A Robust Wavelet Packet based Blind Digital Image Watermarking using HVS characteristics

C. Patvardhan
Electrical Engineering Deptt.
Dayalbagh Educational Institute
Dayalbagh, Agra, UP, India

A. K. Verma
Electrical Engineering Deptt.
Dayalbagh Educational Institute
Dayalbagh, Agra, UP, India

C. Vasantha Lakshmi
Physics and C.S. Deptt.
Dayalbagh Educational Institute
Dayalbagh, Agra, UP, India

ABSTRACT
In this paper, we present a new method of digital image watermarking in wavelet domain using Discrete Wavelet Packet Transform (DWPT) analysis of the host image. The discrete wavelet packet decomposition is chosen to utilize all high frequency components in order to make the watermarking more imperceptible using Coif5 as wavelet basis. According to the characteristics of Human Visual System (HVS), human eyes are less sensitive in high frequency bands having orientation of 45^0,Therefore, the binary watermark is embedded in the high frequency diagonal components of wavelet packet decomposition tree which have maximum entropy. Watermarking is achieved by generating a pseudo-random sequence and then embedding it into wavelet coefficients according to the watermark bit pattern. Performance of the proposed scheme is evaluated on a variety of images including Lena, Boat, Cameraman and a textured image of Brodatz database. The results show that, the proposed scheme provides good level of imperceptibility as well as robustness against various attacks such as JPEG compression, Filtering, Noise addition, Cropping etc. and competes well with existing methods.

General Terms
Digital media security, Digital image watermarking.

Keywords
Discrete Wavelet Packets Transform, Coif5, Pseudo Random Sequence, Robustness, Correlation, Entropy.

1. INTRODUCTION
With the ubiquitous use of Internet and easily available copying tools, unauthorized tampering of digital media has become a difficult challenge to copyright protection these days. Therefore, protection of multimedia data has become a priority for the researchers. Digital watermarking has emerged as a tool to protect the digital media data against such unwanted tampering. In the process of digital image watermarking, a watermark, which may be in the form of either text or an image (logo), is embedded in the host image thus providing means of ownership identification of the host image.

The major requirements in this process are imperceptibility, robustness and payload. Imperceptibility means that watermark is embedded in the host image with minimum possible visual changes. Robustness of the watermarking scheme indicates the capacity of the scheme to withstand several types of attacks to remove the watermark. Payload of a scheme indicates the amount of data that can be embedded in the host image without compromising the imperceptibility of the watermarked image.

An overview of digital watermarking is presented in [1]. Digital image watermarking can be performed either in spatial domain or in frequency domain. Earlier techniques used spatial domain watermarking methods [2]. However such techniques [3, 4] have relatively low-bit capacity and are not resistant enough to lossy image compression such as JPEG, cropping and other image processing attacks. Frequency domain based techniques provide better imperceptibility and robustness to a variety of attacks. Various types of frequency transforms that have been used are Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). Earlier watermarking schemes used DFT [5] and DCT [6, 7]. However, Wavelet based watermarking schemes are becoming more attractive. A good comparison of all these transform domain schemes is presented in [8]. Wavelet based watermarking methods exploit the frequency information and spatial information of the transformed data in multiple resolutions to gain robustness. A comparative analysis of various wavelet based watermarking methods is presented in [9]. Wavelet packets based watermarking is another approach that can be used for digital image watermarking.

A few wavelet packets based watermarking methods have been proposed in literature. A watermarking method based on quantization of means of wavelet coefficients is presented in [10], which uses 3-level wavelet packet decomposition hence requiring more computational resources. A semi fragile method of watermark embedding along with tamper detection is presented in [11], which emphasizes the tamper detection rather than performance of watermarking against various attacks. A method, which employs best basis selection of wavelet packets for embedding is presented in [12]. But this scheme mainly focuses the robustness against JPEG compression. A method based on wavelet coefficients' energy for selecting appropriate coefficients for watermark embedding specifically in medical images is presented in [13]. In this paper, we present a simple approach of watermarking which utilizes the advantages of wavelet packets, Coif wavelet basis and Human Visual System's characteristics, providing good imperceptibility as well as robustness against various types of attacks. The rest of the paper is organized as follows. Section 2 provides a brief introduction to wavelet packet decomposition. Section 3 describes the proposed watermark embedding and watermark detection algorithms. Section 4 shows the experimental results. Some conclusions are given in section 5.

2. DISCRETE WAVELET PACKET TRANSFORM (DWPT)

Wavelet packets are used to get the advantage of better frequency resolution representation. Wavelet packets analysis is a generalization of orthogonal wavelets that allow richer signal analysis by breaking up detail (high frequency) spaces, which are never decomposed in the case of wavelets. Wavelets packets were introduced by Coifman and Wickerhauser [14] in early 1990s in order to mitigate the lack of frequency resolution of wavelet analysis. The principle is to some extent to cut up detail spaces into frequency sections.

In wavelet analysis, a signal is split into an approximation and a detail. The approximation is then itself split into a second-level approximation and detail, and the process is repeated. For n-level decomposition, there are $n+1$ possible ways to decompose or encode the signal. In wavelet packet analysis, the details as well as the approximations can be split. This yields more than $2^{2^{n-1}}$different ways to encode the signal. The set of functions $w_{j,n} = (\, w_{j,n,k}(x),\ k \in \mathbb{Z})$ is the (j, n) wavelet packet. For positive values of integers j and n, wavelet packets are organized in binary trees. Here scale j defines depth and frequency n defines position in the Tree. The notation $w_{j,n}$ where j denotes scale parameter and n the frequency parameter, is consistent with the usual depth-position tree labeling. [15]. A two-level wavelet packet decomposition is shown in figure 1.

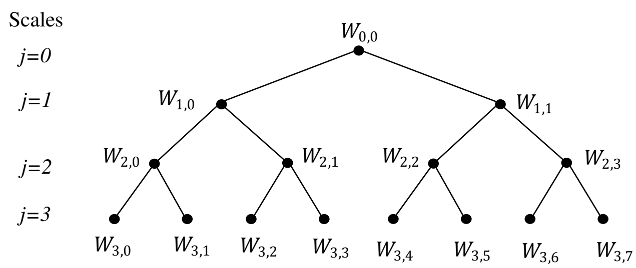


Figure 1: 3 level wavelet packet decomposition binary tree

In the figure 1, $w_{1,0}$ is the outcome of a low pass wavelet filter having low frequency details and known as Approximation Coefficient band. The $w_{1,1}$ is the output of high pass wavelet filter, which contains high frequency details and known as Detailed Coefficient band. The coefficients $w_{1,0}$ and $w_{1,1}$are further split into high and low frequency bands at every scale.

The same theory can be applied to two dimensional signals (images). The binary tree of figure 1 is extended to quad tree as shown in figure 2 for depth 2.

In figure 2, cA represents low frequency coefficients known as Approximation Coefficients and cH, cV and cD represent high frequency coefficients known as Horizontal, Vertical and Diagonal Coefficients respectively.

As an example, 2-level wavelet packet decomposition is applied on Lena image using Haar wavelet basis and is shown in figure 3.

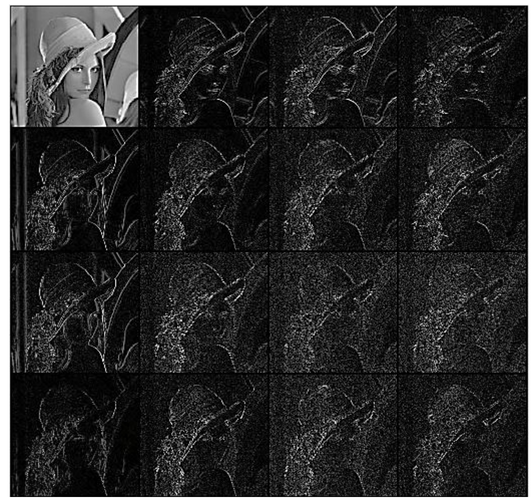


Figure 3: 2 level wavelet packet decomposition of Lena using Haar basis.

For wavelet packet decomposition, the Coif5 wavelet is chosen due to some of its advantages as Coiflet is an orthogonal wavelet with compact support. It has highest number of vanishing moments for both $\psi(t)$(wavelet function) and $\varphi(t)$ (Scaling function) for given support width, flat frequency response and better reconstruction characteristics.

3. WATERMARK EMBEDDING AND EXTRACTION ALGORITHMS

In this paper, Spread Spectrum watermarking scheme is implemented for the proposed robust algorithm. The watermark embedding as well as extraction is evaluated for various types of images with Coif5 as wavelet basis function for packet

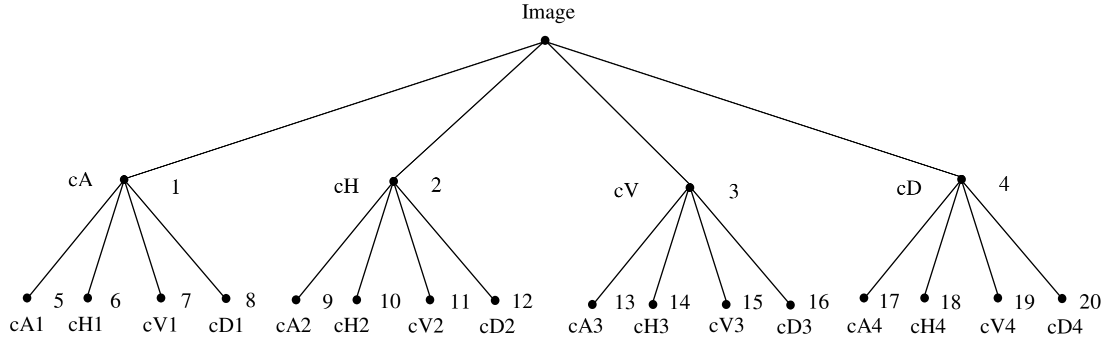


Figure 2: 2–Level wavelet packet decomposition quad tree

decomposition. As suggested in [16], human eye is less sensitive to noise in high frequency bands and bands having orientation of 45 degrees. Thus the watermarking is performed by adding a Pseudo Random Noise (PN) sequence to the high frequency diagonal wavelet coefficients for each of the watermark bit and watermark is extracted by finding correlation between regenerated PN sequence and modified wavelet coefficients.

3.1 WATERMARK EMBEDDING ALGORITHM

The steps of embedding algorithm are as follows:

Input: A grayscale image (I) of type *uint8* and of size $M \times M$ and a binary watermark (W).
Output: Watermarked Image (I_w).

1) Find 2-level discrete wavelet packet transform (DWPT) of Host Image (I) and obtain all 16 coefficients matrices of size $\frac{M}{4} \times \frac{M}{4}$ at level 2 as shown in figure 2.

2) All the high frequency diagonal coefficient bands cD_1, cD_2, cD_3 and cD_4 are considered for watermark embedding. Out of these four matrices, any two matrices having maximum entropy say cD_x and cD_y are selected for watermark embedding. (Here entropy is calculated by log energy method as $E(s) = \sum_i \log(s_i)^2$, where, s_i are the signal's coefficient in orthonormal basis with convention $\log(0) = 0$).

3) Select a Seed to generate a PN sequence (PNS) of size equal to the size of selected matrices cD_x or cD_y .

4) Generate another matrix PN from PNS according to the relation $PN = R1 \times (PNS - R2)$, where, $R1 = 2$ and $R2 = 0.5$.

5) Convert the 2D watermark into 1D array and if watermark bit is 0 (Black) then modify elements of both the selected matrices as, $cD_x = cD_x + k.PN$ and $cD_y = cD_y + k.PN$, Where, k is embedding strength. If watermark bit is 1 (white) then wavelet coefficients are left unchanged.

6) Now repeat the step 4 and 5 for all '0' watermark bits with every time newly generated PN sequence.

7) Put both the modified cD_x and cD_y matrices in their original positions in wavelet packet tree and take inverse DPWT to get back the watermarked image (I_w).

8) Compute the PSNR for I and I_w to check that how much the host image is modified.

The embedding algorithm is shown graphically in figure 4.

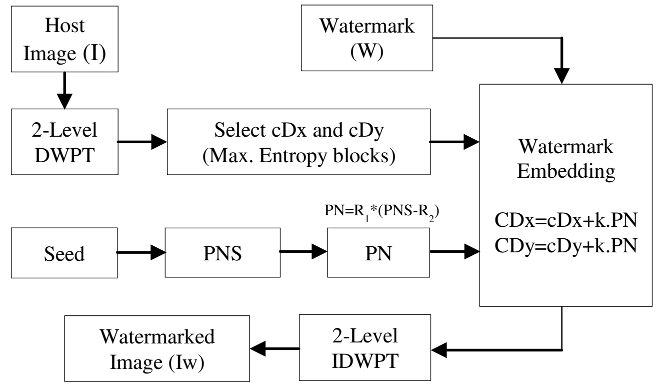


Figure 4: Watermark Embedding Algorithm

3.2 WATERMARK EXTRACTION ALGORITHM

Following are the steps in watermark extraction,

Input: Watermarked Image (I_w).
Output: Extracted Watermark (W_R).

1) Decompose the watermarked image (I_w) in 2 levels by DWPT and get back the same modified coefficients metrics cD_x' and cD_y' as used in case of embedding on the basis of maximum entropy.

2) Generate the same PN sequence (PNS), which was generated in embedding process using same Seed value.

3) Convert the PN sequence (PNS) into $PN = R1 \times (PNS - R2)$ with $R1 = 2$ and $R2 = 0.5$.

4) Compute the correlation coefficients between PN sequence (PN) and modified coefficient matrices cD_x' and cD_y', as $r_1 = corr2(PN, cD_x')$ and $r_2 = corr2(PN, cD_y')$, then find $r = (r_1 + r_2)/2$.

5) Repeat step 4 for all watermark bits and compute the correlation values.

6) Compute the threshold value as $(T = 1.5 * mean(r))$ and initialize a row matrix (W') having all values '1' equivalent to the size of watermark.

7) For every watermark bit, compare r with T and modify the W' as follows,
$$W' = \begin{cases} 0, & r > T \\ 1, & otherwise \end{cases}$$

8) Reshape the row matrix W' into a matrix equivalent to the size of original watermark matrix (W) to get recovered watermark (W_R').

9) Compute the similarity between original watermark (W) and recovered watermark (W_R) to check how well the watermark is extracted.

The watermark extraction algorithm is shown in figure 5.

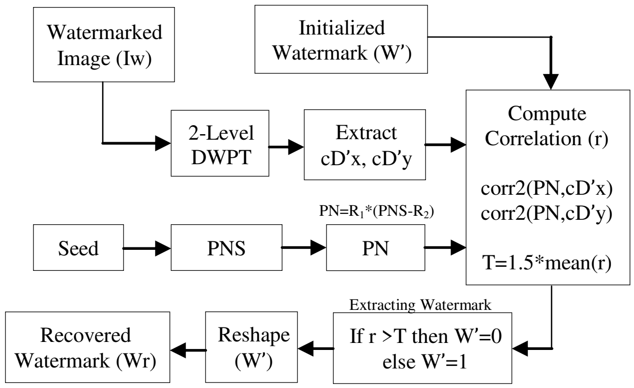


Figure 5: Watermark Extraction Algorithm

4. EXPERIMENTAL RESULTS

This section presents the experimental results. As host images several grayscale images of size 512×512 are tested such as Lena, Cameraman, Boat and D20 (textured image from Brodatz texture database). These images are shown in figure 6.

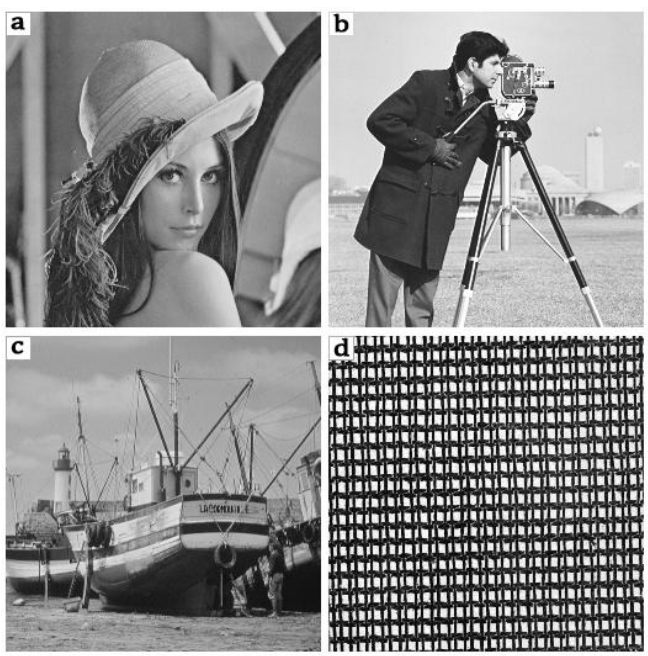


Figure 6: Test Images used for watermarking, (a): Lena, (b): Cameraman, (c): Boat, (d): D20

The Watermark Image is taken a binary image of size 21x12 as shown in figure 7.

Fig.7. Binary Watermark

The binary watermark as shown in figure 7 is embedded in host images using the embedding algorithm of section 3.1. After watermark embedding, PSNR between original image (I) and watermarked image (I_w) is calculated using,

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right)$$

Where, MSE is mean Square Error given by,

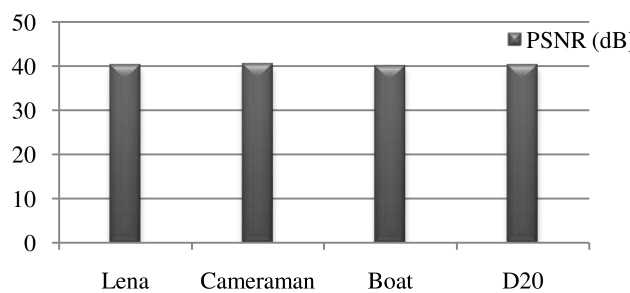
$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}[I(i,j) - I_w(i,j)]^2$$

Where, $I_w(i,j)$ is pixel value of watermarked image and $I(i,j)$ is pixel value of original image at coordinate i and j.

PSNR values for various test images are shown in figure 8 for no attack cases.

Images	PSNR (dB)
Lena	40.36
Cameraman	40.49
Boat	40.10
D20	40.30

(a)



(b)

Figure 8 (a, b): Comparison of PSNR for various test images after watermark embedding.

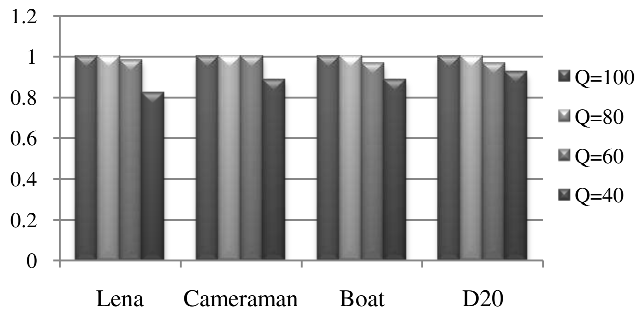
The performance of proposed scheme is also tested under several standard attacks such as compression, noise addition, filtering and geometrical type of attacks etc. The quality of extracted watermark is judged by finding normalized correlation between original watermark $(W)$and recovered watermark (w_R) by the relation,

$$NC = \frac{\sum_i \sum_j W(i,j).W_R(i,j)}{\sqrt{\sum_i \sum_j W^2(i,j)}.\sqrt{\sum_i \sum_j W_R^2(i,j)}}$$

Following section shows the performance of proposed scheme under various test cases (figures 9 through 16).The values$R1 = 0.5$, $R2 = 2$ and embedding strength $k = 1$are taken for the experiment.

Images	NC			
	Q=100	Q=80	Q=60	Q=40
Lena	1.0000	1.0000	0.9830	0.8215
Cameraman	1.0000	1.0000	1.0000	0.8895
Boat	1.0000	1.0000	0.9663	0.8895
D20	1.0000	1.0000	0.9661	0.9235

(a)

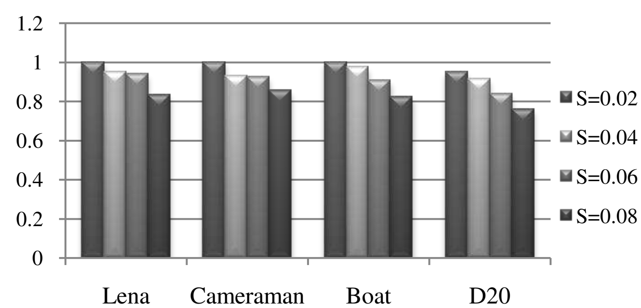


(b)

Figure 9 (a, b): Values of Normalized Correlation Coefficient (NC) under the JPEG compression (Quality Factor =100, 80, 60 and 40) attack.

Images	NC			
	S=0.02	S=0.04	S=0.06	S=0.08
Lena	1.0000	0.9492	0.9408	0.8322
Cameraman	1.0000	0.9326	0.9235	0.8550
Boat	1.0000	0.9747	0.9065	0.8233
D20	0.9492	0.9153	0.8385	0.7608

(a)

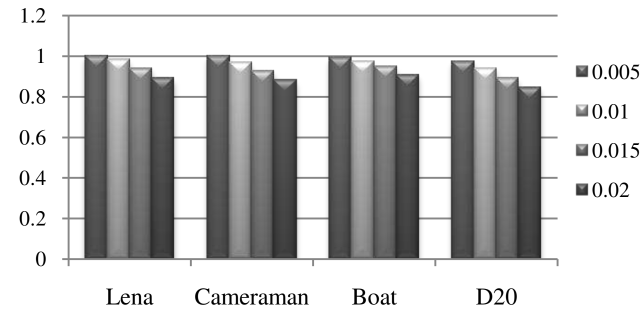


(b)

Figure 10 (a, b): Values of Normalized Correlation Coefficient (NC) under the Salt & Pepper Noise attack (Strength (S) = 0.02, 0.04, 0.06, 0.08).

Images	NC			
	σ^2=*0.005*	σ^2=*0.01*	σ^2=*0.015*	σ^2=*0.02*
Lena	1.0000	0.9830	0.9405	0.8900
Cameraman	1.0000	0.9663	0.9235	0.8807
Boat	0.9915	0.9745	0.9490	0.9065
D20	0.9745	0.9405	0.8895	0.8468

(a)

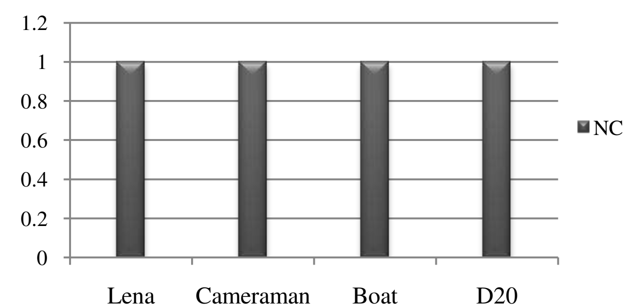


(b)

Figure 11 (a, b): Values of Normalized Correlation Coefficient (NC) under Gaussian Noise attack(μ=0 and σ^2=0.005, 0.010, 0.015, 0.02).

Images	NC
Lena	1.0000
Cameraman	1.0000
Boat	1.0000
D20	1.0000

(a)

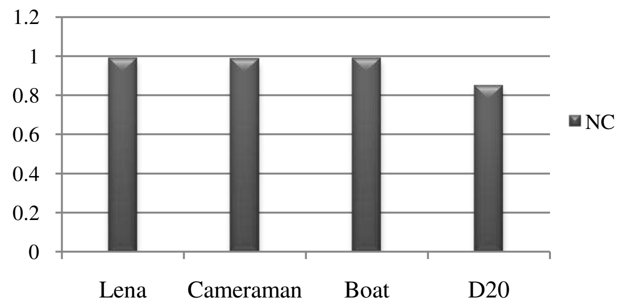


(b)

Figure 12 (a, b): Values of Normalized Correlation Coefficient (NC) under Sharpening attack (Mask = [-1 -1 -1;-1 9 -1; -1 -1 -1]).

Images	NC
Lena	0.9915
Cameraman	0.9831
Boat	0.9915
D20	0.8468

(a)

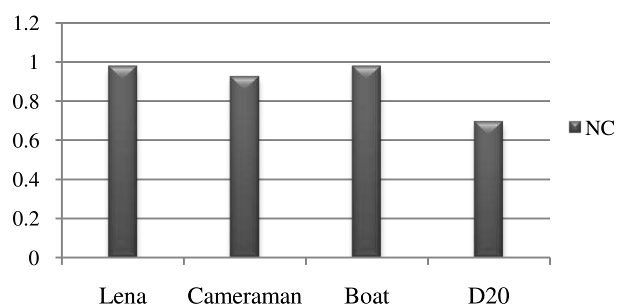


(b)

Figure 13(a, b): Values of Normalized Correlation Coefficient (NC) under Blurring attack ([3x3] Averaging Filter).

Images	NC
Lena	0.9746
Cameraman	0.9235
Boat	0.9747
D20	0.6923

(a)

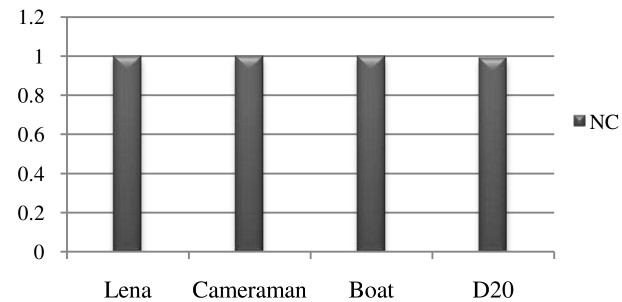


(b)

Figure 14 (a, b): Values of Normalized Correlation Coefficient (NC) under Median Filtering attack ([3x3] Mask).

Images	NC
Lena	1.0000
Cameraman	1.0000
Boat	1.0000
D20	0.9915

(a)

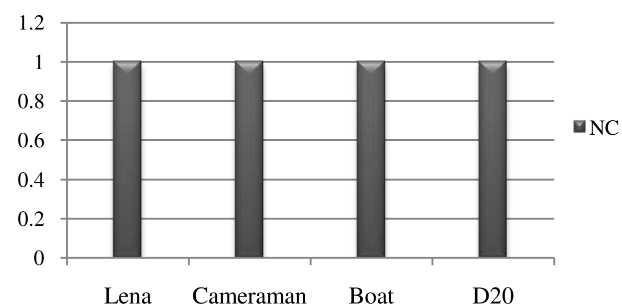


(b)

Figure 15 (a, b): Values of Normalized Correlation Coefficient (NC) under Cropping attack (1/4th upper left corner is cut)

Images	NC
Lena	1.0000
Cameraman	1.0000
Boat	1.0000
D20	1.0000

(a)



(b)

Figure 16(a, b): Values of Normalized Correlation Coefficient (NC) under Histogram Equalization attack.

5. CONCLUSIONS

In this paper, a robust method of spread spectrum digital image watermarking using wavelet packet decomposition is proposed. The algorithm utilizes the high frequency diagonal coefficients of maximum entropy value to achieve high value of imperceptibility (as seen from the results in figure 8). PSNR values above 40dB are obtained for all types of images. Robustness of the algorithm is evident from the value of normalized correlation coefficient between original and recovered watermark after various types of attacks.

In figure 9, the value of NC is shown for various quality factors of Jpeg compression and it can be observed that the value of NC is high even up to quality factor of 40%. In figure 10, the performance of the scheme can be observed in the case of salt and pepper noise of various strengths. In this case, even for high value of noise (strength=0.08), a good value of NC is obtained. Similarly, in case of Gaussian noise, obtained value of NC in various noise strengths, is quite good.

In other attack cases like sharpening (figure 12), cropping (figure 15) and histogram equalization (figure 16), it is able to recover full watermark without any distortion with 100% correlation. In rest of attack cases such as blurring achieved by averaging (figure 13) and median filtering (figure 14), the obtained value of correlation coefficient for textured image (D20) is slightly lower. Overall, the proposed method can be used with advantage as it works well for variety of images such as textured as well as non-textured images.

6. REFERENCES

[1] G. Voyatzis, N. Nikolaidis, I. Pitas, “Digital Watermarking: An overview”, in Proceeding of 9th European Signal Processing Conference, pp: 9-12, Sept 1998.

[2] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, "A digital watermark”, IEEE Proceedings ICIP, vol.2, pp. 86-90, 1994.

[3] N. Nikolaidis, and I. Pitas, Copyright protection of images using robust digital signatures, IEEE International Conference on Acoustics, Speech Signal Processing, vol. 4, pp.2168-2171, May1996.

[4] R. Wolfgang and E. Delp, A watermark for digital image, IEEE Proceedings ICIP, vol.3, pp.211-214, 1996.

[5] Emir Ganic, Scott D. Dexter, Ahmet M. Eskicioglu, Embedding Multiple Watermarks in the DFT Domain using Low and High Frequency Bands, Proceedings on Security, Steganography, and Watermarking of Multimedia Contents, Volume VII, vol. 5681, SPIE.

[6] Lin S. D., Chin Feng Chen, A robust DCT-based watermarking for copyright protection, IEEE Transactions on Consumer Electronics, Vol. 46, Issue.03, pp. 415-421, August, 2000.

[7] I. J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon, Secure Spread Spectrum Watermarking for Multimedia, IEEE Transactions on Image Processing, Vol. 6, No. 12, December 1997.

[8] C. V. Serdean, M. Tomlinson, J. G. Wade and M. A. Ambroze,Protecting Intellectual Rights: Digital WM in the Wavelet Domain, Proceedings of the IEEE International Workshop on Trends and Recent Achievements in Information Technology, Cluj-Napoca, Romania, 16-18 May, 02, ISBN: 973-8335-49-3.

[9] C. S. Woo, Du J., Pham B., Performance Factors Analysis of a Wavelet-based Watermarking Method, Proceedings of 3rd Australian Information Security Workshop (AISW2005), CRPIT, vol. 44, pp. 89-97, 2005.

[10] A. Adhipathi Reddy, B. N. Chatterji, “Wavelet Packet Based Digital Image Watermarking,” Proceedings of the Fourth Indian Conference on Computer Vision, Graphics Image Processing (ICVGIP), pp.364-369, 2004.

[11] A.H. Paquet, R.K. Ward and I. Pitas, “Wavelet packets-based digital watermarking for image verification and authentication", Published in Signal Processing Journal, ACM digital library, Special section: Security of data hiding technologies, Volume 83, Issue 10, October 2003.

[12] Vehel J. L., Manoury A., “Wavelet packet based digital watermarking”, in Proceedings of 15th International Conference on Pattern Recognition, Vol. 03, pp. 423-416., August, 2002.

[13] Salwa A. K. Mostafa, Naser El-Sheimy, A. S. Tolba, F. M. Abdelkader and Hisham M. Elhindy, “Wavelet Packets-Based Blind Watermarking for Medical Image Management”, The Open Biomedical Engineering Journal, Vol. 04, pp. 93–98, 2010.

[14] Coifman R. R., Wirckerhauser M.V., “Entropy based algorithms for best basis selection”, IEEE Trans. On Inf. Theory, vol. 38, no. 2, pp. 713-718, 1992.

[15] M. Misiti, Y. Misiti, G. Oppenheim, J. M. Poggi, “Wavelets and their Applications”, ISTE, ISBN: 978-1-905209-31-6, 2007.

[16] A. B. Watson, G. Y. Yang, J. A. Solomon and J. Villasenor. “Visibility of Wavelet Quantization Noise”. IEEE Transection on Image Processing, vol. 6, pp. 1164-1175, Aug 1997.