A Robust Image Watermarking Based on Image Restoration Using SIFT

Haijun LUO[1], Xingming SUN[1], Hengfu YANG[2], Zhihua XIA[1]

[1]School of Computer and Communication, Hunan University, No. 252, Lushan South Road, Changsha, 410082, China
[2]Dept. of Information Science & Engg., Hunan First Normal Univ., No. 1015, Fenglin 3rd Road, Changsha, 410205, China

sunnudt@163.com, lhjgreen0808@163.com, hengfuyang@hotmail.com

Abstract. *This paper introduces a novel robust watermarking scheme for digital images, which is robust against common signal processing and geometric distortion attacks. In order to be resistant to geometric distortion attacks, the matched feature points determined by the scale-invariance feature transform (SIFT) are used for image restoration to reduce the synchronization errors caused by geometric distortion attacks. An adaptive embedding scheme is applied in discrete Fourier transform (DFT) domain of each subimage. The watermark detection decision is based on the number of matched bits between the retrieved and original watermark in the embedding image blocks. Experimental results show that the proposed watermarking is robust to common signal processing attacks and geometric distortion attacks, including rotation, scaling, cropping, shearing and some combined attacks.*

Keywords

Scale invariance feature transform, geometric attack, image restoration, image watermark.

1. Introduction

As the rapid development of multimedia and Internet, digital content—digital image, audio, video, 3D virtual objects and so on, are widely used in various fields. However, these multimedia objects are so easily obtained, copied and distributed that the digital information protection becomes more difficult. Digital watermark is an efficient method for copyright protection. Recently, many digital watermark schemes have been proposed for protection of ownership rights on digital content. Nevertheless, various attacks have been reported to destroy watermarks [1]. Among those attacks, geometric distortion has been deemed to one of the most difficult attacks to resist, owing to the synchronization errors that geometric distortion induce. Hence, the watermark synchronization process is essential to the robustness of the watermark systems [1].

In recent years, several methods that are resistant to geometric distortions have been proposed. These schemes can be roughly classified as template-based [2], invariant transform domain-based [3], and moment-based [4], [5]. However, the robustness of all three aforementioned watermark approaches is limited. For instance, a new attack called conspiracy attack can destroy the template without any prior knowledge. The interpolation caused by invariant domain transforms and the discretization caused by moments increase the synchronization errors, which make watermark embedding and detection misaligned. Hence, second generation watermark scheme [6] was proposed to improve the robustness of watermark to resist geometrical distortion. This scheme extracts salient feature points which are invariant to geometric transformation for watermark synchronization. Some feature-based watermark approaches [7-13] are primitively reviewed in the following.

Bas et al. [7] proposed a content-based watermark scheme, in which they first use Harris corner detector to extract salient feature points and then compose a set of disjoint triangles through Delaunay tessellation, and finally watermark is embedded using classic additive scheme and detected using correlation properties in these triangles. Experiment results show that the robustness of the watermark scheme depends on the capacity of the Harris detector, due to that the number of feature points depended on the texture of image. Xiaojun Qi et al. [8] proposed an image texture based adaptive Harris corner detector for uniform-distributed and suited-number feature points, regardless of high, medium or low textured images. They use the set of triangles, generated by Delaunay tessellation, to estimate transform factors, such as translation factor, rotation factor and scaling factor. Three identical factors are used to restore the probe image. The performance is acceptable, but it can only embed 8-bit bipolar watermark message due to the spread spectrum technique [14].

In this paper, we develop a robust feature-based watermark scheme, which combines scale-invariant feature transform, one-way hash function, image restoration, blind watermark embedding and detection to reduce the watermark synchronization errors and resist to common image processing attacks and geometric attacks. The reminder of this paper is organized as follows. In section 2, we describe a synchronization method based on the SIFT and image restoration. Section 3 covers the details of our watermark embedding procedure and watermark detection procedure. Section 4 shows the simulation results and finally we conclude the presentation in section 5.

2. Strategy of Synchronization

Geometrical distortion can dramatically deteriorate the performance of the watermark detection because of the synchronization errors. So in order to reduce the effect of synchronization errors, watermark synchronization is essential to the watermark scheme. In our watermark scheme, this process contains two key points: feature points extraction and image restoration. The process of watermark synchronization is fully automated. Now we will introduce both of them in detail.

2.1 Scale Invariant Feature Transform

The scale invariant feature transform (SIFT) was proposed by Lowe [15] and has proved that extracted points are invariant to image translation, rotation, scaling and projective transformations. The main idea of the SIFT is to extract stable features in the scale space. The scale space of an image is defined as a function, $L(x, y, \sigma)$, produced from the convolution of a variable-scale Gaussian and an image:

$$L(x, y, \mathrm{s}) = G(x, y, \mathrm{s}) * I(x, y) \tag{1}$$

where $I(x, y)$ is the image and

$$G(x, y, \mathrm{s}) = \frac{1}{2\mathrm{p}\mathrm{s}^2} e^{-(x^2+y^2)/2\mathrm{s}^2}. \tag{2}$$

To extract SIFT feature, the image is firstly convoluted with Gaussian kernels at different scales to generate the Difference-of-Gaussian (DOG) images.

$$\begin{aligned} D(x, y, \mathrm{s}) &= (G(x, y, k\mathrm{s}) - G(x, y, \mathrm{s})) * I(x, y) \\ &= L(x, y, k\mathrm{s}) - L(x, y, \mathrm{s}) \end{aligned}. \tag{3}$$

Here k is a constant multiplicative factor. In our experiment, we set k to be $\sqrt{2}$ to generate the DOG images. The candidates are selected by comparing each point with its eight neighbors in the current image and the nine neighbors in the scale above and below, respectively. The location is selected only if it is larger or smaller than all of its neighbors. Moreover, the locations being low contrast or poorly localized are removed by a stability measure of each feature using a 2-by-2 Hessian matrix H as follows:

$$\frac{(D_{xx} + D_{yy})^2}{D_{xx}D_{yy} - (D_{xy})^2} < \frac{(r+1)^2}{r}, \tag{4}$$

$$H = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{xy} & D_{yy} \end{bmatrix}. \tag{5}$$

Here r is the ratio between the largest and the smallest magnitude eigenvalue. They use a value of $r = 10$. The quantities D_{xx}, D_{xy}, and D_{yy} are the derivatives of the scale-space images. In order to be invariant to image rotation, they assign a consistent orientation to each key point. By calculating the gradient orientations of sample points within a region around the key point, an orientation histogram is formed. Finally, the peak in the orientation histogram corresponds to dominant direction of this feature.

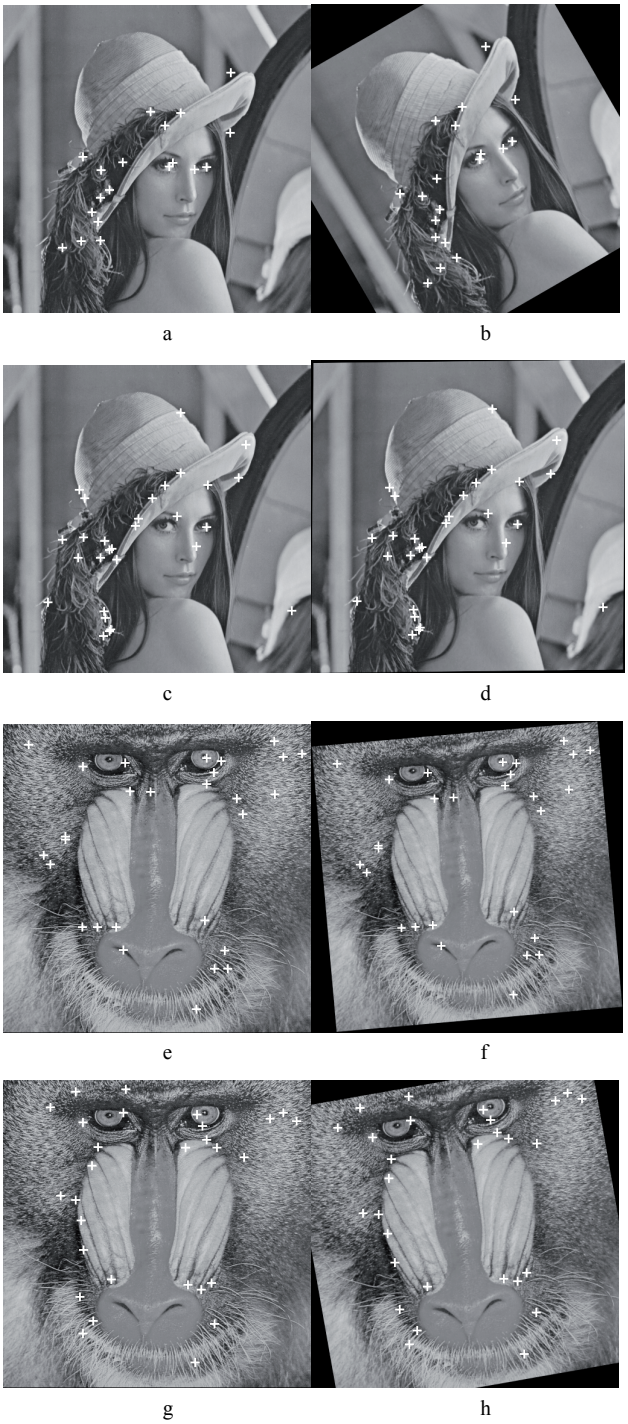


Fig. 1. Matched points using SIFT: **a, c, e, g** the original image, **b** the rotation 30deg and cropping image, **d** the shearing x 1% y 1% image, **e** the rotation 5deg image, **h** the rotation 10deg and cropping image.

The SIFT feature descriptors consist of the key point location, the scale and the orientation. These properties are saved for key point match and image restoration in our scheme. Image restoration will be introduced in section 2.2.

However, the features from the SIFT descriptors are not directly suitable for watermark, due to that the number and the distribution of the features which are dependent on image contents and textures [8]. In addition, image restora-

tion needs more stable features match in our watermark scheme. Therefore, we adjust the number of the features, removing those features that are vulnerable to image attacks. Generally, they use Euclidean distance measure to match a key point between the original image and the distorted image. If the ratio of the nearest and the second nearest distance is less than a threshold, the match is successful. Decreasing this threshold, we can obtain less number and many more stable key points, which is better for our image restoration. After this procedure we obtain the matched points set Ω_1. But there are still few mismatched points existed. In section 2.2, we will introduce the way to eliminate them. Fig. 1 shows the matched points between the original image and the rotation-cropping, shearing image, we can find that SIFT key points are matched precisely.

2.2 Image Restoration

Before the watermark detection, the SIFT descriptors are exploited to restore the approximate image of the original image. A linear transformation including rotation, scaling, translation, etc. can be written using homogeneous coordinate [16] as:

$$\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = A \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} \tag{6}$$

In order to solve matrix $\boldsymbol{A}$, we choose three pairs of matching points between the watermarked image and the distorted image. To decrease the impact of the mismatching points on image restoration, firstly we eliminate these points by comparing the values of matrix $\boldsymbol{A}$ which is obtained from each three-pairs matching points in set Ω_1. Because most of these matched points in set Ω_1 are accurate, we can find these mismatched points and eliminate them to obtain the set Ω_2, where the matching points all are accurate. Fig. 1 shows the performance of image restoration under different geometric distortions using this method. Fig. 2 a(1), b(1), c(1), and d(1) are original image and feature points chosen for image restoration. Fig. 2 a(2), b(2), c(2), and d(2) are given for rotation-cropping (30deg, 512×512), shearing (5% on *x*-axis), rotation (90deg), and shearing (5% on *y*-axis), respectively. Fig. 2 a(3), b(3), c(3), and d(3) show the restored images. Image restoration process is automated without manual intervention.

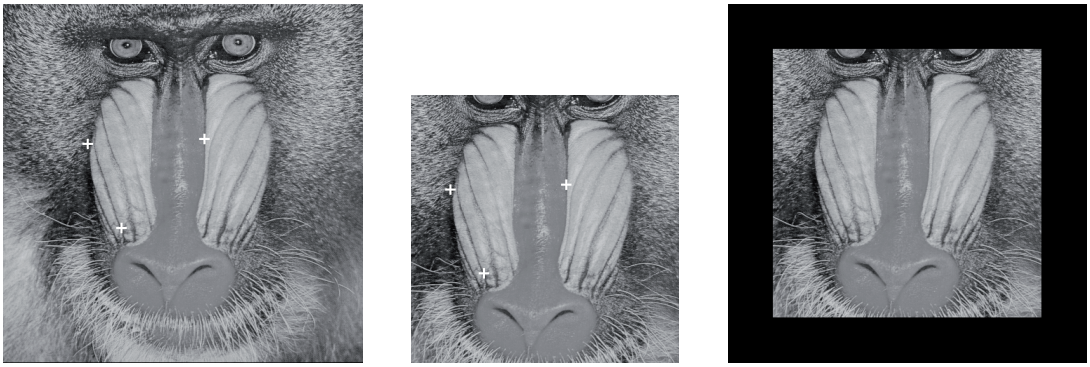
3. Watermark Scheme

The proposed watermark is designed for copyright protection. Each subimage is viewed as independent communication channels. To improve the robustness of the watermark, all subimages carry the same copy of the watermark. The watermark embedding and detection both are applied in the DFT domain of embedding subimage.

a(1) lena a(2) rotated and cropped image by 30deg a(3) lena restored

b(1) lena b(2) sheared image by 5% on *x*-axis b(3) lena restored

c(1) pepper c(2) rotated image by 90deg c(3) pepper restored



d(1) baboon d(2) centered cropped image by 5% d(3) baboon restored

Fig. 2. The performance of image restoration under different geometric distortions.

3.1 Watermark Embedding

In our watermark embed scheme, the watermark is embedded in more than one subimage which are in the middle region of the image. The watermark embedding procedure is shown in Fig. 3 and is detailed step by step as follows.

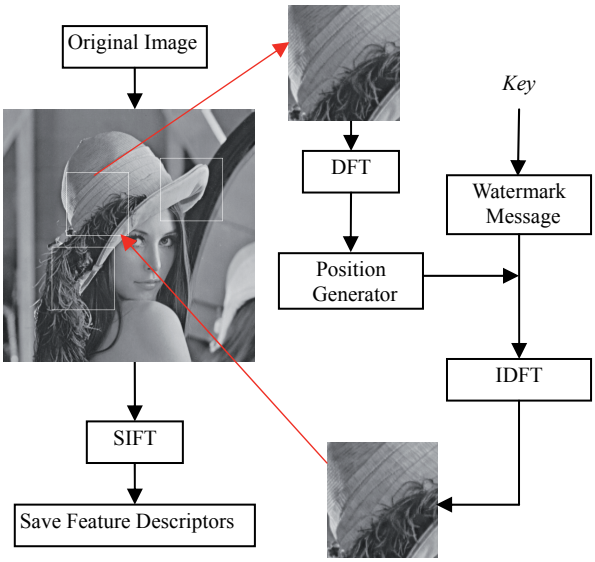


Fig. 3. Watermark Embedding Procedure.

Step 1. First we choose two or three subimages *Img* around the center of the image and the size of subimage is determined by the length of the watermark sequence. Usually the size of subimage we choose is 128×128 while the image size is 512×512, and the length of watermark sequence can be more than one hundred bits.

Step 2. A random sequence $W = \{ w_i \mid i = 1, 2, 3, ..., N \}$, as the digital watermark, is generated by a secret key K, w_i belongs to the set $\{0, 1\}$, and N is the length of the watermark sequence. Then it is coded by error correcting coding to generate an error correcting watermark bit sequence, whose length will be 7/4 times longer than that of the original sequence.

Step 3. For each subimage *Img* obtained in *Step 1*: Firstly we apply DFT to obtain *FImg*, we can obtain the amplitude spectrum F_k, and then we use the one-way hash function [7], to generate secure embedding positions in the middle frequencies ($f_1 \le f \le f_2$) which are in the first quadrant of the *FImg*. Thirdly, we select one embedding position (x_i, y_i) and another position $(-y_i, x_i)$ which is 90° apart from (x_i, y_i), to embed one watermark bit. Both of them are on the upper half DFT plane. One watermark bit is embedded as follows:

a) Calculate the amplitude difference ΔT between (x_i, y_i) and $(-y_i, x_i)$, using formula (7),

$$\Delta T = Fk(x_i, y_i) - Fk(-y_i, x_i) . \quad (7)$$

b) Modify the amplitude spectrum of the position, the rule is that when the watermark bit is 0, make the difference ΔT satisfy that $\Delta T \le -T$, when the embed watermark bit is 1,

make the difference ΔT satisfy that $\Delta T \geq T$, where T is a threshold value. In our scheme, the value of T is determined by the amplitude spectrum of the embedding position, $T = 0.4G(F_k(x_i, y_i) + F_k(-y_i, x_i))$, where G is the embedding strength factor. Intuitive description is as follows:

If the watermark bit w_i is 0 then

If $\Delta T > -T$ then

$F_k'(x_i, y_i) = F_k(x_i, y_i) - (T - \Delta T)/2$

$F_k'(-y_i, x_i) = F_k(-y_i, x_i) + (T - \Delta T)/2$

End

Else

If $\Delta T < T$ then

$F_k'(x_i, y_i) = F_k(x_i, y_i) + (T - \Delta T)/2$

$F_k'(-y_i, x_i) = F_k(-y_i, x_i) - (T - \Delta T)/2$

End

End

where $F_k(x_i, y_i)$, $F_k(-y_i, x_i)$ is the original magnitude, $F'_k(x_i, y_i)$, $F'_k(-y_i, x_i)$ is the new magnitude at (x_i, y_i), $(-y_i, x_i)$. In addition, the symmetric points on the lower half DFT plane have to be altered to the exact same value as well.

Step 4. Lastly, apply IDFT (inverse DFT) *FImg* to obtain the watermarked subimage *Img* and replace the original subimage *Img*.

After all of the watermark bits are embedded, we apply the SIFT to find the important feature points in the watermarked image, and save these feature points for image restoration. To minimize the error of the feature matching, we choose feature points between the watermarked image and the distorted image. In addition, two middle frequency ratios f_1 and f_2, secret key K for watermark sequence, will also be saved. Although there are some important feature points and other key parameters to be saved, the storage is minimal compared to the cost of saving the original image.

3.2 Watermark Detection

In the watermark detection scheme, if the watermark is detected in one subimage, we claim that the watermark is existence in the image. The watermark detector does not need the original image, while we just need the information which is saved during the watermark embedding procedure. The watermark detection scheme is shown in Fig. 4 and step by step as follows:

Step 1. The original watermark sequence $W = \{w_i \mid i = 1, 2, 3, \ldots, N\}$ is generated depending on the saved secret key K.

Step 2. Apply the SIFT to obtain important feature points of the distorted image and to obtain matched points between the distorted image and the watermarked image. Then we restore the approximate original image using the method introduced in section 2.2.

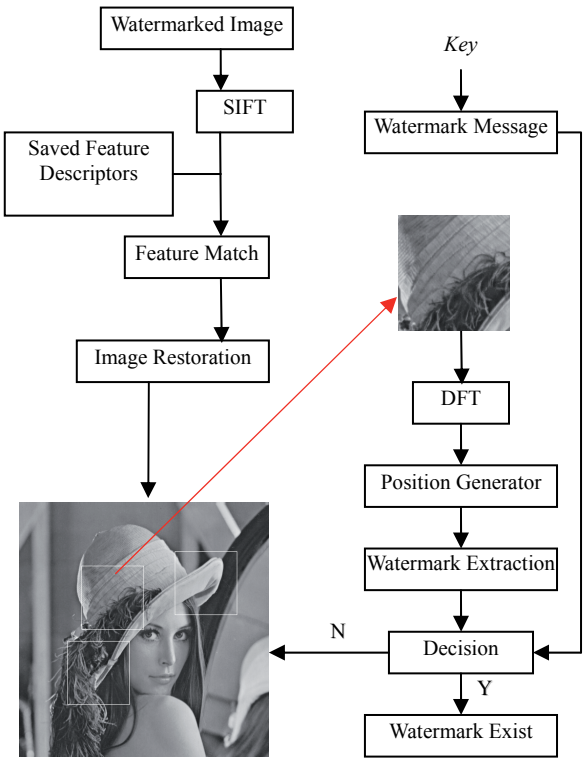


Fig. 4. Watermark Detection Procedure.

Step 3. Apply DFT transform to each subimage, and we can obtain the DFT spectrum *FImg*, amplitude spectrum F_k'. Like the watermark embedding procedure, the middle DFT coefficients ($f_1 \leq f \leq f_2$) are selected in the first quadrant. The embedding positions are obtained by using the one-way hash function [7]. For each pair of selected positions (x_i, y_i) and $(-y_i, x_i)$, we can extract one bit of error correcting watermark sequence, which is determined by

$$w_i' = \begin{cases} 1 & F_k'(x_i, y_i) \geq F_k'(-y_i, x_i) \\ 0 & F_k'(x_i, y_i) < F_k'(-y_i, x_i) \end{cases} \quad (8)$$

where $F'_k(x_i, y_i)$, $F'_k(-y_i, x_i)$ are the magnitudes of the coefficients at locations (x_i, y_i) and $(-y_i, x_i)$. We can obtain all the error correcting watermark sequence one by one.

The retrieved watermark will be compared with the error correcting watermark sequence to determine the presence of the watermark. That is, the number of matched bits between them is compared with a predefined threshold to determine whether the watermark is present in the image. The threshold is calculated based on the false alarm probability that possibly occur in watermark detection. For unwatermarked image, the extracted watermark bits are assumed to be independent random variables (Bernoulli trails). Simply, we assume the successful probability that the extracted watermark bit matches the original watermark bit to be 1/2. The probability of r-bit matched between the n-bit extract watermark and the original watermark is calculated as:

$$P_r = (\frac{1}{2})^n (\frac{n!}{r!(n-r)!}). \quad (9)$$

The false alarm probability $P_{falsealarm}$ is calculated as:

$$P_{falsealarm} = \sum_{r=Th}^{n} \left(\frac{1}{2}\right)^n \left(\frac{(n-\lfloor 0.5n \rfloor)!}{(r-\lfloor 0.5n \rfloor)!(n-r)!}\right). \quad (10)$$

Here n is the length of the watermark sequence, r, Th is the number of matched bits and the threshold value. From this formula, we can obtain a false alarm probability of 10^{-5}, while $Th = 0.75n$ and $n \geq 64$. That is, if the length of the watermark sequence n is more than 64 bits and the number of matched bits r is greater than $0.75n$, we claim the presence of the watermark since 10^{-5} is a low false alarm probability. During the detection procedure, if one copy of the watermark is correctly detected in one embedding subimage, we claim the presence of watermark in image.

4. Simulation Results

The performance of the proposed watermark scheme, including invisibility and robustness, is shown in this section. Firstly, we reported on the invisibility of watermark. And then we evaluate the performance of our proposed watermark scheme by simulation of common signal processing attacks and geometric distortions on various 8-bit grayscale images of size 512×512, like "lena", "baboon", and "pepper", and so on. Moreover, there are several fixed parameters in our system. The length of the pseudorandom sequence is 128 bits. The embedding area in DFT domain is a ring with inner and outer radii of 5% and 15% the size of the subimage.

We use the Peak Signal to Noise Ratio (PSNR) to evaluate the invisibility of watermark. The PSNR value is calculated by the following formula:

$$PSNR = 10\log\left(M 255^2\right) / \sum_{i=1}^{M}\left(x_i^2 - p_i^2\right) \quad (11)$$

where M is the size of the embedded region of image, and x, p is the gray levels of the original image and the watermarked image. The overall PSNR values between the original image and the watermarked image were greater than 40 dB. Fig. 5 showed the relation between *PSNR* values and the embedded strength factor G. To keep the balance of the robustness the invisibility of watermark, the range of factor G is (0.25, 0.35).

We applied the attacks listed in the benchmark software Stirmark 4.0 [17] which includes signal processing attacks and geometrical attacks. These attacks attempt to weaken, distort or desynchronize the watermark. Simulation results under these attacks are shown in Tab. 1, Tab. 2 and Tab. 3. Tab. 1 shows the results of our watermarking scheme under several signal-processing attacks and geometrical attacks. *Similarity* is the ratio between the number of matched bits r and the length of watermark sequence n. In most of the attacks, the similarity r/n was high enough to prove ownership. These simulation results support the contention that our proposed watermarking scheme would be robust to various image attacks.

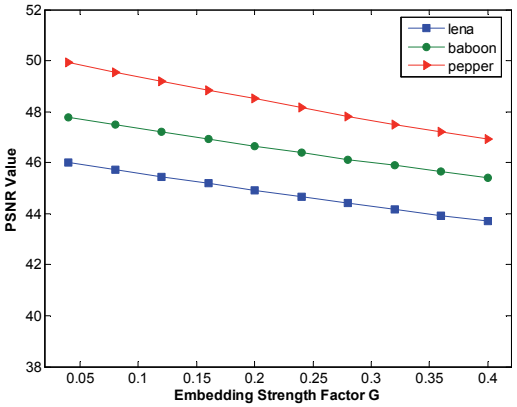


Fig. 5. *PSNR* value with different factor *G*.

Attack name	*Similarity r/n*		
	[1]	[2]	[3]
Watermarked image(no attack)	1	1	1
Median 3×3	0.828	0.906	0.805
Median 5×5	0.781	0.836	0.758
JPEG compression 90%	1	1	1
JPEG compression 70%	1	1	1
JPEG compression 50%	1	1	1
JPEG compression 40%	0.906	1	0.961
Rotation 1 deg + cropping	0.836	0.961	0.813
Rotation 10 deg + cropping	0.969	0.992	0.82
Scaling 0.9	0.805	0.961	0.859
Scaling 1.1	0.781	0.758	0.844
Shearing x 0% y 1%	0.953	0.992	0.875
Shearing x 1% y 1%	0.813	0.906	0.797
Affine geometric transform (1.013 0.008 0.011 1.008)	0.844	0.914	0.765
Rotation, scaling, translation 5deg+80%+[0, 25]	0.859	0.898	0.828

Tab. 1. Performance of the proposed watermarking scheme under various attacks. [1] represents lena, [2] represents baboon, [3] represents peppers.

Simulation results under various image attacks compared with Qi's method [8] are shown in Tab. 2 and Tab. 3. All the results will be recorded as "pass" or "fail" to give an intuitive comparison. Tick represents "pass" and blank cell represents "fail" or no result provided by the author. For the ease of comparison, the method with more "passes" has a better performance. As shown in Tab. 2, our scheme performs well under common image processing attacks, such as median filtering, mean filtering, and Gaussian filtering, JPEG compression down to a quality factor of 40%. It also

performs well under some combined common image processing, including image filter plus JPEG compression, enhancement plus JPEG compression. The robustness against common image processing attacks can be further improved with a stronger embedding factor and stable feature points matching. Tab. 3 lists our watermarking scheme's performance compared with Qi's method under geometric distortion, which includes rotation, scaling, shearing, cropping, and affine geometric transform, even some combined of these attacks.

Attack category	Attack name	Qi's			Proposed		
		lena	baboon	pepper	lena	baboon	pepper
Image filtering	Median filtering 3×3	√	√	√	√	√	√
	Median filtering 5×5				√	√	√
	Gaussian filtering 3×3	√	√	√	√	√	√
	Mean filtering 3×3	√	√	√	√	√	√
JPEG compression	90%	√	√	√	√	√	√
	70%	√	√	√	√	√	√
	50%	√	√	√	√	√	√
	40%	√	√	√	√	√	√
Image filtering+JPEG 70%	Median filtering 3×3	√	√	√	√	√	√
	Gaussian filtering 3×3	√	√	√	√	√	√
Image enhancement+JPEG 70%	Histogram equalization	√	√	√	√	√	√

Tab. 2. The experiment results compared to Qi's method under various common signal processing.

Attack category	Attack name	Qi's			Proposed		
		lena	baboon	pepper	lena	baboon	pepper
Rotation	1 deg	√	√	√	√	√	√
	15 deg	√	√	√	√	√	√
Scaling	0.8	√	√	√	√	√	√
	1.1	√	√	√	√	√	√
Rotation + cropping	10 deg	√	√	√	√	√	√
	45 deg	√	√	√	√	√	√
Shearing	x 0% y 1%	√	√		√	√	√
	x 5% y 5%				√	√	√
Centered cropping	5%	√	√	√	√	√	√
	10%	√	√	√	√	√	√
Affine geometric transform	(1.013 0.008 0.011 1.008)	√	√	√	√	√	√
	(1.010 0.013 0.009 1.011)		√	√	√	√	√
Rotation, scaling, translation	5deg+80%+[0, 25]	√	√	√	√	√	√

Tab. 3. The experiment results compared to Qi's method under different geometric distortions, such as rotation, scaling, shearing and so on.

The robustness of the proposed scheme is due to the following factors: (1) The exact feature points matching in our method guarantee a good performance of image restoration. (2) The DFT domain ensures more resistance to translation and moderate cropping. However, our watermarking scheme fails the JPEG compression with a quality factor lower than 30% due to the mismatch of feature points, and local geometric distortion due to that local geometric distortion can not be written as formula (6).

5. Conclusions

The major contribution is that we have proposed a robust watermarking scheme which resists to both geometric distortion and common signal processing attacks. In our scheme, three pairs of matched SIFT feature points are used to evaluate the geometric transformation and to restore the approximate original image. The watermark is inserted into the middle frequency coefficients of the image DFT domain.

Watermark detection is also achieved in the same domain and the original image is not needed. Experiment simulation results have demonstrated its robustness to rotation, scaling, translation, affine geometric transform and various image processing attacks. Besides, our watermarking scheme satisfies the demand of real-time. Our scheme can be further improved by enhance the performance of image interpolation algorithm and image restoration. Future work will focus on image restoration against local geometric distortion attacks.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (60736016, 60873198, 60973128, 60973113, 61070196, and 61073191), National Basic Research Program 973 (2009CB326202, 2010CB334706).

References

[1] PETITCOLAS, F. A. P., ANDERSON, R. J., KUHN, M. G. Attacks on copyright marking systems. *Information Hiding*, 1998, vol. 1525, p. 218-238.

[2] PEREIRA, S., PUN, T. Fast robust template matching for affine resistant image watermarks. *Information Hiding, Proceedings*, 2000, vol. 1768, p. 199-210.

[3] LIN, C. Y., WU, M., BLOOM, J. A., COX, I. J., MILLER, M. L., LUI, Y. M. Rotation, scale, and translation resilient public watermarking for images. *Security and Watermarking of Multimedia Contents*, 2000, vol. 3971, p. 90-98.

[4] ALGHONIEMY, M., TEWFIK, A. H. Image watermarking by moment invariants. In *Proceedings 2000 International Conference on Image Processing (ICIP 2000)*. Vancouver (Canada), 2000, p. 73-76.

[5] SINGHAL, N., YOUNG-YOON LEE, CHANG-SU KIM, SANG-UK LEE Robust image watermarking based on local zernike moments. In *Proceedings of IEEE 9th Workshop on Multimedia Signal Processing (MMSP 2007)*. Chania Crete (Greece), 2007, p. 401-404.

[6] KUTTER, M., BHATTACHARJEE, S. K., EBRAHIMI, T. Towards second generation watermarking schemes. In *Proceedings 1999 International Conference on Image Processing (ICIP 1999)*. Manchester (United Kingdom), 1999, p. 320-323.

[7] BAS, P., CHASSERY, J. M., MACQ, B. Geometrically invariant watermarking using feature points. *IEEE Transactions on Signal Processing*, 2002, vol. 11, no. 9, p. 1014-1027.

[8] QI, X. J., QI, J. A robust content based digital image watermarking scheme. *Signal Processing*, 2007, vol. 87, no. 6, p. 1264-1280.

[9] WANG, X. Y., HOU, L. M., WU, J. A feature-based robust digital image watermarking against geometric attacks. *Image and Vision Computing*, 2008, vol. 26, p. 980-989.

[10] TANG, CH. W., HANG, H. M. A feature-based robust digital image watermarking scheme. *IEEE Transactions on Signal Processing*, 2003, vol. 51, no. 4, p. 950-959.

[11] HAE-YEOUN LEE, HYUNGSHIN KIM, HEUNG-KYU LEE Robust image watermarking using local invariant features. *Optical Engineering*, 2006, vol. 45, no. 3, 1-11.

[12] DENG, CH., GAO, X. B. TAO, D. CH., LI, X. L. Geometrically invariant watermarking using affine covariant regions. In *Proceedings of 15th IEEE International Conference on Image Processing (ICIP 2008)*. California, 2008, p. 413-416.

[13] PING DONG, BRANKOV, J. G., GALATSANOS, N. P., YONGYI YANG, DAVOINE, F. Digital watermarking robust to geometric distortions. *IEEE Transactions on Image Processing*, 2005, vol. 14, no. 12, p. 2140-2150.

[14] COX, I. J., KILIAN, J., LEIGHTON, F. T., SHAMOON, T. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 1997, vol. 6, no. 12, p. 1673-1687.

[15] LOWE, D. G. Distinctive image features from scale-invariant keypoints. *International Journal of Computer Vision*, 2004, vol. 60, no. 2, p. 91-110.

[16] YAVUZ, E., TELATAR, Z. SIFT based geometric distortion correction method. In *Proceedings of 23rd International Symposium on Computer and Information Sciences (ISCIS'08)*. Istanbul (Turkey), 2008, p. 1-4.

[17] PETITCOLAS, F. A. P. *StirMark* 4.0 (2008), Available at: http://www.petitcolas.net/fabien/watermarking/stirmark/.

About Authors…

Haijun LUO was born in Hunan, China, 1985. He is currently pursuing a M.S. degree in Computer Application at School of Computer and Communication from Hunan University, China. His research interests include Digital Watermarking, and Information Hiding.

Xingming SUN was born in Hunan, China, 1963. He received the B.S. degree in Mathematics from Hunan Normal University, China, in 1984, the M.S. degree in Computing Science from Dalian University of Science and Technology, China, in 1988, and the Ph. D. degree in Computing Science from Fudan University, China, in 2001. He is currently a Professor at the School of Computer and Communication, Hunan University, China. His research interests include Network & Information Security, Digital Watermarking, Wireless Sensor Network Security, and Natural Language Processing.

Hengfu YANG was born in Hunan, China, 1974. He received the M.S. degree in Computer Application from Guizhou University, China, in 2003, and the Ph. D. degree in Computer Application from Hunan University, China, in 2009. He is currently a lector at the Department of Information Science and Engineering, Hunan First Normal University, P. R. China. His research interests include Information Hiding, Information Security, Digital Watermarking, Multimedia and Image Processing.

Zhihua XIA was born in Hunan, China, in 1983. He received his B.S. in Hunan City University, China, in 2006, and is currently pursuing his Ph.D. in Computer Science and technology at the School of Computer and Communication of Hunan University, China. His research interests include Steganography and Steganalysis, digital forensic, image processing, and pattern recognition.