Robust Image Hashing Scheme Based on DWT and Fuzzy ART

Hung-Jen Wang, Chuan-Yu Chang, Sheng-Wen Pan
Graduate School of Computer Science & Information Engineering
National Yunlin University of Science & Technology, Taiwan
chuanyu@yuntech.edu.tw

ABSTRACT

Media hashing is an important skill for resolving copyright infringement. In this paper, we propose a robust image hashing scheme based on DWT and Fuzzy ART. The proposed scheme, which combines many encouraging characteristics from DWT, Fuzzy ART and quantization process, converts an image into a short and robust hash table. The weakness of Fuzzy ART which is sensitive to noise and outliers can be resolved by DWT. In addition, unlike general classification, such as k-mean, fuzzy c-means and so on, we can suitably decide the number of the clusters according to the vigilance parameter of Fuzzy ART. Experimental results demonstrate that the proposed scheme is robust against common image processing and geometric distortions. Moreover, the original image is not required during extracting the embedded watermark.

1: INTRODUCTION

With the rapid development of multimedia and networking technologies, digital media are easily duplicated and the illegal duplicates are rapidly distributed over the Internet. Therefore, it is a very important and urgent issue to protect the intellectual property rights (IPR) of digital media. Although cryptography can be used to protect secret data, cryptographic algorithm only processes text data rather than digital media. Moreover, it does not provide any security for decrypted data. Consequently, media hashing technology is devised to compensate for the drawback of encryption.

In recent years, media hashing technique has received considerable attention for tracing the unauthorized use of digital content. Media hashing, also termed as fingerprinting, digital signature, or passive/non-invasive watermarking, refers to trace possible duplicates of digital content by a unique hash sequence. In contrast with the conventional digital watermarking, media hashing is non-invasive, which means that no additional information has to be embedded in the digital content. Media hashing is also similar to the content-based retrieval. However, the content-based retrieval attempts to find semantically similar media rather than the duplicated media. In consequence, media hashing must provide additional resistance to unintentional and malicious attacks.

In general, image watermarking can be divided into two categories. One is referred to as spatial domain method which directly modifies the intensity value of the image, and the other is referred to as frequency domain method which changes the frequency coefficients. In the spatial domain, Huang *et al.* [1] proposed an efficient and robust watermarking algorithm with vector quantization (VQ). The characteristics of natural images and the efficient VQ compression technique are used to embed the watermark into the secret key. Hence, the quality of the watermarked image would be guaranteed. To achieve the goal of content authentication and copyright protection simultaneously, Lu *et al.* [2] proposed a multipurpose image watermarking algorithm based on multistage vector quantization. The semi-fragile watermark and the robust watermark are embedded in different VQ stages using different techniques, and both of them can be extracted without the original image. In the frequency domain, Hsu *et al.* [3] proposed an image authentication technique which embeds the watermarks with visually recognizable patterns into the images by selectively modifying the middle-frequency components of the image, so as to get a tradeoff between imperceptibility and robustness. Kundur *et al.* [4] proposed a novel fragile watermarking approach which embeds a watermark in the discrete wavelet domain of the image by quantizing the corresponding coefficients. Chen *et al.* [5] proposed a wavelet-based copyright-proving scheme that does not require the original image for logo verification. Without modifying the original image for certificate generation, this scheme is lossless.

However, the main drawback of existing image watermarking methods is their limited resistance to extensive geometric attacks. In addition, the weakness of multiple watermarking which is initially devised to resist geometric attacks is their inability to withstand the watermark-estimation attacks (WEAs) [6], leading to reduce resistance to geometric attacks. In view of these facts, Lu *et al.* [7] proposed a robust image watermarking scheme that can withstand geometric distortions and WEAs simultaneously. Furthermore, media hashing is also an important skill of resolving copyright infringement. Lu *et al.* [8] also proposed a novel geometric distortion-invariant image hashing scheme, which can be employed to perform copy detection and content authentication of digital images.

In this paper, we propose a robust image hashing scheme based on DWT and Fuzzy ART. The proposed scheme, which combines many encouraging characteristics from DWT, Fuzzy ART and quantization process, converts an image into a short and

robust hash table. Experimental results demonstrate that the proposed scheme is robust against common image processing and geometric distortions. Moreover, the original image is not required in the extraction process.

This paper is organized as follows. In Section 2, we briefly introduce discrete wavelet transformation (DWT) and fuzzy adaptive resonance theory (Fuzzy ART). The proposed scheme is presented in Section 3. Experimental results and discussions are shown in Section 4. Finally, some conclusions are given in Section 5.

2: RELATED WORKS

2.1: DWT

Discrete wavelet transformation is a mathematical tool which can examine an image in time and frequency domain, simultaneously. The image is first decomposed into four subbands denoting LL_1, LH_1, HL_1 and HH_1. The subbands LH_1, HL_1 and HH_1 contain high-frequency component. The subband LL_1 is the low-frequency component containing most of energy in the image. Discrete wavelet transformation can be applied again by further decomposing the subband LL_1 into the subbands LL_2, LH_2, HL_2 and HH_2. If the process is repeated t times, we can obtain the subband LL_t through t-level wavelet transformation.

2.2: FUZZY ART

Fuzzy ART proposed by S. Grossberg is an unsupervised learning network [9]. It can be considered as a modified ART1 neural network which only learns to categorize binary input vectors. By incorporating computations from fuzzy set theory into ART1, Fuzzy ART can be used to categorize both discrete and analog input vectors. For example, the intersection ($\cap$) operator used in ART1 learning is replaced by the MIN operator ($\wedge$) of fuzzy set theory.

3: PROPOSED SCHEME

The variation of low-frequency components is smaller than that of high-frequency components under reasonable attacks. Based on this property, we propose a robust image hashing scheme based on DWT and Fuzzy ART. The proposed scheme, which combines many encouraging characteristics from DWT, Fuzzy ART and quantization process, converts an image into a short and robust hash table. Firstly, the low-low frequency sub-image is obtained through wavelet transformation. Thus, most of noises are excluded for resolving the weakness of Fuzzy ART which is sensitive to noise and outliers. Moreover, the indices among neighboring image blocks possess similarity for natural images. Therefore, we calculate the variance of each index and the indices of its surrounding image blocks, and utilize the concept of the quantization process to construct the hash table. Finally, a watermark is embedded in the hash table, i.e. the quantization interval of the variance.

3.1: HASH GENERATION ALGORITHM

Let the original image X be a gray-level image of size $N_1 \times N_2$, and the watermark W be a binary image of size $M_1 \times M_2$. The original image X and the watermark W are respectively represented as follows.

$$X = \left\{ x_{i,j} \middle| \ 0 \le x_{i,j} \le 255,\ 0 \le i < N_1,\ 0 \le j < N_2 \right\} \quad (1)$$

$$W = \left\{ w_{i,j} \middle| \ w_{i,j} \in \{0,\ 1\},\ 0 \le i < M_1,\ 0 \le j < M_2 \right\} \quad (2)$$

Firstly, the original image can be decomposed to obtain the sub-image LL_t (L for short) through t-level wavelet transformation. Here, L is defined as follows.

$$L = \left\{ l_{i,j} \middle| \ 0 \le l_{i,j} \le 255,\ 0 \le i < \left(N_1/2^t\right),\ 0 \le j < \left(N_2/2^t\right) \right\} \quad (3)$$

To resist geometric distortions, a fast two-dimensional (2-D) pseudorandom permutation [3] generated by seed s is used to permute the watermark to disperse its spatial relationship, i.e.,

$$W' = \left\{ w'_{i',j'} \middle| \ w'_{i',j'} = \mathrm{PRP}_s\left(w_{i,j}\right),\ 0 \le i,\ i' < M_1,\ 0 \le j,\ j' < M_2 \right\} \quad (4)$$

where $\mathrm{PRP}_s(\cdot)$ denotes the pseudorandom permutation function with seed s.

Then, the sub-image L is divided into $M_1 \times M_2$ non-overlapping image blocks B_k with size $\left(\left(N_1/2^t\right)/M_1\right) \times \left(\left(N_2/2^t\right)/M_2\right)$, for $1 \le k \le M_1 \times M_2$, as shown in Eq. (5).

$$L = \bigcup_{k=1}^{M_1 \times M_2} B_k \quad (5)$$

For presentation convenience, we replaced the size of each image block by $m_1 \times m_2$. Accordingly, each image block B_k can be regarded as an input vector with $m_1 \times m_2$ elements. We normalize all input vectors $B_k = \left(B_{k1}, B_{k2}, \ldots, B_{k(m_1 \times m_2)}\right)$ by the largest gray-level of the image pixels, such that each element of input vectors is in the interval $[0, 1]$. Each input vector is expanded to vector I_k with $2 \times m_1 \times m_2$ elements according to complement-coding rule. That is,

$$\begin{aligned} I_k &= \left(B_k, B_k^c\right) \\ &= \left(B_{k1}, B_{k2}, \ldots, B_{k(m_1 \times m_2)}, B_{k1}^c, B_{k2}^c, \ldots, B_{k(m_1 \times m_2)}^c\right) \end{aligned} \quad (6)$$

$$I = \bigcup_{k=1}^{M_1 \times M_2} I_k \quad (7)$$

where $1 \le k \le M_1 \times M_2$ and $B_{kl}^c = 1 - B_{kl}$, for $l = 1, 2, \ldots, m_1 \times m_2$. Then, all input vectors I_k are applied to the Fuzzy ART network for classification. The Fuzzy-ART function produces three outputs, a weight matrix (WM), a codebook (CB), and an index table (IT). The CB consists of codewords, and each codeword is the centroid of each cluster. The IT records the cluster index of each image block.

$$(\mathbf{WM}, \mathbf{CB}, \mathbf{IT}) = \text{Fuzzy}-\text{ART}(I, \alpha, \beta, \rho) \quad (8)$$

where α is the choice parameter, β is the learning rate, and ρ is the vigilance parameter.

In order to minimize the variation of the IT index obtained from the test image in the extraction process, the CB is sorted in ascendant order according to the variance of each codeword.

For natural images, the indices among neighboring image blocks possess similarity, so we can make use of this property to generate the hash table H. We calculate the variance of each index and the indices of its surrounding image blocks with

$$\sigma_{m,n}^2 = \left(\frac{1}{9} \sum_{i=m-1}^{m+1} \sum_{j=n-1}^{n+1} y_{i,j}^2 \right) - \left(\frac{1}{9} \sum_{i=m-1}^{m+1} \sum_{j=n-1}^{n+1} y_{i,j} \right)^2 \quad (9)$$

where $y_{i,j}$ is the index in the IT, $0 \le m < M_1$, and $0 \le n < M_2$. We utilize the concept of the quantization process to embed a watermark in the quantization interval of the variance. Then, the hash table H is constructed as follows:

$$H = \left\{ h_{m,n} \middle| \; h_{m,n} \in \{0, 1\},\ 0 \le m < M_1,\ 0 \le n < M_2 \right\} \quad (10)$$

where

$$h_{m,n} = \begin{cases} 1, & \text{if } r\Delta \le \sigma_{m,n}^2 < (r+1)\Delta \text{ for } r = 0,\ 2,\ 4, \ldots \\ 0, & \text{if } r\Delta \le \sigma_{m,n}^2 < (r+1)\Delta \text{ for } r = 1,\ 3,\ 5, \ldots \end{cases} \quad (11)$$

and Δ is a positive real number called the quantization parameter. Note that the value Δ will affect the quality of the extracted watermark. If the value Δ is larger than all variances (i.e. the values of the hash table are all one.), then the hash table is meaningless. That is to say, all hash tables obtained from all images are the same. However, it is difficult to determine an appropriate interval. In general, a meaningful image is usually a natural image with normal distribution. Therefore, the suggested value for the quantization parameter is shown in Eq. (12).

$$\Delta = 3 \times \sigma = 3 \times \sqrt{\left(\frac{1}{M_1 \times M_2} \sum_{m=0}^{M_1-1} \sum_{n=0}^{M_2-1} \sigma_{m,n}^4 \right) - \left(\frac{1}{M_1 \times M_2} \sum_{m=0}^{M_1-1} \sum_{n=0}^{M_2-1} \sigma_{m,n}^2 \right)^2} \quad (12)$$

After obtaining the hash table H, the secret key K can be computed as the bitwise exclusive-OR of H and W'.

$$K = H \oplus W' \quad (13)$$

The secret key K is used to extract the embedded watermark. Six parameters (i.e., s, t, K, **WM**, N_1, and N_2) work together to protect the ownership of the original image. Figure 1 shows the hash generation process.

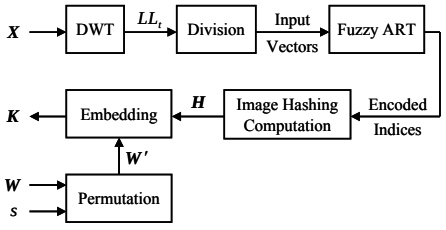


Fig. 1 Hash generation process

3.2: HASH VERIFICATION ALGORITHM

The corresponding extraction process is shown in Fig. 2. Six parameters (i.e., s, t, K, **WM**, N_1, and N_2) are required to extract the embedded watermark without using the original image. For a copyright disputed image, we calculate the estimated hash table H' with the recall of Fuzzy ART. Then, an estimation of the permuted watermark is obtained as:

$$W'' = H' \oplus K \quad (14)$$

Finally, the extracted watermark $\tilde{W}$ is obtained by inversing the permutation in (4) according to the parameter s as follows:

$$\tilde{W} = \left\{ \tilde{w}_{i,j} \middle| \; \tilde{w}_{i,j} = \mathrm{PRP}_s^{-1}\left(w''_{i',j'} \right),\ 0 \le i,\ i' < M_1,\ 0 \le j,\ j' < M_2 \right\} \quad (15)$$

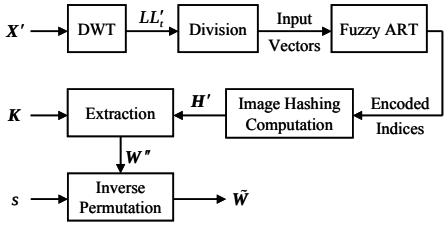
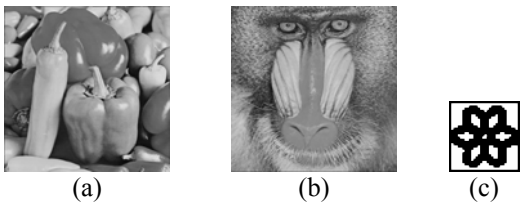


Fig. 2 Hash verification process

4: EXPERIMENTAL RESULTS AND DISCUSSIONS

4.1: EXPERIMENTAL RESULTS

In our experiments, the original images X are respectively 512×512 Peppers and Baboon with 8 bits/pixel resolution as shown in Fig. 3 (a-b). Note that these images represent images with quite different content "complexity". Peppers contains mainly smooth regions, representing low complexity, while Baboon contains large regions of complex texture, representing high complexity. The binary watermark W is the school emblem of National Yunlin University of Science & Technology (NYUST) with size of 64×64 as shown in Fig. 3 (c). The Peppers and Baboon images are both decomposed through two-level wavelet transform and the two sub-images LL_2 of size 128×128 are obtained. For Peppers image, three parameters of Fuzzy ART are respectively set as $\alpha = 0.5$, $\beta = 0.1$, and $\rho = 0.9$. However, for Baboon image, these parameters are respectively set as $\alpha = 0.5$, $\beta = 0.1$, and $\rho = 0.6$. The reason of setting different vigilance parameters for Peppers and Baboon images are given in the discussions.



(a) (b) (c)

Fig. 3 Original images: (a) Peppers and (b) Baboon. Binary watermark: (c) emblem.

We evaluate the quality between the original image and the attacked image using the peak signal-to-noise ratio (PSNR), which is defined as follows:

$$PSNR = 10\log_{10}\left(\frac{E_{peak}^2}{MSE}\right)dB \tag{16}$$

where the mean square error (MSE) is defined as follows:

$$MSE = \frac{\sum_{i=0}^{N_1-1}\sum_{j=0}^{N_2-1}\left(x_{i,j} - x'_{i,j}\right)^2}{N_1 \times N_2} \tag{17}$$

where N_1 and N_2 are the height and width of the image, respectively. $x_{i,j}$ is the original value of the coordinate (i, j) and $x'_{i,j}$ is the altered value of the coordinate (i, j). E_{peak} is the largest gray-level of the image pixels.

The watermark retrieval rate R is used to evaluate the similarity between the original watermark and the extracted watermark. The retrieval rate R is defined as follows:

$$R = 1 - MAE \tag{18}$$

where the mean absolute error (MAE) is defined as follows:

$$MAE = \frac{\sum_{i=0}^{M_1-1}\sum_{j=0}^{M_2-1}\left|w_{i,j} - \tilde{w}_{i,j}\right|}{M_1 \times M_2} \tag{19}$$

where M_1 and M_2 are the height and width of the watermark, respectively. $w_{i,j}$ is the original value of the coordinate (i, j) and $\tilde{w}_{i,j}$ is the altered value of the coordinate (i, j).

To evaluate the robustness of the proposed scheme, we conducted ten different attacks on the original image and compared with Chen's [5], Lu's [2] and Hsu's [3] methods. These ten attacks are blurring, JPEG compression, noising, sharpening, scaling, rotation, print-photocopy-scan, cropping, scaling-cropping, and blind pattern matching (BPM) attacks, respectively. Due to these attacks are identical to Chen's method [5] and the space limitation, the descriptions of these attacks are omitted.

As Table 1 and Table 2 show, our scheme can still extract clear and recognizable watermarks from different attacked images. In the worst case, the proposed method still has a high retrieval rate (up to 90.48%). Despite that Chen's method has better performance for blurring, JPEG compression, noising, sharpening, scaling, and BPM attacks. The retrieval rates of the proposed method are all higher than 93% under these attacks. Moreover, our scheme has a very high retrieval rate for rotation, print-photocopy-scan, cropping, and scaling-cropping attacks. However, Chen's method failed in these attacks. In Lu's method [2], the robust watermark is embedded into the secret key using Huang's method [1] based on index properties. In Hsu's method [3], it embeds watermarks into the middle-frequency components of the image to get a tradeoff between imperceptibility and robustness. From Table 1 and Table 2, Lu's and Hsu's methods failed in some attacks. Lu's method is mainly unable to withstand geometric distortions. In particular, Hsu's method can only extract meaningful watermarks under noising, sharpening, and cropping attacks. However, the watermarks extracted from other attacked images are meaningless. Since Hsu's method is not a lossless one, it can not extract clear and recognizable watermarks under such serious attacks. Obviously, the proposed method is more robust than Chen's, Lu's and Hsu's methods from Table 1 and Table 2.

Table 1 The retrieval rates (%) of the binary watermarks extracted from attacked Peppers images using different methods

Attack \ Method	Chen's method	Lu's method	Hsu's method	Our method
1.Blurring	96.92	76.37	45.07	95.24
2.JPEG	96.85	62.87	44.12	96.53
3.Noising	97.46	89.89	87.77	97.19
4.Sharpening	97.46	91.31	95.04	96.24
5.Scaling	97.53	82.67	42.14	96.02
6.Rotation	84.69	63.35	45.44	90.97
7.Print-Photocopy-Scan	86.87	55.91	65.97	93.36
8.Cropping	84.69	82.25	85.67	95.14
9.Scaling + Cropping	77.95	59.86	47.41	90.94
10.BPM attack	97.12	94.34	44.02	96.22
Average rate	91.75	75.88	60.27	94.79

Table 2 The retrieval rates (%) of the binary watermarks extracted from attacked Baboon images using different methods

Attack \ Method	Chen's method	Lu's method	Hsu's method	Our method
1.Blurring	95.58	66.92	43.56	94.41
2.JPEG	97.29	82.50	45.46	94.73
3.Noising	97.19	97.34	91.21	96.83
4.Sharpening	95.75	95.95	92.41	93.07
5.Scaling	96.63	70.04	42.41	93.51
6.Rotation	73.10	64.28	45.83	92.02
7.Print-Photocopy-Scan	74.68	57.86	61.23	90.48
8.Cropping	80.76	81.62	85.74	92.77
9.Scaling + Cropping	76.17	61.67	45.90	90.67
10.BPM attack	95.78	84.81	44.65	94.60
Average rate	88.29	76.30	59.84	93.31

Furthermore, experimental results under different cropping ratios are shown in Table 3. From these results, the retrieval rates of the binary watermarks extracted from cropped Peppers and Baboon images decrease by cropping ratio progressively increases. From Table 3, we concluded that the proposed method can extract meaningful watermarks under 40% of cropping ratio.

4.2: Discussions

In our experiments, the low-low frequency sub-image is obtained through wavelet transformation. Thus, most of noises are excluded for resolving the weakness of Fuzzy ART which is sensitive to noise and outliers. The reason of choosing two-level wavelet transformation is described as follows. For noising attacks, one-level wavelet transform can not completely

Table 3 The retrieval rates (%) of the binary watermarks extracted from cropped Peppers and Baboon images under different cropping ratios

Cropping ratio \ Image	Peppers Rate	Baboon Rate
10 %	93.77	92.82
20 %	93.58	92.26
30 %	91.72	91.31
40 %	90.72	90.87
50 %	70.78	65.41
60 %	68.92	60.86
70 %	62.48	60.13
80 %	58.98	56.62
90 %	53.86	51.93
100 %	50.83	50.78

remove noise. While three-level wavelet transformation can almost remove noise. Nevertheless, three-level wavelet transformation will cause the size of the sub-image LL_3 is identical to the watermark W. Accordingly, each input vector with only two elements is applied to the Fuzzy ART network. For classification, it is not suitable due to less information. Hence, we chose two-level wavelet transformation to implement our scheme. In general, the appropriate parameter t depends on the sub-image LL_t which has double size of the watermark W. Another advantage is that the training time of the network is very fast since the size of the training patterns is small.

The Fuzzy ART has three fundamental parameters need to establish: the choice parameter α, learning rate β, and vigilance parameter ρ. The choice parameter acts on the category selection. The learning rate controls the speed of the network evolution. Since the choice parameter and learning rate slightly affect the quality of the extracted watermark. Thus, only the vigilance parameter is discussed in this section. The number of the categories formed in the category representation field depends on the vigilance parameter. If ρ is too large, it will generate more categories. If ρ is too small, it will generate few categories. Therefore, different vigilance parameters affect the retrieval rates of the watermarks extracted from attacked images. Table 4 and Table 5 show the retrieval rates of the binary watermarks extracted from attacked Peppers and Baboon images under different vigilance parameters. The retrieval rate marked with a gray rectangle represents the highest rate under different attacks. Observing Table 4, we find that it provides the best performance for Peppers image when the vigilance parameter is equal to 0.9. Moreover, the average rate is also the highest. Therefore, the appropriate vigilance parameter should set to as 0.9 for Peppers image. Nevertheless, the appropriate vigilance parameter should set as 0.6 for Baboon image. Therefore, to obtain high retrieval rate, the vigilance parameter should be appropriately selected according to the complexity of image content. The larger vigilance parameter is used for image with low complexity, while the smaller vigilance parameter is used for image with high complexity. Furthermore, the high retrieval rate can be obtained even though an inadequate vigilance parameter is used.

Table 4 The retrieval rates (%) of the binary watermarks extracted from attacked Peppers images under different vigilance parameters

Attack \ Vigilance value	0.6 Rate	0.7 Rate	0.8 Rate	0.9 Rate
1. Blurring	94.31	94.14	95.02	95.24
2. JPEG	96.12	95.44	96.56	96.53
3. Noising	96.48	96.88	96.66	97.19
4. Sharpening	95.34	95.68	96.17	96.24
5. Scaling	95.70	95.51	95.75	96.02
6. Rotation	91.70	91.11	91.02	90.97
7. Print-Photocopy-Scan	92.31	92.60	93.04	93.36
8. Cropping	93.14	93.92	94.65	95.14
9. Scaling + Cropping	91.65	90.77	90.89	90.94
10. BPM attack	94.60	95.41	96.31	96.22
Average rate	94.14	94.15	94.61	94.79

Table 5 The retrieval rates (%) of the binary watermarks extracted from attacked Baboon images under different vigilance parameters

Attack \ Vigilance value	0.6 Rate	0.7 Rate	0.8 Rate	0.9 Rate
1. Blurring	94.41	93.02	94.48	93.75
2. JPEG	94.73	93.60	94.65	94.70
3. Noising	96.83	96.44	96.02	96.12
4. Sharpening	93.07	93.41	93.60	93.19
5. Scaling	93.51	93.82	93.56	92.58
6. Rotation	92.02	91.53	89.84	87.89
7. Print-Photocopy-Scan	90.48	91.53	89.28	88.38
8. Cropping	92.77	91.58	92.14	92.53
9. Scaling + Cropping	90.67	91.85	89.43	87.79
10. BPM attack	94.60	94.78	93.46	94.36
Average rate	93.31	93.16	92.65	92.13

In addition to the vigilance parameter, the quantization parameter is also an important factor for affecting the quality of the extracted watermark. The larger the quantization interval is, the better the quality of the extracted watermark is. Oppositely, the smaller the quantization interval is, the worse the quality of the extracted watermark is. This result is known and experimental results are shown in Table 6 and Table 7. Table 6 and Table 7 show the retrieval rates of the binary watermarks extracted from attacked Peppers and Baboon images under different quantization parameters, respectively.

For authenticity, non-hashed images are used to demonstrate the authenticity of the proposed scheme. Figure 4 (a) and (b) show non- hashed Elaine and F16 images. The corresponding watermarks extracted from Fig. 4 (a) and (b) are shown in Fig. 5 (a) and (b), respectively. As these results show, we can not extract meaningful watermarks from the non-hashed Elaine and F16 images. The extracted watermarks are meaningless. Hence, the proposed scheme can extract corresponding watermarks from hashed images rather than non-hashed images.

Table 6 The retrieval rates (%) of the binary watermarks extracted from attacked Peppers images under different quantization parameters

Attack \ Quantization interval	σ Rate	2σ Rate	3σ Rate
1. Blurring	80.40	91.55	95.24
2. JPEG	89.04	94.53	96.53
3. Noising	93.02	95.75	97.19
4. Sharpening	87.35	93.75	96.24
5. Scaling	86.08	92.87	96.02
6. Rotation	72.90	82.28	90.97
7. Print-Photocopy-Scan	76.07	86.06	93.36
8. Cropping	79.86	91.28	95.14
9. Scaling + Cropping	71.46	80.27	90.94
10. BPM attack	86.52	93.31	96.22
Average rate	82.27	90.17	94.79

Table 7 The retrieval rates (%) of the binary watermarks extracted from attacked Baboon images under different quantization parameters

Attack \ Quantization interval	σ Rate	2σ Rate	3σ Rate
1. Blurring	78.66	91.80	94.41
2. JPEG	79.66	91.24	94.73
3. Noising	91.75	95.14	96.83
4. Sharpening	77.49	87.01	93.07
5. Scaling	75.68	90.31	93.51
6. Rotation	72.73	89.21	92.02
7. Print-Photocopy-Scan	56.64	87.72	90.48
8. Cropping	69.82	85.33	92.77
9. Scaling + Cropping	71.36	87.62	90.67
10. BPM attack	80.47	91.72	94.60
Average rate	75.43	89.71	93.31

(a) (b)

Fig. 4 Non-hashed images: (a) Elaine and (b) F16.

(a) (b)

Fig. 5 Extracted watermarks: (a) watermark extracted from Fig. 4 (a) and (b) watermark extracted from Fig. 4 (b).

5: CONCLUSION

A robust image hashing scheme based on DWT and Fuzzy ART has been proposed in this paper for content authentication. The proposed scheme, which combines many encouraging characteristics from DWT, Fuzzy ART and quantization process, converts an image into a short and robust hash table. First, the low-low frequency sub-image is obtained through wavelet transformation. Thus, most of noises are excluded for resolving the weakness of Fuzzy ART which is sensitive to noise and outliers. Second, the hash table is constructed using the concept of the quantization process. Finally, a watermark is embedded in the hash table, i.e. the quantization interval of the variance. In addition, unlike general classification, such as k-mean, fuzzy c-means and so on, we can suitably determine the number of the clusters according to the vigilance parameter of Fuzzy ART. Experimental results demonstrate that the proposed scheme is robust enough to resist common image processing and geometric distortions. Moreover, the original image is not required in the extraction process.

ACKNOWLEDGMENT

This work was supported by the National Science Council, Taiwan, R.O.C. under Grants NSC 95-2221-E-224-059.

REFERENCES

[1] Hsiang-Cheh Huang, Feng-Hsing Wang, and Jeng-Shyang Pan, "Efficient and robust watermarking algorithm with vector quantisation," *Electronics Letters*, vol. 37, no. 13, pp. 826-828, 21 Jun. 2001.

[2] Zhe-Ming Lu, Dian-Guo Xu, and Sheng-He Sun, "Multipurpose image watermarking algorithm based on multistage vector quantization," *IEEE Trans. on image processing*, vol. 14, no. 6, pp. 822-831, Jun. 2005.

[3] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden digital watermarks in images," *IEEE Trans. on image processing*, vol. 8, no. 1, pp. 58-68, Jan. 1999.

[4] Deepa Kundur and Dimitrios Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication," *Proc. IEEE*, vol. 87, no. 7, pp.1167-1180, July 1999.

[5] Tzung-Her Chen, Gwoboa Horng, and Wei-Bin Lee, "A publicly verifiable copyright-proving scheme resistant to malicious attacks," *IEEE Trans. on industrial electronics*, vol. 52, no. 1, pp. 327-334, Feb. 2005.

[6] Chun-Shien Lu and Chao-Yong Hsu, "Content-dependent anti-disclosure image watermark," *Proc. 2nd Int. Workshop on Digital Watermarking (IWDW)*, LNCS 2939, pp. 61-76, Seoul, Korea, 2003.

[7] Chun-Shien Lu, Shih-Wei Sun, Chao-Yong Hsu, and Pao-Chi Chang, "Media hash-dependent image watermarking resilient against both geometric attacks and estimation attacks based on false positive-oriented detection," to Appear in *IEEE Trans. on Multimedia*.

[8] Chun-Shien Lu and Chao-Yong Hsu, "Geometric distortion-resilient image hashing scheme and its applications on copy detection and authentication," *ACM Multimedia Systems Journal, special issue on Multimedia and Security*, vol. 11, no. 2, pp. 159-173, Dec. 2005.

[9] G.ail A. Carpenter, Stephen Grossberg, and David B. Rosen, "Fuzzy ART: An adaptive resonance algorithm for rapid, stable classification of analog patterns," in *Proc. Int. Joint Conf. Neural Networks*, pp. 441-416, 1991.