A New Data Fusion Model for Medical Image Encryption in IoT Environment

Reem Atassi, Fuad Alhosban, Milan Dordevic

Higher Colleges of Technology, United Arab Emirates

Emails: ratassi@hct.ac.ae; falhosban@hct.ac.ae ; mdordevic@hct.ac.ae

Abstract

An improvement of the Internet of Things (IoT) was forecast for changing the healthcare industry and is generating the increase of the Internet of Medical Things (IoMT). The IoT revolution was surpassed the present-day human service with promise social prospects, mechanical, and financial. During this condition, it can be essential for framing an effectual approach for guaranteeing the safety and reliability of t patient's symptomatic information which are transmitted and received in IoT criteria. This study introduces a new data fusion model in IoT environment. The proposed model is called SSOECC-MIC model focuses on the design of effective encryption scheme with optimal key generation process for IoT environment. To achieve this, the SSOECC-MIC model designs an ECC model for the encryption and decryption of medical images effectively. To further improve the security performance of the ECC model, the optimal key generation process is carried out by the use of swallow swarm optimization (SSO) algorithm. For examining the enhanced performance of the SSOECC-MIC model, a wide ranging experimental analysis is carried out. The experimental outcomes reported the betterment of the SSOECC-MIC model over recent models.

Keywords: Security; Data Fusion; Internet of Things; Healthcare; Medical images; Encryption; Key generation

1. Introduction

Computerized medicinal images assume an undeniably significant part in the determination and therapy of sicknesses in current emergency clinics which is worked commonly with web of things biological system and along these lines draw in expanding consideration [1-3]. These medicinal images can for the most part contain a great deal of patient protection and some of them are exceptionally touchy as well as secret. Tragic mishaps can happen when unapproved get to ransack, view or utilize these private images. A vindictive data set executive or programmer, for instance, may use unapproved medicinal images for their own restitutions, for example, deceitful cases for protection and medicinal advertising, which may profoundly compromise endanger of life. It is in this way vital to safeguard medicinal images [4]. To get each sort of image, for instance, medicinal images, numerous innovations have been grown up until this point. Encryption is among these advances the most unconstrained and proficient method for changing images into unnoticed examples [5]. Just with the upholding right (secret) key, would the first image be able to be recuperated effectively. A few image encryptions plans have as of late been proposed which can be utilized to safeguard high-security medicinal images [6]. Fig. 1 showcase the process of information security.

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

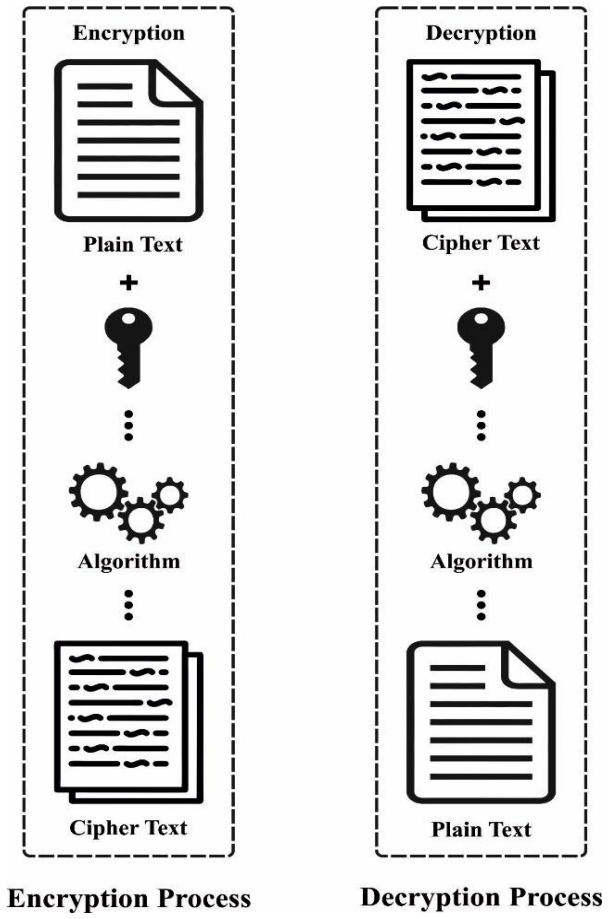

Fig.ure1: Process in Information Security

In addition, the Internet of Things (IoT) is additionally reached out in distributed computing for growing new offices and applications in the medicinal care process [7]. IoT is characterized as the organization of things or articles like sensors, programming, and electronic gadgets interconnected with one another for trading information with the administrator, producer, or other associated gadgets to achieve more noteworthy qualities and administrations. Additionally, IoT offers progressed network among the frameworks, administrations, and gadgets which incorporate different areas, conventions, and applications. IoT and distributed computing are benefitted similarly while consolidating the innovations. The IoT innovation generally upholds the cloud for improving the presentation like computational capacity, energy, stockpiling, and high asset use. Likewise, it inclines toward the cloud to offer many new types of assistance through a conveyed and dynamic methodology [8].

While putting away medicinal information in the cloud stage, it is important to defend the data with the goal that the cloud can't learn anything about the information. Hence, getting the medicinal images in cloud stage is vital. By and large, medicinal images are exceptionally delicate to changes, and accordingly, any modifications in their substance can cause mistakes in medicinal findings [9]. Subsequently, it is likewise critical to keep up with the touchy substance of medicinal images during a reproduction stage. Hence, an encryption calculation is expected for expanding the security and protection of information which gets the medicinal information without releasing any delicate data [10].

In [11], a watermarking method for patient identification and watermark integrity verifications. In order to combine methods, a DWT was executed for dividing the medicinal image as to 4 sub-bands. Lakshmi et al. [12] concentrated on DICOM image encryption was utilized a fuzzy chaotic map for encrypting and the DWT for watermarking. The authors in [13] mention a DICOM image encryption depends on chaotic attractor on frequency domain with integer wavelet transform (IWT) and fused with deoxyribonucleic acid (DNA) sequences on the spatial domain. The authors in [14] examine a new medicinal image watermarking approach with fuzzy based ROI chosen and wavelet transformation system for embedding encrypted watermark.

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

This study introduces a novel Swallow Swarm Optimization with Elliptic Curve Cryptography for Medical Image Encryption (SSOECC-MIC) model in IoT environment. The presented SSOECC-MIC model designs an ECC model for the encryption and decryption of medical images effectively. To further improve the security performance of the ECC model, the optimal key generation process is carried out by the use of swallow swarm optimization (SSO) algorithm. For examining the enhanced performance of the SSOECC-MIC model, a wide ranging experimental analysis is carried out.

2. Medical Image Encryption Technique

In this study, a new SSOECC-MIC model has been developed for effective encryption process with optimal key generation process for IoT environment. To achieve this, the SSOECC-MIC model designs an ECC model for the encryption and decryption of medical images effectively. To further improve the security performance of the ECC model, the optimal key generation process is carried out by the use of SSO algorithm.

2.1 Working of ECC Model

At the initial stage, the SSOECC-MIC model designs an ECC model for the encryption and decryption of medical images effectively. ECC is a public key cryptography model that is based on the arithmetical model of elliptic curve. The ECC chooses a prime number n_p and private key H. It can be provided as follows [15],

$$E = p(i)^3 + u * p(i) + v \tag{1}$$

Where u and v denotes constants. Next, X and Y can be denoted as follows.

$$X = mod(E, n_p) \tag{2}$$

$$Y = mod(p(j)^2, n_p) \tag{3}$$

The optimum points $P_e(k, l)$ and P_f represents public key as provided below [16]:

$$P_f = H * P_e \tag{4}$$

Data $D_x(i, j)$ and $D_y(i + 1, j)$ as well as the point is defined by

$$C_1 = H * P_e \tag{5}$$

$$C_2 = (D_x, D_y) + C_1 \tag{6}$$

To decrypt data, C_{11} is utilized as given below.

$$C_{11} = H * C_1 \tag{7}$$

$$C_{ij} = C_2 - C_{11} \tag{8}$$

$$F_{image} = R + G + B \tag{9}$$

2.2 SSO-basedased Optimal Key Generation Process

To further improve the security performance of the ECC model, the optimal key generation process is carried out by the use of SSO algorithm. SSO dependent upon the combined drive of swallow swarm and the communication amongst particles has obtained optimum outcomes for finding food. SSO has similarity with PSO as it signifies unique features containing utilize of 3 kinds of particles: the Explorer particle or Aimless particle and Leader particle. All the particles are responding to something that makes it guide the colony nearby to an optimum place. The (e_i) particle signifies the main part of colonies. Their responsibility was searching the optimum place from the problem spaces, this particle is play vital role as Head Leader (HL_i) when it can be the optimum place from the problem spaces, however when the Particle is in optimum place, not the optimum from the analogy with their neighboring particle, it can be chosen as local leader (LL_i).

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

The (o_i) particle is the particle that has worse place from the comparison with another particle of colony. Accordingly, its responsibility from the group was exploration and searching arbitrarily from the problem space then it has any connection with places of HL_i and LL_i. It can be easily moving and examining the condition of optimized. An essential update Eq. (10) for (o_i) is [17]:

$$0_{i+1} = 0_i + [rand(\{-1,1\}) * \frac{rand(\min_S, \max_S)}{1+rand()}] \quad (10)$$

In SSO approach, the particle categorizes as to 2 kinds: Local Leaders (LL) and Head Leader (HL). All the colonies are separated as sub-colonies. An optimum place from the sub-colony is chosen as local optimal point and named LL. But, the HL is an optimum place amongst the LL selected; it can be the global optimal point. The particle of colony modified its direction and moved based on the place of leader particles.

Important upgrade formulas in SSO follow:

$$e_{i+1} = e_i + V_{i+1} \quad (11)$$

$$V_{i+1} = V_{HL_{i+1}} + V_{LL_{i+1}} \quad (12)$$

$$V_{HL_{i+1}} = V_{HL_i} + \alpha_{HL} rand()(e_{best} - e_i) + \beta_{HL} rand0(HL_i - e_i) \quad (13)$$

$$V_{LL_{i+1}} = V_{LL_i} + \alpha_{LL} rand0(e_{besT} - e_i) + \beta_{LL} rand()(LL_i - e_i) \quad (14)$$

Whereas $\alpha_{HL}, \beta_{HL}, \alpha_{LL}$ and β_{LL} were the acceleration control co-efficient adaptably determined. V_{HL} = Velocity of HL, V_{LL} = Velocity of LL, e_{besT} =optimum position of the explorer particle, e_i =existing place of explorer particles [18]. Fig. 2 depicts the roles in SSO technique.

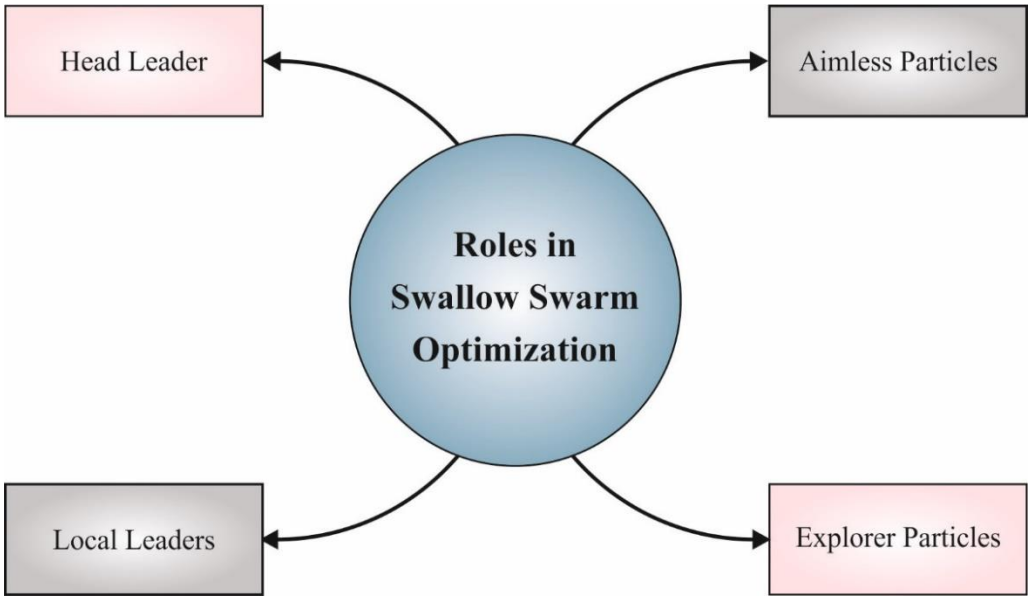

Figure 2: Roles in SSO technique

Algorithm 1: Swallow Swarm Optimization
Begin
Create arbitrarily population of n particle $(e_i, i = 1,2, \dots, n)$
$t = 1$
While ($t <$ max amount of iteration) do

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

for all the particles of swarms do

estimate fitness $f(e_i)$ of all p article

end for

Arrange objective function from min to max and procedure LL_i et 0_i

if$(f(e_i) > f(e_{best}))$ then

$$e_{besT} = e_i$$

end if

if$(f(e_i) > f(LL_i))$ then

$$LL_i = e_i$$

end if

if$(e_i = 0 || e_{best} = 0)$

$$\alpha_{LL} = \beta_{LL} = 2$$

else

determinate α_{LL} and β_{LL}

end if

upgrade velocity $V_{LL_{i+1}}$ [Eq. (6)]

if$(f(e_i) > f(HL_i))$

$$HL_i = e_i$$

end if

if$(e_i = 0 || e_{besT} = 0)$

$$\alpha_{HL} = \beta_{HL} = 1.5$$

else

define α_{HL} and β_{HL}

end if

upgrade velocity $V_{HL_{i+1}}$

upgrade position e_i and velocities V_i of particle and upgrade aimless particle 0_{i+1}

if$(f(0_i) > f(HL_i))$

$$HL_i = 0_i$$

end if

if$(f(LL_i) > f(HL_i))$

$$HL_i = LL_i$$

end if

$$t = t + 1$$

end while

returned optimum of HL

End

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

3. Experimental Validation

In this section, the experimental validation of the SSOECC-MIC model is tested using benchmark medical images, as shown in Fig. 3.

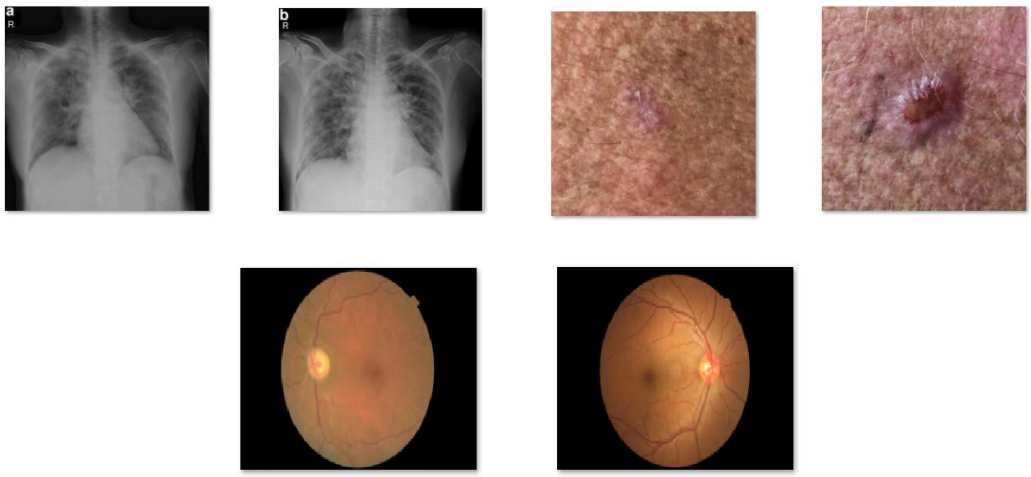

Figure 3: Sample medical images

Table 1 offers experimental outcomes of the SSOECC-MIC model on five distinct class labels. On image-1, the SSOECC-MIC model has offered MSE of 0.107, RMSE of 0.3271, PSNR of 57.84dB, and SSIM of 0.9998. At the same time, on image-3, the SSOECC-MIC system has obtainable MSE of 0.119, RMSE of 0.3450, PSNR of 57.38dB, and SSIM of 0.9995. Along with that, on image-6, the SSOECC-MIC approach has existing MSE of 0.144, RMSE of 0.3795, PSNR of 56.55dB, and SSIM of 0.9997.

Table 1 : Result analysis of SSOECC-MIC technique with distinct images and measures

No. of images	MSE	RMSE	PSNR	SSIM
Image-1	0.107	0.3271	57.84	0.9998
Image-2	0.097	0.3114	58.26	1.0000
Image-3	0.119	0.3450	57.38	0.9995
Image-4	0.144	0.3795	56.55	0.9998
Image-5	0.125	0.3536	57.16	0.9996
Image-6	0.144	0.3795	56.55	0.9997

Table 2: MSE analysis of SSOECC-MIC technique with existing approaches under distinct images

Mean Squared Error				
No. of images	**ECC**	**RSA**	**AES**	**SSOECC-MIC**
Image-1	0.418	0.393	0.306	0.107
Image-2	0.430	0.380	0.308	0.097
Image-3	0.486	0.421	0.319	0.119
Image-4	0.432	0.404	0.379	0.144
Image-5	0.478	0.415	0.307	0.125
Image-6	0.409	0.374	0.358	0.144

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

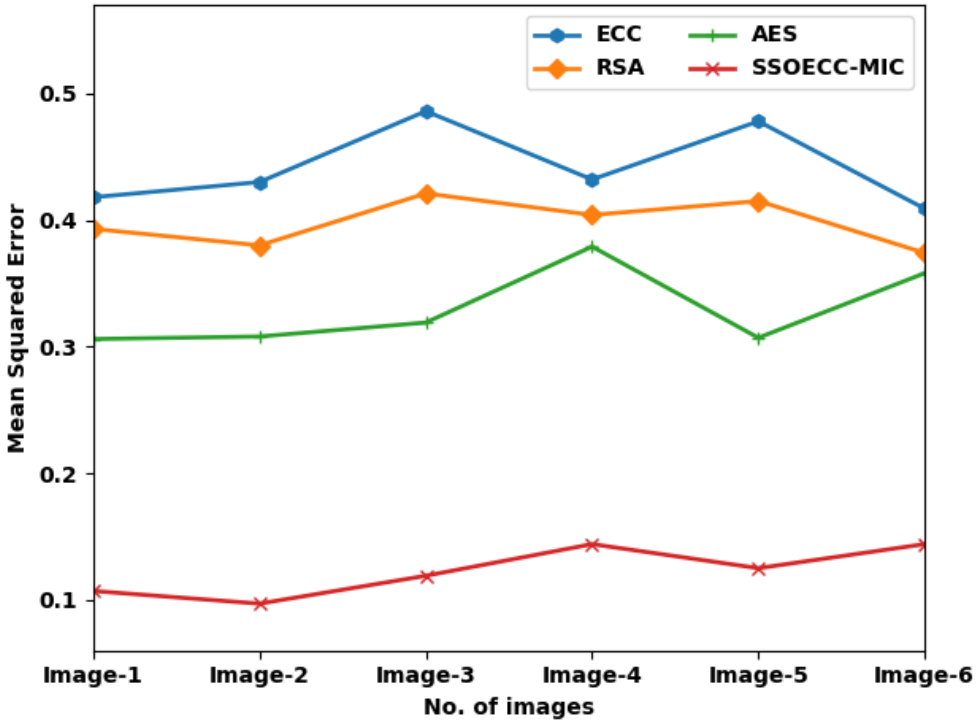

Figure 4: MSE analysis of SSOECC-MIC technique with distinct images

A detailed comparative MSE study of the SSOECC-MIC model with recent models is made in Table 2 and Fig. 4 [19]. The results implied that the SSOECC-MIC model has accomplished minimal values of MSE under every image. On image-1, the SSOECC-MIC model has offered decreased MSE of 0.107 while the ECC, RSA, and AES models have provided increased MSE of 0.418, 0.393, and 0.306 respectively. In addition, on image-3, the SSOECC-MIC approach has obtainable lower MSE of 0.119 while the ECC, RSA, and AES techniques have provided maximum MSE of 0.486, 0.421, and 0.319 respectively. At last, on image-6, the SSOECC-MIC approach has accessible decreased MSE of 0.144 while the ECC, RSA, and AES systems have provided increased MSE of 0.409, 0.374, and 0.358 correspondingly.

A detailed comparative RMSE study of the SSOECC-MIC methodology with recent models is made in Table 3 and Fig. 5. The results implied that the SSOECC-MIC model has accomplished minimal values of RMSE under every image. On image-1, the SSOECC-MIC model has offered decreased RMSE of 0.3271 while the ECC, RSA, and AES models have provided increased RMSE of 0.6465, 0.6269, and 0.5532 correspondingly. Followed by, on image-3, the SSOECC-MIC model has offered decreased RMSE of 0.3450 while the ECC, RSA, and AES models have provided higher RMSE of 0.6971, 0.6488, and 0.5648 respectively. Finally, on image-6, the SSOECC-MIC technique has offered decreased RMSE of 0.3795 while the ECC, RSA, and AES approaches have provided increased RMSE of 0.6395, 0.6116, and 0.5983 correspondingly.

Table 4 and Fig. 6 portray a brief PSNR inspection of the SSOECC-MIC model with recent models. The experimental outcome indicated that the SSOECC-MIC model has gained maximum values of PSNR. For instance, with image-1, the SSOECC-MIC model has depicted enhanced PSNR of 57.84dB whereas the ECC, RSA, and AES models have exhibited reduced PSNR of 51.92dB, 52.19dB, and 53.27dB respectively. Moreover, with image-6, the SSOECC-MIC approach has portrayed enhanced PSNR of 56.55dB whereas the ECC, RSA, and AES models have exhibited reduced PSNR of 52.01dB, 52.40dB, and 52.59dB correspondingly.

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

Table 3: RMSE analysis of SSOECC-MIC technique with existing approaches under distinct images

Root Mean Square Error				
No. of images	**ECC**	**RSA**	**AES**	**SSOECC-MIC**
Image-1	0.6465	0.6269	0.5532	0.3271
Image-2	0.6557	0.6164	0.5550	0.3114
Image-3	0.6971	0.6488	0.5648	0.3450
Image-4	0.6573	0.6356	0.6156	0.3795
Image-5	0.6914	0.6442	0.5541	0.3536
Image-6	0.6395	0.6116	0.5983	0.3795

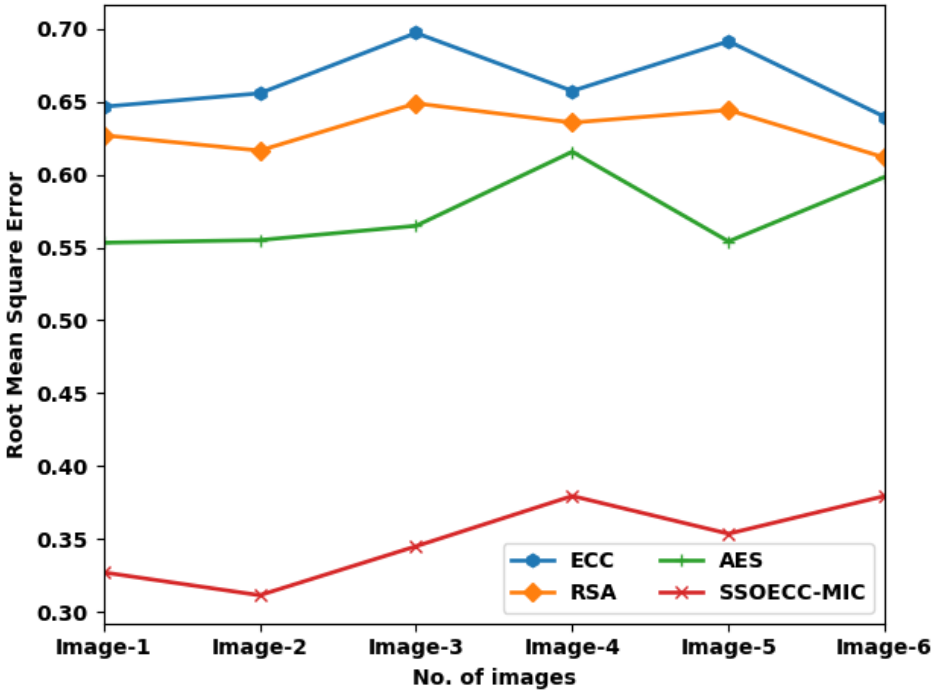

Figure 5: RMSE analysis of SSOECC-MIC technique with distinct images

Table 4: PSNR analysis of SSOECC-MIC technique with existing methods under distinct images

Peak Signal Noise Ratio (dB)				
No. of images	**ECC**	**RSA**	**AES**	**SSOECC-MIC**
Image-1	51.92	52.19	53.27	57.84
Image-2	51.80	52.33	53.25	58.26
Image-3	51.26	51.89	53.09	57.38
Image-4	51.78	52.07	52.34	56.55
Image-5	51.34	51.95	53.26	57.16
Image-6	52.01	52.40	52.59	56.55

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

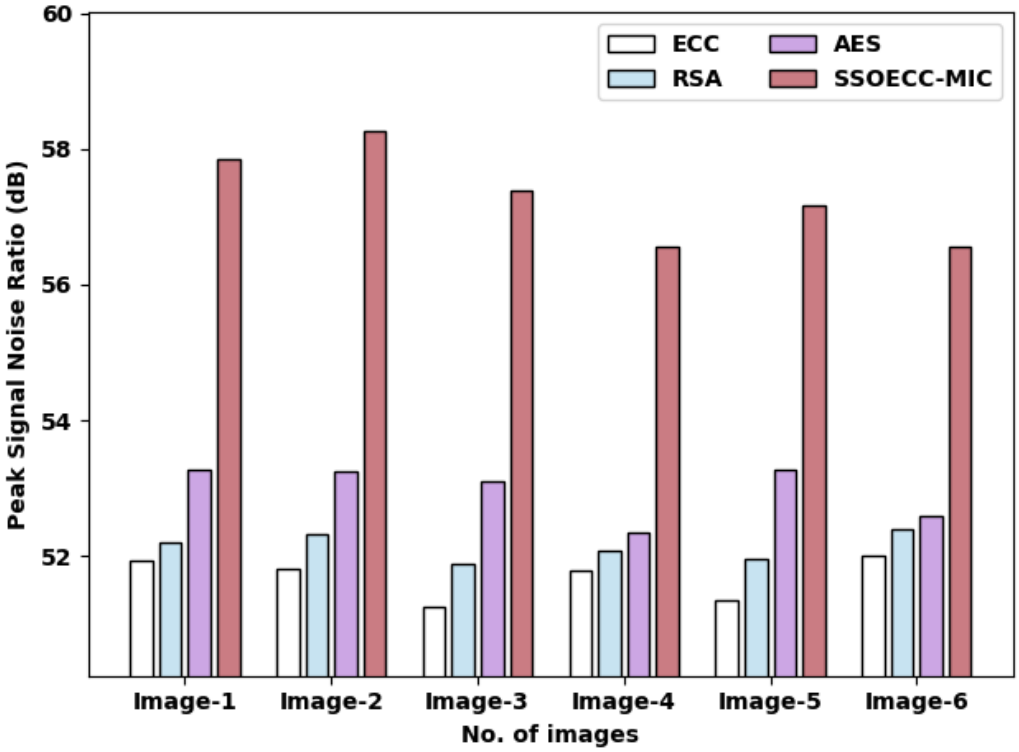

Figure 6: PSNR analysis of SSOECC-MIC technique under distinct images

Table 5: SSIM analysis of SSOECC-MIC technique with existing work under distinct images

Structural Similarity Index Measure				
No. of images	**ECC**	**RSA**	**AES**	**SSOECC-MIC**
Image-1	0.9754	0.9762	0.9929	0.9998
Image-2	0.9767	0.9789	0.9807	1.0000
Image-3	0.9753	0.9762	0.9867	0.9995
Image-4	0.9737	0.9800	0.9878	0.9998
Image-5	0.9774	0.9845	0.9934	0.9996
Image-6	0.9718	0.9783	0.9854	0.9997

Table 5 and Fig. 7 depicts a brief SSIM examination of the SSOECC-MIC approach with recent models. The experimental outcome indicated that the SSOECC-MIC model has gained maximal values of SSIM. For instance, with image-1, the SSOECC-MIC model has depicted enhanced SSIM of 0.9998 whereas the ECC, RSA, and AES models have exhibited reduced SSIM of 0.9754, 0.9762, and 0.9929 respectively. Furthermore, with image-6, the SSOECC-MIC system has depicted enhanced SSIM of 0.9997 whereas the ECC, RSA, and AES models have demonstrated reduced SSIM of 0.9718, 0.9783, and 0.9854 correspondingly.

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

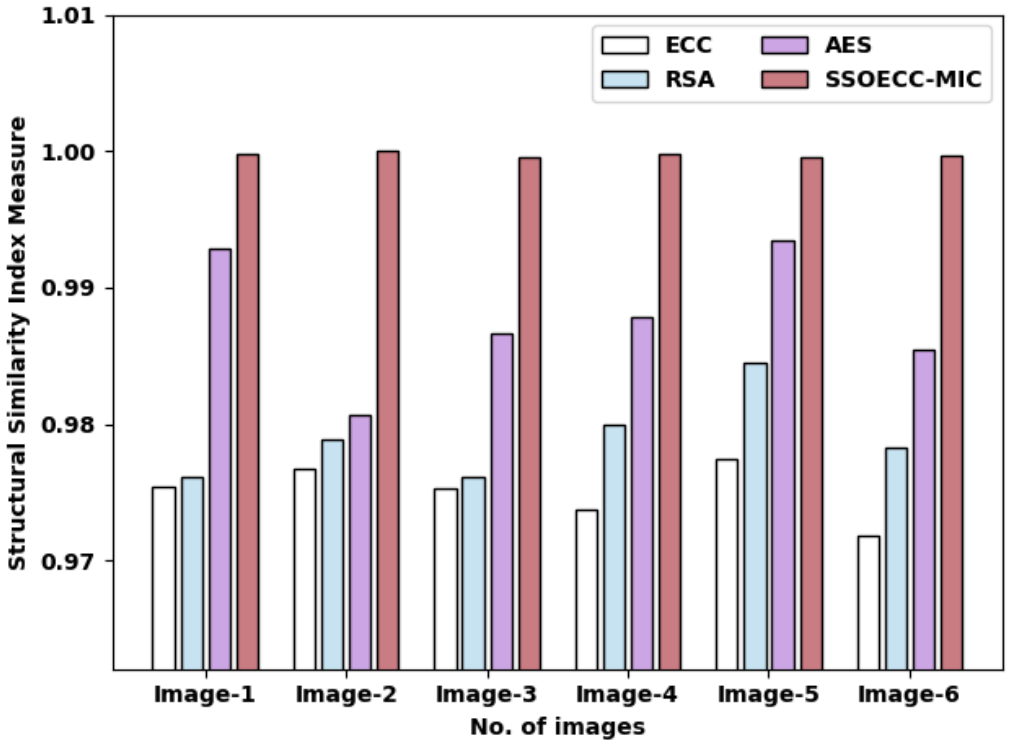

Figure 7: SSIM analysis of SSOECC-MIC technique with distinct images

These results and discussion inferred the enhanced security outcomes of the SSOECC-MIC model over the other models.

4. Conclusion

In this study, a new SSOECC-MIC model has been developed for effective encryption process with optimal key generation process for IoT environment. To achieve this, the SSOECC-MIC model designs an ECC model for the encryption and decryption of medical images effectively. To further improve the security performance of the ECC model, the optimal key generation process is carried out by the use of SSO algorithm. For examining the enhanced performance of the SSOECC-MIC model, a wide ranging experimental analysis is carried out. The experimental outcomes reported the betterment of the SSOECC-MIC model over recent models. Therefore, it can be exploited as an effectual tool for ensuring medical image security. In future, hybrid metaheuristic algorithms can be utilized for optimally choosing the keys.

References

[1] Avudaiappan, T., Balasubramanian, R., Pandiyan, S.S., Saravanan, M., Lakshmanaprabu, S.K. and Shankar, K., 2018. Medical image security using dual encryption with oppositional based optimization algorithm. Journal of medical systems, 42(11), pp.1-11.

[2] Hasan, M.K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.H.A., Habib, S., Islam, M., Alyahya, S., Ahmed, M.M., Kamil, S. and Hassan, M.A., 2021. Lightweight encryption technique to enhance medical image security on internet of medical things applications. IEEE Access, 9, pp.47731-47742.

[3] Akkasaligar, P.T. and Biradar, S., 2020. Selective medical image encryption using DNA cryptography. Information Security Journal: A Global Perspective, 29(2), pp.91-101.

[4] Zhang, B., Rahmatullah, B., Wang, S.L., Zaidan, A.A., Zaidan, B.B. and Liu, P., 2020. A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations. Multimedia Tools and Applications, pp.1-40.

[5] El-Shafai, W., Khallaf, F., El-Rabaie, E.S.M. and El-Samie, F.E.A., 2021. Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. Journal of Ambient Intelligence and Humanized Computing, 12(10), pp.9007-9035.

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022

[6] Tan, Y., Qin, J., Tan, L., Tang, H. and Xiang, X., 2018, June. A survey on the new development of medical image security algorithms. In International Conference on Cloud Computing and Security (pp. 458-467). Springer, Cham.
[7] Balasamy, K. and Suganyadevi, S., 2021. A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. Multimedia Tools and Applications, 80(5), pp.7167-7186.
[8] Abdulbaqi, A.S., Obaid, A.J. and Mohammed, A.H., 2021. ECG signals recruitment to implement a new technique for medical image encryption. Journal of Discrete Mathematical Sciences and Cryptography, 24(6), pp.1663-1673.
[9] Mishra, Z. and Acharya, B., 2020. High throughput and low area architectures of secure IoT algorithm for medical image encryption. Journal of Information Security and Applications, 53, p.102533.
[10] Belazi, A., Talha, M., Kharbech, S. and Xiang, W., 2019. Novel medical image encryption scheme based on chaos and DNA encoding. IEEE access, 7, pp.36667-36681.
[11] Sayah, M.M., Redouane, K. and Amine, K., 2022. A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocessors and Microsystems, p.104490.
[12] Lakshmi, C., Thenmozhi, K., Rayappan, J.B.B. and Amirtharajan, R., 2018. Encryption and watermark-treated medical image against hacking disease—An immune convention in spatial and frequency domains. Computer Methods and Programs in Biomedicine, 159, pp.11-21.
[13] Banu S, A. and Amirtharajan, R., 2020. A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Medical & Biological Engineering & Computing, 58(7), pp.1445-1458.
[14] Balasamy, K. and Suganyadevi, S., 2021. A fuzzy based ROI selection for encryption and watermarking in medical image using DWT and SVD. Multimedia Tools and Applications, 80(5), pp.7167-7186.
[15] Hafsa, A., Sghaier, A., Malek, J. and Machhout, M., 2021. Image encryption method based on improved ECC and modified AES algorithm. Multimedia Tools and Applications, 80(13), pp.19769-19801.
[16] Rasina Begum, B. and Chitra, P., 2021. ECC-CRT: An Elliptical Curve Cryptographic Encryption and Chinese Remainder Theorem based Deduplication in Cloud. Wireless Personal Communications, 116(3), pp.1683-1702.
[17] Slezkin, A.O., Hodashinsky, I.A. and Shelupanov, A.A., 2021. Binarization of the Swallow Swarm Optimization for Feature Selection. Programming and Computer Software, 47(5), pp.374-388.
[18] Poongodi, K. and Kumar, D., 2021. Mining serial positioning episode rules by natural exponent inertia weight based swallow swarm optimization algorithm with constraint based event sequences. Journal of Intelligent & Fuzzy Systems, 40(3), pp.4599-4615.
[19] Elhoseny, M., Shankar, K., Lakshmanaprabu, S.K., Maseleno, A. and Arunkumar, N., 2020. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural computing and applications, 32(15), pp.10979-10993.

Doi : https://doi.org/10.54216/FPA.080102
Received: March 12, 2022 Accepted: August 10, 2022