

# Digital Image Watermark Extraction in Discrete Wavelet Transform Domain using Support Vector Machines

B.Jagadeesh<sup>1</sup>, P.Rajesh Kumar<sup>2</sup>, and P.Chenna Reddy<sup>3</sup>

<sup>1</sup>Associate Professor, E.C.E.Department, G.V.P. College of Engineering, Visakhapatnam, A.P., India.  
Email: bjagadeesh76@yahoo.com

<sup>2</sup>Professor, E.C.E.Department, Andhra University, Visakhapatnam, A.P., India.

<sup>3</sup>Professor, C.S.E.Department, JNTUA College of Engineering, Pulivendula, Kadapa, A.P., India.  
Email: rajeshauce@gmail.com, pcreddy1@rediffmail.com

**ABSTRACT**--This paper proposes a novel image watermarking method in discrete wavelet transform domain using support vector machines. Reference and watermark images are used to modify the coefficients of the particular even and odd blocks of the wavelet transformed image. Good learning ability of SVMs are used to extract the watermark from the watermarked image even after several different image processing attacks. This algorithm is secure and robust to various attacks, viz., JPEG Compression, Salt and Pepper noise, Row-Column blanking, Row-Column copying, Gamma Correction, Low Pass Filtering, Cropping, Bit Plane Removal, Histogram Equalization and Sharpening, etc. The performance of the method is tested using Normalized Cross Correlation (NCC) and Peak Signal to Noise Ratio (PSNR).

**Keywords**- Digital Image Watermarking, Support Vector Machines, Discrete Wavelet Transform.

## I. INTRODUCTION

In Digital Image watermarking, watermark image is inserted into the host image using an embedding algorithm and a private key. The watermark image can be extracted using an extraction algorithm using the same private key. The watermark is inserted invisibly so that it can be extracted later for the proof of rightful ownership [1-2]. An important property of watermarking is its robustness with respect to image processing attacks. This means that the watermark extracted from images that underwent common image processing operations should be understandable. Watermarking Techniques emerged as cost effective tools for protecting multimedia data from copyright thefts and infringements to maintain protected communications.

Digital Image watermarking schemes are classified into two categories: spatial domain methods and transform domain methods. Typically, the transform domain methods are more robust to resist image processing attacks than spatial domain methods. In order to enhance the robustness and security of watermark, researchers are using artificial intelligence and machine learning methods. Support Vector Machines (SVMs) are a set of controlled 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 [3]. Image watermarking algorithms which are based on the artificial intelligence and machine learning theory [4-9] are available in the literature.

Efforts have been made in the recent years, to take advantage of machine learning techniques for watermark embedding and extraction. Knowles et al. [10] proposed a support vector machine aided watermarking method, in which the support vector machine is applied for the tamper detection in the watermark detection procedure. Li et al. [11] proposed 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 source node and its descendant nodes is established using SVM and further watermark is embedded and extracted based on this structuring data using relation. Tsai et al. [12] proposed a novel watermarking technique called SVM-based color image watermarking (SCIW) for the authentication of color images. Fu et al. [13] first embed template and watermark into original image in the same way, then a SVM train model is obtained by using the template samples, and the output of SVM model is obtained and the watermark is extracted. Yu et al. [14] proposed an SVM-based color image watermarking algorithm. The watermark bits and additional 1024 training bits are embedded in the blue channels of pixels. For extraction phase, the 1024 embedded training bits are employed as training samples of the SVM. When the SVM is trained, it is used for extracting the watermark.

In this paper, a novel image watermarking method in discrete wavelet transform domain using support vector machines is presented. Reference and watermark images are used to modify the coefficients of the selected even and odd blocks of the wavelet transformed image. Here the extraction of a watermark can be regarded as a classification problem for binary patterns. Therefore, approaches for solving classification problems can be integrated into the development of a watermark-extraction procedure. SVMs are used to extract the watermark from the watermarked image under several different attacks.

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

## II. PRELIMINARIES

### A. Discrete Wavelet Transform

The Discrete Wavelet Transform (DWT), which is centred on sub-band coding is found to return a fast computation of Wavelet Transform. A one level DWT decomposition can be efficiently achieved by a pyramidal algorithm. With different arrangements of low-pass filter and high-pass filter, an image can be decomposed into low-low (LL), low-high (LH), high-low (HL) and high-high (HH) bands. This process is continued until the desired number of levels determined by the application is reached. Figure 1 shows the two level of decomposition.

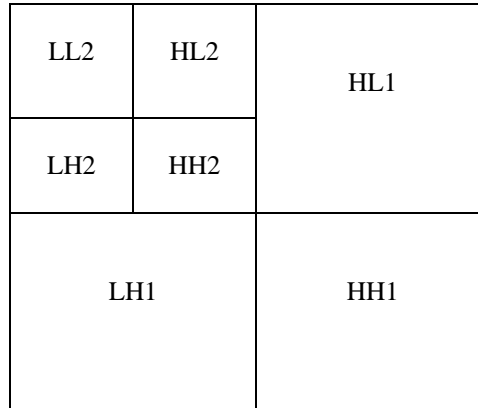


Figure 1. DWT decomposition with two levels

In DWT-based watermarking, the DWT coefficients are modified to embed the watermark data.

### B. Support Vector Machines (SVMs)

The support vector machine (SVM) is a general classification algorithm or a machine learning tool for performing classification and detection tasks. From the statistical learning theory, one can consider the binary classification by support vector machines by considering the theoretical upper bound on the generalization error. It is the theoretical prediction error obtained when the binary classification is applied to new and unknown instances. Consider a binary classification task with data points  $X_i$  ( $i=1,2,\dots,m$ ), having corresponding labels  $y_i=\pm 1$  and the decision function be:

$$f(x) = \text{sign}(w \cdot x + b) \quad (1)$$

Where,  $\cdot$  is the scalar or inner product (so  $w \cdot x \equiv w^T x$ ).

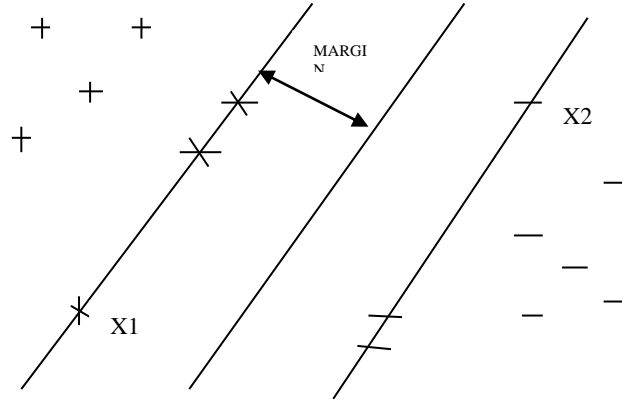


Figure 2. Hyperplane for SVM

From decision function we know that the data is correctly classified if  $y_i(w \cdot x_i + b) > 0 \forall i$ , and  $(w \cdot x_i + b)$  should be positive when  $y_i = +1$ , and it should be negative when  $y_i = -1$ . This leads to a doubt in defining a concept of distance or margin.

Many classification algorithms were previously restricted to linearly separable datasets, but with the use of kernel substitution, they can handle non-separable datasets. The binary-class SVM formulation only one instance of a broad range of *kernelizable* methods. For binary classification with a given choice of kernel, the learning task therefore involves maximization of:

$$W(\alpha) = \sum_{i=1}^m \alpha_i - \frac{1}{2} \sum_{i,j=1}^m K \alpha_i \alpha_j y_i y_j (x_i x_j) \quad (2)$$

### III. THE PROPOSED METHOD

#### A. WATERMARK EMBEDDING

The procedure for embedding the watermark is as follows:

1. The host image is of size 512x512 pixels and the reference and watermark images are of size 64x32 pixels.
2. The host image is partitioned into non-overlapping blocks of size 8x8.
3. Perform 1-level 2D DWT on each image block.
4. Randomly select two sub-bands of every image block using a secret key K.
5. For each selected sub-band block, mean value of its coefficient set is calculated.
6. Modify the coefficients of sub-band of even blocks using reference information and odd blocks using watermark bits.
  - i) If  $w = 1$ , then decrease absolute value of each coefficient in coefficient set 1 and meanwhile increase absolute value of each coefficient in coefficient set 2.
  - ii) If  $w = 0$ , then increase absolute value of each coefficient in coefficient set 1 and meanwhile decrease absolute value of each coefficient in coefficient set 2.
7. Finally, odd and even groups are joined together and each image block is reconstructed by applying inverse wavelet transform.
8. Watermarked image is obtained by combining the all image blocks.

#### B. WATERMARK EXTRACTION

The watermark extraction process from a watermarked image is as follows:

Using Nonlinear mapping ability of SVMs, and regarded as a binary classification problem.

1. Divide the watermarked image into 8x8 non-overlapping blocks.
2. Perform 1-level 2D DWT on each image block.
3. Using the same secret key K select two sub-bands of every image block.
4. Construct a training set S from even image blocks in which reference information has been embedded and train the SVMs.

5. From odd image blocks in which watermark is embedded, construct an input set  $S'$ . By using trained SVMs, calculate the corresponding outputs.
6. Output bits are converted into a two-dimensional watermark image.

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

$$\text{PSNR} = 10 \log_{10} \left( \frac{\sum_{i=1}^N \sum_{j=1}^N (F(i, j))^2}{\sum_{i=1}^N \sum_{j=1}^N (f(i, j) - F(i, j))^2} \right) \quad (3)$$

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

$$\text{NC} = \frac{\sum_{i=1}^N \sum_{j=1}^N (w(i, j) - w_{\text{mean}})(w'(i, j) - w'_{\text{mean}})}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N (w(i, j) - w_{\text{mean}})^2 \sum_{i=1}^N \sum_{j=1}^N (w'(i, j) - w'_{\text{mean}})^2}} \quad (4)$$

In Eq.(4),  $w_{\text{mean}}$  and  $w'_{\text{mean}}$  indicate the mean of the original watermark image and extracted watermark image respectively.

#### IV. EXPERIMENTAL RESULTS AND DISCUSSION

To evaluate the effectiveness of the method, experiments are carried out using host grey-scale images 'GOLDHILL', MANDRILL and 'PEPPERS' as shown in Figure 3.

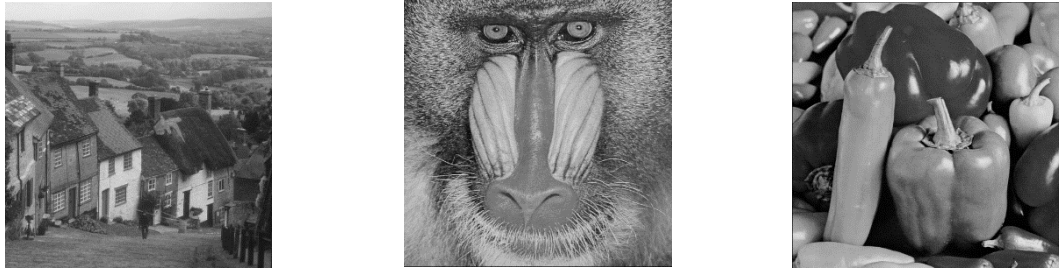


Figure.3. 512x512 (a) Goldhill, (b) Mandrill and (c) Peppers (Host Images)

The size of the host images are 512 x 512 pixels. The Reference and watermark image are of size 64 x 32 pixels as shown in Figure 4.



Figure 4. 64 x 32 (a) Reference image (b) Watermark image

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

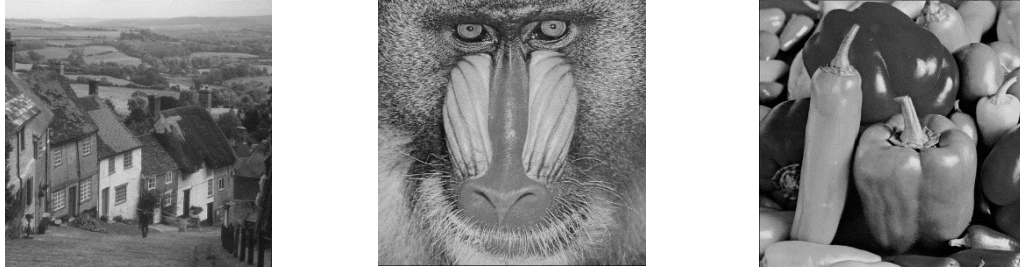


Figure. 5. 512x512 Watermarked (a) Goldhill (45.94dB), (b) Mandrill (41.27dB) and (c) Peppers (42.78dB)

Various image processing attacks used to test the strength of the watermark are JPEG Compression, Salt and Pepper noise, Row-Column blanking, Row-Column copying, Gamma Correction, Low Pass Filtering, Cropping, Bit Plane Removal, Histogram Equalization and Sharpening. All the attacks were tested using MATLAB 7.8.0.



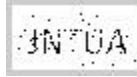
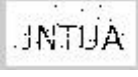


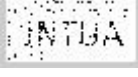
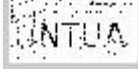
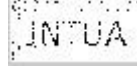
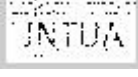
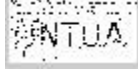
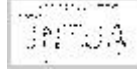

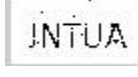
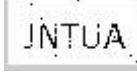


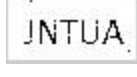
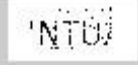
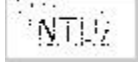
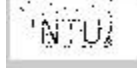
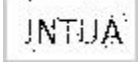

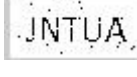
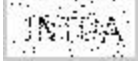

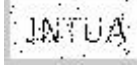
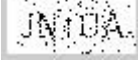
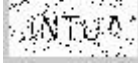
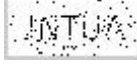
The watermarked image is compressed using JPEG compression with a Quality Factor of 100. The index of JPEG compression varies from 0 to 100, where 0 is for best compression and 100 is for best quality. The watermarked image is added with Salt & Pepper noise with a noise density of  $10^{-3}$ . In row-column copy attack a set of rows and columns are copied to random locations. Here 30<sup>th</sup> row is replaced by 10<sup>th</sup> row, 40 to 70, 120<sup>th</sup> row is replaced by 100<sup>th</sup> and 160<sup>th</sup> row by 140<sup>th</sup> row. In row-column blanking attack a set of rows and columns are deleted. In this experiment 10,30,40,70,100,120 & 140 rows and columns are removed. In Low pass Filtering attack a 3x3 mask containing of 0.9 intensity values is used. In Gamma Correction attack, a gamma value of 0.9 is used. Finally, the proposed algorithm is also resistant to Bit plane removal, cropping, Histogram Equalization and Sharpening attacks. 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. Extracted watermarks from the watermarked images are shown in Table 2.

Table I. The PSNR and NC values for Goldhill, Mandrill and Peppers under various attacks

| Type of Attack         | Goldhill |        | Mandrill |        | Peppers  |        |
|------------------------|----------|--------|----------|--------|----------|--------|
|                        | PSNR(dB) | NCC    | PSNR(dB) | NCC    | PSNR(dB) | NCC    |
| No Attack              | 45.94    | 0.9468 | 41.27    | 0.9226 | 42.78    | 0.9619 |
| Salt & Pepper Noise    | 34.51    | 0.7768 | 33.86    | 0.7079 | 33.61    | 0.7334 |
| JPEG Attack            | 45.64    | 0.9043 | 41.17    | 0.9190 | 42.67    | 0.9168 |
| Row-Column Copying     | 34.66    | 0.6240 | 30.44    | 0.6349 | 30.55    | 0.6891 |
| Row-Column Blanking    | 19.78    | 0.6437 | 20.67    | 0.5699 | 21.03    | 0.4967 |
| Gamma Correction       | 28.42    | 0.9203 | 28.39    | 0.9159 | 28.77    | 0.9196 |
| Low Pass Filtering     | 11.68    | 0.9468 | 10.59    | 0.9226 | 11.71    | 0.9619 |
| Cropping               | 8.36     | 0.6921 | 7.49     | 0.6228 | 8.45     | 0.6283 |
| Bit Plane Removal      | 44.62    | 0.9036 | 40.75    | 0.9067 | 42.10    | 0.8896 |
| Histogram Equalization | 16.82    | 0.5913 | 16.66    | 0.5820 | 17.65    | 0.7190 |
| Sharpening             | 20.20    | 0.5906 | 14.15    | 0.5310 | 21.36    | 0.6025 |

Table. II Extracted Watermarks from the watermarked images

| Type of Attack | Watermarked Image Type |           |           |
|----------------|------------------------|-----------|-----------|
|                | Goldhill               | Mandrill  | Peppers   |
| No Attack      |                        |           |           |
|                | NC: 0.9468             | NC:0.9226 | NC:0.9619 |
|                |                        |           |           |

|                                    |   |  |   |
|------------------------------------|---|--|---|
| Salt & Pepper Noise<br>(0.001)     |    |    |    |
|                                    | NC: 0.7768  | NC:0.7079  | NC:0.7334   |
| JPEG Attack<br>(Q.F.:100)          |    |    |    |
|                                    | NC: 0.9043  | NC:0.9190  | NC:0.7334   |
| Row-Column Copying                 |    |    |    |
|                                    | NC: 0.6240  | NC:0.6349  | NC:0.6891   |
| Row-Column Blanking                |    |    |    |
|                                    | NC: 0.6437  | NC:0.5699  | NC:0.4967   |
| Gamma Correction<br>(0.9)          |   |   |   |
|                                    | NC: 0.9203  | NC:0.9159  | NC:0.9196   |
| Low Pass Filtering<br>(3x3 Kernel) |  |  |  |
|                                    | NC: 0.9468  | NC:0.9226  | NC:0.9619   |
| Cropping                           |  |  |  |
|                                    | NC: 0.6921  | NC: 0.6228   | NC:0.6283   |
| Bit Plane Removal                  |  |  |  |
|                                    | NC: 0.9036  | NC:0.9067  | NC:0.8896   |
| Histogram Equalization             |  |  |  |
|                                    | NC: 0.5913  | NC:0.5820  | NC:0.7190   |
| Sharpening                         |  |  |  |
|                                    | NC: 0.5906  | NC:0.5310  | NC:0.6025   |

## V. CONCLUSIONS

In this paper, a novel Image watermarking scheme using discrete wavelet transform based on the support vector machines have been presented. The quality of the watermarked image is better in terms of perceptibility and PSNR. The proposed method is shown to be robust to JPEG Compression, Salt and Pepper noise, Row-Column blanking, Row-Column copying, Gamma Correction, Low Pass Filtering, Cropping, Bit Plane Removal, Histogram Equalization and Sharpening, etc. The test results are superior in terms of PSNR of the watermarked image and NC values of the extracted watermarks.

## ACKNOWLEDGEMENT

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

## REFERENCES

- [1] I.J.Cox, J.Kilian, T.Leighton and T.Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", *IEEE Transactions on Image Processing*, 6(12), 1673-1687, December, 1997.
- [2] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", *IEEE Proc.* 86, (6), pp. 1064-1087, 1998.
- [3] Vapnik, V, "The nature of statistical learning theory", *Springer, New York, USA*, 1995.
- [4] Steve R Gunn, "Support vector machines for classification and regression", *Technical Report, ISIS Department of electronics and computer science, University of Southampton*, 1998.
- [5] Qun-Ting Yang, Tie-Gang Gao, Li Fan, "A Novel Robust Watermarking Scheme based on Neural Network", *Proceedings of IEEE International Conference on Intelligent Computing and Integrated Systems*, pp.71-75, Oct, 2010.
- [6] Sameh Oueslati, Adnene Cherif, Bassel Solaimane, "Adaptive Image Watermarking Scheme based on Neural Network", *International Journal of Engineering Science and Technology*, Vol. 3, No. 1, Jan 2011.
- [7] P.H.H. Then, and Y.C. Wang, "Support Vector Machine as Digital Watermark Detector," *In Proceedings of SPIE-IS&T Electronic Imaging, SPIE*, 2006.
- [8] Jianzhen Wu., "A RST invariant watermarking scheme utilizing support vector machine and image moments for synchronization", *International conference on information assurance and security*, p.p. 572-74, 2009.
- [9] Hong Peng, Jun Wang, Weixing Wang, "Image watermarking method in multiwavelet Domain based on support vector machine", *J. Sys. Software*, 83 (8) pp.1470-1477, 2010.
- [10] Knowles, H.D., Winne, D.A., Canagarajah, C.N., Bull, D.R., "Image tamper detection and classification using support vector machines," *IEE Proceedings—Vision, Image and Signal Processing* 151 (4), 322-328, 2004.
- [11] Chun-hua Li, Ling He-fei, Lu Zheng-ding, "Semi-fragile watermarking based on SVM for image authentication", *IEEE International Conference on Multimedia and Expo, Beijing, China*, pp. 1255-1258, 2007.
- [12] H.H. Tsai, D.W. Sun, "Color image watermark extraction based on Support vector machines", *Inform. Sci.* 177 (2), pp.550-569, 2007.
- [13] Fu ong-gang, Shen Rui-min, Lu Hong-tao, "Watermarking scheme based on support vector machine for color images", *IEE Electron Letters*, 40(16):986-7, 2004.
- [14] Yu, Pao-Ta, Tsai, Hung-Hsu, Sun, Duen-Wu, "Digital Watermarking of Color Images Using Support Vector Machines", *National Computer symposium (NCS'03)*, 2003.
- [15] Colin Campbell, Yiming Ying, "Learning with Support Vector Machines", Morgan & Claypool Publishers, 2011.

