International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:3, No:11, 2009

A Normalization-based Robust Watermarking Scheme Using Zernike Moments

Say Wei Foo, Qi Dong

***Abstract*—**Digital watermarking has become an important technique for copyright protection but its robustness against attacks remains a major problem. In this paper, we propose a normalization-based robust image watermarking scheme. In the proposed scheme, original host image is first normalized to a standard form. Zernike transform is then applied to the normalized image to calculate Zernike moments. Dither modulation is adopted to quantize the magnitudes of Zernike moments according to the watermark bit stream. The watermark extracting method is a blind method. Security analysis and false alarm analysis are then performed. The quality degradation of watermarked image caused by the embedded watermark is visually transparent. Experimental results show that the proposed scheme has very high robustness against various image processing operations and geometric attacks.

***Keywords*—**Image watermarking, Image normalization, Zernike moments, Robustness.

I. Introduction

DIGITAL images can be easily duplicated without any loss. This feature facilitates the illegal use of copyrighted materials, e.g., unrestricted duplication and dissemination via the Internet. To protect copyrighted images, many approaches, including authentication, encryption and digital watermarking [1]-[6], have been proposed. Encryption methods may guarantee secure transmission of data to authenticated users through unsecured channels. However, once decrypted, the data are identical to the original and their piracy cannot be controlled. Robust digital watermarking is a way to prove the ownership of the materials. It embeds invisible watermarks or ownership information into digital contents. The watermarks should be robust enough to survive various attacks and at the same time, the embedded watermarks should not significantly degrade the visual quality of original host images.

As digital watermarking technologies become more advanced, attacks against watermarking systems have also become more sophisticated. Those attacks can be classified into image processing operations and geometric attacks. Image processing operations, such as lossy compression, noise addition and filtering, reduce the energy of embedded watermarks, while geometric attacks induce synchronization errors between the original and watermarked images. Watermark detection may fail as a result, even if the watermark still exists in the watermarked image. Most of previous watermarking schemes [7]-[28] are able to guarantee high robustness against common image processing operations, but they lack robustness against geometric attacks such as rotation, scaling and translation.

Zernike moments are ideal region-based shape descriptors and they have been shown to be invariant against rotation, flipping, scaling and noise addition [11], [12]. Besides that, low-order Zernike moments are also robust and invariant against common image processing operations. In this paper, we propose a novel robust image watermarking scheme using Zernike moments [12]. Zernike moments are employed for its special invariance properties against distortions. Unlike traditional moment-based watermarking schemes where watermark bits are directly embedded into original host images, we first normalize original host image to a standard form, based on which subsequent watermark embedding and extracting are performed. Zernike transform is applied to the normalized image to obtain Zernike moments. Dither modulation is then adopted to quantize the magnitudes of Zernike moments according to the watermark bit stream followed by security analysis and false alarm analysis. The watermarked images have high visual quality. Experimental results show that the proposed scheme is robust against various image processing operations and geometric attacks.

The rest of this paper is organized as follows. The procedures of image normalization are explained in section II. In section III, the proposed robust image watermarking scheme is described in detail. Experimental results are presented in section IV and the concluding remarks are given in Section V.

II. Image Normalization

Image normalization [17], [18] using moments is a technique used for pattern recognition. In this section, we describe a moment-based normalization process that achieves invariance properties against geometric attacks. The geometric attacks include rotation, scaling and translation of an image. These kinds of attacks can be represented by affine transformations. An affine transformation with scaling parameters (a, b), rotation angle φ and translational parameters (T_x, T_y) is defined as

Say Wei Foo is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: eswFoo@ntu.edu.sg).

Qi Dong is with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore (e-mail: DONG0041@e.ntu.edu.sg).

$$\begin{bmatrix} x_a \\ y_a \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} T_x \\ T_y \end{bmatrix} \quad (1)$$

where (x, y) is a pixel coordinates of an input image and (x_a, y_a) is the corresponding pixel coordinates of the transformed image. The affine transform parameters can be calculated from image moments. The image moments m_{pq} of an input image $f(x, y)$ with size of $N_1 \times N_2$ pixels, is defined in the two dimensional Cartesian coordinates as

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

The centroid of the input image can be calculated using the 0th and 1st moments:

$$\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}} \quad (3)$$

The translation effect can be eliminated by shifting the centroid of input image to $(\bar{x}, \bar{y})$. Thus a centralized image is obtained by setting translational parameters $T_x = -\bar{x}$ and $T_y = -\bar{y}$.

The central moment μ_{pq} is defined as

$$\mu_{pq} = \sum_{y=0}^{N_2-1} \sum_{x=0}^{N_1-1} (x - \bar{x})^p (y - \bar{y})^q \cdot f(x, y) \quad (4)$$

And the covariance matrix based on the central moments is constructed as

$$\begin{pmatrix} \mu_{20} & \mu_{11} \\ \mu_{11} & \mu_{02} \end{pmatrix} \quad (5)$$

Based on the covariance matrix, the rotation angle φ is calculated as

$$\varphi = \frac{1}{2} \tan^{-1} \left[\frac{2\mu_{11}}{\mu_{20} - \mu_{02}} \right] \quad (6)$$

The two eigenvalues of the covariance matrix are given by

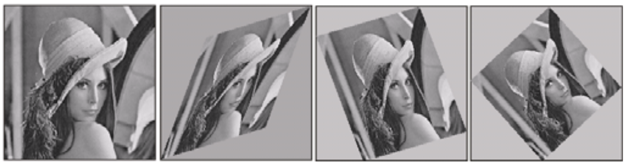
$$\lambda_i = \frac{1}{2} \left[(\mu_{20} + \mu_{02}) \pm \sqrt{4\mu_{11}^2 + (\mu_{20} - \mu_{02})^2} \right] i = 1,2 \quad (7)$$

Based on the eigenvalues, the scaling parameters are calculated as

$$a = (\lambda_1 \lambda_2)^{0.25} / \sqrt{\lambda_1}, b = (\lambda_1 \lambda_2)^{0.25} / \sqrt{\lambda_2} \quad (8)$$

Thus, any input image can be transformed to a normalized form by identifying the transform parameters, $(a, b), \varphi$ and $(\bar{x}, \bar{y})$.

An illustration of this normalization process is presented in the following figures. Figure 1(a) is the original host image. Figure 1(b) and (c) are the images obtained after general affine transformations. By applying the above normalization procedures, these three different images yield the same normalized image, as shown in Fig. 1(d). This normalized image is subsequently used for watermark embedding. As the normalized image has invariance properties against different affine transformations, the embedded watermarks in the normalized image can be accurately synchronized under a variety of possible affine transformations.



(a) (b) (c) (d)

Fig. 1 Demonstration of image normalization

III. Proposed Watermarking Scheme

A. Watermark Embedding Process

For the watermark embedding process, first, Zernike transform is performed to calculate Zernike moments over a normalized image. The values of Zernike orders n and repetitions m are selected as follows. It can be shown that the Zernike moments generated under orders from 0 to 29 are robust against image distortions and Zernike moments with high orders cannot be computed accurately. Zernike moments with repetitions $m = 4i$ $(i \in Z)$ also cannot be computed accurately [11]. According to the features of Zernike moments [12], it is only necessary to consider the case when m is larger than 0. Let $S = \{Z_{nm}: n \le N_{max}, m > 0, m \ne 4i\}$ be the set of candidate Zernike moments for watermark embedding after performing Zernike transform on a normalized image. In the experiments reported in this paper, N_{max} is set to be 29.

Two secret keys are first generated. One (encryption key) is used to encrypt the original ownership information and obtain a pseudo-random watermark bit stream $W = \{w(i), 1 \le i \le L\}$. The other one (position key) is used to pseudo-randomly select L Zernike moments from S to form a Zernike moment vector $Z = (Z_{n_1m_1}, Z_{n_2m_2}, \dots\dots Z_{n_Lm_L})$ which is then used for watermark embedding. These two secret keys are required to extract watermark bits and recover the original ownership information. The dither modulation [21], which is a special form of quantization index modulation for signal quantization, is adopted to quantize the magnitudes of Zernike moments in Z and embed watermark bits. After quantization, a new Zernike moment vector $Z' = (Z'_{n_1m_1}, Z'_{n_2m_2} \dots\dots Z'_{n_Lm_L})$ is produced, where $Z'_{n_im_i}$ is the quantized version of $Z_{n_im_i}$ satisfying

$$|Z'_{n_im_i}| = \left[\frac{|Z_{n_im_i}| - d_i(w(i))}{\Delta} \right] \cdot \Delta + d_i(w(i)), 1 \le i \le L \quad (9)$$

In the above equation, $[\cdot]$ denotes rounding operation, Δ is the quantization step size and $d_i(\cdot)$ is the dither function for i-th quantization such that $d_i(1) = \frac{\Delta}{2} + d_i(0)$. The dither variable $d_i(0)$ is uniformly distributed over $(0, \Delta]$ and is randomly generated by modulation generator. Note that a large Δ can increase embedding strength and robustness, but it can also degrade the quality of watermarked image significantly. The value may be chosen to suit the specific requirements.

The modified Zernike moments is calculated as

$$Z'_{n_im_i} = sgn(Z_{n_im_i}) \cdot |Z'_{n_im_i}|, 1 \le i \le L \quad (10)$$

Note that, the conjugate $Z^*_{n_i,m_i}$ of each $Z_{n_i m_i}$ should also be quantized to have the same magnitude, so the pixel values in the reconstructed image are real.

In the proposed scheme, in order to reduce the quality degradation of watermarked image, the watermarked image is generated by adding quantization errors and original image in spatial domain. Let $e_{n_i m_i} = Z'_{n_i m_i} - Z_{n_i m_i}$ and $e^*_{n_i,m_i} = {Z^*_{n_i,m_i}}' - Z^*_{n_i,m_i}$ denote the quantization errors of $Z_{n_i m_i}$ and $Z^*_{n_i,m_i}$ respectively. The quantization errors in spatial domain is expressed as

$$e(x,y) = \sum_{i=1}^{L} \left[e_{n_i m_i} \cdot V_{n_i m_i}(\rho,\theta) + e^*_{n_i,m_i} \cdot V^*_{n_i m_i}(\rho,\theta) \right] \quad (11)$$

where $V_{n_i m_i}(\rho,\theta)$ is the complex-valued function of Zernike moments. Thus the watermarked normalized image $f'(x,y)$can be obtained by adding original image and quantization errors in spatial domain as follows.

$$f'(x,y) = f(x,y) + e(x,y) \quad (12)$$

The modified Zernike moments can be calculated by performing Zernike transform on the watermarked image and quality degradation is still visually transparent. The final watermarked image is obtained by restoring to the original image size and position before normalization.

B. Watermark Extracting Process

The original image is not required for watermark extraction, so the proposed watermarking method is a blind method.

First, the normalization procedures are performed on the watermarked image which is possibly distorted or attacked. As a result, the normalized watermarked image is obtained. Zernike transform is then applied to calculate Zernike moments up to the order of 29 over the normalized image. The position key is used to locate and select L moments, forming a set of Zernike moments $\tilde{Z} = (\tilde{Z}_{n_1 m_1}, \tilde{Z}_{n_2 m_2}, \dots\dots \tilde{Z}_{n_L m_L})$, which possibly carries the watermark bits.

Two dither variables $d_i(0)$ and $d_i(1)$ are generated. Two quantized versions of each $|\tilde{Z}_{n_i m_i}|$ in $\tilde{Z}$ with respect to the two dither variables are calculated as

$$|\tilde{Z}_{n_i m_i}|_j = \left[\frac{|\tilde{Z}_{n_i m_i}| - d_i(j)}{\Delta} \right] \cdot \Delta + d_i(j), \;\; 1 \le i \le L, j = 0,1 \quad (13)$$

By comparing the distances between $|\tilde{Z}_{n_i m_i}|$ and its two quantized versions, the watermark bit embedded in $|Z_{n_i m_i}|$can be extracted as follows.

$$\widetilde{w}(i) = \operatorname{argmin}_{j \in \{0,1\}} (|\tilde{Z}_{n_i m_i}|_j - |\tilde{Z}_{n_i m_i}|)^2, \;\; 1 \le i \le L \quad (14)$$

This watermark bit extracting method is called minimum distance decoder [16].

The final extracted watermark bit stream is a composite of all single extracted watermark bits. The encryption key is then used to de-encrypt the extracted watermark bit stream and recover the original ownership information.

C. Security Analysis

The security of embedded watermarks is of paramount importance as the embedded watermark can be readily identified and altered if the positions of the watermark bits are easily detected by attackers. For the methods described in [22] and [23], the watermark embedding positions are deterministic so a simple attack, such as adding perturbations to the embedding positions or statistical attack, will be able to cause detection errors while introduce insignificant quality degradation. In the proposed watermarking scheme, L Zernike moments are pseudo-randomly selected from 29 Zernike moments to form a Zernike moment vector for watermarking embedding. By using sophisticated pseudo-random number generation scheme, it will be difficult for an attacker to guess the embedding positions correctly without knowing the position key. If attackers try to average the magnitudes of all Zernike moments, the resulting attacked watermarked image would have very low visual quality. A typical attacked image is given in Fig.2, with PSNR=18.8dB.

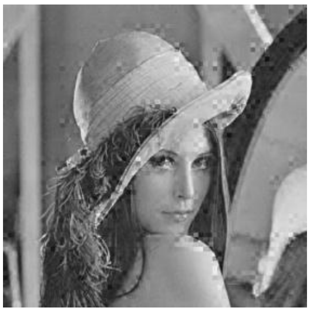


Fig.2 Attacked watermarked image by averaging operation

D. False Alarm Analysis

The false positive error named as false alarm occurs when the watermark extraction result indicates the presence of a watermark in a non-watermarked image [3,8]. In the proposed scheme, to minimize the probability of false alarm, a comparison between the extracted watermark bits and the watermark bits is necessary. For a non-watermarked image, the extracted bits from this image are assumed to be independent random variables (Bernoulli trials) [8]. Each extracted bit has the same probability to match the corresponding watermark bit. For random binary data, this probability is assumed to be 0.5. Let r be the number of extracted bits from one non-watermarked image that can match the watermark bits. As explained, an image is classified as a watermarked image if r is larger than a given threshold. Let L be the length of watermark bit stream and T be the threshold value ($T \le L$). Hence, the false alarm probability of a non-watermarked image is, therefore, the cumulative probability of the cases that $r \ge T$. And it is calculated as

$$P_{image} = \sum_{r=T}^{L} (0.5)^L \cdot \left(\frac{L!}{r!(L-r)!}\right) \quad (15)$$

If L is set to be 25, then the relationship between false alarm probability P_{image} and threshold T is plotted in Fig. 3.

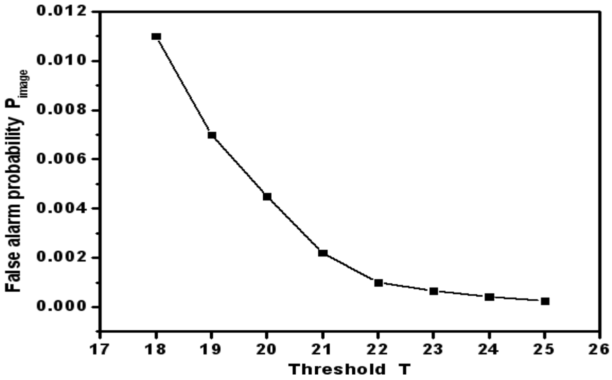


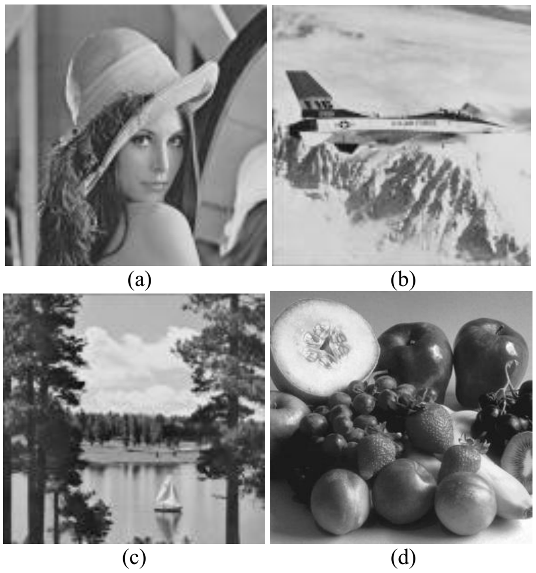
Fig. 3 False alarm probability curve

The curve in Fig. 3 drops sharply for T >22 and it is desirable to have a very small false alarm probability. However, the selection is application dependant. It is assumed that the probability should be less than 0.001. In this case, T should be greater than or equal to 23, and at T =23, the probability is 0.00084. Hence, the length of watermark bit stream should be larger than 23.

IV. Performance of Proposed Scheme

The performance of the proposed scheme is assessed. Several experiments are performed. Details of the experiments and experimental results are presented in this section.

Four 256×256 grey-level images are used as original host images and they are shown in Fig. 4. A 25-bit binary sequence is used as watermark bit stream.



(a) (b)

(c) (d)

Fig. 4 Original host images: (a) Lena, (b) Plane, (c) Lake, (d) Fruits

A. Visual quality evaluation

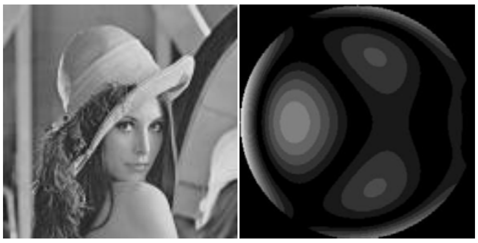
One of the requirements of robust image watermarking is visual transparency of embedded watermark, which means the embedded watermark should not significantly degrade the quality of the host image. The proposed watermark embedding scheme with different quantization step sizes is applied to the host images in Fig. 4. Peak Signal-to-Noise Ratio (PSNR) is used to evaluate quality degradation of watermarked images. The PSNR values for the watermarked images under different quantization step sizes are tabulated in Table I.

TABLE I
PSNR (dB) Values for Different Step Sizes

PSNR (dB)		Watermarked images			
		Lena	Plane	Lake	Fruits
step size Δ	1	45.0	44.1	49.7	48.7
	2	41.2	40.0	45.8	45.2
	3	38.5	39.2	45.6	45.8
	4	32.2	33.0	40.9	40.8
	5	33.5	32.1	39.1	39.7

It can be seen that the PSNR values decrease as step size increases for the same watermarked image, that is, the images suffer more degradation. For a given step size, the PSNR values for highly textured images such as "Lake" and "Fruits" are higher than those of 'simpler' images. However, the step size is positively related to watermark embedding strength. For robust watermarking, it is desirable to achieve highest-possible embedding strength without significant visual quality degradation. For the experiments, the host images, "Lena" and "Plane", are embedded using step size of 3; the host images, "Lake" and "Fruits" are embedded using step size of 5.

The proposed scheme with the quantization step size of 3 is applied to embed the watermark into original Lena image. The watermarked image is shown in Fig. 5(a). The quantization errors which are linearly normalized to the range of [0,255] and rounded to integers are shown in Fig. 5(b).



(a) (b)

Fig. 5 (a) Watermarked image (b) Quantization errors

It can be seen that the watermarked image is visually the same as the original host image. The grey regions in Fig. 5(b) indicate quantization errors and black regions indicate the regions whose pixel values are not modified. The quantization errors are well spread around the watermarked images. The numbers of occurrence for the values of quantization errors are plotted in the form of a histogram in Fig. 6.

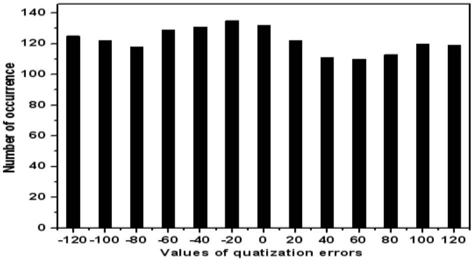


Fig. 6 Histogram of quantization errors

B. Robustness Evaluation

The following is a list of operations and attacks used to test the robustness of proposed watermarking scheme.

(1) JPEG compression with different quality factors: (a) 5, (b) 10, (c) 15, (d) 20, (e) 25, and (f) 30.

(2) Median filtering with different sizes: (a) 4×4, (b) 5×5, (c) 6×6, (d) 7×7, (e) 8×8, and (f) 9×9.

(3) Noise addition: (a) Uniform noise (0.2), (b) Uniform noise (0.3), (c) Gaussian noise (0.2), (d) Gaussian noise (0.3), (e) Salt & pepper noise (0.05), and (f) Salt & pepper noise (0.08).

(4) Common image processing operations: (a) sharpening by kernel $\begin{pmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{pmatrix}$, (b) sharpening by kernel $\begin{pmatrix} 0 & -2 & 0 \\ -2 & 6 & -2 \\ 0 & -2 & 0 \end{pmatrix}$, (c) Gaussian filtering by kernel (1/8) $\begin{pmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 1 & 1 \end{pmatrix}$, (d) Gaussian filtering by kernel (1/16) $\begin{pmatrix} 2 & 2 & 3 \\ 1 & 3 & 5 \\ 3 & 1 & 4 \end{pmatrix}$, (e) frequency mode Laplacian removal (FMLR) attack, and (f) Color quantization. Color quantization is similar to GIF compression.

(5) StirMark bending strength (a) 2, (b) 3, (c) 4, (d) 5, (e) 6, and (f) 7.

(6) Line and column removal: (a) (2, 5), (b) (5, 2), (c) (3, 6), (d) (6, 3), (e) (7, 8), and (f) (8, 7), where each pair of numbers indicate the number of rows and columns removed, respectively. The removed rows or columns are equidistant.

(7) Scaling by different factors: (a) 0.5, (b) 0.75, (c) 0.8, (d) 1.1, (e) 1.5, and (f) 1.8.

(8) Rotation through different angles: (a) -25°, (b) -15°, (c) -10°, (d) 25°, (e) 35°, and (f) 45°.

(9) Aspect ratio change: (a) (0.8, 1.1), (b) (0.9, 1.1), (c) (1.1, 0.8), (d) (1.1, 0.7), (e) (1.2, 0.9), and (f) (1.2, 1.0), where each pair of numbers indicate the amount of scaling in *x* and *y* directions, respectively.

(10) Sharing; (a) (5%, 1%), (b) (2%, 5%), (c) (1%, 3%), (d) (5%, 3%), (e) (2%, 2%), and (f) (5%, 5%), where each pair of numbers indicate the amount of shearing in *x* and *y* directions, respectively.

(11) General affine transformations: (a) matrix transformation $\begin{pmatrix} 1.2 & 0.3 \\ -0.2 & 0.8 \end{pmatrix}$, (b) matrix transformation $\begin{pmatrix} 1.1 & 0.1 \\ -0.3 & 0.9 \end{pmatrix}$, (c) matrix transformation $\begin{pmatrix} 1.0 & 0.5 \\ -0.1 & 0.7 \end{pmatrix}$, (d) matrix transformation $\begin{pmatrix} 1.2 & 0.9 \\ -0.8 & 0.2 \end{pmatrix}$, (e) Horizontal flipping, and (f) Vertical flipping.

(12) Combination attacks: (a) JPEG 15+Rotation 25°, (b) JPEG 20+Scaling 0.8, (c) Median filtering 5×5+Rotation 30°, (d) Median filtering 6×6+Scaling 1, (e) Gaussian noise (0.3)+Shearing(5%,3%), and (f) Salt & pepper noise (0.05)+ Aspect ratio change (0.8, 1.1).

The watermark bits are extracted from the attacked images. The bit error rate (BER), defined as the ratio of the number of incorrectly extracted bits over the total number of embedded watermark bits, is then calculated for all the cases. For ease of presentation, the BER values of the four images subjected to the same operation or attack are averaged. The average BER values are tabulated in Table II.

TABLE II
AVERAGE BER VALUES

Attack or operation	(a)	(b)	(c)	(d)	(e)	(f)
(1)	0.12	0.085	0.056	0.03	0	0
(2)	0.02	0.027	0.034	0.069	0.085	0.127
(3)	0	0.016	0.023	0.029	0.03	0.037
(4)	0.025	0.031	0.082	0.031	0.052	0.026
(5)	0.017	0.026	0.036	0.058	0.127	0.188
(6)	0	0	0.015	0.013	0	0.02
(7)	0.02	0	0	0	0	0.029
(8)	0	0	0	0	0	0
(9)	0	0	0	0	0	0.016
(10)	0.02	0	0	0	0	0.012
(11)	0	0.051	0.022	0.03	0	0
(12)	0.023	0.086	0.071	0.052	0.08	0.045

It can be observed from the experimental results that the proposed scheme is robust against the listed operations and attacks including both image processing operations and geometric attacks, except when StirMark bending strength is very high.

V. CONCLUSION

A novel image watermarking scheme is described in this paper. For the scheme, the original host image is first normalized to a standard form. The watermark bits are then embedded by quantizing the magnitudes of Zernike moments calculated from the normalized image.

It is observed that the quality degradation caused by embedded watermark is not significant while the proposed scheme is very robust against various image processing operations and attacks including geometric attacks.

REFERENCES

[1] J. J. K. O'Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection," in Proc. Inst. Elect. Eng., vol. 143, no. 4, pp. 250–256, Aug. 1996.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, Dec. 1997.

[3] Ning Bi, Qiyu Sun, Daren Huang, Zhihua Yang, Jiwu Huang, "Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition," *IEEE Transactions on Image Processing*, Volume 16, Issue 8, Aug. 2007 Page(s):1956 – 1966

[4] Ching-Yung Lin and Shih-Fu Chang, A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 11 No. 2, 2001, pp. 129 –138

[5] P. S. L. M. Barreto, H.Y. Kim, andV. Rijmen, "Toward secure public-key blockwise fragile authentication watermarking," in Proc. *Inst. Elect. Eng.*, vol. 149, no. 2, pp. 57–62, Apr. 2002.

[6] N. Singhal, Y. Y. Lee, and S. U. Lee, "Robust image watermarking using local Zernike moments," *Science Direct. Image Process.* vol. 11, no. 6, pp. 585–595, Jun. 2008.

[7] Xiang-yang Wang, Li-min Hou and Jun Hu "A feature-based robust digital image watermarking scheme," *IEEE Transactions on Image Processing*, Volume 15, Issue 10, Oct. 2007 Page(s):3189 – 3200.

[8] Ching-Yung Lin and Shi-Fu Chang, "Semi-fragile watermarking for authenticating JPEG visual content", SPIE, Security and Watermarking of Multimedia Contents, pp.140-151, 2000.

[9] Zhe-Ming Lu, Chun-He Liu, Dian-Guo Xu, Sheng-He Sun, "Semi-fragile image watermarking method based on index constrained vector quantization," *Electronics Letters*, Volume 39, Issue 1, 9 Jan 2003 Page(s):35 – 36.

[10] C. S. Lu and H. Y. M. Liao, "Multipurpose watermarking for image authentication and protection," *IEEE Trans. Image Process.*, vol. 10, pp. 1579–1592, Oct. 2001.

[11] Fan Gu, Zhe-Ming Lu, Jeng-Shyang Pan, "Invariant Watermarking Using Zernike Moments," *IEEE International Symposium on Circuits and Systems*, 2005. Vol. 5, Page(s):4417 – 4420.

[12] Zhe-Ming Lu, Dian-Guo Xu, Sheng-He Sun, "A Novel Watermarking Scheme based on SVD and Zernike Moments," *IEEE Transactions on Image Processing*, Volume 14, Issue 6, June 2005 Page(s):822 – 831

[13] Z. M. Lu and S. H. Sun, "Digital image watermarking technique based on vector quantization," *Electron. Lett.*, vol. 36, no. 4, pp. 303–305, Feb. 2000.

[14] Z. M. Lu, J. S. Pan, and S. H. Sun, "VQ-based digital image watermarking method," *Electron. Lett.*, vol. 36, no. 14, pp. 1201–1202, Jul. 2000.

[15] Z. M. Lu, C. H. Liu, and S. H. Sun, "Digital image watermarking technique based on block truncation coding with vector quantization," Chinese J. Electron., vol. 11, no. 2, pp. 152–157, Apr. 2002.

[16] E.-H. Yang and G. Wu, "Joint compression and blind watermarking: A case study in the JPEG-compatible scenario," Proc. of the 43th Allerton Conference on Communications, Control, and Computing, September 28-30, 2005.

[17] Wong, P.H.W. and Au, O.C., "A blind watermarking technique in JPEG compressed domain using image normalization," Proceedings of International Conference on Image Processing. Vol. 3, Issue 24-28, pp. 497 – 500, June 2002.

[18] R. Liu and T. Tan, "A new normalization-based image watermarking method," In Proc. of the 4th *Asian Conference on Computer Vision*, volume I, pages 63--67, January 2000.

[19] V. Gorodetski, L.Popyack, V. Samoilov, and V.Skormi, "SVD-based Approach to Transparent Embedding Data into Digital Images," in Proc. *Int. Workshop, MMM-ACNS*, St. Petersburg, Russia, 2001, pp. 263-274.

[20] K.L. Chung, C.H. Shen, L.C. Chang, "A novel SVD- and VQ-based image hiding scheme," *Pattern Recognition Letter*, pp 1051–1058, 2001.

[21] D.V.S. Chandra, "Digital image watermarking using singular value decomposition," in Proc. of 45th *IEEE Midwest Symposium on Circuits and System*, Tulsa, OK, 2002, pp. 264-267.

[22] R. Liu and T. Tan, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership," *IEEE Transactions on Multimedia*, vol. 4, no. 1, pp. 121-128, March 2006.

[23] S. Xiang, Wu, J. Huang, D. Huang, and Y. Q. Shi. Efficiently Self-synchronized audio watermarking for assured audio data transmission. *IEEE Trans. Broadcasting*, 51(1):69–76, March 2005.

[24] B. Ko, R. Nishimura, and Y. Suzuki. Time-spread echo method for digital audio watermarking using PN sequences ICASSP, 2:2001–2004, 2002.

[25] C. C. Chang, C. C. Lin and Y. S. Hu, "An SVD oriented watermark embedding scheme with high qualities for the resorted images," *International Journal of Innovative Computing, Information and Control*, vol.3, no.3, pp.609-620, 2007.

[26] Xiao-Ping Zhang; Kan Li, "Comments on "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership"," *IEEE Transactions on Multimedia*, Volume 7, Issue 3, June 2005 Page(s):593 – 594.

[27] A. Shnayderman, A. Gusev, and A. M. Eskicioglu, "An SVD-based Grayscale Image Quality Measure for Local and Global Assessment," *IEEE Transactions on Image Processing*, vol. 15, no. 2, pp. 422-429, Feb 2006.

[28] A. S. Lewis and G. Knowles, "Image Compression Using the 2-D Wavelet Transform," *IEEE Transactions on Image Processing*, vol. 1, no. 2, pp. 244-250, Apr 1992.

Say Wei Foo, Associate Professor, School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798. E-mail: eswFoo@ntu.edu.sg. Say Wei Foo has served in various capacities in the Institution of Engineers, Singapore (IES) and is the President of IES from 2004-2006. He is also a board member of the Professional Engineers Board (Singapore) and a member of the ASEAN Academy of Engineering and Technology. He is currently an Associate Professor. His research interests include image processing, information hiding and speech signal processing.

Qi Dong, Ph.D. candidate, School of Electrical and Electronic Engineering, Nanyang Technological University, 50 Nanyang Avenue, Singapore 639798. E-mail: DONG0041@ntu.edu.sg. He is currently a Ph.D. candidate. His research interests include information hiding, digital watermarking and signal processing.