International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-1 Issue-4, April 2012

CRT and ART Based Watermarking Scheme in DCT Domain

V. Priyanka, M. Nireesha, V. Venu Kumar, N. Venkat Ram, A. S. N. Chakravarthy

Abstract- In this paper, we propose Chinese Remainder Theorem (CRT) and Aryabhata Remainder Theorem (ART) based watermarking scheme that work in the Discrete Cosine Transform (DCT) domain.CRT based scheme is more resistant to different types of attacks, particularly to JPEG compression; in addition, it improves the security feature of the watermarking scheme. Experimental results have shown that the proposed scheme makes the watermark perceptually invisible and has better robustness to common image manipulation techniques. ART-based algorithm can be applied to any kind of moduli and its computation cost is less than that of the CRT-based algorithm. Both techniques can be applied for protection of images and information.

Keywords- CRT, ART, DCT, Residue, Remainder, Inverse.

1. INTRODUCTION

Users can make unauthorized modification or copies of the digital content and redistribute them on the Internet and this creates ownership issues. To address this problem, digital watermarking can be used to protect the ownership of the digital content. In digital watermarking[10,11,12], the original author hides the copyright control information (called a watermark) into the digital content (host) by modification of the content itself. Hence, the watermark is used as a mean to detect any modifications applied to the host. Watermarking embedding methods can be generally classified into two categories: spatial domain and frequency (transform) domain. In spatial domain, the watermark is embedded directly to the pixel locations. On the other hand, frequency domain watermarking methods are based on the modification of frequency components. Examples of frequency domains include Discrete Cosine Transform (DCT) [13,14]and Discrete Wavelet Transform (DWT) [15]. The Chinese Remainder Theorem (CRT) is a popular research topic in many fields, such as digital signal processing, information protection systems, and cryptography[1,2]. It provides added security. Up to now, many improvements of CRT are proposed[3,4,5,6,7,8] to reduce the computation time.Aryabhata Remainder Theorem (ART) was firstly proposed by Rao and Yang [9] in 2006.Like CRT, ART can also determine an integer from its remainders with the corresponding set of moduli set.CRT has to compute the modular operation with a large number[1,2] M, where M is the products of all moduli. However, ART does not need to compute such time-consuming operation so that the computation time of ART is less than that of CRT.

Manuscript published on 30 April 2012.
* Correspondence Author (s)
V.Priyanka*, IV/IV B.Tech, Department of ECM University, (E-mail:priyanka.vandarani@gmail.com)
N.Venkat Ram, ASSOCIATE DEAN, Department of ECM, KL University, (E-mail:venkat_ram_ecm@klce.ac.in)
M.Nireesha, IV/IV B.Tech, Department of ECM, KL University, (E-mail:nireesha266@gmail.com),
V.Venu Kumar, IV/IV B.Tech, Department of ECM, KL University, (E-mail:venukumarnani@gmail.com)
Dr.A.S.N.Chakravarthy, Professor, Department of ECM, KL University, (Email:asnchakravarthy@kluniversity.in)

2. CHINESE REMAINDER THEOREM

Chinese remainder theorem will determine a number N that when divided by some given divisors leaves given remainders.

Given a set of relatively prime moduli {u1 ,u2 , ..., un} , let the corresponding residues be {v1 ,v2 , ..., vn} that satisfies $v_i = |N|_{u_i} = N \bmod u_i$ for i _1, 2, ..., n. The CRT can compute N by the equation $|N|_M = \left| \sum_{i=1}^{n} u_i' . |v_i . u_i'^{-1}|_{u_i} \right|_M$, [1, 2],where $M = \prod_{i=1}^{n} u_i$ and $u_i' = M / u_i$ .Here $|u_i'^{-1}|_{u_i}$ is the multiplicative inverse of u_i' modulo u_i .

3. ARYABHATA REMAINDER THEOREM

Aryabhata remainder theorem also determines a number N that when divided by some given divisors leaves given remainders. But the advantage of it is the computation costs of this algorithm are less than those of CRT.

Let u_1 and u_2 be relatively prime moduli and $M = u_1.u_2$

Given $N \bmod u_1 = v_1$, $N \bmod u_2 = v_2$, N has a unique solution in Z_M given by:

$$N = ART(v_1, v_2; u_1, u_2; M)$$
$$= ART(0, c; u_1, u_2; M) + v_1 \text{ where } c = (v_2 - v_1) \bmod u_2$$
$$= A + v_1 \text{ ,[9],where}$$
$$A = u_1 \left[(c.u_1^{-1}) \bmod u_2 \right]$$

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

4. DCT DOMAIN

In this paper we propose embedding the watermark in DCT domain. The initial step is to divide the host image into blocks of 8 x 8 pixels. This is the same block size as used in the JPEG compression. The blocks are then converted into the DCT domain where embedding of watermark information will be processed. After the embedding process, the watermarked DCT blocks will then undergo inverse DCT to reconstruct the watermarked image.

For extraction of watermark, the watermarked image is also divided into blocks of 8 x 8 pixels. These blocks then undergo DCT conversion and the watermark is extracted. As such, the watermarking scheme does all the processing in the DCT domain instead of the spatial domain.

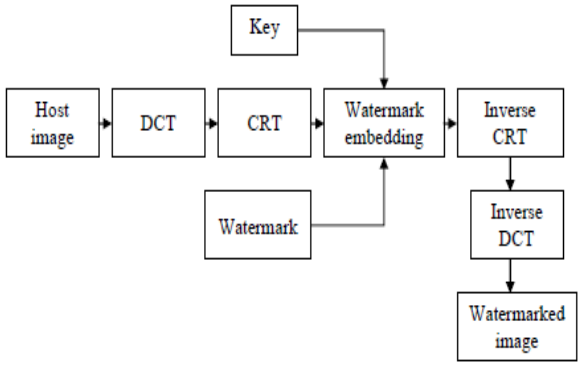

Fig 1: The proposed DCT domain watermarking scheme

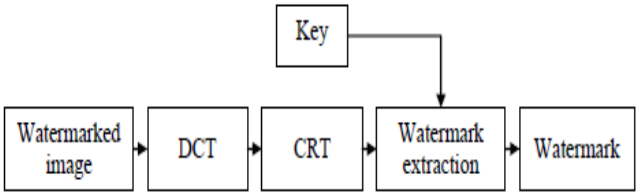

Fig 2: The proposed DCT domain extraction scheme

5. PROPOSED SCHEME

5.1 CRT

Let u and v be pair-wise co-prime positive integers. Two integers are considered co-prime if they have no common divisors other than 1, meaning their Greatest Common Divisor (GCD) = 1. Pair-wise means all the integers in the set must meet the co-prime requirement. Let M be the product of u and v. This is also called the dynamic range. Thus, according to CRT, for any given positive integers p and q; where p < u and q < v, there exists a unique integer N, where N <M. Let us first determine r1 and r2 by:

$$r_1 = M/u = v; r_2 = M/v = u$$

Let us find s1 and s2 such that:

$$(r_1 s_1) \bmod u = 1;\ (r_2 s_2) \bmod v = 1$$

Then, we can find the unique integer N as follows:

$$N = (p.r_1 s_1 + q.r_2 s_2) \bmod M$$

5.2 Inverse CRT

Using inverse CRT an integer N where N is between 0 and M-1 can be represented by a unique pair of integers, p and q. M is the product of u and v, pair-wise co-prime integers. The values of p and q are determined by u and v where p < u and q <v. The relationship between N, p, q,u and v are given below.

$$p = N \bmod u;\ q = N \bmod v$$

Hence, using CRT, we can represent an integer N, by a pair of integers {p, q}..

5.3 Application

From the values p and q, the absolute difference between these two integers, *diff* is given by:

$$diff = |p - q|$$

When we take the absolute difference of p and q, we find that the largest value of diff is one less than the maximum of m and n, as shown.

$$D = \max\{u, v\} - 1.$$

5.4 Embedding procedure

1. Select a random 8 x 8 block from the host image.
2. Apply DCT conversion to the selected 8 x 8 block.
3. Randomly select a watermark bit from the watermark information to embed into the block.
4. Randomly select a DCT coefficient N to be embedded in the block.
5. Let u and v be a pair-wise co-prime numbers with values 38 and 107, respectively, to be used for CRT if N is the DC coefficient. Otherwise, the values of u and v would be 38 and 55 if N is the AC coefficient.
6. Apply the inverse CRT, find p and q.
7. Determine D and diff.
8. To embed watermark bit '1', the required condition is:

$$diff \geq \frac{D}{8}$$

If this is not satisfied, N is modified until it is satisfied. The process of embedding bit '1' is explained below.

9. To embed watermark bit '0', the required condition is:

$$diff \leq \frac{D}{8}$$

If this is not satisfied, then N is modified to N′ until it is satisfied. The process of embedding bit '0' is explained below.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

10. Reconstruct the DCT block with the modified DCT coefficient, N′ and apply inverse DCT to the block to reconstruct the watermarked image block.
11. Repeat steps 1-10 for the remaining blocks until all watermark information bits are embedded.

In Step 5, the values, 38, 55 and 107 were selected so that M remains within the dynamic range of possible DCT coefficients.

To embed bit '1':

If equation in step 8 is satisfied, there is no need to modify the values of p and q. Otherwise, add 8 to N and continue from Step 8 of the embedding procedure with the new N′ and check whether the equation is satisfied. If not, subtract 8 from N and continue with Step 8 of the embedding procedure and check whether equation is satisfied. If it is still not satisfied continue adding or subtracting 8 to N until equation satisfies.

To embed bit '0':

If equation in step 9 is satisfied there is no need to modify the values of p and q. Otherwise continue adding or subtracting 8 to N until it is satisfied. The reason for using ±8 to make modifications to the selected DCT coefficient is because it provides sufficient amount of modification in the DCT domain that would be reflected back in the spatial domain.

5.5 Extraction procedure

The extraction procedure is the same until Step 7 of the embedding procedure. After which, the value of diff is compared with the absolute difference D. If diff is greater than D/8, bit '1' would be extracted, otherwise bit '0' would be extracted. Then repeat these steps for the remaining blocks

to extract all the watermark bits. The extraction phase requires minimal knowledge, because to extract the watermark completely only the following are needed: (i) the watermarked image, (ii) size of the watermark, (iii) seed of the pseudo-random number generator (key) and (iv) the pairwise co-prime numbers u and v.

6. EXPERIMENTAL RESULTS

Experiments were conducted to evaluate the performance of the proposed scheme. To evaluate the performance of the watermarking technique, peak signal to noise ratio (PSNR) is often used as a quantitative index for watermarked images.

6.1 Performance Measures

$$PSNR(db) = 10\log_{10}\left[\frac{255^2}{\frac{1}{M}\frac{1}{N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[A(i,j) - A^{'}(i,j)\right]^2}\right]$$

6.2 Results

Fig 3: Input image

Fig 4: Watermark

Fig 5 : Recovered Image

7. CONCLUSIONS

We have proposed a novel CRT and ART based DCT domain watermarking scheme for image authentication which is quite robust against common attacks. Especially, the proposed scheme is able to withstand the JPEG compression. The PSNR value of the proposed scheme is found to be higher. The proposed scheme is superior to many existing techniques. In summary, the proposed scheme introduces an effective and efficient watermarking approach for image authentication.

References:

[1] C. Ding, D. Pei, and A. Solomaa, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*, World Scientific, Singapore, 1996. [2] N. Szabo and R. Tanaka, *Residue Arithmetic and ItsApplications to Computer Technology*, McGraw Hill, NewYork, 1967.
[2] N. Szabo and R. Tanaka, *Residue Arithmetic and ItsApplications to Computer Technology*, McGraw Hill, New York, 1967.
[3] C. C. Chang and Y. P. Lai, "A Fast Modular Square Computing Method Based on the Generalized Chinese Remainder Theorem for Prime Moduli", *Applied Mathematics and Computation*, Vol. 161, No. 1, pp. 181-194,2005.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

[4] A. S. Fraenkel, "New Proof of the Generalized Chinese Remainder Theorem", *Proceedings of American Mathematical Society*, Vol. 14, pp. 790-791, 1963.
[5] Y. P. Lai and C. C. Chang, "Parallel Computational Algorithms for Generalized Chinese Remainder Theorem",*Computers and Electrical Engineering*, Vol. 29, pp. 801-811,2003.
[6] H. Liao and X. G. Xia, "A Sharpened Dynamic Range of a Generalized Chinese Remainder Theorem for Multiple Integers", *IEEE Transactions on Information Theory*, Vol. 53,No. 1, pp. 428-433, 2007.
[7] Y. Wang, "Residue-to-Binary Converters Based on New Chinese Remainder Theorem", *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Vol.47, No. 3, pp. 197-205, 2000.
[8] X. G. Xia and K. Liu, "A Generalized Chinese Remainder Theorem for Residue Sets with Errors and Its Application in Frequency Determination from Multiple Sensors with Low Sampling Rates", *IEEE Signal Processing Letters*, Vol.12, No.11, pp. 768-771, 2005.
[9] T. R. N. Rao and C. H. Yang, "Aryabhata Remainder Theorem: Relevance to Public-Key Crypto-Algorithms",*Circuits, Systems, and Signal Processing*, Vol. 25, No. 1,pp.1-15, 2006.
[10] V.M. Potdar, S. Han and E. Chang, "A survey of digital image watermarking techniques", IEEE Intl. Conf. Industrial Informatics, Perth, Australia, Aug. 2005, pp. 709 – 716.
[11] E. Kougianos, S. P. Mohanty and R. N. Mahapatra, "Hardware assisted watermarking for multimedia," Computers and Electrical Engineering 35 (2009) 339–358.
[12] C. Shoemaker, "Hidden Bits: A Survey of Techniques for Digital Watermarking", Available online: http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html, Virtual Union, 2002.
[13] V.M. Potdar, S. Han and E. Chang, "A survey of digital image watermarking techniques", IEEE Intl. Conf. Industrial Informatics, Perth, Australia, Aug. 2005, pp. 709 – 716.
[14] C-T. Hsu and J-L. Wu, "Hidden digital watermarks in images", IEEE Trans. on Image Processing, vol. 8, no. 1, pp. 58 – 68, Jan 1999.
[15] I. J. Cox, J. Killian, F.T. Leighton and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transon Image Process., vol. 6, no. 12, pp. 1673–1687, Dec 1997.
[16] C-H. Wu, J-H. Hong and C-W. Wu, "RSA cryptosystem design based on the Chinese remainder theorem", in Proc. AsiaSouth Pacific Design Automation, Yokohama, Japan, 2001,pp. 391 – 395.
[17] J. S. Shyong and Y-R. Chen, "Threshold Secret Image Sharing by Chinese Remainder Theorem," IEEE Asia-Pacific Services Computing Conference, Yilin, Taiwan, Dec. 2008, pp.1332-1337.
[18] P. Meerwald and A. Uhl, "Survey of wavelet-domain watermarking algorithms", in Proc. of SPIE, Electronic Imaging, Security and Watermarking of Multimedia Contents III, vol.4314, pp. 505-516, 2001.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)