Secured Watermarking in DCT Domain using CRT and Complexity Analysis

Varun Kumar
Department of Electronics & Communication Engg
Om Institute of Technology and Management,
HISAR-125001, INDIA

Kuldeep Bhardwaj
Department of Electronics & Communication Engg.
Om Institute of Technology and Management
HISAR-125001, INDIA

Abstract - Digital watermarking techniques have been used as one of the means for copy right protection and authentication of multimedia data. This paper present a secured watermarking method based on image complexity analysis with Chinese Remainder Theorem (CRT). The image complexion information is extracted from DC coefficient in sub blocks transformed by discrete cosine transform (DCT) to make sure macroblock of image adapt to be embedded watermark information [5]. In the proposed watermarking technique the security enhanced without degrading the image quality. Simulation result show the proposed watermarking algorithm has strong robustness against some attacks such as JPEG compression, noise attacks, cropping, tampering and so on [4].

Keywords - CRT, DCT, Digital image watermarking, JPEG compression, image complexity, watermarking algorithm.

I. INTRODUCTION

High speed computer networks, the Internet and the World Wide Web have revolutionized the way in which digital data is distributed. The widespread and easy accesses to multimedia contents and possibility to make unlimited copy without loss of considerable fidelity have motivated the need for the digital rights management [8]. In addition to difficulties in management of many illegal activities such as unauthentication, copying works without permission etc. Another problem, which is related to a numerous of digital files including text, image, audio and video is daily publishing without information of source, origin, authorship, copyright and intellectual property policy. To solve these problems, scientists have launched a variety of methods; mechanisms as well as management policies to protect copyright content and enhance security and safe transmission of important information together with avoid attacks. Among all techniques suggested that digital watermarking is considered to be useful and meet most needs of data protection from others, authentication and copyright products [9].

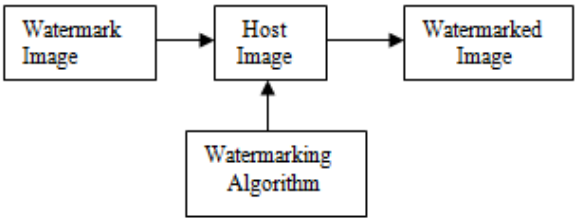


Fig. 1: Watermarking process

In the watermarking process watermark image is embedded or hidden in an original image which is known as host image or original image, such that the watermark can be detected or extracted at any times in order to make an assertion about the object. The main purpose of digital watermarking is to embed information imperceptibly and robustly in host data [3]. The paper is organized as follow: Section 2 presents background of digital watermarking and DCT domain watermarking scheme. Section 3 discusses the image complexity analysis. Section 4 shows the proposed water marking algorithm. Simulation results are given in Section 5 and finally section 6 concludes the paper [8].

II. BACKGROUND

The term "digital watermark" was first coined in 1992 by Andrew Terkel and Charles Osborne. Recently years several companies were established to market watermarking products and have used watermarking technologies for a variety of applications. Watermarking is defined as, “the process of possibly irreversibly embedding information into a digital signal. The signal may be audio, pictures or video” [11]. The Chinese Remainder Theorem is briefly given below:

2.1. The CRT

To make watermark data secure Chinese Remainder Theorem is used. The name of the Chinese Remainder Theorem derives from the historical fact that this theorem was known to the Chinese in the first century A.D. It is said that the CRT is first published by the Chinese mathematician Sun Zi in his book "The Arithmetical Classic of Sun Zi" between the 3rd and the 5th century [14].

Let {m, n} denote a pair-wise co-prime positive integers. The dynamic range N is given by N= m.n. According to CRT for any given pair of positive integer {p, q}, where p < m and q < n, there exists a unique integer Z such that Z < N. Calculation of Z is as follows [5].

First determine r1 and r2 as:

$$r1 = N / m = n$$
$$r2 = N / n = m \quad \text{..... (1)}$$

Next, find s1 and s2 such that (2) is satisfied:

$$(r1s1) \bmod m = 1$$
$$(r2s2) \bmod n = 1 \quad \text{..... (2)}$$

Then, we find the unique integer Z as:

$$Z = (p.r1s1 + q.r2s2) \bmod N \quad \text{..... (3)}$$

2.2. The Inverse CRT:

Using inverse CRT an integer Z, $0 \leq Z \leq N-1$, can be represented by a unique pair of integers {p, q}, where p < m and q < n. The values of p and q are determined as:

.
$$p = Z \bmod m$$
$$q = Z \bmod n \quad \text{..... (4)}$$

Following variables are used in the proposed algorithm [5].

$$D = \max\{m, n\} - 1 \quad \text{..... (5)}$$
$$d = |p - q| \quad \text{..... (6)}$$
$$b = p + q \quad \text{..... (7)}$$

2.3. DCT Domain Watermarking Scheme (Embedding Procedure)

The process begins by dividing the host image into 8×8 blocks. The program will automatically select the appropriate number of watermark bits to be embedded into a block. For example to embed 32×32 binary watermark image into a 512×512 host image, the number of watermark bits per block would be 1 watermark bit per block. There would be exactly one watermark bits as given in the following steps:

1. Choose a secret integer as the seed of the PRNG.
2. Select a random block (8×8) from the host image.
3 Apply Discrete Cosine Transform (DCT) to the selected block. In DCT the image is converted into the frequency domain pattern like as shown below [10]:

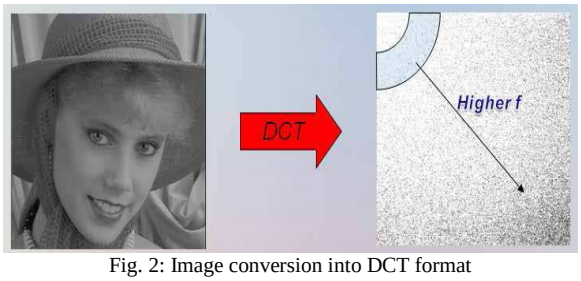


Fig. 2: Image conversion into DCT format

4. Select a watermark bit randomly from the watermark image to embed into the block.
5. Select a DCT coefficient randomly to embed the watermark bit. Let its value be denoted by Z.
6. Let m and n be a pair-wise co-prime numbers with values 38 and 55, respectively, to be used for CRT if Z is the DC coefficient.
7. Apply the inverse CRT, find p and q using equation (4).
8. Determine D using equation (5) and b using equation (7).
9. The required condition to embed watermark bit '1' is: $d \geq D/8$ ..... (8)

If equation (8) is not satisfied, then Z is modified to Z' as explained below until (8) is satisfied.

10. The required condition to embed watermark bit '0' is: $d < D/8$ ..... (9)

If (9) is not satisfied, then Z is modified to Z' as explained below until (9) is satisfied.

11. Reconstruct the DCT block with modified DCT coefficient Z' and apply inverse DCT to the block to construct the watermarked image block. Repeat steps 2-11 for the remaining blocks until all watermark bits are embedded [5].

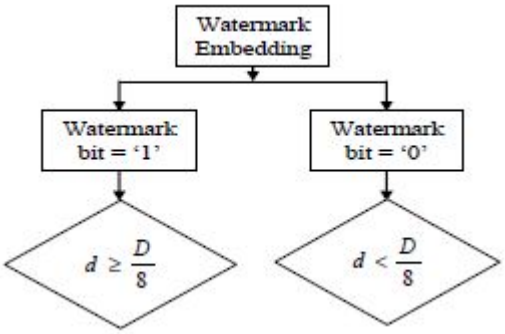


Fig. 3: Watermark embedding procedure

III. IMAGE COMPLEXION ANALYSIS

To find the complexity let us consider an image of 16×16 macroblocks. As shown above in the image has four macroblocks, which has high complexity. The pixel of macroblock 1 changes very slightly and luminance is high, embedding the watermark information in this region will result in pixels overflow. Macroblock 2 is region of eaves, its pixels also changes very slightly and them is very regular it will be easily detected if brim region has change somewhere. Macroblock 3 and 4 shows complexion and irregularity from human vision, which accords with the need of embedding watermark. So we find out firstly the most complex region of host image. By this adequate analysis about the complexion information can do much help on the information hiding [8].

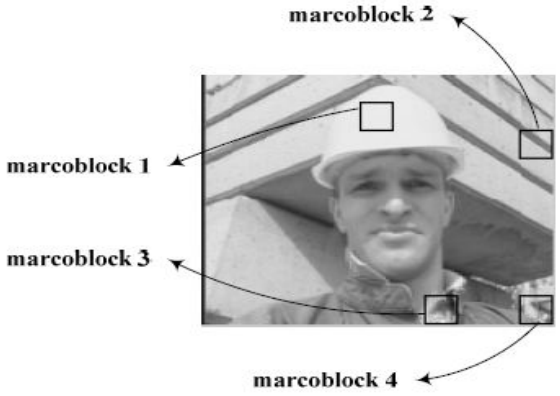


Fig. 4: Four 16×16 macroblocks of original image

The algorithm uses complexity gene of partial image to measure the partial image's complexity. Cgene (Complexity gene) of partial image composes the linear function with direct current component:

Cgene (m, n) = α1σ2m, n + α2 p (em, n) ……..... (1)

α1 and α2 is proportion gene and their values are between 0 and 1. There is need to chose the larger value about Cgene of macroblock to embed watermark. The size of image is N1× N2 and DC m,n(i,j) is 16×16 pixel macroblock's direct coefficient. Complexity of DC m, n (i, j) is:

$$\sigma^2_{m,n} = \frac{1}{16} \sum_{(i,j) \in Y_{m,n}} p(e_{m,n}) \frac{\left| DC_{m,n}(i,j) - e_{m,n} \right|}{e_{m,n}}$$

$$p(e_{m,n}) = \left(1 / e_{m,n} \right)^{\beta}$$

e m, n is average of sixteen DC coefficients of macroblock, p(e m,n) is weighted coefficient. The value of β is between 0.6 and 0.7. The value of Cgene (m, n) is changing as the changing of α1, α2 and β, therefore these three parameters can be used as a key [8].

IV. PROPOSED WATERMARKING ALGORITHM

The complexity based watermark embedding procedure into host image is same as simple embedding procedure except that this has one different step in procedure. After apply DCT on each 8×8 block, blocks are sequential pick according to their complexity rank before apply CRT on them. So, in this method image hidden become more secure without degrading image quality. Watermark Embedding procedure based on complexity step by step as:

1. Chose a JPEG photo as a Host image.
2. Converting this original image into blocks of 8×8.
3. Apply DCT on each block which convert image into frequency domain.
4. To find the complexity of each block using complexity method. Select block sequentially according to the complexity rank and apply CRT on them sequentially.
5. Now start watermark embedding process taking watermark and security key as inputs and watermarked image as output. Apply inverse CRT and inverse DCT on the output of watermarking process. Finally the watermarked or resulted image is obtained in which the watermark information is hidden in host image in a secure manner. In this proposed watermarking scheme the security of watermarked image enhanced without degrading quality of the image. The performance of the proposed technique is also checked by calculating some parameters like PSNR.

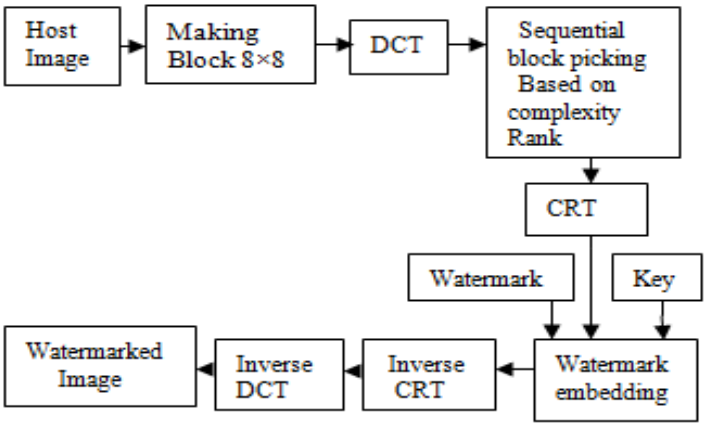
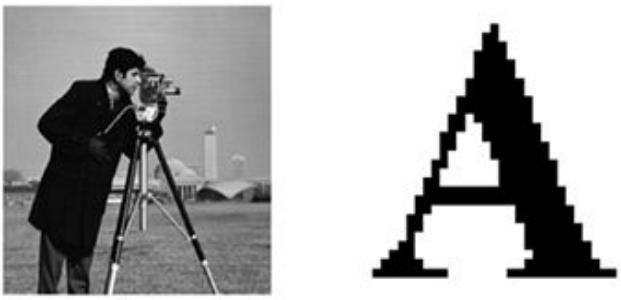


Fig. 5: Complexity based watermarking block diagram

V. SIMULATION RESULTS

Firstly the complexity of the blocks of host image is calculated by using complexity formula and then watermark logo is inserted into most complex regions of the original image according to their complexity ranks. The extraction of the watermark is done for further use at any time. Power to Signal noise ratio (PSNR) is a parameter is used to check the performance of using watermarking technique. If value of PSNR is equal or greater than 30 then the using watermarking process is suitable. The complete proposed watermarking process is explained with the help of both gray scale and coloured images [10].

1)



(a) Original image (b) Watermark image

Fig. 6: Watermark Image is inserted into Original image

.

Fig. 7: Watermarked Image

The black and white watermark is hidden into most complex regions of Gray scale host image and then it is extracted from watermarked image with security enhance without degrading the image quality.

Fig. 8: Extracted watermark

PSNR is also calculated in both processes separately as:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

PSNR (Watermark inserted into the Original Image) = 4.744580e+001.
PSNR (Watermark Extracted from Watermarked Image) = Infinity.

2) This proposed technique can be used for coloured image also. The watermarking process remains same for both colour and gray scale image.

(a) Original image **(b)** Watermark image

Fig. 9: Watermark Image is inserted into Original image

The black and white watermark is hidden into a in most complex regions of coloured host image and then it is extracted from watermarked image without degrading the image quality. The resulted image and extracted watermark image is shown below:

Fig. 10: Watermarked image

Fig. 11: Extracted Watermark

PSNR is also calculated in both processes separately.
Power to Signal Noise Ratio (Watermark inserted into Original Image) = 4.574130e+001.
PSNR (Watermark Extracted from Watermarked Image) = Infinity. The value of PSNR is above 30 so the proposed watermarking technique is established to improve the security of image without degrading the image quality.

VI. CONCLUSION

As demonstrated above in the experimental result, using the proposed watermarking in DCT domain using CRT and complexity analysis technique the security of watermark image enhance without degrading image quality. Some parameters can be calculated to check the performance of proposed watermarking technique. This proposed technique can be used for both gray scale and coloured image. In addition the proposed technique features added more security due to its sequential selection of watermarking blocks based on complexity and sequential selection of location of watermark bit to be embedded. We have compared the performance of proposed watermarking technique with the existing techniques and show that the proposed technique maintains its imperceptibility and robustness more against various attacks. For further increase robustness in watermarking technique we can use artificial intelligence. The proposed technique introduces an effective and efficient watermarking technique for image which may be equally applicable to other form of digital media like text, audio or video. Therefore we conclude that this new proposed technique is more suitable for images to make them more secure and increase their robustness against various attacks without degrading image quality.

REFERENCES

[1] Mrs. Anita Jadhav and Mrs. Megha Kolhekar, "Digital watermarking in video for copy right protection", International Conference on Electronic system, pp.140-144, 7/14 2014 IEEE.
[2] Vikas Chaubey, Chetan Kumar and Vikram Arora, "A Review of Hybrid digital Watermark ing by using singular value decomposition-Discrete Cosine Transform", International Journal of Engineering Trends and Technology, vol. 4, pp.3950-3955, 9 sept. 2013.
[3] S. Priya, B. Santhi and P. Swaminathan, "Image Watermarking Techniques", Research Journal of Applied Sciences, Engineering and Technology, vol. 4(14), pp. 2251-2254, July 15, 2012.
[4] Abduljabbar Shaamala and Azizah A. Manaf, "Study of the effected Genetic Watermarking Robustness under DCT and DWT domains", International Journal of New Computer Architecture and their applications, vol. 2(2) , pp. 353-360, 2012.
[5] Jagdish C. Patra, A.K. Kishore and Cedric Bornand, "Improved CRT based DCT domain Watermarking Technique with Robustness against JPEG Compression for Digital Media Authentication", pp. 2940-2945, 2011 IEEE.
[6] Thi Hoang Ngen Le, Kim Hung Nguyen and Hoai Bac Le, "Literature Survey on Image Watermarking Tools, Watermark attacks and Benchmarking Tools", International Conference on Advances in Multimedia, pp. 67-73, 2010 IEEE.
[7] T. Jayamalar and Dr. V. Radha, "Survey on Digital Video Watermarking Techniques and Attacks on Watermark", international Journal of Engineering Sciences and Technology, vol. 2(12), pp. 6963-6967, 2010.
[8] Max Xuan and Jian Guo Jiang, "A Noval Watermarking Algorithm in Entropy Coding based on image Complexity Analysis", International Conference on Multimedia Information Networking and Security, pp. 126-129, 2009 IEEE.
[9] Sourav Bhattacharya, T. Chattopadhyay and Arpan Pal, "A Survey on Different Video Watermarking Techniques and Comparative Analysis with Reference to H.264/AVC", 2006 IEEE.
[10] Pooja Monshizadeh Naini, "Digital Watermarking Using MATLAB", http://www.intechopen.com, pp. 465-480.
[11] http://imagewatermarking.info.
[12] http://www.watermarker.com/watermark-protector.
[13] http://www.watermarktool.com.
[14] http://wikipedia.org/wiki/Chinese_remainder_theorem