Geometric Invariant Semi-fragile Image Watermarking Using Real Symmetric Matrix

Ching-Tang Hsieh[1]*, Yeh-Kuang Wu[1] and Kuo-Ming Hung[2]

[1]*Department of Electrical Engineering, Tamkang University, Tamsui, Taiwan 251, R.O.C.*
[2]*Department of Information Management, Kainan University, Taoyuan, Taiwan 338, R.O.C.*

Abstract

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

***Key Words*:** Semi-fragile Watermark, Real Symmetric Matrix, Eigenvlaue, Geometric Invariance, Zernike Transform

1. Introduction

Due to advances in digital technologies, most data are digitized and can be easily copied or edited. Such a situation hinders the 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. Rotation, and scale invariance can be achieved by preprocessing the image to a standard image. The test image with geometric distortion is transform to the same standard image and embedded signal can be successfully recovery.

*Corresponding author. E-mail: hsieh@ee.tku.edu.tw

The desired geometric invariance can be achieved by using the fourier mellien transform (FMT). 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 achieve the geometric invariance, but the geometric invariance methods are 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 geometric invariance method is independent to embedding system. But the geometric invariance method is not robust to the malicious attacks, such as rotation and cropping combining as a severely malicious attack.

The watermarking scheme, used for image authentication, is called fragile watermarking. Fragile watermarking ideally should detect even a single bit change in a digital image and is essential for addressing the problem of data integrity. However, most fragile digital watermarks are very fragile even for slight altering. The goal of semi-fragile digital watermarking [1,3–5] is to detect unacceptable image manipulations. 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 did not provide a mechanism to detect the combination of malicious tampering and incident distortion. Lin and Chang [3] stores the DCT coefficients at all pairs of two random 8×8 blocks as the digital signature. Their method can detect malicious tampering under JPEG compression, but the digital signature based method cannot point out tampered regions clearly or some special tampers, such as those with background changed to pure white, and cannot be used for multi-watermarks system [6].

Maeno and Sun [4] used random-bias and non-uniform quantization to detect special tampers, such as object collection. They [7] developed a generic semifragile image authentication watermark framework by combining ECC and PKI security infrastructure. The watermark does not restrict the use of any specific invariant feature. 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 of the images. The method makes a valuable tool for authentication of images and detection of all types of tampering.

In this paper, we propose a novel fast rotation and scale invariance method, multi-rings Zernike transform. And a semi-fragile digital watermarking technology based on the dominant eigenvalue is proposed. 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. Because of the orthogonality 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 robustness against malicious tampering and also resist high quality JPEG compression processing. 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 digital watermarks 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, section 6, concludes the paper.

2. Multi-rings Zernike Transform

2.1 Zernike Transform

Zernike transform of image 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. These properties enable the contribution of each moment to be the unique and independent of the information of the image.

Computing the Zernike moments of an image, the center of the image is taken as the original and pixel coordinates are mapped to the unit circle. The process of calculating the Zernike moment is Zernike transform.

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

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

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

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

$n \geqq 0$, n-|m| is even, and $|m| \leqq n$. 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. For digital image, The Zernike moment of order n with repetition m can be defined as:

$$A_{nm} = \frac{n+1}{\pi} \sum_{x} \sum_{y} f(x,y) V_{nm}^{*}(x,y) \tag{3}$$

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, a novel fast rotation and scale variance method, multi-rings Zernike transform is proposed, 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.

$I = \{I_1\ I_2\ I_3\ \ldots.\ I_m\}$

After the partition, the moment of each ring '*l*' is computed according to (3).

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

Assume that the *l*th 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:

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

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

The rotation angle α^{l} can be obtained by equation (6)

$$\arg(A_{nm}^{l\,r}) = \arg(A_{nm}^{l}) + m\alpha \tag{6}$$

Scale normalization can be accomplished simply by enlarging or reducing each pattern such that the zeroth order regular moment is equal to pre-determined fixed value. $f^{l}(x/a_l, y/a_l)$ is denoted as scaled version of the image in*l*sub-block $f^{l}(x,y)$. A_{00}^{ls} is the zeroth order Zernike moment of the scaled image. The relationship of Zernike moment A_{00}^{l} of $f^{l}(x,y)$ and A_{00}^{lc} of $f^{l}(x/a_l, y/a_l)$:

$$\left|A_{00}^{lc}\right| = a_l^{\,2} \left|A_{00}^{l}\right| \tag{7}$$

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

2.2 Candidate Selection Process

According to section 2.1, 11 estimated rotation angles candidates with 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 crisp c-means algorithm. The algorithm performs a partition for each element in the feature space to c cluster and c centers of the clusters are generated. The crisp c-means algorithm assigns each feature vector to a single cluster and was adopted to separate two clusters, concentrated and distributed ones. In the literature, c is equal to 2.

Euclidean distance is most commonly used to compute the distance between the feature and assigned cluster center. The cluster criterion will be minimized under the constraints of measuring function. If the distance between the feature vector and center bigger than the

$$J(U,V) = \sum_{j=1}^{c} \sum_{i=1}^{n} u_{ij} \left\| x_i - v_j \right\|$$

where V is the vector of cluster centers, and U is the vector of weighting values.

$$u_{ij} = \begin{cases} 1, & d_{ij} = \min_{k=1}^{c}\{d_{ik}\}\ and\ d_{ij} < a \\ 0, & \end{cases}$$

$$d_{ik} = \left\| u_i - v_k \right\|$$

a is the experimental threshold, and the feature distance from the center bigger than the threshold will be isolated. $\|\cdot\|$ is Euclidean distance.

The iterative processes continuous till the cluster center become stable. The difference between cluster centers is insignificant. One of the c clusters will be selected that the variance in this cluster is smaller than other ones.

3. Eigenvectors and Eigenvalues of Real Symmetric Matrix

A real symmetric matrix R is defined by

$$R = A^T \cdot A \tag{8}$$

$$A = [a_{xy}] \qquad x, y = 1, 2...k-1,$$

$$a_{xy} = \begin{cases} l & if\ f_p(i,j) - f_q(i,j) + B_{ij} \geq 0 \\ m & if\ f_p(i,j) - f_q(i,j) + B_{ij} < 0 \end{cases} \quad i, j = 0, 1, .., n-1$$

$$k \leq n$$

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

The influences of "l" and "m" on the quantized divergence and the accuracy of watermark detection are evident. Instead of directly defining the signature bit by the value of "l" or "m" [4], it is defined by the eigenvalues and its corresponding eigenvectors from the real symmetric matrix. In our experiments, "l" is generally set to one and "m" is set to two to avoid the divergence of quantization.

The relation between the embedding and extracting strategy must be one to one and the real symmetric matrix possesses this property. Eigenvectors of the real symmetric matrix are mutually orthogonal and provide positions to embed signature bits. Eigenvalues corresponding to eigenvectors with different directions when the system is non-orthogonal and position of malicious tampers will not be found.

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 remaining eigenvectors are located in the fourth quadrant. The dominant eigenvalue λ and its corresponding eigenvector of the real symmetric matrix R will be evaluated. For eigenvector $[c, d]^T$, the direction θ of the dominant eigenvector is defined by

$$\theta = \tan^{-1}\left(\frac{c}{d}\right) \quad \text{where } 0^\circ \leq \theta \leq 90^\circ \tag{9}$$

The two different matrices, such as {(1,1), (1,1)} and {(4,4), (4,4)}, may have the same eigenvector, but they have the different eigenvalue. The corresponding table between signature bits and direction of dominant eigenvector is defined in Table 1. The sixteen real symmetric matrices will be mapped to seven independent directions of the eigenvectors presented by three bits as signature bits.

4 Proposed Watermarking Methods

4.1 Embedding Algorithm

We divide a given image into several blocks of 8×8 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 DCT_{AC_Value} belongs to the AC part.

In Eq. (2), the quantized DCT_{DC} coefficient is calculated by division by the eigenvalue λ and rounding down. Each DCT_{AC} coefficient is divided by the fixed quantization table Q_i.

The quantization functions Q_λ and Q_v are defined as:

$$Q_\lambda = \left\lfloor \frac{DCT_{DC\_Value}}{\lambda} \right\rfloor \tag{10}$$

Table 1. Signature bits and direction of dominant eigenvector. (The dimension of the real symmetric matrix is 2×2)

Signature bits	001	010	011	100	101	110	111
θ	26.56°	31.71°	37.98°	45°	52.01°	58.28°	63.43°

$$Q_V = \left\lfloor \frac{DCT_{AC\_Value}}{Q_i} \right\rfloor \quad (11)$$

$\lfloor \bullet \rfloor$ is the floor function.

In order to avoid 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 quantizer. According to the above reasoning, an adaptive quantization model incorporating the eigenvalue of the real symmetric matrix as the quantization table is proposed. 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 tampering.

The watermark-based embedding function DCT_{DC_Value} and the signature based embedding function $DCT_{\mathrm{AC\_Value}}$ are given in Eq. (4) and Eq. (5), respectively. W is a binary sequence. The value of r (Eq. (6)) is checked to embed one bit at the pair of blocks. If r is equal to the bit of watermark sequence W, the DCT coefficient is remain unchanged.

$$DCT'_{DC.Value} = \begin{cases} (Q_\lambda - 1) \times \lambda, if\ \mathrm{r} \neq W\ and\ Q_\lambda \geq 0 \\ (Q_\lambda + 1) \times \lambda, if\ r \neq W\ and\ Q_\lambda < 0 \end{cases} \quad (12)$$

$$DCT'_{AC,Value} = \begin{cases} (Q_v - 1) \times Q_i, if\ \mathrm{r} \neq 0, \mathrm{r} \neq 1\ and\ Q_v \geq 0 \\ (Q_v + 1) \times Q_i, if\ r \neq 0, \mathrm{r} \neq 1\ and\ Q_v < 0 \end{cases} \quad (13)$$

$$r = \begin{cases} 0 & ,if\ Q\ is\ even \\ 1 & ,if\ Q\ is\ odd \end{cases} \quad Q = Q_v\ or\ Q_\lambda \quad (14)$$

The flow chart of watermark embedding method is given in Figure 1. The embedding algorithm is:

a. The original image is transformed by the 8 × 8 block DCT.
b. We use Eq. (2) to embed the watermark (W).
c. We determine the corresponding signature bits of θ and embed the signature bits of θ by Eq. (3).
d. Through the IDCT, we can obtain the watermarked image.

4.2 Extraction Algorithm

The procedures for watermark and signature bit extraction, shown in Figure 2, are similar to the embedding method. The extraction algorithm is as follows:

a. The watermarked image is transformed by the 8 × 8 block DCT.
b. We use Eq. (4) to extract watermark (W*) and the signature bits of θ from the watermarked image.

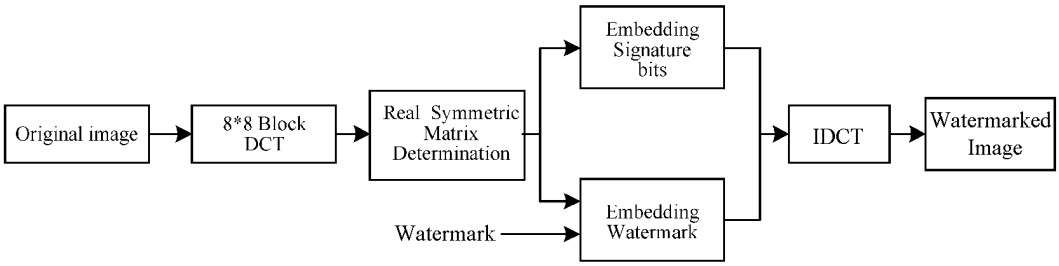

Figure 1. Block diagram of proposed digital watermark embedding system.

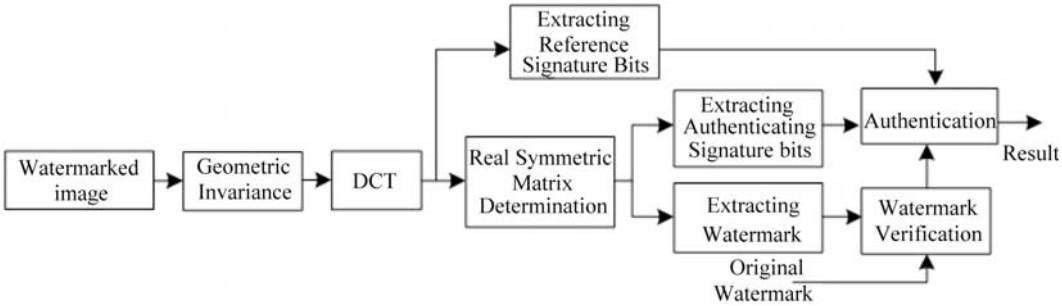

Figure 2. Block diagram of proposed digital watermark extraction system.

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.

The value of r, defined in Eq. (4), should be equal to the value of the watermark sequence W and signature bit θ from the watermarked image without any attacks. Why should we use the constant quantization table for the AC part of the DCT coefficient and use the adaptive quantization table for the DC part of the DCT coefficient? We embed the watermark in the DC part and embed the signature bits, generated by the direction θ of the eigenvector, in the AC part. Even if θ is changed, the embedded 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 the image even if it has been incidentally distorted.

5. Experimental Results

5.1 Rotation and Scaling Invariance

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. The error of the detecting rotation angle in the double attacks, which contains image processing distortion and rotation, of different radius is shown as Table 2. The component, radius of ring equals to 20, can achieve the highest robustness in the global and local attacks.

Table 3 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.

5.2 Image Quality

We use the Lenna, Baboon, Pepper and a natural image with 256 * 256 pixels for testing in our experiments. And the size of digital watermark is 32 × 32 pixels and the watermark is a binary sequence in 0's and 1's. We embed the watermark with the mask of an 8*8 block.

The PSNR of the watermarked test image is evaluated as the perceptual quality measure, and PSNR is given by

$$PSNR[dB] = 10\log_{10}\frac{255^2}{MSE} \tag{15}$$

Table 2. The MSE of the estimating angle under malicious attacks

	Attack with rotation				
	blurring	Mosaic	Noise	Pinch	Compression
radius	Mean square error (MSE)				
10	16.690	11.449	6.196	16.690	4.365
20	3.692	1.379	1.091	3.692	1.058
30	6.767	2.824	5.263	6.767	3.015
40	5.235	3.981	4.577	5.235	5.234
50	4.998	1.169	2.742	4.998	1.513

Table 3. 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

$$MSE = \frac{1}{MN}\sum_{i=1}^{MN}(org_i - emb_i)^2 \quad (16)$$

where MSE is the mean square error of the image, org_i is the ith coefficient of the original image, and emb_i is the ith coefficient of the embedded image. M,N are the length and width of the image. Figure 3 shows the Lenna image before and after watermark insertion. The PSNR value of watermarked image is given in Table 4.

5.3 Dimension Decision of the Real Symmetric Matrix

The dimension of the real symmetric matrix is one of the main features of our system. The capacity of the image watermarking is proportional to the dimension of the real symmetric matrix and inversely proportional to the quality of watermarking image. Table 5 shows the quality of the watermarked image with different dimensions of the real symmetric matrix. In Table 5, we find that the bit error rate dose not decrease with an increase in the real symmetric matrix's dimension.

The bit error rate is given by

Bit error rate =

(watermarks bit error rate + signature bit error rate)/2

$$\text{Watermark bit error rate} = \frac{org_{watermark} \oplus new_{watermark}}{(M \times N) \ / \ (8 \times 8)} \quad (17)$$

(a) (b)

Figure 3. (a) Original Lenna image. (b) Watermarked Lenna image.

Table 4. PSNR value with different dimension of the real symmetric matrix

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

$$\text{Signature bit error rate} = \frac{\sum_{i=0}^{K-1}(org_{sig} \oplus new_{sig})}{K \times (M \times N) \ / \ (8 \times 8)} \quad (18)$$

where $org_{watermark}$ is original watermark, $new_{watermark}$ is the extracted watermark, org_{sig} is the original signature bits, and new_{sig} is the extracted signature bits. K is the length of the signature bits, and $\oplus$ is the Exclusive-Or operator.

According to the above experiments, the dimension of the real symmetric matrix is 2 × 2.

5.4 Comparison

The extracted watermark and signature bits are expected to be the same as the original ones with the reasonable image compression.

Table 6 gives 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 if the JPEG quality is below 60. In Table 7, the value of PSNR given by Lin's method is similar to ours, and is difficult to distinguish between the two methods visually. But in Table 7, it is oblivious that the bit error rate of watermark detection using our method is less than for Lin's.

Table 8 gives a comparison between our method and

Table 5. Bit error rate of images under different quality of JPEG compression

JPEG Quality	Dimension of real symmetric matrix	
	2 × 2	3 × 3
	Bit error rate	
80	0	0
70	0	0
65	0.0004	0.0004
55	0.0029	0.0034
50	0.0097	0.0122

Table 6. Bit error rate of proposed extracting method 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 7. 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

Table 8. Bit error rate for various embedding algorithms

JPEG quality	Proposed method	Kunder's method ($l = 2$)	Kunder's method ($l = 3$)	Lin's method
80	0	0.1355	0.0615	0
70	0	0.2749	0.0732	0
65	0.0010	0.3643	0.1357	0.0010
55	0.0117	0.4265	0.1455	0.0273
50	0.0537	0.4453	0.1729	0.1138

Kunder's. In Kunder's method the value of l is the decomposition level of the wavelet transform. The proposed method outperforms Kunder's method in the different value l, and the performance of malicious tampers detection decreases when the value of l increases. Our proposed method gives the high performance of malicious tampering detection, and a lower bit error rate.

5.5 Image Authentication

For image authentication, we run two simulations, one for the image authentication of artificial manipulations and the other for image processing manipulations.

Figures 4–6 compare image authentication of the artificial manipulations using our method and Lin's method [3]. In the experiment, the modified "Pepper", "Lenna", and "Baboon" images are shown in Figure 4(a), Figure 5(a), and Figure 6(a). In Figure 4(b), Figure 5(b) and Figure 6(b), all the modified areas are detected by our algorithm, which are marked in black. Some modified areas are not detected by Lin's method as shown in Figure 4(c), Figure 5(c), and Figure 6(c). The extracted watermarks or signature bits will be changed in any block. We can detect the modified areas, since we embed watermarks and signature bits in all blocks.

Figure 7 shows the image authentication of the artificial manipulations with 30 degree rotation. The detecting malicious areas are marked by black labels. In our met-

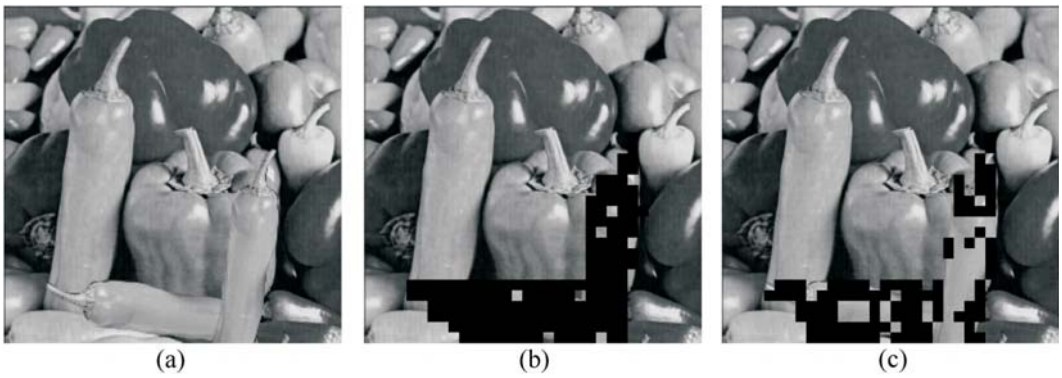

Figure 4. (a) Modified Pepper image. (b) Modified areas detected by proposed method. (c) Modified areas detected by Lin [3] method.

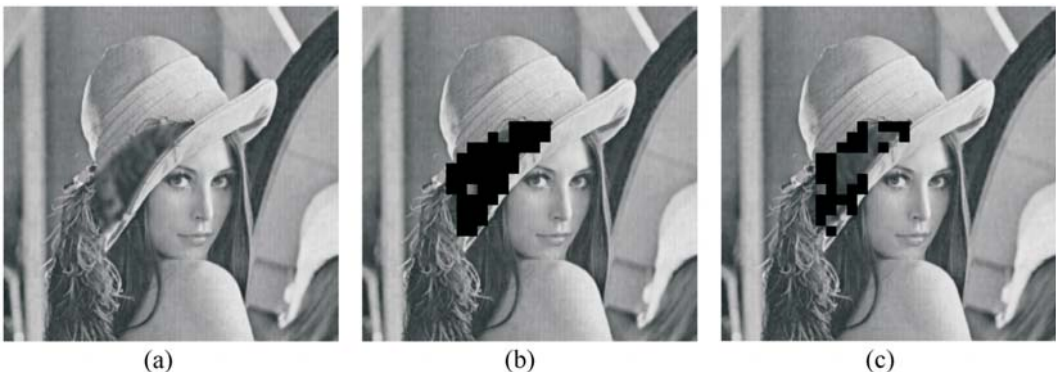

Figure 5. (a) Modified Lenna image. (b) Modified areas are detected by proposed method. (c) Modified areas are detected by Lin [3] method.

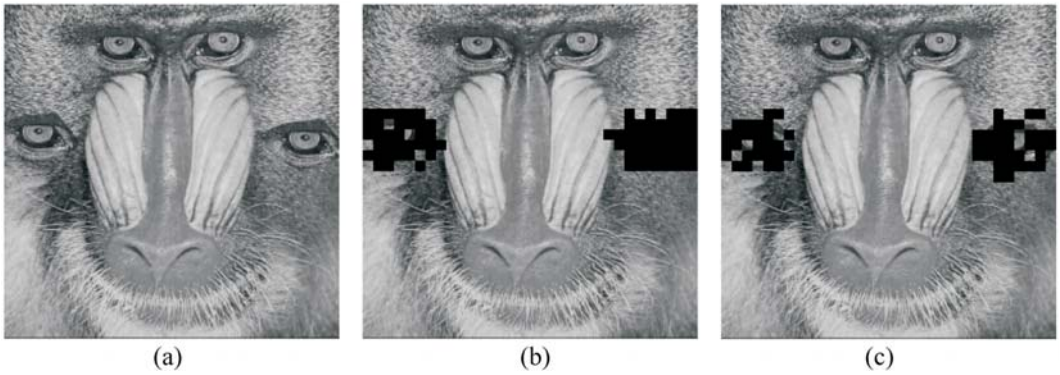

Figure 6. (a) Modified Baboon image. (b) Modified areas are detected by proposed method. (c) Modified areas are detected by Lin [3] method.

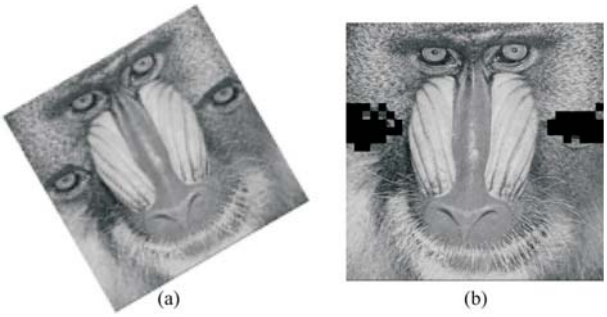

Figure 7. (a) Rotation Baboon image. (b) Simulated result of (a). Modified areas are detected by proposed method.

hod, the MRZT can successfully detect the rotated agree of the attacked image, and the proposed watermarking system can detect the attacked area.

We show the results of authentication for some quite general kinds of image processing manipulations which include

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

Figure 8(a) is a natural image with fragile watermarks, and Figure 8(b) shows the modified Figure 8(c) and Figure 8(d) show the result of authentication using the proposed method and Lin's method, respectively. As seen in Figure 8(c), we detect all the modified areas and mark them in black, which in Figure 8(d) some of the modified areas are not be detected by the Lin's method, such as (A) deleting, (B) deleting background area, and (L) adding an extra limb.

6. Conclusion

In this paper, we successfully put forward a semi-

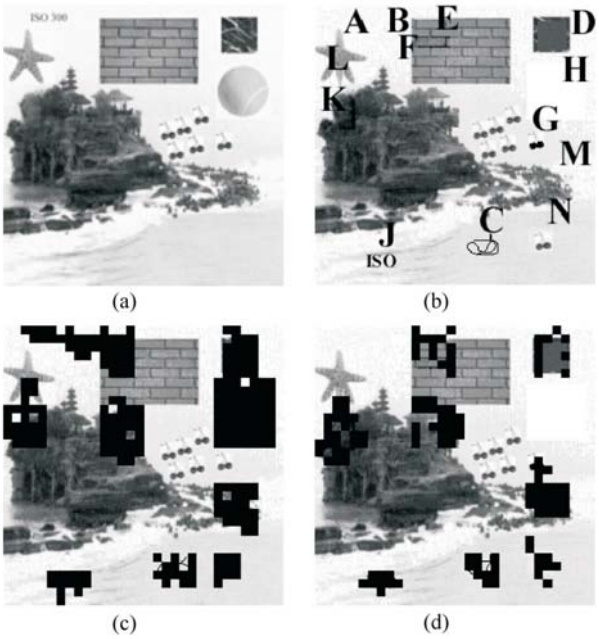

Figure 8. (a) Watermarked natural image. (b) Modified natural image. (c) Modified areas are detected by proposed method. (d) Modified areas are detected by Lin [3] method.

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.

References

[1] Kundur, D. and Hatzinakos, D., "Digital Watermarking for Telltale Tamper Proofing and Authentication," in *Proceedings of IEEE Digital Object Identifier*, Vol. 87, pp. 1167–1180 (1999).

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

[3] Lin, C. Y. and Chang, S. F., "Semi-Fragile Watermarking for Authenticating JPEG Visual Content," in *Proceeding of the SPIE, Security and Watermarking of Multimedia Contents*, pp. 140–151 (2000).

[4] Maeno, K., Sun, Q., Chang, S. F. and Suto, M., "New Semi-Fragile Image Authentication Watermarking Techniques Using Random Bias and Non-Uniform Quantization," in *Proceedong of the SPIE, Security and Watermarking of Multimedia Contents*, pp. 659–670 (2002).

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

[6] Lu, C. S. and Liao, L. Y. M., "Multipurpose Watermarking for Image Authentication and Protection," *IEEE Transactions on Image Processing,* Vol. 10, pp. 1579–1592 (2001).

[7] Sun, Q., Chang, S. F., Maeno, K. and Suto, M., "A New Semi-Fragile Image Authentication Framework Combining ECC and PKI Infrastructures," in *Proceedings of the IEEE Circuits and Systems*, pp. 440–443 (2002).

[8] Fridrich, J., "A Hybrid Watermark for Tamper Detection in Digital Images," in *Proceedings of the Signal Processing and Its Applications*, pp. 301–304 (1999).

[9] Wong, P. W., "A Public Key Watermark for Image Verification and Authentication," in *Proceedings of the ICIP*, Vol. 2, pp. 427–431 (1998).

[10] Coppersmith, D., Mintzer, F., Tresser, C., Wu, C. W. and Yeung, M. M., "Fragile Imperceptible Digital Watermark with Privacy Control," in *Proceedings SPIE, Security and Watermarking of Multimedia Contents*, pp. 79–84 (1999).

[11] Dittmann, J., Steinmetz, A. and Steinmetz, R., "Content-Based Digital Signature for Motion Pictures Authentication and Content-fragile Watermarking," in *Proceedings of IEEE Multimedia Computing and Systems*, Vol. 2, pp. 209–213 (1999).

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

[13] Yin, P. and Yu, H. H., "A Semi-Fragile Watermarking System for MPEG Video Authentication," in *Proceedings of IEEE ICASSP*, pp. 3461–3464 (2002).

[14] Chen, T., Wang, J. and Zhou, Y., "Combined Digital Signature and Digital Watermark Scheme for Image Authentication," in *Proceedings of Info-tech and Info-net*, pp. 78–82 (2001).

[15] Yu, G. J., Lu, C. S., Liao, H. Y. M. and Sheu, J. P., "Mean Quantization Blind Watermarking for Image Authentication," in *Proceedings of Image Processing*, pp. 706–709 (2002).

[16] Kim, H. S. and Lee, H. K., "Invariant Image Watermark Using Zernike Moments," *IEEE Transactions on Circuits and Systems for Video Technology*, pp. 766–775 (2003).

[17] Xin, Y., Liao, S. and Pawlak, M., "A Multibit Geometrically Robust Image Watermark Based on Zernike Moments," in *Proceedings of Pattern Recognition*, pp. 861–864 (2004).

[18] Liu, H., Lin, J. and Huang, J., "Image Authentication Using Content Based Watermark," in *Proceedings of IEEE Circuits and Systems,* pp. 4014–4017 (2005).

[19] Farzam, M. and Shirani, S., "A Robust Multimedia Watermarking Technique Using Zernike Transform," in *Proceedings of IEEE Multimedia Signal Processing,* pp. 529–534 (2004).

[20] Chen, J., Yao, H., Gao, W. and Liu, S., "A Robust Watermarking Method Based on Wavelet and Zernike Transform," in *Proceedings of Circuits and Systems*, pp. 173–176 (2004).

Manuscript Received: Jan. 17, 2006
Accepted: May. 9, 2006