Chaotic Butterfly Optimization with Optimal Multi-key Image Encryption Technique for Wireless Sensor Networks

Disheng Zheng[1], Kai Liang[2]

[1]Ningbo Institute of Technology, Zhejiang University, China

[2] School of Control Engineering, Chengdu University of Information Technology, China

Emails: zds@nit.zju.edu.cn; lk1987@cuit.edu.cn

Abstract

A wireless sensor network (WSN) comprises a set of sensor nodes, mainly used for data collection and tracking processes. The imaging sensors in WSN capture the images from the target environment, which need to be securely transmitted to the base station (BS). Since data transmission in WSN takes place through wireless links, security is a major challenging issue involved in the design of WSN. Image encryption is a commonly available solution to securely transmit the images to the destination without comprising security. Therefore, this study designs a novel Chaotic Butterfly Optimization with Optimal Multi-key Image Encryption (CBO-OMKIE) technique for WSN. The goal of the CBO-OMKIE technique is to securely encrypt the images in WSN. The proposed CBO-OMKIE technique involves the design of a multi-key-based image encryption technique to accomplish security in WSN. In addition, the CBO algorithm is applied to determine the optimal keys involved in the encryption process and it helps for improving the security level to a maximum extent. The performance validation of the CBO-OMKIE technique takes place using benchmark test images and the outcomes were examined under several aspects. The simulation outcome pointed out the enhanced security analysis of the CBO-OMKIE technique over the other techniques.

Keywords: Wireless sensor networks; Image encryption; optimal key generation; Multi-key approach; Butterfly optimization

1. Introduction

A wireless sensor network (WSN) is a kind of Adhoc network in that resource-limited sensor nodes are placed for control or monitoring tasks. A standard architecture of sensors contains more than one processor, one sensing unit, a memory, a power source, and a communication component. Then, these sensor nodes would be utilized for performing the measurement of a few physical magnitudes from the environmental conditions [1]. This measurement can be transformed and processed into an electrical signal that is eventually communicated via the transmission components across a wireless network towards the sink nodes, through a collection of transmission and protocol standards. WSN collects visual information from a monitored field operation under the same standards, however visual transmission, data sensing, and processing are very difficult because of the massive number of data to be processed than scalar information [2]. Generally, sensors consist of transmission, processing, and storage limits invented from their resource-limited nature. Camera-assisted sensor nodes placed for retrieving video streams and image snapshots would normally request additional resources when compared to conventional scalar sensor nodes [3], which brings further problems to the operation and design of wireless visual sensor networks (WVSN). Fig. 1 illustrates the overview of WSN.

DOI: https://doi.org/10.54216/JISIoT.010203

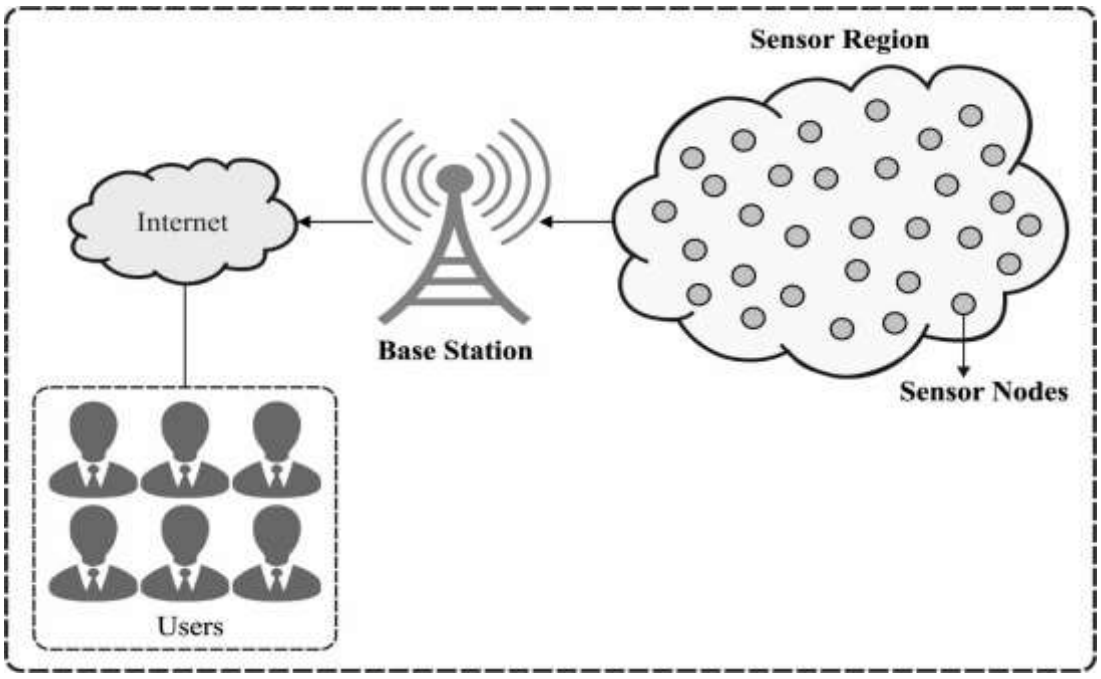

Figure 1: The working procedure of wireless sensor networks

Lately, several researchers have presented advanced solutions for enhancing the efficiency of this network and present potential contributions [4]. In a few instances, transmission and sensing of image snapshots are most convenient when compared to transmission and sensing of video streams, which determine the possibility of a wireless image sensor network (WISN) [5]. Various WISN applications would have privacy needs. Sensors might be placed in huge and harder-to-access domains, whereas the wireless channel could be accessed by a third person. Besides intrinsic difficulties, while trying to guarantee integrity, the communication flow might be subjected to privacy attacks. Eventually, authorization is needed for various applications, for assuring that the retrieved data come from the valid source node. The resource-limited nature of standard WISN applications discourages the usage of conventional privacy methods as used on the Internet [6]. Robust cryptography, e.g., might quickly reduce the constrained energy source of sensors.

Alternatively, several researchers have presented advanced methods for addressing this problem, applying enhanced solutions [7]. WSN has several susceptibilities which can be used by the attackers. Therefore, firstly define the standard susceptibilities in WSN that might affect WISN. Integrity, authenticity, and Confidentiality are always guaranteed by data encryption that is employed as a foundation for various privacy mechanisms. Communication of images needs high energy consumption, large memory, and high bandwidth [8]. Multimedia communication is an error-tolerant protocol. When image compression methods are employed to enhance the quality of broadcast rate, conserve energy and reduce latency. Since the beginning of this decade, Authors have utilized distinct methods of image compression [9].

This study designs a novel Chaotic Butterfly Optimization with Optimal Multi-key Image Encryption (CBO-OMKIE) technique for WSN. The proposed CBO-OMKIE technique involves the design of a multi-key-based image encryption technique to accomplish security in WSN. In addition, the CBO algorithm is applied to determine the optimal keys involved in the encryption process and it helps for improving the security level to a maximum extent. The performance validation of the CBO-OMKIE technique takes place using benchmark test images and the outcomes are examined in several aspects. The simulation outcome pointed out the enhanced security analysis of the CBO-OMKIE technique over the other techniques.

2. Related works

DOI: https://doi.org/10.54216/JISIoT.010203

In Khan et al. [10], DWT based partial image encryption system with hashing mechanism, Hussain's S-Box, and chaotic maps are described. The plaintext image is compressed through DWT and next the image is shuffled row and column-wise through Nonlinear Chaotic Algorithm and Piece-wise Linear Chaotic Map (PWLCM), correspondingly. In order to attain high security, early condition for PWLCM is performed based on the hash function. The transposed images are bitwise XORed using an arbitrary matrix made from an Intertwining Logistic map. For enhancing the additional security, the last ciphertext is attained afterward replacing each element with Hussain's substitution box.

Elhoseny et al. [11] present a novel encryption system based on homomorphic encryption and ECC to protect data forwarding in WSN. The presented system is based on the GASONeC method which employs the GA method for building an optimal network framework through clusters. ECC is utilized for swapping private and public keys because of its capacity of providing higher security with smaller key sizes. The presented encryption keys are 176-bits and are generated by integrating the node detection number, distance to its CH, and ECC key.

In Shankar and Lakshmanaprabu [12], the Homomorphic Encryption (HE) method using optimum key selection for image security was implemented. Now, the histogram equalization is presented to alter image intensity for improving the contrast. In order to improve the security level stimulated Ant Lion Optimization (ALO) has been taken into account, in which the FF as max entropy the optimally-encrypted image is considered as the image with maximum astounding entropy amongst nearby pixels. Istwal and Verma [13] presented a model-based secure communication of data with a modified Arnold Cat map utilizing 802.11a/g in WSN. In order to protect the communication of information, data can be transmuted in the coded format through the data encoding technique. Since data transmitted in the open domain has been secured is a major concern. In Arnold Cat map, initially, information is encrypted, later it can be transmuted to the linear array, and next information is demodulated and modulated by the OQPSK afterward utilizing decryption it back to its novel form.

Gao et al. [14], presented the architecture of Trusted WSN which consists of 2 primary classes that are platform security improvement and Trusted Authentication protocol for enhancing the sensor's security features and authorize the fidelity of node linking the networks correspondingly. In KLEF [15], according to the chaotic map and genetic operation, a lightweight block cipher can be performed for addressing this limitation. The transmission nodes are confirmed by the chaotic map parameter in this cryptographic system as well as output the bit sequence pseudo arbitrarily. In order to encrypt the data blocks, XOR, and mutation crossover operations are utilized. Genetic operations and chaotic maps are utilized in sensor networks for providing security and confidentiality for information.

Mishra and Dastidar [16] utilized images as data for decryption and encryption. This study shows the usage of the Secure Force (SF) model for decryption and encryption system. The research has been conducted by utilizing MATLAB. Many parameters such as Entropy, PSNR, and MSE have been estimated. Elhoseny et al. [17] present a secured image processing and broadcast scheme in WSN with Homomorphic Encryption (HE) and ECC.

Vaseghi et al. [18] considered the secured transmissions in the WSN-based strong adaptive finite time chaos synchronization model in the existence of uncertainty and noise. For that reason, the adapted Chua oscillator is included in the BS and sensors for generating the chaotic signal. The chaotic signal is impregnated using uncertainty and noise. Initially, they employ the adapted independent component analyses for separating the noise from the chaotic signal. Next, with the adoptive finite-time sliding mode controllers, an adaptive parameter tuning and a control law technique are presented for achieving the finite-time chaos synchronization in the parametric uncertainties and noisy conditions.

3. The Proposed Model

In this study, a novel CBO-OMKIE technique is presented to accomplish security in WSN. In addition, the CBO algorithm is applied to determine the optimal keys involved in the encryption process and it helps to improve the security level to a maximum extent. Fig. 2 illustrates the overall block diagram of the CBO-OMKIE model

DOI: https://doi.org/10.54216/JISIoT.010203

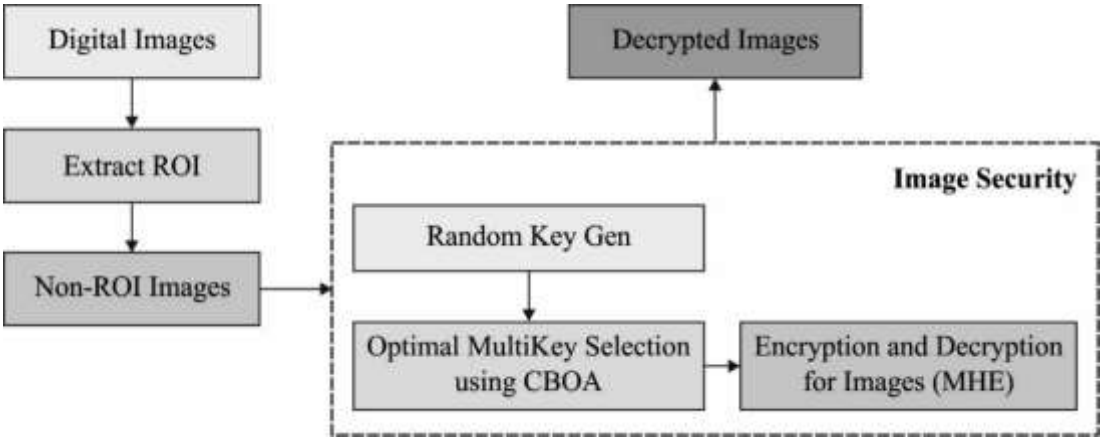

Figure 2: Overall block diagram of CBO-OMKIE model

In order to image security, the Multiple Key Homomorphic Encryption (MHE) method has been utilized. This is a novel technique for privacy protection and image security. The encrypted information is calculated without decryption whereas the result is similar to the 'ascertained one' attained from the initial image. Mostly, encryption and decryption methods exploit public and private keys for MHE for improved image security enhancing keys by using the CBO method. This optimization can be implemented for propelling open and private keys of the receiver and sender process of encrypted security. Afterward the decrypted approach, the produced images are ultimately distinguished as the key image to survey their implementation with the PSNR Entropy. This method is utilized for upgrading the security level of the encoder image by reducing the networks amongst image modules and expanding their entropy esteem.

Region of interest (ROI) for images

It can be a bit of an image where the filter performs many activities. It is a binary image and indistinguishable in size from an image. In the mask images, the pixel characterizes the ROI as fixed to one and each pixel is fixed to zero.

Image security phase

Image encryption methods become an essential portion of an image conveyance procedure, once they point towards productivity and meanwhile, protect the maximum-security level. The related subsection portrays 4 symmetric image encryption methods rapidly. The presented method utilizes MHE as the ideal key to image security procedures.

Multiple key-based Homomorphic encryptions (MHE)

Semantically secured homomorphic public key encryption algorithms are focal cryptographic devices for many secured multi-party estimation problems. The properties of homomorphic are valued for building a secure scheme with a higher security data recovery strategy. This encryption architecture is used for performing tasks with encoder information without no knowing the private key (with no decryption), viz., and the user has a major holder of the confidential key. The homomorphic calculation method considered the polynomial abundant cipher image that is encrypted in N keys, as well as related valuation keys, and deliver a cipher image [19]. It is represented as cascade ciphering, multiple encryptions, and cascade encryption. The presented MHE has 3 phases like encrypt/decrypt technique, optimal key determination, and multiple key generations.

Key generation

A key has been used for encrypting or decrypting whatever information is decrypted or encrypted. A scheme was utilized to encode and decode keys and the interrelated images with a symmetric key; trust value security and secrecy are provided. The relative public key (pu_k) and A private key (pr_k) from manifold keys. Key matching is used by an asymmetric key procedure; now, numerous keys $K =$

DOI: https://doi.org/10.54216/JISIoT.010203

$\{K1, K2, \ldots\ldots\ Kn\}$ are made for MHE. In several instances, the key is arbitrarily created by means of an Arbitrary Number Generator. For selecting the optimum key from numerous keys, the optimization method would be taken into account.

The inspiration behind hand optimized that it improves the privacy of key elections in image decryption and encryption procedure. To improve public and private keys in manifold key sets, CBO is exploited. Now, the transformative method is used for enhancing the encryption process. Finally, the optimum ciphered contents are selected as the final encryption contents. The motivation of the CBO method, adaptive system, and process are represented below.

Encryption and Decryption process

HE proposes encryption wherever cipher images and plain images are processed by an equivalent algebraic operation. HE allows the servers to perform the activities on encrypted information without knowing the initial plain image. Using the confidential key, a user encrypted the novel image and generate pr_k and $pu_{k-optimal}$, along with the public key (pu_k), this cipher image would be directed to the server. $pu_k = (k, i) and K = (p, q)\ Enc(I, pr_k)$ for pick arbitrary parameter ∴r ∈ Z^*_k, Calculate cipher information c = $I.r^k$ mod k^2. An encryption procedure is lately effective for the confidential image of a unique image. The decryption technique is comprised of the usage of 2 masks, especially, the confidential and the Mask in a stable development. Homomorphic processes, e.g., Multiplications and Addition, are implemented on the encoder image that would transmit the novel encrypted image where decryption would provide similar functions. The homomorphic tasks are related to the pixels of 2 encoding images.

Consider Original Image for security procedure

Extract ROI in these images

Produce numerous keys for HE

Manifold Key optimization procedure

Execute CBO update process

Adoptive operation

Select optimal key $pr_k \Rightarrow \{1, 2, , \ldots n\}$ and $pu_k \Rightarrow \{1, 2, , \ldots n\}$

Execute optimum key-based decryption and encryption

3.1 Optimal key generation in CBO

This method is a new speed-enhancing algorithm using optimal resolving convergence and minimal processing complexity. This approach has been progressed by butterfly food exploring behavior. It is a kind of insect using several abilities such as smell, hearing, and taste to assist in detecting partner mating, egg laying, and applicable nectar in an adaptable position and escapes from the attackers. The research exhibits the smelling nature of the butterfly as one of the important characteristics and recognizes the food from a long distance. They seek food by chemoreceptor. It can able to sense, place, and different smells inside an optimum precision. The BOA population is determined by the collection of butterflies as search agents. The expenditure of an objective function in BOA diverges according to the butterfly's position. BOA can be determined by swarm optimization algorithm (SOA) wherein each agent shares the information through another butterfly according to the fragrance distance. The process included in the BO method can be given in the following section.

Fragrance

It can be categorized into 3 portions Stimulus intensity (I), Power exponent (a), and Sensory modality (c). The power is an exponent utilized to select significant density that results in regular, response

DOI: https://doi.org/10.54216/JISIoT.010203

compression, and linear. On the other hand, sensory is determined as the form of energy where modality determines the employed input using sensor nodes. The substance of the butterfly is designed using 2 essential conditions: the variance of fragrance (f) and stimulus intensity (I). This can be formulated by:

$$f = cI^{\beta} \quad (1)$$

whereas a, and β c are in an interval of zero and one.

Movement of butterflies

This can be made up 3 main stages in the following:

- Initialization
- Searching
- Finalizing

Now, the model metrics have been fixed. When the variables are set the optimization method is initialized. The main position of butterflies could be made in an arbitrary way from solution space. When the iteration is initiated, an artificial butterfly presents in a searching space migrating to the novel location and attained the cost value [20]. Next, the butterfly produces a fragrance in a similar position by:

$$x_i^{t+1} = x_i^t + (r^2 \times g^* - x_i^t) \times f_i \quad (2)$$

whereas g^* represent the optimal solution for iteration t, x_i^t determines the solution vector x_i for i^{th} butterfly, the fragrance of i^{th} butterfly is stated as f_i and r represents an arbitrary number in the range of zero and one.

The BOA parameter, as well as partner mating and food exploring of butterflies, are implemented in global and local measures.

The local search in this method is given in the following:

$$x_i^{t+1} = x_i^t + \left(r^2 \times x_j^t - x_k^t\right) \times f_i \quad (3)$$

Algorithm 1: Pseudo Code of BO Algorithm

1: Objective function f(x), x= (x_1, x_2…, x_d)

2: Create a population of n butterfly xi= (i=1, 2…, n)

3: Characterize switch probability p, sensor modality c, and power exponent a

4: while end conditions are not satisfied do

5: for all the butterflies bf in the population do

6: Estimate the fragrance

7: end for

8: Define the optimal bf

9: for all the butterfly's bf in the population do

10: produce a random value of rand from [0, 1]

DOI: https://doi.org/10.54216/JISIoT.010203

11: if rand < p then

12: Move to the optimal butterfly

13: else

14: Move arbitrarily

15: end if

16: Compute the novel butterfly

17: once the novel one is optimal, upgrade the population

18: end for

19: Upgrade the values of c

20: Explore the present global optimal

21: end while

22: Show the reached optimum solution

The BOA method has attained outstanding result in seeking optimal measure that has a limit in convergence. In this way, a novel technique is presented for changing the essential metrics of BOA based on the convergence speed. For resolving this issue, the vector of main variables for BOA is represented as $V = [a, c, r]$ which is based on the chaos concept. Chaos science has been represented as a learning task that is unpredictable and random tasks. It can be extremely utilized in extreme sensations which get influenced by the least adjustment. The feature generates points with better distribution and solved the difficulty of enhancing the point distribution. It can be expressed as follows:

$$V_{i+1}^{j} = f\left(V_i^{j}\right), j = 1,2, \dots, l \tag{4}$$

Whereas, l represents the map dimension and $f\left(V_i^{j}\right)$ denotes a chaotic model generator. Now, Logistic Mapping is used by,

$$a_{k+1} = \rho a_k (1 - a_k) \tag{5}$$

$$c_{k+1} = \rho c_k (1 - c_k) \tag{6}$$

$$r_{k+1} = \rho r_k (1 - r_k) \tag{7}$$

In which, k indicates the iteration number, $a_0, c_0, r_0 \in [0,1]$ denotes the early random measure, and ρ determines a control variable in the range of $\rho \in [0,1] - [0.25, 0.5, 0.75]$. It can be noted $\rho = 4$, the function may be in chaos state.

4. Performance Validation

The performance validation of the CBO-OMKIE technique takes place utilizing benchmark test images and the results are examined under various measures.

Table 1 offers the results analysis of the CBO-OMKIE technique on the test images applied. The results have shown that the CBO-OMKIE technique has accomplished improved performance on every image. For instance, with the Lena image, the CBO-OMKIE technique has attained a PSNR of 65.588dB, CC of 0.992, MSE of 0.009, and entropy of 7.940. Likewise, with the Baboon image, the CBO-OMKIE approach has reached a PSNR of 56.090dB, CC of 0.982, MSE of 0.160, and entropy of 8.250.

DOI: https://doi.org/10.54216/JISIoT.010203

Moreover, with the Pepper image, the CBO-OMKIE technique has attained a PSNR of 69.100dB, CC of 1.000, MSE of 0.008, and entropy of 8.124. Furthermore, with the House image, the CBO-OMKIE methodology has gained a PSNR of 58.588dB, CC of 0.989, MSE of 0.090, and entropy of 8.712.

DOI: https://doi.org/10.54216/JISIoT.010203

Table 1: Result analysis of CBO-OMKIE model with different measures

Images	PSNR	CC	MSE	Entropy
Lena	68.588	0.992	0.009	7.940
Baboon	56.090	0.982	0.160	8.250
Pepper	69.100	1.000	0.008	8.124
House	58.588	0.989	0.090	8.712

A brief PSNR analysis of the CBO-OMKIE technique with other manners is provided in Table 2 and Fig. 3. The PSNR values denoted that the CBO-OMKIE technique has gained higher PSNR values over the other compared methods. For instance, on the Lena image, the CBO-OMKIE technique has resulted in an increased PSNR of 68.59dB whereas the HE-ALO, HE, and ECC techniques have obtained reduced PSNR values of 50.21dB, 46.51dB, and 30.98dB respectively. In line with, on House image, the CBO-OMKIE system has resulted in an enhanced PSNR of 58.59dB whereas the HE-ALO, HE, and ECC techniques have attained minimal PSNR values of 51.22dB, 47.77dB, and 36.37dB correspondingly.

Table 2: PSNR analysis of CBO-OMKIE model with existing manners

PSNR (dB)				
Images	**CBO-OMKIE**	**HE-ALO**	**HE**	**ECC**
Lena	68.59	50.21	46.51	30.98
Baboon	56.09	52.22	45.24	31.77
Pepper	69.10	48.45	48.57	29.55
House	58.59	51.22	47.77	36.37

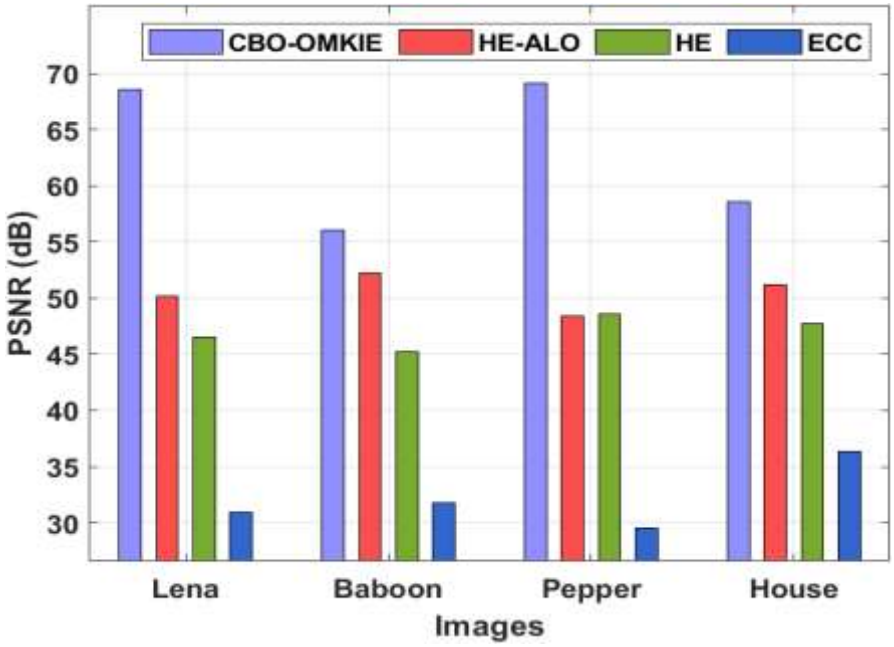

Figure 3: PSNR analysis of CBO-OMKIE model

DOI: https://doi.org/10.54216/JISIoT.010203

Table 3: MSE analysis of CBO-OMKIE model with existing manners

MSE				
Images	**CBO-OMKIE**	**HE-ALO**	**HE**	**ECC**
Lena	0.009	0.012	0.236	0.846
Baboon	0.160	0.210	0.276	0.735
Pepper	0.008	0.010	0.213	0.448
House	0.090	0.130	0.183	0.980

Table 3 and Fig. 4 offer a comparative MSE analysis of the CBO-OMKIE technique with existing ones. The results implied that the CBO-OMKIE technique has attained effectual outcomes with minimal values of MSE. For instance, with the Lena image, the CBO-OMKIE technique has attained a minimum MSE of 0.009 whereas the HE-ALO, HE, and EEC techniques have achieved maximum MSE of 0.012, 0.236, and 0.846 respectively. Furthermore, with the House image, the CBO-OMKIE approach has attained a minimal MSE of 0.090 whereas the HE-ALO, HE, and EEC methods have achieved maximal MSE of 0.130, 0.183, and 0.980 correspondingly.

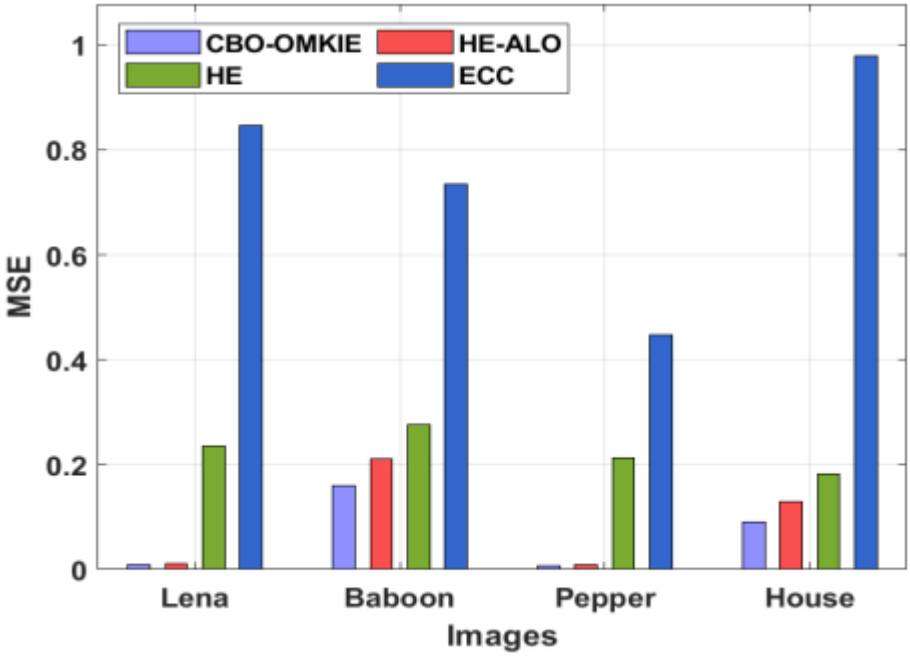

Figure 4: MSE analysis of CBO-OMKIE model

Table 4: CC analysis of CBO-OMKIE model with existing manners

CC				
Images	**CBO-OMKIE**	**HE-ALO**	**HE**	**ECC**
Lena	0.992	0.980	1.306	0.507
Baboon	0.982	0.970	0.648	0.694
Pepper	1.000	1.000	1.064	0.432
House	0.989	0.980	0.742	1.290

DOI: https://doi.org/10.54216/JISIoT.010203

A detailed CC analysis of the CBO-OMKIE technique with other methods is offered in Table 4 and Fig. 5. The CC values represented that the CBO-OMKIE technique has gained higher CC values over the other compared approaches. For instance, on the Lena image, the CBO-OMKIE algorithm has resulted in an increased CC of 0.992 whereas the HE-ALO, HE, and ECC techniques have obtained reduced CC values of 0.980, 1.306, and 0.507 correspondingly. Likewise, on the House image, the CBO-OMKIE manner has resulted in a higher CC of 0.989 whereas the HE-ALO, HE, and ECC systems have obtained lower CC values of 0.980, 0.742, and 1.290 correspondingly.

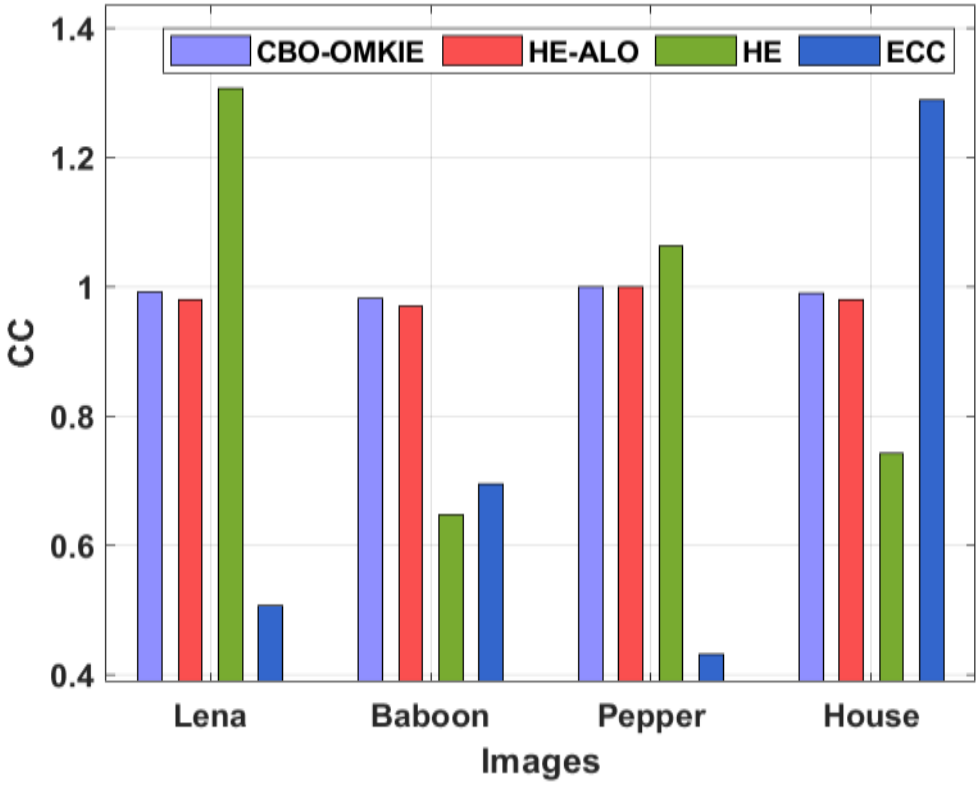

Figure 5: CC analysis of CBO-OMKIE model with existing approaches

Table 5: Entropy analysis of CBO-OMKIE model with existing manners

Entropy				
Images	**CBO-OMKIE**	**HE-ALO**	**HE**	**ECC**
Lena	7.940	7.640	6.009	4.064
Baboon	8.250	7.850	6.375	2.084
Pepper	8.124	7.740	6.578	4.589
House	8.712	8.012	8.571	6.537

A brief entropy analysis of the CBO-OMKIE system with other approaches is provided in Table 5 and Fig. 6. The entropy values signified that the CBO-OMKIE technique has gained higher entropy values over the other related algorithms. For instance, on the Lena image, the CBO-OMKIE method has resulted in an increased entropy of 7.940 whereas the HE-ALO, HE, and ECC systems have obtained fewer entropy values of 7.640, 6.009, and 4.064 respectively. Followed by, on House image, the CBO-

DOI: https://doi.org/10.54216/JISIoT.010203

OMKIE technique has resulted in a superior entropy of 8.712 whereas the HE-ALO, HE, and ECC methodologies have achieved least entropy values of 8.012, 8.571, and 6.537 respectively.

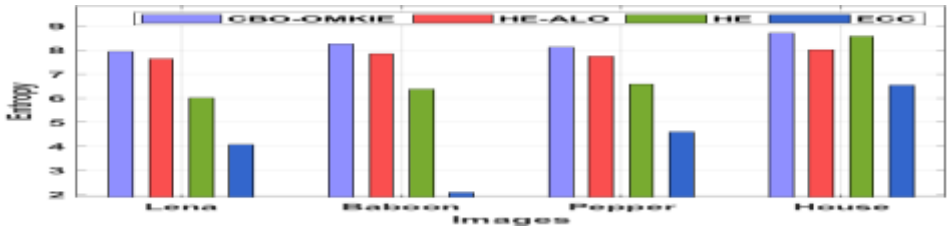

Figure 6: Entropy analysis of CBO-OMKIE model

Table 6: Time complexity analysis of CBO-OMKIE model with existing manners

Time Complexity (sec)				
Images	**CBO-OMKIE**	**HE-ALO**	**HE**	**ECC**
Lena	5.787	8.188	11.080	15.050
Baboon	7.649	10.198	14.217	16.178
Pepper	8.335	12.109	15.050	16.619
House	5.639	7.649	9.610	11.276

Table 6 and Fig. 7 provide a comparative TC analysis of the CBO-OMKIE algorithm with existing ones. The outcomes understood that the CBO-OMKIE technique has attained effectual outcomes with minimal values of TC. For instance, with the Lena image, the CBO-OMKIE technique has reached a decreased TC of 5.787s whereas the HE-ALO, HE, and EEC techniques have achieved higher TC of 8.188s, 11.080s, and 15.050s correspondingly. Moreover, with the House image, the CBO-OMKIE approach has attained a reduced TC of 5.639s whereas the HE-ALO, HE, and EEC methods have achieved increased TC of 7.649s, 9.610s, and 11.276s correspondingly.

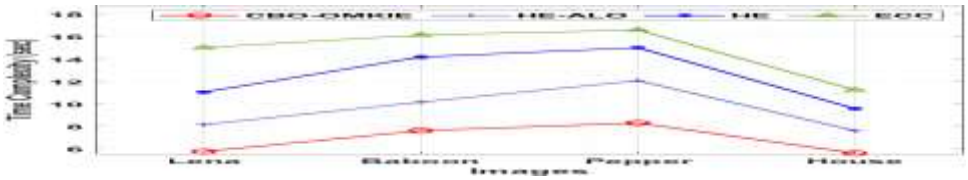

Figure 7: Time complexity analysis of CBO-OMKIE model

5. Conclusion

In this study, a novel CBO-OMKIE technique is presented to accomplish security in WSN. The proposed CBO-OMKIE technique involves the design of a multi-key based image encryption technique to accomplish security in WSN. In addition, the CBO algorithm is applied to determine the optimal keys involved in the encryption process and it helps for improving the security level to the maximum extent. The performance validation of the CBO-OMKIE technique takes place using benchmark test images and the outcomes are studied in many aspects. The simulation outcome pointed out the enhanced security analysis of the CBO-OMKIE technique over the other techniques. In the future, the CBO-MKIE technique can be realized in other wireless networks and the security performance can be further boosted by the image steganography approaches.

DOI: https://doi.org/10.54216/JISIoT.010203

References

[1] Shankar, K., Lakshmanaprabu, S.K., Gupta, D., Khanna, A. and de Albuquerque, V.H.C., 2020. Adaptive optimal multi-key based encryption for digital image security. Concurrency and Computation: Practice and Experience, 32(4), p.e5122.

[2] Zhang Y, Zhang LY, Zhou J, Liu L, Chen F, He X. A review of compressive sensing in the information security field. IEEE Access. 2016;4:2507-2519.

[3] Shankar K, Lakshmanaprabu SK. Optimal key-based homomorphic encryption for color image security aid of ant lion optimization algorithm. Int J Eng Technol. 2018;7(1.9):22-27.

[4] Thirumalai, C. and Kar, H., 2017, April. Memory Efficient Multi Key (MEMK) generation scheme for secure transportation of sensitive data over Cloud and IoT devices. In 2017 Innovations in Power and Advanced Computing Technologies (i-PACT) (pp. 1-6). IEEE.

[5] Jinasena, T.M.K.K., Meegama, R.G.N. and Marasinghe, R.B., 2018. A Novel Elliptic Curve Based Multi-Key Encryption Method for Multicasting Single Content with Access Control.

[6] Yang P, Gui X, An J, Tian F. An efficient secret key homomorphic encryption used in image processing service. Secure Commun Netw. 2017;2017:1-12. 7695751.

[7] Puech W. Image encryption and compression for medical image security. Paper presented at 2008 First Workshops on Image Processing Theory, Tools and Applications; 2008; Sousse, Tunisia.

[8] Khizrai MSQ, Bodkhe ST. Image encryption uses different techniques for high-security transmission over a network. Int J Eng Res Gen Sci. 2014;2(4):299-306

[9] Zheng P, Huang J. An efficient image homomorphic encryption scheme with small ciphertext expansion. In: Proceedings of the 21st ACM international conference on Multimedia; 2013; Barcelona, Spain.

[10] Khan, M.A., Ahmad, J., Javaid, Q. and Saqib, N.A., 2017. An efficient and secure partial image encryption for wireless multimedia sensor networks using discrete wavelet transform, chaotic maps, and substitution box. Journal of Modern Optics, 64(5), pp.531-540.

[11] Elhoseny, M., Elminir, H., Riad, A. and Yuan, X., 2016. A secure data routing schema for WSN using elliptic curve cryptography and homomorphic encryption. Journal of King Saud University-Computer and Information Sciences, 28(3), pp.262-275.

[12] Shankar, K. and Lakshmanaprabu, S.K., 2018. Optimal key-based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology, 7(9), pp.22-27.

[13] Istwal, Y. and Verma, S.K., 2017, September. Secured data transmission using improvised Arnold cat map in WSN. In 2017 3rd International Conference on Advances in Computing, Communication & Automation (ICACCA)(Fall) (pp. 1-4). IEEE.

[14] Gao, Y., Ao, H., Feng, Z., Zhou, W., Hu, S., and Tang, W., 2018. Mobile network security and privacy in WSN. Procedia Computer Science, 129, pp.324-330.

[15] KLEF, V., 2018. An efficient lightweight cryptography algorithm scheme for WSN devices using chaotic map and GE. International Journal of Pure and Applied Mathematics, 118(20), pp.861-875.

[16] Mishra, S. and Dastidar, A., 2018, March. Hybrid image encryption and decryption using cryptography and watermarking techniques for high-security applications. In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT) (pp. 1-5). IEEE.

[17] Elhoseny, M., Farouk, A., Batle, J., Shehab, A. and Hassanien, A.E., 2017. Secure image processing and transmission schema in a cluster-based wireless sensor network. In Handbook of study on ML trends and innovations (pp. 1022-1040). IGI Global.

[18] Vaseghi, B., Pourmina, M.A. and Mobayen, S., 2017. Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control. Nonlinear Dynamics, 89(3), pp.1689-1704.

[19] Xiao, L., Bastani, O. and Yen, I.L., 2012. An Efficient Homomorphic Encryption Protocol for Multi-User Systems. IACR Cryptol. EPrint Arch., 2012, p.193.

[20] Arora, S. and Singh, S., 2017. An improved butterfly optimization algorithm with chaos. Journal of Intelligent & Fuzzy Systems, 32(1), pp.1079-1088.

DOI: https://doi.org/10.54216/JISIoT.010203