Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTEGER DCT-BASED SELF-RECOVERY WATERMARKING ALGORITHM

[1]HONGXIA WANG, [2]QIUCHEN MEN

[1]Prof., School of Information Science and Technology, Southwest Jiaotong University, Chengdu, 610031, P. R. China

[2]Master, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, 610031, P. R. China

E-mail: [1]hxwang@home.swjtu.edu.cn, [2]menqiuchen@163.com

ABSTRACT

To address the problems of the inferior recovery and lower security in existing self-recovery fragile watermarking algorithms, this paper presents a secure self-recovery fragile watermarking scheme based on integer DCT. In the proposed algorithm, first, the original image is divided into 4×4 blocks, then the recovery watermark of each 4×4 block is generated by the image block's integer DCT coefficients, after that, the secure Hash function with three keys is performed on each 4×4 block to get the corresponding offset block, and finally the recovery watermark of each block is embedded into its corresponding offset block under the control of three keys. Thus, the adversary is difficult to counterfeit the watermark information when he/her tampers with image content. Moreover, the offset key space is large enough . Because the forward and inverse integer DCT can contribute an accurate data match, the recovery of tampered area will be more accurate. Compared with current self-recovery fragile watermarking algorithms commonly using DCT technique or encoded pixel values of an image block, the proposed scheme not only resolves the tamper detection problem, but also improves the recovery image quality and system security.

Keywords: *Digital Watermarking, Integer Discrete Cosine Transform (IntDCT), Tamper Localization, Tamper Recovery*

1. INTRODUCTION

As one of the major media in the information age, digital image is playing an extremely important role in the transmission of message. Due to the unprecedented openness of current network and the appearance of image process software with powerful function, any adversary can easily tamper images without arousing suspicion. Hence, the protection of image contents becomes an important research area. As a technical method to protect the image contents, digital watermarking technique has an important application prospect and has achieved an outstanding progress in the past few years. According to the purpose of application, digital watermarking is classified into robust watermarking for copyright protection and fragile watermarking for integrity authentication. Furthermore, the fragile watermarking is divided into three types including full fragile water-making, semi-fragile watermaking and self recovery/ embedding watermarking [1]-[6]. Especially, the self-recovery watermarking is different from other types of watermarking, and it can not only locate the tempered area, but also approximately restore portions of the image that have been cropped out, replaced, damaged or otherwise tampered without accessing the original image [7].

Currently, most typical self-recovery watermarking techniques use DCT (Discrete Cosine Transform) coefficients or encoded pixel values as a mean for tamper detection and recovery in digital images. J. Fridrich *et al.* [7] divides the image into 8×8 blocks that are DCT transformed, quantized, carefully encoded into the LSBs (Least Significant Bits) of other, distant 8×8 blocks. The quality of the reconstructed image is indistinguishable from a 50% quality JPEG compressed original image. However, the low-resolution reconstruction of the modified parts lead to an unsatisfactory quality of the recovery. In addition, since self-recovery watermarking schemes generally insert features of one image block into another block, the resulting block-wise dependency makes it difficult to detect and localize tampering. To address this problem, Lin *et al.* [8] propose the payload of watermark consists of authentication data as well as recovery data. The authentication data for a block is embedded in the block itself, whereas the recovery

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

data is embedded in a different block. This method of tamper detection has also been adopted in some similar schemes [9]-[12].

In [13], the embedded watermark data for content recovery is calculated from the original DCT coefficients of host image and do not contain any additional redundancy. Otherwise, a compressive sensing technique is employed to retrieve the coefficients by exploiting the sparseness in the DCT domain. As a result, the smaller the tampered area, the more the amount of available watermark data will be, leading to in a better quality of restored image content. Qian *et al.* [14] proposes an approach to generate reference data from the original image by encoding different types of blocks into different number of bits. This method reduces the amount of embedding data while maintaining good recovery quality. For robust tampering restoration, a semi-fragile watermarking method for the automatic authentication and restoration of the content of digital images based on the DCT domain polarity information is presented in [15]. The restoration process is robust to common image processing operations such as lossy transcoding and image filtering. However, this scheme can only recover smaller tampered area. For average block-based fragile watermarking in spatial domain, He *et al.* [16] propose a self-recovery watermarking scheme with superior localization based on the average pixel values of 2×2 image block. This scheme improves the robustness against the random tampering and localization precision, but cannot restore tampered image content with high quality because the recovery watermark is generated by the spatial domain image block. Similar method in [3], a tailor-made watermark consists of reference-bits and check-bits that embedded into the host image by using a lossless data hiding method. So the original image can be restored without any error as long as the tampered area is not too extensive.

Most above mentioned watermarking schemes, the features of an image block generally consist of quantized transform coefficients due to the limitation on the watermark embedding capacity,, e.g., important quantized high-order DCT coefficients or average pixel of image block. Attacks that do not alter these features that fails to be detected. To overcome the insecure problems and unsatisfactory quality of the recovery mentioned above, the authors have proposed a secure self-recovery fragile watermarking by using Hash function and integer DCT characterization, rather than the conventional DCT. The remainder of this paper is organized as follows. In Section 2 the integer DCT is described. Section 3 presents secure self-recovery fragile watermarking scheme based on integer DCT. Experimental results and properties analysis are given in Section 4 and conclusions are given in Section 5.

2. INTEGER DISCRETE COSINE TRANSFORM

The integer DCT (IntDCT) is used in the state-of-the-art video compression standard H.264 [17]. The most significant advantage of this transform is that it is free from any floating-point or fixed-point multiplication required by the original DCT and all operations can be carried out with integer arithmetic, without loss of accuracy. IntDCT basically has the same properties as the original DCT, but there are some fundamental differences. First of all, it is an integer transform. All operations can be carried out with integer arithmetic, without loss of accuracy. It does not need floating-point and fixed-point multiplication required by DCT. This reduces the computational complexity and it is much easier for hardware implementation.

Let X and X_1 denote the image pixel matrix and frequency matrix respectively. The forward 2-D 4×4 IntDCT is given by

$$X_1 = CXC^T \tag{1}$$

The inverse 2-D 4×4 IntDCT is given by

$$X = CX_1C^T \tag{2}$$

where,

$$C = \begin{bmatrix} a & a & a & a \\ b & c & -c & b \\ a & -a & -a & a \\ c & -b & b & -c \end{bmatrix},$$

and $a = 1/2$, $b = \sqrt{1/2}\cos(\pi/8)$, $c = \sqrt{1/2}\cos(3\pi/8)$.

The matrix multiplication can be factorized to the following equivalent form:

$$X_1 = (AXA^T) \otimes E \tag{3}$$

where,

$$A = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & d & -d & 1 \\ 1 & -1 & -1 & 1 \\ d & -1 & 1 & -d \end{bmatrix}, E = \begin{bmatrix} a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \\ a^2 & ab & a^2 & ab \\ ab & b^2 & ab & b^2 \end{bmatrix}.$$

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Here, $d = c/b \approx 0.414$, and the symbol $\otimes$ indicates point multiplication operation. To simplify the implementation of the transform and ensure that the transform remains orthogonal, $a = 1/2$, $b = \sqrt{2/5}$. So the final forward 4x4 IntDCT becomes

$$X_1 = (A_f X A_f^T) \otimes E_f \quad (4)$$

where,

$$A_f = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 2 & 1 & -1 & -2 \\ 1 & -1 & -1 & 1 \\ 1 & -2 & 2 & -1 \end{bmatrix},$$

$$E_f = \begin{bmatrix} a^2 & ab/2 & a^2 & ab/2 \\ ab/2 & b^2/4 & ab/2 & b^2/4 \\ a^2 & ab/2 & a^2 & ab/2 \\ ab/2 & b^2/4 & ab/2 & b^2/4 \end{bmatrix}.$$

3. PROPOSED INTEGER DCT-BASED SELF-RECOVERY WATERMARKING SCHEME

3.1. Watermark Generating and Embedding

Consider an *M*×*N* grey-scale image *X*. We set the LSB and less LSB of all pixels in image *X* to zero. The watermark generating process is presented as follows:

Step1. Block: The image *X* is divided into non-overlapping 4×4 blocks denoted by $B_{4\times4}^k$, $k = 1, 2, 3, \cdots, (M \times N)/16$.

Step2. Integer DCT, encoding and generating recovery watermark: Transform each sub-block $B_{4\times4}^k$ using an integer DCT, and obtain the coefficients matrix $Z_{4\times4}^k = (z_{ij}^k)_{4\times4}$. Every element in $Z_{4\times4}^k$ is quantified by

$$Q(z_{ij}^k) = \lfloor z_{ij}^k / \Delta \rfloor + \delta \quad (5)$$

where $\triangle$ is a quantization step, and $\delta \in Z^+$. Consider HVS (Human Visual System), here, we choose the appropriate quantization parameters, namely, let $\triangle$=5, δ=17. According to the size of integer DCT coefficients, we use different coding length to encode quantized integer DCT coefficients of each 4×4 blocks as shown in Figure 1. Then, the coding result values are ordered in a zig-zag manner and the resulting bit-string of length 32 bits for each block as the binary recovery watermark $W^k = \{w_l^k \mid w_l^k \in \{0,1\}, l = 1, 2, \cdots, 32\}$.

8	3	3	3
3	3	3	0
3	3	0	0
0	0	0	0

Figure 1: Coding Length

Step3. Select offset sub-block for watermark embedding: Choose the offset sub-block $B_{f(k)}$ of each sub-block $B_{4\times4}^k$ using Hash function MD5. In order to obtain good performances and high security of watermark embedding, the selection of offset sub-block usually meets the following requirement:

(i) Each image block is corresponding to only one offset sub-block;

(ii) The distance between image block and its offset sub-block should be large, thus the probability of two blocks being tampered synchronously is low as soon as possible.

(iii) To guarantee the security, the key space of choosing an offset sub-block should be large. Thus the attacker is difficult to tamper the watermark information when he/she tamper the image content.

To meet the above requirements, we employ Hash function to design a secure method for choosing offset sub-block with three keys K_1, K_2, K_3 as follows:

$$v = [k/(M/4)],\ u = k \bmod (M/4) \quad (6)$$

$$v = (v + Hash(u, K_1)) \bmod (N/4) \quad (7)$$

$$u = (u + Hash(v, K_2)) \bmod (M/4) \quad (8)$$

$$v = (v + Hash(u, K_3)) \bmod (N/4) \quad (9)$$

$$f(k) = v \times (M/4) + u \quad (10)$$

Finally, the offset value *f*(*k*) is obtained.

Step4. Watermark embedding: The recovery watermark W^k of image block $B_{4\times4}^k$ is embedded into LSB and less LSB of the offset sub-block $B_{f(k)}$.

Step5. Obtain watermarked image: Following Step2~4, the recovery watermark of each 4×4

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

blocks is generated and embedded into its offset sub-block one by one, and finally the watermarked image X^W is obtained.

3.2. Image Tamper Detection and Recover

The received image is denoted as Y which is tampered or not. Y is divided into 4×4 non-overlapping block $\tilde{B}_{4\times4}^k, k=1,2,\cdots,(M\times N)/16$. The tamper detection of each block is performed by comparing the reconstructed watermark with the extracted watermark. Once a tampered image block has been detected, the recovery watermark can restore it. The detailed detection and recovery process is presented as follows:

Step1. Restructured watermark generation: According to the method described in section 3.1, the restructured watermark $\tilde{W}^k$ is generated by the image block $\tilde{B}_{4\times4}^k$ to be detected.

Step2. Watermark extraction: Use the Hash function MD5 to get the offset sub-block $\tilde{B}_{4\times4}^{f(k)}$ of $\tilde{B}_{4\times4}^k$ with three keys K_1, K_2, K_3. Then, the recovery watermark W_{ex}^k can be extracted from $\tilde{B}_{4\times4}^{f(k)}$.

Step3. Tamper detection: The extracted watermark W_{ex}^k is compared with the restructured watermark $\tilde{W}^k$. If $W_{ex}^k=\tilde{W}^k$, the image block $\tilde{B}_{4\times4}^k$ passes detection. Otherwise, the following decision will be employed.

Let $N_8(\tilde{B}_{4\times4}^k)$ represent the indexes of eight neighbor blocks of $\tilde{B}_{4\times4}^k$. We assume the number of image blocks $\tilde{B}_{4\times4}^l$, $l\in N_8(\tilde{B}_{4\times4}^k)$ with extracted watermark $W_{ex}^l\neq\tilde{W}^l$ is T_k, and then

(i) If $T_k=0$, the image block $\tilde{B}_{4\times4}^k$ is not tampered, and pass detection;

(ii) If $T_k\neq0$ and $T_k\geq T_{f(k)}$, the image block $\tilde{B}_{4\times4}^k$ is tampered, and is restored by the recovery watermark W_{ex}^k . Else, the image block $\tilde{B}_{4\times4}^k$ passes detection.

Step4. Image block recovery: The recovery watermark W_{ex}^k is decoded according to the coding length shown in Figure 1, and the decimal quantified integer DCT coefficients block $\tilde{Q}_{4\times4}^k$ is obtained. With the same quantization step $\triangle$ and parameter δ as step2 in section 3.1, we perform an inverse quantification on $\tilde{Q}_{4\times4}^k$ following formula (11), and obtain the restructured integer DCT coefficient block $\tilde{Z}_{4\times4}^k=(\tilde{z}_{ij}^k)_{4\times4}$,

$$\tilde{z}_{ij}^k=(\tilde{q}_{ij}^k-\delta)\times\Delta \qquad (11)$$

We perform inverse 2-D 4×4 IntDCT on $\tilde{Z}_{4\times4}^k$ following formula (2), and obtain the recovery image block $\hat{B}_{4\times4}^k$ of $\tilde{B}_{4\times4}^k$.

Step5. Obtain restored image: Following Step1~4, all image blocks processing is finished. Combining each image block together to form the final restored image $\tilde{Y}$.

4. EXPERIMENTAL RESULTS

In the proposed algorithm, the watermark information is embedded into the LSB and Less LSB of the offset sub-block, so the difference values between the original and watermarked images is limited in range [0, 3], respectively. Assuming that the original distributions of the LSB and less LSB are uniform, the average energy of distortion caused by watermarking on each pixel is

$$E_D=\frac{1}{16}\sum_{u=0}^{3}\sum_{v=0}^{3}(u-v)^2=2.25 \qquad (12)$$

So, the theoretical PSNR of the watermarked image is

$$PSNR=10\cdot\lg(255^2/E_D)=44.6\text{dB} \qquad (13)$$

As an example, the test image “Lake” of size 512×512 is used as the host, shown in Figure 2(a). With three keys K_1=118, K_2=22131, K_3=71311, Figure 2(b) gives its watermarked versions. The PSNR value due to watermark embedding is 42.2 dB. Comparing to the conventional DCT-based methods [9] and image block-based method [4], the PSNR value of method [9] is 37.9dB, and that of [3] is only 26.1dB. So the proposed scheme has a better quality of watermarked image.

Table 1: PSNR Values (dB) of Watermarked Image

Image	Barbara	Lena	Pepper	Baboon
PSNR(dB)	42.5	42.2	42.2	42.3

Table 1 lists the PSNR values of other four watermarked images sized 512×512 in this experiment. As can seen from **T**able 1, all PSNR values are greater than 42 dB, indicating that the watermarked images of the proposed scheme retain good visual quality.

Journal of Theoretical and Applied Information Technology
20th March 2013. Vol. 49 No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(a) Original Image

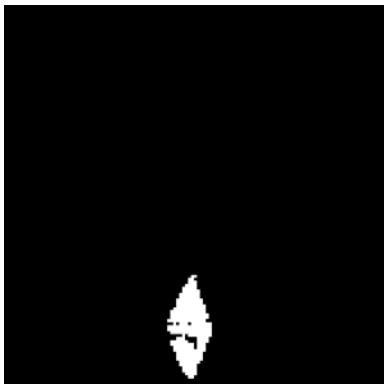
(b) Watermarked Image

Figure 2: Watermark Embedding

For the existent self-recovery watermarking scheme, many typical methods are implemented by encoding DCT coefficients or pixel values of an image block. For example, the methods [9] [14] are based on quantizing and encoding conventional DCT coefficients, and the methods [16] is based on the average pixel values of 2×2 image block. In the proposed scheme, we use IntDCT to generate the recovery watermark. Since IntDCT is designed by using integer values to approximate the floating-point magnitude of the conventional DCT's kernel components, all operations can be carried out by integer arithmetic. So the input and output can be matched accurately after going through forward and inverse transforms, which is a key factor for improving the quality of the restored image by the proposed method.

As an image tamper example, we replicated a boat and its shadow by changing 5.1×10^3 pixels to modify the watermarked images that shown in Figure 2(b). The tampered image is shown in Figure 3(a). Figure 3(b) shows the located tampered areas. By using the image restoration procedure of the proposed scheme, Figure 3 (c) shows the original image "Lake" can be perfectly recovered from the tampered versions. The PSNR value of the restored image is 30.6dB, while that of method [3] is 28.7dB. So the proposed scheme presents a better recovery quality.

(a) Tampered Image



(b) Located Tampered Areas

(c) Restored Image

Figure 3: Tamper Detection and Recovery

Table 2 lists the restoration capability comparison of several self-recovery watermarking schemes. In the previous methods, the recovery watermark is generated by quantizing and encoding DCT coefficients or image blocks, but in the proposed scheme, the recovery watermark is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

generated by quantizing and encoding Integer DCT coefficients so that the original image can be perfectly recovered. As seen from **T**able 2, most PSNR values of restored images are greater than that of conventional DCT-based methods [9] [14] and image block-based method [16], indicating that our scheme has a higher quality restoration capability.

Table 2: Comparison of PSNRs (dB) of Restoration Image among Conventional DCT-Based and Image Block-Based Methods

Image	[9]	[14]	[16]	Proposed
Barbara	24.2	24.8	25.9	28.7
Lena	29.9	32.8	29.6	31.8
Pepper	28.8	31.8	29.3	31.6
Baboon	22.2	22.6	24.8	30.0

The security of fragile watermarking is an important property. Because our scheme embed the recovery watermark into the offset sub-block using Hash function with three keys, the recovery watermark will not be attacked as long as the offset sub-block is not within the tampered area. In addition, the key space is very large. The key length and word type can be set by the user. For example, if each key of three keys is hex with length of 10, the whole key space will be 1.329×10^{36}. Hence, the security is improved.

5. CONCLUSIONS

We present a self-recovery watermarking scheme to improve the restoration capability by using integer DCT characteristic. The proposed algorithm can achieve a good quality of restored image due to the forward and inverse integer DCT can contribute an accurate data match. Moreover, the simplicity of the integer DCT transform offered a significant advantage in shorter processing time and ease of hardware implementation than commonly used DCT techniques. Comparison results among IntDCT, DCT and image block-based self-recovery watermarking methods have also been presented. For future work, the proposed watermarking algorithm by using the integer DCT will be extended to the field of the fragile watermarking for video.

ACKNOWLEDGMENT

This research was supported by the National Natural Science Foundation of China (NSFC) under the grant No. 61170226, the Fundamental Research Funds for the Central Universities under the grant Nos.SWJTU11CX047, SWJTU12ZT02, and the Young Innovative Research Team of Sichuan Province under the grant No.2011JTD0007.

REFRENCES:

[1] S.H. Liu, H.X. Yao, W. Gao, and Y.L Liu, "An Image Fragile Watermark Scheme Based on Chaotic Image Pattern and Pixel-Pairs", *Applied Mathematics and Computation*, Vol. 185, No. 2, 2007, pp. 869-882.

[2] F.D. Martino and S. Sessa, "Fragile Watermarking Tamper Detection with Images Compressed by Fuzzy Transform", *Information Sciences*, Vol. 195, No. 1, 2012, pp. 62-90.

[3] X.P. Zhang and S.Z. Wang, "Fragile Watermarking with Error-Free Restoration Capability", *IEEE Transactions on Multimedia*, Vol. 10, No. 8, 2008, pp. 1490-1499.

[4] B.S. Sergio and A.K.Nandi, "Secure Fragile Watermarking Method for Image Authentication with Improved Tampering Localisation and Self-Recovery Capabilities", *Signal Processing*, Vol. 91, No. 4, 2011, pp. 728-739.

[5] H.X. Wang and C.X. Liao, "Fragile Watermarking with Discrimination of Tampers on Image Content or Watermark for JPEG Images", *IETE Technical Review*, Vol. 27, No. 3, 2010, pp. 244-251.

[6] H.J. He, F. Chen, H.M. Tai, T. Kalker, and J.S. Zhang, "Performance Analysis of a Block-Neighborhood-Based Self-Recovery Fragile Watermarking Scheme", *IEEE Transactions on Information Forensics and Security*, Vol. 7, No. 1, 2012, pp. 185-196.

[7] J. Fridrich and M. Goljan, "Images with Self-Correcting Capabilities", *IEEE International Conference on Image Processing (ICIP)*, Kobe, Japan, October 24-28, Vol. 3, 1999, pp. 792-796.

[8] P. L. Lin, C. K. Hsieh, and P. W. Huang, "A Hierarchical Digital Watermarking Method for Image Tamper Detection and Recovery", *Pattern Recognition*, Vol. 38, No. 2, 2005, pp. 2519-2529.

[9] X. Zhang and S. Wang, "Fragile Watermarking Scheme with Extensive Content Restoration

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Capability", *International Workshop on Digital Watermarking (IWDW)*, LNCS, Vol. 5703, 2009, pp. 268-278.

[10] T.Y. Lee and S. D. Lin, "Dual Watermark for Image Tamper Detection and Recovery", *Pattern Recognition*, Vol. 41, No. 2, 2008, pp. 3497–3506.

[11] Z.X. Qian, G.R. Feng, X.P. Zhang, and S.Z. Wang, "Image Self-Embedding with High-Quality Restoration Capability", *Digital Signal Processing*, Vol. 21, No.2, 2011, pp. 278-286.

[12] C.W. Yang and J.J. Shen, "Recover the Tampered Image Based on VQ Indexing", *Signal Processing*, Vol. 90, No.1, 2010, pp. 331-343.

[13] X.P. Zhang, Z.X. Qian, Y.L. Ren, and G.R. Feng, "Watermarking with Flexible Self-Recovery Quality Based on Compressive Sensing and Compositive Reconstruction", *IEEE Transactions on Information Forensics and Security*, Vol. 6, No. 4, 2011, pp. 1223-1232.

[14] Z.X. Qian and G.R. Feng, "Inpainting Assisted Self Recovery with Decreased Embedding Data", *IEEE Signal Processing Letters*, Vol. 17, No.11, 2010, pp. 929-932.

[15] X.Z. Zhu, A.T.S. Hob, and P. Marziliano, "A New Semi-Fragile Image Watermarking with Robust Tampering Restoration Using Irregular Sampling", *Signal Processing: Image Communication*, Vol. 22, No. 5, 2007, pp. 515-528.

[16] H.J. He, J.S. Zhang, and F. Chen, "A Self-Recovery Fragile Watermarking Scheme for Image Authentication with Superior Localization", *Science in China Series F: Information Sciences*, Vol. 51, No. 10, 2008, pp. 1487-1507.

[17] H. Malvar, A. Hallapuro, and M. Karczewicz, "Low-Complexity Transform and Quantization in H.264 /AVC", *IEEE Transactions on Circuits and System Video Technology*, Vol. 13, No. 7, 2003, pp. 637-644.