Semi-fragile Image Watermarking Using Zernike Moment and Fuzzy C-Means

Ching-Tang Hsieh[1], Yeh-Kuang Wu, Chih-Hsu Hsu[2]

[1] Dep. of Electrical Engineering, Tamkang University, Taipei, Taiwan, 25137
email: hsieh@ee.tku.edu.tw

[2] Department of Information Technology, Ching-Kuo Institute of Management & Health, Keelung 203
hsu552@tpts4.seed.net.tw

Abstract

In order to improve the detection of malicious tampering images, it is necessary to decrease the fragility of hidden watermarks, even for digital images which have been incidentally distorted. In this paper, we propose a new invariant semi-fragile digital watermarking technique based on eigenvalues and eigenvectors of real symmetric matrix generated by the four pixel pairs. A signature bit for detecting the malicious tampering of an image is generated using the dominant eigenvector. And the multi-rings Zernike transform (MRZT) is proposed to achieve geometric invariance based on the fuzzy C-means and Zernike moment. The MRZT method is to the geometric distortions even when the image is under malicious attacks. Experimental results show that this algorithm can resist high quality JPEG compression, and improve the detection performance of various malicious tampering.

Keywords: Use "keywords" style here .

1. Introduction

Due to advances in digital technologies, most data are digitized and can be easily copied or edited. Such situation hinders popularization of digital technologies. Image watermarking provides a solution for protecting the copyright of digital contents.

Many watermarks for still images and video content are sensitive to geometric distortions. It is clear that even very small geometric distortions can prevent the detection of watermarks. However, the geometric distortion of the digital image, such as rotation and scaling, can be inverted with lossless of the image intensity. The desired geometric invariance can be achieved by using the FMT (fourier mellien transform) to convert rotation and scale to spatial shifts. A log-polar transform converts rotation and scaling to spatial shifts, and permits recovery from rotation and scaling.

Of various types of moments defined in the literatures, Zernike moments have been shown to be superior to the others in terms of their insensitivity to image noise, information content, and ability to provide faithful image re- presentation, used as the invariant watermarking [7]-[9]. Some invariant watermark schemes proposed with embedding methods based on the Zernike transform coefficients to achieve the geometric invariance, but the geometric invariance methods is restricted to the proposed watermarking, not suitable for all watermark embedding schemes. Chen [10] proposed a geometric invariance watermarking based on wavelet and Zernike transform where the embedding system is independent to geometric invariance method. But the geometric invariance method is not robust to more than two malicious attacks, such as rotation and cropping combining as a severely malicious attack.

Most fragile digital watermarks are very fragile even for slight altering. It cannot resist any processing even some valid processing such as high quality JPEG compression (lossy compression) and is not suitable for factual application. The goal of semi-fragile digital watermarking is to detect unacceptable image manipulations [1][3][4][5]

In this paper, a novel fast rotation and scale variance method, multi-rings Zernike transform (MRZT) is proposed, consisting of two stages. The scaling and rotation angles are calculated of each sub-ring image, and the rings with huge distortions are rejected to approach accurate estimation. The new semi-fragile digital watermarking technology which is abbreviated EVRSM is adopted [6]. Because of the orthogonality property of real symmetric matrix, superiority of watermark-based and signature-based semi-fragile watermarking technology were combined for image authentication to improve the robustness against the legitimate processing and fragility for malicious tampering. The MRZT reduce the accumulation in the Zernike transform and avoid maliciously attacked components. The proposed watermarking system is a geometric invariance system based on the proposed multi-rings Zernike transform that is robust to geometric attacks even when the image is under malicious or innocuous attacks.

In section 2, we will describe the proposed multi-rings Zernike transform. And the candidate selection process is shown in section 3. Section 4 describes how to embed and extract the digital watermark and analyze the details of semi-fragile digital watermarking technique. The experimental results and the evaluation of the proposed algorithm are presented in section 5. Finally, in section 6, we will make a conclusion.

2. Multi-rings Zernike transform

Zernike transform of image is the mapping of an image onto a set of complex polynomials that have the rotation and scaling invariant characteristics. The rotation invariance of the feature vectors allows the feature set, the magnitude of the Zernike moments extracted from the image, to be the same at any orientation. These properties enable the contribution of each moment to be the unique and independent of the information of the image. Unfortunately, the moment-based methods require too much computation for practical purposes and are sensitive to noise, such as cropping and compression.

Let the set of these polynomials be denoted by V_{nm}(x,y) :

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

where Rnm(ρ) is the radial polynomial defined as :

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

n ≧ 0, n-|m| is even , and |m| ≦ n. ρ is the length of vector from origin to pixel at (x,y). θ is the angle between vector ρ and X axis in counterclockwise direction.

In this paper, we proposed a novel fast rotation and scale variance method, multi-rings Zernike transform, consisting of two stages. In the first stage the image is divided into 11 co-centric rings and the moments are computed based on these co-centric rings. Secondly, the candidates of the non-attacked blocks are selected by K-means method according to the density distribution. The multi-rings method can avoid the regions with malicious attacks, lighten the distortion from statistics of the attacked pixels and be suitable for any watermark scheme.

The image I is divided into m sub-rings.

$$\mathrm{I}=\{\mathrm{I}_1\ \mathrm{I}_2\ \mathrm{I}_3\ldots.\mathrm{I}_\mathrm{m}\ \} \tag{3}$$

After the partition, the moment of ring is computed according to (3). For each sub-image, the original of host image is instead of the center.

$$A_{nm}^{l}=\frac{n+1}{\pi}\sum_{x\in l}\sum_{y\in l}f(x,y)V_{nm}^{*}(x,y)$$

Assume that the lth sub-block image is denoted by $f^l(\rho,\theta)$, α^l is the angle of the rotation. The rotated image is denoted by $f_r^l(\rho,\theta)$. The magnitudes of Zernike moments are invariant to rotation, and scale and translation normalizations are required to achieve similarity. The relation-ship between the original image and the rotated in polar coordination is:

$$f_r^l(\rho,\theta)=f^l(\rho,\theta-\alpha^l) \tag{4}$$

$$A_{nm}^{l\,\mathrm{r}}=A_{nm}^{l}\exp(-jm\alpha^l) \tag{5}$$

3. Candidate selection process

According to section 2, 11 candidates with estimated rotation angles in different radius are computed by the moments of co-centric rings interfered with and without malicious tampers. The clustering is widely performed by an iterative algorithm that is known as the fuzzy c-means algorithm. Fuzzy clustering algorithms consider each cluster as a fuzzy set, while a membership function measures the possibility that each feature vector belongs to a cluster. As a result, each feature vector may be assigned to multiple clusters with some degree of certainty measured by the membership function. The algorithm performs a partition for each element in the feature space to c cluster and c centers of the clusters are generated. In the literature, c is equal to 2.

The iterative processes continuous till the cluster center become stable and there is insignificant difference between cluster centers in two consecutive iterations. One of the c clusters will be selected that the variance in this cluster is smaller than other ones**.** The geometric distortions of image, such as rotation and scaling, can be inverted that the intensity of the images is unchanged.

4. Proposed watermarking methods

In this paper, the previously proposed image authentication technique, EVRSM, is adopted in this paper. Given an image, we divide it into several blocks of 8x8 pixels. Each block is transformed with Discrete Cosine Transform (DCT). We divide frequency domain into DC part and AC part, that is, the DCT_{DC_Value} of DCT coefficients belongs to DC part and the DCT_{AC_Value} of DCT coefficients belong to AC part.

We take the integer rounding operation for $\mathrm{DCT_{DC}}$ coefficient, which is divided into the eigenvalue λ. Each $\mathrm{DCT_{AC}}$ coefficient is divided into the fixed quantization table Q_i.

The quantization functions Q_λ and Q_v are defined below:

$$Q_\lambda = \left\lfloor \frac{DCT_{DC\_Value}}{\lambda} \right\rfloor \quad (2)$$

$$Q_V = \left\lfloor \frac{DCT_{AC\_Value}}{Q_i} \right\rfloor \quad (3)$$

λ is dominant eigenvalue and Q_i is fixed quantization table. $\lfloor \bullet \rfloor$ is the floor function.

An adaptive quantization model is incorporating the eigenvalue of the real symmetric matrix as the quantization table. The adaptive quantization table can be determined according to the significance of the host image. The watermark-based embedding function DCT_{DC_Value} and the signature based embedding function $DCT_{\text{AC\_Value}}$ are given in Eq.(6) and Eq.(7), respectively. W is a binary sequence. The r is checked to embed one bit at the pair of blocks. If r, defined in Eq.(8), is equal to the watermark sequence W, the DCT coefficient is remain unchanged. On the other hand, the DCT coefficient was represented by Eq.(4) and Eq.(5)

$$DCT'_{DC.Value} = \begin{cases} (Q_\lambda - 1) \times \lambda, if \ \mathrm{r} \neq W \ and \ Q_\lambda \geq 0 \\ (Q_\lambda + 1) \times \lambda, if \ r \neq W \ and \ Q_\lambda < 0 \end{cases} \quad (6)$$

$$DCT'_{AC.Value} = \begin{cases} (Q_v - 1) \times Q_i, if \ \mathrm{r} \neq 0, \mathrm{r} \neq 1 \ and \ Q_v \geq 0 \\ (Q_v + 1) \times Q_i, if \ r \neq 0, \mathrm{r} \neq 1 \ and \ Q_v < 0 \end{cases} \quad (7)$$

where W represents the sequence of watermark. Embedding “0” or “1” is dependent on the decision of parameter r for the signature-based embedding function. The definition of parameter r is defined as follows.

$$r = \begin{cases} 0 & , if \ \ Q \ \ is \ \ even \\ 1 & , if \ \ Q \ \ is \ \ odd \end{cases} \quad (8)$$

$Q = Q_v$ or Q_λ

The embedding algorithm is :

a. The original image is transformed by the 8x8 block DCT.
b. We use Eq.(6) to embed the watermark (W).
c. We determine the corresponding signature bits of θand embed the signature bits of θby Eq.(7).
d. Through the IDCT, we can obtain the watermarked image.

And the extracting algorithm is :

a. The watermarked image is transformed by the 8x8 block DCT.
b. We use Eq.(6) to extract watermark (W*) and the signature bits of θ from the watermarked image.
c. Compare extracted watermark (W*) and the original watermark (W) to confirm the copyright.
d. Extracte the new signature bits of $\hat{\theta}$ by repeating the embedding process based on the watermarked image. Compare the extracted signature bits of θ and the new signature bits of $\hat{\theta}$.
e. Combine the results of (c) and (d). Only when these are the same, the watermarked image has not been tampered with.
f. Authenticate the input image.

5. Experimental results

We use the Lenna, Baboon, Pepper and a natural image as the test images in our experiments with 256x256 pixels. And the size of digital watermark is 32x32 pixels and the watermark is a binary sequence in 0’s and 1’s. We embed the watermark with the mask of 8*8 pixels.

The MRZT method is proposed to achieve the rotation and scaling invariance and the robustness for malicious or innocuous attack simultaneously. The framework is suitable for all kinds of watermark system.

Table.1 shows the estimating angles when the watermarked image is under quite general kinds of manipulation with 30 degree rotating. The estimation process in Zernike transform is quite sensitive to image manipulation and the error of the estimating rotation degree is huge. And the estimating rotation degree by the proposed multi-ring Zernike moment method is more accurate than the normal Zernike transform.

(5)

During data transmission, more than one malicious attack usual occurs. However, recently proposed watermarking systems with geometrical invariance can not resolve this problem. The MRZT method with simple and less computation can resist double attacks and have the property of geometric invariance.

The PSNR value of watermarked image is given in Table 2. Table.3 tabulates the bit error rate of the watermarked image compression with JPEG. We can extract the whole watermarks when JPEG quality is 70. Some bit errors will occur under the JPEG quality below 60.

We present the efficiency of authentication with some quite general kinds of image processing manipulations as follows.

(A). Delete (B). Delete Background textures
(C). Add a line drawing (D). Delete
(E). Paste another contents (F). Desaturate
(G). Change Hue (H). Delete
(I). Move (J). Replace by computer generated texts
(K). Delete light colored contents (L). Add Foot
(M). Skew (N). Copy

The authenticated results for image processing manipulations are shown in Fig.1. Fig.1(a) is the natural image with the fragile watermarks, and the modified image by the manipulations is shown in Fig.1(b). The labels in the modified image, Fig.1(b), mark the manipulations mentioned at the above section. Fig1(c) is the simulated image of image authentication with the proposed image, and Fig.1(d) is the simulated image of image authentication using Lin’s method.

6. Conclusion

In this paper, we successfully put forward a semi-fragile digital watermark based on the eigvenvectors and eigenvalues of real symmetric matrix. The multi-ring Zernike moment is proposed to be robust to the geometric distortions with malicious attacks. The conception of multi-ring framework and candidate selection process reduce the accumulation of the attacked coefficients in the Zernike transform and avoid maliciously attacked components.

Table.1 The estimating angle by Zernike transform and proposed multi-ring Zernike transform.

	Zernike Transform	Multi-Ring Zernike Transform
	Estimating angle (degree)	
Noise	45.46	30.12
JPEG	45.25	30.63
Pinch	44.91	29.83
Blurring	28.15	29.83
Sharpening	33.47	29.66
Mosaic	41.69	29.68
Twirl	54.84	29.75

Table.2 PSNR value with different dimension of the real symmetric matrix.

PSNR	Lenna	Baboon	Peppers
2x2	39.42	40.00	39.51
3x3	38.22	39.98	38.42

Table. 3 Bit error rate of the watermarked image under different quality of JPEG compression.

JPEG Quality	Lenna	Baboon	Peppers
90	0	0	0
80	0	0	0
70	0	0	0.0014
60	0.0063	0.0019	0.0053

References.

[1]Deepa Kundur and Dimitrios Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication"*, Proceedings of IEEE,* Vol. 87, No.7, pp. 1167-1180, 1999.

[2]E. T. Lin and E. J. Delp, "A Review of Fragile Image Watermarks"*, Proceedings of the Multimedia and Security Workshop,* pp. 25-29, 1999.

[3]C. Y. Lin and S. F. Chang, "Semi-fragile watermarking for authenticating JPEG visual content", *Proceeding of the SPIE, Security and Watermarking of Multimedia Contents*, 2000, pp. 140-151.

[4]K. Maeno, Q. Sun, S-F Chang, M. Suto, "New Semi-fragile Image Authentication Water-marking Techniques Using Random Bias and Non-Uniform Quantization", *Proceeding of the SPIE,* pp. 659-670, 2002.

[5]Yuichi Nakai, "Multivalued Semi Fragile Watermarking", *Proceeding of the SPIE, Security and Watermarking of Multimedia Contents*, pp. 671-678, 2002.

[6]C. T. Hsieh, Y. K. Wu, "Semi-fragile Image Authentication Using Real Symmetric Matrix", *JISE Trans., Vol. 22, No. 3*, pp. 701-712, 2006

[7]H. S. Kim, H. K. Lee, "Invariant image watermark using Zernike moments", *IEEE Transactions on Circuits and Systems for Video Technology*, pp. 766-775, 2003.

[8]Y. Xin, S. Liao, M. Pawlak, "A multibit geometrically robust image watermark based on Zernike moments", *Proceedings of Pattern Recognition*, pp. 861-864, 2004.

[9]H. Liu, J. Lin, J. Huang, "Image authentication using content based watermark", *Proceedings of Circuits and Systems, IEEE*, pp. 4014-4017, 2005.

[10] J. Chen; H. Yao; W. Gao; S. Liu; "A robust watermarking method based on wavelet and Zernike transform", *Proceedings of Circuits and Systems*, pp. 173-176, 2004.

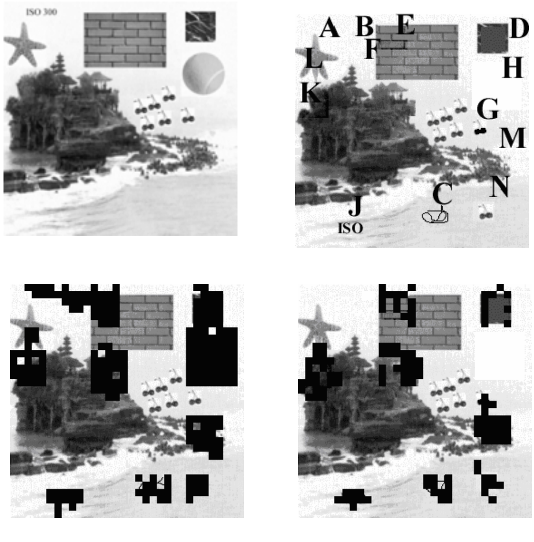

Fig1 (a) Watermarked natural image.
(b) Modified natural image.
(c) Modified areas detected by proposed method.
(d) Modified areas detected by Lin [3] method.