I.J. Intelligent Systems and Applications, **2018, 11, 50-63**
Published Online November 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijisa.2018.11.06

A New Robust and Imperceptible Image Watermarking Scheme Based on Hybrid Transform and PSO

Tamirat Tagesse Takore
Dept. of Electronics and Communication Engineering, Andhra University, Visakhapatnam, India
E-mail: tameauce2014@gmail.com

[a]P. Rajesh Kumar and [b]G. Lavanya Devi
[a]Prof. in Dept. of Electronics and Communication Engineering, [b]Ass. Prof. in Dept. of Computer Science & System Engineering, Andhra University, Visakhapatnam, India
E-mail: rajeshauce@gmail.com, lavanyadevig@yahoo.co.in

Received: 08 November 2017; Accepted: 25 April 2018; Published: 08 November 2018

***Abstract*—**In this paper, a new robust and imperceptible digital image watermarking scheme that can overcome the limitation of traditional wavelet-based image watermarking schemes is proposed using hybrid transforms viz. Lifting wavelet transform (LWT), discrete cosine transform (DCT) and singular value decomposition (SVD). The scheme uses canny edge detector to select blocks with higher edge pixels. Two reference sub-images, which are used as the point of reference for watermark embedding and extraction, have been formed from selected blocks based on the number of edges. To achieve a better trade-off between imperceptibility and robustness, multiple scaling factors (MSF) have been employed to modulate different ranges of singular value coefficients during watermark embedding process. Particle swarm optimization (PSO) algorithm has been adopted to obtain optimized MSF. The performance of the proposed scheme has been assessed under different conditions and the experimental results, which are obtained from computer simulation, verifies that the proposed scheme achieves enhanced robustness against various attacks performed. Moreover, the performance of the proposed scheme is compared with the other existing schemes and the results of comparison confirm that our proposed scheme outperforms previous existing schemes in terms of robustness and imperceptibility.

***Index Terms*—**Lifting wavelet transform, discrete cosine transform, singular value decomposition, edge detection, particle swarm optimization.

I. Introduction

Due to the rapid advancement of digital technologies and widespread of the Internet, digital multimedia recording, storing, copying, modifying, and sharing becomes an easy task. Malicious attackers can use these technologies for illegal recording, copying, distributing or selling copyrighted valuable multimedia data of someone else without getting permission or compensating the authorized owners. Furthermore, they modify or even destroy the whole or part of the document to illegally claim ownership or prevent the information transfer to the intended recipient. Hence, protecting digital properties from unauthorized use become a critical issue to content producers and publishers that the demand for an effective data security technique is growing from time to time. Cryptography is one of the most commonly used methods for digital property protection. The content producer first encrypts the document before delivering it to the user, and the person who has a decryption key can only decrypt and access the data. However, this method fails to ensure security when the document is once decrypted. Pirates can easily purchase a legit single copy and distribute a large number of duplicated copies for a low price or for free over a shared network. Therefore, it is necessary to find another method to protect these digital media data with a more stringent way.

In recent years, the newly emerging technique called digital watermarking becomes the best alternative method to protect a copyright of multimedia data over a shared medium [1-3]. Digital watermarking is a process which embeds a watermark into host multimedia content in such a way that the embedded digital signature is extractable whenever information about the identity of the content owner is required. The embedded secret data could be visible or invisible. Invisible watermark is the most commonly used for copyright protection application. Besides to copyright protection, a digital watermarking technique has been used for many other applications such as content authentication, copy control, broadcast monitoring and tamper detection.

The existing digital watermarking techniques can be classified into numerous groups based on different criteria. Depending upon the embedding domain, they can be categorized into two: spatial domain and transform

domain techniques. Spatial domain watermarking technique embeds a watermark into a host data by modifying the pixel intensity values; whereas, transform domain technique insert a watermark by altering the values of transform coefficients. Although spatial domain watermarking techniques are easy to implement and low in computational complexity, transform domain watermarking techniques are often preferred and widely used for copyright protection application due to their ability to provide better robustness against different attacks. Discrete wavelet transform (DWT), discrete cosine transform (DCT), singular value decomposition (SVD) and Lifting wavelet transformation (LWT) are the most commonly used transforms in digital watermarking field [4-6]. To meet different watermarking requirements in the best way, hybrid transform techniques are the most preferable for watermarking schemes. Hybrid transform technique combines two or more transforms and exploits the advantage of those transforms to enhance the performance. The other classes of watermarking are text, image, audio and video watermarking which are based on the type of signal used as a cover or host document. Furthermore, watermarking techniques can be classified into fragile, semi-fragile and robust based on the ability to resist attacks, and into blind, semi-blind and non-blind depending upon the information required for watermark extraction. However, in this paper, robust and blind image watermarking scheme using a hybrid transform technique is proposed.

For copyright protection application, imperceptibility and robustness are the two major requirements that watermarking schemes are expected to fulfill and often they are used as criteria to evaluate the performance of the schemes. The term imperceptibility refers to the degree of visual similarity between an original image and its watermarked version. Generally, a watermark embedding process is accompanied with quality loss due to the added signal. However, for invisible watermarking schemes, the embedding process should leave the level of degradation unnoticeable to human observers. Peak signal to noise ratio (PSNR) is the most commonly used metric to evaluate the level of imperceptibility. A higher PSNR value indicates a higher imperceptibility. Furthermore, a good watermarking scheme should also satisfy the robustness requirement against different attacks. A watermarking scheme is said to be robust to an attack if the embedded watermark is able to resist the performed attacks and is extractable even after the attacks. Improving the robustness against attacks by preserving the visual quality is the core motivation of most existing watermarking schemes.

The remainder of this paper is organized as follows. Section II provides an extensive literature survey of related works. In Section III, the basic concepts of transforming techniques which we have adopted in the proposed scheme are explained in detail. Brief summary of PSO based scaling factors optimization processes is described in section IV. Section V illustrates the proposed watermark embedding and extraction procedure. Section VI presents experimental setup and results. Finally, our concluding remarks are presented in section VII.

II. Related Works

In the field of watermarking, designing a robust watermarking scheme which can hide information without significantly affecting the visual quality has been the major challenging problem due to the existence of two conflicting watermarking requirements, viz. robustness and imperceptibility. Thus far, different strategies have been adopted to address the issue. Among these strategies, feature extraction based image watermarking technique become more popular due to its advantages, and one of which is the ability to embed a watermark in a region of an image bearing the basic character information such as texture and edge. Edge detection based suitable region selection technique has been used extensively as the best method to improve the robustness and imperceptibility. Authors in [7] proposed a new digital image watermarking algorithm based on texture block and edge detection in the DWT in order to balance between the invisibility and robustness and improve the ability of resisting to attacks of the digital image watermark. Khoo et al. [8] proposed a robust image watermarking scheme based on the human visual system (HVS) and used edge entropy as a HVS character for selecting significant blocks to embed a binary watermark. After the first level of DWT decomposition, the SVD is performed on the low-low sub-band to modify the elements of U matrix according to predefined conditions. However, in the proposed watermark embedding process the defined threshold value (T) which was used to modify U elements could not assure the trade-off between robustness and imperceptibility unless its value is determined by using an optimization algorithm.

The other alternative approach that has been adopted to improve the performance of the watermarking scheme is choosing suitable transform techniques for watermark embedding process. Numerous watermarking schemes using different transform techniques have been proposed and available in the literature. SVD is used widely for watermarking application due to its significant advantages [9, 10]. However, most of SVD based watermarking schemes suffered from the false positive problem, in which fake watermark is detected from the content where a different watermark was embedded. W. Yongdong [11] proposed a watermarking scheme which can resist counterfeiting attack using SVD technique. Although the proposed scheme is able to solve the false positive problem, it may be vulnerable to other attacks. In [12], a novel image watermarking algorithm based on SVD has been proposed and the algorithm performs well in both security and robustness. However, to overcome the drawbacks of SVD based watermarking algorithm and improve the performance, another transform techniques such as DWT, DCT or LWT should be used together with SVD. A watermarking scheme which uses hybrid transform techniques can utilize the advantages these transforms and achieve the required goal. S. Fazli and M.

Moeini [13] proposed a digital image watermarking algorithm using DWT-DCT-SVD techniques, and the algorithm gave improved robustness against various geometric attacks. In recent years, due to its better computational efficiency and lossless decomposition, LWT becomes more popular in watermarking than traditional wavelet transforms. Moreover, LWT can map integer to integer without the rounding error; hence it can be used for lossless data hiding. Ansari et al. [14] proposed robust and false positive free watermarking scheme using LWT and SVD. The authors employed a metaheuristic optimization technique in their scheme to find the optimal value of scaling factor. Scaling factors (SF), which are used to modify the coefficients during watermark embedding process, profoundly determine the level of robustness and imperceptibility. Ramanjaneyulu et al. [15] proposed a quality guaranteed robust image watermarking algorithm using Genetic Algorithm (GA). The objective of optimization was to provide maximum possible robustness without exceeding a predefined distortion limit. The authors in [16] proposed an efficient watermarking scheme which can achieve the desired robustness level without causing significant distortion in the original image. They employed particle swarm optimization algorithm in the scheme to find the optimum multiple scaling factors.

So far, a lot of researchers across the globe have conducted different studies in the field of watermarking and they have proposed several schemes for different applications. But, still there exist some challenging gaps in the area which requires further study. The first challenge is designing a watermarking scheme which can achieve improved robustness and imperceptibility while maintaining better trade-off between them. The other is the challenge of practical implementation. Due to computational complexity and large memory requirement, some proposed schemes are infeasible and uneconomical for practical application. To address aforementioned problem and fill the existing gape, in this paper, we have proposed a new, efficient watermarking scheme which can simultaneously meet imperceptibility and robustness requirement. The scheme uses LWT to avoid rounding error and reduce computational complexity which will occur due to traditional DWT. DCT is another transform which is used to improve the robustness of the scheme against noising, compression, sharpening and filtering attacks. A binary watermark is embedded into the image by modifying the singular value using optimized multiple scaling factors. The two sub-images which are formed from blocks based on the number of edge pixels are used as a reference point for watermark embedding and extracting. Therefore, the scheme requires neither original image nor a watermark for the extraction process. Since our proposed scheme is able to achieve good imperceptibility and improved robustness and is free from false positive problem, it can be an ideal choice for copyright protection application.

III. The Mathematical Preliminaries of used Transforms

A. Lifting wavelet transform

The existing proposed watermarking schemes using traditional wavelet transform have some drawbacks. Since the traditional wavelet transform is a floating point algorithm, the limited ability of a computer to process a finite word length will result in rounding error, and the process of reconstructing the exact signal becomes unattainable. Furthermore, the traditional wavelet transform technique requires sophisticated computation facilities, and this makes hardware implementation to be complex and uneconomical. To overcome the problems the lifting wavelet transform (LWT) technique has been adopted in this paper. LWT is a more flexible technique, and it was first introduced by W. Sweldens in 1995 [17]. The technique inherits multi-resolution properties of traditional wavelet transform and adds new other properties. The primary procedure of LWT involves three main operations, namely splitting, predicting and updating.

Splitting: This operation divides the original signal, C into two sample sets: even $C_k(e)$ and odd $C_k(o)$ sets.

$$\left.\begin{aligned} C_k(e) &= C_{2k}, \\ C_k(o) &= C_{2k+1}. \end{aligned}\right\} \tag{1}$$

Predicting: In this phase, odd samples are predicted from even samples and the difference between the odd samples, and the predicted result is taken as a high-frequency coefficient of the next level.

$$\left.\begin{aligned} C_k^P(o) &= P(C_k(e)), \\ C_k^D(o) &= C_k(o) - P(C_k(e)). \end{aligned}\right\} \tag{2}$$

Updating: This step produces the low-pass coefficient by adding the original even sample and the predicted odd sample after updating them using an update operator.

$$C_k^U(e) = C_k(e) + U(C_k^D). \tag{3}$$

The inverse lifting wavelet transform (ILWT) is obtained by inverting the forward steps and replacing the split operator with a merge operator. In Fig. 1, the block diagram of forward and inverse lifting wavelet transform procedure is shown [18].

B. Discrete cosine transforms

Discrete cosine transform (DCT) is a well-known transform method that converts an image from a spatial domain to a frequency domain. Let 2D image of size M×N is defined as, F= {g (x, y), x=0, 1, 2… M, y=0, 1, 2… N}, then formulae for forward DCT and inverse DCT can be given as:

$$G(u,v)=\sigma(u)\sigma(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}g(x,y)\cos\left[\frac{(2x+1)u\pi}{2M}\right]\times \cos\left[\frac{(2y+1)v\pi}{2N}\right], \quad (4)$$

$$g(x,y)=\sigma(u)\sigma(v)\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}G(u,v)\cos\left[\frac{(2x+1)u\pi}{2M}\right]\times \cos\left[\frac{(2y+1)v\pi}{2N}\right], \quad (5)$$

where $\sigma(u),\sigma(v)=\frac{1}{\sqrt{2}}$, for $u,v=0$, and $\sigma(u),\sigma(v)=1$, for u=1,2,…, M and v=1,2,…, N.

Fig. 2 shows the various frequency regions of 8×8 block size DCT coefficients [13]. In this proposed algorithm, we have used DCT to mitigate the limitation of SVD and improve the robustness of the scheme to noise, compression, sharpening and filtering attacks.

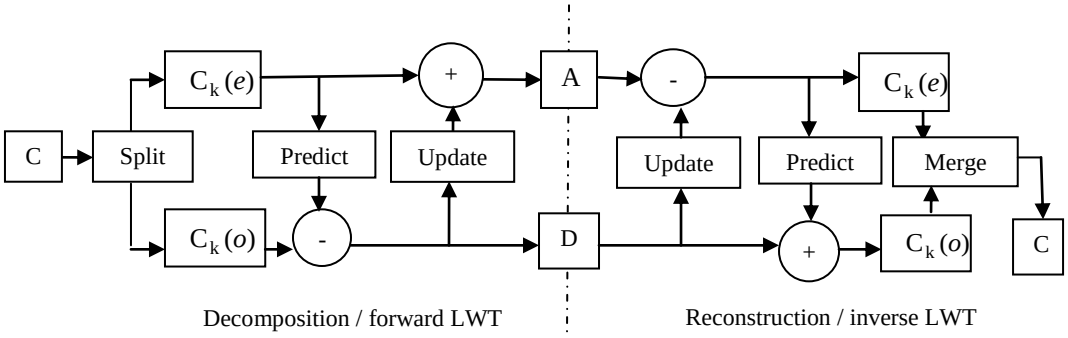


Fig.1. Block diagram of lifting scheme.

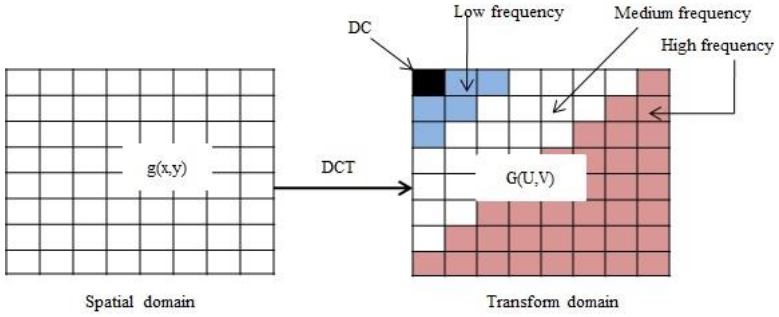


Fig.2. DCT frequency region for 8x8 block size.

C. Singular value decomposition

From the perspective of image processing, a digital image can be viewed as a matrix such that pixels intensity values are considered as elements of the matrix. Thus, SVD which is a linear algebra technique can be used in digital watermarking due to its unique properties. SVD factorize an image F of size M×N into three unique matrices U, S and V such that,

$$F=USV^T=\begin{pmatrix}u_{11}&\cdots&u_{1M}\\u_{21}&\cdots&u_{2M}\\\vdots&\ddots&\vdots\\u_{M1}&\cdots&u_{MM}\end{pmatrix}\times\begin{pmatrix}s_{11}&0&\cdots&0\\0&s_{22}&\cdots&0\\\vdots&\vdots&\ddots&0\\0&0&\cdots&s_{MN}\end{pmatrix}\times \begin{pmatrix}v_{11}&\cdots&v_{1N}\\v_{21}&\cdots&v_{2N}\\\vdots&\ddots&\vdots\\v_{N1}&\cdots&v_{NN}\end{pmatrix}^T, \quad (6)$$

where $F\in\Re^{M\times N}$, $U\in\Re^{M\times M}$, $S\in\Re^{M\times N}$ and $V\in\Re^{N\times N}$. The matrix U and V are called the left and right singular vectors. Since U and V are orthogonal matrices, then

$$\left.\begin{aligned}UU^T=U^TU=I,\\VV^T=V^TV=I.\end{aligned}\right\} \quad (7)$$

The matrix S is a nonnegative diagonal matrix containing the square root of the eigenvalues of either U or V, and the elements are arranged in descending order (i.e. $s_{11}\geq s_{22}\geq\cdots s_{MN}$). The process of singular value decomposition begins with pre-multiplying both sides of expression (6) by F^T.

$$F^TF=(USV^T)^T(USV^T)=VS^TU^TUSV^T. \quad (8)$$

$$FF^T=(USV^T)(USV^T)^T=US^TV^TVSU^T. \quad (9)$$

Based on (7), UU^T and VV^T give the identity matrix I and $S^TS = SS^T = S^2$ because S is diagonal matrix.

Inserting the expression into (8) and (9) we can obtain

$$\left.\begin{aligned} F^T F &= VS^2V^T, \\ FF^T &= US^2U^T. \end{aligned}\right\} \tag{10}$$

Since the result of multiplication F^TF and FF^T is a symmetrical matrix, the problem $F^TF=VS^2V^T$ and $FF^T=US^2U^T$ can be solved by using Eigen-decomposition operation. For square matrix F of size $k \times k$, if λ is an associated Eigenvalues then:

$$Fv_j = \lambda v_j, \quad for\ j = 1, 2, ...k, \tag{11}$$

where, v is called eigenvector of matrix F, associated with eigenvalues λ.

Using identity matrix I of size k×k, the expression (11) can be rewritten as,

$$\left.\begin{aligned} Fv_j &= \lambda I v_j, \\ (F - \lambda I)v_j &= 0. \end{aligned}\right\} \tag{12}$$

Equation (10) will have non-zero solution if the determinant of $(F- \lambda I)$ is equal to zero, (i.e. $|F- \lambda I|=0$). Solving this equation, eigenvalues of the matrix can be obtained. For each eigenvalues, the corresponding eigenvectors can be found by plugging back into expression (11). Singular matrix S is obtained by taking the square root of the eigenvalues and populating them diagonally in descending order. The process to calculate the right singular vector U follows the same steps as calculation of V.

In this paper, we have employed block based SVD to embed a binary watermark by modifying singular values using multiple scaling factors. The following are the benefits that we can obtain when we use SVD technique in image watermarking scheme.

The visual quality of the cover image is not affected significantly due to a slight change of singular values.

Singular values have good stability and their values are rotationally invariant.

SVD can a pack large energy signal within few coefficients.

IV. PSO BASED SCALING FACTOR OPTIMIZATION

In watermarking, robustness and imperceptibility highly depend on the quantity of signal embedded. Scaling factors which are used to modulate the coefficients during watermark embedding can control the quantity. Therefore, the problem of finding suitable scaling factors, which can give optimum performance and maintain the trade-off between imperceptibility and robustness, can be viewed as an optimization problem. However, some authors use a trial-and-error method to set the value of these scaling factors. Indeed, suitable optimized scaling factors can be obtained using metaheuristic optimization algorithms. For robustness R and imperceptibility Q, the optimization problem can be defined as,

$$\left.\begin{aligned} &Maximize\ : R(\alpha_k), \\ &Mantaining : Q(\alpha_k) \geq Q_{Th}, \end{aligned}\right\} \tag{13}$$

where αk is scaling factors and QTh is a user defining quality threshold. Putting the above objectives into consideration, we have formulated the fitness function (ff) as follows.

$$ff = Max\left\{ PSNR(F, F_w) + \gamma \sum_{i=1}^{n} NCC(W, W_E) \right\}, \tag{14}$$

where PSNR (.) and NCC (.) are metrics to measure imperceptibility and robustness respectively, and their definition is presented in section VI. F and Fw are an original host image and a watermarked image respectively; while W and WE are an original watermark and extracted watermark respectively.

In this paper, we have used particle swarm optimization (PSO) to find optimized scaling factors that can provide the best compromise between robustness and imperceptibility. PSO algorithm was first developed by Eberhart and Kennedy in 1995 [19]. The algorithm starts a searching process by initializing particles randomly having position, xi(t) and velocity, vi(t). Then, the quality of each particle is evaluated using a fitness function (also known as objective function), and based on their fitness score both personal best (pbest) and overall global best (gbest) are determined. Until the predefined stopping conditions are satisfied, the algorithm continues searching the optimum value by updating the velocity and position using formulae,

$$\begin{aligned} v_i(t+1) = w_i v_i(t) + C_1 rand\,(p_{best} - x_i(t)) + \\ C_2 rand\ (g_{best} - x_i(t)), \end{aligned} \tag{15}$$

$$x_i(t+1) = x_i(t) + v_i(t+1), \tag{16}$$

where wi is inertia weight which determines the step size and C1 and C2 are learning factors which determine the effectiveness of local and global learning. The term 'rand' refers to an operation which randomly generates numbers between 0 and 1. In Fig. 3, the flowchart of PSO based solution searching and objective value calculation is shown.

V. PROPOSED WATERMARKING SCHEME

Digital image watermarking scheme based on feature detection based reference sub-image forming technique becomes a popular strategy to improve the performance of the scheme and enables designers to select the best region (or blocks) of the image for watermark embedding

[16]. The blocks having the desired feature are used as a reference point for watermark embedding and extraction. There exist different feature extracting methods, and in this study, we have used canny edge detector due to its superior performance in edge detection. Thus, a watermarking scheme using edge detection based reference sub-image (EDBRI) forming technique is proposed. A flowchart of EDBRI forming technique is shown in Fig. 4, and from the figure, we can observe that two sub-images are formed from selected significant blocks. The first sub-image, which is formed from blocks having largest number edge pixels, is used as a region for watermark embedding and the other one is used as a reference point for watermark extraction. After the watermark is embedded, the watermarked image can be obtained by merging the sub-images and placing the blocks back to their original place using blocks position indexes (P_k) as keys.

A. Proposed watermark embedding procedure

The proposed watermark embedding algorithm takes a host image, F of size M×N and binary watermark W of size h×l as an input and gives watermarked image F_W as an output. The steps involved in the proposed watermark embedding process are given as follows.

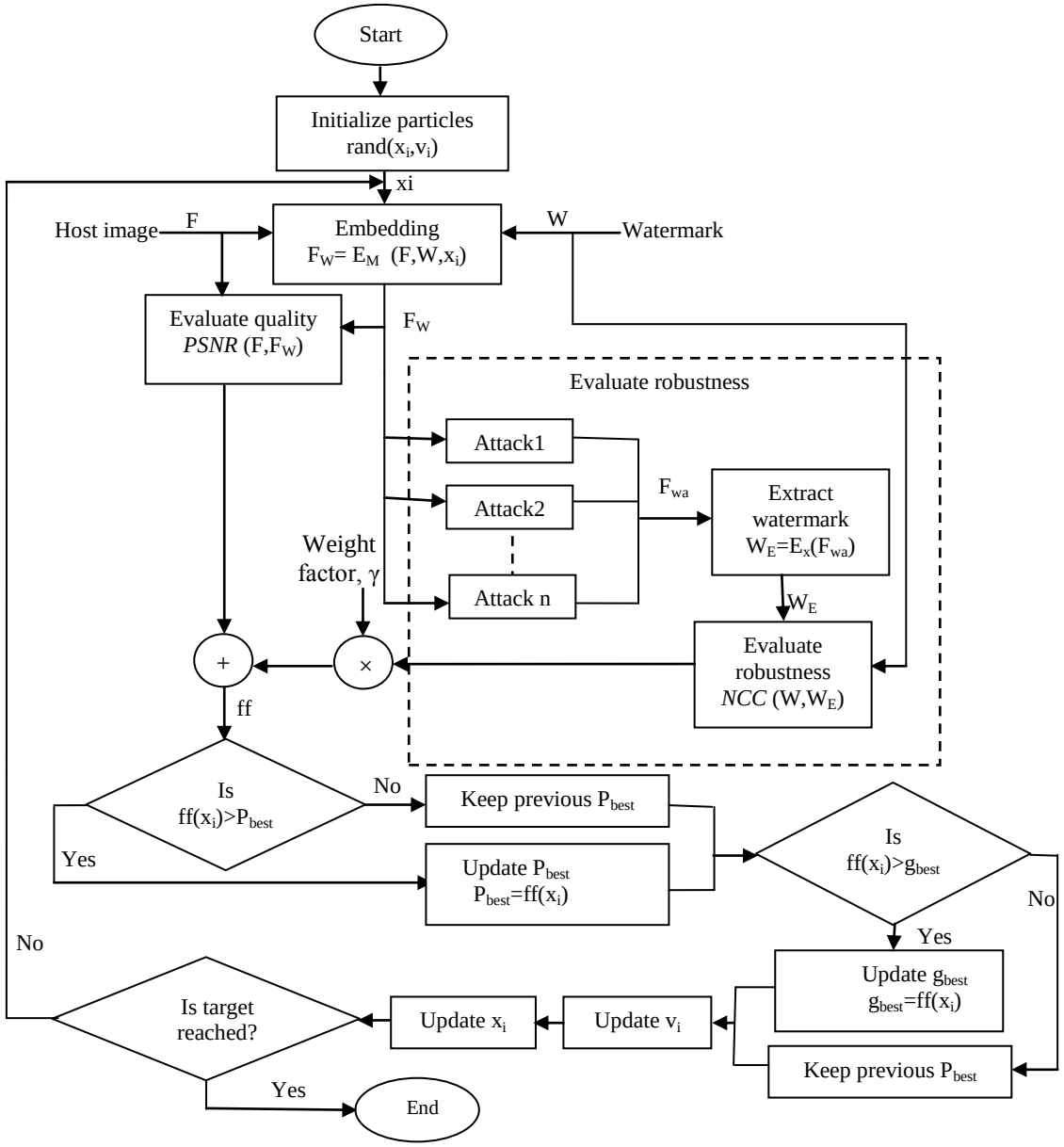


Fig.3. Flowchart for PSO based solution searching and objective value calculation.

Step1: Form reference sub-images F_{rf}^{H} and F_{rf}^{L} using the discussed procedure.

Step2: perform LWT operation on the sub-images.

$$\left.\begin{aligned}(A_{rf}^{H}, H_{rf}^{H}, V_{rf}^{H}, D_{rf}^{H}) = LWT(F_{rf}^{H}),\\ (A_{rf}^{L}, H_{rf}^{L}, V_{rf}^{L}, D_{rf}^{L}) = LWT(F_{rf}^{L}),\end{aligned}\right\} \quad (17)$$

where, A, H, V and D represent approximation, horizontal, vertical and diagonal sub-bands of the sub-images respectively.

Step3: Apply block based DCT on approximation sub-band coefficients using block size of 4×4.

$$\left.\begin{aligned} A_{rf(m,n)}^{DCT1} &= DCT(A_{rf}^{H}), \\ A_{rf(m,n)}^{DCT2} &= DCT(A_{rf}^{L}). \end{aligned}\right\} \quad (18)$$

Step4: Factorize DCT coefficient using SVD operation.

$$\left.\begin{aligned} [U_{rf(m,n)}^{H}, S_{rf(m,n)}^{H}, V_{rf(m,n)}^{H}] &= SVD(A_{rf(m,n)}^{DCT1}), \\ [U_{rf(m,n)}^{L}, S_{rf(m,n)}^{L}, V_{rf(m,n)}^{L}] &= SVD(A_{rf(m,n)}^{DCT2}). \end{aligned}\right\} \quad (19)$$

Using multiple scaling factors (MSF) to modulate different ranges of selected coefficients significantly improve the performance of the scheme than a single scaling factor (SSF). A coefficient falling in a particular interval is modified by a corresponding scaling factor, and the procedure which we have used to determine the intervals are presented as follows.

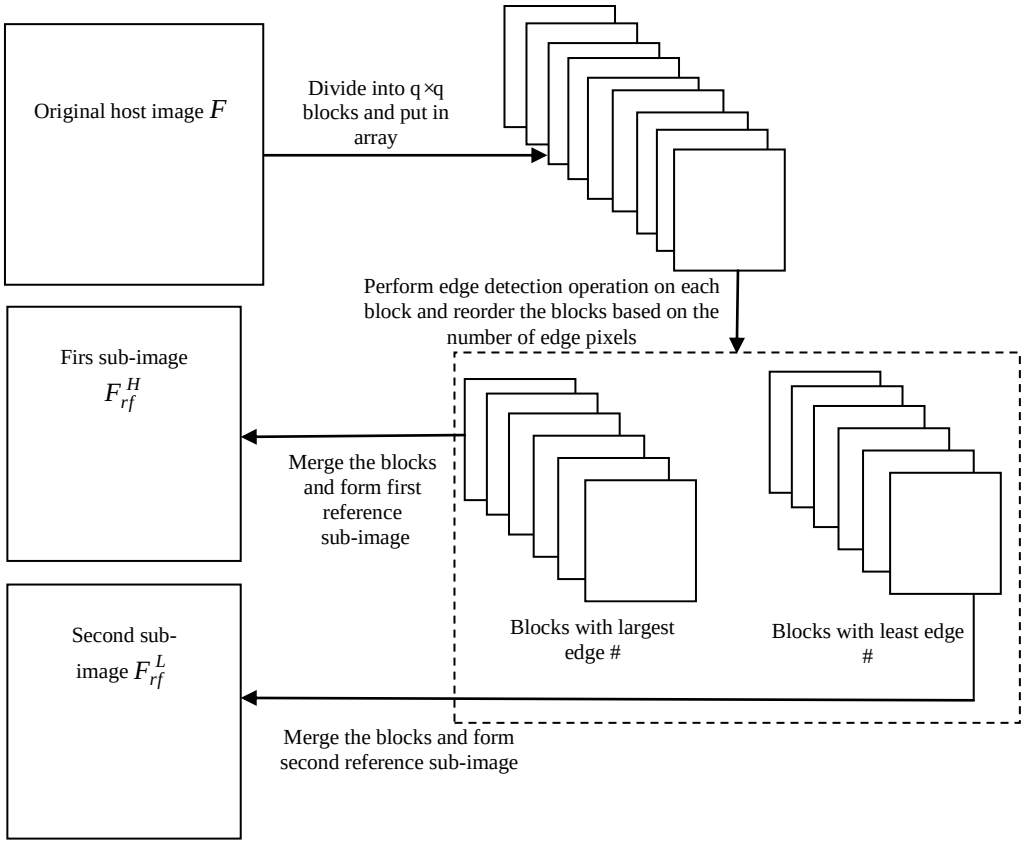


Fig.4. Flow chart of edge detection based reference sub-image (EDBRI) forming technique.

Take singular value matrices $S_{rf(m,n)}^{H}$ and $S_{rf(m,n)}^{L}$, and compute the difference and store the value in array D(m,n),

$$D(m,n) = \left| S_{rf(m,n)}^{H}(i,j) - S_{rf(m,n)}^{L}(i,j) \right|, \quad (20)$$

where i=j=1 and (m×n) refer to row and column indices of sub-image blocks.

Find the maximum and minimum value of $D(m,n)$ and divide the values of the array into q number of non-overlapping sub-ranges (r_k) so that the corresponding scaling factor (α_k) can be used for coefficient modification.

$$\left.\begin{aligned} D_{\max} &= \max(D(m,n)), \\ D_{\min} &= \min(D(m,n)), \\ d &= (D_{\max} - D_{\min})/q, \\ r_k &= [(k-1)d, (kd)), \ \ for\ k = 1,2,....,q. \end{aligned}\right\} \quad (21)$$

For the completion of embedding process q numbers of scaling factors are needed. In this paper, we have used five scaling factors (k=1,2,…,5.) such that $\alpha_k > \alpha_{k+1}$.

Step5: Once an appropriate scaling factor for each interval is obtained, the binary watermark bits can be embedded by modifying singular values using the rule,

$$S^{H}_{Wrf(m,n)}(i,j)=\begin{cases} \text{if } W(m,n)=1 \\ \begin{cases} S^{H}_{rf(m,n)}(i,j), & \text{if } S^{H}_{rf(m,n)}(i,j) > S^{L}_{rf(m,n)}(i,j), \\ S^{H}_{rf(m,n)}(i,j)+\alpha S^{L}_{rf(m,n)}(i,j), & \text{if } S^{H}_{rf(m,n)}(i,j) \le S^{L}_{rf(m,n)}(i,j), \end{cases} \\ \text{if } W(m,n)=0 \\ \begin{cases} S^{H}_{rf(m,n)}(i,j), & \text{if } S^{H}_{rf(m,n)}(i,j) < S^{L}_{rf(m,n)}(i,j), \\ S^{H}_{rf(m,n)}(i,j)-\alpha S^{L}_{rf(m,n)}(i,j), & \text{if } S^{H}_{rf(m,n)}(i,j) \ge S^{L}_{rf(m,n)}(i,j), \end{cases} \end{cases} \tag{22}$$

where, i=j=1 and $\alpha=\alpha_k$ if the magnitude $\left|S^{H}_{rf(m,n)}(i,j)-S^{L}_{rf(m,n)}(i,j)\right|$ is in the interval r_k.

Step6: Perform inverse SVD operation to obtain watermarked blocks $B^{H}_{W(m,n)}$.

$$B^{H}_{W(m,n)}=U^{H}_{rf(m,n)}\times S^{H}_{Wrf(m,n)}\times V^{H^T}_{rf(m,n)}. \tag{23}$$

Step7: Apply inverse DCT and merge the blocks to get watermarked approximation coefficient A^{H}_{Wrf}.

Step8: apply inverse LWT to obtain watermarked sub-image

$$F^{H}_{Wrf}=ILWT(A^{H}_{Wrf},H^{H}_{rf},V^{H}_{rf},D^{H}_{rf}). \tag{24}$$

Step9: Finally a watermarked image F_W is obtained by merging the two sub-images and placing the blocks back to their original position using key Pk .

Proposed watermark extraction procedure

The propose watermark extraction process requires only a watermarked image and keys Pk as an input for the watermark extraction process. The steps of the proposed watermark extraction process are given as follows.

Step1: Take an attacked watermarked image and form reference sub-images using position key Pk.

Step2: Perform 1-level LWT.

$$\left.\begin{aligned}(A^{H^*}_{rf},H^{H^*}_{rf},V^{H^*}_{rf},D^{H^*}_{rf})&=LWT(F^{H^*}_{rf}),\\ (A^{L^*}_{rf},H^{L^*}_{rf},V^{L^*}_{rf},D^{L^*}_{rf})&=LWT(F^{L^*}_{rf}).\end{aligned}\right\} \tag{25}$$

Step3: Divide $A^{H^*}_{rf}$ and $A^{L^*}_{rf}$ into non-overlapping blocks and perform DCT.

$$\left.\begin{aligned}A^{DCT1^*}_{rf(m,n)}&=DCT(A^{H^*}_{rf}),\\ A^{DCT2^*}_{rf(m,n)}&=DCT(A^{L^*}_{rf}).\end{aligned}\right\} \tag{26}$$

Step4: Factorize DCT coefficients using SVD,

$$\left.\begin{aligned}[U^{H^*}_{rf(m,n)},S^{H^*}_{rf(m,n)},V^{H^*}_{rf(m,n)}]&=SVD(A^{DCT1^*}_{rf(m,n)}),\\ [U^{L^*}_{rf(m,n)},S^{L^*}_{rf(m,n)},V^{L^*}_{rf(m,n)}]&=SVD(A^{DCT2^*}_{rf(m,n)}).\end{aligned}\right\} \tag{27}$$

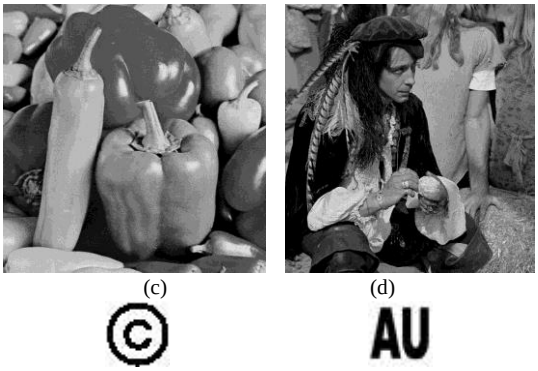
Step5: Finally, Extract the watermark using the rule,

$$W_E(m,n)=\begin{cases}1, & \text{if } S^{H^*}_{rf(m,n)}(i,j)\ge S^{L^*}_{rf(m,n)}(i,j),\\ 0, & \text{otherwise.}\end{cases} \tag{28}$$

VI. Experimental Results and Discussion

This section presents the experimental setup and a series of tests that have been conducted to assess the performance of the proposed schemes. We have used Matlab software to implement the scheme. Different standard grayscale images of size 512×512 have been used as test images. Fig. 5 shows the test images and watermark logos. A binary watermark of size 32×32 is inserted into the host image using the proposed watermark embedding procedure, and the performance of the scheme under various conditions has been evaluated using imperceptibility and robustness criteria. To achieve the highest possible robustness while maintaining the imperceptibility within an acceptable level, multiple scaling factors (MSF) have been used to modify the coefficients during watermark embedding. PSO algorithm is used to find suitable scaling factors. In this study, the PSO parameters C_1 and C_2 were set to be 2, and the value of the inertia weight w_i was made to vary adaptively depending on the iteration. Furthermore, due to computational time burden, the number of particles and iteration were set to be 20 and 100 respectively. The objective of optimization is to maximize the robustness, while keeping the imperceptibility above pre-defined level (i.e. 40 dB).

(a) (b)



(c) (d)

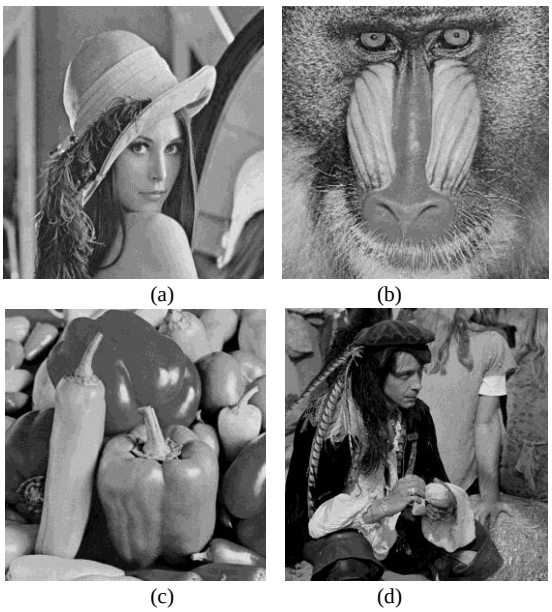
(e) (f)

Fig.5. The test images (a) Lena (b) mandrill (c) pepper (d) man (e) binary watermark logo, WM_1 (f) binary watermark logo, WM_2.

Currently, there are several metrics to measure the degree of similarity between the original and watermarked image. However, Peak Signal to Noise Ratio (PSNR) is the most widely used method. For an original host image F and watermarked image F_W of size $M \times N$, $PSNR$ can be defined as,

$$PSNR = 10 \log \frac{255^2}{\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(F_W(x,y) - F(x,y))^2} dB. \quad (29)$$

Obtaining higher value of PSNR shows that the watermarking scheme can provide a good quality watermarked image which looks nearly identical to the original image. In the field of watermarking, the minimum acceptable PSNR value is 38dB [18]. In Fig. 6, watermarked Lena, mandrill, pepper and man images are shown. Their corresponding PSNR values are presented in Table 1. As we can observe, both watermarked and original images are visually identical and the obtained PSNR results also prove that the proposed scheme satisfies the preset imperceptibility requirements.



(a) (b)

(c) (d)

Fig.6. Watermarked images. (a) Lena (b) mandrill (c) pepper (d) man.

Table 1. PSNR of watermarked images using MSF in an attack-free scenario.

Images	Lena	Mandrill	Pepper	Man
PSNR	46.5085	46.0012	45.9021	45.9726

In addition to the five test images, we have also used fifty different standard images to further assess the quality performance of the proposed scheme. In Fig. 7 a plot of PSNR values is shown. From the figure we can observe that the proposed scheme is able to provide higher PSNR results and this confirms that the scheme gives better quality watermarked images regardless of image types.

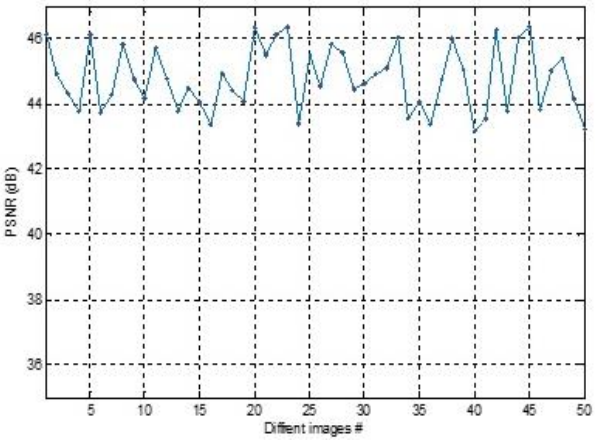
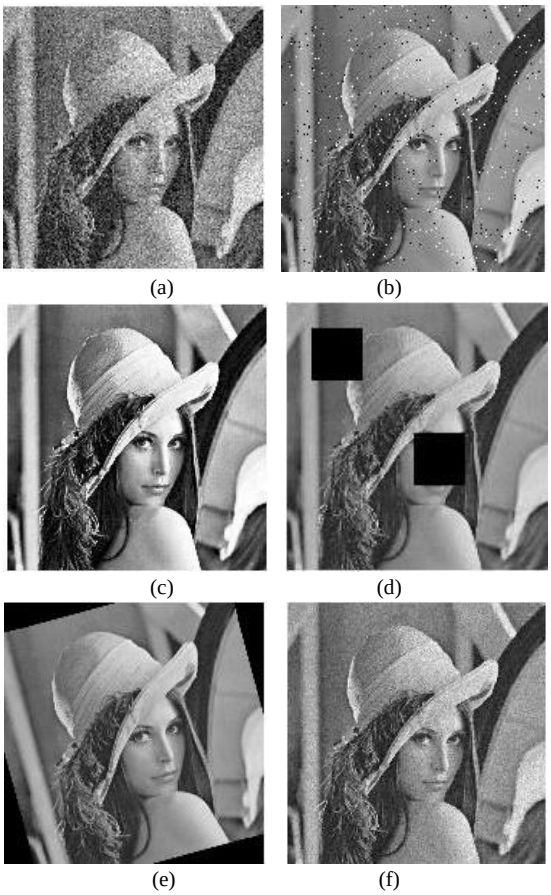


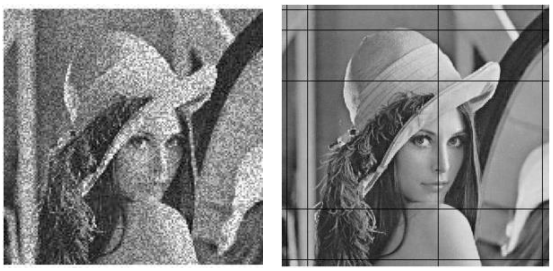
Fig.7. PSNR result obtained for different images in attack free scenario.



(a) (b)

(c) (d)

(e) (f)



(g) (h)

Fig.8. Attacked watermarked Lena images: (a) Gaussian noise (b) salt & pepper noise (c) histogram equalization (d) Cropping (e) rotation (f) Poisson noise (g) speckle noise (h) rows columns blanking.

For copyright protection application, robustness is a key requirement that designers should consider while developing a new watermarking scheme. The term robustness refers to the ability of the embedded watermark to resist different attacks. An image processing techniques which can degrade or destroy the embedded watermark are considered as an attack, and in this paper, we have applied eighteen different types of attacks on the watermarked images to evaluate the robustness level of the proposed methods. The attacks are: noise addition (Gaussian white noise, salt & pepper noise, poison noise, and speckle noise), filtering attacks (median filter, average filter, Gaussian low-pass filter, Weiner filter), geometric attacks (rotation attack, cropping attack, resizing attack and row-column blanking attack) and other attacks (histogram equalization, gamma correction, JPEG compression, camera motion, least bit removing and sharpening attack). For the sake of convenience, in the latter sections, these attacks are identified as GNA, SPNA, PNA, SNA, MFA, AFA, GLPFA, WFA, RTA, CRA, RSA, RCBA, HEA, GCA, JPCA, CMA, LBRA, and ISRA respectively. Fig. 8 shows the attacked watermarked Lena images using different attacks.

The existence of the embedded watermark resisting applied attacks is checked by extracting the watermark from the attached images using the proposed extracting procedures. In Fig.9, extracted watermarks from the attacked watermarked images are shown. From the figures, we can notice that the proposed method could give good quality extracted watermark image against all the attacks except the rotation attack. The quality of the extracted watermark can be measured using many metrics. In this work, we have adopted the normalized correlation coefficient (NCC) to measure the robustness by evaluating the degree of similarity between the original and extracted watermarks after an attack. For an original watermark W and extracted watermark WE of size h×l, the NCC can be calculated as,

$$NCC = \frac{\sum_{i=1}^{h}\sum_{j=1}^{l}(W(i,j)-\mu)(W_E(i,j)-\mu_E)}{\sqrt{\sum_{i=1}^{h}\sum_{j=1}^{l}(W(i,j)-\mu)^2}\sqrt{\sum_{i=1}^{h}\sum_{j=1}^{l}(W_E(i,j)-\mu_E)^2}}, \quad (30)$$

where μ and μ_E represent the mean of original and extracted watermark respectively.

When the NCC value is closer to 1 for a given applicable attack, then the scheme is said to be robust against this attack. In general, the robustness of the scheme is at an acceptable level if the NCC value is equal to 0.75 or higher [18]. In Table 2, the level of transparency and robustness achieved under different attack conditions are presented in terms of PSNR and NCC respectively. From the results, we can observe that the maximum NCC value obtained is 1 and the minimum is 0.7133 which is for the rotation attack. Furthermore, all obtained PSNR values are greater than the minimum acceptable level and this shows that the proposed scheme achieves a better trade-off between robustness and imperceptibility. Compared to single scaling factor (SSF), using multiple scaling factors (MSF) for watermarking scheme gives improved NCC and PSNR. The optimized scaling factors (MSF) for JPEG compression attack are given in Table 3.

The watermarked image further compressed by compression rates of 10,20,30,40,50,60,70,80,90, and 95 to evaluate the robustness of the scheme to JPEG compression attack. Fig. 10 depicts the plot of NCC results versus quality factors. From the plot, we can observe that the proposed scheme is able to score good NCC result even for lowest compression rate and this illustrates that the proposed scheme is efficient and robust to JPEG attack. We have compared our proposed method with other existing schemes [16, 20] to assess the performance level, and the comparison results are presented in Table 4 and Fig. 11. The results given in Table 4 clearly show that of the proposed scheme is able to provide improved NCC value compared to the other two schemes. This verifies that the proposed scheme maintains a better balance between robustness and imperceptibility and outperforms previous schemes for all attacks performed except the rotation attack.

Attacks performed	Extracted watermarks from host images							
	Using SSF				Using MSF			
	Lena		Mandrill		Lena		Mandrill	
	WM_1	WM_2	WM_1	WM_2	WM_1	WM_2	WM_1	WM_2
Attack free (ATF)								
Gaussian Noise attack (GNA) (μ=0, v=0.001)								
Salt & pepper noise attack (SPNA) (D=0.02)								
Median filter attack (MFA) (3x3)								
Histogram Equalization attack (HEA)								
Gamma correction attack (GCA) (γ=0.925)								
Cropping attack (CRA) (25% cropped)								
Rotation attack (RTA) (5^o)								
JPEG compression attack (JPCA) (QF=70%)								
Average filter attack (AVFA) (3x3)								
Gaussian low pass filter (GLPFA) (3x3)								
Camera motion attack (CMA) (len=9,θ=0)								
Least bit removing attack (LBRA) (LSB removed)								
Image sharpening attack (SRA)								
Resizing attack (RSA) (512→256→512)								
Wiener filter attack (WFA) (3x3)								
Poison noise attack (PNA)								
Speckle noise attack (SNA) (μ=0, v=0.04)								
Row-Column blanking attack (RCBA)								

Fig.9. Extracted watermarks from Attacked watermarked images using Proposed Algorithm.

Table 2. PSNR and NCC result obtained from simulations using WM_1.

Attacks	PSNR and NCC obtained using proposed Algorithm							
	Using SSF				Using MSF			
	Lena		Mandrill		Lena		Mandrill	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
AF	45.5017	1	45.2801	1	46.2781	1	45.8172	1
GNA	43.66444	0.9969	44.11755	0.9939	43.96941	0.9985	44.632	0.9992
SPNA	42.24956	0.9586	42.71774	0.9395	44.05564	0.9658	44.01332	0.9497
MFA	42.81885	0.9743	43.08412	0.9639	44.06895	0.9782	45.09106	0.9685
HEA	44.03595	0.9523	43.12224	0.9048	45.01206	0.9859	43.22681	0.9949
GCA	44.74875	0.9953	44.70624	0.8525	45.01995	0.9975	44.84521	0.9998
CRA	44.96997	0.9675	44.99858	0.9586	44.97377	0.9746	44.973	0.9776
RTA	44.53768	0.7133	44.46561	0.7214	44.82333	0.7528	44.88613	0.7511
JPCA	43.43962	0.9978	43.04458	1	43.86933	1	44.28311	1
AVFA	42.41549	0.9671	42.939	0.9544	43.74854	0.9798	43.15701	0.9457
GLPFA	43.09612	0.9977	44.534	0.9817	44.88039	0.998	43.97615	0.9947
CMA	44.46667	0.8867	42.64526	0.9772	44.80934	0.9036	43.35653	0.9395
LBRA	44.50285	0.9932	45.01619	0.9947	44.99763	1	44.85486	1
SRA	44.97714	0.9947	43.9252	0.9902	45.00733	0.9964	44.79106	0.9984
RSA	44.3489	0.9969	42.87884	0.9939	44.43792	0.9987	43.07747	0.9984
WFA	42.87331	0.9984	42.93158	0.9937	43.31461	0.9904	43.3828	0.9845
PNA	43.03124	0.9947	43.70847	0.9926	44.23103	0.9917	44.0405	0.9931
SNA	42.52919	0.9111	42.20916	0.9947	43.78754	0.9236	43.09012	0.9956
RCBA	43.5521	0.9288	43.70665	0.9377	44.08556	0.9396	43.83636	0.9377

Table 3. Optimized multiple scaling factors obtained from PSO for cover image Lena, Baboon and pepper and man.

Cover image	PSNR	NCC (JPCA, QF=50)	Optimized MSF [αk] for different ranges				
			α_1	α_2	α_3	α_4	α_5
Lena	43.86933	0.9940	0.159042	0.153103	0.087749	0.076312	0.037375
Mandrill	44.28311	0.9959	0.150937	0.141873	0.129263	0.097953	0.089117
Pepper	43.09612	0.9916	0.135941	0.131021	0.055205	0.032522	0.023801
Man	42.41549	0.9937	0.191858	0.109443	0.051502	0.029859	0.027725

Table 4. The comparison results of the proposed method with other existing methods in terms of NCC.

Attacks performed	Attack level		Existing methods		Proposed method
			V.S.Verma et al. [20]	TT.Takore et al. [16]	
MFA	Window	(3x3)	0.9570	0.9641	0.9782
		(5x5)	0.8125	0.8630	0.8917
AVFA		(3x3)	0.8945	0.9491	0.9798
		(5x5)	0.7383	0.8152	0.9021
GLPFA			0.9766	0.9990	0.9980
SRA			0.9766	0.9853	0.9987
HE			0.9297	0.9861	0.9859
GNA	Variance	(0.01)	0.9727	0.9772	0.9942
		(0.02)	0.8555	0.8974	0.9075
SPNA	D	(0.02)	0.7464	0.9311	0.9879
JPCA	QF	10	0.8789	0.7480	0.8983
		20	0.9414	0.7911	0.9532
		30	0.9922	0.9112	0.9864
		70	1	0.8925	1
RSA	Ratio	1/2	0.9844	0.9851	0.9987
CRA	Ratio	1/4	0.9336	0.9730	0.9746
RTA	Degree	0.1	0.8564	0.7152	0.7728

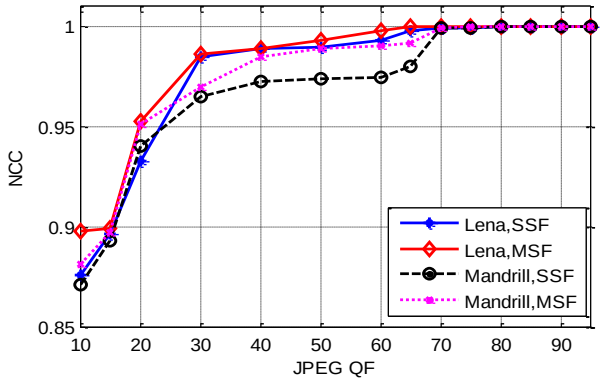


Fig.10. NCC values of extracted watermark for JPEG attack with different QF for Lena and Mandrill images.

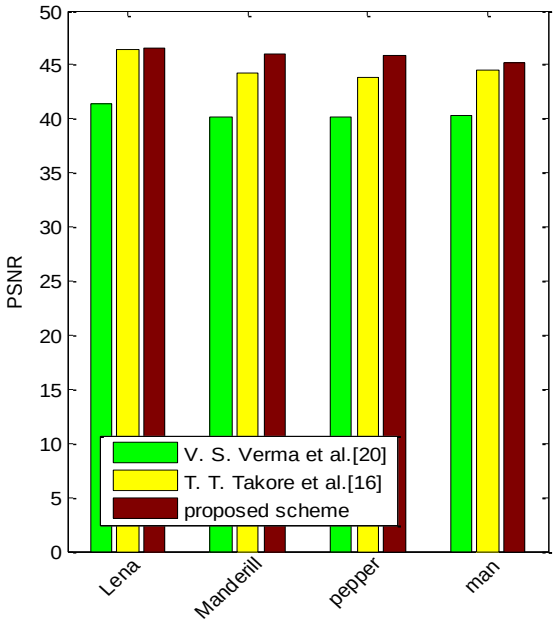


Fig.11. PSNR comparison results.

The overall experimental results which are presented in this section confirm that the proposed scheme satisfies the imposed watermarking requirements and achieves enhanced performance which makes it more preferable for the use of various multimedia security applications.

VII. Conclusions

In this paper, a new robust and imperceptible digital image watermarking scheme using the LWT, DCT, and SVD is proposed. The scheme used edge detection based reference sub-image forming technique to select the best region of the image for watermark insertion. Optimized MSF, which can achieve the best trade-off between imperceptibility and robustness, is obtained from PSO algorithm. A maximum number of attacks have been performed on watermarked images to assess the level of robustness and the obtained experimental results verify that the proposed method provides the best PSNR and NCC value for the attacks performed. Two other existing schemes have been considered for comparison and the obtained results confirm that the proposed method gives significantly improved robustness and imperceptibility compared to the other reported methods.

References

[1] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data. A state-of-the-art overview," IEEE Signal Process. Mag., vol. 17, no. 5, pp. 20–46, 2000.

[2] C.-H. Chou and K.-C. Liu, "Robust and transparent watermarking scheme for colour images," IET Image Process., vol. 3, no. 4, pp. 228–242, Aug. 2009.

[3] S. Bajracharya, R. Koju,"An Improved DWT-SVD Based Robust Digital Image Watermarking for Color Image", International Journal of Engineering and Manufacturing (IJEM), Vol.7, No.1, pp.49-59, 2017.

[4] N. M. Makbol and B. E. Khoo, "Robust blind image watermarking scheme based on Redundant Discrete Wavelet Transform and Singular Value Decomposition," AEU - International Journal of Electronics and Communications, vol. 67, no. 2, pp. 102–112, 2013.

[5] A. Dixit, R Dixit, "A Review on Digital Image Watermarking Techniques", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.9, No.4, pp.56-66, 2017.

[6] V. S. Verma and R. K. Jha, "LWT–DSR based new robust framework for watermark extraction under intentional attack conditions," Journal of the Franklin Institute, vol. 354, no. 14, pp. 6422–6449, 2017.

[7] Y. Wang, X. Bai, and S. Yan, "Digital image watermarking based on texture block and edge detection in the discrete wavelet domain," In Proc. IEEE International Conference on Sensor Network Security Technology and Privacy Communication System, 2013.

[8] B. E. Khoo, N. M. Makbol, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," IET Image Process., vol. 10, no. 1, pp. 34–52, Jan. 2016.

[9] G. Çetinel, L. Çerkezi,"Robust Chaotic Digital Image Watermarking Scheme based on RDWT and SVD", International Journal of Image, Graphics and Signal Processing (IJIGSP), Vol.8, No.8, pp.58-67, 2016.

[10] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, "An improved SVD-based watermarking technique for copyright protection," Expert Syst. Appl., vol. 39, no. 1, pp. 673–689, Jan. 2012.

[11] W. Yongdong, "On the security of an SVD-based ownership watermarking," IEEE Trans. Multimed., vol. 7, no. 4, pp. 624–627, Aug. 2005.

[12] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimed., vol. 4, no. 1, pp. 121–128, 2002.

[13] S. Fazli and M. Moeini, "A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks," Optik - International Journal for Light and Electron Optics, vol. 127, no. 2, pp. 964–972, 2016.

[14] I. A. Ansari, M. Pant, and C. W. Ahn, "Robust and false positive free watermarking in IWT domain using SVD and ABC," Engineering Applications of Artificial Intelligence, vol. 49, pp. 114–125, 2016.

[15] K. Ramanjaneyulu and K. Rajarajeswari, "Wavelet-based oblivious image watermarking scheme using genetic algorithm" IET Image Processing, vol. 6, no. 4, pp. 364, 2012.

[16] T. T. Takore, P. R. Kumar, and G. L. Devi, "Robust Image Watermarking Scheme Using Population-Based Stochastic Optimization Technique," International Journal of Image, Graphics and Signal Processing, vol. 9, no. 7, pp. 55–65, Aug. 2017.
[17] W. Sweldens, "The lifting scheme: A construction of second generation wavelets." SIAM journal on mathematical analysis, vol. 29, no. 2, pp. 511-546, 1998.
[18] N. M. Makbol and B. E. Khoo, "A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition," Digit. Signal Process., vol. 33, pp. 134–147, Oct. 2014.
[19] J. Kennedy and R. Eberhart, "Particle swarm optimization," Proceedings of IEEE International Conference on Neural Networks, Piscataway, NJ.vol. 4, pp. 1942–1948.1995.
[20] V. S. Verma, R. K. Jha, and A. Ojha, "Significant region based robust watermarking scheme in lifting wavelet transform domain," Expert Systems with Applications, vol. 42, no. 21, pp. 8184–8197, 2015.

Authors' Profiles

Tamirat Tagesse Takore received his M.Tech. in Electronics and Computer Engineering from Addis Ababa University in 2010. He is currently working towards his Ph.D. at Andhra University College of Engineering, Visakhapatnam, India. His research interests are in the area of image processing and digital signal processing.

Dr. P. Rajesh Kumar is a Professor in Electronics and Communication Engineering department, College of Engineering, Andhra University, Visakhapatnam, India. He received his M.E. and Ph.D. from Andhra University. He has twenty two years experience of teaching undergraduate, postgraduate and guided more than hundred postgraduate theses. He has published more than hundred research papers in National and International Journals and fifteen research scholars received PhD under his guidance. Presently he is guiding ten PhD students and his research interests are in the area of Digital image processing, Digital signal processing, Radar signal processing and Biomedical signal processing.

Dr. G. Lavanya Devi is an Ass. Professor in department of Computer Science and System Engineering, Andhra University College of Engineering, Visakhapatnam, India. She has graduated in Engineering from Nagarjuna University and pursued her Masters in Computer Science Engineering, M. Tech. from Andhra University. She received Ph.D in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad for her work in the area of Data Mining in Bioinformatics. She has over 16 years of experience in Academia and Research. With passion towards Teaching and Research, she has worked for various Engineering Institutions with various designations. She was awarded with IEI's Young Engineer Award and also received prestigious Young Faculty Research Fellowship from MieTY, Government of India. Dr. Lavanya has published and presented more than 90 Research Articles in the areas of Data Mining, Computational Intelligence and Bioinformatics in various Journals and National/International Conferences. Her research focuses include mining and modeling massive volumes of data, building hybrid prediction systems for various applications like Medical Diagnosis, Web Recommender Systems and Image Processing. She is passionate about building real-time intelligent systems that operate in multidisciplinary environments to solve real-world problems.

How to cite this paper: Tamirat Tagesse Takore, P. Rajesh Kumar, G. Lavanya Devi, "A New Robust and Imperceptible Image Watermarking Scheme Based on Hybrid Transform and PSO", International Journal of Intelligent Systems and Applications(IJISA), Vol.10, No.11, pp.50-63, 2018. DOI: 10.5815/ijisa.2018.11.06

