An Effective Group Key-based Secure Data Transfer in IoMT using Rossler Hyper Chaotic System with Modified Polar Bear Optimization

S. Bhuvaneswari[1*], T. Pramananda Perumal[2]
[1]Research Scholar (PT), Dept. of Computer Science, Presidency College, Chennai-600 005.
[2]Principal (Retired), Presidency College, Chennai-600 005.
*bhuvanaparthi@gmail.com

Abstract

Objectives: The main objective of this study is to improve the security of data transfer in Internet of Medical Things (IoMT) and also to minimize the processing time and memory size.

Methods: The group key, generated by dual encryption scheme(using AES and RSA algorithms), is optimized by proposed Modified Polar Bear Optimization (MPBO) algorithm and then it is used in Rossler Hyper Chaotic System (RHCS) method for medical data encryption and decryption in IoMT. **Findings**: The total processing times of an image and a signal for their secure transfer by using the proposed Modified Polar Bear Optimization-Rossler Hyper Chaotic System (MPBO-RHCS) are 16.717ms and 6.6593ms respectively. In this case, the memory size of an image and a signal, occupied during their secure transfer are 2.0586 x 10^{07} bytes and 5.7639 x 10^{07} bytes respectively. They are the least values of total processing time and memory size of an image when they are compared to other existing optimization algorithms viz. Arithmetic Optimization Algorithm (17.518ms, 3.8851 x 10^{07}bytes), Tunicate Swarm Algorithm (17.72ms, 3.0118 x 10^{07}bytes), Harris Hawks Optimizer (17.004ms, 2.5395 x 10^{07}bytes) and Polar Bear Optimization (17.297ms, 2.3478 x 10^{07}bytes). Similarly, total processing time and memory size of a signal for its secure transfer by using the proposed MPBO-RHCS method are the least values when they are compared to other existing optimization algorithms viz. Arithmetic Optimization Algorithm (7.5129ms, 9.7243 x 10^{07}bytes), Tunicate Swarm Algorithm (7.6142ms, 6.5892 x 10^{07}bytes), Harris Hawks Optimizer (6.9031ms, 6.1497 x 10^{07}bytes) and Polar Bear Optimization (7.0785ms, 6.2333 x 10^{07}bytes).

The total processing time and memory size of an image for its secure transfer by using the proposed MPBO-RHCS method have the least values (16.717ms, 2.0586 x 10^{07}bytes) when they are compared to other existing chaotic methods viz. Henon chaotic map (18.466ms, 2.8851 x 10^{07}bytes), Logistic chaotic map (17.693ms, 2.7210 x 10^{07}bytes), Arnold cat chaotic map (17.848ms, 3.0051 x 10^{07}bytes) and RHCS (17.97ms, 3.9003 x 10^{07}bytes). The total processing time and memory size of a signal for its secure transfer by using the proposed MPBO-RHCS method have the least values (6.6593ms, 5.7639 x 10^{07}bytes) when they are compared to other existing chaotic methods viz. Henon chaotic map (9.1488ms, 8.7243 x 10^{07}bytes), Logistic chaotic map (7.9677ms, 6.7639 x 10^{07}bytes), Arnold cat chaotic map (7.6088ms, 7.1497 x 10^{07}bytes) and RHCS (8.3185ms, 9.8333 x 10^{07}bytes).

Novelty: In the existing Polar Bear Optimization (PBO) algorithm, α is a random number in the interval [0, 1]. In the proposed MPBO, the random number α is modified by $\alpha = \frac{\beta}{\lambda}$**,** where, β is a random number in the range [0, 1]. λ is a random value in the range [0, ω]. Here, ω is the distance between the two spatial coordinates, measured in Euclidean metric. The group key is optimized by using proposed MPBO. The initial parameters (x_0,y_0,z_0), generated after optimization are fed into the Rossler hyper chaotic system for encryption.

Keywords: Group Key-based Secure Data Transfer Scheme, IoMT, Rossler Hyper Chaotic System, Modified Polar Bear Optimization Algorithm.

1. Introduction

Real-time patient monitoring has a benefit, offered by the Internet of Medical Things (IoMT) such as a network of innovative medical gadgets and sensors [1]. These devices use a shared network to gather process and transmit critical health data such as electrocardiograms, body temperature, sugar levels, oxygen levels, blood pressure and heart rate to the healthcare systems [2]. More connected medical equipments can be found in the normal hospitals, including oxygen pumps, remote Intensive Care Unit (ICU), ventilators, patient monitors, MRI scan machines, therapeutic lasers, smart beds etc.[3]. IoMT also includes home-based healthcare systems such as automatic insulin injection, intelligent medicine box, mental health monitoring, sleep monitoring, fall detection etc. [4].

Significant obstacles to IoMT are the privacy and security of information that travel through the Internet [5]. The information has been shared by many IoMT data transfer models and it is vulnerable to security, creating a number of attacks [6]. Cybercriminals can take advantage of IoMT's vulnerabilities to do a number of methods like sensor hijacking and controlling medical gadgets, confidential clinical file theft, private patient information theft, obscuring network traffic, interfering with medical procedures and demanding ransom payments [4].

In general, asymmetric encryption with a group key strategy has been employed for information protection and for transferring the data between the groups [7]. Therefore, a new group key-based secured data transfer scheme has been implemented with the help of advanced encryption algorithm. In order to share the information in the IoMT environment, a group has been formed and the formed group consists of patients, a group manager and doctors. When the message has been forwarded in the group, the group manager receives the message and forwards it to the doctors. The group manager will maintain the time stamp and key. If the key values are known by the doctors, then they will have the ability to view the data. If the time period is elapsed, then the validated doctors are not able to view the information. This way of providing timestamp and key-based data encryption highly protects the data from unauthorized users. When a user newly joins the group, a new key will be provided for the user and this key will be shared to all the members in the group to view the personal data among the IoMT community. Here, 256-bit group key will be generated for highly protecting the information [8].

Data owner based attributes are used in cloud computing, instead of machine learning-based discrimination to separate a particular database into sensitive and non-sensitive groups. Sensitive values have been separated into subgroups based on how they are used between organizations and the data owner's willingness. Each subgroup is encrypted using group keys. The non-sensitive parameters are combined with the encrypted sensitive groupings [9].

In order to balance the load on a key server, a novel master-key management strategy has been proposed to manage the key and also to improve the security of healthcare information [10]. A lightweight encryption technique with crossover operator of a genetic algorithm and logistic-tent map has been proposed. Using a logistic-tent map and crossover, the random key for encryption of the image has been generated for each image encryption [11].

A resource-constrained IoMT device might make efficient use of a lightweight and fast member authentication group key agreement using a symmetric XOR operation and binary polynomial for group communications [12]. To lower the IoMT computational cost, a group key-based protocol has been used in the dynamic groups. Physical unclonable function (PUF) uses message fingerprints so that the user is not necessary to store a private key [13].

The healthcare systems are used to provide high security, privacy and information quality. Better group key management protocols are required to provide higher security over IoMT. Providing high resistance over the statistical and differential attacks is very important in IoMT. Several group key agreement-based mechanisms are developed to give high security over the medical data [6]. Hence, a proposed MPBO-RHCS group key-based secured data transfer scheme is introduced to transmit medical data with high security.

The objectives of the group key-based secure data transfer scheme are summarized as follows.

- To implement a group key-based secure data transfer scheme for effectively moving patient's data, in order to prevent data thefts from hackers and to preserve the privacy of the data in IoMT.
- To develop a Rossler Hyper Chaotic System **(**RHCS)-based encryption by using Modified Polar Bear Optimization **(**MPBO) algorithm to optimize the parameters for enhancing the performance to minimize the total processing time and memory size.
- To compare the performance of the proposed MPBO-RHCS group key-based secure data transfer scheme with the other existing optimization algorithms and chaotic systems.

This paper is organized as follows. In Section 2, the gathered dataset and scheme for the proposed model are described. The results and discussion are summarized and discussed in Section 3. We highlight the principal outcome of the study in Section 4.

2. Methodology

In our study, to provide a high security for group communication in IoMT, a group key-based secure data transfer scheme is proposed by using encryption with optimization.

2.1 Proposed Secure Data Transfer Scheme

Normally, the data transfer scheme does not provide more security and privacy for data. Increasing number of devices like sensors etc. and using low standard devices in an e-health cloud are the key challenges and security issues while transferring the data [14]. The other major issues are efficient authentication and secure data transmission. In order to address these issues, hybrid lightweight authentication scheme is proposed [15]. Hence to overcome these issues, a new scheme Modified Polar Bear Optimization- Rossler Hyper Chaotic System (MPBO-RHCS) group key-based secure data transfer scheme is proposed for data security.

The proposed MPBO-RHCS group key-based secure data transfer scheme is used for securing medical data and transmitting the data to the valid user. It is used to prevent unauthorized access. The images and signals have been gathered from the Internet. The gathered images are given to the encryption section. Here, the encryption can be performed using an RHCS-based algorithm. The proposed MPBO algorithm is adopted for optimizing the initial parameters to minimize the total processing time and memory size. In addition, the spectrogram images are extracted from the gathered signals. The extracted spectrogram images are given to the same RHCS-based encryption for effectively securing the signals. Here also, the initial parameters for the RHCS are optimized by using MPBO to increase the performance of the encryption. The authenticated user with the known group key can access the data at anywhere and anytime within a specific period of time.

2.2 Dataset used in IoMT

IoMT is a set of medical devices and applications that connect to healthcare systems through online. The IoMT reduces needless hospital visits and the strain on the healthcare system by connecting patients and doctors through a secure network and enabling the exchange of medical data. The IoMT devices collect the data from patients by keeping some electronic devices on the patient's forehead, hand, leg, chest etc., The dataset which are used in IoMT are gathered from websites as follows.

Dataset-1 (Image Data): The images are gathered using the link: "https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection: Access date: 2023-04-25". This dataset contains 253 files. These files are present in anyone of the formats viz. jpg, png and jpeg. Also, it contains normal or abnormal images from the patients and it is presented in a jpg (joint photographic expert group) format.

Dataset-2 (ECG Dataset): The signals are gathered using the link:
"https://www.kaggle.com/datasets/devavratatripathy/ecg-dataset: Access date: 2023-04-25". It contains ECG (Electro Cardiogram) readings of patients. This dataset contains 98 files. The file is presented in a CSV (Comma Separated values) format with 141 columns. Columns 0-139 have showed an ECG data point of patients. The normal or abnormal representations are shown using the values 0 or 1 in the dataset.

2.3 Dual Data Encryption

2.3.1 Group Key Generation with dual Encryption Scheme

A plain message is divided into two part. The left part is encrypted using AES algorithm. Using the RSA algorithm, right part is encrypted utilizing the private key. The fully encrypted message contains both the parts which are correctly indexed and stored. Hash function is used to compress both the full encrypted message and the encrypted key. The size of a fully encrypted key have 256 bits. Currently, this fully encrypted key is a group key that the group manager has been used to communicate. This group key can be used as an encryption and decryption key by the communication network components when they want to send or receive data from other communication network components.[8].

2.3.2 Rossler Hyper Chaotic System (RHCS)-based encryption of an image

Chaotic encryption systems are used to improve the degree of security in image encryption. One of the most well-known chaotic systems is the Rossler hyper-chaos, which has been proposed by Otto Rossler in 1976 [16]. The differential equations of Rossler hyper-chaotic are given in Eq. (1).

$$\begin{aligned} \frac{dx}{dt} &= -(y + z) \\ \frac{dy}{dt} &= x + \alpha y \\ \frac{dz}{dt} &= \beta + z(x - \gamma) \end{aligned} \tag{1}$$

where α, β and γ are real parameters, called as Rossler parameters and x, y and z are the three variables which evolves with the time. In other words, these variables denote the state of the system at the given time t. The first two equations have linear terms that create oscillations in the variable x and y. The last equation has only one nonlinear term (*zx*) so the expected chaotic behavior is appeared in the system. The values of α, β and γ are first studied by Rössler. When α & β =0.2 and γ =5.7, the attractors (which are a set of states of points in the phase space in dynamics system) of the hyper-chaos are generated by the Runge-Kutta method [16]. The Rossler hyper-chaotic system is used to encrypt the data using the secret key [16-18].

The image encryption and decryption procedures using the Rossler hyper chaotic system are as follows.

In the Rossler hyper chaotic system encryption process, the images are given as input. The values of **Rossler** parameters (α, β and γ) are also fed into the system. The generation of chaotic sequence is done by using **initial** parameters (x_0, y_0 and z_0) which are produced after optimization and Rossler parameters. Then the chaotic sequence is converted into a 2-Dimensional array. The dimension of original image is compared with the chaotic sequence dimension. If the dimensions are equal, pixel replacement of original image is executed by bit-wise XOR operation between the original image and the chaotic sequence *x(i,j)*. Now, pixel shuffling operation is performed with help of sequence *yz* to get encrypted image. In the decryption process, the initial parameters are serving as decryption keys. These parameters must be sent to the receiver in a secure manner. The decryption process is the inverse process of encryption.

2.3.3 Rossler Hyper Chaotic System-based encryption of a signal: The gathered signals are given as input to spectrogram image converter, since it is very difficult to encrypt the signals than the images. The Short-Time Fourier transform (STFT) is employed here as the conversion method. Now, the converted spectrogram image is very easier to encrypt. So, the spectrogram image is given as input to the encryption process. The Flow diagram of the proposed MPBO-RHCS for secure data transfer scheme is shown in Fig.1.

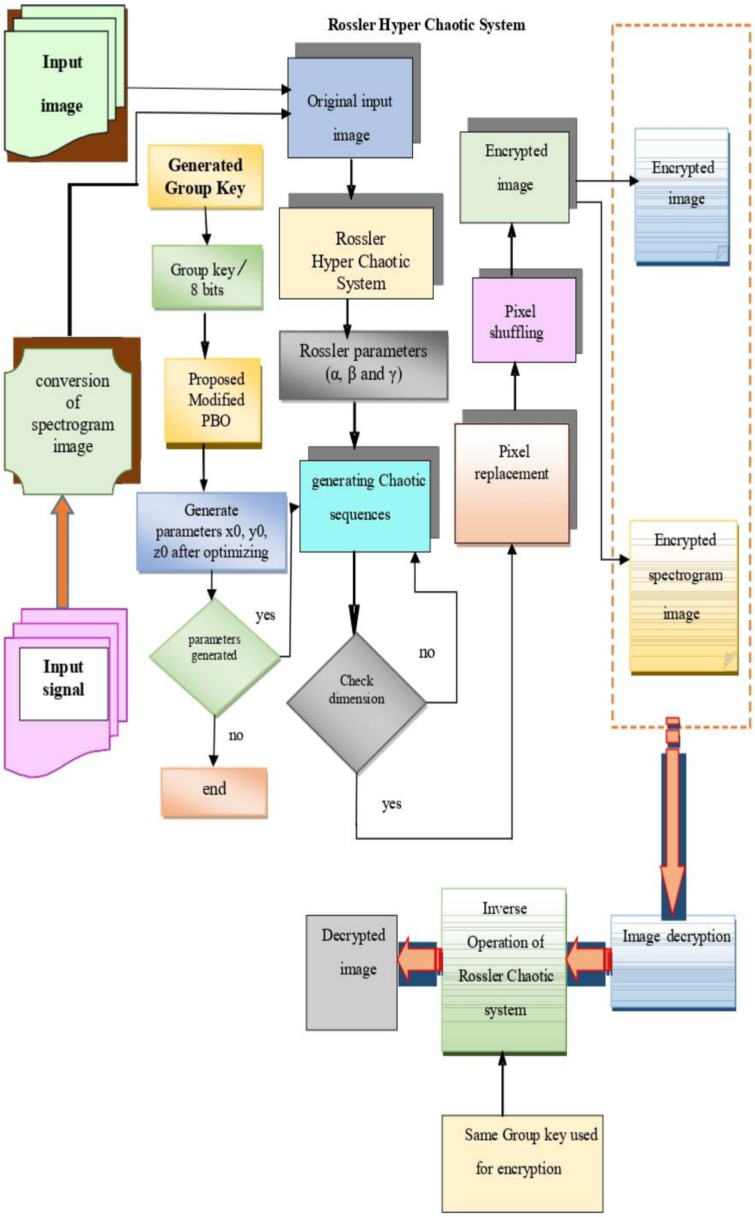

Rossler Hyper Chaotic System
Input image
Original input image
Generated Group Key
Group key / 8 bits
Proposed Modified PBO
Generate parameters x0, y0, z0 after optimizing
parameters generated
yes
no
end
Rossler Hyper Chaotic System
Rossler parameters (α, β and γ)
generating Chaotic sequences
Check dimension
no
yes
Pixel replacement
Pixel shuffling
Encrypted image
Encrypted image
Encrypted spectrogram image
conversion of spectrogram image
Input signal
Image decryption
Inverse Operation of Rossler Chaotic system
Decrypted image
Same Group key used for encryption

Fig.1. Flow diagram of the proposed MPBO-RHCS for secure data transfer scheme

2.4 Polar Bear Optimization (PBO) Algorithm

PBO [19, 20]: Polar Bear Optimization (PBO) is a nature-inspired optimization algorithm designed to mimic the hunting abilities of polar bears in harsh arctic environments. The algorithm consists of three stages in a single algorithm: i) global search, where the polar bear glides ice floats; ii) local search, where the polar bear encircles and catches prey and iii) dynamic population control.

i) Global search: Each polar bear is represented as a point of multiple *n* coordinates, described as X=(x_0,x_1,….,x_{n-1}). The movement of the polar bear towards the fittest individual of X in the whole population at the mth iteration of PBO is given in Eq. (2).

$$\left(X_j^m\right)^{(i)} = \left(X_j^{m-1}\right)^{(i)} + sign(\omega) \ \alpha + \gamma \tag{2}$$

Here, $\left(X_j^{m-1}\right)^{(i)}$ indicates the whole population in the search space, where i denotes the number of polar bears and j denotes the given co-ordinates. The ith polar bear having j coordinates in tth iteration towards the fittest value is noted by $\left(X_j^t\right)^{(i)}$. The term α is a random number in the interval [0, 1], ω is the distance between two spatial coordinates and γ is random value in the range <0, ω>. The term ω = $d\left((X)^{(i)},(X)^{(j)}\right)$ is the distance between two spatial coordinates, measured in Euclidean metric as given in the Eq. (3).

$$\omega = d\left((X)^{(i)},(X)^{(j)}\right) = \sqrt{\sum_{k=0}^{n-1}\left((x_k)^{(i)}-(x_k)^{(j)}\right)^2} \tag{3}$$

Here, the terms $(X)^{(i)}$and $(X)^{(j)}$ are the spatial coordinates of the two points. In the iteration of the motion model, a global search is carried out for each individual, but positions are only updated when better places are found. All bears that are actively hunting and they modeled the world's march towards the fittest person.

ii) Local search: After getting the position of the prey, every polar bear march towards the prey. The bear softly approaches potential prey to determine the best position. It moves as quickly as it can to capture the prey when it gets close enough to attack. Normally the prey prefer to stay on the ice most of the time. If the prey senses any threat, it will dive into the water. The polar bear also immediately jump into the water and try catch the prey. The radius r of the view of a polar bear is given in Eq. (4).

$$r = 4a\cos(\phi_0)\sin(\phi_0) \tag{4}$$

The term *a* is the distance in which polar bear can see the prey, where *a* range from [0, 0.3]. The term (ϕ_0) is the angle subtended when the polar bear jump to the prey range from 0 to π/2.

The movements of a particular individual in the population are measured using Eq. (5).

$$\begin{cases} x_0^{new} = x_0^{actual} \pm r\cos(\phi_1) \\ x_1^{new} = x_1^{actual} \pm \left[r\sin(\phi_1) + r\cos(\phi_2) \right] \\ x_2^{new} = x_2^{actual} \pm \left[r\sin(\phi_1) + r\sin(\phi_2) + r\cos(\phi_3) \right] \\ \quad \cdots \\ x_{n-2}^{new} = x_{n-2}^{actual} \pm \left[\sum_{k=1}^{n-2} r\sin(\phi_k) + r\cos(\phi_{n-1}) \right] \\ x_{n-1}^{new} = x_{n-1}^{actual} \pm \left[\sum_{k=1}^{n-2} r\sin(\phi_k) + r\sin(\phi_{n-1}) \right] \end{cases} \tag{5}$$

Here, the term x_0^{new} denotes the new position of the polar bear and *actual* defines the actual position in the search space. The term ϕ_1 is the random number from 0 to 2π. The polar bear food searching process is validated using $x_1^{actual} \pm$. Polar bear begins to move forward (sign ± is changed to +) and move backward (sign ± is changed to -) in search of food to get into a better attacking posture. The PBO algorithm uses a random leaf location that corresponds to the local search optimization phase to show this circumstance.

iii) Dynamic population control: At the starting of the algorithm, the polar bear population consists of 75% of created individuals and the remaining 25% depends on the population growth. The reproduction process depends on the value K, which is randomly chosen from the range of (0,1). If the population is less than maximum population and K value is greater than 0.75, a new individual is generated by using Eq. (6). If the population is more than the half of the maximum population and K is less than 0.25 then the worst individuals will die.

$$\left(X^t{}_j \right) = \frac{\left(X^t{}_j \right)^{best} + \left(X_j^t \right)^{(i)}}{2} \tag{6}$$

Here, the best individual is indicated by $\left(X_j \right)^{best}$. The termination condition is taken based on the maximum iteration number and it is indicated by t.

2.5 Proposed Modified Polar Bear Optimization (MPBO) Algorithm

While using the original PBO algorithm, its processing time is low then some other optimization algorithms [20]. Hence we can achieve better solution through this proposed Modified Polar Bear Optimization (MPBO) algorithm. In the proposed MPBO algorithm, α in the original PBO global search in Eq. (2) is replaced by the following Eq. (7).

$$\alpha = \frac{\beta}{\lambda} \tag{7}$$

where, β is a random number in the range [0, 1]. λ is a random value in the range [0, ω].

We expect the best and effective performance in the group key-based secure data transfer scheme due to the MPBO.

The pseudo-code of the proposed MPBO is given in the Algorithm1.

Algorithm 1: Implementing MPBO

```
Set the space solution, population size, iteration t and distance
Evaluate the fitness function f
Determine the random parameters , i=0
    While $(i \leq t)$
        For each bear in a population
            Update the $\alpha$ random parameter  using the fittest concept
            Determine the new updated location
            Evaluate the radius
            If $(new < actual)$
                Evaluate the bear movement
            Sort the polar bear initial values
            Evaluate the fitness function
            If(K >0.75)
                Calculate the reproduction
            Else
                Determine the worst individuals
            End if
            End if
        End For
        Find the best polar bear individual solution
    End while
    Return the parameters
End
```

During the execution of the proposed MPBO algorithm, number of iterations 50, number of optimization parameters 5 and a population size 10 are given as input values.

2.6 Implementation

MatlabR2020a is used to implement the group key-based secure data transfer scheme. First, the proposed model RHCS with MPBO group key-based secure data transfer scheme is executed and the results are found. Second, the RHCS with various other existing optimization algorithms such as Arithmetic Optimization Algorithm (AOA) [21], Tunicate Swarm Algorithm (TSA) [22], Harris Hawks Optimizer (HHO) [23] and PBO [19] are executed and the results are found. From the results, the performance metrics like Mean Square Error (MSE), Number of Pixels Change Rate (NPCR), Peak Signal to Noise Ratio (PSNR), Unified Average Changing Intensity (UACI), Known Plaintext Attack (KPA), Chosen Plain text Attack (CPA) are calculated and tabulated for comparison.

The various other existing chaotic methods such as Henon chaotic map [24], Logistic chaotic map [25], Arnold cat chaotic map [26] and RHCS [16] are executed without any group key optimization and the results are found. From the results the performance metrics are calculated and tabulated for comparison.

The total time taken for execution of a single data (image /signal) secure transfer is known as the total processing time (T) in milliseconds(ms). It is calculated by summing the encryption and decryption times of each data secure transfer. The total amount of memory space, used for a single secure data transfer is known as memory size (M) in bytes.

3. Result and Discussion

3.1 Results of the proposed model

The encrypted images by using proposed MPBO-RHCS model are given in Fig.2. The encrypted signals by using proposed MPBO-RHCS model are given in Fig.3.

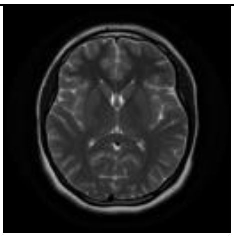
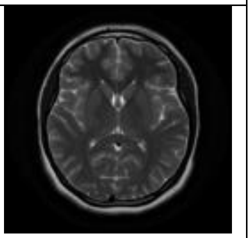
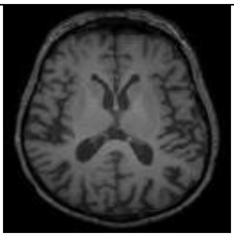
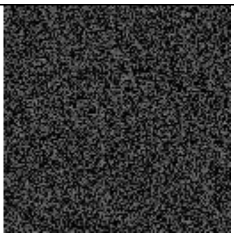
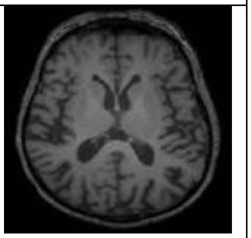
Terms	Images encryption		
Image Sets	Original Images	Encrypted Images	Decrypted Images
Image-1			
Image-2			

Fig.2. Results of the encrypted images using proposed MPBO-RHCS model

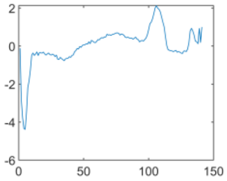
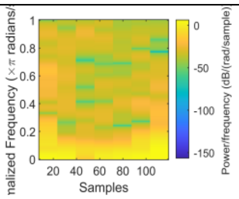
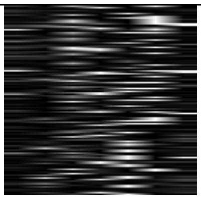
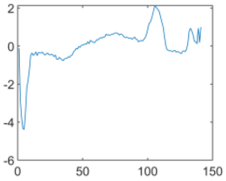
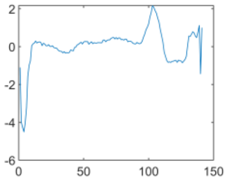
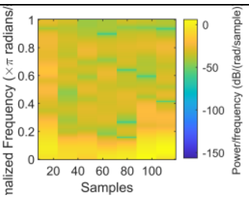
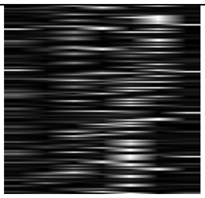
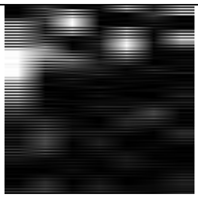
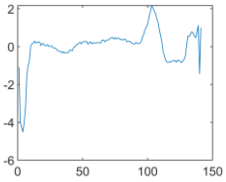
Signal encryption					
Signal Sets	Original signals	Spectrogram Images	Encrypted Images	Decrypted Images	Obtained signals
Image-1					
Image-2					

Fig.3. Results of the encrypted signals using proposed MPBO-RHCS model

3.2 Comparison of performance metrics of the proposed model with other existing optimization algorithms

The results of the proposed MPBO-RHCS group key-based secure data transfer scheme over various existing optimization algorithms with respect to image and signal datasets are shown in Table 1. It is found from the tabular column that the proposed MPBO-RHCS secure data transfer model is the most effective algorithm when it is compared to other existing optimization algorithms.

Table.1. Comparison between performance metrics of the proposed MPBO-RHCS and that of other existing optimization algorithms

Terms	AOA-RHCS [21]	TSA-RHCS [22]	HHO-RHCS [23]	PBO-RHCS [19]	Proposed MPBO-RHCS
Image					
MSE	2036.5	2128.5	1814.6	1942.6	1527.2
NPCR	99.667	99.343	99.721	99.047	99.86
PSNR	15.042	14.85	15.543	15.247	16.292
UACI	33.155	33.898	33.045	33.925	33.974
Encryption Time(ms)	17.373	17.566	16.899	17.181	16.616
Decryption Time(ms)	0.14461	0.15387	0.10469	0.11542	0.10127
Total Processing Time(ms)	17.518	17.72	17.004	17.297	16.717
Memory Size(bytes)	3.8851x10^{+07}	3.0118 x10^{+07}	2.5395 x10^{+07}	2.3478 x10^{+07}	2.0586 x10^{+07}
Signal					
MSE	0.20219	0.41875	0.2916	0.21038	0.18107
NPCR	99.382	99.612	99.357	99.489	99.69
PSNR	6.9423	3.7805	5.3522	6.77	7.4216
UACI	33.552	33.635	33.528	33.13	33.82
Encryption Time(ms)	6.3873	6.5531	5.9402	6.124	5.7255
Decryption Time(ms)	1.1257	1.0611	0.96296	0.95457	0.93378
Total Processing Time(ms)	7.5129	7.6142	6.9031	7.0785	6.6593
Memory Size(bytes)	9.7243x10^{07}	6.5892x10^{07}	6.1497 x10^{07}	6.2333 x10^{07}	5.7639 x10^{07}

3.3 Comparison of performance metrics of the proposed model with other existing chaotic methods

The results of the proposed MPBO-RHCS group key-based secure data transfer scheme over various existing chaotic methods with respect to image and signal datasets are shown in Table 2. It is found from the tabular column that the proposed MPBO-RHCS secure data transfer model is the most effective algorithm when it is compared to other existing chaotic methods.

Table.2. Comparison between performance metrics of the proposed MPBO-RHCS and that of other existing chaotic methods

Terms	Henon chaotic map [24]	Logistic chaotic map [25]	Arnold cat chaotic map [26]	Rossler RHCS [16]	Proposed MPBO-RHCS
Image					
MSE	2108.5	2007.5	2128.5	2043.7	1527.2
NPCR	99.438	99.695	99.485	99.792	99.86
PSNR	15.85	13.85	14.85	15.627	16.292

UACI	33.882	33.579	33.374	34.021	33.974
Encryption Time(ms)	17.454	17.224	17.46	17.694	16.616
Decryption Time(ms)	1.0118	0.46823	0.38721	0.2757	0.10127
Total Processing Time(ms)	18.466	17.693	17.848	17.97	16.717
Memory Size(bytes)	$2.8851x10^{+07}$	$2.7210 x10^{+07}$	$3.0051 x10^{+07}$	$3.9003 x10^{+07}$	$2.0586 x10^{+07}$
Signal					
MSE	0.20013	0.21013	0.20193	0.42398	0.18107
NPCR	99.457	99.651	99.323	99.623	99.69
PSNR	6.7079	6.9479	6.5439	6.9962	7.4216
UACI	33.401	33.306	33.281	33.377	33.82
Encryption Time(ms)	7.2029	6.0783	6.125	6.5749	5.7255
Decryption Time(ms)	1.9459	1.8894	1.4839	1.7436	0.93378
Total Processing Time(ms)	9.1488	7.9677	7.6088	8.3185	6.6593
Memory Size(bytes)	$8.7243 x10^{07}$	$6.7639 x10^{07}$	$7.1497 x10^{07}$	$9.8333 x10^{07}$	$5.7639 x10^{07}$

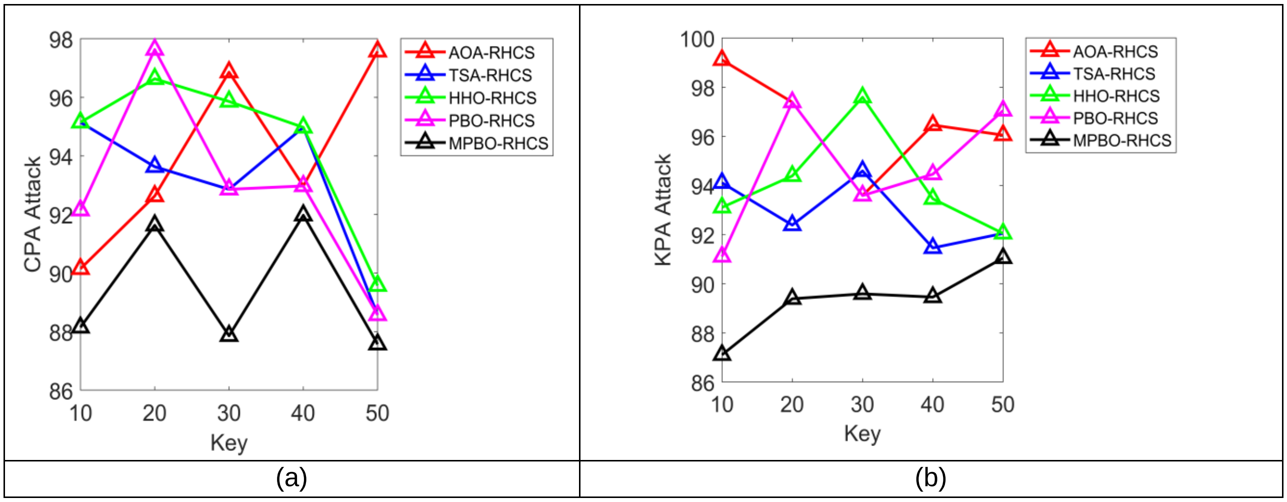
3.4 Comparison of performance analysis of the proposed model with various other existing optimization algorithms

3.4.1 For an image:

The effectiveness of the proposed MPBO-RHCS-based secure data transfer scheme is compared to the existing optimization algorithms for an image.

a) CPA attack and KPA attack:

The CPA and KPA analysis of the proposed MPBO-RHCS-based secure data transfer scheme are shown in Fig.4 (a) and Fig.4 (b). The CPA and KPA value of proposed MPBO-RHCS is lower than AOA, TSA, HHO and PBO.

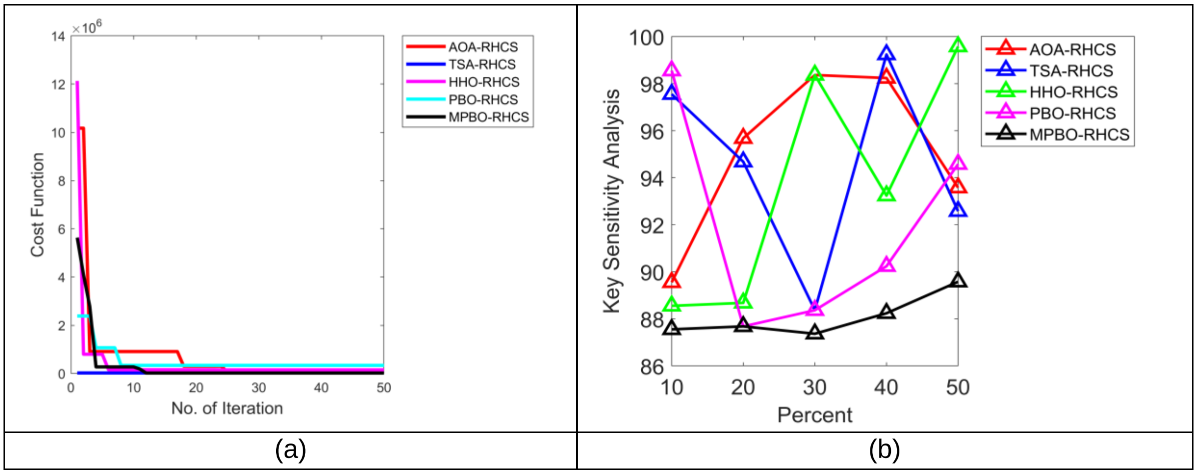


(a) (b)

Fig.4. (a) CPA attack (b) KPA attack

b) Convergence analysis and Key sensitivity analysis: The convergence analysis and Key sensitivity analysis of the proposed MPBO-RHCS-based secure data transfer scheme is shown in

Fig.5 (a) and (b). The convergence analysis and Key sensitivity analysis of proposed MPBO-RHCS is less than AOA, TSA, HHO and PBO.



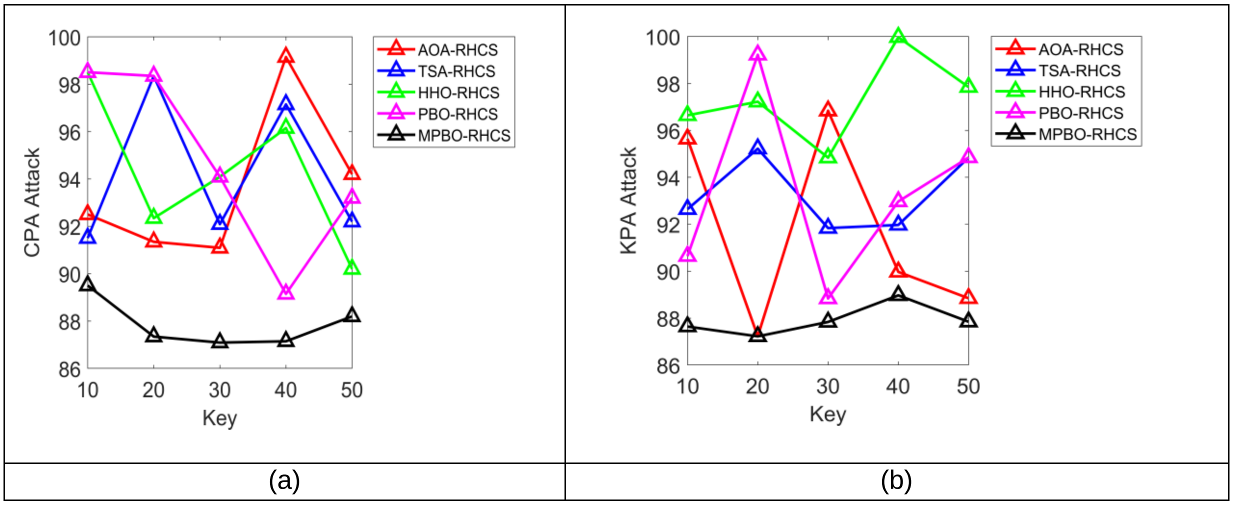
(a) (b)

Fig.5. (a) convergence analysis (b) Key sensitivity analysis

3.4.2 For a signal:

The effectiveness of the proposed MPBO-RHCS-based secure data transfer scheme is compared to the existing optimization algorithms for a signal.

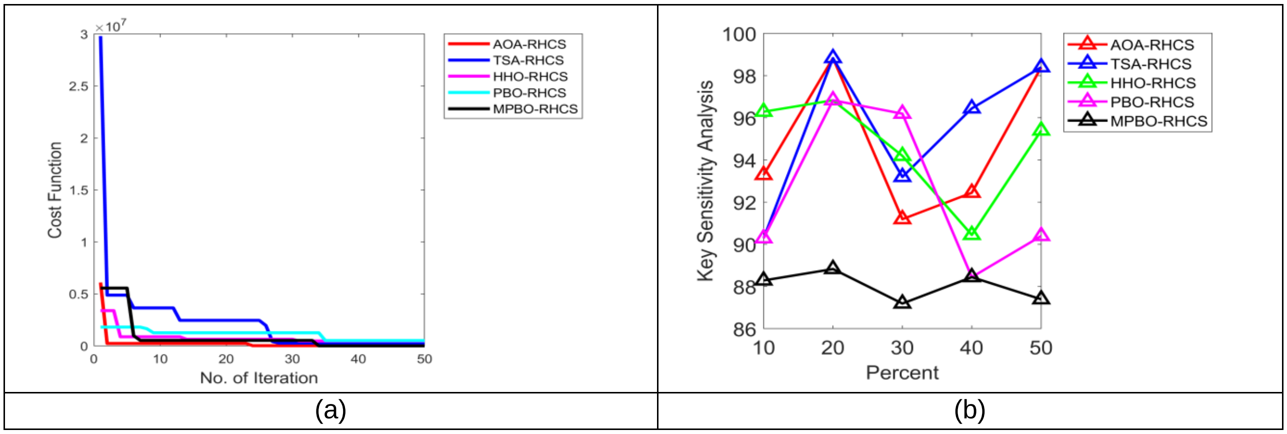
a) CPA attack and KPA attack: The CPA and KPA analysis of the proposed MPBO-RHCS-based secure data transfer scheme is shown in Fig.6 (a) and (b) The CPA and KPA value of proposed MPBO-RHCS is lower than AOA, TSA, HHO and PBO.



(a) (b)

Fig.6. (a) CPA attack (b)KPA attack

b) Convergence analysis and Key sensitivity analysis: The convergence analysis and Key sensitivity analysis of the proposed MPBO-RHCS-based secure data transfer scheme is shown in Fig.7 (a) and (b). The convergence analysis and Key sensitivity analysis of proposed MPBO-RHCS is lower than AOA, TSA, HHO and PBO.



(a) (b)

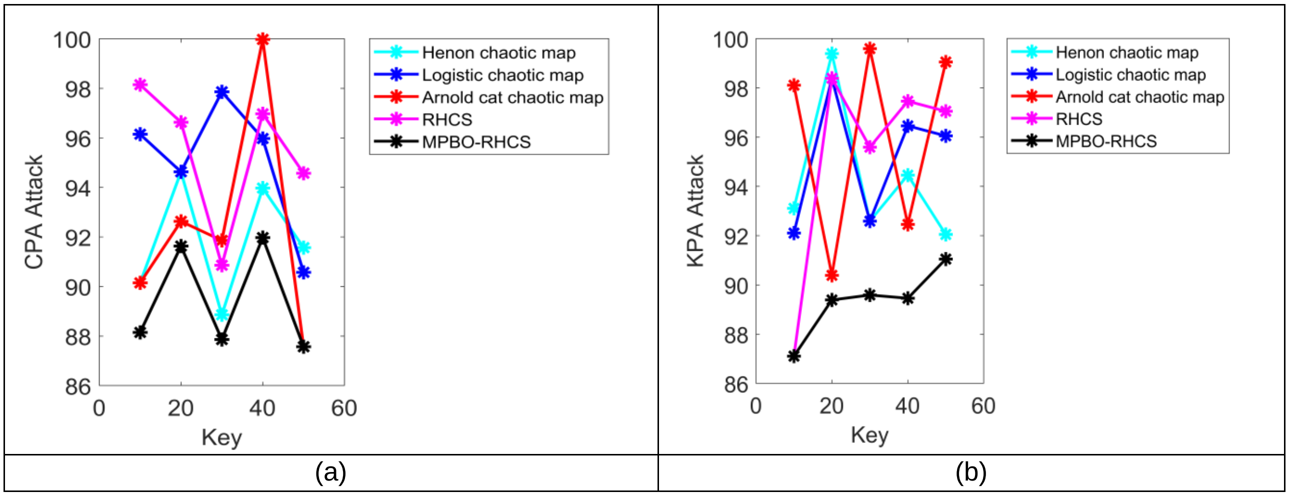
Fig.7. (a) convergence analysis (b) key sensitivity analysis

3.5 Comparison of performance analysis of the proposed model with other existing chaotic methods

3.5.1 For an image:

The effectiveness of the proposed MPBO-RHCS-based secure data transfer scheme is compared to the existing chaotic methods for an image.

a) **CPA attack and KPA attack**: The CPA and KPA attack analysis of the proposed MPBO-RHCS-based secure data transfer scheme is shown in Fig.8 (a) and (b). The CPA value of MPBO-RHCS is lower than Henon chaotic map, Logistic chaotic map, Arnold cat chaotic map and RHCS.



(a) (b)

Fig.8. (a) CPA attack (b) KPA attack

b) **Key sensitivity analysis:** Fig.9.shows the key sensitivity analysis of the proposed MPBO-RHCS-based secure data transfer scheme. The key sensitivity value of the proposed MPBO-RHCS is less than the Henon chaotic map, Logistic chaotic map, Arnold cat chaotic map and RHCS.

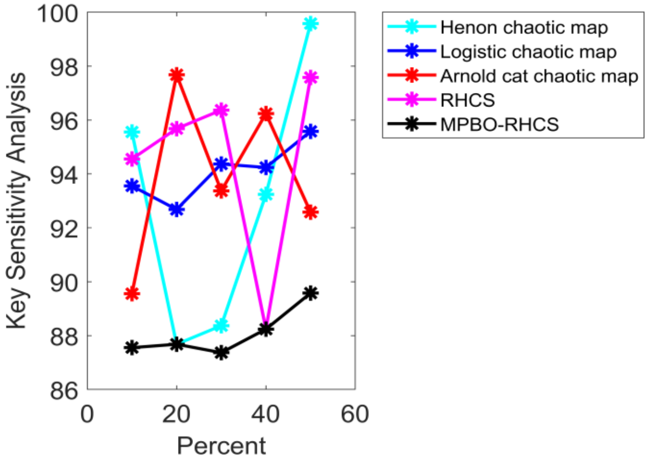
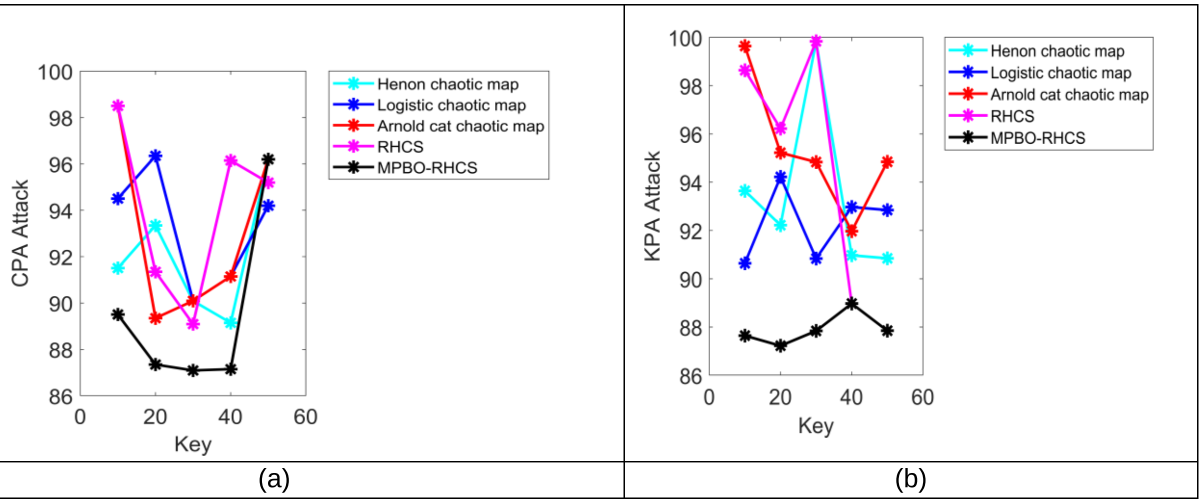


Fig.9. Key sensitivity analysis

3.5.2 For a signal:

The effectiveness of the proposed MPBO-RHCS-based secure data transfer scheme is compared to the existing chaotic methods for a signal.

a) **CPA and KPA attack**: The CPA and KPA analysis of the proposed MPBO-RHCS-based secure data transfer scheme is shown in Fig.10 (a) and (b). The CPA value of MPBO-RHCS is lower than Henon chaotic map, Logistic chaotic map, Arnold cat chaotic map and RHCS.



(a) (b)

Fig.10. (a) CPA attack (b) KPA attack

b) **Key sensitivity analysis:** Fig.11.shows the key sensitivity analysis of the proposed MPBO-RHCS-based secure data transfer scheme. The key sensitivity value of the proposed MPBO-RHCS is less than the Henon chaotic map, Logistic chaotic map, Arnold cat chaotic map and RHCS.

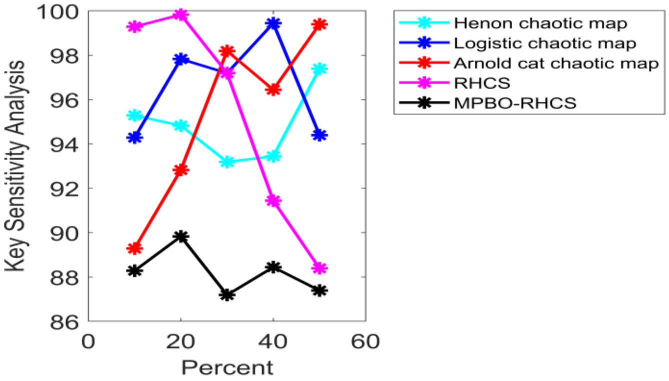


Fig.11. Key sensitivity analysis

4. Conclusion

Our proposed Modified Polar Bear Optimization-Rossler Hyper Chaotic System (MPBO-RHCS) group key-based secure data transfer scheme is used for securing patient's data and effectively transfer them in IoMT (It is executed in the local system cloud storage). It has been used to prevent unauthorized access. The inputs like images and signals have been gathered from the Internet. The gathered images have been given as input to the encryption section. The RHCS-based algorithm has been used to encrypt the images. The initial parameters, given to the RHCS have been optimized using the proposed MPBO algorithm to minimize the processing time and memory size. From the gathered signals, the spectrogram images have been extracted. Then, the extracted spectrogram images have been given to the RHCS-based encryption by using proposed MPBO-RHCS to secure the data. This secured data has been transmitted in IoMT.

The processing time of the proposed MPBO-RHCS of an image when it is compared to other existing optimization algorithms is 4.79% less than AOA, 5.99 % less than TSA, 1.71% less than HHO and 3.46 % less than PBO. The memory size of the proposed MPBO-RHCS of an image is 88.65% less than AOA, 46.31 % less than TSA, 23.35% less than HHO and 14.05 % less than PBO. The processing time of the proposed MPBO-RHCS of a signal when it is compared to other existing optimization algorithms is 12.80% less than AOA, 14.31% less than TSA, 3.66% less than HHO and 6.29 % less than PBO. The memory size of the proposed MPBO-RHCS of a signal is 68.74% less than AOA, 14.32 % less than TSA, 6.69% less than HHO and 8.14% less than PBO.

The processing time of the proposed MPBO-RHCS of an image when it is compared to other existing chaotic methods is 10.45% less than Henon chaotic map, 5.82% less than Logistic chaotic map, 6.76% less than Arnold cat chaotic map and 7.48% less than RHCS. The memory space of the proposed MPBO-RHCS of an image when it is compared to various existing chaotic methods is 40.14% less than Henon chaotic map, 32.15 % less than Logistic chaotic map, 45.96% less than Arnold cat chaotic map and 89.50 % less than existing RHCS. The processing time of the proposed MPBO-RHCS of a signal when it is compared to various existing chaotic methods is 37.33% less than Henon chaotic map, 19.64% less than Logistic chaotic map, 14.24% less than Arnold cat chaotic map and 24.84% less than RHCS. The memory space of the proposed MPBO-RHCS of a signal when it is compared to various existing chaotic methods is 51.43% less than Henon chaotic map, 17.34 % less than Logistic chaotic map, 24.03% less than Arnold cat chaotic map and 70.58 % less than existing RHCS.

In the performance analysis, the important performance metrics for an image encryption process such as MSE, NPCR, PSNR, UACI, Encryption and Decryption time values for the proposed MPBO-RHCS system is found to be better than the other existing optimization algorithms such as AOA, TSA, HHO and PBO. It is also found to be better than the other existing chaotic methods such as Henon chaotic map, Logistic Chaotic map, Arnold cat chaotic map and RHCS. Again, the proposed MPBO-RHCS performance analysis (like CPA Attack, KPA Attack, Convergence analysis and Key Sensitivity analysis) results are found to be better than that for the other existing optimization algorithms and chaotic methods.

Hence, it is observed that the performance of the proposed MPBO-RHCS group key-based secure data transfer scheme has taken less processing time and occupies less memory size than that for the other existing optimization algorithms and chaotic methods. In future, the robustness of our proposed scheme may be improved by using hybrid optimization encryption techniques.

Acknowledgements

We would like to express our special thanks to Dr.K.S.Easwarakumar, Professor, Department of Computer Science, Anna University CEG campus, Chennai for useful discussions, his interest and encouragement. The first author (SB) is very grateful to “**Baby-Perumal Research Institute**” at Chennai for research guidance and supporting us with computing facilities.

References

1. Nimra Dilawar et al., “Blockchain: Securing Internet of Medical Things (IoMT)”, *International Journal of Advanced Computer Science and Applications*, Vol.10 No. 1, pp. 82-89, 2019. Available from: 10.14569/IJACSA.2019.0100110
2. Jalel Ktari et al., “IoMT-Based Platform for E-Health Monitoring Based on the Blockchain”, *Electronics*, vol. 11:2314, pp.1-19, 2022.
   Available from: https://doi.org/10.3390/electronics11152314
3. Nipuni Nanayakkara, Malka N. Halgamuge and Ali Syed, “Security and Privacy of Internet of Medical Things (Iomt) Based Healthcare Applications: A Review”, *International conference on Advances in Business Management and Information Technology*, 2019.
4. Zarlish Ashfaq et al., “A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem”, *Ain Shams Engineering Journal*, Vol.13, No.4, pp.101660, 2022.
   Available from: https://doi.org/10.1016/j.asej.2021.101660
5. Shilan S. Hameed et al., "A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches”, *Peer Jcomputer science*, vol.7, 2021. Available from: 10.7717/peerj-cs.414
6. Yingnan Sun, Frank P.-W.Lo and Benny Lo, “Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey”, *IEEE Access*, Vol.7, pp.183339-183355, 2019. Available from: 10.1109/ACCESS.2019.2960617
7. Zhang Qikun et al., “Group Key Agreement Protocol Based on Privacy Protection and Attribute Authentication”, *IEEE Access*, Vol.7, pp.87085-87096, 2019.
   Available from: 10.1109/ACCESS.2019.2926404
8. S. Bhuvaneswari and T. PramanandaPerumal, “Secure Group Key Management for Group Communication in IoMT Environment with Dual Encryption Scheme”, *Scandinavian Journal of Information Systems*, Vol.35, No.1, pp. 616–627, 2023.
   Available from: http://sjisscandinavian-iris.com/index.php/sjis/article/view/359.
9. M. Sumathi and S. Sangeetha, “A group-key-based sensitive attribute protection in cloud storage using modifed random Fibonacci cryptography”, *Complex & Intelligent Systems*, Vol. 7, pp.1733–1747, 2021.
   Available from: https://doi.org/10.1007/s40747-020-00162-3

10. Arun Mailerum Perumal and Edward Rajan Samuel Nadar, “Architectural framework of a group key management system for enhancing e-healthcare data security”, *Healthcare Technology Letters*, Vol. 7, No.1, pp.13–17, 2020.
    Available from: 10.1049/htl.2018.5114
11. Manish Gupta et al., “An Intelligent Session Key-Based Hybrid Lightweight Image Encryption Algorithm Using Logistic-Tent Map and Crossover Operator for Internet of Multimedia Things”, *Wireless Personal Communications*, Vol.121, No.3, pp.1-22, 2021.
    Available from: 10.1007/s11277-021-08742-3
12. Chingfang Hsu et al., “Fast and Lightweight Authenticated Group Key Agreement Realizing Privacy Protection for Resource-Constrained IoMT”, *Wireless Personal Communications*, Vol.129, No.4, pp.2403-2417, 2023.
    Available from: https://doi.org/10.1007/s11277-023-10239-0
13. Tian-Fu Lee, Xiucai Ye and Syuan-Han Lin, “Anonymous Dynamic Group Authenticated Key Agreements Using Physical Unclonable Functions for Internet of Medical Things”, *IEEE Internet of Things Journal*, Vol. 9, No.16, pp. 15336-15348, 2022.
    Available from: 10.1109/jiot.2022.3149117
14. Ranjeeta Pandhare and Swatee S. Nikam, “Security of IoMT healthcare data using cryptographic techniques”, *International Journal of Advanced Trends in Computer Science and Engineering*, Vol.10, No.1, pp. 372-377, 2021.
    Available from: 10.30534/ijatcse/2021/531012021
15. Muhammad Adil et al., “An AI-enabled Hybrid lightweight Authentication Scheme for Intelligent IoMT based Cyber-Physical Systems”, *IEEE Transactions on Network Science and Engineering*, 2022.
    Available from: 10.1109/TNSE.2022.3159526
16. Wei Huang et al., “A Novel Double-Image Encryption Algorithm Based on Rossler Hyperchaotic System and Compressive Sensing”, *IEEE Access*, Vol.9, pp.41704-41716, 2021.
    Available from: 10.1109/ACCESS.2021.3065453
17. Mrinal K.Mandal et al., “Symmetric key image encryption using chaotic Rosslersystem”, *Security and Communication Networks*, Vol. 7, No.11, pp.2145-2152, 2014.
    Available from: 10.1002/sec.927
18. Yasir Ahmed Hamza and Marwan Dahar Omer, “An Efficient Method of Image Encryption Using Rossler Chaotic System”, *Academic Journal of Nawroz University (AJNU)*, Vol.10, No.2, pp.11-22, 2021.
    Available from: 10.25007/ajnuv10n2a916
19. Dawid Połap and Marcin Wo ´zniak, “Polar Bear Optimization Algorithm: Meta-Heuristic with Fast Population Movement and Dynamic Birth and Death Mechanism”, *Symmetry*, Vol.9, pp.203, 2017.
    Available from: https://doi.org/10.3390/sym9100203
20. Saqib Fayyaz et al., “Solution of Combined Economic Emission Dispatch Problem Using Improved and Chaotic Population-Based Polar Bear Optimization Algorithm”, *IEEE Access*, Vol.9, pp.56152-56167, 2021.
    Availablefrom:10.1109/ACCESS.2021.3072012
21. Manoharan Premkumar et al., “A New Arithmetic Optimization Algorithm for Solving Real-World Multiobjective CEC-2021 Constrained Optimization Problems: Diversity Analysis and Validations”, *IEEEAccess*, Vol.9, pp.84263-84295, 2021.
    Availablefrom: 10.1109/ACCESS.2021.3085529
22. Amirbahador Arabali et al., “An Adaptive Tunicate Swarm Algorithm for Optimization of Shallow Foundation”, *IEEE Access*, Vol.10, pp. 39204-39219, 2022.
    Available from:10.1109/ACCESS.2022.3164734

23. Ranya Al-Wajih et al., “Hybrid Binary Grey Wolf with Harris Hawks Optimizer for Feature Selection”, *IEEE Access*, Vol. 9, pp.31662-31677, 2021.
Available from:10.1109/ACCESS.2021.3060096
24. Lisungu Oteko Tresor and Mbuyu Sumbwanyambe, “A Selective Image Encryption Scheme Based on 2D DWT, Henon Map and 4D Qi Hyper-Chaos”, *IEEE Access*, Vol.7,pp.103463-103472,2019. Available from: 10.1109/ACCESS.2019.2929244
25. Hegui Zhu, Yiran Zhao and Yujia Song, “2D Logistic-Modulated-Sine-Coupling-Logistic Chaotic Map for Image Encryption”, *IEEE Access*, Vol.7, pp.14081-14098,2019.
Available from: 10.1109/ACCESS.2019.2893538
26. Carlos E. C. Souza, Daniel P. B. Chaves and Cecilio Pimentel, “One-Dimensional Pseudo-chaotic Sequences Based on the Discrete Arnold’s Cat Map Over Z3m”, *IEEE Transactions on Circuits and SystemsII: ExpressBriefs*, Vol.68,No.1,pp.491-495,2021.
Availablefrom:10.1109/TCSII.2020.3010477.