Zernike Moments and Edge Features Based Semi-Fragile Watermark for Image Authentication with Tampering Localization

[1] Chia-Wen Kao, [2]Long-Wen Chang
[1,3]Institute of Information Systems and Applications
[2,3]Department of Computer Science
National Tsing Hua University
Hsinchu, Taiwan
[1]g946325@oz.nthu.edu.tw, [2]lchang@cs.nthu.edu.tw

***Abstract*—This paper present a novel content-based image authentication framework which embeds the semi-fragile image feature into the host image based on wavelet transform. In this framework, two features of a target image from the low frequency domain to generate two watermarks: Zernike moments for classifying of the intentional content modification and Sobel edge features for indicating the modified location. In particular, we design a systematic method for automatic order selection of Zernike moments and in order to tell if the processing on the image is malicious or not. We also propose a weighted Euclidean distance by a reconstruction process. An important advantage of our approach is that it can tolerate compression and noise to a certain extent while rejecting common attack of the image like rotation. Experimental results show that the framework can locate the malicious tampering for the resolution of a 8x8 block. Also, it is robust to content preserved processing, such as JPEG compression Q≧30 and Gaussian noise variance ≦20.**

1. INTRODUCTION

With the rapid progress of multimedia technologies, any people can perfectly modify digital image using widely available editing software. The authentication of digital image content is necessary in real world. However, the authentication of images and multimedia content in general differs from the traditional problems of authentication in cryptography. Digital watermarking is an approach by adding a signal to a digital content to ensure the authenticity. It has become a very active research field and been widely accepted as a promising technique for multimedia security.

According to embedding purposes, watermarks can have two types: robust and fragile watermarks. Robust watermarks are designed to withstand arbitrarily malicious attacks, such as image scaling bending, cropping, and lossy compression. They are usually used for copyright protection to declare the rightful ownership. On the contrary, for the purpose of image authentication, fragile watermarks are adopted and designed to detect any unauthorized modification. However, in most multimedia applications, minor data modifications are acceptable as long as the content is authentic. The semi-fragile watermark is developed and used in content authentication. Semi-fragile watermarking has the characteristics of both robust and fragile watermarking. It can tolerate some normal signal processing such as JPEG compression, filtering etc, at the same time it can inspect whether original image is tampered and decide the tampered area.

A typical approach of semi-fragile watermarking based authentication of an image can be stated as below:
Step 1: The image feature is extracted from the original image.
Step 2: Quantized the image feature.
Step 3: The quantized feature is embedded as a message into the image.
During authenticity verification, the message is detected using the watermarking detector, and the image feature is extracted from the watermarked image. A typical authenticity verification is based on the comparison between a preset threshold and the distance of the extracted features and the detected watermark.

There are many existing private schemes for semi-fragile watermarking. Some of the previous techniques [1] [2] focused on detecting whether an image was tampered with or not. However, they did not clearly specify how and where the image was changed. Zhou et.al in [3] propose a semi-fragile watermark scheme which extracts a signature from the original image and inserts this signature into the discrete wavelet transform coefficients. However, the signature itself is not robust to the normal image processing. The false alarm rate is high and the robustness to JPEG is Q=60. [4] based on an important property of JPEG compression and present a semi-fragile watermarking scheme which tolerates JPEG compression to a pre-determined lowest quality factor, and rejects all other malicious manipulations, either in spatial domain or in transform domain. However, it needs to pre-determine quality factor and to extend applicability of the proposed scheme to JPEG2000 standard. Kang and Park in [5] propose a semi-fragile watermarking algorithm using JND (just Noticeable Differences). It improved the performance of Delp's method [6], which is a representative semi-fragile watermarking. The algorithm can tell only the attack is malicious or non-malicious, but it cannot tell the position of the malicious processing.

In this paper, we propose a content-based semi-fragile watermarking algorithm in DWT domain. It generates two watermarks by extracting the image features from the low frequency domain: Zernike moments and Sobel edge for determining the intentional content modification and indicating the modified location.

2. Related Works

The success of the semi-fragile watermark system is closely related to how to extract the adequate image features. In this way, the most important issue in the semi-fragile watermark is the selection of appropriate embedded features that are invariant to all kinds of common image processing. There are different features such as (1) image moments features (2) image edge features, and (3) transform domain features can be used to identify the image content. They all have different advantages and limitations. In this paper we choose the moment invariants methods based on Zernike transform to generate the primary image features and at the same time extract the Sobel edge features as our secondary image features to achieve localization capability.

Zernike [8] first introduced a set of complex polynomials $\{V_{nm}\}$ which form a complete orthogonal set over the unit disk of $x^2 + y^2 \le 1$ in polar coordinates. The form of the polynomials is defined as:

$$V_{nm}(x, y) = V_{nm}(\rho, \theta) = R_{nm}(\rho) e^{im\theta}$$

where n is positive integer or zero; m is integers subject to constraints $n - |m|$ is even, and $|m| \le n$; ρ is the length of the vector from the origin to the pixel (x, y); θ is the angle between the vector ρ and x axis in counterclockwise direction; $R_{nm}(\rho)$ is Radial polynomial defined as:

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

The Zernike moment of order n with repetition m for function $p(x, y)$ is defined as:

$$A_{nm} = \frac{n+1}{\pi} \iint_{x^2+y^2 \le 1} p(x, y) V_{nm}^*(x, y) dxdy ,$$

where $V_{nm}^*(x, y) = V_{n,-m}(x, y)$

To compute the Zernike moment of a digital image, we just need to change the integrals with summations:

$$A_{nm} = \frac{n+1}{\pi} \sum_x \sum_y p(x, y) V_{nm}^*(x, y), x^2 + y^2 \le 1$$

Suppose we know all Zernike moments A_{nm} of $p(x, y)$ up to order N , we can reconstruct the image by:

$$p'(x, y) = \sum_{n=0}^{N} \sum_m A_{nm} V_{nm}(x, y)$$

Zernike moments are less sensitive to noise and invariant to linear transformations. They can be effectively used for image reconstruction.

3. THE PROPOSED METHOD

3.1 Feature extraction

Feature extraction is the most important step in the proposed watermarking scheme. In order to detect watermarks without access to the original image, we look for feature points that are perceptually significant and can thus resist various types of common signal processing and geometric distortions. We know the orthogonal moments based on Zernike polynomials can extract a set of features in which every feature can represent unique information about an image. In terms of feature representation and sensitivity to noise, Zernike moments have better performance compared to the other moments. In addition, these moment functions are defined in polar coordinates. Even though they are not invariant with respect to scale and translation, these properties can be achieved using the methods proposed by Khotanzad [9] or Chong [10]. Zernike moment has been used as shape descriptor in trademark and logo retrieval systems due to its many desirable properties, such as robustness to noise or small variance, and invariant characteristics. The image features are in complex form and are represented by their phase and magnitude.

In this paper, Zernike moment magnitudes (ZMMs) [11] are used as a feature set, we firstly apply 3-level DWT to the $M \times N$ host image, get 10 subbands, LL_3, HL_3, LH_3, HH_3, HL_2, LH_2, HH_2, HL_1, LH_1, HH_1. The low frequency subband, LL_3 subband is a lowpass approximation of the original image, we select this subband to compute the ZMMs. Additionally, we also adopt a Sobel edge detection on the LL_3 component to get $\frac{1}{8}M \times \frac{1}{8}N$ binary Sobel edge map W_E, it has good performance in differentiating malicious attack from non-malicious attack and locating the malicious attacked area correctly. We can use W_E to help us know which part of the image is maliciously attacked. Consequently, ZMMs and W_E are used as the embedded watermark .

3.2 Number of features selection & Weighting Mechanism

We know how to use Zernike moments to reconstruct the original image. The difference between an image and its reconstructed version from a finite set of its moments is a good measure of the image representation ability of the considered set of moments. The ease of image reconstruction from Zernike moments makes it practical to base the feature selection process on such a measure. The idea is that *n*, the maximum order, is one which can generate a reconstructed image which is similar to the original in the sense of a defined threshold.

Let $\overline{I}_j$ denote the image reconstructed by using Zernike moments of order 0 through *j* extracted from the original image I , and the Euclidean distance between the two

images $E(\overline{I}_j, I)$ is employed to quantify this difference, that is a simple measure of image representation ability between $\overline{I}_j$ and the original image I . If $E(\overline{I}_j, I)$ is small enough, then it can be concluded that enough information is extracted and no additional order of moments needs to be computed, i.e., order=*j*. Here we can use a threshold α to facilitate our judgment. Obviously, the smaller the α is, the higher the needed order is. Based on different applications, by presetting the α, the proposed scheme can embed ZMMs of various orders. When a high level of robustness is specified, we should need a smaller α that it will embed more watermark bits. Meanwhile, it also may affect the quality of watermarked image degrade. In other words, with a larger α, fewer watermark bits will be embedded and a higher fidelity of the watermarked image will be achieved. However, this will decrease the performance of semi-fragile feature, because of less image information embedded.

The above procedure not only decides the highest order needed, but also provides a way to treat features each order differently. Furthermore, we hope to understand how important the ZMMs of different orders are on our semi-fragile watermark scheme. We can get the important degree of ZMMs by calculating its contribution and use it to weight the corresponding features. The contribution of *j*th order moments to the reconstruction process can be measured by computing how much closer $\overline{I}_j$ is to original I compared to $\overline{I}_{j-1}$ .The contribution of the *j*th order moments denoted by $D(j)$, is computed as

$$D(j) = E(\overline{I}_{j-1}, I) - E(\overline{I}_j, I).$$

A large positive value of $D(j)$ indicates that the *j*th order moments do capture a lot of important information about the shape. On the other hand, a small positive or a negative $D(j)$ is an indication that the corresponding moments focus on unimportant aspects of the image under study. Consequently, it distinctly weight the important degree of ZMMs of various orders. Thus, we can introduce a weighting mechanism based on their corresponding $D(j)'s$, Euclidean distance is again employed to carry out this task. That is, after the related order ZMMs have been extracted, we will multiply different weights to these order ZMMs to compute a weight Euclidean distance during authentication stage. Finally, we obtain the distance as a judge factor to determine whether the image was suffered by malicious attack. The weight of order j is defined as:

$$w_j = \frac{D(j) - D(\min)}{D(\max) - D(\min)}, \quad j = 1, 2, ..., order$$

$D(\max)$: The maximal $D(j)$

$D(\min)$: The minimal $D(j)$

The formula scale the w_j into range of [0, 1] first, and utilize the value as order weight to compute the weighted Euclidean distance. Note that if $D(j)$ is negative, w_j is not set to zero, and the weight of the zeroth order and first order moments are set to 0.5 since there is no previous image for comparison. These above processes will enhance the precision of the formula because it doesn't omit any available information. We get the weighted Euclidean distance shown below:

$$E_w(I, \overline{I_{order}}) = \sqrt{\sum_{m=0}^{order} w_m (ZMM_{m,n} - \overline{ZMM_{m,n}})^2}$$

Table 1 shows some statistics including corresponding $E(\hat{I}_j, I)$, $D(j)$, and w_j for reconstructed images in Fig.1 when threshold α=21000, as aforementioned we know we can adjust α flexibly by a variety of different applications, here we can see the order is 11. Table 2 lists the numbers of ZMMs from order 0 to order 11. Therefore, in this case, we have to compute 42 ZMMs (normalized to [0, 1]) to get the features of host image. From W_j value we can get the weighted Euclidean distance, the distance of modulated image will be a judge factor to decide whether this image is suffered from malicious tampering or not.

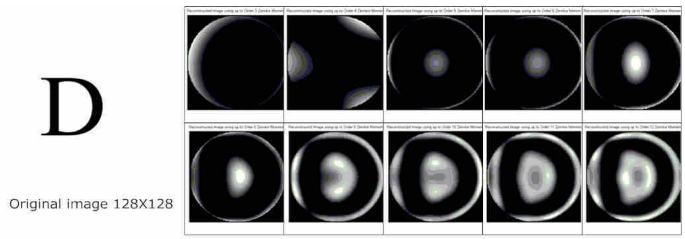

Fig.1. The reconstructed image of letter D. From top left to right, reconstructed image with up to third order moment through to twelfth order moment.

Table1. Euclidean distance and its corresponding weight for reconstructed images shown in Fig.1.

Order	Euclidean distance	D(order)	Weight
1	25952	N/A	0.5
2	27041	-1089	0
3	26881	160	0.3080
4	27342	-461	0.1549
5	27129	213	0.3211
6	25766	1363	0.6047
7	25714	52	0.2814
8	22748	2966	1
9	22442	306	0.3440
10	21792	650	0.4289
11	20959	833	0.4740

Table 2. List of zernike moments and their corresponding number of features from order zero to order eleven.

Order	Zernike Moments	Numbers Of Zernike Moments
0	$Z_{0,0}$	1
1	$Z_{1,1}$	1
2	$Z_{2,0}$,$Z_{2,2}$	2
3	$Z_{3,1}$,$Z_{3,3}$	2
4	$Z_{4,0}$,$Z_{4,2}$,$Z_{4,4}$	3
5	$Z_{5,1}$,$Z_{5,3}$,$Z_{5,5}$	3
6	$Z_{6,0}$,$Z_{6,2}$,$Z_{6,4}$,$Z_{6,6}$	4
7	$Z_{7,1}$,$Z_{7,3}$,$Z_{7,5}$,$Z_{7,7}$	4
8	$Z_{8,0}$,$Z_{8,2}$,$Z_{8,4}$,$Z_{8,6}$,$Z_{8,8}$	5
9	$Z_{9,1}$,$Z_{9,3}$,$Z_{9,5}$,$Z_{9,7}$,$Z_{9,9}$	5
10	$Z_{10,0}$,$Z_{10,2}$,$Z_{10,4}$,$Z_{10,6}$,$Z_{10,8}$,$Z_{10,10}$	6
11	$Z_{11,1}$,$Z_{11,3}$,$Z_{11,5}$,$Z_{11,7}$,$Z_{11,9}$,$Z_{11,11}$	6

3.3 Feature quantization

Up to now, the discussion has centered on how to select the right order of Zernike moments and its corresponding feature weights. Besides, feature vectors usually exist in a very high dimensional space. Due to this high dimensionality, it has enabled us to use so many bits to embed these feature vectors as our watermark. Moreover, these bits will be extracted to calculate the distance from the feature vectors of the watermarked image, therefore we need to retain only finite meaningful bits. In other words, when ZMMs are embedded as watermark, they need to be quantized.

In our feature quantization work, we first normalized ZMMs to a real number less than 1, and quantized to 16 bits. Table 3 shows the semi-fragile characteristics of the ZMMs of LL3 subband, where Q of JPEG compression represents compression quality factor and the variance of Gaussian noise denotes different strength of additive noise attack. In additional, for simplicity, the difference of ZMMs of LL3 subband between the original image and the manipulated image is defined by the square of Euclidean distance.

In the JPEG compression, because the image feature is extracted from low-frequency, the robustness is required. However, even though the damage which JPEG attacked is slight, but we can see that the distances of ZMMs between letter D and Lena caused by JPEG compression are quite different, and we conjecture that Lena contains much significant texture and than it has considerably higher quality than simple logo figure such as letter D during JPEG compression. In other words, the resistance against JPEG compression closely related to the frequency distribution of this image. Therefore, we will observe this part of noise attack, and learn from the noise attack caused by the destruction and image itself is not particularly relevant. More importantly, the distances of Gaussian Noise attack (variance above 30) are much higher than the other compression and noise attacks without respect to Lena or letter D. We will be able to make use of the distortion Gaussian noise attack caused (variance above 30) to be the threshold to help us judge whether this image of malicious tampering. That is to say, we can use this difference to classify the manipulations as non-malicious or malicious.

Table 3. The semi-fragile characteristics of ZMMs of LL3 subband.

Manipulation	The squre of Euclidean distance of Fig2.(Letter D)	The squre of Euclidean distance of Lena(256x256)
JPEG (Q=80)	4.1481e-005	6.1729e-007
JPEG (Q=70)	8.1645e-005	1.5031e-006
JPEG (Q=60)	9.3117e-005	2.0328e-006
JPEG (Q=50)	1.3043e-004	3.3964e-006
JPEG (Q=40)	1.6868e-004	5.1404e-006
JPEG (Q=30)	2.1014e-004	1.2615e-005
Slight Gaussian Noise (variance=3)	4.2322e-006	2.2279e-006
Medium Gaussian Noise (variance=10)	6.6616e-005	2.0133-005
Heavy Gaussian Noise (variance=30)	5.5952-004	2.2818e-004

In our experiments and analysis, the goal is to find the minimum of the most significant bits of each moment that are enough to make correct decision. Our experiments show that difference to classify the manipulations as non-malicious or malicious usually is about 10^{-4}. That is to say, we can use the value to decide which bits are discard.

Table 4. The contributions of different bits of ZMMs (normalized to 0~1, and quantized to 16 bits.).

Bit	1	2	3	4	5	6	7	8
Significant	2^{-1}	2^{-2}	2^{-3}	2^{-4}	2^{-5}	2^{-6}	2^{-7}	2^{-8}
Squre of Significant	2^{-2}	2^{-4}	2^{-6}	2^{-8}	2^{-10}	2^{-12}	2^{-14}	2^{-16}
Bit	9	10	11	12	13	14	15	16
Significant	2^{-9}	2^{-10}	2^{-11}	2^{-12}	2^{-13}	2^{-14}	2^{-15}	2^{-16}
Squre of Significant	2^{-18}	2^{-20}	2^{-22}	2^{-24}	2^{-26}	2^{-28}	2^{-30}	2^{-32}

From Table 4 we got the contributions of different bits of ZMMs, and we found that when the bit is 9, the contributions are $2^{-18} \times 42 = 0.00016$. However, the contributions of the 10 bits are $2^{-20} \times 42 = 0.00004 < 10^{-4}$. In conclusion, before embedding ZMMs as watermark, we first quantize the ZMMs to most significant 10 bits. The feature quantization process will not change the performance of our scheme instead of increasing its watermark payload. It will improve the robustness and the quality of the watermarked image.

3.4 Watermark embedding

In order to protect the original image, our watermark extraction process is designed in a blind-detection manner. Blind detection means the original image is not required for

watermark extraction. Among the existing blind watermarking schemes, the quantization-based watermarking approach is the simplest one that achieves the goal.

As proposed in [12], the authors embedded a binary watermark in the wavelet transform domain. In this method, the insertion was done by the even or odd quantization of selected wavelet coefficients. In other words, a watermark value is encoded by modulating a selected wavelet coefficient into a quantized interval. The advantages of this approach are clear and significant, from the observation that subtle modifications in the wavelet domains do not change the image significantly, while minor changes in the image alter the coefficients locally, but noticeably. This characteristic is a good premise for watermark invisibility and fragility. Moreover, quantization-based watermarking is the simplest protocol because it requires the least storage of information. Embedding the watermarks ZMMs and W_E in the middle frequency components of wavelet decomposition HL_2, LH_2 contributes to both appropriated invisibility and robustness synchronously.

The quantization-based watermarking approach divides a real number axis in the wavelet domain into intervals with equal size at each scale and assigns watermark symbols to each interval periodically. As shown in Assume that x is a wavelet coefficient, and Q is the size of a quantization interval, the watermark symbol, which is either 0 or 1, is determined by a quantization function Quan(x, Q), where

$$Quan(x,Q) = \begin{cases} 0 & if \quad tQ \le x < (t+1)Q \quad for \ t = 0, \pm 2, \pm 4, \ldots \\ 1 & if \quad tQ \le x < (t+1)Q \quad for \ t = \pm 1, \pm 3, \pm 5, \ldots \end{cases}$$

Let w denote the target watermark value that is to be encoded for a wavelet coefficient x. The watermark bit w is embedded by modifying the wavelet coefficient x so that Quan(x, Q) is equal to w. The coefficient is modified to the nearest 0 bin (the double arrowhead) or 1 bin (the single arrowhead) according to w, and the bins of 1 and 0 locate in the middle of the quantization step Q. Specifically, the wavelet coefficient x is updated to x^* by

$$x^* = \begin{cases} \left\lfloor \frac{(x + \frac{Q}{2})}{Q} \right\rfloor \cdot Q + \frac{Q}{2} & if \quad Quan\ (x + \frac{Q}{2}) = w \\ \left\lfloor \frac{(x + \frac{Q}{2})}{Q} \right\rfloor \cdot Q - \frac{Q}{2} & if \quad Quan\ (x + \frac{Q}{2}) \neq w \end{cases}$$

where $\lfloor \cdot \rfloor$ is the floor operator and x^* is the expected updated wavelet coefficient. When all watermark bits of ZMMs and W_E are separately embedded into HL_2, LH_2 subbands by quantization-based method, IDWT using updated wavelet coefficients is employed to produce the watermarked image. Fig.2 shows an overview of our watermarking process.

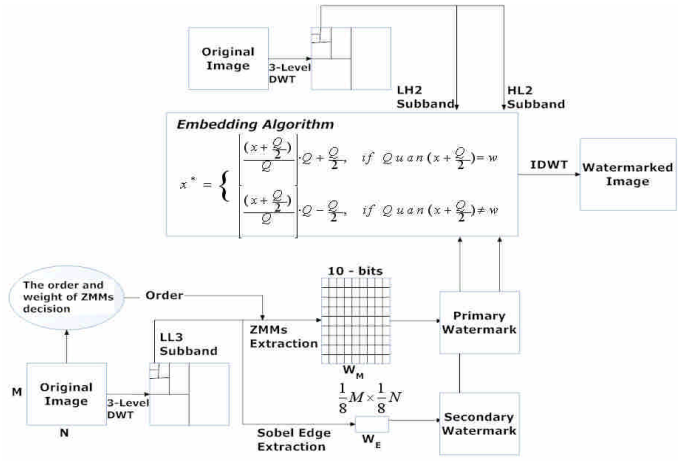

Fig.2. Overview of the watermark embedding process

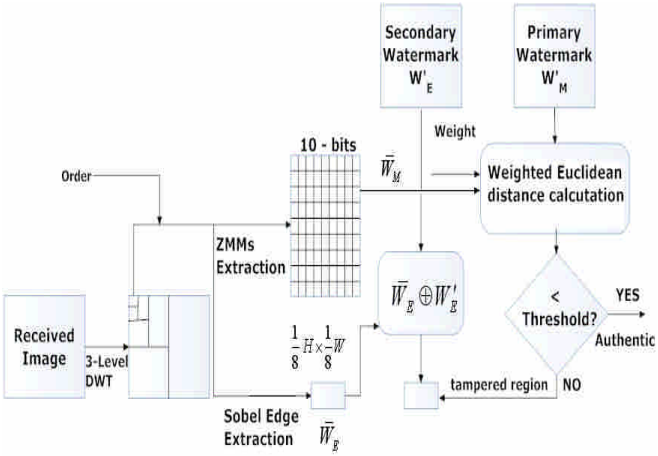

Fig.3. Overview of the authentication process.

3.5 Watermark retrieval

The framework of the watermark retrieval process is almost the same as that of the watermark embedding process, except that the order and weight of ZMMs decision is discarded. The selected order and corresponding weight of Zernike moments, threshold, and the quantization step Q are conveyed to the watermark detector as side information. First, take a three-level wavelet decomposition on $M \times N$ watermarked image I'. Next, the coefficients in the two subbands HL, LH of the 2th level are ready to be extracted as ZMMs watermark and Sobel edge watermark. The quantization process of all the wavelet coefficients in HL_2 and LH_2 is recalculated and the watermark bit is extracted by $w' = Quan(x^*, Q)$.

3.6 Authenticity verification & Localization capability

To authenticate the received image, the extracted watermarks W_M' and W_E' are compared with the generated image features $\overline{W}_M$ and $\overline{W}_E$, respectively. If all the extracted image features match the original ones, the image is claimed

authentic; otherwise, it may be tampered. An authentication decision is made after the weighted Euclidean distance comparison by moment feature with a received threshold, and the purpose of the edge feature comparison is help us localize the tampered areas. In order to achieve the capability of localizing tampered regions, many existing watermarking schemes embed the watermark in a block-based way. The image is divided into blocks and the watermark information is embedded into every block. The block content authentication is done by verifying whether the watermark can be successfully extracted from the block. In our block-based methods, the content of the image is monitored by the edge features embedded in the wavelet domain. Thanks to the spatial-frequency localization of the wavelet transform, every position is verified by the edge watermark bit embedded in the corresponding wavelet coefficient. Therefore, we will achieve the capability of localizing tampered regions. The authentication matrix D_E is defined to estimate the difference between W_E' and $\overline{W}_E$ by $D_E = W_E' \oplus \overline{W}_E$. Based on the fact that the tampering commonly occurs in a continuous area of the image in the practical applications, only the region with the high density of the unverified coefficients should be the actual manipulation. In consequence, we define those isolated unverified coefficients as noise dots. Other continuous unverified coefficients, which are mapped back to adjacent positions, are identified as the actually tampered ones. An illustration of the authentication process is given in Figure 3.

4. EXPERIMENTAL RESULTS

In the final section, the power of the proposed semi-fragile watermarking scheme is experimentally tested and the results are reported. Furthermore, the performance of the method is compared to the other popular algorithms.

4.1 The order and weight of ZMMs decision

The proposed scheme is tested with a variety of images, but here we only give the results of using the gray image Lena and Baboon (256×256) for example. We choose the judge factor for image authentication is 2, and quantization step Q=6 in the watermark embedding. First, Table 5 and Table 6 show the D(i) and its corresponding weights for Lena and Baboon. Again note that the weights of zeroth order and first order moments are set to 0.5 since there is no previous order. The information can help us embed watermark and it will be transmitted to the receiver.

4.2 Quality of watermarked image

In the proposed authentication scheme, the image distortion is caused by the wavelet coefficients modification in the watermark embedding process. The quality metric is based on PSNR (Peak Signal to Noise Ratio). The PSNR of the watermarked image with different Q is plotted in Figure 4. Obviously, the quantization step Q used in watermark embedding will affect how much the quality of the watermarked image degrades. A larger quantization step will incur more modification to the wavelet coefficients, consequently resulting in more degradation of the watermarked image. However, it better ensure the correctness of watermark. The original and watermarked images are shown in Fig.5. Fig.5 (a) is the original images, the rest are the watermarked images with quantization step Q =6, 8, 12. We can see that the quality degradation is acceptable.

4.3 The robustness performance of the semi-fragile watermark

Next, we will test the authentication for incidental distortion and content modification. The embedded ZMMs watermark was extracted from a watermarked image, and the weighted Euclidean distance were used to assure the authentication of the received image. In the part of incidental distortion, we consider using JPEG compression and Gaussian noise as the possible distortion during image processing or network transmission, additionally we hope the scheme can be robust to rotation. In the content modification, four sets of tests in Fig.6 were performed to assess the algorithm. Fig.6 (a) is to remove the mirror image of the watermarked image, Fig.6 (b) adds a flower on her hat in Fig.6 (a), Fig.6 (c) and Fig.6 (d) adds a tag on upper left and lower left corner.

Finally, the experimental results are shown in Table 7. It shows the common processing image after JPEG compression with a quality factor of 80 to 30, Gaussian noise with variance of 3, 10, 30 and rotation image. The decision threshold was set at 2. It can be seen that the proposed watermarking algorithm is robust to common image processing. In other words, JPEG30-100, medium noise and rotation attack can be classified correctly as non-malicious processions, and the other images that suffered content modification are interpreted as a malicious attack. Fig.7 shows the location of different content modification in the original image and the authentication results show that localization capability can be clearly achieved by our system.

4.4 Comparison

The proposed watermarking algorithm is compared with two other semi-fragile watermarking with tampering localization capability:

Algorithm 1: Image Authentication Using Content Based Watermark [11]

Algorithm 2: Using two semi-fragile watermark for image authentication [12]

The comparative results are list in Table 8. First, we observe the experimental results of algorithm1. Because the embedded image feature is also Zernike moment that it makes the scheme can resist against rotation. However, the algorithm only embed the most significant 4 bits of each moment as watermark, and it will increase in the quality of the images but decrease the robustness of JPEG compression and Gaussian noise. Algorithm2 embedded edge feature and its hash version, even though it has a good semi-fragile capability, but it still need to make the watermark robust to rotation. Also, the scheme embedded a few more watermark bits that it degraded the quality of watermarked image.

It is obvious that the proposed watermarking algorithm has better robustness performance of the semi-fragile watermark,

and from PSNR values we know the watermark is almost imperceptible. Besides, the unit of the detection is 8x8 compared with the algorithm 1 whose unit of detection 16x16 block. Our system can locate the malicious processing more accurately .

5. CONCLUSION

We propose a content based watermarking scheme to detect and localize tampered regions in images. It significantly improves the robustness performance of the semi-fragile watermarking that accepts JPEG compression, additive noise and rotation attack on the watermarked image, while rejects malicious manipulations such as adding and removing objects in the watermarked image. Especially, the use of two watermarks based on image content can locate the malicious tamper locally and provides very good classification of malicious and incidental tampering. Experimental results show that this scheme has superior performance over the existing authentication scheme, offer better classification of intentional content modification and higher detection resolution. Therefore, the proposed semi-fragile watermarking algorithm is practicable for image authentication.

6. References

[1] G. L. Friedman, "The trustworthy digital camera: restoring credibility to the photographic image," IEEE Trans. on Consumer Electronics, Vol.39, pp.905-910, 1993.

[2] M. M. Yeung and F. Mintzer, "An invisible watermarking technique for image verification," Proc. of IEEE Conf. Image Processing, Vol.2, pp.680-683, 1997.

[3] X. Zhou, X. Duan and D. Wang, "A semi-fragile watermark scheme for image authentication," Proc. of the 10th International Multimedia Modeling Conference, 2004.

[4] C. K. Ho and C. T. Li, "Semi-Fragile Watermarking Scheme for Authentication of JPEG Images," Proc. of ITCC, 2004.

[5] H. H. Kang and J. H. Park, "A semi-fragile watermarking using JND," Proc. of STEG, pp.127-131, July. 2003.

[6] E. T. Lin, C. I. Podilchuk and E. J. Delp, "Detection of image alteration using semi-fragile watermarks," Proc. of SPIE Int. Conf. Security and Watermarking of Multimedia Contents 2, Vol. 3971, Jan. 2000.

[7] M. Hu, "Visual Pattern Recognition by Moment Invariants," IRE Transaction on Information Theory, Vol. IT-8, pp.179-187, Feb.1962.

[8] F. Zernike, Physica, Vol.1, pp.689, 1934.

[9] A. Khotanzad, "Invariant Image Recognition by Zernike Moments," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 12, No.5, May. 1990.

[10] C. W. Chong, P. Raveendran and R. Mukundan, "Translation Invariants Of Zernike Moments," Pattern Recognition, Vol. 36, pp.1765-1773, 2003.

[11] H. Liu, J. Lin and J. Huang, "Image Authentication Using Content Based Watermark," IEEE International Symposium on Circuits and Systems, Vol. 4, pp.4014-4017, May. 2005.

[12] Y. P. HU and D. Z. HAN, "Using two semi-fragile watermark for image authentication," Proc. of Machine Learning and Cybernetics International Conference, 2005.

Table5. Order information and its corresponding weights for Lena256x256.

Order	Euclidean distance	D(order)	Weight
1	3528.1	N/A	0.5
2	3338.4	189.7	0.7645
3	3344.5	-6.1	0.5018
4	3176.3	168.2	0.7356
5	3068.9	107.4	0.6541
6	2870.2	198.7	0.7765
7	2782.2	88	0.6280
8	3162.4	-380.2	0
9	3101.4	61	0.5918
10	2736.1	365.3	1

Table 6. Order information and its corresponding weights for Baboon 256x256.

Order	Euclidean distance	D(order)	Weight
1	3682.8	N/A	0.5
2	3371	311.8	0.6759
3	3156.6	214.4	0.5791
4	3525.2	-368.4	0
5	3614.3	-89.1	0.2775
6	3861.9	-247.6	0.12
7	3816.7	45.2	0.4110
8	3178.7	638	1
9	3101.4	77.3	0.4429

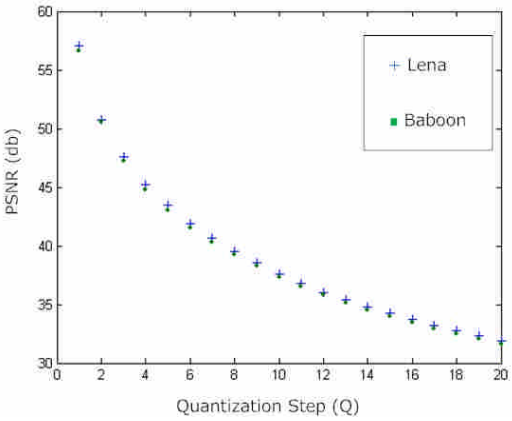

Fig.4. Image quality with different quantization step.

Fig. 5. Demonstration of the invisibility for Lena. PSNRs of (b), (c) and (d) are 41.92, 39.55 and 36.05 respectively.

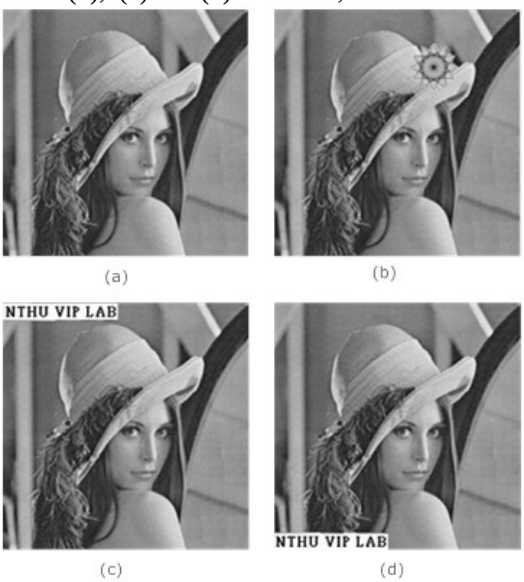

Fig.6. The malicious attack (a)~(d) for Lena.

Table 7 . Robustness to non-malicious processing.

Manipulation	Lena	Baboon
JPEG (Q=80)	0.54109	0.55164
JPEG (Q=70)	0.58429	0.70715
JPEG (Q=60)	0.76045	0.70752
JPEG (Q=50)	0.81664	1.0762
JPEG (Q=40)	1.3569	1.2745
JPEG (Q=30)	1.8848	1.6166
Gaussian Noise (variance=3)	0.58426	0.70716
Gaussian Noise (variance=10)	1.3539	1.3801
Gaussian Noise (variance=30)	2.2238	2.6452
Rotation	1.1282	1.3025
Malicious Attack (a)	2.3039	2.1105
Malicious Attack (b)	2.5938	2.3214
Malicious Attack (c)	2.6104	2.5541
Malicious Attack (d)	2.7111	2.3864

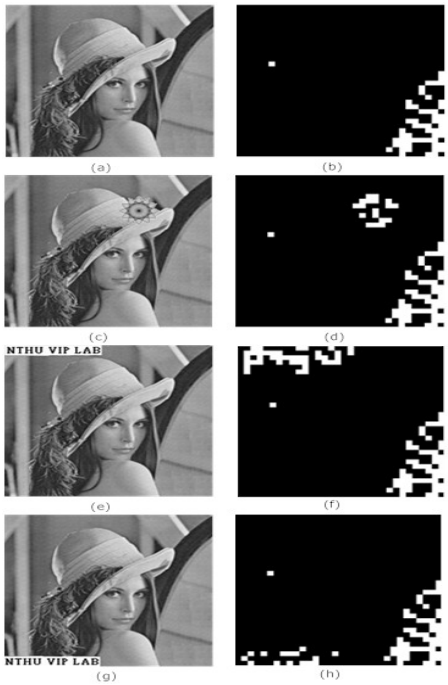

Fig.7. Locate the malicious attack in the image for Lena

Table 8 . Comparison with the other popular algorithms

	The proposed scheme	Algorithm 1	Algorithm 2
Robust to JPEG	Q=30	Q=50	Q=40
Robust to Gaussian Noise	Variance = 20	Variance = 3	Variance = 8
Robust to rotation	YES	YES	NO
Resolution of tampering detection	8x8	16x16	8x8
PSNR	41.92	44.15	38.4