

Genetic Algorithm Optimized Multi Objective Optimization for Medical Image Watermarking using DWT and SVD

Mr. .Venugopal Reddy .CH, Dr. Siddaiah.P

Abstract--- Integrity of data has to be preserved at all cost especially in the case of medical Images. Watermarking has been used a primary tool in maintaining the integrity of the medical images over a period of time. The primary objective of the proposed work is to design a tool for watermarking and encrypting medical images to protect integrity and provide authenticity. In this work is multi objective optimization function is proposed for medical image watermarking to ensure that the watermark maintains its structural integrity along with robustness and imperceptibility. Genetic Algorithm optimization is employed to optimize the objective function to choose a correct type of wavelet and scaling factor. The water marking is proposed to be implemented using a hybrid approach which encompasses Discrete Wavelet Transforms (DWT) and Singular Value Decomposition (SVD) technique. 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 is tested by measuring different performance parameters and subjecting it to various attacks

Index Terms: Medical Image, DWT, SVD, GA, Multi Objective Optimization, Encryption.

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 [1], given the ease with which digital content can be manipulated. In addition to diagnosis, these images also serve as valid document evidences in legal trials and insurance claims and as well as education material for illustrations in medical research etc. The integrity of such records needs be protected from unauthorized modification or destruction of information. Digital watermarking has an

important application to protect and authenticate the medical images. Digital watermarking algorithms must follow the following two important properties: firstly, it should be implemented in such a way that the visual quality degradation should not be perceptible by any human beings (called imperceptibility) and at the same time it cannot be removed by some common image processing application (called its robustness). Secondly, a good watermark algorithm should be capable to embed more amount of payload into a host signal without disturbing its imperceptibility and robustness. 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.

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 nontensor product wavelet filter banks [16] 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 [17]. 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 [18]. A novel optimal watermarking scheme based on singular value decomposition (SVD) using differential evolution algorithm (DE) is explained in [19]. Differential evolution (DE) algorithm to balance the tradeoff between robustness and imperceptibility by exploring multiple scaling factors in image watermarking is proposed in [20].

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 multiobjective optimization approach is proposed to maintain the fidelity of the watermark (medical image) as it contains valuable diagnostic information. This multiobjective 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 Genetic Algorithm to choose a particular wavelet in selected wavelet family and scaling factor of the Singular Value Decomposition (SVD). 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, smoothing, 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 Discrete Wavelet Transforms (DWT) and Singular Value Decomposition (SVD) to provide a robust and imperceptible watermark. Similarity 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

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. DWT is computed with a cascade of filters followed by a factor 2 subsampling.

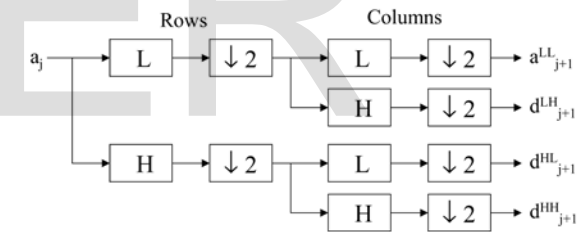


Figure (1): Discrete Wavelet Transform tree for two-dimensional image

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

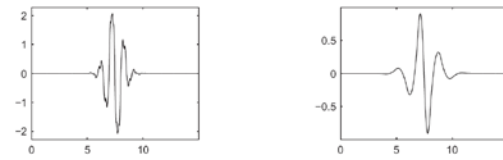
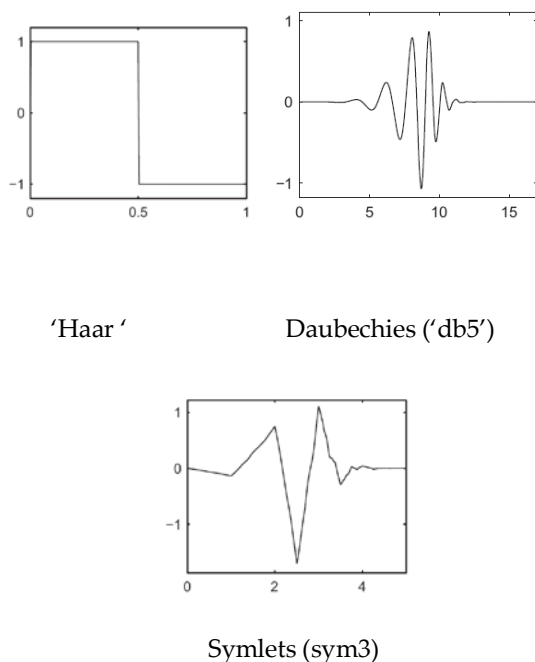
$$(2) a_{j+1}[p] = \sum_{n=-\infty}^{+\infty} l[n-2p]a_j[n] \quad (1)$$

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

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-pass 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 figure (3).



Biorthogonal ('bior3.7')

Figure (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 continue 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 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. 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.

$$A = USV^T \quad (3)$$

$$U = [u_1, u_2, \dots, u_r, u_{r+1}, \dots, u_m] \quad (4)$$

$$V = [v_1, v_2, \dots, v_r, v_{r+1}, \dots, v_n] \quad (5)$$

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.

$$S = \begin{bmatrix} \sigma_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \sigma_2 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \sigma_r & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \sigma_{r+1} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & \sigma_n \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix} \quad (6)$$

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.

2.3 Encryption Algorithms

Ron Rivest, Adi Shamir, and Leonard Adleman (RSA) Algorithm. RSA is an asymmetric key encryption algorithm [22]. 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 [22]. Advanced Encryption Standard (AES) was published by NIST (National Institute of Standards and Technology) in 2001[23]. 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 [23].

3 GENETIC ALGORITHM OPTIMIZATION

Genetic algorithm (GA) is one of the most widely used artificial intelligent techniques for optimization. GA was first developed by John Holland [24]. GA is stochastic searching algorithm based on the mechanisms of natural selection and genetics, and is very efficient in searching for global optimum solutions. The main idea of GA is to mimic the natural selection and the survival of the fittest [24]. In GA, the solutions are represented as chromosomes. The chromosomes are evaluated for fitness values and they are ranked from best to worst based on fitness value. The process to produce new solutions in GA is mimicking the natural selection of living organisms, and this process is accomplished through repeated applications of three genetic operators: selection, crossover, and mutation. First, the better chromosomes are selected to become parents to produce new offspring (new chromosomes) [24]The selection probabilities are usually defined using

the relative ranking of the fitness values. Once the parent chromosomes are selected, the crossover operator combines the chromosomes of the parents to produce new offspring (perturbation of old solutions). Mutation is a mechanism to inject diversity into the population to avoid stagnation. In addition to the population size and the maximum number of iterations, several decisions on parameters must be made for GA. Crossover method and crossover probability are the second set of decisions to be made. Finally, the mutation method and mutation probability must be selected as they may help to maintain the diversity of the population by injecting new elements into the chromosomes. In general, these three sets of decisions are set empirically using pilot runs. The flow chart of the Genetic Algorithm is shown in Figure (3).

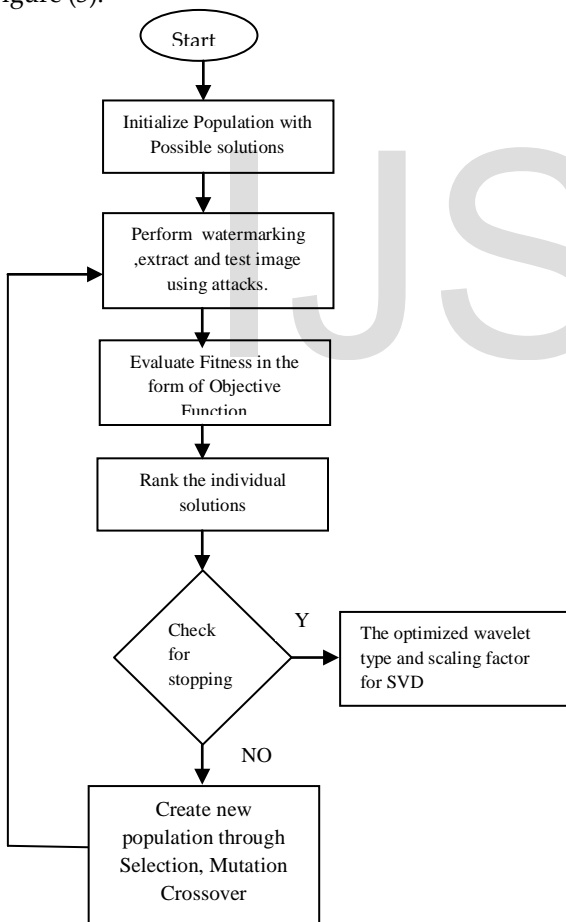


Figure (3): The flow chart of the Genetic Algorithm for the proposed optimization problem

In this work Genetic Algorithm (GA) function available in the Matlab optimization tool box is used in the proposed work. The population size is fixed at 20. The elite count used is fixed at 10 % of the population which 2. The selection is based on ranking. The cross over fraction is fixed at 0.2 and the adaptive feasible mutation function is used. The migration of the population is fixed as forward with a forward fraction of 0.2. The maximum number of generations is fixed at 100.

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

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

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.

$$PSNR = 10 \times \log_{10} \frac{MaxBits^2}{MSE} \quad (8)$$

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

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.

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

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 Eq. (11).

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

5 PROPOSED ALGORITHM

The water marking is proposed to be implemented using a hybrid approach which encompasses Discrete Wavelet Transforms (DWT) 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.

a) Watermark Embedding and Encryption.

Step 1: Obtain the medical image to be embedded and the input natural

Step 2: Perform DWT 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: Apply SVD to HL sub band i.e., $A_i = U_i S_i V_i^T$ where $A_i = HL$

Step 4: Apply SVD to the watermark i.e., $W = U W S W V W^T$ where $W = \text{Watermark}$

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

Step 6: Then apply 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 DWT coefficients, i.e., $A_{iw} = U_i \times S_{S_{iw}} \times V_i^T$

Step 7: Obtain the watermarked image A_w by applying inverse DWT using one modified and other non modified DWT coefficients.

Step 8: Then encrypt the watermarked image with RSA or AES algorithms in the time domain.

b) Decryption and Watermark Extraction

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

Step 2: Apply the chosen DWT to decompose the watermarked image A_w in to four sub bands (i.e., $LL, H, HL, \text{and } HH$).

Step 3: Apply SVD to HL sub band i.e., $i_w = U_i w S_i w V_i w T$, Where $A_{i_w} = HL$ Compute $S_w^* = (S_i w - S_i) / \alpha$, where S_w^* singular matrix of extracted watermark

Step 4: Apply SVD to S_w^* i.e., $S_w^* = U_{S_w^*} S_{S_w^*} V_{S_w^*} T$

Step 5: Now Compute extracted watermark W^* i.e., $W^* = U_{S_w^*} S_{S_w^*} V_{S_w^*} T$

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.



Figure(3): Screen Shot of the GUI

The functional icons present in the GUI can be described as below in reference to the Figure (3).

- 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, a Knee MRI image, a Lung CT image and an Ultrasound image of fetus are considered is 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 below figure (4)

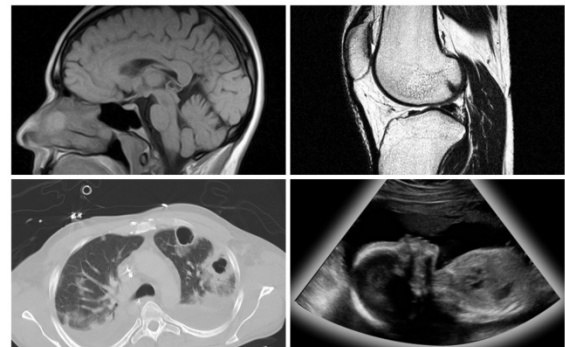


Figure (4): Different Medical Images used in this work. Three standard test images are used as natural images for embedding the watermark. The details of the images are enlisted in the table (1) below.

Table (1): 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

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 Optimization function GA is used for optimization, the process can be initiated through the GUI. The below figure illustrates the steps involved in operation of the method and the tool designed.

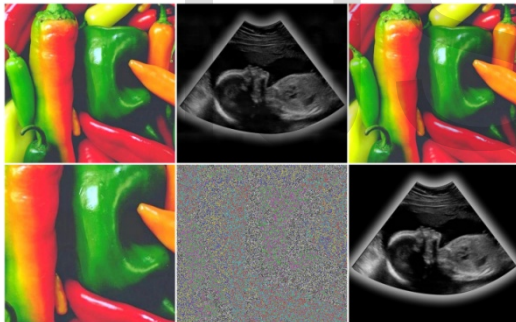


Figure (5): From Top Left: Natural Image, Watermark, Watermarked image, Cropped Watermarked image, Encrypted image, Extracted Watermark

The proposed algorithm is tested against different types of attacks namely, rotation, cropping, motion blur, sharpening and different types of noise attacks like, salt and pepper, Gaussian, speckle and poisson. The rotation operation performs a geometric transform which maps the position (x1, y1) of a picture element in an input image onto a position (x2, y2) in an output image by rotating it through user-specified angle about an origin O. Gaussian Noise is the most common form of noise encountered in most of the communication channels. The Gaussian noise with variance of 0.01, 0.05, 0.1, and 1 were added to the

image for testing. Salt and pepper noise is also known as impulse noise. Salt and pepper noise with variance of 0.001, 0.005, 0.01, 0.02, and 0.05 were added to the image for testing. The figure (6) illustrates the different attacks on the watermarked image.



Figure (6) Watermarked image attacked with different types of attacks.

The Natural image, Image 3 is taken as a representative image for analysis, and similarly the Brain MRI image is considered to be the watermark. The watermark embedding process is optimized using GA and the results presented below are the best of the ten trial runs. The below tabular column specifies performance of different types of wavelets families and the scalar function as optimized by the proposed approach. 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

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

Where x and y represents the input and encrypted image.

Table (2): Performance Measures of Different Images using different DWT approaches.

DWT	Type	Scalar Value	PSNR (db)	MSE	NC	SSIM		CV	
						RS A	AE S	RS A	AE S
Haar	Haar	0.108571	68.99033	0.0010876	0.953567	0.90012	0.900296	0.00214613	0.00219778
Daubecies	db9	0.102857	70.7744	0.000843935	0.949067	0.899188	0.899364	0.001767	0.00181864
Symlets	Sym3	0.108571	69.1677	0.00091021	0.953158	0.900059	0.900748	0.00188177	0.00194399
BiorSplines	bior3.9	0.105714	70.5463	0.000863402	0.949682	0.89936	0.90004	0.00194399	0.0020212

The table gives an indication about the influence on different types of wavelets on image watermarking

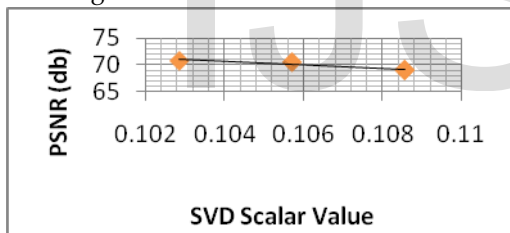


Figure (6) Plot of optimized Scalar value and PSNR of watermarked image

From the above plot (figure 6) it can be observed that low scalar value results in high PSNR value for the watermarked image

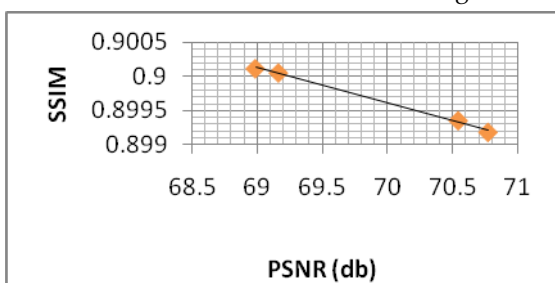


Figure (6) Plot between PSNR and SSIM

The above figure clearly shows the fact that with PSNR on the higher side the Structural Similarity Index (SSIM) moves toward the lower end. This also points to the importance of having a multi – objective function in arriving at optimization of embedding parameters.

The performance of the watermarked image under different noise attacks is illustrated for 'haar' and 'bior spline' wavelets in the below tabular column. Sharpening or brightness attack is carried out using a high pass filter and smoothing 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, degree of rotation, amount of cropping 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.

Table (3): Performance of watermark under different attacks

DWT	Attack	PSNR (db)	NC
Haar	Sharpening	52.1428	0.956058
	Smoothing	69.525	0.949277
	MotionBlurr	53.3472	0.92462
	Salt & Pepper Noise	40.0989	0.938764
	Gaussian Noise	46.7222	0.938373
	Speckle Noise	46.5712	0.91951
Bior Splines (bior .3.9)	Sharpening	52.2515	0.955004
	Smoothing	69.9922	0.948185
	MotionBlurr	53.4324	0.923468
	Salt & Pepper Noise	40.1928	0.937052
	Gaussian Noise	46.7826	0.937562
	Speckle Noise	46.6406	0.918624

From above table (3) 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 'Bio Splines in regard to NC values and slightly lower performance in regard to PSNR.

To emphasize the fact that the choice of natural image also plays a role maintaining the integrity and the performance of the watermark. A single medical image, the ultrasound image of fetus is taken and is embedded in to the three images and the performance measures analyzed. For illustrative convenience 'Haar' wavelet is chosen for embedding the watermark.

From the below table it can be clearly observed that the choice of the images also play a very crucial role in defining the performance of the watermarking procedure. From the table it can be clearly concluded that the natural image, Image 1 is more suited for embedding this chosen watermark. The PSNR performance of all the three images is comparable, but when compared for SSIM, Image 1 gives a superlative performance when compared to all other images as illustrated in the figure (7) below.

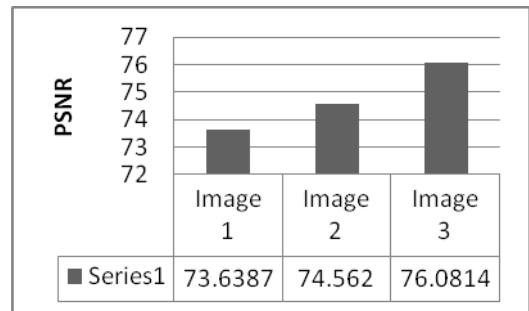
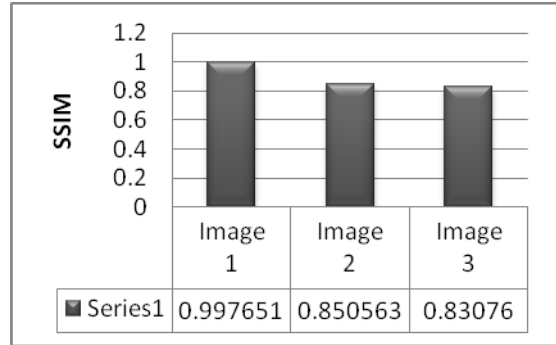


Figure (7): Plot of PSNR and SSIM values as obtained for watermark embedded in 3 natural images

Table (4): Performance Measures of a single chosen medical image when embedded in different natural images

Image	DWT Type	Scalar Value	PSNR (db)	MSE	NC	SSIM		CV	
						RSA	AES	RSA	AES
Image 1	Haar	0.102857	73.6387	0.000633741	0.950221	0.997651	0.997827	0.00334314	0.00339479
Image 2	Haar	0.108571	74.562	0.000577847	0.938612	0.850563	0.850739	0.00217783	0.00222948
Image 3	Haar	0.102857	76.0814	0.000496393	0.933832	0.83076	0.830936	0.00213863	0.00219028

8 CONCLUSION

A robust watermarking approach is designed and implemented for medical images. Such a dual approach of having watermarking and encryption improves the authenticity and the integrity of the medical images to a great extent. Genetic algorithm based optimization and formulation of multi objective optimization has ensured the water mark is optimized and the tradeoff between imperceptibility and robustness is acceptable. 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.

REFERENCES

- (1) S. Boucherkha and M. Benmohamed, A lossless watermarking based authentication system for medical images, *World Acad Sci Eng Technolgy*, (2005), 100–103.
- (2) M. Jiansheng, L. Sukang, and Tan Xiaomei, A digital watermarking algorithm based on DCT and DWT, *Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA '09) Nanchang, PR China, May 22–24, (2009)*, pp. 104–107.
- (3) C. Piao, D. Woo, D. Park, and S. Han, Medical image authentication using hash function and integer Wavelet transform, *Congress on Image and Signal Processing*, (2008).
- (4) C.S. Woo, J. Du, and B. Pham, Multiple watermark method for privacy control and tamper detection in medical images, *WDIC2005 pages, Australia, February, (2005)*, pp. 59–64.
- (5) M. Nambakhsh, A. Ahmadian, and H. Zaidi, A contextual based double watermarking of PET images by Patient ID and ECG Signal, *Comput Meth Prog*, 104 (2001), 341–353.
- (6) X. You, L. Du, Y. Cheung, and Q. Chen, A blind watermarking scheme using new nontensor product wavelet filter bank, *IEEE Trans On Image Processing*, 19 (2010).
- (7) W. Lin, S. Horng, T. Kao, P. Fan, C. Lee, and Y. Pan, An efficient watermarking method based on significant difference of wavelet coefficient quantization, *IEEE Trans On Multimedia*, 10 (2008), 746–757.
- (8) A. Kannammal and S. Subha Rani, Double watermarking of DICOM medical images using wavelet decomposition technique, *Eur J Sci Res* (1) (2012), 46–55.
- (9) R.Z. Liu and T.N. Tan “An SVD-Based Watermarking Scheme for Protecting Rightful Ownership”, *IEEE Trans. On Multimedia*, Vol. 4, No. 1, pp. 121–128, 2002.
- (10) Chin-Chen Chang, Piyu Tsai, Chia-Chen Lin, SVD-based digital image watermarking scheme, *Pattern Recognition Letters*, Volume 26, Issue 10, 15 July 2005, Pages 1577-1586
- (11) D. Bouslimi, G. Coatrieux, M. Cozic, A joint encryption/watermarking systems for verifying the reliability of medical images, *IEEE Trans Information Technol Biomed*, 16 (2012).
- (12) F. Cao, H.K. Huang, X.Q. Zhou, Medical image security in HIPAA mandated PACS environment, *Comput Med Imaging Graphics* 27 (2003), 185–196.
- (13) L.O.M. Kobayashi, S.S. Furuie, and P.S.L.M. Barreto, Providing Integrity and Authenticity in DICOM Images: A Novel Approach, *IEEE Trans Inform Technol Biomed*, 13 (2009).
- (14) E. Thambiraja, G. Ramesh, and R. Umarani, A survey on various most common encryption techniques, *Int J Adv Res Comput Sci Software Eng*, 2 (2012), 226–233.
- (15) W. Puech, J.M. Rodrigues, A new crypto watermarking method for medical images safe transfer, *Proc of the 12th European signal processing conference, Vienna, Austria, 2004*, 1481–1484.
- (16) X. You, L. Du, Y. Cheung, and Q. Chen, A blind watermarking scheme using new nontensor product wavelet filter bank, *IEEE Trans On Image Processing*, 19 (2010).
- (17) Sikander, B.; Ishtiaq, M.; Jaffar, M.A.; Tariq, M.; Mirza, A.M., "Adaptive Digital atermarking of Images Using Genetic Algorithm," *Information Science and Applications (ICISA)*, 2010 International Conference on , vol., no., pp.1,8, 21-23 April 2010
- (18) Sawsan morkos gharghory “Hybrid Of Particle Swarm Optimization With Evolutionary Operators To Fragile Image Watermarking Based Dct” *international journal of computer science & information technology (ijcsit)*, vol 3, no 3, june 2011
- (19) V. Aslantas , “Optimal SVD based Robust Watermarking using Differential Evolution Algorithm” *Proceedings of the World Congress on Engineering 2008 Vol I WCE 2008, July 2 - 4, 2008, London, U.K.*
- (20) Musrrat Ali, Chang Wook Ahn, Millie Pant, “A Robust image watermarking technique using SVD and differential evolution in DCT domain”, *Optik - International Journal for Light and Electron Optics*, Volume 125, Issue 1, January 2014

- (21) Matlab R 2012 a Wavelet Tool Box Reference Manual.
- (22) PKCS #1 v2.2: RSA Cryptography Standard RSA Laboratories October 27,, 2012.
- (23) Federal Information Processing Standards Publication 197,Advanced Encryption Standard (AES), November 26, 2001
- (24) Matlab R 2012 a Optimization Tool Box Reference Manual.

Guntur, A.P,India. He has taught a wide variety of courses for UG & PG students and guided several projects. Several members successfully completed their PhD under his guidance. He has published several papers in National and International Journals and Conferences. He is a life member of FIETE, IE, and MISTE.

Authors Biography



CH. Venugopal Reddy is working as Professor in the department of ECE, Priyadarshini College of Engineering & Technology, Nellore, affiliated to JNTU Anantapur, A.P. Has more than 13 years of teaching experience. He got his B.Tech(ECE) from K.S.R.M. Engg College, Kadapa, A.P, affiliated to S.V University, Tirupathi, A.P. M.E (Commn.Sys) from Dr. M.G.R Engg College, Chennai, T.N affiliated to Anna University, Chennai. He is presently pursuing Ph.D in the area of Digital Image Water Marking, Acharya Nagarjuna University, Guntur. He has a good No. of research publications in his credit. His research interests are in the areas of Signal Processing, Image Processing and Communications.



Dr.P.Siddaiah obtained 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 Principal, University College of Engineering and Technology, Acharya Nagarjuna University,