CSIT (November 2014) 2(3):163–168
DOI 10.1007/s40012-014-0052-6

ORIGINAL RESEARCH

DCT based Secure Data Hiding for Intellectual Property Right Protection

Harsh Vikram Singh · Ashutosh Kumar Singh · Suman Yadav · Anand Mohan

Received: 22 July 2013 / Accepted: 5 August 2014 / Published online: 9 September 2014

Abstract In this paper, an algorithm for embedding copyright mark into host image based on discrete cosine transform (DCT) and Spread Spectrum has proposed. The proposed algorithm works by dividing the cover into blocks of equal sizes and then embeds the watermark in middle band of DCT coefficient of cover image. Performance evaluation of proposed algorithm has been made using bit error rate and peak signal to noise ratio value for different watermark size and images: Lena, Girl, and Tank images yield similar results. This algorithm is simple and does not require the original cover image for watermark recovery. A set of systematic experiments, including JPEG compression, Gaussian filtering and addition of noise are performed to prove robustness of our algorithm.

Keywords Data embedding · Watermarking · Robust steganography · Spread spectrum

1 Introduction

The growth of high speed computer networks and that of internet have made reproduction and distribution of digital data easier than ever before. It raises problem of copyright protection. One way for copyright protection is digital watermarking [1, 2] which means embedding of certain specific information about the copyright holder (company logos, ownership identification, etc.) into the media to be protected. Digital watermarking is a kind of data hiding technology. It has been used for a variety of applications, including copyright protection, data hiding, and authentication and fingerprinting. Watermarking is a young field and it is growing exponentially [4, 5]. Digital watermarking schemes can be categorized as "visible" and "invisible" watermarking. The visible watermarks are easily identified; they are usually not robust against common image processing operation.

The invisible watermarks are more secure and robust than visible watermarks. In invisible watermarking, the watermarked image should look similar to the original image. Based on the processing domain the watermarking schemes can be classified as spatial domain and transform domain [6, 7] techniques. The spatial domain watermarking is computationally simple and straight forward wherein host media data is directly replaced by watermark data using substitution techniques. However, these techniques are more fragile to external attacks and thus provide poor robustness of the watermark. On the other hand the transform domain techniques require more computations but they achieve superior robustness against lossy compressions and different filtering operations such as median, high-pass and low-pass, addition of noise etc. [8, 9]. Therefore transform domain techniques have proved better choice for achieving enhanced security of watermark and thus for greater assurance of originality of a multimedia data at the receiving end. Generally digital document distribution may consist of image, audio or text or their permutations distributed through open channel. In this paper, our present study focuses on copyright

H. V. Singh (✉) · S. Yadav
Department of Electronics, Kamla Nehru Institute of Technology, Sultanpur 228118, India
e-mail: harshvikram@gmail.com

A. K. Singh
Department of Electrical and Computer Engineering, Curtin University of Technology, Sarawak Campus, Miri, Malaysia

A. Mohan
National Institute of Technology, Kurukchetra, India

protection on still image documents. Common transform domain techniques mainly are discrete cosine transform (DCT) or discrete wavelet transform (DWT) [10, 11], Discrete Fourier transform (DFT), but DCT is frequently preferred because it is widely used in JPEG and MPEG [12, 13]; and thus it has merited our attention under the present study.

This paper describes an algorithm for achieving enhanced robustness of watermark data. Higher robustness of watermark has been achieved using spread spectrum technique. Embedding of watermark data into mid-band DCT coefficients has been carried out to achieve visual imperceptibility [14, 15] of the hidden watermark which is statistically undetectable and robust against image manipulation attacks. The benefits of the developed algorithm are illustrated through simulation studies by hiding binary logo image into different IEEE standard images such as Lena, Girl and Tank images. The qualitative performance analysis of the suggested algorithm has been carried out through analysis of histogram, JPEG compression, low pass filtering and addition of noise steganalysis techniques [16].

The rest of paper is organized as follows. Section II describes DCT and algorithm principle of watermark. Details of the proposed algorithm are presented in Section III. Experiment and results are discussed in Section IV. The performance under various attacks is examined in Section V. Finally, the conclusions have been made in Section VI.

2 Model of algorithm

This section, describes algorithm principle of watermark, DCT to obtain watermarked image. Watermarked image is combination of cover image and hidden image. DCT is used to convert watermarked object in spatial domain into watermarked image in frequency domain. All the images are assumed to be in standard format.

2.1 Discrete cosine transform

The DCT has been widely used for source coding in context of JPEG and MPEG and was later also considered for the use of embedding a message inside images and video. It processes some other characteristics and advantages such as vector base good embodiment about image information, small computational complexity, high compression ratio, low error rate, good concealing, and so on, so it is considered the optimal transformation in the digital image processing [18]. Two-dimensional DCT and its inverse transform are defined as [19]:

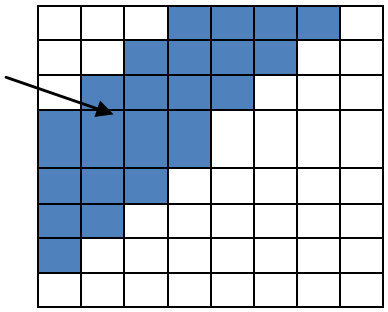

Fig. 1 Mid-frequency DCT region

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

$$f(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} \alpha(u)\alpha(v)c(u,v) \cos\left[\frac{\Pi(2x+1)u}{2N}\right]\cos\left[\frac{\Pi(2y+1)v}{2N}\right]$$

where u, v = 0, 1, 2,..., N−1x, y = 0, 1, 2,…, N−1 α(u) is defined as follows:

$$\alpha(u) = \sqrt{\tfrac{1}{N}} \quad u = 0; f_L, f_M \text{ and}$$

$$\alpha(u) = \sqrt{\tfrac{2}{N}} \quad u = 1, 2, \ldots, N-1$$

The major benefits of DCT include its high energy compaction properties and availability of fast algorithms for the computation of transform. The energy compaction property of the DCT results in transform coefficients with only few coefficients having values, thus making it well suited for watermarking. Embedding rules in DCT domain are more robust to JPEG/MPEG.

2.2 Algorithm principle

The basic principle of digital watermarking algorithm consists of two parts: watermark embedding and recovery. In watermark embedding, original image is first divided into 8 × 8 sub blocks and then embed watermark bit is spread over middle frequency band DCT coefficient values in the image blocks. The spreading is done by two pseudo-random (PN) sequences, one for zero bit and other for one bit of watermark. At last, watermarked image comes from taking inverse discrete cosine transform (IDCT).In watermark recovery it is an inverse process of embedding which finds correlation between middle frequency band DCT coefficient values in the image and corresponding two PN sequences and recovery of watermark.

The middle frequency coefficients are usually chosen due to their moderate variance property. The mid-frequency region is a popular choice for data embedding in order to limit the distortion and enable the algorithm to be

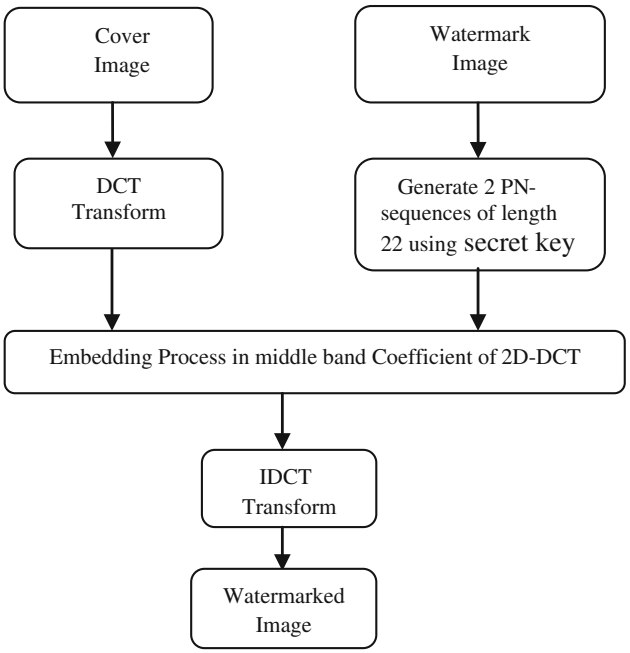

Fig. 2 Watermark embedding

robust against a multitude of image manipulating attacks. The mid-frequency regions of the DCT coefficient blocks are used to embed the hidden data as shown in Fig. 1, where f_L, f_M and f_H represent the low, medium and high frequency bands respectively [17].

3 Proposed algorithm

The proposed algorithm relies on two PN sequences [20], one for zero bit and other for one bit of watermark with low correlation. A PN noise sequence is generated by using the rand function in MATLAB. This uniform PN sequence generator must be initialized using a predefined 'key'. This key is available at both embedding and recovery locations and it can be communicated through secure channel prior to sending watermark image over open channel. The proposed algorithm is a combination of spread spectrum watermarking and transform domain watermarking techniques. Use of spread spectrum entails robustness and it combination with DCT domain increases the robustness of this algorithm. The proposed algorithm must provide robustness against a variety of image manipulation attacks.

3.1 Watermark embedding

This paper presents an algorithm of digital watermark embedding in the middle frequency band. Instead of using n PN sequences as in [3] here only two PN sequences are used. Figure 2 illustrates the watermark embedding process. The algorithmic steps are discussed below: Fig. 3.

1. Read Cover image and n-bit watermark signal.
2. Generate two PN sequences of length 22 (for 22 mid-band DCT coefficients) using a secret key to reset the random number generator, one for 'zero' and other for 'one' bit.
3. Transform the original image using 8 × 8 block 2D-DCT.
4. Hide the ith watermark bit, modulate the ith DCT block of the host using Eq. 1 for a '0' or a '1' bit. For Mi = 1 to n.

$$I_{W(u,v)} = \begin{cases} I(u,v) + \alpha^* W_i(u,v), & \text{if } u,v \in f_M \\ I\ (u,v), & \text{if } u,v \notin f_M \end{cases} \quad (1)$$

where f_M are the mid-band coefficient. α is the gain factor (in present simulation $\alpha = 9$) used to specify the strength of the embedded data; W_i is the appropriate pseudo random noise sequence, based on the ith watermark bit; ***I(u, v)*** represents the 8 × 8 DCT block of the original image. $I_W(u,\ v)$ represents the corresponding watermarked DCT block
5. To take Inverse transform each of the watermarked DCT blocks, I_W (u, v), using 8 × 8 blocks inverse 2D-DCT to get the final watermarked image I_W (x, y).

3.2 Watermark recovery

The watermark recovery procedure is based on correlation between the middle frequency band DCT coefficients of the image and corresponding PN sequences [3]. Watermark recovery is the inverse process of the embedding. The steps involved in recovery are listed below:

1. Read watermarked image.
2. Generate two pseudo-random (PN) sequences of length 22 (for 22 mid-band DCT coefficients) after resetting the random number generator using the same secret key as the encoder one for '0' and other for '1'.
3. Transform the watermarked image using 8 × 8 block 2D-DCT.
4. 4Extract the middle band coefficients which have recorded the location, determine the watermark information.
5. For M***i*** = 1 to ***n*** Calculate the correlation between the mid-band coefficients of ith block and ith PN-sequences.
6. Extract the jth watermark bit, b_j, using the following expression

$$b_j = \begin{cases} 0, & \text{if } \mathrm{corr}(0) > \mathrm{corr}(1) \\ 1, & \text{if } \mathrm{corr}(1) > \mathrm{corr}(0) \end{cases} \quad (2)$$

where **c**orr (0) i**s** the correlation between extracted coefficient of jth block and PN sequence generated for bit '0'. Corr (1) is the correlation between extracted

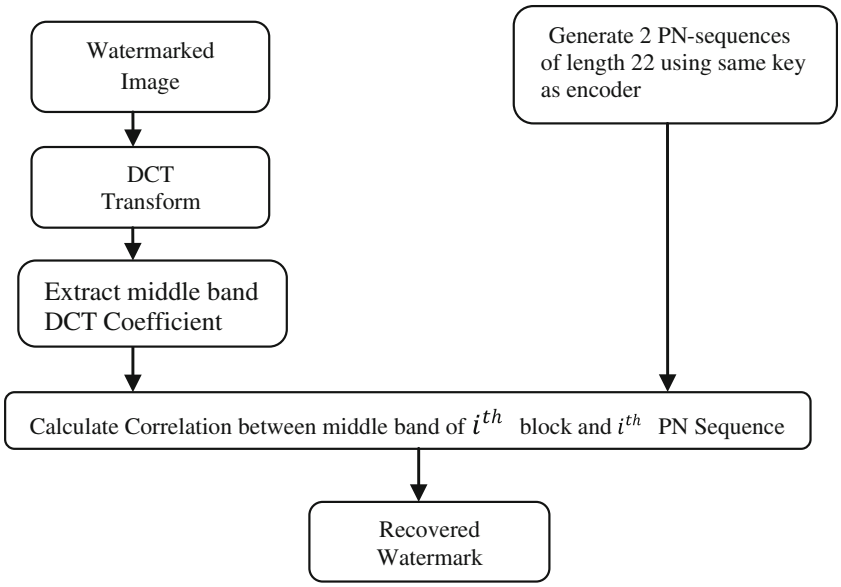

Fig. 3 Watermark recovery

Original Watermark Recovered Watermark

Fig. 4 Original and recovered watermarks without attacks

coefficient of *j*th block and PN sequence generated for bit '1'.

4 Experiments and results

The proposed watermarking algorithm is tested with the 512 × 512 gray scale Lena image, tests with other images yield similar results. The watermark as shown in Fig. 4 is used in simulation. The watermark is binary logo of size (55 × 52) which is converted into a row vector of size 2860 × 1 as the watermarking signal, these watermark bits are embedded into the middle band DCT coefficient of cover image. Performance metrics of watermarking algorithm such as PSNR, BER are computed with and without attacks. The PSNR of watermarking algorithm is reasonable high and the artifacts introduced by watermark embedding are almost invisible. Experimental results without attacks i.e., original image, watermarked image, original and recovered watermarks are shown in Table 1, Fig. 4 and 5. Table 2 shows PSNR value for different watermark sizes and images.

Table 1 Performance metrics of watermarking algorithm without attacks

Peak signal to noise ratio (PSNR)	37.29
Bit error rate (BER)	0.0178
Processing time for embedding	12.95 S
Processing time for extraction	15.14 S

512 x 512 original image 512x512 Watermarked image

Fig. 5 Original and watermarked image without attacks

Table 2 PSNR value for different watermark sizes and images

Images	55 × 52	64 × 61	64 × 17	96 × 27
Lena	37.2962	37.0212	37.8894	37.7054
Girl	37.2961	37.0212	37.8894	37.7052
Tank	37.2960	37.0212	37.8894	37.7052

Figure 6 shows that there are few pixels having different intensity level of watermarked image as compared to original image due to insertion of watermark.

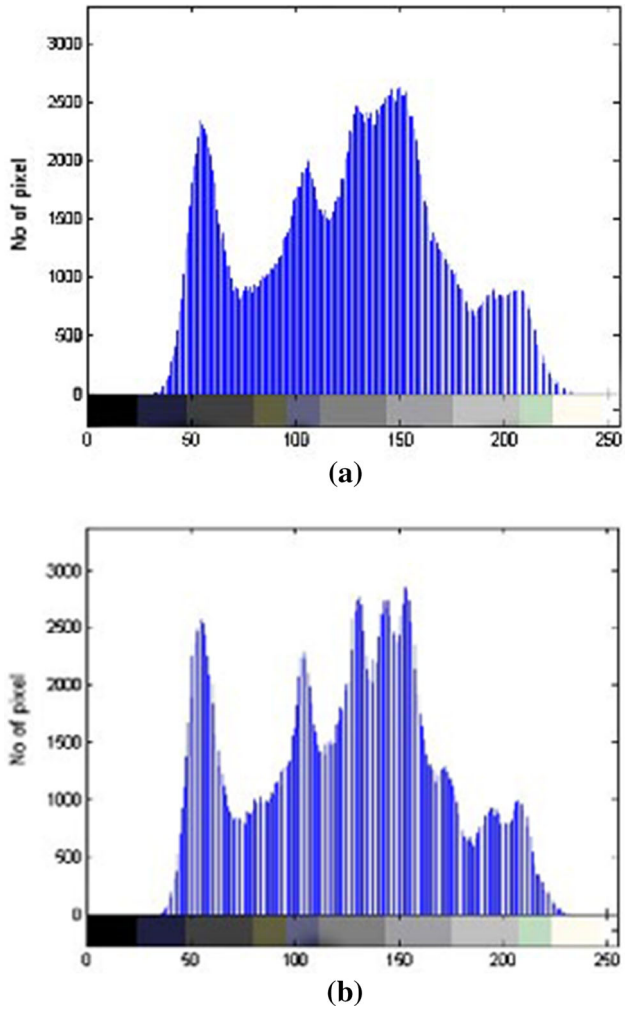

Fig. 6 Histogram of ***a*** Original image ***b*** Watermarked image

Table 3 BER value under JPEG compression with different quality factor

Quality factor for JPEG compression	Lena BER	Girl BER	Tank BER
(Q-100)	0.0371	0.0381	0.0357
(Q-80)	0.0290	0.0248	0.0259
(Q-50)	0.0213	0.0161	0.0171

5 Performance under various attacks

5.1 JPEG compression

JPEG is important standard for still image compression, so compressed watermarked image at various levels of quality factors and BER is calculated by subjecting the watermarked image to JPEG compression with quality factor 100,80 and 50 to test robustness of the proposed algorithm shown in Table 3.

Table 4 BER of retrival watermark for a low pass filtring with different gaussian variance (σ)

Variance (σ)	Lena BER	Girl BER	Tank BER
0.0004	0.0175	0.0171	0.0199
0.0006	0.0213	0.0196	0.0213
0.0008	0.0231	0.0241	0.0234
0.001	0.0271	0.0294	0.0241
0.002	0.0434	0.0490	0.0545

Table 5 Performance metric with addition of salt pepper noise attack

Noise density	Lena BER	Girl BER	Tank BER
0.002	0.0280	0.0245	0.0266
0.004	0.0392	0.0350	0.0364
0.006	0.0647	0.0612	0.0643
0.01	0.0723	0.0731	0.0720
0.04	0.1850	0.1822	0.1829
0.06	0.2311	0.2252	0.2206
0.1	0.2874	0.2941	0.2822

Table 6 Performance metrics with addition of Gaussian noise attack

Gaussian variance (σ)	Lena BER	Girl BER	Tank BER
0.5	0.0612	0.0556	0.0654
1.0	0.0923	0.0836	0.1049
1.2	0.1133	0.1133	0.1304
1.5	0.1552	0.1811	0.1969
2.0	0.2885	0.3283	0.3290

5.2 Low-pass filtering

Gaussian low-pass filtering used as another kind of attack. The obtained result in Table 4 shown BER is increasing as gaussian variance (σ) increases.

5.3 Addition of noise

Adding salt pepper noise and Gaussian noise to the watermarked image and by varying noise density in case of salt pepper noise and variance in case of Gaussian noise. The obtained results show BER is increasing as noise density increases. In case of Gaussian noise BER is increasing as variance increases. The obtained results are tabulated in Table 5 and 6.

6 Conclusion

This paper proposed a novel digital image watermaking alogrithm based on DCT and spread spectrum. This

algorithm provides statistical security and robustness against various attack. Experimental result demonstrate that the proposed alogrithm is resistant to several image mainpulating operations and JPEG compression attack. In the case of JPEG compression attacks, even low quality compression (Q-50) resulted in BER of 0.0213 for IEEE standard Lena image i.e., more than 97 % of the embedded data recovered without any error. The algorithm induces low distortion in the cover image with a PSNR of more than 37 dB.

Acknowledgments The authors gratefully acknowledge financial support from the Council of Science & Technology, Government of Uttar Pradesh (India) under young scientist scheme.

References

1. Li B, He J, Huang J, She YQ (2011) A survey on image steganography and steganalysis. J Inf Hiding Multimed Signal Process 2(2):142–172
2. Swain G, Lenka SK (2013) Steganography using two sided, three sided, and four sided side match Methods. CSIT 1(2):127–133
3. Singh HV, Singh SP, Mohan A (2008) A new algorithm for enhanced robustness of copyright mark. Int J Electr, Comput, and Syst Eng 2(2):121–126
4. Petitcolas FAP, Anderson RJ, Kuhn MG (1999) Information hiding—a survey. Proc IEEE 87(7):1062–1078
5. Johnson N, Jajodia S (1998) Exploring stenography: seeing the unseen. IEEE Comput 58(8):26–34
6. Bruyndockx J, Quisquater J, Macq B (1995) Spatial method for copyright labeling, IEEE Workshop on Image Processing, pp. 456–459
7. Wolfgang RB, Delp EJ (1997) A watermarking technique for digital imagery: further studies, International Conference on Imaging Science, pp. 279–287
8. Westfeld A, Pfitzmann A Attacks on steganographic systems,Lecture Notes in Computer Science, pp. 61–75, vol. 1768, Springer–Verlag, 2000.
9. Schyndel VRG, Tirkel AZ, Osborne CF (1994) A digital watermark, IEEE International Conference on Image Processing, pp. 86–89
10. Hsieh MS, Tseng DC, Huang YH (2001) Hiding digital watermarks using multiresolution wavelet transform. IEEE Trans Industr Electron 48(5):875–882
11. Koch E, Zhao J Toward robust and hidden image copyright labeling, Proceedings Workshop Nonlinear Signal and Image Processing, Marmaros, Greece, June 1995
12. Podilchuk C, Zeng W Watermarking of the JPEG bitstream, in Proceedings of International Conference on Imaging Science, Systems,and Applications (CISST'97), pp. 253–260, Las Vegas, June 1997.
13. Guan YL, Jin J An objective comparison between spatial and DCT watermarking schemes for MPEG video, Proceedings International Conference on Information Technology: Coding and Computing, pp.207–211, 2001.
14. Podilchuk CI Digital image watermarking using visual models, Proceedings of Electronic Imaging, vol. 3016, San Jose, CA, 1996.
15. Podilchuk CI, Zeng W Perceptual watermarking of still images, Proceedings of Workshop Multimedia Signal Processing, Princeton, NJ, June 1997.
16. Wang H, Wang S (2004) Cyber warfare: steganography versus steganalysis. Commun ACM 47:76–82
17. Amin PK, Liu N, Subbalakshmi KP Statistical Secure Digital Image Data Hiding. IEEE 7th workshop on Multimedia Signal Processing. pp.1–4, 2005.
18. Yu-jin Zhang (1998) Image processing and analysis. Tsinghua-University Press, Beijing
19. Strang G (1999) The discrete cosine transform. SIAM Review 41(1):135–147
20. Mac William FJ, Sloane NJA Pseudorandom Sequences and Arrays, Proc. of the IEEE, Vol. 64, No. 12, pp 1715–1729, Dec 1976.