iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: XI Month of publication: November 2017

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

An Improved Digital Image Watermarking Scheme using Particle Swarm Optimization Technique

Tamirat Tagesse Takore[1], P. Rajesh Kumar[2], G. Lavanya Devi[3]
[1, 2] *Dept. of ECE, College of Engineering (A), Andhra University, Visakhapatnam, India*
[3]*Dept. of CS&SE, College of Engineering (A), Andhra University, Visakhapatnam, India*

Abstract: Digital watermarking has been proposed as most effective ways to protect a copyright of digitally formatted multimedia documents in networked environments by inserting secret data into host image without significantly affecting the visual quality. Robustness to different accidental or intentional attacks is the most desired watermarking requirements for copyright protection application. This study presents a robust, blind and an imperceptible image watermarking scheme based on lifting wavelet transforms (LWT), discrete cosine transform (DCT), singular value decomposition (SVD) and particle swarm optimization (PSO). Block-based DCT and SVD are performed on reference sub-images which are formed by taking alternative pixels across row and column. A binary watermark is embedded in the first reference sub-image by modifying singular values and the other sub-image is used as a reference for both watermarks embedding and extracting. Different standard grayscale images have been used as test images and the obtained experimental results show improvement in both imperceptibly and robustness against various attacks.
Keywords: Digital watermarking, LWT, DCT, SVD, PSO, PSNR, NCC

I. INTRODUCTION

The advent and proliferation of high speed computers along with high capacity storage device and fast Internet have made the task of copying, reproducing, modifying and sharing digital multimedia data simple. Thus, digital data can be lossless copied and rapidly disseminated at large scale with less expense and effort. However, these technologies have also created a means for malicious attackers to copy, modify and redistribute copyrighted digital resources illegally without the consent of legit producers. This seriously violates the commercial advantages of many digital resources producing corporations. As a result, protecting digital properties from unauthorized use has become an issue of critical concern that the needs for tools which can protect ownership, guarantee authenticity and trace an illegal copy distribution, is extremely increasing from time to time. Cryptography provides a means for secure delivery of contents to the legitimate consumer with a key to decrypt the content. But untrustworthy consumers can buy a single copy of a legit document and distribute decrypted copies in a manner that is not allowed by content producers. Therefore, other effective copyright protection techniques are necessary to prevent unauthorized copying of digital content or trace illegal copy distribution. The newly evolving digital watermarking technique is the most effective method for digital property protection, and it complements the cryptographic process [1-3]. Digital watermarking is a process that inserts a digital message, signature, text or logo called watermark in a host object such that the embedded watermark, which fully characterizes the person who applies it can be extracted later to make an assertion about the object. It has been used to address the problem of authenticity verification, copyright protection and illegal dissemination of valuable digital resources. In fact, the field of digital *watermarking* is relatively young, and gained popularity as a research topic starting 1993 when Tirkel et al. [4] presented two techniques to hide data in images.

A typical watermarking system consists of two major components, namely watermark Embedder and Detector/ Extractor. Fig. 1 shows a block diagram of a generic watermarking scheme [5, 6]. The watermark Embedder E (.) takes a host image ‘H’, watermark ‘W’, and key ‘K’ as input parameters and provides a watermarked content ‘H_w’ as an output.

$$Hw=E(H,W,K) \tag{1}$$

The watermarked content may be transmitted through a vulnerable communication channel that malicious pirates could intrude and perform attacks on the content. After receiving possibly an attacked content, the extraction algorithm extracts the watermark and this procedure is defined as follows.

$$W_E = E_x(H_w^*, K, [H], [W]) \quad (2)$$

Where, *Ex (.)* is the watermark extraction algorithm. Hw^*, W_E represent the attacked watermarked content and extracted watermark respectively. The enclosed braces around *H* and *W* are used to denote optional input for watermark extraction.

Therefore, depending upon the type of input data required for watermark detection/extraction, watermarking techniques can be classified into blind (or oblivious) and non-blind.

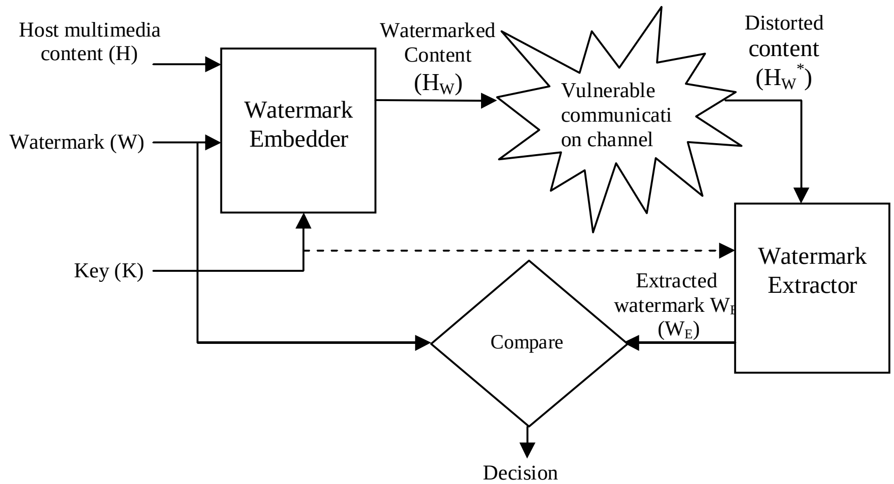


Fig. 1 A block diagram of generic watermarking system

Blind watermarking schemes extract the embedded watermark without the knowledge of original data (i.e., without using original host data and original watermark). Only with the help of a secret key, the watermark is extracted. However, non-blind watermarking techniques require original host document and a copy of the embedded watermark as input for watermark extraction. Compared to non-blind, a blind watermarking scheme is more preferred for a huge amount data-oriented watermarking applications due to its advantages such as reduced transmission time and storage cost overhead. Digital watermarking techniques can also be classified into four groups depending upon the type of data to be watermarked: text watermarking, image watermarking, audio watermarking, and video watermarking [7]. However, in this paper, only gray image watermarking technique is considered.

Furthermore, the watermarking techniques can be classified into spatial domain and transform domain watermarking techniques based on the working domain. Spatial domain watermarking techniques are straightforward and embed a watermark directly manipulating the pixel values of the host image. Usually, these types of watermarking techniques are computationally simple and easy to implement; however, they are less robust to various attacks. Least significant bit (LSB) substitution, correlation and spread spectrum based watermarking methods are common spatial domain based watermarking techniques. The transform domain techniques insert the watermark into transformed coefficients of the cover image. These watermarking techniques provide more information hiding capacity, better imperceptibility and more robustness compared to spatial domain techniques. A watermarking scheme is said to be robust when the embedded watermark is capable to survive against both accidental and intentional attacks. Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Singular Value Decomposition (SVD) and Lifting Wavelet Transform (LWT) are the most popular transforming techniques which are often used in transform domain watermarking techniques [8-11].

Designing a robust and imperceptible image watermarking scheme for copyright protection applications that can insert a watermark without significantly affecting the visual quality of the host image has become the major challenge in the field of digital watermarking due to the existence of two inversely related watermarking properties namely robustness and imperceptibility. Different watermarking schemes employing various techniques have been proposed to address this issue. Recently, blind-image watermarking techniques that embed a watermark into sub-images which are derived from the host image have become the most popular watermarking technique. Different reference sub-images forming methods have been proposed and available in the literature [12]. Authors in [13] proposed a blind and robust image watermarking scheme using Multiple Descriptions Coding (MDC) and Quantization Index Modulation (QIM). MDC was used to partition the host image into two sub-images called even description and odd description. A binary watermark has been embedded into the odd description using the even description as the reference.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

Murity et.al [14] proposed semi-blind reference based image watermarking scheme using DWT-SVD for copyright protection application. The authors formed reference sub-images by taking alternative blocks based on the magnitude of spatial frequency.

The other alternative strategy that has been adopted to address the aforementioned design challenges is using appropriate transform technique in the proposed scheme for watermark embedding. Numerous image watermarking schemes have been proposed employing different transform techniques and available in the literature. Singular value decomposition has been used widely for image watermarking due to its unique properties [15]. R. Liu et.al [16] proposed a novel watermarking scheme based on SVD and the proposed method can perform well in both security and robustness. The watermark has been embedded into the host image by modifying singular values. However, the scaling factor which controls the strength of the watermark to be inserted could not guarantee the trade-off between imperceptibility and robustness. SVD operation can be performed either at the whole image or block wise. But, recently, block-based image watermarking techniques become more popular because of their advantages, one of which is the ability to process each block individually [17]. To boost the performance of imperceptibility and robustness of the scheme and to overcome the drawbacks of SVD, several authors have proposed watermarking schemes using other transform techniques like DWT, DCT, and LWT in combination with SVD [18]. However, in recent years, because of its higher computational efficiency and lossless decomposition, lifting wavelet transform technique (LWT) widely used 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. I. A. Ansari et al. [19] 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), that are employed to adjust the coefficients during watermark embedding process, extremely determine the trade-off between imperceptibility and robustness. In [20] robust digital image watermarking scheme based on edge detection and singular value decomposition has been proposed. A sub-image, which is used as a region for watermark embedding, has been formed from selected blocks based on the number of edges. PSO algorithm has been used to achieve enhanced performance by searching embedding parameters which can maintain a better trade-off between robustness and imperceptibility.

The primary objective of this work is to build a secured, robust and perceptual transparent digital image watermarking system in a hybrid domain (i.e., employing LWT, DCT, and SVD) using PSO to find suitable multiple SF, which can give an optimal performance maintaining the trade-off between imperceptibility and robustness. Two non-overlapping sub-images are formed by taking even and odd pixels alternatively across the row and column, and a binary watermark is embedded into the even sub-image using an odd sub - image as a reference point. Fig. 2 depicts the two sub-image formed from the original Manderill image. We have used quality metric normalized-correlation-coefficient (NCC) and peak-signal-to-noise-ratio (PSNR) to measure the robustness and transparency of the proposed scheme respectively.

Fig. 2 Mandrill host image, even sub-image and odd sub-image

The rest of this paper is organized as follows. In section II provides a mathematical description of the transform techniques, which we have used in the proposed scheme, is explained briefly. Detail of PSO based MSF optimization processes are described in section III. Section IV illustrates the proposed watermark embedding and extraction procedure. Section V presents experimental setup and results. Finally, the concluding remarks are presented in section VI.

II. THE MATHEMATICAL PRELIMINARIES OF USED TRANSFORMS

A. Discrete cosine transforms

Discrete cosine transform (DCT) is a well-known transform in image processing which transforms an image from the spatial domain to frequency domain. It helps separate the image into parts (or spectral sub-bands) of differing importance (with respect to the image's visual quality). Fig. 3 shows the various frequency regions of DCT coefficients. For 2D host image h (x, y) of size M×N, the general equation for forward and inverse DCT are defined by the following equations.

$$H(u,v)=\sigma(u)\sigma(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}h(x,y)\cos\left[\frac{(2x+1)u\pi}{2M}\right]\cos\left[\frac{(2y+1)v\pi}{2N}\right] \tag{3}$$

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

$$\sigma(u),\sigma(v)=\begin{cases}\frac{1}{\sqrt{2}} & for\, u,v=0\\ 1 & for\, u=1,2,\cdots,M;\quad v=1,2,\cdots,N,\end{cases} \tag{5}$$

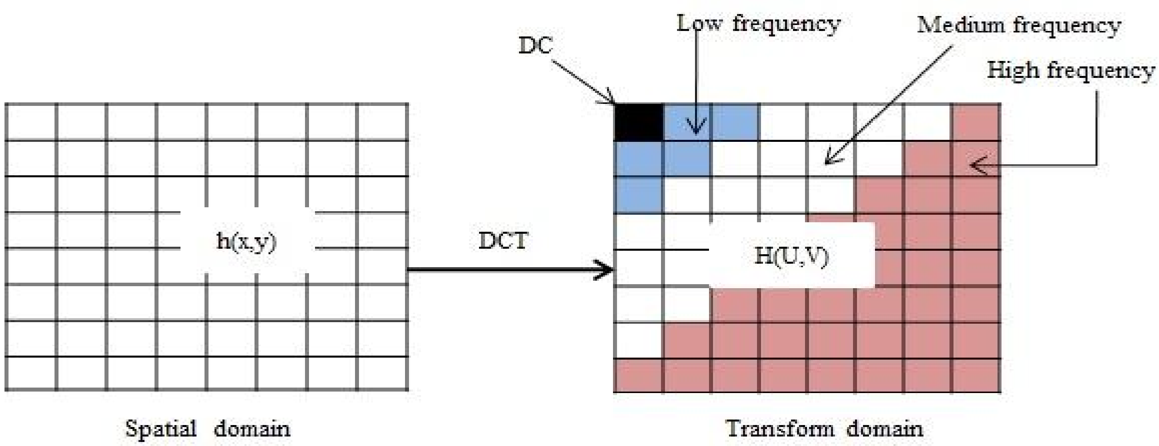


Fig. 3 Different frequency regions of DCT coefficients

B. Lifting wavelet transform

Using traditional wavelet transform for watermark scheme designing faces certain limitations. Since traditional wavelet transform is a floating point algorithm, Computers with limited data processing ability create rounding error such that the process of reconstructing the exact signal becomes unattainable. Moreover, this transform needs sophisticated computation facility, and it makes hardware implementation to be complex and costly. The mentioned constraints can be resolved by using lifting wavelet transforms. LWT is a more versatile technique, and it was first introduced by W. Sweldens in 1995 [21]. The technique inherits multi-resolution properties of traditional wavelet transform while adding new other properties. The main procedure of LWT involves three main operations viz. splitting, predicting and updating and the block diagram of forward and inverse LWT is shown in Fig. 4.

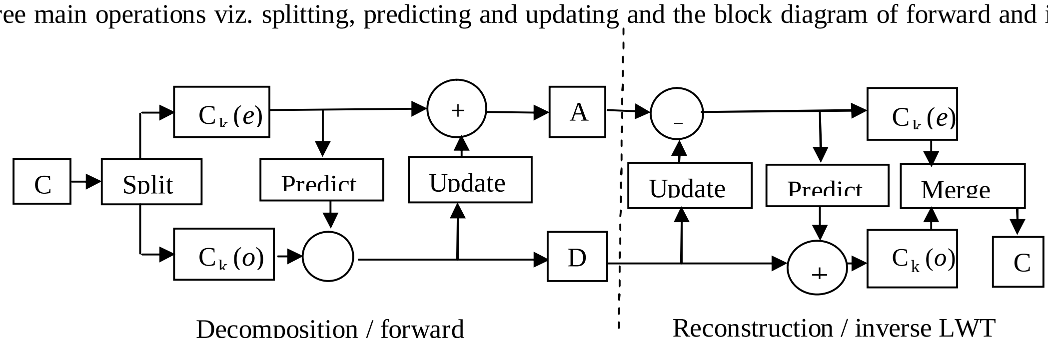


Fig. 4 Block diagram of lifting scheme.

C. Singular value decomposition

From the view of image processing, a digital image can be considered as a matrix such that pixel intensity values represent entries of the matrix. So, a linear algebra technique, namely singular value decomposition (SVD) can be used for digital image watermarking because of its popular advantages. The SVD of an image matrix H of size M×N is the factorization of H into the product of three matrices U, S, and V such that,

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

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

$$UU^T = U^TU = I \text{ and } VV^T = V^TV = I \quad (7)$$

S is a nonnegative diagonal matrix containing the square root of the eigenvalues of either U or V matrix and the elements is arranged in descending order $s_1 \geq s_2 \geq \cdots s_{MN}$.

III. PARTICLE SWARM OPTIMIZATION

The amount of signal embedded into host image determines the level of robustness and imperceptibility of the watermarked image. In fact, robustness and imperceptibility are the most required watermarking properties for the copyright protection application. However, both properties are conflicting with each other that increasing one decreases the other and vice-versa. The quantity of signal embedded and robustness have a direct relationship, whereas imperceptibility and the amount of embedded signal are inversely related. Scaling factors (SF), which are used to modify the coefficients during watermark embedding control the quantity of the signal to be embedded. Therefore, the problem of finding suitable SF, which can give optimum performance and maintain the trade-off between transparency and robustness, can be viewed as an optimization problem. Appropriate SF can be obtained using a metaheuristic optimization algorithm, and in this paper, we have used particle swarm optimization algorithm. PSO algorithm was first developed by Eberhart and Kennedy in 1995 [22]. The algorithm starts searching process by randomly initializing particles having position x_i (t) and velocity v_i (t). The particles update their position and velocity in every iteration using the following equation.

$$v_i(t+1) = W_i v_i(t) + C_1 rand\,(p_{best} - x_i(t)) + C_2 rand\,\,(g_{best} - x_i(t)) \quad (8)$$

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (9)$$

Where, p_{best} and g_{best} are personal best and global best of the particles at a given iteration. W_i is inertia weight which determines the step size, C_1 and C_2 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.

The fitness function *ff* is formulated from quality measuring metric PSNR and NCC, and the definition is presented as follows.

$$ff = Max\left\{PSNR(H, H_w) + \beta \sum_{i=1}^{n} NCC(W, W_E)\ \right\} \quad (10)$$

Where, *H* and *Hw* are original host image and watermarked image respectively; while W and W_E are original watermark and extracted watermark respectively. The detail definition of PSNR and NCC are presented in section V. The flowchart for the proposed PSO based optimum scaling factors searching and objective value computation is shown in Fig. 5.

IV. PROPOSED WATERMARKING SCHEME

The proposed watermarking scheme consists of two main algorithms: watermark embedding and extraction algorithms. The detail of each algorithm is presented in the following sub-section.

A. *Proposed watermark embedding algorithm*

The watermark embedding algorithm takes a host image and a watermark logo as an input and provides a watermarked image as an output. The followings are the steps involved in the watermark embedding.

1) *Step1:* perform LWT operation on host image.

$$(LL, LH, HL, HH) = LWT(H) \quad (11)$$

2) *Step2:* take approximation coefficient (*LL*) and split it into two sub-images called even and odd description (i.e., H_{rf}^{E} and H_{rf}^{O} by taking alternative pixels along the row and column wise.
3) *Step3:* Apply block based DCT on the reference images using block size of 4×4.

$$\left.\begin{aligned} H_{rf\,(m,n)}^{DCT1} &= DCT(F_{rf}^{E}) \\ H_{rf\,(m,n)}^{DCT2} &= DCT(F_{rf}^{O}) \end{aligned}\right\} \quad (12)$$

4) *Step4:* Factorize DCT coefficient using SVD operation.

$$\left.\begin{aligned} U_{rf\,(m,n)}^{E}\, S_{rf\,(m,n)}^{E}\, V_{rf\,(m,n)}^{E} &= SVD(H_{rf\,(m,n)}^{DCT1}) \\ U_{rf\,(m,n)}^{O}\, S_{rf\,(m,n)}^{O}\, V_{rf\,(m,n)}^{O} &= SVD(H_{rf\,(m,n)}^{DCT2}) \end{aligned}\right\} \quad (13)$$

5) *Step5:* Use the obtained multiple scaling factors (MSF) from PSO and insert binary watermark by modifying singular values using equation (14).

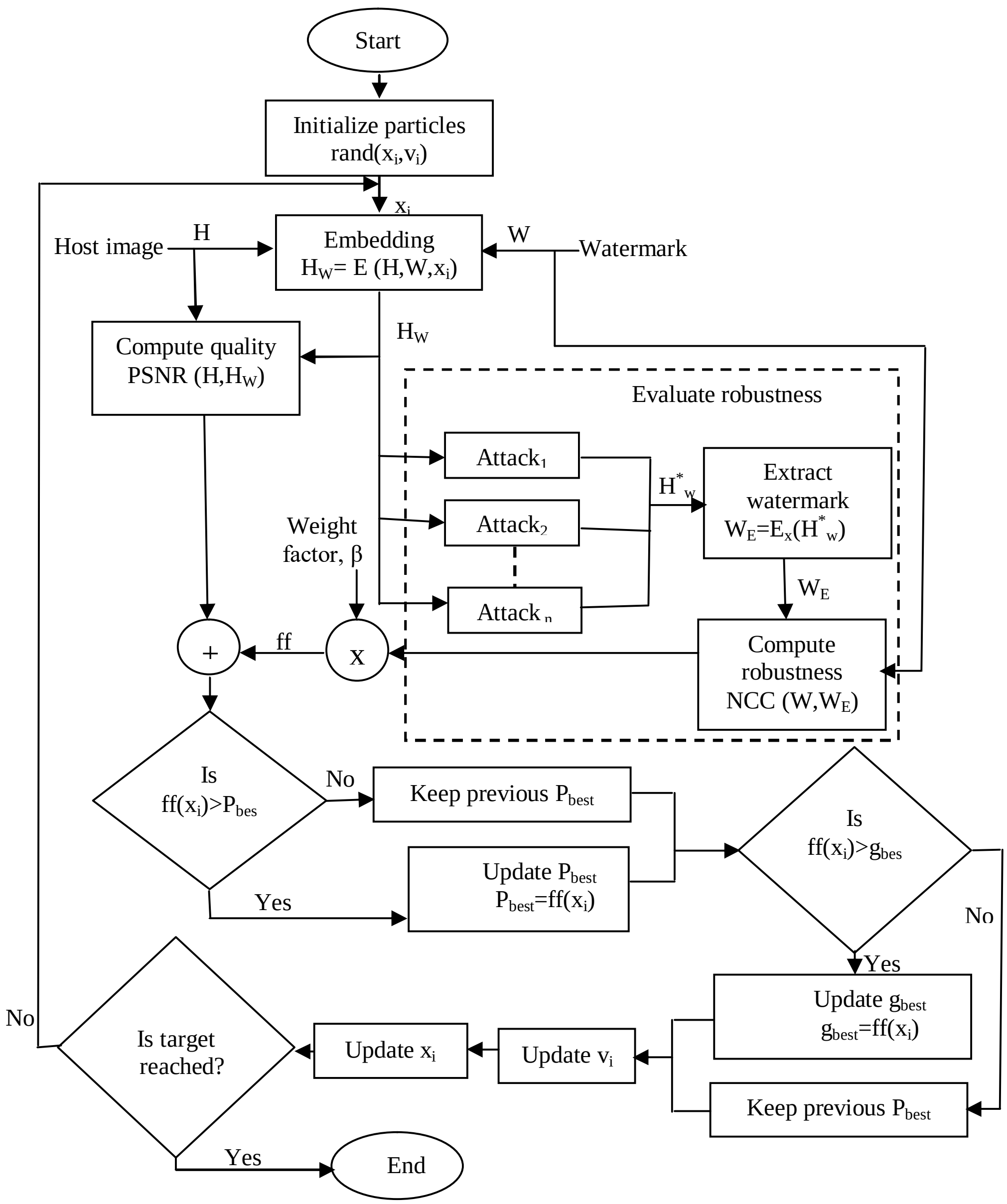


Fig 5. A flowchart of PSO based scaling factor optimization.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

$$S^{E}_{Wrf(m,n)}(i,j)=\begin{cases} \quad if\ W(m,n)=1 \\ \begin{cases} S^{E}_{rf(m,n)}(i,j), & if\ S^{E}_{rf(m,n)}(i,j)>S^{O}_{rf(m,n)}(i,j) \\ S^{E}_{rf(m,n)}(i,j)+\lambda S^{O}_{rf(m,n)}(i,j), & if\ S^{E}_{rf(m,n)}(i,j)\le S^{O}_{rf(m,n)}(i,j) \end{cases} \\ \quad if\ W(m,n)=1 \\ \begin{cases} S^{E}_{rf(m,n)}(i,j), & if\ S^{E}_{rf(m,n)}(i,j)<S^{O}_{rf(m,n)}(i,j) \\ S^{E}_{rf(m,n)}(i,j)-\lambda S^{O}_{rf(m,n)}(i,j), & if\ S^{E}_{rf(m,n)}(i,j)\ge S^{O}_{rf(m,n)}(i,j) \end{cases} \end{cases} \tag{14}$$

Where i=j=1 and $\lambda=\lambda_k$ if the magnitude $\left|S^{E}_{rf(m,n)}(i,j)-S^{O}_{rf(m,n)}(i,j)\right|$ is in the interval r_k .

6) *Step6:* Perform inverse SVD operation to obtain watermarked blocks.

$$B^{E}_{W(m,n)}=U^{E}_{rf(m,n)}S^{E}_{Wrf(m,n)}V^{E^{T}}_{rf(m,n)} \tag{15}$$

7) *Step7:* Apply inverse DCT on $B^{E}_{W(m,n)}$ and merge the blocks to get watermarked sub-image.

$$H^{E}_{Wrf}=IDCT(B^{E}_{W(m,n)}) \tag{16}$$

8) *Step8:* Merge the two sub-images (i.e. H^{E}_{Wrf} and H^{O}_{rf}) together to obtain watermarked approximation coefficient LL^{W} .

9) *Step9:* Finally a watermarked image F_W can be obtained by performing inverse LWT.

$$F_W=ILWT(LL^{W},LH,HL,HH) \tag{17}$$

B. Proposed watermark extraction algorithm

Since the proposed watermarking scheme is blind, neither original host image, nor a copy of embedded watermark is required for extraction. The watermark extraction algorithm takes only watermarked image only which could also be an attacked one by pirates while being transmitted through an insecure medium. The steps of the proposed watermark extraction algorithm are presented as follows.

1) *Step1:* Take possibly an attacked watermarked image (H^{*}_{w}) and performs LWT.

$$(LL_{xt},LH_{xt},HLxt,HH_{xt})=LWT(H^{*}_{W}) \tag{18}$$

2) *Step2:* Split LL_{xt} into two sub-image H^{xtE}_{rf} and H^{xtO}_{rf} .

3) *Step3*: Divide the sub-images into non-overlapping blocks and perform DCT.

$$\begin{aligned} H^{xtDCT1}_{rf}&=DCT(H^{xtE}_{rf}) \\ H^{xtDCT2}_{rf}&=DCT(H^{xtO}_{rf}) \end{aligned} \tag{19}$$

4) *Step4:* Factorize DCT coefficients.

$$\left.\begin{aligned} (U^{xtE}_{rf(m,n)}\ S^{xtE}_{rf(m,n)}\ V^{xtE}_{rf(m,n)})&=SVD(F^{xtDCT1}_{rf(m,n)}) \\ (U^{xtO}_{rf(m,n)}\ S^{xtO}_{rf(m,n)}\ V^{xtO}_{rf(m,n)})&=SVD(F^{xtDCT2}_{rf(m,n)}) \end{aligned}\right\} \tag{20}$$

5) *Step5:* Finally, Extract the watermark using the following equation.

$$W_E(m,n)=\begin{cases} 1, & if\ S^{xtE}_{rf(m,n)}(i,j)\ge S^{xtO}_{rf(m,n)}(i,j) \\ 0, & otherwise \end{cases} \tag{21}$$

The proposed watermark embedding and extracting steps, which are discussed above, are presented in Fig. 6 and Fig. 7 in well-organized manner using flowcharts.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

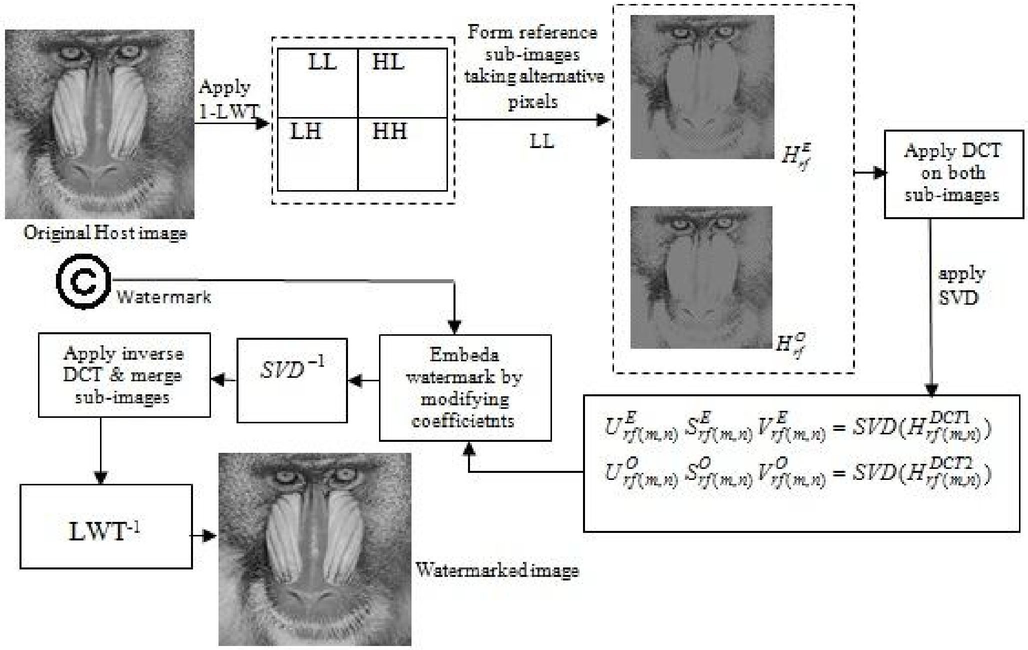


Fig. 6 Flowchart of the proposed watermark embedding algorithm

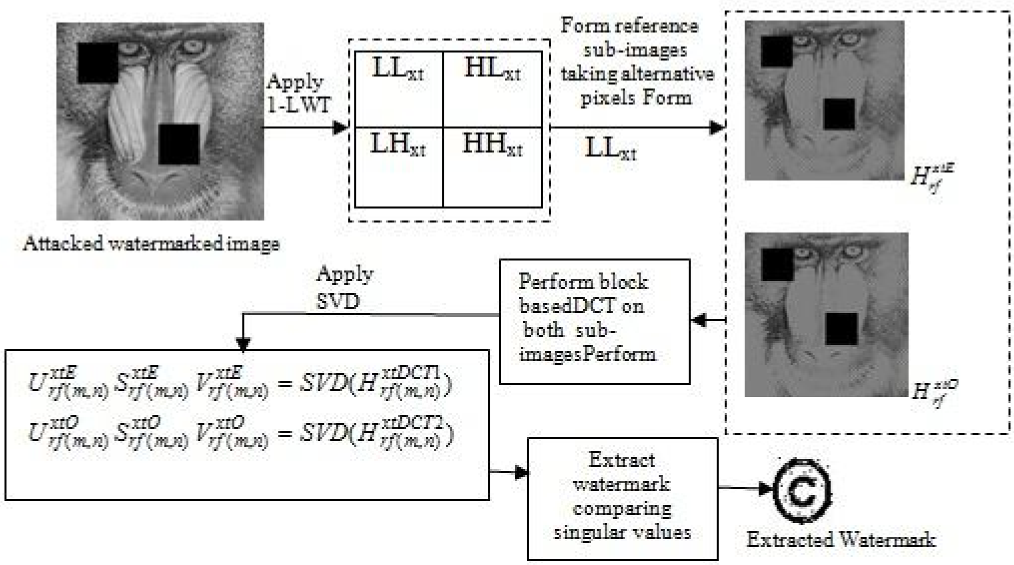


Fig. 7. Flowchart of the proposed watermark extraction algorithm

V. EXPERIMENTAL RESULTS AND DISCUSSION

We have simulated the proposed watermarking algorithm using Matlab software and have conducted a series of experiments to examine the performance of the scheme. The grayscale image of Lena, Manderill, man, and pepper of size 512×512 has been used as test cover images. In addition, the scheme takes the copyright logo and 'AU' character of size 32×32 as input watermarks and inserts them into the host images using the proposed procedure. Fig. 8 shows the test images and watermark logo images. We have employed multiple scaling factors (MSF) instead of a single scaling factor (SSF) to improve the robustness maintaining the quality of the watermarked image within an acceptable level. The PSO parameters C_1 and C_2 are set to be 2, and the value of the inertia weight W_i is made to vary adaptively depending on the iteration. To reduce computational burden, we have set a number of particles and maximum iteration to 20 and 100 respectively.

The binary watermarks are embedded into the cover images by using the proposed embedding technique, and the obtained watermarked images are shown in Fig. 9. The most widely used quality metric knows as PSNR has been used in this work to

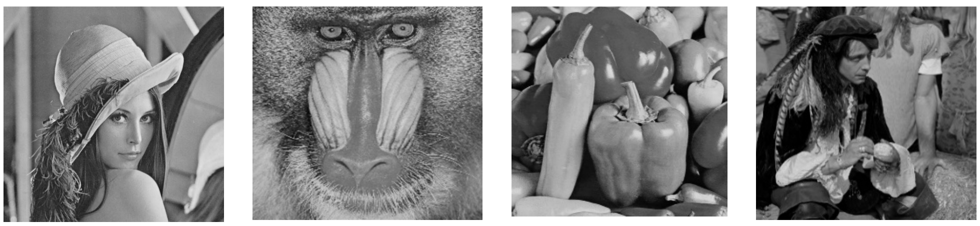
International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

measure the degree of similarity between the original cover image and watermarked image. The definition of PSNR is given in equation 22.

$$PSNR = 10\log\frac{255^2}{\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(H_W(x,y)-H(x,y))^2}dB \qquad (22)$$

Where, H is original cover image and H_W is a watermarked image.

In the field of digital image watermarking, the minimum acceptable PSNR value is 38 dB [23]. Attaining higher value of PSNR confirms that the watermarking scheme is able to insert secret information into cover image without causing significant quality loss.



(a) (b) (c) (d)

(e) (f)

Fig. 8. The test images (a) Lena (b) mandrill (c) pepper (d) man (e) watermark logo, WM_1 (f) binary watermark logo, WM_2

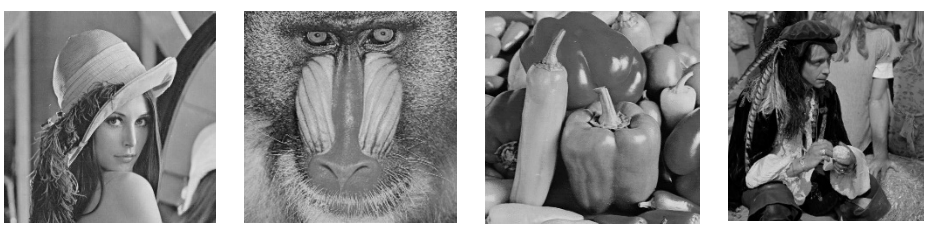


Fig. 9 Watermarked test images.

By merely looking the obtained watermarked images which are shown in Fig. 9, we can conclude that the proposed scheme is capable to achieve the imposed quality requirement. The obtained PSNR values in attack free scenario are given in Table1.

TABLE 1

PSNR OF WATERMARKED IMAGES USING MSF IN ATTACK FREE SCENARIO.

Images	Lena	Mandrill	Pepper	Man
PSNR	46.2781	45.8172	45.4817	45.079

Furthermore, a watermarking scheme for media copyright protection application should be robust to various intentional or accidental attacks. The term ‘robustness’ refers to the ability of an embedded watermark to survive against the performed attacks. Any image processing techniques which can degrade or destroy the inserted information are treated as attacks in this paper, and eighteen different attacks have been employed to evaluate the level of robustness. These 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, the 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. 10 shows attacked watermarked Lena images using different attacks. After the attacks, the affected watermarked images are passed to

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

the proposed watermark extraction algorithm as input to check the existence of the embedded watermark resisting the performed attacks. Fig. 11 shows the list of attacks performed and the respective extracted watermark images.

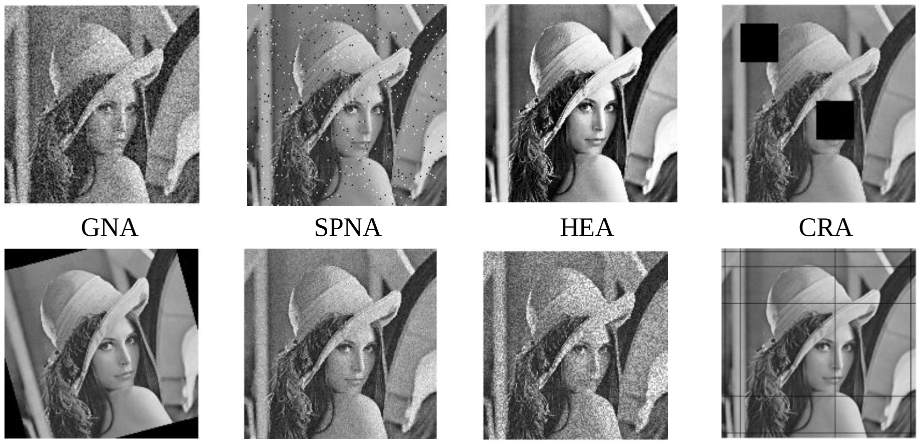
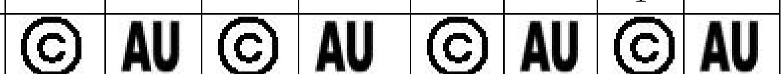
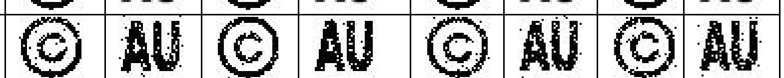
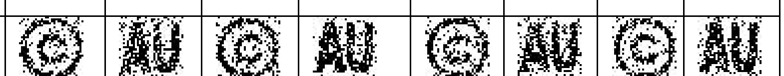
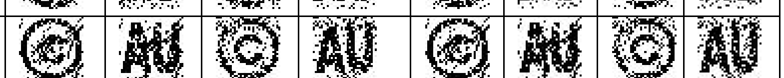
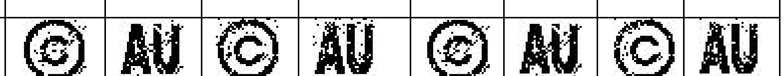
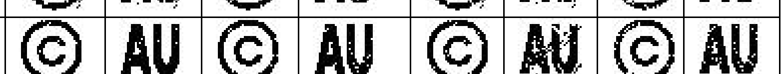
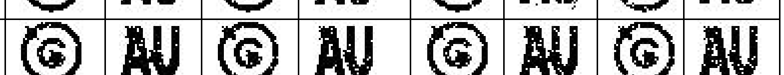


Fig. 10 Attacked watermarked Lena images

As we can see from the figure, the proposed watermarking scheme is able to provide good quality extracted image after the performed attacks. The metric, normalized correlation coefficient (NCC) has been used to measure the level of similarity between the original and extracted watermark. Let W is an original watermark and W_E is extracted watermark of size (p,q), then the NCC can be computed by using the following equation.

$$NCC = \frac{\sum_{i=1}^{p}\sum_{j}^{q}(W(i,j)-\mu)(W_E(i,j)-\mu_E)}{\sqrt{\sum_{i=1}^{p}\sum_{j}^{q}(W(i,j)-\mu)^2}\sqrt{\sum_{i=1}^{p}\sum_{j}^{q}(W_E(i,j)-\mu_E)^2}} \qquad (23)$$

Attacks	Extracted watermark							
	Using SSF				Using MSF			
	Lena		Mandrill		Lena		Mandrill	
	WM1	WM2	WM1	WM2	WM1	WM2	WM 1	WM2
Attack free (AF)								
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)								

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue XI November 2017- Available at www.ijraset.com

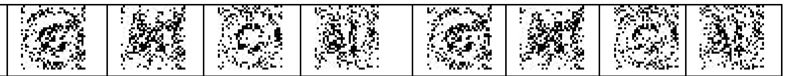
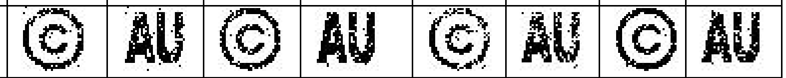
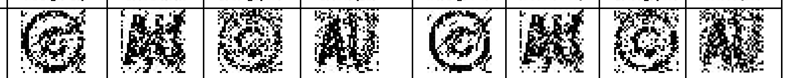
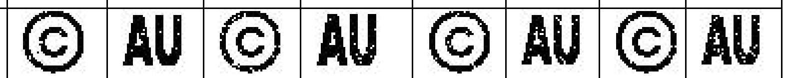
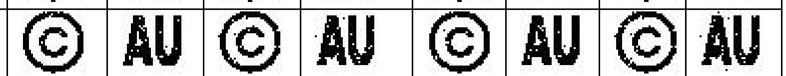
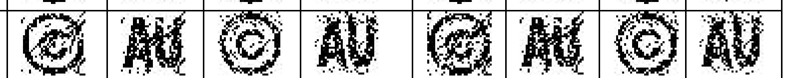
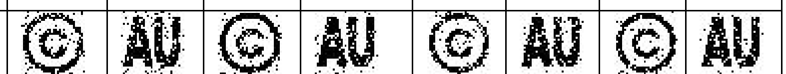
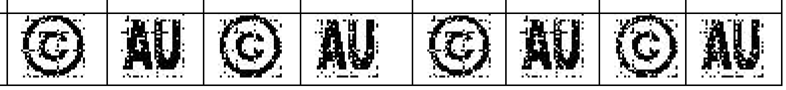
Rotation attack (RTA) (5^o)	
JPEG compression attack (JPCA) (QF=70%)	
Average filter attack (AVFA) (3x3)	
Gaussian low pass filter (GLPFA) (3x3)	
Camera motion attack (CMA) (len=9,θ=0)	
Least bit removing attack (LBRA) (LSB removed)	
Image sharpening attack (SRA)	
Resizing attack (RSA) (512→256→512)	
Wiener filter attack (WFA) (3x3)	
Poison noise attack (PNA)	
Speckle noise attack (SNA) (μ=0, v=0.04)	
Row-Column blanking attack (RCBA)	

Fig. 11 Extracted watermark images from attacked images

A watermarking scheme is said to be robust to a given attack when the NCC between an original watermark and extracted watermark is closer to 1. In fact, a robustness of a scheme is at an acceptable level if the NCC value is greater than or equal to 0.75 [23]. Table 2 shows the value of PSNR and NCC of proposed watermarking scheme using SSF and MSF by applying different attacks. From the table, we can notice that the PSNR and NCC values are in the acceptable level except rotation attack. Therefore, from overall result one can confirm that the proposed scheme can attain the imposed quality and robustness requirements.

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	44.5362	1	45.3521	1	45.0125	1	45.8632	1
GNA	43.6644	0.9664	44.1175	0.9828	43.9694	0.9719	44.632	0.9838
SPNA	42.2495	0.9386	41.7177	0.9278	44.0556	0.9584	44.0133	0.9471
MFA	42.8188	0.9471	43.0841	0.9435	44.06895	0.95082	45.0913	0.9499
HEA	44.0359	0.9541	43.1222	0.9527	45.0121	0.9626	43.2268	0.9932
GCA	44.7487	0.9942	44.7062	0.9981	45.0199	0.9959	44.8452	0.9995
CRA	44.9699	0.9579	44.9985	0.9577	44.9737	0.9586	44.9733	0.9582
RTA	44.5376	0.6851	44.4656	0.6547	44.8233	0.7263	44.8861	0.7297
JPCA	43.4396	0.9523	43.0445	0.9763	43.8693	0.9648	44.2832	0.9784

AVFA	41.4154	0.9341	42.9391	0.9352	43.7485	0.9573	43.1576	0.9426
GLPFA	43.0961	0.9743	44.5342	0.9836	44.8803	0.9768	43.9761	0.9867
CMA	44.4666	0.8679	41.6452	0.9081	44.8093	0.8924	43.3565	0.9155
LBRA	44.5028	0.9925	45.0161	0.9925	44.9976	0.9945	44.8548	0.9946
SRA	44.9771	0.9925	43.9254	0.9874	45.0073	0.9932	44.7919	0.9964
RSA	44.3489	0.9358	42.8788	0.9475	44.4379	0.9546	43.0774	0.9501
WFA	42.8733	0.9533	42.9315	0.9147	43.3146	0.9617	43.3828	0.9165
PNA	42.8312	0.9441	43.1235	0.9551	43.0152	0.9572	43.9018	0.9595
SNA	42.1291	0.9031	42.3941	0.9129	42.4632	0.9184	42.9712	0.9194
RCBA	43.0521	0.9236	42.7812	0.9302	43.0125	0.9355	43.0528	0.9357

TABLE 3 OPTIMIZED MSF FOR JPCA (QF=80%)

Cover image	PSNR	NCC (JPCA, QF=80)	Optimized MSF [λ_k] for different ranges				
			λ_1	λ_2	λ_3	λ_4	λ_5
Lena	43.8693	0.9949	0.1737	0.1635	0.1550	0.0169	0.0009
Mandrill	44.2832	0.9969	0.1821	0.1600	0.0863	0.0800	0.0520
Pepper	43.0961	0.9934	0.1884	0.0808	0.0483	0.0264	0.0193
Man	42.4154	0.9929	0.1912	0.1150	0.0706	0.0470	0.0120

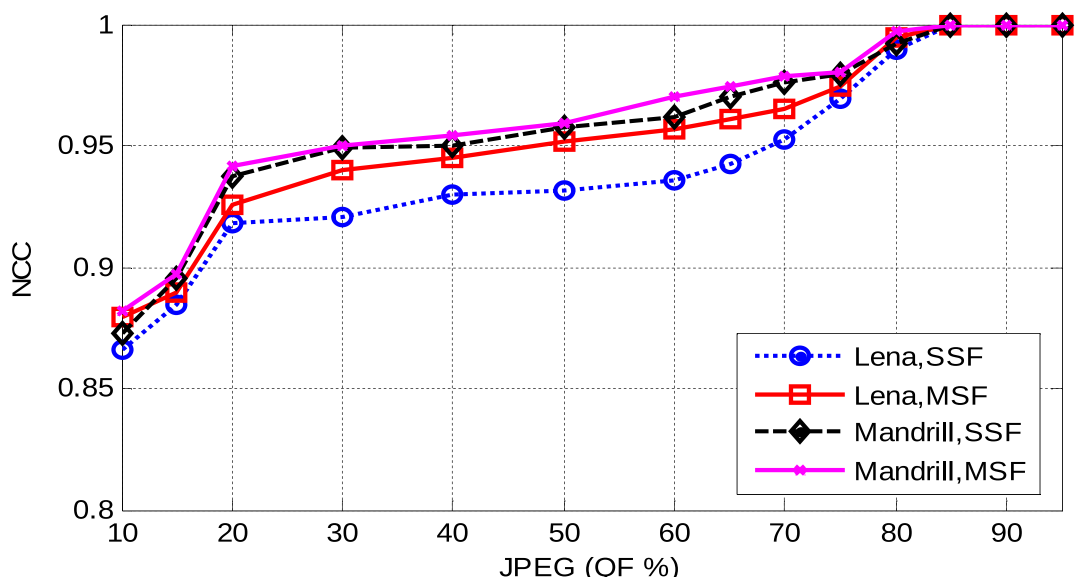


Fig. 12 NCC values of extracted watermark for JPEG attack

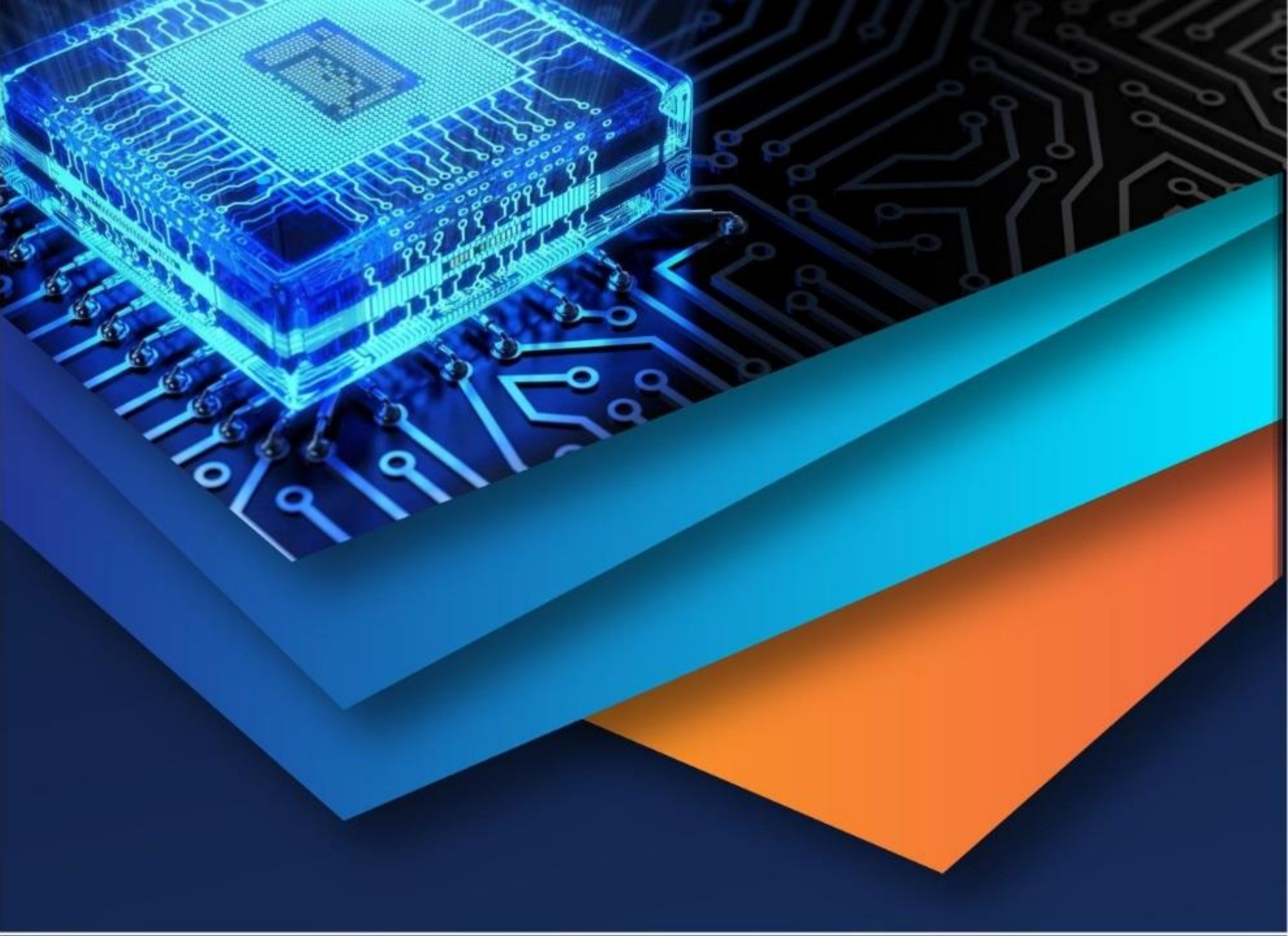
Table 3 shows the result of optimized multiple scaling factors in the case of JPEG compression attacks. In Fig. 12 plot of NCC value versus QF of JPCA for both SSF and MSF is shown. From the above results we can observe that using MSF improve the result of PSNR and NCC compared SSF.

VI. CONCLUSION

In this paper, a blind digital image watermarking scheme for copyright protection application, which can satisfy the robustness and imperceptibility requirement, is proposed using hybrid transforms and PSO. The original cover image is split into two sub-images by taking alternative pixels across row and column. A binary watermark is embedded into the first-sub image by modifying singular values and the second sub image is used as reference for both watermark inserting and extracting. The challenge of maintaining balance between imperceptibility and robustness is solved by employing MSF and particle swarm optimization method is used to obtain optimized parameters. Compared to existing schemes, the performance of the proposed scheme has been evaluated by applying a maximum number of attacks and the obtained confirm that the scheme is able to provide improved NCC and PSNR results.

REFERENCES

[1] L. Me and G. Arce, "A class of authentication digital watermarks for secure multimedia communication," IEEE Transactions on Image Processing, vol. 10, no. 11, pp. 1754–1764, 2001.
[2] P. C. Korus, "Digital image integrity – a survey of protection and verification techniques," Digital Signal Processing, vol. 71, pp. 1–26, 2017.
[3] C. Rey and J.-L. Dugelay, "A Survey of Watermarking Algorithms for Image Authentication," EURASIP Journal on Advances in Signal Processing, vol. 2002, no. 6, pp. 613–621, 2002.
[4] A.Z.Tirkel et al., Electronic Watermark, Aust. Pattern Recognition. Soc., Canberra, ACT, Australia, pp. 666–673, 1993.
[5] H. Nyeem, W. Boles, and C. Boyd, "Digital image watermarking: its formal model, fundamental properties and possible attacks," EURASIP Journal on Advances in Signal Processing, vol. 2014, no. 1, 2014.
[6] H. Tao, L. Chongmin, J. M. Zain, and A. N. Abdalla, "Robust Image Watermarking Theories and Techniques: A Review," Journal of Applied Research and Technology, vol. 12, no. 1, pp. 122–138, 2014.
[7] C. Song, S. Sudirman, and M. Merabti, "Recent advances and classification of watermarking techniques in digital images," in Proceedings of post graduate network symposium, pp. 1–6, 2009.
[8] S. Liu, Z. Pan, and H. Song, "Digital image watermarking method based on DCT and fractal encoding," IET Image Processing, vol. 11, no. 10, pp. 815–821, Oct. 2017.
[9] Xiangui Kang, Jiwu Huang, Y. Q. Shi, and Yan Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 776–786, Aug. 2003.
[10] T. T. Takore, P. R. Kumar, and G. L. Devi, "Efficient gray image watermarking algorithm based on DWT-SVD using genetic algorithm," Proc. IEEE, in International Conference on Information Communication and Embedded Systems (ICICES), pp. 1–6, 2016.
[11] Z. Zhang, L. Wu, S. Xiao, and S. Gao, "Adaptive reversible image watermarking algorithm based on IWT and level set," EURASIP Journal on Advances in Signal Processing, vol. 2017, no. 1, Dec. 2017.
[12] T. T. Takore, P. R. Kumar, and G. L. Devi, "A modified blind image watermarking scheme based on DWT, DCT and SVD domain using GA to optimize robustness," Proc. IEEE, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT),pp. 2725–2729, 2016.
[13] K. Ramanjaneyulu and K. Rajarajeswari ,"An Oblivious and Robust Multiple Image Watermarking Scheme Using Genetic Algorithm," The International journal of Multimedia & Its Applications, vol. 2, no. 3, pp. 19–38, 2010.
[14] P. Satyanarayana Murty, M. Uday Bhaskar, Nanna Babu, and Rajesh Kumar, "A Semi-Blind Reference Watermarking Scheme Using DWT-SVD for Copyright Protection," The International journal of Multimedia & Its Applications, vol. 3, no. 3, pp. 61–70, Aug. 2011.
[15] R. A. Ghazy et al., "Block-based SVD image watermarking in spatial and transform domains," International Journal of Electronics, vol. 102, no. 7, pp. 1091–1113, Jul. 2015.
[16] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121–128, 2002.
[17] M.-R. Keyvanpour and F. Merrikh-Bayat, "Robust dynamic block-based image watermarking in DWT domain," Procedia Computer Science, vol. 3, pp. 238–242, 2011.
[18] Z. Zhang, C. Wang, and X. Zhou, "Image watermarking scheme based on Arnold transform and DWT-DCT-SVD," in Signal Processing (ICSP), 2016 IEEE 13th International Conference on, 2016, pp. 805–810.
[19] 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, Mar. 2016.
[20] Department of Electronics and Communication Engineering, Andhra University, Visakhapatnam, India, T. Tagesse Takore, P. Rajesh Kumar, and G. Lavanya 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, Jul. 2017.
[21] W. Sweldens, "The lifting scheme: A construction of second generation wavelets." SIAM journal on mathematical analysis, vol. 29, no. 2, pp. 511-546, 1998.
[22] J. Kennedy and R. Eberhart, "Particle swarm optimization," vol. 4, pp. 1942–1948, 1995.
[23] 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," Digital Signal Processing, vol. 33, pp. 134–147, Oct. 2014.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY