Journal of Information Hiding and Multimedia Signal Processing ©2011 ISSN 2073-4212
Ubiquitous International Volume **2**, Number **3**, July **2011**

Multipurpose Watermarking Based on Blind Vector Quantization (BVQ)

Chih-Hung Lin

Dep.of Graduate Institute of Mathematics and Science Education
National Chiayi University
No.85 Wenlong Vil., Minxiong Township, Chiayi County 62103, Taiwan
chuck@ncyu.edu.tw

Ching-Yu Yang

Dept. of Computer Science and Information Engineering
National Penghu University of Science and Technology
No. 300, Liu-Ho Rd., Magong, Penghu, 880 Taiwan
chingyu@npu.edu.tw

Received April 2010; revised July 2010

Abstract. *Several different digital watermarking methods have been researched and proposed in the last ten years. However, most of the proposed methods focused on a single purpose. Recently, some multipurpose watermarking methods have been proposed, but most of them were focused on combining copyright protection and integrity verification. In this paper, we propose a multipurpose watermarking method that provides copyright protection, integrity verification, and simultaneous identification of malicious and non-malicious attacks. Additionally, a novel mechanism called blind vector quantization (BVQ), which is used to generate authentic information and to verify that the received image is authentic, is also proposed. These capabilities allow improved transmission performance relative to the performance of traditional watermarking methods based on vector quantization. The results obtained in our experiments verified the beneficial effects of the proposed method.*

Keywords: Multipurpose watermarking, Blind vector quantization, Copyright protection, Integrity verification.

1. **Introduction.** The explosive growth of digital multimedia techniques and the extensive distribution of digital images over the Internet have made digital media readily available. However, these media can be attacked and modified easily during transmission, and, as a result, several related issues have been studied, such as data hiding [5,18], digital image copyright protection, and content authentication. Many digital watermarking schemes have been proposed and used to solve the attack and modification problems; these schemes can be classified generally into three categories, i.e., robust, fragile, and semi-fragile. Robust watermarking schemes [2,11] for copyright protection are used to verify ownership when digital images are attacked. Fragile watermarking schemes [3,13], which are used for digital content verification, detect whether digital images have been altered and distinguish the altered areas from the extracted watermark without using the original images. Semi-fragile watermarking schemes [4,10] are used to reject malicious manipulations, but they are able to accept non-malicious manipulations, such as lossy compression.

Multipurpose watermarking methods [1,7,8,12,14-17] have been proposed recently, because single-purpose digital watermarking methods cannot satisfy specific, desired conditions simultaneously, such as copyright protection and integrity verification. Chang et al. [1] embedded authentication information and a copyright logo into 10 sub-bands of a three-level, digital wavelet transform (DWT). Chang et al.s method provides a watermarked image of good visual quality (50.03 dB), but it is not robust in dealing with a Gaussian noise attack. Further, they did not specify in their paper whether their method has the ability to identify modified parts. Yuan et al. [8] separated color images into R, G, and B components. A robust watermark is embedded into the frequency domain of the G component, and fragile watermarking is embedded into the spatial domain of the B component. Yuan et al. used repetitive codes to correct the error bits of the watermark, which requires that additional watermarking bits be embedded in the image, resulting in a huge distortion of the watermarked image. The peak signal to noise ratio (PSNR) of the watermarked image was 37.23 dB in their experiment. In Changs and Yuans methods, only two purposes, robust and fragile watermarking, are achieved. Lu et al. [17] also proposed a multipurpose watermarking method that was based on embedding robust and semi-fragile watermarks in the original image, but, again, only two purposes, i.e., robust and semi-fragile watermarking, were achieved. Their method should have two stages, allowing the embedding of the robust watermark and the semi-fragile watermark in the image in the first stage and the second stage, respectively, by using vector quantization. In their method, the extensive image distortion is obvious, and the PSNR of the watermarked image is 30.55 dB. Lus method reduces the visual quality of the watermarked image, and it should transmit two codebooks to the receiver. Wu and Wangs multipurpose watermarking method [6] notifies the copyright owner with a reversible visible watermark in the region of interest (ROI) of the original image and protects the copyright with an invisible watermark in the remaining part of the image. However, whether the method has the abilities to authenticate content and distinguish the type of manipulation was not mentioned in reference [6]. In addition, other multipurpose watermarking methods [15,9,19] that have been proposed recently have the same drawbacks, i.e., (1) they can achieve only copyright protection (robust watermarking) and integrity verification (fragile watermarking), and (2) a codebook must be transmitted to the receiver if vector quantization is used.

Due to the drawbacks described above, we proposed a multipurpose watermarking method based on blind vector quantization. The term blind vector quantization is used because there is no need to transmit a codebook to the receiver. Significantly, three purposes can be achieved by the scheme, i.e., copyright protection (robust), integrity verification (fragile), and differentiation between malicious and non-malicious attacks (semi-fragile). The rest of the paper is organized as follows. In Section 2, we introduce the previous method based on BVQ. The experimental results and the conclusions are presented in Sections 3 and 4, respectively.

2. Digital watermarking method based on blind vector quantization (BVQ).

Since the proposed method can provide robust, fragile, and semi-fragile image authentication simultaneously, two important pieces of information, i.e., copyright information and verification information, must be generated and embedded in the original image. The details are described in the following sub-sections.

2.1. Generation and embedding of copyright information.

The symbol M represents a copyright binary image with size $b \times b$, and the image is scrambled as M^s with key_1. The original image I with size $W \times H$ pixels is divided into $b \times b$ non-overlapping blocks $I_{i,j}$ with size $w \times h(= W/b \times H/b)$. Then M^s is separated into two sets that have an equal number of elements, i.e., W^{emd} and W^{key}, respectively. W^{emd} is embedded into I, and the W^{key} is used as a secret key and passed to the receiver. The binary matrix P with size $b \times b$ is designed, and the numbers of element 0 and element 1 are equal, and each element in P is denoted as $P_{i,j}$. Assume that $LL^{\lambda}_{i,j,u,v}$ denotes the (u, v) wavelet coefficient in λ-level LL sub-band of $I_{i,j}$, and that each bit of W^{emd} that denotes w^{emd}_k is embedded into $LL^{\lambda}_{i,j,u,v}$, where $P_{i,j}$ is 1 and (u, v) is chosen by key_2. Then, we adjust $LL^{\lambda}_{i,j,u,v}$ as $LL''^{\lambda}_{i,j,u,v}$ according to w^{emd}_k. The embedding formula of copyright information follows:

$$LL'^{\lambda}_{i,j,u,v} = \begin{cases} round(LL^{\lambda}_{i,j,u,v}/Q) \times Q + Q/2, & if(LL^{\lambda}_{i,j,u,v} - round(LL^{\lambda}_{i,j,u,v}/Q) \times Q) \geq 0 \\ round(LL^{\lambda}_{i,j,u,v}/Q) \times Q - Q/2, & else \end{cases}$$

$$LL''^{\lambda}_{i,j,u,v} = \begin{cases} LL^{\lambda}_{i,j,u,v} + Q/4, & if w^{emd}_k = 1 \\ LL^{\lambda}_{i,j,u,v} - Q/4, & if w^{emd}_k = 0 \end{cases} \tag{1}$$

where Q is a quantization interval that depends on the lower-bound image, and refers to the round-off function. Finally, the watermarked image is generated by performing inverse DWT (IDWT).

2.2. **Generation of verification information.** This method achieves the ability of protecting copyright, and it also has the ability to verify integrity and distinguish whether the attack on the received image was malicious or not. Therefore, verification information must be generated by the sender and verified by the receiver. First, image I is divided into $s \times s$ segments, denoted $S_{i,j}$, which include $\alpha \times \beta$ non-overlapping blocks, denoted $S_{k,l,m,n}$. Also, the matrix P is divided into $s \times s$ segments with $\alpha \times \beta$ elements in each segment, and the(m, n) element at (k, l) segment is denoted $P_{k,l,m,n}$. For $S_{k,l}$, those blocks $S_{k,l,m,n}$ for which $P_{k,l,m,n}$ is 0 are chosen and trained to generate a codebook $C_{k,l}$ by the well-known Linde-Buzo-Gray (LBG) algorithm. The length of the codebook is denoted as LC for all $C_{k,l}$, and the x^{th} codeword with size $w \times h$ bits in $C_{k,l}$ is denoted $c_{k,l,x}$, $1 \leq x \leq LC$. The mean of $c_{k,l,x}$, denoted $c^{mean}_{k,l,x}$, is computed as follows:

$$c^{mean}_{k,l,x} = \sum_{y=0}^{w \times h-1} c_{k,l,x,y}/w \times h \tag{2}$$

where $c_{k,l,x,y}$ is the y^{th} bit of $c_{k,l,x}$. All codewords that belong to $C_{k,l}$ are re-sorted according to the ascendant order of $c^{mean}_{k,l,x}$, and a new sorted codebook $C^{sort}_{k,l}$ is generated. The target of re-sorting $C_{k,l}$ is arising the stable authentication. Then, each $S_{k,l,m,n}$ can find a representable index by looking-up codebook $C^{sort}_{k,l}$, and the index table of the original image I, denoted T^{ori}, can be cascaded by each segments index table $T^{ori}_{k,l}$. Second, five low-bound images that are performed JPEG2000 compression with quality factor 50, 60, 70, 80, and 90, denoted I^{JQF} and $QF \in \{50, 60, 70, 80, 90\}$, are used in this method. The average block that corresponds to index x for the (k, l) segment of I^{JQF} is computed and denoted as $AS^{JQF}_{k,l,x}$. The Euclidean distance between $AS^{JQF}_{k,l,x}$ and $S^{JQF}_{k,l,m,n,x}$ is computed, where $S^{JQF}_{k,l,m,n,x}$ is the (m, n) block in the (k, l) segment and belongs to index x of I^{JQF}. The

$AS^{JQF}_{k,l,x}$ is recomputed from block set $\{\{S^{JQF}_{k,l,m,n,x}\} - \{MS^{JQF}_{k,l,x}\}\}$ and denoted as $AS'^{JQF}_{k,l,x}$, where $\{MS^{JQF}_{k,l,x}\}$ denotes the blocks that have the maximum Euclidean distance among $S^{JQF}_{k,l,x}$ for index x, and then codebook $C^{JQF}_{k,l}$ is reconstructed as $\{AS'^{JQF}_{k,l,x} \mid 1 \leq x \leq LC\}$. Therefore, the codebook $C^{JQF,sort}_{k,l}$ is generated after sorting the codeword $AS'^{JQF}_{k,l,x}$ of codebook $C^{JQF}_{k,l}$ by ascendant order, and then index table $T^{JQF}_{k,l}$ is generated by looking-up $C^{JQF,sort}_{k,l}$. Third, the maximum and minimum differences of the index between $T^{ori}_{k,l}$ and all $T^{JQF}_{k,l}$, denoted as $t\_\max_{k,l}$ and $t\_\min_{k,l}$, are computed as follows:

$$\begin{aligned} t\_\max_{k,l} =& \max(\max(T^{ori}_{k,l,m,n} - T^{JQF}_{k,l,m,n})) \\ t\_\min_{k,l} =& \min(\min(T^{ori}_{k,l,m,n} - T^{JQF}_{k,l,m,n})) \end{aligned} \tag{3}$$

where $QF \in \{50, 60, 70, 80, 90\}$. The $t\_\max_{k,l}$ and $t\_\min_{k,l}$ are used as the maximum and minimum index differences for the (k,l) segment after non-malicious manipulations. Finally, find the blocks that belong to $t\_\max_{k,l}$ and $t\_\min_{k,l}$ and compute the Euclidean distance of the codeword between $T^{ori}_{k,l}$ and $T^{JQF}_{k,l}$, as follows:

$$\begin{aligned} t\_dis^{max}_{k,l} =& \max(ED(c^{ori}_{k,l,m,n} - c^{JQF}_{k,l,m,n}) \mid \forall(T^{ori}_{k,l,m,n} - T^{JQF}_{k,l,m,n}) = t\_\max_{k,l}) \\ t\_dis^{min}_{k,l} =& \min(ED(c^{ori}_{k,l,m,n} - c^{JQF}_{k,l,m,n}) \mid \forall(T^{ori}_{k,l,m,n} - T^{JQF}_{k,l,m,n}) = t\_\min_{k,l}) \end{aligned} \tag{4}$$

where $ED(\cdot)$ denotes the function of computing Euclidean distance, and the final maximum distance that corresponds to $S_{k,l}$, denoted as $t\_dis_{k,l}$, is set between $t\_dis^{max}_{k,l}$ and $t\_dis^{min}_{k,l}$. Finally, the T^{ori}, P, $t\_\max_{k,l}$, $t\_\min_{k,l}$, $t\_dis_{k,l}$, W^{key}, Key_1, and Key_2 are transmitted to the receiver, but the transmission does not include the codebook.

2.3. **Verification of copyright information.** The received image I^{rec} with size $W \times H$ pixels is divided into $b \times b$ non-overlapping blocks $I^{rec}_{i,j}$ with size $w \times h (= W/b \times H/b)$, and the location (u,v) of λ-level LL-subband coefficient in block $I^{rec}_{i,j}$ that is embedded watermark bit w^{rec}_k can be found by matrix P and key_2, and the coefficient denotes $LL^{rec,\lambda}_{i,j,u,v}$. The watermark bit is extracted as follows:

$$w^{rec}_k = \begin{cases} 0, & if(LL^{rec,\lambda}_{i,j,u,v} - round(LL^{rec,\lambda}_{i,j,u,v}/Q) \times Q) \geq 0 \\ 1, & else \end{cases} \tag{5}$$

The location relationship for k and (i,j) can be found by P and key_2, and the extracted watermark W^{emd} is cascaded by w^{rec}_k. Then, the copyright information M^{rec} is generated by scrambling $M^{rec,s}$ with key_1, where $M^{rec,s}$ is cascaded with W^{emd} and the received W^{key}. Finally, the M^{rec} is used by the receiver to verify the copyright.

2.4. **Verification of the received image.** First, the received image I^{rec} is segmented, and $S^{rec}_{k,l,m,n}$ denotes the (m,n) block in (k,l) segment. Those $S^{rec}_{k,l,m,n}$ where $P_{k,l,m,n}$ belongs to 0 are selected and used to reconstruct the codebook denoted $C^{rec}_{k,l}$ according to the received $T^{ori}_{k,l}$. The reconstruction of the algorithm of $C^{rec}_{k,l}$ is similar to the generation of $C^{sort,JQF}_{k,l}$ described in section 2.2. Then, the index of $S^{rec}_{k,l,m,n}$ can be found by looking up $C^{sort,JQF}_{k,l}$ and cascaded as index table $T^{rec}_{k,l}$. Second, the difference of index between $T^{ori}_{k,l}$ and $T^{rec}_{k,l}$ for $S''_{k,l,m,n}$ is computed and denoted $dif_{k,l,m,n}$. The $S^{rec}_{k,l,m,n}$ is regarded as an authenticated block when $t\_dis^{min}_{k,l} \leq dif_{k,l,m,n} \leq t\_dis^{max}_{k,l}$; otherwise, it is regarded as a suspicious block and verified further as follows:

$$S^{rec}_{k,l,m,n} = \begin{cases} authentic & , \ if ED(c^{ori}_{k,l,m,n}, c^{rec}_{k,l,m,n}) \leq t\_dis_{k,l} \\ non-authentic & , \ else \end{cases} \tag{6}$$

where $c^{rec}_{k,l,m,n}$ is the codeword of the (m, n) block in the (k, l) segment of $T^{rec}_{k,l}$. Finally, the blocks that underwent malicious manipulations are located, and the effect of related experiments is shown in the following section.

3. **Experimental Results.**

The three test images, i.e., Boat, Airplane, and Baboon, all sized 512 × 512 pixels, and the binary copyright logo with a size of 64 × 64 pixels are shown in Figures 1 and 2.

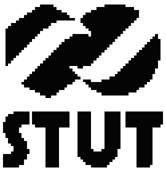


Figure 1. Original binary copyright logo

The test image is divided into blocks of 8 × 8 pixels and segmented into 4 × 4 non-overlapping segments, 7×7 overlapping segments, and 8×8 overlapping circular segments for three different experiments, respectively. Therefore, there are 16 × 16 blocks within each segment. The codebook size LC is set to 16, and each codeword size is 64 bits. The threshold of LBG training is set as 0.000001. The quantization factor Q is set as 380, λ-level is set as 3-level, and the PSNR of the watermarked images in Figure 2 are listed in Table 1. Referring to Table 1, the watermarked images still preserve good visual quality according to the human visual system (HVS) theorem. Then, the watermarked image has undergone several manipulations, such as JPEG compression, sharpening, smoothing, Gaussian noise, pasting and cropping attacks. Then, the copyright and integrity of these attacked images are verified further. Detailed information about the manipulations used in this paper is listed in Table 2.

Table 1. The PSNR of watermarked image

Image	Boat	Airplane	Baboon
PSNR	43.95dB	43.88dB	43.84dB

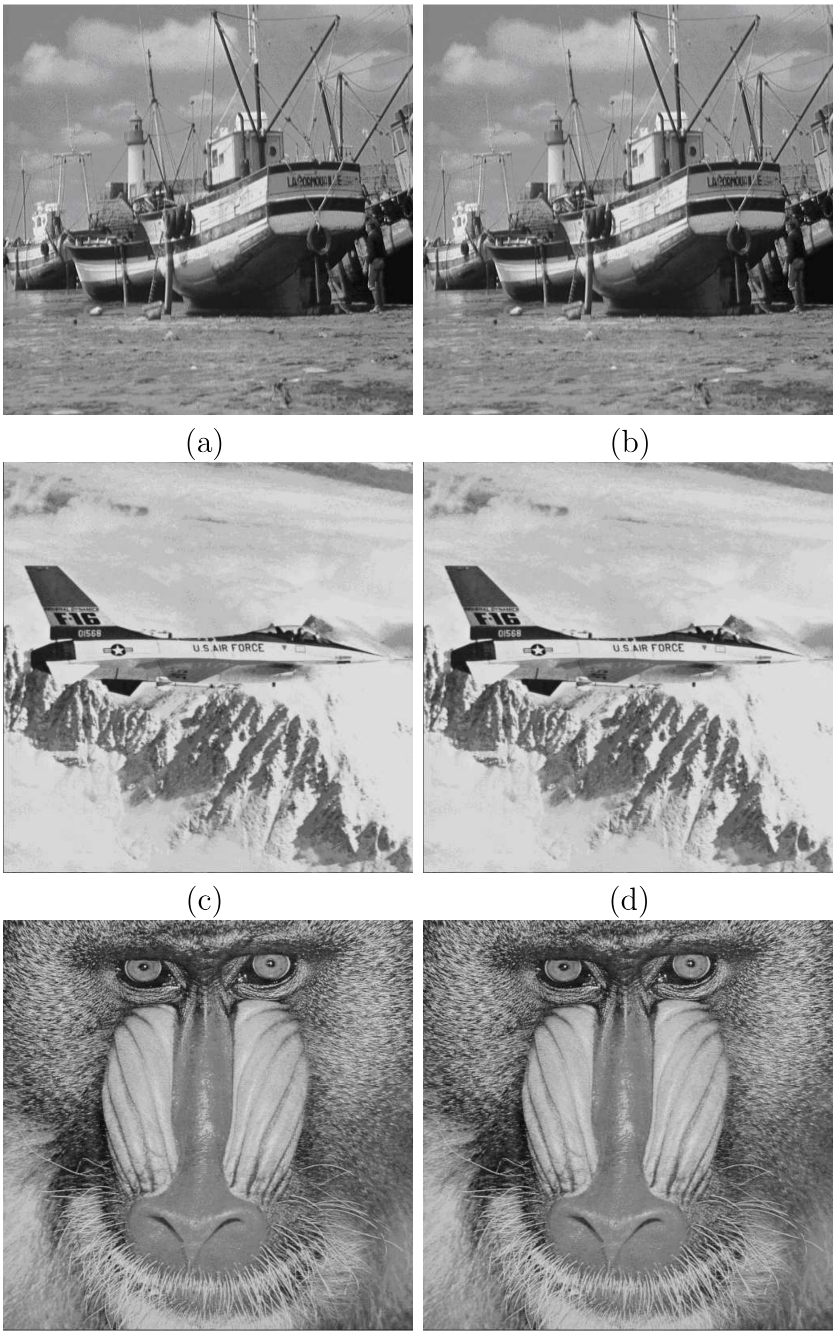
3.1. **Experiment of verifying copyright.**

The watermark must be extracted from the received image and then the copyright must be verified. Figure 3 shows the watermarks extracted from Boat images modified by several image processions listed in Table 2. The normalized correlation (NC) was used to evaluate the visual quality of the extracted watermark, and the NC is defined as follows:

$$NC = \sum_{i=1}^{m} \sum_{j=1}^{n} W_{i,j} W'_{i,j} / \sum_{i=1}^{m} \sum_{j=1}^{n} W^2_{i,j} \tag{7}$$

where $W_{i,j}$ and $W'_{i,j}$ denote the original and extracted watermarks, respectively, and the NC values of the extracted watermarks are shown in Table 3.

The two experiments from Figure 3 and Table 3 must be explained, i.e., one is the results of sharpening, and the other one is the results of combined manipulations such



(a) (b)

(c) (d)

(e) (f)

Figure 2. (a),(b),(c) Original image; (d),(e),(f) Watermarked image

as cropping 25% + pasting + (JPEG QF=50). Although the NC value of the extracted watermark for the sharpening attack was close to 0.8 as shown in Table 3, the copyright information still can be understand and identified. In addition, the proposed method is also robust to combined manipulations, and the value of the extracted watermark for combined attack can be as high as 0.99. Therefore, the results of Figure 3 and Table 3 demonstrate that the proposed method is robust for copyright protection because of the good visual quality of the extracted watermark.

3.2. **Experiment of verifying integrity.** The copyright of the received image must be verified, but the integrity must also be verified and the parts modified by malicious

Table 2. Detailed information of the manipulations used in the experiment

Manipulations	Detail information
JPEG compression	compression with quality factor (QF) 80, 70, 60, 50, 40, 30, 20, 10 by application software PhotoImpact
sharpening	mask1: $\begin{bmatrix} 0,-1,0 \\ -1,4,-1 \\ 0,-1,0 \end{bmatrix}$ mask2: $\begin{bmatrix} -1,-1,-1 \\ -1,8,-1 \\ -1,-1,-1 \end{bmatrix}$
smoothing	mask1: $\frac{1}{9}\times \begin{bmatrix} 1,1,1 \\ 1,1,1 \\ 1,1,1 \end{bmatrix}$ mask2: $\frac{1}{16}\times \begin{bmatrix} 1,2,1 \\ 2,4,2 \\ 1,2,1 \end{bmatrix}$
pasting	past something by application software PhotoImpact
cropping	crop 25 % of original image by application software PhotoImpact

Table 3. NC values of the extracted watermarks

Image processing	NC	Image processing	NC
JPEG(QF=90)	1.000	sharpening1	0.796
JPEG(QF=80)	1.000	sharpening2	0.760
JPEG(QF=70)	1.000	smoothing1	0.924
JPEG(QF=60)	1.000	smoothing2	0.947
JPEG(QF=50)	1.000	Gaussian Noise	0.998
JPEG(QF=40)	0.997	pasting	0.994
JPEG(QF=30)	0.969	cropping	0.995
JPEG(QF=20)	0.805	(JPEG QF=50) + pasting	0.992
JPEG(QF=10)	0.768	cropping 25%+ pasting+ (JPEG QF=50)	0.984

manipulations must be located. For verifying the integrity of the received image, we propose three different segmentation measures, i.e., 4×4 non-overlapping segments, 7×7 overlapping segments, and 8×8 overlapping circular segments. Each segment includes 16×16 blocks with sizes of 8×8 pixels. Table 4 illustrates the results obtained for verifying the integrity of the received image, and three different segment measures were used for comparison.

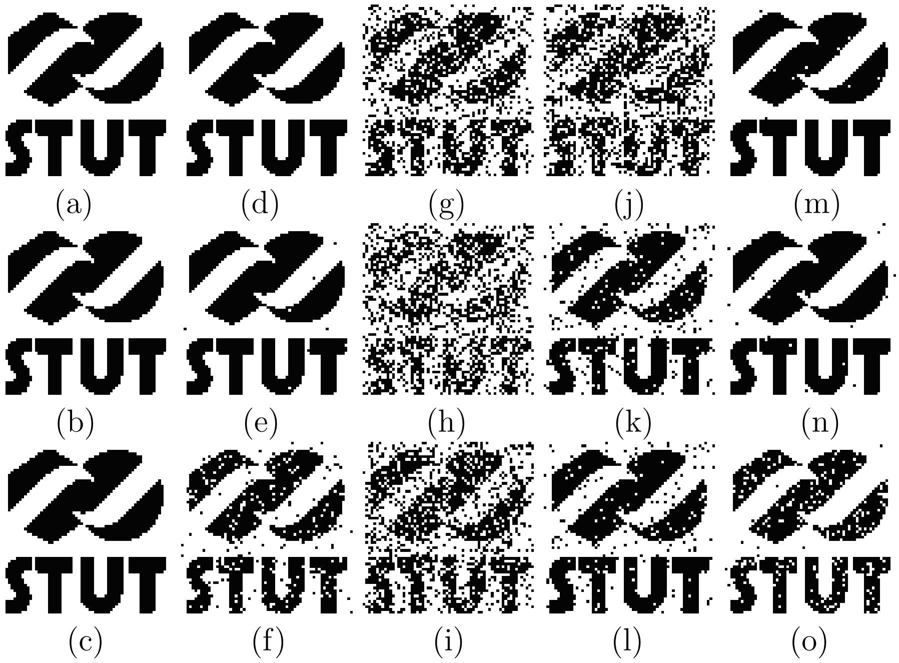
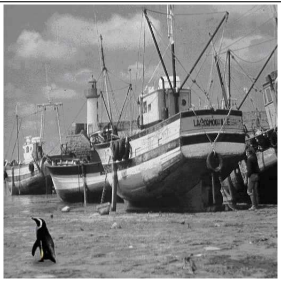
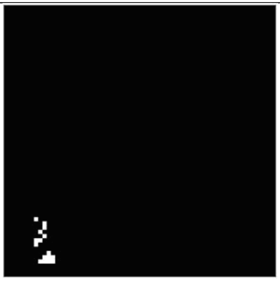
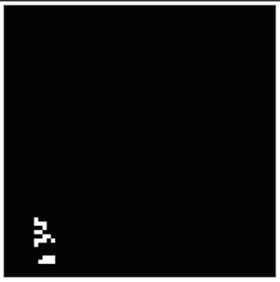
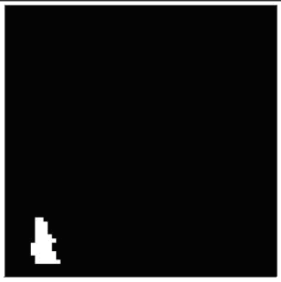
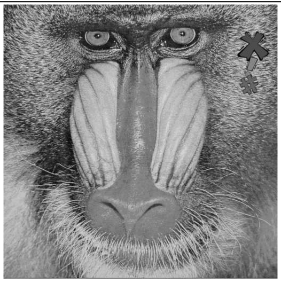
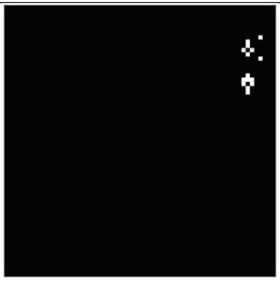
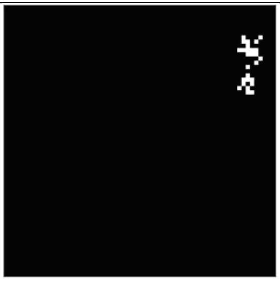
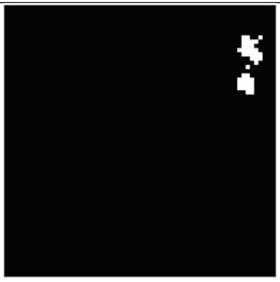
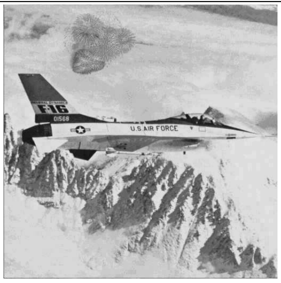
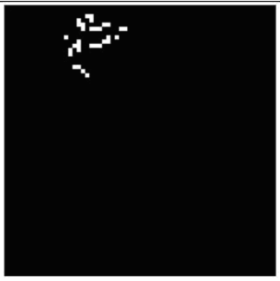
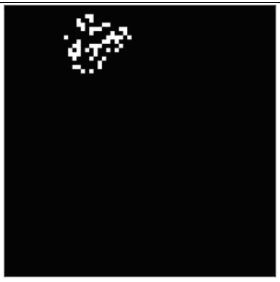
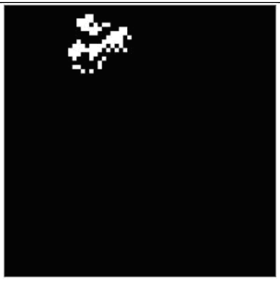


Figure 3. Extracted watermarks with attacks: (a)-(h) JPEG QF=80, 70, 60, 50, 40, 30, 20, 10; (i) sharpening with mask1; (j) sharpening with mask2; (k) smoothing with mask1; (l) smoothing with mask2; (m) Gaussian noise; (n) pasting; (o) cropping

Table 4. Results for verifying integrity of received image

	Segmentation measure		
Received image	Measure1	Measure2	Measure3
	4 × 4non-overlapping segments	7 × 7overlapping segments	8 × 8 overlapping circular segments
			
			
			

Referring to Table 4, measure 1 has the worst localization ability because the authentication information is only offered for one segment. Measure 2 improves this shortcoming, and the segmentation is defined as overlapping; therefore, more authentication information can be offered and the localization ability is better than measure 1. Further, the concept of circular segment is used and improves for measure 2, and each block can be authenticated by two segmentations. Therefore, the accuracy of localization is improved, becoming greater than measure 1 and measure 2.

4. Conclusions. In this paper, we propose a multipurpose watermarking method that can protect the copyright, verify the integrity, and distinguish between malicious and non-malicious manipulations. It can also locate the parts that underwent malicious attacks. Blind vector quantization is a novel measure and is proposed for use in our proposed scheme. No codebooks have to be transmitted to the receiver, so the performance of transmitting is improved relative to traditional watermarking methods based on vector quantization. Our proposed method also can preserve the good visual quality of the watermarked image, and it has the ability to locate the parts that have been manipulated by malicious attacks. The positive results achieved with the proposed scheme are shown in the experimental results.

Acknowledgment. This work is partially supported by the National Science Council, Taiwan, grant NSC99-2221-E-218-039. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

[1] C. C. Chang, W. L. Tai and C. C. Lin, A multipurpose wavelet-based image watermarking, *Proc.of International Conference on Innovative Computing, Information and Control*, vol. 3, pp. 70-73, 2006.

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

[3] C. H. Lin and W. S. Hsieh, Applying projection and B-spline to image authentication and remedy, *IEEE Trans. Consumer Electronics*, vol. 49, no. 4, pp. 1234-1239, 2003.

[4] C. Y. Lin and S. F. Chang, Semi-fragile watermarking for authenticating JPEG visual content, *Proc. of SPIE International Conference on Security and Watermarking of Multimedia Contents II*, vol. 3917, no. 13, pp. 140-151, 2000.

[5] C. Y. Yang, W. C. Hu and C. H. Lin, Reversible data hiding by coefficient-bias algorithm, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 2, pp. 91-100, 2010.

[6] D. Wu and G. Wang, Multipurpose digital watermarking for copyright notification and protection, *Proc. of ISECS International Colloquium on Computing, Communication, Control, and Management*, vol. 2, pp. 68-71, 2009.

[7] H. C. Huang, Y. H. Chen and A. Abraham, Optimized watermarking using Swarm-based bacterial foraging, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 1, pp. 51-58, 2010.

[8] J. Yuan, G. H. Cui and Y. J. Zhang, A practical multipurpose color image watermarking algorithm for copyright protection and image authentication, *Proc. of IEEE International Conference on Digital Telecom- munications*, pp. 72-72, 2006.

[9] J. S. Tsai, W.B. Huang, C. L. Chen and Y. H. Kuo, A feature-based digital image watermarking for copyright protection and content authentication, *Proc. of IEEE International Conference on Image Processing*, vol. 5, pp. 469-472, 2007.

[10] K. Maeno, Q. Sun, S. F. Chang and M. Suto, New semi-fragile image authentication watermarking techniques using random bias and nonuniform quantization, *IEEE Trans. Multimedia*, vol. 8, no. 1, pp. 32-45, 2006.

[11] L. D. Li and B. L. Guo, Robust image watermarking using feature based local invariant regions, *International Journal of Innovative Computing, Information and Control*, vol. 4, no. 8, pp. 1977-1986, 2008.

[12] M. Q. Fan and H. X. Wang, A novel multipurpose watermarking scheme for copyright protection and content authentication, *Proc. of IEEE Second Workshop on Digital Media and its Application in Museum and Heritages*, pp. 19-24, 2007

[13] M. U. Celik, G. Sharma and A. M. Tekalp, Lossless watermarking for image authentication: a new framework and an implementation, *IEEE Trans. Image Processing*, vol. 15, no. 4, pp. 1042-1049, 2006.

[14] T. H. Chen, T. H. Hung, G. Horng and C. M. Chang, Multiple watermarking based on visual secret sharing, *International Journal of Innovative Computing, Information and Control*, vol. 4, no. 11, pp. 3005-3026, 2008.

[15] Y. T. Wu and F. Y. Shih, An adjusted-purpose digital watermarking technique, *Pattern Recognition*, vol. 37, no. 12, pp. 2349-2359, 2004.

[16] Z. M. Lu, C. H. Liu and H. Wang, Image retrieval and content integrity verification based on multipurpose image watermarking scheme, *International Journal of Innovative Computing, Information and Control*, vol. 3, no. 3, pp. 621-630, 2007.

[17] Z. M. Lu, D. G. Xu and S. H. Sun, Multipurpose image watermarking algorithm based on multistage vector quantization, *IEEE Trans. Image Processing*, vol. 14, no. 6, pp. 822-831, 2005.

[18] Z. H. Wang, T. D. Kieu, C. C. Chang and M. C. Li, A novel information concealing method based on exploiting modification direction, *Journal of Information Hiding and Multimedia Signal Processing* vol. 1, no. 1, pp. 1-9, 2010.

[19] Z. Wang, B. Yang, X. Niu and Y. Zhang, A practical multipurpose watermarking scheme for visual content copyright protection and authentication, *Proc. of Intelligent Information Hiding and Multimedia Signal Processing, International Conference on*, pp. 461-464, 2006.