A Robust Watermarking Technique for Copyright Protection Using Discrete Wavelet Transform

WEN-TZENG HUANG [1], SUN-YEN TAN [2], YUAN-JEN CHANG [3], CHIN-HSING CHEN [3]

[1] Department of Computer Science and Information Engineering
Mingsin University of Science and Technology
No.1, Xinxing Rd., Xinfeng Hsinchu 30401, Taiwan, R.O.C.
wthuang@must.edu.tw

[2] Department of Electronic Engineering
National Taipei University of Technology
No. 1, Sec. 3, Chung-hsiao E. Rd., Taipei,10608, Taiwan, R.O.C.
sytan@ntut.edu.tw

[3] Department of Management Information Systems
Central Taiwan University of Science and Technology
No.666, Buzih Road, Beitun District, Taichung City 40601, Taiwan, R.O.C.
{ronchang, chchen }@ctust.edu.tw

Abstract- The arrival of digital world coming soon, the digital media content can be easily altered, duplicated, and spread, which causes the copyright of media are violated. Therefore, attention is to discuss the protection of the intellectual property (IP) rights of digital media. Then, the digital watermarking can be a simple and effective approach to provide copyright protection of IP. In this study, a method of robustness and blind extraction watermark for static images is proposed. It utilizes discrete wavelet transform and applies three coding methods according to the different characteristics of band coefficients: lattice code based on the communication principle, modification of insignificant coefficients based on the just-noticeable distortion of the human visual model, and quantization index modulation based on singular value decomposition. Together, these methods embed a watermark while maintaining image fidelity. From our experimental results in this study, all of them can indicate that the proposed approach is high robust against frequency-based and time domain geometric attacks. Additionally, since our approach produces a blind watermark and thus neither the original image nor any of its related information is needed, it is a very convenient and practical watermarking technique for applications.

Keywords: Digital watermark, Discrete wavelet transform, Copyright protection, Blind watermark, Watermark Extraction procedure.

1 Introduction

Komatsu and Tominaga first proposed the term of the digital watermark in 1988 [1]. The technique of the digital watermark had more studies and applications fields till 1990 [2]. The major purpose of the digital watermark is to effectively provide the copyright protection [24] of intellectual property, which is thoroughly protected by law to ensure that the rights of original authors are not violated by others. There are three parts, the watermark embedding, watermark extraction, and verification watermark, within the technique of one typical digital watermark. The structure of the watermark embedding, that the original image, watermark logo, and key are embedded within the embedded image, is shown in Fig. 1. Then, the structure of the watermark and extraction and verification is shown in Fig. 2. The operation of watermark extraction can be gotten from the original image, embedded image,

and key. After getting the extract watermark, the watermark extraction can be gotten by comparing the correlation between the original watermark and extract one.

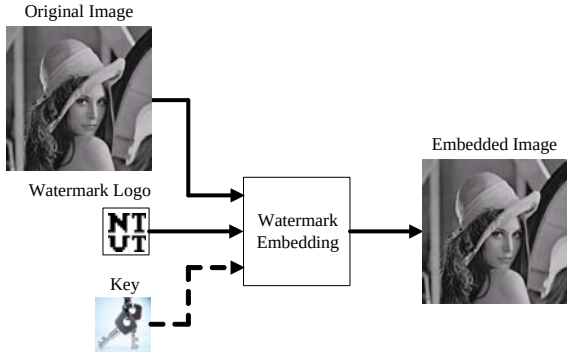

Fig.1. The diagram of the watermark embedding.

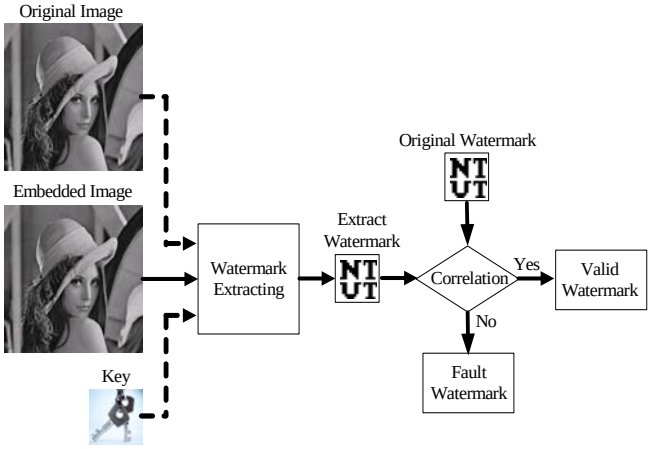

Fig.2. The diagram of the watermark extraction and verification.

However, while all materials that take time and effort to produce qualify for protection, it is becoming increasingly difficult to prove who created a given work in the current digital era. Due to the rapid development of information and computer technologies, more and more information is presented in digital form, which is very easy to duplicate, store, and revise. The Internet also makes digital materials easy to distribute. In addition, digital works can be pirated, and any signatures or other markings used to identify them can be easily altered. This has led to an "epidemic" of unauthorized materials being spread via the Internet without the consent of the original authors, which in many cases has caused huge damage to the owners of such works. Therefore, it is important to develop different methods for enhancing the protection of intellectual property. Digital watermarks are one such technique [1]. Watermarking technology can be used to hide discernible copyright information in target media efficiently and cheaply, and if a problem arises, one can retrieve the information to prove who the legal owner is.

The remainder of this paper is organized as follows. In Section 2, we briefly review the literature on digital watermarks. In Section 3, we describe our proposed method for embedding watermarks in images. Section 4 describes an experiment we conducted to test our method, presents the results, and compares them to previous methods. Finally, we summarize our conclusions in Section 5.

2 Digital watermark

In 1997, Cox *et al.* [2] proposed using the spread spectrum of communication to embed a digital watermark in an image. In this concept, the original image is a channel for communication and watermarking uses this channel to deliver information. It utilizes random serial numbers generated by Gaussian-spreading numeric code, and then uses these numbers as alternating (AC) parameters for a discrete cosine transform (DCT) function. This method successfully resists common media/digital attacks. However, it requires information from the original image to retrieve the watermark; that is, it is a non-blind watermark. In 2004, Wang and Lin [3] proposed a new method using coefficients derived from discrete wavelet transform (DWT). In this scheme, all wavelet coefficients are grouped into "data trees" that are further organized into a larger structure called a super tree. It quantizes the coefficients in the super tree and embeds a watermark bit in every tree pair. Because the quantized coefficients are numerically different from all non-quantized data, they can be used to detect the watermark. This method requires no information from the original image; that is, it is a blind watermark. The virtue of this method is that it can detect the watermark even after attacks such as image compression and space filtering. However, some degradation of image quality occurs. In 2006, Yu and Liu [4] proposed a blind marking method that uses the error ranges of DCT and inverse DCT to define an embedding threshold for modifying watermark coefficients. It uses the maximum transform error to define the extract threshold to avoid the error caused by DCT, and resists common image processing and geometry scaling. However, it also damages the image quality.

Moreover, Hien *et al.* [5] proposed a watermarking approach by redundant discrete wavelet transform (RDWT) and independent component analysis (ICA). This method belongs to a blind watermarking which extracts the watermark without original information. For watermark security reason, embedded logo watermarks are encrypted to random noise signal. To embed logo watermarks, the original image is decomposed by RDWT, and watermarks are embedded into middle frequency at LH and HL sub-bands. The perceptual model is applied with a stochastic multi-resolution model for adaptive watermark embedding.

Ni *et al.* [6] developed a reversible data hiding algorithm which can recover the original image without any distortion from the marked image after the hidden data have been extracted. This algorithm adjusts histogram by shifting the specific value right. Furthermore, a lossless data hiding scheme (i.e., reversible data hiding) is presented that the watermark are embedded into the integer wavelet domain. Their computational complexity of proposed technique was low and the execution time was short. Hence, their proposed algorithm has been successfully applied to a wide range of images, including commonly used images, medical images, texture images, aerial images and all of the 1096 images in CorelDraw database. Zou *et al.* [7] proposed scheme can be integrated into the JPEG2000 standard smoothly. That is, they proposed a semi-fragile lossless digital watermarking scheme based on integer wavelet transform. The wavelet family applied is the 5/3 filter bank which serves as the default transformation in the JPEG2000 standard for image lossless compression. Hence, the original cover image can be losslessly recovered if the stego-image has not been altered. Furthermore, the hidden data can be retrieved even after incidental alterations including image compression have been applied to the stego-image. A statistical aspect of watermark robustness for multiplicative spread-spectrum watermarking was considered by Huang and Zhang [8]. The authors study the robust detection structure for multiplicative watermarking. A detection-simulation (DS)-based approach to determine the contamination factor is also presented. Moreover, considering that the strengths of the watermark signals may be adapted to host signals and will very likely change after being distorted by attacks, we go further to propose the asymptotically robust detector for multiplicative watermarks, which can be viewed as the SR counterpart of the locally most powerful watermark detector in the same sense that the SR detector with full knowledge of the watermark strengths is the corresponding parallel for the optimum detector. Experiments on real images demonstrate the superiority of the new schemes over the conventional ones.

The robust watermark detector was designed to be an optimum detector. For embedding a watermark into color image, a high redundant basis decomposition algorithm has been introduced [9]. The proposed approach decomposes the image into a set of feature bases which can hide the watermark in the redundant bases. Hence, the image decomposition is randomized thus improving the stego-message undetectability, and making the hidden message undetectable by targeted steganalyzers explicitly developed to exploit the weaknesses. Their security scheme was evaluated by testing it against blind steganalyzers and compared to that of embedding algorithm applied in the pixel domain. Moreover, our earlier paper discussed the discrete wavelet transform based robust watermarking for copyright protection [10].

Therefore, from above literal discussion, since the digital data with many different formats, such as voice, video, static image, and text, the different watermark approaches with different function and characteristic can be applied to their corresponding format, respectively. According to the watermark characteristics, the watermark identification, (the watermark content; the watermark robust; the watermark embedding; the watermark interception) can be divided into the visibility and non-visibility types (the statistics sequence and meaningful image; the strong, fragile, and semi-fragile types; the space and frequency types; the blind, non-blind, and semi-blind types), respectively. Since the digital watermark is one of methods applied to effectively protect the original image of intellectual property, it must own some characteristics, the non-visibility, strong robust, distinctness, security, non-statistics, and non-removability.

3 Proposed watermarking scheme

Our approach is to employ the Discrete Wavelet Transform and three watermark embedding methodologies, Lattice codes encode [2], Just Noticeable Distortion (JND) [11][12][13], and the Quantization Index Modulation (QIM) of Singular Value Decomposition (SVD) [14][6][7], such that our approach of the embedded watermark can increase the higher resistance by various geometry attacks, in this study.

3.1 Lattice Coding

The Lattice code encode discussed in this section, Cox *et al*. [2][15] proposed the concept, which is the watermark as an added external information can be made the information encode of a communication system, in 1999 as shown in Fig. 3. Since the object is want to increase the more resistance of the embedded watermark attacked by loss compression and space filter operations, this concept is adopted in the low-frequency of the image Wavelet transform (LL2) approach.

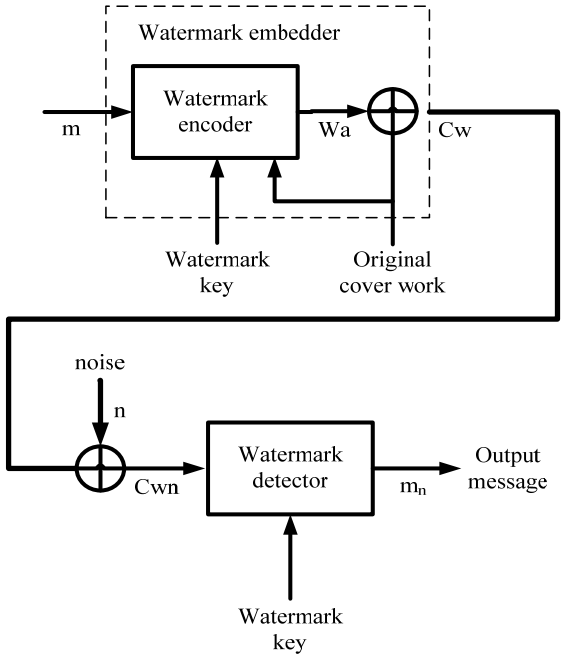

Fig. 3. A watermarking structure as a communication system with the side information.

We employ lattice coding [16], which assumes that reference vectors point to elements. The result of N elements derived from the lattice code can be taken as a set of N reference vectors and a set of integer N elements, as shown in equation (1), where w_r is a set of reference vectors, z is a set of integers, and w_{ri} is an approach (dithered index modulation, [11][12]) to find integers between the vector v and reference vector. To calculate each integer, the length of the vector that projects to w_{ri} is first calculated, as shown in equation (2). Then this vector length is divided by the length of the reference vector w_{ri} to obtain the closest integer to the quotient, as shown in equation (3). To encode with external information, we first need to define the total number of symbols S that are to be encoded, represented as $m[i]$, where $(1 \le i \le N)$ and N is the total number of messages. After adding external information, the closest integer between vector v and the reference vector w_{ri} is determined as shown in equation (4).

$$w_m = \sum_{i=1}^{N} z[i] w_{ri} \tag{1}$$

$$l[i] = \frac{v \cdot w_{ri}}{|w_{ri}|} \tag{2}$$

$$z[i] = \left\lfloor \frac{l[i]}{|w_{ri}|} + 0.5 \right\rfloor = \left\lfloor \frac{v \cdot w_{ri}}{w_{ri} \cdot w_{ri}} + 0.5 \right\rfloor \tag{3}$$

$$z_m[i] = S\left\lfloor \frac{l[i]/\,|\,w_{ri}\,| - m[i]}{S} + 0.5 \right\rfloor + m[i] \tag{4}$$

To adjust embedding robustness, we multiply the reference vector by a robustness parameter β, modifying equation (4) to become equation (5). After calculating $z_m[i]$, the reference vector of the embedded watermark can be derived using equation (6). Adding the results to the original image blocks embeds the watermarks.

$$z_m[i] = 2\left\lfloor \frac{l[i]/\beta|w_{ri}| - m[i]}{2} + 0.5 \right\rfloor + m[i] \tag{5}$$

$$w_a = \beta\, z_m[i] w_{ri} \tag{6}$$

Equation (7) is used to retrieve a watermark using lattice coding. The equation uses the integer z to determine the bit value of the embedded watermark. If z is odd then the watermark bit is 1; otherwise it is 0.

$$z = \left\lfloor \frac{v \cdot w_r}{\beta(w_r \cdot w_r)} + 0.5 \right\rfloor \tag{7}$$

3.2 Adjustment Coefficients Based on DWT Domain Just-Noticeable Distortion

There are four wavelet bands, namely low frequency low frequency (LL), high frequency low frequency (HL), low frequency high frequency (LL), high frequency high frequency (HH), of the wavelet transform [13][14][17][25]. In this section, we describe watermarking that uses just-noticeable distortion, which determines threshold values in the wavelet subbands, HL2 and LH2, and then uses them to embed watermarks [13][14][17]. The purpose of JND is to adjust the gray level or coefficient to the

maximum value that cannot be detected by the human eye [13]. It is based on four factors related to the noise sensitivity of the human eye: background luminance, edge proximity, band sensitivity, and texture masking.

Equations (8)–(11) calculate the JND value from four input parameters, where r, s, x, and y represent the scale $r \in \{0,1,2,3\}$ and wavelet band $s \in \{LL, LH, HL, HH\}$ of the wavelet transform, based on the x and y coordinates of the wavelet coefficients, and α is a constant. Equation (9) is based on the mathematical model of the Human Vision System (HVS), which images content under different frequencies [18]. Added this equation defines changes in luminance and hue, based on the sensitivity of the human eye, in different wavelet transform levels and wavelet bands. Equation (10) is based on Weber's law [6] and assumes that human eyes are less sensitive to changes in noise when viewing an object against a bright background. Equation (11) assumes that human eyes are less sensitive to noise changes against high-density textures. The sum of the luminance variable in the low-frequency band and the edge variance in the high-frequency band determines the texture of an image [19].

$$JND(r,s,x,y) = \alpha \cdot frequency(r,s) \cdot bright(r,x,y) \cdot texture(r,x,y)^{0.034} \quad (8)$$

$$frequency(r,s) = \begin{Bmatrix} \sqrt{2}, & \text{if s = HH} \\ 1, & \text{otherwise} \end{Bmatrix} \cdot \begin{Bmatrix} 1.00, & \text{if r = 0} \\ 0.32, & \text{if r = 1} \\ 0.16, & \text{if r = 2} \\ 0.10, & \text{if r = 3} \end{Bmatrix} \quad (9)$$

$$bright(r,x,y) = 3 + \frac{1}{256}\sum_{i=1}^{2}\sum_{j=1}^{2} I^{r,LL}(i+x, j+y) \quad (10)$$

$$texture(r,x,y) = \sum_{k=0}^{3-r}\sum_{s}^{LH,HL,HH}\sum_{i=1}^{2}\sum_{j=1}^{2} \frac{\left(I^{k+r,s}\left(i+\left\lfloor\frac{x}{2^k}\right\rfloor, j+\left\lfloor\frac{y}{2^k}\right\rfloor\right)\right)^2}{16^k} + \sigma^2(I^{r,LL}(\{1,2\}+x,\{1,2\}+y)) \quad (11)$$

JND-based watermarking assumes that most wavelet coefficients will be close to zero in the frequency bands HL2 and LH2. We calculate the JND values for the HL2 and LH2 bands and use the smallest JND as the embedding threshold value. If the absolute value of the wavelet coefficient is greater than the threshold, then that coefficient is considered an important one; otherwise it is defined as an unimportant coefficient. To embed a watermark, we separate HL2 and LH2 into 8 × 8 blocks, each with 64 wavelet coefficients. The wavelet coefficients are modified according to the value of each watermark bit. If a watermark bit is equal to 1, then the first 32 unimportant coefficients are replaced by the corresponding JND values and the polarity is left unchanged. Otherwise, the last 32 unimportant coefficients are modified. To extract the watermark bit, we calculate the first 32 and last 32 coefficients in each block. If the number of unimportant coefficients in the first 32 coefficients is less than those in the last 32 coefficients, then the embedding watermark bit is identified as 1; otherwise it is identified as 0.

3.3 Watermarking using Singular Value Decomposition Quantization Index Modulation

Equation (12) describes an N × N image *A* based on three N × N singular value decomposition matrixes, where U and V are two orthogonal matrixes. If A is symmetric, U will be equal to V. The diagonal component of matrix S is the eigenvalue of A. This eigenvalue is a singular value composed of N nonzero singular values, organized in decreasing numerical order from the top left to the bottom right of the matrix. SVD has an intriguing mathematical virtue, whereby a singular value represents the luminance of a target image and U and V represent the geometry of the image: a bigger singular value will not only maintain image intensity better but will also be most robust against attacks. Also, a slight change to a singular value will not be noticed by the human eye [20].

$$A = USV^T \quad (12)$$

To embed watermark bits using a SVD QIM, we separate the HH1 subband into 16 × 16 blocks, decompose each block with SVD, and then calculate the Euclidean distance d of the diagonal singular matrix using equation (13). Equation (14) is used to obtain integer z, where qs is a constant representing the quantized step. The bigger the qs is, the more robust the watermark will be. The integer z is modified according to the watermark bits. If a bit is equal to 1, then z is an odd value; otherwise it is an even value. Then equation (15) is used to calculate a new Euclidean distance d', and equation (16) is used to calculate each singular value λ' in each matrix.

Finally, equation (17) is used to modify each singular value and perform a SVD inverse transform. This new block is embedded as a watermark bit. To extract watermark bits using SVD QIM, the Euclidean distance of each singular value is dividing by the quantized step to determine integer z. This procedure is the same as the embedding procedure. If integer z is an odd number, the embedded watermark bit is 1; otherwise it is 0.

$$d = \|v\| + 1, \text{ where } v = (\lambda_1, \lambda_2, ..., \lambda_N) \quad (13)$$

$$z = \lfloor d / qs \rfloor \quad (14)$$

$$d' = qs \times z + qs/2 \quad (15)$$

$$(\lambda_1', \lambda_2', ..., \lambda_N') = (\lambda_1, \lambda_2, ..., \lambda_N) \times d'/d \quad (16)$$

$$\tilde{C} = \sum_{i=1}^{N} \lambda_i' U_i V_i^T \quad (17)$$

Fig.4. Watermark logo permutation by the Arnold's cap map operation.

3.4 Arnold's Cap Map

Arnold's cap map [18] is an important encryption technique used to improve the security of digital watermarks. It exhibits periodicity depending on the size of a watermark logo, whereby after several transform processes, the logo will revert back to the original one. Arnold's cap map is defined in equation (18).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix} \bmod N, \quad (x, y \in \{0,1,2,...,N-1\}) \quad (18)$$

where x and y are the coordinates of a pixel in the original watermark logo, x' and y' are the new coordinates after the transform process, and N is the total pixel number. Fig. 4 shows the process of Arnold's cap map. Assuming that the watermark image can recover over I transform processes, we define I as the Arnold's cap map period of a watermark logo. Before starting the embedding process, we can perform *t* repetitions of Arnold's cap map as a scramble process. To recover the watermark, $I - t$ repetitions of Arnold's cap map must be performed after finishing the retrieving process. So it can be viewed as a key for retrieving the watermark.

3.5 Watermark Verification

To verify an extracted watermark, we use normalized correlation (NC) as shown in equation (19), where W and W' are the original and extracted watermarks, respectively. Because we use a {1,–1} serial array to represent watermark bit values, (19) can be simplified into equation (20), where N_w is the number of watermark bits.

$$NC(W, W') = \sum_{m=1}^{N_w} w_m w'_m \Big/ \sqrt{\sum_{m=1}^{N_w} w_m^2 \sum_{m=1}^{N_w} w'^2_m} \quad (19)$$

$$NC(W, W') = \sum_{m=1}^{N_w} w_m w'_m / N_w \quad (20)$$

The closer the resulting NC value is to 1, the higher the similarity will be between the extracted and original watermark.

3.6 Watermark Embedding Procedure

1. Convert watermark binary W into a {1,–1} sequence, then apply Arnold's cap map transform to rearrange W by the embedded key.
2. Apply two-level DWT decomposition to the original image, then divide each LL2, LH2, and HL2 subband into 8 × 8 blocks and each HH1 subband into 16 × 16 blocks, where Ci {i=1,2,3…,*N*} and *N* is the number of blocks.
3. Set the embedding parameters, the β of lattice coding, and the quantized step qs of the SVD QIM method, and calculate the JND of the LH2 and HL2 subbands.
4. For i=0 to *N* –1
   if s=LL2 then
   Lattice_encode(Ci, Wi, β);
   else if s=LH2 or s=HL2 then
   Coefficients_Adjust(Ci,Wi, JNDi);
   else if s=HH1 then
   SVD_QIM_encode(Ci, Wi, qs);
   end if
   end for
5. Let *T* be the smallest JND value as a threshold for the extraction procedure, then apply an inverse two-level DWT to obtain the watermarked image.

3.7 Watermark Extraction Procedure

1. Apply two-level DWT decomposition to the watermarked image, divide each LL2, LH2, and LH2 subband into 8 × 8 blocks and each HH1 subband into 16 × 16 blocks, where Ci {i=1,2,3…,*N*}and *N* is the number of blocks.
2. For $i = 0$ to $N-1$
   if s = LL2 then
   $W1i$ = Lattice_decode(Ci , β);
   else if s=LH2 or s=HL2 then
   $W2i$ = Coefficients_Compare(Ci , T);
   else if s=HH1 then
   $W3i$ = SVD_QIM_decode(Ci, qs);
   end if
   end for
3. Apply Arnold's cap map transform using the embedding key to obtain the original watermark.

4 Experimental results

The minimum Mean Square Error (MSE) and the Peak Signal-to-noise Ratio (PSNR) [22][23] are used to evaluate the similarity degree between the original image and embedded watermark image one as shown in equations (21) and (22) [26]. High PSNR is high similarity degree between the original image and embedded watermark image one.

$$MSE = \sum_{i=1}^{height} \sum_{j=1}^{width} (I_{ij} - I_{ij}')^2 / size(I) \qquad (21)$$

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \ \text{(dB)} \qquad (22)$$

The watermark used in this experiment was a 256-bit binary image as shown in Fig. 5. After the Arnold's cap map process, we presented it with a {1,–1} series and then embedded it into a 512 × 512 Lena grayscale image as shown in Fig. 6. To demonstrate the robustness of the proposed watermarking scheme, we performed seven different attacks on the watermarked image and then compared the results to previous watermarking schemes [3][4][21]. The experimental results are presented in Figures 7–13. The watermark produced by our proposed scheme performed much better than those produced by previous methods.

Fig.5. Watermark logo.

The different JPEG compression operations with the quality coefficients and compression rate are employed in the embedded watermark of our experiments. The loss of the image quality with lower compression quality coefficient and higher compression rate is more serious. The robust degree test of Lena with after JPEG compression operations with different parameters in our approach is shown in Table 1. Then, compared with other methods, the NC curves of Lena attacked by JPEG are shown in Fig. 7. From our results, while the JPEG compression rate is 25 in our approach, the extraction Lena can be clear identified by the vision.

Fig.6. The watermarked Lena image of our experiments.

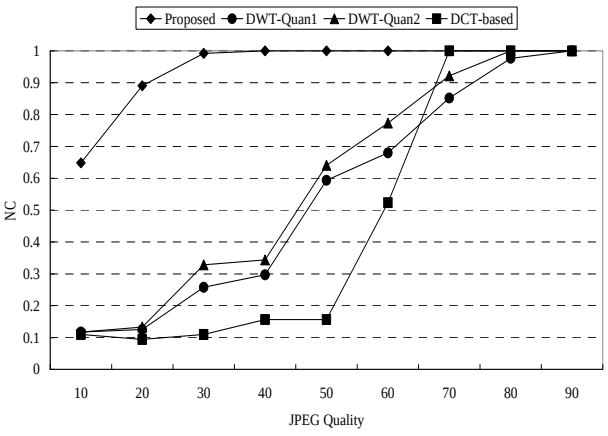

Fig.7. The NC curves of Lena attacked by JPEG.

The robust degree test of Lena with after JPEG2000 compression operations with different bit-rates in our approach is shown in Table 2. Comparing with other methods and the NC curves of Lena attacked by JPEG2000 are shown in Fig. 8. Table 3 shows that the robust degree test of Lena after medium filter operations with 3 mask sizes in our approach. Comparing with other methods and the NC curves of Lena attacked by the medium filter operation with different mask sizes are shown in Fig. 9.

Table 1. The robust degree test of Lena after JPEG compression operation with different quality coefficients and compression rates in our approach.

Quality Coefficient	Compressed rate	PSNR (dB)	NC	Extraction
70	8.66	37.00	1	
50	12.21	35.60	1	
30	17.06	34.16	0.99	
20	21.88	32.90	0.89	
15	25.93	31.91	0.79	
10	32.74	30.39	0.65	

Table 2. The robust degree test of Lena with after JPEG2000 compression operation with different bit-rates in our approach.

Compression bit rate	PSNR (dB)	NC	Extraction
1.5	39.95	1	
1.0	38.51	1	
0.75	37.69	0.96	
0.5	36.09	0.91	
0.3	33.89	0.63	
0.15	30.90	0.32	

Table 3. The robust degree test of Lena after the medium filter in our approach.

Mask sizes	PSNR (dB)	NC	Extraction
3x3	33.67	0.96	
5x5	29.61	0.70	
7x7	27.52	0.51	

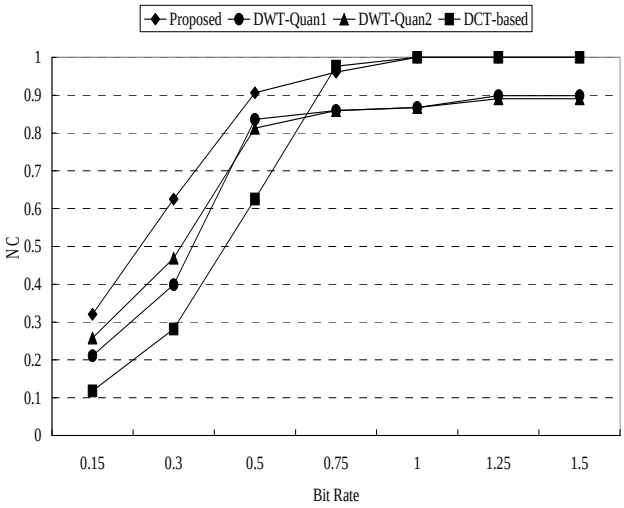

Fig.8 The NC curves of Lena attacked by JPEG2000.

Table 4 shows that the robust degree test of Lena after the Gaussian filter operation with 3 mask sizes in our approach. Then, compared with other methods, the NC curves of Lena attacked by Gaussian filter operation with different mask sizes are shown in Fig. 10. Table 5 shows that the robust degree test of Lena after the scaling geometry operations in our approach. Then, compared with other methods, the NC curves of Lena attacked by scaling geometry operation with different mask sizes are shown in Fig. 11.

Table 4. The robust degree test of Lena after the Gaussian filter operation in our approach.

Mask sizes	PSNR (dB)	NC	Extraction
3x3	35.00	0.98	
5x5	33.30	0.95	
7x7	33.14	0.95	

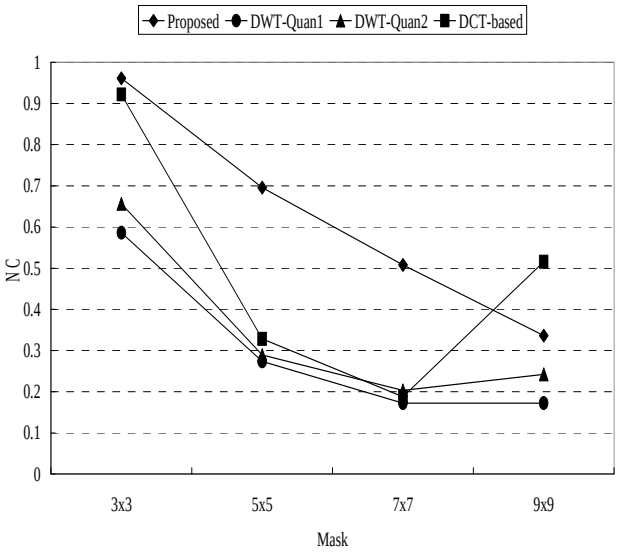

Fig.9 The NC curves of Lena attacked by a medium filter.

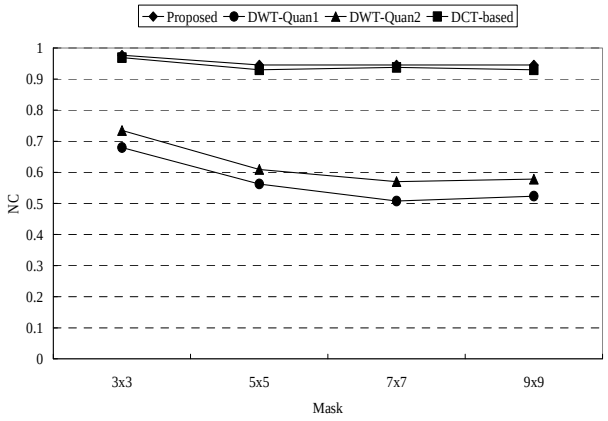

Fig.10 The NC curves of Lena attacked by a Gaussian filter.

Table 6 shows that the robust degree test of Lena after the rotation geometry operation in our approach. Then, compared with other methods, the NC curves of Lena attacked by rotation geometry operation with different angles are shown in Fig. 12.

Table 7 shows that the robust degree test of Lena after the Gaussian noise operation with different variances in our approach. Then, compared with other methods, the NC curves of Lena attacked by Gaussian noise operation with different variances are shown in Fig. 13.

Table 5. The robust degree test of Lena after the scaling geometry operations in our approach.

Scaling ratio	PSNR (dB)	NC	Extraction
85%	33.29	0.95	
70%	30.44	0.88	
50%	28.17	0.84	

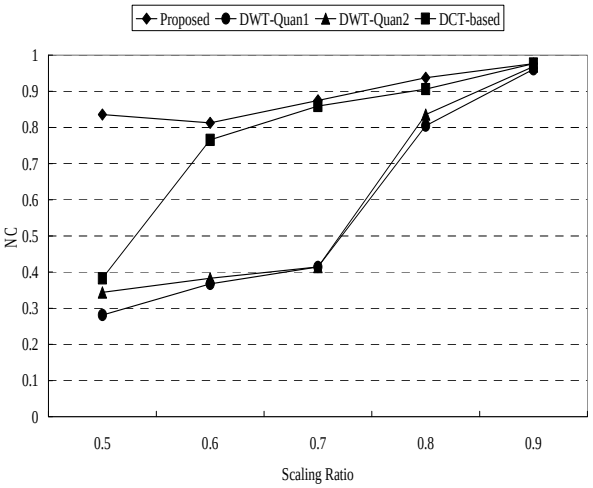

Fig.11 The NC curves of Lena attacked by scaling.

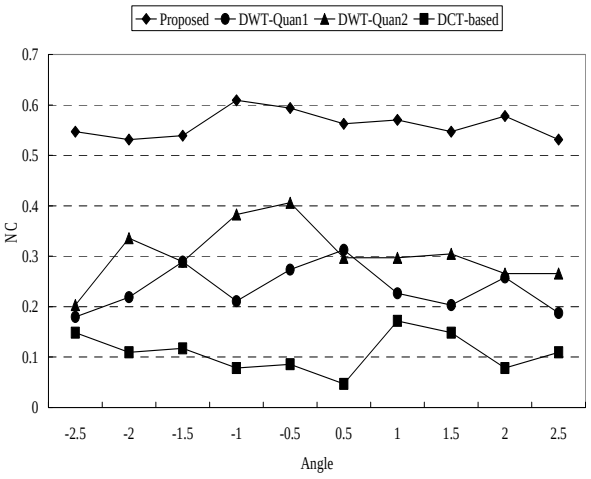

Fig.12. The NC curves of Lena attacked by rotation.

Table 6. The robust degree test of Lena after the rotation geometry operation in our approach.

Rotation angle	PSNR (dB)	NC	Extraction
0.5	22.20	0.56	
1.5	19.04	0.55	
2.5	17.11	0.53	
-0.5	21.66	0.59	
-1.5	19.10	0.54	
-2.5	17.32	0.55	

Table 7. The robust degree test of Lena after the Gaussian noise operation in our approach.

Variance	PSNR (dB)	NC	Extraction
0.001	29.90	1	
0.003	25.25	0.82	
0.005	23.09	0.71	

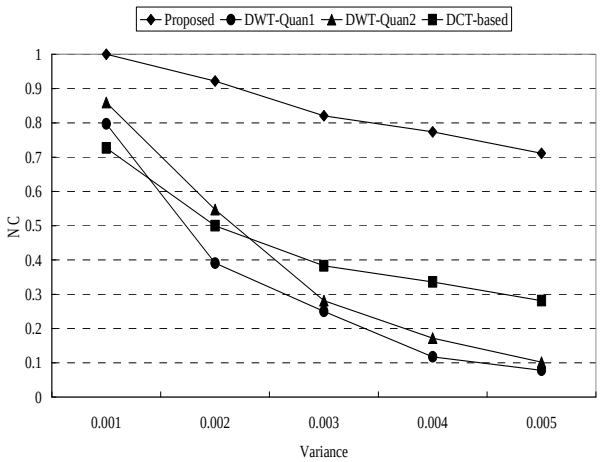

Fig.13. The NC curves of Lena attacked by adding Gaussian noise.

5 Conclusion

A robust, blind watermarking method was presented in this paper. It embeds a watermark using a gray-level image to perform two-level wavelet transform and modify wavelet coefficients using four different methods according to the differences in wavelet coefficients on different wavelet subbands. According to the results of an experiment, our method improves the robustness of watermarks. Our method has the following features: it only slightly modifies wavelet parameters, minimizing image degradation; it provides better protection against various attacks; it makes watermarking more convenient and practical because no information from the original image is needed for authentication.

Acknowledgements

The authors would like to thank the National Science Council of the Republic of China for financially supporting this research under Contract NSC 98-2221-E-166-008- and NSC 98-2218-E-320-001-.

References

[1] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital watermarking, Morgan Kaufmann Publishers Inc.*, San Francisco, CA, USA, 2002.

[2] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Transactions on Image Processing*, Vol. 6, 1997, pp. 1673-1687.

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

[4] P. Yu and B. Liu, Public watermarking algorithm based on the polarity of DCT coefficients, *IEEE Proceedings of the 6th International Conference on Intelligent Systems Design and Applications*, 2006.

[5] T. D. Hien, Z. Nakao, and Y. W. Chen, Robust Multi-logo Watermarking by RDWT and ICA, *Signal Processing*, Vol. 86, No. 10, 2006, pp. 2981-2993.

[6] Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, Reversible Data Hiding, *IEEE Transactions On Circuits and System for Video Technology*, Vol. 16, No. 3, 2006, pp. 354-362.

[7] Dekun Zou, Yun Q. Shi, Zhicheng Ni, and Wei Su, A Semi-Fragile Lossless Digital Watermarking Scheme Based on Integer Wavelet Transform, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 16, No. 10, 2006, pp. 1294-1300.

[8] Xingliang Huang, and Bo Zhang, Statistically Robust Detection of Multiplicative Spread-Spectrum Watermarks, *IEEE Transactions on Information Forensics and Security*, Vol. 2, No. 1, 2007, pp. 1-13.

[9] Giacomo Cancelli and Mauro Barni, MPSteg-Color: Data Hiding Through Redundant Basis Decomposition, *IEEE Transactions on Information Forensics and Security*, Vol. 4, No. 3, 2009, pp. 346-358.

[10] Wen-Tzeng Huang, Sun-Yen Tan, Yuan-Jen Chang, Chin-Hsing Chen, A Discrete Wavelet Transform Based Robust Watermarking for Copyright Protection, Proceedings of the 12th International Conference on Networking, VLSI and Signal Processing (ICNVS '10), Feb., 2010, pp.39-43.

[11] B. Chen and G. W. Wornell, An information-theoretic approach to the design of roust digital watermarking systems, *IEEE Conference on Acoustics, Speech, and Signal Process*, Vol. 4, 1999, pp. 2061-2064.

[12] B. Chen and G. W. Wornell. Digital watermarking and information embedding using dither modulation, *IEEE Second Workshop on Multimedia Signal Processing*, 1998, pp. 273-278.

[13] A. S. Lewis and G. Knowles, Image compression using the 2-D wavelet transform, *IEEE Transactions on Image Processing*, Vol. 1, No. 2, April 1992, pp. 244-250.

[14] M. Bertran, J. F. Delaigle, and B. Macq, Some improvements to HVS models for fingerprinting in perceptual decompressors, *in Proceedings of the IEEE International Conference on Image Processing (ICIP'01)*, Vol. 3, Oct. 2001, pp. 1039-1042.

[15] G. Buchsbaum, An analytical derivation of visual nonlinearity, *IEEE Transactions on biomedical engineering*, Vol. 27, 1980, pp. 237-242.

[16] J. Cox, M. L. Miller, and A. McKellips, Watermarking as communications with side information, *Proceedings of the IEEE*, Vol. 87, No. 7, July 1999, pp. 1127-1141.

[17] 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, January 2005.

[18] G. Peterson, *Linear Algebra*, Arnold's cat map, 1997.

[19] A. B. Watson and J. A. Solomon, A model of visual contrast gain control and pattern masking, *Journal of the Optical Society of America*, 1997, pp. 2377-2391.

[20] A. Shnayderman, A. Gusev, and A. M. Eskicioglu, An SVD-based grayscale image quality measure for local and global assessment, *IEEE Transactions on Image Processing*, Vol. 15, No. 2, February 2006, pp. 422-429.

[21] X. Niu, E. Li, and H. Liang, Blind image watermarking scheme based on wavelet tree quantization robust to geometric attacks, *IEEE Proceedings of the 6th World Congress on Intelligent Control and Automation*, June 2006.

[22] Y. Zhang, Blind Watermark Algorithm Based on HVS and RBF Neural Network in DWT Domain, *WSEAS Transactions on Computers*, Issue 1, Volume 7, January 2008, pp.174-183.

[23] P. Kumsawati, K. Attakitmongcol, and A. Srikaew, An Optimal Robust Digital Image Watermarking Based on Genetic Algorithms in Multiwavelet Domain, *WSEAS Transactions on Signal Processing*, Issue 1, Volume 5, January 2009, pp. 42-51.

[24] Y-S. Lee, H.-J. Kang, and Y.-H. Kim, A Study on the Copyright Protection using Watermarking Technique in Power Line Communication Network, *Proceedings of the 5th WSEAS International Conference on Applications of Electrical Engineering*, Prague, Czech Republic, March 12-14, 2006, pp. 65-68.

[25] K.-M. Hung, Y.-T. Wang and C.- H. Yeh, A Robust Watermarking Technique for Copyright protection of digital images, *Proceedings of the 2007 WSEAS International Conference on Computer Engineering and Applications*, Gold Coast, Australia, January 17-19, 2007, pp. 248-252.

[26] K.-M. Hung, A Novel Robust Watermarking Technique Using IntDCT Based AC Prediction, *WSEAS Transactions on Computers*, Issue 1, Volume 7, January 2008, pp. 16-24.