Geometrically robust image watermarking by sector-shaped partitioning of geometric-invariant regions

Huawei Tian, Yao Zhao, Rongrong Ni, and Gang Cao

Institute of Information Science, Beijing Jiaotong University, Beijing, China, 100044
hwtian@live.cn

Abstract: In a feature-based geometrically robust watermarking system, it is a challenging task to detect geometric-invariant regions (GIRs) which can survive a broad range of image processing operations. Instead of commonly used Harris detector or Mexican hat wavelet method, a more robust corner detector named multi-scale curvature product (MSCP) is adopted to extract salient features in this paper. Based on such features, disk-like GIRs are found, which consists of three steps. First, robust edge contours are extracted. Then, MSCP is utilized to detect the centers for GIRs. Third, the characteristic scale selection is performed to calculate the radius of each GIR. A novel sector-shaped partitioning method for the GIRs is designed, which can divide a GIR into several sector discs with the help of the most important corner (MIC). The watermark message is then embedded bit by bit in each sector by using Quantization Index Modulation (QIM). The GIRs and the divided sector discs are invariant to geometric transforms, so the watermarking method inherently has high robustness against geometric attacks. Experimental results show that the scheme has a better robustness against various image processing operations including common processing attacks, affine transforms, cropping, and random bending attack (RBA) than the previous approaches.

OCIS codes: (100.0100) Image Processing; (100.2000) Digital Image Processing; (100.5760) Rotation-invariant Pattern Recognition.

References and links

1. J. Dugelay, S. Roche, C. Rey, and G. Doerr, "Still-image watermarking robust to local geometric distortions," IEEE Trans. Image Process. **15**(9), 2831–2842 (2006).
2. M. Barni, "Effectiveness of exhaustive search and template matching against watermark desynchronization," IEEE Signal Process. Lett. **12**(2), 158–161 (2005).
3. J. Ruanaidh, and T. Pun, "Rotation, scale and translation invariant spread spectrum digital image watermarking," Signal Processing **66**(3), 303–317 (1998).
4. D. Zheng, J. Zhao, and A. Saddik, "Rst-invariant digital image watermarking based on log-polar mapping and phase correlation," IEEE Trans. Circuits Syst. Video Technol. **13**(8), 753–765 (2003).
5. C. Y. Lin, M. Wu, J. Bloom, I. Cox, M. Miller, and Y. Lui, "Rotation, scale, and translation resilient watermarking for images," IEEE Trans. Image Process. **10**(5), 767–782 (2001).
6. M. Alghoniemy, and A. Tewfik, "Image watermarking by moment invariants", in *Proceedings of IEEE International Conference on Image Processing* (Vancouver, BC, Canada,2000), pp.73–76.
7. M. Alghoniemy, and A. H. Tewfik, "Geometric invariance in image watermarking," IEEE Trans. Image Process. **13**(2), 145–153 (2004).
8. L. Zhang, G. Qian, W. Xiao, and Z. Ji, "Geometric invariant blind image watermarking by invariant Tchebichef moments," Opt. Express **15**(5), 2251–2261 (2007), http://www.opticsinfobase.org/oe/abstract.cfm?URI=oe-15-5-2251.
9. H. Kim, and H. Lee, "Invariant image watermark using zernike moments," IEEE Trans. Circuits Syst. Video Technol. **8**, 766–775 (2003).
10. Y. Xin, S. Liao, and M. Pawlak, "Circularly orthogonal moments for geometrically robust image watermarking," Pattern Recognit. **40**(12), 3740–3752 (2007).

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

11. S. Pereira, and T. Pun, “Robust template matching for affine resistant image watermarks,” IEEE Trans. Image Process. **9**(6), 1123–1129 (2000).
12. M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi, “Towards second generation watermarking schemes”, in *Proceedings of IEEE International Conference on Image Processing* (Kobe, Japan, 1999), pp. 320–323.
13. P. Bas, J. Chassery, and B. Macq, “Geometrically invariant watermarking using feature points,” IEEE Trans. Image Process. **11**(9), 1014–1028 (2002).
14. C. Tang, and H. Hang, “A feature-based robust digital image watermarking scheme,” IEEE Trans. Signal Process. **51**(4), 950–959 (2003).
15. J. S. Seo, C. D. Chang, and D. Yoo, “Localized image watermarking based on feature points of scale-space representation,” Pattern Recognit. **37**(7), 1365–1375 (2004).
16. J. Weinheimer, X. Qi, and J. Qi, “Towards a robust feature-based watermarking scheme”, in *Proceedings of IEEE International Conference on Image Processing* (Atlanta, GA, USA, 2006), pp. 1401–1404.
17. X. Qi, and J. Qi, “A robust content-based digital image watermarking scheme,” Signal Processing **87**(6), 1264–1280 (2007).
18. X. Wang, J. Wu, P. Niu, “A new digital image watermarking algorithm resilient to desynchronization attacks,” IEEE Trans. Info. Forens. Sec. **4,** 655–663 (2007).
19. C. Schmid, R. Mohr, and C. Bauckhage, “Evaluation of interest point detectors,” Int. J. Comput. Vis. **37**(2), 151–172 (2000).
20. H. Lee, I. Kang, H. Lee, and Y. Suh, “Evaluation of feature extraction techniques for robust watermarking”, in *Proceedings of 4th Int. Workshop on Digital Watermarking*(Siena, Italy, 2005), pp. 418–431.
21. X. Zhang, M. Lei, D. Yang, Y. Wang, and L. Ma, “Multi-scale curvature product for robust image corner detection in curvature scale space,” Pattern Recognit. Lett. **28**(5), 545–554 (2007).
22. K. Mikolajczyk, and C. Schmid, “Scale & affine invariant interest point detectors,” Int. J. Comput. Vis. **60**(1), 63–86 (2004).
23. B. Chen, and G. W. Wornell, “Preprocessed and postprocessed quantization index modulation methods for digital watermarking,” SPIE **3971**, 48–59 (2000).
24. R. C. Gonzalez, R. E. Woods, and S. L. Eddins, “Digital Image Processing Using MATLAB”, in *Prentice Hall*, (New Jersey, 2003).
25. F. Mokhtarian, and A. Mackworth, “A theory of multiscale, curvature-based shape representation for planar curves,” IEEE Trans. Pattern Anal. Mach. Intell. **14**(8), 789–805 (1992).
26. R. M. Haralick, K. Shanmugam, and I. Dinstein, “Textural features for image classification,” IEEE Trans. Syst. Man Cybern. **3**(6), 610–621 (1973).
27. A. Tinku, and K. Ajoy, “Image processing principles and applications”, John Wiley and Sons Inc., (New Jersey, 2005).
28. F. A. P. Petitcolas, and R. J. Anderson, “Evaluation of copyright marking systems”, in *Proceedings of IEEE Multimedia Systems* (Florence, Italy, 1999), pp. 574–579.
29. M. Hsieh, and D. Tseng, “Perceptual digital watermarking for image authentication in electronic commerce,” Electron. Commerce Res. **4**(1/2), 157–170 (2004).

1. Introduction

Digital media is widely spread along with the booming development of computer science and Internet technology. However, unrestricted reproduction and convenient manipulation of digital media cause a considerable financial loss to the media creators and the content providers. Digital watermarking is introduced to safeguard such loss. Applications of digital watermarking include copyright protection, fingerprinting, content authentication, copy control and broadcasting monitoring.

The watermarking runs on two basal characteristics, namely fidelity and robustness. Fidelity can be seen as the perceptual similarity between the original and the watermarked images. Robustness means the resistibility of the watermarking to all the intentional and accidental attacks including geometric distortions, such as rotation, scaling, translation, RBA, cropping, etc, and common image processing attacks, such as JPEG compression, low-pass filtering, noise addition, etc. Generally speaking, geometric attacks break the synchronization between the encoder and the decoder, therefore the detector fails to extract the watermark, even if it still exists. Unlike geometric attacks, common image processing attacks make the watermarking inefficient by reducing its energy rather than introducing synchronization errors.

Though most of the previous robust watermarking schemes perform well under common image processing attacks, they are fragile against geometrical attacks. Geometrical distortion is the Achilles heel for many watermarking schemes [1]. Nowadays, approaches counterattacking geometric distortions can be roughly divided into five groups: *exhaustive search watermarking*,

#115773 - $15.00 USD   Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

invariant-domain-based watermarking, moment-based watermarking, template-based watermarking, and feature-based watermarking.

1) *Exhaustive search watermarking:* One obvious solution to resynchronization is to randomly search for the watermark in the space including a set of acceptable attack parameters. One concern in the exhaustive search [2] is the computational cost in the large search space. Another is that it dramatically increases the false alarm probability during the search process.

2) *Invariant-domain-based watermarking:* Researchers have embedded the watermark in affine invariant domains, such as the Fourier-Mellin transform domain, to achieve robustness to affine transforms [3–5]. Despite that they are robust against global affine transforms, these techniques are usually difficult to implement and vulnerable to cropping and RBA.

3) *Moment-based watermarking:* These methods utilize the geometric invariants of the image, such as geometrical moments [6, 7], Tchebichef moments [8] and Zernike moments [9,10], to prevent the synchronization between the watermark and its cover image. Watermarking techniques utilizing invariant moments are usually vulnerable to cropping and RBA.

4) *Template-based watermarking:* In this kind of watermarking schemes, additional templates are often intentionally embedded into cover images [11]. As anchor points for the alignment, these templates assist the watermark synchronization in detection process. However, for cropping, the template may lose its role due to the permanent loss of cropped image content.

5) *Feature-based watermarking:* This kind of techniques is also called the second generation scheme [12], and our approach belongs to this class. The basic strategy is to bind a watermark with the geometrically invariant image features, so the detection of the watermark can be conducted with the help of the features [13–15].

In general, feature-based watermarking algorithms are the best approaches to resist geometric distortions, because feature points provide stable references for both watermark embedding and detection [16]. In such algorithms, a challenging task is how to find GIRs which are robust under a broad range of image processing operations typically employed to attack watermarking schemes. Harris detector and Mexican hat wavelet method are two efficient methods to extract robust feature regions [13, 14, 17, and 18,]. The Harris detector is stable under majority attacks; however, the feature regions detected can hardly survive under scaling distortion [19]. The Mexican Hat wavelet method is stable under noise-like processing, yet it is sensitive to some affine transforms [20]. These two feature extracting methods have been applied in watermarking. Bas *et al.* used Harris detector to extract features and Delaunay tessellation to define watermark embedding regions [13]. Tang *et al.* used the Mexican hat wavelet method to extract feature points, and several copies of the watermark are embedded in the normalized regions [14]. An image-content-based adaptive embedding scheme is implemented in discrete Fourier transform (DFT) domain of each perceptually high textured subimage [17]. An image-texture-based adaptive Harris corner detector is used to extract geometrically significant feature points, which can determine the possible geometric attacks with the aid of the Delaunay-tessellation-based triangle matching method. The watermark is detected in the geometric correction image.

In this paper, we develop a novel robust watermarking scheme based on MSCP [21], characteristic scale selection [22] and sector-shaped partitioning. Instead of commonly used Harris detector or Mexican hat wavelet method, a more robust corner detector MSCP is adopted to extract salient features in this paper. Based on such features, a disk-like GIRs detecting method is designed, which consists of three steps. First, robust edge contours are extracted.

Then, a robust corner detector in curvature scale space is utilized to detect the centers for GIRs. Third, the characteristic scale selection is performed to calculate the radius of each GIR. A novel sector-shaped partitioning method for the GIRs is developed, which can divide a GIR into several sector discs with the help of the most important corner (MIC). The watermark message is then embedded in each sector by using Quantization Index Modulation (QIM) [23]

The paper is organized as follows: Section 2 presents an overview of the proposed watermarking scheme, Section 3 covers the details of the GIRs detection, Section 4 is the descriptions of the GIR partition, and Section 5 describes the details of watermark embedding and detection procedure. Some important parameters are analyzed in Section 6. The experimental results comparing our scheme with Tang's scheme [14] and Qi's scheme [17] are shown in Section 7. Lastly, Section 8 concludes the paper.

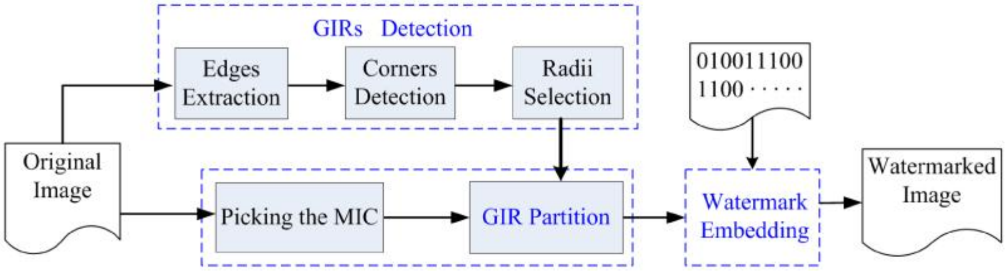


Fig. 1. Watermark embedding framework.

2. An overview of the proposed approach

Figure 1 is an overview of our proposed watermark embedding scheme. The watermark embedding scheme consists of three main steps: GIRs detection, GIR partition and watermark embedding. First, the contours of the objects of interest in the original image are extracted. Then, the corners of the contours are detected by MSCP and selected as the centers of GIRs. Third, the characteristic scale are determined and used to calculate the radius of each GIR. A new sector-shaped partitioning of the GIRs is accomplished with the help of the MIC which is picked from the image corners. Finally, the watermark bits are embedded in the sectors with QIM.

The watermark extracting process resembles watermark embedding, which comprises three main steps: GIRs detection, GIR partition and watermark extraction. Firstly, GIRs are detected as watermark embedding process. Then GIRs are partitioned according to the length of the watermark sequence. Lastly, the watermark bits are extracted with the voting measure.

3. GIRs detection

Detecting the GIRs is the linchpin, upon which a watermarking scheme's success or failure depends. There are some salient features in an image such as corner points, edges, and regions, which are the vital parts of the image. In this paper, instead of commonly used Harris detector or Mexican hat wavelet method, a more robust curvature corner detector called MSCP is adopted to extract salient features. The GIRs are constructed by taking the feature points as centers. Generally speaking, the GIRs can be in any shape, such as triangle, rectangle, hexagon, and circle, but it is important to ensure that the region is invariant to rotation. Thus, the disk-shaped GIRs are selected to embed watermark in this paper. The characteristic scale is then calculated to determine the radii of GIRs. Since the characteristic scale varies proportionally with the image zoom-scale, the detected GIRs cover the same contents even if the image is zoomed.

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

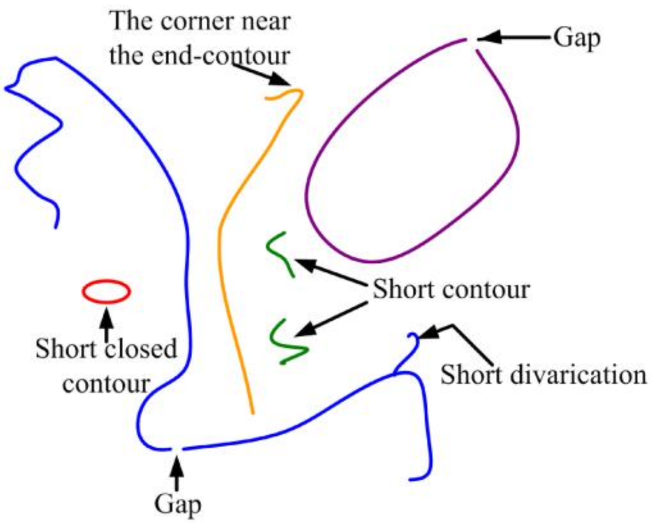


Fig. 2. Exceptive edge contours.

3.1 Robust edge contours extraction

At first, the Canny edge detector [24] is applied to the gray level image and a binary edge-map is obtained. From a large number of experiments, we find that the gap, the short contour, the short closed contour and the short divarication as shown in Fig. 2 are unstable. Post processings, such as filling in the gaps, deleting the short contours, deleting the short closed contours and deleting the short divarications, are implemented to ensure the robustness.

3.2 Robust corners detection

The MSCP corner detector [21] in curvature scale space is used to extract the corner of the contour. At the beginning, let Γ represent a regular planar curve which is parameterized by the arc length u, so $\Gamma(u) = (x(u), y(u))$. Then we quote the definition of curvature from [25] as

$$k(u,\sigma) = \frac{X_u(u,\sigma)Y_{uu}(u,\sigma) - X_{uu}(u,\sigma)Y_u(u,\sigma)}{(X_u(u,\sigma)^2 + Y_u(u,\sigma)^2)^{1.5}} \tag{1}$$

where $X_u(u,\sigma) = x(u) * g_u(u,\sigma)$, $X_{uu}(u,\sigma) = x(u) * g_{uu}(u,\sigma)$, $Y_u(u,\sigma) = y(u) * g_u(u,\sigma)$, $Y_{uu}(u,\sigma) = y(u) * g_{uu}(u,\sigma)$ and $*$ is the convolution operator, while $g(u,\sigma)$ denotes a Gaussian function with zero mean and deviation σ, and $g_u(u,\sigma)$, $g_{uu}(u,\sigma)$ are the first and second derivatives of $g(u,\sigma)$ respectively.

Let $g(u,\sigma_j)$ denote the Gaussian function $g(u)$ dilated by a scale factor σ_j, i.e., $g(u,\sigma_j) = \frac{1}{\sigma_j\sqrt{2\pi}} e^{\frac{-u^2}{2\sigma_j^2}}$, where $j = 1, 2, \cdots$. According to [21], we can compute the curvature at the *j*th scale, and we have the MSCP as

$$P_N(u) = \prod_{j=1}^{N} k(u,\sigma_j) \tag{2}$$

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

To begin with, MSCP $P_N(u)$ at N scales are computed on each edge contour. Then, consider those maxima as initial corners whose absolute MSCP are above a threshold T. But some corners from MSCP are not robust enough for watermarking synchronization. So we should perform post processing to select more robust corners. This is accomplished by the following steps:

1) Avoid selecting the corners near borders. For example, a corner that falls within 20% of the image width/height from the border is not considered because the corner might be removed due to cropping attacks.

2) Discard the corners near the end-contours. For example, a corner that falls within 1/8 of the length of the edge contour from the end is not considered as a robust corner. The end-contour shape deforms sharply due to geometrical attacks.

3) Remove one of the two near corners. If the distance between two corners is shorter than the minimal diameter $2R_{\min}$ of circular regions (which will be discussed in detail in Section 3.3 and Section 6.3), remove the corner with less multi-scale curvature product.

3.3 Radii selection

The characteristic scale is used to determine the radius of each GIR because it varies proportionally with the image scale. So the same content region can be detected even if the image is zoomed. In [22], Mikolajczyk *et al.* used the LoG (Laplacian-of-Gaussians) to select the characteristic scale. The LoG is defined as

$$LoG(x,y,\delta_i) = \delta_i^2 \,|\, L_{xx}(x,y,\delta_i) + L_{yy}(x,y,\delta_i) \,| \qquad (3)$$

Given a set of scales δ_i, the characteristic scale δ is the scale at which LoG attains the extreme.

The radius of the GIR is defined as

$$R = k \cdot \delta \qquad (4)$$

where R is the radius of the GIR, δ is the characteristic scale, and k is a positive number, which is used to adjust the radius of the GIR. If k is too small, the GIR could be small, which results in less robustness of the watermarking scheme. Whereas if k is too large, the fidelity decreases. Therefore, there is a tradeoff between robustness and fidelity. Besides, the interference among GIRs should be avoided. Therefore we can get well-pleasing radii by the following algorithm:

```
$k = k_0$
$WHILE \quad k \cdot \delta < R_{\min}$
        $k = k + 1$
$END$
$WHILE \quad k \cdot \delta > R_{\max}$
        $k = k - 1$
$END$
$R = k \cdot \delta$
```

where

$$R_{\min} = lower \cdot \min(height, width) \qquad (5)$$

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

$$R_{\max} = upper \cdot \max(height, width) \tag{6}$$

where *height* and *width* are the image's height and width respectively. Both *lower* and *upper* are predefined. Now, each radius is kept between $R_{\min}$ and $R_{\max}$. k_0 is essentially a secret key, and the receiver who doesn't know it will not be able to generate accurate GIRs.

GIRs detection algorithm consists of these three steps: robust edge contours extraction, robust corners detection and radii selection. They are all autonomous without user intervention. So, GIRs can be extracted without specially tuning the algorithm for any image. The details will be discussed carefully in Section 6. Figure 3 shows the performance of GIRs detection. In Fig. 3, Fig. 3(a) is the original Lena image and Fig. 3(b) illustrates the GIRs of Lena image using GIRs detection algorithm. Figure 3(c)-Fig. 3(l) are the distorted visions of Lena by some typical geometric transforms and their detected GIRs. The circular regions are selected GIRs, and non-GIRs are shown in black. Figure 3(m)-Fig. 3(p) are the original Baboon and Peppers images and their GIRs. From Fig. 3, it can be easily found that the GIRs are detected robustly even with rotation, scaling, cropping, rotation plus cropping and RBA from different texture categories images.

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

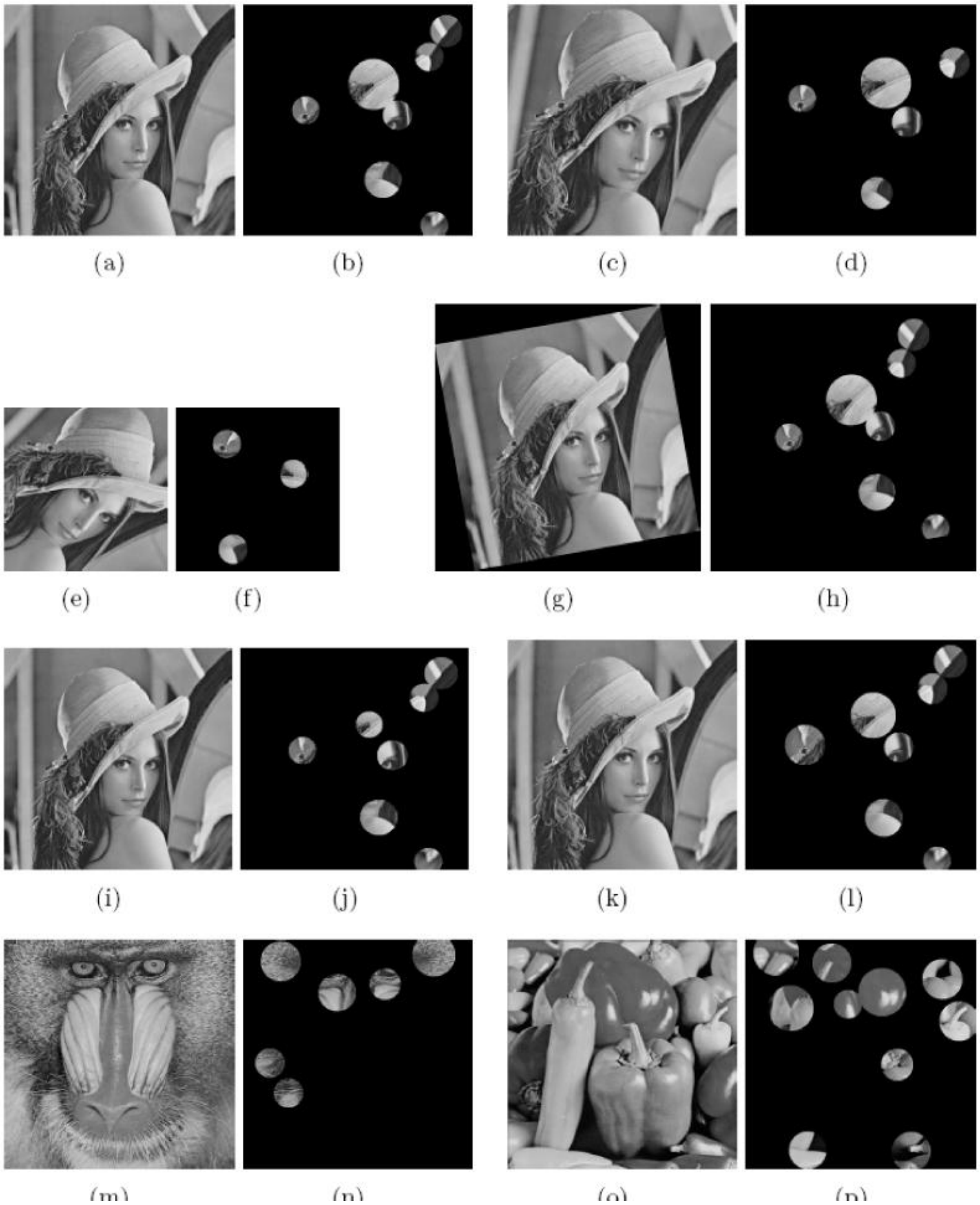


Fig. 3. Performance of GIRs detection. (a)Original Lena image. (b)GIRs of (a). (c)Rotated by 10 degree plus cropping and scaling. (d)GIRs of (c). (e)Rotated by 45 degrees plus cropping. (f)GIRs of (e). (g)Rotated by −10 degrees. (h)GIRs of (g). (i)Removed 17 rows and 5 columns. (j)GIRs of (i). (k)StirMark RBA. (l)GIRs of (k). (m)Original Baboon image. (n)GIRs of (m). (o)Original Peppers image. (p)GIRs of (o).

4. GIR partition

In this section, we introduce a method of GIR partition. First, the MIC is picked. Subsequently, each GIR is divided into several sector discs with the help of the image MIC.

4.1 The MIC picking

In order to partition the GIR, we need pick one corner named MIC as a referenced point from all robust corners detected in Section 3.2. The MIC is very pivotal to the GIR partition and the watermark embedding and extraction, so we must be cautious to pick the MIC. Primarily, the corners near borders of the image are unavailable because the corners might be removed due to rotation and cropping attacks. Second, the center part of the image is more stable, because it is not usually cropped. Consequently, the corner which is nearest to the center of the image is defined as the MIC. Because the MIC is the most robust corner, a GIR can be divided into several sector discs with its help.

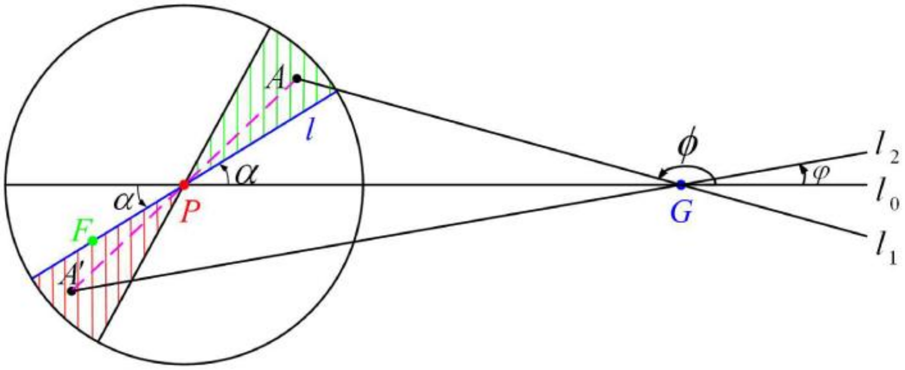


Fig. 4. The GIR partition.

4.2 The GIR partition

As shown in Fig. 4, baseline l_0 joins the center of the circular GIR P and the image MIC G. Suppose that F is an arbitrary pixel and line l goes cross F and P. Two lines l_0 and l intersect at P and form four angles, which are two pairs of opposite vertical angles. We define the angle from l_0 to l as α, which is formed via the line l_0 counterclockwise rotating to l. So that

$$\tan\alpha = \frac{k_l - k_{l_0}}{1 + k_l k_{l_0}} \tag{7}$$

where k_{l_0} and k_l are the slopes of the lines l_0 and l respectively.

Let l_0 be the initiative line which joins the point P and the point G, take the counterclockwise direction as forward direction, and averagely divide the circular region into N pairs of sector discs according to Eq. (7), whose central angle is θ, $\theta = \frac{\pi}{N}$. Pixel F falls in the n*th* sector pair, if $\frac{(n-1)\pi}{N} \le \alpha \le \frac{n\pi}{N}$, where $n = 1, 2, \cdots, N$. As shown in Fig. 4, any pair of sector discs, which contain the point A and A', is symmetrical.

It is easy to distinguish two symmetrical sector discs. The line l_1 connects A and G, and the line l_2 connects A' and G. The angle from l_0 to l_1 is ϕ, and the angle from l_0 to l_2 is φ. Apparently $\phi > \pi/2$ and $\varphi < \pi/2$, so that the points in symmetrical sector discs are distinguished and the circular region contains $2N$ sector discs.

Without the help of the referenced point, the GIR centered in the MIC cannot be partitioned. The corner which is the nearest to the center of the image except the MIC can be picked as the referenced point. Now, the GIR centered in the MIC can be also partitioned using the above scheme.

5. Watermark embedding and extraction

5.1 Watermark embedding

From the communication model of watermarking, we regard all GIRs as independent communication channels. To improve the robustness of the transmitted watermark sequence $W = (w_0 w_1 \cdots w_i \cdots w_{2N})$, where $w_i \in \{0,1\}$, the sequence is repeatedly embedded in each GIR. If the length of the watermark sequence is not even, a "0" is appended to the tail of the watermark sequence. During the watermark extraction process, we claim the existence of watermark if at least two copies of the embedded watermark sequences are correctly detected. Each watermark bit will be embedded in all pixels of each sector discs using QIM [23].

First, we construct two quantizers $Q(.;w)$, where $w \in \{0,1\}$. In this paper, we consider the case where $Q(.;w)$ is a uniform, scalar quantizer with stepsize Δ and the quantizer set consists of two quantizers shifted by $\Delta/2$ with respect to each other. Δ is pre-defined and known to both embedder and extractor, meanwhile it affects the robustness to common signal processing and the quality of the watermarked image. In order to further increase the robustness while ensuring the fidelity, the property of Human Visual System (HVS) is considered in choosing the stepsize, so the stepsize should be different for images with different textures.

For Sector n, according to the corresponding watermark bit w_n, each pixel $f(x,y)$ is quantized with quantizer $Q(.;w_n)$.

$$f_w(x,y) = Q(f(x,y);w_n) \tag{8}$$

After every pixel in GIRs is quantized, the watermark embedding process is finished.

5.2 Watermark extraction

The extracting process resembles watermark embedding, which consists of three main steps: GIRs detection, GIR partition and watermark extraction. GIRs are detected as watermark embedding. If the length of the watermark sequence is $2N$ (if it is $2N-1$, a "0" is appended to the tail of the watermark sequence, and then it becomes $2N$), each GIR is then divided into $2N$ sector discs. For each pixel $f_w(x,y)$ in Sector n, determine the embedded watermark bit with QIM. If $|f_w(x,y) - Q(f_w(x,y);1)| \leq |f_w(x,y) - Q(f_w(x,y);0)|$, the watermark bit embedded in this pixel is 1. Else the watermark bit is ascertained to be 0. When geometrical distortions or/and common image processing attacks occur, even in a same sector disc, some pixels are detected to embed bit 1, and some pixels are detected to embed bit 0. Let $Num_n(1)$ denote the number of pixels hiding bit 1 in Sector n and $Num_n(0)$ denote the number of pixels hiding bit 0 in Sector n. The *n*th bit of watermark sequence is extracted as

$$\hat{w}_n = \begin{cases} 1, & if\ Num_n(1) \geq Num_n(0) \\ 0, & if\ Num_n(1) < Num_n(0) \end{cases} \tag{9}$$

From the image watermarking point of view, the alteration of the pixels value under geometrical distortions or/and common image processing attacks is limited, because the attacked image should keep an acceptable level of visual quality. In addition, the watermark embedding and extraction are robust to such limited pixel value alteration, which attributes to the above QIM strategy. As a result, the whole watermarking scheme has a better robustness against various geometrical distortions and image processing operations.

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

6. Parameters analysis

6.1 Parameters of robust edge contours extraction

Canny edge operator [24] exploits a Gaussian filter with a specified standard deviation, σ_0, to smooth the image. The smaller the σ_0 is, the more edges can be extracted. But some of them are not robust enough. In order to extract robust edges, we select σ_0 according to the texture complexity $C_{texture}$ of an image. The higher the image texture complexity is, the larger σ_0 should be selected and vice versa, *viz.* $\sigma_0 \propto C_{texture}$.

The ridge pixels of Canny edge detector are thresholded with two values, T_1 and T_2, where $T_1 < T_2$. Ridge pixels with values greater than T_2 are said to be "strong" edge pixels, and Ridge pixels with values between T_1 and T_2 are said to be "weak" edge pixels [24]. Experiments demonstrate that the "weak" edges are not robust enough to resist geometric distortions and common image processing attacks. In order to discard the "weak" edge pixels and only get "strong" edge pixels, the difference between T_1 and T_2 should be very small (i.e. $T_1 = 0.299, T_2 = 0.300, T_2 - T_1 = 0.001$) and T_1 and T_2 should be selected according to the texture complexity of an image. The higher the image texture complexity is, the larger T_1 and T_2 should be and vice versa, *viz.* $T_1 \propto C_{texture}$ and $T_2 \propto C_{texture}$.

Originally introduced by Haralick et al. [26], gray level co-occurrence matrix (GLCM) measures the second-order texture characteristics of an image which plays an important role in human vision, and has been shown to achieve a high level of classification performance. Entropy measure E_{GLCM} computed from the GLCM yields a measure of complexity and it has been shown that complex textures tend to have high entropy [27], *viz.* $C_{texture} \propto E_{GLCM}$, so $\sigma_0 \propto E_{GLCM}$, $T_1 \propto E_{GLCM}$ and $T_2 \propto E_{GLCM}$. Hence, we can select σ_0, T_1 and T_2 according to the mean-entropy ME_{GLCM} of an image. $ME_{GLCM} = E_{GLCM} / N_p$, where N_p is the number of pixels in an image. Many experiments have been done on some higher texture images and lower texture images. It showed that σ_0 =2, T_1 =0.249 and T_2 =0.250 could achieve good results for the images with $ME_{GLCM} < 1.3$, and σ_0 =10, T_1 =0.349 and T_2 =0.350 could achieve good results for the images with $ME_{GLCM} \geq 1.3$.

6.2 Parameters of the robust corners detection

The MSCP corner detector involves only one important parameter, i.e., the global threshold T. It shows that $T = 0.0003$ can achieve good results for almost all images [21]. The same value of the threshold works well for different test images. The threshold depends on the set of scales. In our experiments, the scale factors σ_j of Gaussian function are also chosen as 2, 2.5 and 3, respectively.

6.3 Parameters of the radii selection

In Eqs. (5) and (6), $lower$ and $upper$ are predefined. They give a bound to the radius of each GIR. If they are too small, the GIRs could be small, which results in less robustness of the watermarking scheme, whereas if they are too large, the fidelity decreases. Besides, the superposition among GIRs should be avoided. Experiments show that $lower \approx 5.9\%$ and $upper \approx 11.7\%$ give good results for 512×512 images. At the same time, k_0 is essentially a secret key. Users can select it discretionarily and the receiver without it cannot generate GIRs accurately.

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

6.4 Parameters of watermark extraction

Two kinds of errors are possible in the watermark extraction: the *false-alarm* probability (no watermark embedded but one extracted) and the *miss* probability (watermark embedded but none extracted). Simplified models are thus assumed in choosing the extraction parameters with the method of paper [14], as shown below.

False-alarm probability: For an unwatermarked image, the extracted bits are assumed to be independent Bemoulli random variables with the same "success" probability P_s. It is called a "success" if the extracted bit matches the embedding watermark bit. We further assume the success probability P_s is 1/2. Let *r* be the numbers of matching bits in a GIR. Then based on the Bemoulli trials assumption, *r* is an independent random variables with binomial distribution $P_r = (\frac{1}{2})^{2N} \cdot (\frac{(2N)!}{r!(2N-r)!})$, where $2N$ is the length of the watermark sequence. A GIR is claimed watermarked if the number of its matching bits is greater than a threshold t_s. The false-alarm error probability of a GIR P_{F-GIR} is the cumulative probability of the cases that $r \geq t_s$.

$$P_{F-GIR} = \sum_{r=t_s}^{2N} (\frac{1}{2})^{2N} \cdot (\frac{(2N)!}{r!(2N-r)!}) \tag{10}$$

Furthermore, an image is claimed watermarked if at least m GIRs are detected as "success". Under this criterion, the false-alarm probability of one image is

$$P_{F-image} = \sum_{i=m}^{N_{GIR}} (P_{F-GIR})^i \cdot (1 - P_{F-GIR})^{N_{GIR}-i} \cdot \begin{pmatrix} N_{GIR} \\ i \end{pmatrix} \tag{11}$$

where N_{GIR} is the total number of GIRs in an image. On our experiences, when the parameters are chosen as: $2N = 16, N_{GIR} = 10, m = 2, t_s = 15$, the $P_{F-image} = 3 \times 10^{-6}$ according to Eq. (11).

Miss probability: In an attacked watermarked image, we again assume that the matching bits are independent Bernoulli random variables with equal success probability P_S. The success extraction probability of r bits in a GIR of $2N$ watermarked bits is $P_r = P_s^{\ r} \cdot (1 - P_s)^{2N-r} \cdot (\frac{(2N)!}{r!(2N-r)!})$. A GIR is claimed watermarked if the number of its matching bits is greater than a threshold t_s. The success extraction probability of a GIR P_{S-GIR} is the cumulative probability of the cases that $r \geq t_s$.

$$P_{S-GIR} = \sum_{r=t_s}^{2N} P_r \tag{12}$$

Furthermore, an image is claimed watermarked if at least m GIRs are detected as hiding watermark. So the miss probability of an image is

$$P_{M-image} = 1 - \sum_{i=m}^{N_{GIR}} (P_{S-GIR})^i \cdot (1 - P_{S-GIR})^{N_{GIR}-i} \cdot \begin{pmatrix} N_{GIR} \\ i \end{pmatrix} \tag{13}$$

It is difficult to evaluate the success extraction probability of a watermarked bit P_S, because it depends on the attacks. However, a "typical" success detection probability may be estimated from the experiments on real images with attacks. Because we want to see the extraction performance under geometric distortion, a more difficult case is chosen from Table 3—image Lena, Baboon and Peppers under combined distortions of 1° rotation, cropping, and

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

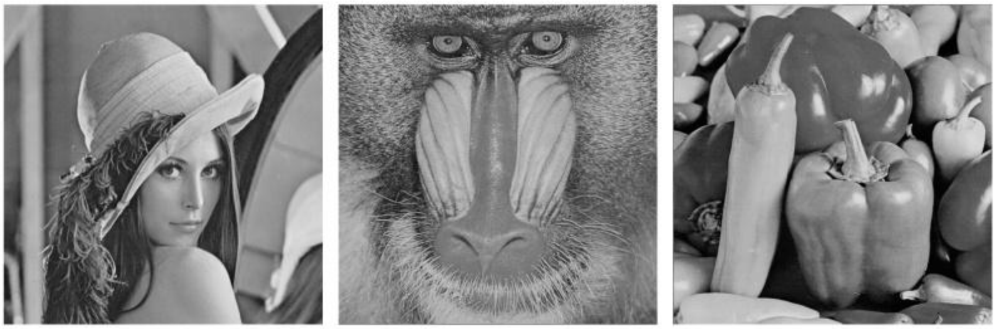
JPEG compression at a quality factor of 70. The simulation is done using ten watermarked Lena image, ten watermarked Baboon image and ten watermarked Peppers image imposed with(randomly generated) different watermarks. The selected value of P_S is the total number of matching bits divided by the total number of embedded bits. In this experiment, we obtain $P_S = 0.8285$. Based on this P_S value, when the parameters are chosen as: $2N = 16, N_{GIR} = 10, m = 2,\ t_s = 15$, the $P_{M-image} = 0.3392$ according to Eq. (13).

7. Experimental results

To evaluate the performance of the proposed watermarking scheme, experiments have been conducted on three standard 8-bit grayscale images (Lena, Baboon and Peppers) of size 512×512 and the StirMark 3.1 [28] is used to test the robustness.

7.1 Watermark fidelity

Watermark fidelity is evaluated on images of Lena, Baboon, and Peppers. These three images correspond to three texture categories. As shown in Fig. 3, we extract 7, 6 and 10 GIRs for Lena, Baboon and Peppers, respectively. Figure 5 demonstrates the performance of our watermarking algorithm. The PSNR values of the watermarked images are 46.0dB, 40.2dB and 42.6dB, respectively. These PSNR values are all much greater than 30.0dB, which is greater than the empirical value for the image without any perceivable degradation [29]. At the same experimental environments and using Qi's method [17], the PSNR values between the original and the watermarked images of Lena, Baboon and Peppers are 43.33, 44.06, and 37.62, respectively.



(a) Lena (b) Baboon (c) Peppers

Fig. 5. The watermarked images

7.2 Important parameters

Table 1. Several images texture dependent parameters

	Lena	Baboon	Peppers
$[T_1, T_2]$	$[0.249, 0.250]$	$[0.349, 0.350]$	$[0.249, 0.250]$
σ_0	2	10	2
k_0	1.5	1.5	1.5
$lower$	5.9%	5.9%	5.9%
$upper$	11.7%	11.7%	11.7%
Δ	12	20	12

The length of the watermark sequence is 8 bits, so each GIR is divided into 8 sector discs for embedding the watermark sequence. The same copy of the 8-bit watermark sequence is

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

embedded in each GIR. When the watermark sequence is set to 16 bits, the parameters should be altered accordingly. To compare the robustness with Qi's method and Tang's method impartially, two different kinds of watermark capacity are configured. Table 1 summarizes the adaptive parameters for the three textured images, where $[T_1, T_2]$ is the threshold of Canny edge detector; σ_0 is the standard deviation of Canny edge detector; k_0, $lower$ and $upper$ are used to adjust the radii of the GIRs in Eq. (4), Eq. (5),and Eq. (6), respectively; Δ is the step size of quantizer $Q(.;s)$.

7.3 Watermark robustness

Experiments of common image processing attacks and geometric distortions have been performed to prove the effectiveness of the proposed watermarking scheme. The experimental results comparing with Tang's method and Qi's are demonstrated in Table 2 and Table 3. If more than two watermark sequences are correctly detected by the watermarking scheme, the experiment is "pass", otherwise it is "fai". "●" indicates a "pass", blank cell means a "fail".

As shown in Table 2, our scheme performs better than Tang's method and is comparable to Qi's method under common image processing attacks, such as median and Gaussian filtering, color quantization, sharpening, and JPEG compression down to a quality factor of 30. It also behaves well under some combined common processing attacks including sharpening plus JPEG compression and image filtering plus JPEG. However, it does not perform very well under additive uniform noise attack, because QIM is fragile against noise addition attack.

Table 2. The comparisons among the proposed method, Tang's method and Qi's method under different common processing attacks. [a]

Attack category	Attack name	Tang's			Qi's			Our		
		1	2	3	1	2	3	1	2	3
Watermarked image	Watermarked image	●	●	●	●	●	●	●	●	●
image filtering	Median filter 2×2		●		●	●	●	●	●	●
	Median filter 3×3		●		●	●	●	●	●	●
	Sharpening 3×3	●	●	●	●	●	●	●	●	●
	Gaussian filter 3×3	●	●		●	●	●	●	●	●
	Mean filter 2×2				●	●	●	●	●	●
	Mean filter 3×3				●	●	●	●	●	●
Quantization	Color quantization	●	●		●	●	●	●	●	●
Additive uniform noise	Scale=0.1	●	●	●	●	●	●			●
	Scale=0.15	●	●	●	●	●	●		●	●
	Scale=0.2		●				●			●
JPEG compression	JPEG 80	●	●	●	●	●	●	●	●	●
	JPEG 70	●	●	●	●	●	●	●	●	●
	JPEG 60	●	●		●	●	●	●	●	●
	JPEG 50	●	●	●	●	●	●	●	●	●
	JPEG 40	●	●		●	●	●	●	●	●
	JPEG 30	●	●		●	●	●	●	●	●
Image filtering + JPEG 90	Median filter 2× 2	●	●		●	●	●	●	●	●
	Median filter 3× 3				●	●	●	●	●	●
	Sharpening 3× 3	●	●	●	●	●	●	●	●	●
	Gaussian filtering 3× 3	●	●		●	●	●	●	●	●

[a] 1, 2 and 3 represent Lena, Baboon, and Peppers, respectively. "●" indicates a "pass", the blank cell means a "fail".

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

Table 3. The comparisons among the proposed method, Tang's method and Qi's method under different geometric distortions.

Attack category	Attack name	Tang's			Qi's			Our		
		1	2	3	1	2	3	1	2	3
Row and column removal	1 rows and 5 columns	●	●	●	●	●	●	●	●	●
	5 rows and 17 columns		●		●	●	●	●	●	●
Centered cropping	5%	●	●	●	●	●	●	●	●	●
	10%	●	●	●	●	●	●	●	●	●
Shearing	x-1%,y-1%	●	●		●	●	●	●	●	●
	x-0%,y-5%	●	●		●	●	●	●	●	●
	x-5%,y-5%		●					●	●	●
Rotation, cropping, and/or scaling	1° +Cropping + Scale		●	●	●	●	●	●	●	●
	1° +Cropping	●	●	●	●	●	●	●	●	●
	2° +Cropping				●	●	●	●	●	●
	5° +Cropping				●	●	●	●	●	●
Linear geometric transform	(1.007, 0.01, 0.01, 1.012)	●	●		●	●	●	●	●	●
	(1.01,0.013,0.009, 1.011)	●	●		●	●	●	●	●	●
	(1.013,0.008,0.011,1.008)	●	●		●	●	●	●	●	●
Row and column removal+JPEG70	1 rows and 5 columns	●	●	●	●	●	●	●	●	●
	5 rows and 17 columns		●		●	●	●	●	●	●
Centered cropping +JPEG 70	5%	●	●	●	●	●	●	●	●	●
	10%	●	●	●	●	●	●	●	●	●
Shearing + JPEG70	x-1%, y-1%	●	●		●	●	●	●	●	●
	X-0%, y-5%	●	●		●	●	●	●	●	●
	x-5%, y-5%							●	●	●
Rotation, cropping, and/or scaling + JPEG 70	1° +Cropping+Scale		●		●	●	●	●	●	●
	1° +Cropping	●	●		●	●	●	●	●	●
	2° +Cropping				●	●	●	●	●	●
	5° +Cropping				●	●	●	●	●	●
Linear geometric transform + JPEG70	(1.007, 0.01, 0.01, 1.012)	●	●		●	●	●	●	●	●
	(1.01,0.013,0.009, 1.011)	●	●	●		●		●	●	●
	(1.013,0.008,0.011,1.008)	●	●			●		●	●	●
Rotation	15°	●	●	●	●	●	●	●	●	●
	35°		●	●	●	●	●	●	●	●
	210°				●	●	●	●	●	●
Scaling	50%							●	●	●
	70%		●		●	●	●	●	●	●
	80%	●	●	●	●	●	●	●	●	●
	90%	●	●	●	●	●	●	●	●	●
	150%					●		●	●	●
Rotation, Scaling, translation (RST)	5° +80%+[0,25]				●	●	●	●	●	●
	15° +90%+[2,25]		●		●	●	●	●	●	●
RST attacks + JPEG 70	5° +90%+[5,5]		●	●	●	●	●	●	●	●
	78° +90%+[15,25]				●	●	●	●	●	●
	10° +80%+[10,10]				●	●	●	●	●	●
	50° +140%+[0,25]					●		●	●	●
RBA	StirMark RBA					●		●	●	●

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

As shown in Table 3, our scheme outperforms Tang's method and Qi's method under a variety of geometric attacks. The geometric attacks include random relatively small and large rotations, scaling, any combination of RST attacks, and the combined geometric attacks and JPEG compression. The simulation results outline that the proposed scheme can easily resist cropping, shearing and linear geometric transform. More exhilaratingly, our approach works well for the RBA.

Tables 4 and 5 demonstrate the fraction of correctly detected watermarked GIRs under several common image processing and geometric attacks comparing with Tang's method, where the length of the watermark sequence is 16 bits. In Tables 4 and 5, Tang's experimental results are both from paper [14]. The simulation results also outline that our scheme performs better than Tang's method under geometric attacks and nearly all of common image processing. Our scheme is comparable to Tang's method under additive uniform noise attack, because QIM is fragile against noise addition attack.

Table 4. The comparisons of the proposed method and Tang's method under different common processing attacks. The length of the watermark sequence is 16 bits

Attacks	Lena		Baboon		Peppers	
	Tang's	Our	Tang's	Our	Tang's	Our
Watermarked image	7/8	7/7	10/11	5/6	4/4	8/10
Median filter 2 × 2	1/8	5/7	6/11	2/6	1/4	7/10
Median filter 3 × 3	1/8	5/7	2/11	3/6	1/4	8/10
Sharpening filter 3 × 3	4/8	6/7	4/11	3/6	4/4	5/10
Color quantization	7/8	7/7	4/11	5/6	1/4	8/10
Gaussian filtering 3 × 3	5/8	5/7	8/11	3/6	1/4	4/10
Additive uniform noise(scale=0.1)	5/8	2/7	6/11	0/6	4/4	3/10
Additive uniform noise(scale=0.15)	4/8	1/7	4/11	2/6	2/4	4/10
Additive uniform noise(scale=0.2)	1/8	0/7	5/11	0/6	1/4	3/10
JPEG 80	6/8	5/7	9/11	5/6	3/4	7/10
JPEG 70	7/8	5/7	11/11	4/6	3/4	5/10
JPEG 60	6/8	3/7	7/11	3/6	1/4	4/10
JPEG 50	5/8	2/7	7/11	2/6	3/4	2/10
JPEG 40	3/8	2/7	5/11	2/6	1/4	2/10
JPEG 30	2/8	1/7	4/11	1/6	1/4	2/10
Median filter 2 × 2 + JPEG 90	2/8	5/7	6/11	1/6	0/4	5/10
Median filter 3 × 3 + JPEG 90	1/8	5/7	1/11	3/6	1/4	6/10
Sharpening filter 3 × 3 + JPEG 90	4/8	5/7	2/11	3/6	4/4	4/10
Gaussian filtering 3 × 3 + JPEG 90	5/8	4/7	8/11	1/6	2/4	3/10

The false-alarm probability and the miss probability are calculated according to Eq. (11) and Eq. (13), respectively. In Table 2, $m = 2$ and $t_s = 7$. The length of watermark message is 8 bits, so $2N = 8$. The total number of GIRs N_{GIR} in Lena, Baboon and Peppers is 7, 6 and 10, respectively. According to Eq. (11), the false-alarm probability $P_{F-image}$ of the three images is 0.023, 0.017 and 0.046, respectively. According to Eq. (13), we can get that the miss probability of the three images is 0.022, 0.046 and 0.002, respectively. In Table 4, $m = 2$ and $t_s = 14$. The length of watermark message is 16 bits, so $2N = 16$. The total number of GIRs N_{GIR} in Lena, Baboon and Peppers is also 7, 6 and 10, respectively. According to Eq. (11), the false-alarm probability $P_{F-image}$ of the three images is 9×10^{-5}, 7×10^{-5} and 2×10^{-4}, respectively. According to Eq. (13), we can get that the miss probability of the three images is 0.088, 0.144 and 0.018, respectively.

Table 5. The comparisons of the proposed method and Tang's method under different geometric distortions. The length of the watermark sequence is 16 bits.

Attacks	Lena		Baboon		Peppers	
	Tang's	Our3	Tang'	Our3	Tang'	Our3
Removed 1 row and 5 columns	3/8	7/7	6/11	5/6	3/4	8/10
Removed 5 row and 17 columns	0/8	5/7	3/11	4/6	1/4	7/10
Centered cropping 5% off	2/8	6/7	2/11	2/6	2/4	7/10
Centered cropping 10% off	2/8	5/7	2/11	2/6	2/4	6/10
Shearing-x-1% -y-1%	4/8	5/7	5/11	2/6	1/4	6/10
Shearing -x-0% -y-5%	2/8	6/7	3/11	2/6	1/4	8/10
Shearing-x –5% -y-5%	1/8	4/7	2/11	3/6	0/4	5/10
Rotation 1° + Cropping + Scale	0/8	6/7	4/11	3/6	2/4	5/10
Rotation 1° + Cropping	3/8	6/7	3/11	2/6	2/4	6/10
Rotation 2° + Cropping	0/8	7/7	1/11	2/6	1/4	6/10
Rotation 5° + Cropping	0/8	6/7	0/11	3/6	0/4	5/10
Linear geometric transform (1.007,0.01,0. 01,1.012)	5/8	5/7	4/11	3/6	1/4	7/10
Linear geometric transform (0.010,0.013,0.009,1.011)	4/8	5/7	4/11	2/6	1/4	9/10
Linear geometric transform (1.013,0.008,0.011,1.008)	4/8	5/7	5/11	2/6	0/4	8/10
Removed 1 row &5 columns+JPEG 70 77070JPEG 70 JPEG 70 JPEG 70 JPEG 70	4/8	4/7	6/11	3/6	3/4	3/10
Removed 5 rows&17 columns+JPEG 70	1/8	4/7	3/11	2/6	1/4	3/10
Centered cropping 5% off+JPEG 70	2/8	5/7	2/11	1/6	2/4	4/10
Centered cropping 10% off+JPEG 70	3/8	4/7	2/11	1/6	2/4	2/10
Shearing -x-1% -y-1%+JPEG 70	5/8	2/7	4/11	2/6	1/4	3/10
Shearing-x –0% -y-5%+JPEG 70	6/8	4/7	3/11	2/6	0/4	3/10
Shearing-x-5%-y-5%+JPEG 70	4/8	4/7	0/11	1/6	0/4	3/10
Rotation 1° +Cropping+Scale+JPEG70	0/8	5/7	4/11	2/6	0/4	3/10
Rotation 1° +Cropping+ JPEG70	4/8	3/7	3/11	2/6	1/4	3/10
Rotation 2° +Cropping+ JPEG70	1/8	4/7	1/11	2/6	1/4	3/10
Rotation 5° +Cropping+ JPEG70	1/8	4/7	0/11	3/6	0/4	2/10
Linear geometric transform (1.007,0.01,0.01,1.012) +JPEG 70	4/8	3/7	3/11	3/6	1/4	3/10
Linear geometric transform (1.010,0.013,0.009,1.011) +JPEG 70	4/8	4/7	5/11	2/6	3/4	3/10
Linear geometric transform (1.013,0.008,0.011,1.008) +JPEG 70	3/8	4/7	5/11	2/6	0/4	3/10

8. Conclusions

In this paper, we have proposed a watermarking scheme which is robust against geometrical distortions and common image processing attacks. The major contributions are: 1) Introduce a novel GIRs detection method that is implemented by robust edge contours extraction, robust corners detection, and radii selection. To ensure a GIR cover the same content even the image is

#115773 - $15.00 USD Received 17 Aug 2009; revised 2 Nov 2009; accepted 3 Nov 2009; published 13 Nov 2009

rotated or zoomed, the MSCP corner detector and the characteristic scale are adopted. 2) Design a new sector-shaped partitioning method for GIR. The sector-shaped partitioning is invariable to geometric transforms, so the sequence of sectors will not be out-of-order under geometric transforms. The proposed watermarking scheme is robust against a wide variety of attacks as indicated in the experimental results. Experiments also demonstrate that the presented scheme works well for RBA. Our approach can be further improved by developing more robust embedding method than QIM and increasing the watermark capacity.

Acknowledgments

Special thanks go to Dr. Xiaohong Zhang of Chongqing University, Di Liu, Lunming Qin and Lifang Yu of Beijing Jiaotong University, for their kind helps. This work was supported in part by National Natural Science Foundation of China (No.60776794, No.90604032, and No.60702013), 973 program (No.2006CB303104), 863 program (No.2007AA01Z175), PCSIRT (No.IRT0707), Beijing NSF (No.4073038) and Specialized Research Foundation of BJTU (No. 2006XM008, No. 2005SZ005).