Proceedings of the 5th WSEAS International Conference on Signal Processing, Istanbul, Turkey, May 27-29, 2006 (pp70-75)

Geometric Invariant Semi-fragile Image Watermarking Using Real Symmetric Matrix

Ching-Tang Hsieh, and Yeh-Kuang Wu

Dep. of Electrical Engineering, Tamkang University,
Taipei, Taiwan, 25137, R.O.C.

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. 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.

Key-Words: fragile watermarking, Eigenvalue, Geometric invariance, Zernike moment

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. O'Ruanaidh et al. first have outlined the theory of integral transform invariants and showed that are resistant to rotation, scaling, and translation. However, the log-polar mapping used in this technique causes a loss of image quality and the quality is definitely unacceptable.

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 representation, used as the invariant watermarking [16]-[20]. 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 [16]-[19]. Chen [20] 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.

Fragile digital watermarking is essential for addressing the problem of data integrity, but 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. Some of semi-fragile digital watermarking [1][3][4][5] has been brought forward and researched. Typical approaches of semi-fragile digital watermarking can be categorized as signature-based or watermark-based or a combination of both. Kundur and Hatzinakos [1] embedded a watermark value by modulating a selected wavelet coefficient into the quantized interval determined by the corresponding watermark value. However, they didnot provide a mechanism to detect the combination of malicious tampering and incident distortion. Lin

and Chang [3] stores the relation of DCT coefficients at all pairs of two random 8x8 blocks as digital signature. Their method can detect malicious tampering under JPEG compression, but the digital signature based method cannot point out tampering regions clearly or some special tampers, such as those with background changed to pure white, and cannot be used for multi-watermarks system [6]. Fridrich[8] proposed a multi-watermarking system by embedding fragile watermarks on top of robust watermarks. The fragile watermarks detect all the tampers, and the robust watermarks can distinguish malicious and innocuous changes in the images. The method makes a valuable tool for authentication of images and detection of all types of tamperings.

In this paper, we propose a new semi-fragile digital watermarking technology based on the dominant eigenvalue and its corresponding eigenvector of real symmetric matrix, the proposed method is abbreviated as EVRSM. Because of the orthogonal property of real symmetric matrix, we combine both superiority of watermark-based and signature-based semi-fragile watermarking technology for image authentication in our method to improve the performance of malicious tampering and also resist high quality JPEG compression processing. 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. The MRZT reduce the accumulation of the attacked coefficients in the Zernike transform and avoid maliciously attacked components.

In section 2, we will describe the proposed multi-rings Zernike transform. And the new semi-fragile watermarking 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 is the mapping of an image onto a set of complex polynomials that have the rotation 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.

Let the set of these polynomials be denoted by Vnm(x,y) :

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

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

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

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. Unfortunately, the moment based methods require too much computation for practical purposes and are sensitive to noise, such as cropping and compression.

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.

$$I=\{I_1\ I_2\ I_3\ \ldots.\ I_m\} \quad (3)$$

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 relationship between the original image and the rotated in polar coordination is:

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

$$A_{nm}^{lr}=A_{nm}^{l}\exp(-jm\alpha^{l}) \quad (5)$$

The geometric distortions of image, such as rotation and scaling, can be inverted that the intensity of the images is unchanged.

According to above section, 11 estimated rotation angles candidates with different radius are computed consisted of coefficients interfered with and without malicious tampers. The clustering is widely performed by an iterative algorithm that is known as the crisp c-means algorithm. The crisp c-means algorithm assigns each feature vector to a single cluster and was adopted to separate two clusters, concentrated and distributed ones. 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.

3 Eigenvector and eigenvalue of real symmetric matrix

The real symmetric matrix R is defined by

$$R = A^T \cdot A$$
$$A = [a_{xy}] \qquad x, y = 1,2...k-1,$$
$$a_{xy} = \begin{cases} l & if \ \ f_p(i,j) - f_q(i,j) + B_{ij} \geq 0 \\ m & if \ \ f_p(i,j) - f_q(i,j) + B_{ij} < 0 \end{cases} \quad i, j = 0,1,.., n-1 \qquad (6)$$
$$k \leq n$$

where A^T is the transpose of matrix A, $f_p(i,j)$ and $f_q(i,j)$ are the DCT coefficients of the block p and q, respectively, and B_i is random bias. f_p and f_q are selected at the same frequency in different non-overlap block. The values of selected block p and q are close and will be served as a secret key. k is the dimension of the matrix. The experimental results will not locate off the original point since the random bias B_i is added to the f_p and f_q [4].

The largest eigenvalues are called dominant eigenvalues and their corresponding eigenvectors are called dominant eigenvectors. The dominant eigenvector with the main direction is located in the first quadrant and the rest eigenvectors are located in the four quadrant. λ and its corresponding dominant eigenvector of the real symmetric matrix R will be evaluated. Then we calculate. For eigenvector $[c, d]^T$, the direction θ of the dominant eigenvector is defined by

$$\theta = \tan^{-1}(\frac{c}{d}) \quad \text{where } 0^{\circ} \leq \theta \leq 90^{\circ}.$$

4 Proposed watermarking method

4.1 Embedding algorithm

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.

In Eq.(7), the quantized DCTBDCB coefficient was integer rounding operation by dividing into the eigenvalue . Each DCTBACB coefficient is divided into the fixed quantization table QBiB.

The quantization functions Q_λ and Q_V are defined below:

$$Q_\lambda = \left\lfloor \frac{DCT_{DC\_Value}}{\lambda} \right\rfloor \qquad (7)$$

$$Q_V = \left\lfloor \frac{DCT_{AC\_Value}}{Q_i} \right\rfloor \qquad (8)$$

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

In order to avoid the noise and artifact in JPEG compression, Kunder et al. [1] proposed the watermarking to reduce the noise completely, but significant information may be ignored by the constant quantization. According to the above reasoning, an adaptive quantization model is incorporating the eigenvalue of the real symmetric matrix as the quantization table. The adaptive quantization table is determined according to the significance of the host image. If the watermarked image is altered with malicious tampering, The watermarking method is robust, since the quantization table will change according to the malicious tampered image.

The watermark-based embedding function DCT_{DC_Value} and the signature based embedding function DCT_{AC_Value} are given in Eq.(9) and Eq.(10), respectively. W is a binary sequence. The r is checked to embed one bit at the pair of blocks. If r, defined in Eq.(11), is equal to the watermark sequence W, the DCT coefficient is remain unchanged. On the other hand, the DCT coefficient will be represented by Eq.(9) and Eq.(10)

$$DCT'_{DC\_Value} = \begin{cases} (Q_\lambda - 1) \times \lambda, if \ \ r \neq W \ and \ Q_\lambda \geq 0 \\ (Q_\lambda + 1) \times \lambda, if \ \ r \neq W \ and \ Q_\lambda < 0 \end{cases} \qquad (9)$$

$$DCT'_{AC\_Value} = \begin{cases} (Q_v - 1) \times Q_i, if \ \ r \neq 0, r \neq 1 \ and \ Q_v \geq 0 \\ (Q_v + 1) \times Q_i, if \ \ r \neq 0, r \neq 1 \ and \ Q_v < 0 \end{cases} \qquad (10)$$

$$r = \begin{cases} 0 & , if \ \ Q \ \ is \ \ even \\ 1 & , if \ \ Q \ \ is \ \ odd \end{cases} \qquad (11)$$

The watermark "0" or "1" is dependent on the decision of parameter r for the signature-based embedding function. The value of parameter r is defined as follows.

The value of signature bit is compared with the watermarks at the procedure of the signature-based

embedding system. If they are different, the embedding system is described by (9) and (10).
The embedding algorithm is approached as follows.

a. The original image is transformed by the 8x8 block DCT.
b. We use Eq.(9) to embed watermark (W).
c. We determine the corresponding signature bits of θ and embed the signature bits of θ̣ by Eq.(10).
d. Through the IDCT, we can obtain the watermarked image.

The procedures of watermarks and signature bits extractions are similar as the embedding method.

The value of r, defined in Eq.(10), should be equal to the value of the watermark sequence W and signature bit θ from the watermarked image without any attacks. We embed the watermark to DC part and embed the signature bits, generating by the direction θ of eigenvector to the AC part. Even that θ is changed, the embedding signature bits will not be changed. If we change eigenvalue λ, the extracted watermarked image will be changed. Thus we can detect malicious tampering of image even the image have also been incidentally distorted.

5. Experimental results

We use the Lenna, Baboon, Pepper and a natural image as the test images in our experiments with 256 * 256 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.

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 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.

Fig. 1 shows the result of digital watermarking on Lenna image by the proposed watermark embedding system. 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. In Table.5, the value of PSNR given by Lin's method is similar to ours, and it's difficult to distinguish between the two methods with subjective human eyes. But in Table.5, it is oblivious that the bit error rate of the watermark detecting using our method is less than the Lin's one.

In the simulations of image authentication, we take two experiments in our simulations. One simulation gives the image authentication of the artificial manipulations. And the other one is the image processing manipulations.

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.2. Fig.2(a) is the natural image with the fragile watermarks, and the modified image by the manipulations is shown in Fig.2(b). The labels in the modified image, Fig.2(b), mark the manipulations mentioned at the above section. Fig2(c) is the simulated image of image authentication with the proposed image, and Fig.2(d) is the simulated image of image authentication using Lin's method.

(a) (b)

Fig.1 (a) Original Lenna image.
(b) Watermarked Lenna image.

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
100	0	0	0
90	0	0	0
80	0	0	0
70	0	0	0.0014
60	0.0063	0.0019	0.0053

Table.4 PSNR value of watermarked image.

PSNR	Lenna	Baboon	Peppers
Proposed method	39.42	40.00	39.51
Lin [3] method	40.55	41.07	40.81

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 experimental results show that this algorithm can resist high quality JPEG compression, avoid the malicious attacks and detect the malicious tampering correctly. In the proposed method, we can choose a good result for bit error rate after the JPEG compression robustness and malicious tampering detection.

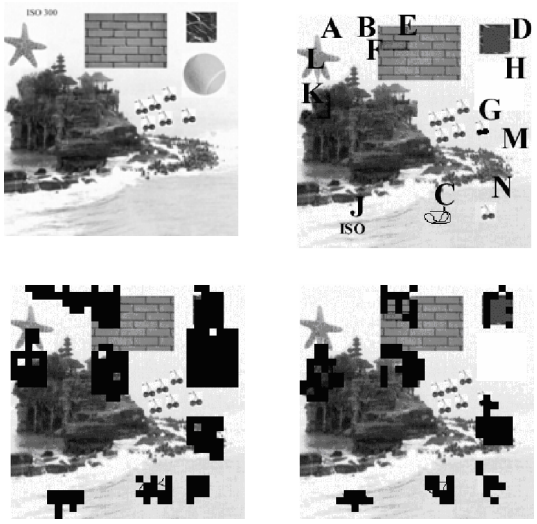

Fig2 (a) Watermarked natural image.
(b) Modified natural image.
(c) Modified areas are detected by proposed method.
(d) Modified areas are detected by Lin [3] method.

References:

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

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

[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 Watermarking Techniques Using Random Bias and Non-Uniform Quantization, *Proceeding of the SPIE, Security and Watermarking of Multimedia Contents*, 2002, pp. 659-670.

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

[6] C.S. Lu, L.Y. Liao, Multipurpose watermarking for image authentication and protection *IEEE Trans. on image Processing*, Vol. 10, 2001, pp. 1579 –1592.

[7] Q. Sun, S.-F. Chang, K. Maeno and M. Suto, A new semi-fragile imageauthentication framework combining ECC and PKI infrastructures,

Proceedings of the IEEE Circuits and Systems, 2002, pp. 440-443.

[8] J. Fridrich, "A hybrid watermark for tamper detection in digital images", in Proceedings of the Signal Processing and Its Applications, 1999, pp. 301-304.

[9] P. W. Wong, A Public key watermark for image verification and authentication, *Proceedings of the ICIP*, Vol.2, 1998, pp. 427-431.

[10] D. Coppersmith, F. Mintzer, C. Tresser, C-W. Wu, and M. M. Yeung, Fragile imperceptible digital watermark with privacy control *Proceedings SPIE, Security and Watermarking of Multimedia Contents, San Jose, California,* 1999, pp. 79-84.

[11] J. Dittmann, A. Steinmetz, and R. Steinmetz, Content-based digital signature for motion pictures authentication and content-fragile watermarking, *Proceedings of IEEE Multimedia Computing and Systems*, Vol.2, 1999, pp.209-213.

[12] R. B. Wolfgang and E. J. Delp, Fragile Watermarking Using the VW2D Watermark, *Proceedings of SPIE, Security and Watermarking of Multimedia Contents*, 1999, pp. 204-213.

[13] P. Yin and H. H. Yu, A semi-fragile watermarking system for MPEG video authentication, *Proceedings of IEEE ICASSP*, 2002, pp. 3461-3464.

[14] T. Chen, J. Wang and Y. Zhou, Combined Digital Signature and Digital Watermark Scheme for Image Authentication, 2001, pp. 78-82.

[15] G.J. Yu, C.S. Lu, H.Y. M. Liao and J.P. Sheu, Mean quantization blind watermarking for image authentication, *Proceedings of Image Processing*, 2000, pp. 706-709.

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

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

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

[19] Farzam, M., Shirani, S., A robust multimedia watermarking technique using Zernike transform, *Proceedings of Multimedia Signal Processing, IEEE*, 2004, pp. 529-534.

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