Multimodal Medical Imaging Security using Hybridization of Honey Encryption Algorithm with Binary Particle Swarm Optimization

Jayahari Prabhu G[a], and Perumal B[b]

[a,b]
Department of ECE, Kalasalingam Academy of Research and Education,
Virudhunagar, Tamil Nadu, India. jayahariprabhu@gmail.com,
palanimet@gmail.com

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28April 2021

Abstract: Transmitting and receiving information through any network requires some sort of security. One of the major application requires data security is Medical Imaging System. Especially, for owning any significant information about patient details. This Medical Imaging System does the operation of encryption and decryption, for which the security key has been built to protect information using numerous cryptographic algorithms. Choosing an algorithm for secured information correspondence, to attain quality parameters such as higher privacy, confidentiality, integrity and effectiveness. This work proposed by hybridization of Honey Encryption Algorithm with Binary Particle Swarm Optimization to scramble the restorative medical data. Comparatively, this proposed algorithm reduces the Mean Square Error (MSE) to 1% and increased the Peak Signal to Noise Ratio (PSNR) value to 98.7%. The subsequent operation is performed using Binary particle swarm optimization for overhauling the keys.

Keywords: Medical Imaging data, Honey Encryption, Particle Swarm Optimization, Image Security, encryption and Decryption

1. Introduction

With the improvement of medical imaging technique, Security is a basic requirement for all applications to protect the stored data and to transmit over a network [1]. The Internet will trade in medical imaging techniques and digital image applications with extensive changes in connectivity and technology. Digital images play nominal role in day today's communication. Whereas, the encryption technique for security is a process to convert data in an unreadable format by unauthorized users using cryptographic algorithms to preserve data. The better algorithms will meet the requirements of the security, to protect the encryption components. The best part of simple encryption calculations is used as content details or matched data [2].

This information on cryptographic algorithms can be used to provide various security methods, such as privacy, validation, uprightness and authorization. there are standard ciphers such as AES, DES and RSA cannot be used for medical image security optimization [3]. The widely used optimization algorithms like Grasshopper Optimization (GO), Blowfish optimization and Signcryption Optimization algorithms has the disadvantage in the primary ciphers, which require higher system power and computational time. The hybridization of HE with BPSO is performed to attain the optimization of keys, using the primary parameter "PSNR" [4].

It is important to ensure the value of encryption for medical information. [5]. The proposed work is on hybridizing the HE algorithm with BPSO for Medical security. It is used to keep sensitive data more secure and it will be tedious for unauthorized users to access. Using symmetric and asymmetric key encryption scheme to classify a restorative medical image to any unintelligible configuration, this cryptographically based protection helps to offer the required security data or information.

Some existing algorithms do not handle all optimization issues, even though most of them could take care of a variety of problems [6]. Here we proposed hybridizing the HE Algorithm with BPSO technique. The data about the efficient image encryption security is supplied with authentication. The proposed work focuses on hybridizing an encryption technique that could easily handle certain issues, with an optimization technique [7]. Section II explains related work, section III explains the methodology, followed by which the result of the proposed work is explained in section IV. This proposed work is concluded with Performance analysis.

2. Related Work

In 2019, Shankar et al [8] proposed an insertion of self-recovery bits is measured by means of Transformation of Arnold, which restores the original image even after a high rate of tampering. Watermarking SVD-based Knowledge enhances image authentication and offers a way to identify various areas of the watermarked image that have been targeted. The suggested framework is checked against different attacks.

In 2019, Hussaini et al [9] proposed the storage of data (e.g. images, videos, audio and so on). Due to the inevitable dishonour of abundant mobile devices and cloud computing, in the cloud has become a trend among separable and categorised customers. Regardless, cloud service providers cannot be completely trusted to ensure the availability or confidentiality of consumer data re-appropriated/transferred to the cloud. To enhance the cybersecurity of cloud data, a new security model is introduced, along with optimal key selection. The hidden data collected using the K-Mediod clustering algorithm based on a calculation of data distance is the first cluster in the proposed study. Then, using Blowfish Encryption (BE), the clustered data is encrypted and stored in the cloud.

In 2018, Nematzade et al [10] proposed The goal is to propose a method of medical image encryption based on the modified genetic algorithm hybrid model. Next, The MGA applies both to improve the Cipher-image entropy and to lower the algorithm's computational time. On computers, experimental results and simulations Both show that not only does the suggested hybrid algorithm solution perform excellent encryption, but it can also withstand a number of conventional attacks. MGA and map coupling lattices. First, in the proposed technique, coupled map lattice is used to produce the number of stable cipher images as an initial MGA population.

In 2017, Vengadapurvaja et al [11] proposed The Health Information Technology for Economic and Clinical Health (HITECH) Act encourages the use of technology for health information. Electronic Wellness Reports. EHR enhances accessibility of data, facilitates computerised data updating and enables e-messaging.

In 2020, Ji, B et al [12] proposed It's between providers. For health care units, cloud computing includes various resources, and the data is stored in the cloud. Feature selection is an effective strategy to minimise the number of data features that increase the efficiency of classification in machine learning. In this paper, we formulate a common problem of function selection to reduce the number of selected features, thereby improving accuracy. A better one to fix the problem, the binary particle swarm optimization (IBPSO) algorithm is suggested.

In 2020, Ayeni et al [13] proposed DNN Optimization of Particle Swarm (PSO) aided process to improve the accuracy of heart disease diagnosis, which is suggested to be very nuanced in healthcare practices. The purpose of this research is to improve the accuracy of diagnosis Heart sickness. A conceptual structure for CAD heart research Disease was created with the overall aim of enhancing human health.

3 .Methodology

For the research work, source of data, the multimodel medical image security is identified. it is therefore necessary to preserve the data. and protection of the multimodel medical image is interpreted in the block diagram shown in Fig.1 [14].The Fig.1 shows the conceptual prototype. And its starts collecting multimodel medical image, it undergo data processing. where the data is being pre-processed, then it proceeds to the Proposed HE in combination with Binary Particle Swarm Optimization (HE-BPSO).Here the reconstruction takes place by decrypting the original image [15].

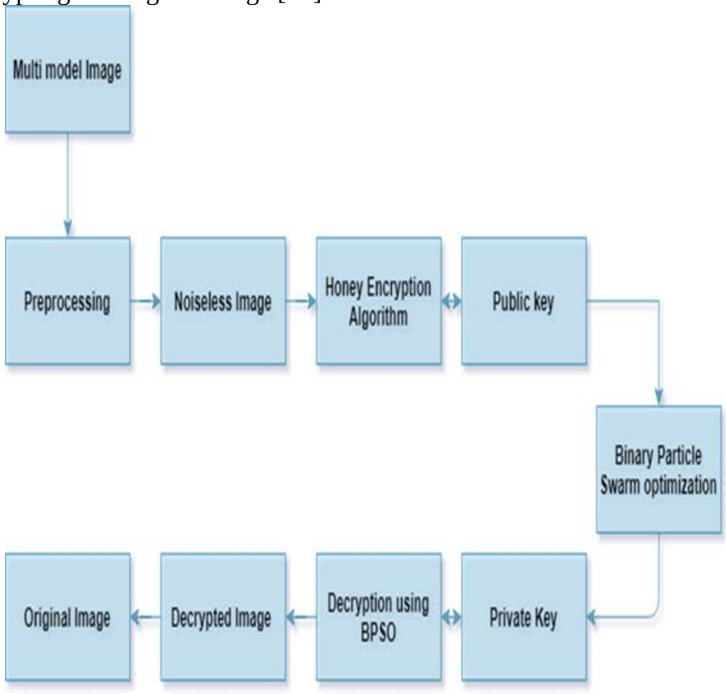


Fig.1 Block diagram for Proposed HE-BPSO.

The issue of data encryption for medical image protection prompted us to introduce the HE algorithm. HE frequently denotes a false resource in medical safety intended to attract or trick an intruder. HE safeguards a selection of information that has some common features. The message space is assumed to be a set of data. We should decide the possible message space prior to encrypting a message. You can map a message to several seeds and the seed is randomly chosen.

3.1 MULTIMODEL MEDICAL TRANSMISSION USING HE

Let us consider HE to encrypt the input medical images, as shown in Figure.2. The input medical image consists of multimodal images collected from the brain web and ADNI dataset These datasets input images are arranged alphabetically. Let us assume that 2/8 of the first input image, 2/8 of the second image, 3/8 of the third image and 1/8 of the fourth image has the image space. A 3-digit space is the seed space. We use DTE to map these image spaces in the seed space according to these probability statistics. From the corresponding seed set, the DTE randomly selects a seed. The cipher text is generated by XORed the seed with the HE-BPSO. To obtain the seed, the cypher text is XORed with the BPSO during decryption. The DTE then maps the seed inversely to the original reconstructed images shown in Fig.2 However, since we sort plain image, we therefore construct an inverse table consisting of cumulative probability mappings to the plain image. By locating the seed, we can determine the range of potential seeds. By determining the seed range, we can measure the cumulative possibility shared by the seed range and the plain image.

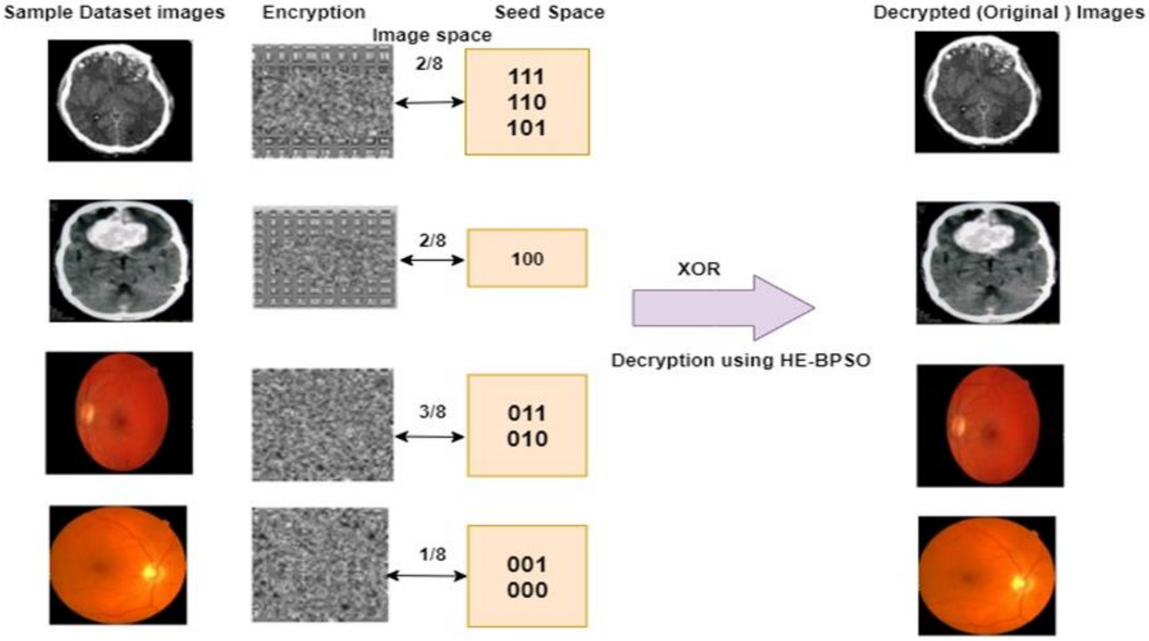


Fig.2 Graphical model for proposed HE-BPSO

3.2 KEY GENERATION STAGE

BPSO (Binary Particle Swarm Optimization) is an optimization method that uses evolutionary computation. It is based on swarm theory and social behaviour of birds gathering or fish swarming. This algorithm works by keeping some of the solutions in the search space at the same time. Initially, like HE with BPSO is initialized with a population of random solutions in the search space. BPSO is Only the knowledge about the fitness values of the particles. Key generation involves the selection of parameters and the development of private and public keys, the additional process is also performed with HE in the public key cryptosystem. There are four functions performed from key generation to decryption [16]. Honey produces the same result for the first one by performing decryption of the medical or honey data. The BPSO makes use of random keys for decryption and encryption purposes [6].

```
For BPSO
Initialize the Swarm
 Find the fitness of each search agent
End
   If the fitness value is better than its personal best
   Update the best search agent
For each particle swarm
      Calculate particle velocity
         Update particle position
End
```

3.3 INITIALIZATION PROCESS

When the key is generated, prime numbers are taken into account to decide the size of the particle swarm. And the following equation is used as the input solution.

$Input\ solution = \{s1, s2, s3, \dots S_n\}$ (1)

3.3.1 OBJECTIVE FUNCTION OF KEY SELECTION

With HE and BPSO, the objective feature for key selection is optimized. To scramble and unscramble data from a medical image, the key selection method uses the ‘fitness function' as the maximum key with the highest Peak Signal to Noise ratio. And it's exemplified by the following situation:

$\text{Fitness} = \text{MAX}\{\text{PSNR}\}$ (2)

3.4 BINARY PARTICLE SWARM OPTIMIZATION

The velocity and new refreshed solutions are evaluated for HE key selection using key parameters such as the global best (G-best) and particle best (P-best) in this PSO.

3.4.1 VELOCITY AND POSITION UPDATION

The BPSO is regarded as the G best and P best attribute among fitness values. After the iteration, P best is chosen as the current fitness value, and G best is chosen as the overall best fitness value. The velocity vector of a particle is updated based on the best G and P values. The following is the formula for updating velocity and position.

$$Vi(t+1) = vi(t) + g1 * r * \left(p_{best(t)} - ni(t)\right) + g2 * r * \left(G_{best_{(t)}} - ni_{(t)}\right) \quad (3)$$

$$Ni(t+1) = ri(t) + v(t+1) \quad (4)$$

The particle velocity is Vi; the current particle is Ri; and rand is an arbitrary number between 0 and 1. Ith particle position coordinates the situation of global best arrangement and location best arrangement.

3.5 PROPOSED OPTIMIZATION (HE-BPSO) FOR SECURITY

Encryption is the method of translating information for security purposes. During the transmission, security issues such as key management and other security issue was identified, it is therefore necessary to preserve the data and protection of the medical image is interpreted in the block diagram shown in Fig.1 [17]. Flow chart of HE and ALO is shown in Fig.3 By initialize the swarm velocity and position.

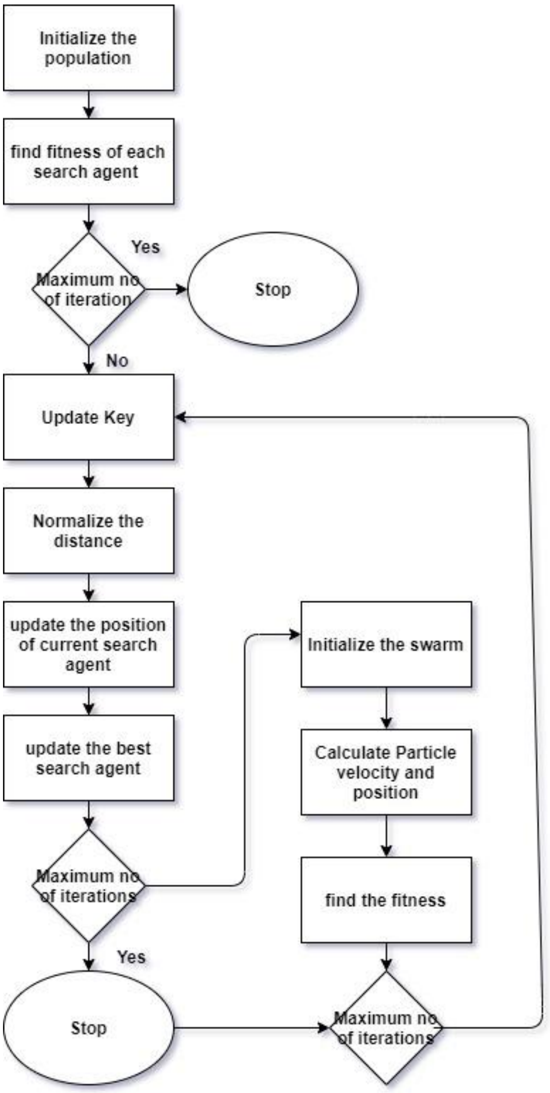

Initialize the population
find fitness of each search agent
Maximum no of iteration
Yes
Stop
No
Update Key
Normalize the distance
update the position of current search agent
update the best search agent
Maximum no of iterations
Yes
Stop
Initialize the swarm
Calculate Particle velocity and position
find the fitness
Maximum no of iterations

Fig.3 Flow chart for HE and Algorithm and BPSO

4. Results

Existing algorithms such as GO-PSO,Signcryption,blowfish and other optmization algorithm will have some attacks during the transmisson. The proposed HE Algorithm with BPSO will be safe and secure for transfering medical information. The Medical Image is encoded with the HE-BPSO. The final decoding is performed in order to receive the medical image back [1,4]. From the graph, relative to the proposed algorithm, the medical image has a high PSNR average estimation. here MATLAB 2019 with an i5 processor and 8GB RAM was used to perform the medical imaging protection process. Medical images were obtained from hospitals for security analysis, and the equations below address some of the parameters.

Mean Square Error:

$$\text{MSE}= \frac{\sum_{M,N}[l1(m,n)-l2(m.n)]\hat{}2}{M*N} \tag{5}$$

In the previous equation(6), The input Medical images will be M and N .it determines rows and column. Then the Peak Signal to Noise ratio will be

$$\text{PSNR}= log_{10}\, 10\, (255^2|MSE) \tag{6}$$

R in the previous equation is the maximum fluctuation in the data type of the input image. For example, if the input image has a floating-point data type with double-precision, then R is 1. R is 255, etc., if it has an 8-bit unsigned integer data type by the eqn (7)

$$\text{BER} = 1/\text{PSNR} \tag{7}$$

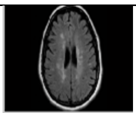
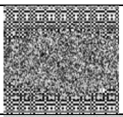
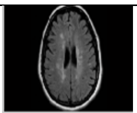
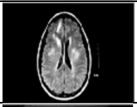
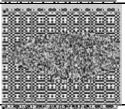
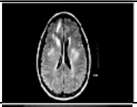
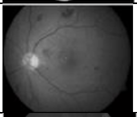
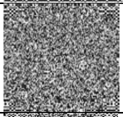
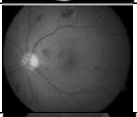
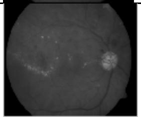
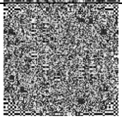
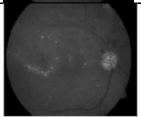
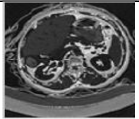
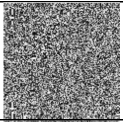
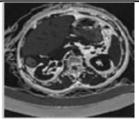
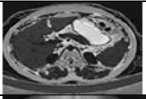
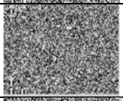
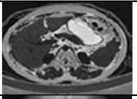
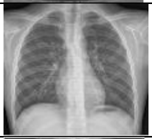
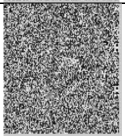
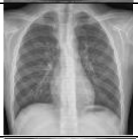
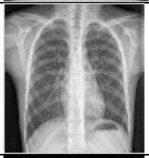
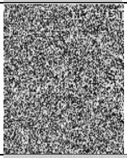
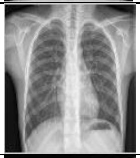
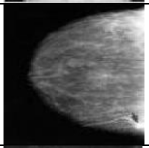
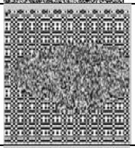
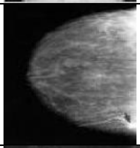
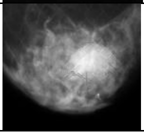
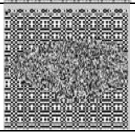
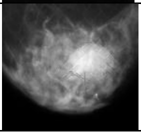
In view of the pixels, SSI is made reliable against the neighbouring pixels and improved as a measure compared to PSNR and MSE

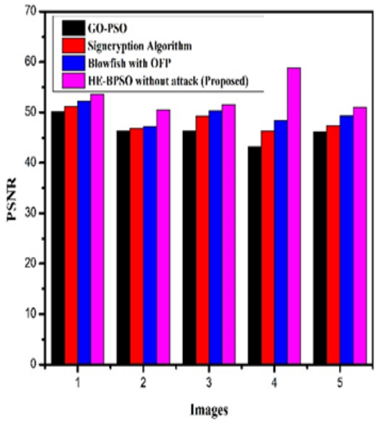
$$SSI = \frac{2mean(A*B)+c1)(2con(a+b)+c2}{mean(a^2)+mean(b^2)+c1(com(a^2)+com(b^2)+c2} \tag{8}$$

5. PERFORMANCE MEASURE

The proposed Honey Algorithm Encryption is optimized and compared with other existing algorithms like GO-PSO, Signcryption Algorithm, and Blowfish with OFP evaluation measures. At that point, the Medical imaging is encoded with the existing algorithms and the comparative analysis PSNR, MSE, BER and SSI also done and shown in Fig. [18]. HE algorithm that transmit the safe and reliable way of medical image [19]. In order to get the picture back, decoding is achieved at the end. From the Table.1 An efficient Image Encryption Comparative Result is shown in Fig .4 average estimation of HE algorithm is high than the other existing algorithms [20]. This demonstrates that the HE algorithm also operates for an extensive range of medical images as well relationship coefficient is nearly unity. The MSE is determined by calculating the error in the medical image [21] show in Fig.4 (b) where the mean square error is low for the proposed method as it appears differently in comparison to the other comparable algorithm.

Table.1 An Efficient Image Encryption Comparative Result for HE-BPSO

Input	Images	Encrypted Images	Decrypted Images	PSNR [6]	MSE [5]	BER [7]	SSI [8]
Input1				62.69	0.10	0	1
Input2				63.93	0.07	0	1
Input3				61.21	0.08	0	1
Input4				62.89	0.09	0.01	1
Input5				64.79	0.08	0	0..9
Input6				61.91	0.08	0	0.9
Input7				59.31	0.10	0.01	1
Input8				60.39	0.07	0	0.9
Input9				62.94	0.10	0	0.97
Input10				62.89	0.07	0.01	1



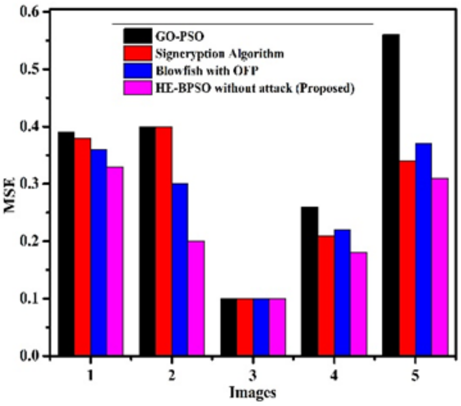


Fig.4 a) PSNR

Fig.4 b) MSE

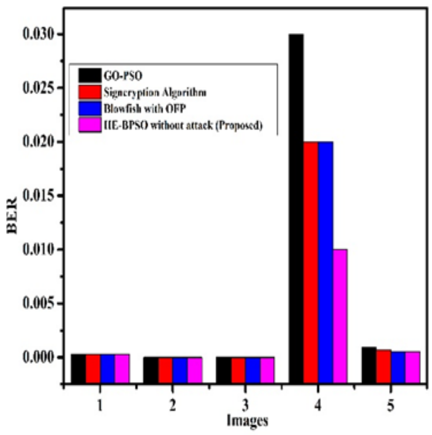


Fig.4 c) BER

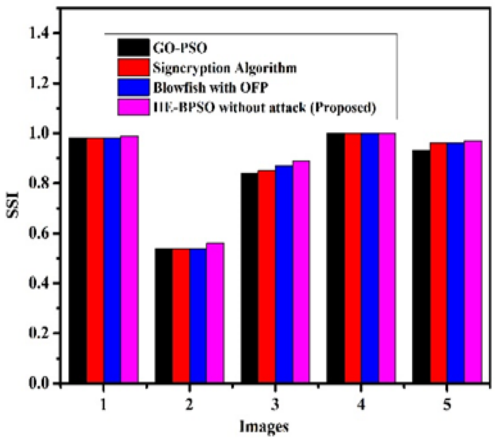


Fig.4 d) SSI

Fig.4 suggests the comparative evaluation of PSNR, MSE, BER system for GO-PSO, Signcryption Algorithm, Blowfish with OFP and proposed algorithm. Fig.4 d) depicts the performance of SSI, which is high in proposed system when compared with an existing Algorithm. And it is determined with the numerous image securities and minimal error rate.

6. Conclusion

In this article, the HE algorithm is optimized to extend the protection of medical imaging techniques with BPSO cryptographic keys have been optimized by 1% is shown in Fig. 4 using Honey Algorithm during encryption process. Compared to the same parameters with other existing algorithms, the HE algorithm efficiently estimated PSNR and MSE.The SSI maximizes in HE Algorithm and the PSNR value seems to be high than the other existing algorithms.The computation time decreased using this Honey Algorithm .Hence, the efficient image encryption security is discussed using Honey Algorithm with optimization Technique.

References

1. Avudaiappan, T., Balasubramanian, R., Pandiyan, S. S., Saravanan, M., Lakshmanaprabu, S. K., & Shankar, K. (2018). Medical image security using dual encryption with oppositional based optimization algorithm. Journal of medical systems, 42(11), 1-11.
2. Shankar, K., Elhoseny, M., Perumal, E., Ilayaraja, M., & Kumar, K. S. (2019). An efficient image encryption scheme based on signcryption technique with adaptive elephant herding optimization. In Cybersecurity and Secure Information Systems (pp. 31-42). Springer, Cham.
3. Shankar, K., Elhoseny, M., Chelvi, E. D., Lakshmanaprabu, S. K., & Wu, W. (2018). An efficient optimal key based chaos function for medical image security. IEEE Access, 6, 77145-77154.
4. Elhoseny, M., Shankar, K., Lakshmanaprabu, S. K., Maseleno, A., & Arunkumar, N. (2018). Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural computing and applications, 1-15.
5. Guhan, S., Arumugham, S., Janakiraman, S., Rengarajan, A., & Rajagopalan, S. (2018, May). A Trio Approach Satisfying CIA Triad for Medical Image Security. In International Conference on ISMAC in Computational Vision and Bio-Engineering (pp. 1109-1121). Springer, Cham.
6. Shankar, K., & Lakshmana Prabu, S. K. (2018). Optimal key based homomorphic encryption for color image security aid of ant lion optimization algorithm. International Journal of Engineering & Technology, 7(9), 22-27.
7. Shehab, A., Elhoseny, M., Muhammad, K., Sangaiah, A. K., Yang, P., Huang, H., & Hou, G. (2018). Secure and robust fragile watermarking scheme for medical images. IEEE Access, 6, 10269-10278.
8. Shankar, K., Lakshmanaprabu, S. K., Khanna, A., Tanwar, S., Rodrigues, J. J., & Roy, N. R. (2019). Alzheimer detection using Group Grey Wolf Optimization based features with convolutional classifier. Computers & Electrical Engineering, 77, 230-243.
9. Hussaini, S. (2020). Cyber Security in Cloud Using Blowfish Encryption. International Journal of Information Technology (IJIT), 6(5).

10. Nematzadeh, H., Enayatifar, R., Motameni, H., Guimarães, F. G., & Coelho, V. N. (2018). Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Optics and Lasers in Engineering, 110, 24-32.
11. Vengadapurvaja, A. M., Nisha, G., Aarthy, R., & Sasikaladevi, N. (2017). An efficient homomorphic medical image encryption algorithm for cloud storage security. Procedia computer science, 115, 643-650.
12. Ji, B., Lu, X., Sun, G., Zhang, W., Li, J., & Xiao, Y. (2020). Bio-inspired feature selection: An improved binary particle swarm optimization approach. IEEE Access, 8, 85989-86002.
13. Ayeni, B. K., Ahmad, B. I., & Jamilu, A. A. (2020). An Improved Classification Method for Diagnosing Heart Disease using Particle Swarm Optimization.
14. Thakur, S., Singh, A. K., Ghrera, S. P., & Mohan, A. (2020). Chaotic based secure watermarking approach for medical images. Multimedia Tools and Applications, 79(7), 4263-4276.
15. Gupta, M., Gupta, K. K., & Shukla, P. K. (2020). Session key based fast, secure and lightweight image encryption algorithm. Multimedia Tools and Applications, 1-26.
16. Saddam, M. J., Ibrahim, A. A., & Mohammed, A. H. (2020, October). A Lightweight Image Encryption and Blowfish Decryption for The Secure Internet of Things. In 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) (pp. 1-5). IEEE.
17. Ismail, S. M., Said, L. A., Radwan, A. G., Madian, A. H., & Abu-Elyazeed, M. F. (2018). Generalized double-humped logistic map-based medical image encryption. Journal of advanced research, 10, 85-98.
18. Ma, L., Chen, L., & Wang, S. (2019). Security analysis of a reversible watermarking algorithm for encrypted images in wavelet domain. Multimedia Tools and Applications, 78(8), 9827-9843.
19. Abdmouleh, M. K., Khalfallah, A., & Bouhlel, M. S. (2017). A novel selective encryption scheme for medical images transmission based-on JPEG compression algorithm. Procedia computer science, 112, 369-376.
20. Shankar, K., & Eswaran, P. (2015). Sharing a secret image with encapsulated shares in visual cryptography. Procedia Computer Science, 70, 462-468.
21. Kanso, A., & Ghebleh, M. (2015). An efficient and robust image encryption scheme for medical applications. Communications in Nonlinear Science and Numerical Simulation, 24(1-3), 98-116.