A Dual Security Approach for Medical Images using Encryption and Watermarking Optimized by Differential Evolution Algorithm

Mr. Ch. Venu Gopal Reddy¹, Dr. Siddaiah.P²
Professor, Department of ECE, Priyadarshini College of Engineering and Technology, Nellore, A.P, INDIA¹
Professor and Dean, Department of ECE, Principal, University College of Engineering and Technology, Acharya Nagarjuna University, Guntur, A.P, INDIA²

Abstract: Cryptography and watermarking combination appears as a good promising tool in regard to medical image security and management. In this paper a dual security approach of watermarking and encryption is proposed along with a Multi-objective function for medical image watermarking to ensure that the watermark maintains its structural integrity along with robustness and imperceptibility. Differential Evolution (DE) 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 both Discrete Wavelet Transforms (DWT) and Singular Value Decomposition (SVD) techniques. The encryption is done 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. The performance of the optimization is compared with the optimisation results of Genetic Algorithm (GA).

Keywords: Medical Image, DWT, SVD, DE, GUI, RSA, AES.

I. Introduction

Advent of multimedia combined with information and communication technology boost the potential of medical information handling and sharing with applications ranging from telediagnosis to telesurgery and cooperative and working session. Medical information protection derives from strict ethics and legislatives rules. Regulations like USA's HIPAA and Europe's EC 95/46 Directive are expressions of such a constraint. Focusing on medical information records, which for a patient are a complex set of clinical examinations, diagnosis annotations and other findings and images centered in its EPR, we recall the three mandatory security characteristics; confidentiality, availability and reliability. In Medical Information Systems (MIS), these characteristics are maintained through five security services [1]: integrity, availability, authentication, confidentiality, and non-repudiation. If availability, integrity and confidentiality services have similar definition in respect with the corresponding security component, the authentication service is “designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorizations to receive specific categories of information” [1]. Non-repudiation service manages proofs of delivery and of the message sender's identity. At the interface between the information and the MIS security services, watermarking can improve information protection from the information side.

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.

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 Differential Evolution (DE) 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. The performance measures are compared and contrasted with that of the performance measures as achieved by Genetic Algorithm (GA).

II. 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. Similar 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.
A. 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.

\[
\begin{align*}
a_{j+1}[p] &= \sum_{n=-\infty}^{\infty} l[n-2p] a_j[n] \\
d_{j+1}[p] &= \sum_{n=-\infty}^{\infty} h[n-2p] a_j[n]
\end{align*}
\]

Elements \(a_j\) are used for next step (scale) of the transform and elements \(d_j\), called wavelet coefficients, determine output of the transform. Outputs of these filters are given by equations (1) and (2).

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

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).

Elements \(a_j\) are used for next step (scale) of the transform and elements \(d_j\), called wavelet coefficients, determine output of the transform. Outputs of these filters are given by equations (1) and (2).

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 2.
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.

B. 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 ≤ n ≤ 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 × n is a factorization of the form given by.

\[ A = USV^T \]  

\[ U = \left[ u_1, u_2, \ldots, u_r, u_{r+1}, \ldots, u_m \right] \]  

\[ V = \left[ v_1, v_2, \ldots, v_r, v_{r+1}, \ldots, v_n \right] \]

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.

\[ S = \begin{bmatrix} \sigma_1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & \sigma_2 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \sigma_r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \sigma_{r+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & \cdots & \sigma_n \\ 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \end{bmatrix} \]

(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.

C. 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].

III. Optimization using Differential Evolution

Evolutionary methods for solving optimization problems have become a very popular research topic in recent years. There are three main processes in all evolutionary algorithms. The first process is the initialization process where the initial population of individuals is randomly generated according to some solution representation. Each individual represents a solution, directly or indirectly. If an indirect representation is used, each individual must first be decoded into a solution. Each solution in the population is then evaluated for fitness value in the second process. The fitness values can be used to calculate the average population fitness or to rank the individual solution within the population for the purpose of selection. The third process is the generation of a new population by perturbation of solutions in the existing population. DE was proposed by Storn and Price (1995) for global optimization over continuous search space. Its theoretical framework is simple and requires a relatively few control variables but performs well in convergence. In DE algorithm, a solution is represented by a D-dimensional vector [24]. DE starts with a randomly generated initial population of size N of D-dimensional vectors. In DE, the values in the D-dimensional space are commonly represented as real numbers. Again, the concept of solution representation is applied in DE in the same way as it is applied in GA. The key difference of DE from GA is in a new mechanism for generating new solutions. DE generates a new solution by combining several solutions with the candidate solution. The population of solutions in DE evolves through repeated cycles of three main DE operators: mutation, crossover, and selection. However, the operators are not all exactly the same as those with the same names in GA. The key process in DE is the generation of trial vector. Consider a candidate or target vector in a population of size N of D-dimensional vectors. The generation of a trial vector is accomplished by the mutation and crossover operations and can be summarized as follows. 1) Create a mutant vector by mutation of three randomly selected vectors. 2) Create trial vector by the crossover of mutant vector and target vector.

![Figure 3: The flow chart of Differential Evolution](image-url)

DE starts with a randomly generated initial population of size N of D-dimensional vectors. In DE, the values in the D-dimensional space are commonly represented as real numbers. Again, the concept of solution representation is applied in DE in the same way as it is applied in GA. The key difference of DE from GA is in a new mechanism for generating new solutions. DE generates a new solution by combining several solutions with the candidate solution. The population of solutions in DE evolves through repeated cycles of three main DE operators: mutation, crossover, and selection. However, the operators are not all exactly the same as those with the same names in GA. The key process in DE is the generation of trial vector. Consider a candidate or target vector in a population of size N of D-dimensional vectors. The generation of a trial vector is accomplished by the mutation and crossover operations and can be summarized as follows. 1) Create a mutant vector by mutation of three randomly selected vectors. 2) Create trial vector by the crossover of mutant vector and target vector.

![Figure 3: The flow chart of Differential Evolution](image-url)
As shown in Figure (3), the first process is the generation of a population of new solutions called vectors. Each vector in the population is evaluated for fitness value. Each vector takes turns as a candidate or target vector, and for each target vector, a trial vector is formed. The selection process simply chooses between the target vector and trial vector, i.e., the winning vector between the trial vector and the target vector survives into the next round while the losing vector is discarded. Several observations are made here. First, since a new solution would be selected only if it has better fitness, the average fitness of the population would be equal or better from iteration to iteration. Any improvement in the solution is immediately available to be randomly selected to form a mutant vector for the next target vector. This is different from GA and PSO where an improvement would take effect only after all the solutions has completed the iteration.

In contrast with GA where parent solutions are selected based on fitness, every solution in DE takes turns to be a target vector (one of the parents), and thus all vectors play a role as one of the parents with certainty. The second parent is the mutant vector which is formed from at least three different vectors. In other words, the trial vector is formed from at least four different vectors and would replace the target vector only if this new vector is better than the target vector; otherwise, it would be abandoned. This replacement takes place immediately without having to wait for the whole population to complete the iteration. This improved vector would then immediately be available for random selection of vectors to form the next mutant vector. In this work, Differential Evolution is coded using Matlab. The Parameters used and the settings are mentioned as mentioned below:

\[
\begin{align*}
\text{DEParamsDefault.CR} & = 0.7; \\
\text{DEParamsDefault.F} & = 0.8; \\
\text{DEParamsDefault.NP} & = 30; \\
\text{DEParamsDefault.strategy} & = 1; \\
\text{DEParamsDefault.minvalstddev} & = -1; \\
\text{DEParamsDefault.minparamstddev} & = -1; \\
\text{DEParamsDefault.nofevaliter} & = 10; \\
\text{DEParamsDefault.nochangeiter} & = 10; \\
\text{DEParamsDefault.maxiter} & = \text{inf}; \\
\text{DEParamsDefault.maxtime} & = \text{inf}; \\
\text{DEParamsDefault.refreshiter} & = 10; \\
\text{DEParamsDefault.refreshtime} & = 60; \text{ seconds}
\end{align*}
\]

### IV. 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 to 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 used in the multi-objective optimization function. The fitness function used for this multi-objective optimization is

\[
\text{Min } f = (100 - \text{PSNR}) + (1 - \text{NC}) + (1 - \text{SSIM}) + \text{MSE}
\]

(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*N monochrome images f and z and it is given by Equation (9). MaxBits gives the maximum possible pixel value (255) of the image.

\[
\text{PSNR} = 10 \times \log_{10} \frac{\text{MaxBits}^2}{\text{MSE}}
\]

(8)

\[
\text{MSE} = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} (f(x, y) - z(x, y))^2
\]

(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.
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 \( N*N \) on image using Equation (11).

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

V. 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 image.

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 \( S_{iw} = S_{iw} + \alpha \times S_w \), Where \( S_{iw} \) is modified singular matrix of \( A_i \) and \( \alpha \) denotes the scaling factor, is used to control the strength of watermark signal the value of which is optimized through Differential Evolution (DE) using the multi objective function.

Step 6: Then apply SVD to this modified singular matrix \( S_{iw} \) i.e., \( S_{iw} = U_{iw} S_{iw} V_{iw} V_{iw}^T \) and obtain the modified DWT coefficients, i.e., \( A_{iw} = U_{iw} S_{iw} V_{iw} V_{iw}^T \).

Step 7: Obtain the watermarked image \( Aw \) 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 \( Aw \) in to four sub bands (i.e., LL, LH, HL, and HH).

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

Step 4: Apply SVD to \( S_{w*} \) i.e., \( S_{w*} = U_{S_{w*}} S_{S_{w*}} V_{S_{w*}} V_{S_{w*}}^T \).

Step 5: Now Compute extracted watermark \( W* \) i.e., \( W* = U_{S_{w*}} S_{S_{w*}} V_{S_{w*}} V_{S_{w*}}^T \).

VI. The Graphical User Interface (GUI)

The functional icons present in the GUI can be described as below in reference to the Figure (4).

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 are displayed here.
VII. 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 below Figure (5). The results of Differential Evolution (DE) optimization is compared with that of Genetic Algorithm (GA).

Three standard test images are used as natural images for embedding the watermark. The details of the images are enlisted in the Table I below.

Figure 4: Screen Shot of the GUI.

Figure 5: Different Medical Images used in this work.
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 algorithm Differential Evolution is used for optimization, the process can be initiated through the GUI. The below Figure (6) 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

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

Where \(x\) and \(y\) represents the input and encrypted image.

The Natural image, Image 2 is taken as a representative image for analysis, and the CT Lung image is considered to be the watermark. The watermark embedding process is optimized using Differential Evolution (DE) and the results presented below are the best of the ten trial runs. The results are also compared against the results of Genetic Algorithm based optimization. The below tabular column specifies performance of different types of wavelets families and the scalar function as optimized by the proposed approach.

![Figure 6: From Top Left: Natural Image, Watermark, Watermarked image, Cropped Watermarked image, Encrypted image, Extracted Watermark](image-url)

Table II Performance Measures PSNR, NC, MSE of Different Images using different DWT approaches

<table>
<thead>
<tr>
<th>DWT</th>
<th>Type</th>
<th>Scalar Value</th>
<th>DE PSNR</th>
<th>GA PSNR</th>
<th>DE MSE</th>
<th>GA MSE</th>
<th>DE NC</th>
<th>GA NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Haar</td>
<td>Haar</td>
<td>0.102353</td>
<td>59.5259</td>
<td>58.357</td>
<td>0.00259911</td>
<td>0.00262427</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Daubechies</td>
<td>db10</td>
<td>0.101303</td>
<td>60.2331</td>
<td>59.9389</td>
<td>0.00242163</td>
<td>0.00249393</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Symlets</td>
<td>sym3</td>
<td>0.104706</td>
<td>59.1847</td>
<td>59.5369</td>
<td>0.00268931</td>
<td>0.00259625</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Bior Splines</td>
<td>bior2.4</td>
<td>0.102353</td>
<td>59.7208</td>
<td>59.3307</td>
<td>0.00254893</td>
<td>0.00265034</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
Table III  Performance Measures SSIM and CV of Different Images using different DWT approaches Optimized using DE and GA

<table>
<thead>
<tr>
<th>DWT</th>
<th>SSIM (RSA)</th>
<th>SSIM (AES)</th>
<th>CV (RSA)</th>
<th>CV (AES)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DE</td>
<td>GA</td>
<td>DE</td>
<td>GA</td>
</tr>
<tr>
<td>Haar</td>
<td>0.998978</td>
<td>0.998873</td>
<td>0.999155</td>
<td>0.998100</td>
</tr>
<tr>
<td>Daubechies</td>
<td>0.998848</td>
<td>0.998815</td>
<td>0.999024</td>
<td>0.998991</td>
</tr>
<tr>
<td>Symlets</td>
<td>0.998896</td>
<td>0.998942</td>
<td>0.999072</td>
<td>0.999118</td>
</tr>
<tr>
<td>Bior Splines</td>
<td>0.999039</td>
<td>0.999051</td>
<td>0.999216</td>
<td>0.999227</td>
</tr>
</tbody>
</table>

From table (3) it can be observed that multi-objective optimization has resulted in very high PSNR values and NC values. Both Genetic Algorithm (GA) and Differential Evolution optimization performs well for this optimization problem, and the fact despite having such a high SNR, the NC value and the SSIM is very close to 1. This shows that, this kind of optimization approach is highly suitable in medical watermarking. 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 $(x_1, y_1)$ of a picture element in an input image onto a position $(x_2, y_2)$ in an output image by rotating it through user-specified angle about an origin O. The Figure (7) illustrates the different attacks on the watermarked image.

![Figure 7: Watermarked image attacked with different types of attacks.](image-url)
From above Table IV 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 ‘DE gives slightly better performance when compared to GA based optimization. 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 noise density of 0.001, 0.005, 0.01, 0.02, and 0.05 were added to the image for testing as shown in Figure (8) and (9).

<table>
<thead>
<tr>
<th>DWT</th>
<th>Attack Type</th>
<th>PSNR (db)</th>
<th>NC</th>
<th>PSNR (db)</th>
<th>NC</th>
</tr>
</thead>
<tbody>
<tr>
<td>'db 10'</td>
<td>Sharpening</td>
<td>46.8779</td>
<td>1</td>
<td>46.7961</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Smoothening</td>
<td>59.9865</td>
<td>1</td>
<td>59.702</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>MotionBlur</td>
<td>52.5703</td>
<td>0.983088</td>
<td>52.4407</td>
<td>0.984671</td>
</tr>
<tr>
<td></td>
<td>Salt &amp; Pepper Noise</td>
<td>40.2183</td>
<td>1</td>
<td>40.2511</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Gaussian Noise</td>
<td>44.265</td>
<td>1</td>
<td>44.1905</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Speckle Noise</td>
<td>45.7445</td>
<td>0.995355</td>
<td>45.6927</td>
<td>0.996652</td>
</tr>
<tr>
<td>Symlets</td>
<td>Sharpening</td>
<td>46.6024</td>
<td>1</td>
<td>46.7037</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Smoothening</td>
<td>58.9608</td>
<td>1</td>
<td>59.3022</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>MotionBlur</td>
<td>52.0849</td>
<td>1</td>
<td>52.2461</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Salt &amp; Pepper Noise</td>
<td>40.1723</td>
<td>1</td>
<td>40.158</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Gaussian Noise</td>
<td>44.0332</td>
<td>1</td>
<td>44.1144</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Speckle Noise</td>
<td>45.4582</td>
<td>1</td>
<td>45.5673</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 8: Reduction in PSNR of the watermarked image with increase in noise density of the salt and pepper noise.

Figure 9: Reduction in PSNR of the watermarked image with increase in variance of the Gaussian Noise.
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 natural image, Image 3 is taken and all the 4 medical images are used as watermarks alternately to understand how it performs for different optimization. For illustrative convenience ‘Haar’ wavelet is chosen for embedding the watermark.

**Table V Performance Measures of a single chosen natural image when embedded with different medical images. – GA based optimization**

<table>
<thead>
<tr>
<th>Image</th>
<th>DWT Type</th>
<th>Scalar Value</th>
<th>PSNR (db)</th>
<th>MSE</th>
<th>NC</th>
<th>SSIM</th>
<th>CV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Image : Image 3- Peppers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MI1</td>
<td>Haar</td>
<td>0.105714</td>
<td>69.6959</td>
<td>0.000940038</td>
<td>0.949029</td>
<td>0.89196</td>
<td>0.892113</td>
</tr>
<tr>
<td>MI2</td>
<td>Haar</td>
<td>0.108571</td>
<td>63.402</td>
<td>0.0017694</td>
<td>0.967536</td>
<td>0.931073</td>
<td>0.931249</td>
</tr>
<tr>
<td>MI3</td>
<td>Haar</td>
<td>0.108571</td>
<td>60.1999</td>
<td>0.00242969</td>
<td>0.97891</td>
<td>0.947487</td>
<td>0.947663</td>
</tr>
<tr>
<td>MI4</td>
<td>Haar</td>
<td>0.102857</td>
<td>76.0814</td>
<td>0.000496393</td>
<td>0.933832</td>
<td>0.83076</td>
<td>0.830936</td>
</tr>
</tbody>
</table>

**Table VI Performance Measures of a single chosen natural image when embedded with different medical images. – DE based optimization.**

<table>
<thead>
<tr>
<th>Image</th>
<th>DWT Type</th>
<th>Scalar Value</th>
<th>PSNR (db)</th>
<th>MSE</th>
<th>NC</th>
<th>SSIM</th>
<th>CV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural Image : Image 3- Peppers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MI1</td>
<td>Haar</td>
<td>0.104706</td>
<td>69.8833</td>
<td>0.000922588</td>
<td>0.948566</td>
<td>0.892037</td>
<td>0.892213</td>
</tr>
<tr>
<td>MI2</td>
<td>Haar</td>
<td>0.104706</td>
<td>64.101</td>
<td>0.00164486</td>
<td>0.965235</td>
<td>0.931205</td>
<td>0.939033</td>
</tr>
<tr>
<td>MI3</td>
<td>Haar</td>
<td>0.102353</td>
<td>61.3406</td>
<td>0.00216777</td>
<td>0.974583</td>
<td>0.948741</td>
<td>0.948917</td>
</tr>
<tr>
<td>MI4</td>
<td>Haar</td>
<td>0.102353</td>
<td>76.1734</td>
<td>0.000491749</td>
<td>0.933666</td>
<td>0.830781</td>
<td>0.830957</td>
</tr>
</tbody>
</table>

From the tables mentioned above it can be observed that both the methods of optimization provide results which converge and are in close agreement with each other. Although Differential Evolution (DE) based optimization yields results which slightly in better than the results obtained through Genetic Algorithm (GA) From the above tables it can also be concluded that Medical Image 3 (MI 3) is best suited for embedding in this natural image and the image MI4 results in very low SSIM if embedded in this natural image.

**VIII. Conclusion**

A dual security approach using watermarking and encryption is proposed and implemented. The watermark embedding is optimized using a multi objective optimization function. The optimization is carried out using evolutionary approaches like Genetic Algorithm (GA) and Differential Evolution (DE). The results prove that this optimization procedure is capable providing high robustness and imperceptibility while maintaining the structural integrity of the medical images.

**References**


Acknowledgements
The author’s would like to acknowledge the Priyadarshini College of Engineering & Technology, Nellore and University College of Engineering and Technology, Acharya Nagarjuna University, Guntur for providing a platform for doing this research work.

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 Ph.D 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, 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, IEEE, and MISTE.