Feature-Based Robust Image Watermarking Using DTT and SVD for Copyright Protection

J L Divya Shivani [1], Ranjan K. Senapati [2]

Department of ECE
KLEF (Deemed to be a University)
Green Fields, Vaddeswaram, Guntur (dist.)
Andhra Pradesh, 522502, India.
e-mail: [1] shivanidivya18@gmail.com, [2] rkphd@gmail.com

***Abstract* - This paper presents a simple yet efficient watermarking algorithm based on scale invariant feature transform (SIFT), singular value decomposition (SVD) and discrete Tchebichef transform (DTT). The generation process of SIFT algorithm, and generation of feature points are described. In the proposed method, first DTT is applied to the 8×8 blocks of an image data. The 8×8 blocks of coefficients are then arranged like coefficients in a 3 level wavelet pyramid. SVD is applied to appropriate pyramid level/s for embedding the watermark. The feature points obtained from SIFT are used for correction of geometrical attacks, e.g., rotation, scale and translation (RST) attacks. The effect of combined attacks such as rotation and scale, translation and scale, translation and rotation, rotation with noise, translation with noise, scale with noise, rotation with JPEG compression have been also analysed. Experimental results demonstrate that the proposed algorithm has stronger robustness and better imperceptibility compared to previous schemes in most of the attacks.**

Keywords - Scale invariant feature transform; Discrete Tchebichef Transform; Singular Value Decomposition; RST attacks; Blind Watermarking.

I. INTRODUCTION

Many digital data contents in internet are having intellectual property rights and copyright protection. Anyone can modify the internet content using recently developed sophisticated editing tools. This invariably drives the researchers to develop techniques for copyright protection and authentication.

Watermarking technique is the most popular technique in the domain of copyright protection. Watermarking techniques should satisfy robustness and imperceptibility. Robustness means the extracted watermark should not get destroyed with various geometrical transformations that include analog-to-digital and digital-to-analog conversion and compression. Imperceptibility specifies the fidelity of the watermarked image which indicate watermark neither noticeable to the user nor degrade the quality of the image. Many algorithms exist to trade off these two parameters [1]-[10]. Watermarking techniques are broadly classified in two categories: (i) spatial domain and (ii) transformed domain based. As opposed to spatial domain techniques, transformed domain techniques provide better capacity that can embed a large number of data without incurring noticeable visual distortion. In addition, transformed domain schemes provide better robustness against common image processing attacks and geometrical attacks. The common examples of transformed domain techniques incorporates Discrete cosine transform (DCT) [11], Finite Ridgelet transform (FRIT)[12], Discrete Fourier transform (DFT)[13], Discrete wavelet transform.(DWT)[14], Redundant discrete wavelet transform (RDWT)[15-18], Non Subsampled Contourlet Transform (NSCT) [19] and Singular value decomposition (SVD)[20-24]. Some researchers suggested hybrid watermarking schemes that combines two or three transforms to provide better robustness and high imperceptibility [20].

The SVD transform always shows a good performance while combine with the other transform domain techniques. Its primary advantages are (1) good stability, i.e., when small perturbation added to an image, no large variation occur in its singular values (SVs), (2) SVs represents the algebraic properties, specifying an image luminance, and (3) The corresponding pair of singular vector represents the geometry properties of an image. However, the SVD with other transforms to geometrical attacks such as rotation, scale and translation are not satisfying. Therefore, it is necessary to carry out research and propose a watermarking method which can resist to RST attacks. In order tosolve the problem, the scale invariant feature transform (SIFT) is applied in image watermarking [25-29]. SIFT is an efficient method for detection of interesting feature points as well as local feature description. Because of this important property SIFT is mostly embraced in computer vision domain such as image matching, object recognition, image indexing, segmentation, registration and data hiding. SIFT is robust to RST and affine transformation.

II. MATERIALS AND METHODS

Recently, SIFT is extensively applied in digital watermarking for copyright protection. A local invariant feature based watermarking is proposed by Lee et al [25], where embedding the watermark is done into the patches of circular region of the cover image. An adaptive watermarking scheme that uses DFT and SIFT is proposed in [26]. In this method DFT is computed on the local sub-image regions of the host image for watermarking. A DWT and SIFT based image watermarking scheme is proposed by Lyu et al. [27], wherein first DWT is applied on the selected areas and then SIFT is applied in those areas to extract feature points. Thorat and Jadhav [28] proposed an anti-geometrical attack scheme for color images, which is based on IWT and SIFT.First, SIFT is applied on the red components of the image and feature points are extracted. Then IWT is performed on the blue and green components. Finally, the low-frequency coefficients of IWT are used for embedding watermark. A robust watermarking scheme based on SIFT and DCT is proposed by Pham et al.[29], where watermark embedding is done into the selected feature region after DCT. Beside the geometric invariance of watermarking schemes, watermarking is applied to the moments transform domain based schemes. Yuan and Pun [30] proposed Zernike moments and SIFT based scheme. SIFT is applied to obtain the circular region, and Zernike moment performed on binary regions. Then, magnitude of local Zernike moments is modified for embedding watermark. Wang et al. [31] proposed a geometrically invariant watermarking scheme which uses Radial harmonic Fourier moments to embedding the watermark into their quantized magnitudes. An effort of comparative performance analysis is made by Tsougenis et al.[32] on moment based watermarking schemes. Zhang et al. [33] recently proposed a RST resilient watermarking scheme using DWT-SVD and SIFT. In that scheme extracted feature points of the watermarked image are used as the key for embedding and extraction process. From the above literatures it is certain that combining SIFT with various transforms is becoming an alternative option for robust image watermarking.

With the advantage of the robustness features of SIFT and SVD, as well as better energy concentration of DTT in low frequencies, the combined approach is expected to provide better result. To the best of our knowledge SIFT is not combined with DTT for watermarking in literature. This leads us to develop the concept of combining digital watermarking with SIFT,SVD and DTT. The proposed work is compared with some recently proposed DWT-SVD and SIFT based schemes to show its efficiency.

The remainder of the paper is outlined as follows: Section 3 describes the embedding and extraction process of the proposed algorithm in detail. Simulation results and discussion are highlighted in Section 4. Finally, conclusion and future works are presented in Section 5.

III. PROPOSED ALGORITHM

The watermark embedding and extraction process of the proposed algorithm which combines DTT, SVD and SIFT is presented in subsection 3.1 and 3.2 respectively. The watermark is randomly permuted before embedding the principal components of the watermark with the diagonal component of the sub-band coefficients of DTT. This provides additional security to the proposed algorithm. The block diagram of watermark embedding and extraction process is shown in Figure 1.

A. Watermark Embedding Algorithm

The steps are as follows:

Crop the cover image into 8×8 blocks and apply DTT to these 8×8 blocks. Zigzag scan the coefficients of all 8x8 blocks. Arrange the coefficients in a 3 level pyramidal decomposition process, which is shown in Figure 2. Let the highest decomposition levels be named as:

$\{LL_3, HL_3, LH_3, HH_3\}$

Apply SVD on all highest decomposition levels according to Equation (1):

$$Z_i = SVD(I_i)$$

where I_i can be any of the sub-band such as:

$\{LL_3, HL_3, LH_3, HH_3\}$

Thus,

$$Z_i = U_i S_i V_i^T \tag{1}$$

Let W be the watermark image. Apply permutation operator and then computing SVD on W produces matrices:

$uw1, sw1$ and $vw1$.

The $uw1$ and $vw1$ are left and right singular vectors and $sw1$ is a diagonal matrix (also called singular value). The process of decomposition is represented in Equation (2):

$$W \xrightarrow{Permute} P(W) \xrightarrow{SVD} (uw1)(sw1)(vw1^T) \tag{2}$$

Modify the singular values of Z_i by embedding the watermark as shown in Equation (3):

$$S_i^c = S_i + \beta(uw1 \times sw1) \tag{3}$$

where $\beta = 1$ for LL_3 sub-band, 0.08 for HL_3, LH_3, and 0.06 for HH_3 sub-band. The values are selected iteratively and provide better trade off of imperceptibility and robustness values. It is to be noted that $vw1$ is used as the key for watermark extraction.

Apply SVD of each sub-band with the modified coefficients S_i^c

$$I_i^m = SVD(S_i^c) = U_i^m S_i^m V_i^{mT} \quad (4)$$

Where I_i^m indicate the modified sub-bands of : $\{LL_3, HL_3, LH_3, HH_3\}$

Apply inverse SVD using the singular value S_i^m with U_i and V_i of the original image of left and right singular vector matrices according to Equation (5):

$$I^w = U_i S_i^m V_i^T \quad (5)$$

Apply inverse hierarchical coefficient arrangement, inverse Zigzag scan, inverse DTT to 8×8 blocks and merge operation to obtain watermarked image I^w.

Finally, extract feature points by applying SIFT to the watermarked image, I^w . Descriptors (coordinates, scale and orientations) of watermarked image are saved as keys for feature matching during the extraction process.

B. Watermark Extraction Algorithm

Apply SIFT and obtained feature points from the attacked image. The attacked image is possibly a distorted watermarked image I^{w*} .

Apply 8×8 DTT to the distorted watermarked image I^{w*}, Perform Zigzag scan and 3 levels of hierarchical pyramid arrangement to I^{w*} so as to generate DTT sub-bands: $\{LL_3^*, HL_3^*, LH_3^*, HH_3^*\}$

Apply SVD on each distorted sub-band according to Equation (6)

$$I_i^{w*} = U_i^{w*} S_i^{w*} V_i^{wT*} \quad (6)$$

Apply inverse SVD to each sub-band using singular value S_i^{w*} , while keeping U_i^m and V_i^m obtained in Equation (4) of embedding process as the keys.

$$I_i^{m*} = U_i^m S_i^{w*} V_i^m \quad (7)$$

Find the parameter:

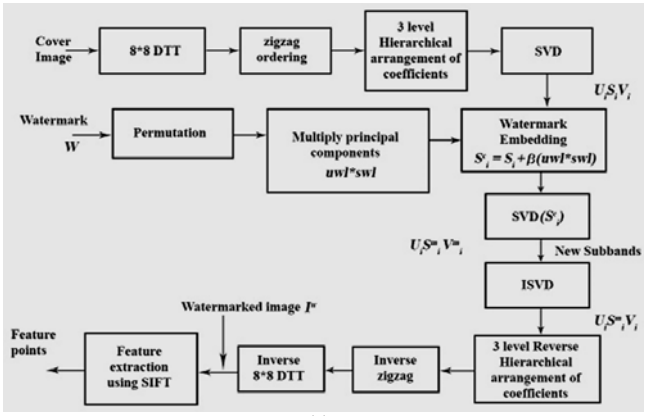
$$W_p = \frac{I_i^{m*} - S_i}{\beta} \quad (8)$$

Where β =1 for LL_3^* , 0.08 for $\{HL_3^*, LH_3^*\}$ sub-bands, and 0.06 for HH_3^* sub-band. The parameter, S_i is the singular value obtained in Equation (2) of embedding algorithm.

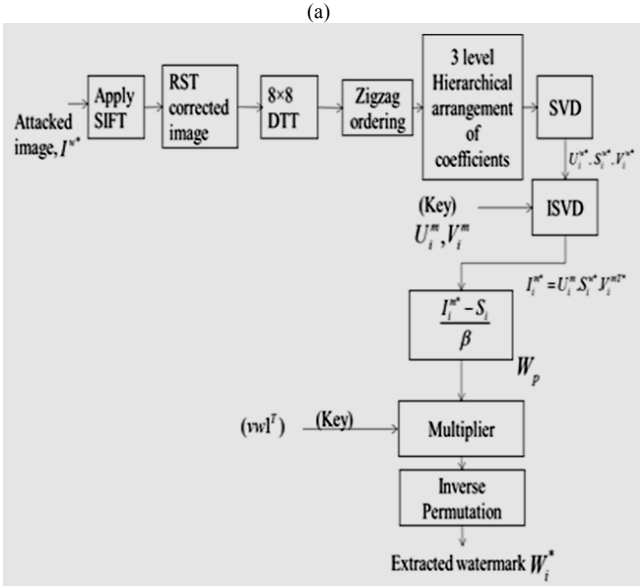
Extract the watermark using the formula according to Equation(9):

$$W_i^* = W_p \times vw1^T \quad (9)$$

where $vw1^T$ the right singular vector of watermark W and is also used as Key for watermark extraction.



(a)



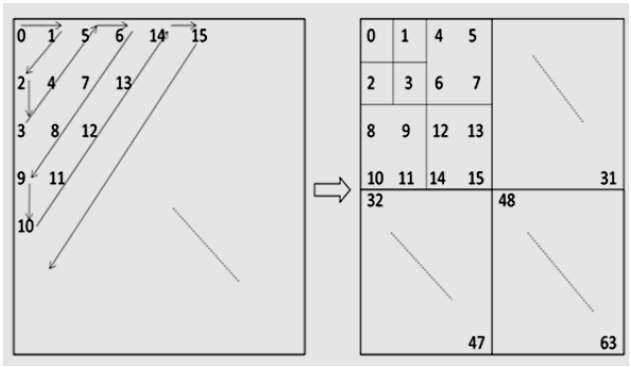
(b)

Figure 1. Procedure for (a) Watermark Embedding and (b) Watermark extraction process

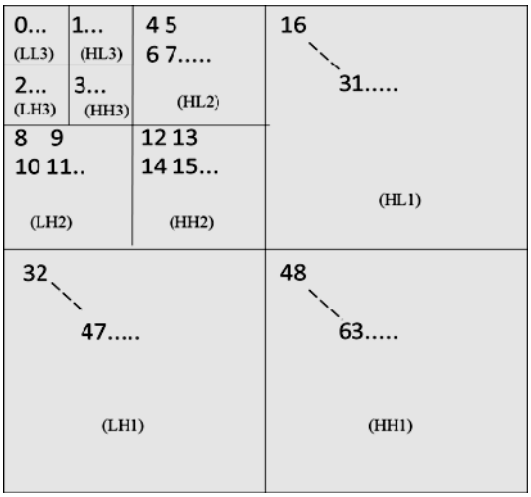
C. Three Level Pyramidal Arrangement of DTT Coefficients

The cover image is cropped into 8×8 blocks. Zigzag arrangement of coefficients is performed on all the 8×8 blocks of image as shown in Figure 2 (a). All the 64 coefficients of an 8×8 block are arranged in a 3 level

hierarchical pyramid like shown in Figure 2 (b). Figure 2(c) shows the arrangement of a typical 8×8 block of coefficients that map into the image block of size 512×512. The 0th coefficient of all 8x8 blocks are mapped into the top left LL3 , the 1st coefficients of all 8x8 blocks are mapped to HL3 , the 2ndcoefficients of all 8x8 blocks are mapped to LH3 and the 3rd coefficients of all 8x8 blocks are mapped to HH3. Similar arrangement and mapping will be performed for other 8×8 blocks of DTT coefficients to fill the entire sub-bands of image data.



(a) (b)



(c)

Figure 2 Hierarchical arrangements of DTT coefficients (a) Zigzag scanning of a typical 8×8 block, (b) arrangement of coefficients in a 3-level hierarchical pyramid of the 8×8 block, (c) mapping of all 8×8 blocks of coefficients to an image size (512×512).

D. Scale Invariant Feature Transform (SIFT):

The local scale-invariant feature keypoint descriptors for matching the two images are proposed by Lowe [24]. The SIFT feature descriptors are briefly described in four parts below:

D1. Scale-Space Extrema Detection

The goal of keypoint detection is to identify scales and locations that can be repeatedly found in different view-sight of the same object or scene. For scale-invariant points, it is important to search not only every possible location in the image, but also across all the possible scales, using a continuous function known as scale space. Gaussian convolution kernel [24] is applied for achieving the scale transformation. The scale space of an image is defined as a $L(i, j, \sigma)$ produced from the convolution of a variable-scale Gaussian and an image as:

$$L(i, j, \sigma) = G(i, j, \sigma) * I(i, j) \tag{10}$$

where $I(i,\ j)$ is the image and

$$G(i, j, \sigma) = \frac{1}{2\pi\sigma^2} e^{-(i^2+j^2)/2\sigma^2} \tag{11}$$

Where $G(i, j, \sigma)$ is the scale variable Gaussian function. (i, j) is the spatial coordinate and σ is the scale-space factor which decides the smoothness of the image.

To extract SIFT features, the image is convolved first with Gaussian kernels ate different scales to generate difference of Gaussian (DOG) images represented by Equation (12):

$$D(i,j,\sigma)=[G(i,j,k\sigma)-G(i,j,\sigma)]*I(i,j)=L(i,j,k\sigma)-L(i,j,\sigma) \tag{12}$$

Where k is a constant multiplicative factor.

With the help of DOG scale-space, all extreme points can be calculated as key points.

D2. Accurate Keypoint localization:

The initial implementation approach followed by Lowe [24] uses the Taylor expansion (up to the quadratic terms) of the scale-space function $D(i, j, \sigma)$ shifted so that the origin is at the sampled point:

$$D(\xi) = D + \frac{\partial D^T}{\partial \xi}\xi + \frac{1}{2}\xi^T \frac{\partial^2 D}{\partial \xi^2}\xi \tag{13}$$

Where D and its derivatives are evaluated at the sample point and $\xi = (i, j, \sigma)^T$ is the offset from this point. The location of the extremum, ξ' is determined by taking the derivative of the function w.r.t ξ and setting it to zero, giving

$$\xi' = -\frac{\partial^2 D^{-1}}{\partial \xi^2}\frac{\partial D}{\partial \xi} \tag{14}$$

Substituting Equation (14) into Equation (13), we get the function value at the extremum, which is useful for rejecting extrema with low contrast. The function $D(\xi')$ is expressed in Equation(15):

$$D(\xi') = D + \frac{1}{2}\frac{\partial D^T}{\partial \xi}\xi' \quad (15)$$

D3. Orientation Assignment:

The keypoint descriptor can be represented relative the orientation to achieve invariance to image rotation. In scaling smooth image I_L , the central derivative of I_L at every point is calculated. Further, scale and orientation at every keypoint (i, j) is calculated by Equation (16) as:

$$\theta(i,j) = \arctan2\{[I_L(i,j+1) - I_L(i,j-1)]/[I_L(i+1,j) - I_L(i-1,j)]\}$$
$$g(i,j) = \sqrt{[I_L(i+1,j) - I_L(i-1,j)]^2 + [I_L(i,j+1) - I_L(i,j-1)]^2} \quad (16)$$

where $\theta(i, j)$ is the direction of the gradient and $g(i, j)$ is the gradient modulus value.
After obtaining gradient direction and amplitude, the gradient direction of the keypoint can be determined by gradient direction histogram. The peak of the histogram is set as the main direction of the keypoint and auxiliary direction is taken as the 80% of main peak's value to improve robustness.

D4. Keypoint Descriptor Representation:

The gradient direction histogram is used to represents the local image descriptor of keypoints. The procedures of keypoint can be calculated with following three steps:

Step1: The computation of scale and orientation are performed in the 16×16 neighbor of keypoints.
Step2: The 16×16 neighborhood blocks are divided into 4x4 blocks. This gives rise to 16 blocks in the neighbor of every keypoint and 8 orientations in the central point of every 4×4 block.
Step3: A vector size of 1×128 orientations is obtained as the keypoint feature vector.

IV. SIMULATION RESULTS AND DISCUSSION

In this section, several simulations are conducted to examine the robustness and imperceptibility of the proposed algorithm. Simulations are carried out using two images, Lena, and Barbara as cover/ host images. Cameraman image of size 64×64 is used as watermark image. The sizes of the host images are 512×512. The objective quality (i.e., imperceptibility) of the watermarked image and extracted watermark are measured in terms of peak-signal-to-noise-ratio (PSNR) and normalized correlation (NC) respectively. The PSNR value in decibels (dB) indicates similarity between the host image and watermarked image, while NC verifies the presence of watermark. These are given below:

$$\text{PSNR} = 10\log_{10}\frac{I_{Peak}^2}{MSE} \quad (17)$$

Where MSE is the mean square error between the watermarked image, I^w and its original image, I.

$$\text{MSE} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}[I(i,j) - I^w(i,j)]^2}{N^2}$$

Structural similarity index (SSIM) which considers image degradation as a perceived change in structural information, while also incorporating perceptual phenomenon, i.e., luminance masking and contrast masking terms, overcomes the deficiency of PSNR. It is represented by Equation (18):

$$SSIM(I, I^w) = \frac{(2\mu_I\mu_{I^w} + c_1)(2\sigma_{II^w} + c_2)}{(\mu_I^2 + \mu_{I^w}^2 + c_1)(\sigma_I^2 + \sigma_{I^w}^2 + c_2)} \quad (18)$$

Where:

μ_I and σ_I is the mean and variance of I, μ_{I^w} and σ_{I^w} mean and variance of I^w. σ_{II^w} is the covariance of I and I^w. c_1 and c_2 are positive constants. The range of SSIM is between 0 and 1. SSIM= 1 indicates the images I and I^w are identical.

The NC value between original watermark (W) and extracted watermark (W^*) is defined as:

$$\text{NC} = \frac{\sum_{i=0}^{M}\sum_{j=0}^{M}[W(i,j)W^*(i,j)]}{\sum_{i=0}^{M}\sum_{j=0}^{M}[W(i,j)]^2} \quad (19)$$

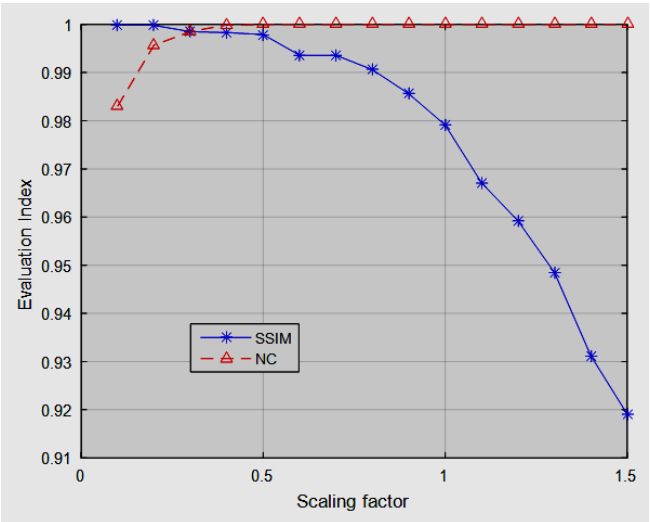


Figure 3. SSIM and NC values of the proposed method with different quantization steps

The watermark of size 64×64 is embedded into the LL3, HL3, LH3 and HH3 band of the host image after three level of DTT coefficient arrangement with different scaling factor. The scaling factor is set as 1 for LL3 subband (shown in Figure 3) in order to resolve the trade-off between imperceptibility and robustness.

Correction of RST Attack Based on SIFT:

The proposed scheme shows the watermarked image and it's extracted watermark under various RST attack in Figure 5, 7 and 9 respectively. The rotation angles are 20, 50, 100, 300 and 450 is made. In scaling attacks, the image is scaled to 0.25, 0.5, 0.9 and 1.2. Similarly, in translation attack, vertical and horizontal translation of 60 and 20 pixels, vertical translation of 128 pixels and horizontal translation of 128 pixels is performed to test the robustness performance of the proposed scheme.

First, SIFT features of an image such as the horizontal coordinates, vertical coordinates, scales, orientation factors and key point descriptors are obtained. Then, the descriptors of feature points saved in embedding process are matched with the descriptors of feature points of the attacked image. Let there are M pairs of matching points are obtained. These M pairs of matching points are used for correction of the following attacks.

Scaling Attack:

The size of the image is changed in scaling attacks. The match between scaled image and watermarked image is shown in Figure 4.

Figure 4. Feature matching between watermarked image (left) and Scaling attacked image (right).

The scaling value can be founding by considering the size relationship between scaled image and watermarked image. For M pair of matching points, if W_{iq} and S_q are the q^{th} scale values of matching points in watermarked image and scaled image respectively, then the scale value s can be found as:

$$s = \frac{1}{M}\sum_{q=1}^{M}\frac{W_{iq}}{S_q} \tag{20}$$

After calculating the scaled parameter, the received image (scaled) should be scaled by $1/s$ parameter to achieve restored image.

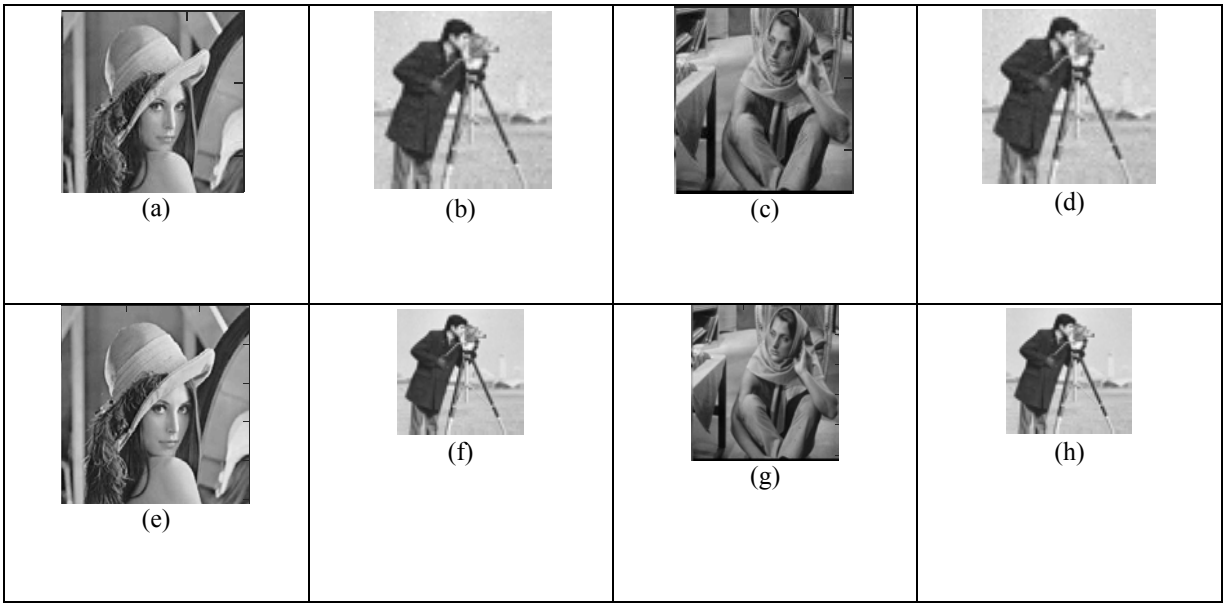


Figure 5. Watermarked image and retrieved watermark on scaling attacks (a) scaled (0.25) Lena with (b) retrieved watermark; (c) scaled (0.25) Barbara with (d) retrieved watermark, (e) scaled(0.5) Lena with (f) retrieved watermark; (g) scaled (0.5) Barbara with (h) retrieved watermark.

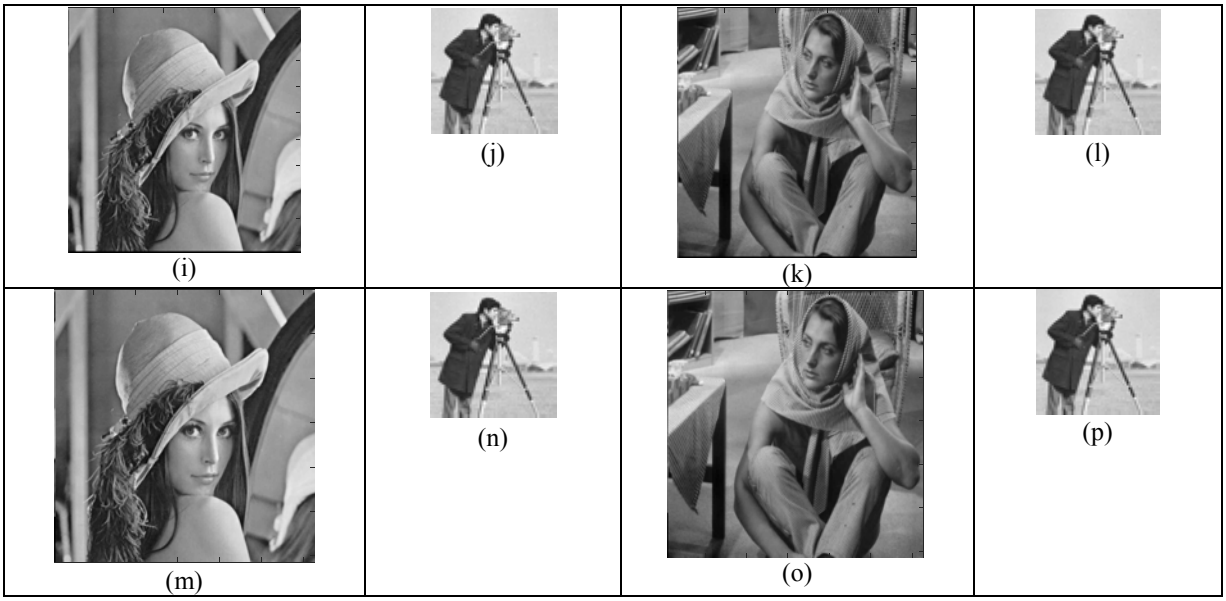


Figure 5, continued, (i) scaled (0.9) Lena with (j) retrieved watermark; (k) scaled (0.9) Barbara with (l) retrieved watermark; (m) scaled(1.2) Lena with (n) retrieved watermark; (o) scaled (1.2) Barbara with (p) retrieved watermark.

Translation Attack

In translation attack the image will move upward or downward or both upward and downward from its original location. The translation attack does not change the shape and size of the image but results in loss of image information. Figure 6 shows the right image is translated 20 pixels horizontally and 60 pixels vertically with respect to the image shown in left.

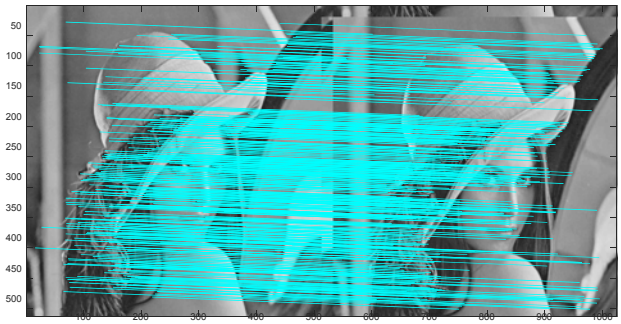


Figure 6 Feature matching between watermarked image (left) and translation attacked image (right).

Similar to the scaling attack correction, let the coordinates of the watermarked image and translated image are set as (p_w, q_w) and (p_t, q_t). Then for an image of size $N \times N$, the corrected horizontal and vertical coordinated (p_c, q_c) can be calculated by Equation (21):

$$p_c = \begin{cases} p_t - p_w + N, & p_t < p_w \\ p_t - p_w, & \text{elsewhere} \end{cases}, \quad q_c = \begin{cases} q_t - q_w + N, & q_t < q_w \\ q_t - q_w, & \text{elsewhere} \end{cases}. \tag{21}$$

After finding the values (p_c, q_c), the image can be corrected by setting $(-p_c, -q_c)$.

Figure 7 Watermarked image and retrieved watermark under translation attack (a) vertically and horizontally translated Lena (60 pixels,20 pixels) with (b) retrieved watermark; (c) vertically and horizontally translated Barbara (60,20) with (d) retrieved watermark; (e) vertically translated Lena (128pixels) with (f) retrieved watermark, (g) vertically translated Barbara (128 pixels) with (h) retrieved watermark; (i) horizontally translated Lena (128 pixels) with (j) retrieved watermark; (k) horizontally translated Barbara (128 pixels) with (l) retrieved watermark.

Rotation attack:

The image is rotated by some angle which results in loss of information. The match between rotated image and watermarked image is shown in Figure 8. The angle of rotatin can be found as follows:

Let (i_w, j_w) be the feature point of the watermarked image, and (i_r, j_r) be the same feature point of the rotated image that is rotated by an angle θ with respect to (i_w, j_w). Let the vector point from center to (i_w, j_w) be $\vec{x}$ and vector point from center of rotated image to (i_r, j_r) be $\vec{y}$. If there are M matching feature points, and θ_k is the k^{th} matching point, then the average rotated angle Θ can be expressed in Equation (22).

$$\Theta = \frac{1}{M}\sum_{k=1}^{M}\theta_k \quad , \quad \text{where,} \quad \theta_k = \arccos\left[\frac{\vec{x}.\vec{y}}{|\vec{x}||\vec{y}|}\right] \qquad (22)$$

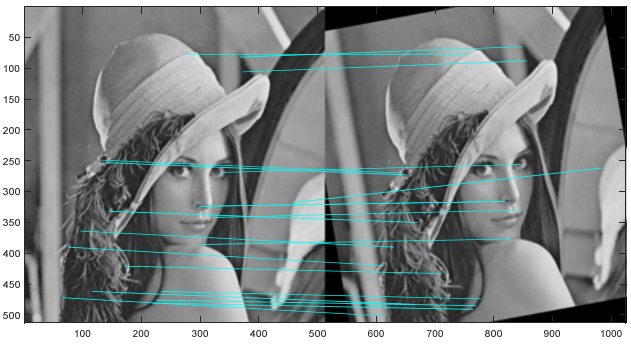


Figure 8 Feature matching between watermarked image (left) and rotation attacked image (right)

Figure 9 Watermarked images and retrieved watermarks under rotation attack, (a) Rotated Lena (20) with (b) retrieved watermark; (c) Rotated Barbara (20) with (d) retrieved watermark; (e) rotated Lena (50) with (f) retrieved watermark; (g) rotated Barbara (50) with (h) retrieved watermark; (i) rotated Lena(100) with (j) retrieved watermark; (k) rotated Barbara (100) with (l) retrieved watermark; (m) rotated Lena (300) with (n) retrieved watermark; (o) rotated Barbara (300) with (p) retrieved watermark; (q) rotated Lena (450) with (r) retrieved watermark; (s) rotated Barbara (450) with (t) retrieved watermark.

B. Performance Analysis & Comparison

Table I shows the rotation attack for Lena and Barbara images on LL3, HL3, LH3 and HH3 sub-bands. It has been observed that embedding watermark in HL3 sub-band give rise to better robustness than any other sub-band in both images. However, the robustness performance (NC values) is very similar irrespective on both images for scaling and translation attacks in all sub-bands. Only the result on LL3 band is represented in Table II as illustration. Table III shows the robustness performance on different combination of attacks. High NC values in all cases shows that the proposed scheme has better ability to withstand multiple attacks.

To evaluate further, the proposed scheme is compared with the two previous schemes presented in [27] and [33]. Table IV shows the robustness performance of our proposed method with Lyu et al.[27] and Zhang et al.[33]. It has been observed that our scheme shows better robustness (i.e., higher NC values in median filtering, JPEG compression, rotation and scaling attacks. However, robustness to centre cropping (25%) attack is relatively poor (i.e. NC=0.2789). The may be due to the partial cropping of the higher significant coefficients in DTT subbands. Still, the extracted watermark of such values can be easily perceived. It has been seen form the experiments that the PSNR values of our scheme are as high as 50 dB for Lena image.

TABLE I ROBUSTNESS PERFORMANCE ON ROTATION ATTACKS ON LENA AND BARBARA IMAGES IN DIFFERENT SUBBANDS.

Rotation angle (in degree)	Lena image			
	LL3 (β=1)	HL3 (β=0.08)	LH3 (β=0.08)	HH3 (β=0.06)
2	0.9741	0.9914	0.3804	0.5575
5	0.8690	0.9932	0.5265	0.7043
10	0.7096	0.9811	0.5810	0.7826
30	0.5020	0.8643	0.6247	0.9058
45	0.4331	0.9303	0.6788	0.8735
	Barbara image			
2	0.9736	0.9924	0.4056	0.8350
5	0.8736	0.9812	0.5633	0.8511
10	0.7169	0.9426	0.6166	0.6434
30	0.4665	0.8175	0.6352	0.4492
45	0.4021	0.8564	0.8360	0.4120

Table V shows the comparative analysis of the proposed scheme with other schemes. Makbol's scheme directly embeds the watermark into the diagonal components of each RDWT sub-band. Though the capacity and robustness improves; the scheme still exhibits false positive problem. Comparing with the above schemes, our proposed scheme shows high watermark capacity, better imperceptibility (shown in Table 1), robust and false positive free. Ali and Ahn's scheme embed principal components of the watermark to avoid false positive problem. Zhang et al. embed 64x64 binary watermark into the LL3 subband of 512x512 image, while Lyu et al. embed 32x32 watermark in all the subbands. Our proposed method embed 256x256 watermark into all the subbands and the quality of the reconstructed watermark is still high. The imperceptibility of the watermarked image is also high. Therefore, comparing with the above schemes, the watermarking capacity of our scheme is quite high.

TABLE II. ROBUSTNESS PERFORMANCE ON SCALING AND TRANSLATION ATTACKS ON LENA AND BARBARA IMAGES

Scaling attack		
Scale	Lena	Barbara
0.25	0.9972	0.9977
0.5	0.9998	0.9998
0.9	0.9996	0.9996
1.2	0.9996	0.9997
Translation attack		
Vertical 60, and horizontal 20 pels	0.9998	1
Vertical 128 pels	1	1
Horizontal 128 pels	1	1

TABLE III. ROBUSTNESS PERFORMANCE ON BARBARA IMAGE IN CASE OF (A) COMBINED ATTACKS AND (B) MIXED ATTACKS

A	Combined attacks	NC values
	Rotation(100)+scale(0.5)	0.6865
	Scale(0.5)+Horizontal translation (128 pixels)	0.9998
	Horizontal translation (128 pixels)+rotation(100)	0.7073
B	Mixed Attacks	
	Horizontal translation(128 pixels)+Gaussian noise(0, 0.05)	0.9030
	Horizontal translation(128 pixels)+S & P noise(0,0.05)	0.9599
	Horizontal translation(128 pixels)+median filter(3x3)	0.9991
	Horizontal translation (128 pixels)+center crop(25%)	0.2488
	Horizontal translation(128 pixels)+JPEG(100)	0.9633
	Scale(0.5)+Gaussian(0,0.05)	0.8753
	Scale(0.5)+S & P noise(0,0.05)	0.9559
	Scale(0.5)+median filter(3×3)	0.9942
	scale(0.5)+center crop(25%)	0.2583
	Scale(0.5)+JPEG(100)	0.9794
	Rotation(100)+Gaussian noise(0, 0.05)	0.7890
	Rotation(100)+Gaussian noise(0, 0.05)	0.7647
	Rotation(100)+median filter(3×3)	0.7068
	Rotation(100)+center crop(25%)	0.2667
	Rotation(100)+JPEG(100)	0.7629

TABLE IV. ROBUSTNESS COMPARISON OF THE PROPOSED SCHEME WITH LYU ET AL.[27] AND ZHANG ET AL. [33] SCHEMES

Attacks	Lyu et al.[27]	Zhang et l.[33]	Ali and Ahn [22]	Makbol and Khoo [17]	Proposed
Median Filtering (3×3)	0.6450	0.9913	0.9100	0.987	0.9992
Centre cropping (25%)	0.9800	0.9179	0.8777	0.2169	0.2789
JPEG(100)	0.9820	0.9966	0.7262	0.9980	0.9580
Rotation (20)	0.9400	0.9741	0.6620	0.9810	0.9914
Rotation(50)	0.9310	0.9813	0.3671	0.4912	0.9932
Rotation(100)	0.8860	0.9861	0.4754	0.5425	0.9811
Scaling(0.9)	0.9560	0.9931	0.9912	0.9485	0.9996
Scaling(1.2)	0.9820	0.9906	0.9949	0.9690	0.9997

C. Comparative Analysis

TABLE V COMPARATIVE ANALYSIS OF THE PROPOSED SCHEME WITH OTHER SCHEMES

Description	Proposed	Makbol & Khoo[17]	Lyu et al.[27]	Zhang et al.[33]	Ali and Ahn[38]
Type of scheme	Blind	Blind	Blind	Blind	Blind
Type of transform	DTT-SIFT-SVD	RDWT-SVD	DWT-SIFT-SVD	DWT-SVD-SIFT	DWT-SVD
Embedding sub-bands	All	All	All	LL3	All
Size of the host image	512×512	512×512	512×512	512×512	512×512
Size of the watermark	256×256	512×512	32x32	64×64	256×256
Tested host image	Lena, Baboon, pepper	Lena, Baboon, Pepper	Lena	Lena, Barbara	Lena, Baboon, Pepper
Type of watermark	Gray	Gray	Binary	Binary	Gray
Scaling factor	0.08(LL), 0.05(LH,HL, HH)	0.05(LL), 0.005(HL, LH,HH)	-	0.05(LL3)	0.08(LL) 0.05(LH, HL, HH)
False positive problem	No	Yes	No	Yes	No

D. False Positive Test

A false positive test is conducted using the proposed method. Figure 10 (a), (b) and (c) shows the original image (512×512), watermarked image (512×512) and watermark image (64×64) respectively. It has been seen that the proposed method can embed the watermark with high PSNR (36.53 dB). A high quality watermark is retrieved (NC=1) shown in Figure 10 (c). A false positive test is conducted by taking Goldhill image (64×64) as watermark shown in Figure 10 (d). It has been seen that by changing values of the original watermark image with Goldhill image, the correct watermark could not be retrieved. The retrieved watermark is shown in Figure 10 (e) with NC=0.0055. Therefore, an adversary cannot retrieve his own watermark and therefore, cannot lay claim of the ownership.

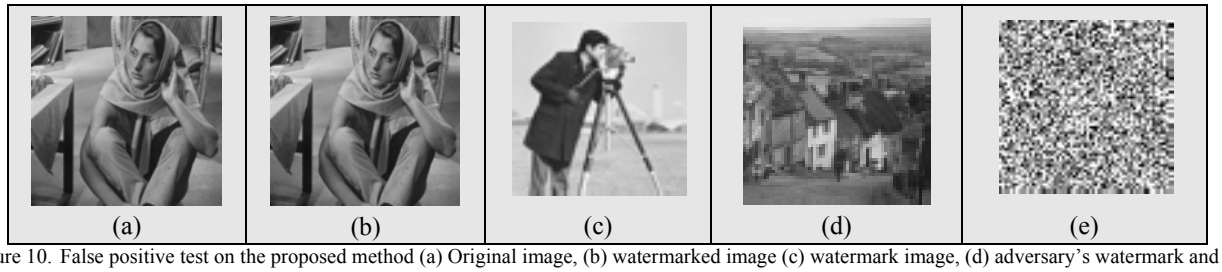


Figure 10. False positive test on the proposed method (a) Original image, (b) watermarked image (c) watermark image, (d) adversary's watermark and (e) adversary's retrieve watermark.

V. CONCLUSIONS

A feature based robust watermarking scheme is proposed in this paper. The scheme combines DTT and SVD to obtain better imperceptibility and robustness. In the proposed scheme the principal components of gray scale watermark of size 64×64 is embedded into the singular values of the DTT coefficients. RST attacks on the host image is corrected to enhance robustness using of SIFT. Extensive experiments show that the proposed scheme can withstand different attacks such as common image processing, malicious attacks and false positive attacks. Notably, compared with other schemes, our scheme provides better imperceptibility and robustness to RST and Combined attacks. Our scheme can be extended to multidimensional images as future work.

REFERENCES

[1] IJ Cox, J Kilian, T Leighton, T Shamoon, Secure spread spectrum watermarking for images, audio and video, IEEE Int. Conf. Image Processing, 3, 243-246, (1996)

[2] WR Bender, D Gruhl, N Morimoto, Techniques for data hiding, in Proceedings of SPIE Storage and Retrieval of Image and Video Databases, 2420, 1995, pp. 164-173.

[3] RG Van Schyndel, AZ Tirkel, CF Osborne, A digital watermark, in Proceedings of IEEE Int. Conf. Image Processing, Austin, TX, USA, II, 1994, pp. 86-90.

[4] J Zhao, E Koch, Embedding robust labels into images for copyright protection, in Proc. of the Int. Cong. on Intell. Property Rights for Special. Info. Knowledge and new Tech., Vienna, (1995), pp. 241-251.

[5] JJKO Ruandaidh, C Dautzenberg, FM Boland, Watermarking digital images for copyright protection, IEE Proceedings-Vision, Image and Signal Processing, 144(4), 250-256, (1996)

[6] JL Divya Shivani, RK Senapati, Robust image watermarking using DTT and Listless SPIHT, Future Internet, 9(3),33 (2017)

[7] JL Divya Shivani, RK Senapati, A based watermarking scheme using DTT, ARPN J. of Engg. and Applied Sciences, 12(11), 3600-3607, (2017)

[8] M Swanson, B Zhu, A Tewfik, Transparent robust image watermarking, in Proc. Int. Conf. on Image Processing, 3, (1996), pp. 211-214

[9] R Wolfgang, E Delp,A watermark for digital images, in Proc. Int. Conf. on Image Processing, 3, (1996), pp. 219-222

[10] IJ Cox, ML Miller, Review of watermarking and the importance of perceptual modeling, in Proceedings SPIE Human Vision and Elect. Imaging II, 3016, 92-99, (1997)

[11] S Lin, CF Chen, A robust DCT-based watermarking for copyright protection, IEEE Trans. Consumer Electron., 46(3), 415-421, (2000)

[12] P Campisi, D Kundur, A Neri, Robust digital watermarking in the ridgelet domain. IEEE Signal Process Lett., 11(10), 826-830, (2004)

[13] P Premaratne, C Ko, A novel watermark embedding and detection scheme for images in DFT domain in 7th international conference on image processing and its applications, Manchester, UK, 1999, pp. 780-783.

[14] CC Lai, CC Tsai, Digital image watermarking using discrete wavelet transform and singular value decomposition, IEEE Trans. Instrum. Meas., 59(11), 3060-3063, (2010)

[15] S Lagzian, M Soryani, M Fathy, A new robust watermarking scheme based on RDWT-SVD, IJIIP Int. J Intel. Inform. Process., 2(1), 22-29, (2011)

[16] H-C Ling, C-W Raphael Phan, S-H Heng, Comment on Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition, Int. J. Electron. Commun. (AEU), 67(10), pp. 894-897, (2013)

[17] NM Makbol, BE Khoo, Robust blind image watermarking scheme based on Redundant discrete wavelet transform and singular value decomposition, Int. J. Electron. Commun. (AEU), 67(2), 2,102-112, (2013)

[18] L Khaled, R Ahmed, Z Khalil, Ambiguity attacks on robust blind image watermarking schemebased on redundant discrete wavelet transform and singular value decomposition, J. Electr. Syst. Inform. Technol, 4(3), 359-368, (2017)

[19] S Rastegar, F Namazi, K Yaghmaie, A Aliabadian, Hybrid watermarking algorithm based on singular value decomposition and randon transform, Int. J. of Electron Commun (AEU), 65 (7), 275-285, (2011)

[20] J-M Guo, H Prasetyo, False-positive-free SVD-based image watermarking, J. Vis. Commun. Image R., 25(5), 1149-1163, (2014)

[21] A Ranade, SS Mahabalarao, S Kale, A variation on SVD based image compression, Image Vision Comput. 25(6), 771-777, (2007)

[22] M Ali, CW Ahn, Comments on optimized gray-scale image watermarking using DWT-SVD and Firefly algorithm, Expert Systems with Applications, 42(5), 2392-2394, (2015)

[23] E Ganic, AM Eskicioglu, Robust embedding of visual watermarks using discrete wavelet transform and singular value decomposition, J Electronic Imaging, 14(4), 1-13 (2005)

[24] D G Lowe, Object recognition from local scale-invariant features. In proceedings of the 7th IEEE Int. conf on computer vision, Kerkyra, Greece, 20-27 sept 1999; pp. 1150-1157.

[25] H. K. Lee, H. Kim, H.Y.Lee, Robust image watermarking using local invariant features. Opt. Eng. 2006, 45, 535-545.

[26] H.J. Luo, X.M.Sun, H.F.Yang, Z.H.Xia, A Robust image watermarking based on image restoration using SIFT. Radio Eng. 2011, 20, 525-532.

[27] W. L. Lyu, C.C. Chang, T.S.Nguyen, C.C.Lin, Image watermarking scheme based on scale-invariant feature transform. KSII Trans. Internet Inf. Syst. 2014, 8, 3591-3606.

[28] C.G. Thorat, B.D.Jadav, A blind digital watermark technique for color image based on integer wavelet transform and SIFT. Porcedia Comput. Sci. 2010,2,236-241.

[29] V.Q.Pham, T. Miyaki, T. Yamasaki, K. Aizawa, Geometrically invariant object based watermarking using SIFT feature. In Proceedings of the 14th IEEE Int. Conf. on Image Process, San Antorio, TX, USA, 16-19 Sept 2007. Pp. 473-476.

[30] X.C.Yuan, C.M.Pun, Feature extraction and local Zernike moments based geometric invariant watermarking, Multimedia Tools Appl. 2014, 72, 777-799.

[31] C.P.Wang, X.Y. Wang, Z.Q.Xia, Geometrically invariant watermarking scheme based on fast radial harmonic fourier moments, Signal Process. Image Commun, 2016, 45, 10-23.

[32] E.D.Tsougenis, G.A.Papakostas, D.E.Koulouriotis, V.D.Tourassis, Performance evaluation of moment-based watermarking methods: A review. J. Syst. Software. 2012, 85, 1864-1884.

[33] Y. Zhang, C. Wang and X. Zhou, RST resilient watermarking scheme based on DWT-SVD and SIFT, algorithms, 2017, 10(2), 41.