A Feature-based Invariant Watermarking Scheme Using Zernike Moments

Say Wei Foo, Qi Dong

Abstract**—**In this paper, a novel feature-based image watermarking scheme is proposed. Zernike moments which have invariance properties are adopted in the scheme. In the proposed scheme, feature points are first extracted from host image and several circular patches centered on these points are generated. The patches are used as carriers of watermark information because they can be regenerated to locate watermark embedding positions even when watermarked images are severely distorted. Zernike transform is then applied to the patches to calculate local Zernike moments. Dither modulation is adopted to quantize the magnitudes of the Zernike moments followed by false alarm analysis. Experimental results show that quality degradation of watermarked image is visually transparent. The proposed scheme is very robust against image processing operations and geometric attacks.

Keywords**—**Image watermarking, Zernike moments, Feature point, Invariance, Robustness.

I. Introduction

WITH the rapid development of worldwide computer networks and digital multimedia technologies, it is relatively easy to make and distribute unauthorized copies of digital files. Copyright protection and multimedia security become very important issues. Digital watermarking is proposed as an effective solution to the problems of copyright protection and data authentication in networked environment [1]-[6]. Digital watermarking is a process of embedding hidden information called watermark into original image, audio or video signals. The embedded watermark is usually coded in binary format and it should not significantly degrade the quality of original host signals.

For image watermarking [3]-[5], the embedded watermarks should be visually transparent. They can be broadly classified into two types, robust and fragile watermarks. Robust watermarks are used for copyright protection and ownership verification [3], [4]. They must be robust against image processing operations as well as geometric attacks. The embedded watermark should be accurately located and extracted from watermarked image when the watermarked image is subject to a variety of possible attacks. High robustness is the key requirement of robust watermarking techniques. Fragile watermarks, on the other hand, are generally used for data and content authentication [5]. They are readily altered or destroyed when watermarked images are tampered. Other than these two extreme types of watermarking, some multipurpose watermarking schemes are proposed to integrate the both robust and fragile watermarking techniques for specific applications [6].

Many robust image watermarking schemes have been proposed in the literature [7]-[21]. These schemes can be grouped into three main categories: schemes in spatial domain, schemes in transformation domain and schemes in compression domain. The main weakness of the schemes which do not take into consideration of geometric attacks is the low robustness against rotation, scaling, and general affine attacks [12], [13]. As a result of geometric attacks, synchronization of embedded watermark is lost. These types of attacks do not introduce visible quality degradation and yet watermark extraction is severely affected.

Zernike moments are introduced to combat geometric attacks by making use of their special invariance properties [9-11]. For the scheme proposed in [9], host image is divided into co-centric rings and a watermark signal is modulated into the Zernike moments of each ring. The watermarked image is achieved by reconstructing the image from the modulated moments of the segmented sub-images. However, the reconstruction procedures are computationally expensive and there is severe fidelity loss during the reconstruction process. A generalized approach using Zernike moments is proposed in [10] to correct geometric distortion. The image is translated and scaled to a standard size before watermark embedding and the watermarked image is inversely transformed to its original form for distribution. At the decoder, the watermarked image is transformed to the same standard image and embedded watermark can be successfully extracted. One problem of this approach is that the positions of embedded watermark cannot be re-located accurately and the watermark extraction rate is low after geometric or de-synchronization attacks. An improvement of the above scheme was proposed by Kim and Lee in [11]. The scheme adaptively modifies normalized Zernike moments vector of the host image. High robustness against different types of attacks can be achieved, but this scheme requires a lot of side information to extract the embedded watermark.

In this paper, a robust image watermarking scheme that combat geometric attacks is proposed. In the proposed scheme, some feature points which are highly invariant against geometric attacks, are extracted from the host images. Several circular patches centered on these points are then generated. These patches are used as stable carriers of watermark information because they can still be regenerated to accurately

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).

locate watermark embedding positions even when watermarked images are severely distorted. Zernike transform is applied to the patches to obtain local Zernike moments. Dither modulation is adopted to quantize the magnitudes of Zernike moments according to watermark bit stream followed by false alarm analysis. The visual quality of the watermarked images so obtained remains perceptually intact. Experimental results show that the proposed watermarking scheme is highly robust against various image processing operations and geometric attacks. For those very damaging combination attacks, the proposed watermarking scheme can still guarantee relatively high robustness compared with other feature-based watermarking schemes.

The rest of this paper is organized as follows. Zernike moments and their invariance properties are described in Section II. In Section III, the proposed watermarking scheme is presented in detail. The performance of the proposed scheme is assessed through various experiments and the results are shown in Section IV. Concluding remarks are given in the last section.

II. Zernike Moments and Invariance Properties

Zernike moments consist of a set of complex polynomials that form a complete orthogonal set over the interior of a unit disk [14], [17]. They are widely used in image processing, pattern recognition, and multi-resolution analysis. Zernike moments are ideal region-based shape descriptors and they have been shown to be invariant against rotation, flipping, scaling and noise addition. In this section, Zernike moments and their invariance properties are explained in detail. Results of experiments to test invariance and stability of Zernike moments are also presented.

A. Zernike Moments

The Zernike moments $Z_{nm}$of order n with repetition m for a continuous function $f(x,y)$ that vanishes outside a unit disk are defined as

$$Z_{nm} = \frac{n+1}{\pi} \iint_{x^2+y^2 \le 1} f(x,y) \cdot V_{nm}^*(x,y) dxdy \qquad (1)$$

where n is a nonnegative integer; m is an integer such that $n-|m|$ is nonnegative and even. The complex-valued function $V_{nm}(x,y)$ is defined as

$$V_{nm}(x,y) = V_{nm}(\rho,\theta) = R_{nm}(\rho) \cdot \exp(jm\theta) \qquad (2)$$

where $\rho = \sqrt{x^2+y^2}$ and $\theta = tan^{-1}(y/x)$. They represent polar coordinates over the unit disk and R_{nm} are Zernike radial polynomials of ρ which is given by

$$R_{nm}(\rho) = \sum_{s=0}^{\frac{n-|m|}{2}} \frac{(-1)^s[(n-s)!]\rho^{n-2s}}{s!\left(\frac{n+|m|}{2}-s\right)!\left(\frac{n-|m|}{2}-s\right)!} \qquad (3)$$

Note that $R_{nm}(\rho) = R_{n,-m}(\rho)$. For a digital image signal, the integrals in (1) are replaced by summations and its Zernike moments are calculated as

$$Z_{nm} = \frac{n+1}{\pi} \sum_x \sum_y f(x,y) \cdot V_{nm}^*(\rho,\theta) \qquad (4)$$

Suppose that if the Zernike moments Z_{nm} of $f(x,y)$ up to a given order N $(N \le n)$ are known, the original signal function can be reconstructed as

$$\hat{f}(x,y) = \sum_{n=0}^{N} \sum_m Z_{nm} \cdot V_{nm}(\rho,\theta) \qquad (5)$$

However, the quality of reconstructed image through this process is significantly degraded due to large cumulative computation errors.

B. Invariance Properties

The reason why Zernike moments are adopted for robust watermarking is that they have some very special and important properties. For example, the magnitudes of Zernike moments are invariant against geometric attacks such as rotation, scaling flipping and affine attacks [10]. The details are reported in [15]-[18].

Other than geometric attacks, the watermark embedded in the magnitudes of Zernike moments must also be robust against image processing operations such as JPEG compression, noise addition and filtering. According to our previous work, we find that all the magnitudes of Zernike moments are very invariant and robust against image processing operations when the order n is below 30. Other than the orders to be used, some Zernike moments are more suitable for robust watermarking than others. This is because the invariance properties of some Zernike moments are compromised due to geometric error of a unit disk clipping, approximation error of Zernike polynomial integration or interpolation error of rotated and scaled images [11].

In summary, the following considerations should be made in the selection of Zernike moments for watermark embedding. First, the moments with order higher than a certain threshold N_{max} cannot be computed accurately and reliably due to cumulative computation errors, and thus they are ruled out. Second, due to the deviation from orthogonality of sampled Zernike polynomials, it can be shown that those moments with repetitions $m = 4i$ $(i \in Z)$ cannot be computed accurately, thus they are not suitable for watermark embedding [10], [17].

Zernike moments are ideal region-based shape descriptors due to their invariance properties against different types of attacks. However, careful selection must be made to achieve the specific objectives.

III. Proposed Invariant Watermarking Scheme

In this section, we describe the proposed watermarking scheme using Zernike's moments and some related issues. First, the methods to identify watermarking regions are discussed. This is followed by details of watermark embedding process and watermark extracting process. Finally, false alarm analysis of proposed scheme is performed.

A. Determination of Watermarking Regions

For robustness as well as preservation of visual quality, it is necessary to identify suitable regions for watermark embedding. These regions are used as carriers of watermark information. They should be readily regenerated to reveal the watermark embedding positions even when watermarked images are severely distorted.

Feature point extraction is an approach in pattern recognition to extract features of the content of digital images [18], [19]. In general, regions around the feature points contain higher energy than other regions of the image; so these regions are more robust against image distortions. Hence feature points can be used to determine the image regions for robust watermark embedding. Harris corner detector [18] is a good method for feature point extraction. Harris corner detector is based on a specific description called second moment matrix [18], which reflects the local distribution of gradient directions in the image. In the proposed scheme, Harris corner detector is employed to extract feature points from host image and the method in [19] proposed by C. W. Tang is adopted to generate circular patches centered on the feature points. This method adaptively calculates radii of circular patches according to local image characteristics around feature points. Hence, the most suitable patches for robust watermarking can be achieved using this method. These patches do not interfere with each other. As an illustration, the extracted feature points and generated circular patches on Lena image are presented in Fig.1.

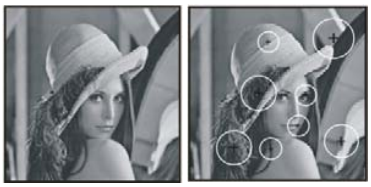

(a) (b)

Fig. 1 (a) Original host image (b) Feature points and circular patches

Several experiments are performed to test invariance and robustness of these circular patches against geometric attacks,. The host image in Fig. 1(a) is rotated through an angle of 10°, 20°, 30° and 40° respectively. The re-extracted feature points and corrresponding ciucular patches on the rotated images are shown in Fig. 2.

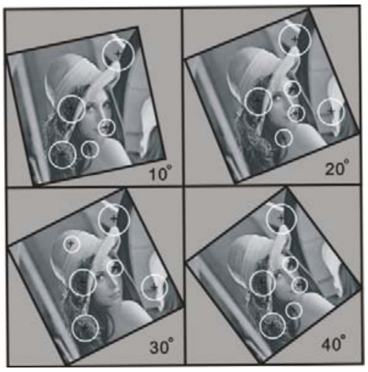


Fig. 2. Invariance of patches under rotation attacks

It can be seen that a majority of feature points can be re-extracted accurately on the rotated images. The locations and radii of the regenerated ciucular patches are indentical to the corresponding patches on the original host image. Hence, the rotation-invariant watermark can be achieved by embedding watermarking information in those cicular patches.

The host image in Fig. 1(a) is scaled or resized to 80%, 90%, 110% and 120% of its original size respectively. The re-extraced feature points and corresponding regenerated circular patches on sacled images are shown in Fig. 3.

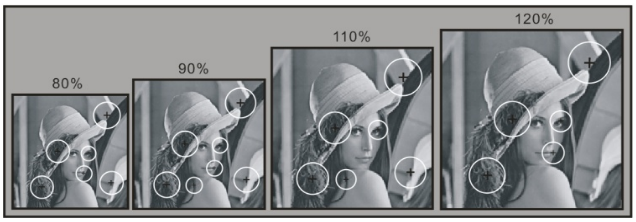


Fig. 3 Invariance of patches under sclaing attacks

It can be seen that more than half of the feature points can be re-extracted accurately on the scaled images. Hence, it is possible to create scale-invariant watermark by embeding watermarks in these circular patches.

Some other general affine attacks are performed on the original Lena image. The re-extracted feature points and corresponding regenerated circular patches on attacked images are shown in Fig. 4.

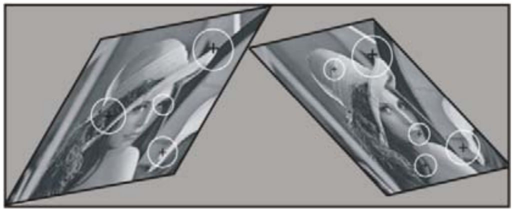


Fig. 4 Invariance of patches under affine attacks

It is observed that even when the image is severly distorted, there are still sufficient numbers of feature points that can be re-extracted accurately. Watermark embedded in the patches centered on these points will be robust against general affine attacks.

From the results of the series of experiments mentioned, it can be concluded that the feature points extracted by Harris corner detector are highly invariant against geometric attacks and circular patches centered on these points are stable carriers of robust watermark. The patches can be acurately regenerated to synchronizae watermark embedding positions even when watermarked images are servely distorted.

B. Watermark Embedding Process

Having identified the image regions for watermark embedding, the watermark is then embedded into these regions using Zernike's moments. To calculate local Zernike moments over a circular image patch $f(x, y)$ with radius r, equation (4) is modified as

$$Z_{nm} = \frac{n+1}{\pi r^2} \sum \sum f(x, y) \cdot V_{nm}^{*}(\rho, \theta) \quad x^2 + y^2 \le 1 \qquad (6)$$

Order n and repetition m are selected as follows. As mentioned in Section 2, it is desirable to choose n to be between 0 and 30, and the moments with repetitions $m = 4i$ $(i \in Z)$ cannot be computed accurately. As $A_{nm}^{*} = A_{n,-m}$, it is only necessary to consider the case when m is larger than 0. For ease of further discussion, let the set of candidate Zernike moments for watermark embedding be denoted by $S=\{Z_{nm}: n\le N_{max}, m>0, m\ne 4i\}$. For the experiments reported in this paper, N_{max} is set to be 30 to maximize watermark embedding capacity.

On the security of watermark protection, we proceed as follows. Two secret keys, labeled as encryption key and position key, are first generated [8]. The encryption key is used to generate a pseudorandom bit sequence. This bit sequence is used to encrypt original ownership information to obtain an encrypted watermark bit stream $W=\{w(i), 1\le i\le L, L\le N_{max}\}$. The position key is used to pseudo-randomly select L Zernike moments from the set S to form a Zernike moment vector $Z=(Z_{n_1m_1}, Z_{n_2m_2}, \ldots\ldots Z_{n_Lm_L})$ which is then used for watermark embedding. The dither modulation [15], 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 $Z'=(Z'_{n_1m_1}, Z'_{n_2m_2}\ldots\ldots Z'_{n_Lm_L})$ is produced. $Z'_{n_im_i}$ is the quantized version of $Z_{n_im_i}$ satisfying

$$\left|Z'_{n_im_i}\right|=\left[\frac{\left|Z_{n_im_i}\right|-d_i(w(i))}{\Delta}\right]\cdot\Delta+d_i\big(w(i)\big), 1\le i\le L \qquad (7)$$

where $[\cdot]$ denotes rounding operation and Δ is the quantization step size; $d_i(\cdot)$ is the dither function for ith quantizer such that $d_i(1)=\frac{\Delta}{2}+d_i(0)$. The key-independent dither variable $d_i(0)$ is uniformly distributed over $(0,\Delta]$ and it is randomly generated by the modulation generator [15,16]. A suitable step size Δ must be determined because a large Δ can increase embedding strength and robustness, but it can also degrade the quality of watermarked image.

The modified Zernike moments are then calculated as

$$Z'_{n_im_i}=\frac{\left|Z'_{n_im_i}\right|}{\left|Z_{n_im_i}\right|}\cdot Z_{n_im_i}, 1\le i\le L \qquad (8)$$

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

Due to cumulative computational errors of Zernike transform and quantization errors in the embedding process, it is difficult to reconstruct watermarked patch without visible quality degradation directly using (5). In the proposed scheme, in order to reduce the quality degradation of watermarked patches, the watermarked patch is reconstructed by adding quantization errors and original patch in the spatial domain. Let $e_{n_im_i}=Z'_{n_im_i}-Z_{n_im_i}$ and $e^*_{n_i,m_i}=Z^{*\,'}_{n_i,m_i}-Z^*_{n_i,m_i}$ denote the quantization errors of $Z_{n_im_i}$ and $Z^*_{n_i,m_i}$ respectively. The quantization errors in the spatial domain are expressed as

$$e(x,y)=\sum_{i=1}^{L}\left[e_{n_im_i}\cdot V_{n_im_i}(\rho,\theta)+e^*_{n_i,m_i}\cdot V^*_{n_im_i}(\rho,\theta)\right] \quad (9)$$

The watermarked patch $f'(x,y)$ can then be obtained by adding original patch and quantization errors in the spatial domain as follows.

$$f'(x,y)=f(x,y)+e(x,y),\ x^2+y^2\le r^2 \qquad (10)$$

The watermark embedding process repeats until all circular patches on original host image are embedded with watermark information. This repeating process improves the robustness and security of proposed scheme. The watermark embedding process is summarized in the form of a flow chart in Fig.5.

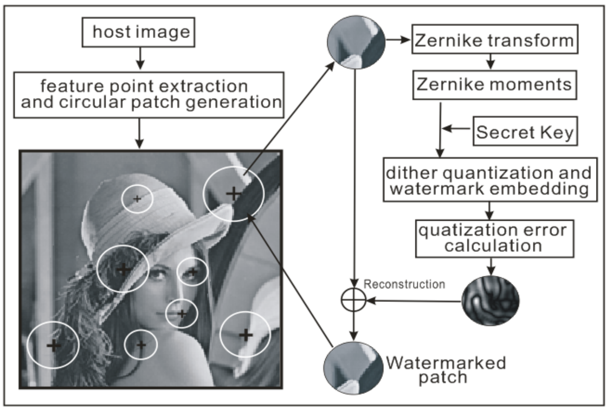

host image
feature point extraction and circular patch generation
Zernike transform
Zernike moments
Secret Key
dither quantization and watermark embedding
quatization error calculation
Reconstruction
Watermarked patch

Fig. 5 Illustration of watermark embedding process

C. Watermark Extracting Process

The watermark extracting method of proposed scheme is a blind method, and the original image is not required for watermark extraction.

Similar to the embedding process, all feature points on the received or attacked image are extracted by Harris corner detector and circular patches centered on these points are then regenerated. Zernike transform is applied to calculate local Zernike moments up to the order of 30 over each regenerated patch. The position key is used to locate and select L moments, forming a set of Zernike moments $\tilde{Z}=(\tilde{Z}_{n_1m_1}, \tilde{Z}_{n_2m_2}, \ldots\ldots \tilde{Z}_{n_Lm_L})$, where watermark bits are probably embedded.

Two dither variables $d_i(0)$ and $d_i(1)$ are then generated. Two quantized versions of each $\left|\tilde{Z}_{n_im_i}\right|$ in $\tilde{Z}$ with respect to the two dither variables are calculated using

$$\left|\tilde{Z}_{n_im_i}\right|_j=\left[\frac{\left|\tilde{Z}_{n_im_i}\right|-d_i(j)}{\Delta}\right]\cdot\Delta+d_i(j),\ \ 1\le i\le L, j=0,1 \qquad (11)$$

By comparing the distances between $\left|\tilde{Z}_{n_im_i}\right|$ and its two quantized versions, the watermark bit embedded in $\left|Z_{n_im_i}\right|$can be extracted by

$$\tilde{w}(i)=\mathrm{argmin}_{j\in\{0,1\}}(\left|\tilde{Z}_{n_im_i}\right|_j-\left|\tilde{Z}_{n_im_i}\right|)^2,\ 1\le i\le L \quad (12)$$

This method is called minimum distance decoder [16].

The sequence of watermark bits so extracted is then de-encrypted using the pseudorandom sequence generated with the encryption key to recover the original ownership information. The flow chart of the watermark extracting process over one circular patch is presented in Fig. 6. This extracting process continues until all regenerated circular patches on the watermarked image are processed and decoded.

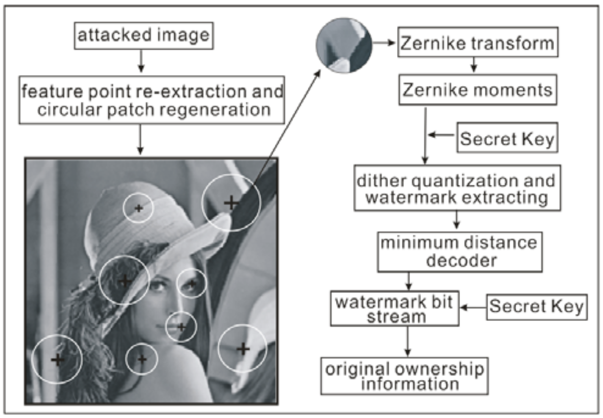

attacked image
feature point re-extraction and circular patch regeneration
Zernike transform
Zernike moments
Secret Key
dither quantization and watermark extracting
minimum distance decoder
watermark bit stream
Secret Key
original ownership information

Fig. 6 Illustration of watermark extracting process

Some patches cannot be regenerated if watermarked image is subject to certain attacks. In addition, some regenerated patches on the attacked image may not contain sufficient watermark information for recovery of ownership information. Thus, a regenerated patch is classified as a watermarked patch if the number of correctly extracted bits from this patch is larger than a given threshold and these correctly extracted bits are sufficient to recover original ownership information.

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 patch, the extracted bits from this patch 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 patch that can match the watermark bits. As explained, a patch is classified as a watermarked patch if r is larger than a given threshold. Let L be the length of watermark bit stream and T be the threshold value ($T \leq L$). Hence, the false alarm probability of a non-watermarked patch is, therefore, the cumulative probability of the cases that $r \geq T$. And it is calculated as

$$P_{patch} = \sum_{r=T}^{L} (0.5)^L \cdot (\frac{L!}{r!(L-r)!}) \tag{13}$$

Furthermore, an image is classified as a watermarked image if at least two patches on it are classified as watermarked patches. Under this criterion, the false alarm probability of a non-watermarked image is:

$$P_{image} = \sum_{i=2}^{N} (P_{patch})^i \cdot (1 - P_{patch})^{N-i} \cdot \binom{N}{i} \tag{14}$$

where N is the total number of patches on the image. If L=25 and N=10, then the relationship between false alarm probability P_{image} and threshold T is plotted in Fig. 7.

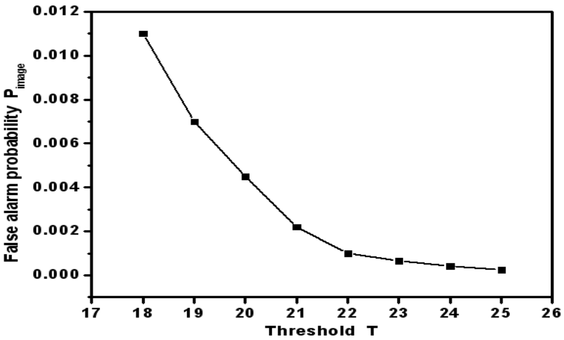


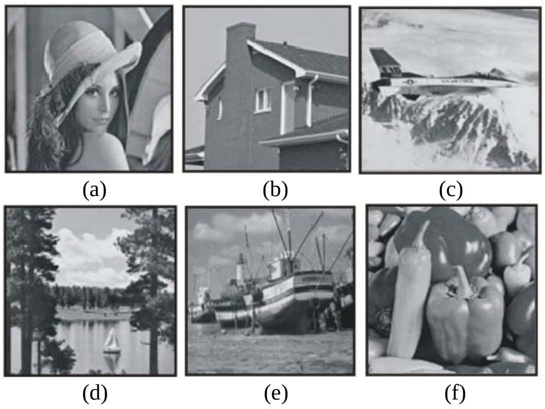
Fig. 7 False alarm probability curve

The curve in Fig. 7 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. Note that the false alarm probability decreases as the value of N decreases for a given threshold value.

IV. Performance of Proposed Scheme

Several experiments are performed to assess the performance of the proposed watermarking scheme.

For the experiments reported in this paper, six 256×256 grey-level images shown in Fig. 8 are used as original host images for the experiments. A 25-bit binary sequence is used as ownership information. The threshold value is set to be 23.


(a) (b) (c)

(d) (e) (f)

Fig. 8 Original host images: (a) Lena, (b) House, (c) Plane, (d) Lake, (e) Boat, and (f) Peppers

A. Assessment of Visual Degradation

A basic requirement for robust image watermarking is visual transparency of the embedded watermark. In other words, the embedded watermark should not significantly degrade the visual quality of the host image. The proposed watermarking scheme with different quantization step sizes is applied to the host images shown in Fig. 8. Peak Signal-to-Noise Ratio (PSNR) is used as objective measure of visual quality of the watermarked images. After calculation, the PSNR values for all watermarked images with different quantization step sizes are tabulated in Table I.

TABLE I
PSNR (DB) VALUES OF DIFFERENT STEP SIZES

PSNR (dB)		Watermarked images					
		Lena	House	Plane	Lake	Boat	Peppers
step size Δ	1	44.2	42.8	43.3	48.6	47.9	47.4
	2	40.9	40.9	40.7	46.5	46.3	46.2
	3	37.7	36.4	38.4	44.5	45.0	43.8
	4	33.3	32.5	34.1	41.1	40.9	41.0
	5	32.6	31.1	33.4	39.7	39.2	38.8

It can be seen that for the same watermarked image, PSNR values decrease as step size increases. For a given step size, the PSNR values for highly-textured images such as “Lake”, “Boat” and “Peppers” are higher than those for images that have simple texture. However, it is found that higher watermark embedding strength can be achieved with larger step size. Hence for robust watermarking, large step-size that does not result in significant degradation in visual quality is chosen. For the experiments conducted, step-size of 3 is used for host images, “Lena”, “House” and “Plane”; and step size of 5 are used for the more highly-textured host images, “Lake”, “Boat” and “Peppers”.

The case of Lena image is illustrated in detail in the following. The watermarked image is shown in Fig .9(a). For ease of displaying, the quantization errors are normalized to the range of [-127,128] and rounded to the nearest integers. They are shown in Fig. 9(b).

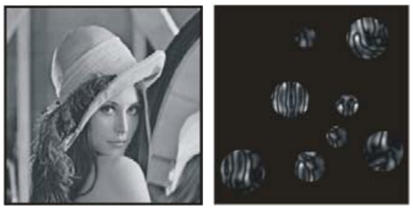

(a) (b)

Fig. 9 (a) Watermarked image (b) Quantization errors

It can be observed that the watermarked image in Fig. 11(a) is visually the same as the original host image in Fig. 10(a), thus quality degradation is not visible. The circular grey regions in Fig. 9(b) indicate quantization errors; the white regions are the regions with the largest errors and the black regions are the regions whose pixel values are not modified. The numbers of occurrence for the values of quantization errors are plotted in the form of a histogram in Fig. 10.

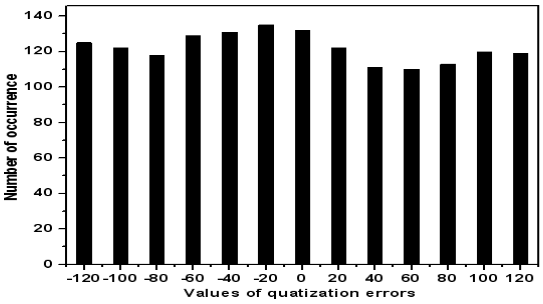


Fig. 10 Histogram of quantization errors

It can be seen that the values of quantization errors are well spread around zero value and the numbers of occurrence are close to uniform distribution. This implies that it is difficult for an attacker to detect the existence of embedded watermark using statistical analysis. Similar experimental results are obtained for other host images.

B. Assessment of Robustness against Attacks

In this part, we assess the robustness of proposed scheme against different types of attacks. The proposed scheme is first applied to the host images in Fig. 8 to generate patches for watermark embedding. The numbers of generated patches on each image are shown in Table II.

TABLE II
NUMBERS OF GENERATED PATCHES ON EACH IMAGE

	Original host images					
	Lena	House	Plane	Lake	Boat	Peppers
Patches	8	7	8	11	9	10

The 25-bit binary sequence is then embedded in the patches using proposed watermarking scheme. The following is a list of attacks and operations used to attack watermarked images.

1) JPEG compression with the following quality factors: (a) 10, (b) 15, (c) 20, (d) 25, (e) 30, and (f) 35.
2) Median filtering with the following 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) Scaling by the following factors: (a) 0.75, (b) 0.8, (c) 0.9, (d) 1.1, (e) 1.2, and (f) 1.5.
5) Rotation by the following angles: (a) 10°, (b) 20°, (c) 30°, (d) 40°, (e) 45°, and (f) -10°.
6) Change of aspect ratio: (a) (0.8, 1.1), (b) (0.9, 1.1), (c) (1.0, 0.8), (d) (1.1, 0.7), (e) (1.2, 0.9), and (f) (0.7, 0.9) where each pair of numbers indicate the amount of scaling in x and y directions, respectively.
7) Combination attacks: (a) JPEG 15+Rotation 10°, (b) JPEG 15+ Scaling 0.8, (c) JPEG 20+ Rotation 20°, (d) JPEG 20+ Scaling 1.1, (e) JPEG 25+ Rotation 30°, and (f) JPEG 25+ Scaling 1.2.

The watermarked images are put through the listed operations. Watermark extracting process is then carried out to extract watermark bits. As mentioned, a regenerated patch on an attacked image is classified as a watermarked patch if the number of correctly extracted bits from this patch is larger than the threshold (T=23). Furthermore, an attacked image is classified as a watermarked image if at least two regenerated patches on it are classified as watermarked patches. The watermarked patches on all attacked images are first determined. The average number of watermarked patches on all six different images subjected to the same type of attack is then calculated. All average numbers of watermarked patches are tabulated in Table III.

TABLE III
AVERAGE NUMBER OF WATERMARKED PATCHES

Attacks	(a)	(b)	(c)	(d)	(e)	(f)
(1)	2.6	2.7	4.0	4.2	4.5	4.8
(2)	5.3	5.3	4.2	3.2	2.3	2.3
(3)	5.5	5.3	5.0	4.6	4.0	3.5
(4)	3.0	3.8	4.9	4.5	4.1	3.2
(5)	4.0	4.2	3.7	3.3	3.9	3.8
(6)	3.9	3.8	4.1	4.1	3.4	4.5
(7)	2.3	2.5	2.7	2.3	2.8	3.1

It can be observed from the data in Table III that when the watermarked images are subject to different types of attacks and operations, the average numbers of watermarked patches on the attacked images are all larger than two for the proposed scheme. For the proposed scheme, the attacked images can still be considered as watermarked images even when subjected to very damaging attacks. That is to say, the proposed watermarking scheme is very robust against common image processing operations and geometric attacks.

Based on the above experimental results, it can be concluded that the proposed watermarking scheme is able to achieve very high robustness without perceptual quality degradation.

V. Conclusion and Future Research

A novel image watermarking scheme, which is very robust against image processing operations and geometric attacks, is described in this paper. In the scheme, the patches centered on feature points are generated to carry watermark information. The watermark bits are then embedded by quantizing the magnitudes of local Zernike moments of the patches. Experimental results show that the embedded patches can be regenerated and watermark bits can be extracted even when the watermarked images are severely distorted.

Future research may focus on increasing robustness against combination attacks and reducing computational load of the proposed watermarking scheme.

References

[1] J. J. Ruanaidh, W. J. Dowling, and F. M. Boland, Watermarking digital images for copyright protection, in *Proc. Inst. Elect. Eng*., (1999), vol. 143, no. 4, pp. 250–256.

[2] M. Barni, I.J. Cox, T. Kalker, Digital watermarking, *Fourth International Workshop on Digital Watermarking*, Siena, Italy, 2005.

[3] M. Swanson, B. Zhu, and A. Tewfik, Transparent Robust Image Watermarking, *Proc. IEEE Int. Conf. on Image Processing*, (1998), vol. III, pp. 211-214.

[4] J.F. Liu, D. Huang, and J.W. Huang, Survey on watermarking against geometric attacks, *J. Electron. Technol*. (2004), 26 (9) 1495–1503.

[5] W. Bender, D. Gruhl, N. Morimoto, Techniques for data hiding, *IBM System Journal 25* (1999) 313–335.

[6] I.J. Cox, L.M. Matthew, A.B. Jeffrey, et al., Digital Watermarking and Steganography, *Morgan Kaufmann Publishers (Elsevier)Burlington*, MA, 2007.

[7] C. Hsu and J. Wu, Hidden signatures in images, in *Proc. IEEE Int. Conf. Image Processing*, (1998), Vol. 3, pp. 223-226.

[8] X.Y. Wang, L.M. Hou, and J. Wu, A Feature-based robust digital image watermarking against geometric attacks, *Image & Computer Vision, ScienceDirect*, (2008), vol. 122, no. 10, pp. 350–356.

[9] Y. Xin, S. Liao, M.A. Pawlak Multibit, Geometrically robust image watermark based on zernike moments, in: P*roceedings of the 17th International Conference on Pattern Recognition (ICPR'2004)*, (2005), pp. 861–864.

[10] Y. Xin, S. Liao, M. Pawlak, A multibit geometrically robust image watermark based on Zernike moments, IEEE Int. Conf. Pattern Recognit., (2004), vol. 4, pp. 861–864.

[11] H.S. Kim, H.K. Lee, Invariant image watermark using Zernike moments, *IEEE Trans. Circuits Syst. Video Technol*. 13 (2003), (8) 766–775.

[12] L. Chang and L. Z. Yang, Desynchronization attacks on digital watermarks and their countermeasures, *J. Image Graphics* 10 (2005) 403–409.

[13] V. Licks, R. Jordan, Geometric attacks on image watermarking system, *IEEE Trans on Multimedia* 1 (2005) 68–78.

[14] A. S. Lewis and G. Knowles, Image Compression Using the 2-D Wavelet Transform, *IEEE Transactions on Image Processing*, (1998), vol. 1, no. 2, pp. 244-250.

[15] B. Mathon, F Cayre and P. Bas, Practical performance analysis of secure modulations for WOA spread-spectrum based image watermarking, *ACM Multimedia and Security Workshop 2007*, Dallas , Texas, USA.

[16] N. Bi, Q. Sun, D. Huang, Z. Yang, J.W. Huang, Robust image watermarking based on multiband wavelets and empirical mode decomposition, *IEEE Transactions on Image Processing*, (2007), Volume 16, Issue 8.

[17] P. Dong, and N. P. Galatsanos, Affine transformation resistant watermarking based on image normalization, *Proc. IEEE Int. Conf. on Image Processing*, (2008), vol. I, Oct, pp. 451-4.

[18] C.H. Lai and J.L. Wu, Robust image watermarking against local geometric attacks using multiscale block matching method, *IEEE Int. Conf. on Image Processing*, (2000), vol. III, pp. 318-322.

[19] P. Bas, J.M. Chassery, and B. Macq, Geometrically invariant watermarking using feature points, *IEEE Trans Image Processing*. 2002, 11(9):1014-28.

[20] B.S. Kim, J.G. Choi and K.H. Park, Image normalization using invariant centroid for RST invariant digital image watermarking, *Lecture Notes in Computer Science*, Springer Berlin, (2003), Volume 2613/2003.

[21] F. Gu, Z.M Lu, J.S. Pan, Multipurpose image watermarking in DCT domain using subsampling, *IEEE International Symposium on Circuits and Systems*, (2005), Vol. 5, Page(s):4417 – 4420.

[22] Z.M. Lu, D.G. Xu, S.H. Sun, Multipurpose image watermarking algorithm based on multistage vector quantization, *IEEE Transactions on Image Processing*, (2005), Volume 14, Issue 6, Page(s):822 – 831.

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

[24] A**.** Watson, G. Yang, J. Solomon, J. Villasenor, Visibility of wavelet quantization noise, *IEEE Transactions on Image Processing*, (1998), vol. 6, no.8, pp. 1164-1175.

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.