International Journal of Latest Trends in Engineering and Technology
Vol.(8)Issue(3), pp.270-277
DOI: http://dx.doi.org/10.21172/1.83.041
e-ISSN:2278-621X

WATERMARKING METHOD BASED ON DCT INTENDED FOR HIGH EMBEDDING CAPACITY

Sahil G. Mujawar[1] and Amar A. Dum[2]

Abstract- In digital image watermarking, for applications like covert communication, high embedding capacity is desired. Hence, new method is proposed, which consists of two parts – embedding part and detection part. In first part, first step is dividing image into small blocks. Then DCT is applied to each block and embed the watermark data into image block. Here, the secret key is used to randomly select the DCT coefficients from middle frequency area of image. A secret key is used for security purpose. In detection part, the detection matrices are formed from received image to extract the watermark data. The proposed method requires only 3 coefficients to hide 2 watermark bit, normally it can achieve high embedding capacity.

Keywords – Discrete cosine transform, High embedding capacity, Image Watermarking.

I. INTRODUCTION

These days the copyright destruction has become a serious issue. Consequently, the demands for the copyright protection of digital multimedia are growing. The digital watermarking is a promising technique way out. In digital watermarking, the copyrighted information (such as signature, logo, ID number, etc.) is embedded into multimedia file itself. When owners want to proclaim their copyright, they can extract this copyright information.

With regards to image watermarking, imperceptibility, robustness, embedding capacity and security are of essential concerns. Until now, various image watermarking techniques were built, such as histogram, moment, spatial feature region, spread spectrum (SS) and quantization. As go through available literature, it is clear that, all watermarking methods developed are promises to tackle the piracy problem and with some extent of these major points. Different methods have different extent of these points. In numerous applications, for example, covert communication, high embedding capacity is required.

Compared to the Histogram, moment and spatial feature region watermarking methods, the methods based on SS and quantization can normally achieve higher embedding capacity under given imperceptibility and robustness. But, the SS-based watermarking approach suffers from the problem of host signal interference (HSI). It is known that HSI can greatly degrade the performance of watermark detection, especially in the presence of attacks, and thus lower robustness. However, similar to the SS-based watermarking methods, the quantization based watermarking methods do not perform well under high embedding rates. The remainder of the paper is organized as follows. Section II introduces the proposed image watermarking method. The simulation results are shown in Section III. Section IV concludes the paper.

II. PROPOSED METHOD

2.1 Embedding part-

Consider a grey level host image I of size R × C. Without loss of generality, I is partitioned into N non-overlapping blocks I1, I2,…, IN, where the size of each block is M × M and M is a positive integer power of '2'. The 2-D discrete cosine transform is applied to each block to obtain the DCT counterparts F{I1}, F{I2},…, F{IN} of dimension M × M. Since low frequency components carry perceptually important information and high frequency

[1] *Department of Electronics Technology Dept. of Technology, Shivaji University, Kolhapur, Maharashtra, India*
[2] *Department of Electronics Technology Dept. of Technology, Shivaji University, Kolhapur, Maharashtra, India*

components are vulnerable to image compression attack, it is appropriate and common to use the DCT coefficients corresponding to the middle frequency range for watermark embedding. In each block, we use a secret key to randomly select 's' suitable DCT coefficients to form a DCT coefficient set, where the 's' is the number which is multiple of 3.The purpose of using a secret key is to introduce security.

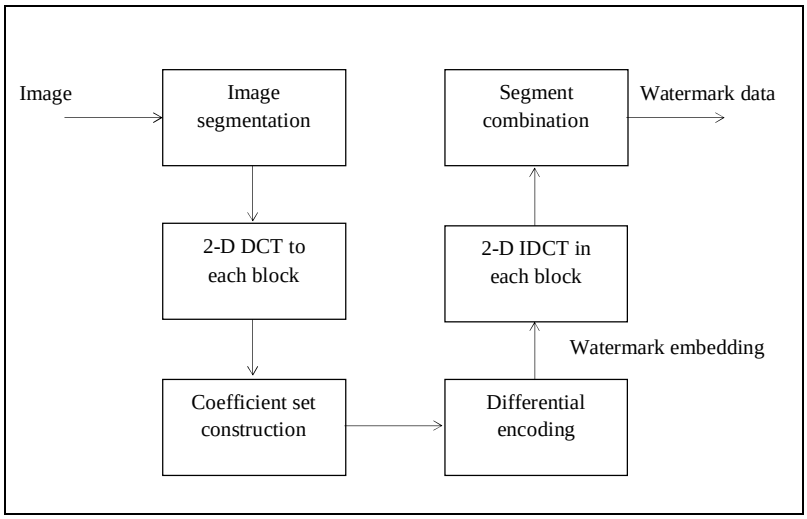

Figure 1. Block diagram of Watermark embedding part

Denote the length-s coefficient set in the n'th block by

$$X_n = [X_n(1), X_n(2), \ldots, X_n(s)] \quad (1)$$

where n = 1,2,. . . ,N. From X_n we can obtain 'K'- groups containing 3 DCT coefficients each. The DCT coefficients set of k'th group is

$$X_{n,k} = [X_n(k-2), X_n(k-1), X_n(k)] \quad (2)$$

where k = 1, 2, ... , K. Based on (1) and (2), it follows

$$X_n = [X_{n,1}, X_{n,2}, \ldots, X_{n,K}] \quad (3)$$

where n = 1,2,. . . ,N. Each group of DCT coefficients will be used to hide two watermark bits.

$$w_n = [w_n(1), w_n(2), \ldots, w_n(Z)] \quad (4)$$

be the sequence of 'Z' watermark bits to be embedded into the n'th image block, where the watermark bits $w_n(z)$, z = 1,2, . . . ,Z. take values from {0,1}. Hence, the total length of the watermark sequence is N×Z.

Then, check whether, if $X_n(k-2) = X_n(k-1)$, then adding some constant 'c' to $X_n(k-2)$.

i.e. $X_n(k-2) = X_n(k-2) + c$

Similarly, if $X_n(k-1) = X_n(k)$, then adding some constant 'c' to $X_n(k)$.

i.e. $X_n(k) = X_n(k) + c$

where, 'c' can be any non-zero value.

Now, define the 3×3matrix A_n, and initiate it as a zero matrix.

Let,

$$A_1 = \begin{bmatrix} 0.3333 & 0.3333 & 0.3333 \\ 0.3333 & 0.3333 & 0.3333 \\ 0.3333 & 0.3333 & 0.3333 \end{bmatrix}, \quad A_2 = \begin{bmatrix} 0.5 & 0.5 & 0 \\ 0.5 & 0.5 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$A_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0.5 & 0.5 \\ 0 & 0.5 & 0.5 \end{bmatrix}, \quad A_4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad (5)$$

For k'th group of coefficients, update the values of A_n based on values of watermark data, as shown in Table 1.

Then multiply k'th group of coefficients with matrix A_n, to form Y_n.

$$Y_n = X_{n,k} \times A_n. \quad (6)$$

where, n = 1, 2, . . . , N.

Table - 1 Matrix A_n up-gradation

$W_n(z-1)$	$W_n(z)$	A_n
0	0	A_1
0	1	A_2
1	0	A_3
1	1	A_4

Let,

$$Y_n = [\, Y_n(1), Y_n(2) \ldots, Y_n(S)]. \quad (7)$$

be the watermarked counterpart of X_n.

The sequence of watermark bits W_n is embedded into X_n using the formula (6). By replacing X_n in F{ I_n} with Y_n, one can get the watermarked counterpart of F{I_n}, denoted a F{ I_n^W }. After that, we apply the 2-D inverse discrete cosine transform (IDCT) to F{ I_n^W } to obtain the watermarked image block I_n^W. Finally, the watermarked image I^W can be constructed by combining all of the watermarked image blocks together.

2.2 Detection part-

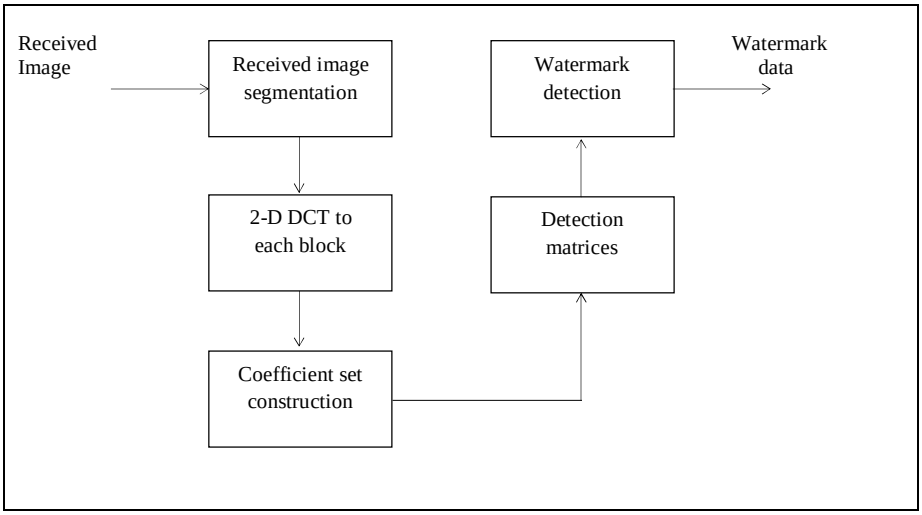

Figure 2. Block diagram of Watermark detection part.

Denote the received image as I'. Similar to the embedding process, I' is divided into N non-overlapping blocks. I1',I2', . . . , IN' of dimensions M×M. Applying 2-D DCT to the received image blocks yields the corresponding DCT components F{I'1}, F{I'2},…,F{I'N} of dimensions M×M. In the n'th block F{I'n}, the secret key can be used to find the length- 's' DCT coefficients set X_n containing Z watermark bits. Denoting by

$$X'_n = [X'_n(1), X_n(2) \ldots, X'_n(S)] \quad (8)$$

where n = 1,2,. . . ,N. From X'_n we can obtain K- groups of 3 DCT coefficients each. The DCT coefficients set of k'th group is

$$X'_{n,k} = [X'_n(k - 2), X'_n(k - 1), X'_n(k)] \quad (9)$$

where k = 1, 2, ... , K. Based on (8) and (9), it follows

$$X'_n = [X'_{n,1}, X'_{n,2}, \ldots, X'_{n,K}] \quad (10)$$

where n = 1,2,. . . ,N.

One can sequentially compute,
$\Delta 1_n(k) = | X'_n(k - 2) - X'_n(k - 1)|$ and $\Delta 2_n(k) = | X'_n(k - 1) - X'_n(k)|$. (11)

And
$T1'(k) = \max \{\Delta 1_n(k), 0\}$ and $T2'(k) = \max \{\Delta 2_n(k), 0\}$. (12)

Based on T1'(k) and T2'(k), construct the detection matrices $X1_{n,k}$ and $X2_{n,k}$ for the extraction of the $w_n(z-1)$ and $w_n(z)$ watermark bit resp. in k'th group of n'th block.

$$X1_{n,k} = \begin{bmatrix} 0 & T1'(K) \\ T1'(K) & 0 \end{bmatrix} \quad \text{and} \quad X2_{n,k} = \begin{bmatrix} 0 & T2'(K) \\ T2'(K) & 0 \end{bmatrix} \tag{13}$$

Where, k = 1, 2, . . . , K and n = 1, 2, . . . , N.

In order to use $X1_{n.k}$ and $X2_{n.k}$ to extract the watermark bits (i.e.: $w_n(z-1)$ and $w_n(z)$), let us analyse the property of X1n,k in the absence of attacks. Since attacks are absent, it is obvious that $I' = I^w$, which results in $X'_n = Y_n$ or $X'_n(s) = Y_n(s)$. The analysis is conducted for two cases as following.

Case 1) Consider, watermark bits are $w_n(z-1) = 0$ and $w_n(z) = 0$, for k'th group of coefficients in for n'th block. And, $X_n(k - 2) \neq X_n(k - 1) \neq X_n(k)$

For this case, it follows from equations (5), (6) and table no.1.
$[X_n(k - 2), X_n(k - 1), X_n(k)]$

$= [X_n(k - 2), X_n(k - 1), X_n(k)]$. A1

$$= \left[\frac{Xn(k-2) + Xn(k-1) + Xn(k)}{3}, \frac{Xn(k-2) + Xn(k-1) + Xn(k)}{3}, \frac{Xn(k-2) + Xn(k-1) + Xn(k)}{3}\right] \tag{14}$$

which means,

$| X_n(k - 2) - X_n(k - 1)| = 0$ and $| X_n(k - 1) - X_n(k)| = 0$.

Since, $X'_n(s) = Y_n(s)$, it yields from (11) and (14) that

$\Delta 1_n(k) = 0$, and $\Delta 2_n(k) = 0$. (15)

Based on (12) and (15) it follows
$T1'(k) = \max \{0,0\} = 0$ and $T2'(k) = \max \{0,0\} = 0$ (16)
Substituting (16) into (13), we can see that both detection matrices are rank deficient as its entries have the same value '0'.

Case 2) Consider, watermark bits are $w_n(z-1) = 1$ and $w_n(z) = 1$, for k'th group of coefficients in for n'th block. And, $X_n(k - 2) \neq X_n(k - 1) \neq X_n(k)$

For this case, it follows from equations (5), (6) and table no.1.
$[X_n(k - 2), X_n(k - 1), X_n(k)]$
$= [X_n(k - 2), X_n(k - 1), X_n(k)]$. A4
$= [X_n(k - 2), X_n(k - 1), X_n(k)]$ (17)

Since, X'n(s) = Yn(s), it yields from (11) and (17) that
$\Delta 1_n(k) = X_n(k - 2) - X_n(k - 1)$ and $\Delta 2_n(k) = X_n(k - 1) - X_n(k)$. (18)

Based on (12) and (18) it follows

$T1'(k) = \max\{\Delta 1_n(k), 0\} = \Delta 1_n(k)$ and $T2'(k) = \max\{\Delta 2_n(k), 0\} = \Delta 2_n(k)$ (19)

Substitute (19) into (13)

$$X1_{n,k} = \begin{bmatrix} 0 & \Delta 1_n(k) \\ \Delta 1_n(k) & 0 \end{bmatrix}, \quad \text{and} \quad X2_{n,k} = \begin{bmatrix} 0 & \Delta 2_n(k) \\ \Delta 2_n(k) & 0 \end{bmatrix} \tag{20}$$

We can see that, the ranks of detection matrices $X1_{n,k}$ and $X2_{n,k}$ resp., are full of rank.
Similarly, for $w_n(z-1) = 0$ and $w_n(z) = 1$. The rank of detection matrix $X1_{n,k}$ is rank deficient and while rank of $X2_{n,k}$ is full of rank. Since, in that case, we can find, the values $T1'(k) =$ '0' and $T2'(k) = \Delta 2_n(k)$.

Similarly, for $w_n(z-1) = 1$ and $w_n(z) = 0$. The detection matrix $X1_{n,k}$ is full of rank and $X2_{n,k}$ is rank deficient. Since, in that case, we can find, the values $T1'(k) = \Delta 1_n(k)$ and $T2'(k) =$ '0'.

Based on the rank of $X1_{n,k}$ and $X2_{n,k}$, the $w_n(z-1)$ and $w_n(z)$ watermark bit in the nth block can be extracted using the following detection rule:

Table - 2 Detection matrices

Detection Matrices		Watermark data	
$X1_{n,k}$	$X2_{n,k}$	$W'_n(z-1)$	$W'_n(z)$
Rank deficient	Rank deficient	0	0
Rank deficient	Full of rank	0	1
Full of rank	Rank deficient	1	0
Full of rank	Full of rank	1	1

Where k = 1, 2,…, K and n = 1, 2,…,N. Finally, the extracted watermark sequences $w'_n(1)$, $w'_n(2)$,…,$w'_n(Z)$can be obtained by combining all of the detected watermark bits.

III. SIMULATION RESULTS

Evaluation of the performance of proposed system is carried out by simulations, in comparison with methods [5], [10]. Eight standard 512 × 512 8-bit gray scale images Elaine, Hill, Bee, Zelda, Goldhill, Lighthouse, Lenna, and Truck used as host(original) images as shown. The peak signal-to-noise ratio (PSNR) index and the bit error rate (BER) index are utilized to measure perceptual quality and robustness, respectively. The performance parameters PSNR and BER are figured by averaging the outcomes acquired from the eight images. With respect to, the bigger PSNR esteem the better perceptual quality. It is specified in [12] that the PSNR estimation of 40dB shows great perceptual quality.
For instance, the bottom two rows of Figure 4. shows, the watermarked counterparts of the up to said eight images by our technique, where PSNR = 44.9525dB. Obviously, there is no visual difference between the original images and their watermarked images. With respect to robustness, a littler BER value shows better robustness, and vice-versa. In the simulations, we choose N = 4096 for all images. Embedding rates is considered as 16384 watermark bits per image, which correspond to K = 2.

3.1 Embedding capacity-

Embedding rate is 16384 bits which is much more than other methods. Proposed method achieves high embedding capacity, since our method required as little as '3' coefficients to embed '2' watermark bits.

Table - 3 Watermarking Embedding capacity for different methods

Watermarking methods	Proposed method	Method in [5]	Method in [10]
Embedding Capacity	16384	8192	12288
Ratio = $\frac{\text{Number of Watermarked bits}}{\text{Number of coefficients required}}$	$\frac{2}{3}$	$\frac{1}{4}$	$\frac{1}{31}$

3.2 Imperceptibility-

PSNRs of different watermarking methods are as shown in Table 4. Obviously, there is no any difference in original images and corresponding watermarked images. Hence, the proposed system is imperceptible.

Table - 4 PSNR value for different methods

Watermarking methods	Proposed method	Method in [5]	Method in [10]
PSNR(dB)	44.9525	41.76	39.93

(a) Original Elaine (b) Original Hill (c) Original Bee (d) Original Zelda

(e) Original Goldhill (f) Original Lighthouse (g) Original Lenna (h) Original Truck

(a) Watermarked Elaine (b) Watermarked Hill (c) Watermarked Bee (d) Watermarked Zelda

(e) Watermarked Goldhill (f) Watermarked Lighthouse (g) Watermarked Lenna (h) Watermarked Truck

Figure 4. Upper two rows - Original images Elaine, Hill, Bee, Zelda, Goldhill, Lighthouse, Lenna, and Truck. Lower two rows: watermarked counterparts of these images.

3.3 Robustness-

3.3.1 In the absence of attack-

For any watermarking method its BER value obtained in the absence of attacks indicates the impact of HSI. Since HSI does not exist in the proposed method, perfect watermark detection can be achieved.

Table - 5 BER in the absence of attack

Watermarking methods	Proposed method	Method in [5]	Method in [10]
BER	0	0.0746	0.0001

3.3.2 In the presence of constant luminance change attack -

Table – 6 BER in the presence of attack

Luminance change	Proposed method	Method in [5]	Method in [10]
+10	**0**	**0.0746**	**0.0024**
-10	**0**	**0.0770**	**0.0057**
+30	**0**	**0.0770**	**0.0213**
-30	**0**	**0.0910**	**0.1077**

Table 6 shows that, BER of our method remains ideal in the presence of constant luminance change attacks. This is because the constant luminance change does not alter the DCT coefficients of the watermarked image block, except for the DCT coefficient at (u, v) = (0, 0) [11]. Since, the proposed system uses medium frequency region to select DCT coefficients for watermark embedding. Hence, there is no any change in BER in the presence of constant luminance change attack.

IV CONCLUSION

In this paper, we proposed a new technique for image watermarking in the DCT area. The proposed watermarking technique has some necessary striking features. Our technique can use as little as three DCT coefficients to embed two watermark bits, which leads to high embedding capacity. Secondly, the proposed system is free of HSI. Thirdly, it can remarkably tolerate the errors brought on by attack. Second and third features make the proposed technique robust against constant luminance change attack. The superior execution of the new strategy was verified by simulation results.

REFERENCES

[1] S. Xiang, H. J. Kim, and J. Huang, "Invariant image watermarking based on statistical features in the low-frequency domain," IEEE Trans. Circuits Syst. Video Technol., vol. 18, no. 6, pp. 777-790, Jun. 2008.

[2] T. Zong, Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, and G. Beliakov, "Robust histogram shape-based method for image watermarking," IEEE Trans. Circuits Syst. Video Technol., vol. 25, no. 5, pp. 717-729, May 2015.

[3] M. Alghoniemy and A. H. Tew_k, "Geometric invariance in image watermarking," IEEE Trans. Image Process., vol. 13, no. 2, pp. 145-153, Feb. 2004.

[4] P. Dong, J. G. Brankov, N. P. Galatsanos, Y. Yang, and F. Davoine, "Digital watermarking robust to geometric distortions, " IEEE Trans. Image Process., vol. 14, no. 12, pp. 2140-2150, Dec. 2005.

[5] M. Li, M. K. Kulhandjian, D. A. Pados, S. N. Batalama, and M. J. Medley, "Extracting spread-spectrum hidden data from digital media," IEEE Trans. Inf. Forensics Security, vol. 8, no. 7, pp. 1201-1210, Jul. 2013.

[6] X. Gao, C. Deng, X. Li, and D. Tao, "Geometric distortion insensitive image watermarking in affine covariant regions," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 40, no. 3, pp. 278-286, May 2010.

[7] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia,"IEEE Trans. Image Process., vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[8] J. Cannons and P. Moulin, "Design and statistical analysis of a hash-aided image watermarking system," IEEE Trans. Image Process., vol. 13, no. 10, pp. 1393-1408, Oct. 2004.

[9] H. S. Malvar and D. A. F. Florencio, `"Improved spread spectrum: A new modulation technique for robust watermarking," IEEE Trans. Signal Process., vol. 51, no. 4, pp. 898-905, Apr. 2003.

[10] Q. Li and I. J. Cox, "Using perceptual models to improve fidelity and provide resistance to valumetric scaling for quantization index modulation watermarking," IEEE Trans. Inf. Forensics Security, vol. 2, no. 2, pp. 127-139, Jun. 2007.

[11] T. Zong, Y. Xiang, S. Guo and Y. Rong, "Rank-Based Image Watermarking Method With High Embedding Capacity and Robustness," in IEEE Access, vol. 4, no., pp. 1689-1699, 2016.

[12] H. Zhang et al., "Affine Legendre moment invariants for image watermarking robust to geometric distortions, " IEEE Trans. Image Process., vol. 20, no. 8, pp. 2189-2199, Aug. 2011.

[13] P. C. Su, Y. C. Chang, and C. Y. Wu, "Geometrically resilient digital image watermarking by using interest point extraction and extended pilot signals," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1897-1908, Dec. 2013.

[14] A. K. Parthasarathy and S. Kak, "An improved method of content based image watermarking," IEEE Trans. Broadcast., vol. 53, no. 2, pp. 468-479, Jun. 2007.