RST resilient multi-bit image watermarking based on BITPLANE centroids

Y. Zhao*[1], J.-S. Pan[2] and Z. F. Zhu[1]
[1]Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China

[2]Department of Electronic Engineering, Kaohsiung University of Applied Sciences, 415 Chien-Kung Road, Kaohsiung 807, Taiwan

Abstract: How to efficiently resist geometric attacks remains a challenging direction in watermarking research. In this paper, a multi-bit image watermarking scheme based on image centroids is presented. Some measures including adaptive low pass filter, finely tuning the partitioning are used to further improve the performance. The experimental results show that the scheme can achieve high capacity as well as good robustness against rotation, scaling and translation (RST) attacks and considerable robustness against typical image processing.

Keywords: digital watermarking, data hiding, geometric attacks, RST, centroid

INTRODUCTION

The idea of using a robust digital watermark to detect and trace copyright violations has stimulated significant interest among artists and publishers.[1] A digital watermark is an invisible mark embedded in a digital medium which may be used for a number of purposes including captioning and copyright protection. The research has inspired many researchers and a variety of approaches have been proposed.[2–5]

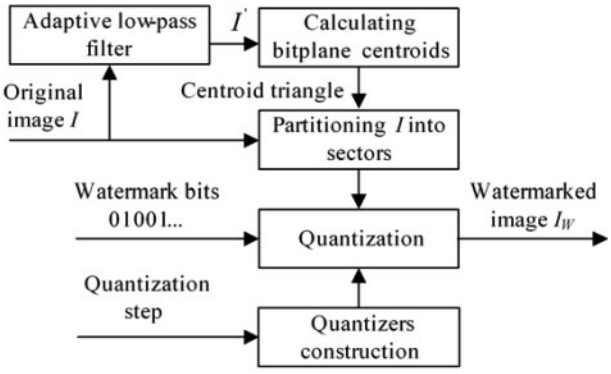
Most approaches can resist attacks such as compression, filtering, enhancing and other signal processing operations. However, recently it has become clear that even very small geometric distortions can prevent the detection of a watermark. This problem is most pronounced when the original image is unavailable to the detector.[6] Therefore, how to efficiently resist such kind of attacks remains a challenging direction in watermarking research, and some schemes have been proposed.

The current approaches to resist geometrical attacks may be classified into three categories:

(i) exhaustive search: the typical geometrical transformations commonly used in image edition are applied on the whole image, and in many ways can be easily represented by a mathematical operation. One basic idea to identify the transformation is to perform an exhaustive detection considering all possible geometrical transformations of the marked image. In this case, the computing cost will dramatically increase[2]

(ii) geometrically reverse transformation: in fact, after geometrical transformation, the watermark signal is still there. The detector cannot detect it only because the generated random sequence and the embedded random sequence are not synchronised. Therefore, if the authors know the geometrical transform applied on the marked image, then the authors can reverse the transformation and then can extract the watermark bit by correlation calculation. This category can be further divided into two classes: semiblind correlation and blind correlation. In semiblind correlation, the detector needs the original image to identify the geometrical transform by the matching pairs of the feature points of original image and the attacked marked image.[7,8] Since it

The MS was accepted for publication on 24 October 2006.
* *Corresponding author: Yao Zhao, Institute of Information Science, Beijing Jiaotong University, Beijing 100044, China; email: yzhao@center.njtu.edu.cn*



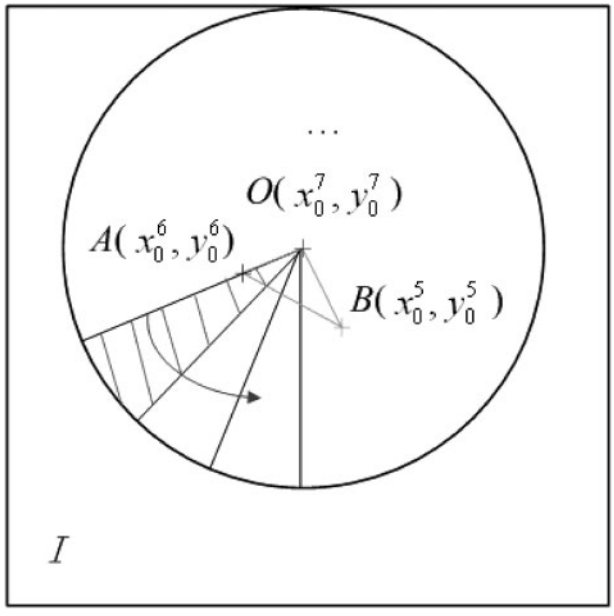
1 Watermark embedding process

needs not the original image in detection process, blind correlation becomes the main direction and some approaches have been proposed. Some researchers proposed resynchronisation based on template technology.[9–11] In embedding process, the scheme embeds meaningful watermark, and meanwhile embeds a special template. After malicious geometrical attacks, the detector can predict the geometrical transform according to the shape change of the special template

(iii) geometrical invariants: researchers try to exploit the moments or features invariant to geometrical transforms, and modulate the invariants with the watermark signals.[12–14]

Moments due to its ability to represent global features have found extensive applications in the field of image processing. In 1962, Hu introduced moment invariants which are position, size and orientation independent.[15] For this significant property, in this paper, the authors will use these moments in a watermarking system to combat geometrical attacks. The embedding scheme partitions the original image into sectors based on the centroids of the three most significant bitplanes, then quantise each sectors according to watermark bits. The detecting scheme also partitions the watermarked image into sectors based on centroids, and can then easily decode the watermark bits. Since the geometric invariant property of centroids, the detector can resynchronise even after RST attacks. In order to further increase the accuracy of synchronisation, adaptive low pass filter and finely tuning are proposed.

The rest of the paper is organised as follows: the embedding procedure is described in the section on 'Enbedding procedure', the following section describes the extraction procedure, the section on 'experimental results' presents some experimental results, and the section on 'Conclusions' concludes the paper.



2 Image partitioning

EMBEDDING PROCEDURE

The embedding procedure is shown in Fig. 1.

A grey image I consists of a number of bitplanes, for example, a 256 level image has eight bitplanes, i.e. bitplane 7, bitplane 6, bitplane 5,…, bitplane 1 and bitplane 0.

For the three most significant bit (MSB) planes, i.e. bitplane 7, bitplane 6 and bitplane 5, calculate the centroids O: (x_0^7,y_0^7), A: (x_0^6,y_0^6), B: (x_0^5,y_0^5). The centroid of a certain bitplane is defined as

$$x_0 = \frac{m_{10}}{m_{00}};\ y_0 = \frac{m_{01}}{m_{00}} \tag{1}$$

where m_{00}, m_{10} and m_{01} are Cartesian moments which are calculated according to equation (2).

$$m_{pq} = \sum_{x=0}^{N_1-1} \sum_{y=0}^{N_2-1} x^p y^q B(x,y) \tag{2}$$

where $B(x,y)$ is the bit value at position (x,y) of a bitplane, and $N_1 \times N_2$ is the size of image I.

OAB constructs a triangle called centroid triangle, as shown in Fig. 2.

Based on the centroid triangle, the authors partition I into sectors. First, with the centroid O as

centre, search for the maximum circle covering I. The authors then uniformly segment the circle into N sectors, where N is the total number of watermark bits. The partition begins from one side of the centroid triangle, i.e. a line OA, along the direction to the other centroid B. The procedure is shown in Fig. 2.

The centroid has been proved to be invariant to some geometrical attacks, such as RST.[15] The image segmentation bases on the centroid triangle, so in theory it is easy to resynchronise the partition after some geometrical attacks. However, in many practical experiments, it can be found that after RST transformation with bilinear interpolation or compression, the centroid position dithers a little. In order to decrease the position error, in embedding and extraction, the authors adaptively filter the images with a filter in equation (3) before calculating their centroids.

$$I'(i,j)=\frac{1}{M}\sum_{\{(k,l)|d((i,j),(k,l))\leqslant R\}} I(k,l) \tag{3}$$

where R is the radius of the filter covered area, M is the total number of the pixels in the filter covered area. The filter radius R adapts with the image size. In the experiments, $R=(1/128)N_1$. Since the filter covered area is round and also its covered area is proportional to the image size, so whatever RST performs, the filter can always cover the same area. Obviously, the filter in equation (3) is a low pass one.

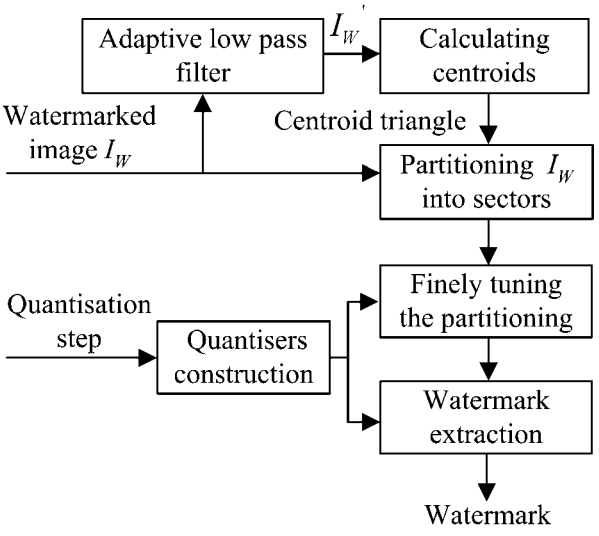
The pixel values are always interfered a little when the image is processed by RST transformation or compression. The low pass filter in equation (3) can significantly decrease the noise and thus decrease the centroids position error. The filtered image is only used to calculate the centroids, but it is not involved in the following quantisation step.

The authors then embed the watermark bits into the sectors using quantization index modulation (QIM).[16]

First, the authors construct two quantisers $Q(.;s)$, where $s\in\{0,1\}$ according to the watermark bits. In this paper, the authors consider the case where $Q(.;s)$ is a uniform, scalar quantizer with stepsize Δ and the quantizer ensemble consists of two quantisers shifted by $\Delta/2$ with respect to each other.

For sector n, according to the corresponding watermark bit w_n, quantise each pixel with quantiser $Q(.;w_n)$.

From the above analysis, it can be known that bitplane 7, 6, 5 are vital in watermark detection,



3 Extraction process

however, without any constrain, after the quantisation, the three bit planes may change. Therefore, the authors should modify the five least significant bitplane, and bound the quantisation value.

Let

$$I^{765}(i,j)=I(i,j)\&(11100000)_2 \tag{4}$$

Then the bound quantisation value

$$I_W(i,j)=\begin{cases} Q(I(i,j);w_m), & \text{if } Q(I(i,j);w_m)\geqslant I^{765} \\ Q(I(i,j);w_m)+\Delta, & \text{if } Q(I(i,j);w_m)<I^{765} \end{cases} \tag{5}$$

EXTRACTION PROCEDURE

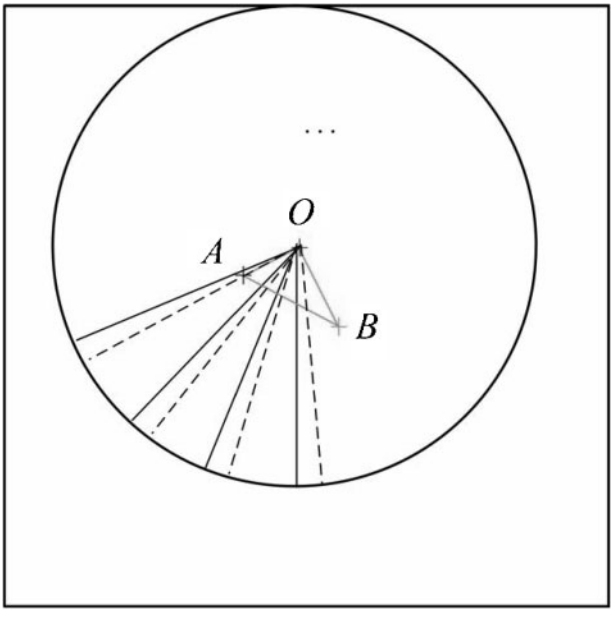
The extracting process is shown in Fig. 3.

The first four steps, i.e. adaptive low pass filter, calculating centroids, partitioning I_W into sectors and quantisers construction are the same as embedding. In the section, the authors will introduce the other two steps in detail: the finely tuning the partition and watermark extraction.

After image processing or malicious attacks, bitplane 7, 6, 5 may be changed, resulting in little displacement of centroids and wrongly partitioning. Although the authors have used adaptive low pass filter and bounding the quantisation value to decrease the position error, there still exist some position error. Comparatively, the position error of O is the least, then A, and then B. The angle θ_0 of OA affects the start of partitioning, as shown in Fig. 4.

Next, the authors propose a method called finely tuning the partitioning to emend OA angle.

For any pixel in sector n, determine the watermark bit embedded. Because of inaccurately partitioning or



4 Correct (solid) and wrong (dash) partitioning

attacks, usually in one sector, some pixels are detected to embed bit 1, and some pixels are detected to embed bit 0. Let *Num(1)* denote the number of '1' pixels in a sector and *Num(0)* denote the number of '0' pixels in a sector. The authors define

$$Maj_{\mathrm{n}}(\theta)=\begin{cases} Num(1), & \text{if } Num(1)\geqslant Num(0) \\ Num(0), & \text{if } Num(1)<Num(0) \end{cases} \tag{6}$$

as the majority pixel number in sector n when the start angle is θ. Define

$$Maj_{\mathrm{all}}(\theta)=\sum_{\mathrm{n}=1}^{\mathrm{N}} Maj_{\mathrm{n}}(\theta) \tag{7}$$

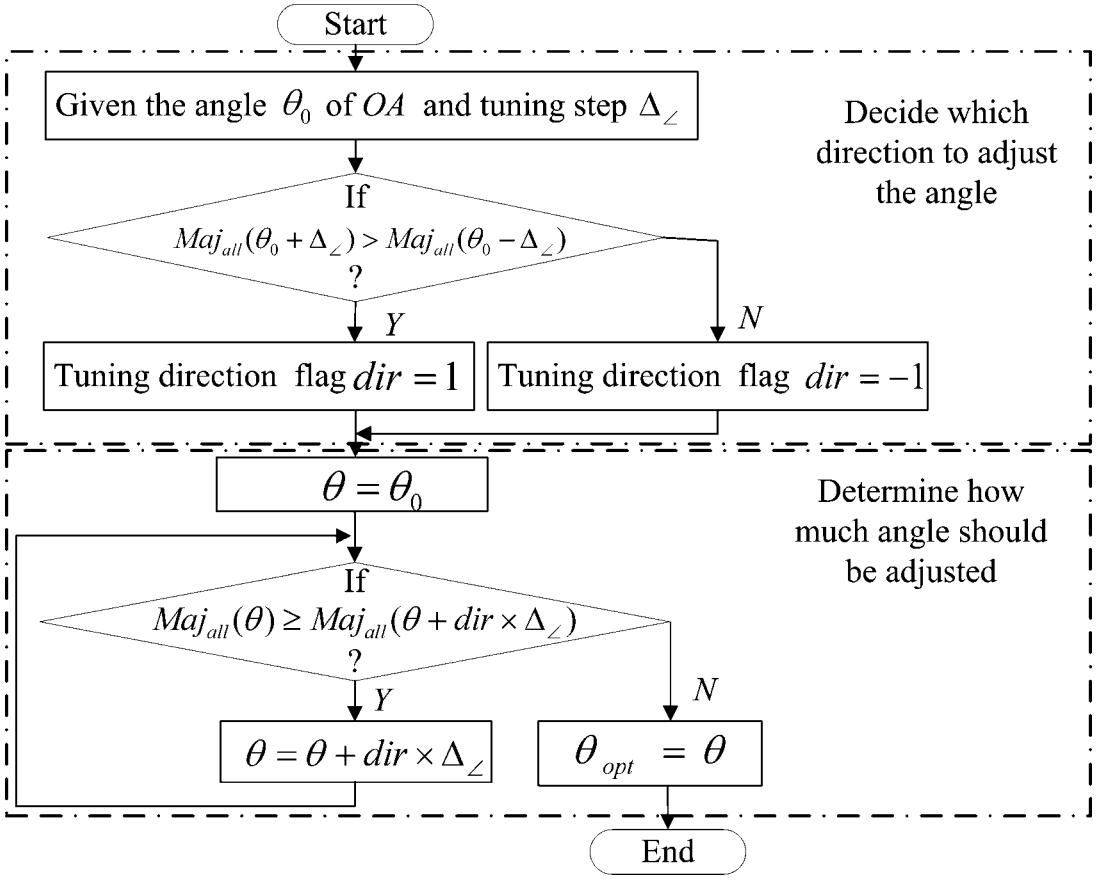
as the majority pixel number in the whole image when the start angle is θ.

Using $Maj_{\mathrm{all}}(\theta)$ as the criteria, the authors will first determine which direction the authors rotate the partition angle, and then determine how much angle the authors rotate. The tuning process is shown in Fig. 5.

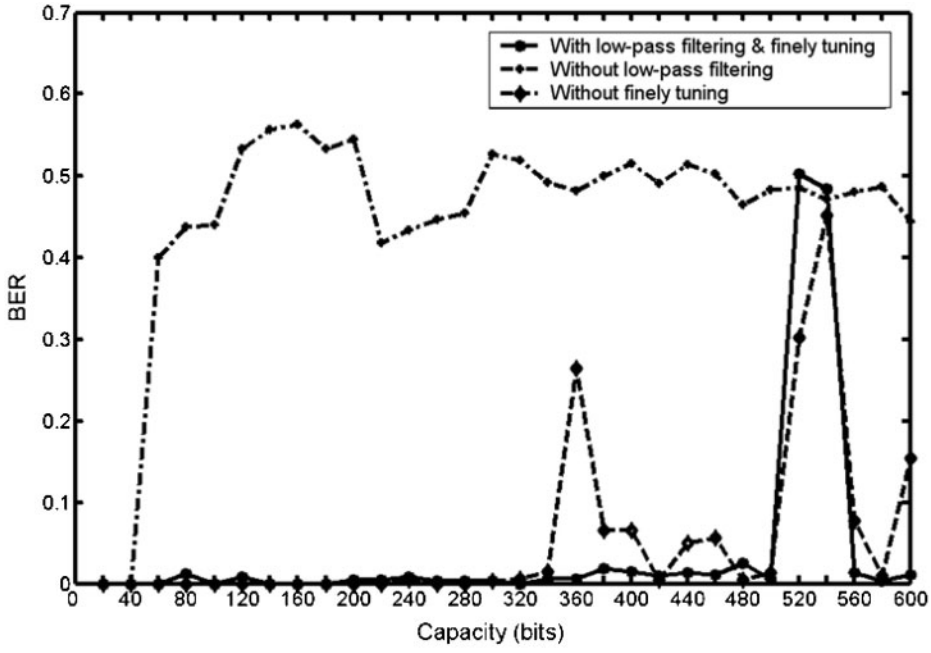
After the optimal angle is obtained, the authors extract the watermark bit with minimum distance decoder.

EXPERIMENTAL RESULTS

The red component of the standard 512×512 colour Lena is used as the test image.



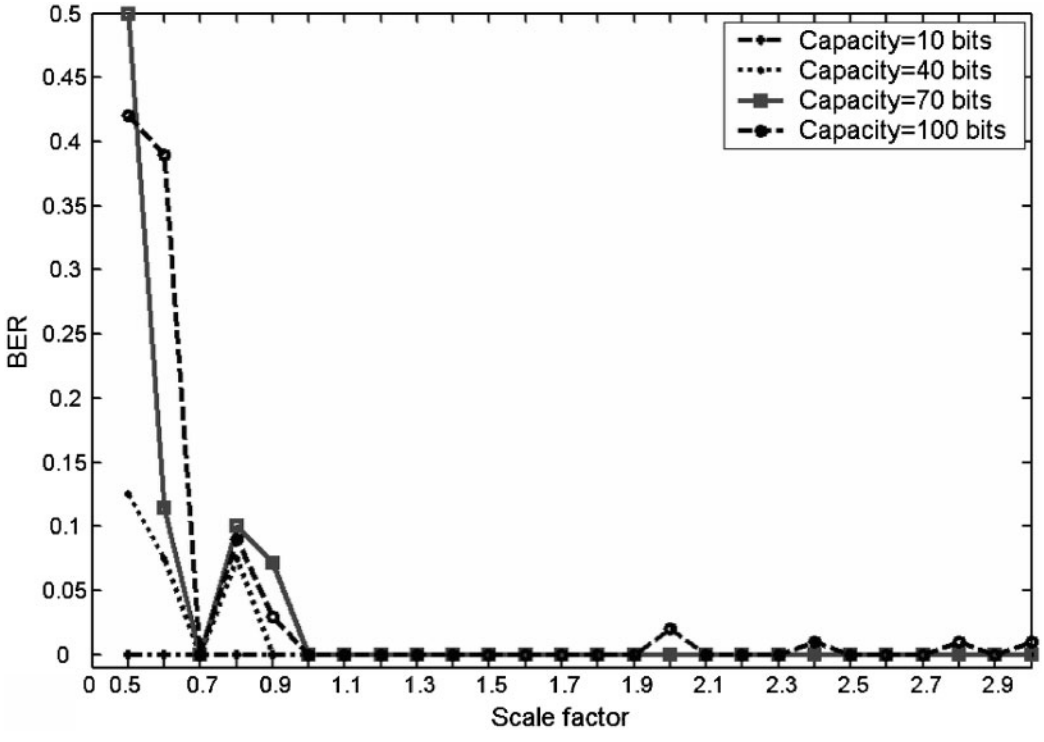
5 Steps of finely tuning process



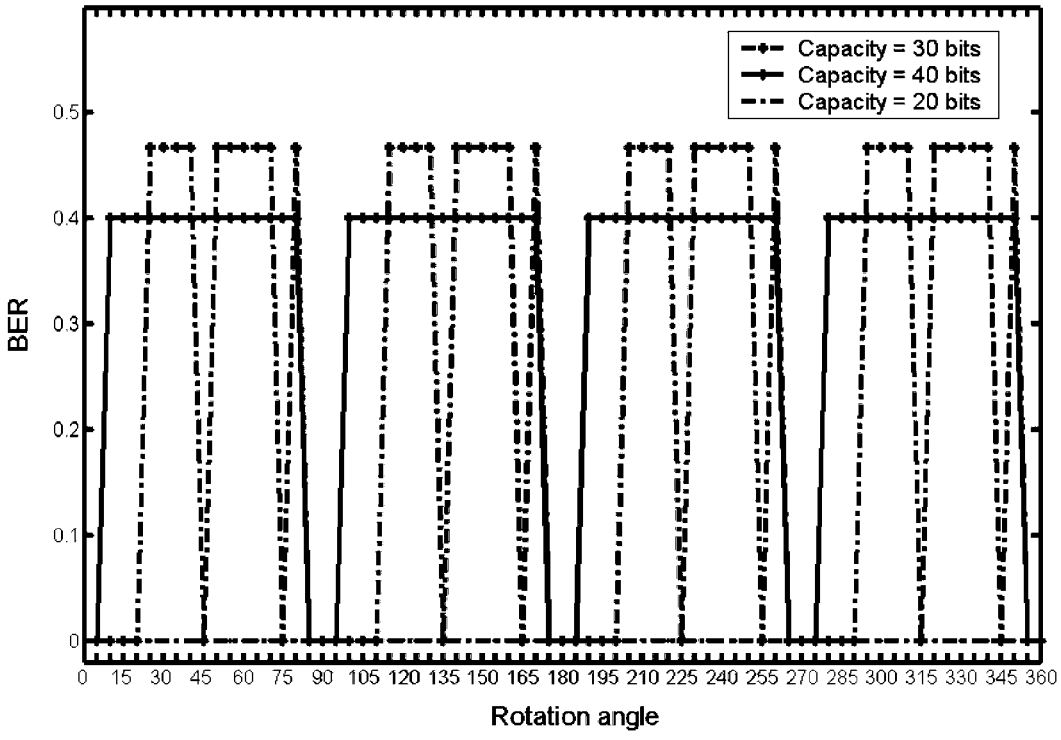
6 BER versus capacity

Figure 6 shows the curves of BER versus capacity, where $\Delta=6$ and the watermarked image is 125% scaled. The average PSNR=43.13 dB. In order to test the functions of adaptive low pass filter and finely tuning, Fig. 6 also presents the curves of the schemes without adaptive low pass filter and finely tuning respectively.

From the experiments, it is know that the scheme with both adaptive low pass filter and finely tuning has the best performance and can achieve high



7 BER versus scale

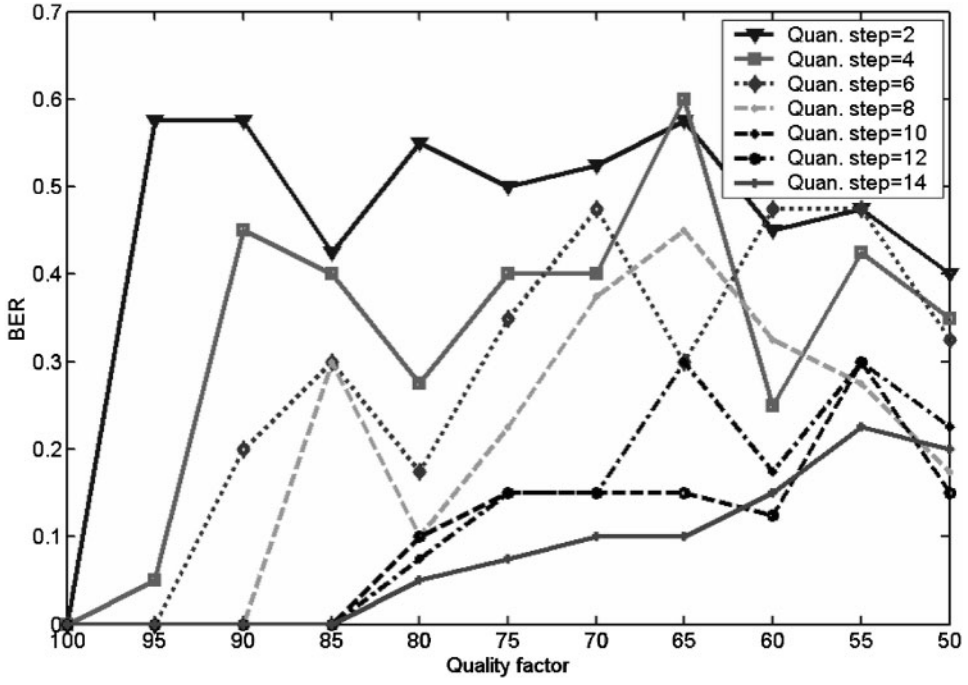


8 BER versus rotation angle

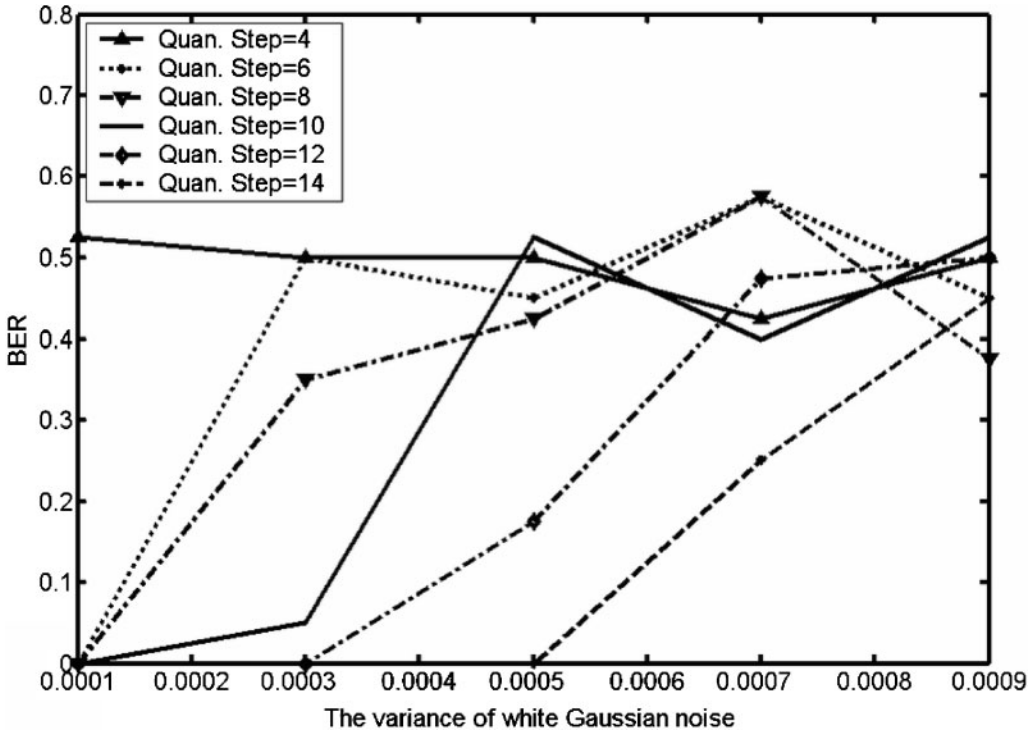
capacity. The scheme without adaptive low pass filter has the worst performance.

Figure 7 shows the curves of BER versus scale, where $\Delta=6$. The average PSNR=43.3 dB. When the image is scaled down (scale factor less than 1) and capacity is high, there are detection bit errors. This is because some pixels are lost when the image is scaled down. When the image is scaled up, the scheme has good performance.

Figure 8 presents the curves of BER versus rotation angle, where $\Delta=6$. The average PSNR= 43.4 dB. When embedding capacity=20 bits, the



9 BER versus quality factor



10 BER versus variance of white Gaussian noise

scheme can resist all rotation angles, when embedding capacity=30 bits and 40 bits, BER increases in some rotating angles.

The authors also test the performance against translation without cropping, the scheme can successfully detect all the watermark bits.

The experiments also test the performance against JPEG compression, Fig. 9 presents the results. In the experiment, capacity=50 bits. Δ=2, 4, 6, 8, 10, 12, 14 and PSNR=53.0, 46.64, 43.22, 39.87, 39.53, 36.23 and 35.08 dB respectively. By comparing the curves, it is clear that the bigger Δ is, the better the robustness.

Figure 10 summarises the performance when the watermarked image is attacked by a white Gaussian noise. In all the curves, the capacity is 40 bits. The white Gaussian noise is zero mean with different variance. Also it is clear that the quantisation step affects the robustness and the bigger Δ is, the better the robustness.

CONCLUSIONS

The paper presents a novel scheme which exploits the geometrical invariant moments to combat geometric attacks. Some measures, such as low pass filtering, quantisation bounding and finely tuning, are proposed to further improve the robustness. The scheme can achieve high capacity as well as good robustness against RST attacks and considerable robustness against typical image processing.

ACKNOWLEDGEMENT

This work was supported in part by 973 program (no. 2006CB303104), National Natural Science Foundation of China (no. 90604032, no. 60373028), Program for New Century Excellent Talents in University and Specialized Research Fund for the Doctoral Program of Higher Education.

REFERENCES

1 K. Tanaka, Y. Nakamura and K. Matsui: Proc. 1990 IEEE Military Commun. Conf., Monterey, CA, USA, September 1990, IEEE, 216–220.
2 G. C. Langelaar, I. Setyawan and R. L. Lagendijk: *IEEE Signal Process. Magazine*, September 2000, **17**, (5), 20–46.
3 P. Y. Tsai, Y. C. Hu and C. C. Chang: *Signal Process.*, January 2004, **84**, (1), 95–106.
4 M.-S. Hwang, C.-C. Chang and K.-F. Hwang: *IEEE Trans. Consumer Electron.*, May 1999, **45**, (2), 286–294.

5 Z. Liu and A. Inoue: *IEEE Trans. Circuits Syst. Video Technol.*, 2003, **13**, (8), 801–812.
6 F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn: Proc. Workshop Information Hiding, Portland, OR, USA, April 1998, 218–238, Springer-Verlag.
7 C.-W. Tang and H.-M. Hang: *IEEE Trans. Signal Process.*, April 2003, **51**, (4), 950–959.
8 P. Bas, J.-M. Chassery and B. Macq: *IEEE Trans. Image Process.*, September 2002, **11**, (9), 1014–1028.
9 S. Pereira, J. Ruanaidh, F. Deguillaume, G. Cscurka and T. Pun: Proc. Int. Conf. on 'Multimedia computing and systems', Florence, Italy, June 1999, IEEE, 870–874.
10 M. Kutter: Proc. SPIE Int. Symp. on 'Voice, video and data communication', Boston, MA, USA, November 1998, Vol. 3528, 423–431.
11 X. G. Kang, J. W. Huang, Y. Q. Shi and Y. Lin: *IEEE Trans. Circuits Syst. Video Technol.*, August 2003, **13**, (8), 776–786.
12 J. Oruanaidh and T. Pun: *Signal Process.*, 1998, **66**, (3), 303–317.
13 M. Alghoniemy and A. H. Tewfik: Proc. IEEE Int. Conf. on 'Image processing', Vancouver, Canada, January 2000, IEEE Signal Processing Society, Vol. 2, 73–76.
14 Y. Zhao and R. L. Lagendijk: Proc. IEEE Int. Conf. on 'Image processing', Rochester, NY, USA, 2002, IEEE, 145–148.
15 M.-K. Hu: *IRE Trans. Inform. Theory*, February 1962, IT-8, 179–187.
16 B. Chen and G. W. Wornell: Proc. SPIE: security and watermarking of multimedia contents II, San Jose, CA, USA, January 2000, SPIE, Vol. 3971, 48–59.