Front. Electr. Electron. Eng. China 2008, 3(1): 20–24
DOI 10.1007/s11460-008-0005-7

RESEARCH ARTICLE

Leida LI, Baolong GUO

Image adaptive RST invariant watermark using pseudo-Zernike moments

© Higher Education Press and Springer-Verlag 2008

Abstract Rotation, scaling and translation (RST) attacks can desynchronize watermark detection, which causes failure in many watermarking systems. In this paper, an image adaptive RST invariant watermark (AWPZM) is proposed by using the rotation invariant property of pseudo-Zernike moments (PZM) and odd-even quantization. PZM of the original image is computed first, and then those suitable for watermark generation are selected. Then, magnitudes of them are odd-even quantized to generate the watermark. In detection, a normalized hamming function is employed to determine the similarity of the watermark. Experimental results show its robustness to rotation and scaling. For traditional attacks, such as JPEG compression, added noise and filtering, the similarities are all above 0.95.

Keywords information hiding, adaptive watermark, pseudo-Zernike moments (PZM), odd-even quantization

1 Introduction

Image watermarking is the technique to embed some information into an image without causing visible artifacts, which can be extracted even when the watermarked image is subjected to various kinds of attacks [1]. Digital watermarking is commonly used for copyright protection, content authentication, and secret communication, etc [2–8]. Geometric attacks, such as rotation, scaling and translation (RST), can destroy the synchronization between the watermark and the cover image. As a result, the watermark detection may fail due to any slight attacks. Therefore, the resistance of watermarking against geometric distortions has been the subject of much research.

Invariant moment of the image has been adopted in literature for designing geometrically robust watermarking schemes. Among the invariant moments, Zernike moment has a desirable property of rotation invariance. Besides, it is insensitive to added noise [9], thus providing the theoretic fundamentals for designing geometrically robust watermarking algorithms. Kim et al. [2] proposed an RST invariant watermarking scheme, where the watermark is embedded by modifying Zernike moments with orders lower than 5. Chen et al. [3] first computed the Zernike moments of the watermark image. Then the Zernike moments are reconstructed and added into the original image to obtain the watermarked image. Xin et al. [4] first extracted the Zernike feature vector of the original image. Then the watermark bits are embedded by modifying the Zernike vector using dither modulation. The watermark can be extracted from the invariant magnitudes of the Zernike moments using a minimum distance decoder.

Compared with Zernike transform, the pseudo-Zernike transform generates more independent moments, and it shows better robustness against added noise. As a result, the authors believe that it is much more suitable for designing watermarking schemes. In this paper, an image adaptive RST invariant watermark using pseudo-Zernike moments (AWPZM) is proposed using the rotation invariant property of pseudo-Zernike magnitudes, combined with odd-even quantization. The pseudo-Zernike moments (PZM) of the original image are first computed, and those that are appropriate for watermark generation are selected to generate the adaptive watermark sequence employing odd-even quantization. During watermark detection, the normalized Hamming similarity (NHS) is calculated to estimate the similarity between the extracted watermark and the original one. In the proposed scheme, the watermark is generated from the image content and the original image is not needed in detection. Experimental results show that AWPZM can efficiently resist geometric attacks, such as rotation and scaling. It is also robust to traditional signal

Translated from *Journal of Xidian University*, 2007, 34(1): 38–42 [译自: 西安电子科技大学学报]

Leida LI (✉), Baolong GUO
School of Mechano-electronic Engineering, Xidian University, Xi'an 710071, China
E-mail: reader1104@163.com

processing attacks, such as JPEG compression, added noise and filtering.

2 PZM

2.1 Computation of PZM

The PZM of an image can be obtained by projecting the original image onto a set of complex functions, which are called basis polynomials of the PZM. Let the polynomials be denoted by $\{V_{nm}(x, y)\}$, which forms a complete orthogonal set over the interior of the unit circle, i.e., $x^2+y^2 \leqslant 1$. The form of these polynomials is

$$V_{nm}(x, y) = V_{nm}(\rho, \theta) = R_{nm}(\rho)\exp(jm\theta). \quad (1)$$

Here, n is a nonnegative integer while m is an integer subject to the constraint of $|m| \leqslant n$. ρ, θ represent polar coordinates over the unit disk. $R_{nm}(\rho)$ is the radial polynomial defined as follows:

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

Given a digital image $f(x, y)$, the PZM with order n and repetition m is defined as

$$A_{nm} = \frac{n+1}{\pi}\sum_x\sum_y f(x,y)\ V^*_{nm}(\rho,\theta). \quad (3)$$

To compute the PZM of a given image, the center of the image is taken as the origin of polar coordinates and pixels inside the unit circle are mapped into polar coordinates. Those pixels falling outside the unit circle are not utilized in the computation.

2.2 Rotation invariant property of PZM

The magnitudes of PZM are rotation invariant. Given an original image $f(x, y)$ and its α degree rotated version, the original moment A_{nm} and that of the rotated one A^r_{nm} is related by

$$A^r_{nm} = A_{nm}\exp(-jm\alpha). \quad (4)$$

Therefore, $|A^r_{nm}| = |A_{nm}|$, i.e., the magnitudes of the PZM remain constant after rotation. If the watermark is generated from the magnitudes of the PZM, then it is invariant rotation.

We have conducted some experiments on the image Lena, of which the PZM with orders 2 and 3 are computed and some of their magnitudes are listed in Table 1, where μ is their respective sample mean, σ is the sample standard deviation and σ/μ indicates the percentage of the spread of $|A^r_{nm}|$ values from their corresponding means. It is observed from Table 1 that the rotation invariant property of PZM is well achieved. The reason for not obtaining exact invariance consists in the discrete nature of the image [10].

Table 1 Magnitudes of some of the PZM for image Lena and some rotated versions

	$\|A_{20}\|$	$\|A_{22}\|$	$\|A_{31}\|$	$\|A_{33}\|$
0°	76.337	170.69	150.53	160.91
30°	71.619	168.72	148.71	158.73
60°	72.622	171.78	151.25	161.00
90°	76.337	170.69	150.53	160.91
150°	72.622	171.78	151.25	161.00
300°	71.619	168.72	148.71	158.73
μ	73.52	170.39	150.16	160.21
σ	1.815	1.387	1.171	1.077
σ/μ	0.0247	0.0081	0.0078	0.0067

2.3 Image reconstruction from PZM

Given all the PZM with maximum order $n_{\max}$, the image can be reconstructed by way of the following equation:

$$\hat{f}(x,y) = \sum_{n=0}^{n_{\max}}\sum_{m=-n}^{n} A_{nm}\ V_{nm}(x,y). \quad (5)$$

Figure 1 demonstrates the reconstructed image from a binary image of the character E with orders ranging from 2 to 12. Note that the reconstructed images are mapped into the range [0, 255] followed by a binarization operation with the threshold 128. It can be seen from Fig. 1 that lower order moments capture gross shape information and high frequency details are filled by higher order moments.

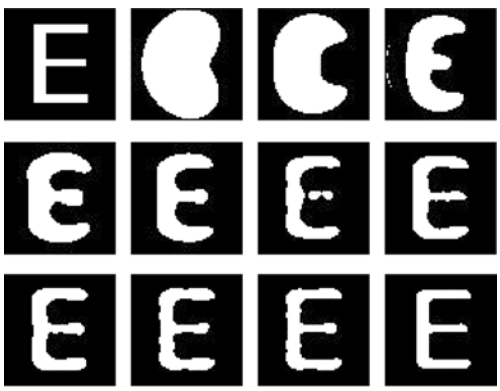

Fig. 1 The reconstructed images of character E
Note: Graphics from the top row sequencing from left to right are original image, reconstructed image with orders ranging from 2 to 12

3 AWPZM watermarking scheme

The proposed AWPZM algorithm employs the rotation invariant property of PZM. The PZM are first computed from the original image, and those with better accuracy are then selected. The watermark sequence is generated adaptively from the magnitudes of these moments using odd-even quantization. The generation of the watermark depends on the magnitudes of the PZM. In the decoder, the PZM are first extracted from the attacked image, and the same parameter is employed to quantize the selected moments and produce the extracted watermark. Finally, the normalized Hamming similarity (NHS) is adopted to estimate the similarity of the watermark.

3.1 Selection of PZM

The discrete nature of digital image results in the computation error of PZM, and some of the moments cannot be obtained accurately. The inaccuracy moments are not suitable for watermark generation. Consequently, the initially computed moments must be carefully selected before watermark generation. In this paper, two aspects are considered in selecting the moments: 1) The PZM with orders higher than a specific value, that is, $N_{\max}$, cannot be obtained accurately. In this paper, $N_{\max}$ is set to be 18. 2) The moments with repetitions $m=4i$, ($i=0, 1, 2, ...$) are not accurate [10], thus they cannot be used for watermark generation. Furthermore, because of the conjugate symmetric property of PZM, only half of the remaining moments are independent. Let the finally selected moments be denoted by S, then $S=\{A_{nm}| n\leqslant N_{\max},\ m\geqslant 0,\ m\neq 4i\}$. It is easy to know that the number of PZM in the S is as follows:

$$|S|_{\mathrm{PZM}}=\begin{cases}\dfrac{3N_{\max}^2+6N_{\max}}{8}, & N_{\max}=4i\\ \dfrac{3N_{\max}^2+6N_{\max}-1}{8}, & N_{\max}=4i+1\\ \dfrac{3N_{\max}^2+6N_{\max}}{8}, & N_{\max}=4i+2\\ \dfrac{3N_{\max}^2+6N_{\max}+3}{8}, & N_{\max}=4i+3\end{cases}, \tag{6}$$

where i is nonnegative integers.

3.2 Odd-even quantization and watermark generation

Odd-even quantization is in fact an operation that projects a set into another one with elements belonging to {0, 1} [5]. Odd-even quantizing each magnitude of the PZM equals the operation that a bit is assigned to it. Then the projection of all the PZM in S produces a binary sequence, which shall be denoted by w. Figure 2 shows the detailed procedure of odd-even quantization on the magnitudes of PZM.

It is observed from Fig. 2 that each element $|A_{nm}|$ in S is mapped into a bit 0 or 1.

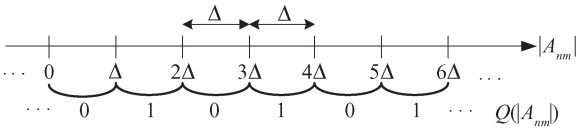

Fig. 2 Odd-even quantization on the magnitudes of PZM

Suppose that the quantization function is $Q(\cdot)$. Then the detailed quantization operation is as follows:

$$w=Q(|A_{nm}|)=\begin{cases}0, & r\Delta\leq|A_{nm}|\leq(r+1)\Delta,\\ & r=0,\ \pm2,\ \pm4,\ ....\\ 1, & r\Delta\leq|A_{nm}|\leq(r+1)\Delta,\\ & r=\pm1,\ \pm3,\ \pm5,\ ...\end{cases}. \tag{7}$$

Here, Δ is a positive integer, i.e., the quantization step. The proposed AWPZM algorithm employs the binary sequence $w=\{w_1, w_2, \ldots, w_l\}$ which is generated by odd-even quantizing the magnitudes of PZM as the adaptive watermark signal. As the watermark is generated from the magnitudes, the rotation invariant property of the magnitudes ensures that the watermark is robust against rotation attacks. Besides, the original image is not modified during watermark generation, so that there is no quality degradation of the original image.

3.3 Watermark detection

In the detector, the PZM are first computed from a possibly distorted image. Then the same filtering step is conducted to obtain accurate moments. The magnitudes of these moments are odd-even quantized using the same quantization parameter Δ to produce the extracted watermark. Let the extracted watermark be denoted by $\hat{w}=\{\hat{w}_1, \hat{w}_2, \ldots, \hat{w}_l\}$. The NHS is computed as follows:

$$\mathrm{NHS}=1-\frac{H_D(w,\hat{w})}{l}, \tag{8}$$

where w and $\hat{w}$ are the original watermark and the extracted one respectively. $H_D(\cdot,\cdot)$ denotes the Hamming distance between w and $\hat{w}$, l is the length of the watermark. Obviously, NHS$\in$[0 1], the bigger the NHS value is, the better the extracted watermark is.

4 Experimental results and discussions

In our experiments, a 64-bit-long watermark and a 128-bit-long watermark are generated from the standard image Lena with size 256×256 respectively. Then, experiments are conducted on the image. Note that the bilinear interpolation is adopted when the image is rotated or scaled.

Robustness to rotation: The image is subjected to rotations with angles ranging from 0 to 90 degrees (Note

that 0–360 degrees can be seen as a periodic repetition of 0–90 degrees). The interval of the rotations is 5 degree. Figure 3 shows the relation between NHS and the rotation angle.

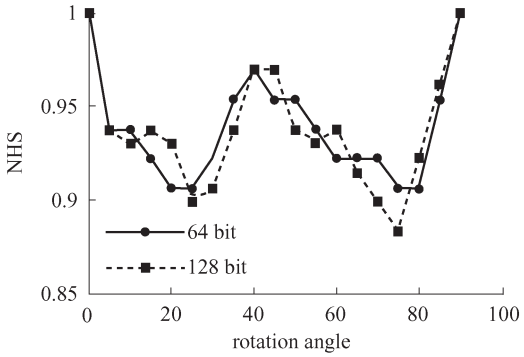

Fig. 3 NHS versus rotation

It is observed that when the watermark is 64 bits long, all the NHS values are above 0.9. In case of a 128-bit watermark, the NHS value is lower than 0.9 only at angles of 25 degrees and 75 degrees. In Ref. [2], the watermark capacity is only one bit, and the detection ratio is 0.95 at small angles, while large rotation will result in failure in watermark detection. The scheme in Ref. [4] is only robust against small rotations, i.e., from 0–10 degree. Our scheme outperforms the latter two methods with regard to rotation attacks.

Robustness to scaling: The image is subject to scaling attacks with factors ranging from 0.5 to 4. Moreover, the attacked image is scaled back to its original size before watermark detection. Figure 4 shows the relation between the NHS and the scaling factor. It is easily observed that the NHS values are higher than 0.95 when the image is scaled up. When the image is scaled down, the NHS values turn smaller. But they are still all higher than 0.9. In Ref. [2] the watermark detection ratio is only 0.87 during scaling attacks.

The proposed AWPZM algorithm is robust to scaling attacks in that the computation of the PZM depends on the image content. Our scheme scales the attacked image back to its original size, which guarantees that the image content inside the unit circle remains unchanged. When the image is scaled down, smaller NHS values are obtained. This is due to the fact that some of the image information are lost, which results in the inaccurate computation of the PZMs.

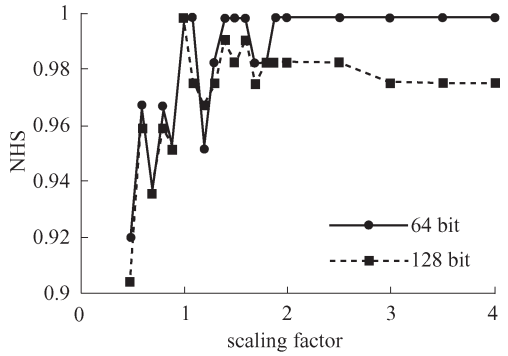

Fig. 4 NHS versus scaling

Robustness to JPEG compression: The image is subject to JPEG compression with different quality factors. The relation between the NHS values and JPEG quality factors is demonstrated in Fig. 5. It is observed that the watermark can be accurately extracted when the quality factor is higher than 40%, regardless of whether a 64-bit or 128-bit watermark is used. As a result, AWPZM is very robust to JPEG compression. Our scheme achieves comparable results than those of Ref. [4], and both perform better than Ref. [2].

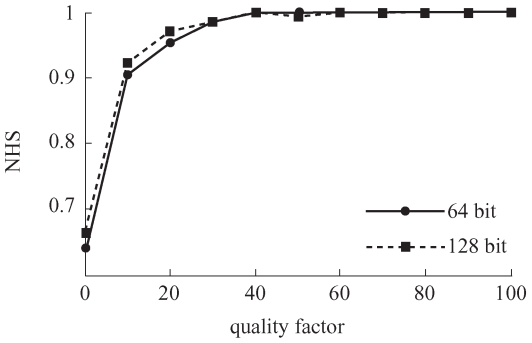

Fig. 5 NHS versus JPEG compressions

Other attacks: Table 2 shows the watermark robustness against filtering and noise-addition attacks. It can be seen from Table 2 that AWPZM performs well on both filtering attacks and added noise. This also demonstrates that PZM is a good image content descriptor.

Table 2 NHS values under filtering and noise-addition attacks

watermark	median-filtering	Gaussian noise	salt & pepper noise	multiplicative noise
64 bit	0.9688	0.9844	0.9531	0.9531
128 bit	0.9609	0.9688	0.9609	0.9688

5 Conclusions

In this paper, we studied the fundamental theory of PZM. The rotation invariant property of PZM and the image reconstruction from PZM are discussed in this paper in detail. A new adaptive image watermarking scheme (AWPZM) is proposed for resisting geometric attacks by using the rotation invariant property of PZM and odd-even quantization. The proposed scheme can resist rotation attacks with random angles, scaling

attacks, JPEG compression as well as filtering attacks. Future work will be emphasized on how to embed real watermark bits.

Acknowledgements This work was supported by the National Natural Science Foundation of China (Grant No. 60572152) and the Ph. D. Programs Foundation of the Ministry of Education of China (No. 20060701004).

References

1. Barnett R. Digital watermarking: applications, techniques and challenges. Electronic & Communication Engineering Journal, 1999, 11(4): 173–183
2. Kim H S, Lee H K. Invariant image watermark using Zernike moments. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(8): 766–775
3. Chen Q, Yang X L, Zhao J Y. Robust image watermarking with Zernike moments. In: Proceedings of Canadian Conference on Electrical and Computer Engineering, 2005, 1340–1343
4. Xin Y Q, Liao S, Pawlak M. A multibit geometrically robust image watermark based on Zernike moments. In: Proceedings of 17th International Conference of Pattern Recognition, 2004, 4: 861–864
5. Kundur D, Hatzinakos D. Digital watermarking for telltale tamper proofing and authentication. In: Proceedings of the IEEE, 1999, 87(7): 1167–1180
6. Guo L, Guo B L, Chen L T, et al. Wavelet zerotree-based watermarking algorithms for still images. Journal of Xidian University, 2003, 30(5): 677–681 (in Chinese)
7. Guo B L, Zhang Y P, Guo L. Hierarchical semi-fragile watermarking based on the reconstruction of DCT coefficients. Journal of Xidian University, 2004, 31(1): 1–5 (in Chinese)
8. Zhang Y P, Guo B L. SAF: semi-fragile authentication watermarking with feedback. Journal of Xidian University, 2004, 31(5): 724–727 (in Chinese)
9. Teh C H, Chin R T. On image analysis by the methods of moments. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1988, 10(4): 496–513
10. Liao S X, Pawlak M. On the accuracy of Zernike moments for image analysis. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, 20(12): 1358–1364