A Watermarking Scheme Based on DCT using HVS Characteristic

Asri Rizki Yuliani, Didi Rosiyadi
Research Center for Informatics
Indonesian Institute of Sciences, LIPI
Bandung, Indonesia
Email: asri.rizki.yuliani@lipi.go.id, rosiyadi@informatika.lipi.go.id

***Abstract*—This paper presents a watermarking scheme based on DCT using HVS characteristic. The proposed watermarking scheme hides watermark into an image, and takes HVS characteristic into consideration during the watermark embedding process. The image is first divided into blocks. Blocks containing significant DC coefficients, which represent the bright area of the image, are selected for insertion of binary-image watermark. The watermark is inserted by modifying coefficients in the mid frequency domain into positive or negative value according to the watermark bits. Experiment results show that the proposed algorithm is imperceptible and robust against various image processing attacks such as scaling, cropping, noise attacks, filter attacks, and compression.**

I. Introduction

The emergence of the Internet and communication network provides enormous convenience for the exchange of information in the form of digital media. However, security towards information must be prioritized to keep authentication and copyright protection, and to prevent the duplication of information. As a result, digital watermarking technique, which embeds owners information into digital media contents, is seen to be an effective solution of protecting copyright.

Digital watermarking schemes fall into two categories, spatial domain and transform domain. Spatial domain works by modifying pixel values of the image, while transform domain works by modifying transform domain coefficients. The transformation domain, especially DCT, has been frequently applied because of its property [1]–[3]. Li and Qin [1] proposed embedding scrambled watermark into an image in DCT domain. Zhao et al. [2] presented a blind watermarking based on DCT by modifying AC coefficients. In [3], visible watermarking scheme based on DCT in five different positions is proposed. The advantage of using DCT is it can be incorporated with the features of Human Visual System (HVS) in order to determine the watermark embedding strength and position.

In watermark embedding process, HVS model plays important role to control the robustness and invisibility of an image. Several HVS based watermarking schemes have been proposed for digital media protection. Lai [4] proposed watermarking scheme based on DCT and SVD using visual entropy and edge entropy of HVS. Golikeri and Nasiopoulos [5] presented a method based on DCT and texture characteristics to determine watermark embedding position.

The scheme proposed in this paper takes HVS characteristic into consideration for embedding invisible image watermark in the DCT domain. Performance evaluation is done by comparing the proposed scheme with previous schemes presented in [2] and [6].

II. Review of DCT

The discrete cosine transform (DCT) is a technique for converting a signal into frequency components and it is widely used in JPEG compression standard [7]. DCT transforms an array comprising the pixel value to become components divided in accordance to its frequency; low frequency, medium frequency, or high frequency. Then, the image can be recovered from DCT transform by applying the Inverse Discrete Cosine Transform. The two-dimensional block based DCT technique is used in this proposed scheme, which is defined by:

$$c(k,l) = b(k)b(l)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\left\{f(x,y)cos\left[\frac{(2x+1)\pi k}{2N}\right]cos\left[\frac{(2y+1)\pi l}{2N}\right]\right\} \quad (1)$$

The corresponding inverse 2D DCT transform is given by:

$$f(x,y) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1}\left\{b(k)b(l)c(k,l)cos\left[\frac{(2x+1)\pi k}{2N}\right]cos\left[\frac{(2y+1)\pi l}{2N}\right]\right\} \quad (2)$$

In the formula: c(k,l) represents a function of DCT that has a pixel value at coordinates (k,l); f(x,y) represents the function of inverse DCT that has a pixel value at coordinates (x,y) in which its index is started from 0; b(k) and b(l) are the functions to get a value back in which:

$$ifk = l = 0, b(k) = b(l) = \frac{1}{\sqrt{N}} \quad (3)$$

$$others, b(k) = b(l) = \sqrt{\frac{2}{N}} \quad (4)$$

III. Proposed Watermarking Scheme

A watermark algorithm includes two steps: watermark embedding and extraction. The luminance feature of HVS is taken into account during the watermark embedding process. HVS study found that human eyes are less sensitive to changes in bright area of the image [8] and relatively sensitive to low frequency noise [1]. Therefore, the bright area of the image are selected for insertion of binary-image watermark. In addition,

978-1-4799-8773-3/15/$31.00 ©2015 IEEE

the proposed algorithm embeds the watermark into the mid frequency domain in order to balance the invisibility and robustness. Mid frequency domain are mostly chosen because modifications on this domain do not deteriorate the visual quality of the image [9].

A. Watermark Embedding

The embedding process is depicted as follows:

1) DCT transform: The original image *I* is first divided into non-overlapping 8x8 blocks and each block is transformed into DCT coefficients.

2) Blocks selection: Compute the average luminance of the image $\bar{D_0}$ and select the appropriate number of blocks with significant DC coefficients equal to number of watermark bits.

$$\bar{D_0} = \frac{64}{MN} \sum_{k=1} D_0^k \qquad (5)$$

D_0^k denotes the DC coefficient of the *k*th block in the image. The image block is selected when $D_0^k \geqslant \bar{D_0}$.

3) DCT coefficients selection: Arrange DCT coefficients of selected blocks in JPEG zigzag scan order in order to select coefficients in the mid frequency domain.

4) Watermark insertion: Insert one bit of watermark *W* per block by modifying the selected coefficients into positive or negative value with the following equation:
If watermark bit is 1,

$$I'(i,j) = |I(i,j)| + p \qquad (6)$$

If watermark bit is 0,

$$I'(i,j) = -|I(i,j)| - p \qquad (7)$$

In the formula: |I(i,j)| denotes the absolute value of selected coefficients of the image *I* at coordinates (i,j); *p* denotes watermark strength.

5) Rearrange DCT coefficients: Modify the coefficients back to their original position using inverse zigzag scan order.

6) IDCT transform: Apply inverse DCT transform on each block to obtain the watermarked image.

B. Watermark Extraction

The embedding process is depicted as follows:

1) DCT transform: The watermarked image *I'* is divided into non-overlapping 8x8 blocks and apply DCT on each block.

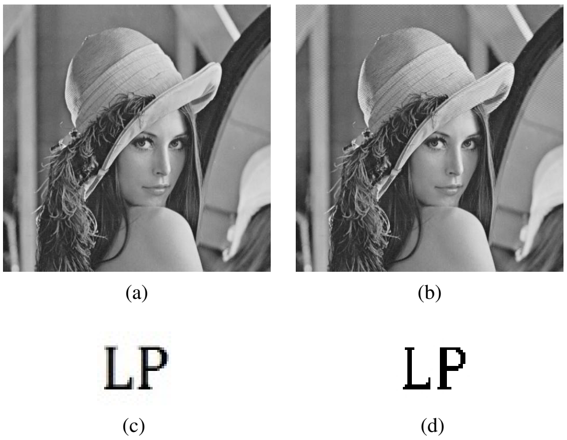
2) Blocks selection: Select the appropriate number of DCT blocks used in embedding process.

3) DCT coefficients selection: Arrange DCT coefficients in JPEG zigzag scan order to select coefficients in the mid frequency domain.

4) Watermark extraction: Extract watermark *W'* from selected coefficients with the following equation:

$$w' = 1 \ when \ I'(i,j) > 0 \qquad (8)$$

$$w' = 0 \ when \ I'(i,j) < 0 \qquad (9)$$



(a) (b)

(c) (d)

Fig. 1. (a) Original image of Lena, (b) Watermarked image, (c) Original watermark, (d) Extracted watermark

TABLE I
THE RESULT OF PSNR OF WATERMARKED IMAGES (WITHOUT ANY ATTACKS)

Image	PSNR (dB)	NC
Lena	38.4144	1
Cameraman	39.7808	1
Peppers	38.1488	1

IV. EXPERIMENT RESULT

In this section, the algorithm is tested on variety of images. The gray-scale images of Lena, cameraman, and peppers, are used as the host image *I*, whereas the binary image of LP is used as the watermark image *W*. The corresponding sizes of those host and watermark images are 512 x 512 and 32 x 32 respectively.

The peak signal to noise ratio (PSNR) and the normalized correlation (NC) are computed in order to evaluate the performance of watermarking scheme. PSNR is used to measure the level of perceptibility of watermarked image and NC is used to measure the level of resistant of watermark against various image processing attacks. PSNR and NC are defined by equation (10) and (12). Without any attacks the PSNR of watermarked image *I'* and the NC of extracted watermark *W'* are shown in Table 1. The results of PSNR show that the watermarked image has good imperceptibility. The original and watermarked image of Lena are shown in Fig. 1(a), (b) respectively.

$$PSNR = 10 \ log_{10} \frac{255^2}{MSE} \qquad (10)$$

where,

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - I'(i,j)]^2 \qquad (11)$$

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)\ W'(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W(i,j)^2}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} W'(i,j)^2}} \quad (12)$$

The experiments are carried out to evaluate the performance of the proposed watermarking scheme. Several kinds of attacks on the watermarked image are performed, which include scaling, cropping, Gaussian noise, Salt and Pepper noise, Speckle noise, median filter, Gaussian low-pass filter, Wiener filter, JPEG compression, and histogram equalization. Afterward, the watermark from attacked image is extracted and compared to the original image using normalized correlation.

The watermarked image is transformed into Fig. 2 after geometric attacks. Watermarked image after scaling with scale factor of 0.5 is shown in Fig. 2(a), after left cropping is shown in Fig. 2(b), after center cropping 256x256 or cropping a quarter of the image is shown in Fig. 2(c). Extracted watermark from attacked images are shown in Fig. 2(d), (e), (f) respectively. The results of PSNR and NC are provided in Table II.

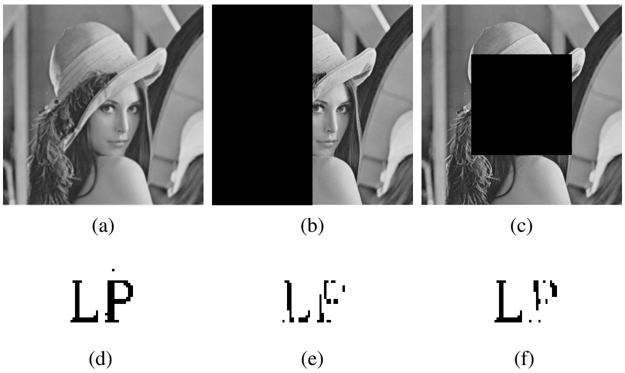


Fig. 2. Watermarked images and extracted watermarks after geometric attacks (a) Scaling 0.5, (b) Left cropping, (c) Center cropping

TABLE II
THE RESULTS OF PSNR AND NC AFTER GEOMETRIC ATTACKS

Geometric attacks	Image	PSNR	NC
Scaling 0.5	Lena	30.3009	0.9923
	Cameraman	27.7325	0.9848
	Peppers	31.1336	0.9848
Left cropping	Lena	9.632	0.7299
	Cameraman	9.4354	0.7344
	Peppers	9.7932	0.7614
Center cropping 128x128	Lena	17.1603	1
	Cameraman	19.3393	1
	Peppers	17.8326	0.9884
Center cropping 256x256	Lena	11.6433	0.7880
	Cameraman	13.132	1
	Peppers	11.9693	0.9174

The watermarked image is transformed into Fig. 3 after noise attacks. Watermarked image after adding Gaussian noise with variance of 0.002 is shown in Fig. 3(a), after adding Salt and Pepper noise with strength of 0.01 is shown in Fig. 3(b), after adding Speckle noise with strength of 0.01 is shown in Fig. 3(c). Extracted watermark from attacked images are shown in Fig. 3(d), (e), (f) respectively. The results of PSNR and NC are provided in Table III.

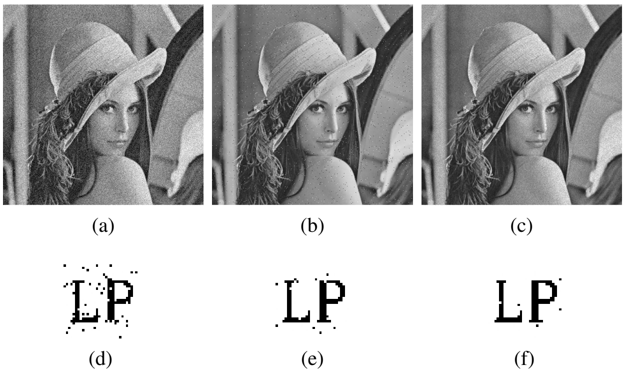


Fig. 3. Watermarked images and extracted watermarks after noise attacks (a) Gaussian noise, (b) Salt and Pepper noise, (c) Speckle

TABLE III
THE RESULTS OF PSNR AND NC AFTER NOISE ATTACKS

Noise attacks	Image	PSNR	NC
Gaussian noise (Variance = 0.002)	Lena	19.9955	0.8405
	Cameraman	20.3299	0.8156
	Peppers	20.1176	0.8527
Salt and Pepper noise (Strength = 0.01)	Lena	25.1508	0.9511
	Cameraman	24.8304	0.9318
	Peppers	24.8687	0.9591
Speckle (Strength = 0.01)	Lena	25.4112	0.9772
	Cameraman	25.4018	0.9702
	Peppers	26.3207	0.9809

The watermarked image is transformed into Fig. 4 after filter attacks. Watermarked image after median filter 3x3 is shown in Fig. 4(a), after Gaussian low-pass filter 3x3 is shown in Fig. 4(b), after Wiener filter 3x3 is shown in Fig. 4(c). Extracted watermark from attacked images are shown in Fig. 4(d), (e), (f) respectively. The results of PSNR and NC are provided in Table IV. Table V shows the results of PSNR and NC of Lena image after JPEG compression in different quality factor and image histogram equalization.

Table VI shows comparison result of NC values of Lena image between the proposed scheme and the previous schemes reported by Zhao [2] and Tataru [6]. As seen from Table VI, NC values under several types of attacks; Salt and Pepper noise 0.01, median filter 3x3, Gaussian low-pass filter 3x3, Wiener filter 3x3, and JPEG compression 30 are higher than Zhao's and Tataru's method. The results indicate that the embedded watermark is relatively robust to image processing attacks.

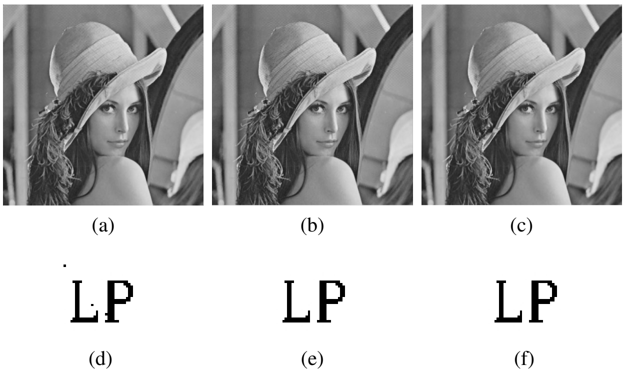


Fig. 4. Watermarked images and extracted watermarks after filter attacks (a) Median filter, (b) Gaussian low-pass filter, (c) Wiener filter

TABLE IV
THE RESULTS OF PSNR AND NC AFTER FILTER ATTACKS

Filter attacks	Image	PSNR	NC
Median filter 3x3	Lena	30.3948	0.9886
	Cameraman	30.2613	0.9886
	Peppers	35.8052	1
Gaussian low-pass filter 3x3	Lena	36.8556	1
	Cameraman	35.8064	1
	Peppers	38.1286	1
Wiener filter 3x3	Lena	37.3136	1
	Cameraman	35.4518	1
	Peppers	37.6553	1

TABLE V
THE RESULTS OF PSNR AND NC AFTER JPEG COMPRESSION AND HISTOGRAM EQUALIZATION

Type of Attacks	PSNR	NC
JPEG Compression		
QF = 30	33.1294	1
QF = 25	32.9541	1
QF = 20	32.1216	1
QF = 10	29.493	0.5901
Histogram Equalization	19.0988	1

V. CONCLUSION

In this paper, a robust watermarking scheme in DCT domain is presented. The luminance feature of HVS has taken into consideration during the watermark embedding process. DCT blocks containing significant DC coefficients are selected for watermark placement. The watermark is inserted into an image by modifying selected mid frequency coefficients into positive or negative value. Then, the watermark is extracted by changing the watermark bits back to 1 or 0 according to the value of modified coefficients. The results of experiment show that luminance feature has improved the invisibility of the watermark. Furthermore, the algorithm has stronger robustness against several types of attacks.

TABLE VI
THE COMPARISON RESULT OF NC VALUES

	Proposed	[2]	[6]
Center cropping	0.7880	0.8666	0.87
Gaussian noise (0.002)	0.8405	0.9646	0.89
Salt and Pepper noise (0.01)	0.9511	0.9473	-
Median filter 3x3	0.9886	0.9473	0.81
Gaussian low-pass filter 3x3	1	0.9646	-
Wiener filter 3x3	1	0.9192	0.89
JPEG Compression QF=30	1	-	0.84

REFERENCES

[1] C. Li and Z. Qin, “A blind digital image watermarking algorithm based on dct,” in *Smart and Sustainable City 2013 (ICSSC 2013), IET International Conference on*. IET, 2013, pp. 446–448.

[2] Z. Rui-Mei, L. Hua, P. Hua-Wei, and H. Bo-Ning, “A watermarking algorithm by modifying ac coefficies in dct domain,” in *Information Science and Engineering, 2008. ISISE’08. International Symposium on*, vol. 2. IEEE, 2008, pp. 159–162.

[3] D. Rosiyadi and F. H. Muttaqien, “A robust watermarking scheme againts various attacks based on dct in five different positions of the host image area,” *Jurnal Teknologi Indonesia (JTI)*, vol. 36, no. 3, 2015.

[4] C.-C. Lai, “An improved svd-based watermarking scheme using human visual characteristics,” *Optics Communications*, vol. 284, no. 4, pp. 938–944, 2011.

[5] A. Golikeri and P. Nasiopoulos, “A robust dct energy based watermarking scheme for images,” *Journal of Proceedings of IEEE*, 2005.

[6] R. L. Tataru, S. El Assad, and O. Déforges, “Improved blind dct watermarking by using chaotic sequences,” in *Internet Technology And Secured Transactions, 2012 International Conference for*. IEEE, 2012, pp. 46–50.

[7] D. Rosiyadi, S.-J. Horng, P. Fan, X. Wang, M. K. Khan, and Y. Pan, “Copyright protection for e-government document images,” *MultiMedia, IEEE*, vol. 19, no. 3, pp. 62–73, 2012.

[8] Y. Q. Shi and H. Sun, *Image and video compression for multimedia engineering: Fundamentals, algorithms, and standards*. CRC press, 1999.

[9] T. K. Tewari and V. Saxena, “An improved and robust dct based digital image watermarking scheme,” *International Journal of Computer Applications*, vol. 3, no. 1, pp. 28–32, 2010.