Geometrically robust image watermarking using scale-invariant feature transform and Zernike moments

Leida Li (李雷达), Baolong Guo (郭宝龙), and Kai Shao (邵 凯)

ICIE Institute, Xidian University, Xi'an 710071

Received December 20, 2006

In order to resist geometric attacks, a robust image watermarking algorithm is proposed using scale-invariant feature transform (SIFT) and Zernike moments. As SIFT features are invariant to rotation and scaling, we employ SIFT to extract feature points. Then circular patches are generated using the most robust points. An invariant watermark is generated from each circular patch based on Zernike moments. The watermark is embedded into multiple patches for resisting locally cropping attacks. Experimental results show that the proposed scheme is robust to both geometric attacks and signal processing attacks.

OCIS codes: 100.2000, 100.5010, 100.5760.

Digital watermarking is a promising way to protect the copyright of digital products[1,2]. The ownership can be established by extracting previously embedded information. Geometric attacks desynchronize watermark information thus cause incorrect detection. How to efficiently resist such attacks is still an open problem.

Many geometrically robust watermarking schemes are based on invariant domain, such as Fourier-Mellin transform and Zernike transform. Ruanaidh *et al.* first reported rotation, scaling, and translation (RST) invariant watermarking in Fourier-Mellin domain[3]. Kim *et al.* designed a RST invariant watermark in Zernike domain[4]. The main drawback is that the watermarked images degrade much and they cannot resist cropping attacks, because the watermark is embedded in the global image. Bas *et al.* proposed a feature-based watermark synchronization method[5]. They used the Harris corner detector to extract interest points. Then the Delaunay tessellation was applied on the detected points, producing a set of triangles. The watermark was embedded into all triangles additively in spatial domain. Scale-invariant feature transform (SIFT) was proposed by Lowe[6]. SIFT feature points are highly distinctive and they can be detected with high repeatability. Compared with Harris corners, SIFT features are more stable thus are more suitable for watermark synchronization. Recently, Lee *et al.* developed a SIFT based watermarking scheme[7]. They extracted feature points by SIFT and used them to generate a series of patches. The watermark was embedded into all patches, also in spatial domain. The scheme outperformed Bas' method. However, both schemes embed the watermark in spatial domain, like added noise. As a result, the embedded watermark can be easily affected by attacks, leading to low watermark similarities.

In this paper, we propose a new image watermarking algorithm using SIFT and Zernike moments. It is a patch based scheme in which the watermark is embedded into image local patches. And the patches are generated using SIFT. A rotation and scaling invariant watermark is generated on the patches. The proposed scheme is robust to rotation, scaling, cropping, and common signal processing attacks.

SIFT keypoints are extracted through a cascade filtering approach[6]. Four steps are necessary for extracting SIFT features: 1) candidate keypoint detection in the scale space of the difference-of-Gaussian (DoG) function; 2) accurate keypoint localization by eliminating low-contrast points and points that are poorly localized along edges; 3) orientation assignment based on local image properties; 4) SIFT descriptor generation.

As shown in Fig. 1, the original image is successively convolved with a Gaussian function, producing a set of smoothed images. Adjacent smoothed images are subtracted to produce a DoG image. In order to detect the local maxima and minima, each sample point in the DoG image is compared with its eight neighbors in the current image and nine neighbors in the scale above and below. It is selected only if it is larger or smaller than all of these neighbors.

Once a candidate keypoint has been found, a detailed fit is performed to the nearby data for location, scale, and ratio of principle curvatures, aiming at rejecting points that have low contrast. To eliminate keypoints that are poorly localized along an edge, the principle curvature is computed from a 2×2 Hessian matrix, H, computed at the location and scale of the keypoint

$$H = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix}. \tag{1}$$

The stability of a feature point is computed by

$$\text{Stability} = \frac{(D_{xx} + D_{yy})^2}{D_{xx}D_{yy} - D_{xy}^2} < \frac{(r+1)^2}{r}, \tag{2}$$

where r is the ratio between the largest eigenvalue and the smallest one, and D_{xx}, D_{xy}, and D_{yy} are the

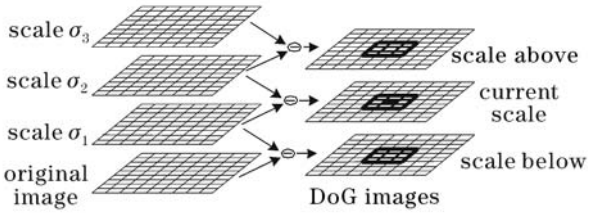

Fig. 1. DoG images and neighbors of a keypoint.

1671-7694/2007/060332-04

derivatives of the scale-space image, respectively.

The third step is to assign an orientation to each keypoint based on local image properties. The keypoint descriptor can be represented relative to the orientation and therefore achieve invariance to image rotation.

After assigning location, scale and orientation to a keypoint, a 128-dimension keypoint descriptor for the local image region is computed. The descriptor is highly distinctive and can be directly used in image analysis. The detailed feature point extraction procedure can be found in Ref. [6].

The SIFT extracts keypoints with their location (p_1, p_2), scale σ, and orientation θ. In this paper, we adopt the location and scale information to generate a circular patch centered at the feature point as

$$(x-p_1)^2+(y-p_2)^2=(k\sigma)^2, \tag{3}$$

where k is a magnification factor to control the radius of the patch.

The SIFT was originally designed for image matching. It extracts many interest points which densely cover the image content. To adapt them to the watermarking system, keypoints must be pre-processed. In this paper, we determine their distribution using feature matching. For an original image, it is first rotated. Then we extract SIFT keypoints from the original image and the rotated one, respectively. Then feature matching is applied on those detected points using fast nearest-neighbor algorithm[6] by setting a threshold. Then a set of matched keypoints from the original image are obtained together with their descriptors. These points are the initial candidates for patch generation.

The candidate points are then filtered according to their scale. The SIFT detects keypoints from a set of Gaussian smoothed images. So candidate keypoints have different scales. A keypoint whose scale is small or large has a low probability of being redetected because it is unstable when image contents are modified. As a result, we select keypoints from the candidate points whose scales are between a minimum value and a maximum value[7]. Ideally, the minimum value should be larger than 2 and the maximum value should be smaller than 10.

Upon feature matching and scale selection, the next step is to reduce keypoints that are too close together. In feature matching, each candidate point is related to a distance ratio which is produced in the fast nearest-neighbor algorithm. The smaller the ratio, the more robust the keypoint is. As a result, we first select the point with the smallest distance ratio. Then we compute the distance between any other point and this one. If it is smaller than the sum of the two expected radiuses $(k\sigma)$, the point is reduced, otherwise selected. This operation is done circularly until all points are processed. At last, we reduce the keypoints that are too close to the image edge. Finally, we obtain the most robust keypoints and use them to generate non-overlapped circular patches using Eq. (3). And these patches are rotation and scale invariant. Figure 2 shows an example of patches generated on the image Lena.

The Zernike moments of order n and repetition m for a digital image $f(x,y)$ that vanishes outside the unit circle are

Fig. 2. Circular patches for watermarking.

$$A_{nm}=\frac{n+1}{\pi}\sum_x\sum_y f(x,y)\,V_{nm}^*(x,y), \tag{4}$$

where n is the nonnegative integer and m is the integer subjected to constraints that $n-|m|$ is nonnegative and even. $V_{nm}(x,y)$ is the complex function defined as

$$V_{nm}(x,y)=V_{nm}(\rho,\theta)=R_{nm}(\rho)\exp(jm\theta), \tag{5}$$

where $\rho=\sqrt{x^2+y^2}$, $\theta=\tan^{-1}(y/x)$. $R_{nm}(\rho)$ is the radial polynomial defined by

$$R_{nm}(\rho)=\sum_{s=0}^{(n-|m|)/2}(-1)^s\cdot\frac{(n-s)!}{s!(\frac{n+|m|}{2}-s)!(\frac{n-|m|}{2}-s)!}\rho^{n-2s}. \tag{6}$$

Given all Zernike moments with the maximum order $N_{\max}$, the image can be reconstructed as

$$f(x,y)=\sum_{n=0}^{N_{\max}}\sum_{m=-n}^{n}A_{nm}V_{nm}(x,y). \tag{7}$$

Zernike moment has an important property that its magnitude is rotation invariant. For scale invariance, image normalization can be adopted.

Kim *et al.*[4] designed an invariant watermark by modifying Zernike moments. For a digital image, normalized Zernike moments are first calculated. Then they are modified and reconstructed, producing a signal. The signal is added into the original image to obtain a watermarked image. In detection, normalized Zernike moments of the distorted image are calculated and subtracted from the original moments. Ideally, the watermark can only be found where the moments are modified.

In this paper, we incorporate the Zernike based invariant watermark into the circular patches. Take one patch for example: normalized Zernike moments of the patch are first computed and denoted by $\{A_{nm}\}$. Then we modify A_{nm} by Δ_{nm}, and the modified moments are reconstructed as the watermark. Then we add it into the original patch in spatial domain. If we only modify $A_{k,l}$ of the moment and add the watermark into the patch. Then the difference of normalized Zernike moments will produce a peak at order (k,l). For illustration purpose, we modify the Zernike moments of a patch at order $(3,1)$, and compute the magnitude difference. The simulation result is shown in Fig. 3. Note that for the conjugate symmetry of Zernike moments, $(3,-1)$ also has to be

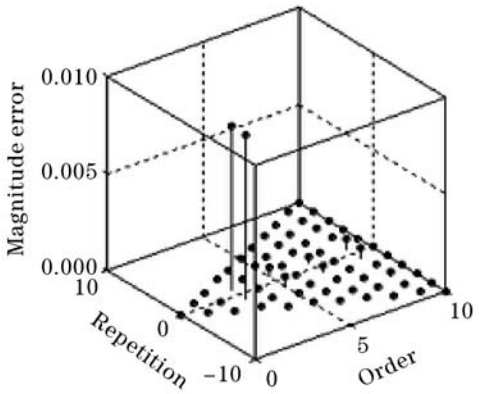

Fig. 3. Detected watermark at $(3, -1)$ and $(3, 1)$.

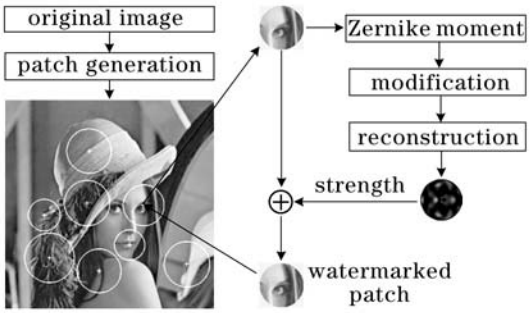

Fig. 4. Diagram of watermark embedding.

modified to obtain a real image. As a result, there are two peaks located at $(3, -1)$ and $(3, 1)$ respectively in Fig. 3.

Normalized Zernike moment is rotation and scaling invariant. As a result, whether a patch is rotated or scaled, if only the content of the patch remains the same, the peaks can always be detected.

Watermark embedding is implemented by first extracting circular patches. For each patch, normalized Zernike moments are first computed. Then they are modified at predetermined order. The modified moments are reconstructed using Eq. (7), producing the watermark. The watermark is embedded into the original patch in spatial domain, producing a watermarked patch. Then the original patch is replaced by the watermarked patch. The detailed diagram of watermark embedding is shown in Fig. 4.

In order to detect the watermark from an attacked image, SIFT keypoints are first extracted and matched to the original descriptors using fast nearest-neighbor algorithm. Those matched keypoints are used to synchronize the patches using Eq. (3). For a patch, normalized Zernike moments are calculated and subtracted from the original ones. If a peak is produced where the moment was modified, then we can say that the inserted watermark is detected, otherwise not. In practice, if peaks can be found in at least one patch, we can claim the presence of the watermark. For scaling attacks, the watermark can be directly detected from the distorted images, because SIFT features are scale invariant. The diagram of watermark extraction is shown in Fig. 5.

Although the proposed scheme is not completely blind, we only need the original descriptors and the

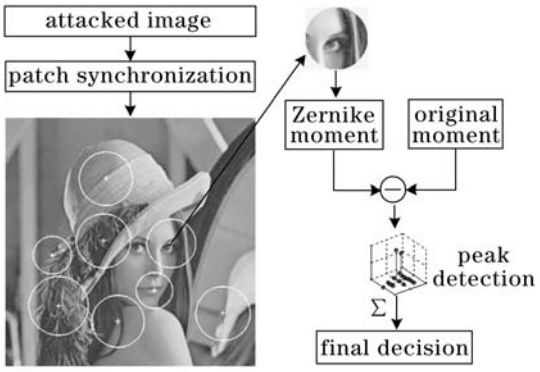

Fig. 5. Diagram of watermark extraction.

corresponding Zernike moments. The original image is not needed at the detector.

In experiments, gray level images with size 512×512 are used, including Lena, Baboon, House etc.. Figure 6 shows the original image, watermarked image, and the corresponding residue image. Note that the residue image is magnified for better display. As we embed the watermark into image local patches, the inserted watermark is invisible to the naked eyes. The peak signal to noise ratio (PSNR) values are all higher than 40 dB.

Next, we test the watermark robustness to attacks. Experimental results on signal processing attacks and geometric attacks are listed in Tables 1 and 2, respectively. The numbers of original patches used for watermarking are 9, 12, and 7, respectively for Lena, Baboon, and

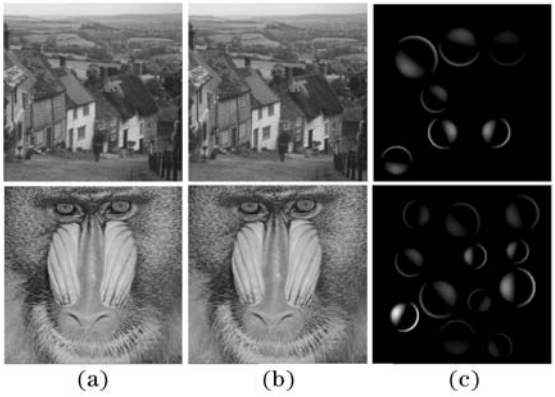

Fig. 6. Watermark invisibility. (a) Original images; (b) watermarked images; (c) residual images.

Table 1. Watermark Robustness to Signal Processing Attacks

Attack	Image		
	Lena	Baboon	House
JPEG 50%	4/7	8/11	4/7
JPEG 60%	6/9	7/10	5/7
JPEG 70%	5/9	7/11	6/7
JPEG 80%	4/7	8/12	6/7
JPEG 90%	7/9	7/11	7/7
Added Noise	6/8	3/8	5/7
Median Filter 3×3	4/7	3/8	4/7

Table 2. Watermark Robustness to Geometric Attacks

Attack	Image		
	Lena	Baboon	Peppers
Rotation 5°	6/8	7/10	4/7
Rotation 10°	6/9	7/12	4/7
Rotation 15°	4/7	6/10	3/7
Rotation 30°	4/8	7/11	3/7
Rotation 45°	4/8	4/10	2/7
Scaling 0.6	2/2	1/1	1/1
Scaling 0.8	5/5	3/4	1/3
Scaling 1.2	4/5	8/10	6/6
Scaling 1.5	3/5	8/11	4/4
Rotation 2° + Scaling + Crop	5/7	5/8	4/7
Rotation 10° + Scaling + Crop	4/7	6/11	5/7
Rotation 15° + Scaling + Crop	4/8	7/11	3/6
Centered Cropping 10%	7/9	7/11	7/7
Centered Cropping 25%	6/7	6/8	6/6
Centered Cropping 50%	1/2	4/5	1/1

House. In Tables 1 and 2, the denominator denotes the number of synchronized patches during watermark detection and the numerator denotes the number of patches from which the watermark can be successfully detected.

Table 1 shows that most patches can be synchronized using SIFT, and the watermark can be detected from a considerable number of the synchronized patches. Added noise and median filtering tend to have more effect on image Baboon because it contains more noise.

Table 2 shows that the proposed scheme is robust to rotation, scaling, cropping as well as combined attacks. In scaling attacks, the watermark can be directly detected from the scaled image. Our scheme is less robust to scaling down attacks, because when the watermarked image is scaled smaller there is information loss. The scheme is also robust to locally cropping attacks, even when 50% of the image is cropped.

In conclusion, a new image watermarking algorithm based on SIFT and normalized Zernike moments is proposed for resisting geometric attacks. We use SIFT to extract interest points and use them to generate circular patches. For each patch, an invariant watermark is produced using Zernike moments. As we embed the watermark into local patches, the watermarked images are of high quality. In detection, the watermarked patches are first resynchronized using the fast nearest-neighbor algorithm. The watermark is detected by comparing magnitudes of normalized Zernike moments. Simulation results show that the proposed watermark is robust to geometric attacks and signal processing attacks. One drawback of our method is that side information from the original image is used in watermark detection. Future work will focus on the design of a completely blind scheme using SIFT.

This work was supported by the National Natural Science Foundation of China under Grant No. 60572152. L. Li's e-mail address is reader1104@163.com or reader1104@hotmail.com.

References

1. L. Guo and B. Guo, in *Proceedings of ICCIMA'03* 419 (2003).
2. F. Zhang and H. Zhang, Chin. Opt. Lett. **2,** 634 (2004).
3. J. J. K. O'Ruanaidh and T. Pun, Signal Processing **66,** 303 (1998).
4. H. S. Kim and H.-K. Lee, IEEE Trans. Circuits Sys. Video Technol. **13,** 766 (2003).
5. P. Bas, J.-M. Chassery, and B. Macq, IEEE Trans. Image Processing **11,** 1014 (2002).
6. D. G. Lowe, Intl. J. Computer Vision **60,** 91 (2004).
7. H.-Y. Lee, H. Kim, and H.-K. Lee, Opt. Eng. **45,** 037002 (2006).