International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249–8958, Volume-1 Issue-3, February 2012

Discrete Cosine Transformation based Image Watermarking for Authentication and Copyright Protection

Ritu Pareek, P.K. Ghosh

Abstract: ***In this paper, a digital image watermarking algorithm based on DCT transformation is proposed. The imperceptibility and robustness is provided against different attacks. A binary image is embedded in the host image by two different techniques based on DCT. One is middle band coefficient exchange technique, it utilizes comparison of two middle-band DCT coefficients to encode a single bit into a DCT block. Coefficient locations are selected based on the recommended JPEG quantization table. Second is based on PN sequence, PN sequences of the watermark bits are embedded in the coefficients of the corresponding DCT middle frequencies. In extraction stages, the watermarked image, which may be attacked, is processed the same way as the embedding process.***

Finally, correlation and PSNR values are calculated to determine the level of accuracy and imperceptibility. Experimental results show that the proposed method improved the performance of watermarking algorithm.

Index Terms: Discrete Cosine Transform, Digital watermarking, PN Sequence, Middle band frequency, Copyright protection, CDMA.

I. INTRODUCTION

In recent years, the study of watermarking scheme has attracted researchers in the emergent areas of watermarking security and image authentication [1-3]. It is indeed an important research field in Computer science, Cryptography, Signal Processing and Communication [4-8]. Digital Watermarking is an effective solution for protecting intellectual property of audio, image and video data.

Watermarking is broadly classified into two categories, namely Spatial Domain Watermarking and frequency domain watermarking. Frequency domain watermarking is found most robust. The watermarking schemes broadly consist of the three stages: Watermarking generation and Embedding, Distribution, Possible attacks and watermarking detection [9]. The embedded data should preserve the quality of the host signal after watermarking. Basic requirements for watermarking generation are:

(i) Robustness: This refers to the fact that for general signal processing operations [filtering, compression], geometric transformations, malicious attacks, the watermark has the ability of surviving.

(ii)Imperceptibility: The watermarked should not be visible, audible to the human eyes or ears. It means that the quality of the original image after special processing should not be altered.

(iii) Security: The watermark image should only be detected by authorized agent. Illegal detection, extraction of information or modification of the watermark shall not be done by unauthorized user.

(iv) Capacity: This refers to a number of bits that can be embedded in the host image in unit time. The cover image, therefore, needs to have sufficient redundant data. However, Watermarking system may often tradeoff the capacity, security for additional robustness [10].

II. SYSTEM MODEL FOR DIGITAL WATERMARKING

Digital Watermarking embeds data called the watermark or digital signature or some tag or level which stands for particular identity of the owner by some sort of algorithm into a multimedia object. The object may be an image, audio, video or even text. One can extract the watermark to verify the identity of copyright information and ensure legitimate ownership by using appropriate algorithms. In essence a complete digital watermark system comprises of three basic modules:

- The watermark
- Encoder algorithm
- Decoder algorithm

Manuscript published on 28 February 2012.
* Correspondence Author (s)
Ritu Pareek*, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Mody Institute of Technology and Science (Deemed University), Lakshmangahr, Dist. Sikar, Rajasthan, PIN 332311, India
(e-mail: ritupareek135@gmail.com).
P. K. Ghosh*, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, Mody Institute of Technology and Science (Deemed University), Lakshmangahr, Dist. Sikar, Rajasthan, PIN 332311, India
(e-mail: pkghosh_ece@yahoo.co.in).

The general framework of watermarking is shown in fig.1

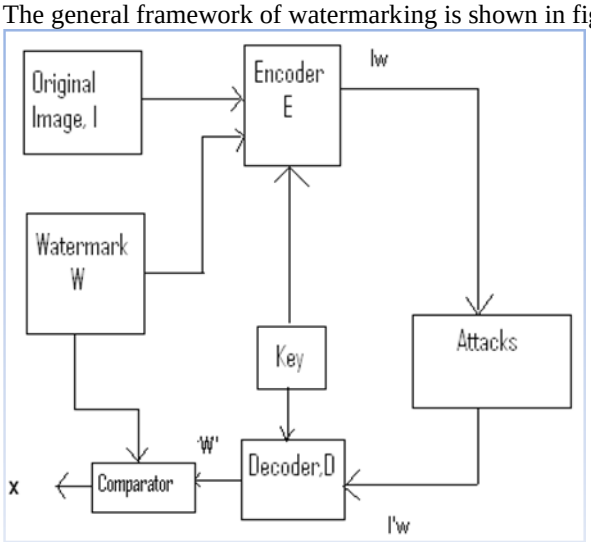


Fig.1 General framework of watermarking system

The watermark procedure requires the information of original image, the watermark and the key. The role of the key is to determine certain parameters of the embedding function which should be kept secret to avoid eavesdropping by attacks. The secret key should be transmitted to the authenticated receiver for extraction of watermark. Without this key the attacker would not know in which domain the embedding took place. The encoding process begins with an original image, I, a watermark, W and a secret key, K. The watermarked image, I_W is generated by the encoding function as follows

$$E(I,W,K) = I_W \qquad (1)$$

The watermarked image I_W may have suffered possible modifications due to channel distortion, noise addition etc. The decoder works with this modified watermarked image I'_W, the key K, to extract the image W' which we call the estimated image through the decoder function

$$D(I'_W,K) = W' \qquad (2)$$

The estimated watermark image W' should be identical with the original watermark W. To verify this a comparator function may be used which operates with extracted watermark and the original watermark to generate the binary function x, as shown in fig.1. The comparator function is defined by

$$C(W',W)=\begin{cases}1\\0\end{cases} \qquad (3)$$

The extraction of watermark is very useful for verifying ownership.

III. Transformed Domain Digital Watermarking Technique

Digital watermarking in frequency domain has been proposed by I.Cox, et al [11] which is based on the idea of spread spectrum communication technology. The algorithm does a kind of orthogonal transformation of the image, embeds the watermark information in the transformed domain of the image and finally takes the inverse transformation for image recovery in spatial domain. This technique has the advantage in terms of transparency, robustness to signal processing and attempts to remove watermark. The robustness is realized by inserting the watermark in the perceptually significant portion of the image.

Most common frequency domain digital image watermarking methods are:

a. Discrete Cosine Transform (DCT)
b. Discrete Fourier Transform (DFT)
c. Discrete Wavelet Transform (DWT)

The watermark algorithm in the frequency domain is based on the principle that both the watermark image and the cover image to be watermarked are transformed into frequency domain. The marking is performed by taking the two images in certain proportions and inverse frequency transformation recovers the watermarked image. The image watermarking based on DCT is very important for image compression, coding and other applications.

The main idea in selecting DCT is due to its compatibility with the exiting standards. Normally in the DCT domain we select the middle frequency components for watermark superposition.

Let X be the original image, Y be the watermarked image and W be the watermark image to be inserted. We denote the DCT coefficients X and Y as X_D and Y_D respectively. Taking X_i and Y_i be the ith DCT coefficients in X_D and Y_D respectively, we can write the watermarking algorithm has

$$Y = X_i(1+\alpha W_i) \qquad (4)$$

[11]. The constant α is a controlling parameter deciding the visibility of the watermark. For the extraction of the watermark, the value of α must be known.

The extraction of watermark is the reverse of the embedding process. To obtain a copy of W (say $\hat{W}$) from a possible forged image Z, we find as follows

$$\hat{W} = \frac{1}{\alpha}\left[\frac{z_i}{x_i} - 1\right] \qquad (5)$$

where, Z_i are the DCT coefficients of Z.

Because of possible distortions due to attacks or channel noise, the extracted version $\hat{W}$ may be different from W between W and $\hat{W}$ can be computed from the quality factor called the correlation.

$$\rho(W,\hat{W}) = \frac{W.\hat{W}}{\sqrt{W^2.\hat{W}^2}} \qquad (6)$$

The correlation factor ρ lies between 0 and 1.

Mention be made here that the DCT transform is based on the whole image rather than usual block-based approach, this transformation does not provide any local spatial control of the watermarks embedding process. This means that the addition of watermark to one of DCT coefficients affects the entire image. However there is another process that modulates some pre-selected DCT coefficients [12]. The main task of watermark embedding in DCT domain can be summarized as follows:

- Calculation of DCT transform of original image.
- Selection of N random no's with normal distribution.
- Transformation and superposition based on equation (4).

The random number is used in embedding as well as extraction process. The random number is treated as noise and used for testing robustness for the purpose of security. As a checking, noise is added to the watermarked image to vary the image pixel values by the use of the key. The extraction of original image from the watermarked image without this key will result in blurred image, different from watermark. However by using the secret key at the receiver end the authorized user can extract the watermark.

One another DCT technique utilizes the comparison of middle-band DCT coefficients to encode a single bit into a DCT block. To begin, we define the middle-band frequencies (F_M) of an 8 x 8 DCT block as shown below in figure 2 [13].

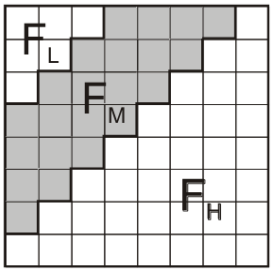


Fig.2 Definition of DCT Region

The middle-band frequencies (F_M) of an 8x8 DCT block are shown in Fig.2 In this Figure, F_L is used to denote the lower frequency components of the block and F_H is used to denote the higher frequency components. F_M is chosen as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. First, 8 x 8 DCT of an original image is taken. Then, two locations DCT (u1,v1) and DCT (u2,v2) are chosen from the FM region for comparison of each 8 x 8 block [14]. These locations are selected based on the recommended JPEG quantization table shown in Table I.

Table I. Quantization values used in JPEG compression scheme

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	55	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

If two locations are chosen such that they have identical quantization values, then any scaling of one coefficient will scale the other by the same factor to preserve their relative strength. Embedding in DCT domain is simply done by altering the DCT coefficients.

Another possible technique is to embed a PN sequence W into the middle frequencies of the DCT block. We can modulate a given DCT block (x,y) using the equation shown below for embedding of CDMA watermark into DCT middle frequencies:

$$I_{Wx,y}(u,v) = \begin{cases} I_{x,y}(u,v) + k \times W_{x,y}(u,v), & u,v \in F_M \\ I_{x,y}(u,v), & u,v \notin F_M \end{cases} \quad (7)$$

For each 8 x 8 block of the image, the DCT for the block is first calculated. In that block, the middle frequency components FM are added to the pseudo random noise sequence W, multiplied by a gain factor k. Coefficients in the low and middle frequencies are copied over to the transformed image unaffected. Each block is then inverse-transformed to give us our final watermarked image I_W.

IV. MATHEMATICAL ANALYSIS

We can consider an image x(m,n) as a matrix MxN in the spatial domain. The 2-D DCT can be obtained with the following expression

$$X(k,l) = \frac{2}{\sqrt{MN}} c(k)c(l) \sum_{m=0}^{M-1}\sum_{n=0}^{N-1} x(m,n).X \quad (8)$$

$$X = \cos\left[\frac{(2m+1)k\pi}{2M}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

$$K = 0,1,2,\dots\dots.M-1;$$
$$l = 0,1,2,\dots\dots,N-1$$

The inverse transform of DCT is:

$$x(m,n) = \frac{2}{\sqrt{MN}} \sum_{k=0}^{M-1}\sum_{l=0}^{N-1} c(k)c(l)X(k,l).Y \quad (9)$$

$$y = \cos\left[\frac{(2m+1)k\pi}{2M}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

$$m = 0,1,2,\dots\dots,M-1;$$
$$n = 0,1,2,\dots\dots,N-1$$

Where,

$$C(k) = \begin{cases} \frac{1}{\sqrt{2}}, & k = 0 \\ 1, & k = 1,2,\dots,M-1 \end{cases}$$

$$c(l) = \begin{cases} \frac{1}{\sqrt{2}}, & l = 0 \\ 1, & l = 1,2,\dots,N-1 \end{cases}$$

The effectiveness of digital watermarking technique for embedding and extraction of watermark image are evaluated by the metric called Peak Signal to Noise Ratio (PSNR) and the Mean Square Error (MSE).

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

The equation of PSNR can be described as

$$PSNR=10log_{10}\left(\frac{255^2}{MSE}\right) \quad (10)$$

where, M is taken to be 256.

The expression for MSE of the image with MxN pixels is defined as

$$MSE=\frac{1}{MN}\left(\sum\sum\left(f(m,n)-\overline{f(m,n)}\right)\right) \quad (11)$$

where, f(m,n) is the original pixel value and $\overline{f(m,n)}$ is the processed pixel value.

V. Experimental Results

We select a 512 x 512 pixels, grayscale Lena as the original image and 20×50 pixel grayscale image as the watermark image as shown in figure 3. There are 256 different grayscale level in the original image (8-bit resolution).

(a)

(b)

Fig. 3 (a) Original Image (b) Watermark

Table II shows various observations for different values of threshold k. Without any attacks the technique is Imperceptible and shows good recovered watermark. Quality of watermarked image degrades as the value of k increases. Note particularly that the value of PSNR degrades at higher k values. Normalized Correlation (NC) in Table II is between original image and watermarked image.

Table II. The Quality rates under various executions

k	PSNR (dB)	Elapsed time (embedding) (seconds)	Elapsed time (extraction) (seconds)	NC
10	43.5423	1.2031	.5938	.9999
15	41.9248	1.1563	.5938	.9998
20	40.4127	1.1406	.5938	.9997
30	37.8265	1.1406	.6094	.9994
50	34.0900	1.1563	.6094	.9986
70	31.4810	1.1719	.6094	.9974

Table III. Watermark extraction under different attacks (NC)

k	JPEG Q60	JPEG Q20	Salt & Pepper Noise
10	.8755	.8958	.8606
15	.9729	.8972	.8892
20	1	.8978	.8990
30	1	.9109	.9396
50	1	.9723	.9820
70	1	1	.9938

Table III demonstrate the results of proposed method precision versus common image processing attacks. The success rates of watermark extraction are listed. There is a trade-off between imperceptibility and robustness. Mid-Band coefficient exchange is quite efficient against JPEG compression, cropping, noising and other common image manipulation operations

The use of two PN sequences watermarking is based on the idea of spread spectrum communications. Table IV shows the quality rates under various executions and Table V shows PSNR and NC values for different values of k (gain factor).

Table IV. Quality rates under various executions

k	PSNR (dB)	Elapsed time (embedding) (seconds)	Elapsed time (extraction) (seconds)
5	42.1804	1.6094	1.0938
10	35.4356	1.6563	1.0938
20	30.5297	1.5930	1.0938
30	26.6209	1.5938	1.1094
50	22.6376	1.6094	1.0781
70	19.8752	1.6094	1.0781

The technique is motivated by perceptual transparency and watermark robustness. Results of the correlation-based DCT techniques were fairly similar. Correlation-based DCT appeared to be slightly weaker for lower levels of distortion, yet stronger for the higher levels. The use of two PN sequences is better in almost all aspects.

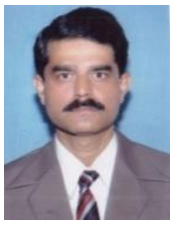
The elapsed time of embedding and extraction process for different values of k is more or less the same. PSNR above 20dB shows perceptually good watermarked image. In Table V as the JPEG Quality (Q) increases the PSNR increases and for particular JPEG quality decreases as k increases.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

REFERENCES

[1] Barni, M., P´erez-Gonz´alez, F.: Special session: watermarking security. In Edward J. Delp III, Wong, P.W., eds.: Security, Steganography, and Watermarking of Multimedia Contents VII. Volume 5681., San Jose, California, USA, SPIE (2005) 685–768.
[2] P´erez-Gonz´alez, F., Furon, T.: Special session on watermarking security. In Barni, M., Cox, I., Kalker, T., Kim, H.J., eds.: Fourth International Workshop on Digital Watermarking. Volume 3710., Siena, Italy, Springer (2005) 201–274.
[3] Bassia P., Pitas I., and Nikolaidis 2001, "Robust Audio Watermarking in Time Domain", IEEE Trans. On Multimedia, Vol. 3, pp. 232-241.
[4] R. B. Wolfgang and E. J. Delp, "Overview of image security techniques with applications in multimedia systems," Proceedings of the SPIE International Conference on Multimedia Networks: Security, Displays, Tenninals, and Gateways, November 4-5, 1997, Dallas, Texas, vol. 3228, pp. 297-308.
[5] I. J. Cox and M. L. Miller, "A review of watermarking and the importance of perceptual modeling," Proceedings of the SPIE International Conference on Human Vision and Electronic Imaging II, Feb. 10-13, 1997, San Jose, CA, USA, pp. 92-99.
[6] Darko Kirovski Henrique S. Malvar and Yacov Yacobi,(2002) "Multimedia Content Screening using a Dual Watermarking and Fingerprinting System", Proceedings of the tenth ACM international conference on Multimedia, pp.372-381.
[7] Sung Jin Lim, Hae Moon, Seung-Hoon Chae, Sung Bum Pan, Yongwha Chung and Min Hyuk Chang,(2008), "Dual Watermarking Method for Integrity of Medical Images", Second International Conference on Future Generation Communication and Networking, IEEE computer Society,pp. 70-73.
[8] Mingyi Jiang. Giiopiiig Xo, Dongfeiig Yuan (2004) "A Novel Blind Watermarking Algorithm Based on Multiband Wavelet Transform", Proceedings of ICSP, pp. 857-860.
[9] Barni, M., et al., Watermark embedding: hiding a signal within a cover image. Comm. Magazine, IEEE, 39(8): p. 102-108. 2001.
[10] Shoemaker, C., "Hidden bits: A survey of techniques for digital watermarking", Independent study, EER 290, spring 2002.
[11] I. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, December, 1997, pp. 1673-1687. F. M. Boland, J. J. K. 6 Ruanaidh and C. Dautzenberg.
[12] "Watermarking digital images for copyright protection," Proceedings of the International Conference on Image Processing and its Applications, Edinburgh, Scotland, July 1995, pp. 321-326.
[13] N.F. Johnson, S.C. Katezenbeisser, "A Survey of Steganographic Techniques" *in Information Techniques for Steganography and Digital Watermarking*, S.C. Katzenbeisser et al., Eds. Northwood, MA: Artec House, Dec. 1999, pp 43-75.
[14] A. Piva, M. Barni, E Bartolini, V. Cappellini.," DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image." s.l.: IEEE Transactions on image processing,1997.

Ritu Pareek was born in Jaipur, Inadia in 1989. She received her B.Tech degree in 2010 from Rajasthan Technical University, Kota. She is pursuing her M.tech in Signal Processing from Mody Institiute of Technology and Science (MITS), Lakshmangarh.



Dr. P. K. Ghosh was born in Kolkata, India in 1964. He received his B.Sc (Hons in Physics), B.Tech and M.Tech degrees in 1986, 1989, and 1991, respectively from Calcutta University. He earned Ph.D.(Tech) degree in Radio Physics and Electronics in 1997 from the same University. He served various institutions, namely, National Institute of Science and Technology (Orissa), St. Xavier's College (Kolkata), Murshidabad College of Engineering and Technology (West Bengal), R. D. Engineering College (Uttar Pradesh) and Kalyani Government Engineering College (West Bengal) before he joins Mody Institute of Technology and Science (Rajasthan). To his credit, he has more than 30 research papers in Journals of repute and conference proceedings. He is life member of Indian Society for Technical Education (ISTE), New Delhi. His research interests are in the areas of reduced order modeling, VLSI circuits & devices, wireless communications and signal processing.

Table V. The Quality rates under various executions

k	*JPEG Q20*		*JPEG Q60*		*JPEG Q100*		*Salt & Pepper Noise*	
	PSNR	NC	PSNR	NC	PSNR	NC	PSNR	NC
5	33.5196	.8065	36.5456	.8286	43.9887	.8669	36.4700	.8780
10	33.1722	.8454	32.8056	.9842	35.6882	.9757	30.1607	.9091
20	28.7331	.9397	27.7682	.9911	28.9670	.9842	27.1473	.9014
30	25.1015	.9905	23.9516	.9989	28.0738	.9900	26.3017	.9431
50	21.8071	.9922	20.7600	.9990	21.1026	.9989	21.4901	.9484
70	17.1751	1	19.2363	.9994	20.2104	1	20.7726	.9871