Extended DCT domain for improving the quality of watermarked image

Ta Minh Thanh, Nguyen Trung Thanh
Dept. of Network Security, Le Quy Don Technical University, 236 Hoang Quoc Viet, Cau Giay, Ha Noi, Viet Nam. Email: thanhtm@mta.edu.vn.

***Abstract*—In this paper, we propose a novel and robust image watermarking based on the extended DCT domain, called q-DCT domain. By using the extended DCT domain, we can control the quality of the watermarked image. In our proposed scheme, we embed the watermark in the low-frequency of q-DCT domain in order to achieve the robustness of watermark. We also choose in our method a watermarking technique in the category of quantization index modulation (QIM) due to its good robustness and blindness. In our proposed method, the tradeoff of robustness and quality can be controlled by the parameters of QIM and the parameter q of logarithm transform.**

***Keywords*-q-logarithm DCT (q-DCT), Image Watermarking, Quantization Index Modulation (QIM)**

I. Introduction

With the development of computer and network techniques, the Internet-based data transmission has become the most popular channel for various forms of digital media such as picture, audio, movie, and so on. However, since the environment of the Internet is open, everyone can easily copy and alter or even stole the digital content. Therefore, the protection of digital content via network has become a great deal of an important research topic in recent years. Among them, digital watermarking is the promising technique to achieve copyright protection which protects the digital content by embedding the secret information (users' information) directly into the content. This secret information can be extracted later for authentication, copyright protection, traitor detection, etc [1]. Important requirements of digital watermarking are invisibility, robustness, and the embedded data capacity. Namely, the watermark should not be perceived the changes of the digital content to maintain content quality. It also must be robust to image distortions applied to the embedded content. Finally, the watermark must be easily extracted to prove ownership and to detect the traitor.

In general, watermarking methods can be classified into two categories: spatial domain watermarking and transform domain watermarking. In the spatial domain watermarking, watermark information is embedded directly into the components of original content such as RGB information by modifying its value [2]. It has the advantages of low complexity and easy to implement. However, the spatial domain watermarking methods are not robust against image processing attacks, geometrical attacks. On the other hand, the transform domain watermarking methods embed the watermark information by adjusting the magnitude of coefficients in the transform domain such as discrete Fourier transform (DFT), discrete cosine transform (DCT), discrete wavelet transform (DWT), singular value decomposition (SVD), and so on [3], [4], [5]. These techniques on transform domains seem more robust but rather complicated to compute because of a large quantity of computation and unmeet the requirement on data high accuracy.

In the past few years, most of the recently proposed watermarking techniques focus on how to improve the robustness of watermark. They usually embed watermark information into the low-frequency part of images [6], [7]. The low-frequency coefficients of DCT domain, especially, the DC coefficients are usually used to embed watermark information. The reason to choose the DC coefficient is that DC coefficients have much larger perceptual capacity than AC coefficients. The DC coefficients can be maintained under some attacks [6]. Therefore, watermark information can be extracted from DC coefficients even if the embedded image is attacked. With another idea, Lin $et\ al.$ [7] proposed the embedding method by using DC coefficients with including AC coefficients within low-frequency. Lin's method perform well under general JPEG compression but the watermarks may be destroyed under higher compression ratio. To achieve the robustness of watermark and to improve quality of embedded image, Lin $et\ al.$ [8] also proposed another method by using the concept of mathematical remainder while embedding process. However, their method did not improve the quality of embedded image well. Therefore, to maintain the quality of the embedded image, seeking new frequency domain for watermarking schemes is a recent challenging problem.

In this paper, we propose the novel frequency domain, q-logarithm DCT domain (q-DCT), for image watermarking. We embed the watermark in the low-frequency of q-DCT domain in order to achieve the robustness of watermark. We also choose in our method a watermarking technique in the category of QIM due to its good robustness and blindness. In our proposed method, the tradeoff of robustness and quality can be controlled by parameter S of QIM and the parameter q of logarithm transform. Therefore, by using our method, we can not only improve more the quality of embedded image, but also achieve the robustness of watermark.

This paper is organized as follows. The proposed q-DCT

978-1-4673-8013-3/15 $31.00 © 2015 IEEE
DOI 10.1109/KSE.2015.70

domain is described in Section II. We also explain why the q-DCT domain is suitable for our watermarking method. Section III describes our proposed watermarking method using QIM on q-DCT domain. Our simulation results are shown in Section IV. Section V concludes our paper.

II. Proposed q-logarithm DCT domain (q-DCT)

Suppose an image I of size $N \times N$ pixels is given. The forward and inverse q-DCT conversion are described as follows:

1) Forward q-DCT: First, I is transformed to q-logarithm as below,

$$I_q(i,j) = log_q\{I(i,j)\} = \frac{\{I(i,j)\}^{1-q} - 1}{1-q}, \qquad (1)$$

where $I(i,j)$ and $I_q(i,j)$ represent the pixel and the coefficient at coordinate (i,j) of spatial domain and q-logarithm domain.

Afterwards, the equation of forward DCT regarding an image I_q block of size $M \times M$ pixels is given in Eq. (2).

$$\begin{aligned} I_q^d(u,v) &= C(u) \times C(v) \times \sum_{i=0}^{M-1}\sum_{j=0}^{M-1} I_q(i,j), \\ &\times \cos\frac{(2i+1)u\pi}{2M} \cos\frac{(2j+1)v\pi}{2M}, \end{aligned} \qquad (2)$$

where $I_q^d(u,v)$ denotes the coefficient at coordinate (i,j) in the DCT domain and

$$C(u), C(v) = \begin{cases} \sqrt{\frac{1}{M}} & \text{for } i,j = 0, \\ \sqrt{\frac{2}{M}} & \text{for } i,j = 1,2,\cdots,M-1. \end{cases}$$

2) Inverse q-DCT: The inverse transform of q-DCT is first performed by inverse transform on q-logarithm domain.

$$\begin{aligned} I_q(i,j) &= \sum_{u=0}^{M-1}\sum_{v=0}^{M-1} C(u) \times C(v) \times I_q^d(u,v), \\ &\times \cos\frac{(2i+1)u\pi}{2M} \cos\frac{(2j+1)v\pi}{2M}, \end{aligned} \qquad (3)$$

where $C(u), C(v)$ are the same as the forward transform.

Next, the inverse image I can be obtained by using inverse transform of q-logarithm, q-exponential, as follows:

$$I(i,j) = exp_q\{I_q(i,j)\} = (1 + (1-q)\{I_q(i,j)\})^{\frac{1}{1-q}}. \qquad (4)$$

3) The advantages of q-DCT: Since q-logarithm domain of image pixels are very stable with almost the same values, the low-frequency of q-DCT domain is considered to be more robust and to be suitable for image watermarking. Therefore, the watermarking using the q-DCT can be expected to improve not only the quality of embedded image, but also to maintain the robustness of watermark.

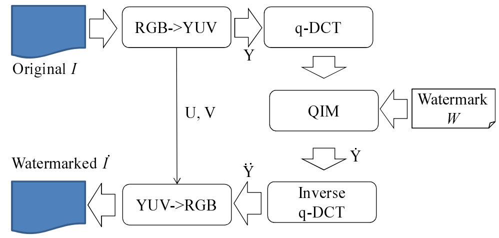

Figure 1. Embedding method using q-DCT and QIM.

III. Watermarking based on q-DCT domain

A. Watermark embedding algorithm

Before embedding, we prepare a logomark W as watermark information and extract a binary sequence bits denoted by $w_i \in \{0,1\}$, i-th bit of watermark. **Fig. 1** describes the detailed steps in our proposed embedding method.

–**Step 1.** Convert the RGB image to YUV color space[1]. We adopt the luminance information Y of YUV color transformation to implement our proposed method. The reasons to choose Y component is that human visual system is more sensitive to luminance than to the other two chrominance (U and V) components, and standard JPEG compression typically use higher density for Y than for the other two components.

–**Step 2.** Transform Y component to a frequency domain using q-DCT, to obtain Y_q^d.

–**Step 3.** Embed the binary sequence $\{w_i\}$ into Y_q^d by QIM method [10]:

$$\dot{Y}_q^d(u,v) = \begin{cases} \lfloor Y_q^d(u,v)/S \rfloor \times S + sgn(3S/4) & \text{for } w_i = 1, \\ \lfloor Y_q^d(u,v)/S \rfloor \times S + sgn(S/4) & \text{for } w_i = 0, \end{cases} \qquad (5)$$

where $Y_q^d(u,v)$ and $\dot{Y}_q^d(u,v)$ are coefficients of Y component in q-DCT domain at coordinate (u,v) of the original image and the watermarked image. sgn function is equal to "+" if $Y_q^d(u,v) > 0$, "−" if $Y_q^d(u,v) < 0$. $\lfloor \ \rfloor$ denotes the floor function, and S denotes the embedding strength chosen to maintain the quality of embedded image.

–**Step 4.** Compute the inverse q-DCT to obtain the modified $\ddot{Y}_q^d$ component.

–**Step 5.** Include U, V components with $\ddot{Y}$ and convert the modified $\dot{Y}_d^q$UV to the embedded image $\dot{I}$.

According to above process, we embed the watermark W into q-DCT domain of the Y component. We can control the quality of embedded image based on two parameters: parameter q of q-DCT domain, and parameter S for watermark strength. Therefore, our proposed method is more flexible than conventional methods.

B. Watermark extraction algorithm

The extraction is performed without using the original image. Basic steps involved in the watermarking extraction, shown in **Fig. 2**, are given as follows:

[1]http://en.wikipedia.org/wiki/YUV

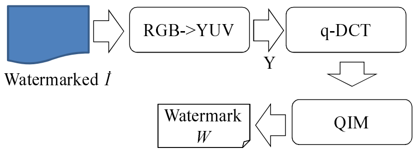

Figure 2. Extraction method using q-DCT and QIM.

Table I
PSNR AND NC VALUES BASED ON DIFFERENT q AND S (LENA IMAGE).

S	q	0.6	0.8	1.2	1.4	1.6	1.8
0.05	PSNR	46.73	47.70	49.03	49.52	49.88	50.15
	NC	1	1	0.995	0.982	0.980	0.963
0.10	PSNR	41.34	42.71	44.88	45.78	46.61	47.30
	NC	1	1	1	1	0.996	0.989
0.15	PSNR	37.64	39.11	41.61	42.70	43.64	44.53
	NC	1	1	1	1	1	0.999
0.20	PSNR	34.92	36.43	39.00	40.15	41.24	42.21
	NC	1	1	1	1	1	1
0.25	PSNR	32.77	34.29	36.94	38.13	39.25	40.26
	NC	1	1	1	1	1	1
0.30	PSNR	31.03	32.56	35.24	36.41	37.53	38.61
	NC	1	1	1	1	1	1
0.35	PSNR	29.55	31.07	33.75	34.97	36.10	37.19
	NC	1	1	1	1	1	1
0.40	PSNR	28.26	29.78	32.47	33.67	34.85	35.93
	NC	1	1	1	1	1	1

–**Step 1.** Extract Y component of watermarked image $\dot{I}$ based on YUV conversion transform.

–**Step 2.** Transform Y component to a frequency domain based on q-DCT transformation to obtain $\dot{Y}_q^d(u,v)$.

–**Step 3.** Extract the binary sequence of watermark based on the following rule.

$$\dot{w}_i = \begin{cases} 1 & \text{if } \dot{Y}_q^d(u,v) - \lfloor \dot{Y}_q^d(u,v)/S \rfloor \times S \geq sgn(S/2) \\ 0 & \text{if } \dot{Y}_q^d(u,v) - \lfloor \dot{Y}_q^d(u,v)/S \rfloor \times S < sgn(S/2) \end{cases} \quad (6)$$

–**Step 4.** Reconstruct $\{\dot{w}_i\}$, we can obtain the logomark $\dot{W}$.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

For assessing the performance of the proposed algorithm, we conducted 4 color images of SIDBA (Standard Image Data-BAse) databaseAll these test images are with size 512×512 pixels, and the logomark used in our experiments is a binary image with size 64×64.

In order to evaluate the quality of watermarked images, we employ PSNR (Peak Signal to Noise Ratio) criterion [11]. To provide objective judgment of the robustness of extraction, we use the normalized correlation (NC) value [12] between the original watermark W and the extracted watermark W''.

First, we survey the efficiency of the parameters q and S for the visual quality of watermarked image and the robustness of watermark information. We tries with various values of q and S to find out the appropriate values. The experimental results of the color image, Lena, is given in **Table I**. According to Table I, it can be observed that we can control the visual quality of watermarked image and the robustness of watermark information based on the parameter q of q-DCT domain and the embedding strength S. When q is with the larger value, PSNR value is more larger. It means that the quality of the embedded image is better. When S is with the larger value, NC value is close to 1. It means that the robustness of watermark is better. Therefore, according the our purpose, we can choose the appropriate q and S parameters for it.

Table II
PSNR[dB] AND NC VALUES UNDER JPEG COMPRESSION WITH DIFFERENT QUALITY FACTOR ($q = 1.2, S = 0.35$).

Image	QF	No attack	90	80	70	60	50
Lena	PSNR	42.77	36.84	32.66	31.84	31.28	30.85
	NC	1	0.952	0.905	0.885	0.801	0.769
F16	PSNR	36.69	34.49	31.79	31.16	30.54	30.10
	NC	1	0.997	0.992	0.989	0.981	0.978
Baboon	PSNR	33.43	29.24	25.77	25.12	24.62	24.24
	NC	1	0.985	0.963	0.939	0.908	0.872
Scene	PSNR	39.53	32.00	28.65	28.09	27.66	27.31
	NC	1	0.968	0.926	0.892	0.843	0.812

Table III
PSNR[dB] AND NC VALUES UNDER JPEG COMPRESSION WITH DIFFERENT QUALITY FACTOR ($q = 1.4, S = 0.30$).

Image	QF	No attack	90	80	70	60	50
Lena	PSNR	45.04	37.31	32.84	31.99	31.41	30.98
	NC	0.847	0.845	0.824	0.788	0.742	0.693
F16	PSNR	38.54	35.50	32.29	31.61	30.97	30.40
	NC	0.989	0.987	0.983	0.975	0.962	0.947
Baboon	PSNR	33.70	29.34	25.81	25.16	24.65	24.27
	NC	0.968	0.954	0.914	0.885	0.831	0.787
Scene	PSNR	41.40	32.28	28.78	28.19	27.76	27.42
	NC	0.880	0.865	0.839	0.813	0.766	0.737

In this paper, we choose $\{q = 1.2, S = 0.35\}$ and $\{q = 1.4, S = 0.30\}$ to simulate on the experimental images. The simulation results of the color images, Baboon, F16, Lena, and Scene, are given **Table II**, **Table III**. Table II and Table III show the NC values of extracted watermarks and the image quality (i.e., the PSNR values) of watermarked images after attacking by JPEG compression with different quality factors (QF). Here, the QF for JPEG images is an integer value ranging from 1 to 100, which denotes the predetermined image quality of JPEG compression. When the larger QF is assigned, the lower compression ratio the compressed image is obtained and the better quality the compressed image is maintained. Obviously, the image watermarking needs to be robust against, at least, JPEG compression to ensure for image transmission via network. Note that, image is always compressed to JPEG image with quality equals 75 before transmission. **Fig. 3** illustrates the watermarks extraction from the embedded image F16 after JPEG compression with low QF such as 50 and 20. It is clear that the extracted watermarks can be easily recognized by the human eyes. Therefore, according to the results of Table II and Table III, our proposed method is useful under the JPEG compression. Comparing the results of Table II and Table III, we find that when we use $\{q = 1.4, S = 0.30\}$ (Table III) instead of $\{q = 1.2, S = 0.35\}$ (Table II), the quality of watermarked images are improved, however, the robustness of watermark is degraded. Therefore, based on the experimental results, it is clear that the choosing of the parameters q and S decides the tradeoff of robustness of

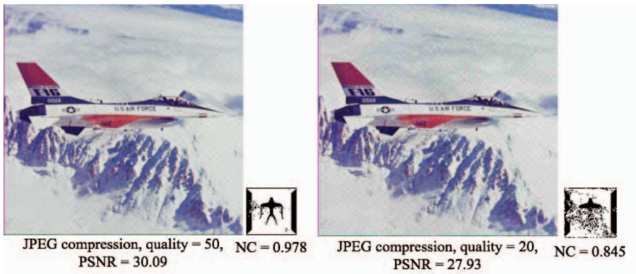

Figure 3. Watermark extraction from embedded image F16 after JPEG compression with QF 50 and 20, respectively, when $q = 1.2, S = 0.35$.

Table IV
COMPARISON AMONG [8] AND OUR PROPOSED METHOD.

	Our method		Lin et al. [8]	
Attacks	PSNR	NC	PSNR	NC
Equalize	15.05	0.723	22.59	0.854
Sharpen	31.98	0.551	28.00	0.969
Despeckle	34.84	0.537	30.51	0.797
Auto level	42.76	0.958	20.04	0.775
Auto contrast	18.82	0.745	27.53	0.998
Brightness	26.77	0.963	NA	NA
Normalize	22.74	0.784	NA	NA
Grayscale	17.68	0.920	NA	NA
Median 3x3	42.76	0.957	NA	NA
Flip	12.55	0.875	NA	NA
Hue 110	25.72	0.864	NA	NA

watermark and quality of embedded image.

In order to show the robustness of our proposed method against common image processing attacks, we use the PhoToShop on the embedded image Lena using $\{q = 1.2, S = 0.35\}$. We also compare our method with Lin $et\ al.$ method [8] and the comparison of those is shown in **Table IV**. Note that "NA" means the corresponding experimental datum is unavailable. **Fig. 4** also shows some examples of simulation results against common image processing attacks. Here, we also can easily recognize the watermark by the human eyes. According to the results shown in Table IV, our proposed method maintains the quality of embedded images better than Lin $et\ al.$ method. As shown in Table IV, our method can be robust to common image processing attacks such as median, normalization, brightness, auto contrast, and so on.

Based on the experiments of our proposed method, we find that the idea employing q-DCT domain for image watermarking is useful for maintaining the quality of embedded images. It also can archive the robustness of JPEG compression and some common image processing attacks.

V. CONCLUSION

We have proposed a novel and robust image watermarking based on q-DCT domain, which is not yet proposed for watermarking field before. The watermark is embedded in the low-frequency of q-DCT domain in order to achieve the robustness of watermark and to maintain the quality of embedded image. According to our experimental results, the embedded watermark can successfully survive after attacked by image processing attacks, especially for the JPEG compression. Moreover, because we employed QIM method to watermarking method, the watermark embedding and extracting processes are very simple and the watermark can be extracted without the original image. Beside, the tradeoff of robustness and quality can be controlled by the parameter S of QIM and the parameter q of logarithm transform. Simulation results show that the proposed scheme outperforms the earlier works. Therefore, we conclude that our proposed method is suitable for images that will be highly JPEG-compressed and transmitted via network.

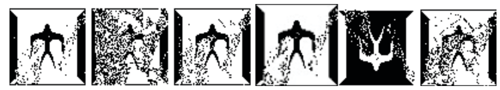

Figure 4. Some extracted watermarks (from left to right: Brightness, Normalize, Grayscale, Median 3x3, Flip, Hue attack).

VI. ACKNOWLEDGMENTS

This work was also funded by the Research Fund RF@K12, Faculty of Information Technology, Le Quy Don Technical University.

REFERENCES

[1] F. Y. Shih (eds.), "Digital Watermarking and Steganography: Fundamentals and Techniques," Taylor & Francis Group, CRC Press., Inc., Boca Raton, FL, USA, 2008.

[2] M. M. Yeung, "Digital watermarking," Commun. ACM, vol. 41, no. 7, 1998.

[3] A. Nikolaidis and I. Pitas, "Asymptotically optimal detection for additive watermarking in the DCT and DWT domains," IEEE Trans. Image Process., vol. 12, no. 5, pp. 563–571, May 2003.

[4] P. Bao and X. Ma, "Image adaptive watermarking using wavelet domain singular value decomposition," IEEE Trans. Circuits and Systems for Video Technology, vol. 15, no. 1, pp. 96–102, 2005.

[5] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership," IEEE Trans. Multimedia, vol. 4, no. 1, pp. 121–128, Mar. 2002.

[6] J. Huang, Y.Q. Shi, Y. Shi, "Embedding image watermarks in DC components," IEEE Trans. on Circuits and Systems for Video Technology, vol. 10, no. 6, pp.974–979, 2000.

[7] S.D. Lin, S.C. Shie, C.F. Chen, "A DCT based image watermarking with threshold embedding," International Journal of Computers and Applications, vol. 25, no. 2, pp.130–135, 2003.

[8] Shinfeng D. Lin, Shih-Chieh Shie, J.Y. Guo, "Improving the robustness of DCT-based image watermarking against JPEG compression," Computer Standards & Interfaces, vol. 32, issue 1–2, pp. 54-60, 2010.

[9] C. Tsallis, "Possible generalization of BoltzmannGibbs statistics," J.Stat. Phys. vol. 52, pp.479–487, 1998.

[10] B. Chen and G. W. Wornell, "Quantization index modulation methods for digital watermarking and information embedding of multimedia," J. VLSI Signal Process. Syst., vol. 27, pp. 733, 2001.

[11] M. Iwakiri, T. M. Thanh, "Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management," The 26th IEEE International Conf. on AINA, pp. 763–770, 2012.

[12] T. M. Thanh, P. T. Hiep, T. M. Tam, K. Tanaka, "Robust semi-blind video watermarking based on frame-patch matching," J. of Electronics and Communications, ISSN 1434-8411, 2014.