SIViP (2014) 8:859–872
DOI 10.1007/s11760-012-0312-6

ORIGINAL PAPER

A robust watermark authentication technique based on Weber's descriptor

Ekta Walia · **Anu Suneja**

Received: 25 June 2011 / Revised: 3 April 2012 / Accepted: 7 April 2012 / Published online: 5 May 2012

Abstract One of the major challenges in the field of digital image watermarking is to authenticate the presence of watermark in the watermarked image even after it has been transformed intentionally or unintentionally. Transformation can be geometric-like rotation, scaling, and translation of image or may be due to any signal processing attack like noise corruption, compression, and cropping of image. There may also be some photometric changes, for example change in the brightness of watermarked image during transmission, due to which it becomes difficult to validate whether received image is watermarked or not. Illumination invariance property of Weber's descriptor has engrossed to use it in the proposed watermark authentication technique. Weber's descriptor is a descriptor based on two parameters of a pixel, differential excitation and orientation. These parameters are computed using the relative intensity value of neighbor pixels and current pixel. This descriptor remains the same even after intensity changes due to the contribution of all neighbor pixel's intensity in its computation. It is also known to be robust to scaling and rotation. Experimental results show that the proposed watermarking technique is able to authenticate the presence of watermark in the watermarked image even when it is distorted due to geometric and photometric attacks. In addition to this, it is found to be robust against noise, cropping, and compression attacks.

E. Walia
Department of Computer Science, South Asian University,
New Delhi, India
e-mail: wekta@yahoo.com

A. Suneja (✉)
MMICT&BM Department, Maharishi Markandeshwar University,
Mullana, Ambala, Haryana, India
e-mail: anusuneja3@gmail.com

Keywords Illumination invariance · Dense descriptors · Watermarking · Weber's descriptor

Symbols

η	Normalized coefficient of correlation
ρ	Euclidean distance
χ	Differential excitation
λ	Orientation
δ_p	Dominant orientation in pth bin
P	Number of dominant orientation bins
$D_{i,p,b}$	Weber's descriptor of watermarked image
$f(x, y)$	Host image
Q_e	Quantization to nearest even value
Q_o	Quantization to the nearest odd value
$F(u, v)$	DCT coefficient at position (u, v)
Δ	Scaling quantity
μ	Mean of Gaussian noise
σ^2	Variance of Gaussian noise

1 Introduction

Watermarking is a very extensively used copyright protection technique for digital images, audio, or video information. A prominent watermarking technique should be able to authenticate the existence of watermark pattern in a watermarked image even after it has been distorted. Watermark information can either be embedded in the global region or in the local region of the host image. In global watermarking, watermark information can be embedded anywhere in the entire image and global features of the host image are used for watermark insertion. Watermarking scheme that modifies Zernike moments [1] of entire image is an example of global watermarking technique. In local watermarking techniques, RST(rotation, scaling, and translation) invariant feature points are located initially and then watermark is embedded in the regions around these feature points. For example, in SIFT(scale invariant feature transform)-based techniques, key points are obtained around which the watermark is embedded.

A number of watermarking techniques based on feature points and descriptors have been proposed by many researchers. These descriptors are classified into two categories: first category relates to the sparse descriptors and second is the dense descriptors [2–4]. In sparse descriptors, first, feature points are located and then descriptor is designed patch wise around them. SIFT descriptor proposed by Lowe [5] falls in this category and is very commonly used in watermarking.

A number of watermarking techniques based on SIFT feature points have been proposed in the literature [6–11]. Tang and Hang [12] devised a synchronization scheme that uses Mexican hat wavelet for intensity-based feature extraction and image normalization. Due to the sensitivity of normalization to the image contents, robustness of these patches degrades when the watermarked image is distorted. Dajun et al. [13] have proposed an object-based video authentication system in which a set of angular radial transformation coefficients is selected as feature to represent the video object and the background. Li et al. [14] have presented a blind robust image watermarking scheme based on Harris interest points for generating some non-overlapped circular regions. Watermark bits are inserted into these circular regions by quantizing PZMs (pseudo Zernike moments) of that region. The drawback of all feature point-based watermarking techniques is that many of the extracted feature points from the original image and distorted images do not match, due to which it is not possible to extract watermarked bits exactly.

In dense descriptors, features are computed for every pixel and information is stored in the form of a histogram. Weber's descriptor [2], LBP (local binary pattern) [3], and Gabor wavelets [4] fall in the category of dense descriptors. In [3], authors present a scheme to protect biometric templates using LBP-based watermark authentication. First, the m-LSB (least significant bit) of biometric templates is set to zeros. Then, the modified biometric templates are partitioned into non-overlapping image blocks, whose LBP features are obtained, and the authentication watermark bits are generated from these features.

Descriptors of an image can also be categorized on the basis of methods used to represent the characteristics of the image. These are [15]: distribution-based descriptors, spatial-frequency-based descriptors, and differential descriptors. Distribution-based descriptors use histograms to represent different characteristics of the profile of a digital image.

Lazebnik et. al [16] have proposed an intensity-based rotation invariant descriptor that is based on spin image, which is a 2D histogram based on intensity domain and represents the allocation of intensity values of the pixels of image in an affine-normalized patch. SIFT descriptor proposed by Lowe [5] also falls in the category of distribution-based descriptors. It is a 3D histogram of gradient location and orientation and is of dimension $128(4 \times 4 \times 8)$. Mikolajczyk et al. [15] have proposed an extension of the SIFT called GLOH(Gradient location-orientation histogram) descriptor, which is designed to increase the robustness and uniqueness of SIFT. The drawback of GLOH descriptor [15] is that it is only scale invariant and not affine invariant. Ke and Sukthankar [17] have used PCA(principal component analysis)-SIFT descriptor to define features of an image. It however does not work well for blurred images.

Spatial-frequency-based descriptors define a descriptor with the frequency content of an image. In differential descriptors, a set of image derivatives are computed up to a given order that approximates neighborhood of a pixel. In these descriptors, components of the local derivatives are combined to obtain rotation invariance.

One of the major challenges in existing watermarking techniques is the synchronization problem, in which the position of embedded watermark gets changed in watermarked image due to rotation, scaling, or translation [18]. In this paper, our focus is on finding the solution of watermark synchronization problem and to authenticate the watermarked image even if it is not clear, due to change in brightness or blur effect. The proposed watermarking technique is based on the descriptor defined according to Weber's law. This descriptor is designed in a way such that it is robust against geometric and photometric attacks [2], and thus overcome the problem of synchronization in watermarked images and authenticate the watermark from distorted watermarked image. In addition to this, it is known to be computationally efficient than SIFT descriptor, which is one of the prominent methods of watermark authentication. The paper is organized as: Sect. 2 gives an overview of Weber's descriptor and method for finding the descriptor. In Sect. 3, steps for proposed watermark authentication technique are given. In Sect. 4, the experimental results are given, and in Sect. 5, analysis of the Weber's descriptor for watermark authentication has been given. It also presents a detailed comparison of the proposed approach with SIFT and LBP-based watermark authentication schemes. Conclusions are presented in Sect. 6.

2 Weber's descriptor

Weber's descriptor proposed by Chen et al. [2] is the descriptor based on the Weber's law that states that the ratio of the increment threshold to the background intensity is constant [19]. Weber's descriptor is defined on the basis of two components: differential excitation (χ) and orientation (λ) of a

Fig. 1 Neighboring order of pixel *I*

I_0	I_1	I_2
I_7	I	I_3
I_6	I_5	I_4

pixel. To compute the differential excitation value of pixel $(x_{i,}y_i)$, its difference with intensity of eight neighbors is computed and then the ratio of differences to the intensity of the current pixel is evaluated. As given in Eq. (1), inverse tangent is then applied on this ratio.

$$\chi(x_i, y_i) = \arctan\left(\sum_{j=0}^{n-1} \frac{I_j - I_i}{I_i}\right) \tag{1}$$

where I_i is the intensity of the current pixel $(x_{i,}y_i)$, n is the number of neighbors(which is taken to be eight here) and I_j is the intensity of jth neighbor pixel. Value of $\chi(x_i, y_i)$ lies in the range $[-\pi/2, \pi/2]$. If both numerator and denominator in this ratio evaluate to zero, then differential excitation $\chi(x_i, y_i)$ is taken as zero.

Orientation of pixel $(x_{i,}y_i)$ is computed using Eq. (2):

$$\lambda(x_i, y_i) = \arctan\left(\frac{I_7 - I_3}{I_5 - I_1}\right) \tag{2}$$

where I_1, I_3, I_5, and I_7 are 1st, 3rd, 5th, and 7th neighbor of ith pixel, respectively, which are defined in the order shown in Fig. 1.

After computing orientation λ, it is mapped to λ' using Eq. (3), such that λ' lies in between the interval $[0, 2\pi]$.

$$\lambda' = \arctan 2\left(\frac{I_7 - I_3}{I_5 - I_1}\right) + \pi \tag{3}$$

Then, λ' is quantized into "P" number of dominant orientation bins using Eq. (4):

$$\delta_p = \frac{2p}{P}\pi \tag{4}$$

where "p" is computed using Eq. (5):

$$p = \bmod\left(\left\lfloor \frac{\lambda'}{2\pi/P} + \frac{1}{2} \right\rfloor, P\right) \tag{5}$$

Here, "mod()" function returns the remainder when first argument is divided by the second argument.

A 2D histogram is computed using λ' and χ of all the pixels of given image, where each column of 2D histogram consists of dominant orientation δ_p and each row consists of differential excitation values. Each column of this 2D histogram is then stored in an individual 1D histogram such that the excitations of all the pixels having same dominant orientation are grouped in same 1D histogram. After dividing 2D histogram into 1D histograms, each 1D histogram is further divided into "N" number of sub-histograms, where each sub-histogram has a LB (lower bound) and UB (upper bound), which is calculated using Eq. (6):

$$\left.\begin{aligned} \mathrm{LB}_i &= \left(\tfrac{i}{N} - \tfrac{1}{2}\right)\pi \\ \mathrm{UB}_i &= \left[\left(\tfrac{i+1}{N}\right) - \tfrac{1}{2}\right]\pi \end{aligned}\right\} \tag{6}$$

Here, LB_i and UB_i are the lower bound and upper bound of ith sub-histogram, $i \in [0, N-1]$, and N is the total number of sub-histograms.

Each sub-histogram is further divided into "B" number of bins using Eq. (7):

$$D_{i,p,b} = \sum_r \Delta(B_r == b) \tag{7}$$

where $b = 0, 1, 2, \ldots\ldots\ldots, B-1$, and $r = 0, 1, 2.\ldots\ldots M-1$, M is the number of excitations in ith sub-histogram of pth dominant orientation, B_r is computed using Eq. (8), and $\Delta(.)$ is delta function defined using Eq. (9).

$$B_r = \left\lfloor \frac{\chi_r - \mathrm{LB}_i}{\mathrm{UB}_i - \mathrm{LB}_i} + \frac{1}{2} \right\rfloor \tag{8}$$

$$\Delta(\text{Condition}) = \begin{cases} 1, & \text{if condition is true} \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

$D_{i,p,b}$ is the final descriptor for the given image.

3 Proposed watermark authentication based on Weber's descriptor

In the proposed watermark authentication technique, watermark bits are embedded in the host image using modification of DCT coefficient [20] of selected 8 × 8 pixel blocks.

The steps followed in the watermark insertion are:

1. The host image $f(x, y)$ is divided into a number of 8×8 pixels blocks.
2. DCT transformation is applied on each block and their DCT coefficients are computed.
3. Watermark bits to be embedded are also divided in the subgroups of sixteen bits(4×4) each.
4. With the help of a key '$k1$', a number of random blocks are selected according to the required size of watermark to be inserted in these blocks.
5. First sixteen low frequency DCT coefficients(excluding DC component) of first block in random sequence are selected in zig zag order.
6. First subgroup of watermark bits are embedded in the coefficients selected in step 5 using Eq. (10)

$$\left.\begin{aligned} F(u,v) &= \Delta Q_e\left(\tfrac{F(u,v)}{\Delta}\right) && \text{if } b_i = 1, \\ F(u,v) &= \Delta Q_o\left(\tfrac{F(u,v)}{\Delta}\right) && \text{if } b_i = 0 \end{aligned}\right\} \tag{10}$$

Fig. 2 Proposed watermark authentication algorithm

```
1. Begin
2. Load the host image I and watermark bits $b_i$.
3. Embed the bits $b_i$ in the host image I using DCT coefficient modification
   technique and store the watermarked image as WI.
4. Compute the Weber descriptor D of watermarked image WI using the
   method given in Section 2. Store it in some register file together with key
   'k1' and encrypt this file using AES.
5. At receiver end, assume that WI has been transformed into WI' due to
   some signal processing attack (e.g. Geometric Attack, Photometric
   attack etc.).
6. Compute the Weber descriptor D' for the received image WI'.
7. Decrypt the register file using AES and find Normalized Coefficient of
   Correlation( $\eta$ ) and Euclidean distance ( $\rho$ ) using Eq.(11) and Eq.(12)
8. If ( $\eta > T_1$ )AND( $\rho < T_2$ )then
           Image is authenticated as watermarked image
   else
           Image is not authenticated as watermarked image
9. End
```

where Q_e is the quantization to nearest even value and Q_o is the quantization to the nearest odd value, $F(u, v)$ is the DCT coefficient at position (u, v), b_i is the watermark bit to be embedded and Δ is the scaling quantity.

7. Steps 5 and 6 are repeated for all the randomly selected blocks until all the watermark bits are embedded.

Followed by the bits insertion, Weber's descriptor of the watermarked image is computed and stored in some register file together with key "$k1$." The register file is encrypted using a symmetric encryption method, that is, AES(advanced encryption standard) [21], which needs a shared secret key to be exchanged between the sender and the receiver. The exchange of secret key is accomplished by using asymmetric RSA [22] key exchange technique. The secret key used by AES is encrypted by the sender using the public RSA key. At the receiver's side, receiver uses its private RSA key to obtain the secret key of AES and decipher the register file using this secret key. At the receiver end, the descriptor of received watermarked image is matched with the decrypted register file to authenticate the watermarked image. Normalized coefficient of correlation (η) and Euclidean distance (ρ) are used to perform matching of stored and received descriptors. Value of η is computed using Eq. (11) [12,23] and ρ is computed using Eq. (12) [24].

$$\eta = \sum_{i=0}^{C-1} \frac{D(i) * D'(i)}{\sqrt{\sum_{i=0}^{C-1} D^2(i)}\sqrt{\sum_{i=0}^{C-1} D'^2(i)}} \tag{11}$$

where D is the descriptor of watermarked image stored in register file after watermark insertion, and D' is the descriptor of transformed watermarked image, and C is the size of descriptor.

$$\rho = \sqrt{\sum_{i=1}^{C} (D'(i) - D(i))^2} \tag{12}$$

If the value of η is greater than some threshold value (T_1) and the value of ρ is below some threshold value (T_2), then the received image is confirmed as watermarked image. The algorithm used for proposed watermarking technique is given in Fig. 2.

The flow diagram of the procedure followed in the insertion and authentication of watermark in the proposed technique is shown in Fig. 3a, b.

4 Experimental results

To evaluate the performance of the proposed watermark authentication technique using Weber's descriptor, gray level images of different nature have been used [25] as host images. These are the standard images having different characteristics like "*Woman*" is a low-contrast image, "*Lena*" is a high-contrast image, "*Pepper*" is a continuous tone image, "*Mandrilla*" is an image of discrete tone image category, and "*Cameraman*" is an image with sharp and clear edges. Through exhaustive experimentation, it has been proved that the proposed watermark authentication technique is able to authenticate the watermarked image of any nature. Different watermark bit patterns have been inserted using DCT coefficient modification technique [20] described in Sect. 3. The

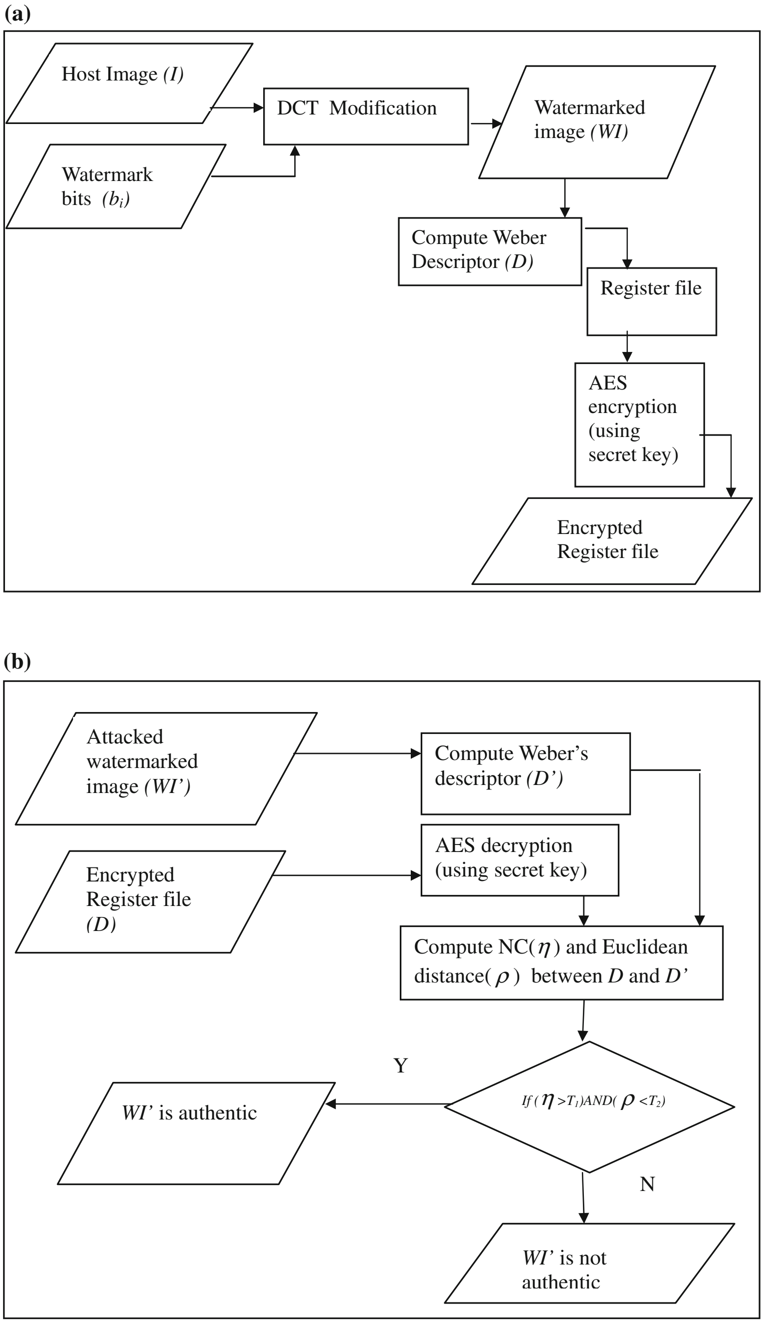
(a)
Host Image (I)
DCT Modification
Watermarked image (WI)
Watermark bits (b_i)
Compute Weber Descriptor (D)
Register file
AES encryption (using secret key)
Encrypted Register file
(b)
Attacked watermarked image (WI')
Compute Weber's descriptor (D')
Encrypted Register file (D)
AES decryption (using secret key)
Compute NC(η) and Euclidean distance(ρ) between D and D'
Y
If (η>T_1)AND(ρ<T_2)
WI' is authentic
N
WI' is not authentic

Fig. 3 **a** Flow diagram for watermark insertion, **b** flow diagram for watermark authentication

host images of 32 × 32 pixels and watermarked images are shown in Fig. 4. It is clear from Fig. 4 that we are referring to invisible watermarking.

The PSNR (peak signal-to-noise ratio) between 8-bit gray scale host image and watermarked image is computed using Eq. (13) [4].

$$\text{PSNR} = \frac{10\log_{10}(255^2)}{\frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - WI(i,j)]^2} \tag{13}$$

where I and WI are the host and watermarked images, respectively. Each of them is of size $m \times n$.

The average value of PSNR between host image and watermarked images shown in Fig. 4 is 40.17 db for 256 watermark bits. The value of PSNR for watermark of different sizes is given in Table 1.

PSNR should be greater than or equal to 40 for better transparency of watermarked image [26] and the proposed technique returns the desired PSNR. It clearly signifies that the proposed technique (except for the case of 1,024 bits,

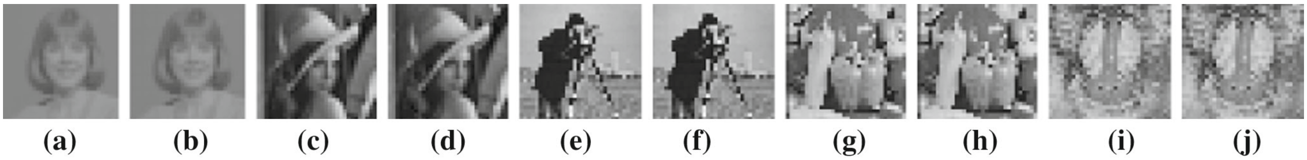

Fig. 4 **a–b** Host and watermarked image "*Woman*", **c–d** host and watermarked image "*Lena*", **e–f** host and watermarked image "*Cameraman*", **g–h** host and watermarked image "*Pepper*", **i–j** host and watermarked image "*Mandrilla*"

Table 1 Value of PSNR for different sized watermark patterns

Watermark bits	Average PSNR (db)
1,024 bits	38.75
512 bits	39.62
256 bits	40.17
128 bits	43.14
64 bits	46.12
32 bits	49.06

where PSNR is quite close to 40db) has better transparency even for large number of watermark bits.

It is observed from Table 1 that a large number of bits can be inserted in the 64 × 64 pixels host image without degrading the visual quality of the watermarked image. The maximum number of bits that can be inserted using the proposed technique is 16 times the number of 8 × 8 sized DCT blocks (*nblocks*) of the host image, which can be calculated using Eq. (14).

$$\text{nblocks} = \frac{\text{size of Host Image}}{8 \times 8} \times 16 \tag{14}$$

Thus, maximum number of bits that can be inserted without degrading the quality of image are 1,024 bits for 64 × 64 image. As the size of host image increases, the maximum number of bits that can be inserted also increases.

A number of experiments have been performed to analyze the performance of the proposed watermark authentication technique, and it has been observed that the Weber's descriptor-based watermark authentication technique is very much robust against all the geometric and photometric attacks. To find the similarity between transmitted watermarked and received watermarked image after a possible attack, normalized coefficient of correlation (η) and the Euclidean distance between two histograms (ρ) are computed. In this set of experiments, threshold value T_1 for η is set to 0.7 and T_2 for ρ is set to 107. If the factor η is greater than equal to T_1 and factor ρ is less than T_2, received image is authenticated as watermarked image otherwise not.

As per the survey done by Kutter and Petitcolas [25], the attacks against which watermarking system should be judged are geometric attacks which include horizontal flip, rotation, cropping ; enhancement attacks like sharpening and low-pass filtering; and noise addition which can corrupt the watermarked image to great extent. Watermarking systems are also tested against JPEG compression. In the following subsections, we give detailed behavior of our proposed approach against all these variations.

4.1 Geometric attacks

4.1.1 Effect of rotation

To analyze the robustness of proposed watermarking technique against rotation, all the watermarked images are have been rotated at various angles in MATLAB 7.0 using bilinear interpolation and cropping method. We have rotated only that part of watermarked images, which is inside the disk. This has been shown in Fig. 5.

It has been observed using experiments that the descriptor of the rotated watermarked image is close to the descriptor of the original watermarked image. Values of η and ρ for the rotated images (shown in Fig. 5) are summarized in Table 2.

The difference in descriptor of rotated and original watermarked image is due to the fact that intensity values of rotated images are not exactly equal to the intensity value of original images. This attributes to the fact that there is computation error in the algorithm used to rotate the images.

4.1.2 Effect of flipping

To analyze the robustness of proposed watermark authentication technique against flipping operation, watermarked images are flipped both horizontally and vertically in Paint Shop Pro 5.0 [27]. The flipped watermarked images are shown in Fig. 6.

Values of the factors η and ρ for the flipped watermarked images shown in Fig. 6 are summarized in Table 3.

It has been observed that Weber's descriptor is robust against flipping attack for both horizontal as well a vertical flipping.

4.1.3 Effect of cropping

Watermarking based on Weber's descriptor is also robust against cropping attack. Vertical and random cropping are applied to the images. These cropped images (shown in

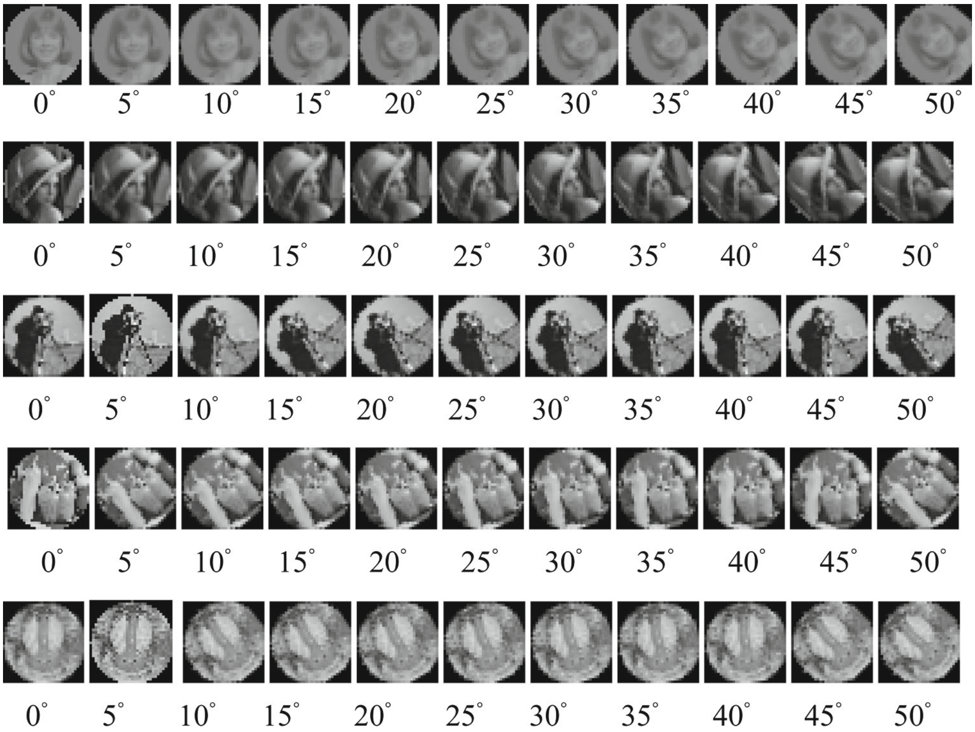

Fig. 5 Rotated watermarked images at different angles

Table 2 Comparison of original watermarked image and rotated watermarked images

S. No.	Angle of rotation	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
		ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
1	5°	61.61	0.94	52.42	0.94	58.10	0.93	65.65	0.90	64.64	0.89
2	10°	61.61	0.94	54.97	0.93	61.74	0.92	59.75	0.93	54.85	0.92
3	15°	65.48	0.93	58.82	0.92	58.29	0.93	57.93	0.93	62.05	0.90
4	20°	69.53	0.93	56.36	0.93	60.33	0.92	64.92	0.91	58.89	0.91
5	25°	70.80	0.92	62.74	0.91	59.33	0.92	65.73	0.90	59.65	0.91
6	30°	67.38	0.93	67.27	0.82	64.88	0.90	65.89	0.90	59.51	0.91
7	35°	67.28	0.93	65.05	0.90	63.87	0.90	72.40	0.87	61.11	0.90
8	40°	80.98	0.90	70.76	0.88	63.70	0.91	83.62	0.83	68.10	0.87
9	45°	78.00	0.90	78.47	0.85	66.18	0.89	86.60	0.81	64.25	0.89
10	50°	80.72	0.90	86.66	0.81	64.17	0.90	92.15	0.78	65.13	0.89

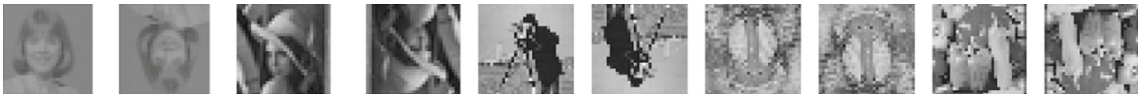

Fig. 6 Flipped watermarked images

Table 3 Comparison of original watermarked image and flipped watermarked images

S. No.	Direction of flipping	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
		ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
1	Horizontal	54.82	0.93	61.3	0.92	43.77	0.83	16.02	0.91	45.25	0.70
2	Vertical	51.09	0.94	56.1	0.94	28.24	0.93	45.34	0.86	40.19	0.79

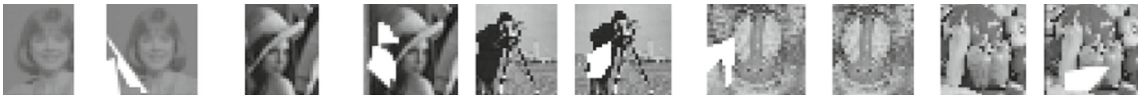

Fig. 7 Cropped watermarked images

Table 4 Comparison of original watermarked image and cropped images

S. No.	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
	ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
1	81.61	0.93	65.85	0.86	42.23	0.88	29.69	0.94	33.94	0.76
2	43.41	0.98	49.34	0.86	66.64	0.75	64.74	0.73	65.81	0.85

Table 5 Comparison of original watermarked image and scaled-up images

	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
	ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
Scaling by factor of 2	31	0.98	49	0.94	31	0.91	37.5	0.9	48	0.82
Scaling by factor of 4	46	0.86	58	0.91	49.2	0.87	54.5	0.79	50	0.81

Table 6 Comparison of original watermarked and translated images

	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
	ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
Translation about centroid	35	0.97	35	0.98	52.9	0.81	33.5	0.92	33	0.86

Fig. 7) are then used to analyze the robustness of the proposed watermark authentication technique. The similarity of these cropped images with original watermarked image is given in Table 4.

4.1.4 Effect of scaling

To make Weber-based watermarking scale invariant, scale normalization [9] is used. In scale normalization, the watermarked image is scaled to a predefined size. Then, descriptor of the scaled image is compared with the descriptor stored in register file to authenticate the watermarked image. To analyze the robustness of proposed technique against scale variation, watermarked images shown in Fig. 4 have been scaled up with factor of 2 and 4. These scaled up images are then normalized to standard size of 32 × 32 pixels and their descriptors are compared with the descriptor stored in register file to find the value of η and ρ as shown in Table 5. From Table 5, it is concluded that the proposed method is scale invariant.

4.1.5 Effect of translation

The proposed watermark authentication technique is also robust against translation. To analyze the effect of translation, we have translated the watermarked image 16 pixels along x-axis and 16 pixels along y-axis for 32 × 32image using 2D translation. The values of η and ρ obtained from the normalized translated image are shown in Table 6.

4.2 Noise addition

To analyze the robustness of proposed watermark authentication technique against noise attack, the Gaussian noise with different mean and variance has been added to different watermarked images in MATLAB 7.0. The noise attacked images are shown in Fig. 8.

Values of the factors η and ρ for the watermarked images (shown in Fig. 8) are summarized in Table 7.

It has been observed from the values of correlation coefficient that the effect of noise is more on low-contrast images like "*Woman*" as compared to high-contrast images. Despite this, the proposed method is able to successfully authenticate all the noisy images.

4.3 Enhancement techniques

4.3.1 Effect of brightness/contrast change

With the help of thorough experimentation, it has been proved that Weber's descriptor is very much robust against intensity variation. To analyze the robustness of proposed watermark authentication technique against intensity variation, brightness of watermarked images has been changed in Adobe Paint Shop Pro 5.0. The watermarked images with change in brightness are shown in Fig. 9.

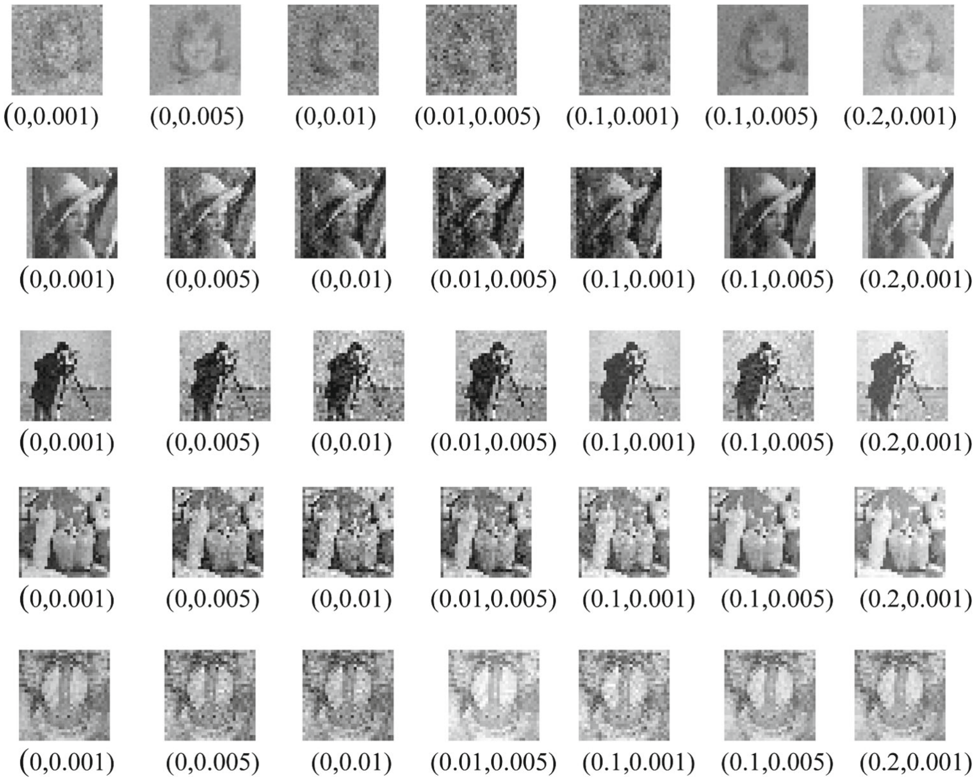

Fig. 8 Watermarked images after noise attack with different mean and variance

Table 7 Comparison of original watermarked image and noise attacked images

S.No.	Mean and variance of Noise (μ, σ^2)	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
		ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
1	(0,0.001)	51.09	0.72	48.31	0.90	43.49	0.81	52.23	0.79	25.88	0.88
2	(0,0.005)	73.91	0.73	65.98	0.83	67.88	0.76	72.56	0.74	50.71	0.77
3	(0,0.01)	87.23	0.70	76.11	0.80	85.14	0.71	89.33	0.71	60.39	0.76
4	(0.01,0.005)	75.35	0.71	72.12	0.81	74.06	0.78	69.62	0.72	42.84	0.72
5	(0.1,0.001)	93.81	0.76	56	0.89	49.39	0.74	47.89	0.83	86.42	0.70
6	(0.1,0.005)	50.81	0.78	66.43	0.82	62.88	0.76	58.79	0.73	44.02	0.76
7	(0.2,0.001)	82.19	0.75	81.08	0.72	48.04	0.75	45.16	0.85	42.75	0.79

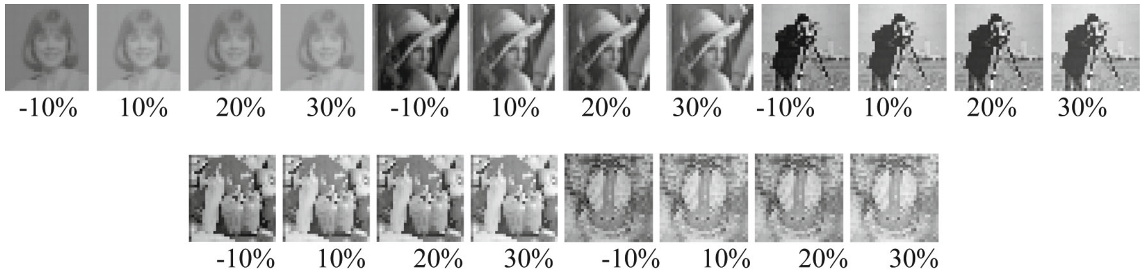

Fig. 9 Watermarked images after change in brightness with different factors

Values of factors η and ρ for the watermarked images with increased and reduced brightness (shown in Fig. 9) are summarized in Table 8.

It has been observed from the values of correlation coefficient given in Table 8 that high-contrast images like "*Lena*" are more affected with change in brightness as compared

Table 8 Comparison of original watermarked image and watermarked image with change in brightness

S. No.	Change in brightness/contrast (%)	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
		ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
1	Reduced (10)	11.14	1	23.4	0.98	22.13	0.99	13.65	0.98	13.63	0.96
2	Increased (10)	11.58	1	20.9	0.98	16.18	0.98	13.71	0.98	13.56	0.96
3	Increased (20)	16.25	1	39.5	0.91	22.84	0.95	11.91	0.99	21.58	0.90
4	Increased (30)	24.78	0.99	49.3	0.86	28.63	0.92	28.53	0.94	36.94	0.83

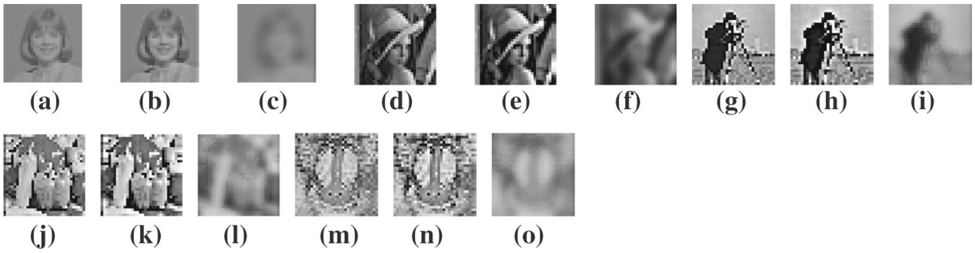

Fig. 10 Watermarked images after change in sharpness

Table 9 Comparison of original watermarked image and image with increased sharpness

S. No.	Change in sharpness	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
		ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
1	Sharpen	52.73	0.96	54.7	0.85	32.19	0.92	53.58	0.87	56.06	0.84
2	More sharpen	93.2	0.84	71.7	0.76	43.38	0.85	72.95	0.78	93.17	0.76
3	Blurred image	80.29	0.94	72.7	0.91	60.26	0.77	52.13	0.83	67.09	0.88

Table 10 Comparison of original watermarked image and compressed images

S. No.	Quality factor for compressed Image	"*Woman*"		"*Lena*"		"*Cameraman*"		"*Pepper*"		"*Mandrilla*"	
		ρ	η	ρ	η	ρ	η	ρ	η	ρ	η
1	1	77.64	0.9	56.15	0.81	39.11	0.87	57.16	0.74	69.87	0.70
2	5	70.34	0.92	56.87	0.8	37.33	0.87	52.51	0.79	36.79	0.76
3	8	73.76	0.94	56.92	0.8	28	0.93	32.46	0.92	28.77	0.83

to low-contrast images. All such variations are successfully handled by the proposed method.

4.3.2 Effect of change in sharpness

To analyze the robustness of proposed watermark authentication technique against increased sharpness, sharpen and more sharpen operations (of Paint Shop Pro 5.0) are applied on the watermarked image. The watermarked image "*Woman*" with increased sharpness is shown in Fig. 10a, b. The same image with decreased sharpness has also been shown in Fig. 10c. The same trend follows for all other images in Fig. 10.

Values of factors η and ρ for the watermarked image with change in sharpness (shown in Fig. 10) are summarized in Table 9.

It has been observed that Weber's descriptor is able to authenticate the watermarked image even when the watermarked image is blurred and also does so when its sharpness is increased by using sharpen and more sharpen operations.

4.4 Effect of JPEG compression

The proposed technique is also found to be robust against JPEG compression. To analyze it, the watermarked images shown in Fig. 4b, d, f, h, and j are compressed with quality factors of 1, 5, and 8, and ρ and η for such images have been computed and depicted in Table 10.

4.5 Effect of parameters P, N, and B

Value of these parameters should neither be too small or nor be too large [2]. If the values of P, N, and B are very large, then the size of histogram will be large and accordingly the descriptor will become more discriminable but the number of values in each bin will become small, so reliability of histogram will be reduced. If the values of P, N, and B are very small, then each bin will have very large value and descriptor will become more reliable but size of histogram will also become small, so it will become less discriminable.

Table 11 Mean and Variance of NC(η) for random bit patterns

Attack type	*Bit pattern 1*		*Bit pattern 2*		*Bit pattern 3*	
	$\mu(\eta)$	$\sigma^2(\eta)$	$\mu(\eta)$	$\sigma^2(\eta)$	$\mu(\eta)$	$\sigma^2(\eta)$
Rotation 5°	0.92	0.0004	0.87	0.0004	0.87	0.0006
10°	0.93	0.0001	0.86	0.0002	0.85	0.0004
15°	0.92	0.0001	0.85	0.0000	0.84	0.0000
20°	0.92	0.0001	0.86	0.0000	0.85	0.0001
25°	0.91	0.0001	0.85	0.0000	0.85	0.0001
30°	0.89	0.0014	0.85	0.0002	0.84	0.0002
35°	0.90	0.0004	0.84	0.0006	0.83	0.0004
40°	0.88	0.0008	0.85	0.0009	0.84	0.0009
45°	0.87	0.0011	0.86	0.0009	0.87	0.0006
50°	0.86	0.0026	0.84	0.0014	0.85	0.0017
Horizontal flipping	0.86	0.0075	0.82	0.0038	0.82	0.0035
Vertical flipping	0.89	0.0035	0.86	0.0013	0.85	0.0014
Vertical crop	0.87	0.0041	0.85	0.0021	0.86	0.0004
Random crop	0.83	0.0080	0.81	0.0033	0.81	0.0029
Scaling by factor of 2	0.91	0.0028	0.86	0.0005	0.85	0.0005
Scaling by factor of 4	0.85	0.0019	0.82	0.0010	0.84	0.0017
Translation about centroid	0.91	0.0042	0.85	0.0004	0.86	0.0003
Noise(0, 0.001)	0.81	0.0041	0.79	0.0022	0.81	0.0039
Noise(0, 0.005)	0.77	0.0015	0.77	0.0041	0.79	0.0028
Noise(0, 0.01)	0.73	0.0017	0.73	0.0019	0.73	0.0017
Noise(0.01, 0.005)	0.76	0.0017	0.76	0.0017	0.78	0.0051
Noise(0.1, 0.001)	0.81	0.0035	0.81	0.0039	0.83	0.0030
Noise(0.1, 0.005)	0.77	0.0011	0.81	0.0012	0.79	0.0018
Noise(0.2, 0.001)	0.77	0.0024	0.72	0.0028	0.77	0.0020
Brightness decreased 10 %	0.99	0.0001	0.89	0.0038	0.89	0.0043
Brightness increased 10 %	0.99	0.0001	0.89	0.0038	0.89	0.0043
Brightness increased 20 %	0.96	0.0013	0.89	0.0038	0.89	0.0042
Brightness increased 30 %	0.93	0.0022	0.87	0.0002	0.86	0.0003
Compression	0.83	0.0037	0.80	0.0016	0.82	0.0031
(Quality factor = 1)	0.85	0.0028	0.81	0.0007	0.81	0.0005
Compression	0.90	0.0032	0.85	0.0010	0.84	0.0010
Sharpen	0.90	0.0018	0.84	0.0007	0.83	0.0005
More sharpen	0.81	0.0015	0.80	0.0015	0.83	0.0007
Blur	0.86	0.0045	0.84	0.0020	0.84	0.0020

Thus, on the basis of experiments conducted, we set the values of P to 8, N to 4, and B to 4 (for 32×32 image), 10 (for 128×128 image), and 20 (for 256×256 image).

5 Analysis of Weber's descriptor for watermark authentication

5.1 Reliability

To analyze the reliability of results of Sect. 4, random bit patterns are inserted in all the host images shown in Fig. 4. From the experiments, it has been verified that Weber's descriptor-based watermarking can successfully authenticate the watermarked image for any bit pattern. The value of η for 3 different bit patterns for all the watermarked images is computed, and the mean and variance are shown in Table 11.

False-positive probability of proposed technique is analyzed using a set of 50 unwatermarked images [28] including the host image. It has been observed that out of 50 images, only one unwatermarked image is wrongly authenticated as watermarked image using the proposed technique, which is the host image. Thus, it has been analyzed that the proposed

Table 12 Results for SIFT descriptor

Attack type	Number of keypoints matched, $P(e)$									
	"*Woman*" (keypoints: 15)		"*Cameraman*" (keypoints: 11)		"*Lena*" (keypoints: 14)		"*Mandrilla*" (keypoints: 9)		"*Pepper*" (keypoints: 13)	
Brightness decreased 10 %	15	1.00	11	1.00	13	0.93	9	1.00	13	1.00
Brightness increased 10 %	15	1.00	11	1.00	14	1.00	9	1.00	13	1.00
Brightness increased 20 %	15	1.00	11	1.00	14	1.00	9	1.00	13	1.00
Brightness increased 30 %	15	1.00	11	1.00	14	1.00	9	1.00	13	1.00
Sharpen	10	0.67	7	0.64	7	0.50	6	0.67	8	0.62
More sharpen	7	0.47	6	0.55	6	0.43	3	0.33	7	0.54
Blur	4	0.27	2	0.18	4	0.29	2	0.22	3	0.23
Vertical crop	10	0.67	6	0.55	6	0.43	6	0.67	9	0.69
Random crop	8	0.53	0	0.00	3	0.21	3	0.33	5	0.38
Compression (quality factor = 1)	12	0.80	7	0.64	3	0.21	4	0.44	2	0.15
Compression (quality factor = 5)	12	0.80	10	0.91	6	0.43	6	0.67	12	0.92
Compression (quality factor = 8)	12	0.80	11	1.00	10	0.71	7	0.78	11	0.85
Noise 1 %	15	1.00	11	1.00	12	0.86	9	1.00	11	0.85
Noise 5 %	14	0.93	10	0.91	10	0.71	7	0.78	12	0.92
Noise10 %	5	0.33	7	0.64	6	0.43	5	0.56	11	0.85
Rotation 5°	13	0.87	10	0.91	11	0.79	9	1.00	10	0.77
10°	11	0.73	9	0.82	9	0.64	9	1.00	9	0.69
15°	7	0.47	5	0.45	8	0.57	5	0.56	5	0.38
20°	7	0.47	6	0.55	8	0.57	6	0.67	6	0.46
25°	7	0.47	5	0.45	9	0.64	5	0.56	5	0.38
30°	6	0.40	6	0.55	8	0.57	6	0.67	6	0.46
35°	6	0.40	6	0.55	7	0.50	6	0.67	6	0.46
40°	7	0.47	6	0.55	9	0.64	6	0.67	6	0.46
45°	5	0.33	6	0.55	7	0.50	6	0.67	6	0.46
50°	7	0.47	5	0.45	6	0.43	5	0.56	5	0.38
Vertical flipping	2	0.13	2	0.18	1	0.07	2	0.22	0	0.00
Horizontal flipping	1	0.07	2	0.18	1	0.07	1	0.11	0	0.00

technique can discriminate between watermarked and unwatermarked images except the host image. The problem of false-positive for host image is resolved when extraction of the bits (using key "$k1$") from the host image never results in a watermark with desired detection ratio. The value of η between watermarked image of "*Lena*" and unwatermarked image of "*Woman*" is 0.28 and value of ρ is 209.22. It has been observed that the value of η between watermarked image of "*Lena*" and 50 other unwatermarked images is always less than 0.5. The proposed method always reports zero false-negatives, so there is no chance that watermarked will be authenticated as unwatermarked.

5.2 Comparative analysis

Here, a comparison of the proposed watermark authentication scheme is done with other state-of-the-art watermark authentication schemes.

A number of watermark authentication techniques based on SIFT have been proposed by many researchers. Although SIFT is very efficient against RST attacks, still one of the shortcoming of SIFT that tempted us to use Weber's descriptor for watermark authentication is that a prerequisite for SIFT is clear and sharp images [29]. On the other hand, Weber's descriptor is highly robust against illumination and contrast changes. With the help of Weber's descriptor, watermarked image can be authenticated even if the image has been blurred or sharpened.

WLD descriptor is computed for 3 × 3 blocks around each pixel, whereas SIFT descriptor is computed for 16 × 16 block around feature points due to which size of SIFT descriptor is large as compared to WLD descriptor. Also, the time complexity of WLD descriptor is very low as compared to the time complexity of SIFT descriptor. Time complexity of WLD descriptor and of SIFT descriptor for an $m \times n$ image is given below [2]:

$$\text{complexity}_{\text{WLD}} = kmn \tag{15}$$

$$\text{complexity}_{\text{SIFT}} = k\alpha\beta(lq)(mn) \tag{16}$$

where k is the proportionality constant, $l \times q$ is the size of convolution mask, α is the levels of octave, and β is the scale of each octave.

For 32 × 32 image, when $k = 0.5$, complexity of Weber's descriptor is of the order of 512 and complexity factor of SIFT descriptor is of the order of 27,648 for 3 × 3 sized convolution mask, 2 levels of octave and 3 scales in each octave.

To compare the performance of Weber's descriptor with SIFT descriptor, results for SIFT are obtained in MATLAB 7.0 for various attacks on watermarked image and their similarity probability $P(e)$ is summarized in Table 12.

From the results of Sect. 4 and Table 12, it can be concluded that SIFT is not invariant to flipping, whereas Weber's descriptor can authenticate the watermarked image even when the image is flipped horizontally or vertically. Also, SIFT is not able to authenticate the watermarked image when it is blurred, whereas Weber's descriptor can authenticate the blurred watermark image successfully. SIFT-based authentication is invariant to noise to certain extent because as noise increases, its performance decreases (as shown in Table 12 for 10 % noise), particularly for low-contrast images.

Performance of the proposed watermark authentication technique has also been compared with the LBP (local binary pattern)-based watermark authentication technique [3], where descriptor is generated using LBP features of the watermarked image. To compare the performance of the proposed watermark authentication technique with LBP-based authentication technique, LBP descriptors for watermarked images of Fig. 4 are computed using MATLAB 7.0 and average value of normalized correlation using LBP and Weber's technique is shown in Table 13.

From the results shown in Table 13, it has been observed that the LBP-based watermark authentication technique is not able to authenticate blurred watermarked images. To test the performance of LBP descriptor for blurred images, values of normalized correlation for blurred watermarked images shown in Fig. 10 are depicted in Table 14.

Table 13 Comparison of LBP and Weber's descriptor

Attack type	$\mu(\eta)$ (LBP)	$\mu(\eta)$ (Webers)
Brightness decreased 10 %	0.98	0.98
Brightness increased 10 %	0.99	0.98
brightness increased 20 %	0.99	0.95
brightness increased 30 %	0.99	0.90
Sharpen	0.98	0.89
More sharpen	0.92	0.80
Blur	0.50	0.87
Vertical crop	0.98	0.87
Random crop	0.94	0.83
Compression (Quality factor = 1)	0.90	0.80
Compression (Quality factor = 5)	0.97	0.83
Compression (Quality factor = 8)	0.98	0.88
Noise 1 %	0.99	0.98
Noise 5 %	0.98	0.94
Noise10 %	0.98	0.90
Rotation 5°	0.96	0.92
15°	0.98	0.92
25°	0.97	0.91
35°	0.97	0.90
45°	0.96	0.97
Vertical flipping	0.99	0.89
Horizontal flipping	0.98	0.86
Scaling with factor 2	0.99	0.91
Scaling with factor 4	0.97	0.84
Translation about centroid	0.99	0.90

Table 14 η for blurred watermarked images using LBP descriptor

"*Woman*"	"*Lena*"	"*Pepper*"	"*Mandrilla*"	"*Cameraman*"
0.65	0.56	0.47	0.48	0.32

6 Conclusions

In the proposed technique, watermarked image is authenticated using Weber's descriptor of original and transformed watermarked image. Descriptors of the original watermarked and transformed watermarked images are matched using two parameters, that is, normalized correlation coefficient and Euclidean distance. Through exhaustive experimentation, it has been concluded that:

1. Watermark authentication using Weber's descriptor is found to be robust to most of the geometric and

photometric attacks. It is also found to be robust against noise, cropping and compression attacks.

2. It overcomes the drawbacks of SIFT based watermark authentication techniques in terms of time complexity, illumination invariance and image flipping. It outperforms LBP based watermark authentication when the watermarked image is blurred.
3. Low contrast images are more affected by noise as compared to high contrast images whereas change in brightness has more effect on high contrast images as compared to low contrast images. But in all cases, the watermarked image is successfully authenticated by the proposed method.
4. The performance of the proposed method has been found to be invariant to the contents of watermark bit pattern.

Acknowledgments We are extremely thankful to the anonymous reviewers for their valuable comments that helped us to improve the quality of this paper.

References

1. Bas, P., Chassery, J.M., Macq, B.: Geometrically invariant watermarking using feature points. In: IEEE Trans. Image Process. **11**, 1014–1028 (2002)
2. Chen, J., Shan, S., He, C., Zhao, G., Pietikainen, M., Chen, X., Gao, W.: WLD: a robust local image descriptor. In: IEEE Trans. Pattern Anal. Mach. Intell. **32**, 1705–1720 (2010)
3. Li, C., Wang, Y., Ma, B.: Protecting biometric templates using LBP-based authentication watermarking. In: Proceeding Chinese Conference on Pattern Recognition, pp. 1–5 (2009)
4. Manjunath, B.S., Ma, W.Y.: Texture features for browsing and retrieval of image data. Proc. In: IEEE Trans. Pattern Anal. Machine Intell. **18**, 837–842 (1996)
5. Lowe, D.: Distinctive image features from scale-invariant key point. Int. J. Comput. Vis. **2**, 91–110 (2004)
6. Lee, H.Y., Kim, H., Lee, H.K.: Robust image watermarking using local invariant features. Opt. Eng. **45**, 1–11 (2006)
7. Pham, V.Q., Miyaki, T., Yamasaki, T., Aizawa, K.: Geometrically invariant object based watermarking using SIFT feature. Proc. In: IEEE Int. Conf. Image Process. **6**, 473–476 (2007)
8. Sun, J.G., He, W.: RST invariant watermarking scheme based on SIFT feature and pseudo-Zernike moment. In: Second International Symposium on Computational Intelligence and Design, pp. 10–13 (2009)
9. Singhal, N., Lee, Y.Y., Kim, C.S., Lee, S.U.: Robust image watermarking based on local Zernike moments. In: IEEE 9th Workshop on Multimedia Signal Processing, pp. 401–404 (2007)
10. Sun, J., Lan, S.: Geometrical attack robust spatial digital watermarking based on improved SIFT. In: Proceeding International Conference on Innovative Computing and Communication and 2010 Asia-Pacific Conference on Information Technology and Ocean Engineering, pp. 98–101 (2010)
11. Luo, H., Sun, X., Yang, H., Xia, Z.: A robust image watermarking based on image restoration using SIFT. J. Radio Eng. **20**, 525–532 (2011)
12. Tang, C.W., Hang, H.M.: A feature based robust digital image watermark scheme. In: IEEE Trans. Signal Process. **51**, 950–995 (2003)
13. Dajun, H., Sun, Q., Tian, Q.: A secure and robust object based video authentication system. EURASIP J. Appl. Signal Process. **14**, 2185–2200 (2004)
14. Li, L.D., Guo, B.L., Guo, L.: Combining interest point and invariant moment for geometrically robust image watermarking. J. Inf. Sci. Eng. **25**, 499–515 (2009)
15. Mikolajczyk, K., Schmid, C.: A performance evaluation of local descriptors. In: IEEE Trans. Pattern Anal. Mach. Intell. **7**, 1615–1630 (2005)
16. Lazebnik, S., Schmid, C., Ponce, J.: A sparse texture representation using affine-invariant regions. Proc. Comput. Vis. Pattern Recogn. **2**, 319–324 (2003)
17. Ke, Y., Sukthankar, R.: PCA-SIFT: a more distinctive representation for local image descriptors. Proc. In: IEEE Conf. Comput. Vis. Pattern Recogn. **2**, 506–513 (2004)
18. Cox, I.J., Miller, M.L., Bloom, J.A., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography. Morgan Kaufmann Series Virgina, Ch. 10, pp. 360 (2008)
19. Jain, A.K.: Fundamentals of Digital Image Processing. pp. 51 Prentice-Hall, U.S. (1989)
20. Al-Gindy, A., Tawfik, A., Al-Ahmad, H., Qahwaji, R.: A new blind image watermarking technique for dual watermarks using low-frequency band DCT coefficients. In Proceeding 14th In: IEEE International Conference on Electronics Circuits and Systems, pp. 538–541 (2007)
21. Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES) (November 2001). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
22. Anoop, M.S.: Public Key Cryptography—Applications Algorithms and Mathematical Explanations. http://www.tataelxsi.com/whitepapers/pub_key2.pdf?pdf_id=public_key_TEL.pdf
23. Lin, W., Horng, S., Kao, T., Fan, P., Lee, C., Pan, Y.: An efficient watermarking method based on significant difference of wavelet coefficient quantization. In: IEEE Trans. Multimed. **10**, 746–757 (2008)
24. Yang, Z., Mueller, R.: Unbiased histogram matching quality measure for optimal radiometric normalization. In: Proceeding of American Society for Photogrammetry and Remote Sensing Annual Conference Portland, Oregon (2007)
25. Kutter, M., Petitcolas, F.A.P.: A fair benchmark for image watermarking systems. Proc. SPIE Conf. Secur. Watermarking Multimed. Contents **3657**, 226–239 (1999)
26. Xina, Y., Liao, S., Pawlak, M.: Circularly orthogonal moments for geometrically robust image watermarking. J. Pattern Recogn. **40**, 3740–3752 (2007)
27. http://www.brothersoft.com/paint-shop-pro-247267.html
28. Weber, A.G.: The usc-sipi image database. http://sipi.usc.edu/database
29. Bakken, T.: An evaluation of SIFT algorithm for CBIR. Telenor R & I Research Note, pp. 1–31 (2007)