

STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN

Blossom Kaur¹, Amandeep Kaur², Jasdeep Singh¹

¹Department of Computer Science, B.M.S.C.E.T, Muktsar.

²Department of Information Technology, A.I.E.T, Faridkot.

ABSTRACT

Since all the multimedia products are released via internet so it's an urgent need today to protect the data from malicious attacks. This lead to the research in the area of Digital watermarking which intends to protect the copyright information of the intellectuals. In this paper a DCT based watermarking scheme is proposed which provides higher resistance to image processing attacks such as JPEG compression, noise, rotation, translation etc. In this approach, the watermark is embedded in the mid frequency band of the DCT blocks carrying low frequency components and the high frequency sub band components remain unused. Watermark is inserted by adjusting the DCT coefficients of the image and by using the private key. Watermark can then be extracted using the same private key without resorting to the original image. Performance analysis shows that the watermark is robust.

KEYWORDS

Steganography, Discrete Cosine Transform (DCT), Image Watermarking.

1. INTRODUCTION

Steganography comes from the Greek words Steganós (Covered) and Graptos (Writing). Steganography is a data hiding technique that has been widely used in information security applications [1]. It is similar to watermarking and cryptography techniques. However, these three techniques are different in some aspects. i) Watermarking mainly prevents illegal copy or claims the ownership of digital media but it is not geared for communication ii) Cryptography scrambles the data to be communicated so that unintended receivers cannot perceive the information. However, the fact that the communication has been carried out is known to everyone. [9] iii) Steganography transmits data by actually hiding the existence of the message so that a viewer cannot detect the transmission of message and hence cannot try to decrypt it. Digital watermarking has been proposed as a solution to the problem of copyright protection of multimedia data in a networked environment. Currently the digital watermarking technologies can be divided into two categories by the embedding position-spatial domain and transform domain watermark. Spatial domain techniques were developed earlier and is easier to implement, but is limited in robustness, is more sophisticated and robust. [3] The frequency image transformations include Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT). In this paper a watermarking algorithm for digital images is used: the method, which operates in the frequency domain and embeds a pseudo-random sequence of real numbers in a selected set of DCT coefficients. After embedding, the watermark is adapted to the image by exploiting the characteristics of the human visual system, thus ensuring the watermark invisibility. By exploiting the statistical properties of the embedded sequence, the watermark can be extracted without resorting to the original uncorrupted image. [2] The watermark has been tested using various types of noise such as Gaussian, speckle and salt and

pepper. The paper is divided into following sections. Section 2 gives the description of the common DCT based watermark insertion technique which works as the base of our proposed algorithm section 3 gives the description of the proposed scheme Section 4 describes the results and the discussion followed by the conclusion in Section 5.

2. DCT BASED WATERMARKING

DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. [10] One dimensional DCT can be described with the help of (1) and (2):

$$F(0) = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} f(x) \quad (1)$$

$$F(u) = \sqrt{\frac{2}{N}} \sum_{x=0}^{N-1} f(x) \cos \frac{2(x+1)u\pi}{2N} \quad (2)$$

Where $F(u)$ is cosine transform coefficient, u is general frequency variable, $u=1, 2, 3, \dots, N-1$; if $f(x)$ is M sequence of time domain, $x=1, 2, 3, \dots, N-1$, one dimensional inverse discrete cosine transform is defined as (3):

$$f(x) = \sqrt{\frac{1}{N}} F(0) + \sqrt{\frac{2}{N}} \sum_{u=1}^{N-1} F(u) \cos \frac{2(x+1)u\pi}{2N} \quad (3)$$

Two dimensional DCT can be defined analogously as (4):

$$f(x, y) = C(u)C(v) \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} F(u, v) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2y+1)v\pi}{2N} \right] \quad (4)$$

The inverse of two dimensional DCT can be defined as (5):

$$F(u, v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x, y) \cos \left[\frac{(2x+1)u\pi}{2N} \right] \cos \left[\frac{(2y+1)v\pi}{2N} \right] \quad (5)$$

For $x, y=0, 1, 2, \dots, N-1$. N is horizontal and vertical pixel number of pixel block, generally $N=8$. If N is more than 8, efficiency is increased a little but complexity is increased many times [11].

DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted. The literature survey reveals that mostly the middle frequency bands are chosen because embedding the watermark in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted [3]. Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component, most techniques utilize the comparison of middle band DCT coefficients to embed a single bit of watermark information into a DCT block. The middle-band frequencies (F_M) of an $8*8$ DCT block can be shown below in figure 2.1. DCT block consists of three frequency bands-Low frequency band (F_L), High frequency band (F_H), mid frequency band (F_M). We have chosen F_M for embedding the watermark.

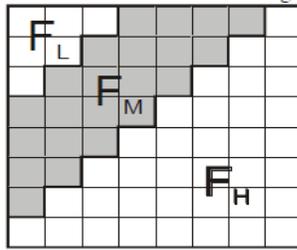


Fig 2.1 DCT regions

Two locations $M_i(u_1, v_1)$ and $M_i(u_2, v_2)$ from the frequency band F_M are chosen as the region for comparison. The choice in selection of the two locations is dependent on the JPEG quantization table given below in table 2.1. The two locations with similar quantization values are chosen for embedding one watermark bit of information.

Table 2.1 Quantization values

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	56	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

The DCT block will encode a “0” if $M_i(u_1, v_1) < M_i(u_2, v_2)$, otherwise it will encode a “1”. The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded [6]. The number of watermark bits that can be embedded is directly dependent on the number of pairs of locations in quantization table with similar values. The robustness of the watermark can be improved by introducing a watermark strength or gain constant k , such that $M_i(u_1, v_1) - M_i(u_2, v_2) > k$. Coefficients that do not meet this criteria are modified though the use of random noise as to then satisfy the relation. Increasing k thus reduces the chance of detection errors at the expense of additional image degradation [4].

Another category of DCT based watermarking techniques add a pseudo number sequence in the mid frequency band of the image to be watermarked. A strength factor k is used which gives robustness to the watermark. The value of k should be intelligently decided otherwise imperceptibility of the watermarked image with the original unwatermarked is reduced. For the mid frequency band of given DCT block x, y the embedding process can be shown using the equation (6) shown below:

$$I_{W_{xy}}(u, v) = \begin{cases} I_{xy}(u, v) + K * W_{xy}(u, v), & u, v \in F_M \\ I_{xy}(u, v), & u, v \notin F_M \end{cases} \quad (6)$$

2.1 Watermark embedding algorithm

The embedding function E for a watermarked image I_w is defined as (7):

$$I_w = E(I_0, W) \quad (7)$$

Where I_0 denotes the original multimedia signal (audio, image or video), W denotes the watermark containing the information that the owner wishes to embed.

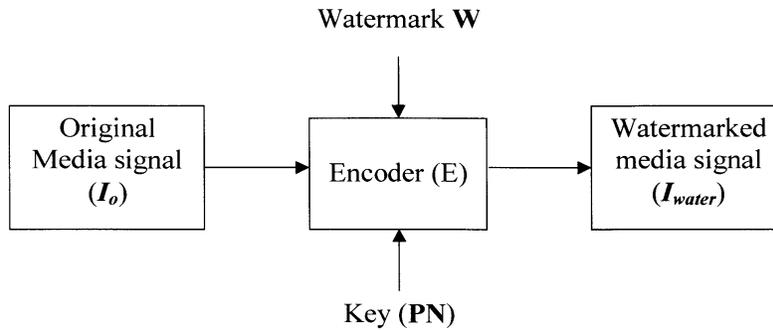


Fig. 2.1.1 The process of embedding

The algorithm for embedding a watermark in our case is:

1. Segment the image into two sub band blocks with half the size of the original image where the first part gives the high intensity pixels block & the second one gives the low intensity pixels block.
2. Break the image into blocks of size 8* 8 and DCT of each block is calculated.
3. Private Key is used to generate two pseudo random number sequences of domain { -1, 0, 1 } which are highly uncorrelated. [5][3]
4. Preprocess the watermark by converting watermark into a binary sequence using (8).

$$W(m * n) = W(s * 1) \quad \text{Where } s=m*n \quad (8)$$

5. Embed the watermark on each of the DCT block in the mid band of each coefficient block using the pseudo random number sequence and the watermark sequence.
6. After embedding the watermark the inverse DCT operation is done on the sub band to obtain the averaged image band again.
7. Inverse operation of step 2 is done to obtain the watermarked image.

2.2 Watermark extraction algorithm

For watermark extraction, detecting function D is used and is represented by (9):

$$W' = D(R, I_o) \quad (9)$$

Where R is the signal to be tested, whether it is watermarked or not and R could be a distorted version of I_w . The extracted watermark sequence (W') is compared with W and a Yes/No decision is made accordingly [7].

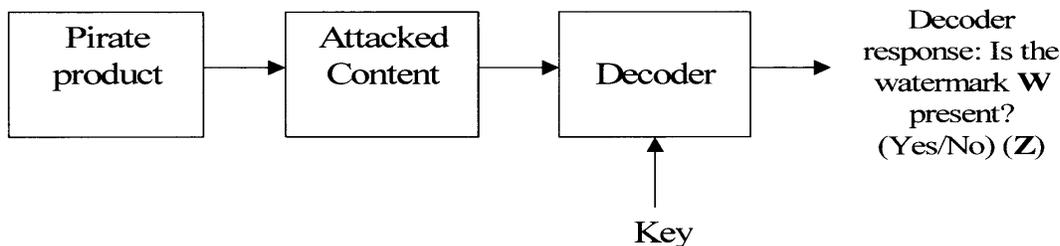


Fig 2.2.1 The process of extraction

The steps involved in the watermark extraction algorithm are given below. Take the image which is suspected of having the watermark and apply the following algorithm:

1. Repeat step I and II of watermark embedding algorithm
2. Extract the watermark using the private key.

3. Compare the watermark with the original watermark.
4. Similar watermark will prove the authenticity.

3. RESULTS AND DISCUSSIONS

The cover image used is 512x512 grayscale 'Lena' and the logo is a 64x64 grayscale image of 'copyright'. The cover image which is watermarked with the logo is subjected to various types of noise. For each type of noise the results are computed for the maximum extent that can be tolerated.

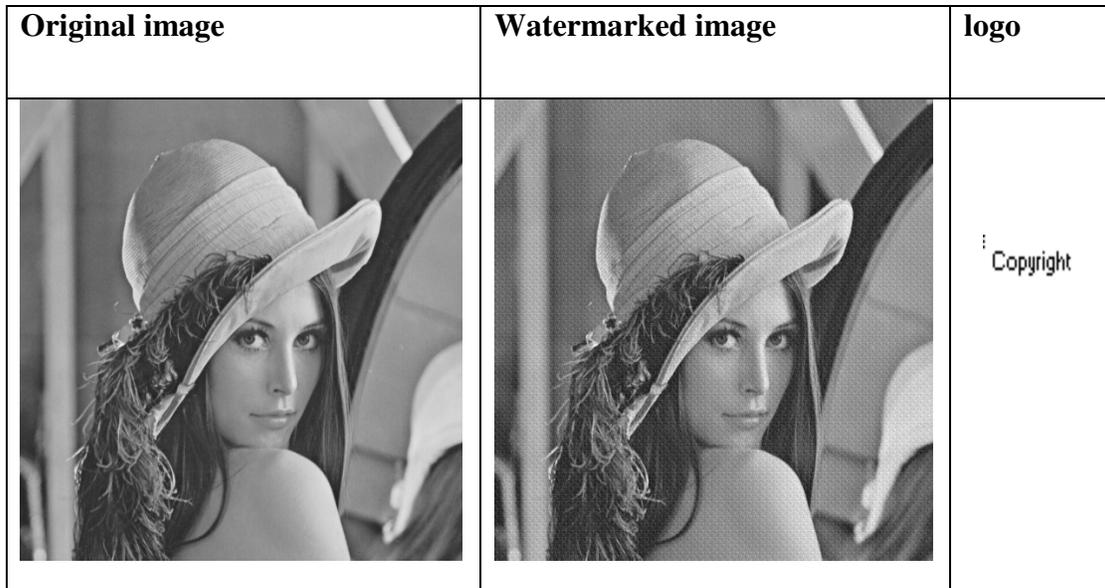


Fig 3.1 The cover image and extracted watermark

Table 1: Watermarked image under Gaussian noise attack

Noise density	Watermarked image (db)	Watermark sign(db)
0.02	80.8767	41.4806
0.04	75.4820	36.8411
0.06	71.0076	34.1501
0.08	70.4231	32.4872

Table 2: Watermarked image under salt and pepper noise attack

Noise density	Watermarked image (db)	Watermark sign(db)
0.02	50.5630	65.0830
0.04	43.8889	58.6052
0.06	40.8363	50.4970
0.08	36.7028	48.2900

Table 3: Watermarked image under speckle noise attack

Noise density	Watermarked image (db)	Watermark sign(db)
0.02	51.1103	29.0887
0.04	44.5117	28.9883
0.06	41.6380	28.5545
0.08	39.9855	29.1710

4. CONCLUSION

The transform domain watermarking techniques are better than spatial techniques, for both reasons of robustness as well as imperceptibility. Embedding in the DCT domain proved to be highly resistant to JPEG compression as well as significant amounts of noise. By anticipating which coefficients would be modified by the subsequent transform and quantization, we were able to produce a watermarking technique with moderate robustness, and low visual artifacts. But as all the DCT based images suffers from visual artifacts as DCT is done on the blocks, our approach is no exception. We have here with our approach tried to explore the DCT domain for digital image watermarking for gray scale images. Our technique could also be applied to the multi-resolution image structures with some modification about the choice of middle frequency coefficients.

5. FUTURE SCOPE

DCT technique can be combined up with DWT technique for security reasons. The idea of applying two transform is based on the fact that combined transforms could compensate for the drawbacks of each other, resulting in effective watermarking. DCT can also be combined up with Single-Value Decomposition (SVD) method for added robustness

REFERENCES

- [1] C.-T Hsu and J.-L.Wu, (1998) "Multiresolution watermarking for digital images," *IEEE Trans. Circuits Syst. II*, vol. 45, pp. 1097–1101.
- [2] F.A.P. Petitcolas,(2000) "Watermarking Schemes Evaluation ", in *IEEE Signal Processing Magazine*, Vol 17, pp 58-64.
- [3]. G. Langelaar, I. Setyawan, R.L. Lagendijk, (2000) "Watermarking Digital Image and Video Data", in *IEEE Signal Processing Magazine*, Vol 17, pp 20-43..
- [4]. Hsu, C.-T., Wu, J.-L., (1998) "Multiresolution Watermarking for Digital images", in *IEEE Transactions on Circuits and Systems - II: Analog and Digital Signal Processing*, vol. 45,no. 8, pp. 1097-1101.
- [5]. Lin Liu, "A Survey of Digital Watermarking Technologies", www.ee.sunysb.edu/~cvi/.../Lin%20Liu/ese558report_LinLiu.pdf
- [6]. Mauro Barni, Franco Bartolini, Vito Cappellini, Alessandro Piva(1998), "A DCT-domain system for robust image watermarking", *Signal Processing* 66 (1998), pp.357–372
- [7]. Mohamed A. Suhail, (2003) "Digital Watermarking-Based DCT and JPEG Model" *IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT*, VOL. 52, NO. 5
- [8]. Rafael C. Gonzalez, Richard E. Woods, —*Digital Image Processing*, 2nd Edition, Prentice hall publishers.

- [9]. Xiaojun Qi and KokSheik Wong, (2005) "An Adaptive DCT-Based MOD-4 Steganography Method", 0-7803-9134-9/05 IEEE.
- [10]. Gengming Zhu, and Nong Sang, (2008)," Watermarking Algorithm Research and Implementation Based on DCT Block", World Academy of Science, Engineering and Technology 45.
- [11]. Syed Ali Khayam, (2003) "The Discrete Cosine Transform (DCT): Theory and Application", ECE 802 – 602: Information Theory and Coding.

Authors' biography

Er. Blossom Kaur is a student of M.Tech in Computer Science from B.M.S.C.E.T, Muktsar. She has completed her degree of B. Tech in CSE from A.I.E.T, Faridkot in the year 2007.



Er. Amandeep Kaur is a student of M. Tech in information technology from A.I.E.T, Faridkot. She has done her degree of B. Tech from L.L.R.IE.T, Moga in the year 2008.



Er. Jasdeep Singh is presently working as Assistant Professor in B.M.S.C.E.T, Muktsar. He has completed his degree of B. Tech from A.I.E.T, Faridkot in the year 2006 and M. Tech from P.A.U, Ludhiana in the year 2009.

