Multimed Tools Appl (2018) 77:14407–14434
DOI 10.1007/s11042-017-5035-9

Geometric distortion correction based robust watermarking scheme in LWT-SVD domain with digital watermark extraction using SVM

Mohiul Islam[1] · Rabul Hussain Laskar[1]

Received: 2 January 2017 / Revised: 2 June 2017 / Accepted: 12 July 2017 /
Published online: 31 July 2017

Abstract With the advent of technology, digital image watermarking turns to be an effective technique to protect digital images from illegal usages and manipulation. In digital image watermarking, one of the major challenges is to provide robustness against geometrical attack maintaining adequate level of imperceptibility and security. In this work, a robust digital image watermarking scheme is proposed based on the combination of lifting wavelet transform(LWT) and singular value decomposition(SVD). To achieve better correlation between the extracted and original watermark, SVM-based binary classification approach is integrated in watermark extraction. In the proposed technique, geometric distortion correction based approach is incorporated with SVM based binary watermark detection to achieve improved robustness against de-synchronization attack. The 3-level LWT is performed on the cover image where horizontal (HL) sub-band is chosen for binary watermark insertion. The training and testing patterns are formed using an optimized set of features along with the singular values of corresponding blocks. In case of de-synchronization attacks, geometrical distortion correction is required before performing watermark extraction. In the detection process, the geometric distortion parameters of the attacked watermarked image are estimated by the geometric correction method. This algorithm provides high robustness against both the geometrical and non-geometrical attacks. It has been observed that the algorithm gives average imperceptibility of ~42.27 dB with the watermark capacity of 512 bits. Experimental results suggest that the proposed watermarking scheme provides significant improvement in terms of robustness and security of the watermark. The subjective analysis also suggests that proposed scheme provides improved performance over some of the recent existing techniques.

Keywords Image watermarking · Lifting wavelet transform(LWT) · Singular value decomposition(SVD) · Support vector machine(SVM) · Invariant centroid · Radon transform

✉ Mohiul Islam
mohiul292@gmail.com

[1] Department of ECE, NIT Silchar, Silchar, Assam 788010, India

1 Introduction

The advancement of computer technologies and the growth of the Internet and digital consumer devices have significantly changed the world and daily lives by making the capture, distribution, and storage of digital data extremely easy and convenient. However, this also brings many practical problems like illegal transmissions and manipulations, and the issue has become problematic in many areas. To secure digital data from unauthorized access and usages, various information hiding techniques [1, 2, 4, 7, 13, 15] have been developed. Cryptography [17], steganography [3, 14, 20, 34, 35] and watermarking [5, 7, 19, 28, 47] are the popular techniques available to hide data securely. Digital image watermarking is an effective solution for authentication and copyright protection of images in popular communication environments like the Internet, which is vulnerable to illegal usages. The basic principle of image watermarking is to hide some covert data that provides ownership or copyright information as a watermark into a cover image which acts as host. Based on embedding domain, watermarking techniques are classified as spatial domain technique and transform domain technique. It has been observed from the literature that though the spatial domain techniques [5] are simple and easy to implement, but it provides less robustness as compared to transform domain techniques.

Over the past few years, several transform domain techniques [19, 22, 27, 28, 31, 47] based on discrete wavelet transform (DWT), lifting wavelet transform (LWT), discrete cosine transform (DCT), discrete Fourier transform (DFT) etc. have been proposed. These techniques employ signal characteristics and human perception property so as to obtain better performance in contrast to spatial domain techniques. Different decomposition techniques like singular value decomposition (SVD), QR decomposition also have been integrated with transformation techniques to achieve enhanced performance [18, 29, 30, 32, 33, 42, 45].

To resist geometric attacks, many algorithms have been proposed based on Fourier–Mellin transform [40], geometric moments [10], Radon transform [54], angular radial transform (ART) [41], and Zernike moments [23], that embed the watermark in the geometric invariant domains. Generally, these techniques perform effectively under the scaling or rotation attacks. However, these techniques can provide significantly degraded performance against other geometric attacks like cropping [6]. Li et al. [23] have proposed a watermarking method in DWT and SVD domain utilizing the invariant centroid and Zernike transform that estimates the effect of de-synchronization attacks likely rotation, flipping, scaling, translation, and RST. But the technique fails to provide robustness against scaling attack. C. Deng et al. [8] have proposed a content-based watermarking technique which combines the invariant feature extraction with watermark embedding by using Tchebichef moments. In that approach, the watermark is embedded in magnitudes of Tchebichef moments via dither modulation to realize the robustness to common image processing operations and the blind detection. Likewise, X. Gao [12] have also proposed a novel robust watermarking technique that embeds watermark in affine covariant regions (ACR) insensitive to geometric distortions. C. Deng et al. [9] have proposed another robust watermarking scheme based on local histograms that can resist both the global as well as local geometric attacks. However, main drawback of the technique is that watermark embedding capacity is low.

Recently, there has been a trend of using machine learning and soft computing approaches to achieve improved performance. These approaches have been applied in different fields of image processing applications like digital watermarking, image retrieval, hand gesture recognition, face recognition systems etc. [24–26, 39, 44, 48]. Different machine learning techniques have also been applied in watermarking to achieve better robustness. Yu et al. [53] have proposed a spatial domain digital watermarking scheme based on artificial neural network(ANN) where multi-layer perceptrons (MLPs) based neural networks have been employed to learn the characteristics of the embedded watermark related to the watermarked image. Using discrete wavelet transform (DWT) and genetic algorithm(GA), Ramanjaneyulu et al. [37] have proposed a watermarking scheme that outperforms previous scheme. In this method, the watermark embedding and extraction procedures are characterized by scaling factor parameters and GA has been used for parameter optimization. Though, the scheme is robust against various types of image processing attacks, but, fails to provide sufficient robustness against lossy compression attack and sharpening operation.

A methodical review of the literature shows that the SVM-based schemes give better performance than other learning methods. Specifically, classification problem based on SVM classifier provides better solutions than that of conventional neural networks, such as radial basis functions and MLPs. Tsai and Sun [46] presents an SVM-based color image watermarking approach in spatial domain, where watermark detection has been considered as a binary classification problem. Wang et al. [49] proposes an image watermarking technique to survive geometrical attack such as rotation, scaling, translation etc. Peng et al. [36] utilizes the special frequency band and property of image in multi-wavelet domain for watermarking. Though this scheme provides a quite good amount of robustness against several attacks, but fails to provide adequate robustness against scaling attack, JPEG compression, average filtering and mean filtering. Wang et al. [50] have also presented a robust image watermarking technique based on the SVM and Gaussian Hermite Moments (GHMs). Though, the scheme provides good robustness against different geometric attacks, but, fails to provide sufficient robustness against JPEG compression attack. Verma et al. [48] have proposed a digital image watermarking scheme based on LWT and SVM which is robust against noising attack, de-noising attack, JPEG compression attack etc. But, it fails to provide sufficient robustness against rotation and translation attack. Fazli et al. [11] have proposed a robust image watermarking scheme based on the combinations of DWT, DCT, and SVD domains. This paper proposes a new synchronization technique to recover geometrically attacked image via detection of desired image corners.

In recent decades, various robust image watermarking schemes have been developed. Initially, the techniques have been proposed in spatial domain as it is easy and convenient to implement. In contrast to spatial domain, watermarking based on transform domain provide better robustness. Different transform domain techniques based on the combination of DWT, DCT, SVD etc., have been developed. In these techniques, the coefficients are modified to embed a watermark bit in such a way that it has less visual effect. Though these techniques provide adequate imperceptibility, but fail to offer sufficient robustness against some of the attacks like de-synchronization attacks, JPEG attack with low Q factor etc. To improve robustness of the technique under distorted environment, various machine learning based watermark detection approaches have been proposed. The techniques are able to provide satisfactory robustness against noising attacks, de-noising attacks, image processing attacks, lossy compression attacks, but, itis not capable enough to resist different geometric attacks together. Robustness against geometric attacks can be achieved by either embedding the watermark in affine invariant domain or performing geometric distortion correction before watermark extraction. Watermark embedding in invariant domain to achieve robustness fails to provide adequate performance against cropping attack. Whereas, in geometric distortion correction, the attacked watermarked image is corrected before performing watermark extraction. Generally, geometric distortion correction is done using two approaches. One method is to store the geometric shape information of the watermarked image using various figure description operator such as Zernike moment, Radon transform, polar harmonic moment etc. During watermark extraction, the stored synchronization information is used to correct geometrically distorted image. The second approach for geometric distortion correction is based on machine learning in which the system is trained with the various distorted version of watermarked image. The problem with the existing machine learning based geometric distortion correction approach is computational time and complexity.

In this work, we have tried to design a system with better robustness keeping imperceptibility in a satisfactory level. This paper proposes a new robust image watermarking scheme which can effectively resist both common geometric attacks as well as signal processing attacks. The SVM based binary watermark detection and geometric distortion correction based scheme have been integrated to obtain improved performance sunder diverse attack conditions. Geometric distortion correction is performed using Radon transform and invariant centroid. This watermark embedding scheme is based on LWT and SVD. Horizontal high frequency HL sub-band is selected for watermark embedding as it provides optimum performance in terms of both transparency and robustness against different attacks. Watermark embedding in low frequency LL sub-band has a direct effect on the perceptual quality of the image. High frequency HH band have the edge and texture information of an image. Generally, HH sub band coefficients are removed during image compression. The alternate option is to choose HL and LH band. But, the human visual system is less sensitive in horizontal than vertical (Sing et al. 2012, [43]) sub-band. Hence, horizontal HL sub-band is chosen for binary watermark bit embedding. Singular values have been chosen for quantization as it is less sensitive to image modifications. When a small perturbation is added to an image, large variation of singular values does not occur. In this scheme, the watermark embedding is based on quantization of singular values of LWT transformed SVD decomposed coefficients and the watermark extraction is treated as a binary classification problem. LWT is used as an alternative to DWT in our work as it is computationally efficient in time and requires less memory. The motivation of using SVM is due to the good learning ability and generalization performance even when the watermarked image is vigorously distorted. The contributions of this work is as follows:

- Geometric distortion correction is incorporated with SVM based binary watermark detection technique. It has been proposed to achieve improved robustness against geometric attacks. Geometric distortion correction has been performed using invariant centroid and Radon transform which makes the system computationally more efficient than other robust watermarking method. This technique provides robustness against both the geometrical and non-geometrical attack.
- Energy compaction property of LWT, good stability of singular values and good learning capability of SVM together can resist more image distortions. The third level LWT sub-band is chosen in such a way so that it can get a better balance between imperceptibility and robustness. Singular values are less sensitive to image manipulation and have been modified adaptively depending on the image.
- The third level LWT coefficients and blocks are randomized using different keys (key 1 and key 2) and watermark bits are encrypted using key 3 to make the system more secure. Two keys (key 1 and key 2) are used for making it difficult for an intruder to find the

locations of watermark bits even though the intruder may have enough knowledge of watermark embedding and extraction procedure.

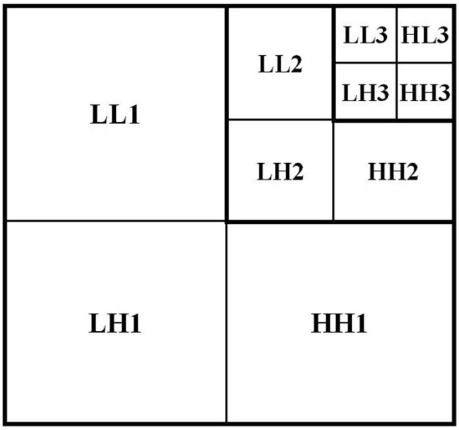
- The experimental analysis have been carried out on different set of database such as USC-SIPI image database, CVG-UGR image database, and standard database available at www.imageprocessingplace.com to check the efficiency of the algorithm for different types of images.
- A comparative analysis has been performed with different state of the art method. Different performance parameters like imperceptibility, robustness and capacity have been used to evaluate the systems.

Rest of the paper is arranged as follows: In section 2, methodology of the proposed watermarking algorithm has been discussed in detail. Section 2 also describes geometric distortion correction method to nullify the effect of de-synchronization attacks. In section 3, the performances of the algorithm and comparisons with different schemes have been explained in detail. Section 4 describes the conclusion and future scope of the paper.

2 Proposed watermarking algorithm

In this work, a new robust image watermarking scheme with good transparency and reasonable resistance toward a variety of image processing operations has been proposed. Firstly, the original image is decomposed using LWT up to the third level, and HL3 sub-band has been selected for watermark embedding purpose as shown in Fig. 1. Then HL3 sub-band coefficients are randomized using a secret seed(key 1), and consecutively non-overlapped coefficients are grouped to form blocks. Then, all the blocks are also shuffled randomly using another secret seed(key 2). SVD is performed on the 2 × 2 block and singular values are modified for embedding a binary watermark bit. The difference between the singular values is calculated and higher singular value is quantized based on the binary watermark bit. Then a threshold difference is maintained according to the binary bit. The thorough embedding process is illustrated in the watermark embedding section. During extraction, watermark bits are extracted based on SVM based binary classification. The blocks of HL3 sub-band coefficients of watermarked image are obtained in a similar way as in embedding process.

Fig. 1 LWT sub band



Then SVD is performed on every 2 × 2 block. Then, different features of the singular matrix are calculated using different standard statistical parameters such as Energy, mean, and variance. The training and testing data are prepared by the concatenating feature set along with corresponding singular values. The features of the singular matrix of the corresponding block where reference watermark is embedded along with reference watermark bits are used as input to train the SVM. Then the trained SVM is used for extracting the signature watermark. The extraction procedure is discussed in detail in watermark extraction section. To counter the de-synchronization attacks, geometric distortion correction is performed before watermark extraction. Geometric distortion correction using Radon transform and invariant centroid have been discussed in section 2.3.

2.1 Watermark embedding procedure

In this work, watermark W of length L_w consists of two components, the reference information RW of length L_r and the signature information SW of length L_s. The reference information bits contain some random binary bits and geometric shape description information. The one dimensional reference information is of length 512 bits, out of which first 448 bits are generated randomly and next 64 bits contain shape description information. This reference watermark(RW) bits act as key 3 which is used to encrypt the signature watermark(SW) bits. In this case, one dimensional vector of signature information bits (i.e. logo watermark image) is encrypted using ‘XOR’ operation with key 3.The reference watermark(RW) and signature

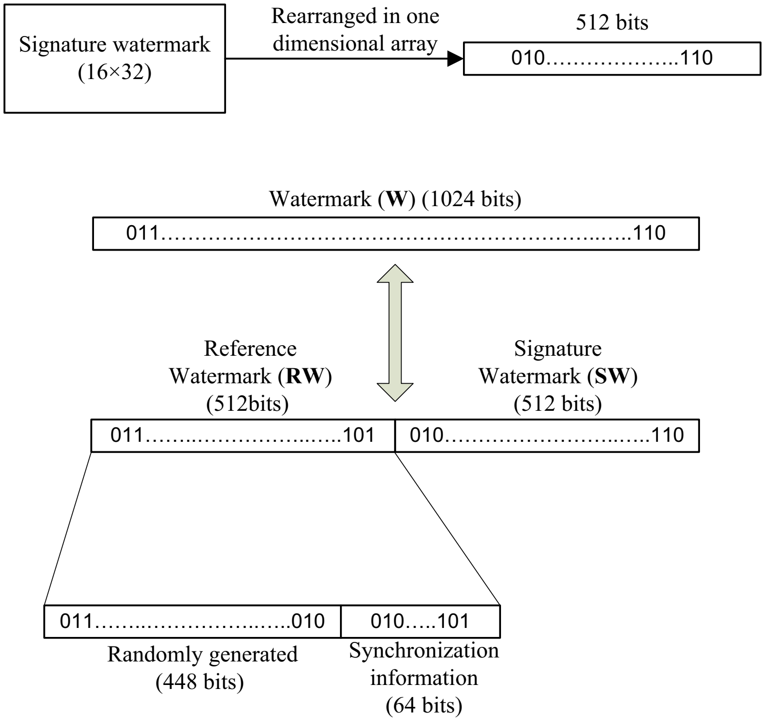

Signature watermark (16×32)
Rearranged in one dimensional array
512 bits
010………………..110
Watermark (W) (1024 bits)
011……………………………………………………..….110
Reference Watermark (RW) (512bits)
Signature Watermark (SW) (512 bits)
011……..……………….….101
010…………………….….….110
011……..………………..…..010
010…..101
Randomly generated (448 bits)
Synchronization information (64 bits)

Fig. 2 Watermark bit combination

watermark(SW) have been concatenated and represented as a single unit as: $W = RW + SW = W_1; \ldots.., W_{L_r}; W_{L_r+1}, \ldots.., W_{L_r+L_s} = W_1, \ldots.., W_{L_w}$. The watermark bit combination is shown in Fig. 2.

The RW is used to generate a training pattern, while, the SW is used to generate a testing pattern. The graphical representation for generating SVM training and testing pattern is shown in Fig. 3.

The mathematical formulation to embed watermark bits is shown in Table 1. For each watermark bit, the higher singular values of the corresponding block in HL3 sub-band is quantized as shown in the Table 1.

In Table 1, T stands for embedding threshold used in quantizing singular value and $d_{i\max}$ is the difference between two singular values λ_1 and λ_2 of the corresponding i^{th} block. λ_1 is the dominant singular value. The average difference between singular valuesγ of all L_w singular matrices is expressed as:

$$\gamma = \left[\frac{\sum_{i=1}^{L_W} d_{i\max}}{L_W} \right] \tag{1}$$

Here, L_w is the total number of blocks or singular matrices in HL3 sub-band where the watermark bits are embedded. The flowchart of the proposed embedding procedure is shown in Fig. 4.

The embedding procedure for the binary watermark bits is as follows:

Step 1. LWT is performed three times on the original host image to obtain HL3 sub-band.

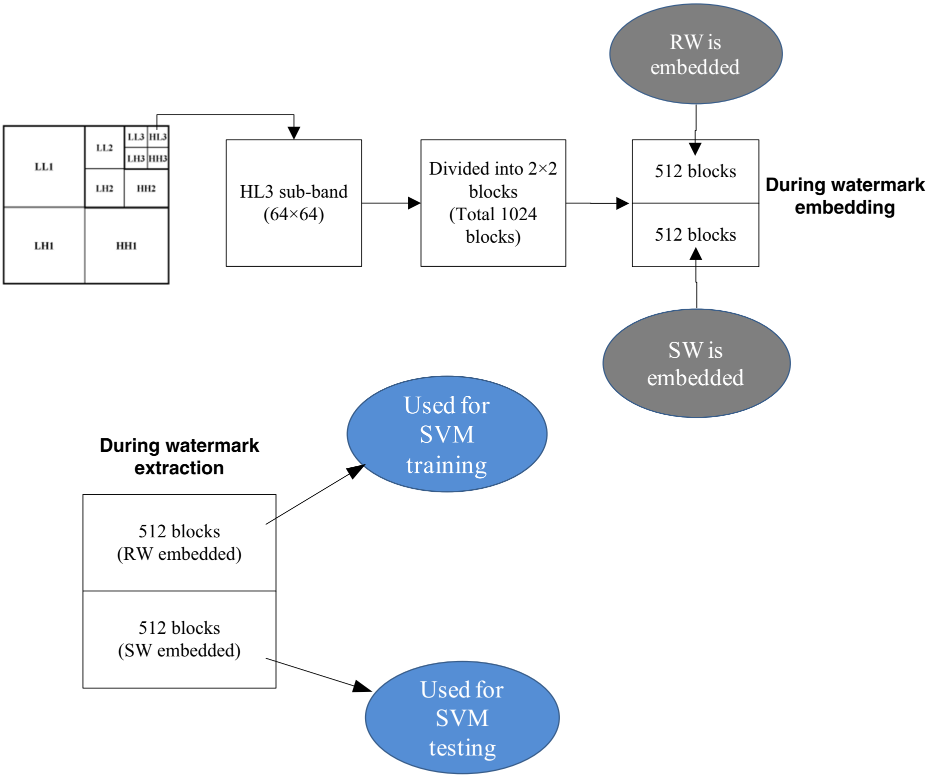


Fig. 3 Block diagram representation for generating SVM training and testing patterns

Table 1 Modification of singular values

If the watermark bit is 1	If the watermark bit is 0
$\lambda_1 = \begin{cases} \lambda_1 + T, \text{if } d_{i\max} < \max(\gamma, T) \\ \lambda_1, \quad \text{otherwise} \end{cases}$	$\lambda_1 = \lambda_2$

Step 2. HL3 sub-band coefficients are then randomized using secret seed key1.

Step 3. HL3 sub-band coefficients are arranged in non-overlapping 2 × 2 blocks, and all these blocks are scrambled using secret seed key2.

Step 4. Then, SVD is performed on every block and the singular matrix is considered for quantization.

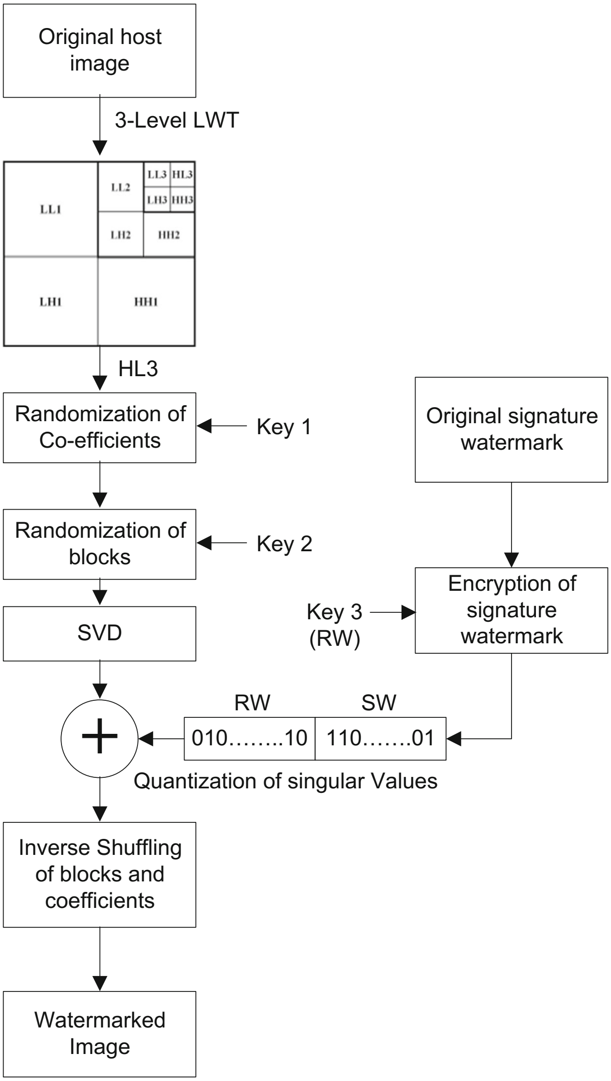

Original host image
3-Level LWT
LL1
LL2
LL3
HL3
LH3
HH3
LH2
HH2
LH1
HH1
HL3
Randomization of Co-efficients
Key 1
Original signature watermark
Randomization of blocks
Key 2
Encryption of signature watermark
SVD
Key 3 (RW)
RW
SW
010……..10
110…….01
Quantization of singular Values
Inverse Shuffling of blocks and coefficients
Watermarked Image

Fig. 4 Watermark embedding procedure

Step 5. The average difference between singular values γ is calculated using eq. (1).
Step 6. A one dimensional vector of binary watermark W of length L_w is created by concatenating the reference watermark RW and signature watermark SW.
Step 7. For all L_w bits of watermark do following:

i. In each block, the singular values λ_1 and λ_2 are considered for modification.
ii. Depending on the embedded watermark bit i.e. either0 or 1, the dominant significant singular value λ_1 is modified according to Table 1.

Step 8. Then, the updated non-overlapping blocks are reconstructed with by recomposing using the left singular matrix, right singular matrix and modified singular matrix.
Step 9. All the blocks and updated coefficients of HL3 sub-band are inversely shuffled using the same keys as mentioned in ***Step 3*** and ***Step 2***.
Step 10. Finally, watermarked image is obtained by performing inverse LWT operation.

2.2 Watermark extraction procedure

Watermark extraction problem has been considered as a binary classification problem, and the SVM classifier is used for this purpose. The reasons of using SVMs are as follows:

1. From watermark embedding procedure described in the watermark embedding section, we can see that embedded watermark bit (1 or 0) corresponds to some particular pattern of singular values. It is observed that a nonlinear function relationship exists between the watermark bits $W_i \in (0, 1)$ and the two singular values present in i^{th} block, i.e., $W_i = f(\lambda_{1i}, \lambda_{2i})$. As SVMs has powerful nonlinear mapping ability, it can be used to learn the nonlinear relationship.
2. It is well known that watermarked image may suffer from different signal processing operations or attacks, such as, JPEG lossy compression, additive noise, filtering, etc. From transform domain perspective, this results in the change of LWT coefficients correspondingly singular values. The changes can be viewed as the case that these coefficients are polluted by different type noises. So, it is required that designed watermark detector should have high ability to resist the noises. In Machine learning viewpoint, the detection of a binary watermark can be realized as an ability of generalization. In proposed scheme, SVM has been used as a watermark detector because the SVM has good generalization ability, and it can help to achieve better robustness of the watermarking system.

The proposed scheme is oblivious because neither the original image nor the watermark (SW) is required in case of watermark detection. The RW or SW are set of binary patterns. During this training phase, input data set is classified into set of decision. It has been decided on the basis of prediction error. If the prediction is greater than some predefined error, then it is in class '0' i.e. 0 bit was embedded and class '1' where bit 1 was embedded.

Firstly, HL3 sub-band coefficient blocks of watermarked image are extracted where the reference information is embedded. Then SVD is performed on every block. Subsequently different statistical parameters such as: mean (p1), variance (p2), standard deviation (p3), median (p4), covariance (p5), moment (5th order) (p6), quantile (p7), difference between the singular values (p8), difference between the square of singular values (p9), and Energy (p10) of singular matrix of all the corresponding blocks are evaluated. The set of parameters (p1; p2;. ..; p10) is called as features vector and represented as (f_1;. ..; f_{10}) i.e. feature vector set. It is given as input feature to train the SVM machine. Total number of HL3 sub-band coefficient block of size 2 × 2 is 1024, in which, 512 blocks are utilized to generate the training pattern and the next 512 blocks are used to prepare the testing pattern. The testing pattern provides signature watermark. So, the dimension of feature vector set {p(k)} is 512 × 10. A set of training pattern is created using the feature set along with the singular values of corresponding block. Likewise, the set of testing pattern is also generated. The SVM is used to classify a set of training patterns. At last, the trained SVM is used to classify a set of testing patterns. Using the results provided by the trained SVM, the signature watermark (SW) can be detected. The flowchart of the proposed extraction scheme is shown in Fig. 5. The steps for binary watermark extraction is described below.

Step 1. LWT is performed on the watermarked image in the similar way as in embedding process to obtain HL3 sub-band coefficients.

Step 2. The coefficients and corresponding blocks of HL3 sub-band are randomized using secret keys (key 1 and key 2).

Step 3. Perform SVD on every 2 × 2 block and the singular matrix is considered for feature extraction.

Step 4. Generate features set $\{p_i(k)|k = 1, 2, \ldots 10\}$ of singular matrices where reference information (RW) are embedded.

Step 5. SVM training

5.1. A training pattern ψ is constructed by utilizing the feature sets along with the singular values of corresponding blocks where the reference information $(W_1, W_2, \ldots.. W_{L_r})$ has been embedded.

$$\begin{aligned}\psi &= \left\{(x_i, y_i)\in R^N \times R | i = 1, 2, \ldots. L_r\right\} \\ &= \{(f_i(1), f_i(2), \ldots. f_i(10), \lambda_{1i}, \lambda_{2i}), w_i | i = 1, 2, \ldots. L_r\}\end{aligned} \tag{2}$$

Where $f_i(1)$,$f_i(2)$, . …$f_i(10)$ are the features, λ_1 and λ_2 are the singular values of the corresponding ith block, w_i is the desired output, $i = 1 , 2 , . \ldots L_r$.

5.2. The "RBF" kernel of SVMs is described as follows

$$K(x_i, x) = e^{\left(-\|x_i - x\|^2/\sigma^2\right)} \tag{3}$$

here, σ is the width parameter of "RBF" kernel.

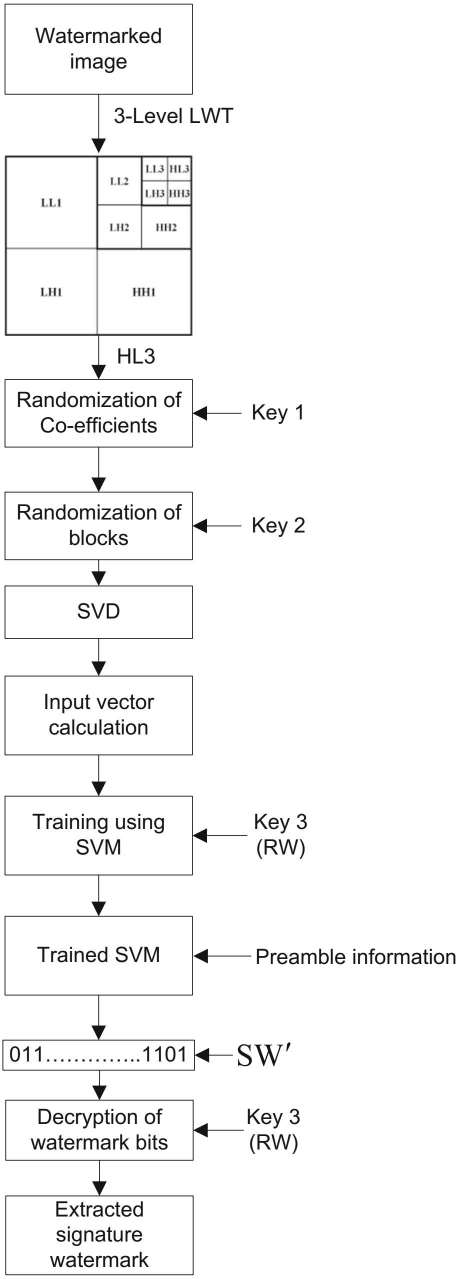
5.3. The optimal model can be defined as

$$Maximize \ \sum_{i=1}^{L_r}\alpha_i - \frac{1}{2}\sum_{i=1}^{L_r}\sum_{j=1}^{L_r}\alpha_i\alpha_j y_i y_j K\left(x_i, x_j\right) \tag{4}$$

subject to $\sum_{i=1}^{L_r}\alpha_i\alpha_j = 0, \quad 0 \le \alpha_i \le C, \ i = 1, 2, \ldots L_r.$

Where C is the penalty parameter, and $\alpha_i(i = 1, 2, \ldots. L_r)$ are the training parameter. If the optimal solution is $\alpha = (\alpha_1, \alpha_2, \ldots.., \alpha_{L_r})$, the decision function y can be expressed as

Fig. 5 Watermark extraction procedure



$$y = f(x) = sign\left(\sum_{i=1}^{L_r} \alpha_i y_i K(x_i, x) + b\right) \quad (5)$$

where $b \in R$ is a bias.

Step 6. A set of testing pattern is generated by calculating feature vectors form the blocks in which SW was embedded in a way similar to training process. To extract the signature information SW', construct the testing pattern ψ' for well trained SVM. $\psi' = \left\{x'_u = \left(f_u{}'(1), f_u{}'(2), \dots . f_u{}'(10), \lambda'_{1u}, \lambda'_{2u}\right)\right\}$. Then, by using well trained SVM in Eq. (5), we can obtain their corresponding outputs $\left\{y'_u | u = 1, \dots \dots, L_s\right\}$ i.e.,

$$\begin{cases} y'_u = f\left(x'_u\right), u = 1, \dots \dots, L_s \\ x'_u = \left(f_u{}'(1), f_u{}'(2), \dots . f_u{}'(10), \lambda'_{1u}, \lambda'_{2u}\right) \in \psi' \end{cases} \tag{6}$$

Thus, the signature information bits (SW') can be obtained by

$$w'_u = \begin{cases} 1, & if\ y'_u = 1 \\ 0, if\ y'_u = -1 \end{cases} \tag{7}$$

Step 7. The detected signature information bits has been stored in one dimensional vector SW' of length N_s, which are decrypted using the same seed key3 as used in the embedding process.

Step 8. The extracted SW' is reshaped same as the size of original logo watermark image.

It is to be noted that the using of “RBF kernel” function in SVM classifier gives the better result than other kernel function in comparison to “Linear kernel” and “Polynomial kernel” under different attacks condition. So, all the experiments have been done using RBF kernel for the rest of the paper.

2.3 Modified algorithm for de-synchronization attacks

In case of de-synchronization attacks, the algorithm fails to provide robustness. This is because de-synchronization attacks like rotation, scaling, and translation induces synchronization error between encoder and decoder. However, the algorithm provides satisfactory robustness against geometric attack if the geometric distortion correction is performed on the image before watermark extraction.

The reference watermark (RW) of length L_r contains synchronization bits of length S_b and randomly generated binary bits of length R_b. Out of 512 reference bits, first 448 bits are generated randomly and the last 64 bits are used as synchronization bits. The synchronization bits consists of three parts, in which, first 24 bits are used for storing invariant centroid of the watermarked image, and next 24 bits are for storing the size of the image that can be used for rectifying the scaled distorted image. Last 16 bits of synchronization bits are used for storing phase information of radon transform of the watermarked image to correct the effect of rotation attack.

Now, the scaling factor, translation factor as well as the angle of rotation by which the image shall be corrected will be estimated accordingly. Then we can rotate the corrupted watermarked image back to its original orientation or rescale it back to its original size before extracting the watermark. Using that the synchronizations of watermark embedding and the extracting process will be recovered.

We have used Radon transform [54] for detecting degree of rotation attack. The phase information is used for correcting a distorted image attacked by rotation. The radon transform of the original watermarked image is calculated and the phase information is stored as synchronization bits of the reference watermark. The phase information θ which is calculated in radian is converted into decimal form and then stored in the reference watermark. The reference information for the original watermarked image is stored during watermark embedding. Subsequently, when an attacked rotated image is received we calculate the phase information of the rotated image $\theta^{'}$ in radian. Then we calculate the amount of rotation attack by deducting the phase information of attacked image θ' from phase information θ of the original image. After finding the amount of rotation, we re-rotate the image by the calculated degree.

For translation attack, we have used invariant centroid method proposed by Bum-Soo Kim et al. [21]. In the proposed algorithm, we have calculated invariant centroid of the original watermarked image. Then this information is stored in binary form in the synchronization bits of reference watermark. Total 24 binary bits are used for storing the invariant centroid information. Before watermark extraction, the invariant centroid of the attacked image is calculated and the attacked image is geometrically corrected using the rule used mentioned in [21].

The size of the host image have been stored as synchronization bits in the reference watermark. So, later on before watermark extraction, this side information can be used for correcting the scaled distorted image.

3 Results and discussion

The performance analysis of the proposed algorithm and its comparative result with some of the recent watermarking schemes are presented in this section. The algorithm is tested on a large image database consists of 200 grayimages. The image database includes both the standard benchmark images along with real life images. These images are collected from www.imageprocessingplace.com, USC-SIPI image database, and CVG-UGR image database. Some of the test images are shown in Fig. 6. The binary watermarks are collected from the MPEG7_CE_shape descriptor database. The detailed analysis and experimentation are performed in windows 7 based Matlab(R2013a) platform. The hardware used is Dell computer with RAM 16 GB and Intel core i5 processor. All the experiments have been performed keeping embedding threshold at $T = 35$ which gives optimum performance in terms of imperceptibility and robustness.

Imperceptibility has been measured in terms of peak signal to noise ratio(PSNR) which is measured between the original host image and watermarked image. Robustness between original watermark and extracted watermark is measured in terms of mean square error (MSE), normalized correlation coefficient(NC), structural similarity index measure(SSIM) and bit error rate (BER).

Mean square error between any two images I and $I^{'}$ is defined as follows

$$MSE = \frac{\sum_{i=1}^{m_1} \sum_{i=1}^{m_2} \left(I(i,j) - I^{'}(i,j)\right)^2}{m_1 \times m_2} \tag{8}$$

Where $I(i,j)$ and $I^{'}(i,j)$ are the gray level intensity value at the location (i,j) of the images and the images are of size $(m_1 \times m_2)$. For imperceptibility, MSE is measured between the

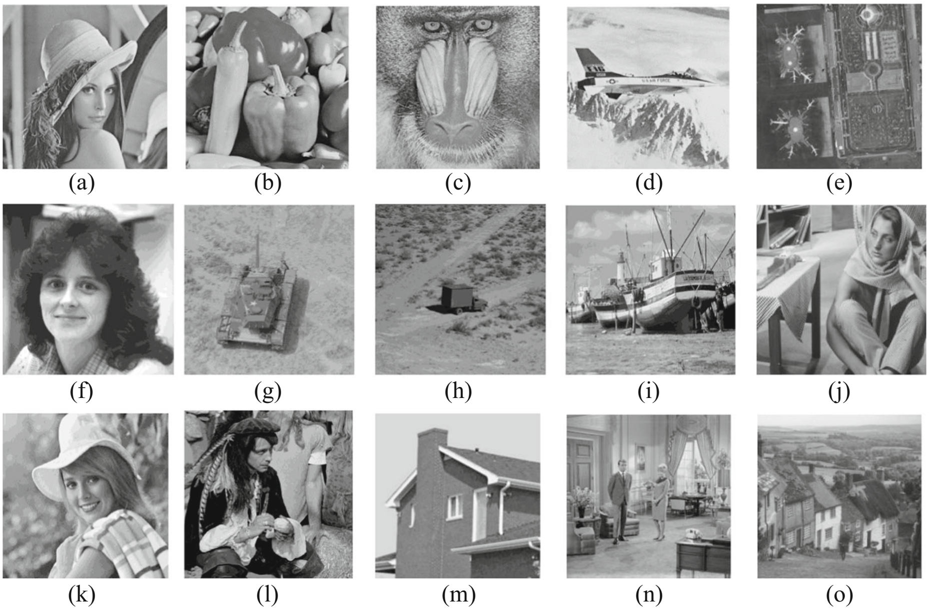


Fig. 6 Standard benchmark images (a) Lena, (b) Peppers, (c) Mandril, (d) Jetplane, (e) Airport, (f)woman, (g) Truck, (h)Tank, (i) Boat, (j)Barbara (k) Elaine, (l) Man, (m) House, (n) Livingroom, and (o) Goldhil

original host image and watermarked image whereas for robustness it is measured between the original watermark and extracted watermark.

The PSNR is defined as

$$PSNR = 10\log_{10}\frac{255^2}{MSE} \tag{9}$$

For original image x and watermarked image y, the SSIM index as [38] is defined as in eq. (10),

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{10}$$

with μ_x the average of x; μ_y the average of y; σ_x^2 the variance of x; σ_y^2 the variance of y; σ_{xy} the covariance of x and y; $c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$ two variables two stabilize the divisions with weak denominator; $L = (2^{bitsperpixel} - 1)$ is the dynamic range of the pixel-values, For gray image it is 255 and for binary image it is 1. $k_2 = 0.01$ $k_1 = 0.01$ and $k_2 = 0.03$ by default.

The NC and BER can be computed as follows:

$$NC = \frac{\sum_i\sum_j W_{ij}W'_{ij}}{h \times w} \tag{11}$$

where W_{ij} and W'_{ij} are the values located at (i,j)th location of the original and extracted watermark and set to 1 if the watermark bit is1otherwise it is set to −1; and h, w are height and width of the watermark, respectively.

$$BER = \frac{B}{h \times w} \tag{12}$$

where, B is the number of incorrectly detected bits, $h \times w$ is the size of the watermark image.

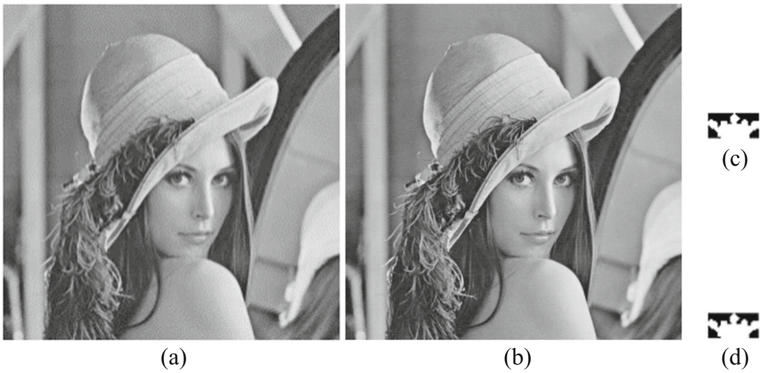


Fig. 7 (a) Original image "Lena" of size (512 × 512), (b) Watermarked image with PSNR = 43.670 dB, (c) Original watermark of size (16 × 32), and (d) extracted watermark

3.1 Imperceptibility

The performance of the proposed scheme in terms of imperceptibility has been tested on different image database. The imperceptibility is measured in PSNR(dB) between the host image and the watermarked image. The watermarked Lena image with PSNR = 43.670 dB, NC = 1, and BER = 0 and extracted watermark under no attack condition are shown in Fig. 7. The performance of the algorithm has been tested on 200 images and the average PSNR is found to be 42.27 dB. It is observed that the embedding threshold T balances the two performance parameter imperceptibility and robustness. With higher value of T, robustness increases and imperceptibility decreases, and vice-versa. It is found that the embedding threshold, T = 35 gives better balance between imperceptibility and robustness. For this value of T, the PSNR for 15 different standard images is graphically represented in Fig. 8.

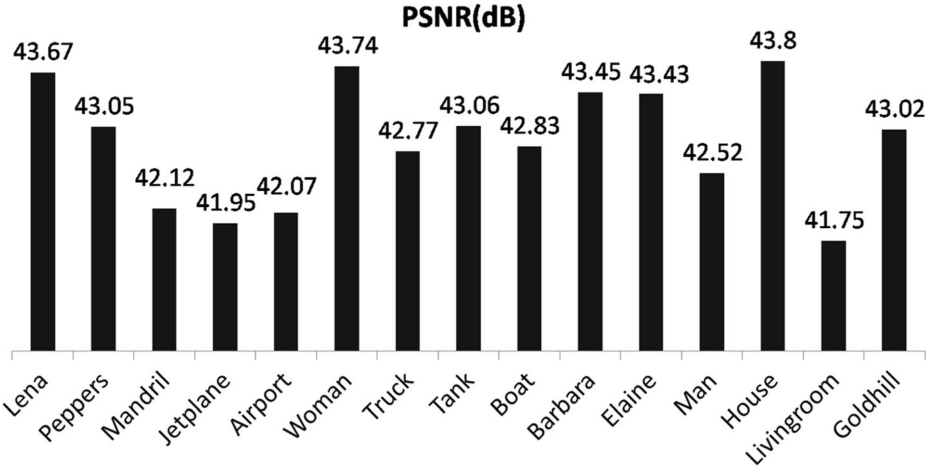


Fig. 8 The imperceptibility for different images

Table 2 NC values of extracted watermark for different attacks over fifteen images

Images	JPEG 20	JPEG 30	JPEG 40	JPEG 50	HE	IS	SPN (0.01)	SN (0.01)
Lena	0.7395	0.9454	0.9764	0.9882	0.9803	1.0000	0.7319	0.7389
Peppers	0.6587	0.9457	0.9494	0.9684	0.9646	0.9606	0.7132	0.7749
Mandril	0.6414	0.8856	0.9098	0.9449	0.9093	0.9329	0.8266	0.7793
Jetplane	0.5548	0.8673	0.9644	0.9842	0.7409	0.9570	0.7111	0.5236
Airport	0.7223	0.8652	0.9212	0.9606	0.8748	0.9370	0.7711	0.8972
Woman	0.6726	0.9124	0.9646	1.0000	0.9565	0.9921	0.7272	0.7077
Truck	0.6438	0.8854	0.9187	0.9568	0.8823	0.9921	0.8300	0.8861
Tank	0.5982	0.9138	0.9645	0.9842	0.8866	1.0000	0.7796	0.7498
Boat	0.5994	0.8978	0.9067	0.9842	0.8288	0.9258	0.8201	0.7865
Barbara	0.5780	0.9016	0.9492	0.9921	0.9921	0.9725	0.7269	0.7739
Elaine	0.7318	0.9803	0.9568	0.9763	0.9921	0.9921	0.7434	0.7683
Man	0.6366	0.8557	0.9104	0.9687	0.9684	0.8190	0.7251	0.8422
House	0.6712	0.8931	0.9066	0.9842	0.8102	0.9607	0.6230	0.7274
Livingroom	0.6618	0.7983	0.8905	0.9492	0.8285	0.9016	0.7547	0.8280
Goldhill	0.7395	0.9009	0.9567	0.9686	0.9568	1.0000	0.7953	0.7752

3.2 Robustness

The effect of various attacks on the watermarking scheme has been observed and analyzed. The attacks include both non-geometrical and geometrical attack like salt and pepper noise (SPN), speckle noise (SN), Gaussian noise (GN), Gamma correction (GC), average filtering (AF), median filtering (MF), Gaussian filtering (GF), histogram equalization (HE), image sharpening (IS), JPEG compression with given quality factor (JPEG(QF)), cropping (CR), rotation (RT), scaling (SCL), and translation (TR). The robustness test is performed on different types of images. The result is shown for fifteen images in Tables 2, 3 and Table 5. From the results, it can be seen that the scheme provides satisfactory performance against lossy compression attack, image processing attacks. The scheme provides adequate robustness against de-synchronization attacks provided geometric distortion correction is performed before watermark extraction. The scheme provides slightly degraded performance against noising attack and de-noising

Table 3 NC values of extracted watermark for different attacks over fifteen images

Images	AF 3X3	MF 3X3	GF 3X3	CR 10%	CR 20%	CR 50%	SCL (0.5)	SCL (0.75)
Lena	0.6001	0.5490	0.9882	0.9176	0.9372	0.7026	0.6478	0.9882
Peppers	0.5997	0.5636	0.9421	0.9071	0.9413	0.7102	0.6235	0.9289
Mandril	0.4105	0.3431	0.9724	0.8310	0.7563	0.5051	0.4690	0.8459
Jetplane	0.4023	0.4177	0.9171	0.8426	0.9045	0.6459	0.4803	0.9337
Airport	0.4186	0.4465	0.9684	0.8363	0.8187	0.6400	0.4326	0.9019
Woman	0.7551	0.6832	0.9565	0.9057	0.9275	0.7654	0.7844	0.9921
Truck	0.3951	0.3938	0.9921	0.8683	0.8332	0.6492	0.4679	0.9605
Tank	0.4406	0.4360	0.9842	0.8933	0.9145	0.7443	0.5181	0.9882
Boat	0.3755	0.3529	0.9723	0.9170	0.9166	0.7508	0.4885	0.9452
Barbara	0.5339	0.4586	0.9725	0.8937	0.8925	0.6439	0.5482	0.9688
Elaine	0.6116	0.4990	0.9687	0.9170	0.9568	0.7271	0.6252	0.9882
Man	0.3658	0.3797	0.9565	0.8861	0.9229	0.7122	0.4023	0.8935
House	0.5729	0.5453	0.9527	0.9726	0.9649	0.7060	0.6716	0.9725
Livingroom	0.3511	0.3674	0.9566	0.8660	0.8924	0.6859	0.3569	0.8863
Goldhill	0.4432	0.4162	0.9253	0.9334	0.9192	0.6180	0.4690	0.9684

Table 4 Results of geometric distortion correction for four different images in case of rotation and translation attack

Images	Distortion parameter	Rotation					Translation		
Lena	Actual	5°	15°	30°	45°	90°	(2, 15)	(10, 10)	(20,20)
	Corrected	5.00	15.00	30.0012	44.9976	90.00	(2.00, 15.01)	(10.01, 10.02)	(20.03, 20.02)
Peppers	Actual	5°	15°	30°	45°	90°	(2, 15)	(10, 10)	(20,20)
	Corrected	5.00	15.00	30.0024	44.9986	90.00	(2.00, 15.03)	(10.02, 10.02)	(20.02, 20.02)
Mandril	Actual	5°	15°	30°	45°	90°	(2, 15)	(10, 10)	(20,20)
	Corrected	5.00	15.00	30.0022	44.9982	90.00	(2.00, 15.02)	(10.02, 10.02)	(20.04, 20.02)
Barbara	Actual	5°	15°	30°	45°	90°	(2, 15)	(10, 10)	(20,20)
	Corrected	5.00	15.00	30.0016	44.9980	90.00	(2.00, 15.02)	(10.02, 10.01)	(20.03, 20.04)

attack. As the watermark is embedded in mid frequency sub-band, so the scheme is not able to provide superior robustness against low pass filtering for instance average filtering and median filtering. The robustness test is performed on 200 images and the average performances (μ) on all 200 images in terms NC, BER, and SSIM are shown in Table 6. The standard deviation (σ) and variance (σ^2) performance of robustness on all 200 images are also shown in the Table 6. The extracted watermark *SW'* for Lena watermarked image for different attacks is shown in Table 6.

3.3 Robustness against de-synchronization attacks

The modified algorithm for de-synchronization attacks provides adequate robustness against rotation, scaling, translation attacks. The actual distortion parameter and the corrected distortion parameter for rotation and translation attack are shown in Table 4. For correcting a watermarked image attacked by rotation, the phase information of the image is calculated using Radon transform. Subsequently, the amount of rotation distortion is determined by comparing with the phase information of the original watermarked image. Similarly, Invariant

Table 5 NC values of extracted watermark for different rotation and translation attacks over fifteen images

Images	RT 5°	RT 15°	RT 30°	RT 45°	RT 90°	TR (2, 15)	TR (10, 10)	TR (20, 20)	TR (30,30)
Lena	0.9526	0.8775	0.8160	0.7618	1.0000	0.9961	0.9882	0.9607	0.8961
Peppers	0.8973	0.8458	0.7786	0.7959	1.0000	0.9609	0.9649	0.9108	0.8266
Mandril	0.9334	0.8035	0.7409	0.7826	1.0000	0.9765	0.9803	0.9349	0.8616
Jetplane	0.9131	0.8062	0.7071	0.7709	1.0000	0.9882	0.9921	0.9303	0.8260
Airport	0.9251	0.8701	0.7461	0.7468	1.0000	0.9882	0.9843	0.9494	0.9349
Woman	0.8973	0.8736	0.7904	0.8610	1.0000	0.9765	0.9842	0.9108	0.8895
Truck	0.9328	0.8699	0.8273	0.7988	1.0000	0.9882	0.9803	0.9303	0.8660
Tank	0.9447	0.8815	0.7723	0.8731	1.0000	0.9805	0.9921	0.9726	0.8988
Boat	0.9211	0.8617	0.7559	0.7112	1.0000	0.9805	0.9609	0.9245	0.8737
Barbara	0.9172	0.7477	0.6470	0.6485	1.0000	0.9725	0.9726	0.9494	0.8302
Elaine	0.9409	0.8933	0.8264	0.8237	1.0000	0.9921	0.9647	0.9725	0.8696
Man	0.9131	0.7786	0.7525	0.6566	0.9961	0.9842	0.9492	0.8943	0.8678
House	0.8858	0.8625	0.7943	0.7084	1.0000	0.9423	0.9690	0.9091	0.8326
Livingroom	0.9092	0.8262	0.7388	0.7304	1.0000	0.9728	0.9805	0.9293	0.8309
Goldhill	0.9408	0.9016	0.8096	0.8446	1.0000	0.9766	0.9763	0.9646	0.9296

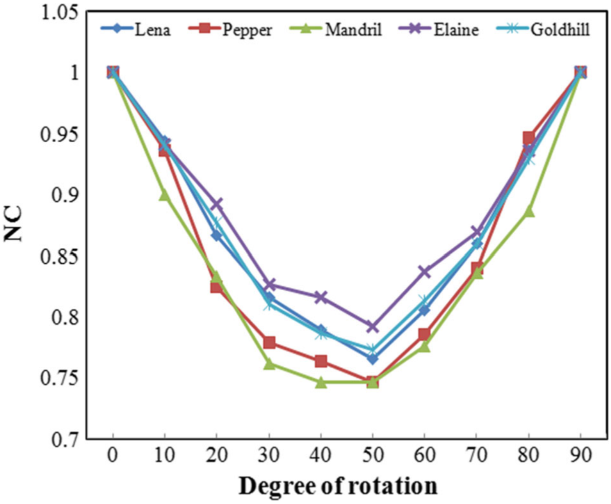


Fig. 9 Robustness against rotation attack

centroid of the attacked translated image is calculated and the amount of translation effect along X-axis and Y-axis is determined. The size of watermarked image can be determined from the synchronization bits stored in the reference watermark. Then accordingly, the attacked scaled image is resized.

The performance against de-synchronization attack is observed after geometric distortion correction. The robustness against rotation and translation attacks is shown in Table 5 in terms of normalized correlation. The robustness against rotation attack have been observed for different degree of rotation ranging from 0° to 90°. The performance against rotation attack is shown for 5 different standard images in Fig. 9. From the results shown in fig. 9, it is seen that the performance decreases when

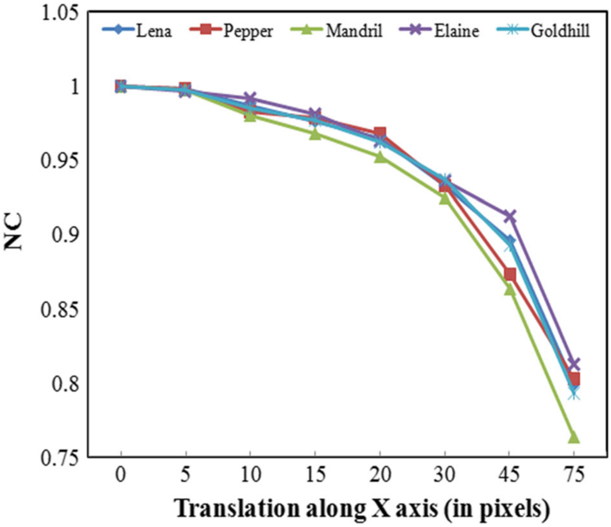


Fig. 10 Robustness against Translation attack

Table 6 Average Robustness performance (over 200 images) against different attacks

Attacks	NC			BER			SSIM			SW'
	μ	σ	σ^2	μ	σ	σ^2	μ	σ	σ^2	
RT (5°)	0.9272	0.0246	0.0006	0.0361	0.0122	0.00014	0.8170	0.0777	0.0060	
RT (15°)	0.8648	0.0517	0.0027	0.0672	0.0259	0.00067	0.6997	0.0854	0.0073	
RT (30°)	0.7997	0.0687	0.0047	0.1016	0.0368	0.0014	0.5865	0.0989	0.0098	
RT (45°)	0.8099	0.0837	0.0070	0.0982	0.0469	0.0022	0.5823	0.1021	0.0104	
TR (0, 10)	0.9844	0.0132	0.0002	0.0077	0.0066	0.00004	0.9396	0.0435	0.0019	
TR (10, 0)	0.9814	0.0175	0.0003	0.0093	0.0088	0.00017	0.9309	0.0553	0.0031	
TR (2, 15)	0.9730	0.0274	0.0008	0.0135	0.0137	0.00018	0.8918	0.0761	0.0058	
TR (10, 10)	0.9691	0.0249	0.0006	0.0154	0.0125	0.00015	0.8795	0.0758	0.0057	
SCL (0.5)	0.5508	0.1334	0.0178	0.2291	0.0780	0.0061	0.3705	0.1443	0.0208	
SCL (0.75)	0.9426	0.0704	0.0050	0.0285	0.0349	0.0012	0.8894	0.1431	0.0205	
CR 10%	0.8946	0.0366	0.0013	0.0524	0.0181	0.0003	0.7507	0.0929	0.0086	
CR 20%	0.9017	0.0503	0.0025	0.0502	0.0261	0.0007	0.7051	0.0971	0.0094	
CR 50%	0.4788	0.2914	0.0849	0.2821	0.1644	0.0270	0.3026	0.1873	0.0351	
AF 3X3	0.5043	0.1351	0.0183	0.2643	0.0905	0.0082	0.3263	0.1565	0.0245	
MF3X3	0.4819	0.1160	0.0134	0.2794	0.0840	0.0071	0.2926	0.1530	0.0234	
GF 3X3	0.9588	0.0421	0.0018	0.0205	0.0209	0.0004	0.8925	0.1026	0.0105	
SPN (0.01)	0.8081	0.0522	0.0027	0.0955	0.0262	0.0007	0.6157	0.0862	0.0074	
SN(0.01)	0.8577	0.0835	0.0070	0.0708	0.0419	0.0018	0.6857	0.1268	0.0161	
JPEG 30	0.8902	0.1538	0.0237	0.0577	0.0892	0.0080	0.7454	0.1662	0.0276	
JPEG 40	0.9591	0.0298	0.0009	0.0203	0.0148	0.00022	0.8839	0.0807	0.0065	
JPEG 50	0.9740	0.0220	0.0005	0.0129	0.0110	0.00012	0.9155	0.0727	0.0053	
IS	0.9906	0.0242	0.0006	0.0047	0.0120	0.00014	0.9745	0.0562	0.0032	
HE	0.9152	0.0687	0.0047	0.0425	0.0344	0.0012	0.7711	0.1306	0.0171	

degree of rotation approaches 45° and again it increases till 90°. This is due to the fact that the rotation attack leads to a loss of information and loss is maximum for 45° rotation. In our analysis, rotation of the watermarked image is performed keeping the image size constant. The performance against translation attack is also observed

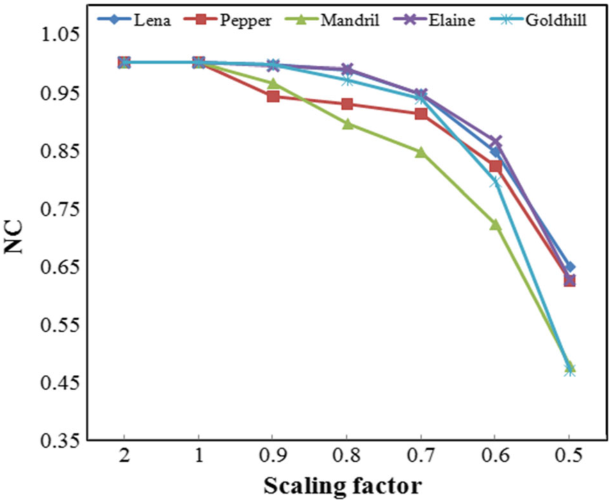


Fig. 11 Robustness against scaling attack

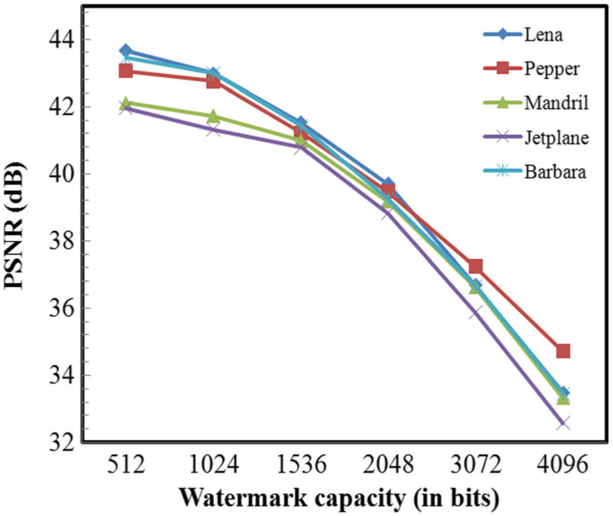


Fig. 12 The variation of imperceptibility with capacity

for 5 different standard images for varying pixel translation ranging from 0 to 75 pixels and is demonstrated in Fig. 10. For representative result, the robustness against translation along X axis is shown in Fig. 10. It has been observed that the algorithm provides satisfactory performance when the amount of translation is less than or equal to 50 pixels. From Tables 5 and 6, it is seen that the algorithm provides desired performance against rotation and translation attacks.

The robustness against scaling attack for two different scaling factors (0.5 and 0.75) over 15 standard images is illustrated in Table 3. The variation in robustness for different scaling factors is shown in Fig. 11. The performance decreases for low scaling factor. The algorithm provides adequate performance against scaling attack for scaling factor greater than or equal to 0.6.

3.4 Capacity analysis

In the proposed work, one of the 3-level LWT sub band has been used for watermark embedding purpose. The process can embed a total of 1024 bits. Out of which, 512 bits are used for signature watermark purpose. The size of the signature watermark (SW) that has been used in rest of the analysis is 16 × 32 i.e. 512 bits. The capacity of the watermarking system can be increased by utilizing more number of 3-level LWT sub bands. In this analysis, the parameters such as block size, size of cover image used, the ratio of training and testing bits used have been kept fixed.

Table 7 The variation of average imperceptibility (over 200 images) for different watermark capacity

Watermark capacity (in bits)		512	1024	1536	2048	3072	4096
Imperceptibility	μ	42.27	41.85	40.98	39.16	36.52	33.06
	σ	1.3234	1.6254	1.8392	2.1052	2.8362	3.8562

Table 8 Summary of different comparative methods

Methods	[47]	[19]	[32]	[42]	[48]	[52]	[16]	Proposed
Domain used	LWT	LWT-SVD	LWT-QR	DWT-DCT & SVD	LWT	UDWT	DWT	LWT-SVD
Embedding sub-band	LL	HH	LL	LH, HL	LL	LL	LL	HL
Extraction algorithm category	Blind	Semi-blind	Blind	Blind	Blind	Blind	Semi-blind	Blind
Size of host image	512 × 512	512 × 512	512 × 512	1024 × 1024	512 × 512	512 × 512	512 × 512	512 × 512
Watermark size	16 × 32	26 × 26	32 × 32	128 × 128	16 × 32	64 × 64	16 × 16	16 × 32
Imperceptibility on Lena image (in dB)	41.40	41.44	45.92	52.34	41.51	40.18	43.45	43.67
Geometric Distortion correction used	No	No	No	No	No	Yes	No	Yes
Robustness against de-synchronization attacks	Poor	Poor	Scaling attack only	Poor	Moderate	Good	Moderate	Good

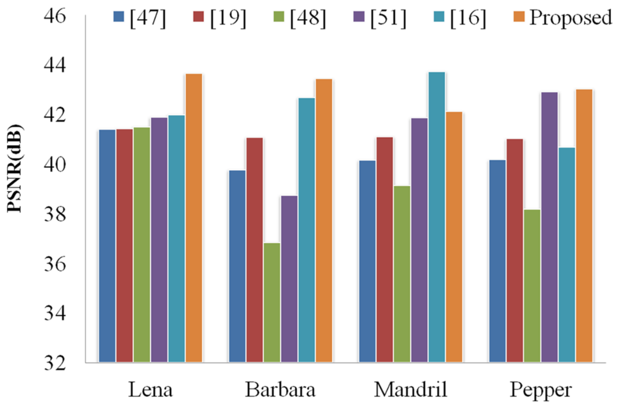


Fig. 13 Comparison of imperceptibility in terms of PSNR

The variation of imperceptibility has been observed for signature watermark capacity varying form 512 bits to 4096 bits. For a embedding a signature watermark of capacity 4096 bits, 8 number of LWT sub bands have been used. The variation of imperceptibility with capacity is shown for 5 different standard images in Fig. 12. From Fig. 12, it is seen that the invisibility of the proposed scheme decreases with increase in capacity. Imperceptibility and robustness are the conflicting parameters. So, the increase in capacity may increase the robustness of the system. The effect of watermarking becomes visible when PSNR goes below 35 dB i.e. when watermark capacity is increased to 4096 bits or more. This analysis have been performed over 200 images including different class of images. The average performance (μ) along with the standard deviation (σ) of the results obtained from all images have been illustrated in Table 7.

3.5 Security analysis

A system that can maintain a high level of imperceptibility and robustness using watermarking scheme is desired to have a high security. To make the system more secure against multiple claims of ownership problems, false positive detection and unauthorized access of the system, two level security approaches is included. Firstly, using different keys (key 1 and key 2), the third level LWT sub-band coefficients and

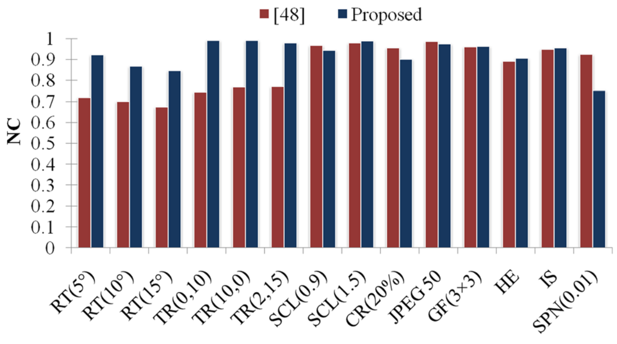


Fig. 14 Comparison of average robustness for different attacks

Table 9 The comparison results with [42] for different attacks in terms of NC

Attacks	Lena		Elaine		Man	
	[42]	Proposed	[42]	Proposed	[42]	Proposed
JPEG 30	0.9290	0.9454	0.9268	0.9803	0.9307	0.8557
JPEG 40	0.9428	0.9764	0.9356	0.9568	0.9374	0.9104
JPEG 50	0.9461	0.9882	0.9447	0.9763	0.9499	0.9687
JPEG 60	0.9571	0.9912	0.9530	0.9842	0.9564	0.9732
JPEG 70	0.9685	1.0000	0.9612	0.9954	0.9629	0.9823
IS	0.8616	1.0000	0.8632	0.9921	0.8689	0.8190
HE	0.8472	0.9803	0.8531	0.9921	0.8563	0.9684
GC	0.9430	0.9954	0.8953	0.9756	0.9230	0.9432
SN (0.05)	0.9384	0.6329	0.9238	0.7132	0.9247	0.8024

blocks are scrambled. These keys are used to give random embedding of watermark bits and its extraction correspondingly. Randomization is necessary for making it difficult for an intruder to find the locations of watermark even though the intruder have enough knowledge of watermark embedding and extraction process. Secondly, the binary watermark is encrypted by using reference watermark which acts as a key 3.

3.6 Comparative performance analysis

The performance of the proposed scheme is compared with some of the recent watermarking techniques [16, 19, 32, 42, 47, 48, 50–52]. Some important characteristics like watermark capacity, sub band used, robustness against de-synchronization attacks etc. of the related methods have been summarized in Table 8. The comparison of imperceptibility in terms of PSNR (dB) for 4 standard images is shown in Fig. 13. It is observed that the proposed technique provides better imperceptibility than the techniques proposed by Vermaet. al [47, 48], Kasana et al. [19], Wang et al. [51] and Hamghalam et al. [16] in most of the cases. The average robustness (over 15 images) in terms of NC is compared with the scheme proposed by Verma et al. [48] in Fig. 14. From Fig. 14, it is observed that our scheme provides better robustness than

Table 10 The comparison results with [32] for different attacks in terms of BER

Attacks	Lena		Peppers		Mandril		Jetplane	
	[32]	Proposed	[32]	Proposed	[32]	Proposed	[32]	Proposed
SPN (0.005)	0.0566	0.0562	0.0557	0.0473	0.0518	0.0472	0.0400	0.0328
SPN (0.01)	0.1152	0.1250	0.1230	0.1219	0.1025	0.0840	0.0889	0.0732
SPN (0.02)	0.1638	0.1582	0.1973	0.1855	0.1768	0.1758	0.1523	0.1435
GN (0.001)	0.0547	0.0467	0.0557	0.4648	0.0684	0.0572	0.0430	0.0439
GN (0.005)	0.2490	0.2132	0.2637	0.1926	0.2480	0.2289	0.2266	0.2264
GN (0.01)	0.3584	0.3456	0.3635	0.3652	0.3281	0.2985	0.3213	0.3213
IS	0.0107	0.0059	0.0107	0.0062	0.0557	0.0092	0.0039	0.0062
JPEG 50	0.0020	0.0020	0.0020	0.0020	0.0256	0.0117	0	0.0032
JPEG 70	0	0	0	0	0.0049	0	0	0
RT 0.5°	0.3574	0.0009	0.3291	0	0.2813	0.0009	0.3428	0.0020
RT 5°	0.4983	0.0372	0.5023	0.0395	0.4277	0.0892	0.4922	0.0742

Table 11 The comparison results with [48, 50, 52], for common image processing operations in terms of BER

Attacks	Images											
	Lena				Barbara				Mandril			
	[48]	[52]	[50]	Proposed	[48]	[52]	[50]	Proposed	[48]	[52]	[50]	Proposed
GF(3×3)	0.0215	0.0469	0.0117	0.0098	0.0137	0.0352	0.0188	0.0117	0.0332	0.0435	0.1802	0.0195
AF(3 × 3)	0.0684	0.0740	0.0413	0.1660	0.0625	0.0713	0.0669	0.2090	0.0391	0.1079	0.3706	0.3379
SPN(0.01)	0.0430	0.0369	0.0081	0.1250	0.0605	0.0400	0.0166	0.1465	0.0352	0.0491	0.0684	0.0840
HE	0.0332	0.5435	0.3354	0.0020	0.0117	0.7170	0.5044	0.0020	0.0257	0.6226	0.4946	0.0234
JPEG30	0.0195	0.1328	0.0903	0.0254	0.0117	0.1113	0.1011	0.0449	0.0234	0.0601	0.3806	0.0527
JPEG40	0.0156	0.0925	0.0681	0.0098	0.0156	0.0867	0.0769	0.0059	0.0195	0.0571	0.3467	0.0078
JPEG50	0.0098	0.0769	0.0466	0.0020	0.0098	0.0681	0.0588	0.0039	0.0117	0.0479	0.2917	0.0117
JPEG70	0	0.0459	0.0242	0	0	0.0466	0.0256	0	0	0.0403	0.1714	0
RT(10°)+ SCL(0.9)	0.1543	0.0498	0.0747	0.0859	0.1660	0.0869	0.0977	0.0664	0.1504	0.1287	0.3293	0.1113
RT (5°)+ JPEG 50	0.1328	0.0798	0.0746	0.0371	0.1270	0.0781	0.0833	0.0664	0.1230	0.0750	0.3201	0.0781
SCL(0.9)+ JPEG 70	0.0117	0.0630	0.0835	0.0273	0.0156	0.0601	0.0925	0.0352	0.0273	0.0667	0.3591	0.0605
RT(15°)+ TR(2,15)	0.1680	0.0374	0.0186	0.0566	0.1426	0.0793	0.0625	0.0996	0.1543	0.1267	0.2151	0.0938

Verma et al. [48] for de-synchronization and image processing attacks. However, the proposed algorithm gives equivalent performances against some noising and de-noising attacks. This may be due to the use of HL sub-band for watermark embedding. The robustness comparisons are also shown in Tables 9, 10, and 11. In Table 9, the comparison is made in terms of NC for 3 different standard images with Singh et al. [42]. Table 10 shows the comparative performance with Mehta et al. [32] in terms of BER. The robustness comparison is also evaluated in terms of BER with the techniques proposed by Verma et al. [48], Yang et al. [52],and Wang et al. [50] for three different standard images and is tabulated in Table 11. In Table 11, the attacks include lossy compression standard, noising, de-noising, geometric attack along with the combination of different attacks. The proposed technique outperforms other techniques in robustness against geometric attacks, image processing attacks, and lossy compression attacks. Though the proposed algorithm does not provide better robustness against noising and de-noising attacks, but provides comparable performance in terms of NC and BER. Therefore, the simulation results illustrate that proposed technique gives better solution for copyright protection under different attack conditions, especially against geometric attacks.

4 Conclusion

In this work, the advantage of geometric distortion correction based watermarking approach has been combined with SVM classification based binary watermark detection to achieve robustness against both geometrical and non-geometrical attack. In this proposed algorithm, the combination of LWT and SVD is used for watermark embedding and extraction purpose. During watermark extraction, SVM classifier has been incorporated for the classification technique to detect binary watermark with maximum possible correlation. The algorithm provides an average imperceptibility of 42.27 dB on a large image database with an embedding capacity of 512 bits. Geometric distortion correction is done using Radon transform and invariant centroid to achieve robustness against de-synchronization attack. The security of the proposed algorithm is enhanced by using random shuffling of coefficients, blocks using different keys and encryption of signature watermark using another key (reference watermark). It is also observed that the technique works not only against non-geometrical attacks buts also against geometrical attacks. Experiments have been performed on different types of image database under various signal processing attacks. The algorithm provides satisfactory performance against geometrical attacks, JPEG compression, and some common image processing operations maintaining an adequate level of imperceptibility. It has been observed that the proposed system provides better performances as that of the existing techniques under diverse signal processing attacks. As a scope of future work, emphasis may be given to improve robustness against noising and de-noising attacks. Further improvements may be done by enhancing the capacity of the system maintaining the sufficient level of imperceptibility and robustness. The propose technique may also be extended for color image watermarking.

Acknowledgements The authors would like to acknowledge Speech and Image Processing Laboratory, Department of Electronics and Communication Engineering, National Institute of Technology Silchar, India for providing support and necessary facilities for carrying out this work. Moreover, the authors would like to thank Mr. Amarjit Roy, Asst. Professor, School of Engineering and Technology, BML Munjal University, Gurgaon, Haryana, India for his valuable suggestions.

References

1. Abu-Marie W, Gutub A, Abu-Mansour H (2010) Image based steganography using truth table based and determinate array on RGB indicator. Int J Sig Image Process 1(3):196–204
2. Al-Otaibi NA, Gutub AA (2014) 2-leyer security system for hiding sensitive text data on personal computers. Lect Notes on Inf Theory 2(2):151–157
3. Al-Otaibi NA, Gutub AA (2014) Flexible stego-system for hiding text in images of personal computers based on user security priority. In Proceedings of 2014 International conference on Advanced Engineering Technologies (AET-2014) (pp 243–250)
4. Alotaibi N, Gutub A, Khan E (2015) Stego-System for Hiding Text in Images of Personal Computers. In The 12th Learning and Technology Conference: Wearable Tech/Wearable Learning
5. Barni M, Bartolini F, Cappellini V, Piva A (1998) A DCT-domain system for robust image watermarking. Signal Process 66(3):357–372
6. Cedillo-Hernández M, García-Ugalde F, Nakano-Miyatake M, Pérez-Meana HM (2014) Robust hybrid color image watermarking method based on DFT domain and 2D histogram modification. SIViP 8(1):49–63
7. Cox IJ, Miller ML, Bloom JA, Honsinger C (2002) Digital watermarking, vol 1558607145. Morgan Kaufmann, San Francisco
8. Deng C, Gao X, Li X, Tao D (2009) A local Tchebichef moments-based robust image watermarking. Signal Process 89(8):1531–1539
9. Deng C, Gao X, Li X, Tao D (2010) Local histogram based geometric invariant image watermarking. Signal Process 90(12):3256–3264
10. Dong P, Brankov JG, Galatsanos NP, Yang Y, Davoine F (2005) Digital watermarking robust to geometric distortions. IEEE Trans Image Process 14(12):2140–2150
11. Fazli S, Moeini M (2016) A robust image watermarking method based on DWT, DCT, and SVD using a new technique for correction of main geometric attacks. Optik-Int J Light Electron Opt 127(2):964–972
12. Gao X, Deng C, Li X, Tao D (2010) Geometric distortion insensitive image watermarking in affine covariant regions. IEEE Trans Syst Man Cybern Part C Appl Rev 40(3):278–286
13. Gutub AAA, Khan FAA (2012) Hybrid Crypto Hardware Utilizing Symmetric-Key and Public-Key Cryptosystems. In Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on (pp 116–121). IEEE
14. Gutub A, Ankeer M, Abu-Ghalioun M, Shaheen A, Alvi A (2008) Pixel indicator high capacity technique for RGB image based Steganography. In WoSPA 2008-5th IEEE International Workshop on Signal Processing and its Applications
15. Gutub A, Al-Qahtani A, Tabakh A (2009) Triple-A: Secure RGB image steganography based on randomization. In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on (pp 400–403). IEEE
16. Hamghalam M, Mirzakuchaki S, Akhaee MA (2014) Geometric modelling of the wavelet coefficients for image watermarking using optimum detector. IET Image Process 8(3):162–172
17. Hou YC (2003) Visual cryptography for color images. Pattern Recogn 36(7):1619–1629
18. Hu HT, Hsu LY (2016) Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics. Multimed Tools Appl 76(5):6575–6594
19. Kasana G, Kasana SS (2017) Reference based semi blind image watermarking scheme in wavelet domain. Optik-Int J Light Electron Opt 142:191–204
20. Khan F, Gutub AAA (2007) Message concealment techniques using image based steganography. In The 4th IEEE GCC Conference and Exhibition
21. Kim BS, Choi JG, Park CH et al (2003) Robust digital image watermarking method against geometrical attacks. Real-Time Imaging 9(2):139–149
22. Lai CC, Tsai CC (2010) Digital image watermarking using discrete wavelet transform and singular value decomposition. IEEE Trans Instrum Meas 59(11):3060–3063
23. Li J, Zhu Y (2010) A geometric robust image watermarking scheme based on DWT-SVD and Zernike moments. In Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Vol. 1, pp. 367–371). IEEE
24. Li Q, Zhou X, Gu A, Li Z, Liang RZ (2016) Nuclear norm regularized convolutional Max Pos@ Top machine. Neural Comput Applic. doi:10.1007/s00521-016-2680-2
25. Liang RZ, Shi L, Wang H, Meng J, Wang JJY, Sun Q, Gu Y (2016) Optimizing top precision performance measure of content-based image retrieval by learning similarity function. arXiv preprint arXiv:1604.06620
26. Liang RZ, Liang G, Li W, Gu Y, Li Q, Wang JJY (2016) Learning convolutional neural network to maximize Pos@ Top performance measure. arXiv preprint arXiv:1609.08417

27. Lin SD, Shie SC, Guo JY (2010) Improving the robustness of DCT-based image watermarking against JPEG compression. Comput Stand Interface 32(1):54–60
28. Lutovac B, Daković M, Stanković S, Orović I (2016) An algorithm for robust image watermarking based on the DCT and Zernike moments. Multimed Tools Appl. doi:10.1007/s11042-016-4127-2
29. Makbol NM, Khoo BE (2013) Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. AEU-Int J Electron Commun 67(2): 102–112
30. Makbol NM, Khoo BE (2014) A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. Digital Signal Process 33:134–147
31. Mehta R, Rajpal N, Vishwakarma VP (2015) A robust and efficient image watermarking scheme based on Lagrangian SVR and lifting wavelet transform. Int J Mach Learn Cybern 8(2):379–395
32. Mehta R, Rajpal N, Vishwakarma VP (2016) LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR. Multimed Tools Appl 75(7):4129–4150
33. Mishra A, Agarwal C, Sharma A, Bedi P (2014) Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm. Expert Syst Appl 41(17):7858–7867
34. Parvez MT, Gutub AAA (2008) RGB intensity based variable-bits image steganography. In Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE (pp. 1322–1327). IEEE
35. Parvez MT, Gutub AAA (2011) Vibrant color image steganography using channel differences and secret data distribution. Kuwait J Sci Eng 38(1B):127–142
36. Peng H, Wang J, Wang W (2010) Image watermarking method in multiwavelet domain based on support vector machines. J Syst Softw 83(8):1470–1477
37. Ramanjaneyulu K, Rajarajeswari K (2012) Wavelet-based oblivious image watermarking scheme using genetic algorithm. IET Image Process 6(4):364–373
38. Roy A, Laskar RH (2016) Multiclass SVM based adaptive filter for removal of high density impulse noise from color images. Appl Soft Comput 46:816–826
39. Roy A, Singha J, Devi SS, Laskar RH (2016) Impulse noise removal using SVM classification based fuzzy filter from gray scale images. Signal Process 128:262–273
40. Ruanaidh JJO, Pun T (1998) Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal Process 66(3):303–317
41. Singh C, Ranade SK (2013) Geometrically invariant and high capacity image watermarking scheme using accurate radial transform. Opt Laser Technol 54:176–184
42. Singh D, Singh SK (2016). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimed Tools Appl 76(11):13001–13024
43. Singh P, Agarwal S, Pandey A (2013) A hybrid DWT-SVD based robust watermarking scheme for color images and its comparative performance in YIQ and YUV Color Spaces. In Advance Computing Conference (IACC), 2013 I.E. 3rd International (pp. 1213–1218). IEEE
44. Singha J, Laskar RH (2015) ANN-based hand gesture recognition using self co-articulated set of features. IETE J Res 61(6):597–608
45. Thakkar FN, Srivastava VK (2016) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl 76(3):3669–3697
46. Tsai HH, Sun DW (2007) Color image watermark extraction based on support vector machines. Inf Sci 177(2):550–569
47. Verma VS, Jha RK, Ojha A (2015) Significant region based robust watermarking scheme in lifting wavelet transform domain. Expert Syst Appl 42(21):8184–8197
48. Verma VS, Jha RK, Ojha A (2015) Digital watermark extraction using support vector machine with principal component analysis based feature reduction. J Vis Commun Image Represent 31:75–85
49. Wang XY, Yang HY, Cui CY (2008) An SVM-based robust digital image watermarking against desynchronization attacks. Signal Process 88(9):2193–2205
50. Wang XY, Miao EN, Yang HY (2012) A new SVM-based image watermarking using Gaussian–Hermite moments. Appl Soft Comput 12(2):887–903
51. Wang XY, Liu YN, Xu H, Wang AL, Yang HY (2016) Blind optimum detector for robust image watermarking in non sub-sampled shearlet Domain. Inf Sci 372:634–654
52. Yang HY, Wang XY, Wang CP (2013) A robust digital watermarking algorithm in undecimated discrete wavelet transform domain. Comput Electr Eng 39(3):893–906
53. Yu PT, Tsai HH, Lin JS (2001) Digital watermarking based on neural networks for color images. Signal Process 81(3):663–671
54. Zhu H, Liu M, Li Y (2010) The RST invariant digital image watermarking using Radon transforms and complex moments. Digital Signal Process 20(6):1612–1628

Mohiul Islam has received his M.Tech degree in 2014 from National Institute Technology Agartala and B.E degree from Assam Engineering College in 2011. He is currently pursuing Ph.D. in the Department of Electronics and Communication Engineering at National Institute of Technology Silchar. His research interests include Image processing, Machine Learning, Digital Image Watermarking. E-mail: mohiul292@gmail.com

Rabul Hussain Laskar has completed his PhD from National Institute of Technology, Silchar, India and his M.Tech from Indian Institute of Technology, Guwahati. He is currently working as Assistant Professor in the Department of Electronics and Communication Engineering at NIT Silchar. His major research interests are in Speech processing, Image processing, Digital signal Processing, machine learning. E-mail: rabul18@yahoo.com