https://doi.org/10.48047/AFJBS.6.15.2024.10081-10091

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

AN OPTIMAL KEY BASED ELLIPTIC CURVE CRYPTOGRAPHY FOR SECURING BIO METRIC IMAGES IN INTERNET OF THINGS

Ms.P.Shobana[1] Dr.D.Kannan[2]

Ph.D Scholar, Department of Comp.Science and Applications, Pollachi College of Arts and Science
&
Assistant Professor in IT , Sree Saraswathi Thiyagaraja College,Pollachi,India
shobana.send2@gmail.com

Principal,Pollachi College of Arts and Science, Pollachi, India.
kd.khannan@gmail.com

Volume 6, Issue 15, Oct 2024

Received: 15 Sep 2024

Accepted: 05 Oct 2024

Published: 25 Oct 2024

doi: 10.48047/AFJBS.6.15.2024.10081-10091

Abstract: Biometric security measures are available at several locations along the data process that comprises the Internet of Things (IoT). Saving and transmitting biometric data in the format of images across public networks necessitates using a fast, seamless, secure encryption system capable of preserving biometric image data while protecting them. More encryption techniques are introduced in the IoT environment. However, it consumes high power and more computational complexity and provides less security. Hence, this paper proposed a novel security approach using optimal key-based elliptic curve cryptography (OKECC) for biometric images in IoT. In this system, the biometric images are initially collected from the FVC2004 DB-3 dataset. Then the image compression is performed using Modified Huffman Encoding (MHE) to diminish the encryption model's storage space and computation burden. After that, image compression is performed using OKECC to encrypt the compressed image. Finally, on the receiver side, the reverse encryption and compression process is done to retain the original image. The experimental results reveal that the proposed system offers better security than the existing systems for biometric images.

Keywords: *Biometric images, Encryption, Decryption, Compression, Internet of Things, and Peak Signal to Noise ratio.*

1. INTRODUCTION

The Internet of Things (IoT) includes various devices with inbuilt sensors and processors that can handle their internal states or the external environment surrounding them and have become a part of people's daily necessities [1]. Most IoT applications currently encourage users to employ biometric authentication for security. Intelligent devices can control a smart house's electronic devices and door lock systems. Biometric authentication increases the security of these smart devices [2]. "Biometrics" is a combination of the Greek words "bio" (life) and "metrics" (to measure). The use of biometrics is familiar; the identification and authentication of humans based on bodily characteristics may be dated back thousands of years [3]. Physiological biometrics and behavioural biometrics are the two categories of biometric attributes. The physiological model recognizes people based on their body shape, similar to a fingerprint, face recognition, iris identification, hand geometry, palm print, and retina recognition. The body that determines the body's behaviour is the behavioural biometric in the second model [4, 5].The problem is that clients use biometrics indefinitely and need help to modify them. It is recommended that irreversible changes be used to prevent the theft of biometric pictures [6]. It is a difficult task in the case of IoT applications due to sensor constraints in terms of memory and computing efficiency [7]. The encryption technologies should preserve the confidentiality of the biometric image to guard against future generations of attacks[8]. Encryption ensures the secrecy of data by making it unreadable and worthless, even if lost or corrupted [9]. Researchers have been drawn to chaos algorithms among encryption systems due to their superior performance in noise production and image pixel permutation applications. The chaos-based encryption technique achieves outstanding picture diffusion, sensitivity to initial circumstances, and confusion [10]. It is more secure than traditional encryption methods such as DES, AES, and RSA. The robustness of chaotic-based encryption methods has significantly improved [11].On the other hand, the chaotic encryption technique requires floating calculations, which makes practical software or hardware implementation of such systems inefficient and complex. So, the proposed system employs an efficient OKECC-based encryption algorithm for biometric images in IoT. The contributions of the proposed system are as follows:

- To present an MHE method to compress biometrics to reduce the system's storage space and computation burden in data security.
- To propose, OKECC encrypts the compressed biometric images to transmit the data over the network securely.
- To present an ISSO algorithm to optimally select the private keys in ECC to improve the system's security for biometric images.
- To perform the comprehensive evaluation of the proposed and existing models regarding image security metrics to prove the performance efficiency of the proposed method.

The remaining phases of the manuscript are described: Section 2 presents the survey of recent image encryption methodologies for securing IoT. Section 3 presents a detailed explanation of the proposed research model. The simulation analysis of the proposed and existing methodologies is given in section 4. Finally, the conclusion of the suggested model is given in section 5.

2. RELATED WORK

Some researchers provide security solutions for biometric images In IoT. **Muhammed Golec *et al.* [12]** presented a biometric-based authentication approach, BioSec, to secure the IoT network. The biometric used to provide authentication of IoT users was a fingerprint. In addition, to ensure the security of the biometric data (fingerprint), an advanced encryption standard with a 128-bit key module was presented. The security of the user biometric data was maintained in both the database and transmission medium. This way, the technique offered security to the IoT environment and the user's biometrics data. The performance of the techniques was analyzed regarding processing time, and the presented AES technique outperformed other related schemes. **Rajendran Sujarani *et al.* [13]** recommended a lightweight bio-cryptosystem to secure biometric templates in IoT applications. The approach worked in three phases: key generation, confusion and diffusion. Initially, a 2-dimensional logistic sine map was utilized to perform a critical generation process. Then, diffusion-based DNA encoding and ciphering were used to ensure the data integrity and diminish the burden of the encryption process. The outcomes proved that the technique was robust and achieved a satisfactory level of security with lower computational complexity. **Shadi Yoosefian Dezfuli Nezhad *et al.* [14]** suggested an encryption method for fingerprint biometric images using DNA sequence and chaotic tent map. Initially, the fingerprint image was encrypted using the DNA sequences. The DNA-encrypted image was further encrypted by applying the XOR operator and chaotic mapping sequences to them. The average entropy for the final encrypted fingerprint image was obtained as a final step. The results showed that the technique attained good data encryption results and worked well against common attacks in the network.

Noha A. Hikal and Marwa M. Eid [15] presented a hybrid chaotic map-based encryption technique to secure palm print biometric images. The chaotic hybrid map was the combination of different chaotic maps applied to the specific control parameters of the biometric image. In addition, they are designed to overcome the difficulties of confusion and diffusion and to offer a larger key space. The results proved that the technique worked well against several well-known attacks in the network, such as brute force, statistical, and differential attacks. From the results of encryption and decryption time, it was also observed that the approach was more applicable in real-time network scenarios than other related schemes. **Ayman Altameem *et al.* [16]** presented a hybrid encryption scheme including chaos mapping and advanced IoT encryption standards (AES). Initially the authentication of the IoT users was done using the fingerprint system. Then the user's biometric template was encrypted using the hybrid encryption scheme and stored in the cloud to prevent the template from additional attacks. The system achieved better security results than the existing approaches.

The previous attempts benefit security and execution speed by addressing the critical distribution challenge or developing quicker algorithms. However, they have the following shortcomings: Most existing systems use a DNA encoding model for image encryption. Encoding and encryption are accomplished by applying complementary rules and arithmetic operations. However, the main disadvantage of this approach is that it necessitates longer processing times and consumes more power. Also, some researchers used a chaotic-based encryption algorithm, which provides better results. Nevertheless, it has numerous floating calculations and high computational complexity. Additionally, the works already done are focused on something other than compression algorithms. Compression algorithms provide additional security to the biometric system by reducing its storage space in the cloud system. Thus, motivated by the above limitations, this paper proposes a novel security approach using OKECC with an efficient compression scheme for biometric images in IoT.

3. PROPOSED METHODOLOGY

This paper proposes a novel security approach for securing IoT users' biometric-templated data transmission. Initially, the biometric images of the users are collected from the publicly available database. After that, the collected biometric images are compressed using the MHE. Then these compressed images are encrypted using the OKECC technique in which the key generation process of the ECC is done optimally using an ISSO to maximize PSNR. The reverse operation of the above processes is done to get the original biometric data. Fig.1 shows the proposed system's flow diagram.

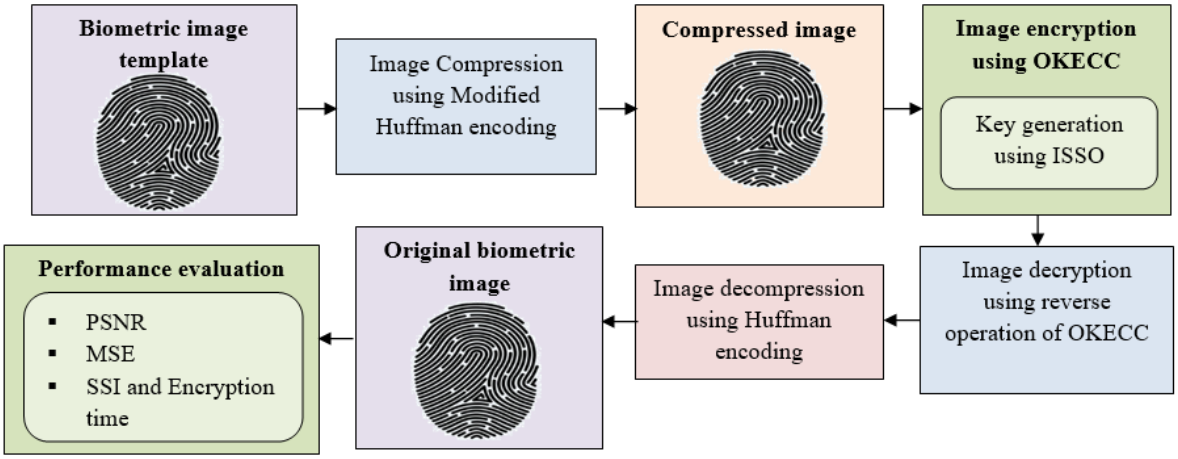

Figure 1: Workflow of the proposed work

3.1 Biometric Image Compression

Initially, the fingerprint images are taken from the FVC2004 DB-3 dataset. Next, image compression is performed on the collected data. Image compression seeks to reduce the irrelevant and redundant portions of the image to store or transmit data efficiently. This reduces the memory required to hold images and enables faster image transmission. The suggested system employs the MHEtechnique in this case. Huffman coding is a type of lossless data compression. A variable-length code is used in Huffman code to encode a source symbol (such as a character in a file) that has been introduced about the predicted probability of the source symbol. Because of this concept, the average code length is reduced, and the overall size of compressed data is smaller than the original. Nevertheless, the input images are directly given to the Huffman encoding increases the overhead during computation and leads to suboptimal performance. Instead of directly applying the input image into Huffman encoding, the proposed system randomly segments the images into blocks of smaller sub-image with size 64×64 to reduce the complexity of the computational process.This improvisation in conventional HE is named as MHE. The steps involved in the MHE are explained as follows:

Step 1: First, scale up the dimensions of the given biometric image to the following integral multiples of 64 by replicating the last row and column the required number of times. Further, it is divided into 64 × 64 blocks, and HE is applied on each block independently.

Step 2: Next, sort the probabilities of each block in descending order, while the occurrence of a specific pixel intensity value's probability $\left(\widehat{\underleftarrow{P}}_{sn}\right)$ is calculated as:

$$\widehat{\underleftarrow{P}}_{sn} = \frac{\underleftarrow{N}_{pix}}{\underleftarrow{T}_{num}} \tag{1}$$

Where, $\underleftarrow{N}_{pix}$ indicates the number of occurrences of a pixel with a specific intensity value and $\underleftarrow{T}_{num}$ is the count of pixelsin the sub image' blocks.

Step 3: After that, create a new node using the symbols of the two lowest probabilities $\widehat{\underleftarrow{P}}_{X}$ and $\widehat{\underleftarrow{P}}_{Y}$, of which these two probabilities re branches; the new node ismarked with the arithmetic sum of these two probabilities.

Step 4:Continue the process by replacing the new node with the original one until only one node remains.

Step 5: Mark the lower branch as one and the upper branch as 0.

Step 6: Identify the code of every source symbol by traversing the tree from root to leaf, noting the branch label of each node traversed. Thus, the compressed input image is given to the OKECC to encrypt the compressed image.

3.2 Image Encryption

After biometric image compression, image encryption is carried out using OKECC, which converts an image into a series of bytes such that third parties cannot view the original image. ECC is a public key encryption model based on the algebraic structure of elliptic curves over finite fields. It is more secure than other methods because it offers optimal security with shorter key lengths. The encryption and decryption process of the cryptographic model is done using the public and private keys. The private key of the algorithm is chosen randomly, which makes the task of third-party access easier to get the key. So, to improve the security of an ECC model, this paper generates the private key of the model optimally using the Improved Salp Swarm Optimization (ISSO) algorithm. Thus, optimally chosen keys in conventional ECC are termed OKECC. The steps involved in the OKECC are explained as follows:

Step 1: Key generation using ISSO

SSO was inspired by the swarming behaviour of salps when travelling and hunting in oceans. During this process, these salps try to find the best food location by following the leading salps. The first Salp is the leader, and the others are followers. It chooses the optimal keys with greater accuracy, yet, it faces several issues, like poor exploitation, slower convergence, and imbalanced exploration and exploitation operations. It also has a premature convergence issue. So, the proposed system uses some modifications in conventional SSO to enhance the population diversity of the SSO and prevent the algorithm from local optimum solutions. Firstly, the attraction approach is employed as the population initialization strategy that increases the diversity of the model and improves the exploration capability. Secondly, the population's dynamic step parameter

(DSP) is included in SSO to stabilize the exploration and exploitation capabilities of the model. These improvisations in conventional SSO are termed ISSO. The steps are as follows. The population of salps using the attraction strategy is implemented first to reduce the complexity. Each Salp here is drawn to any other better Salp. It denotes that a bad Salp (solution) progresses to a series of better salps. Thus, it is expressed as follows:

$$\underleftarrow{Z}_s(\tau+1) = \underleftarrow{Z}_s(\tau) + \xi(DT_{uv}).\left(\underleftarrow{Z}_{us}(\tau) - \underleftarrow{Z}_{vs}(\tau)\right) + \varphi + \varepsilon_u \tag{2}$$

$$\xi(DT_{uv}) = \xi_0 . e^{-DT_{uv}^2} \tag{3}$$

$$DT_{uv} = \sqrt{\sum_{s=0}^{S}\left(\underleftarrow{Z}_{us} - \underleftarrow{Z}_{vs}\right)^2} \tag{4}$$

Where, DT_{uv} refers to the distance between $\underleftarrow{Z}_u$ and $\underleftarrow{Z}_v$, ξ_0 indicates the attractiveness for $DT = 0$.When $\underleftarrow{Z}_u$ and $\underleftarrow{Z}_v$ are two different solutions and $\underleftarrow{Z}_v$ is superior to $\underleftarrow{Z}_u$, $\underleftarrow{Z}_u$ will move to $\underleftarrow{Z}_v$ by the attractiveness $\xi(DT_{uv})$. In addition, $\varepsilon_u \in [-0.5, 0.5]$ is a random value and $\varphi \in [0,1]$ indicates the step parameter. After population initialization, the fitness $(\underleftarrow{FiF})$of the individuals in the initialized population is estimated using equation (5). The individual obtaining the maximum peak signal-to-noise ratio (PSNR) is the best in the current iteration. The PSNR is the ratio of the maximum potential signal power to the power of the corrupted noise.

$$\underleftarrow{FiF} = \max(PSNR) \tag{5}$$

$$PSNR = 20 * \log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \tag{6}$$

$$MSE = \frac{1}{\breve{K}}\sum_{p=1}^{\breve{K}}\left(\breve{A}_{ve} - \breve{P}_{ve}\right) \tag{7}$$

Where, MSE denotes the mean squared error, $\breve{A}_{ve}$ and $\breve{P}_{ve}$ refers to the actual and predicted value and $\breve{K}-$ indicates the number of instances. Next, update the position of the leader using the following equation:

$$\underleftarrow{Z}_s^{lp} = \begin{cases} \underleftarrow{fp}_s + \lambda_1\left(\left(UB_s - LB_s\right)\lambda_2 + LB_s\right).\psi_{pm}, & \lambda_3 \geq 0.5 \\ \underleftarrow{fp}_s - \lambda_1\left(\left(UB_s - LB_s\right)\lambda_2 + LB_s\right).\psi_{pm}, & \lambda_3 < 0.5 \end{cases} \tag{8}$$

Where, $\underleftarrow{Z}_s^{lp}$ indicates the position of the best and possible solution, LB_s and UB_s refers to the lower and upper bounds of the s^{-th} dimension, and $\underleftarrow{fp}_s$ signifies the food source position. The control parameters includes λ_1, λ_2, and λ_3, among which λ_2 and λ_3 are arbitrary numbers between [0, 1], they control step size and direction and λ_1 is the primary control parameter, thatstabilizes the

algorithm's exploration and exploitationabilities.In addition, ψ_{pm} refers to the DSP, which gradually decreases from its initial value $(\psi_{pm})_0$, until it reaches the minimum threshold $(\psi_{pm})_{\min}$ as iterations advance and avoids the premature convergence problem in SSO. It is computed as follows:

$$\psi_{pm}^{\tau+1} = \psi_{pm}^{\tau} \cdot \left(1 - \frac{\tau}{Max\_Iterations}\right) \tag{10}$$

Then update the position of the follower by using the following equation.

$$\underleftarrow{Z}_s^r = \frac{1}{2}\left(\underleftarrow{Z}_s^r - \underleftarrow{Z}_s^{r-1}\right).\psi_{pm} \tag{11}$$

Where, $\underleftarrow{Z}_s^r$ represents the position of the r^{-th} follower at the s^{-th} dimension and $r \geq 2$. After updating the Salp follower's position at each iteration, all locations should be confirmed to respect the problem requirements. In this way, the optimal keys are selected using ISSO and the encryption process is proceeded further. This procedure is repeated until the stopping criteria are satisfied.

Step 2:Next, in ECC, the prime value is elected as V_p and the optimal private key is preferred as $\underleftarrow{W}_{PR}$. Next, The ECC process is expressed as follows:

$$\underleftarrow{E} = p(a)^3 + \hat{\alpha} * p(a) + \hat{\beta} \tag{12}$$

Where, $\hat{\alpha}$ and $\hat{\beta}$ represents the constant value $\hat{\alpha} = \hat{\beta} = 2$. One of the primary advantages of ECC is its tiny key size, transmission conditions and minimal storage. The best points are chosen for ECC when the condition $\underleftarrow{I} = \underleftarrow{J}$ is satisfied. Additionally, $\underleftarrow{I}$ and $\underleftarrow{J}$ are the two variables whose values are between zero and it is demonstrated in equation (13) and (14),

$$\underleftarrow{I} = \mathrm{mod}\left(\underleftarrow{E}, V_p\right) \tag{13}$$

$$\underleftarrow{J} = \mathrm{mod}\left(p(b)^2, V_p\right) \tag{14}$$

Where, $p(a,b)$ refers to the point of the elliptic curve and V_p denotes a prime number.Thus, the optimum base point p_{op} and $\underleftarrow{W}_{PU}$ refers to the public key as given below:

$$\underleftarrow{W}_{PU} = \underleftarrow{W}_{PR} * p_{op} \tag{15}$$

Where, $\underleftarrow{W}_{PR}$ indicates the optimal private key selected by ISSO. Then the encryptionprocess is performed on the input compressed data using the following equation.

$$CiText_1 = \left(\underleftarrow{R}_n * p_{op}\right) \tag{16}$$

$$CiText_2 = \left(\underline{\underline{FcI}} + \left(\underleftarrow{R}_n * \underleftarrow{W}_{PU}\right)\right) \tag{17}$$

Where $\underline{\underline{FcI}}$ refers to the compressed image to be encrypted and $\underleftarrow{R}_n$ signifies the arbitrary number, between1 to $n-1$, $CiText_1$ and $CiText_2$ indicates two ciphertexts.This encrypted image is securely transmitted to the cloud server.

3.3 Image Decryption

The decryption process performs the reverse encryption operation to get the compressed biometric data. The decryption is performed using optimal private key $\underleftarrow{W}_{PR}$ of the ECC model and which is estimated as

$$\underline{\underline{FcI}} = \left(\left(CiText_2 - \underleftarrow{W}_{PR}\right) * CiText_1\right) \tag{18}$$

Where $\underline{\underline{FcI}}$ indicates the input compressed image. After decrypting the compressed images, decompression is done using the MHE algorithm to get the original input biometric data.

4. RESULTS AND DISCUSSION

This section evaluates the outcomes of the proposed security approach using OKECC for biometric images in IoT against the existing security schemes. The system was implemented in the working platform of Python with machine configuration as follows: OS: Windows 10 Professional Edition; CPU: Intel i5, 8 GB RAM; GPU: Nvidia RTX 2060, 6 GB. The experimentation is carried out using FVC2004 DB-3 dataset. The dataset contains a total of 80 fingerprint biometric data from 10 individuals. From the dataset, 80% of the data is used for training, and 20% is used for testing. The results are plotted for the dataset's five randomly chosen biometric samples.

4.1 Performance Analysis for Compression Method

This section evaluates the outcomes of the proposed MHE with the existing HE, Arithmetic Encoding (AE), Contourlet Transform (COTR), and Bandelet Transform (BATR) regarding compression ratio. In image processing, the compression ratio is commonly stated as the ratio of the original image size to the compressed image size. A higher compression ratio implies that more data has been reduced, resulting in a smaller size of the compressed image. The compression ratio of the proposed and existing schemes is plotted in Fig. 2. The proposed one offers high compression ratio for images 1 to 5 than the existing methods because it utilizes an efficient MHE algorithm. For example, for image 1, the existing HE, AE, COTR, and BATR offers compression ratio of 74.98 %, 73.12 %, 71.87 %, and 67.14 %, respectively, but the proposed one offers a high compression ratio of 76.34%. Similarly, for the remaining number of images (2 to 5), the proposed achieves high compression ratio than the existing methods. Thus, it shows the effectiveness of the proposed work for compressing the biometric samples of IoT users.

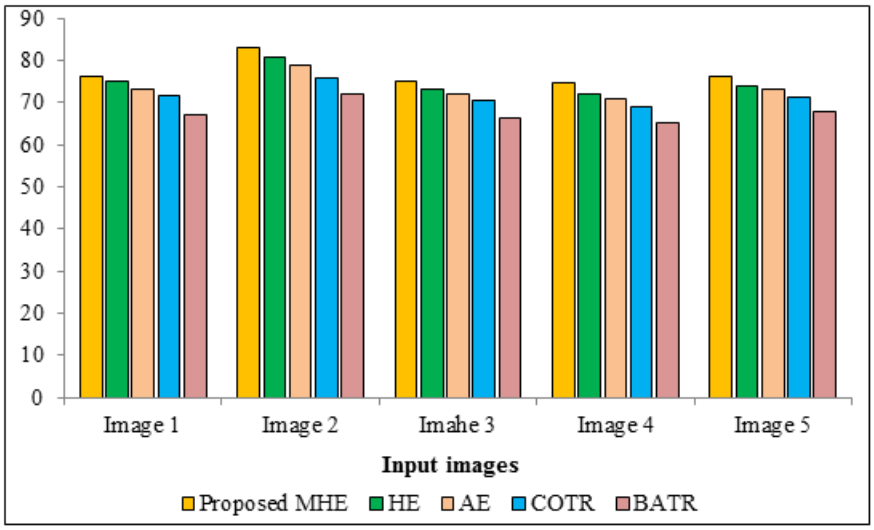

Figure 2: Compression ratio analysis

4.2 Performance analysis for Image Encryption

This section compares the outcomes of the proposed OKECC with the conventional ECC, Chaotic Encryption (CHE), Deoxyribonucleic Acid (DNA), and AES regarding MSE, PSNR, Structural Similarity Index (SSI), and Encryption time (ET), which is shown in table 1.

Table 1: MSE, PSNR, and SSI of the encryption schemes

Metrics	Input images	Proposed OKECC	ECC	CHE	DNA	AES
MSE	Image 1	0.045	0.075	0.106	0.126	0.158
	Image 2	0.039	0.065	0.129	0.138	0.146
	Image 3	0.054	0.085	0.109	0.129	0.138
	Image 4	0.032	0.061	0.089	0.143	0.169
	Image 5	0.041	0.072	0.087	0.129	0.158
PSNR	Image 1	63.38	59.37	57.92	57.15	56.31
	Image 2	63.98	59.99	57.04	56.81	56.43
	Image 3	62.34	58.82	57.9	57.11	56.69
	Image 4	64.03	60.28	59.04	56.31	55.23
	Image 5	63.54	59.53	59.12	57.06	56.25
SSI	Image 1	0.919	0.889	0.856	0.824	0.809
	Image 2	0.911	0.881	0.859	0.828	0.802
	Image 3	0.905	0.874	0.845	0.814	0.798
	Image 4	0.923	0.894	0.869	0.836	0.814
	Image 5	0.915	0.885	0.857	0.826	0.806

The minimum value of MSE shows the better achievement of the suggested system with lower errors. The proposed one has a minimum MSE for all sample images compared to existing ones. For example, for image 5, the proposed one has an MSE of 0.041, which is comparatively lesser than the existing ECC (0.072), CHE (0.087), DNA (0.129), and AES (0.158). Likewise, the proposed one has minimum MSE values for the remaining sample images. Regarding PSNR measures, a higher PSNR number is better because it indicates a higher signal-to-noise ratio. Here also, the proposed has a higher PSNR than the existing methods for images 1 to 5. For images 1 to 5, the proposed one achieves a maximum PSNR of 64.03db, but the existing methods have a minimum PSNR of 55.23db. The SSI evaluates the structural distortion of the decrypted image and the original biometric images, ranging between [0, 1]. SSI's most significant value shows the encryption model's better performance. The proposed one also has a higher SSI than the existing methods. Thus, the overall results demonstrate that the proposed one attains superior outcomes contrasted to the existing methods. Fig.3 shows the ET obtained by the proposed and existing encryption schemes.

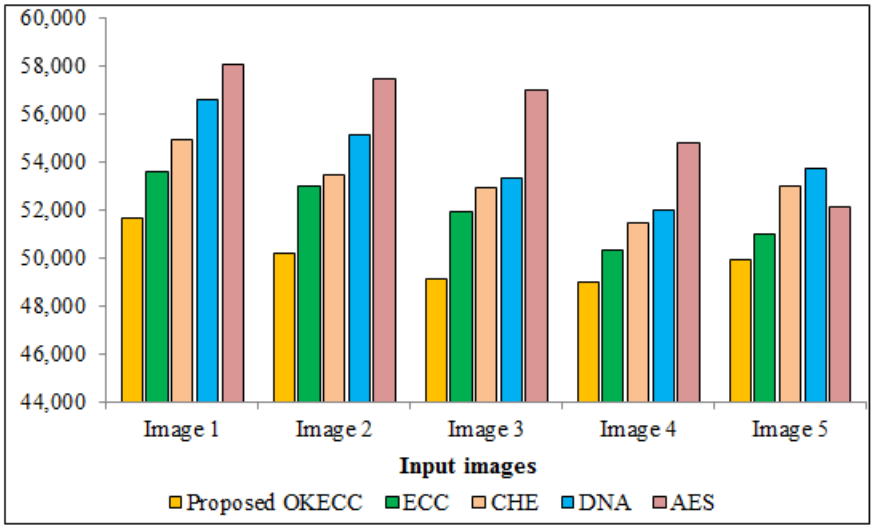

Figure 3:ET analysis

For image 1, the proposed one takes less time to encrypt the image of 51,643ms respectively, but the existing ECC, CHE, DNA, and AES take time to encrypt the image of 53,567ms, 54,897ms, 56,567ms, and 58,023ms, respectively. Similarly, for the remaining number of images, the proposed one takes less time to encrypt the image. From this assessment, it is appropriate that the proposed OKECC is more secure than the other systems. The proposed system is more secure with less time and low memory usage. Because the ECC algorithm is simple and secure, and the conventional ECC complex key generation is solved using the ISSO algorithm. Thus, it proves the security efficiency of the system.

5. CONCLUSION

This paper proposes a novel security approach called OKECC for securing biometric images in network transmission. It mainly comprises '2' phases: image compression and image encryption. The experimentation is done by using the FVC2004 DB-3 dataset. To investigate the proposed work's outcomes, the proposed MHE is first analyzed with the existing HE, AE, COTR, and BATR

in terms of compression ratio metrics for sample images 1 to 5. Herein, the proposed MHE has a higher average compression ratio of 83.23%, which is superior to the existing methods. Next, the performance of the proposed OKECC is investigated against the existing ECC, CHE, DNA, and AES in terms of MSE, PSNR, SSI, and encryption time. Here, the proposed one achieves higher PSNR with low MSE values for the sample images. The overall experimental results outlined that the proposed work provides high security, reliability, quick execution and higher efficiency than other encryption methods. In the future, the secrecy can be further improved by using advanced encryption and compression techniques.

REFERENCES

[1] Yang, W., Wang, S., Sahri, N. M., Karie, N. M., Ahmed, M., & Valli, C. (2021). Biometrics for internet-of-things security: A review. *Sensors*, *21*(18), 6163.

[2] Sadhukhan, D., Ray, S., Biswas, G. P., Khan, M. K., & Dasgupta, M. (2021). A lightweight remote user authentication scheme for IoT communication using elliptic curve cryptography. *The Journal of Supercomputing*, *77*, 1114-1151.

[3] Montasari, R., Jahankhani, H., Hill, R., & Parkinson, S. (Eds.). (2021). *Digital forensic investigation of Internet of Things (IoT) devices*. Springer.

[4] Moradi, M., Moradkhani, M., & Tavakoli, M. B. (2022). A real-time biometric encryption scheme based on fuzzy logic for IoT. *Journal of Sensors*, *2022*.

[5] Alsellami, B. M., & Deshmukh, P. D. (2021, March). The recent trends in biometric traits authentication based on internet of things (IoT). In *2021 international conference on artificial intelligence and smart systems (ICAIS)* (pp. 1359-1365). IEEE.

[6] El-Hameed, H. A. A., Ramadan, N., El-Shafai, W., Khalaf, A. A., Ahmed, H. E. H., Elkhamy, S. E., & El-Samie, F. E. A. (2021). Cancelable biometric security system based on advanced chaotic maps. *The Visual Computer*, 1-17.

[7] Roy, S., Rawat, U., Sareen, H. A., & Nayak, S. K. (2020). IECA: an efficient IoT friendly image encryption technique using programmable cellular automata. *Journal of Ambient Intelligence and Humanized Computing*, *11*, 5083-5102.

[8] Taher, B. H., Liu, H., Abedi, F., Lu, H., Yassin, A. A., & Mohammed, A. J. (2021). A secure and lightweight three-factor remote user authentication protocol for future IoT applications. *Journal of Sensors*, *2021*, 1-18.

[9] Gafsi, M., Abbassi, N., Hajjaji, M. A., Malek, J., & Mtibaa, A. (2020). Improved chaos-based cryptosystem for medical image encryption and decryption. *Scientific Programming*, *2020*, 1-22.

[10] El-Shafai, W., Khallaf, F., El-Rabaie, E. S. M., & El-Samie, F. E. A. (2022). Proposed 3D chaos-based medical image cryptosystem for secure cloud-IoMT eHealth communication services. *Journal of Ambient Intelligence and Humanized Computing*, 1-28.

[11] Siswanto, A., Katuk, N., & Ku-Mahamud, K. R. (2020). Chaotic-based encryption algorithm using henon and logistic maps for fingerprint template protection. *International Journal of Communication Networks and Information Security*, *12*(1), 1-9.

[12] Golec, M., Gill, S. S., Bahsoon, R., & Rana, O. (2020). BioSec: A biometric authentication framework for secure and private communication among edge devices in IoT and industry 4.0. *IEEE Consumer Electronics Magazine*, *11*(2), 51-56.

[13] Sujarani, R., Manivannan, D., Manikandan, R., & Vidhyacharan, B. (2021). Lightweight bio-chaos crypt to enhance the security of biometric images in internet of things applications. *Wireless Personal Communications*, *119*, 2517-2537.

[14] Nezhad, S. Y. D., Safdarian, N., & Zadeh, S. A. H. (2020). New method for fingerprint images encryption using DNA sequence and chaotic tent map. *Optik*, *224*, 165661.

[15] Hikal, N. A., & Eid, M. M. (2020). A new approach for palmprint image encryption based on hybrid chaotic maps. *Journal of King Saud University-Computer and Information Sciences*, *32*(7), 870-882.

[16] Altameem, A., Poonia, R. C., & Saudagar, A. K. J. (2023). A Hybrid AES with a Chaotic Map-Based Biometric Authentication Framework for IoT and Industry 4.0. *Systems*, *11*(1), 28.