Robust Digital Image Watermarking Scheme in Discrete Wavelet Transform domain using Support Vector Machines

B.Jagadeesh
Associate Professor
E.C.E. Department
G.V.P. College of Engg.
Visakhapatnam, A.P., India.

P.Rajesh Kumar
Associate Professor
E.C.E. Department
Andhra University
Visakhapatnam, A.P., India.

P.Chenna Reddy
Professor
C.S.E. Department
JNTUA College of Engg.
Pulivendula, Kadapa, India

ABSTRACT

This paper presents a robust and blind watermarking scheme for copyright protection of images in discrete wavelet transform domain based on the support vector machines (SVMs). This scheme is based on the relation between the coefficients in various sub bands in discrete wavelet transform decomposition. The proposed scheme is very secured and robust to various attacks, viz., Low pass Filtering, Salt & Pepper noise, Gamma Correction, JPEG Compression, Row-Column Copying, Row-column blanking, Bit plane removal, Cropping, Resize and Histogram Equalization etc. Experimental results show that the proposed scheme has significant improvements in both robustness and imperceptibility and superior to an algorithm proposed by Li et al. in terms of Normalized Cross correlation (NC) and Peak Signal to Noise Ratio (PSNR).

KEYWORDS

Digital Image Watermarking, Discrete Wavelet Transform, Support Vector Machines.

1. INTRODUCTION

Digital Image watermarking is one of the proposed solutions for copyright protection of digital images. The process of embedding a watermark i.e. (Image or pseudo random sequence) in a multimedia object is termed as watermarking [1]. This watermark is embedded through invisible means in host image so that it can be extracted as the evidence of rightful ownership, when required. Once the watermark is embedded several image processing attacks may be experienced because the multimedia object can be digitally processed. In order to enhance the precision, robustness and security of watermark, many scholars have researched artificial intelligence and machine learning methods. Support Vector Machines (SVMs) are a set of supervised learning methods proposed by Vapnik et al. in the mid of 1990s, which is based on statistical learning theory and the Vapnik-Chervonenkis (VC) dimension [2]. Image watermarking algorithms which are based on the machine learning theory [3-7] are available in the literature.

Fu et al. [8] proposed an SVM-based watermarking method in which the difference of the intensity level of pixels of blue components was used to train the SVM. Tsaia et al. [9] presented a robust lossless watermarking algorithm based on α-trimmed mean algorithm and support vector machines (SVMs), in which the SVM is trained to memorize the relationship between the watermark and image-dependent watermark other than inserting watermark into the host image. Li et al. [10] introduced a semi-fragile watermarking algorithm based on SVM's. This algorithm first gives the definition of wavelet coefficient direction tree, then a relation mathematical model between root node and its offspring nodes is established using SVM and further watermark is embedded and extracted based on this structuring data using relation (relational model). Hong et al. [11] proposed a novel image watermarking method in multiwavelet domain based on support vector machines (SVMs), in which the special frequency band and property of image in multiwavelet domain are employed for the watermarking algorithm.

In this paper, a modified watermarking method using discrete wavelet transform and support vector machines for embedding and extracting the watermark based on an algorithm proposed by Li et al. [10] is presented. This scheme is based on the relation between the root coefficients and offspring coefficients in discrete wavelet transform decomposition and the corresponding sub bands.

This paper is organized as follows: In section 2 Preliminaries about Discrete Wavelet Transform and Support Vector Machine are described. Section 3 explains the proposed watermarking method. Experimental results are shown in section 4. The conclusions are specified in section 5.

2. PRELIMINARIES

2.1 Discrete Wavelet Transform

The transformation of an image from the spatial domain to the frequency domain by passing it through a series of low-pass filters and high-pass filters is done by a two-dimensional DWT. The outputs of such filters correspond to multi-resolution sub-bands each possessing unique characteristics making it suitable for specific digital image processing applications. The decomposition of each level produces four bands of data denoted by LL, HL, LH, and HH. To obtain another level of decomposition LL subband can further be decomposed. This process is continued until the preferred number of levels determined by the application is reached.

The wavelet coefficients across different decomposition levels are correlated based on the spatial-frequency characteristics of wavelet transformation. This can be described as parent-children relationship as shown in Figure 1. For example, here one coefficient from HL_3, 4 coefficients from HL_2, and 16 coefficients from HL_1 correspond to the same spatial location, so they are closely correlated.

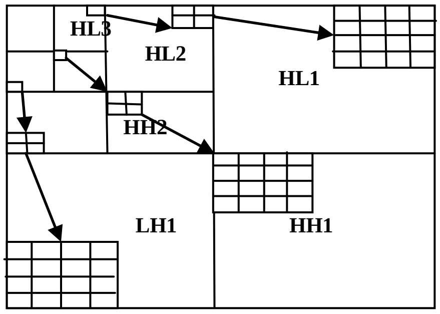


Figure 1. Demonstration of root node and offspring nodes

A direction tree is a set of coefficients from the same orientation but different decomposition levels corresponding to the same spatial location, denoted as Dij. Therefore, for an image of size $M/2^m$ x $N/2^m$ there are a total of M X N direction trees, each direction tree can be used to hide at least one bit watermark. So, in the same direction tree, there exists a very close relation among coefficients and any modifications made on the image will affect this relation.

2.2 Support Vector Machines (SVMs)

The support vector machines (SVMs) is a machine learning tool or a universal classification algorithm used for performing classification and detection tasks. SVM has been successfully applied to pattern recognition problems and numerous classifications such as image recognition, text categorization and bioinformatics. The classifier based on SVM is used to minimize the structural misclassification risk, whereas the classification based on conventional techniques often produce minimization of the empirical risk, for that reason, SVM is claimed to lead improved generalization properties. Further, for a classification problem appliance of SVM outcome in the worldwide solution. As the efficiency do not directly depends on the dimension of the classified entities, SVM-based classification is more attractive. The number of error classification features do not have to be radically limited, so this property is very useful in fault diagnostics.

In SVM algorithm two sets of vectors are considered, one is of real numbers and the other is output vector consisting of positive and negative examples. In order to minimize the number of errors, a machine to learn the mapping from input to output is to be constructed. Hyper plane is the separating plane between positive and negative examples.

A classification task usually involves with training and testing data consisting of some data instances, where each instance in the training set contains one “target value (class labels)” and several “attributes (features)”. The final goal of SVM is to produce a model by predicting a target value of data instances in the testing set which are given only the attributes.

In general SVM’s are used to learn the mapping between training set and positive and negative values. To learn the mapping: X €Y where x€X is some object and y€Y is a class label. Let’s take the simplest case 2-class classification, so: x€R ,y€{+ or(-)1}.A classifier function is defined as y=f(x,α),where α are the parameters of the function .in other words it can be written as f(x,{w,b})=sign(w.x+b).where w and b are some constants used to determine the test errors.

Training and Test errors: Training error is also called as empirical risk .which is given by the equation.

$$R_{emp}(\alpha) = \frac{1}{m}\sum_{i=1}^{m} l(f(xi,\alpha), yi) = \text{Training Error}$$

Test error ≤ Training error+ complexity of set of models. Complexity gives an idea about the number of training sets involved in the mapping. To reduce the test error the complexity or the capacity function should be minimized.

The general form of the classifier function is f(xi,α) = W.xi+b and is shown in Figure 2.

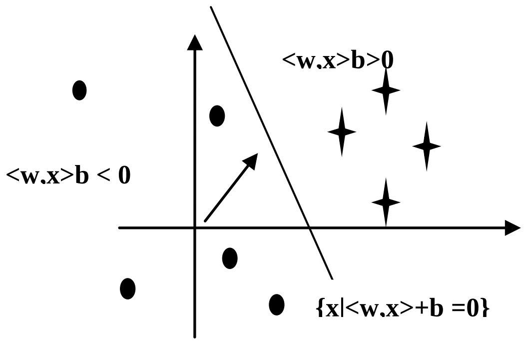


Figure 2. SVM Classifier

Requirements of SVM:

Support Vector Machine is used to the extracted image in order to enhance the quality of the image. It supports the requirements of the watermarking image like

Imperceptibility: If we apply SVM to the detected watermarks, the obtained image, after applying SVM is same as watermark image.

Efficiency: SVM supports the Efficiency by selecting the appropriate pixels during the predictions. The efficiency of the SVM increases with the increase of the database providing for the machine learning.

3. THE PROPOSED METHOD

3.1 WATERMARK EMBEDDING

The procedure for embedding the watermark is as follows:

1. The host image of size 512x512 pixels and the watermark image of size 64x64 pixels.
2. Scramble the original watermark image W_{ij} according to the secret key K_1.
3. Perform 2-level 2D DWT on host image.
4. Randomly generate 64x64 coefficients from the sub bands in host image called root coefficients R_{ij}.
5. Construct the corresponding direction tree coefficients called offspring coefficients Dij.

6. Generate the output coefficients X_{ij} using SVM (training, testing and prediction) with inputs as offspring coefficients D_{ij}.
7. The embedding operation is done as

R_{ij}=max (R_{ij}, $X_{ij}+\beta$), if W_{ij}=1
=min (R_{ij}, $X_{ij}- \beta$), otherwise

8. Inverse DWT is applied to reconstruct the watermarked image.

3.2 WATERMARK EXTRACTION

The watermark extraction process from a watermarked image is as follows:
1. Perform 2-level 2D-DWT on watermarked image.
2. Randomly generate 64x64 coefficients from the sub bands in watermarked image called root coefficients Rij.
3. Construct the corresponding direction tree coefficients called offspring coefficients D_{ij}'.
4. Generate the output coefficients X_{ij}' using SVM (training, testing and prediction) with inputs as offspring coefficients D_{ij}'.
5. After calculating the output of SVM X_{ij}', scrambled watermark W_{ij}' can be obtained as

W_{ij}'=1, if $R_{ij}' > X_{ij}'$
=0, otherwise

6. Original watermark can be obtained after descrambling according to the secret key K_1.

The performance metrics used to test the proposed algorithm are Peak Signal to Noise Ratio (PSNR) and Normalized Cross correlation (NC). Let the host image of size NxN is $f(i,j)$ and the watermarked counterpart is $F(i,j)$, then PSNR in dB is given by

$$\text{PSNR}=10\log_{10}\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(F(i,j))^2}{\sum_{i=1}^{N}\sum_{j=1}^{N}(f(i,j)-F(i,j))^2}\right) \quad [1]$$

Let the watermark image is denoted by $w(i,j)$ and the extracted watermark is denoted by $w'(i,j)$ then NC is defined as

$$\text{NC}=\left(\frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{mean})(w'(i,j)-w'_{mean})}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(w(i,j)-w_{mean})^2\sum_{i=1}^{N}\sum_{j=1}^{N}(w'(i,j)-w'_{mean})^2}}\right) \quad [2]$$

In Eq.(2), w_{mean} and w'_{mean} indicate the mean of the original watermark image and extracted watermark image respectively.

4. EXPERIMENTAL RESULTS AND DISCUSSION

Experiments are performed to evaluate the effectiveness of the method using host grey-scale images 'LENA', 'GOLDHILL' and 'PEPPERS' shown in Figure 3.

(a)

(b)

(c)

Figure.3. 512x512 (a) Lena, (b) Goldhill and (c) Peppers (Host Images)

The sizes of the host images are 512 x 512. The watermark image is 64 x 64, a logo having the letters 'JNTUACEA' as shown in Figure 4.

Figure.4. Watermark Image

In Figure 5 watermarked LENA, GOLDHILL and PEPPERS are shown.

(a)

(b)

(c)

Figure. 5. 512x512 Watermarked (a) Lena (45.15dB), (b) Goldhill (42.39dB) and (c) Peppers (44.59dB)

The various attacks that are used to test the robustness of the watermark are Low pass Filtering, Salt & Pepper noise, Gamma Correction, JPEG Compression, Row-Column Copying , Row-column blanking, Bit plane removal, Cropping, Resize and Histogram Equalization. All the attacks were tested using MATLAB 7.14.0.

For a Low pass Filtering attack a 3x3 mask that consists of 0.9 intensity values are used. The recovered watermark image and NC values are shown in Table.4 that shows its resilience to low pass filtering attack. The watermarked image is also attacked by salt & pepper noise with a noise density of 0.001. The watermarked image is compressed with the use lossy JPEG compression. The index specified in the JPEG compression ranges from 0 to 100, where 0 is finest compression and 100 is finest quality. In the row-column blanking attack, a few set of rows and columns are deleted. In row-column copy attack, a set of rows and columns are copied to the adjacent or random locations. In this attack 10^{th} row values is copied to 30^{th} row, 40 into 70, 100 into 120 and 140^{th} row is copied into 160^{th} row.

In resizing attack, at first the watermarked image is reduced from 512x512 size to 400x400. By using the bicubic interpolation the dimensions are increased to 512x512. Finally, the proposed algorithm also is resistant to cropping, biplane removal, and gamma correction and histogram equalization attacks, as shown in Table 4.

The Peak Signal to Noise Ratio (PSNR) and the Normalized Cross correlation (NC) are used as a metric to compare the imperceptibility and robustness respectively are summarized in Table 1, 2 and 3. Extracted watermarks from the watermarked image under various attacks are shown in Table 4.

Table. 1 The PSNR and NC values for Lena with Li et al.'s method and the proposed method

Type of Attack	Li et al.'s method		Proposed method	
	PSNR (dB)	NC Value	PSNR (dB)	NC Value
No attack	45.09	1	45.15	1
Low pass Filtering (3x3 Kernel)	11.37	0.5923	11.38	0.9811
Salt & Pepper Noise(0.001)	34.60	0.4827	34.85	0.9634
Gamma Correction(0.9)	29.01	0.4896	29.02	0.9525
JPEG Compression (QF:100)	44.47	0.4920	44.91	0.9300
Row-Column copying	32.01	0.8931	31.98	0.9028
Row-Column blanking	21.35	0.4293	21.37	0.8025
Bit plane removal	44.33	0.4803	44.38	0.8557
Cropping	8.07	0.3222	8.08	0.6551
Resize(512-400-512)	38.00	0.3339	38.01	0.4561
Histogram Equalization	18.62	0.3499	18.63	0.5611

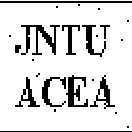
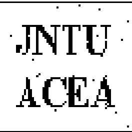
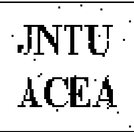
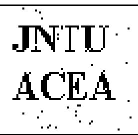
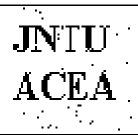
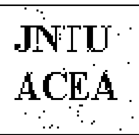
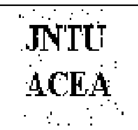
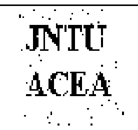
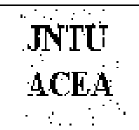
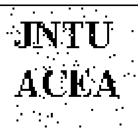
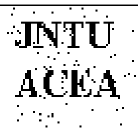
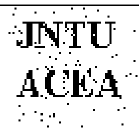
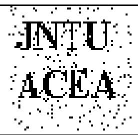
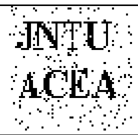
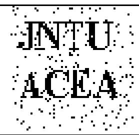
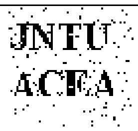
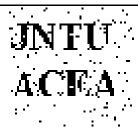
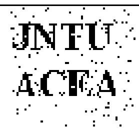
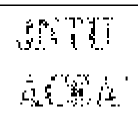
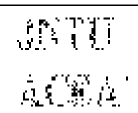
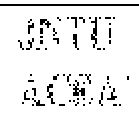
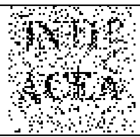
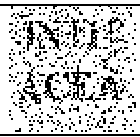
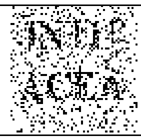
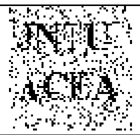
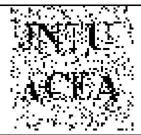
Table. 2 The PSNR and NC values for Goldhill with Li et al.'s method and the proposed method

Type of Attack	Li et al.'s method		Proposed method	
	PSNR (dB)	NC Value	PSNR (dB)	NC Value
No attack	42.29	1	42.39	1
Low pass Filtering (3x3 Kernel)	11.66	0.8183	11.67	0.9397
Salt & Pepper Noise(0.001)	34.10	0.4731	34.13	0.9699
Gamma Correction(0.9)	28.23	0.4912	28.32	0.9746
JPEG Compression (QF:100)	42.23	0.4918	42.25	0.9679
Row-Column copying	34.23	0.9004	34.25	0.9330
Row-Column blanking	19.76	0.4543	19.77	0.8777
Bit plane removal	41.72	0.4619	41.75	0.8827
Cropping	8.33	0.2146	8.36	0.3077
Resize(512-400-512)	34.30	0.3053	34.33	0.4121
Histogram Equalization	16.81	0.3821	16.82	0.6013

Table. 3 The PSNR and NC values for Peppers with Li et al.'s method and the proposed method

Type of Attack	Li et al.'s method		Proposed method	
	PSNR (dB)	NC Value	PSNR (dB)	NC Value
No attack	44.49	1	44.59	1
Low pass Filtering (3x3 Kernel)	11.70	0.9490	11.70	0.9711
Salt & Pepper Noise(0.001)	34.02	0.4861	34.16	0.9634
Gamma Correction(0.9)	28.81	0.4822	28.82	0.9265
JPEG Compression (QF:100)	44.30	0.4832	44.35	0.9304
Row-Column copying	30.64	0.9102	30.62	0.9202
Row-Column blanking	21.04	0.4421	21.04	0.8144
Bit plane removal	43.51	0.4488	43.53	0.8203
Cropping	8.44	0.3223	8.45	0.6547
Resize(512-400-512)	35.23	0.3541	35.26	0.4484
Histogram Equalization	17.65	0.3509	17.67	0.5588

Table. 4 Extracted Watermarks from the watermarked image

Type of attack	Watermarked image Type		
	Lena	Goldhill	Peppers
Low pass Filtering (3x3 Kernel)	 NC: 0.9811	 NC: 0.9397	 NC: 0.9711
Salt & Pepper Noise(0.001)	 NC: 0.9634	 NC: 0.9699	 NC: 0.9634
Gamma Correction(0.9)	 NC: 0.9525	 NC: 0.9746	 NC: 0.9265
JPEG Compression (QF:100)	 NC: 0.9300	 NC: 0.9679	 NC: 0.9304
Row-Column copying	 NC: 0.9028	 NC: 0.9330	 NC: 0.9202
Row-Column blanking	 NC: 0.8025	 NC: 0.8777	 NC: 0.8144
Bit plane removal	 NC: 0.8557	 NC: 0.8827	 NC: 0.8203
Cropping	 NC: 0.6551	 NC: 0.6077	 NC: 0.6547
Resize(512-400-512)	 NC: 0.4561	 NC: 0.4121	 NC: 0.4484
Histogram Equalization	 NC: 0.5611	 NC: 0.6013	 NC: 0.5588

5. CONCLUSIONS

In this paper, a robust and blind Image watermarking scheme using discrete wavelet transform based on the support vector machines have been presented. The quality of the watermarked image is fine in terms of perceptibility and PSNR. The proposed method is shown to be more robust to Low pass Filtering, Salt & Pepper noise, Gamma Correction, JPEG Compression, Row-Column Copying, Row-column blanking, Bit plane removal, Cropping, Resize and Histogram Equalization. The test results are superior to Li et al.'s method in terms of NC values of the extracted watermarks and PSNR of the watermarked image.

6. ACKNOWLEDGEMENTS

Thanks to Dr.L.Venkat, G.V.P. College of Engineering, Visakhapatnam for the valuable discussions related to this work.

7. REFERENCES

[1] Cox, IJ, Miller, ML & Bloom, JA, 2002, "*Digital Watermarking*", Morgan Kaufmann Publisher, San Francisco, CA, USA.

[2] Steve R Gunn, 1998, "*Support vector machines forclassification and regression*", Technical Report, ISIS Department of electronics and computer science, University of Southampton.

[3] Wu. Jianzhen, 2009, "*A RST invariant watermarking scheme utilizing support vector machine and image moments for synchronization*", Fifth International Conference on Information Assurance and Security, China, pp.572–574.

[4] Xiang-Yang Wang, Zi-Han Xu, Hong-Ying Yang, 2009, "*A robust image watermarking algorithm using SVM detection*", Expert Sys. Appl. 36 (5), pp.9056–9064.

[5] H.H. Tsai, D.W. Sun, 2007, "*Color image watermark extraction based on support vector machines*", Inform. Sci. 177 (2), pp.550–569.[6] P.H.H. Then, and Y.C. Wang, 2005, "*Perceiving Digital Watermark Detection as Image Classification Problem using Support Vector Machine*", *Proc. of CITA05*, pp.198-206.

[7] P.H.H. Then, and Y.C. Wang, 2006, "*Support Vector Machine as Digital Watermark Detector*," In Proceedings of SPIE-IS&T Electronic Imaging, SPIE.

[8] Fu, Y., Shen, R., Lu, H., 2004, "*Optimal watermark Detection based on support vector machines*", Proceedings of the International Symposium on Neural Networks, Dalian, China, pp. 552–557.

[9] H.H. Tsaia, H.C. Tsenga, Y.S. Laib, 2010, "Robust *lossless image watermarking based on α-trimmed mean algorithm and support vector machine"*, J. Sys. Software. 83 (6), pp.1015 –1028.

[10] Chun-hua Li, Ling He-fei, Lu Zheng-ding, 2007, "*Semi-fragile watermarking based on SVM for image authentication*", IEEE International Conference on Multimedia and Expo, Beijing, China, pp. 1255–1258.

[11] Hong Peng, Jun Wang, Weixing Wang, 2010, "Image watermarking method in multiwavelet Domain based on support vector machine", J. Sys. Software, 83 (8) pp.1470 –1477.

[12] Colin Campbell, Yiming Ying, 2011, "Learning with Support Vector Machines", Morgan & Claypool Publishers.