

International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164



Chief Editor

Dr. J.B. Helonde

Executive Editor

Mr. Somil Mayur Shah

ABSTRACT

The implementation of a secret data sharing algorithm along with water marking, steganography and cryptography can have various applications besides medical data privacy. It can be used for improving the authentication ability of confidential data too, so the demand of this type of approaches increases rapidly. We know that, Steganography is a scientific technique that is used to provide safe communication through multimedia carrier, for example, a combination of confidential information might be in the form of images, audio, and video files. If this feature is visible, the attack point is open, so the goal here is always to hide the existence of relevant information. Steganography has a variety of useful applications. But like any science, it can be used for bad intentions. In this research, medial image steganography model is designed to provide the security while transmitting the information in the form of a medical image by utilizing the concept of Discrete Wavelet transformation (DWT) as a decomposition approach with Modified Jamal Encryption Algorithm (MJE) encryption. In addition the concept of Particle Swarm Optimization (PSO) as an optimization technique used to find out the better hiding location in the medical images. To provide high security different processes are implemented such as pre-processing that is used to resize and conversion of the image with image decomposition. At last, the performance parameters such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), entropy and correlation coefficients are measured and compared with the existing work to validate the proposed model.

KEYWORDS: Steganography, Cryptography, Remotely Medical image, Patient's information, Data hiding method, DWT, MJE encryption, PSO.

1. INTRODUCTION

In recent times, the popularity of multimedia technologies based communication process and data transfer or sharing rapidly increase with the development in the modern world and also have turned out to be considerably much more comfortable and quicker and yet the issues identified with information security [1]. The technology of information hiding become a more popular and demanding academic as well as research zone for the students and researchers, because of their high demanding applications based model such as copyright in media, watermarking for copyright protection, fingerprinting or face based authentication module, steganography for general purpose or medical data security [2]. Image or data based steganography approach is the most ideal method for hiding a secret message in harmless media bearers (image, audio, video and text) [3]. But steganography approach can fail in some cases and important information may be leaked, so, we need to create a most secure approach. Regarding this steps, we presented an optimized encryption based steganography model to secure the patient medical image or information. The target of optimized encryption based steganography model is concealing the implanted data into the cover medical image with the end goal that the presence of payload in the cover image is vague to the individuals [4].

An optimized encryption based steganography for medical data or images is the art and science of invisible communication in the sense that it does not specify anything whether any communication is taking place or not. Encryption based secret message writing on cover or medical image is a lossless approach that can improvised the embedding capacity by more than 20% compare to the simple approach of steganography [5]. The secret message is applied using the Modified Jamal Encryption Algorithm (MJE) encryption that provides higher security inside the cases of attackers in the prevention of medical images or information [6].

It is expected that the proposed MJEA encryption technique will produce imperceptible encrypted images with the proposed encryption based steganography model with high embedding capacity and high image quality [7]. MJEA is expected to dissipate the high correlation among pixels and increase the entropy value by dividing the image into blocks but in case of failure, losses will be maximum. So, we used the concept of Discrete Wavelet transformation (DWT) as a decomposition approach and divide image into four different bands [8]. In this research work, we use the concept of histograms and entropy to measure the security level of the encrypted images based on the Particle Swarm Optimization (PSO) technique as a metaheuristic approach that helps to search the best pixel position to embed the secret message or information in the medical images [9]. Secret message or information encryption is referred to as cryptography technique that rearrangement the position of secret information, so that it is not detectable by eavesdroppers [10]. In these days, Security of data or medical data is the primary concern in the modern world and lots of technique were used to hide a sensitive piece of data during the transferring or sharing to prevent the data from intruders and hackers and prevention became a difficult task [11]. So, we developed an optimized encryption based steganography model using the concept of PSO with hybridization of DWT and MJEA and the block diagram of transmitter side model is shown in the below Fig. 1 and receiver side model is shown in the Fig. 2.

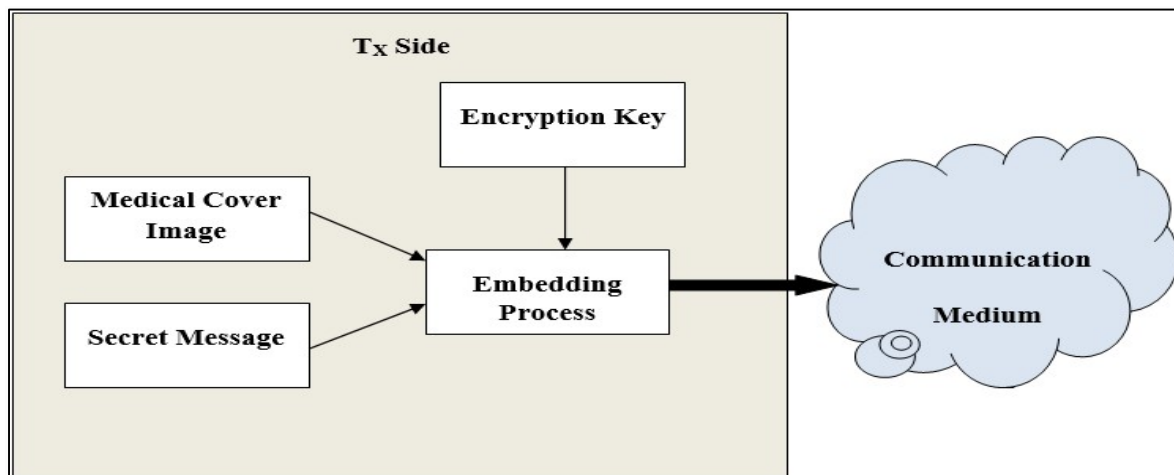


Fig 1: Transmitter Side Block Diagram of Optimized Encryption based Steganography Model

Fig 1 represents the block diagram of proposed optimized encryption based steganography model, where secret message is embedded with the medical cover image with a unique encryption key using the concept of PSO with hybridization of DWT and MJEA [11]. The proposed improved steganography work is a data hiding technique that is widely used in securing medical images and patient information from the attackers. At transmitter side of model, developed model transmits medical data or images by hiding the existence of the secret message, so that a viewer or third party cannot identify the transmitted message over the transmission medium and hence not able to decrypt it without key [12]. This research proposes a medical data securing technique that is used for hiding multiple character based text messages into a single medical image using the concept of PSO based DWT with MJEA. The cover medical image is split up into four part such as LL, LH, HL and HH planes using the DWT decomposition technique and find out the best pixels group for hiding the secret messages or information. Secret messages are embedded into these planes based on their position using classified by the PSO using fitness function. A 2-level DWT decomposition is apply on the cover medical image and the secret messages is embedding using an encryption key for the security purpose [13]. The above figure demonstrates the general block diagram of encryption based steganography process at the transmitter side or end. In the proposed research, at the transmitting end, secrete message is embedded into the cover medical image along with some defined keys using the concept of MJEA encryption technique and then the embedded data is transmitted to the receiver end through the communication medium. At the receiving end, reverse process (extraction process) is performed to get the desired secrete messages from the cover medical image by entering the accurate key. If the key is not matched then the secrete message is not extracted and an encrypted image will appears on the receiver end.

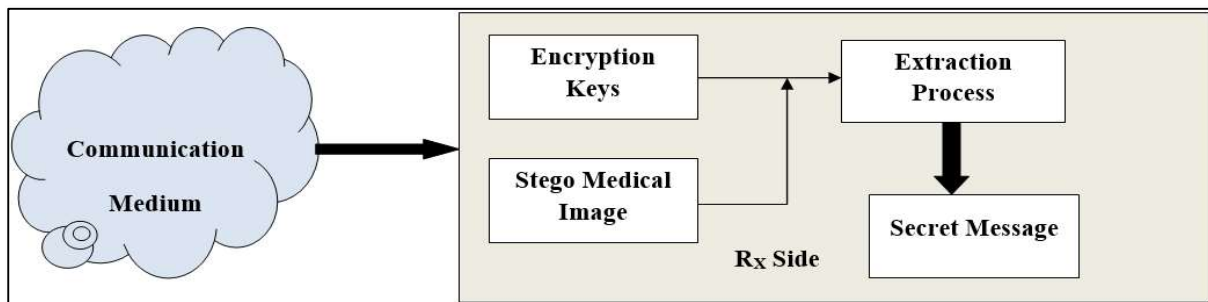


Fig 2: Receiver Side Block Diagram of Optimized Encryption based Steganography Model

There lots of research already proposed by different authors using different approaches but in the existing model the concept of pixel bit optimization to embed the secret message in not used. Also the researchers faced many security and hiding problem mainly in the in case of medical data and medical data is very important data and need to attention regarding the security and hiding capacity. So, the main motivation behind the development of optimized encryption based steganography model is the existing drawbacks and we introducing a secure and medical data related model using the concept of PSO with hybridization of DWT and MJEA encryption technique and the major contributions in this research are listed as:

- Hybridization of DWT with JAEN encryption approach is presented to decompose the cover medical image and encrypt the secret message before the transmission from transmitter (T_x) to receiver (R_x) end via communication medium.
- The concept of PSO based optimization algorithm with a novel fitness function is used to find out the exact pixel pattern to embed the secret message data into medical images.
- To validate the proposed optimized encryption based steganography model, a comparison with the existing steganography model with different techniques are performed on the behalf of performance parameters like PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), Entropy and Correlation Coefficients [14].

We introducing the concept of an optimized encryption based steganography model using PSO with hybridization of DWT based decomposition and MJEA encryption technique and the remaining paper is systematized as follows. In Sect. 2, related works regarding the steganography are reviewed. Sect. 3 describes the material and method of an optimized encryption based steganography model and the experimented simulation results are presented in Sect. 5. Finally, the conclusion with the future possibilities of medical data based steganography is presented in the Sect. 6.

2. RELATED WORK

In this section, existing work are analyzed to find out the issues related to the steganography model for medical data or images because the researchers did not pay much attention toward the security and hiding issues like, if medical cover image dimensions are not suitable to form image blocks for embedding then how to carry out data hiding and whether this method is prone to various types of attackers. In 2019, *JNB Salameh* had conducted a research to develop a new approach for securing medical images and patient's information by using a hybrid system. In this research, author developed a new hybrid security system using the combination of cryptography and steganography techniques that helps to achieve better hiding capacity for both the medical images and patient's information. To use the cryptography in model, author develop a MJEA (encryption algorithm because it is a symmetric (64-bit) block encryption algorithm with (120-bit) key and help to improve the security. After the development of model, author verify the simulation results in terms of PSNR and MSE and all experimental results proved the strength of the proposed system but need more attention regarding the security because the used data is more confidential. A realization of an adaptive data hiding system for electronic patient record, embedding in medical images was presented by *SA Parah et al.* in 2019. An adaptive EPR (Electronic Patient Record) hiding system utilizing medical images has been presented by authors in this research article. They use the concept of EPR based information embedding using the Discrete Cosine Transform (DCT) coefficients. Firstly they divide medical cover image is divided into 8×8 patches or non-overlapping blocks and then apply DCT on each block to

generate a coefficients. The developed model uses an adaptive embedding factor method to select a block unlike the conventional way of predefining an embedding factor and verify the model using various image quality matrices like PSNR, Structural Similarity Index (SSIM), and Normalized Cross Co-relation (NCC) that show the experimental simulation results are capable of providing better quality system. A secure and reversible data or information hiding system related to medical system using the Internet of Things (IoT) was designed by *JA Kaw et al.* in 2019. Authors aim to ensure security of medical data such as EPR, by utilizing a novel high-capacity and reversible data hiding approach for securely embedding EPR within the medical images using Optimal Pixel Repetition (OPR). OPR changes over each pixel of the information picture to a 2×2 square to encourage reversibility by guaranteeing all the pixels in a 2×2 square to have various qualities. Since a 2×2 square is contained 4-pixel components, which could be organized in sixteen potential manners; we produce a query table relating to sixteen potential places of pixels. EPR stowing away in each square is accomplished by permuting the pixels of a square as per the four-piece expression of mystery information, bringing about a histogram invariant stego picture. The histogram invariance improves the vigor of the proposed plan to factual assaults. A stego picture is said to conceal installed information safely, when it gives better imperceptivity to an apparently high payload. In this way, while utilizing data inserting approach for making sure about customer information on a portable cloud stage, high imperceptivity is an alluring element. Exploratory outcomes show that normal PSNR acquired is 42 dB for payload 1.25 BPP by our plan, indicating its viability for forestalling unapproved access to customer's delicate information. In 2019, *A. Giakoumaki et al.* presented a secure and efficient health data management model through multiple watermarking on medical images. Authors presented a research efforts in the area of medical-oriented watermarking model by utilize the concept of a wavelet-based scheme. The aim of this scheme in research is to address critical health information management issues, including origin and data authentication, protection of sensitive data, and image archiving and retrieval. As per the exacting impediments applying to clinical pictures, the plan permits the meaning of a ROI (region of interest) whose symptomatic worth is secured, since the main extra data inserted in that focuses on trustworthiness control. The vigor of the strategy is improved through a type of half breed coding, which incorporates dreary installing of BCH encoded watermarks. The exploratory outcomes on various clinical imaging modalities exhibit the productivity and straightforwardness of the watermarking plan.

Based on the above survey of existing research, we concluded and decided to present a model using the concept of PSO-based optimization to develop a secure and effective steganography model for medical data using the concept of MJEА-based encryption approach.

3. MATERIAL AND METHOD

In this section of research paper, we explain the used materials and methodology of proposed encryption based steganography model with algorithms. The designed model in dived into two different parts named as embedding part and extraction part. The brief details about both parts are given in the below section of this paper and Fig.3 show the embedding and extraction part of the proposed steganography model in terms of flowchart.

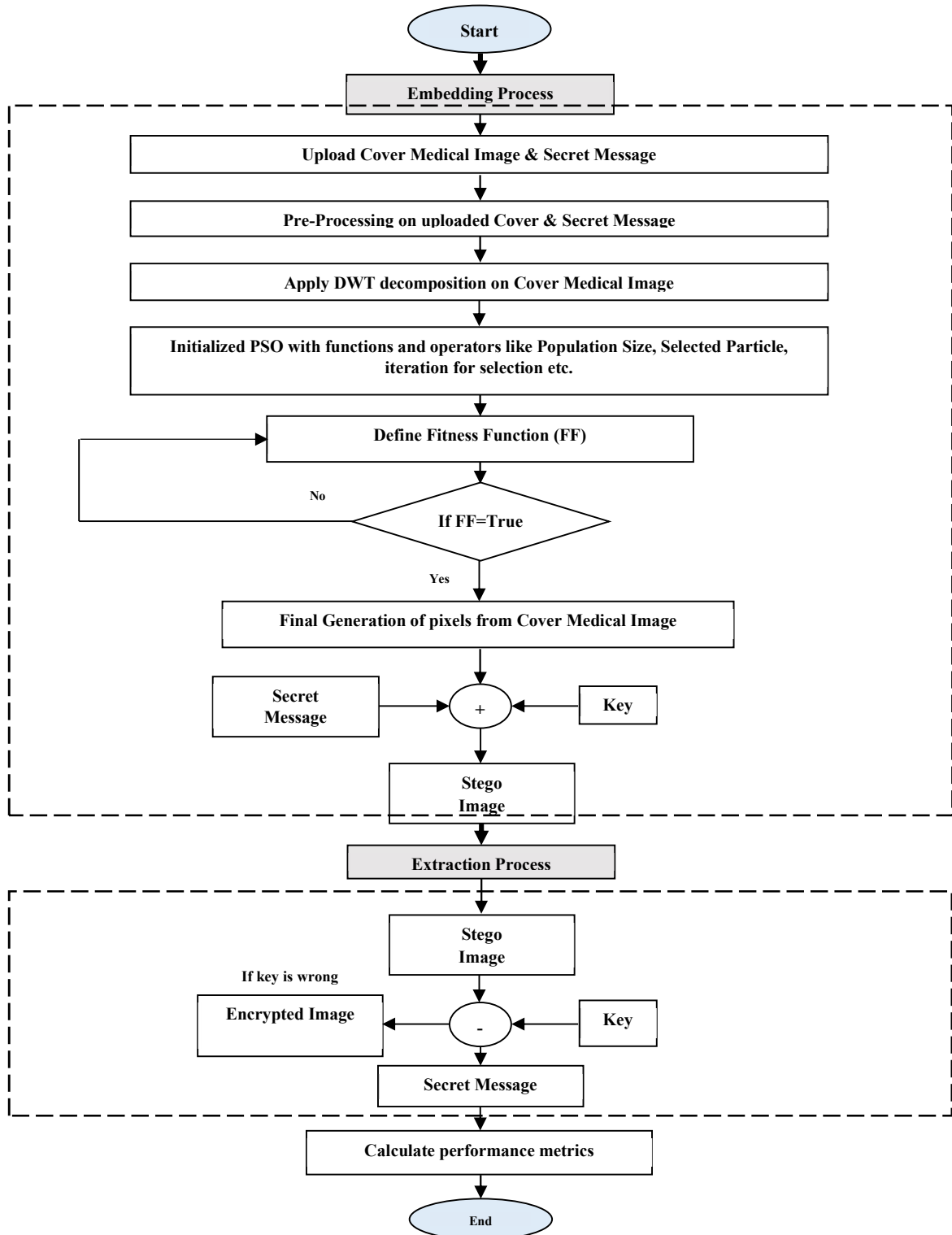


Fig 3: Flowchart of Proposed Encryption-based Steganography Model

Above Fig. 3 shows the model flowchart using the using the concept of PSO with hybridization of DWT and MJEA encryption technique. To design and develop a framework for the simulation of Medical Image Steganography Model, some basic steps are given as:

Step 1: To design a framework using the concept of GUI for simulation of proposed “An Optimized Encryption based Steganography Model to Secure Medical Images using Metaheuristic Technique” for improvement in security and data hiding capacity.

Step 2: Develop a code to upload medical cover image and secret message to embed in cover image.

Step 3: Pre-processing is applied on uploaded medical cover image and secret messages. In pre-processing step, some basic process like, resizing, color conversion etc. will be applied to make the uploaded medical image useful.

Step 4: After that, DWT decomposition is applied on the medical cover image to divide image into small coefficients like LL, LH, HL and HH that can help to select the better embedding region or set of pixels.

Step 5: Develop a code for the histogram construction of medical cover image and initialized the PSO algorithm for the optimization of histogram pixels. In a more general mathematical sense, a histogram is a function H_i that counts the number of observations that fall into each of the disjoint categories (known as bins), whereas the graph of a histogram is merely one way to represent a histogram. Thus, if we let n be the total number of observations and m be the total number of bins, the histogram H_i meets the following conditions and the mathematical expression of histogram construction technique is;

$$H_i = \sum_{i=1}^m \frac{1}{n_i}$$

Step 6: After that set the fitness function of PSO according to the requirement so we can find out the appropriate and optimal pixel group.

$$Fitness = \begin{cases} F_s(True) & \text{if } F_s \geq F_t \\ F_t(False) & \text{otherwise} \end{cases}$$

Where F_s is the selected value of feature and F_t is the threshold value of feature which is calculated by the given expression where n is the total number of feature and F is the feature value.

$$F_t = \frac{1}{n} \sum_{i=1}^n F_i = \frac{1}{n} (F_1 + F_2 + F_3 + \dots + F_i)$$

Step 7: After that we apply the PSO algorithm to the optimization of histogram pixels and select the bit pattern for embedding purpose and MJEA encryption technique also applied for security purpose. The algorithm of PSO is written as:

Algorithm 1: PSO Algorithm

Input: Pre-processed pixels and Fitness Function

Output: Optimized Pixel Sets

1 Strat optimization

2 Calculate, R as row and C as columns of pre-processed pixels (Img)

3 Initialize PSO parameters – Iterations (T)
– Population Size (P)

4 Optimized Pixel = []

5 for $i = 1 \rightarrow R$

6 for $j = 1 \rightarrow C$

7 $P_{val} = \sum_{i=1}^P \text{Img}(i)$

9 $Threshold_{val} = \frac{\sum_{i=1}^P \text{Img}(i)}{\text{Length of Img}}$

10 $Fit Fun = Fit Fun(P_{val}, Threshold_{val})$

11 $Optimized Pixel = PSO(Fit Fun, Initialize Parameters)$

12 end

13 end

14 Returns: Optimized Pixel Sets

15 end - Algorithm

Step 8: The secret message is embedded into the medical cover image based on the classified bits in the previous step.

Step 9: After the embedding, extraction part enable and receiver can extract the secret message from the medical cover image using private key and if key is correct then they got the secret message otherwise they cannot extract the secret message.

Step 10: At last of simulation, the performance parameters of proposed work will be calculated and compare with exiting work in terms of PSNR, MSE, Entropy and Correlation Coefficients etc.

Above flowchart and algorithms are shows procedural steps of proposed encryption-based steganography model. By using above procedure we achieve better results which are well described in the next section of this research paper on the behalf of some medical images. The list of used medical images is shown in the Fig. 4 named as Database of Medical Images.

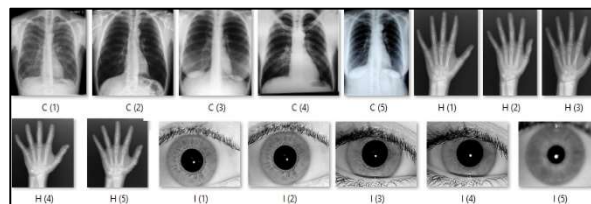
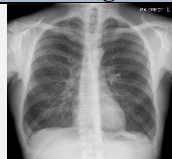

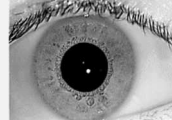


Fig 4: Database of Medical Images

Above Fig. 4 represent the used medical image database in the proposed encryption-based steganography module. In the figure, Chest, Hand and Iris images are shown and there details are given in the Table I with the description.

Table I: Description of Medical Images Database

No.	Image	Name	Format	Size
1		Chest X-ray	JPG	95.7 KB (98,023 bytes)
2		Hand X-ray	JPG	2.00 MB (2,101,802 bytes)
3		Iris	JPG	225 KB (230,454 bytes)

The simulation results of proposed encryption-based steganography model using PSO with DWT and MJEА encryption algorithm is described in the below section of paper.

4. RESULTS AND ANALYSIS

In this section, we describe the simulation results of the proposed encryption-based steganography model using PSO with DWT and MJEА encryption algorithm and the simulation results based on the PSNR of Stego image is given in the Table II and compare with existing work by *JNB Salameh* [14] is given as:

Table II: PSNR Comparison

Images	Existing	Proposed
1-Irsi	18.5	39.92
2-Chest	17.5	41.42
3-Hand	18.8	43.59
Average	18.26	41.64

In the point of view of secure and efficient communication in medical area, the proposed encryption-based steganography model have achieved better performance in terms PSNR that is shown in the Fig. 5 based on the comparison with existing work.

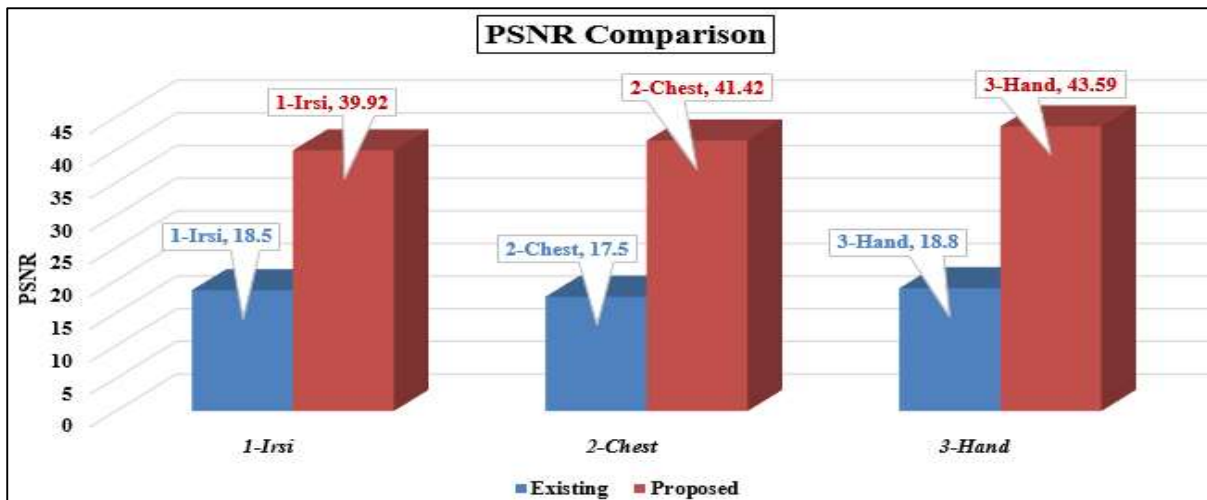


Fig 5: Comparison of PSR

According to the above figure, we observed that the PSNR value in case of encryption-based steganography model is improved by utilization of PSO with DWT and MJEa encryption algorithm as a data hiding concept. The average PSNR of proposed encryption-based steganography model is 41.64 but in the existing work this is only near to 18.28. The PSNR of proposed encryption-based steganography model is more, then the MSE is reduces that is given in the Table III. We also provided the comparison of MSE for proposed encryption-based steganography model and existing work.

Table III: MSE Comparison

Images	Existing	Proposed
1-Irsi	912.29	6.64
2-Chest	1150	5.12
3-Hand	1350	4.87
Average	1137.43	5.54

The graphical representation of MSE comparison is shown in the Fig. 6 with existing work.

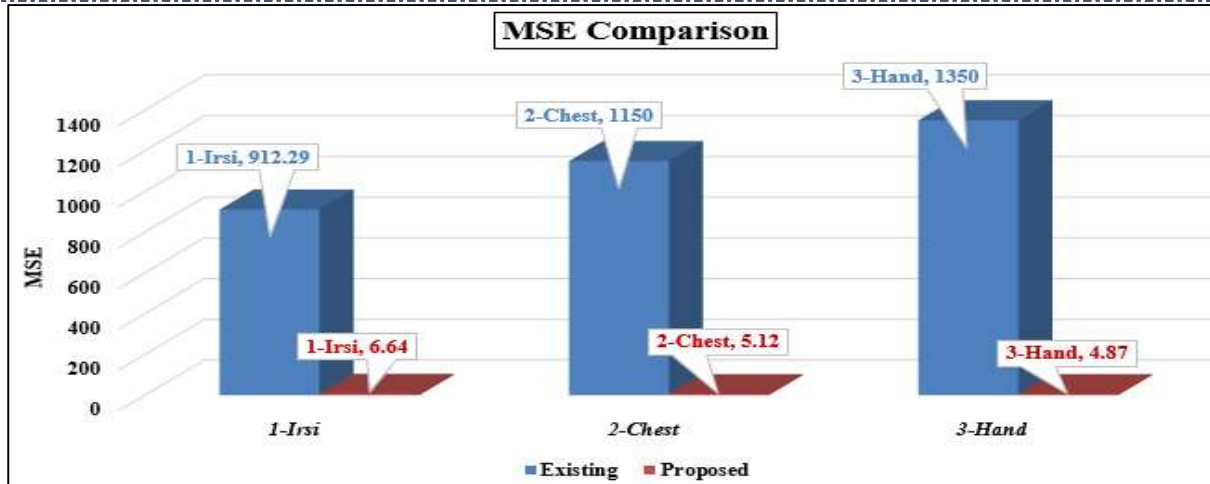


Fig 6: Comparison of MSE

In the point of view of secure and efficient communication in medical area, the proposed encryption-based steganography model have less MSE as compare to the existing work that indicates the utilization of PSO with DWT and MJEa encryption technique is a beneficial step. We also presents some other parameters of proposed work in the Table IV.

Table IV: Entropy and Correlation Coefficients

Images	Entropy	CC
1-Irsi	6.43	0.99
2-Chest	7.45	0.99
3-Hand	7.93	0.99
Average	7.27	0.99

Above simulation results based on the Entropy and Correlation Coefficients show that the proposed encryption-based steganography model have its own impact and also show the improved results and impact of swarm-based metaheuristic technique in the area of medical image security.

5. CONCLUSION AND FUTURE WORK

In this paper, an optimized encryption based steganography model to secure medical images using metaheuristic technique is proposed for secure and effective medical data hiding and communication purpose. The main contribution of this research is developing a new security system that combine the concept of cryptography and steganography techniques to provide a secure distribution for both the medical images and patient’s information by utilizing the metaheuristic approach to prevent the data from third party or attackers. The obtained results regarding the PSNR, MSE, Entropy and Correlation Coefficients values are favorably acceptable under consideration to show the effectiveness of proposed model. Experimental and simulation results indicated that our proposed novel method is secure and robust and found superior than previous published work in the area of medical image steganography. The validity of the proposed work is further strengthened using subjective measure for evaluating the medical stego image quality. Therefore, the proposed encryption-based steganography model is providing multi-level security mechanism by exploiting steganography and metaheuristic based encryption technique for health applications. In future, proposed model could be develop for the medical data like audio, medical signal and video data based on the artificial intelligence approach to protect the data from the attackers.

REFERENCES

- [1] S. Ushll, G. Kumal, K. Boopathybagan, "A Secure Triple Level Encryption Method Using Cryptography and Steganography", in Proceedings of the International Conference on Computer Science And Network Technology, pp. 1017-1020, 2011.
- [2] S. Laskar, K. Hemachandran, "High Capacity Data Hiding Using LSB Steganography and Encryption", International Journal of Database Management Systems, Vol. 4, No. 6, pp. 57-62, 2012.
- [3] W. Al-qwider, J. Bani Salameh, "A Novel Technique for Securing Data Communication Systems by Using Cryptography and Steganography", Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 3, No. 2, pp. 110-130, 2017.
- [4] W. Hong, T. Chen, and H. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match", IEEE Signal Processing Letters, Vol. 19, No. 4, 2011, pp. 199–202, 2012.
- [5] A. Lavanya and V. Natarajan, "Watermarking Patient Data in Encrypted Medical Images", in Proceedings of the Sadhana-Academy in Engineering Sciences, Vol. 37, pp. 723–729, 2012.
- [6] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, pp. 826–832, 2012.
- [7] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A Joint Encryption /Watermarking System for Verifying the Reliability of Medical Images", IEEE Transactions on Information Technology in Biomedicine, Vol. 16, pp. 891–899, 2012.
- [8] S. Zhang, G. Tiegang, and L. Gao, "A Novel Encryption Frame for Medical Image with Watermark Based on Hyperchaotic System", Mathematical Problems in Engineering, Vol. 11, 2014.
- [9] A. Umamageswari, U. Ferni, and G. Suresh, "A Survey on Security in Medical Image Communication", International Journal of Computer Applications, Vol. 30, No.3, 2011.
- [10] D. Bouslimi, and G. Coatrieux, "A joint Watermarking/ Encryption Algorithm for Verifying Medical Image Integrity and Authenticity in Both Encrypted and Spatial Domains", in Proceedings of the 33th Annual International Conference of the IEEE- EMBS, Massachusetts USA, 2011.
- [11] P. Viswanathan and P. Krishna, "Randomized Cryptographic Fusion Watermarking Medical Image with Reversible Property", International Journal of Computer Information Systems, Vol. 2, 2011.
- [12] J. Bani Salameh, "A New Symmetric-Key Block Ciphering Algorithm", Middle-East Journal of Scientific Research (MEJSR), Vol. 12, No. 5, pp. 662-673, 2012.
- [13] J. Bani Salameh, "An Investigation of the Use of MJEA in Image Encryption", WSEAS Transactions on Computers, Vol. 15, pp. 12-23, 2016.
- [14] Salameh, J. N. B. (2019). A New Approach for Securing Medical Images and Patient's Information by using a hybrid System. IJCSNS, 19(4), 28.
- [15] Parah, S. A., Ahmad, I., Loan, N. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2019). Realization of an adaptive data hiding system for electronic patient record, embedding in medical images. In Security in smart cities: models, applications, and challenges (pp. 47-70). Springer, Cham.
- [16] Kaw, J. A., Loan, N. A., Parah, S. A., Muhammad, K., Sheikh, J. A., & Bhat, G. M. (2019). A reversible and secure patient information hiding system for IoT driven e-health. International Journal of Information Management, 45, 262-275.
- [17] Giakoumaki, A., Pavlopoulos, S., & Koutsouris, D. (2006). Secure and efficient health data management through multiple watermarking on medical images. Medical and Biological Engineering and Computing, 44(8), 61.