CRT-BASED SELF-RECOVERY WATERMARKING TECHNIQUE FOR MULTIMEDIA APPLICATIONS

Banani Patra[1] and Jagdish C. Patra[2]

[1]IBM, Singapore
[2]Swinburne University of Technology, Melbourne, Australia
Banani1106@msn.com, JCPatra@swin.edu.au

ABSTRACT

We propose a Chinese remainder theorem (CRT)-based computationally efficient self-recovery watermarking technique for multimedia applications. Taking few examples of digital images we have shown that the proposed technique can recover the tampered region in the watermarked image quite effectively. Using an optimal quantizing technique we generate a 21-bit watermark from the DCT coefficients of an 8x8 block. This watermark is embedded in a randomly selected block using CRT. Due to modular operations of CRT the watermark embedding and extraction phases are computationally efficient. Experimenting with different size and location of tampering, we have shown effectiveness of our proposed technique. We have also shown the results of a tampered cheque for bank application.

Index Terms— Self-recovery watermarking, Chinese remainder theorem, authentication, digital forensic.

1. INTRODUCTION

Due to rapid expansion of the Internet applications and mobile wireless technologies thousands and thousands of images, videos, and other contents are being daily uploaded/ downloaded through the Internet. Thus it is quite important for a user to verify the authenticity and integrity of these digital contents. Digital watermarking is used to verify authenticity and integrity of the digital contents [1]-[2]. A watermark representing the owner's identity is embedded invisibly in the original digital content (host). The watermarked image is transmitted or uploaded to the Internet. An user can verify the authenticity of the watermarked image by extracting the watermark. If there is a good match between the original and the extracted watermarks, then the image is authenticated.

Several techniques in spatial and transform domains, e.g., discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD), independent component analysis (ICA), etc., have been proposed by different researchers [2]-[4]. These techniques can authenticate the digital content even when the watermarked image undergoes several intentional or unintentional modifications (called attacks), e.g., addition of noise, low-pass filtering, tampering, cropping, JPEG compression, etc. In these techniques the emphasis is to verify the authentication of the contents. However, in some of the emerging applications, e.g., digital forensic, it is not only necessary to authenticate but also to recover the content in the tampered region. In this direction there are only a few published reports available [5]-[8]. Recently, Patra et al. [9]-[10] have reported Chinese remainder theorem (CRT) based computationally-efficient watermarking schemes both in spatial and DCT domain and shown their effectiveness for image authentication under various attacks.

In this paper we propose a CRT-based watermarking scheme which not only authenticates the watermarked image but also faithfully recovers the original contents in the tampered regions of the image. First, using a optimal quantizing technique a 21-bit number is generated from DCT coefficients of an 8x8 block of the host image, which represents the compressed version of the block and is used as the watermark. Next, these 21-bits are embedded in a randomly selected 8x8 block in spatial domain using CRT. At the receiver, in order to authenticate and recover the contents in case of tampering, the recipient generates two images called reconstructed image and decompressed image from the watermarked image. If the mean square error (MSE) between the reconstructed and decompressed image blocks exceed a threshold then the watermark block in the watermarked image is replaced by the block from the reconstructed image. With several experiments we have shown that the proposed technique effectively recovers the contents even when the tampered area is quite large.

2. GENERATION OF WATERMARK BITS

We generate a 21-bit watermark from a selected 8x8 block of an image using an optimal quantizing technique [11]. First DCT is performed and the DC component and another six coefficients are retained for the compression. As shown in Fig. 1 the DC component is quantized with 4 bits, and the seven AC coefficients are quantized with 4, 3 or 2 bits, using the quantization Table given in [11]. With 8-bits

C1 (4)	C2 (4)	C6 (2)	C7 (2)	0	0	0	0
C3 (3)	C5 (2)	C8 (2)	0	0	0	0	0
C4 (2)	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Coeff	C1				C2				C6		C7		C3			C5		C8		C4	
Bit position	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
Bit value	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	0	0	1	1	1

Fig.1 Generation of a 21-bit watermark from DCT coefficients of an 8x8 block.

per pixel, it gives rise to a compression ratio of 8x8x8/21 = 24.38.

3. CHINESE REMAINDER THEOREM

Using CRT an integer can be represented by a pair of smaller integers. It is an elegant and computationally efficient technique as it involves only modular arithmetic. Here we briefly explain the CRT, which is used in the proposed watermarking technique.

Let $\{S_1, S_2\}$ be two integers which are pair-wise co-prime (i.e., the only common factor between S_1 and S_2 is 1) and let $S = S_1 \cdot S_2$. The objective of the CRT is to represent any integer Z, $\{0 < Z \leq S-1\}$ by a pair of integers $Z = \{R_1, R_2\}$, such that $R_1 < S_1$ and $R_2 < S_2$. The R_1 and R_2 are obtained by solving the following congruence:

$$Z \equiv R_1 \pmod{S_1}$$
$$Z \equiv R_2 \pmod{S_2} \qquad (1)$$

Let us take an example in which $S_1 = 6$ and $S_2 = 11$. Therefore, $S = S_1 \cdot S_2 = 66$. Let the given integer be $Z = 52$. Using (1), $52 \equiv R_1 \pmod 6$ and $52 \equiv R_2 \pmod{11}$. Thus, we get $R_1 = 4$ and $R_2 = 8$. Therefore, Z can be represented as $Z = \{4, 8\}$. For more discussions on CRT, one can refer to any textbook on number theory or cryptography [12].

4. WATERMARKING SCHEME

4.1. Watermark Embedding

Fig. 2 shows the watermark embedding scheme. The host image A (MxN) is divided into non-overlapping blocks of size 8x8. A 21-bit watermark $W_{m,n}$ is generated (as shown in Fig. 1) from a block $a(m,n)$ $\{1 \leq m \leq M/8,\ 1 \leq n \leq N/8\}$ chosen from a random block location (m,n) (using a SEED value). Using CRT $W_{m,n}$ is embedded in block $a(i,j)$ to generate the watermarked block $b(i,j)$ $\{1 \leq i \leq M/8,\ 1 \leq j \leq N/8\}$. In this way all the blocks of the host image A are embedded to obtain the watermarked image B (MxN).

4.2. Watermark Extraction

The watermark extraction and restoration are carried out in two phases. As shown in Fig. 3, in *Phase-I*, the watermarked image B is divided into blocks of 8x8. The 21-bit watermark

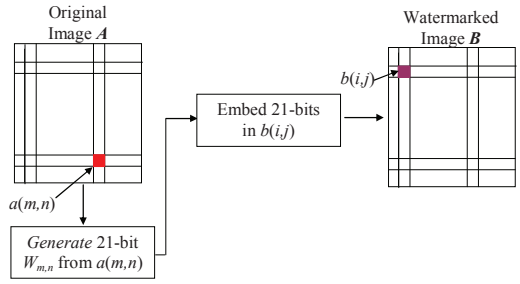

Fig. 2 Watermark embedding scheme.

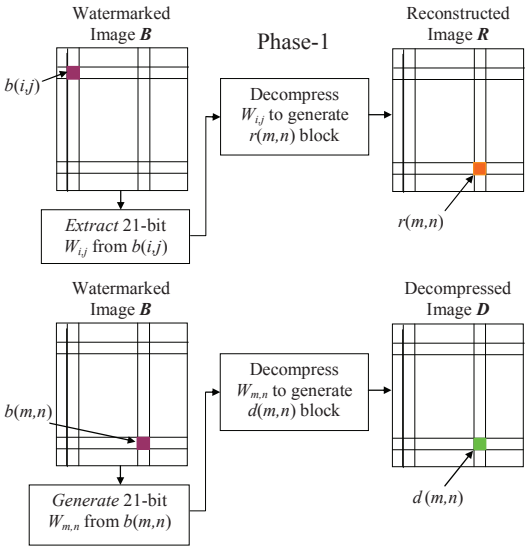

Fig. 3 Watermark extraction: *Phase 1*.

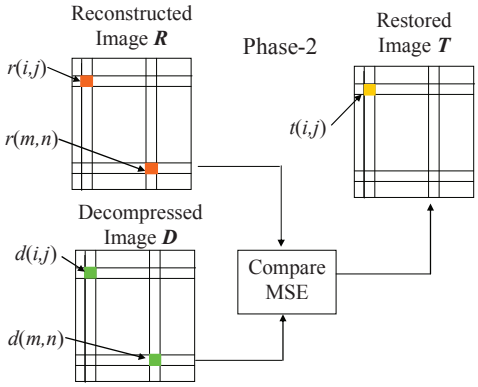

Fig. 4 Watermark extraction: *Phase 2*.

$W_{i,j}$ is *extracted* from the block $b(i,j)$ and then decompressed to form a 8x8 block $r(m,n)$ which is placed at the location (m,n). In this way a reconstructed image R (MxN) is generated. Next, the watermark $W_{m,n}$ is *generated* from the block $b(m,n)$, decompressed to generate $d(m,n)$ and placed at location (m,n). In this way a decompressed image D (MxN) is generated.

In *Phase-2* of extraction process, as shown in Fig. 4, the mean square error (MSE) between the blocks of R and D are compared. Let $\theta_{i,j}$ denote the MSE between blocks $r(i,j)$ and $d(i,j)$ which is defined as follows:

$$\theta_{i,j} = \frac{1}{64}\left(\sum_{k=1}^{64}[x(r,k) - x(d,k)]^2\right), \quad (2)$$

where $x(r,k)$ and $x(d,k)$ denote the pixel intensity at kth position of the $r(i,j)$ and $d(i,j)$ blocks, respectively. Similarly $\theta_{m,n}$ is defined.

4.3. Restoration

Note that the watermark embedded in the block $b(i,j)$ has been generated from block position (m,n). Assume that the block $b(i,j)$ of the watermarked image B has been tampered. In such situation, the reconstructed block $r(m,n)$ will be erroneous. Also the decompressed block $d(i,j)$ will be erroneous. Therefore in order to detect the error in $b(i,j)$ and to restore block $t(i,j)$ we adopt the following strategy:

$$\begin{aligned} &\text{if } ((\theta_{i,j} \geq threshold) \text{ AND } (\theta_{m,n} \geq threshold)) \\ &\qquad \text{then } t(i,j) = r(i,j) \\ &\qquad \text{else } t(i,j) = b(i,j) \end{aligned} \quad (3)$$

Considering the average, minimum and maximum values of the MSE, after several trials, the *threshold* value is selected. In this way the restored image T (MxN) is generated.

5. WATERMARKING PROCESS

5.1. CRT-based Embedding Process

The 21-bit watermark $W_{m,n}$ generated (as shown in Fig. 1) from a random block $a(m,n)$ is embedded in block (i,j) to get embedded block $b(i,j)$. In the embedding process shown in Fig. 5, the required conditions of embedding are as follows:

$$\text{If watermark bit=1, } p_1 \geq p_2 \quad (4)$$

$$\text{If watermark bit=0, } p_1 < p_2 \quad (5)$$

Using CRT, p_1 and p_2 are selected to satisfy (4) and (5).

5.2. Watermark Extraction Process

The recipient after getting the watermarked image B would like to authenticate and restore the image in case of any tampering. The recipient has the following information: (i) the watermarked image, B, (ii) the size of the original image, (iii) the *SEED* of the random number generator, (iv) the *threshold* value, and (v) the values of S_1 and S_2. The extraction process of the 21-bit watermark $W_{i,j}$ from a selected block $b(i,j)$ is explained in Fig. 6.

5.3. Decompression Process

In Fig. 1, we have shown the process of generating a 21-bit watermark from an 8x8 block. Decompression is the reverse process in which a 21-bit watermark $W_{i,j}$ is used to create an 8x8 block of pixels. Using the values defined in the Tables [11], DCT coefficients are generated and then inverse DCT is performed to generate an 8x8 block.

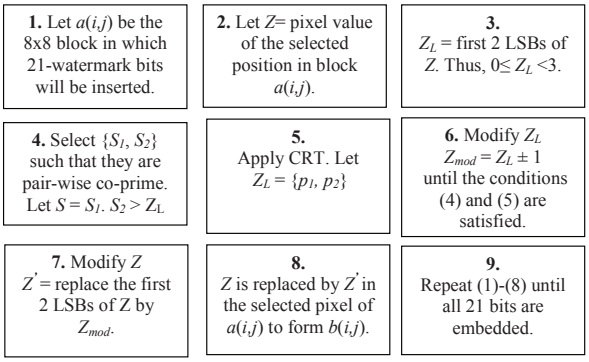

Fig. 5 Watermark embedding process.

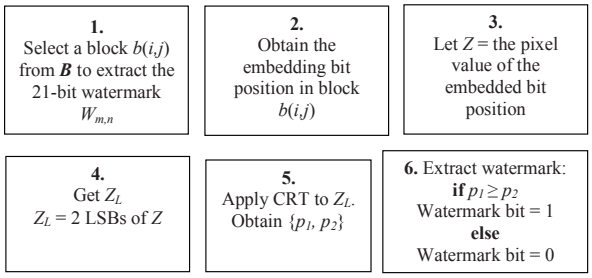

Fig. 6 Watermark extraction process.

6. EXPERIMENTAL RESULTS

We provide the experimental results for two images under different scenarios. We also conducted experiments for a few other images and observed similar encouraging results (not shown here due to space constraint).

6.1. Pre-processing of Images

Since we choose a block size of 8x8, the given image is resized such that the height and width are divisible by 8. The values of S_1 and S_2 were selected as 3 and 5, respectively. The threshold values for Lenna and Cheque were selected as 80 and 1500, respectively, and the SEED was chosen as 1257.

6.2. Experiment 1: Lenna Image

The gray scale Lenna image 512x512 was watermarked using the proposed CRT-based technique. The original and the watermarked Lenna images are shown in Fig. 7. The peak signal to noise ratio (PSNR) of the watermarked image is found as 43.02 dB. Considering embedding of 21 watermark-bits in a block of 8x8, this value is reasonably good. We have considered three scenarios of tampering with the Lenna watermarked image. The low, medium and high levels of tampered and their respective restored images are shown in Fig. 8. It can be seen that the proposed scheme is able to recover the tampered images quite satisfactorily. The PSNR of the three restored images, Fig. 8 (d), (e) and (f) were found as 38.85, 38.24 and 29.37dB, respectively.

(a) (b)

Fig. 7 Lenna images (a) original, (b) watermarked.

(a) (b) (c)

(d) (e) (f)

Fig. 8 Tampered and restored Lenna images: (a)-(c) tampered , (d)-(f) respective restored images.

Fig. 9 The Cheque images: (a) original, (b) watermarked, (c) tampered, (d) restored.

6.2. Experiment 2: Digital Cheque

Here we consider a practical application of self recovery of a tampered cheque, as an example of forensic and banking applications. A digital signed cheque is received by the recipient (C. M. How). Suppose this cheque is tampered and presented to the Bank for clearance. The Bank would like to authenticate and recover the original cheque. As shown in Fig. 9, the amount, both in figure and words in the original cheque (a) and watermarked cheque (b) is S$13,204. However, the amount, both in figure and words, in the received cheque as shown in Fig. 9(c), has been tampered and made to S$31,204, and presented to the bank. The bank checks for authenticity and is able to know that the cheque was tampered. As shown in Fig. 9.(d) the recovered image clearly restores the original amount S$13,204 both in figure and words. The bottom four sub-images in Fig. 9 are the magnified version of (c) and (d). The PSNR of the watermarked image (b) and restored image (d) were found as 33.69 and 28.79 dB, respectively. The effectiveness of the proposed technique is hereby clearly demonstrated.

7. CONCLUSIONS

We have proposed a novel CRT-based self recovery watermarking scheme which effectively recovers the original content from the tampered watermarked image. The CRT-based scheme is computationally quite efficient as it involves only modular arithmetic. The proposed technique is able to recover the tampered region faithfully even for large-sized tampering in the watermarked images. Because of its effectiveness this technique may be used in video, text and other digital media.

8. REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, A. Lu, "Techniques for data hiding", *IBM Systems Journal*, vol. 35, no. 3&4, pp. 313–336, 1996.

[2] I.J. Cox, M.L.Miller, and J.A.Bloom, *Digital Watermarking*, Morgan Kaufmann Publishers Inc., California, USA, 2001.

[3] A. Cheddad, J. Condell, K. Curran, P. Mc. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, pp. 727-752, 2010.

[4] T.V. Nguyen, J.C. Patra and P.K. Meher, "WMicaD: A New Digital watermarking technique using independent component analysis," *EURASIP J. Advances in Signal Processing*, 2008, Article ID 317242, 2008.

[5] C-Y. Lin. and S-F. Chang, "SARI: self-authentication-and-recovery image watermarking system", in Proc. *ACM Multimedia*, Ottawa, Canada, 2001, pp.628-629.

[6] H-J. He, J-S. Zhang and F. Chen, "Adjacent-block based statistical detection method for self-embedding watermarking techniques," *Signal Processing*, vol. 89, pp. 1557-1566, 2009.

[7] C. Shenbing, C. Zugao and S. Xu, "Reearch on image self-recovery algorithm based on DCT," *Journal of Multimedia*, vol. 5, no. 3, pp. 290-297, June 2010.

[8] W.C. Seng, J. Du and B. Pham, "Semi fragile watermark with self authentication and self recovery," *Malaysian Journal of Computer Science*, vol. 22, no. 1, 2009, pp. 64-84.

[9] J.C. Patra, A. Karthik, C. Bornand, "A novel CRT-based watermarking technique for authentication of multimedia contents," *Digital Signal Processing*, vol. 20, pp. 442–453, 2010.

[10] J.C. Patra, J.E. Phua and C. Bornand, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression," *Digital Signal Processing*, vol. 20, pp. 1597- 1611, 2010.

[11] Y.Q. Shi and H. Sun. *Image and Video Compression for Multimedia Engineering: fundamentals, algorithms, and standards,* CRC Press, Washington D.C., USA, 1999.

[12] W. Stallings, *Cryptography and Network Security*, Fifth Edition, Pearson Education Inc., 2011.