electronics

Article

Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security

Jeeva Selvaraj [1], Wen-Cheng Lai [2,3], Balasubramanian Prabhu Kavin [1], Kavitha C. [4,*] and Gan Hong Seng [5,*]

[1] Department of Data Science and Business System, SRM Institute of Science and Technology, Kattankulathur Campus, Chennai 603203, Tamil Nadu, India
[2] Bachelor Program in Industrial Projects, National Yunlin University of Science and Technology, Douliu 640301, Taiwan; wenlai@mail.ntust.edu.tw
[3] Department Electronic Engineering, National Yunlin University of Science and Technology, Douliu 640301, Taiwan
[4] Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai 600119, Tamil Nadu, India
[5] School of AI and Advanced Computing, XJTLU Entrepreneur College (Taicang), Xi'an Jiaotong—Liverpool University, Suzhou 215400, China
* Correspondence: kavitha.cse@sathyabama.ac.in (K.C.); HongSeng.Gan@xjtlu.edu.cn (G.H.S.)

Abstract: The expansion of the Internet of Things is expected to lead to the emergence of the Internet of Medical Things (IoMT), which will revolutionize the health-care industry (IoT). The Internet of Things (IoT) revolution is outpacing current human services thanks to its bright mechanical, economical, and social future. Security is essential because most patient information is housed on a cloud platform in the hospital. The security of medical images in the Internet of Things was investigated in this research using a new cryptographic model and optimization approaches. For the effective storage and safe transfer of patient data along with medical images, a separate framework is required. The key management and optimization will be chosen utilizing the Rivest–Shamir–Adleman-based Arnold map (RSA-AM), hostile orchestration (HO), and obstruction bloom breeding optimization (OBBO) to increase the encryption and decryption processes' level of security. The effectiveness of the suggested strategy is measured using peak signal-to-noise ratio (PSNR), entropy, mean square error (MSE), bit error rate (BER), structural similarity index (SSI), and correlation coefficient (CC). The investigation shows that the recommended approach provides greater security than other current systems.

Keywords: Internet of Things; Rivest–Shamir–Adleman-based Arnold map; hostile orchestration; obstruction bloom breeding optimization

check for updates

Citation: Selvaraj, J.; Lai, W.-C.; Kavin, B.P.; C., K.; Seng, G.H. Cryptographic Encryption and Optimization for Internet of Things Based Medical Image Security. *Electronics* **2023**, *12*, 1636. https://doi.org/10.3390/electronics12071636

Academic Editors: Imed Ben Dhaou, Mueen Uddin and Moez Krichen

Received: 9 January 2023
Revised: 22 March 2023
Accepted: 23 March 2023
Published: 30 March 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With yearly increases in revenue and employment, the health-care sector ranks among the greatest in the developing world [1]. Early on, the only way to diagnose rare diseases was through a thorough physical examination and analytical review conducted on hospital grounds. A smartwatch can now assist us in identifying any health issues, e.g., a sluggish heartbeat in an elderly person. Technology plays a crucial role in slowing down the rapid spread of an epidemic disease such as Ebola by educating the general public and encouraging them to take the necessary precautions. According to the Centers for Disease Control and Prevention (CDC), patients should never take medication without first consulting a physician [2,3]. On the other hand, recent advancements in technology enable the patient to receive the initial diagnostics. As technology advances, the focus of health-care services is shifting from hospital-centric care to individual-centric services. The Internet of Things (IoT), which enables objects to connect to it, makes it possible for information to be sent and received over the internet. The idea of the IoT has developed into a number of different

technologies, such as sensors, embedded systems, machine learning, and real-time analysis. It has to do with other internet-based technology that is wireless or wired, such as the concept of a "smart hospital" [4]. Smart devices can collect data and communicate them in everyday life to perform the necessary tasks. Smart cities, connected health care, connected automobiles, electronics, and entertainment systems all make use of IoT applications. The Internet of Things' adoption in the medical industry is centered on a wide range of sensors, medical instruments, artificial intelligence (AI), diagnostic tools, and cutting-edge imaging equipment. In both established and developing sectors and civilizations, these innovations raise productivity and living standards. Many security professionals who are drawn to the similarities of chaotic systems and methods use them for a variety of cryptographic applications, such as hash, public key infrastructure, picture and video encryption, image privacy protection, and image encryption. Electrocardiography (ECG) signals, in addition to other biometric personal qualities, are utilized for identification and cryptography in a variety of application contexts, including the Internet of Things [5,6]. It is crucial to protect medical photographs saved on digital media. These photographs may be numerous and large, and the majority of them contain private images [7]. The reason for doing this is that since digital images are often two-dimensional, we must be able to trace and disconnect links between pixels quickly [8]. We leverage the decimal development of an irrational number to build a higher-dimensional encryption key, which we then use to alter the pixel layout in the hidden image, as digital images are often two-dimensional [9]. Encryption is a very effective tool for storage and transport, but once the sensitive data are decoded, the data are no longer secure [10,11]. It is crucial to protect medical photographs saved on digital media. If the photographs are in plain text, it will be impossible for the intruder to access them and the daily records. The focus of the majority of fundamental encryption methods is on text data or paired data. Image encryption algorithms are related to plaintext, and combine two diffusion operations and a transform related to plaintext to encrypt the image and use a hyperchaotic system to generate the key stream [12,13]. In order to obtain an extremely grounded medical services research [14], framework [15,16] undertaken earlier sought to improve the security of medical data transfer.

The study's objective is to use the best private and public key-based security possible for IoT-based therapeutic images to find the perfect key. Obstruction bloom breeding optimization considers a multitude of factors, from which the study's researchers selected and examined the important unresolved issues of IoT security improvement. The authentication review provides information on the appropriate key-based security technique.

This paper's primary contribution is the hostile orchestration search (HOS) method, which creates the public and private key pair needed to encrypt and decrypt a picture. During the encryption and decryption process, the Rivest–Shamir–Adleman-based Arnold map (RSA-AM) is utilised to generate the public key and the private key (H). Obstruction bloom breeding optimization associated with the key in encryption procedures is made more secure using this cryptographic approach. As long as the communal and private keys are fully protected, this type of encryption is very secure.

The rest of this paper is structured as follows. The issues in medical picture security are discussed in Section 2, which also reviews the literature. Section 3 discusses the suggested image encryption and decryption, key generation, and optimization procedure. The experimental findings are presented in Section 4, and the algorithm's impacts are examined and tested in Section 5. Conclusions are provided in Section 6.

2. Literature Survey

Haralick features are extracted, which are also known as local binary pattern (LBP), the histogram of oriented gradients (HOG), and the gray-level co-occurrence matrix (GLCM). If more features are used, the classifier will become more sophisticated and produce better results. This research employs the pigeon-inspired optimization (PIO) feature selection technique as a result. When the user submits a collection of query photos during the testing

phase, an artificial neural network (ANN) classifier is used to compare the training images from the dataset to the query images in order to extract the relevant images [17].

A hyperchaotic image encryption system is based on cellular automata (CS) and the particle swarm optimization (PSO) algorithm. The initial setup of the hyperchaotic system is formed by the hash function value, which is closely related to the plaintext picture to be encrypted in order to increase resistance to plaintext attacks. The correlation coefficient between adjacent image pixels indicates PSO's fitness. Cellular automata technology, which is based on a hyper-chaotic system, can make populations more complex, diverse, and random, making encryption systems safer and preventing them from reaching a local optimum [18].

Image steganography uses a variety of techniques to provide security for the secret data, such as an image encryption method based on binary bit-plane decomposition (BBPD). After that, an adaptive embedding method based on the salp swarm optimization algorithm (SSOA) is suggested in order to maximize the payload capacity by altering the settings of the steganographic embedding function for edge and smooth blocks. In this case, the SSOA method is effectively employed to localize the edge and smooth blocks. After that, a hybrid fuzzy neural network and a backpropagation learning strategy are utilized to enhance the quality of the stego images. Finally, using an extremely secure IoT protocol, these stego images are sent to the target [19].

Interfaces that are user-friendly, enduring, secure, and scalable are necessary for the difficult challenges that arise during photo analysis and restoration. Even though there are many benefits to the cloud paradigm that have been suggested, there are still many issues with privacy and secrecy. The approach's originality comes from its use of agile, secure cloud pallets for image processing, advancement of ant colony optimization-based algorithms for better resource utilization when running compute- and resource-intensive image analysis tools [20], and extension of conventional cloud architecture.

Lévy flight-based gray wolf optimization is used to select the most significant features for the steganalysis method from a set of original features. For the reason, SPAM and AlexNet have been used to generate the high-dimensional features. The random forest classifier is also used to divide the photos with particular attributes into cover images and stego images [21]. A novel bilateral-based, bio-inspired optimization filtering method is taken into consideration for the MI denoising procedure (BF). Gaussian and spatial weights are affected by the implementation of the denoising procedure, or the choice of the best parameters. The swarm-based dragonfly (DF) and modified firefly (MFF) algorithms are utilized in this instance to select these options. For recreation investigation, multiobjective wellness (PSNR and VRMSE) is utilized. The denoised cycle has been used to investigate the aftereffects of the proposed BF boundaries with connection to clinical pictures once the ideal boundaries had been picked [22].

A feature extraction method for encrypted image retrieval is presented. First, we extract the image features using the enhanced Harris method. Second, the SURF technique and BOW model are integrated to build the feature vectors of each image, making it easier to obtain data from the cloud server. The parameters of the LSH method are then improved and used to generate the searchable index with the goal of increasing retrieval efficiency [23–25].

In the field of medical imaging, image denoising has been of particular significance (MI). The hardest part of image denoising is preserving data-bearing surfaces such as edges and surfaces to achieve acceptable visual quality while boosting peak signal-to-noise ratio (PSNR). In this paper, the MI denoising process is considered using a creative, bio-inspired optimization-based filtering system known as the bilateral filter (BF). The decision to choose the best parameters, i.e., Gaussian and spatial weights, is influenced by how the denoising process is carried out. These parameters are selected in this case using the swarm-based dragonfly (DF) and modified firefly (MFF) algorithms [26].

The current security techniques pigeon-inspired optimization (PIO) [17], particle swarm optimization (PSO) [18], salp swarm optimization algorithm (SSOA) [19], ant colony

optimization (ACO) [20], gray wolf optimization [21] bio-inspired optimization [22,26,27] and Harris corner optimization [23,28] also employ encryption, steganography, or combinations of the two. There is a special, ideal technique for image encryption that can be totally protected against unauthorized access, withmprovements in peer verification to prevent the leak of personal data and potentially dangerous instigating behaviors.

3. Proposed Method

It is critical to inform customers about IoT security and protection and to adamantly state that there would be no real risk to the integrity of their data, secrecy, or the confidentiality of a professional in the medical system. This will allow businesses to profit from IoT innovation. The deciding factor for IoT to anchor the transmission of medical images is its quick advancement on a large scale.

This research develops a hybrid encryption method for IoT security where the computation suggested has unique features in encryption and decoding in terms of speed, even with optimal keys. The quality of cryptographic primitives for safeguarding sensitive data heavily relies on random numbers, which are represented by encryption keys. The integrity and confidentiality of the image must be preserved because the processing and communication of digital medical images raises various security issues. The verification of medical images will serve as the main means of ensuring the prevention, stability, which is shown in Figure 1. The original image's blocks are randomly deleted and reassembled inside the image. The edited image is again put through a twofold encryption procedure for medical image security that first uses RSA-AM encryption and then also uses an obstruction bloom breeding optimization-based signcryption technique. To strengthen the encryption security of the sender's and receiver's private and public keys, this hostile orchestration search key generation is carried out. The yielding image and the initial image are then contrasted to see how well they performed using the PSNR after the decryption procedure. With stronger PSNR, this tactic aims to raise the security level of encrypted images.

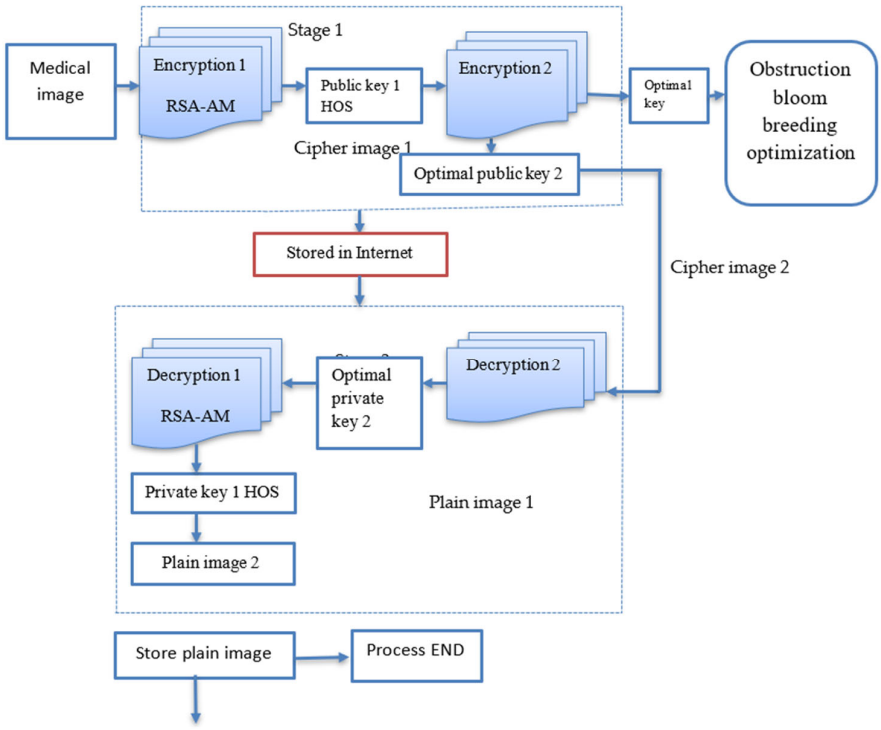


Figure 1. Block diagram of proposed work.

3.1. Medical Image Transmission in IoT

Lung cancer fatality rates are higher than those of other cancers, making lung screening absolutely necessary. An early and popular screening technique for chest imaging

called a radiograph has benefits including low measurements and little work. An expert evaluates the medical imaging, suggests a quick course of action, together with the required medications, and instantly transmits it back to the original core. In this way, the motivation behind the suggested philosophy, i.e., providing medical protection in a moment of emergency using IoT as the principal weapon, takes care of its demand. Small default stages of key generation, encryption, decryption, and optimization are included in this cryptographic security technique. An optimization approach is taken into consideration for key generation in order to increase the security level of IoT frameworks. Achieving practical and skilled implementation depends on search institutionalization.

3.2. Key Generation Stage

The keys and associated picture are encoded and translated using a hostile orchestration, which offers both mystery and dependability. Asymmetric key (public key) calculations employ a key match, which consists of a private key and the associated public key.

It is characterized as follows

$$O_j^* = L_j + H_j - O_j \tag{1}$$

In the improbable case that O is a result in the search area that is currently open and when $O_j^* \in [L_j, H_j]$, the aforementioned equation then shows a new solution O_j^* in the modified space in accordance with the hostile orchestration model.

3.2.1. Initialization Process

The key selection procedure is thought to produce a new key size as a result of this initialization of prime numbers.

$$Key_{1,2,\ldots n} = \{x_1, x_2, \ldots . x_n\} \tag{2}$$

3.2.2. Hostile Orchestration for Key Generations

Improvisational creation is the process of producing a fresh hostile arrangement. HO is the stage in which a musician performs a song from memory. The estimations from the other choice criteria are chosen for comparison. The HO is the likelihood of choosing one inducement at random from the set of possible characteristics as well as the likelihood of choosing one incentive from the set of real qualities stored in hostile orchestration.

$$P_i' = P_i \in \begin{Bmatrix} P_i^1, P_i^2, \ldots . P_i^{HMS} \; with \; probability \; HMCR \\ P_i' \in P \; with \; probability (1 - HMCR) \end{Bmatrix} \tag{3}$$

For instance, if the harmony memory consideration rate is 0.90, the HO calculation will most likely (by 90%) select the preferred variable reward for most of the HO's put-away characteristics.

3.3. Image Encryption Process

With confusion and diffusion technologies and asymmetric image encryption, this work develops a groundbreaking technique. The picture encryption scheme is Algorithm 1. Figure 2 shows the flow of image encryption. The precise encryption procedure is detailed as follows.

Step 1: choosing prime numbers p and q to create a new key

$$n = p \times q, \varphi(n) = (p-1)(q-1) \tag{4}$$

Step 2: Using the hostile orchestration technique, create a private key d and a public key e.

Step 3: As confidential information, four positive numbers (x_{01}, x_{02}, x_{03}, and x_{04} are chosen at random. Using Equation (4), y_{0i}, $i = 1, 2, 3, 4$ is calculated to equal.

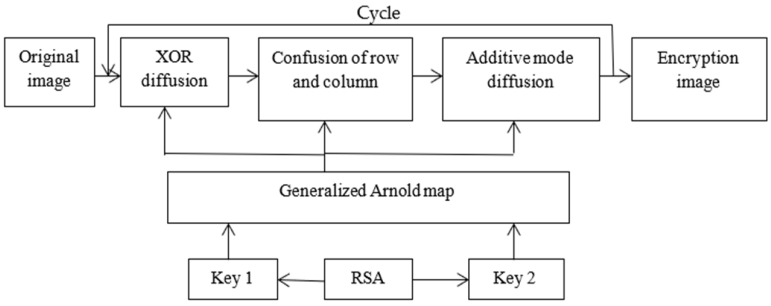


Figure 2. The image encryption algorithm.

Step 4: Public key e is used to calculate the public ciphertext $c_i = y_{0i}^e \bmod n$, $i = 1, 2, 3, 4$ before Equation (5) is applied to determine the parameter pairs a and b of the Arnold map:

$$\begin{cases} y_{01} = x_{01} + x_{02}, \\ y_{02} = x_{02} + x_{03}, \\ y_{03} = x_{03} + x_{04}, \\ y_{04} = x_{01} + x_{04}, \end{cases} \tag{5}$$

$$\begin{cases} a_1 = fix(x_{01} + sqrt(\log(c_1 + y_{01}))) \\ b_1 = fix(x_{02} + sqrt(\log(c_2 + y_{02}))) \\ a_2 = fix(x_{03} + sqrt(\log(c_3 + y_{03}))) \\ b_2 = fix(x_{04} + sqrt(\log(c_4 + y_{04}))) \end{cases} \tag{6}$$

Step 5: To produce chaotic sequences s and r, insert the following parameters into the generalised Arnold map equation: a_1, b_1, a_2, and b_2. Then, change the values produced into the 0–255 range.

$$S = mod\left(floor\left((s + 100) \times 10^{14}\right), 256\right), \tag{7}$$

$$R = mod\left(floor\left((r + 100) \times 10^{14}\right), 256\right) \tag{8}$$

Step 6: Save the simple as it appears as P and, using the generated key stream S, do the follows XOR diffusing procedure to acquire image A:

$$A_i = A_{i-1} \oplus P_i \oplus S_i \tag{9}$$

where A_i, P_i and S_i stand in for the components A, P, and S.

Step 7: S is converted into a matrix. Next, apply cyclical scramble to the initial row and column of the image matrix S, where image A is located, to create image B.

Step 8: To create image C, an additive mode diffusion operation is employed with image B and the chaotic sequence R.

$$C_i = C_{i-1} + B_i + R_i mod\ 256 \tag{10}$$

where C_i, B_i, and R_i, are the components of C, B, and R, respectively.

Step 9: discovered after two iterations of computation.

The three channels R, G, and B can be used to treat the color image as three grayscale images. Therefore, each channel uses the same encryption.

The encryption process supplies two inputs: the plaintext version of the data picture and the encryption key. In this case, the length of the unique image data bit stream is divided into the hostile orchestration building blocks. Each line of the array's byte components corresponds to one of the image's output lines, and the image's lines are

completely encrypted. The array's byte components are stored in row order from left to right.

Algorithm 1: Image encryption pseudocode

Input : original image P, sec ret keys $x_{01}, x_{02}, x_{03}, x_{04}$
Examine the image's size. $M \times N$
Find the Arnold map's a and b using Equations (5) and (6) using RSA. and $x_{01}, x_{02}, x_{03}, x_{04}$
Create the two important streams S and R using Equations (7) and (8)
Get X and Y by sorting a row and a column from S.
$B = P \oplus S$;//Perform XOR diffusion operations
For $i = 1 : M$
    $D(X(i),:) = B(i,:)$;//Confusion on the row direction
end
For $i = 1 : N$
    $E(:, Y(i)) = D(:, i)$;//Confusion on the column direction
end
$C = mod\ (E + R, 256)$;//Perform additive mode diffusion operation
Output: encryption image C

3.4. Image Description Process

The pseudocode for the image decryption algorithm is Algorithm 2, and it goes like this. The opposite of encryption is image decryption.

Step 1: Private key d, or $y_{oi} = c_i^d mod\ n, i = 1, 2, 3, 4$, is used to decrypt public ciphertext data $c_i, i = 1, 2, 3, 4$. The Arnold map's parameter pairs a and b are then constructed using (3) and (4).

Step 2: The chaotic sequences s' and r' are produced when the two pairs of parameters are replaced into the generalized Arnold map equation, and the values produced are translated into the range from 0 to 255:

$$S' = mod\Big(floor\Big(\big(s' + 100\big) \times 10^{14}\Big), 256\Big), \tag{11}$$

$$R' = mod\Big(floor\Big(\big(r' + 100\big) \times 10^{14}\Big), 256\Big) \tag{12}$$

Step 3: The process of inverse diffusion and modulus addition is used to combine the cypher image E and chaotic sequence R' to create the image C'.

$$C_i' = 2 \times 256 + E_i - E_{i-1} - R_i' mod\ 256 \tag{13}$$

where C_i', E_i', and R_i' represent the elements of C', E', and R'.

Step 4: A matrix is created from S', Then, using a confusing of C' to create image B'.

Step 5: to obtain image A', conduct the XOR diffusion procedure with images B' and S', as given by

$$A_i' = B_{i-1}' \oplus B_i' \oplus S_i' \tag{14}$$

where A_i', B_i' and S_i' signify the essentials of A', B', and S'.

Step 6: After completing two rounds of decryption, plain picture P' is acquired.

The suggested method makes use of the best private key to increase medical image security. In order to significantly improve the picture security process, we use obstruction bloom breeding optimization approach in this case.

Algorithm 2: Pseudocode of image decryption

encryption image C, public information c_i, $i = 1, 2, 3, 4$
Read the image size $M \times N$
Use private key d to decrypt to get y_{0i}, $i = 1, 2, 3, 4$
Calculate the a, b for Arnold map by Equations (5) and (6)
Generate the key stream S' and R' by Equations (7) and (8)
Take a row and a column from S' and sort them, then get X' and Y'
$C' = mod(2 \times 256 + E - R')$;
$for\ i = 1\ :\ M$
$E'(i, :) = C'(X'(i) :)$;
end
$for\ i = 1\ :\ N$
$B'(:, i) = E(:, Y'(i))$;
end
$A' = B' \oplus S'$;
Output : original image A'

3.5. Key Optimization Using Bloom Breeding Optimization

In order to find the hash function using OBBO and the oppositional process, we must optimize the signcryption strategy's key parameters. Most often, bloom breeding is associated with the exchange of dust, which is accomplished by breeders such as insects, birds, bats, other animals, or wind. Some bloom varieties require particular breeders for breeding to be successful. In our effort, we developed the OBBO algorithm for selecting the security process's best keys, which includes the following advancements.

3.5.1. Initial Bloom Explanation Generation (Keys)

The algorithm begins by randomly generating food source locations related to the search space's answers. Let D be a bloom arrangement with a key that contains breed. Thus, $Sol = \{x_1, x_2 \ldots\ldots x_D\}$, is the initial solution, and each bloom converses with $k_D = \{C_1, C_2, \ldots\ldots C_L\}$,.

3.5.2. Obstruction Solution for Bloom Breeding Optimization

The opposition is preferable to coming up with additional random solutions and selecting the best one. This is because one of the opposition candidates is always closer to the solution. Both the current solution and its opposite solution simultaneously display indications of a more accurate estimate for the current answer. It is anticipated that a random breed solution has a lower probability of being near the total optimum layout than an opposing breed solution. This approach uses the following conditions to create (15).

$$Opp_{Sol} = \{O_1, O_2, \ldots\ O_{Km}\} \tag{15}$$

where $O_{ki} = L_i + H_i - K_i$ and the position of the ith obstruction O_{ki} Using the initialization method mentioned above, determine the fitness function.

3.5.3. Fitness Evaluation

A crucial consideration in the bloom breeding optimization algorithm is the choice of fitness. This medical picture security procedure takes into account each image's PSNR with the best possible solution, and it communicates:

$$Fitnes_{F_i} = Max(PSNR) \tag{16}$$

3.5.4. Update New Key Solution for Bloom Breeding Optimization

Update the solutions with the bloom breeding technique following the fitness calculation. The bloom breeding algorithm has undergone two key upgrades, including global

and local breeding. The first and third criteria are combined in the global pollination step to determine the conveyed in the condition solution (17).

$$K_i^{t+1} = K_i^t + \beta Levy(\beta)\left(Y \times -K_i^t\right) \tag{17}$$

where $K_i^t \rightarrow$ breeding. Insects can fly regularly and migrate across a larger area; therefore, in the worldwide breeding process, breeding like insects spreads bloom breeding, which may go over a long distance. In this case, breeding capacity is relevant to Lévy flight-based advance size.

$$Levy \sim \frac{\beta\sqrt{(\beta)}\sin(\pi\beta/2)}{\pi} \times \frac{1}{y^{1+\beta}}(y \gg y_0 > 0) \tag{18}$$

The typical function is $\sqrt{(\beta)}$, and this distribution is accurate for large steps $(y > 0)$. The innovative blooming solution and local breeding strategy presented by:

$$K_i^{t+1} = K_i^t + \varepsilon\left(K_j^t - K_k^t\right) \tag{19}$$

where there are f variations of the same plant species imitating the bloom speed in a small area, ε as [0, 1]. The majority of bloom breeding activities can take place both locally and globally. Consecutive bloom fixes or bloom in the nearby area will eventually likely be produced by local bloom breeders rather than those who are far away.

3.5.5. Stop Criteria

The method is created to provide precise solutions in light of maximizing the objective function after the best solutions that achieve the goal function are identified. The process is continued until the best key is found.

3.6. Optimal Key-Based Signcryption Stage

With the aid of the signcryption method and the aforementioned perfect key system, the picture will be safe. A public key primitive called "signcryption" uses the recipient's public key and the value to determine the hash value, combining the capabilities of encryption and digital signatures into a single operation (S). The result of the hash function (O_H) as a 128-bit evaluation.

(i) Choose the $\left[1 \ldots\ldots\ldots\ldots\ldots P_{f-1}\right]$ range for the sender value (S).

(ii) The recipient's best public key (opt_B_{K2}) is used to find the sender's hash function, which converts the sender's 128-bit plain image into two 64-bit hash outputs (O_{H1} and O_{H2}).

$$O_H = Hash\left(B_{k2}^S mod\ P_N\right) \tag{20}$$

(iii) The image is encrypted using the encryption E process from this hash, and the result is a cypher image (C_I) with a 64-bit output value.

$$C_I = Enc_{O_{H1}(Image)} \tag{21}$$

(iv) The sender then uses the restricted keyed hash function KHf's (O_{H2}) value to obtain the image's hash. Additionally, this output value is considered to be (M_I).

$$M_I = KH_f O_{H2}(Image) \tag{22}$$

(v) Using the public key and prime factor values, the sender finally calculates the encrypted image, which is represented by:

$$P_I = \frac{S}{(M_I + A_{k1}) mod P_f} \tag{23}$$

Sending the three different values independently across secure transmission channels would strengthen security and sign-encrypt the image, which the sender owns (C_I, M_I and P_I). These three values are then transmitted to the recipient.

3.7. De-Signcryption Process

This chapter shows how the recipient can decrypt an image that the sender has already sent. In this stage, the recipient receives the message's signed image (C_I, M_I and P_I) from the sender and decrypts it.

(i) Sender values (M_I and P_I) recipients private key (A_{K2}), recipient public key (A_{K2}), and to create a hash that would produce 128 bits.

$$O_H = Hash\left(B_{k2} * i^{M1}\right)^{P_1^*} A_{k1} P_N \tag{24}$$

(ii) The 128-bit output is divided into two 64-bit parts, much like a sign-encryption operation, which would show the (O_{H1}, O_{H2}) key match. This key combination and the key match used to sign the image would be identical, making it impossible to tell them apart.

(iii) The image is then provided by the receiver after using the key O_{H1} to decode the cypher image C_I.

$$Dec_{Image} = Dec\, O_{H1}(C_I) \tag{25}$$

If they match, it means that Alice actually marked and sent the message. If not, Bob will recognize that Alice either did not mark the message or that Alice's message was blocked and altered by an outsider. It advances and is authentic when the next level, the de-signcryption, indicating that the received image m is authentic. when the signcrypted image (C_I, M_I and P_I) received from the reliable outsider has to supply keys. It is strongly advised to encrypt images using a powerful block cypher. The best possible keys were created to safeguard the medical imaging.

Two cloaks, the mystery cover and the even masks, are used in a relentless movement to incorporate the decryption process. Thus, decoding an image entails using an unscrambling system to each encrypted estimate of a pixel in the encrypted image. When a simple encryption scheme is being used, all image handling operations may only be performed on the unencrypted image.

4. Performance Measure

The robustness and security of the proposed cryptosystem are assessed using a number of tests. Peak signal-to-noise ratio (PSNR), mean square error (MSE), bit error rate (BER), structural similarity index (SSI), and coefficient are a few examples of statistical evaluations.

4.1. Peak Signal-to-Noise Ratio

Several tests are used to evaluate the security and resilience of the proposed cryptosystem. Some of the statistical evaluations include the peak signal-to-noise ratio (*PSNR*), mean square error (*MSE*), bit error rate (BER), structural similarity index (SSI), and correlation coefficient.

$$PSNR = 10 \log\left(\frac{I^2}{MSE}\right) \tag{26}$$

where I stands for the highest pixel in the image's probable range of values

4.2. Mean Square Error

The *MSE* algorithm determines the size of the normal error among the stego-image and the original image. The *MSE* is determined as shown below:

$$MSE = \frac{1}{[R \times C]^2} \sum_{i=0}^{n} \sum_{j=1}^{m} (X_{ij} - Y_{ij})^2 \tag{27}$$

where R and C are the cover image's row and column counts, X_{ij} is the cover image's pixel's brightness, and Y_{ij} is the stego image's pixel's brightness.

4.3. Bit Error Rate

The likelihood that a bit may be wrongly received due to noise is calculated using the BER. It is calculated by deducting the quantity of unintentionally received bits from the total amount of bits supplied. This equation is used to compute the *BER*:

$$BER = \frac{Errors}{Total\ Number\ of\ Bits} \tag{28}$$

4.4. Structural Similarity Index (SSI)

The SSI between two sequences A and B at a certain pixel P is calculated using the formula shown below:

$$SSI = \frac{(2mean(A \times B) + c_1)(2con(A * B) + c_2)}{(mean(A^2) + mean(B^2) + c_1)(con(A^2) + con(B^2) + c_2)} \tag{29}$$

where $mean(A \times B)$ is the mean value of sequences A and B calculated over a constrained XY window centered on P, $con(A)$ and $con(B)$ are the A and B standard deviations calculated over the same frame, respectively, and cov(P), which is calculated across the same window, is the covariance between A and B.

4.5. Correlation Coefficient

The relationship between pixels is shown by the correlation coefficient. We determine the correlation coefficients of two neighboring pixels and of three adjacent pixels using the formula below.

$$CC = \frac{\sum_{i=1}^{N}(l_i - d(I)) - (m_i - d(m))}{\sqrt{\sum_{i=1}^{N}(l_i - d(l))^2 - (m_i - d(m))^2}} \tag{30}$$

The symbol M in the performance measurements above denotes the image's highest pixel value, while N designates one of the image's dimensions. The input and encrypted pictures are represented by A and B, while the regularization constants are indicated by c_1 and c_2.

5. Results and Analysis

MATLAB 2016 supports the recommended best key-based security strategy with an i5 processor and 4 GB of RAM. Medical photographs from websites, including brain, lung EEG images, and other images, were gathered for security examination. As seen in Figure 3, the researchers looked at a variety of diagnostic scans, including those for the brain, lung, glaucoma, and cancer. They came from medical organizations using cloud storage. The secret image was examined both before being conveyed and after being received by the intended receiver. This is done to ensure that the first cover record has a tiny distortion once the hidden image has been masked over.

Results of the suggested approach are shown in Table 1 using several picture measurements: time, PSNR, MSE, BER, CC, and SSI. The optimal key is selected to divide the message into three equal portions with the highest level of fitness, and after that, the entire input is encrypted. These test images have a maximum PSNR of 63.25 dB, which is significantly greater than the "MSE and BER" of 0.15 and 0 and the most exciting SSI of 1. Additionally, this table shows the cover picture and scrambled image histograms. The convergence of the fitness function (PSNR) is shown in Figure 4 in comparison to the obstacle bloom breeding optimization model and conventional optimization. The obstacle bloom breeding strategy in this diagram requires the fewest iterations possible to produce the best results. In keeping with this, it is increased to 63.25, which was accomplished in 78 cycles, the hybrid's initial fitness estimation is 11.36, whereas the underlying fitness

calculation for other approaches is 9.48. Then, with variations in light of the tactics, the emphasis is altered in accordance with the implementation.

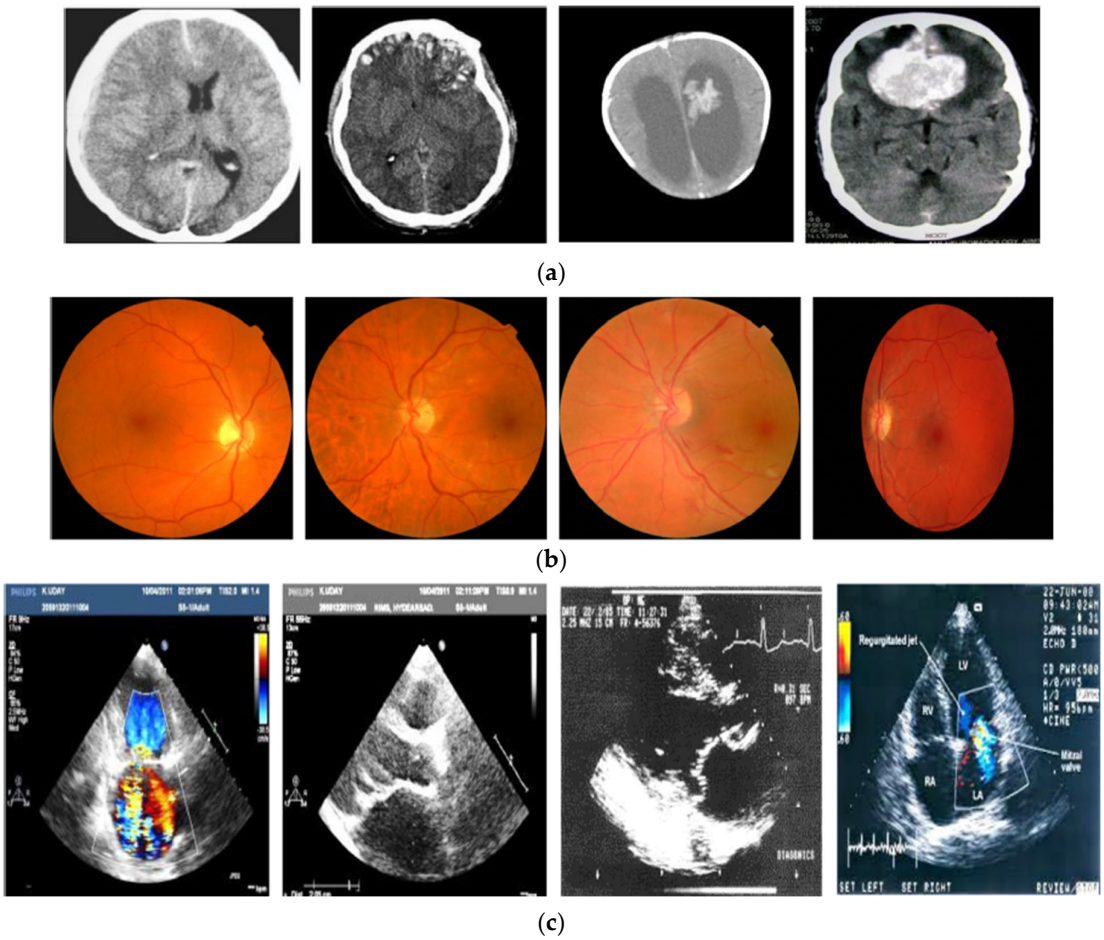


Figure 3. Images from a sample database for the suggested model of (**a**) The brain image, (**b**) Glaucoma image, (**c**) Echocardiography image.

Table 1. Results of the proposed model (hostile orchestration and obstruction bloom breeding optimization).

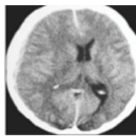
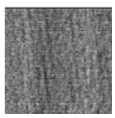
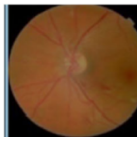
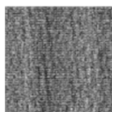
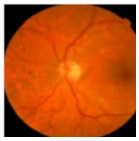
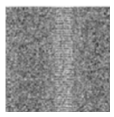
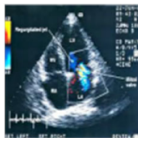
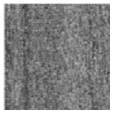
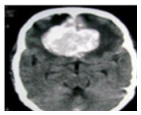
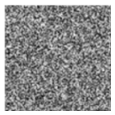
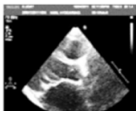
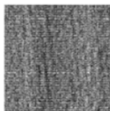
Images	Encrypted Image	PSNR	MSE	BER	SSI	CC
		59.23	0.12	0	1	0.95
		58.22	0.09	0	1	1
		59.34	0.15	0.01	1	0.98

Table 1. *Cont.*

Images	Encrypted Image	PSNR	MSE	BER	SSI	CC
		63.25	0.10	0	0.01	0.96
		59.64	0.12	0.98	0.02	0.97
		60.36	0.11	1	0	1

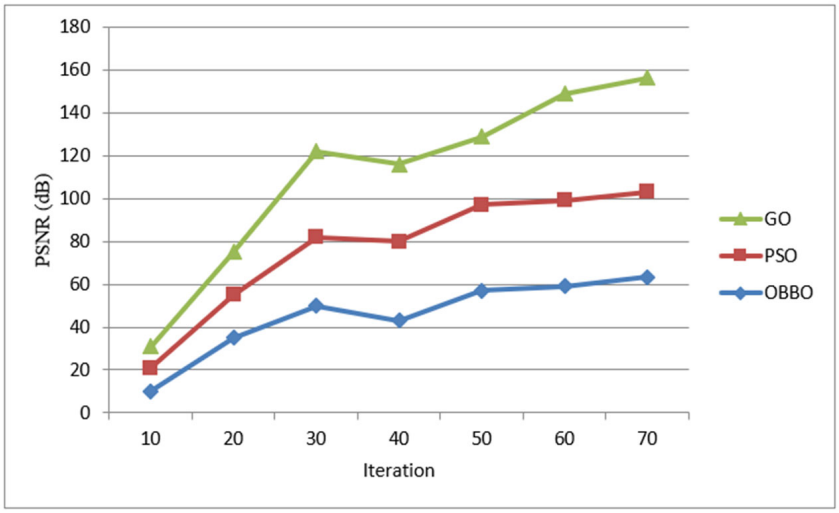


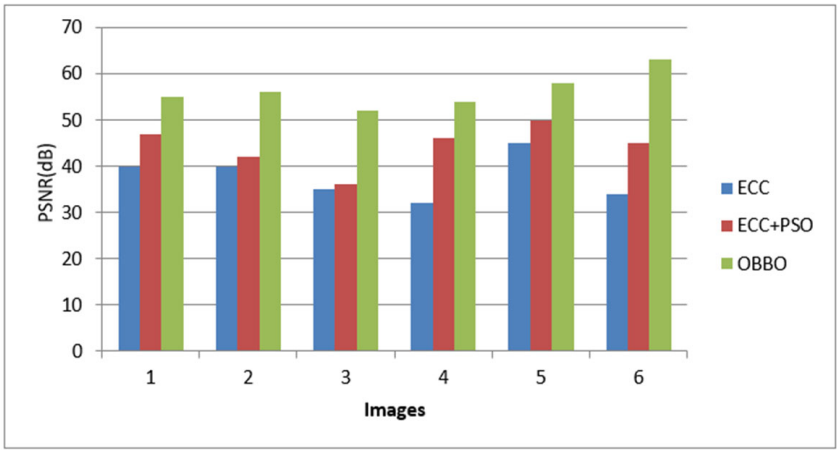
Figure 4. Fitness evaluation.

Figure 5a–e shows a comparable analysis using different measurements. Here, different approaches—elliptic curve cryptography (ECC) [29,30], ECC + PSO, and OBBO with hybrid improvement—are taken into consideration to handle the correlation part. Figure 5a shows how a hybrid technique that contrasted with the current strategy was used to examine the PSNR measure, where the most extreme result is 63.25 dB. The output images are recognized and the proposed approach is connected to the image by the images and by their PSNR values. By 2.89%, it differs from ECC, ECC + PSO, and OBBO. The MSE and BER are shown in Figure 5b,c. All the images of the suggested model are currently valued. There was no variety between the considered images in the BER, where its qualities were zero for the two images, meaning there was no difference between the considered images. The MSE value for the suggested hybrid encryption approach, which is 0.68, is the highest. In Figure 5d, neighboring pixel situations hold significant information about the structural substance of the image. The encryption and decryption process over this lengthy computing time in the least possible time, which is 1.5 min, as illustrated in Figure 5e. According to the current research, the Rivest–Shamir–Adleman-based Arnold map (RSA-AM), hostile orchestration (HO), and OBBO technique provided are faster at encrypting and decrypting data than existing technologies.

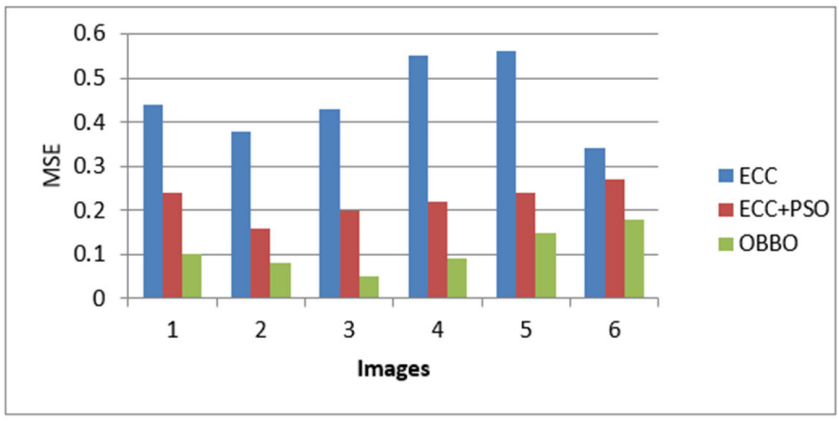
The proposed model has the best fitness compared to PSO (particle swarm optimization) and GO (generic optimization), where the difference is 12.56% to 13.5%, and to the other method, which has a further differentiation of 14.85%. The proposed OBBO technique uses a diagram to simply determine the ideal fitness esteem with successful results.

Running time indicate the shortest amount of time needed for this security technique, i.e., 1.5 min, to complete the encrypting and decryption process in this lengthy contrast and computing time. By comparing the suggested AES and ECC + GO, ECC + PSO technique to an existing technology, the encryption and decryption times are reduced.

Figure 6 demonstrates the final photos of medical image security of PSNR, MSE, BER, SSI, and CC under attack versus without attack. The PSNR assessment of "without assault image" works best when the assaults are coupled with various images. The PSNR value fluctuates and is visually represented when the noise density increases. The encryption of PSNR values for the two processes quickly degraded as the noise level increased. The quality of the clear image decreases due to substantial distortion in the reconstructed image if the limit rate is significantly increased in all three modalities.

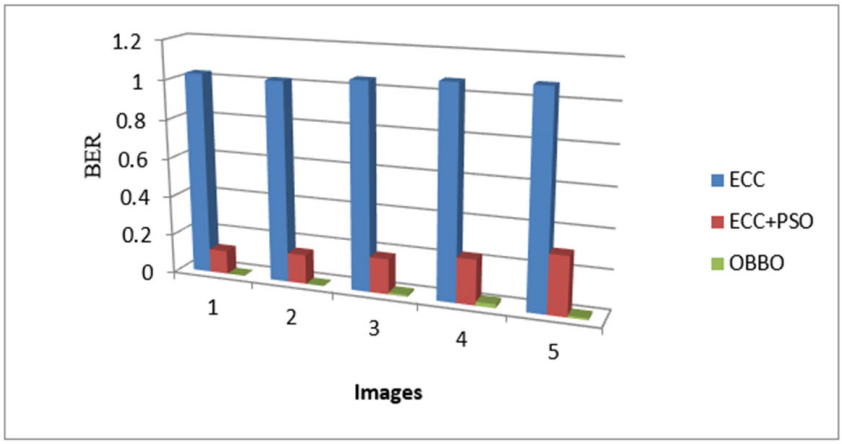


(**a**)

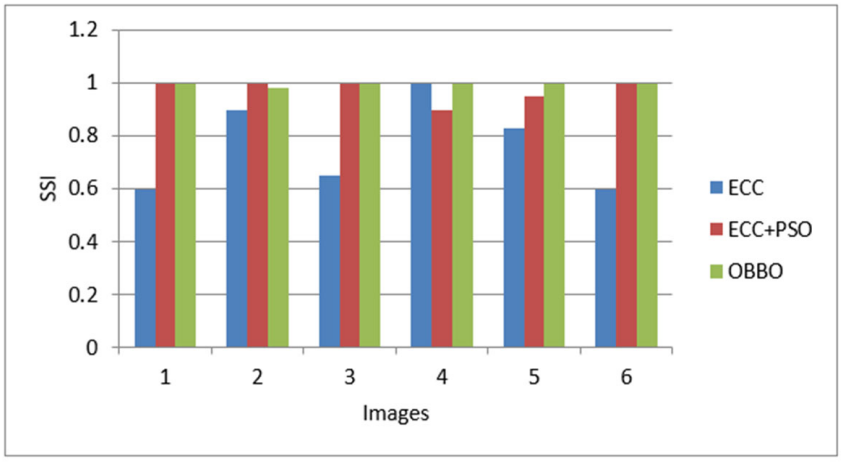


(**b**)

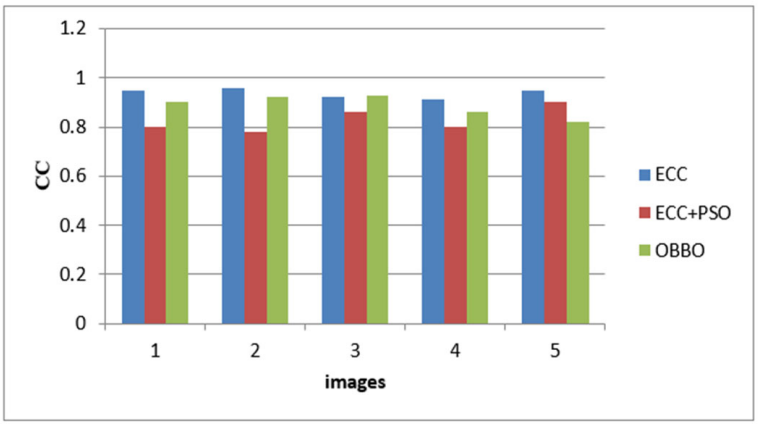
Figure 5. *Cont.*



(**c**)



(**d**)



(**e**)

Figure 5. Comparison of the suggested methods. (**a**) Comparative analysis for PSNR (**b**) Comparative analysis for MSE (**c**) Comparative analysis for BER (**d**) Comparative analysis for SSI (**e**) Comparative analysis for CC.

Figure 7 shows the running time indicate the shortest amount of time needed for this security technique, i.e., 1.5 min, to complete the encrypting and decryption process in this lengthy contrast and computing time. By comparing the suggested AES and ECC + GO, ECC+PSO technique to an existing technology, The encryption and decryption times are reduced in these recent works.

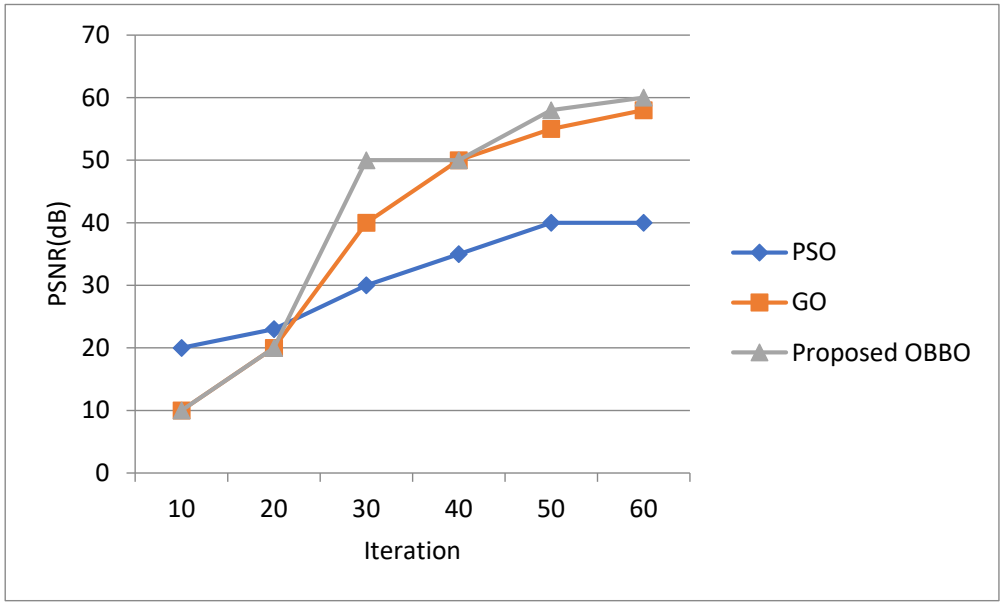


Figure 6. Fitness comparison with existing algorithms.

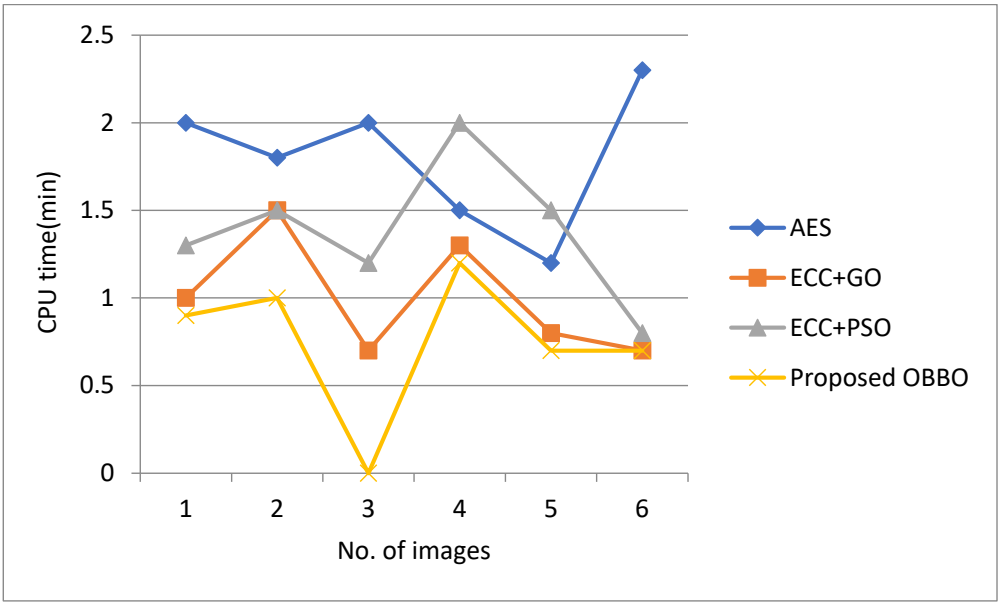


Figure 7. Running time comparison of proposed method with existing methods.

The final images of medical image security with and without attack are shown in Figure 8a–e. demonstrates the final photos of medical image security of PSNR, MSE, BER, SSI, CC under attack versus without attack. The PSNR assessment of "without assault image" works best when the assaults are coupled to various images. The PSNR value fluctuates and is visually represented when the noise density increases. The encryption of PSNR values for the two processes quickly degraded as the noise level increased. The quality of the clear image decreases due to substantial distortion in the reconstructed image if the limits rate is significantly increased in all three modalities.

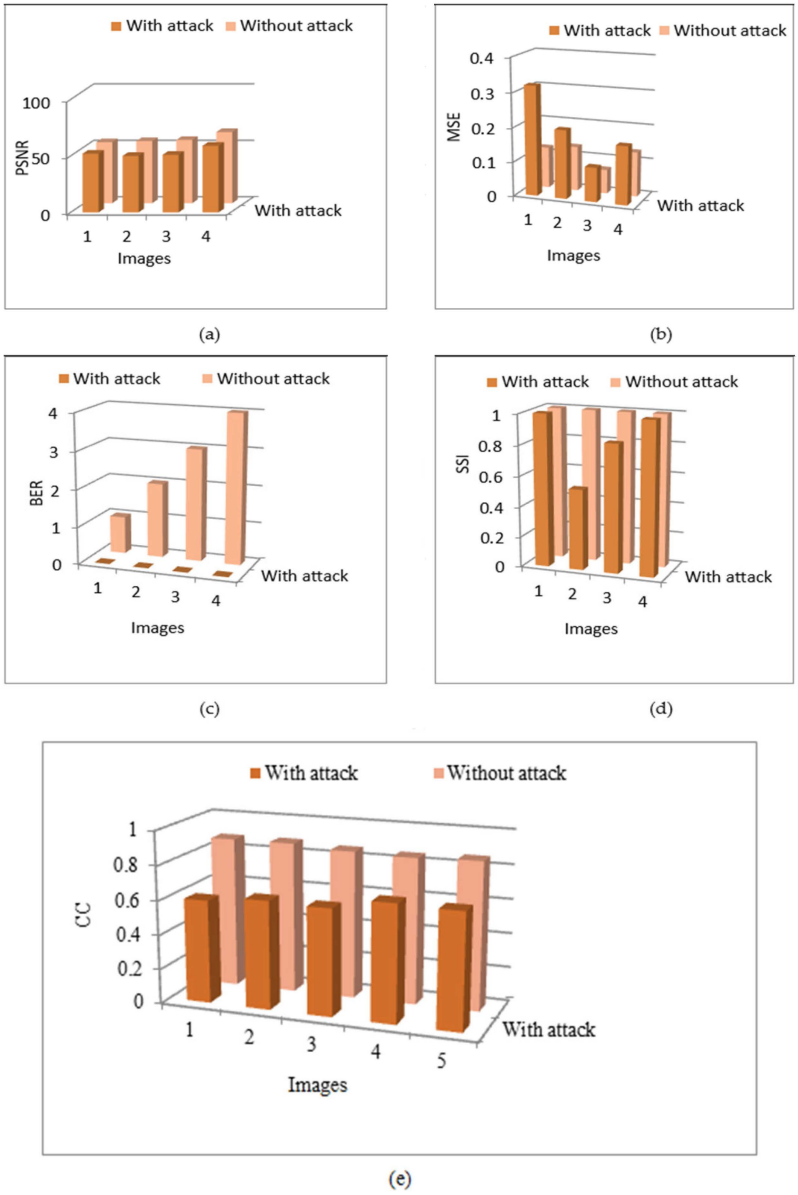


Figure 8. (**a**) Attack versus without an attack of PSNR. (**b**) Attack versus without an attack of MSE. (**c**) Attack versus without an attack of BER. (**d**) Attack versus without an attack of SSI. (**e**) Attack versus without an attack of CC.

6. Conclusions

It is crucial to expand on the few concepts raised and bring about more advancements in medical image security. The proposed hybrid encryption algorithm technique used as a component of IoT was taken into account in the current study. Key management and optimization are chosen utilizing the Rivest–Shamir–Adleman-based Arnold map (RSA-AM). The employment of hostile orchestration (HO) and obstacle bloom breeding optimization raises the security level of the encryption and decryption process. In order to create the desired message, this recommended approach uses multinomial usage throughout both encryption and decoding. Because the financial position is less ambiguous, this strategy takes less memory. The researchers presented this study employing a variety of data and crucial metrics, including PSNR and SSI, which have shown control image quality in comparison to all tests. It is evident that the approach is insufficiently safe because it never produced considerable ability. Consequently, more research is needed to enhance the security level. The recommended method decodes and encrypts data more quickly.

Future research should put more emphasis on tamper-localization techniques than the strict-integrity functionality used in the previous algorithms in order to have respectability based on content.

Author Contributions: J.S. and K.C.: research concept and methodology, writing—original draft preparation; G.H.S.: investigation; W.-C.L.: validation and funding acquisition; B.P.K.: review, revision, and editing. All authors contributed to the article and have approved the submitted version. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Yunlin University of Science and Technology, Douliu.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The datasets used and/or analyzed during the current study are available at http://www.adcis.net/en/Download-Third-Party/Messidor.htmldownload-en.php%20-%20retinal%20database (accessed on 8 January 2023), http://nist.mni.mcgill.ca/?page_id=672 (accessed on 8 January 2023), and http://www.via.cornell.edu/lungdb.html (accessed on 8 January 2023).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Ali, Z.; Hossain, M.S.; Muhammad, G.; Sangaiah, A.K. An intelligent healthcare system for detection and classifcation to discriminate vocal fold disorders. *Future Gener. Comput. Syst.* **2018**, *85*, 19–28. [CrossRef]
2. Jagadeeswari, V.; Subramaniyaswamy, V.; Logesh, R.; Vijayakumar, V. A study on medical Internet of Things and Big Data in personalized healthcare system. *Health Inf. Sci. Syst.* **2018**, *6*, 14. [CrossRef] [PubMed]
3. Topol, E. *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*; Basic Books: Hachette, UK, 2019.
4. Javaid, M.; Ibrahim, H.K. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J. Oral Biol. Craniofac. Res.* **2021**, *11*, 209–214. [CrossRef] [PubMed]
5. Peris-Lopez, P.; Gonzalez-Manzano, L.; Camara, C.; de Fuentes, J.M. Effect of attacker characterization in ECG-based continuous authentication mechanisms for internet of things. *Future Gener. Comput. Syst* **2018**, *81*, 67–77.
6. Hatzivasilis, G.; Othonas, S.; Sotiris, I.; Christos, V.; Giorgos, D.; Christos, T. Review of security and privacy for the Internet of Medical Things (IoMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini Island, Greece, 29–31 May 2019; pp. 457–464.
7. Shen, M.; Yawen, D.; Liehuang, Z.; Xiaojiang, D.; Nadra, G. Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach. *IEEE Netw.* **2019**, *33*, 27–33. [CrossRef]
8. Alsaffar, M.; Gharbi, A.; Abdullah, A.; Saud, A.; Tariq, S.; Almurayziq, A.; Abdullah, H.; Vishal, K.; Assaye, B. Detection of tuberculosis disease using image processing technique. *Mob. Inf. Syst.* **2021**, *2021*, 7424836. [CrossRef]
9. Wen, H.; Liu, Z.; Lai, H.; Zhang, C.; Liu, L.; Yang, J.; Lin, Y.; Li, Y.; Liao, Y.; Ma, L.; et al. Secure DNA-coding image optical communication using non-degenerate hyperchaos and dynamic secret-key. *Mathematics* **2022**, *10*, 3180. [CrossRef]
10. Mou, J.; Yang, F.; Chu, R.; Cao, Y. Image compression and encryption algorithm based on hyper-chaotic map. *Mob. Netw. Appl.* **2021**, *26*, 1849–1861. [CrossRef]
11. Poornima, E.; Srinivasulu, S.; Dileep Kumar, P.R.; Ramesh, G. A Generic Framework for Sharing Data Using Attribute Based Cryptography in Hybrid Cloud. *Int. J. Intell. Syst. Appl. Eng.* **2022**, *10*, 634–640.
12. Abdulbaqi, A.S.; Ahmed, J.O.; Alyaa, H.M. ECG signals recruitment to implement a new technique for medical image encryption. *J. Discret. Math. Sci. Cryptogr.* **2021**, *24*, 1663–1673. [CrossRef]
13. Shen, Y.; Tang, C.; Xu, M.; Lei, Z. Optical selective encryption based on the FRFCM algorithm and face biometric for the medical image. *Opt. Laser Technol.* **2021**, *138*, 106911. [CrossRef]
14. Alassaf, N.; Adnan, G.; Shabir, A.P.; Manal Al, G. Enhancing speed of SIMON: A light-weight-cryptographic algorithm for IoT applications. *Multimed. Tools Appl.* **2019**, *78*, 32633–32657. [CrossRef]
15. Moraes, J.L.; Rocha, M.X.; Vasconcelos, G.G.; Vasconcelos, F.J.E.; de Albuquerque, V.H.C. Advances in photopletysmography signal analysis for biomedical applications. *Sensors* **2018**, *18*, 1894. [CrossRef]
16. Shehab, A.; Elhoseny, M.; Muhammad, K.; Sangaiah, A.K.; Yang, P.; Huang, H.; Hou, G. Secure and robust fragile watermarking scheme for medical images. *IEEE Access* **2018**, *6*, 10269–10278. [CrossRef]
17. Buvana, M.; Muthumayil, K.; Jayasankar, T. Content-based image retrieval based on hybrid feature extraction and feature selection technique pigeon inspired based optimization. *Ann. Rom. Soc. Cell Biol.* **2021**, *25*, 424–443.
18. Zeng, J.; Wang, C. A novel hyperchaotic image encryption system based on particle swarm optimization algorithm and cellular automata. *Secur. Commun. Netw.* **2021**, *2021*, 6675565. [CrossRef]

19. Dhawan, S.; Chinmay, C.; Jaroslav, F.; Rashmi, G.; Arun, K.R.; Subhendu, K.P. SSII: Secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. *IEEE Access* **2021**, *9*, 87563–87578. [CrossRef]
20. Suresh, S.; Bhavani, H.R.; Hanumanthappa, M. A Secured Cloud-Based Framework for Image Processing Using Ant Colony Optimization. In *Rising Threats in Expert Applications and Solutions*; Springer: Singapore, 2021; pp. 211–221.
21. Pathak, Y.; Arya, K.V.; Tiwari, S. Feature selection for image steganalysis using levy flight-based grey wolf optimization. *Multimed. Tools Appl.* **2019**, *78*, 1473–1494. [CrossRef]
22. Elhoseny, M.; Shankar, K. Optimal bilateral filter and convolutional neural network based denoising method of medical image measurements. *Measurement* **2019**, *143*, 125–135. [CrossRef]
23. Qin, J.; Li, H.; Xiang, X.; Tan, Y.; Pan, W.; Ma, W.; Xiong, N.N. An encrypted image retrieval method based on Harris corner optimization and LSH in cloud computing. *IEEE Access* **2019**, *7*, 24626–24633. [CrossRef]
24. Qureshi, M.B.; Qureshi, M.S.; Tahir, S.; Anwar, A.; Hussain, S.; Uddin, M.; Chen, C.-L. Encryption Techniques for Smart Systems Data Security Offloaded to the Cloud. *Symmetry* **2022**, *14*, 695. [CrossRef]
25. Hussain, S.; Ullah, S.S.; Uddin, M.; Iqbal, J.; Chen, C.-L. A Comprehensive Survey on Signcryption Security Mechanisms in Wireless Body Area Networks. *Sensors* **2022**, *22*, 1072. [CrossRef] [PubMed]
26. Hussain, S.; Ullah, S.S.; Shorfuzzaman, M.; Uddin, M.; Kaosar, M. Cryptanalysis of an online/offline certificateless signature scheme for internet of health things. *Intell. Autom. Soft Comput.* **2021**, *30*, 983–993. [CrossRef]
27. Reegu, F.A.; Abas, H.; Jabbari, A.; Akmam, R.; Uddin, M.; Wu, C.M.; Chin-Ling, C.; Khalaf, O.I. Interoperability Requirements for Blockchain-Enabled Electronic Health Records in Healthcare: A Systematic Review and Open Research Challenges. *Secur. Commun. Netw.* **2022**, *2022*, 9227343. [CrossRef]
28. Uddin, M.; Memon, M.S.; Memon, I.; Ali, I.; Memon, J.; Abdelhaq, M.; Alsaqour, R. Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records. *Comput. Mater. Contin.* **2021**, *68*, 2377–2397. [CrossRef]
29. Shankar, K.; Lakshmanaprabu, S.K. Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. *Int. J. Eng. Technol.* **2018**, *7*, 22–27.
30. Lai, W.C.; Srividhya, S.R. A Modified LBP Operator-Based Optimized Fuzzy Art Map Medical Image Retrieval System for Disease Diagnosis and Prediction. *Biomedicines* **2022**, *10*, 2438. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.