

CRT-Based Color Image Zero-Watermarking on the DCT Domain

HyungDo Kim

Department of Management Information Systems
Hanyang Cyber University, Seoul, 04763, Rep. of Korea

ABSTRACT

When host images are watermarked with CRT (Chinese Remainder Theorem), the watermark images are still robust in spite of the damage of the host images by maintaining the remainders in an unchanged state within some range of the changes that are incurred by the attacks. This advantage can also be attained by “zero-watermarking,” which does not change the host images in any way. This paper proposes an improved zero-watermarking scheme for color images on the DCT (Discrete Cosine Transform) domain that is based on the CRT. In the scheme, RGB images are converted into YCbCr images, and one channel is used for the DCT transformation. A key is then computed from the DC and three low-frequency AC values of each DCT block using the CRT. The key finally becomes the watermark key after it is combined four times with a scrambled watermark image. When watermark images are extracted, each bit is determined by majority voting. This scheme shows that watermark images are robust against a number of common attacks such as sharpening, blurring, JPEG lossy compression, and cropping.

Key words: CRT, Color Images, DCT, Watermarking, Zero-watermarking.

1. INTRODUCTION

Digital watermarking is the process for hiding a digital watermark into a digital signal such as image data. As the age of Internet and multimedia advances, such a technique for protecting intellectual property of digital contents from illegal usage becomes more and more important. Most methods of digital watermarking modify the original data while embedding the watermark [1]. The secret watermark information distorts more or less the original data at the same time. This incurs a conflict between robustness and invisibility.

Zero-watermarking was proposed for solving this conflict. It is a way to build some connection between the original data and the watermark [2]. There is no distortion of the original data in building the connection. That is, the distortion problem to the original data due to watermark embedding is completely eliminated. After retrieving the so-called relationship, it could be stored in a watermark registration center, where it became the resource for copyright protection. The most important part of a zero-watermarking method is the image feature detection method [3]. Two desirable properties are stability and otherness. The one is the ability to detect the image feature after it is attacked. The other is the ability to differentiate the image features from those of different images.

Chinese remainder theorem (CRT) [4] is about how to find an integer, when some divisors and their corresponding remainders are given. The use of the CRT in watermarking gray

images provides advantage in terms of improved security and low computational complexity as the study of Patra et al. [5] shows. In addition, CRT-based watermarking is robust by keeping remainders unchanged within some range of changes in spite of distortion in host images.

For employing this advantage of CRT in zero-watermarking, DCT0CRT (DCT domain Zero-watermarking based on CRT) [6] was proposed. It is a CRT-based zero-watermarking technique for gray images in the domain of DCT. Among the DC and two low-frequency AC coefficients of each DCT block chosen in a chaotic way from the original data (i.e. host image in image watermarking), one is selected by testing whether it satisfies the CRT-based condition matching with the watermark bit to be embedded. The first element of the DCT block, i.e. the DC coefficient, is the average of the pixel values, while the remaining elements, i.e. AC coefficients, are independent of the average. Low frequency AC coefficients represent gradual color change across the pixel values. That is, the most stable and important coefficients of each DCT block are used for building the relationship. Experimental results show that inserted watermarks are robust against some common attacks such as sharpening, blurring, and JPEG lossy compression. However, DCT0CRT is just for gray images and has some drawbacks in protecting host images against attacks such as cropping. This paper proposes how to apply CRT-based zero-watermarking to color images with enhanced robustness by improving the drawbacks.

The rest of the paper is organized as follows: Section 2 reviews the previous work in the area of CRT-based DCT-domain watermarking. The zero-watermarking scheme for color images is then proposed in Section 3. The experimental

* Corresponding author, Email: hdkim@hycu.ac.kr
Manuscript received Jun. 18, 2015; revised Aug. 27, 2015;
accepted Sep. 03, 2015

results and performance comparison with the other two schemes introduced in Section 2 are provided in Section 4. Finally, the paper is summarized with some future research directions in Section 5.

2. RELATED WORK

2.1 CRT

The theorem can be compactly defined as follows [5]. Let μ be a set of r integers given by $\mu = \{M_1, M_2, \dots, M_r\}$, such that any two M_i are pair-wise relatively prime. Let's assume that a set of r simultaneous congruences be given by

$$Z \equiv R_i \pmod{M_i}, \quad (1)$$

where $R_i, i = 1, 2, \dots, r$, are called residues. The solution for the integer Z can be found as

$$Z \equiv \left(\sum_{i=1}^r R_i \frac{M}{M_i} K_i \right) \pmod{M}, \quad (2)$$

where M is the product of all M_i , and K_i are determined from

$$K_i \frac{M}{M_i} \equiv 1 \pmod{M_i} \quad (3)$$

Let us take a simple example with $r = 2, M_1 = 7, M_2 = 9, R_1 = 3$ and $R_2 = 4$. That is, Z satisfies the two congruences: $Z \equiv R_1 \pmod{M_1}$ and $Z \equiv R_2 \pmod{M_2}$. M is 55 by the product of M_1 and M_2 . K_1 and K_2 are determined by the two congruences $K_1 M_2 \equiv 1 \pmod{M_1}$ and $K_2 M_1 \equiv 1 \pmod{M_2}$. We can find that $K_1 = 4$ and $K_2 = 4$ satisfy the congruences. From $Z \equiv R_1 M_2 K_1 + R_2 M_1 K_2 \pmod{M}$, we can conclude that $Z = 31$.

Inverse CRT is to represent a positive integer Z (which is less than M) by a set of integers $\{R_1, R_2, \dots, R_r\}$ given μ and M . Each R_i is obtained from the congruence (1). Let us take a simple example with $M_1 = 7, M_2 = 9, Z = 49$. From $49 \equiv R_1 \pmod{7}$ and $49 \equiv R_2 \pmod{9}$, we can find that $R_1 = 0, R_2 = 4$. Therefore, Z can be represented as $\{0,4\}$.

2.2 CRT-Based Watermarking on the DCT Domain

Digital watermarking techniques can be classified into two categories: spatial-domain techniques and transform-domain techniques [7]. The former techniques modify the pixel values of the host image. On the other hand, the latter techniques first convert the host image into frequency domain by a transformation method such as discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT), and so on. Transform-domain coefficients are then modified by the watermark. Inverse transform is finally applied to obtain the watermarked image. Transform-domain techniques are generally more robust against attacks than spatial-domain ones.

A discrete cosine transform (DCT) expresses a finite sequence of data points in terms of a sum of cosine functions

oscillating at different frequencies. There are several variants of the DCT with slightly modified definitions. The most commonly used form can be expressed by the following equation. N real numbers x_0, \dots, x_{N-1} are transformed into N real numbers X_0, \dots, X_{N-1} according to the equation.

$$X_k = \sum_{n=0}^{N-1} x_n \cos \left[\frac{\pi}{N} \left(n + \frac{1}{2} \right) k \right], \quad k = 0, 1, \dots, N-1 \quad (4)$$

DCT is usefully employed in diverse science and engineering applications, e.g. JPEG lossy image compression, where N is typically 8. The 64 coefficients of a JPEG DCT block are arranged in a sequence of Fig. 1 in which the left-top element is the DC (zero-frequency) component and entries with increasing vertical and horizontal index values represent higher vertical and horizontal spatial frequencies. The DC coefficient is the average of the pixel values, while the remaining elements, i.e. AC coefficients, are independent of the average. Low frequency AC coefficients represent gradual color change across the pixel values.

	0	1	2	3	4	5	6	7
0	0	1	5	6	14	15	27	28
1	2	4	7	13	16	26	29	42
2	3	8	12	17	25	30	41	43
3	9	11	18	24	31	40	44	53
4	10	19	23	32	39	45	52	54
5	20	22	33	38	46	51	55	60
6	21	34	37	47	50	56	59	61
7	35	36	48	49	57	58	62	63

Fig. 1. Sequence numbers of coefficients of a DCT block

Based on the CRT properties, a CRT-based DCT-domain watermarking scheme has been reported in [5] in order to improve a CRT-based spatial-domain watermarking scheme [8] whose main drawback is its inability to withstand JPEG compression. CRT is mainly employed in watermarking for increasing security. A large integer Z can be represented by a set of smaller integers called residues of dividing it by a set of relatively prime numbers. Such computation is efficient due to the CRT properties of simultaneous congruence and modular arithmetic. On the contrary, it is very difficult to get back the original integer Z without knowledge of the set of divisors.

The scheme embeds one watermark bit per DCT block by checking the required condition of $d \geq D/s$ for watermark bit 1 and of $d < D/s$ for watermark bit 0, where $d = \text{abs}(R1-R2), R1 = Z \text{ mod } M1, R2 = Z \text{ mod } M2, D = \text{max}(M1,M2) - 1, s = 2$ if Z is DC coefficient, otherwise, $s=4$. $M1$ and $M2$ are the pair-wise co-prime numbers to be used in the CRT. If the condition does not satisfy, then 8 is added to or subtracted from Z recursively until the condition satisfies. The reason for using ± 8 to make

modifications to the selected DCT coefficient is that it provides sufficient amount of modification in the DCT domain that would be reflected in the spatial domain [5]. However, it is inevitable that this modification degrades the quality of the host image in spite of much effort for maintaining imperceptibility.

2.2 CRT-Based Zero-Watermarking on the DCT Domain

Zero-watermarking was proposed for solving the conflict between robustness and invisibility in conventional digital watermarking, where the secret watermark information embedded into the host image distorts more or less the original data. Instead of watermark embedding, zero-watermarking extracts some distinctive features from the host image. As a result, there is no distortion of the original data in zero-watermarking. The owner's information is not reflected in the image features because they are just meaningless bit stream. An encryption method can be employed for embedding meaningful information into the features. The zero-watermark is then stored in a watermark registration center, where it becomes the resource for copyright protection.

Two desirable properties of zero-watermarking are stability and otherness [3]. The one is the ability to detect the image features after it is attacked. The other is the ability to differentiate the image features from those of different images. For supporting the properties, there are many fields of research on image zero-watermarking [9]: spatial-domain, transform-domain, image moment, principal components analysis, and so on.

DCT has been a hot topic for the digital watermarking in transform domain because it needs less computation and is compatible with the international standards of data compression [10]. Based on DCT, a zero-watermarking method DCT0CRT for gray images was introduced by Kim and Sohn [6], where CRT was applied to one of DC and 2 low-frequency AC values of each DCT block chosen by a chaotic way. The method tries to embed one watermark bit per DCT block by checking the required condition of $d \geq D/s$ for watermark bit 1 and of $d < D/s$ for watermark bit 0, where $d = \text{abs}(R1-R2)$, $R1 = Z \text{ mod } M1$, $R2 = Z \text{ mod } M2$, $D = \text{max}(M1,M2) - 1$. The same variables are used as in the CRT-based DCT-domain watermarking scheme. If the condition satisfies with DC, two bits of '00' are added to the private key K. If not, the two AC coefficients are checked sequentially. Two bits of '01' or '10' are added to the private key, if the condition satisfies. Otherwise, two bits of '11' are added to the private key.

The use of the CRT in the zero-watermarking method provides advantage in terms of improved security and low computational complexity as in conventional watermarking [5]. In addition, it is robust by keeping watermark data from damage in spite of some degree of the host image distortion. This enhances the stability of the zero-watermarking. However, the method does not consider color images and the key does not catch the image features. Furthermore, the method does not use any encryption method to embed meaningful information into image features or the key.

Simple DCT-based zero-watermarking methods are also proposed for protecting medical images [10] and text images [11]. They are using signs of low-frequency AC coefficients of

DCT blocks as the zero-watermark. They are also just for gray images.

3. PROPOSED SCHEME FOR COLOR IMAGES

Current zero-watermarking algorithms mainly focus on the methods of embedding watermarks into the gray host image in spite of much research on the conventional watermarking algorithms for color images [12]. Based on the DCT0CRT, this paper proposes an improved zero-watermarking algorithm for color images.

3.1 Watermark Embedding Procedure

In the first phase, a RGB host image is converted to YCbCr color space by the following equations, where Y component is luminance, Cb component blue chrominance, and Cr component red chrominance.

$$\begin{aligned}
 Y &= 0.299 * R + 0.587 * G + 0.114 * B \\
 Cb &= -0.168736 * R - 0.331264 * G + 0.5 * B + 128 \\
 Cr &= 0.5 * R - 0.418688 * G - 0.081312 * B + 128
 \end{aligned}$$

This is done because the latter is more robust and has higher imperceptibility than the former [13]. The algorithm uses the blue chrominance component for extracting features from the cover(host) image on the basis of HVS (Human Visual System). According to the HVS, the higher the background luminance and the more complicated the image texture, the lower the human visual system's sensitivity to its variations. In order to get better transparency, it is strongly recommended to select those blocks with high luminance and complicated texture for the conventional image watermarking [14]. There were largely two approaches for block selection in the conventional image watermarking: the selection of best blocks [14] and the selection of a best region such as a quadrant [13]. In order to simplify the zero-watermarking process, the algorithm removes the complex selection of blocks or regions. Instead, the algorithm adopts multiply embedding the watermark image into regions such as quadrants.

In the watermark embedding process, scrambling transformation is applied to the binary watermark W, where the watermark image becomes a meaningless chaotic one. It plays the role of secondary encryption of the watermark image via upsetting the relationship between the space locations of pixels [15]. This will improve the robustness of the algorithm. Two-dimensional Arnold scrambling as follows is used:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ mod } N, \quad x, y \in \{0,1,\dots, N-1\} \quad (5)$$

The pixel coordinates of the original space are x and y, while those after scrambling are x' and y'. N is the size of the rectangular image, also referred to as a step number. The transformation can be applied iteratively taking K as the iteration number.

The initial state can be restored according to the corresponding iterations by the following equation.

$$\begin{bmatrix} x \\ y \end{bmatrix} = \left\{ \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \right\} \bmod N, \quad x', y' \in \{0, 1, \dots, N-1\} \quad (6)$$

The watermark embedding algorithm can be described as follows:

- (1) Divide the host image I into 8x8 pixels blocks.
- (2) Set the private key K to blank.
- (3) For each block
 - A. Apply DCT conversion to the block.
 - B. Select DC and 3 low-frequency AC coefficients of a block to extract the features of the host image.
 - C. Let M1 and M2 be the pairwise co-prime numbers to be used in CRT with values 38 and 107, respectively, in the case of DC. Otherwise, those of M1 and M2 are selected as 38 and 55, respectively.
 - D. Find R1 and R2 by applying the inverse CRT to the selected DC and AC coefficients.
 - E. Determine $d = \text{abs}(R1-R2)$ and $D = \max(M1, M2) - 1$.
 - F. Add '1' bit to the private key K if $d \geq D/s$. Otherwise, add '0' bit to K.
- (4) Scramble the watermark image W of size $m \times n$ with IN as the iteration number of Arnold transformation into the scrambled watermark SW.
- (5) Apply bitwise XOR operations to the key K and a multiple of the scrambled watermark MSW in order to build the watermarked key. The multiple is noted as MSW. The scrambled watermark can be used multiple times if the key is longer than the scrambled watermark. If we are using quadrants of the host image for extracting features corresponding to the watermark, the scrambled image is used 4 times.
- (6) Register the watermarked key into the third party to preserve the ownership of the host image.

3.2 Watermark Extraction Procedure

The process of acquiring the features of a test image is the same as in steps (1)-(3) of the watermark embedding procedure. Let the features (i.e. the private key of the test image) be noted as K' . The watermark extraction algorithm can be summarized as follows:

- (1) Divide the test image I' into 8x8 pixels blocks.
- (2) Set the private key K' to blank.
- (3) For each block
 - A. Apply DCT conversion to the block.
 - B. Select DC and 3 low-frequency AC coefficients of a block to extract the features of the test image.
 - C. Let M1 and M2 be the pairwise co-prime numbers to be used in CRT with values 38 and 107, respectively, in the case of DC. Otherwise, those of M1 and M2 are selected as 38 and 55, respectively.
 - D. Find R1 and R2 by applying the inverse CRT to the selected DC and AC coefficients.
 - E. Determine $d = \text{abs}(R1-R2)$ and $D = \max(M1, M2) - 1$.
 - F. Add '1' bit to the private key K' if $d \geq D/s$. Otherwise, add '0' bit to K' .
- (4) Apply bitwise XOR operations to the private key K' of the test image and the watermarked key K, fetched from the third party, in order to extract multiple scrambled images, denoted as MSW'.

(5) Unscramble MSW' with IN as the iteration number of Arnold transformation into multiple images MW'.

(6) Determine the extracted watermark image W' from MW' using a strategy such as voting and best region selection. In the voting strategy, each region votes for the bit value of a specific position of the extracted watermark image. This strategy does not need the watermark image. On the other hand, in the best region selection strategy, one region such as a quadrant of MW' is selected as W' for best matching the watermark image. Tamper Assessment Function (TAF) [16] as follows can be used for selecting the best region.

$$TAF(W, W') = \frac{1}{mn} \left[\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} W(i, j) \oplus W'(i, j) \right] \times 100 \quad (7)$$

(7) Calculate TAF between W and W'. Given a watermark detection threshold T, if $TAF < T$, then we conclude that there is the watermark in the test image. Otherwise, we conclude that there is not.

4. EXPERIMENTAL RESULTS

In order to verify the effectiveness of the proposed algorithm, experiments are carried out using 24-bit true color host images of size 512x512 commonly called "Lena", "Peppers", and "Baboon" as in Fig. 2. A gray image of size 64x64 shown in Fig. 3 has been used for the digital watermark.



(a) Lena (b) Peppers (c) Baboon
Fig. 2. The three host images (512x512)



Fig. 3. The watermark image (64x64)

For demonstrating the watermark embedding and extraction processes, let us take an example of "Lena" image. The image in RGB color space is first converted to one in YCbCr color space. The values of the Cb component are then divided into 64x64 blocks, from which the private key K is extracted. The key has the size of 4x64x64 and looks like Fig. 4. The 4-fold replications of the watermark image as Fig. 5 are embedded into the key after its scrambling. The result of the scrambling looks like Fig. 6. An XOR operation is utilized to embed the scrambled into the key. Finally, we get the watermarked key (i.e. the zero-watermark) of Fig. 7. We should

keep the watermarked key into the third party to preserve the ownership of the host image.

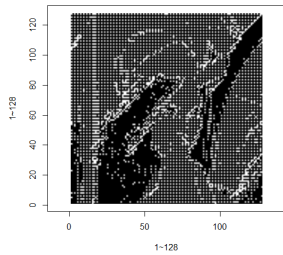


Fig. 4. The private key extracted from “Lena”

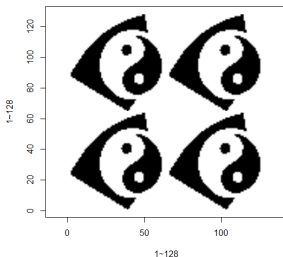


Fig. 5. The 4-fold replication of the watermark image

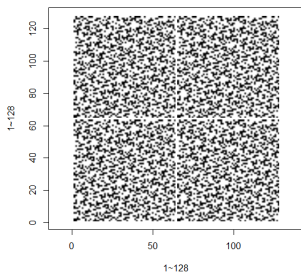


Fig. 6. The scrambled result

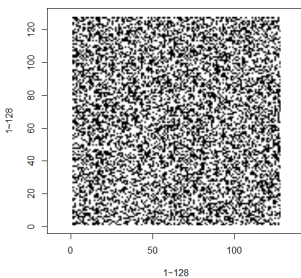


Fig. 7. The watermarked key (the zero-watermark)

The extraction process is the reverse of the embedding process. Let’s assume the test image is the same with the host image. If we apply an XOR operation to the private key Fig 4 extracted from the test image and the watermarked key, we get the scrambled image of Fig. 6. Through unscrambling, we get the extracted watermark image of Fig 5. Using any strategy, we get the watermark image of Fig. 3.

In this study, performance comparison is carried out among the 3 CRT-based watermarking schemes: the scheme of Patra et al. [5], DCT0CRT [6], and the scheme proposed in this paper, considering the quality of the watermarked images, the quality of the watermarks extracted, and robustness of the schemes to different attacks. The quality of modified (watermarked) images against the host image is measured by Peak Signal-to-Noise Ratio (PSNR), which is given by the following equation:

$$PSNR(dB) = 10 \log_{10} \left[\frac{mn \times \{\max_{i,j} I(i,j)\}^2}{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \{I(i,j) - I'(i,j)\}^2} \right] \quad (8)$$

Because DCT0CRT and the scheme proposed in this paper are using the zero-watermarking technique which makes watermarked images distortion-free, quality of watermarked images in PSNR is infinite by the definition of (8) and is better than that of Patra et al.’s as the following table shows.

Table 1. Quality of watermarked images compared with respective host image

Scheme \ Image	Patra et al. [5]	DCT0CRT [6]	Proposed Scheme
Lena	48.85	∞	∞
Peppers	49.21	∞	∞
Baboon	49.33	∞	∞

Comparative experiments of robustness resisting typical kinds of conventional attacks such as sharpening, blurring, JPEG lossy compression (quality factor 90), cutting edges, and cutting a quadrant have been performed. Samples of the zero-watermarked Lena images under the attacks are shown in Fig. 8.

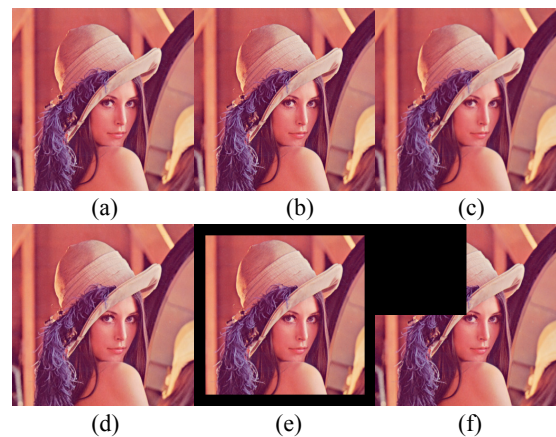


Fig. 8. Zero-watermarked Lena image under different attacks: (a) without attack, (b) sharpening, (c) blurring, (d) JPEG lossy compression, (e) cutting edges, and (f) cutting a quadrant.

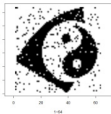
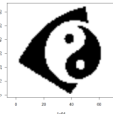
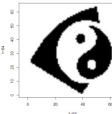
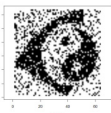
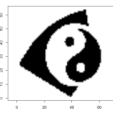
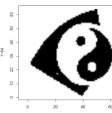
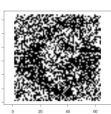
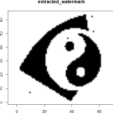
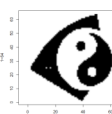

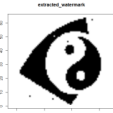
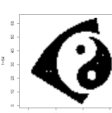

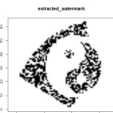
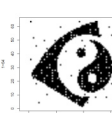
The quality of an extracted watermark is determined by its TAF value. A lower TAF value indicates that the extracted watermark is more similar to the original watermark. The

extracted watermarks from the watermarked Lena images can be summarized by as in Table 2, those from the watermarked Peppers images in Table 3, and those from the watermarked Baboon images in Table 4.

As you can see from the tables, the scheme of Patra et al. does not show better performance than the other two schemes under all attacks. Even without any attacks, extracted watermarks have some errors due to the rounding in the conversion of RGB and YCrCb as well as the watermark embedding. Furthermore, it is hard to recognize the symbol of the watermark image from extracted watermarks in attacks other than sharpening. If we select a TAF value as the threshold for watermark detection, e.g., 5.0%, it is impossible to detect the watermark from all the attacked images in the scheme.

The scheme of DCT0CRT and the proposed scheme show much better performance than that of Patra et al. However, under attacks of cropping (edges and a quadrant), performance of the DCT0CRT scheme is not so good. On the other hand, good performance is retained in the proposed scheme even under the cropping attacks due to the redundancy in watermark embedding and voting in extraction.

Table 2. Comparison of extracted watermarks for Lena (Values in TAF)

Scheme Attack	Scheme of Patra et al.	Scheme of DCT0CRT	Proposed scheme
No attack	 6.01%	 0.00%	 0.00%
Sharpening	 20.09%	 0.00%	 0.02%
Blurring	 38.82%	 0.10%	 0.05%
JPEG lossy compression	 48.68%	 0.12%	 0.10%
Cutting edges	 31.03%	 14.79%	 3.10%

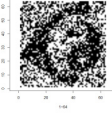
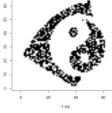
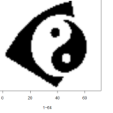
Cutting a quadrant	 32.59%	 11.11%	 0.0%
--------------------	--	---	---

Table 3. Comparison of extracted watermarks for Peppers (Values in TAF)

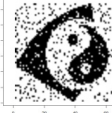
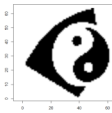


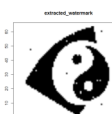

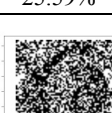
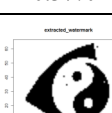

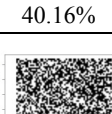
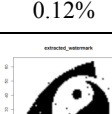

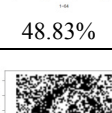
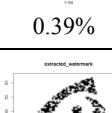
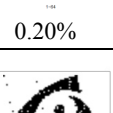
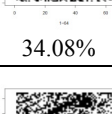
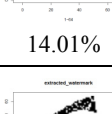
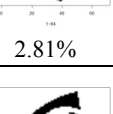



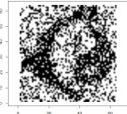

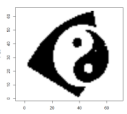


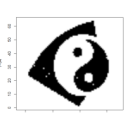


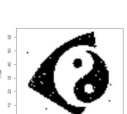


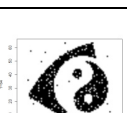
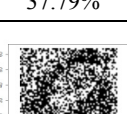


Scheme Attack	Scheme of Patra et al.	Scheme of DCT0CRT	Proposed Scheme
No attack	 10.79%	 0.00%	 0.00%
Sharpening	 25.59%	 0.37%	 0.02%
Blurring	 40.16%	 0.12%	 0.02%
JPEG lossy compression	 48.83%	 0.39%	 0.20%
Cutting edges	 34.08%	 14.01%	 2.81%
Cutting a quadrant	 35.40%	 9.01%	 0.00%

Table 4. Comparison of extracted watermarks for Baboon (Values in TAF)

Scheme Attack	Scheme of Patra et al.	Scheme of DCT0CRT	Proposed Scheme
No attack	 8.57%	 0.00%	 0.00%

Sharpening	 28.83%	 0.15%	 0.05%
Blurring	 40.50%	 0.46%	 0.17%
JPEG lossy compression	 46.61%	 TAF: 0.83%	 TAF: 0.88%
Cutting edges	 37.79%	 16.48%	 3.64%
Cutting a quadrant	 37.21%	 10.25%	 0.00%

5. CONCLUSION

In this paper, a novel zero-watermarking scheme for color images has been presented. It applies DCT and CRT to the blue chrominance channel of color images in the YCrCb color space. As in watermarking host images conventionally with CRT, where watermark images are robust in spite of damages in host images, the proposed zero-watermarking scheme has a very strong robustness against different attacks. In addition, it has no affect on the quality of the original image as zero-watermarking schemes do. The following can be concluded by the experimental results:

- i) the performance of the scheme is fundamentally better than that of the conventional CRT-based scheme,
- ii) the performance of the scheme is mostly better than that of the CRT-based zero-watermarking scheme for gray images, and
- iii) redundant embedding of a watermark and voting in the watermark extraction improves the quality of extracted watermarks, especially in cropping.

Further research directs toward how to apply the scheme to diverse applications such as sharing delivery receipts watermarked for identifying their receivers in mobile environments.

REFERENCES

- [1] C. Hanqiang, X. Hua, L. Xutao, L. Miao, Y. Sheng, and W. Fang, "A Zero-Watermarking Algorithm Based on DWT and Chaotic Modulation," Proc. of SPIE, vol. 6247, , Apr. 2006, pp. 624716-1-624716-9.
- [2] L. Zhang, P. Cai, X. Tian, and S. Xia, "A Novel Zero-Watermarking Algorithm Based on DWT and Edge Detection," Proc. of 4th Int. Congress on Image and Signal Processing, Oct. 15-17, 2011, pp.1016-1020.
- [3] X. Leng, J. Xiao, and Y. Wang, "A Robust Image Zero-Watermarking Algorithm Based on DWT and PCA," Proc. of 1st Int. Conf. on Communications and Information Processing, Mar. 7-11, 2012, pp.484-492.
- [4] Y.H. Ku and X. Sun, "The Chinese Remainder Theorem," Journal of the Franklin Institute, vol. 329, no. 1, Jan. 1992, pp.93-97.
- [5] 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, Dec. 2010, pp. 1597-1611.
- [6] H. D. Kim and K. S. Sohn, "DCT Domain Zero-Watermarking Based on CRT," Journal of the Korea Contents Associations, vol. 11, no. 1, Jan. 2011, pp. 9-15.
- [7] I. Nasir, Y. Weng, and J. Jiang, "A New Robust Watermarking Scheme for Color Image in Spatial Domain," Proc. of 3rd Int. IEEE Conf. on Signal-Image Technologies and Internet-based System, Dec. 16-18, 2007, pp. 942-947.
- [8] J. C. Patra, A. Karthik, and C. Bornand, "A Novel CRT-Based Watermarking Technique for Authentication of Multimedia Contents," Digital Signal Processing, vol. 20, no. 2, Mar. 2010, pp. 442-453.
- [9] X. Leng, J. Xiao, D. Li, and Z. Shen, "Study on the Digital Image Zero-Watermarking Technology," Advanced Materials Research, vol. 765-767, 2013, pp. 1113-1117.
- [10] C. Dong, J. Li, H. Zhang, and Y. Chen, "Robust Zero-Watermarking for Medical Image Based on DCT," Proc. of 6th Int. Conf. on Computer Sciences and Convergence Information Technology, Nov. 29 – Dec. 1, 2011, pp. 900-904.
- [11] G. Feng and X. Huang, "An Improved DCT Based Zero-Watermarking Algorithm for Text Image," Proc. of 2012 Int. Conf. on Anti-Counterfeiting, Security and Identification (ASID), Aug. 24-26, 2012, pp. 1-4.
- [12] T. Zhang and Y. Du, "A Digital Watermarking Algorithm for Color Images Based on DCT," Proc. of Int. Conf. on Information Engineering and Computer Science (ICIECS), Dec. 19-20, 2009, pp. 1-4.
- [13] G. B. Sulong, H. Hasan, A. Selamat, M. Ibrahim, and Saparudin, "A New Color Image Watermarking Technique Using Hybrid Domain," Int. Journal of Computer Science Issues, vol. 9, no. 6, Nov. 2012, pp. 109-114.
- [14] Y. Zhou and J. Liu, "Blind Watermarking Algorithm Based on DCT for Color Images," Proc. of 2nd Int. Congress on Image and Signal Processing, Oct. 17-19, 2009, pp. 1-3.
- [15] J. Li and S. Miao, "The Medical Image Watermarking Using Arnold Scrambling and DFT," Proc. of 2nd Int. Conf.

on Computer Science and Electronics Engineering (ICCSEE), Mar. 22-23, 2013, pp. 192-195.

- [16] D. Kundur and D. Hatzinakos, "Digital Watermarking for Telltale Tamper Proofing and Authentication," Proc. of the IEEE, vol. 87, no. 7, Jul. 1999, pp. 1167-1180.



HyoungDo Kim

He received his B.S. in industrial engineering from Seoul National University, Korea and also received his M.S. and Ph.D. degrees in management science from KAIST. Since then, he worked for a telecommunication company in the research of electronic commerce and Internet services for more than 6 years. He joined the faculty of Hanyang Cyber University in 2003. His main research interests include data mining, electronic commerce, digital watermarking, and e-learning.