The Robust Digital Image Watermarking Scheme With Back Propagation Neural Network In DWT Domain

Nallagarla Ramamurthy† and S. Varadarajan††,

†Research Scholar, JNTUA,Anantapur, A.P, INDIA
††Professor,Dept.of ECE,S.V.University college of Engg., Tirupati, INDIA

Summary
The copyright protection of digital content became a critical issue now a days. Digital image watermarking is one of the techniques used to protect digital content. A novel image watermarking approach based on back propagation neural network in DWT domain is proposed in this paper. The cover image is decomposed up to 3-levels using DWT. The bitmap is selected as a watermark. The back propagation neural network is implemented while embedding and extracting the watermark. The proposed watermarking algorithm is imperceptible and robust to some normal attacks such as JPEG compression, salt and pepper noise, rotation and cropping.

Key words:
Digital Image Watermarking, Back Propagation Neural Network, DWT, Bitmap, Imperceptible, Robust, JPEG compression, Cropping.

1. Introduction

Copyright protection of multimedia data has become critical issue due to the massive spreading of broadband networks , easy copying, and new developments in digital technology. As a solution to this problem, digital image watermarking became very popular now-a-days. Digital image watermarking is a kind of technology , that embeds copyright information into multimedia content. An effective image watermarking scheme mainly includes watermark generation, watermark embedding, watermark detection, and watermark attack [6].Digital image watermarking provides copyright protection to image by hiding appropriate information in original image to declare rightful ownership [16]. There are four essential factors those are commonly used to determine quality of watermarking scheme. They are robustness, imperceptibility, capacity, and blindness. Robustness is a measure of immunity of watermark against attempts to image modification and manipulation like compression, filtering, rotation, scaling, noise attacks, resizing, cropping etc. imperceptibility is the quality the cover image should not be destroyed by the presence of watermark. Capacity includes techniques that make it possible to embed majority of information . Extraction of watermark from watermarked image without the need of original image is referred to as blind watermarking. The non-blind watermarking technique requires that the original image to exist for detection and extraction. The semi-blind watermarking scheme requires the secrete key and watermark bit sequence for extraction. Another categorization of watermarks based on the embedded data are visible and invisible [14].

According to the domain of watermark insertion, the watermarking techniques fall into two categories: spatial domain methods and transform domain methods. Many techniques have been proposed in the spatial such as LSB (Least Significant Bit) insertion method, the patch work method and the texture block coding method [15]. These techniques process the location and luminance of the image pixel directly. The LSB method has a major disadvantage that the least significant bits may be easily destroyed by lossy compression. Transform domain method based on special transformations, and process the coefficients in frequency domain to hide the data. Transform domain methods include Fast Fourier Transform(FFT), Discrete Cosine Transform(DCT), Discrete Wavelet Transform(DWT), Curvelete Transform(CT), Counterlet Transform(CLT) etc. In these methods the watermark is hidden in the high and middle frequency coefficients of the cover image. The low frequency coefficients are suppressed by filtering as noise, hence watermark is not inserted in low frequency coefficients [15]. The transform domain method is more robust than the spatial domain method against compression, filtering, rotation, cropping and noise attack etc.

The [12] presents a blind image watermarking scheme that embeds watermark messages at different wavelet blocks is presented base on the training of BPNN in wavelet domain. The [13] presents an adaptive image watermarking algorithm which is based on synthetic human visual system (HVS) characteristic and associative memory function of neural network. The [2] presents a blind watermark embedding/ extracting algorithm using the Radial Basis Function Neural Network [RBFN]. Reference [4] proposed a system SBS-SOM a neural network algorithm was

Manuscript received January 5, 2013
Manuscript revised January 20, 2013

trained to generate digital watermark values from the image. Reference [6] presents a DWT domain image watermarking scheme, where genetic algorithm is used to select the fit wavelet coefficients to embed watermarking bits into the host gray image. The[7] presents an adaptive image watermarking scheme based on Full Counter Propagation Neural Network (FCNN). Reference [8] proposed a novel approach to neural network watermarking for uncompressed video in yhe wavelet domain. Summrina Kanwal Wajid et al proposed the robust and imperceptible image watermarking using Full Counter Propagation Neural Network.[9], with lesser complexity and easy apprehension. Cheng-Ri. Piao et al proposed a new blind watermark embedding/extracting algorithm using the RBF Neural Network[10]. Pao-Ta. Yu et al developed watermarking techniques, integrating both color image processing and cryptography, to achieve content protection and authentication for color images[11]. In this paper a new blind watermarking scheme to embed bitmap into the Blue(B) plane of the cover image is presented. This technique is based on training Back Propagation Neural Network(BPNN) in the Discrete wavelet Transform Domain. While embedding the watermark , a secrete key is generated to determine the beginning of the watermark location. BPNN is implemented to embed and extract the watermark. The experimental results show that the proposed watermark technique is invisible and robust to attacks such like compression , cropping, rotation, median filtering, and salt& pepper noise attack.

2. Disrete wavelet Transform(DWT)

The discrete wavelet transform was invented by the Hungarian mathematician Alfred Haar. For on input represented by a list of 2n numbers, the Haar Wavelet Transform simply pair up input values, storing the deference and passing the sum [4]. This process is repeated recursively, pairing up the sums, finally resulting in 2n-1 differences and one final sum. DWT decomposes input image into four components namely LL, HL, LH, and HH. The lowest resolution level LL consists of the approximation part of the original image. Haar wavelet uses two types of filters. One is lowpass filter and the other is a high pass filter. The output of the lowpass filter is obtained by averaging the input, while the output of the high pass filter is obtained from the differences of the inputs [2]. Low pass filter contained more information than high pass filter, because most of signal energy is concentrated in low pass filter.

When an image is passed through a series of lowpass and high pass filters, DWT decomposes the image into sub brands of different resolutions [17]. Most of the energy of the image is concentrated in LL band. Hence modification of these low frequency sub bands would cost severe and unacceptable image degradation. So the watermark is not embedded in LL sub band. The good areas for watermark embedding are high frequency sub bands (vertical, horizontal and diagonal components). Human visual system is insensitive to these high frequencies bands and effective watermark embedding is achieved without being perceived by human visual system.

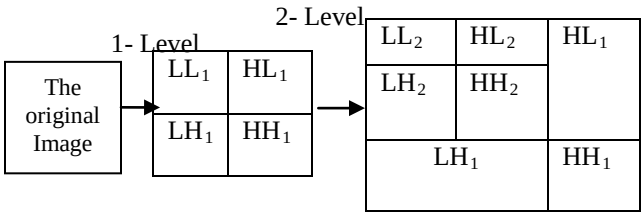

Figure (1):Discrete wavelet transformation

The basic idea of the DWT for a two dimensional images described as follows. An image is first decomposed into four parts of high, middle, and low frequency sub components (LL_1, HL_1, LH_1, and HH_1) by critically sub sampling horizontal and vertical channels using sub component filters. The sub components HL_1, LH_1 and HH_1 represent the finest scale wavelet coefficients. To obtain next level scaled wavelet components the sub component LL_1 is further decomposed and critically sub sampled. This process repeated several times, which is determined by the application at hand [3].

3. Back Propagation Neural Network(BPNN)

A neural network represents a highly parallelized dynamic system with a directed graph topology that can receive the output information by means of reaction of its state on the input nodes. The ensembles of interconnected artificial neurons generally organized into layers of fields include neural networks. The behavior of such ensembles varies greatly with changes in architectures as well as neuron signal functions [5]. Artificial neural networks are massively parallel adaptive networks of simple non liner computing elements called neurons which are intended to abstract and model some of the functionality of the human nervous system in an attempt to partially capture some of its computational strengths. Neural networks are classified as feed forward and feedback networks. Back propagation network is of feed forward type. In BPNN the errors are back propagated to the input level.

The back propagation network with input, hidden and output layers is shown in figure (2). Bias is applied to both the hidden units and output units. The bias is always set to 1. The aim of this network is to train the net to achieve the

balance between the ability to respond correctly to the input pattern that are used for training and the ability to provide good response to the input that are similar.

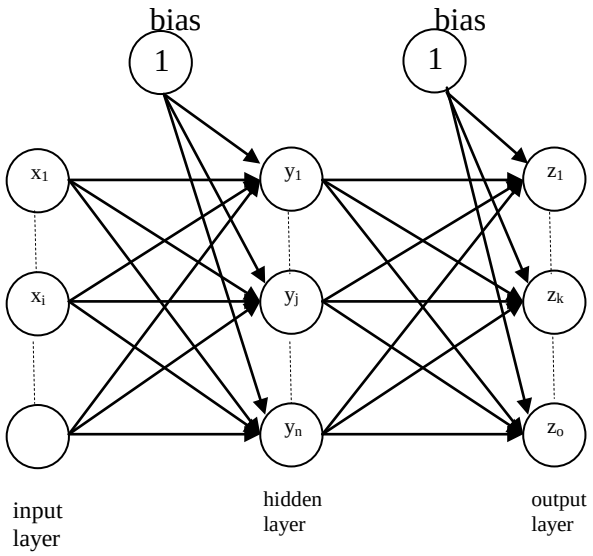

Figure (2): Back propagation neural network

The weight updating formula for BPNN is

$$W_{jk}(t+1) = W_{jk}(t) + \alpha\delta_k\ y_j + \mu\ [W_{jk}(t) - W_{jk}(t-1)] \quad \ldots (1)$$

$$V_{ij}(t+1) = V_{ij}(t) + \alpha\delta_j\ x_i + \mu\ [V_{ij}(t) - V_{ij}(t-1)] \quad \ldots (2)$$

Where

W_{jk} are weights between hidden layer and output layer

V_{ij} are weights between input layer and hidden layer

α is the learning rate parameter

μ is the momentum factor

t represents time

δ_k is the error signal between output and hidden layers

δ_j is the error signal between hidden and input layers

Back Neural Network has good nonlinear approximation ability. It can establish the relationship between original wavelet coefficients and watermarked wavelet coefficients by adjusting the network weights and bias before and after embedding watermark. Owning to the use of neural network, we can extract watermark without the original signal and thus reduce the limit in practical applications. Using the neural network based on BPNN algorithm will meet the problem: how to determine the optimal structure of BPNN namely how to choose the network layers and the number of neurons. If we can't select an appropriate network, it is difficult to significantly improve network performance, even if a large number of improvements have been made to the training algorithm.

The embedded technique of transform domain is proposed in this paper. And in order to improve the robustness, neural network is introduced, since it can fully approximate any complicated non-linear relationship. Thus the neural network model can well describe the relationship between selected wavelet packet coefficients and their neighborhood. For the multi-layer network, the number of input nodes and output nodes are determined by the problem itself. Choosing the size of network is mainly determining the size of nodes in hidden layer. The selection of nodes in hidden layer is very important for network training and studying. If hidden nodes are very few, the network will not have the necessary ability to learn and necessary information processing capabilities. Conversely, too many hidden nodes increases the complexity of network structure greatly, and is easier for neural network to fall into local minimum in the learning process. Meanwhile, It make the network learn very slowly. The common method of selecting is the trail and error method, generally based on experience to select the hidden layer of nodes, is very random. The empirical formula for determining the number of hidden nodes is

$$n = (om + cm + d)^{1/2} \quad \ldots\ldots (3)$$

Where n is the hidden nodes; m is the number of input nodes; o is the number of output nodes; c & d are the parameters to be determined. In general, the following posterior formula is used.

$$n = (om + 1.6799m + 0.9298)^{1/2} \ldots\ldots (4)$$

In this paper, m = 8, o = 1, $n \approx 4.8$,taking n = 5 ,The neural network has three layers, there are 8 nodes in input layer, 5 nodes in hidden layer, 1 node in output layer.

4. Watermark Embedding

The cover image is resized with 512x512 pixels, the R, G and B planes are separated and blue (B) plane is selected to embed watermark. The bitmap is selected as watermark and is resized to 64x64 pixels. The DWT is applied to blue plane of cover image and watermark is embedded in high and middle frequency components. The quantization levels selected as Q1=16 and Q2=6. The back propagation neural network is used to embed and extract watermark. The schematic diagram of 4-level wavelet transformation is shown in figure (3)

LL_4	HL_4			

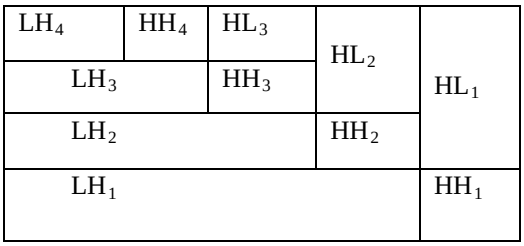

Figure (3): 4-level wavelet transformation

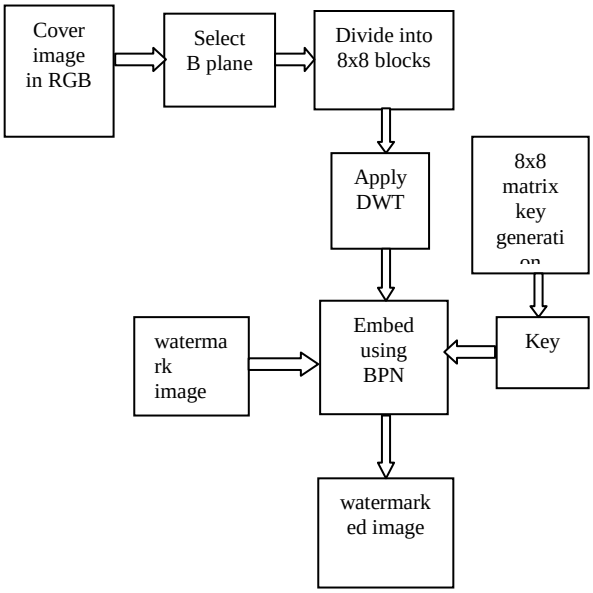

Figure (4): Watermark embedding.

Watermark Embedding Algorithm

Step 1. Read the color image of size NxN.

Step 2. Resize the color image to 512x512 pixels and use it as a cover image.

Step 3. Select the Blue (B) plane to embed the watermark.

Step 4. Read the image of size 64x64 as the watermark.

Step 5. The frequency subcomponents {HH1, HL1, LH1, {HH2, HL2, LH2}, {HH3, LH3, LL3}}} are obtained by computing the third level DWT of the Blue plane of RGB cover image.

Step 6. Select the beginning position of watermark using the secret key.

Step 7. Quantize the DWT coefficient $T_{(j+key)}$ by Q as the input to the BPNN, then get the output of BPNN.

Step 8. Embed the watermark using the following equation

$$T'_{(j+key)} = BPNN(round((T_{(j+key))}/Q) + x_j \quad \ldots.(5)$$

Where x_j is the random watermark sequence.

Step 9. Perform IDWT on each coefficient to get watermarked image.

5. Training Process of Neural Network

The training process is completed before embedding. After getting the coefficients from the watermark image , the relationship between the high frequency wavelet coefficients and the watermark can be established. The extra information is used to train the neural network to make it sure it must have the capability of memorizing the characteristics of relations between the watermarked image and the watermark. Sigmoid activation function is used in the hidden layer and linear activation function is used in the output layer. The performance and training states of neural network are shown in figure(5) and Figure(6).

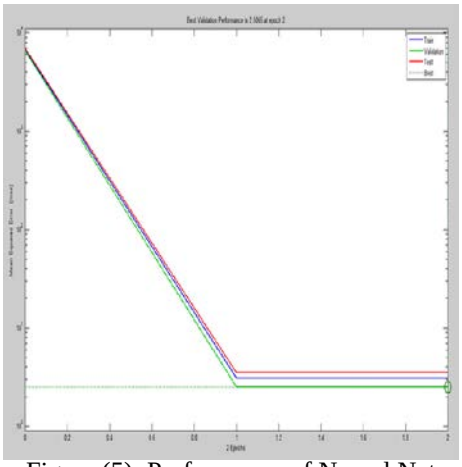

Figure (5): Performance of Neural Network.

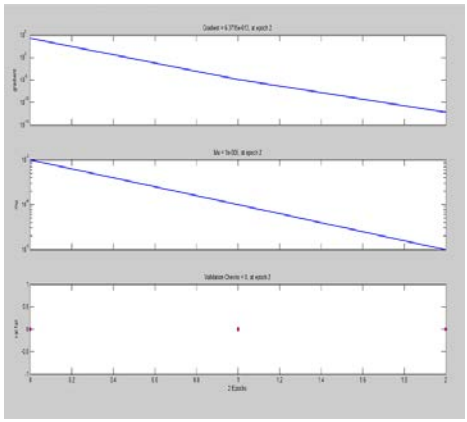

Figure (6): Training state of Neural Network

6. Watermark Extraction

The watermark extraction process is I that anti- process of watermark embedding. The trained neural network is used in the extraction process, because neural networks have

associative memory which can realize blind detection. The normalized correlation coefficient is used to detect the correlation between the original watermark and extracted watermark.

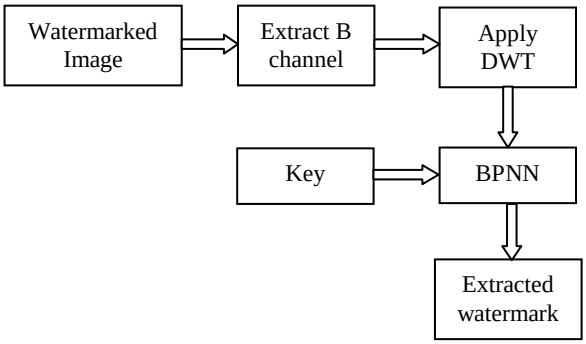

Figure (7): Watermark Extraction.

Watermark Extraction Algorithm

Step1. Transform the watermarked image by the DWT.

Step 2. Quantize the DWT coefficient T''(j) by Q, as the input of BPNN, then get the output of BPNN as round[$T''_{(j)}$/Q].

Step 3. Extract the watermark x' using the equation

$x'_i = T''(j) - BPNN(round(T''_{(j)}/Q))$ …. (6)

where j=1 to8.

Step 4. measure the NC of the extracted watermark x' and the original watermark x.

7. Experimental Results

The algorithm of watermark embedding and extraction are implemented using MATLAB. Pears image of size 256x256 is selected as the cover image. Gray scale bitmap image of size 64x64 Barbara is selected as the watermark. The PSNR of the watermarked image is calculated using the formula

$$PSNR = 10 \log_{10} \frac{(R * R)}{MSE} \quad \ldots\ldots \quad (7)$$

Where R= maximum fluctuation in the input image=511

$$MSE = \sum_{j=1}^{r} \sum_{k=1}^{c} \frac{[W(j,k) - W'(j,k)]^2}{rc} \quad \ldots\ldots \quad (8)$$

Where r = number of rows

c = number of columns

W(j,k) and W'(j,k) represent blue plane of cover image and watermarked image.

$$NC = \frac{\sum_j \sum_k W(j,k) * W'(j,k)}{\sum_j \sum_k W(j,k) * W(j,k)} \quad \ldots \quad (9)$$

The performance evaluation of the method is done by measuring imperceptibility and robustness. The normalized correlation coefficient (NC) is used to measure the similarity between the cover image and the watermarked image. Peak Signal-to-Noise Ratio (PSNR) is used to measure the imperceptibility of the watermarked image. The robustness of the watermarked image is tested by attacks such as JPEG compression, cropping, median filtering, salt & pepper noise attack, and rotation.

The Haar wavelet is used to decompose the image and the decomposition level is 3.The cover image of size 256x256 and watermark of size 64x64 are shown in figure(8). The watermarked image and extracted watermark without any attack are shown in figure (8).The cropping attacked image extracted watermark after cropping are shown in figure (9). The JPEG compression attacked image and extracted watermark after JPEG compression are shown in figure (9). The median filtering attacked image and extracted watermark after median filtering are shown in figure (10). The salt & pepper noise attacked image and Extracted watermark after salt & pepper noise attack are shown in Figure (10). The rotation attacked image and extracted watermark after rotation attack are shown in figure (11). The PSNR of the watermarked image after all the attacks is higher than 51, from which we can say that the imperceptibility is excellent.

Figure (8) : Cover Image, Watermark, Watermarked Image, and Extracted watermark without any attack

Figure (9) : Cropped Image, Extracted Watermark after Cropping, JPEG Compressed Image, and Extracted Watermark after Compression.

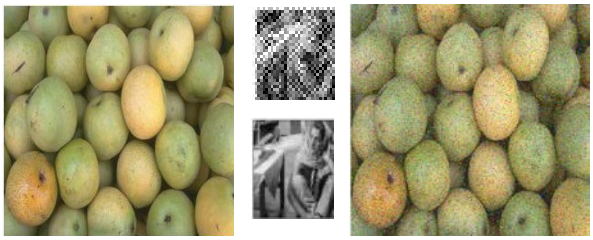

Figure (10) : Median Filtering attacked Image, Extracted watermark, salt & Pepper Noise attacked Image, and Extracted Watermark after Salt & Pepper Noise attack.

Figure (11) : Rotation attacked Image, and Extracted Watermark after Rotation attack.

Table 1 : Comparison of various attacks

.

Type of Attack	Intensity	MSE	PSNR	NC
Watermarked image		0.9102	48.5396	0..9981
cropping	10%	0.4541	51.5593	0.9645
	20%	0.4678	51.4304	0.9639
	30%	0.4609	51.4944	0.9177
	40%	0.4502	51.5968	0.9081
JPEG Compression	Q=20	0.4570	51.5313	0.8347
Median Filtering	–	0.4424	51.6728	0.8054
Salt& Pepper Noise	2%	0.6238	50.1805	0.9955
	5%	0.6208	50.2009	0.9954
	10%	0.6201	50.2061	0.9953
	20%	06199	50.2078	0.9951
Rotation	5^o	0.6218	50.1941	0.9952
	10^o	0.6243	50.1771	0.9951
	15^o	0.6208	50.2009	0.9950
	20^o	0.6468	50.0299	0.9949

7. Conclusion

In this paper the watermark is embedded into the blue plane of the color image using DWT and BPNN. Algorithm is robust to Salt & Pepper noise attack, cropping and rotation but weak to JPEG compression, and median filtering attacks. The PSNR is better than the methods proposed in [15] and [2]. Robustness to JPEG Compression, and median filtering attacks can be improved by proper training of neural network and proper selection of coefficients .Robustness can also be improved by applying Fuzzy Logic approach. This algorithm can also be applied to video images.

References

[1] Vijaya.k.Ahire, and VIvek Kshirsagar, "Robust watermarking Scheme Based on Discrete wavelet Transform (DWT) and discrete Cosine Transform (DCT) for Copyright Protection of Digital Images" IJCSNS International Journal of Computer science and Network Security, Vol. 11, No. 8,August,2011, pp. 208-213.

[2] Yanhong Zhang , " Blind Watermark Algorithm Based on HVS and RBF Neural Network in DWT Domain", WSEAS TRANSACTIONS on COMPUTERS, Issue 1, Volume 8, January 2009, pp. 174-183.

[3] Divyakant T. Meva& Amit D .Kothari, " Adoption of Neural Network Approach in Steganography and Digital Watermarking for Covert Communication and Copyright Protection", International journal of Information Technology and Knowledge Management, July-December 2011, Volume 4, No. 2, pp. 527-529.

[4] N.Chenthalir Indra and Dr. E . Ramraj, " Fine Facet Digital Watermark (FFDW) Mining From The Color Image Using Neural Networks", International Journal of Advanced Computer Science and Applications, special Issue on Image Processing and Analysis, pp. 70-74.

[5] Bibi Isac and V. Santhi, " A Study on Digital Image and Video Watermarking Schemes using Neural Networks", International Jounal of Computer Applications, Vol. 12, No. 9, January 2011, pp. 1-6.

[6] Chen Yongqinang, Zhang Yanqing, and Peng Lihua, " A DWT Domain Image Watermarking Scheme Using Genetic Algorithm and Synergetic Neural Network", Academy Publisher,2009, pp. 298-301.

[7] Samesh Oueslati, et al, " Adaptive Image Watermarking Scheme based on Neural Network", international Journal of Engineering Science and Technology, Vol. 3, No. 1, Jan 2011, pp. 748-756.

[8] Maher EL` ARBI, Chokri BEN AMAR and Henri NICOLAS, "Video watermarking based on Neural Networks", 2006 IEEE transactions, pp. 1577-1580.

[9] Summrina Kanwal Wajid, M. Arfan Jaffar, et al, " Robust and Imperceptible Image Watermarking using Full Counter propagation Neural Networks", 2009 International Conference on Machine Learning and Computing, IPCSIT Vol. 3 (2011), pp. 385-391.

[10] Cheng-Ri Piao, Seunghwa Beack, Dong-Min Woo, and Seung-Soo Han, " A Blind Watermarking algorithm Based

on HVS and RBF Neural Network for Digital Image", Springer-Verlag Berlin Heidellberg 2006, pp. 493-496.
[11] Pao-Ta Yu, Hung-Hsu Tsai, and Jyh-Shyan Lin, "Digital Watermarking Based On neural networks for color images", signal Processing 81 (2001), pp. 663-671.
[12] Yonghong Chen and jiancong Chen, "A Novel Blind watermarking Scheme Based on Neural Networks for Image", 2010 IEEE Transactions, pp. 548-552.
[13] He Xu, Chang Shujuan , " An Adaptive Image Watermarking Algorithm based on Neural Network", IEEE Computer Society,2011 ,4th International Conference on Intelligent Computation Technology and automation, pp. 408-411.
[14] K. Yogalakshmi and R. Kanchana, " Blind watermarking scheme for digital images", International journal of technology and Engineering systems- Jan-March 2011, Vol 2, No. 3, pp 276-282.
[15] Nagaraj. v , Dharwadkar, B. B . Amberker, " An Efficient non blind watermarking scheme for colour images using discrete wavelet transformation", International journal of computer applications, Vol. 2, No. 3, May 2010, pp 60-66.
[16] Baisa L.Gunjal and R.RManthalkar, "An overview of transform domain robust digital image watermarking algorithms", Journal of Engineering trends in computing and information sciences, Vol. 2, No. 1, 2010-2011, pp 37-42.
[17] Baisa L.Gunjal and R.RManthalkar, "An overview of transform domain robust digital image watermarking algorithms", Journal of Engineering trends in computing and information sciences, Vol. 2, No. 1, 2010-2011, pp 37-42.

Nallagarla Ramamurthy received his B.Tech. and M.Tech.from S.V.University in 1998 and 2006, respectively.During the period 2000-2006 he worked as an Asst. Professor in Sree Vidyanikethan Engg Cpllege, Tirupati., INDIA. Now he is pursuing Ph.D from JNTUA, Anantapur, INDIA.

S. Varadarajan did his M.Tech from NIT, Warangal, India and Ph.D from Sri Venkateswara University. His specializations include Signal Processing and digital Communications. He is working as Associate Professor in the department of Electrical and Electronics Engineering, Sri Venkateswara University College of Engineering, Tirupati, India. He is a fellow of Institution of Electronics and Telecommunication Engineers, India and member of IEEE.