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.

I. 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 modifying 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.

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 $\{u_1, u_2, ..., u_n\}$, let the corresponding residues be $\{v_1, v_2, ..., v_n\}$ that satisfies $v_i = |N| u_i^{-1} \mod u_i$ for $i = 1, 2, ..., n$. The CRT can compute $N$ by the equation

$$ N_M = \sum_{i=1}^{n} u_i^{-1} |v_i| u_i^{-1} \mod u_i, \quad [1, 2], $$

where $M = \prod_{i=1}^{n} u_i$ and $u_i^{-1} = M / u_i$. Here $u_i^{-1} \mod u_i$ is the multiplicative inverse of $u_i$ modulo $u_i$.

III. 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 $N \mod u_1 = v_1, N \mod u_2 = v_2$, $N$ has a unique solution in $Z_M$ given by:

$$ N = ART (v_1, v_2; u_1, u_2; M) = ART (0, c; u_1, u_2; M) + v_1 $$

where $c = (v_2 - v_1) \mod u_2$.

IV. 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 $8 \times 8$ 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.

Manuscript received on March 20, 2012
V. Priyanka, l/v/f, B.Tech, Ece Department, KL University, (E-mail: priyanka.vandanam@gmail.com)
N. Venkat Ram, Associate Dean, Ecm Department, KL University, (E-mail: venkat_ram_ecm@klce.ac.in)
M. Nireesha, l/v/f, B.Tech, Ece Department, KL University, (Email: nireesha266@gmail.com)
V. Venu Kumar, l/v/f, B.Tech, Ece Department, KL University, (Email: venukumarmanani@gmail.com)
Dr. A. S. N. Chakravarthy, Professor, Ecm Department, KL University, (Email: Aschakravarthy@kluniversity.in)
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.

\[ r_1 = M / u = v; \quad r_2 = M / v = u \]

Let us find \( s_1 \) and \( s_2 \) such that:

\[ (r_1 s_1) \mod u = 1; \quad (r_2 s_2) \mod v = 1 \]

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

\[ N = (p r_1 s_1 + q r_2 s_2) \mod M \]

1.2 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.

\[ p = N \mod u; \quad q = N \mod v \]

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

1.3 Application

From the values \( p \) and \( q \), the absolute difference between these two integers, \( \text{diff} \) is given by:

\[ \text{diff} = |p - q| \]

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

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

1.4 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 \( \text{diff} \).
8. To embed watermark bit ‘1’, the required condition is:

\[ \text{diff} \geq \frac{D}{8} \]

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:

\[ \text{diff} \leq \frac{D}{8} \]
If this is not satisfied, then N is modified to N’ until it is satisfied. The process of embedding bit ‘0’ is explained below.

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.

1.5 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.

VI. 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.

1.6 Performance Measures

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

1.7 Results

Fig 3: Input image

Fig 4: Watermark

Fig 5: Recovered Image

VII. 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:


