Robust Zero-watermarking Scheme Using Local Invariant Keypoints

Li Jing [1,2] Shuhong Li [2]
1. Information Science and Technology Institute, ZhenZhou
No.7, JianXue road, Zhengzhou, Henan, 450002 P.R. China
Tel: +86-371-65719185
2. College of Information, Henan University of Finance and Economy
No.80, WenHua road, Zhengzhou, Henan, 450002 P.R. China
Tel: +86-371-63752670

Abstract: - This paper presents a novel zero-watermarking scheme, which is robust to geometric distortions and common signal processes. Zero-watemarking technique is different from traditional digital image watermarking, which constructs watermark from its host image, instead of watermark inserting. We construct watermark from low-frequency coefficients in discrete wavelet transform (DWT) domain, which is robust to signal processes. Before DWT, we performs log-polar mapping (LPM) in the host image for being against scaling and cropping. For translation and rotation invariance, we apply Scale Invariant Feature Transform (SIFT) feature descriptors to locate two local invariant keypoints. One of them is regarded as the original of LPM and both of them are as reference points in correcting rotation distortion. Extensive experiments show that our scheme is effective and outperforms the previous watermarking schemes in resisting signal process, aspect ratio change, scaling and shearing.

Key-Words: - Zero-watermarking; Discrete wavelet transform; Scale invariant feature transform; Log-polar mapping; geometrical distortion.

1 Introduction

In recent years, digital watermarks have emerged as a means to protect the copyright of digital images. Up to now, many watermarking methods have been proposed. Generally digital image watermarking has certain requirements, the most important being invisibility and robustness. The traditional watermarking schemes, embedding watermarks into their host image, can not meet the two requirements at the same time because there is a conflict between invisibility and robustness. To overcome the conflict, the zero-watermarking concept was proposed by some researchers[1,2], which constructs the watermark based on the essential characters of image instead of modifying the host image in the watermark embedding process. The watermarked image has no difference from the host image, but it is protected because the constructed watermark has been registered in the database of IPR (Intellectual Property Rights).

Robustness means the embedded watermarks can not be removed by intentional or unintentional operations, called attack. Various attacks have been reported. Among them geometric distortion is known as one of the most difficult attack to resist because geometrical transforms can introduce the synchronization errors into the watermarking system. To solve the problem, plenty of watermarking schemes have been reported, such as Image normalization-based watermarking [3], template-based watermarking [4], Invariance-domain-based watermarking methods [5,6] and Content-based watermarking [7,8,9]. Image normalization-based method is highly sensitive to cropping and computationally expensive. In template-based methods, templates can easily be erased because they usually represent peaks in the transform domain. Invariance-domain-based methods degrade the quality of watermarked images for poor interpolation accuracy during log-polar mapping (LPM) and inverse log-polar mapping (ILPM). In content-based watermarking methods the feature points do not depend on a secret key, so it could be easy for a malicious party to rebuild the same image tessellation and to then perform a collusion attack[10].

In this paper we present a novel zero-watermarking approach which combines the advantages of DWT, LPM and SIFT to resist geometrical distortions and signal process. First we obtain LPM of the original image, then the LPM image is decomposed in wavelet domain and the watermark is constructed besed on the coefficients of low frequency sub-bands. We chose two SIFT [11] keypoint descriptors to decide two invariant points, being as the reference points to correct the rotation distortions during detecting. One of them is used as the origin of LPM for translation invariance.

This paper is organized in the following manner. In the next section, we will introduce the related techniques including LPM and SIFT; the proposed watermarking scheme will be proposed in section 3; and experimental results are shown in section 4; Section 5 contains conclusions and the related discussions.

2 The Related Techniques

2.1 Log-polar Mapping

LPM transforms the point (x, y) on Cartesian coordinates into (r, θ) on log-polar coordinates as:

$$\begin{cases} x - x_0 = e^{r \times \Delta r} \cos(\theta \times \Delta\theta) \\ y - y_0 = e^{r \times \Delta r} \sin(\theta \times \Delta\theta) \end{cases} \quad (1)$$

where (x_0, y_0) are the Cartesian coordinates used as the origin of the log-polar coordinates, Δr and $\Delta\theta$ are the sampling step size for the r and θ axis, respectively. $\Delta r = \ln(\max len) / N_r - 1$ (*maxlen* points to the maximal distance from origin), $\Delta\theta = 2\pi / N_\theta$, and $r = \{0,1,\ldots, N_r - 1\}$, $\theta = \{0,1,,\ldots, N_\theta - 1\}$.

The scale of an image on log-polar coordinates is not changed, if the sampling rates, N_r and N_θ of LPM on the radial and angular direction are constant. Fig.1 shows a visual representation of the properties of LPM. The original image is shown in Fig. 1(a), while the scaling-attacked image is shown in Fig. 1(c). LPM results of Fig. 1(a) and (c) are represented by Fig. 1(b) and (d), respectively, which exhibit LPM properties of scaling invariance.

The LPM is just like a sampling process. The sampling points on the Cartesian plane are used to construct the transformed image on the log-polar plane. The bilinear interpolation is used to compute the values of those sampling points. It is concluded from Eq(1) that sampling in the region around origin is higher than that in borders of the Cartesian plane, as can be seen in Fig.1(e) and (f). This property will induce that LPM image is sensitive to central cropping but less to border cropping of original image.

2.2 Scale Invariant Feature Transform

The SIFT, proposed by Lowe, is a method to extract distinctive invariant features from images for object recognition. These features have been proved to be invariant to image rotation, scaling, translation, partial illumination changes, and projective transformations in [11].

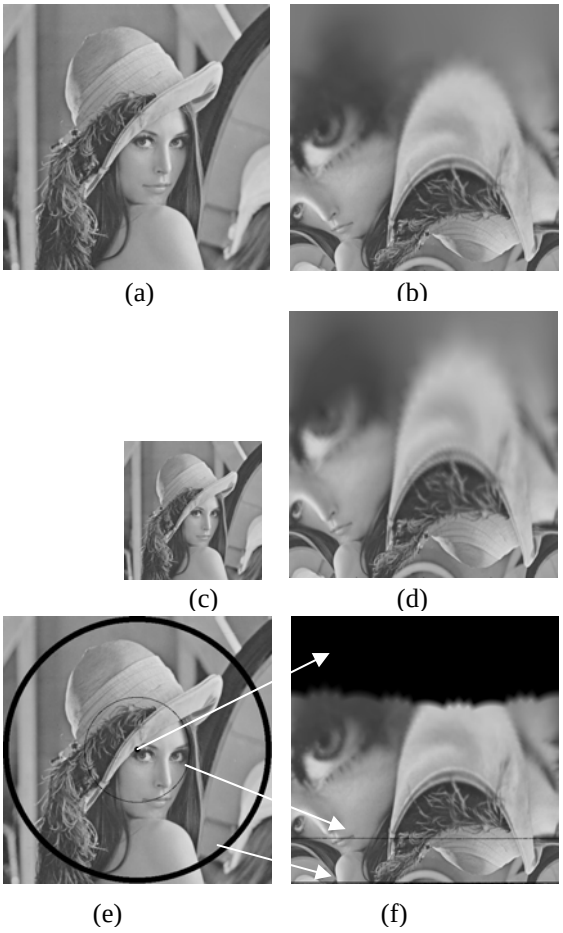


Fig.1 Properties of LPM: (a) original image; (b) LPM of (a); (c) 50% scaling of (a); (d) LPM of (c); (e) the sampling points ion the Cartesian plane, (f) the corresponding points on the Log-polar plane after LPM, arrows show the corresponding mapping.

There are several steps to compute these features as follows: (1) select candidates for features by searching peaks in the scale space from difference-of-Gaussian (DoG) function, (2) locate keypoints using measures of their stability, (3) assign orientations based on local image gradient directions and (4) calculate the local keypoint descriptors based on the set of surrounding image gradients. Each feature descriptor, a vector with 4×4×8 elements, includes coordinates of the detected keypoint.

The DoG function can be computed from the difference of two nearby scales separated by a constant multiplicative factor *k*:

$$\begin{aligned} D(x, y, \sigma) &= (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) \\ &= L(x, y, k\sigma) - L(x, y, \sigma) \end{aligned} \quad (2)$$

where * is the convolution operation in x and y; $L(x, y, \sigma)$ is a scale space of the image $I(x, y)$; and

$$G(x,y,\sigma)=\frac{1}{2\pi\sigma^2}e^{-(x^2+y^2)/2\sigma^2} \quad (3)$$

After candidate locations have been found, a detailed model is fitted by a 3D quadratic function to determine accurately the keypoints location (*t*1, *t*2) and scale *s*. In addition, candidate locations that have a low contrast or are poorly localized along edges are removed by measuring the stability of each feature using a 2×2 Hessian matrix *H* as follows:

$$stability=\frac{(D_{xx}+D_{yy})^2}{D_{xx}D_{yy}-D_{xy}{}^2}<\frac{(r+1)^2}{r},\quad H=\begin{bmatrix}D_{xx} & D_{xy}\\ D_{xy} & D_{yy}\end{bmatrix} \quad (4)$$

The *r* value is ratio between the largest and smallest eigenvalues and used to control stability. *D* represents the derivative of the scale-space image in *x*- and *y*-axis.

In order to achieve invariance to image rotation, they assign a consistent orientation to each feature. In the Gaussian smoothed image with the scale of the extracted features, they calculate gradient orientation of all sample points within the circular window of a feature location and form an orientation histogram. The peak in this histogram corresponds to the dominant direction of that feature. The gradient magnitude $m(x,y)$ and orientation $\theta(x,y)$ are precomputed using pixel differences:

$$m(x,y)=\sqrt{(L(x+1,y)-L(x-1,y))^2+(L(x,y+1)-L(x,y-1))^2} \quad (5)$$
$$\theta(x,y)=\tan^{-1}((L(x,y+1)-L(x,y-1))/(L(x+1,y)-L(x-1,y)))$$

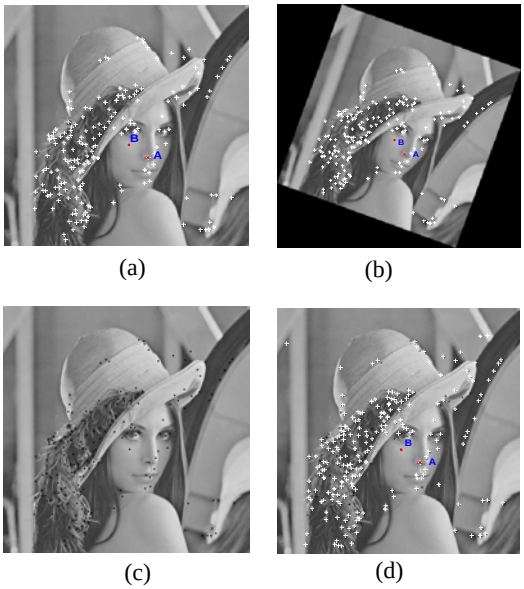
Keypoints descriptor matches are identified by taking the source image feature and finding the nearest neighbor feature at the target image. In this work, Euclidean distance between feature vectors is used as the metrics of similarity. Compare the distance of the closest neighbor to that of the second-closest neighbor and get the distance ratio. We accept all matches in which the distance ratio is smaller than 0.7.

3 Proposed Watermarking Scheme

3.1 Locate two Invariant Points

In our method we select two SIFT keypoint descriptors A and B of the host image, which are used for locating two invariant points by matching the corresponding SIFT features descriptors of detecting image when detecting.

SIFT generates large number of features that densely cover the image across a wide range, but some descriptors can not match precisely between the source image and the images distorted by lossy compression, additive Gaussian noise and aspect ratio change. We remain the keypoint descriptors that can match accurately with those of the images distorted by a variety of attacks. These descriptors form a *Stable Set*, in which we select the two keypoint descriptors A and B, as show in Fig.2 (a). Fig.2 (b) shows the *Stable Set* robust to rotation. Even when the keypoints in the *Stable Set* are erased, most of them can be matched successfully if the distorted image is median filtered, see Fig.2 (c) and (d). This guarantees that points A and B can be matched successfully if their locating areas are not cropped. For this property of the keypoint descriptors in the *Stable Set*, the point A and B are not erased easily and can overcome the weakness of the template-based methods.



(a) (b)

(c) (d)

Fig.2 Example of SIFT keypoints in geometrical distorted images: (a) *stable set* and the selected points A and B; (b) matched keypoints in rotated image; (c) keypoints in stable set are erased; (d) matched keypoints after (c) was median filtered.

The keypoints A and B should be selected in central area or the important part of image to guarantee not to be cropped, as shown in Fig.2 (a). Point A is the origin of LPM and point B, as a reference point, is used to calculate the rotation angle of image with A. If the image is rotated by an angle θ_r, the locations of points A and B are also rotated by the same angle.

Let A and B of the original image be $(x_A,y_A),(x_B,y_B)$, A and B of the rotated image be $(x_A',y_A'),(x_B',y_B')$, Then θ_r can be calculated as:

$$\theta_r=\alpha_r-\alpha \quad (6)$$

where α_r and α are angular distances of AB in rotated image and original image respectively , and can be calculate as:

$$\alpha_r = \tan^{-1}(\frac{y_B' - y_A'}{x_B' - x_A'}) \quad \alpha = \tan^{-1}(\frac{y_B - y_A}{x_B - x_A}) \tag{7}$$

3.2 Watermark Constructing

The watermark constructing process is outlined in Fig. 3. This scheme is detailed step by step as follows:

1. For m×n gray image *I(x,y)*, transform it into LPM $I_{LPM}(r,\theta)$, using the invariant keypoint A as the origin. And $0 \le r \le m-1, 0 \le \theta < 2\pi$.

2. Decomposed the m×m LPM image into three-level in wavelet domain. The size of the low-frequency bands LL3 is $(m/2^3)\times(m/2^3)$.

3. Select N coefficients in the low-frequency bands LL3 randomly with key *K*, and $N \le (m/2^3)\times(m/2^3)$. For the selected coefficients $p_i, 1 \le i \le N$, the watermark *W* is generated by comparing the adjacent coefficients as follows:

$$w_j = \begin{cases} 1 & if\ p_{2j-1} - f_{2j} > 0 \\ 0 & if\ p_{2j-1} - f_{2j} \le 0 \end{cases} \qquad j = 1,2\cdots N/2 \tag{8}$$

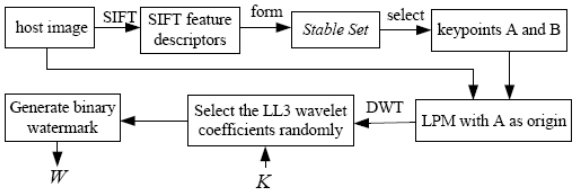


Fig.3 Watermark constructing process

In Fig.3 the *stable set*, keypoints A and B have illuminated in part 3.1. The host image is transformed into LPM image using invariant point A as the origin, which can keep LPM image being invariant to translation. And the sampling rates of LPM on the radial and angular direction being constant can keep LPM image being invariant to scaling. To defeat rotating, keypoints A and B are used as reference points to correct rotating in watermarking detecting. Furthermore, watermark constructed in the low frequency bands of wavelet domain can get better performence in resisting signal process than in other domain. And we need not worry about the invisibility because we do not embed any digital mark in the host image.

3.3 Watermark Detecting

In watermark detecting, we first perform the rotating correction as the following steps.

1. Extract feature descriptors *FF* from the test image *I* using SIFT;
2. Match the recorded keypoints A and B with *FF* in the method described in 2.2;
3. Compute the rotating angle θ_r of the test image I with the method described in 3.1; if $\theta_r = 0$, run step 6 directly;
4. Correct rotation by rotating the test image *I* with the inverted θ_r, and get the corrected image *I'*;
5. Extract SIFT feature descriptors from the image *I'* to match keypoint A;
6. Perform LPM for *I'* with point A as the origin, and the sampling rates of LPM are same with those used in watermark constructing.

The next steps are similar to watermark constructing. Decompose the image to three-level in wavelet domain and select N coefficients in LL3 sub band with the same key used in constructing. Generate *W'* through Eq.(8). Compare *W* and *W'*, if the count of equal elements in *W* and *W'* is C, the similarity degree between *W* and *W'* could be defined as:

$$sim = C / N \tag{9}$$

Whether the watermark is present or not is determined based on the *sim* compared with a threshold T.

$sim < T \Rightarrow$ watermark is not present
$sim \ge T \Rightarrow$ watermark is present

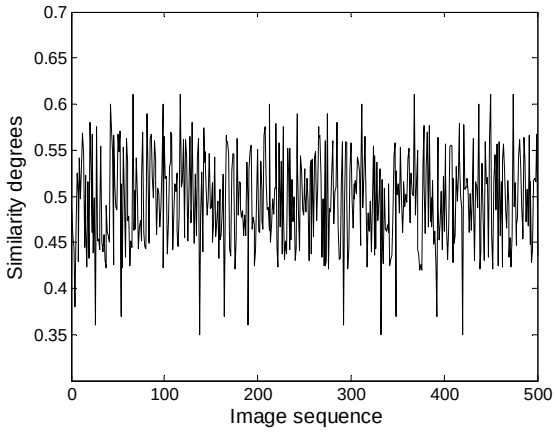


Fig.4 Similarity degree curve of watermark detected from 500 images

The watermark *W* compose of {0, 1} binary sequence. Each element reflects the difference between two adjacent coefficients chosen randomly. For a test image that is unrelated to the original one,

each element in its watermark is equal to the one in that of the original image in a probability of 0.5. To verify this point we use gray image Lena (512×512) as the original image, and collect 400 gray images (512×512) that include natural scenes, portraits, animals and food as well as 100 gray images (512×512) that are generated with random sequences as the test images. We detect the *W'* of the test images, and compute their sim with the proposed detecting method. The similarity degrees are shown in Fig.4. The minimum similarity degree is 0.35 while the maximum one is 0.61. So the threshold is set to be 0.70.

4 Experience and Results

We test the proposed scheme in many images. All these tests can show that this watermark scheme is very robust against geometric transforms and signal process. Only the results obtained from 512×512 gray lena and baboon images are presented due to space limitation. N_θ and N_r in LPM are 512. The image and its LPM image are decomposed to three-level in DWT domain and randomly select 1024 LL3 coefficient, so the length of the watermark is 512. Threshold T is set to be 0.70. Keypoints A and B are chosen at a horizontal line from *stable set* in order to calculate rotating angle conveniently.

4.1 Detection Results for Rotation

Accurate detection of the rotation degree in the spatial domain is crucial for this scheme to resist rotating distortions. The rotation degrees between 0° and 360° can be correctly detected with the method described in 3.1. The rotation degree and detection results are shown in Tables 1. The imprecision is within acceptable range. According to the detection results, the rotated image can be corrected by rotating the invert degree.

Table 1 Rotation degree detection

Rotation degree	Detected rotation degree	
	lena	baboon
5	4.99	4.91
10	10.21	9.89
30	29.98	30.15
60	60.12	60.24
90	90.00	90.00
125	124.94	125.36
180	180.00	180.00
250	250.43	249.38
300	300.16	299.54

Fig.5 shows the robustness of our method against rotating with cropping. Fig.5 (a) is the image attacked by 20° rotating with 60% cropping, and the two matched keypoints (marked as cross). Fig.5 (b) is the corrected image of (a). The detected similarity degree *sim* of Fig.5 (a) is 0.79

(a) (b)

Fig.5 (a) 20° anticlockwise rotation with 60% cropping; (b) the corrected (a)

4.2 Geometrical and Signal Attacks

To demonstrate the robustness of our scheme, we applied most of the attacks listed in Stirmatk 3.1, including global translation and local distortion. Some simulation results are shown in Table 2, from which we can see our method is robustness to shearing, rand bending, row-column removal, rotation+scaling+cropping, translation and aspect ratio. Our scheme also defeats signal process such as JPEG compress, filter and noise, as shown in table 3.

Table 2 The similarity (sim) under geometric distortions

Geometrical attacks	lena	baboon
Random bend	0.86	0.83
Translation(-40,40)	1	1
Row 1 and column 20 removal	0.97	0.95
Row15 and column 20 removal	0.93	0.92
Shearing *x* 10% *y* 0%	0.88	0.86
Shearing *x* 20% *y* 0%	0.86	0.86
Shearing *x* 10% *y* 10%	0.86	0.86
Cropping(20%,460×460)	0.85	0.83
Cropping(30%,430×430)	0.83	0.80
Cropping(40%,390×390)	0.76	0.75
Rotation 5°, 45°,90°,120°	>0.94	>0.92
Rotation 30°+cropping(360×360)	0.80	0.80
Rotation 20°+cropping(280×260)	0.79	0.78
Scaling (0.5, 256×256)	0.81	0.79
Scaling (0.75, 384×384)	0.92	0.87
Scaling (1.5, 768×768)	0.89	0.87
Scaling (2.0, 1024×1024)	0.84	0.79
Rotation 15°+scaling(0.75)+crop	0.89	0.85
Rotation 15°+scaling(1.2)+crop	0.90	0.88
Rotation 30°+scaling(0.75)+crop	0.82	0.79
Rotation 30°+scaling(1.2)+crop	0.85	0.81
Aspect ratio change (400×450)	0.91	0.89
Aspect ratio change (350×300)	0.87	0.84
Aspect ratio change (500×600)	0.87	0.86

Table 3 The similarity (sim) under signal process (*Q* denotes compression-quality-factor)

Signal process attacks	lena	baboon
JPEG compression (Q=70)	1	1
JPEG compression (Q=30)	0.98	0.98
JPEG compression (Q=5)	0.91	0.89
JPEG compression (Q=1)	0.89	0.85
Median filter 2×2	0.98	0.98
Median filter 3×3	0.98	0.98
Median filter 4×4	0.98	0.98
Gaussian filter 3×3	0.99	0.99
Additive uniform noise	0.97	0.96
Dithering	0.97	0.95

4.2 Performance comparison

In this section, we compare the performance of the watermarking scheme proposed in this paper with those proposed in [2,4,8]. Table 4 shows the compared results, from which we find our method outperforms theirs in resisting signal process and geometric distortion such as JPEG compression, aspect ratio change, shearing and scaling. This is because of the application of the wavelet low-frequency band coefficients. In addition, SIFT and LPM are crucial to resist geometric attacks.

Table 4 Comparisons with other methods

methods	JPEG(Q)	Aspect-ratio	scaling	shearing
In [4]	75-100	no	0.75-2.0	0.1%
In [8]	40-100	no	0.7-2.0	5%
In [2]	1-100	no	no	no
proposed	1-100	yes	0.5-2.0	20%

Note: in table 4 “no” means have the corresponding ability while “yes’ means have no the ability.

4 Conclusion

The proposed zero watermarking scheme combines the advantages of DWT, LPM and SIFT, which has better performance in resisting geometrical distortions and signal process. The SIFT keypoints A and B selected in *stable set* can match successfully in the image distorted by signal and geometric attacks, even their location are erased, which keeps our scheme robustness and security. In addition, this scheme does not need an original image to detect the watermark, only need two keypoint descriptors taking up 256 bytes.

Acknowledgement

This work is supported partially by Natural Science Foundation of Education Department of Henan, China (No.2004922081), Science Technology Project of Henan, China (NO.072102210001, No. 0624260019) and National Natural Science Foundation of China (No.60374004)

References:

[1] Q. Wen, T. Sun, and S. Wang, Concept and Application of Zerowatermark,” *Acta Electronica Sinica.*. 2003, 31(2), pp. 214–216 (in Chinese).

[2] H.Xiang, H.Q.Cao, K.N.Wu and F.Wei, A Zero water-marking Algorithm Based on Chaotic Modulation, *Journal of Image and Graphics*, 2006,11(5), pp.720-724 (in Chinese).

[3] Dong P., J. B., G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, Digital watermarking robust to geometric distortions, *IEEE Trans. Image Process*, 2005, 14(12) , pp.2140–2150.

[4] S. Pereira and T. Pun, Robust template matching for affine resistant image watermark, *IEEE Trans. Image Process.* 2000,9(6), pp.1123-1129.

[5] D. Zheng, J. Zhao, A. El Saddik, RST- invariant digital image watermarking based on log-polar mapping and phase correlation, *IEEE Trans. Circuits Syst. Video Technol.* 2003,13(8) , pp.753–765.

[6] C.Y. Lin, M. Wu, J.A. Bloom, I.J. Cox, M.L. Miller, Y.M. Lui, Rotation, scale, and translation resilient watermarking for images, *IEEE Trans. Image Process.* 2001, 10 (5), pp.767–782.

[7] M. Kutter, S.K. Bhattacharjee, T. Ebrahimi, Toward Second Generation Watermarking Schemes, in: *Proceedings of IEEE International Conference Image Processing*, October 1999, vol. 1, Kobe, Japan, pp. 320–323.

[8] Bas, P., J. M. Chassery, and B. Macq, Geometrically Invariant Watermarking Using Feature Points, *IEEE Trans. Image Processing*, 2002, 11(9), pp. 1014–1028.

[9] H. Y. Lee, H. kim and H. K. Lee, Robust Image Watermarking using local Invariant Features, *SPIE, Journal of Optical Engineering*, 2006,45(3) , pp. 037002(1-11).

[10] Jean-Luc D., Stéphane Roche, Christian Rey, and Gwenaël Doërr, Still-Image Watermarking Robust to Local Geometric Distortions, *IEEE Trans. Image Processing*, 2006, 15(9), pp. 2831-2842.

[11] D. G. Lowe, Distinctive image features from scale-invariant keypoints, *International Journal of Computer Vision*, 2004,60(2), pp.91-110.