposed BWO algorithm which is popular for its mating behaviour followed by killing spree of BW spiders. In the presented model, cannibalism is an exclusive model. Naturally, these 8-legged spiders are assumed to be air-breathing arthropods with venomous fangs. Being arachnids, these species are of large order that rank seventh in species hierarchy with an incomplete diversity. Moreover, various dimensions have been hypothesized by experts on decoding the relations among these spider families. BWO algorithm starts with an initial spider population in which every spider yields a result [23]. Next, the female BW stores sperms and produces the egg in sacks. After 11 days, the spiderlings hatch out of egg sacs. The basic characteristics of BWO (as shown in Fig. 2) are discussed herewith.

The possible answers for every issue are measured as BW spider. Every BW spider is considered as an issue parameter in the equation given below.

$$W = \left[X^1, X^2, \ldots, X^{N^{Var}}\right] \tag{6}$$

Here, N^{Var} represents the dimension of parameters, X^1, X^2 denote the floating-point numbers accomplished with the fitness function. It can be expressed as follows.

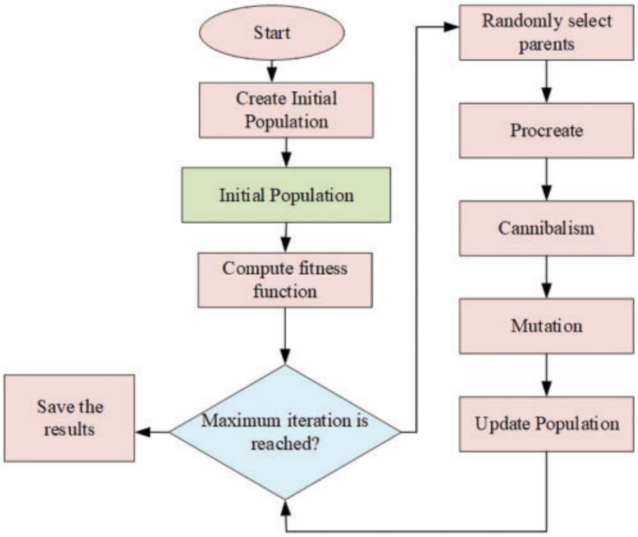


Figure 2: Flowchart of the BWO algorithm

$$F\,(W) = f\left[X^{1}, X^{2}, \ldots, X^{N^{Var}}\right] \tag{7}$$

To reproduce the optimization model, the candidate widow matrix is created with early populace of spiders. After that, parent pairs are arbitrarily designated to proceed with breeding process, during when the male spider is killed by female BW spiders after mating process is over.

Once the initial population is completed, the fitness function is computed. According to the fitness function, the best possible coefficient value of logistic map is calculated. The fitness function is evaluated by considering the PSNR value. The PSNR should be maximized to enable efficient secure operation. Hence, the fitness function is formulated with the maximization of PSNR. The fitness function is achieved by selecting the optimal logistic map coefficient value. The fitness function is mathematically formulated as follows.

$$\mathrm{FF} = \mathrm{MAX}\,\{\mathrm{PSNR}\} \tag{8}$$

$$PSNR = 10log_{10}\left(\frac{MAX^{P}}{MSE}\right) \tag{9}$$

$$MSE = \frac{1}{N{*}M}\sum_{X=1}^{N}\sum_{Y=1}^{M}\left[I_{image}\,(A,B) - I_{d-image}(A,B)\right]^{2} \tag{10}$$

where, $I_{d-image}(A,B)$ is described as decrypted image and $I_{image}\,(A,B)$ is described as the input image. Based on fitness function, the logistic sine map coefficients are selected and are utilized to enhance the optimal hybrid cryptography procedure.

After this, the mating procedure is initiated to generate the novel population. In real-world application, over 1,000 eggs are produced after every mating process. Eventually, spiderlings grow in a strong manner.

$$\begin{cases} Y^{1} = \alpha \times X^{1} + (1-\alpha) \times X^{2} \\ Y^{2} = \alpha \times X^{2} + (1-\alpha) \times X^{1} \end{cases} \tag{11}$$

Finally, the array is sorted according to cannibalism rating and fitness parameter. Further, the optimal solutions are gathered to the freshly-created population.

i, Cannibalism

Among the three different types of cannibalisms reported, sexual cannibalism is considered here in which the female kills the male counterpart after the breeding is over [24]. According to male and female cannibalism, the fitness value is estimated.

ii, Mutation

In this method, mute pop number is selected automatically with the population. All the solutions are randomly chosen which transfers two components in the array [25].

iii, Convergence

Like other models, the end criteria is checked using three stages such as (i) different iterations (ii), achieving the specified level of accuracy, and (iii) adherence to no variation in fitness value. BWO is practical in optimization issues and the algorithm generates the optimum solutions.

The adaptive projected technique is employed to choose the key parameter of the projected encryption algorithm. BWO optimization algorithm gets enhanced with the help of fitness function which in turn empowers the security of the algorithm since the optimal values of key parameters are selected. The complete flowchart of the presented methodology is briefed herewith.

Initially, random key parameters are selected in the security algorithm which degrades the security of image. Optimal key parameter selection is an essential task to enable efficient security process for the image. Initialization of the algorithm is a random key parameter for image security. BWO is utilized to select the optimal parameters with reverse solution initialization. Finally, the proposed model is employed to choose the optimum key parameters of the presented model.

4 Performance Evaluation

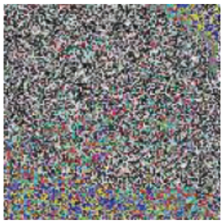
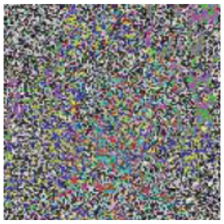
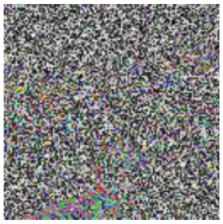
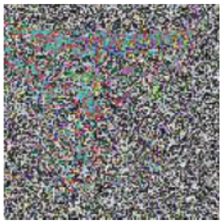
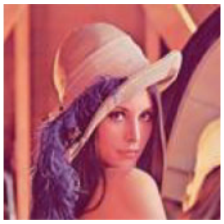
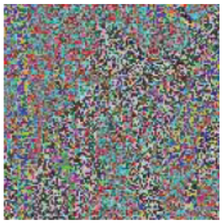
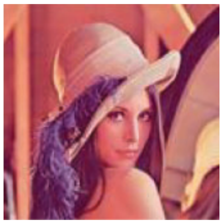
In this subsection, the performance of the projected technique was validated through comparison and performance analysis. The projected hybrid cryptographic technique was tested in a PC with system configurations such as Intel Core i5-2450M CPU 2.50 GHz laptop and 6 GB RAM. This methodology was implemented in MATLAB software R2016b. To validate the performance, image databases were collected from the literature [26] with 512∗512 dimension images. The images were labeled as Lena, Boat, hairstyle girl, Barbara, hill station and low bit rate images. The projected technique was analyzed based on performance metrics such as PSNR, Error rate, CC, Encryption time, and Decryption time. The parameters for the implementation of the projected method are shown in Tab. 1.

Table 1: Proposed methodology parameters

S. No	Method	Description	Value
1	Proposed method	Number of populations	50
2		Crossover %	0.8
3		Mutation %	0.4
4		Cannibalism %	0.5
5		Number of iterations	100

The performance of the presented methodology was analyzed based on performance metrics which validates the security of images.

Table 2: Experimental analysis of the proposed methodology

S. No	Input image	Encrypted image	Output image
1			
2			
3			
4			
5			
6			

Tab. 2 shows the images used to validate the proposed method which contain the input image, encrypted image, and output image. With the help of the presented technique, the images were encrypted and stored in Cloud Computing through encryption. The images were encrypted using a hybrid cryptographic algorithm. Hybrid cryptography was utilized to secure the image data in cloud server unit. The projected method is mainly designed to secure the image and empower user authentication process. Tab. 3 shows the performance metrics used to evaluate the proposed method. The projected technique achieved secure data storage and user authentication process. Secure authentication process was enabled with the help of login process as shown in Fig. 3.

Table 3: Performance analysis of the proposed method

S. No	Input image	PSNR	Error	CC	Encryption time	Decryption time
1	Image 1	48.3008	0.96161	1	0.005097	0.002091
2	Image 2	48.2003	0.98413	1	0.001654	0.001674
3	Image 3	48.1308	1	1	0.001953	0.001628
4	Image 4	48.1334	0.99941	1	0.001595	0.001719
5	Image 5	48.1308	1	1	0.001584	0.001582
6	Image 6	48.1311	0.99994	1	0.001595	0.001597

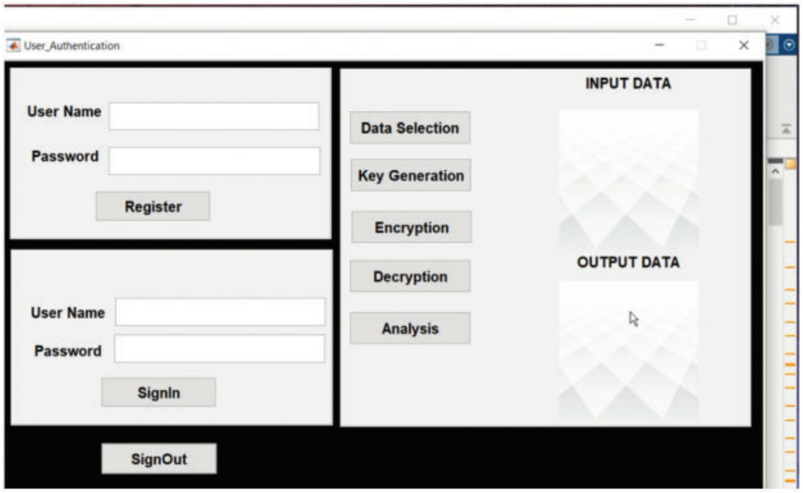


Figure 3: Encryption and decryption process

The performance of the projected model was validated under different performance metrics and the results were compared against established methods such as ECC and RSA. The PSNR results achieved by the proposed methodology are shown in Fig. 4. The projected method achieved 48.3008 PSNR rate for image 1. However, ECC achieved a PSNR value of 42.12 for image 1 while RSA achieved a PSNR value of 38.12 for image 1. Thus, the analysis results infer that the proposed method achieved a high PSNR rate compared to existing methodologies such as ECC and RSA. The MSE results achieved by the proposed approach and other approaches are shown in Fig. 5. The presented approach achieved an error rate of 0.0383 for image 1. However, ECC achieved an error rate of 0.0745 for the same image whereas RSA achieved an error rate of 0.0912. This result conclude that the proposed method is superior to previously-designed methods like ECC and RSA.

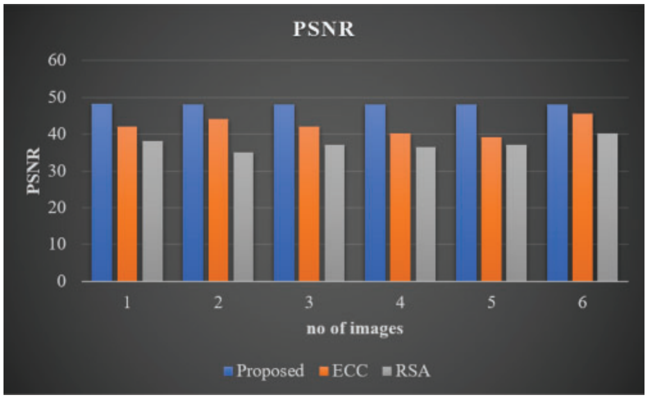


Figure 4: PSNR analysis of proposed model

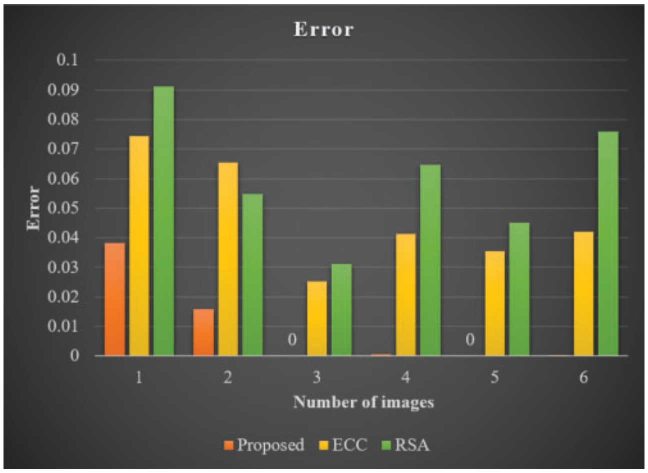


Figure 5: MSE analysis of proposed model

In line with the above, the encryption time of the methodologies were compared and the results are shown in Fig. 6. The proposed method achieved an encryption time of 0.005097 for image 1. Similarly, ECC achieved an encryption time of 0.05412 for image 1 while RSA achieved an encryption time of 0.0615 for the same image. Thus, the analysis results conclude that the projected method consumed low encryption time compared to other two techniques i.e., ECC and RSA. Fig. 7 shows the decryption times achieved by the proposed methods and other compared methods. The proposed method achieved a decryption time of 0.00201 for image 1. However, ECC achieved a high decryption time of 0.0201 for the same image 1. Further, RSA too achieved a high decryption time of 0.0305 for the same image. From the analysis, it can be included that the proposed method is superior to the previously-designed methods like ECC and RSA. The CC value of the developed methodology and other two methods are demonstrated in Fig. 8. The developed method achieved 1 as the CC value for image 1. However, ECC achieved 0.5 CC and RS achieved 0.6 CC for the same image 1. This analysis outcomes too conclude the superiority of the proposed method compared to previously-designed methods like ECC and RSA.

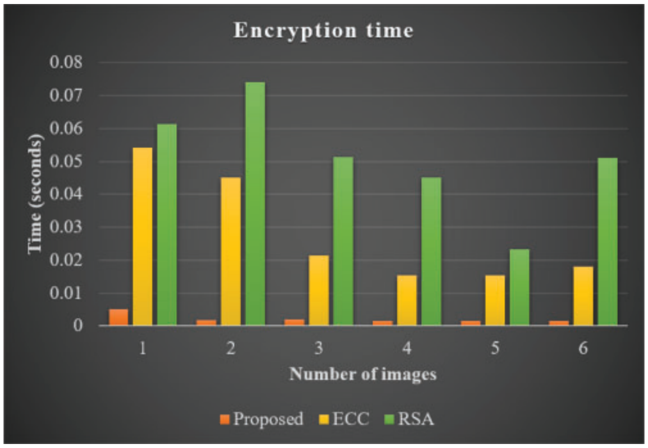


Figure 6: Encryption time analysis of proposed model

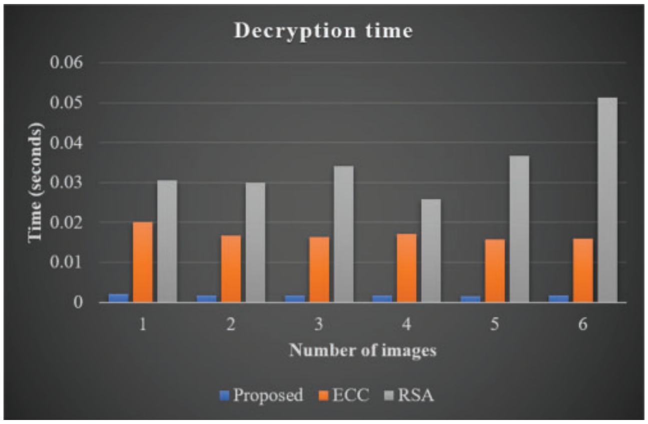


Figure 7: Decryption time analysis of proposed model

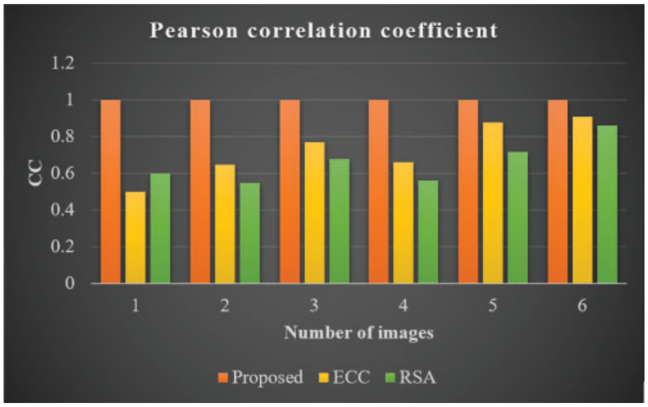


Figure 8: Pearson correlation coefficient analysis of proposed model

5 Conclusion

In current study, the researchers proposed a Novel Lightweight Cryptography Method to enhance the security in IoT. The proposed encryption algorithm is a blend of CCC and BWO. In the proposed encryption algorithm, CCC is utilized to optimize the encryption process of cryptography. The proposed encryption algorithm works on the basis of encryption and decryption processes. BWO algorithm is used to perform the optimal key selection process. Due to the combination of AI technique and CCC, the optimal security operation gets improved in IoT. The proposed method was simulated in MATLAB and was tested using different sets of images under various performance metrics such as encryption time, decryption time, PSNR, CC, Error, encryption time and decryption time. When the results achieved by the proposed method was compared against the existing methods such as ECC, and RSA, the proposed method was found to have achieved better results in terms of image encryption. In future, multi-modal fusion techniques can be developed for healthcare sector.

Acknowledgement: This work was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under Grant No. (D-387-135-1443). The authors, therefore, gratefully acknowledge DSR technical and financial support.

Funding Statement: This work was funded by the Deanship of Scientific Research (DSR), King Abdulaziz University, Jeddah, under Grant No. (D-387-135-1443).

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

References

[1] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, no. 8, pp. 1154–1169, 2021.

[2] Y. Chen, W. Zheng, W. Li and Y. Huang, "Large group activity security risk assessment and risk early warning based on random forest algorithm," *Pattern Recognition Letters*, vol. 144, no. 4, pp. 1–5, 2021.

[3] J. Porras, J. Pänkäläinen, A. Knutas and J. Khakurel, "Security in the Internet of Things—A systematic mapping study," in *Proc. of the 51st Hawaii Int. Conf. on System Science*, Hawaii, USA, pp. 3750–3759, 2018.

[4] Z. Han and A. Xu, "Ecological evolution path of smart education platform based on deep learning and image detection," *Microprocessors and Microsystems*, vol. 80, no. issue 9, pp. 103343, 2021.

[5] B. Alhayani, S. T. Abbas, D. Z. Khutar and H. J. Mohammed, "Best ways computation intelligent of face cyber attacks," in *Materials Today: Proc.*, pp. S2214785321016989, 2021. DOI 10.1016/j.matpr.2021.02.557.

[6] B. Wang, B. F. Zhang and X. W. Liu, "An image encryption approach on the basis of a time delay chaotic system," *Optik*, vol. 225, pp. 165737, 2021.

[7] M. Anuradha, T. Jayasankar, N. B. Prakash, M. Y. Sikkandar, G. R. Hemalakshmi *et al.,* "IoT enabled cancer prediction system to enhance the authentication and security using cloud computing," *Microprocessors and Microsystems*, vol. 80, no. 1, pp. 103301, 2021.

[8] J. Fan, B. Bingwei, W. Zehong, L. Hongqi, W. Yu *et al.,* "Flexible, switchable and wearable image storage device based on light responsive textiles," *Chemical Engineering Journal*, vol. 404, pp. 126488, 2021.

[9] H. Chen, Z. Liu, C. Tanougast, F. Liu and W. Blondel, "Optical cryptosystem scheme for hyperspectral image based on random spiral transform in gyrator domains," *Optics and Lasers in Engineering*, vol. 137, no. 3, pp. 106375, 2021.

[10] M. Wang, X. Wang, T. Zhao, C. Zhang, Z. Xia *et al.,* "Spatiotemporal chaos in improved cross coupled map lattice and its application in a bit-level image encryption scheme," *Information Sciences*, vol. 544, no. 6, pp. 1–24, 2021.

[11] 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.

[12] H. Wen, C. Zhang, P. Chen, R. Chen, J. Xu *et al.,* "A quantum chaotic image cryptosystem and its application in iot secure communication," *IEEE Access*, vol. 9, pp. 20481–20492, 2021.

[13] M. Gupta, K. K. Gupta and P. K. Shukla, "Session key based image cryptographic algorithm using logistic-sine map and crossover operator for IoT," *Journal of Scientific Research*, vol. 65, no. 1, pp. 260–265, 2021.

[14] S. S. Gopalan, A. Raza and W. Almobaideen, "IoT Security in healthcare using AI: A survey," in *2020 Int. Conf. on Communications, Signal Processing, and their Applications (ICCSPA)*, Sharjah, United Arab Emirates, pp. 1–6, 2021.

[15] V. C. S. R. Shankar, R. U. S. D. V. Prasad, R. V. Adiraju, R. V. V. Krishna and D. Nanda, "A review paper based on image security using watermarking," in *Proc. of Int. Conf. on Recent Trends in Machine Learning, IoT, Smart Cities and Applications*, Singapore, Springer, pp. 697–706, 2021.

[16] Archana, Sachin and P. Singh, "Cascaded unequal modulus decomposition in Fresnel domain based cryptosystem to enhance the image security," *Optics and Lasers in Engineering*, vol. 137, no. 7, pp. 106399, 2021.

[17] M. D. Khatavkar and A. S. Mali, "A image security with image steganography using dct coefficient and encryption," *International Journal of Innovations in Engineering Research and Technology*, vol. 3, no. 9, pp. 1–8, 2016.

[18] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Information Sciences*, vol. 547, no. 8, pp. 1154–1169, 2021.

[19] Z. Hua, Z. Zhu, S. Yi, Z. Zhang and H. Huang, "Cross-plane colour image encryption using a two-dimensional logistic tent modular map," *Information Sciences*, vol. 546, pp. 1063–1083, 2021.

[20] Y. Wu, L. Zhang, T. Qian, X. Liu and Q. Xie, "Content-adaptive image encryption with partial unwinding decomposition," *Signal Processing*, vol. 181, no. 1, pp. 107911, 2021.

[21] V. Nežerka and J. Trejbal, "Assessment of aggregate-bitumen coverage using entropy-based image segmentation," *Road Materials and Pavement Design*, vol. 21, no. 8, pp. 2364–2375, 2020.

[22] G. K. Jankee and B. Ganapathisubramani, "Comparison between object and image plane cross-correlation for stereoscopic PIV in the presence of pixel locking," *Experiments in Fluids*, vol. 61, no. 3, pp. 89, 2020.

[23] V. Hayyolalam and A. A. P. Kazem, "Black widow optimization algorithm: A novel meta-heuristic approach for solving engineering optimization problems," *Engineering Applications of Artificial Intelligence*, vol. 87, no. 1, pp. 103249, 2020.

[24] E. H. Houssein, B. E. Helmy, D. Oliva, A. A. Elngar and H. Shaban, "A novel Black Widow Optimization algorithm for multilevel thresholding image segmentation," *Expert Systems with Applications*, vol. 167, no. 12, pp. 114159, 2021.

[25] S. Memar, A. M. Meymand and W. Sulisz, "Prediction of seasonal maximum wave height for unevenly spaced time series by black widow optimization algorithm," *Marine Structures*, vol. 78, no. 10, pp. 103005, 2021.

[26] http://imageprocessingplace.com/root_files_V3/image_databases.htm.