Comparative Analysis of Dual Secure Based Medical Image Watermarking Technique to Increase Security of Watermark Data Using BFOA

C. H. Venugopal Reddy[1*], P. Siddaiah[2]

[1]Department of ECE, Nalanda Institute of Engineering and Technology, Guntur, A.P, India.
[2]Acharya Nagarjuna University College of Engineering and Technology, Guntur, A.P, India.

* Corresponding author. Email:venugopalreddy.sai@gmail.com
Manuscript submitted May 21, 2015; accepted April 17, 2016.
doi: 10.17706/ijcce.2016.5.6.381-397

Abstract: Medical image security and privacy are two issues that are interrelated and highly sensitive. Protecting the privacy and data integrity has to be done without comprising on the structural integrity of the data. Watermarking and encryption have served the purpose of data security for long. In this research work, a dual security approach is employed where watermarking and encryption is used to provide two layers of security. The watermarking is proposed to be implemented using a hybrid approach which encompasses Discrete Wavelet Transforms (DWT), Lifted Wavelet Transforms (LWT) and Singular Value Decomposition (SVD) techniques. Bacterial Foraging Optimization (BFOA) is used for optimizing the watermarking parameters. The encryption is proposed to be effected using RSA and AES encryption algorithms. A Graphical User Interface (GUI) which enables the user to have ease of operation in loading the image, watermark it, encrypt it and also retrieve the original image whenever necessary is also designed and presented in this paper. The robustness and the integrity of the watermark are tested by measuring different performance parameters and subjecting it to various attacks.

Key Words: DWT, LWT, SVD, BFOA, AES, RSA, GUI.

1. Introduction

Medical Imaging has opened new avenues in diagnosis and health care. Different imaging modalities are used for imaging of specific regions of the human body, thus giving rise to a huge volume of medical data whose integrity has to be protected. With exponential increase of processing power of computing system coupled with the growth in capacity of storage elements, the use of medical images has breached many boundaries. This is also aided by the increase in availability of bandwidth for transmitting data over a network. The advances in multimedia and communication technology have provided new ways to distribute access and store medical data in a digital format. In contrast, these advances have introduced new risks for inappropriate use of medical information circulating in open networks. Similarly the advances in recording, editing, and broadcasting multimedia contents in digital form motivate to protect these digital contents from illegal use, such as duplication, manipulation, and redistribution.

Medical images play a significant role in diagnosis of many diseases. Medical image protection and authentication are becoming increasingly important in an e-Health environment where images are readily distributed over electronic networks. Research has shown that medical image watermarking is a relevant

process for enhancing data security, content verification and image fidelity. At the same time, it is necessary to preserve as much original information in the image data as possible, to avoid causing performance loss for human viewers. Security of medical information, derived from strict ethics and legislatives rules, gives rights to the patient and duties to the health professionals. Medical tradition is very strict with the quality of biomedical images, in that it is often not allowed to alter in any way the bit field representing the image (non-destructive). Thus the watermarking method must be reversible, in that the original pixel values must be exactly recovered. This limits significantly the capacity and the number of possible methods. It also constrains to have dedicated routines to automatically suppress and introduce the mark in order to prevent the transmission of unprotected documents.

A watermarking method is usually designed depending on an application framework striking a compromise between different requirements: capacity (amount of information that can be embedded), robustness (a fragile watermark will not survive any image processing), privacy (secret knowledge for watermark content access — usually a secret key) and imperceptibility. We can say that the higher the strength of the watermark signal, the more it is robust and/or of higher capacity albeit perceptibility is compromised. Consequently, if it is envisioned to process the image with an information loss, a robust watermark is desirable to authenticate the image origins, while at the same time the watermark should not interfere with the image content interpretation. However each property has its own limitation and conflict with each other. It will be a challenging task to design a good algorithm by coupling both the concept of reversibility and robustness with proper optimization. It is well known that the integrity and confidentiality of medical folders are a critical issue for ethical as well for legal reasons. Classical encryption technology is an important tool that can be used to protect data transmitted over computer networks but it does not solve all digital data protection problems. At the receiver's side, decrypted content may be subjected to unauthorized use or manipulation [1].

In transform domain watermarking can be performed using DCT (Discrete Cosine Transform) [2] or IWT (Integer Wavelet Transform) [3]. Different approaches have been proposed in order to improve the security of medical image transmission using watermarking, which gives one level security. A Tamper Assessment Factor (TAF) of the watermarked image with the physician's signature and patient diagnosis information embedded into wavelet transform coefficients of the medical images is proposed in [4]. Similarly, a novel blind watermarking method with secret key is proposed by embedding Electrocardiograph (ECG) signals in medical images combined with the EZW-based wavelet coder [5]. A blind watermarking scheme using the non-tensor product wavelet filter banks are used for copyright protection is presented in [6]. An efficient watermarking method based on the significant difference of wavelet coefficient quantization is proposed in [7]. A multiple, fragile image authentication scheme is proposed for DICOM images using discrete wavelet transform in [8] in this work multiple watermarks are embedded into wavelet domains, the multiple watermarks serve as reference watermarks. A novel watermarking algorithm based on singular value decomposition (SVD) is proposed in [9]. Both of the *D* and *U* components of SVD are explored for embedding the watermark in [10].

To enforce integrity and authenticity several works have been implemented that provides two level security for transmission of medical images. In joint encryption/watermarking [11] method, watermarking and encryption step processes are merged. Joint watermarking/encryption system is slower than simply encrypting the image but it provides reliability control functionalities. Watermarking is done by Quantization Index modulation. (QIM) method and AES (Advanced Encryption standard) and RC4 (Rivest cipher 4) algorithms do encryption. A Digital envelope (DE) method to assure data integrity and security that outlines the systematic evaluation, development, and deployment of the DE method for PACS environment is proposed in [12]. A new cryptographic means to improve the trustworthiness of medical

images is implemented [13].

A comparative study of AES and RC4 algorithm is done in [14] in the case of AES algorithm, as the key size increases the encryption and decryption time increases, whereas for RC4 it remains almost constant and it is less than AES. Similarly, several methodologies have been proposed for medical image security [15]. These methods can detect, whether the medical images are tampered or modified but cannot protect the images from tampering. In this work, the digital watermarking is done by using special symmetric matrices to construct the new non-tensor product wavelet filter banks [6] which can capture singularities in all directions. Here, natural image is considered as original image and medical image is taken as watermark to avoid the attacker's attention toward the medical information.

The optimization of watermark through evolutionary approaches has also been researched extensively. A new method for adaptive watermark strength optimization in Discrete Cosine Transform (DCT) domain in which watermark strength is intelligently selected through Genetic Algorithm (GA) is proposed in [16]. A novel hybrid PSO, namely (HPSO) to improve the performance of fragile watermarking based DCT which results in enhancing both the quality of the watermarked image and the extracted watermark is implemented in [17]. A novel optimal watermarking scheme based on singular value decomposition (SVD) using differential evolution algorithm (DE) is explained in [18]. Differential evolution (DE) algorithm to balance the tradeoff between robustness and imperceptibility by exploring multiple scaling factors in image watermarking is proposed in [19]. A new improved watermarking scheme is proposed using lifting wavelet transform (LWT) [20] and SVD for medical images. The medical images of patients are watermarked with the image of that particular patient which is extracted at the doctor's end to identification. Lifting wavelets have distinctive advantage that is explored and is missed in traditional wavelet transform. With lifting wavelets the inverse transformation is undoing the operations of forward transform which reduce the artifacts during transformation.

In this work, we have implemented a dual security approach for maintaining the data integrity of the medical images. Watermarking and encryption of watermarked image is proposed. In order to preempt any attack from attacker the medical image is considered as water mark and is embedded in to a natural image. A multi-objective optimization approach is proposed to maintain the fidelity of the watermark (medical image) as it contains valuable diagnostic information. This multi-objective approach ensures that there is an optimum tradeoff between robustness, imperceptibility and structural integrity of the watermark. Maintaining the structural integrity of the watermark is necessitated by the fact that most of the diagnostic approaches in medical image consider the morphological factors of the image to divulge precious information about the prognosis of a particular clinical condition. Different performance parameters like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalized Coefficient (NC) and Structural Similarity Index (SSIM) is used to frame an objective function. This objective function is optimized using Bacterial Foraging Optimization (BFOA) to choose a particular wavelet in selected wavelet family and scaling factor of the Singular Value Decomposition (SVD). A lifting scheme is further employed to enhance the performance of the selected wavelet family.

The medical image security is further enhanced by encrypting the watermarked image using Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) Algorithm and Advanced Encryption Standard (AES) algorithms. Correlation Value (CV) between the watermarked image and the encrypted image is used to measure the efficacy of watermark. The watermarked image is tested for different types of attacks like sharpening, smoothening, rotation , cropping and different types of noises which include speckle noise, salt and pepper noise, Gaussian noise and Poisson noise. To enable ease of use and seamless integration of the user a Graphical User Interface (GUI) is designed to automate the process of embedding, encrypting, decrypting and extracting. The tool helps user in analyzing and testing different scenarios and choose the best possible

one for a watermarking a given medical image.

2. Methodologies

This work aims at exploiting the features of Lifting Wavelet Transforms (LWT) along with Discrete Wavelet Transforms (DWT) and Singular Value Decomposition (SVD) to provide a robust and imperceptible watermark. Similarly RSA and AES algorithms are used for encrypting the watermarked images to provide an extra layer of security. This section dwells on these concepts and methods used in this research work.

2.1. Discrete Wavelet Transforms (DWT)

The first recorded mention of what we now call a "wavelet" seems to be in 1909, in a thesis by Alfred Haar. The concept of wavelets in its present theoretical form was first proposed by Jean Morlet and the team at the Marseille Theoretical Physics Center working under Alex Grossmann in France. The methods of wavelet analysis have been developed mainly by Y. Meyer and his colleagues, who have ensured the methods' dissemination. The main algorithm dates back to the work of Stephane Mallat in 1988 [21]. In numerical analysis and functional analysis, a discrete wavelet transform (DWT) is any wavelet transform for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution: it captures both frequency *and* location information (location in time). Thus discrete wavelet transform (DWT) is a linear transformation that operates on a data vector whose length is an integer power of two, transforming it into a numerically different vector of the same length. It is a tool that separates data into different frequency components, and then studies each component with resolution matched to its scale [22]. DWT is computed with a cascade of filters followed by a factor 2 sub sampling (see Fig. 1).

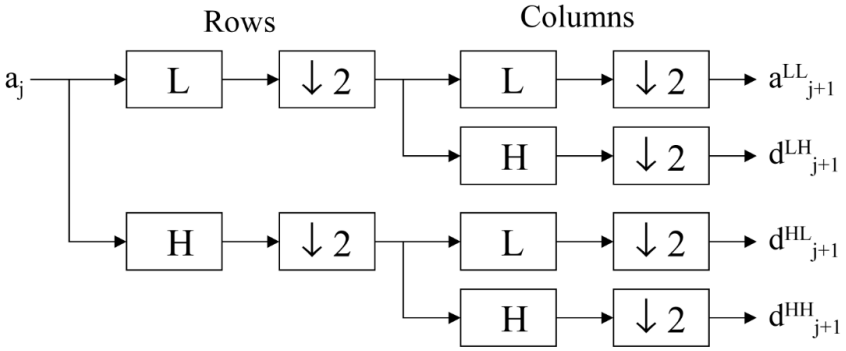

Fig. 1. Discrete wavelet transform tree for two-dimensional image.

H and *L* denote high and low-pass filters respectively followed by sub sampling. Outputs of these filters are given by equations (1) and (2)

$$a_{j+1}[p] = \sum_{n=-\infty}^{+\infty} l[n-2p]a_j[n] \tag{1}$$

$$d_{j+1}[p] = \sum_{n=-\infty}^{+\infty} h[n-2p]a_j[n] \tag{2}$$

Elements a_j are used for next step (scale) of the transform and elements d_j, called wavelet coefficients, determine output of the transform. $l[n]$ and $h[n]$ are coefficients of low and high-pas filters respectively one can assume that on scale $j+1$ there is only half from number of a and d elements on scale j. This causes that

DWT can be done until only two a_j elements remain in the analyzed signal. These elements are called scaling function coefficients. The types of wavelets used in this work are described here. Haar wavelet is discontinuous, and resembles a step function. It represents the same wavelet as Daubechies 'db1' Ingrid Daubechies, invented what are called compactly supported orthonormal wavelets — The names of the Daubechies family wavelets are written dbN, where *N* is the order, and db the "surname" of the wavelet. The db1 wavelet, as mentioned above, is the same as Haar wavelet. Biorthogonal family of wavelets exhibits the property of linear phase, which is needed for signal and image reconstruction. By using two wavelets, one for decomposition (on the left side) and the other for reconstruction (on the right side) instead of the same single one, interesting properties are derived. The Symlets are nearly symmetrical wavelets proposed by Daubechies as modifications to the db family. The properties of the two wavelet families are similar. The Wavelets function psi of different wavelet families used in this work are represented in the below Fig. 2.

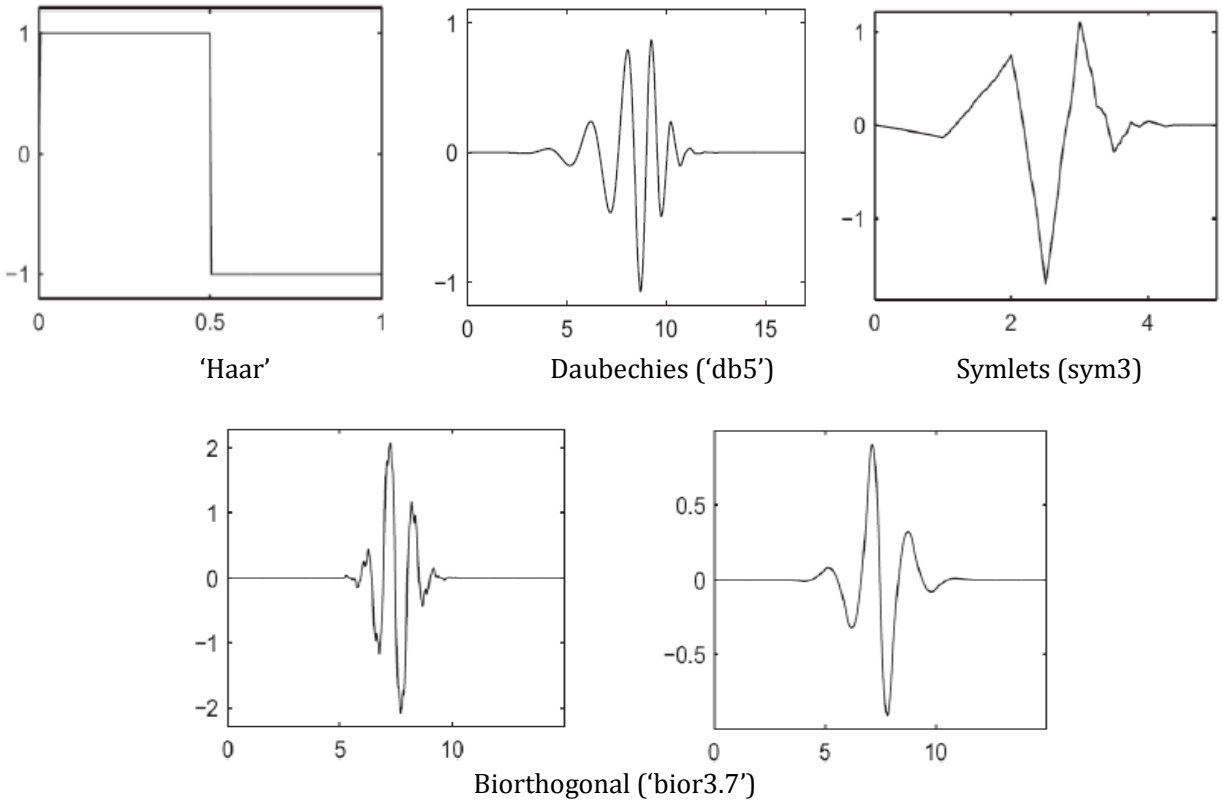

Fig. 2. psi of different wavelet families used in this research work.

The main feature of DWT that makes it attractive for image processing applications is multiscale representation of function. By using the wavelets, given function can be analyzed at various levels of resolution. The DWT is also invertible and can be orthogonal. DWT involves decomposition of image into frequency channel of constant bandwidth. This causes the similarity of available decomposition at every level. DWT is implemented as multistage transformation. Level wise decomposition is done in multistage transformation. At level 1: Image is decomposed into four sub bands: LL, LH, HL, and HH where LL denotes the coarse level coefficient which is the low frequency part of the image. LH, HL, and HH denote the finest scale wavelet coefficient. The LL sub band can be decomposed further to obtain higher level of decomposition. This decomposition can continues until the desired level of decomposition is achieved for the application. The watermark can also be embedded in the remaining three sub bands to maintain the quality of image as the LL sub band is more sensitive to human eye.

2.2. Lifting Wavelet Transforms (LWT)

Lifting wavelets come under the category of second generation wavelets that have distinctive advantages over traditional first generation wavelets. The lifting wavelets trim down the computing time and memory requirements as they adopt an in position realization of wavelet transform. Unlike traditional wavelets the computations for lifting wavelets are performed in integer domain rather than real domain. More over the inverse process in lifting wavelets is ruination of the processes performed during the forward transformation. *Lifting* designs perfect reconstruction filter banks by beginning from the basic nature of the wavelet transform. Wavelet transforms build sparse representations by exploiting the correlation inherent in most real world data [20] (see Fig. 3).

A single lifting step can be described by the following three basic operations:

Split — the signal split into disjoint components. A common way to do this is to extract the even and odd polyphase components explained in Polyphase Representation. This is also known as the *lazy wavelet*.

Predict — the odd polyphase component based on a linear combination of samples of the even polyphase component. The samples of the odd polyphase component are replaced by the difference between the odd polyphase component and the predicted value. The predict operation is also referred to as the *dual lifting step*.

Update — the even polyphase component based on a linear combination of difference samples obtained from the predict step. The update step is also referred to as the *primal lifting step*.

In practice, a normalization is incorporated for both the primal and dual lifting's.

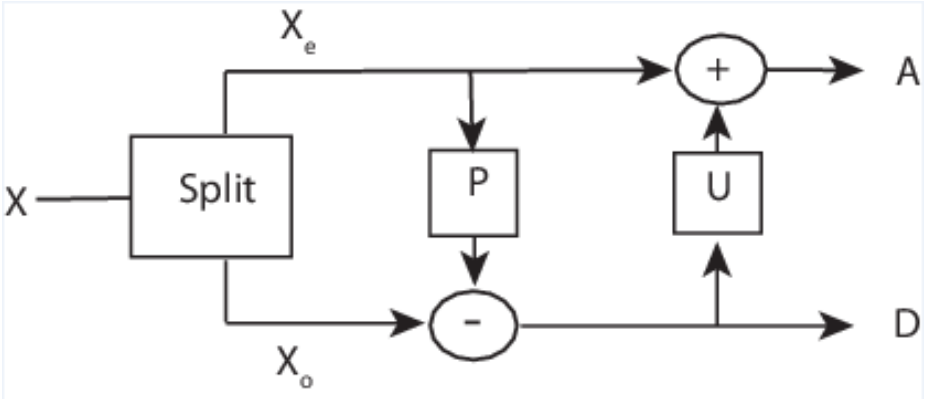

Fig. 3. One lifting step illustration.

2.3. Singular Value Decomposition (SVD)

Among the methods to write a matrix as a product of matrices, Singular Value Decomposition (SVD) is a very useful method. Singular Value Decomposition (SVD) is said to be a significant topic in linear algebra by many renowned mathematicians [19]. SVD has many practical and theoretical values; Special feature of SVD is that it can be performed on any real (m, n) matrix. Let's say we have a matrix A with m rows and n columns, with rank r and $r \leq n \leq m$. Then the A can be factorized into three matrices: Since an image can be represented as a matrix of positive scalar values SVD for any image say A of size $m \times m$ is a factorization of the form given by.

$$A = USV^T \tag{3}$$

$$U = [u_1, u_2, ..., u_r, u_{r+1}, ..., u_m] \tag{4}$$

$$V = [v_1, v_2, \ldots, v_r, v_{r+1}, \ldots, v_n] \tag{5}$$

where *U* and *V* are orthogonal matrices in which columns of *U* are left singular vectors and columns of *V* are right singular vectors of image A. *S* is a diagonal matrix of singular values in decreasing order.

$$S = \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & \sigma_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \sigma_{r+1} & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & \sigma_n \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} \tag{6}$$

The basic idea behind SVD technique of watermarking is to find SVD of image and the altering the singular value to embed the watermark. In Digital watermarking schemes, SVD is used due to its main properties namely

a) A small agitation added in the image, does not cause large variation in its singular values.
b) The singular value represents intrinsic algebraic image properties.

2.4. Encryption Algorithms

Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) Algorithm. RSA is an asymmetric key encryption algorithm [23]. Over 1000 bits long numbers are used. Therefore, it can avoid attacks like brute force, man-in-middle, and so on. RSA algorithm (Zhou *et al*., 2011) involves the following steps (a) Key (private, public) generation. (b) Encryption is performed using receiver's public key c) At the receiver's side decryption is performed using the receiver's private key [24]. Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001 [25]. It has 128,192, or 256 bits variable key length. AES encryption is fast and flexible in block ciphers and can be implemented on various platforms. AES (specifies a cryptographic algorithm that can be used to protect electronic data. AES algorithm is a symmetric block cipher, which can encrypt and decrypt the information. In this work 8 rounds and 256 bit key lengths are used. AES Encryption includes the following steps. 1. Key Expansion, 2. Initial Round, 3. Nine Rounds, 4. Final Round. Initial round has only added round key operation. Each round has the following steps, a. Substitute Bytes, b. Shift Rows. Mix columns. Add Round Key. In the final round steps a, b, and d are performed, excluding step: c. AES Decryption part a 10 set of reverse rounds are performed to transform encrypted image into the watermarked images using the same encryption key [25].

3. Bacterial Foraging Optimization Algorithm (BFOA)

Swarm intelligence, as an emerging intelligent computing technology, has been the focus of attention of artificial intelligence researchers. In 2002, Passino who was inspired by the social foraging behavior of Escherichia coli, proposed the Bacteria Foraging Optimization Algorithm (BFOA), which has become a new member in the coveted realm of swarm intelligence [26]. Since its inception, BFOA has drawn the attention

of researchers in different fields of knowledge, in terms of its biological motivation, and elegant structure. The algorithm has been instructed in optimal search by swarm intelligence, which is produced by cooperation and competition among individuals within groups. It has advantages, such as parallel distributed processing, insensitivity to initial value, and global optimization. In the process of foraging, E. coli bacteria undergo four stages, namely, chemo taxis, swarming, reproduction, and elimination and dispersal. In search space, BFOA seek optimum value through the chemo taxis of bacteria, and realize quorum sensing via assemble function between bacterial, and satisfy the evolution rule of the survival of the fittest make use of reproduction operation, and use elimination-dispersal mechanism to avoiding falling into premature convergence [26].

The motion patterns that the bacteria will generate in the presence of chemical attractants and repellents are called chemo taxis. For E. coli, this process was simulated by two different moving ways: run or tumble. A Bacterium alternates between these two modes of operation its entire lifetime. The bacterium sometimes tumbles after a tumble or tumbles after a run. This alternation between the two modes will move the bacterium, and this enables it to "search" for nutrients. An interesting group behavior has been observed for several motile species of bacteria including E.coli and S. typhimurium. When a group of E. coli cells is placed in the center of a semisolid agar with a single nutrient chemo-effector, they move out from the center in a traveling ring of cells by moving up the nutrient gradient created by consumption of the nutrient by the group. To achieve this, function to model the cell-to-cell signaling via an attractant and a repellent.

The Steps involved in BFOA is as given below.

Step 1: Initialization of BFOA parameters.

Step 2: Evaluate Fitness in the form of Objective Function.

Step 3: Initiate Chemo taxis Tumble / Run

Step 4: Check for End of Chemo taxis if yes go to Step5 otherwise go to Step 2

Step 5: Start Reproduction

Step 6: Check if it is end of Reproduction as initiate, if yes go to Step 7 else go to Step 2

Step 7: Initiate Elimination and dispersion

Step 8: If end of Elimination and dispersion then go to next Step, or else go to Step 2

Step 9: Provide the Optimized parameters for embedding watermark.

BFOA is coded using MatLab and the parameters of algorithm used in this research work are as mentioned Table 1.

Table 1. Control Parameters of Bacterial Foraging Optimization Algorithm

S.No	Parameters	Values
1	Number of bacterium, S	50
2	Maximum number of steps, Ns	4
3	Number of chemo tactic steps, Nc	100
4	Number of reproduction steps, Nre	4
5	Number of elimination-dispersal steps, Ned	2
6	Probability, Ped	0.25
7	Size of the step, $C(i)$	0.1

4. Problem Formulation for Multi-objective Optimization

Multi-objective optimization is an appropriate tool for handling different incommensurable objectives with conflicting/ supporting relations or not having any mathematical relation with each other. In this work the multi-objective optimization problem is transformed into a scalar optimization problem with different

performance measures represented in it. This kind of scenario is typical of medical images in which it is of foremost importance maintain and preserve the diagnostic information in the medial image.

Unlike regular watermarking scheme where in the original image is of importance to the user, in this proposed scheme the watermark (medical image) is of much value to the user. Different performance parameters like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalized Coefficient (NC) and Structural Similarity Index (SSIM) is used to frame this multi-objective function Any watermarking scheme should provide robustness, imperceptibility and also should be capable of maintaining the structural integrity of the watermark (medical image). The watermark embedding parameters plays a very crucial role in defining these parameters. In this work the type of wavelet in a particular wavelet family of Discrete Wavelet Transform (DWT) and the scaling factor used in Singular Value Decomposition (SVD) are using the multi-objective optimization function. The fitness function used for this multi-objective optimization is

$$\text{Min } \{f = (100\text{-}PSNR) + (1\text{-}NC) + (1\text{-}SSIM) + MSE\} \tag{7}$$

The Peak Signal to Noise Ratio (PSNR) is used to find the deviation of watermarked and attacked image from the original image. Equation (8) represents the PSNR. In this equation mean squared error (MSE) for two $M \times N$ monochrome images f and z and it is given by Equation (9). MaxBits gives the maximum possible pixel value (255) of the image.

$$PSNR = 10X \log_{10} \frac{\max Bits^2}{MSE} \tag{8}$$

$$MSE = \frac{1}{MxN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} ((f(x,y) - z(x,y))^2 \tag{9}$$

Normalized Coefficient (NC) gives a measure of the robustness of watermarking. After extracting the watermark, the normalized correlation coefficient (NC) is computed between the original watermark and the extracted watermark using Equation (10). This is used to judge the existence of the watermark and to measure the correctness of the extracted watermark.

$$NC = \frac{\sum_i^j w(i,j)w'(i,j)}{\sqrt{\sum_i^j w(i,j)^2 \sum_i^j w'(i,j)^2}} \tag{10}$$

where, w and w' represent the original and extracted watermark, respectively.

Structural Similarity Index (SSIM) index is a method for measuring the similarity between embedded and extracted watermark images. The SSIM is measured between two windows X and Y of common size $N \times N$ on image using Equation (11).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{11}$$

A typical flow chart representation of the optimization process is described in the Fig. 4 below

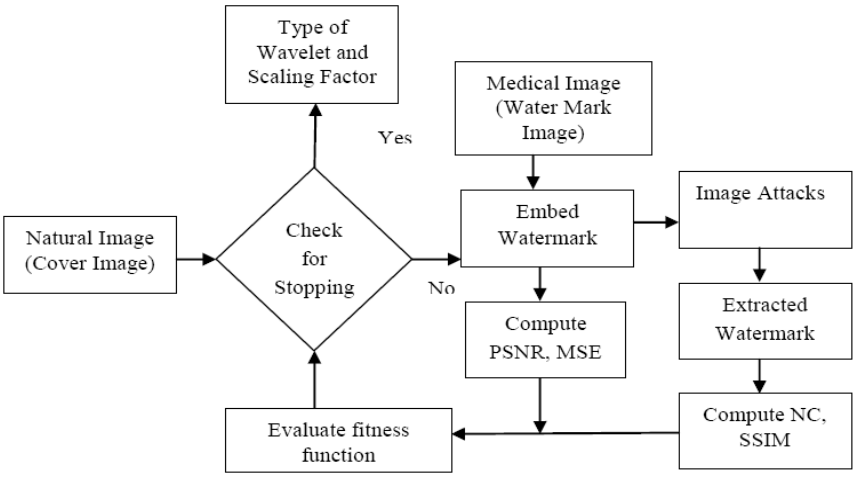

Fig. 4. Flow chart of optimization process used in this work.

5. Proposed Algorithm

The water marking is proposed to be implemented using a hybrid approach which encompasses Lifting Wavelet Transforms (LWT) and Singular Value Decomposition (SVD) techniques. The resultant of multi-objective optimization in form type of wavelet in a particular wavelet family of Discrete Wavelet Transform (DWT) and the scaling factor used in Singular Value Decomposition (SVD) is used in the process of embedding and extracting the watermark. In this algorithm, Medical image is taken as the watermark and it is embedded in each block of the Natural image (cover image) by altering the wavelet coefficients of selected DWT sub bands. The steps involved in this process are described below.

5.1. Watermark Embedding and Encryption

Step 1: Obtaining the medical image(watermark) to be embedded and the input natural image(original image).

Step 2: Performing LWT by using the optimized selection of wavelet obtained through optimization approach on the natural image to decompose it into four non-overlapping sub-bands: LL, HL, LH, and HH.

Step 3: Applying SVD to *HL* sub band i.e., $A_i=U_iS_iV_iT$, where $A_i=HL$

Step 4: Applying SVD to the watermark i.e., $w=U_wS_wV_wT$, where $W=Watermark$

Step 5: Modifying the singular value of A_i by embedding singular value of W such that , $S_{iw}=S_i+\alpha\times S_w$,Where *Siw* is modified singular matrix of *Ai* and α denotes the scaling factor, is used to control the strength of watermark signal the value of which is optimized through metaheuristic approaches(GA/DE/BFOA) using the multi objective function.

Step 6: Then applying SVD to this modified singular matrix S_{iw} i.e., $S_{iw}=U_S_{iw}S_S_{iw}V_S_{iw}$T and obtain the modified LWT coefficients, i.e., $A_{iw}=U_i\times S\_S_{iw}\times V_iT$

Step 7: Obtaining the watermarked image *Aw* by applying inverse LWT using one modified and other non modified LWT coefficients.

Step 8: Encrypting the watermarked image with RSA or AES algorithms in the time domain

5.2. Decryption and Watermark Extraction

Step 1: Decrypting the encrypted image to obtain the watermarked image.

Step 2: Applying the chosen LWT to decompose the watermarked image *Aw* in to four sub bands (i.e., *LL, nd HH*).

Step 3: Applying SVD to *HL* sub band i.e., $iw=U_{iw}S_{iw}V_{iw}$, where $A_{iw}=HL$. Compute $S_w*=(S_{iw}-S_i)/\alpha$, where S_w* singular matrix of extracted watermark.

Step 4: Applying SVD to S_w* i.e., $S_w{}^*=U\_S_w*S\_S_{wn}*V\_S_w*T$.

Step 5: Computing the extracted watermark W^* i.e., $W^*=U_w \times S\_S_w{}^* \times V_w T$.

6. The Graphical User Interface (GUI)

A comprehensive tool capable of performing watermarking and different analysis as required by the user is designed. The tool is proposed to be in the form of a Graphical User Interface (GUI) which enables the user to have ease of operation in loading the image, watermark it, encrypt it and also retrieve the original image whenever necessary. The tool is coded using Matlab Version 7.1. A Graphical User Interface enable the user to have seamless use and flexibility of operation. The implementation is carried out in a system having Core 2 Duo processor cloaking at a speed of 2 GHz with a RAM of 2GB.

Fig. 5. Screen shot of the GUI.

The functional icons present in the GUI can be described as below in reference to the Fig. 5.

1) Functional icon used to load the natural image and the medical image to be watermarked and encrypted.

2) This functional icon is used to choose different wavelet techniques and method for the implementation of watermarking.

3) This functional icon enables the user to test the watermark images against a set of standard attacks.

4) Functional icon used to implement the encryption of the image.

5) Functions used to decrypt the image and retrieve the watermark which in this case is the medical image.

6) The resultant images of the process are displayed here.

7) The values of the validation parameters arte displayed here.

7. Results and Discussion

To validate the proposed approach, a Brain MRI image (MI1), a Knee MRI image (MI2), a Lung CT image (MI3) and an Ultrasound image (MI4) of fetus are considered as the medical image that has to be used as the watermark image. The medical images are resized to have a size of 512×512 to enable ease of computation and comparison of test results. The medical images used are indicatively represented in the Fig. 6.

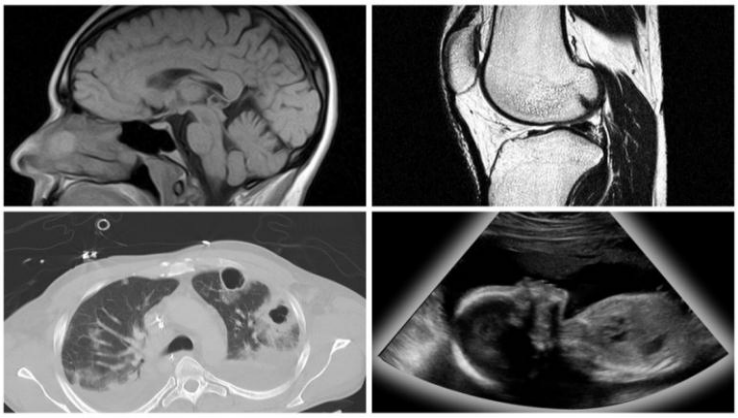

Fig. 6. Different medical Images used in this work.

Four standard test images are used as natural images for embedding the watermark. The details of the images are enlisted in the Table 2.

Table 2. Natural Images Used for Embedding the Watermark

S.No.	Image	Name	Size (Pixels)	Memory (Kilo Bytes)
1	Image 1	Lena	512×512	443
2	Image 2	Fruits	512×512	169
3	Image 3	Pepper	512×512	31.2
4	Image 4	Baboon	512×512	75.4

Four different Discrete Wavelet families namely Haar, Daubechies, Symlets and Bior splines are used in this work. RSA and AES encryption algorithms are used for encrypting the watermarked images. The Bacterial Foraging Optimization Algorithm is used for optimization, the process can be initiated through the GUI. The Fig. 7 illustrates the steps involved in operation of the method and the tool designed.

The encryption algorithm is evaluated on the basis of correlation values. The correlation between two images refers to similarity in them. The correlation value is computed using Equation (10).

$$CV = \frac{E(xy) - E(x)E(y)}{\sqrt{E(x^2) - (E(x))^2}\sqrt{E(y^2) - (E(y))^2}} \tag{10}$$

where x and y represents the input and encrypted image

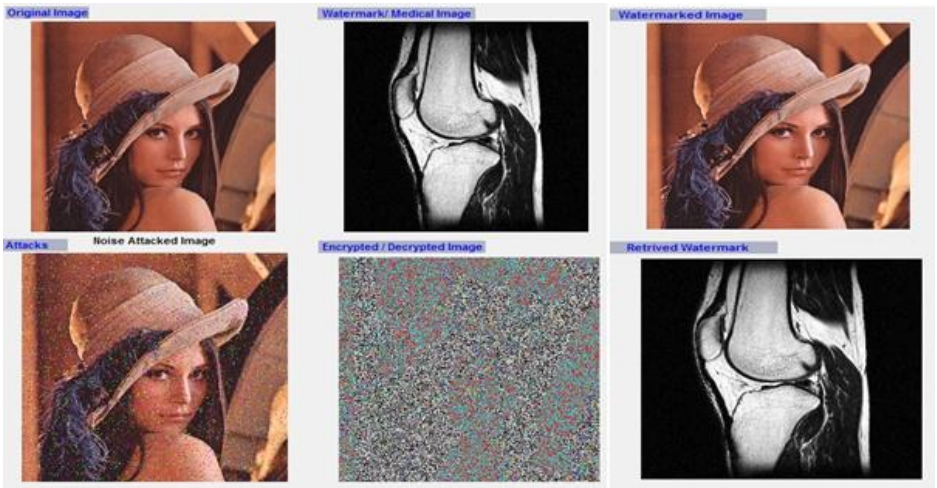

Fig. 7. From Top Left: Natural image, watermark, watermarked image, cropped watermarked image, encrypted image, extracted watermark.

The Natural image, Image 1 is taken as a representative image for analysis, and the MRI Knee Image (MI2) is considered to be the watermark. The watermark embedding process is optimized using Bacterial Foraging Optimization (BFOA) and the results presented below are the best of the ten trial runs. Table 3 and Table 4 represent the performance of different types of wavelets families and the scalar function as optimized by the proposed approach.

Table 3. Comparison in Performance of PSNR, NC and SSIM between DWT and LWT

DWT	PSNR(dB)		NC		SSIM			
	DWT	LWT	DWT	LWT	DWT-RSA	DWT-AES	LWT-RSA	LWT-AES
Haar	62.4577	62.4577	0.995303	0.995303	0.998865	0.999041	0.998865	0.999041
Daubechies	68.0497	69.7784	0.971385	0.96528	0.999285	0.999461	0.999347	0.999523
Symlets	62.7395	62.7395	0.993972	0.993972	0.998905	0.999081	0.998905	0.999081
Bior Splines	61.812	62.2497	0.998431	0.996262	0.998795	0.998971	0.996262	0.999039

Table 4. Comparison of DWT Type, Scalar Value and CV for DWT and LWT

DWT	DWT Type		Scalar value		CV			
	DWT	LWT	DWT	LWT	DWT-RSA	DWT-AES	LWT-RSA	LWT-AES
Haar	haar	Haar	0.102353	0.102353	0.00247327	0.00252491	0.00247327	0.00252491
Daubechies	db10	db10	0.08	0.0733333	0.00305214	0.00310378	0.00353845	0.0035901
Symlets	sym5	sym5	0.102353	0.102353	0.00268098	0.00273263	0.00268098	0.00273263
Bior Splines	bior2.4	bior2.4	0.107059	0.104706	0.00243458	0.00248623	0.00252918	0.00258082

Table 3 and Table 4 give an indication about the influence on different types of wavelets on image watermarking. The Fig. 8 depicts the plot of PSNR as obtained by both of DWT and LWT schemes. It can be observed that both the schemes are capable of returning high PSNR values across different wavelet families. Fig. 9 and Fig. 10 provide the comparison of DWT and LWT schemes in relation between the scalar coefficient values used for SVD and its effect on PSNR. It can be observed that low scalar value results in high PSNR (see Fig. 11).

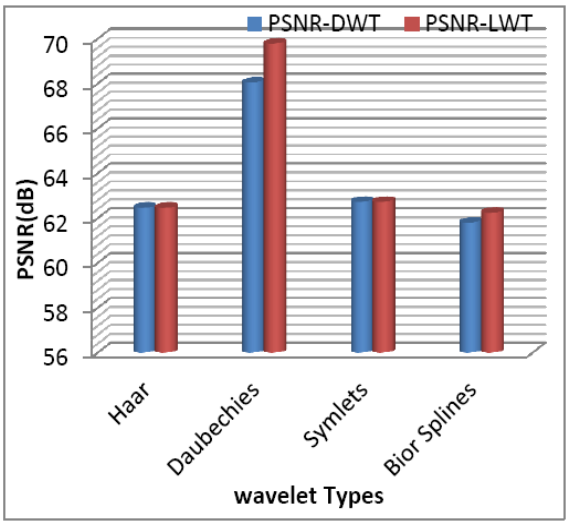

Fig. 8. Plot of PSNR values for DWT and for LWT.

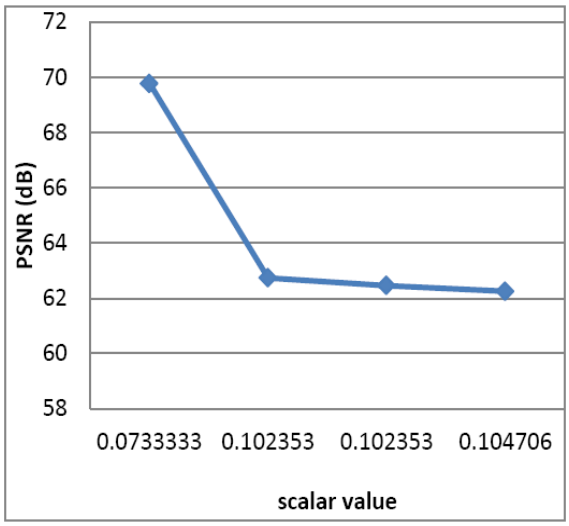

Fig. 9. Plot of optimized scalar value and PSNR of watermarked Image (DWT).

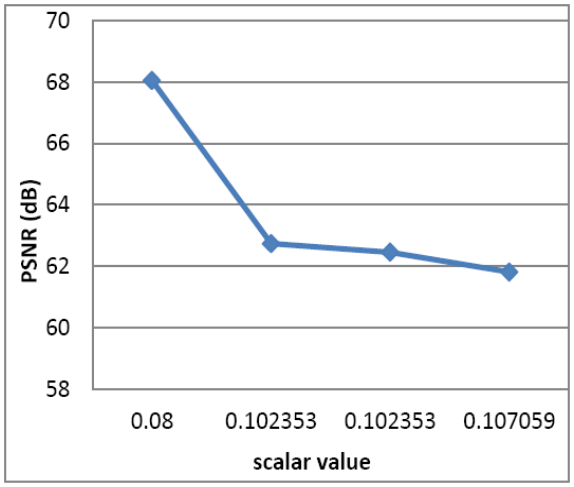

Fig. 10. Optimized scalar value and PSNR of watermarked Image.

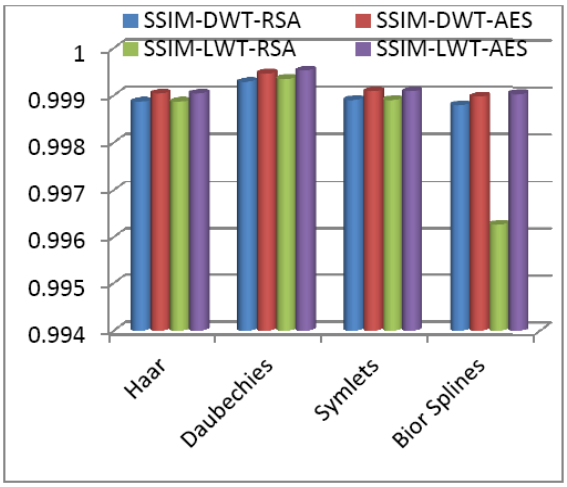

Fig. 11. SSIM for different wavelet families.

Table 5. Comparison in Performance of Watermarking for Different Noise Attacks between DWT and LWT

DWT	Attack	PSNR(dB)		NC	
		DWT	LWT	DWT	LWT
Haar	No Attack	62.4577	62.4577	0.995303	0.995303
	Sharpening	47.2594	47.2594	1	1
	Smoothening	62.1787	62.1787	0.992956	0.992956
	MotionBlurr	53.6825	53.6825	0.971143	0.971143
	Salt &pepperNoise	40.5562	40.5505	0.991573	0.991364
	Gaussian Noise	44.6866	44.7029	0.992237	0.991674
	Speckle Noise	46.3532	46.3656	0.984188	0.98385
	Poisson	56.6391	56.1148	0.993706	0.997988
Dabuchies	No Attack	68.0497	69.7784	0.999285	0.96528
	Sharpening	48.0031	48.9149	0.995213	0.974826
	Smoothening	65.4188	70.8148	0.977789	0.956832
	MotionBlurr	54.8412	56.2307	0.956095	0.935604
	Salt&pepper Noise	40.8121	41.1321	0.977051	0.957369
	Gaussian Noise	45.1954	45.7263	0.977065	0.957615
	Speckle Noise	47.068	47.9524	0.969974	0.950306
	Poisson	58.3901	60.8417	0.978922	0.958032
Symlets	No Attack	62.7395	62.7395	0.993972	0.993972
	Sharpening	47.3365	47.332	1	1
	Smoothening	62.4757	62.394	0.991607	0.992005
	Motion Blurr	53.8089	53.7778	0.969635	0.970037
	Salt&Pepper Noise	40.4751	40.5343	0.989688	0.990567
	Gaussian Noise	44.736	44.7507	0.99105	0.991176
	Speckle Noise	46.4317	46.4319	0.983783	0.983238
	Poisson	56.7956	56.7612	0.992302	0.992453
Bior Splines	No Attack	61.812	62.2497	0.998431	0.996262
	Sharpening	47.3223	47.2027	1	1
	Smoothening	62.8138	62.0125	0.989901	0.99389
	Motion Blurr	53.959	53.6378	0.967835	0.971835
	Salt&Pepper Noise	40.6741	40.5431	0.988803	0.992254
	Gaussian Noise	44.8093	44.6858	0.989107	0.99269
	Speckle Noise	46.4955	46.3414	0.981511	0.98457
	Poisson Noise	56.9907	56.501	0.990463	0.994691

The performance of the watermarked image under different noise attacks is illustrated for 'Haar', 'Daubechies', 'Symlets' and 'Bior spline' wavelets in Table 5. Sharpening or brightness attack is carried out using a high pass filter and smoothening is implemented using a Gaussian low pass filter. The tools allows the user to select different parameters of attack like noise density, mean of noise, variance of noise etc. The Salt & Pepper noise is tested using a noise density of 0.05; with the Gaussian noise being tested with a mean of 0.0 and variance of 0.01. The speckle noise has a variance of 0.04.

From Table 5, it can be clearly observed that the watermarked preserves its integrity amidst different types of attacks. The PSNR value and the NC value both continue to be on the higher side, implying the fact that the watermarked image is both imperceptible as well as robust. It can also be observed that the 'Haar' wavelet gives slightly better performance compared to 'Bior Splines in regard to NC values and slightly lower performance in regard to PSNR. Fig. 12 and Fig. 13 provide the plots of variation in changes of PSNR and NC values for different wavelet families.

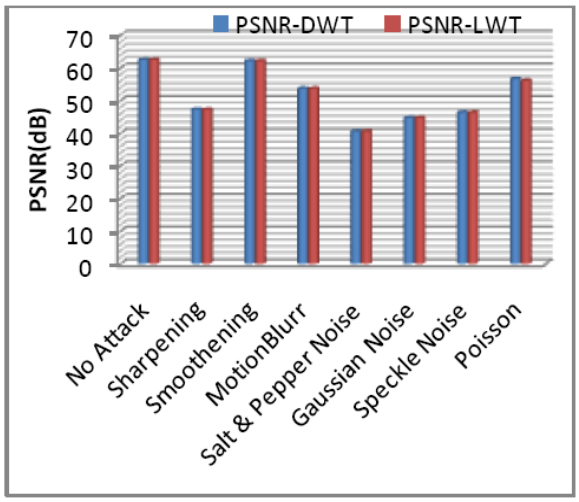

Fig. 12. Plot of degradation in performance of PSNR for No attack, sharpening, smoothening, Motion Blurr, Salt & Pepper Noise, Gaussian Noise, Speckle Noise, Poisson noise attacks for Haar wavelet.

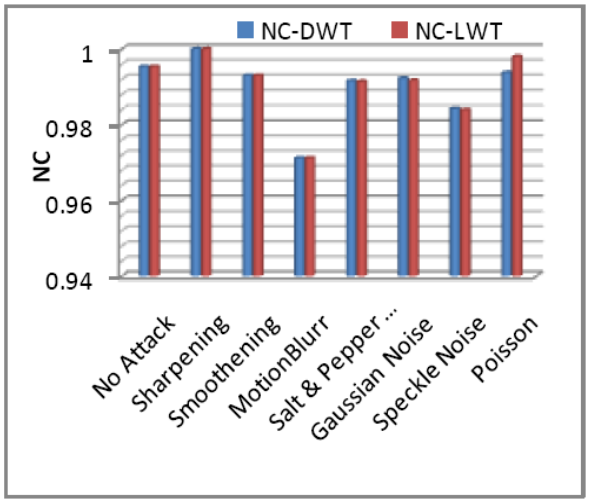

Fig. 13. Plot of degradation in performance of NC for No attack, sharpening, smoothening, Motion Blurr, Salt & Pepper Noise, Gaussian Noise, Speckle Noise, Poisson noise attacks for Haar wavelet.

The best optimized value of BFOA for DWT scheme is presented in Table 6 while the best performance of BFOA for LWT scheme is presented in Table 7.

Table 6. The best Optimization Results by BFOA for DWT

DWT	Type	Scalar Value	PSNR (dB)	MSE	NC	SSIM		CV	
						RSA	AES	RSA	AES
Daubechies	db10	0.08	68.05	0.0011083	0.971385	0.999285	0.999461	0.00305	0.003103

Table 7. The Best Optimization Results by BFOA for LWT

DWT	Type	Scalar Value	PSNR (dB)	MSE	NC	SSIM		CV	
						RSA	AES	RSA	AES
Daubechies	db10	0.0733333	69.79	0.000932	0.96528	0.999347	0.999523	0.00353	0.00359

8. Conclusion

A robust and imperceptible watermarking approach is designed and implemented for medical images. This dual approach of having watermarking and encryption improves the authenticity and the integrity of the medical images to a great extent and at the same time preserves the privacy of the medical information. Bacterial Foraging Optimization Algorithm (BFOA) based optimization and formulation of multi objective optimization has ensured the watermark is optimized and the tradeoff between imperceptibility and robustness is acceptable. The robustness was established by subjecting the watermark to different types of noise attacks. Performance measures indicate that the proposed approach is robust and reliable with most of the approaches producing structural similarity index close to one. The correlation values being close to zero indicate that the encryption is performing satisfactorily and both encryption algorithms gives results in comparable terms. The watermark also proved impervious to different types of attacks. The Graphical User Interface provides the user with flexibility and ease of operation. The objectives of analysis are met like choosing the type of wavelet, comparing the performance of DWT and LWT and studying the effect of BFOA. The LWT method provides a slightly better performance when compared to the DWT method.

References

[1] Schou, C. D., Frost, J., & Maconachy, W. V. (2004). Information assurance in biomedical informatics systems. *IEEE Engineering in Medicine and Biology Magazine*, *23(1)*, 110–118.

[2] Jiansheng, M., Sukang, L., & Tan, X. M. (May 2009). A digital watermarking algorithm based on DCT and DWT. *Proceedings of the 2009 International Symposium on Web Information Systems and Applications* (pp. 104–107). Nanchang, PR China.

[3] Piao, C., Woo, D., Park, D., & Han, S. (2008). Medical image authentication using hash function and integer Wavelet transform. *Congress on Image and Signal Processing*.

[4] Woo, C. S., Du, J., & Pham, B. (February 2005). Multiple watermark method for privacy control and tamper detection in medical images. *Proceedings of WDIC 2005* (pp. 59–64). Australia.

[5] Nambakhsh, M., Ahmadian, A., & Zaidi, H. (2001). A contextual based double watermarking of PET images by patient ID and ECG signal. *Computer Methods and Programs in Biomedicine*, *104(3)*, 341–353.

[6] You, X., Du, L., Cheung, Y., & Chen, Q. (June 2010). A blind watermarking scheme using new nontensor product wavelet filter bank. *IEEE Trans On Image Processing*, *19(12)*, 3271–3284.

[7] Lin, W., Horng, S., Kao, T., Fan, P., Lee, C., & Pan, Y. (June 2008). An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Trans on Multimedia*, *10(5)*, 746–757.

[8] Kannammal A., & Subha-Rani, S. (2012). Double watermarking of DICOM medical images using wavelet decomposition technique. *Eur J. Sci Res, 1(1)*, 46–55.

[9] Liu, R. Z., & Tan, T. N. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Trans. On Multimedia*, *4(1)*, 121–128.

[10] Chang, C.-C., Tsai, P., & Lin, C.-C. (July 2005). SVD-based digital image watermarking scheme. *Pattern Recognition Letters*, *26(10)*, 1577-1586.

[11] Bouslimi, D., Coatrieux, G., & Cozic, M. (Sept. 2012). A joint encryption/watermarking systems for verifying the reliability of medical images. *IEEE Trans Information Technol Biomed*, *16(5)*, 891–899.

[12] Cao, F., Huang, H. K., & Zhou, X. Q. (2003). Medical image security in HIPAA mandated PACS environment. *Computer Med Imaging Graphics, 27(2)*, 185–196.

[13] Kobayashi, L. O. M., Furuie, S. S., & Barreto, P. S. L. M. (2009). Providing integrity and authenticity in DICOM images: A novel approach. *IEEE TransInform Technol Biomed*, *13(4)*, 582–589.

[14] Thambiraja, E., Ramesh, G., & Umarani, R. (2012). A survey on various most common encryption techniques. *Int J. Adv Res Comput Sci Software Eng*, *2(7)*, 226–233.

[15] Puech, W., & Rodrigues, J. M. (2004). A new crypto watermarking method for medical images safe transfer. *Proceedings of the 12th European Signal Processing Conference* (pp. 1481–1484). Vienna, Austria.

[16] Sikander, B., Ishtiaq, M., Jaffar, M. A., Tariq, M., & Mirza, A. M. (April 2010). Adaptive digital watermarking of images using genetic algorithm, information science and applications (ICISA). *Proceedings of International Conference on Information Science and Applications* (pp. 1-8).

[17] Gharghory, S. M. (June 2011). Hybrid of particle swarm optimization with evolutionary operators to fragile image watermarking based DCT. *International Journal of Computer Science & Information Technology*, *3(3)*, 141-157.

[18] Aslantas, V. (July 2008). Optimal SVD based Robust Watermarking using Differential Evolution Algorithm. *Proceedings of the World Congress on Engineering 2008*. London, U. K.

[19] Musrrat, A., Chang, W. A., & Millie, P. (January 2014). A robust image watermarking technique using SVD and differential evolution in DCT domain. *International Journal for Light and Electron Optics*, *125(1)*, 428–434.

[20] Sweldens. (1998). The lifting scheme: A construction of second generation wavelets. *SIAM Journal on Mathematical Analysis*, *29(2)*, 511-546.

[21] *Matlab R 2012 a Wavelet Tool Box Reference Manual*.

[22] *Matlab R 2012 a Optimization Tool Box Reference Manual.*

[23] (October 27, 2012). PKCS #1 v2.2: RSA Cryptography Standard RSA Laboratories.

[24] Zhou, X., & Tang, X. F. (July 2011). Research and implementation of RSA algorithm for encryption and decryption. *Proceedings of 6th International Forum on Strategic Technology* (pp. 1118–1121).

[25] (November 26, 2001). *Federal Information Processing Standards Publication (FIPS 197)*. Advanced Encryption Standard (AES).

[26] Passino, K. M. (Jun. 2002). Biomimicry of bacterial foraging for distributed optimization and control. *Control Systems, IEEE*, *22(3)*, 52-67.

C. H. Venugopal Reddy was born in Nellore, India, in 1978. He is working in the Department of ECE, Nalanda Institute of Engineering & Technology, Sattenapally, Guntur, affiliated to JNTU Kakinada, A. P. he has more than 15 years of teaching experience. He got his B.Tech degree from K.S.R.M. Engg. College, Kadapa, A. P., affiliated to S.V University, Tirupathi, A. P. He received his M.E degree from Dr. M. G. R. Engg. College, Chennai, T. N. affiliated to Anna University, Chennai. He is presently pursuing his PhD degree in the area of digital image water marking, Acharya Nagarjuna University, Guntur. He has a good number of research publications in his credit. His research interests are in the areas of digital image watermarking, signal & image processing and communications.

P. Siddaiah was born in Nellore, India. He obtained a B.Tech degree in electronics and communication engineering from JNTUA college of Engineering in 1988. He received his M.Tech degree from SV University, Tirupathi. He did his PhD program in JNTU, Hyderabad. He is the chief investigator for several outstanding projects sponsored by Defense Organizations and AICTE, UGC & ISRO. He is currently working as a principal of University College of Engineering and Technology, Acharya Nagarjuna University, Guntur, A. P., India. He has published several papers in national and international journals and conferences.