ITC 2/52
Information Technology and Control
Vol. 52 / No. 2 / 2023
pp. 276-287
DOI 10.5755/j01.itc.52.2.32532

Security in Medical Image Management Using Ant Colony Optimization

Received 2022/10/17 | Accepted after revision 2022/12/21

HOW TO CITE: Karthikeyini, S., Sagayaraj, R., Rajkumar, N., Pillai, P. K. (2023). Security in Medical Image Management using Ant Colony Optimization. *Information Technology and Control*, 52(2), 276-287. https://doi.org/10.5755/j01.itc.52.2.32532

Security in Medical Image Management Using Ant Colony Optimization

S. Karthikeyini
Department of Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, 641008, Tamilnadu, India

R. Sagayaraj
Department of Electrical & Electronics Engineering, Muthayammal Engineering College (Autonomous), Rasipuram, Namakkal, Tamilnadu, India

N. Rajkumar
Department of Computer Science and Engineering, Faculty of Engineering and Technology, JAIN (Deemed to be University), Banglore, 560069, Karnataka, India

Punitha Kumaresa Pillai
Department of Electrical and Electronics Engineering, PSR Engineering College (Autonomous) Sivakasi, 626140, Tamilnadu, India

Corresponding author: skarthikeyinires1@outlook.com

Data encryption before transmission is still a crucial step in lowering security concerns in cloud-based environments. Steganography and image encryption methods validate the security of confidential data while it is being transmitted over the Internet. The paper presents the Ant Colony Optimization with Encryption Curve cryptography-based steganography technique to enhance the security of medical image management (ACO-ECC-SMIM). The initial stage is to create the stego images for the used cover image, the ACO algorithm-based image steganography technique is used. The creation of the encryption process is a key focus of the suggested ACO-ECC-SMIM strategy. The encryption process is initially carried out using an ECC technique, or elliptic curve cryptography. To maximize PSNR, the ACO technique is employed to optimize the crucial production process in the ECC model. The host image is subjected to an integer wavelet transform, and the coefficients have been altered. To determine the ideal coefficients where to conceal the data, the ACO optimization technique is utilized. The decryption and sharing reconstruction procedures are then carried out on the receiver side to create the original images. In Image 1, the ACO-ECC-SMIM model showed an improved peak signal-to-noise ratio (PSNR) of 59.37 dB. Due to the

ECC-ACO-SMIM model, Image 5 has an improved PSNR of 59.53dB. A large-scale experimental investigation was conducted to show the improved performance of the proposed PIOE-SMIM method, and the findings demonstrated the superiority of the ACO-ECC-SMIM model over other approaches.

KEYWORDS: Ant colony optimization, Elliptic curve cryptography, steganography, encryption, integer wavelet transform.

1. Introduction

In recent years, most healthcare facilities have adopted an electronic format for their patient record systems [36, 37]. Most leading industries, such as the interplay of commercial news and details about military operations, will preserve the photographs with the utmost confidentiality. Massive image-preserving methods, including data encryption, steganography, and alternative models, are suggested to increase the privacy of sensitive photographs. By hiding sensitive information behind a cover image that seems identical, an adversary will have more trouble determining whether or not the data has been transferred. It demonstrates the significance of transmitting secret information under various cover images.

The use of cryptographic techniques helps ensure secrecy and security by lowering the likelihood that an adversary may intervene. Encryption and the act of managing keys are the two processes involved in cryptography. Every security system ought to provide some security procedure that can reliably maintain the system's confidentiality [30]. Symmetric and asymmetric keys are the two main subcategories of cryptography [31]. In the case of symmetric key cryptography, a single key serves both the purpose of encrypting and decrypting data [25, 26, 27]. Asymmetric Key Cryptography makes use of distinct keys for each of the processes [29].

The art and science of steganography is the ability for two parties to communicate secretly across a standard media without the spectator being able to read what is said. Cryptography, the art and science of secret data communication, are related to steganography. Steganography conceals the existence of covert communication, while cryptography only tries to obscure the substance of the message. However, notice is investigating that contact through a local server or an ISP. Steganography offers a scenario in which transmitter A delivers a message M to recipient B to safeguard this communication. The transmitter received stego object S, embedded it over cover media C, and sent it over an unsecured channel. The phrases "cover object" and "stego object" is used to describe different multimedia items that are employed to conceal data, respectively [1].

Effective steganography properties:

1. Secrecy: By permitting intended users to recover the concealed information [9, 16, 17, 20, 26]
2. Imperceptions: The capacity to be entirely undetectable [10-11]
3. Imperceptions: The capacity to be entirely undetectable [11]
4. Capacity: The most extended hidden information can be inserted into a cover item.
5. Accuracy: The integrated data should be accurately extracted

The unique feature of the approach is that it generates the key stream for encryption using an Ant Colony Optimization technique. This process is done based on the distribution of characters in the plain text identifying the image. It enables the locks in the key stream to be encoded using a mutated character code table to increase system security.

Consequently, the safety of electronic health data/images has received much interest recently, especially when these images are exchanged through networks. An image encryption technique aims to change an original idea into an obscure one. Most security measures in healthcare digital image technologies are based on well-known encryption algorithms, including AES, DES, RSA, and IDEA [35]. In real-time remote monitoring of patients, internet sources create huge electronic medical images to be transferred increasingly frequently over the public network. It is desirable to develop an efficient healthcare image encryption technique. Magnetic resonance imaging (MRI and tomography are only two examples of the numerous applications of digital images in healthcare diagnostics. Multiple approaches are used with electronic images, such

as sound recognition, watermarking, segmentation techniques, feature extraction, noise removal, and image compression [5, 6]. The most important part of health information for analysis and research purposes is likely medical images. These images are frequently shared and distributed between research organizations and hospitals worldwide via mobile phones and the Internet. These days, medical imaging analysis and storage are cloud-based. Finally, stored data is analyzed in a remote location. Since the patient's data is confidential, it cannot be public. To confer with specialists, doctors send patient information via an image to the general community. Thus, while communicating ideas over the Internet network infrastructure, security is essential.

The suggested solution uses the Ant Colony Optimization Algorithm [19], which operates on the same principles. Applying the ACO method will allow you to embed the secret raw data's ASCII values at the best coefficients. Following embedding all private values, the inverse IWT is turned into the stego object and is then prepared for transmission to the recipient. The recipient can retrieve its secret information by receiving it and using the embedding method in reverse.

The technique developed in this study, called ACO-ECC-SMIM Ant Colony Optimization with Encryption Curve cryptography-based steganography technique (security enhancement of medical image), uses encryption. The encryption processes are designed with the proposed ACO-ECC-SMIM approach in mind. The encryption procedure uses an elliptic curve cryptography (ECC) technique. The ACO algorithm is used to create the best possible keys for the ECC model, with the increasing goal of peak signal-to-noise ratio (PSNR). The reconstruction procedures with decryption are done to create the original image data on the receiver side. A thorough simulation analysis is conducted to show the ACO-ECC-SMIM model to have improved performance.

The contributions of the study are listed below in brief: (i) introducing a new ACO ECC-SMIM architecture for the healthcare industry with secured image management; (II) transferring the medical images safely by ECC encryption model; (III) creating an ACO algorithm that will best produce the keys for more secure transfer of medical images; (IV) comparing the suggested model performance to a benchmark dataset and analyzing the outcomes regarding various metrics.

2. Review of Literature

An asymmetric encryption program has been introduced by Shaktawat et al. [31] to encrypt color pathological images under the Dadras difficult hyperactive chaotic system. The program is based on the encryption phase and decryption phases. To generate the initial challenges for the chaotic device, 512 bits of the basic image are subject to the protected hash algorithm (SHA). The system appears to have a critical size that is sufficiently large to defend against the brute force attack, and it also seems to have received a significant deal of sensitivity to the key that is being used.

Seyyedi et al., [27] suggested a secure, high-volume payload steganography technique in their paper that was based on the integer wavelet transform. Reduce distortion while providing a high embedding capacity by combining the Genetic Algorithm (GA), OPAP, and Integer Wavelet Transforms, according to Ghasemi et al. [8].

Sreelaja and Vijayalakshmi Pai [33] came up with the idea for an approach to text encryption that was based on swarm intelligence. In this method, an Ant Colony Optimization Key Generation Algorithm, also known as an AKGA, is utilized to produce the encryption keys for the content that is being protected. Text, unlike binary graphics, can comprise any combination of the universe's potential characters. As a result, the critical stream comprised a 94 characters maximum with a code table for characters.

Ching-Sheng Hsu and colleagues [18] have developed a method to calculate the best possible LSB substitution using the ACO method. This algorithm will incorporate the data into the cover image's final bytes. In addition, the ACO method should be used to construct the optimal matrix to hide the data at the optimal values. A chaos-based picture encryption system was proposed within stream cipher architecture. In the first step of this method, an image is transformed into a stream of binary data. The encrypted image, similar to the input image, is produced by data masking techniques with keystream random, formed by a chaos Pseudorandom Key Generator (PRKG). The PRKG is controlled by a pair of the logistic map, and their behavior is determined by the values of ((1), 0), and (2), as well as y0. These values are kept under wraps, and the cipher key can be derived from them.

Using chaotic encryption and parallel computing, Bhattacharyya [4] suggested a fast and real-time

cryptosystem. The "permutation-substitution" structure of a chaotic encryption system is the concept's foundation. The desired level of diffusion is ensured throughout the entire image collection process. The phase of substitution by encryption is carried out over adjacent images using an expanded Cipher-Blockchain (CBC) model. The batch image is divided into different groups during the permutation stage. Then, multi-threading simultaneously generates permutation coordinates in every group to save time. From these, multiple images are rotated simultaneously.

The optimization technique was utilized by Shubo [33] to conceal the hidden message within the target picture. The optimization was carried out using the PSO algorithm, which produced superior results to the traditional GA-based method. The technique proposed by H. Nematzadeh et al. [21] can select an ideal image block, which may be the most effective location for data hiding. The fitness function that needs to be considered is one in which the ratio maximizes the sum of contrast, energy, entropy, and homogeneity. The findings demonstrate that this algorithm performs better than the PSO method.

The plaintext medical image will initially deal with the 4D hyperchaotic sequence picture. This will involve the generation of pseudorandom sequences, the segmentation of images, and the processing of chaotic systems. In the paper [2], the scientists encoded medicinal images using a V-net at the convolution neural networks (CNNs) model that relies on the 4D hyperchaotic technique. After that, the V-net with CNN model is applied to chaotic sequences for training and to eliminate the periodicity present in chaotic sequences. In the end, the picture of the chaotic sequence goes through diffusion, which alters the actual image pixels and completes the encryption procedure. Paper [3] presents a concept for a hybrid that combines the modified coupled map lattices medical picture encryption approach and genetic algorithm (MGA).

The references [15] and [22] present several methods for encrypting medical images.

It was recommended by Rarhi et al [24] that the picture encryption be carried out with the help of the Blowfish Algorithm because it possesses superior execution and delivery time. The images were hidden using the Least Significant Bit (LSB) approach [12], which was applied by the method. A hybrid strategy, which uses a mixture of picture encryption, image encryption + image concealing, is still recommended for providing a substantial level of protection. To estimate the dynamics, PSNR and MSE have been utilized. Hasan et al. [13] provided an effective and lightweight encryption technique to develop a secure picture coding strategy for the medical sector. The solution that is being given makes use of two permutation strategies to secure medical photos. Parthasarathi et al. [23] descript the key-based cryptography technique to share healthcare records among hospital people in a secure manner. Marco et al. [14] offer a lightweight cryptosystem using Chen's chaotic, Henson's chaotic, and Brownian motion techniques to encrypt healthcare images while maintaining high safety. The experiment results indicate that the proposed model is an efficient method that has the potential to achieve the desired level of security to encrypt image-based patient datasets.

3. Proposed Methodology

During the transmission of images in the network securely, this paper proposed ECC-ACO-SMIM. The encryption process is initially carried out using an ECC technique, or elliptic curve cryptography. To maximize the peak signal-to-noise ratio (PSNR), the ACO technique is employed to generate the key in the process of the ECC model. The host image is subjected to an integer wavelet transform, and the coefficients have been altered. The proposed work is given in Figure 1.

Figure 1
Workflow of ECC-ACO-SMIM work

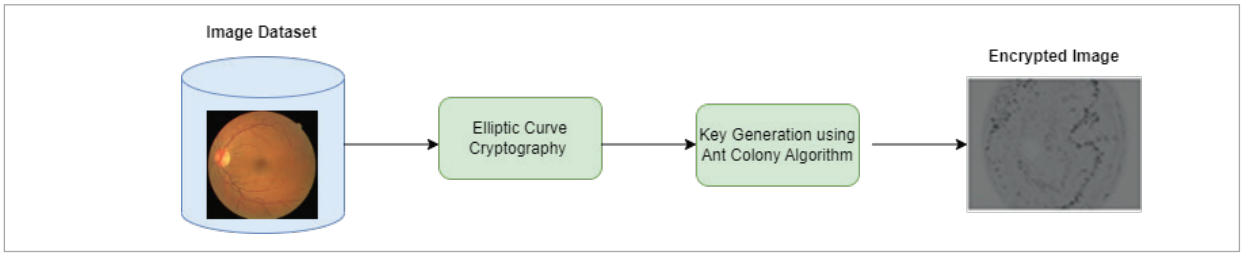


Figure 1 describes the two levels of processing. They are implementing Elliptic curve cryptography (ECC) to secure the image's transmission. The key is generated by implementing an ant colony optimization algorithm.

3.1. ECC-Based Encryption

The Elliptic Curve Cryptography (ECC) technique is a form of public-key cryptography that is based on the algebraic construction of elliptical curves that pass over finite fields. It utilizes non-EC cryptography and comes with a tiny key to provide an equivalent level of safety. At the ECC, the np value for the prime parameter is selected, and the H value for the private key is favored [18]. After that, it can be stated as the following in Equation (1).

$$E = p(i)^3 + x * p(i) + y, \quad (1)$$

where x and y signify the constant value x = y = 2, and where x and y are variables. After ensuring that the condition P = Q has been met, the ECC will select the optimal points for the calculation. After that, we find out what P and Q are in Equations (2)-(3).

$$P = \mathrm{mod}(E, n_p), \quad (2)$$

$$Q = mod(p(j)^2, n_p). \quad (3)$$

Now, the point on the elliptic curve is denoted by the expression p(i, j). n_p is the description of an image. The doubling method is utilized for determining the values of P and Q. The optimum point of the public key is represented by X_e(k, l) and $X_f$in Equation (8):

$$X_f = H * X_e. \quad (4)$$

During the encryption process, each share is represented by a block, and each block in turn is represented by an encrypted part. The total blocks are denoted by the expression k(i, j), where I and j indicate the row and column of the blocks, respectively. All the information's components are now being sent over as input for the data encryption process. The following is a description of how the point, along with the data C_x(i, j), and C_y(i + 1, j), can be represented [34]:

$$D_1 = H * X_e \quad (5)$$

$$D_2 = (C_x, C_y) + D_1. \quad (6)$$

In decryption, the private key (H) is used to decrypt the transmission, and point D_{11} is utilized to solve the pixels. Both of these steps are part of the technique.

$$\begin{aligned} D_{11} &= H * D_1 \\ D_{ij} &= D_2 - D_{11}. \end{aligned} \quad (7)$$

The decryption process has been completed, and the final output may be seen in C_{ij}. Using the results of D_{ij}, color bands (RGB) with pixel values and infrared light are preserved in a distinct manner. In the end, it can be summed up as follows in Equation (12).

$$E_{img} = R + G + B. \quad (8)$$

3.2. Key Generation Using Ant Colony Optimization

The ACO technique is employed to generate the key in the process of the ECC model. The host image is subjected to an integer wavelet transform, and the coefficients have been altered. To provide optimized security of data in the image by applying ACO. To determine the ideal coefficients where to conceal the data, the ACO optimization technique is utilized. In this paper, the ACO-based technique has been used to detect the complex region of the image. To detect the complex region of the image securely, LSB steganography is applied [7]. ACO generates the pheromone matrix and employs the many ants in the medical image. The movements of the ant are implemented by computing the intensity value of pixels in the medical image. The entries in the pheromone matrix contain the pixel value of the cover image. Figure 2 shows the sender and receiver of applying ECC-ACO-SMIM.

Pseudocode for ACO:

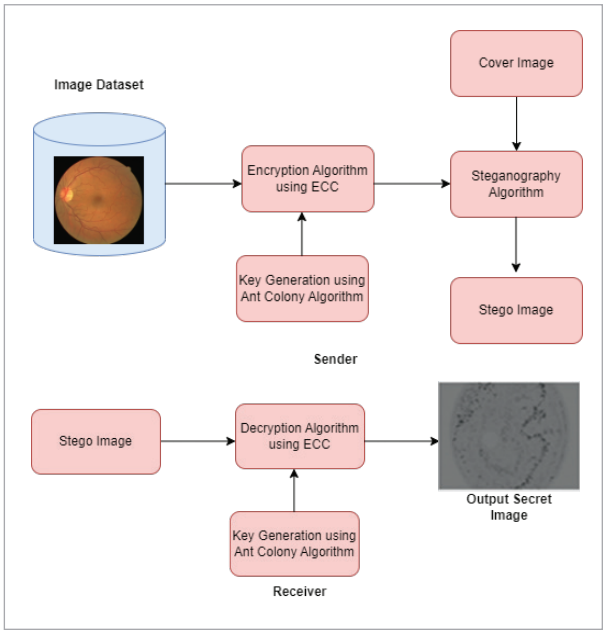
1. Begin
   Initialize
2. While the stopping criterion is not satisfied, do
   Position all ants at starting node
   Repeat
3. For each ant t do
   - Compute heuristic information n State
   - Transition rule is applied for choosing the next node

• Each ant built solution by computing fitness value

end for

4. Update the best solution// trial update
5. In iteration, global best and move is Identified
6. Print the best result and terminate the condition

Figure 2
Sender & Receiver of Applying ECC-ACO-SMIM



The Ant Colony optimization Key Generation algorithm is based on encrypting the input image using ECC into binary Image encryption format. To obtain the key stream for binary image encryption by applying the probability of occurrence of characters of the key stream in the plain text representing the encoded binary image is greater than or equal to the threshold value 0.80.

The optimal solution is obtained by coordination with one another. The pheromones are left on the paths traveled by the ants and serve as communication between the remaining other ants.

By computing the energy value, each ant agent generates the solution by depositing a pheromone. The deposition of the pheromone of each ant agent is represented as a key stream. Compute the ant agent's energy value based on its pheromone deposition. The threshold value of 0.80 is implemented to get the optimal solution. Since at least 80% of the character in the key stream denotes the deposition of the pheromone of the ant agent. Figure 3 shows the workflow of getting a key stream using ACO.

Figure 3
Keystream Generation

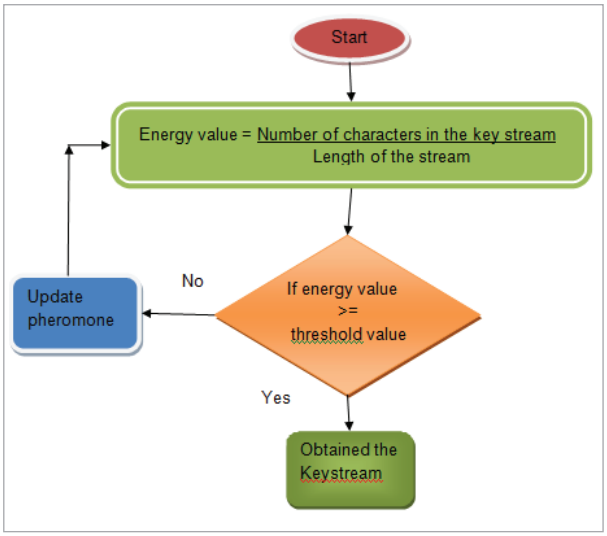


Figure 3 describes that to improve the security of the system, encoding the key stream characters using a character code table. Compute the energy value by counting the occurrence of characters in the key stream and dividing it by the length of the key stream. When the ant agent's energy value is equal to or exceeds its threshold value of 0.80, then the pheromone deposition of the corresponding ant agent is selected as the key stream for encryption.

4. Experimental Results and Discussions

The datasets for diabetic retinopathy, or DR, are used to test the experimental validity of the ACO-ECC-SMIM model.

The PSNR, CC, and MSE are calculated using Equations (9)-(11).

$$PSNR = 20 * \log_{10}\left(\frac{255^2}{\sqrt{MSE}}\right) dB \quad (9)$$

$$MSE = \frac{1}{MN}\sum_{j=1}^{M}\left(I(i,j) - I^{'}(i,j)\right)^{2} \quad (10)$$

$$CC = \frac{n\left(\sum xy\right) - \left(\sum x\right)\left(\sum y\right)}{\sqrt{\left[\sum x^{2} - \left(\sum x\right)^{2}\right]\left[n\sum y^{2} - \left(\sum y\right)^{2}\right]}} \quad (11)$$

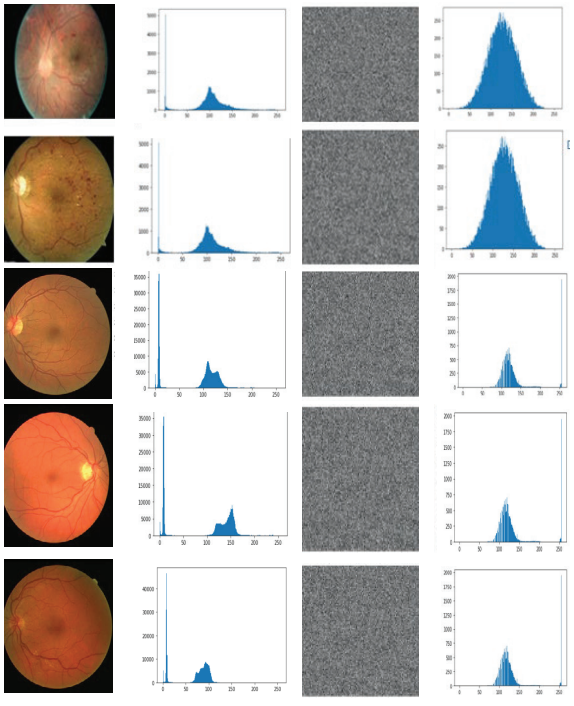
4.1. Uniform Histogram

The histograms of the images produced by the suggested cryptosystem are uniformly distributed. Equation (19) provides the image's histogram H (ri).

$$H(r_{\mathrm{l}}) = n_{i}, \quad (12)$$

where r_i represents an intensity value ith and the number of pixels is defined as n_i in the image with an intensity value equal to r_i

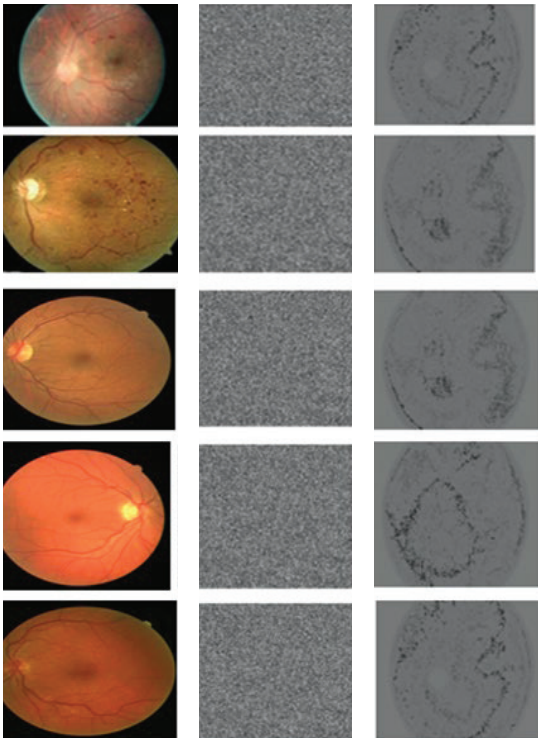
Figure 4



(a) Original DR Image | (b) Original image histogram | (c) Image encryption | (d) Encrypted histogram image

Figure 5

Examining the result of the ACO-ECC-SMIM model under distinct images of tests



(a) Original image | (b) Encrypted image | (c) After ECC

4.2. Correlation Coefficient and PSNR

A measurement of the degree to which individual pixels in an image repeat themselves is provided by the correlation coefficient (CC). The simple image has a high redundancy value, but the encrypted image should have an extremely low CC value. For the correlation coefficient, refer the Equation (17). Figure 6 provides a detailed examination of the ACO-ECC-SMIM method under specific image tests.

Table 1 presents an overview of a preliminary PSNR assessment of the ACO-ECC-SMIM model under the conditions of a specific selection of test images. According to Table 1, the ACO-ECC-SMIM model has produced higher values of PSNR as a consequence of its application. For example, the PIOE-SMIM model determined that the PSNR for Image 1 should be

Figure 6
PSNR analysis

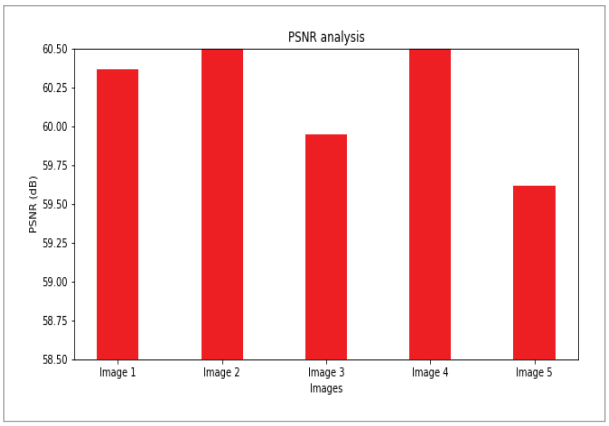


Table 1
PSNR assessment of the ACO-ECC-SMIM model under the conditions of a specific selection of test images

Test images	MSE	PSNR	CC	SSIM
Image 1	0.0761	60.37	99.96	99.91
Image 2	0.0693	60.59	99.92	99.91
Image 3	0.0892	59.95	99.98	99.90
Image 4	0.0690	61.58	99.92	99.94
Image 5	0.0795	59.62	99.97	99.91

60.37 decibels. In addition, the ACO-ECC-SMIM model has produced an image with a PSNR of 60.59 dB concerning Image 2. In an analogous manner, the ACO-ECC-SMIM model has supplied a PSNR of 59.95 dB concerning Image 3. In addition, the ACO-ECC-SMIM model has produced an Image 4 with a PSNR value of 61.58dB when applied to it. At long last, the ACO-ECC-SMIM model has produced an image with a PSNR of 59.62 dB. Figure 7 shows the analysis of PSNR.

Figure 8 presents a detailed study of SSIM and CC in the proposed ACO-ECC-SMIM model under a distinct count of test images. The figure designated that the ACO-ECC-SMIM model has resulted in enlarged values of SSIM and CC. For instance, with Image 1, the ACO-ECC-SMIM model has offered CC and SSIM of 99.96 and 99.91. Moreover, with Image 2, the ACO-ECC-SMIM model has provided CC and SSIM of 99.92 and 99.91. Equally, with Image 3, the ACO-

Figure 7
Comparison of SSIM and CC

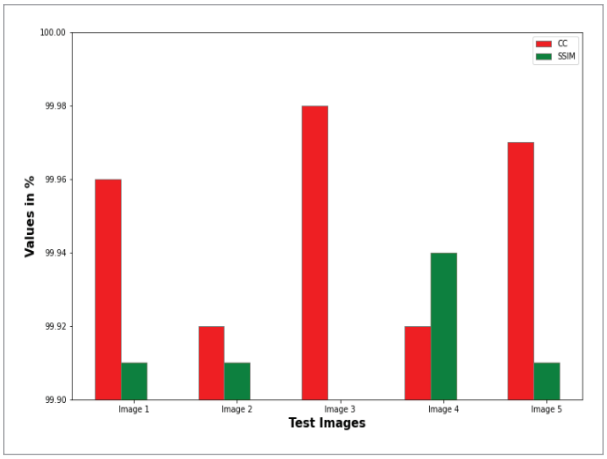
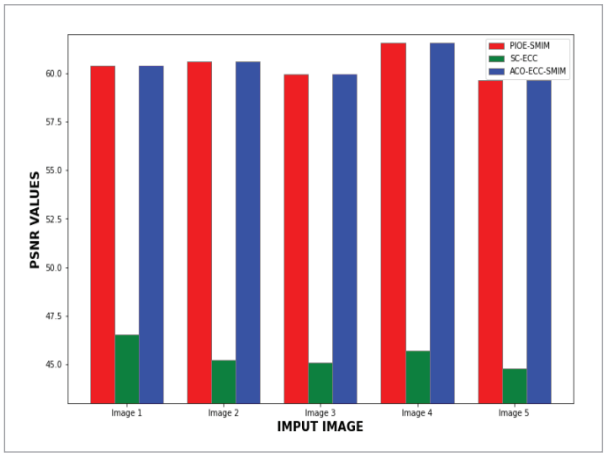


Figure 8
Proposed ACO-ECC-SMIM and existing methods analysis in terms of P SNR



ECC-SMIM model has offered CC and SSIM of 99.98 and 99.90. Furthermore, with Image 4, the ACO-ECC-SMIM model has resulted in CC and SSIM of 99.92 and 99.91. Finally, with Image 5, the ACO-ECC-SMIM model has led to CC and SSIM of 99.97 and 99.91.

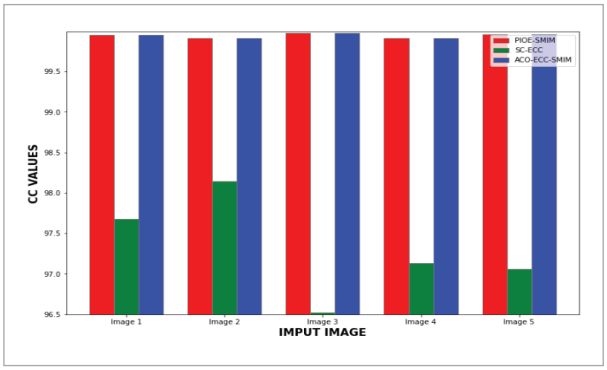
4.3. Comparative Analysis of the ACO-ECC-SMIM Method with the Existing Methods

Table 2 and Figure 9 provide an in-depth PSNR and MSE comparative analysis between the ACO-ECC-SMIM model and other models. The results suggested that the ACO-ECC-SMIM model had improved PSNR values and decreased MSE values. For in-

Table 2
Proposed ACO-ECC-SMIM and existing method comparison in terms of PSNR and MSE

	ACO-ECC-SMIM		PIOE-SMIM		SC-ECC	
Test images	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.0761	60.37	0.0751	59.37	1.4460	46.53
Image 2	0.0693	60.59	0.0652	59.99	1.9453	45.24
Image 3	0.0892	59.95	0.0853	58.82	2.0245	45.07
Image 4	0.0690	61.58	0.0610	60.28	1.7516	45.70
Image 5	0.0795	59.62	0.0725	59.53	2.1652	44.78

Figure 9
Comparison study of the ACO-ECC-SMIM model with other models



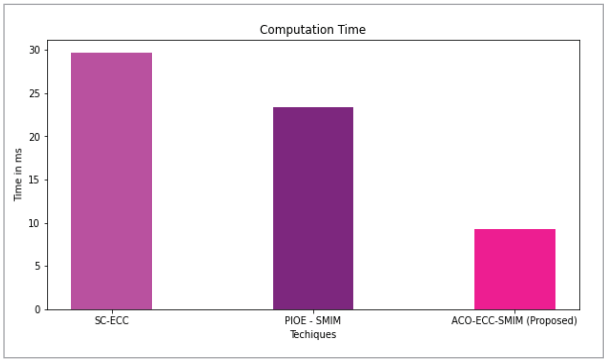
stance, the ACO-ECC-SMIM model produced the lowest MSE of 0.0761 with regard to Image 1, whereas the PIOE-SMIM and SC-ECC models produced higher MSEs of 0.0751 and 1.4460, respectively. The MSE for Figure 5 was simultaneously lowered by 0.0795 for the ACO-ECC-SMIM model and increased by 0.725 for the PIOE-SMIM model and 2.1652 for the SC-ECC model.

Table 3 and Figure 10 present a complete CC comparison study of the ACO-ECC-SMIM model with other models. The results showed that the ACO-ECC-SMIM model produced better CC values. For instance, the PIOE-SMIM and SC-ECC models achieved minimum CC of 99.95 and 97.68 for Image 1, respectively, whereas the ACO-ECC-SMIM model offered a maximum CC of 99.95. As shown in Image 3, the PIOE-SMIM and SC-ECC models only achieved minimal CC of 99.97

Table 3
Comparison study of the ACO-ECC-SMIM model with other models in terms of CC

Test images	ACO-ECC-SMIM	PIOE - SMIM	SC-ECC
Image 1	99.95	99.95	97.68
Image 2	99.91	99.91	98.14
Image 3	99.97	99.97	96.52
Image 4	99.91	99.91	97.13
Image 5	99.96	99.96	97.06

Figure 10
Computation Time



and 96.52, respectively, while the ACO-ECC-SMIM technique provided higher CC of 99.97.

Table 4 shows the analysis of the encryption time and decryption time of various algorithms.

In the observation of Table 4, while securely sharing images from sender to receiver. Time is taken for encryption and decryption of sharing images; our proposed work requires minimum time. Table 5 shows the transmission cost of the input image and storage cost in bits of different techniques.

Table 4
Encryption Time & Decryption Time

Algorithms	Encryption time (ms)	Decryption Time (ms)
ACO-ECC-SMIM	11.67	9.05
PIOE – SMIM	18.15	14.67
SC-ECC	35.73	15.67

From the observation of Table 5, our proposed work ACO-ECC-SMIM algorithm got a minimum communication cost bit and storage cost bit more than other techniques. Figure 9 presents a complete CC comparison study of the ACO-ECC-SMIM model with other models.

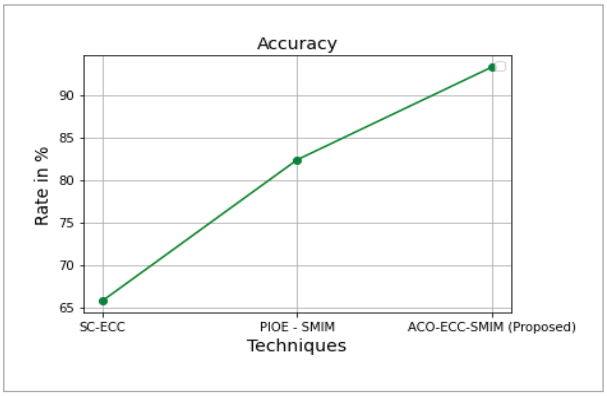
Table 5
Communication cost and Storage cost of different methods

Algorithms	Transmission cost (bits)	Storage cost (bits)
ACO-ECC-SMIM	4370	6310
PIOE – SMIM	3280	2478
SC-ECC	1770	1280

Figure 10 shows the computation time obtained from various ACO-ECC-SMIM, PIOE–SMIM, and SC-ECC methods. Our proposed work IGMM-RSA requires minimum computation time. Figure 11 shows the accuracy rate.

Figure 11 shows the accuracy rate of various algorithms such as ACO-ECC-SMIM, PIOE–SMIM, and SC-ECC. Our proposed work provides a better accuracy rate in securely sharing medical images. The accuracy rate of SC-ECC got 65.78%, PIOE – SMIM got 82.34%, and ACO-ECC-SMIM got 93.23%.

Figure 11
Accuracy Rate



5. Conclusion

In order to provide a secure image transmission system, a new ACO-ECC-SMIM model has been designed in this work. The design of the encryption process is the major emphasis of the proposed ACO-ECC-SMIM approach. The ECC scheme is used for the encryption procedure at the beginning. The ACO algorithm is used to maximize PSNR in the key generation process of the ECC model. The decryption and sharing reconstruction procedures are then carried out on the receiver side to create the original photos. The ant colony optimization algorithm-based proposed method improves large capacity and optimal image steganography methodology. The ACO algorithm can efficiently identify good answers despite the size of the search space. A thorough simulation research was conducted to demonstrate the ACO-ECC-SMIM technique's improved performance, and the findings showed the model's superiority over other methodologies. The study recommends a secure encryption technology to safeguard patient medical image privacy. Comparatively, it is clear from the outcome that the computation required by the suggested algorithm is little. As a result, the proposed algorithm is carefully constructed to obtain the highest level of security to secure the medical image. In the future, a Blockchain can be applied to enhance security in healthcare management. At the same time, the brief evaluation of performance metrics and the crypto analysis can be used for the proposed algorithm on different software and hardware platforms for possible attacks.

References

1. Anjali, T., Seema Rani, Y., Mittal, N. K. A Review on Different Image Steganography Techniques. International Journal of Engineering and Innovative Technology (IJEIT), 2014, 3(7).
2. Aswatha, A. R., Sasi, S., Santhosh, B., Mehta, D., Babuprasad, S. Design and Implementation of Unreliable CFDP Protocol over Elliptic Curve Cryptography. Smart Innovation, Systems and Technologies, 2020, 160, 627-638. https://doi.org/10.1007/978-981-32-9690-9_68
3. Banik, A., Shamsi, Z., Laiphrakpam, D. S. An Encryption Scheme for Securing Multiple Medical Images. Journal of Information Security and Applications, 2019, 49, 102398. https://doi.org/10.1016/j.jisa.2019.102398
4. Bhattacharyya, S. A Survey of Steganography and Steganalysis Technique in Image, Text, Audio, and Video as Cover Carrier. Journal of Global Research in Computer Science, 2011, 2(4), 1-16.
5. Çavuşoglu, U., Kaçar, S., Pehlivan, I., Zengin, A. Secure Image Encryption Algorithm Design Using Novel Chaos-Based S-Box, Chaos. Solitons Fractals, 2017, 95, 92-101. https://doi.org/10.1016/j.chaos.2016.12.018
6. Duraisamy, M., Balamurugan, S. Multiple Share Creation Scheme with Optimal Key Generation for Secure Medical Image Transmission in the Internet of Things Environment. International Journal of Electronic Healthcare, 2021, 11(1). https://doi.org/10.1504/IJEH.2021.10038677
7. Durdu, A. Nested Two-layer RGB-based Reversible Image Steganography Method. Information Technology and Control, 2021, 50(2), 264-283. https://doi.org/10.5755/j01.itc.50.2.27461
8. Elham, G., Jamshid, S., Nima, F. High Capacity Image Steganography Using Wavelet Transform and Genetic Algorithm. In Proceedings of the International Multiconference of Engineers and Computer Scientists, 2011, 1, 16-18.
9. Elhoseny, M., Yuan, X., El-Minir, H. K., Riad, A. M. An Energy-Efficient Encryption Method for Secure Dynamic WSN. Security and Communication Networks, 2016, 9(13), 2024-2031. https://doi.org/10.1002/sec.1459
10. Elhoseny, M., Elminir, H., Riad, A., Yuan, X. A Secure Data Routing Schema for WSN Using Elliptic Curve Cryptography and Homomorphic Encryption. Journal of King Saud University-Computer and Information Sciences, 2016, 28(3), 262-275. https://doi.org/10.1016/j.jksuci.2015.11.001
11. Elhoseny, M., Elminir, H., Riad, A. M., Yuan, X. Recent Advances of Secure Clustering Protocols in Wireless Sensor Networks. International Journal of Computer Networks and Communications Security, 2014, 2(11), 400-413.
12. Geetha, S., Subburam, S., Selvakumar, S., Kadry, S. Damasevicius, R. Steganogram. Removal Using Multidirectional Diffusion in Fourier Domain While Preserving Perceptual Image Quality. Pattern Recognition Letters, 2021, 147, 197-205. https://doi.org/10.1016/j.patrec.2021.04.026
13. Hamza, R., Yan, Z., Muhammad, K., Bellavista, P., Titouna, F. A Privacy-Preserving Cryptosystem for IoT E-Healthcare. Information Sciences, 2020, 527, 493-510. https://doi.org/10.1016/j.ins.2019.01.070
14. Hasan, M.K., Islam, S., Sulaiman, R. Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications. IEEE Access, 2021, 9, 47731-47742. https://doi.org/10.1109/ACCESS.2021.3061710
15. Jia, M., Yin, Z., Guo, Q., Liu, G., Gu, X. Downlink Design for Spectrum Efficient IoT Network. IEEE Internet Things Journal, 2018, 5(5), 3397-3404. https://doi.org/10.1109/JIOT.2017.2734815
16. Karthikeyan, K., Sunder, R., Shankar, K., Lakshmanaprabu, S. K., Vijayakumar, V., Elhoseny, M., Manogaran, G. Energy Consumption Analysis of Virtual Machine Migration in the Cloud Using Hybrid Swarm Optimization (ABC-BA). The Journal of Supercomputing, 2018, 1-17. https://doi.org/10.1007/s11227-018-2583-3
17. Lakshmanaprabu, S.K., Shankar, K., Khanna, A., Gupta, D., Rodrigues, J. J., Pinheiro, P. R., & De Albuquerque, V. H. C. Effective Features to Classify Big Data Using Social Internet of Things. IEEE Access, 2018, 6, 24196-24204. https://doi.org/10.1109/ACCESS.2018.2830651
18. Li, F., Gao, T., Yang, Q., Cao, Y. An Extended Matrix Encoding Algorithm for Steganography of High Embedding Efficiency. Computers and Electrical Engineering, 2011, 37(6), 973-981. https://doi.org/10.1016/j.compeleceng.2011.08.006
19. Marco, D., Thomas, S. Ant Colony Optimization. Prentice Hall of India Private Limited, 2005, 37-38.
20. Metawa, N., Hassan, M.K., Elhoseny, M. Genetic Algorithm-Based Model for Optimizing Bank Lending Deci-

sions. Expert Systems with Applications, 2017, 80, 75-82. https://doi.org/10.1016/j.eswa.2017.03.021

21. Nematzadeh, H., Enayatifar, R., Motameni, H., Guimarães, F. G. Coelho, V.N. Medical Image Encryption Using a Hybrid Model of Modified Genetic Algorithm and coupled Map Lattices. Optics and Lasers in Engineering, 2018, 110, 24-32. https://doi.org/10.1016/j.optlaseng.2018.05.009
22. Pal, S. K., Anand, S. Cryptography Based on RGB Color Channels Using ANNs. International Journal of Computer Network and Information Security, 10(5), 60-69, 2018. https://doi.org/10.5815/ijcnis.2018.05.07
23. Parthasarathi, P., Shankar, S. Weighted Ternary Tree Application for Secure Group Communication among Mobile Applications. Wireless Personal Communication, 2021, 117(4), 2809-2829. https://doi.org/10.1007/s11277-020-07049-z
24. Rarhi, K., Saha, S. Image Encryption in IoT Devices Using DNA and Hyper Chaotic Neural Network. Lecture Notes Network System, 2020, 82, 347-375. https://doi.org/10.1007/978-981-13-9574-1_15
25. Sahu, S., Singh, A. K., Ghrera, S. P., Elhoseny, M. An Approach for Denoising and Contrast Enhancement of Retinal Fundus Image Using CLAHE. Optics & Laser Technology, 2019, 110, 87-98. https://doi.org/10.1016/j.optlastec.2018.06.061
26. Sathesh Kumar, K., Shankar, K., Ilayaraja, M., Rajesh, M. Sensitive Data Security in Cloud Computing Aid of Different Encryption Techniques. Journal of Advanced Research in Dynamical and Control Systems, 2017, 9(18), 2888-2899.
27. Seyyed, A. S., Ivanov, N. High Payload and Secure Steganography Method Based on Block Partitioning and Integer Wavelet Transform. International Journal of Security and Its Applications, 2014, 8(4), 183-194. https://doi.org/10.14257/ijsia.2014.8.4.17
28. Shankar, K., Lakshmanaprabu S. K. Optimal Key-based Homomorphic Encryption for Color Image Security Aid of Ant Lion Optimization Algorithm. International Journal of Engineering & Technology, 2018, 7(9), 22-27. https://doi.org/10.14419/ijet.v7i1.9.9729
29. Shankar, K., Eswaran, P. Sharing a Secret Image with Encapsulated Shares in Visual Cryptography. Procedia Computer Science, 2015, 70, 462-468. https://doi.org/10.1016/j.procs.2015.10.080
30. Shankar, K., Eswaran, P. ECC-based Image Encryption Scheme with the Aid of Optimization Technique Using Differential Evolution Algorithm. International Journal of Applied Engineering Research, 2015, 10(55), 1841-1845.
31. Shaktawat, V. A. R., Lakshmi, S. R. S. N., Panwar, A., A Hybrid Technique of Combining AES Algorithm with Block Permutation for Image Encryption. Rel., Theory Appl., 2020, 15(1), 15.
32. Shubo, L., Sun, J., Xu, Z. An Improved Image Encryption Algorithm Based on Chaotic System. Journal of Computers, 2009, 4. https://doi.org/10.4304/jcp.4.11.1091-1100
33. Sreelaja, N. K., Vijayalakshmi Pai, G. A. Swarm Intelligence Based Key Generation for Stream Cipher. International Journal of Security and Communication Networks, 2011, 4(2), 181-194. https://doi.org/10.1002/sec.132
34. Souvik, B., Gautam, S. Data Hiding in Images in Discrete Wavelet Domain Using PMM. International Journal of Computer and Information Engineering, 2010, 4(8), 1276-1284.
35. Sundarakrishnan, K., Raja, S. P., Jaison, B. A Symmetric Key Multiple Color Image Cipher Based on Cellular Automata, Chaos Theory and Image Mixing. Information Technology and Control, 2021, 50(1), 55-75. https://doi.org/10.5755/j01.itc.50.1.28012
36. Wan, Y., Gu, S., Du, B. A New Image Encryption Algorithm Based on Composite Chaos and Hyperchaos Combined with DNA Coding. Entropy, 2020, 22(2), 171. https://doi.org/10.3390/e22020171
37. Zhang, B., Rahmatullah, B., Wang, S., Zaidan, A., Liu, P. A Review of Research on Medical Image Confidentiality Related Technology Coherent Taxonomy, Motivations, Open Challenges and Recommendations. Multimedia Tools and Applications, 2020. https://doi.org/10.1007/s11042-020-09629-4