A Robust Grayscale Watermarking Scheme Using Angle Quantization

Hsien-Chu Wu[1], Chuan-Po Yeh[2], and Chwei-Shyong Tsai[3]
[1] *Department of Information Management, National Taichung Institute of Technology, 129 Sec. 3, San-min Road, Taichung, Taiwan 404, R.O.C.*
wuhc@ntit.edu.tw
[2] *Institute of Computer Science and Information Technology, National Taichung Institute of Technology, 129 Sec. 3, San-min Road, Taichung, Taiwan 404, R.O.C.*
ycb1127@gmail.com
[3] *Department of Management Information Systems, National Chung Hsing University, 250 Kuo Kuang Road, Taichung, Taiwan 402, R.O.C.*
tsaics@nchu.edu.tw, tsaics@gmail.com

ABSTRACT

Digital life has been an important being of human life with the development of computer science, and the multimedia tort has become serious. Digital watermarking techniques support an efficient copyright protection, as well as the integrity and the ownership of multimedia can be protected by watermarking techniques. In this paper, the discrete wavelet transformation (DWT) is used, and the middle-frequency DWT coefficients are used to generate vectors. The purpose of embedding watermark is achieved by quantizing and adjusting the angle of the vector. Experimental results show that our proposed scheme has a better performance for JPEG lossy compression, and is robust against attacks such as rotation, rescaling, cropping, noise addition, blur, sharpness and brightness adjustment.

1: INTRODUCTIONS

The advancement of computer science has made our lives more than ever convenient in many aspects. In today's digital era, the chance of torts of digital multimedia increases because it is easy to be copied, modified and transmitted. Digital image is the familiar multimedia that is used. Although digital image has many advantages over the traditional image, there are some issues with its inherent properties such that the digital image can be duplicated quickly, modified easily, but hardly distinguished fake. These days, a great many owners of the digital images have suffered a great loss due to a large number of fake images that are widely spread over the Internet. Therefore, it is imperative to provide an effective protection of image copyright.

Common protection scheme for image copyright is to use cryptography. The protected image processed by cryptography is presented as a random noise, and that may decrease the application of the image. Another common protection scheme is digital watermarking technique. The watermark is hidden into the original image with slight modification which humans can't be aware of, and the watermarked image can be obtained. The watermarked image is protected by the hidden watermark. Digital watermarking techniques [10, 11] are divided into two categories according to its purpose of use [1]. The first category is fragile watermarking [2-4], which is used to protect the image integrity. The difference between the watermarked image and the attacked image must be identified if the watermarked image is attacked. The second category is robust watermarking [5-8], whose main purpose is to prevent from the malicious attacks to a reasonable range. In this case, it is suitable for the protection of image copyright.

In recent years, many researches about robust watermarking are proposed. Wu and Shih [5] presented an adjusted-purpose watermarking technique with two parameters on DCT domain. The features of images are extracted based on using mathematical morphology. These features and the watermark are processed together with XOR operator to generate the final watermark and this watermark is then embedded into the image. The *VSTW* parameter is used to control the block size of DCT decomposition. The watermark is embedded into the spatial domain if *VSTW*=1, and is on the contrary embedded into the frequency domain. The *QF* parameter is used to control the quantification level, and uses LSB scheme [9] to embed watermark into the image. Wang and Lin [6] proposed a wavelet-tree-based blind watermarking scheme. The DWT coefficient can be related to four DWT coefficients of inferior level, and this relation is hence used to generate a super tree. The watermark is embedded into DWT coefficients by quantizing the super tree. Kundur and Hatzinakos [7] presented a watermark technique by using multi-resolution wavelet decomposition. Three coefficients in three subbands, respectively, i.e. $HL_i(m, n)$, $LH_i(m, n)$ and $HH_i(m, n)$ where i is the level of DWT decomposition and (m, n) is the index of the coefficient of each subband, are sorted, and the middle coefficient is quantified to embed watermark. Chen and Lin [8] used the mean quantization technique to develop

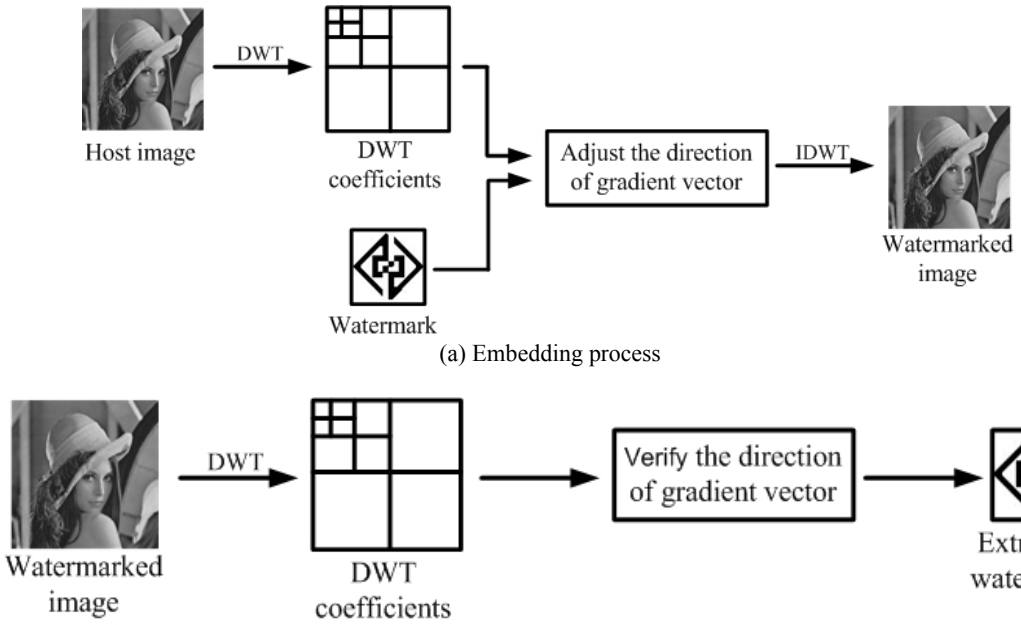
a robust watermarking scheme. The image quality is enhanced by using the human visual system (HVS). The coefficients having a fixed number in DWT domain are calculated to get the JND value of HVS. The mean value of these coefficients is obtained by using JND value to quantify these coefficients. The mean value is adjusted to embed watermark.

The optimal watermarking technique must be capable of resisting various attacks, however general watermarking techniques may be robust to some attacks while fragile to other attacks. In this paper, a watermarking scheme which resists both compression attacks and geometrical attacks is proposed. A grayscale image is transformed into DWT coefficients, and two of the coefficients having the same index in HL subband and LH subband are used to form a vector. The direction of the vector is adjusted to embed the watermark, and the length is increased to adjust the robustness of the watermark.

The layout of this paper is shown as follows. Section 2 introduces the fundamental concept of our scheme and how the scheme is implemented. Experimental results and discussions are in Section 3. Lastly, conclusions and future work are stated in Section 4.

2: The Proposed Scheme

In this paper, the DWT coefficients are used to generate vectors. The direction of the vector is changed to embed watermark, and the adjusted DWT coefficients are returned to spatial domain by using inverse discrete wavelet transformation to obtain the watermarked image. The flowchart is shown in Figure 1.



(a) Embedding process

(b) Extracting process

Fig. 1. The block diagram of the proposed scheme

2.1: Discrete Wavelet Transformation

For any given image $I(m, n)$, it can be transformed from the spatial domain to the frequency domain by using discrete wavelet transformation, and the DWT coefficients of the image $I(m, n)$ can represent image characteristics, where m is the image height and n is the image width. The DWT coefficients can be obtained by using the horizontal and vertical processes. Figure 2 shows the 1-level discrete wavelet transformation, where A, B, C and D are the neighboring pixels. The equations of horizontal processes and vertical processes are shown as follows.

$$\begin{cases} H(i,j) = I(i, 2j-1) + I(i, 2j); \\ H(i, j+\frac{n}{2}) = I(i, 2j-1) - I(i, 2j), \end{cases} \quad (1)$$

where $i \in \{1, 2, \cdots, m\}$ and $j \in \{1, 2, \cdots, n/2\}$.

$$\begin{cases} V(i, j) = H(2i-1, j) + H(2i, j); \\ V(i+\frac{m}{2}, j) = H(2i-1, j) - H(2i, j), \end{cases} \quad (2)$$

where $i \in \{1, 2, \cdots, m/2\}$ and $j \in \{1, 2, \cdots, n\}$.

$H(i, j)$ is the coefficient with the index (i, j) obtained by horizontal process and $V(i, j)$ is the coefficient with the index (i, j) obtained by vertical process. The higher-level DWT coefficients can be obtained by applying the discrete wavelet transformation to the LL1 subband.

The DWT coefficients can be divided into four subbands. Take Figure 1 as an example, the four DWT coefficients are calculated from four pixels A, B, C and D. The LL subband coefficient is the sum of these four pixels, and it represents that this coefficient centralizes energy of these four pixels. The coefficient of HL subband is the difference between the left and the right portion of the pixels. This coefficient can represent the

vertical edge of these four pixels, and the vertical edge will be clearer if this coefficient becomes bigger. The coefficient of LH subband is the difference between the upper and the lower portion of the pixels, and it can represent the horizontal edge of these four pixels. Similarly, the coefficient of HH subband can represent the diagonal edge.

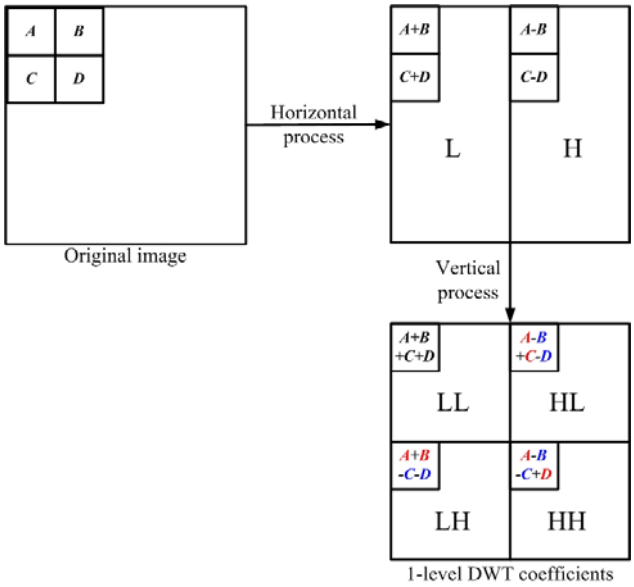


Fig. 2. 1-level discrete wavelet transformation

2.2: Embedding and Extracting Processes

From Section 2.1, it can be observed that the DWT coefficients with the same index in HL subband and LH subband relate to the same region. If the region is attacked, both of the coefficients in HL subband and LH subband will be changed. This property can be used to embed watermark. In order to embed watermark w, the host image $I(m, n)$ is transformed to the DWT coefficients, where m is the image height, n is the image width, and w belongs to 1 or -1. A pair of DWT coefficients which is selected by a random generator is used. The absolute value of the coefficient $a = |HL(p, q)|$ in HL subband and the absolute value of the coefficient $b = |LH(p, q)|$ in LH subband are used to form the vector $v = (a, b)$ with the length $L = \sqrt{a^2 + b^2}$, where (p, q) is the index of the subband. The angle $\alpha = tan^{-1}(b/a)$ between the vector v and the x-axis is calculated. The quantization parameter θ is used to divide the angle between 0° and 90° into several sub-angles. Then, the vector v can be confirmed to belong to which sub-angle. For example, if quantization parameter θ is 10° and the angle α is 43°, the vector belongs to the sub-angle which is from 40° to 49°. The embedding process is shown in Equation (7).

$$\alpha' = \begin{cases} \left\lfloor \frac{\alpha}{\theta} \right\rfloor \times \theta + \frac{\theta}{4}, \text{if } w_i = -1; \\ \left\lfloor \frac{\alpha}{\theta} \right\rfloor \times \theta + \frac{3\theta}{4}, \text{if } w_i = 1, \end{cases} \quad (7)$$

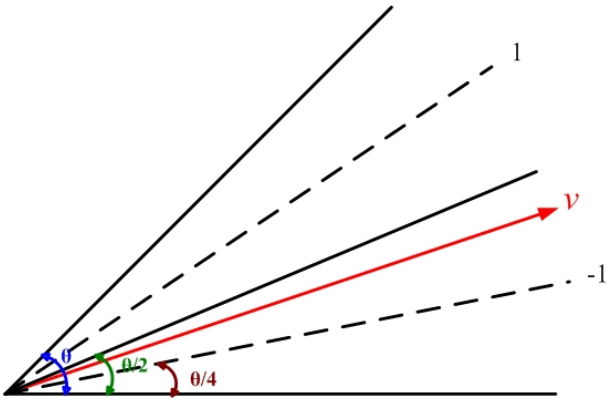
where w_i is the i-th watermark bit. Figure 3 shows the embedding conception. Finally, the adjusted vector v' can be obtained, shown in Equation (8).

$$v' = (L\cos(\alpha'), L\sin(\alpha')). \quad (8)$$

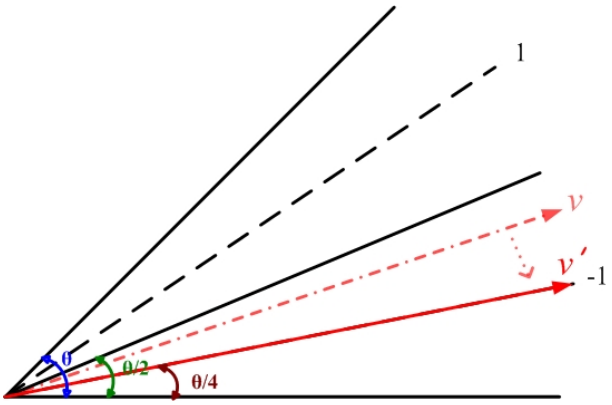
In the extraction process, the angle α' between the vector v' and the x-axis is calculated first. The extracting process is shown in Equation (9).

$$w_i' = \begin{cases} -1, \text{if } \alpha' - \left\lfloor \frac{\alpha}{\theta} \right\rfloor \times \theta \in \left[0, \frac{\theta}{2}\right); \\ 1, \text{if } \alpha' - \left\lfloor \frac{\alpha}{\theta} \right\rfloor \times \theta \in \left[\frac{\theta}{2}, \theta\right), \end{cases} \quad (9)$$

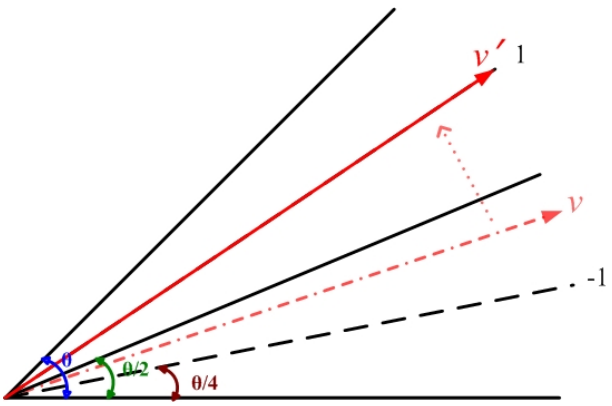
where w_i' is the extracted watermark bit.



(a) The vector v before embedding



(b) After embedding watermark bit -1

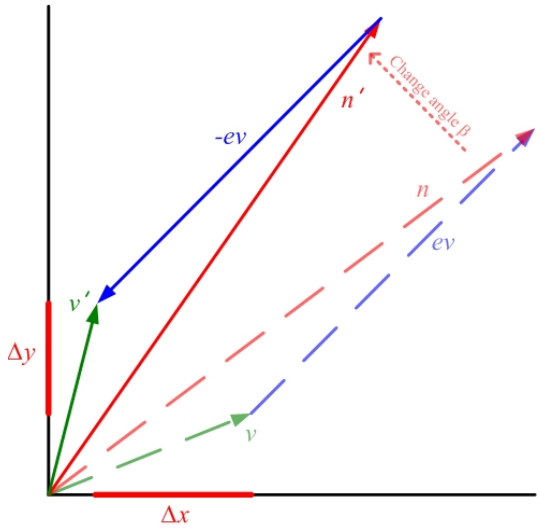


(b) After embedding watermark bit 1

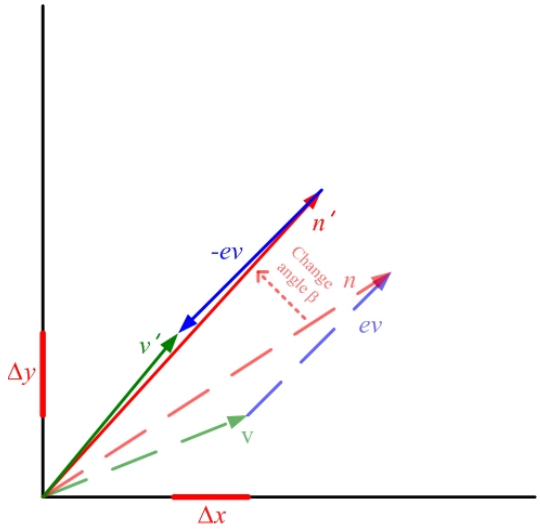
Fig. 3. The embedding conception

2.3: Adjusting Robustness

A vector has two attributes, the direction and the length. The direction is used to embed the watermark, and the length can be used to adjust the robustness. If the adjusted angle is the same, the change of the vector with the longer length will be larger and the robustness will be better.



(a) The result of the extra vector *ev* with longer length



(b) The result of the extra vector *ev* with longer length

Fig. 4. The result of adding extra vectors

For example, assume $v_1 = (100, 100)$ and $v_2 = (500, 500)$. The angles of them are both 45°. After attack, the variations Δx in x-coordinate is 10 and Δy in y-coordinate is 20. Then, the attacked results $v_1' = (90, 80)$ and $v_2' = (490, 480)$ can be obtained, and the attacked angles v_1' and v_2' is about 41.63° and 44.41°, respectively. Therefore, the angle variation of the vector with longer length is smaller for the same change. This property can be used to adjust robustness. A new vector n can be obtained by adding an extra vector ev to the gradient vector v. The adjusted vector n' can be obtained by adjusting the vector n with the angle β. Finally, the adjusted gradient vector can be derived by subtracting the extra vector ev from the adjusted vector n'. From Figure 4, it is observed that the variations Δx in x-coordinate and Δy in y-coordinate are larger if the length of the extra vector ev is longer.

3: Experimental Results and Discussions

The maximum capacity of the watermark is determined by that the watermark is embedded to which level of DWT coefficients. If the watermark is embedded into the higher-level of DWT coefficients, the watermark will be more robust, but it is easy to be observed. It is on the contrary if the watermark is embedded into lower-level DWT coefficient. If the size of the host image is $m \times n$ and the watermark is embedded into i-level DWT coefficients, the maximal capacity of the watermark is $C = (m \times n)/4^i$. In our experiment, the maximal capacity of the watermark is 64 × 64 because the watermark is embedded into the coefficients of three-level DWT decomposition.

In our experiment, two 512 × 512 grayscale images "Lena" and "Pepper" are used as host images, and a 64 × 64 binary image is used as the watermark. The quantization angle is 10°. Attacks for the watermarked image are as follows: JPEG compression (QF = 15), rotation 0.5° (clockwise), rotation 0.5° (anticlockwise), noise addition (variance = 10), rescaling (reduce to 256×256 and restore), blur, sharpness and brightness adjustment. Table 1 shows the results of four watermarked images with the extra vector $ev = (2000, 2000)$ after various attacks. Figures 5 and 6 show watermarked images and the extracted watermarks after various attacks. From the extracted watermark, it can be verified by human vision that the watermark exists after attack. The similarity measure (*SM*) is used to test the performance for the extracted watermark. The definition of *SM* is defined as follows.

$$SM(w, w') = \frac{\sum_{i=0}^{n-1} w_i \times w_i'}{\sqrt{\sum_{i=0}^{n-1} w_i^2}\sqrt{\sum_{i=0}^{n-1} w_i'^2}}, \quad (3.4)$$

where w is the original watermark, w' is the extracted watermark, $w_i, w_i' \in \{1, -1\}$ and n is the size of the watermark.

Table 2 represents the performance for 512 × 512 watermarked image "Lena" (PSNR = 37.38 dB) and 64 × 64 watermark under JPEG compression. The watermark with the extra vector $ev = (2500, 2500)$ is flawless if the quality factor (QF) of JPEG compression is more than 30. Table 3 shows the performance of 512 × 512 watermarked image "Lena" with the different length of the extra vector ev and 64 × 64 watermark under JPEG compression (QF = 15), where the value of x-coordinate is equal to the value of y-coordinate. From

Table 3, it is observed that the performance of resistance against JPEG compression is better if the length of the extra vector *ev* is longer.

Table 4 shows the comparison results with [7] and [8]. The 512 bits watermark is embedded into 256 × 256 grayscale image "Lena" with the extra vector *ev* = (2500, 2500), and the PSNR of the watermarked image is 40.00dB. As a result, the quality of the watermarked image in our scheme is worse than [8], but the robustness of noise addition is close and the performance against other attacks is better.

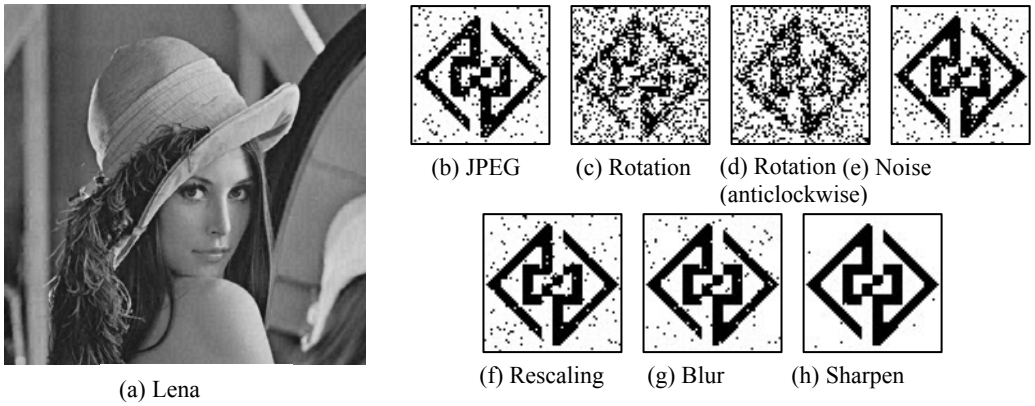


Fig. 5. The watermarked image "Lena" and extracted watermarks

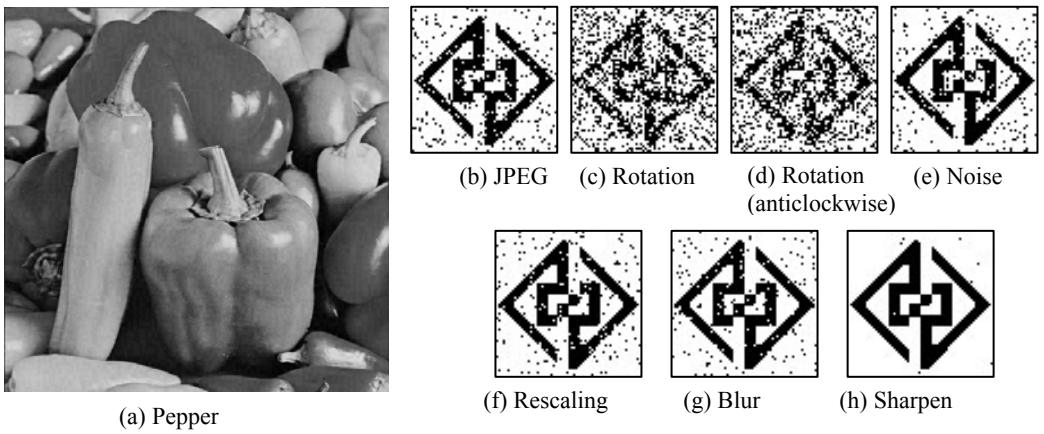


Fig. 6. The watermarked image "Pepper" and extracted watermarks

Table 1. The attack results with the extra vector *ev* = (2000, 2000)

	PSNR (dB)	JPEG	Rotation (clockwise)	Rotation (anticlockwise)
Lena	39.20	0.88	0.54	0.55
Pepper	38.87	0.86	0.52	0.53
Tiffany	39.30	0.82	0.54	0.54
	Noise	**Rescaling**	**Blur**	**Sharpen**
Lena	0.88	0.94	0.96	0.99
Pepper	0.87	0.91	0.92	0.99
Tiffany	0.84	0.93	0.90	0.98

Table 2. The performance of the watermarked image "Lena" under different QF of JPEG compression

Quality factor	50	40	30	20	10
SM	1	1	1	0.99	0.64

Table 3. The performance of the watermarked image "Lena" with different length of extra vector under JPEG compression

Extract vector	1500	1750	2000	2250	2500
PSNR (before compression)	41.20	40,25	39.20	38.24	37.38
SM	0.57	0.74	0.85	0.94	0.95

Table 4. The performance of the watermarked image "Lena" with different length of extra vector under JPEG compression

	JPEG (QF=10)	**Noise (variance=20)**	**Rescaling (reduce to 128×128 and restore)**	**Blur**	**Sharpen**	**Brightness adjustment**
Conventional quantization [7]	0.15	0.27	0.46	0.28	0.61	0.72
Mean quantization [8]	0.62	0.53	0.61	0.84	1	1
The proposed method	0.71	0.51	0.89	0.91	1	1

4: Conclusions

Our proposed method, based on quantifying the angle of the vector, provides an efficient and highly robust watermarking technique. The DWT coefficients in HL subband and LH subband are used to form the vector. The length of the extra vector *ev* is used to adjust the relation between the robustness and the image quality. The watermark is embedded by changing the direction of the vector. From the experimental results, it is confirmed that our proposed scheme is robust under JPEG compression, and has a better performance to resist geometrical attacks of rotation and rescaling. The concept of our proposed scheme can be used not only on the digital images but on digital multimedia as well. By the same token, the watermark can be embedded into signals of the multimedia.

5: References

[1] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information hiding - a survey", *Proceedings of the IEEE*, Vol. 87, No. 7, 1999, pp. 1062-1078.

[2] P. W. Wong and N. Memon, "Secret and public key image watermarking schemes for image authentication and ownership verification", *IEEE Transactions on Image Processing*, Vol. 10, No. 10, 2001, pp. 1593-1601.

[3] C. T. Li, "Digital fragile watermarking scheme for authentication of JPEG images", *IEE Proceedings - Vision, Image and Signal Process*, Vol. 151, No. 6, 2004, pp. 460-466.

[4] P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 15, No. 1, 2005, pp. 96-102.

[5] Y. T. Wu and F. Y. Shih, "An adjusted-purpose digital watermarking technique", *Pattern Recognition*, Vol.37, 2004, pp. 2349-2359.

[6] S. H. Wang and Y. P. Lin, "Wavelet tree quantization for copyright protection watermarking", *IEEE Transactions on Image Processing*, Vol. 13, No. 2, 2004, pp.154-165.

[7] D. Kundur and D. Hatzinakos, "Digital watermarking using multiresolution wavelet decomposition", *Proceedings of the International Conference on Acoustic, Speech and Signal Processing*, Seattle, Washington, USA, 1998, pp. 2969-2972.

[8] L. H. Chen and J. J. Lin, "Mean quantization based image watermarking", *Image and Vision Computing*, Vol.21, 2003, pp. 717-727.

[9] W. Bender, D. Gruhl, N. Morimoto and A. Lu, "Techniques for Data Hiding", *IBM System Journal*, Vol. 35, No. 3-4, 1996, pp. 313-337.

[10] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "Copyright protection of digital images by embedded unperceivable marks", *Image and Vision Computing*, Vol.16, 1996, pp. 897-906.

[11] P. Moulin, "The role of information theory in watermarking and its application to image watermarking", *Signal Processing*, Vol. 81, 2001, pp. 1121-1139.

[12] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform", *IEEE Transactions on Image Processing*, Vol. 13, No. 8, 2004, pp.1147-1156.

[13] Y. Wang, A. Pearmain, "Blind image data hiding based on self reference", *Pattern Recognition Letters*, Vol. 25, 2004, pp. 1681-1689.