COMPARISON OF CRT-BASED DIGITAL IMAGE WATERMARKING AND CRT-BASED ZERO WATERMARKING IN DCT DOMAIN

Oke Afeez Adeshina[1], Kazeem Alagbe Gbolagade[2]

[1] Information Communication Unit, Summit University, Offa, Kwara State, Nigeria
[2] Department of Computer Science, Kwara State University, Malete, Nigeria

Corresponding author: Oke Afeez Adeshina, okeafeez@summituniversity.edu.ng

ABSTRACT: *This paper focuses on the investigation of traditional digital image watermarking with crt and zero watermarking with crt in the dct domain. Functional analysis of imperceptibility, robustness and time of execution is performed. Based on the result of the experiment the crt with zero watermarking provides better performance since there are no distortion with a faster time of execution, however, it is still susceptible to cropping attacks. Traditional crt watermarking still has a high tamper assessment function (taf) without any attack.*
KEYWORDS: *Chinese Remainder Theorem, Discrete Cosine Transform, Digital Watermarking*

1. INTRODUCTION

In recent years, owing to the advancements in information communication technology resulting in dissemination of multimedia via the internet, there has been an increase and continuous problems of copyright abuse and intellectual property [1]. These problems has motivated various researchers to create new methodologies for Digital Watermarking. Digital watermarking is employed as a means for information security in copyright protection, data authentication, broadcast monitoring and secret communication.
Digital image watermarking entails creating a watermark, embedding generated watermark to the cover image, while extraction is the opposite of the previous process. During watermark embedding into a cover image, the image is mostly distorted in some form. The rate of distortion is a function of watermark invisibility and robustness [2].
Zero Watermarking was proposed to solve the problems of image distortion as a result of embedding. A relationship is created between the cover image and the watermark [3]. The application of Chinese Remainder Theorem (CRT) to digital image watermarking improves security and robustness [4] and it is much faster and computationally efficient than other methods such as SVD [5]. CRT has been applied to both conventional and zero watermarking. This paper compares the CRT-based conventional digital watermarking and CRT-based Zero watermarking in the DCT domain in terms of robustness, imperceptibility and resistance to several attacks.
The rest of the paper is organized as follows: Section 2 presents preliminaries based on the comparison. Section 3 presents Literature reviews while methodology is presented in section 4 Experimental results and discussions are presented in section 5. Finally the paper is summarized and concluded in section 6.

2. PRELIMINARIES

Digital watermarking generally involves the process of watermark embedding and watermark extraction processes, prior to embedding, the process begins with generating watermark bits. Discrete Cosine Transform (DCT) is used with CRT in embedding and extracting the watermarks.

2.1 Chinese Remainder Theorem

CRT was majorly applied to the transformation of a Residue Number System (RNS) to its decimal or binary equivalent [6]. However, it has been applied to solve various engineering problems. The principle of applying CRT to digital image watermarking is its extra layer of security during embedding of watermark bits [7].
By choosing a relatively prime integer numbers and applying CRT, a large integer X can be denoted by a set of smaller integer's numbers. It is extremely difficult to retrieve X without knowing the prime numbers. This property of CRT makes it suitable for additional security in Digital Watermarking.
Let $\{m_1, m_2\}$ represent a pair-wise co-prime positive integer numbers. The dynamic range $M = m_1.m_2$. According to CRT for any given pair of positive integer numbers $\{r_1, r_2\}$, where $r_1 < m_1$ and $r_2 < m_2$, there exist a unique integer X, such that X < M. Let us first determine x_1 and x_2 by:

$$x_1 = M/m_1 = m_2$$
$$x_2 = M/m_2 = m_1 \qquad \text{(equation 1)}$$

Next find s_1 and s_2 such that:

$$(x_1 s_1)\ mod\ m_1 = 1$$
$$(x_2 s_2)\ mod\ m_2 = 1 \qquad \text{(equation 2)}$$

Then the unique integer X can be found :

$$X = \left| \sum_{1}^{n} m_i \left| m_i^{-1} \right|_{m_i} r_i \right|_N$$

The above can be simplified using (equation 1) and (equation 2) into:

$$X = (r_1 . x_1 s_1 + r_2 . x_2 s_2) \qquad \text{(equation 3)}$$

2.2 Inverse CRT (Forward Conversion)

Using CRT, an integer X,$0 \le X \le N-1$, can be denoted by a unique pair of integer numbers $\{r_1, r_2\}$, where $r_1 < m_1$ and $r_2 < m_2$. The relationship between the variables is given below:

$$r_1 = X\ mod\ m_1$$
$$r_2 = X\ mod\ m_2 \qquad \text{(equation 4)}$$

2.3 Discrete Cosine Transfrom

A Discrete Cosine Transform (DCT) is a method in frequency domain that is generally applied to image transformations converted to compress JPEG images [8]. The DCT belongs to a family of 6 trigonometric transformation. The type-2 DCT transforms a block of image size $N \times N$ having pixel intensities $S(n_1, n_2)$ into a transform array of coefficients (k_1, k_2), described by the following equations:

$$S(k_1, k_2) = \sqrt{\frac{4}{N^2}} C(k_1) C(k_2) \sum_{n=0}^{N-1} \sum_{n=0}^{N-1} S(n_1, n_2) \cos\left(\frac{\pi(2n+1)k_1}{2N}\right) \cos\left(\frac{\pi(2n+1)k_2}{2N}\right) \qquad \text{(equation 5)}$$

Where $k_1, k_2, n_1, n_2 = 0, 1, \ldots N-1$ and

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}}, & k < 0 \\ 1, & otherwise \end{cases}$$

$S(k_1,k_2)$ and pixel (n_1,n_2) present a DCT coefficient at position (k_1,k_2) and a pixel value at position (x_1,x_2) respectively. The DCT basis image can be computed using the transformation kernel, which is same for both forward DCT and inverse DCT (IDCT) is given by:

$$Pixel\ (n_1, n_2) = \sqrt{\frac{4C(k_1)C(k_2)}{N^2}} \cos\frac{\pi(2n_1+1)k_1}{2N} \cos\frac{\pi(2n_2+1)k_2}{2N}$$

2.4 Zero Watermarking

Zero watermarking was proposed to solve the problems of image alteration during watermark embedding [3], Zero watermarking involves the use of watermark data from the cover image. The image containing the watermark has no difference from the primary image, however, it is usually secured in the database of Intellectual Property rights (IPR) also known as watermark registration center.

The focus of zero watermarking is centered on how to construct watermarking evidence through the use of important features of the original image rather than how to embed the watermarks.

3. LITERATURE REVIEW

Digital image watermarking mainly involve two principles namely: embedding algorithm and extraction algorithm. The strength and robustness of a digital image watermark can be increased by improving the individual methods of watermark embedding and extraction. Series of methods which are based on exploring the most appropriate coefficients to insert watermark information has been implemented and proposed by various researchers.

Patra et al. [4] Proposed a method based on CRT watermark scheme for DCT domain. Their scheme utilizes CRT to hide watermark at low-frequency area of DCT coefficients. DCT is implemented on the selected blocks and the watermark is embedded by altering the coefficients. Their scheme is able to resist JPEG compression along with other common attacks, however, the Tamper Assessment Function (TAF) of the extracted image is found to be low.

Luo et al. [10] Proposed an algorithm for digital image watermarking that inserts secret data into an image and utilizing CRT for embedding in the DCT domain. Experimental findings show that the algorithm is robust to common attacks. However, the extracted watermark is not very clear, the NC and PSNR values are still high.

Benoraira et al. [11] proposed robust and blind image watermarking scheme based on discrete wavelet transform (DWT) and discrete cosine transform (DCT). The use of two DCT transformed sub-vectors to insert the watermark sequence in a differential manner was implemented. Experimental analysis revealed that the proposed technique effectively fulfills the conditions of imperceptibility and provides a high level of robustness against a range of image-processing attacks.

Kasmani et al. [12] proposed a method of first using enhancement filters to the watermarked image as pre-filtering before running watermark extraction in

Discrete Cosine Transform (DCT) domain. The watermarked part and un-watermarked part are differentiated. This differentiation is amplified by these filters; therefore, the watermark information could be obtained with greater accuracy. Experimental results shows that the extracted watermark has better quality than previous approaches.

Qureshi et al. [15] introduced a watermarking method by making watermark as robust and keeping the image fragile simultaneously using Residue Number System (RNS) and Chaotic algorithm. Two watermarks are embedded at two phases while the Residues of Region of Interests (ROI) is generated. The researchers used Spread Spectrum and chaotic key, experimental results show that their method is blind and performs better than some of the previous techniques.

Adi [16] introduced a method that merged CRT and Canny Algorithm which was able to improve the imperceptibility and robustness of watermarked image. The insertion method used embeds the watermark on the edges of the image due to the significant differences in order to maintain imperceptibility. Canny algorithm was employed for indexing the embedding positions. The method has improved the quality of watermarked image with few degradation to the watermarked image.

Sudibyo et al. [18] proposed a method of watermarking by using a sequence of Haar Wavelength Transform (HWT) and Chinese Remainder Theorem (CRT). CRT was applied in embedding the watermarks and the cover image was processed using HWT to produce four sub-bands. Experimental results obtained a Peak Signal to Noise Ratio (PSNR) 63.55dB for watermark with size 8x8 pixel. The method however does not survive some major image processing attacks.

Anggadimas et al. [19] compared the robustness and imperceptibility of watermarking schemes applying the Discrete Cosine Transform-CRT and Discrete Wavelet Transform-CRT methods. The DWT with CRT method is able to provide good compression rate to support the quality of watermark extraction. The same embedding process and watermark bit value in watermarking process result in relatively same PSNR value for both DWT-CRT and DCT-CRT Watermarking.

Prajwalasimha et al. [20] Combined DCT and continuous division based image watermarking. The algorithm execution time decreases at about 25 times than other methods. The algorithms does not experiment the Tamper assessment Function (TAF), however it has much better PSNR and MSE.

Suthar [21] developed a graphical interface tool for image authentication by using two transform technique to embed a watermark. The researcher utilized a combination of Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). The proposed image authentication scheme increases imperceptibility and an increase in robustness. Experimental result indicate that the method is very effective for various security issues and attacks applied on image using single only DCT OR DWT.

Hsu et al. [2] proposed a scheme incorporating the use of Extreme pixel adjustment, mixed modulation (MM), multi-bit party sign-altered mean modulation (MPSAM), , and particle swarm optimization (PSO) using crisscross inter-block quaternion Fourier transform. The scheme was highly efficient in increasing the quality of the image its robustness against most attacks. However, it is computationally complex considering the number of steps involved.

Begum et al. [1] reviewed important aspects of standard watermarking system frameworks and listed some standard accepted requirements that are used in designing watermarking techniques for several different applications and provided a state of art in digital image watermarking. While Security remains a big challenge in digital image watermarking technologies, the adaptation of IoT and block-chain-based authentication schemes provides a challenge for researchers.

4. METHODOLOGY

The main aim of this study is to compare the use of CRT based DCT traditional watermarking algorithm and CRT based DCT zero watermarking algorithm. It will include the process of generating watermark, embedding watermark, extraction and testing.

4.1 Watermark Embedding

In traditional watermark algorithms, once the watermark bit image is generated, CRT technique is used for embedding based [4]. This is achieved by dividing the host image into blocks of 8 X 8 pixels. Thereafter, the selected blocks are then converted into DCT domain where watermark information bits will be embedded.

The scheme applies CRT to the watermark at low frequency area of DCT coefficients. Given the value of X and r=2, then m_1, m_2 are integers of set μ. The residues r_1 and r_2 can be represented as:

$$d = |r_1 - r_2| \qquad \text{(equation 6)}$$

And the maximum value of d by taking the larger of two moduli m_1 and m_2 decrease by one

$$D = max\{m_1, m_2\} - 1 \qquad \text{(equation 7)}$$

4.1.1 CRT Embedding for Traditional Image Watermarking

Step1: Randomly select a 8×8 size block from the host image
Step2: Determine the coefficients block according to DCT conversion
Step3: Select randomly a watermark bit from the watermark information for embedding into the block
Step 4: Choose randomly a DCT coefficient X to be embedded in the block.
Step 5: let $m_1 \, and \, m_2$ be the pair-wise co-prime integer for CRT
Step 6: Apply inverse CRT (forward conversion) to determine x_1 and x_2 by using (equation 4**)**
Step 7: Using (equation 6) determine d and D using (equation 7)
Step 8: if the required condition to embed watermark bit '1' i.e $d \geq \frac{D}{8}$ is not fulfilled, X is modified until it is true.
Step 9: if the required condition to embed watermark bit '0' i.e. $d < \frac{D}{8}$ is not true then X is modified to $\grave{X}$ until it is fulfilled.
Step 10: Rebuild the DCT block with the adjusted DCT coefficient $\grave{X}$ and apply inverse DCT to the block for rebuilding the watermark image block.
Step 11: Repeat all steps from 1-10 for the outstanding blocks until all watermark information bits are embedded into the host iamge.
From Patra [4] the values m1 and m2 is 65, 361 if X is in DC coefficient or 38 and 180 if X is in AC coefficient, .

4.1.2 CRT Embedding for Zero Watermarking

The process procedure of inserting a watermark into a host image is shown in figure 1. The use of the host image is for proofs of key generation during the extraction process. Blocks are extracted in a chaotic way. The process of block selection uses a logistic function based on chaos theory.

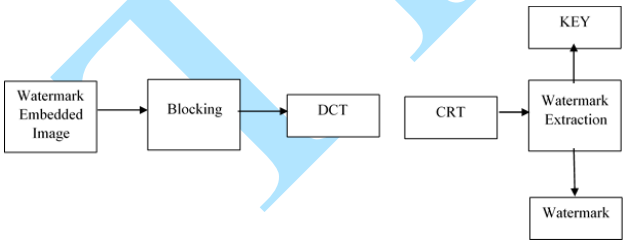


Figure 1. Watermark Embedding using Zero Watermarking

Steps to apply CRT to Zero watermarking is obtained by selecting each DCT block and applying DCT transform to the selected image block is as follows:
Step 1: Split the host image into 8×8 pixel blocks
Step 2: For each block apply DCT and select the DC and 3 low frequency AC coefficients of a block to extract the features of the host.
Step 3: Set the private key K to zero.
Step 4: Let $m_1 \, and \, m_2$ be the pairwise co-prime integers to be used in CRT with values 38 and 107, in that order if region is DC, otherwise $m_1 \, and \, m_2$ are selected as 38 and 55, respectively.
Step 5: find $r_1 \, and \, r_2$ by applying the Inverse CRT (Forward Conversion) to the selected DC and AC coefficients.
Step 6: Determine $d = abs(r_1 \, and \, r_2)$ and $D = \max(m_1, m_2) - 1$.
Step 7: Add 01 or 10 to the secret key K if d $\geq \frac{D}{S}$. if there is no coefficient that satisfies the condition, the binary number is II.
Finally, the produced secret K is recorded with a trusted third party and is used to show its ownership.

4.2 Watermark Extraction

4.2.1 CRT Extraction for Traditional Image Watermarking

Using CRT and Traditional Watermarking, before extracting the watermark, we need some information such as; watermark image, watermark size, start of PRNG (Pseudo Random number generator) and the pair-wise co-prime integers $m_1 \, and \, m_2$.
Utilizing the seed of the PRNG, the watermark information X and DCT coefficient is extracted. The value of b is compared with D. if $b \geq \frac{(D+C)}{2}$, the extracted watermark bit is a '1', otherwise, it is a '0'. This is replicated for the remaining blocks until all watermark information are extracted.

4.2.2 CRT Extraction for Zero Watermarking

Image Blocking, DCT and CRT are applied same way during insertion (See Figure 1), however, the extraction process uses a key to extract the watermark. Additionally the logistic function used during watermark insertion is used to determine the DCT block in which watermark was inserted.
The coefficient X in the block is determined by using the secret key, Forward Conversion (Inverse Chinese Remainder Theorem) is applied to X to get $r_1 \, and \, r_2$, d is determined from $d = abs(r_1 \, and \, r_2)$ and $D = \max(m_1, m_2) - 1$. If $d \geq \frac{D}{s}$, watermark bit '1' is obtained, otherwise, '0' is obtained.

5. RESULTS AND DISCUSSION

Data used in the experiment are 5 images commonly used in digital watermarking schemes, 512 x 512 "Lena", "Mandrill", "Boat", "Jet", and "Pepper". The binary image used as watermark where applicable is 64 x 64 "Panda". The parameter used to test the quality of the watermarking process result is the Peak to Signal Ratio (PSNR) value between the cover

image before watermarking and the watermark image. The equation below is used to calculate PSNR:

$$PSNR = 10\log_{10}\frac{MN(\max P_{x,y})^2}{\sum_{x=1}^{M}\sum_{y=1}^{N}[P_{x,y} - \acute{P}_{x,y}]^2} \quad \text{(equation 8)}$$

5.1 Robustness

Where M and N is the image size $P_{x,y}$ is the initial image and $\acute{P}_{x,y}$ is the watermarked image pixel, while $\max P_{x,y}$ is the maximum intensity value of the image. The results of the watermarking process for the designed scheme are shown in table 1.

Table 1. Comparison of Watermarked image PSNR

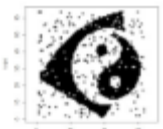
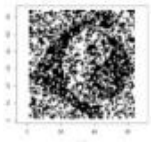
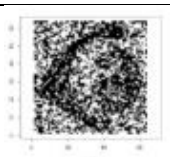
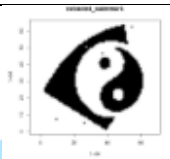
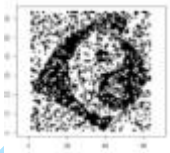
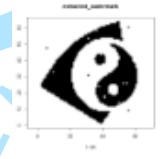
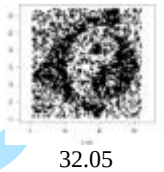
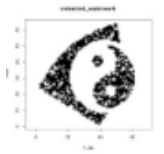
Image	Traditional Watermarking with CRT (dB)	Zero Watermarking with CRT (dB)
Lena	47.95	∞
Mandrill	48.20	∞
Boat	48.71	∞
Jet	49.11	∞
Pepper	49.32	∞

As shown in Table 1, the watermarking process using Traditional Watermarking with CRT and Zero Watermarking with CRT performs differently since Zero watermarking results in distortion free watermarks. The quality of watermarked in PSNR is infinite therefore better than that of traditional watermark embedding.

5.2 Resistance to Attacks

Evaluation of robustness resisting several attacks such as JPEG lossy compression, blurring, sharpening, and cutting edges have been performed. The Tamper Assessment Function (TAF) is used to determine the quality of the extracted image.

Table 2. Relationship between Extracted Watermarks for LENA (Values in TAF) using Traditional Watermarking with CRT and Zero Watermarking with CRT

Attack	Traditional Watermark with CRT %	Zero Watermarking with CRT %
No attack	 3.96	 0.00
JPEG Lossy Compression	 34.09	 0.10
Blurring	 35.40	 0.12
Sharpening	 25.10	 0.30
Cutting Edges	 32.05	 10.01

From Table 2 it can be shown that with no attack, the quality of the extracted watermarks in CRT-based traditional watermarking still contains errors. Zero watermarking with CRT has better performance even though it is susceptible to cropping attacks.

5.3 Time of Execution

The execution time is determined for both embedding and extraction processes. Intel i5 processor @ 1.80 GHz, 8GB DDR RAM and Windows 10 OS. The table shows the execution time in seconds for both approaches.

Table 3. Comparing the time of Execution during Embedding and Extraction

	Traditional Watermarking with CRT	Zero Watermarking with CRT
Watermark Embedding	0.12	0.09
Watermark Extraction	0.46	0.064

CONCLUSION

The Zero watermarking scheme with CRT shows much performance than that of the traditional watermarking with CRT. Without any attack, the traditional Watermarking with CRT still has a high Tamper assessment function due to the DCT

transformation. Zero watermarking with CRT also underperforms under some image processing attacks such as cropping. The computational complexity in Zero watermarking with CRT is better and faster when compared with the traditional watermarking with CRT.

REFERENCES

[1] **M. Begum and M. S. Uddin**, "Digital Image Watermarking Techniques : A Review," 2020.

[2] **L. Hsu and H. Hu**, "Blind watermarking for color images using EMMQ based on QDFT," *Expert Syst. Appl.*, p. 113225, 2020.

[3] **H. Kim**, "CRT-Based Color Image Zero-Watermarking on the DCT Domain," vol. 11, no. 3, pp. 39–46, 2015.

[4] **J. C. Patra, A. K. Kishore, and C. Bornand**, "Improved CRT-based DCT Domain Watermarking Technique with Robustness Against JPEG Compression for Digital Media Authentication," pp. 2940–2945, 2011.

[5] **H. K.-S. S. Kim**, "DCT Domain Zero Watermarking based on DCT," pp. 9–15, 2011.

[6] **M. B. Ibrahim and K. A. Gbolagade**, "A Chinese Remainder Theorem Based Enhancements of Lempel-ziv-welch and Huffman Coding Image Compression," vol. 3, no. 3, pp. 1–9, 2019.

[7] **J. C. Patra, J. E. Phua, and C. Bornand**, "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression," *Digit. Signal Process.*, vol. 20, no. 6, pp. 1597–1611, 2010.

[8] **P. Shiu, C. Lin, J. Jan, and Y. Chang**, "A DCT-based Robust Watermarking Scheme Surviving JPEG Compression with Voting Strategy," vol. 3, no. 4, pp. 259–277, 2018.

[9] **J. C. Patra, A. Karthik, and C. Bornand**, "A novel CRT-based watermarking technique for authentication of multimedia contents," *Digit. Signal Process.*, vol. 20, no. 2, pp. 442–453, 2010.

[10] **X. F. Luo, Q. Xu, and J. Zhang**, "A Digital Watermarking Algorithm Based on Chinese Remainder Theorem," no. 4, pp. 0–3, 2014.

[11] **A. Benoraira, K. Benmahammed, and N. Boucenna**, "Blind image watermarking technique based on differential embedding in DWT and DCT domains," *EURASIP J. Adv. Signal Process.*, vol. 2015, no. 1, 2015.

[12] **S. A. Kasmani**, "A Pre-Filtering Method to Improve Watermark Detection Rate in DCT Based Watermarking," no. March 2014, 2015.

[13] **I. A. Ansari, M. Pant, and C. W. Ahn**, "ABC optimized secured image watermarking scheme to find out the rightful ownership," *Optik (Stuttg).*, vol. 127, no. 14, pp. 5711–5721, 2016.

[14] **I. A. Ansari, M. Pant, and C. W. Ahn**, "Robust and false positive free watermarking in IWT domain using SVD and ABC," *Eng. Appl. Artif. Intell.*, vol. 49, pp. 114–125, 2016.

[15] **I. M. Qureshi and Z. Muzaffar**, "Fi rs t O in nl e P lic ub at," no. March, 2016.

[16] **P. W. Adi**, "Imperceptible Image Watermarking based on Chinese Remainder Theorem over the Edges," no. September, pp. 19–21, 2017.

[17] **U. Sudibyo, F. Eranisa, E. H. Rachmawanto, D. R. Ignatius, M. Setiadi, and C. A. Sari**, "A Secure Image Watermarking using Chinese Remainder Theorem Based on Haar Wavelet Transform."

[18] **U. Sudibyo, F. Eranisa, E. H. Rachmawanto, D. R. Ignatius, M. Setiadi, and C. A. Sari**, "A Secure Image Watermarking using Chinese Remainder Theorem Based on Haar Wavelet Transform," no. October, 2017.

[19] **N. M. Anggadimas, O. Setyawati, and M. Aswin**, "Comparison of DWT-CRT And TLDCT-CRT Methods In Digital Watermarking," vol. 20, no. 3, pp. 73–78, 2018.

[20] **S. N. Prajwalasimha, C. S. S, and C. S. Mohan**, "Performance analysis of DCT and successive division based digital image watermarking scheme," vol. 15, no. 2, pp. 750–757, 2019.

[21] **A. C. Suthar and G. R. Kulkarni**, "Graphical User Interface Software Model for Real Time Image Authentication," no. March 2013, 2019.