WT-DCT domain based image watermarking technique using SVM

Mohiul Islam, Department of ECE, CMR College of Engineering and Technology, Hyderabad, India.
G. Rajesh Kumar, Department of ECE, CMR College of Engineering and Technology, Hyderabad, India.
Abdul Subhani Shaik, Department of ECE, CMR College of Engineering and Technology, Hyderabad, India.
Rabul Hussain Laskar, Department of ECE, NIT Silchar, Silchar, Cachar, Assam, India.

Article Info
Volume 82
Page Number: 3195 - 3200
Publication Issue:
January-February 2020

Article History

Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *19 January 2020*

Abstract

Digital watermarking technique can be utilized for the protection of digital images from unauthorized use and distribution. In this paper a robust image watermarking technique has been developed based on the combination of discrete wavelet transform (DWT) and discrete cosine transform (DCT). To achieve the improved robustness under various attack conditions, support vector machine (SVM) has been incorporated during watermark extraction. The 3-level DWT transformed DCT coefficients are modified to insert a particular binary watermark bit in the host image. The watermarking system provides an average imperceptibility of around 42.45 dB over 300 images. The algorithm also offers improved robustness against different types attacks including both geometrical and non-geometrical attacks. The imperceptibility has been observed in terms of peak signal to noise ration (PSNR) while robustness is carried out using normalized cross-correlation (NC) and bit error rate (BER). Experimental observation suggests that the developed technique may be suitable for the copyright protection applications of digital images.

Keywords: *Disctete Wavelet Transform (DWT), Discrete Cosine Transform (DCT), Image Watermarking, Support Vector Machine (SVM)*

I. INTRODUCTION

Watermarking in wavelet domain has drawn significant attention due to its multiresolution attributes. Digital image watermarking is an effective solution for authentication and copyright protection of images in popular communication environments like the Internet, which is vulnerable to illegal usages. The basic principle of image watermarking is to hide some data that provides ownership or copyright information as a watermark into a cover image as host. Based on embedding domain, watermarking techniques are classified as spatial domain technique and transform domain technique. It has been observed from the literature that though the spatial domain techniques [1-2] are simple and easy to implement, but it provides less robustness as compared to transform domain techniques.

The DWT is a well-known transform for image processing because of its multi-resolution properties in time and frequency. The DCT gives very good energy compaction for highly correlated image data. The combination of both DWT and DCT for watermarking generally exhibits good performance in regards of both the invisibility and robustness. While the LWT has both the energy compaction property as well as multi-resolution attributes. However, apart from these transformation techniques, SVD is another potential numeric tool that can be useful for applications like data hiding and image compression. Over the past few years, several transform domain techniques [3-7] based on DWT, LWT, DCT, DFT etc. have been proposed. These techniques employ signal characteristics and human perception property so as to obtain better performance in contrast to spatial domain techniques. Different decomposition techniques like SVD, QR decomposition also have been integrated with transformation techniques to achieve enhanced performance [8-18].

In this paper, a watermarking techniques in transform domain based on the combination of DWT and DCT is developed. Several watermarking techniques have been developed in which the watermark extraction has been performed using statistical algorithmic based approach. In this approach, the binary watermark bit is detected based on finding some correlation between coefficients. However, it is seen that the statistical watermark extractor provides poor robustness performance under different attack condition. This approach of watermark extraction is not sufficiently robust to different common image processing operations like JPEG attack, noising attack and de-noising attacks as well as geometric attacks. So, for achieving improved robustness against different non-geometric and geometric attacks, machine learning based watermark extraction technique has been developed. In the proposed approaches, SVM have been integrated with the proposed algorithm in wavelet domain so as to maintain the imperceptibility and robustness.

Rest of the paper is organized in the following manner. Section II describes the process of watermark embedding and extraction technique. Experimental results and analysis have been presented in Section III. Section IV concludes the watermarking technique.

II. WATERMARK EMBEDDING AND EXTRACTION PROCESS

Watermarking has been performed in the joint DWT-DCT domain. From the existing literatures, it has been observed that the use of machine learning tool as a watermark extractor helps to achieve improved robustness against diverse attack conditions. So, in the proposed DWT-DCT based algorithm, SVM based watermark extraction technique has been integrated during extraction. The process of embedding and extraction is discussed in detail below.

A. Watermark Embedding

The watermark embedding is carried out in DWT-DCT domain as performed in [19]. For embedding purpose, 4 sub-bands have been used similar to the previous method. However, PN sequences i.e. PN0 and PN1 are kept fixed in this case as PN0= [0 0 0 0] and PN1= [1 1 1 1]. The gain factor β is adjusted so as to achieve better balance between the imperceptibility and robustness. In this method, the watermark (1024 bits) is divided into two parts i.e. reference watermark (RW) (512 bits) and signature watermark (SW) (512 bits). The SW is encrypted by performing 'XOR' operation with 'key 1' i.e. RW. The RW and SW have been concatenated and represented as a single unit as shown in equation (1). The generation of W from RW and SW is presented in Figure 1. Two 3-level sub-bands from HL band (1-level) are utilized to embed the RW bits while the other two sub-bands from LH band are utilized to embed the SW bits.

$$W = RW + SW = w_1,.....,w_{L_r};w_{L_r+1},.....,w_{L_r+L_s} = w_1,.....,w_{L_w} \quad (1)$$

The L_W, L_R, L_S are the length of W, RW and SW respectively.

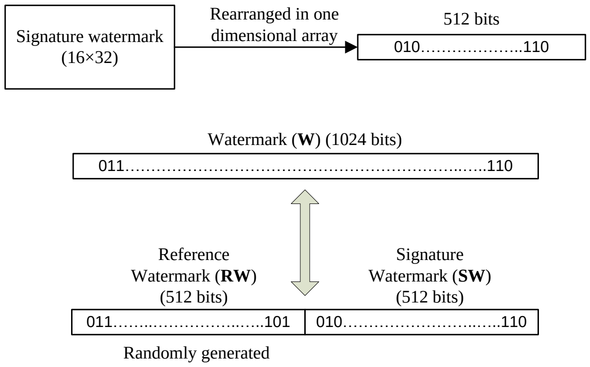
Signature watermark (16×32)
Rearranged in one dimensional array
512 bits
010……………….110
Watermark (W) (1024 bits)
011……………………………………………….110
Reference Watermark (RW) (512 bits)
Signature Watermark (SW) (512 bits)
011………………………101
010…………………………110
Randomly generated

Figure 1 Formation of Watermark (W)

B. Watermark Extraction

In contrast to previous methods in which the binary watermark bit is detected based on finding some correlation between coefficients and PN sequence, some statistical features are calculated from the 4×4 DCT blocks to train an SVM model. The trained SVM model is used to classify embedded watermark bits. The features that are used for training the model are calculated from all the blocks in which RW has been embedded. Whereas, the testing patterns are generated from the blocks in which SW has been embedded. Firstly, the DWT transformed DCT coefficient blocks (4×4) in which RW was embedded are extracted. Then various statistical parameters such as: Entropy (p1), Mean (p2), Variance (p3), Covariance (p4), Standard deviation (p5), Median (p6), Mode (p7), Moment (5th order) (p8), Quantiles (p9) of all the corresponding blocks are evaluated. The set of parameters (p1; p2; . . . ; p9) is called as features vector and represented as (f_1; . . . ; f_9) i.e. feature vector set. The feature vector set is given as input feature to train the SVM machine. The 4 sub-bands have a total of 1024 number of 4×4 blocks. These 1024 blocks are divided into two parts, in which first 512 blocks have been used for generating the training pattern, while the rest of the blocks are utilized for preparing the testing pattern. The testing pattern provides the SW i.e. signature watermark. So, the size of feature vector set {p(k)} is (512×9). The detailed process of watermark extraction has been discussed below:

- **Step 1:** The 3-level DWT is performed on the watermarked image and the 4 sub bands which were used in embedding have been selected.
- **Step 2:** The coefficients are arranged in 4×4 blocks and DCT have been performed on every block. There is a total of 1024 number of 4×4 DCT blocks in which first 512 blocks have been used for embedding RW are utilized for training the SVM model.
- **Step 3:** The features set is generated from the blocks in which RW bits are embedded.
- **Step 4:** A training pattern ψ is created using the feature sets along with the coefficients of corresponding blocks in which the reference watermark (RW) is embedded. The RW bits can be represented as $w_i = \left(w_1, w_2, \ldots\ldots, w_{L_r}\right)$.

$$\begin{aligned}\psi &= \left\{(\mathbf{x_i}, y_i) \in R^N \times R \middle| i = 1, 2, \ldots., L_r\right\}\\ &= \left\{f_i(1), f_i(2), \ldots. f_i(9), w_i \middle| i = 1, 2, \ldots., L_r\right\}\end{aligned} \quad (2)$$

Where, $f_i(1), f_i(2), \ldots. f_i(9)$ are the features and w_i is the desired output, $i = 1, 2, \ldots., L_r$.

The 'RBF' kernel function of SVMs can be described as follows:

$$K(\mathbf{x_i}, \mathbf{x}) = e^{(-\|\mathbf{x_i} - \mathbf{x}\|^2 / \sigma^2)}$$
(3)

Here, σ is the width parameter of 'RBF' kernel, $\mathbf{x}$ is the input vector, $\mathbf{x_i}$ is the image of a support vector in input space and $\|\cdot\|^2$ stands for L$_2$ norm.

The optimum model can be defined by maximizing

$$\sum_{i=1}^{L_r} \alpha_i - \frac{1}{2} \sum_{i=1}^{L_r} \sum_{j=1}^{L_r} \alpha_i \alpha_j y_i y_j K\left(\mathbf{x_i}, \mathbf{x_j}\right) \quad (4)$$

subject to

$$\sum_{i=1}^{L_r} \alpha_i \alpha_j = 0, \qquad 0 \le \alpha_i \le C, \;\; i = 1, 2, \ldots, L_r$$

where C is the penalty parameter, and $\alpha_i \left(i = 1, 2, \ldots., L_r\right)$ are the training parameter. The $\mathbf{x_i}$ and $\mathbf{x_j}$ are the support vectors in input space. If the optimal solution is $\alpha = \left(\alpha_1, \alpha_2, \ldots\ldots, \alpha_{L_r}\right)$ and $b \in R$ is a bias, then decision function y can be expressed as

$$y = f(x) = sign\left(\sum_{i=1}^{L_r} \alpha_i y_i K(\mathbf{x}, \mathbf{x_i}) + b\right) \quad (5)$$

- **Step 5:** For extraction of signature watermark, the testing pattern ψ' is constructed for the well-trained SVM. $\psi' = \{x'_u = (f_u{}'(1), f_u{}'(2), \ldots. f_u{}'(9)\}$. Then, by use of well-trained SVM in Equation (6), the corresponding outputs $\left\{y'_u \middle| u = 1, \ldots\ldots, L_s\right\}$ can be detected.

$$\begin{cases} y'_u = f(x'_u), \; u = 1, \ldots\ldots, L_s \\ x'_u = (f_u{}'(1), f_u{}'(2), \ldots. f_u{}'(9)) \in \psi' \end{cases} \quad (6)$$

Thus, the signature watermark bits (w'_u) can be obtained by

$$w'_u = \begin{cases} 1, & \text{if } y'_u = 1 \\ 0, & \text{if } y'_u = -1 \end{cases}$$
(7)

The trained SVM classifier provides the encrypted signature watermark.

- **Step 6:** The detected signature watermark bits (w'_u) has been arranged in a one dimensional vector of 512 bits, which is decrypted using the seed key (key 1) similar to embedding process.

Step 7: The extracted signature watermark (SW') is finally reshaped same as the size of original logo watermark.

The authors of the accepted manuscripts will be given a copyright form and the form should accompany your final submission.

III. Experimental Results

The DWT-DCT-SVM based watermarking technique is tested on 300 gray images of size (512×512). Different classes of images such as standard images, satellite images, medical images, texture images etc. have been considered in this analysis. These images are collected from different sources such as USC-SIPI image database, CVG-UGR image database and from www.imageprocessingplace.com website. The binary watermarks are collected from the MPEG7_CE_shape descriptor database. For the sake of briefness, the original Lena image (512×512), watermarked Lena image along with original watermark and extracted watermark under no attack condition is shown in the Figure 2. Imperceptibility is measured in terms of peak signal to noise ratio (PSNR) between the original cover image and watermarked image. Robustness is measured in terms of normalized cross correlation (NC) and bit error rate (BER) between original watermark and extracted watermark.

A. Imperceptibility Analysis

The imperceptibility of the algorithm is tested on various image database. It has been observed experimentally that β (gain factor) balances the two performance parameter i.e. imperceptibility and robustness. For lower value of β, imperceptibility increases but robustness decreases, and vice-versa. It has been found that β =30 gives better balance between imperceptibility and robustness. So, for this value of β, all experiments have been performed. Figure 3 shows the PSNR for 10 different standard images. It is seen from the Figure 3 that the technique provides adequate imperceptibility for various images. The performance has been evaluated on 300 images and the average PSNR is found to be 42.45 dB.

B. Robustness Analysis

Robustness of the proposed scheme has been observed against various attacks. The attacks include noising attacks, denoising attacks, image processing attacks and lossy compression attacks. The different attacks are speckle noise (SN), salt and pepper noise (SPN), Gaussian noise (GN), joint photographic experts group (JPEG) with different quality factor, average filtering (AF), Gaussian filtering (GF), histogram equalization (HE), image sharpening (IS), Gamma Correction (GC), and cropping (CR) attacks. The robustness has been observed on different types of images. The representative results are shown for 10 different standard images in Table 1-2. From the experimental results, it has been observed that the technique provides satisfactory performance against image processing attacks and JPEG attack in case of higher values of quality factor. The technique provides moderate performance against noising attacks, de-noising attacks and JPEG attack in case of low quality factor.

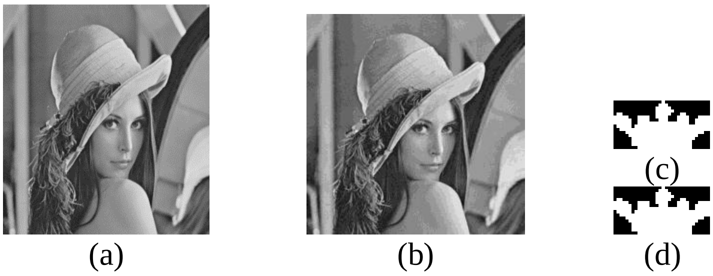

Figure 2 (a) Original image ‘‘Lena’’ of size (512×512), (b) Watermarked image with PSNR = 42.98 dB, (c) Original signature watermark (16×32), and (d) extracted watermark

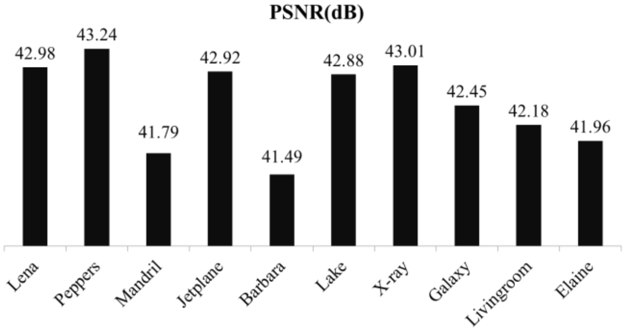

Figure 3 The imperceptibility for different images

Table 1. NC values of extracted watermark for different attacks over 10 images

Images	JPEG 20	JPEG 30	JPEG 40	JPEG 50	AF (3×3)	GF (3×3)	SPN (0.01)
Lena	0.6156	0.7629	0.8904	0.9652	0.6688	0.9821	0.8531
Peppers	0.6562	0.8011	0.8864	0.9741	0.7855	0.9608	0.7887
Mandril	0.5429	0.7954	0.8448	0.9325	0.8847	0.9842	0.8140
Jetplane	0.6115	0.7481	0.8697	0.9429	0.7814	0.9451	0.7495
Barbara	0.6342	0.7632	0.8249	0.9098	0.6934	0.9498	0.7956
Lake	0.6871	0.7751	0.8571	0.9252	0.7591	0.9142	0.8059
X-ray	0.5123	0.7329	0.8041	0.8956	0.8019	0.9363	0.8054
Galaxy	0.5898	0.7592	0.8693	0.9420	0.8115	0.9183	0.8129
Livingroom	0.5775	0.6995	0.8176	0.9145	0.7840	0.9805	0.7495
Elaine	0.6254	0.7142	0.8655	0.9081	0.7955	0.9921	0.7614

Table 2. NC values of extracted watermark for different attacks over 10 images.

Images	SN (0.01)	HE	IS	GC	CR (10%)	CR (25%)	CR (50%)
Lena	0.8459	0.8765	0.9882	0.9114	0.8445	0.7797	0.5428
Peppers	0.7913	0.8882	0.9611	0.9696	0.8647	0.6823	0.5843
Mandril	0.8352	0.8156	0.9378	0.9477	0.8198	0.6909	0.4902
Jetplane	0.7387	0.8715	0.8499	0.9423	0.8272	0.7079	0.4678
Barbara	0.7893	0.8447	0.9404	0.9245	0.8434	0.6781	0.4798
Lake	0.8135	0.8451	0.9142	0.9745	0.8401	0.7059	0.5163
X-ray	0.8218	0.8447	0.9751	0.9649	0.8266	0.7014	0.5921
Galaxy	0.7948	0.8611	0.9489	0.9189	0.8794	0.6732	0.6032
Livingroom	0.7684	0.8719	0.9674	0.9055	0.8907	0.6869	0.5784
Elaine	0.7793	0.8379	0.9348	0.9478	0.8345	0.7387	0.4842

IV. CONCLUSION

In this work, a robust invisible image watermarking technique has been developed in DWT-DCT domain. By integrating SVM during extraction process, the scheme achieves improved against different attacks like lossy compression attacks, noising attacks, de-noising attacks and image processing attacks. The robustness has been obtained maintaining adequate level of imperceptibility. However, the main drawback with this technique is that it is unable to sustain geometric attacks.

ACKNOWLEDGMENT

The authors would like to acknowledge the Department of Electronics and Communication Engineering, CMR College of Engineering and Technology Hyderabad for providing support and necessary facilities for carrying out this work.

REFERENCES

[1] R. Z. Wang, C. F. Lin, and J. C. Lin, “Image hiding by optimal LSB substitution and genetic algorithm,” *Pattern Recognition*, vol. 34, no. 3, pp. 671–683, 2001.

[2] D. P. Mukherjee, S. Maitra, and S. T. Acton, “Spatial domain digital watermarking of multimedia objects for buyer authentication,” *IEEE Transactions on Multimedia*, vol. 6, no. 1, pp. 1–15, 2004.

[3] C. C. Lai and C. C. Tsai, “Digital image watermarking using discrete wavelet transform and singular value decomposition,” *IEEE Transactions on Instrumentation and*

Measurement, vol. 59, no. 11, pp. 3060–3063, 2010.

[4] R. Mehta, N. Rajpal, and V. P. Vishwakarma, “A robust and efficient image watermarking scheme based on Lagrangian SVR and lifting wavelet transform,” *International Journal of Machine Learning and Cybernetics*, vol. 8, no. 2, pp. 379–395, 2017.

[5] V. S. Verma, R. K. Jha, and A. Ojha, “Digital watermark extraction using support vector machine with principal component analysis based feature reduction,” *Journal of Visual Communication and Image Representation*, vol. 31, pp. 75–85, 2015.

[6] V. S. Verma, R. K. Jha, and A. Ojha, “Significant region based robust watermarking scheme in lifting wavelet transform domain,” *Expert Systems with Applications*, vol. 42, no. 21, pp. 8184–8197, 2015.

[7] G. Kasana and S. S. Kasana, “Reference based semi blind image watermarking scheme in wavelet domain,” *Optik*, vol. 142, pp. 191–204, 2017.

[8] M. Islam, A. Roy, and R. H. Laskar, “Neural network based robust image watermarking technique in LWT domain,” *Journal of Intelligent and Fuzzy Systems*, vol. 34 no. 3, 1691-1700, 2018.

[9] H. T. Hu and L. Y. Hsu, “Collective blind image watermarking in DWT-DCT domain with adaptive embedding strength governed by quality metrics,” *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6575-659, 2017.

[10] M. Islam, A. Roy, and R. H. Laskar, “SVM-based robust image watermarking technique in LWT domain using different sub-bands,” *Neural Computing and Applications*, DOI: 10.1007/s00521-018-3647-2, 2018.

[11] F. N. Thakkar, V. K. Srivastava, “A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications,” *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3669-3697, 2017.

[12] N. M. Makbol and B. E. Khoo, “Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition,” *AEU-International Journal of Electronics and Communication*, vol. 67, no. 2, pp. 102-112, 2013.

[13] M. Islam and R. H. Laskar, “Robust image watermarking technique using support vector regression for blind geometric distortion correction in lifting wavelet transform and singular value decomposition domain,” *Journal of Electronic Imaging*, vol. 27, no.5, pp. 053008, 2018.

[14] A. Mishra, C. Agarwal, A. Sharma, P. Bedi, “ Optimized gray-scale image watermarking using DWT–SVD and Firefly Algorithm,” *Expert Systems with Applications*, vol. 41, no. 17, pp. 7858-7867, 2014.

[15] N. M. Makbol and B. E. Khoo, “A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition,” *Digital Signal Processing*, vol. 33, pp. 134–147, 2014.

[16] R. Mehta, N. Rajpal, and V. P. Vishwakarma, “ LWT-QR decomposition based robust and efficient image watermarking scheme using Lagrangian SVR,” *Multimedia Tools and Applications*, vol. 75, no. 7, pp.4129-4150, 2016.

[17] D. Singh and S. K. Singh, “DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection,” *Multimedia Tools and Applications*, vol. 76, no. 11, pp. 13001–13024, 2017.

[18] M. Islam, G. Mallikharjunudu, A. S. Parmar, A. Kumar, and R. H. Laskar, “SVM regression based robust image watermarking technique in joint DWT-DCT domain”, in *IEEE, 2017 International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* pp. 1406-1413, 2017.

[19] R. H. Laskar, M. Choudhury, K. Chakraborty, & S. Chakraborty, "A Joint DWT-DCT Based Robust Digital Watermarking Algorithm for Ownership verification of Digital Images."*In Computer Networks and Intelligent Computing* (pp. 482-491), Springer Berlin Heidelberg, 2011.