# A New Scheme of Neural Network and DCT-Domain Based Digital Watermarking

Mya Thidar Kyaw, and Kyi Soe

***Abstract*—**Digital Watermarking is one of the data hiding technique, has been popular in today multimedia era to prevent and control copyright protection. In this paper, a new blind scheme of digital watermarking is proposed by combining block based DCT domain approach and Neural Network. DCT domain based is used in watermark embedding to achieve better imperceptibility and Neural Network is applied in watermark extraction to improve watermark retrieval performance and achieve more robustness. By combining DCT transform based and Neural Network, the proposed scheme is intended to improve digital watermarking performance. Experimental results will be show and proof the better performances on different images and more robustness against on various attacks.

***Keywords*—**Digital watermarking, Discrete Cosine Transform (DCT) domain, Neural Network.

## I. Introduction

IN our current digital era, the rapidly development of multimedia communication systems and the explosion of the fastest communication has discouraged and damped the multimedia content providers such as authors, publishers to grant the distribution of their document on the network environment. At this situation, one considerable fact is the intellectual property authentication [1]. Especially, digital media data such as image, video and audio can be easily copied and then distributed again and again over the network environments. Hence, the intellectual property authentication is very important for the digital media. In order to solve and consider the problem of the intellectual property authentication, the use of digital watermarking is becoming popular. Actually, digital watermarking is a technique in which secret information called watermark is embedded to a particular digital media. Here, the watermark may be a logo or an image or etc which can be proved who is right owner.

In the recent years, many watermarking methods for digital images have been proposed. Watermarking techniques are generally categorized into two branches, spatial domain and transform domain techniques. While the spatial domain techniques are having least complexity and high payload they cannot withstand in frequency attack such as low pass filtering. The widely accepted schemes for watermarking are in transform domains such as DCT, DFT and DWT [2].

In the frequency domain based approach, one of the first algorithms presented by Cox et al. (1997) used global DCT approach to embed a robust watermark in the perceptually significant portion of the Human Visual System (HVS) [3]. The next work of DCT is block based method and published in 2000 by Huang, J, Shi, YQ and Shi [4]. In this work, an image to be embedded is divided into non-overlap blocks and then they are transformed. In each block, transform coefficients which have large perceptual capacity are selected as DC components to be embedded. Another next publication is "Digital Watermarking based DCT and JPEG model" by M. A. Suhail and M. S. Obaidat in 2003 [5]. The work proposed digital watermarking algorithm based on discrete cosine transformed (DCT) coefficients and image segmentation. Another one for the DCT and DWT transformed approaches is the publication of Zhao et al. in 2004 [6]. They use the DCT domain for watermark generation and DWT domain for watermark insertion.

Furthermore, the recognition power of neural network technology was used in watermarking. In 1999, Yan *et al* [7] proposed a blind digital watermarking algorithm using feed forward neural network. In this algorithm, discrete wavelet transform (DWT) domain was used for HVS model. Radial basis function (RBF) neural net was implemented while watermark embedding and extraction. HVS model was used to determine watermark insertion strength. The neural networks almost exactly recover the watermarking signals from the watermarked images after training and learning. However, it cannot be enough against in many attacks, especially in JPEG. One of next research was the publication of Prof. A. Bansal *et al* [8] in which Full Counterpropagation Neural Network (FCNN) was used in the concept of embedding watermark into synapses of neural net to improve the PSNR of cover image and prevent the cover image quality degradation. The FCNN technique was one of the successful watermarking techniques with better time complexity, higher capacity and higher PSNR. After that a neural net based watermarking technique using Back Propagation Neural Net (BPNN) and Singular Value Decomposition (SVD) was published by Swanirbhar et al [9] in 2010. It was unlike previous works, error control coding (ECC) and artificial neural networks (ANN) was used for the authentication purposes. The ECC and ANN can be increase the robustness of the method against malicious attacks. It can achieve higher imperceptibility and better recovery

Mya Thidar Kyaw irstname, Information and Communication Technology, University of Technology (Yatanarpon Cyber City) Pyin Oo Lwin, Myanmar. (email: myathidarkyawmin@gmail.com).

Dr. Kyi Soe, Registrar of University of Technology (Yatanarpon Cyber City), Pyin Oo Lwin, Myanmar. (email: kyisoe 72@gmail.com)

http://dx.doi.org/10.15242/IIE.E0314147

performance but it cannot be over on the JPEG attack in entirely enough. Next research was adaptive neural net watermarking scheme [10]. In this scheme, block based DCT domain approach was used. In the embedding process, watermark was inserted in the middle frequency components of DCT transformed cover image by the controlling of Neural Net weights. The watermark can be extracted by performing the inverse process of embedding the watermark. The first step of the process is to transform the watermarked image and original image into DCT domain respectively. The embedded coefficients are subtracted and divided by the weights, to extract the corrupted watermark. It can distinctly against JPEG and other attacks but it was not a blind watermarking scheme as the need of original image in the extraction process. Another review journal was published by D. T. Meva *et al* [11]. It presented that the neural network can be used not only in digital watermarking but also in steganography to prevent illegal copyright protection. It also discussed so many types of attacks usually occurred in digital watermarking and steganography and also presented the possible ways to prevent them with the help of neural net based techniques. After that, Neha Bansal and Pooja Pathak published applications of Neural Network in watermarking [12]. In their work, different neural network based approaches were discussed and also describe how the approaches can be used based on their applications for embedding and extracting components of watermarking.

In this paper, DCT transform domain is used to embed watermark and the recognition power of neural network is used for watermark recovery. This paper is structured as follows. Theoretical Issue of Neural Network used in the proposed method and digital watermarking frequency domain are studied in the next section. In section 3, our proposed scheme is briefly described. In section 4, experimental results of the proposed scheme are presented by their performances and robustness depended on various attacks. Finally, some conclusion and further work are drawn in section.

## II. Theoretical Issue

There are mainly two parts in every digital watermarking technique. These two parts are embedding in which watermark is inserted and watermark extraction in which watermark is recovered.

In the frequency domain (Transform domain) based approach, watermarking method is a transform method in which it is need to consider suitable frequency component to embed as watermark energy. Before embedding, host image is needed to transform by using some invertible transformations like discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) and etc. It is because Embedding of a watermark is made by modifications of the transform coefficients, accordingly to the corresponding watermark bit or its spectrum. Finally, the inverse transform is applied to obtain result watermarked image. After inverse transformation, watermark pixels are irregularly distributed over the image pixels. Therefore, detection or manipulation of watermark is more difficult. The watermark signal is usually applied to the middle frequencies of the host image because modifications in the low frequencies can cause visible changes and reduce imperceptibility, and compression and filtering effect the high frequency of the transform and destroy the watermark. Hence, these methods are more complicated and require more computational power than spatial domain based approach. The following figures describe the embedding and extraction of that domain.

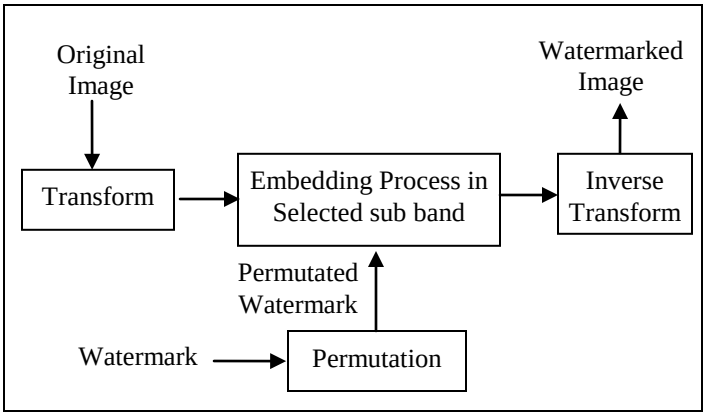



Fig.1Watermark Embedding Process in Frequency Domain

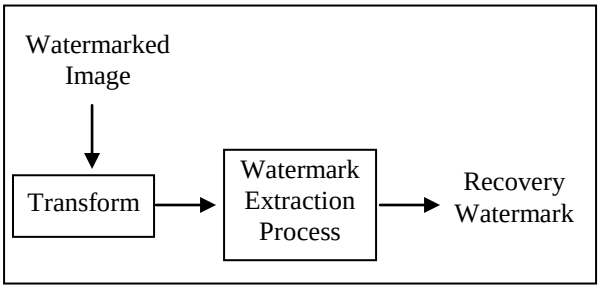



Fig. 2 Watermark Extraction Process in Frequency Domain

In DCT domain based watermarking, there can be classified into *Global* DCT watermarking and *Block based* DCT watermarking [3]. In the Global DCT, the whole original image is transformed to be embedded and then retransformed to produce watermarked. In the Block based, the cover image is divided into block (sub image) before embedding. Then, each block is transformed and embedded. Recombination of the blocks is needed to produce watermarked in there. However, embedding and extraction procedures are generally the same as the figure1 and figure2. The frequency domain transform based algorithms are slow compared with spatial domain based. However, they can give better perceptual transparency.

In not very soon, Neural Network algorithm are used in both frequency domain based digital image watermarking and spatial domain based approach. It is because the recognition power of Neural Network technology is very useful in digital watermarking as like as in other fields. Generally, data of a host image is trained and recognized with Neural Net and after that they are embedded as usual. The embedding process using

Neural Net is shown in figure 3.

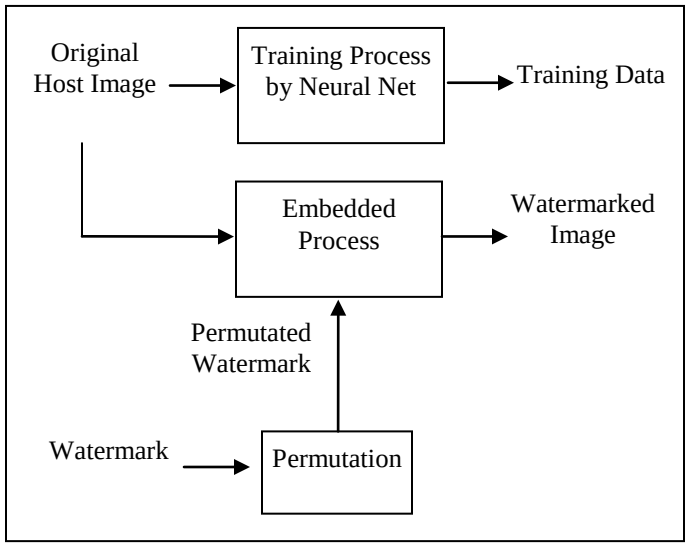



Fig.3 Watermark Embedding Process using Neural Network

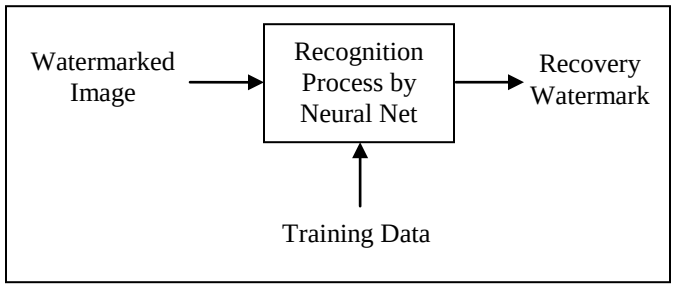



Fig.4 Watermark Extraction Process using Neural Network

In the extraction section, the Neural Net was reused to recognized unmodified data. If a data was recognized by the net, the watermark bit with respected to the data is '1', otherwise '0'. By this way, the embedded watermark can be retrieved by using neural net. The figures 3 and 4 can be illustrated how the Neural Network used in digital watermarking.

By combining transformed based and Neural Network, there are not only better in imperceptibility but also received better recovery performance. However, training data must be used in recovery process so it cannot be called a blind watermarking scheme.

## III. Proposed System

The proposed method is the combination technique of DCT transformed domain and Neural Network. DCT transformed domain is used for watermark embedding and Neural Network are used for watermark retrieval. The proposed scheme can be described as the following three sections.

### *A. Neural Network Design and Training*

In our proposed method, Neural Network is designed with three layers, one input layer, one hidden layer and one output layer. In input layer, there are two neurons which can receive two inputs in one time. There are 20 neurons in hidden layers and nine output neurons.

There are some assumptions we used for the proposed watermarking scheme. Before embedding process, original host image is transformed with DCT. From the DCT transformed image, mid band area is used as watermark embedded media. In the watermark embedded media, there are two sign frequency components, positive sign and negative. In our proposed method, unlike other approaches, the watermark embedded media components are not directly used as training data because of long training time and their values change in the retrieval process. However, their sign values are not change in the retrieval process and robustness experiments. Hence, we do not focus on frequency component values but emphasize on sign values to be embedded.

According to the assumption, the possible signs of the frequency components are negative, positive and zero. Therefore, we take our training data set as 2 x 9 matrix composed of -1's, 0's and 1's.

To improve the imperceptibility performance (PSNR), we take next assumption. When the positive occurrence in embedded media is larger, the media is assumed as positive media and change all frequency component values are positive and then negative watermark energy is used to be embedded on that media. When negative occurrence is larger, all frequency components are changed into negative and positive watermark energy is used to be embedded. According to this assumption, in the positive media, watermark signals are inserted in all negative frequency components. Similarly, in the negative media, all positive frequency components are watermark signals. By using this assumption to recover precise watermark signal, we have to take two target values for the two media in training process and save two corresponding nets depending on each target. The input matrix and target values are as follow.

```
[0 0; 0 1; 1 0; 1 1; -1 1; 1 -1; 0 -1; -1 0; -1 -1];
```

Input matrix

```
[1 0 0 0 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0;
 0 0 0 0 1 0 0 0 0;
 0 0 0 0 0 1 0 0 0;
 0 0 0 0 0 0 1 0 0;
 0 0 0 0 0 0 0 1 0;
 0 0 0 0 0 0 0 0 1];
```

Target matrix for negative media

```
[1 0 0 0 0 0 0 0 0;
 0 1 0 0 0 0 0 0 0;
 0 0 1 0 0 0 0 0 0;
 0 0 0 1 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0;
 0 0 0 0 0 0 0 0 0];
```

Target matrix for positive media

Fig. 5 Description of input matrix and two target matrixes

In our Net design, log-sigmoid transfer function is used in input layer, tan-sigmoid transfer function is in hidden layer and gradient descent with adaptive learning rate backpropagation algorithm is used as training algorithm. The Neural Network design can be described as follow.

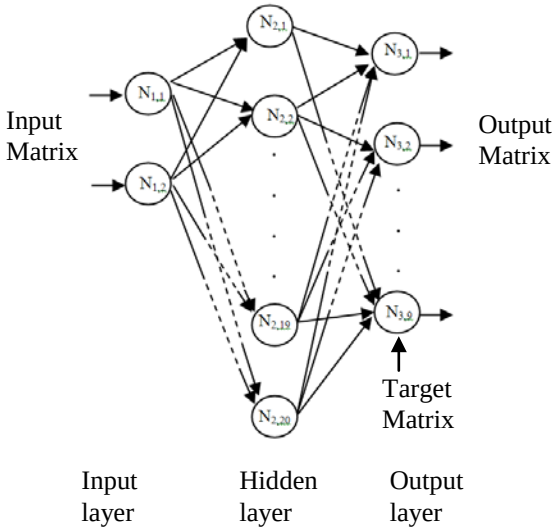



Fig. 6 Design of Neural Network for proposed scheme

*B. Watermark embedding in DCT*

DCT domain watermarking can be classified into *Global* DCT watermarking and *Block based* DCT watermarking [3]. Now, the proposed technique is one of the Block based DCT. Embedding procedures are as followed.

1. Input image is divided into 8x8 sub images (blocks).
2. Each sub image is transformed with DCT.
3. Select minimum high frequency component in the transformed image and used as watermark energy. Eight mid-band frequency components are used as watermark embedded media which is shown as follow.

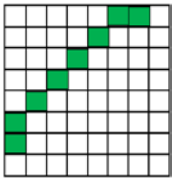


Fig.7 Description of eight frequency components used for watermark media in mid-band of a sub image

4. Count the number of positive and negative occurrence in the embedded media. If positive occurrence is larger, all embedded media frequency components are changed into positive values or all are changed into negative values.
5. If media is positive, negative watermark energy is embedded. If the media is negative, positive watermark energy is used.
6. Watermark image is permutated with a key and convert as one dimension arrays and then the array is divided into 8 elements sub arrays.
7. By figure 7, watermark energy (minimum high frequency component) is inserted in the mid- band frequency of each sub image. In the mid-band frequency components of a sub image, the watermark energy is replaced whenever the watermark bit is 0. If the bit is 1, there is no change in mid-band. The sign of embedded watermark energy has to be used according to the step 4 and 5.
8. After inserting the watermark energy in mid-band of sub image, it is inverse transformed to spatial domain. All retransformed sub images are recombined to produce watermarked image.

*C. Watermark Extraction in DCT*

In the extraction process, watermarked image is divided into 8x8 sub images and then the sub images are transformed with DCT. In embedded media (eight frequency components) of each sub image, each pair (two frequency components) of the media frequency components is normalized and rounded. By this way, after the normalization and round process, each media frequency component pairs are all positive (1's) or all zeros (0's) or one of the pair is 1and another is 0 according to the modification of watermark energy in embedding process. After that, the number of sign values of the embedded media is counted. If positive sign is larger, positive net is used in recovery process or negative net is used. Each pair of embedded media is put into the input of Neural Network to recover watermark bits.

By the previous Network design and training data,

- For the positive net, in each input pair, when we put one negative or both negative values to the input of Neural Network, we recover watermark bit, 0. For other inputs, we recover watermark bit, 1's.
- For the negative net, in each input pair, when we put one negative or both negative values to the input of Neural Network, we recover watermark bit, 1's. For other inputs, we recover watermark bit, 0's.

By this way, embedded watermark is extracted from the watermarked image by pair and pair from block by block. The extraction performance and robustness of the proposed method can be seen in next section.

## IV. Experimental Setting & Results

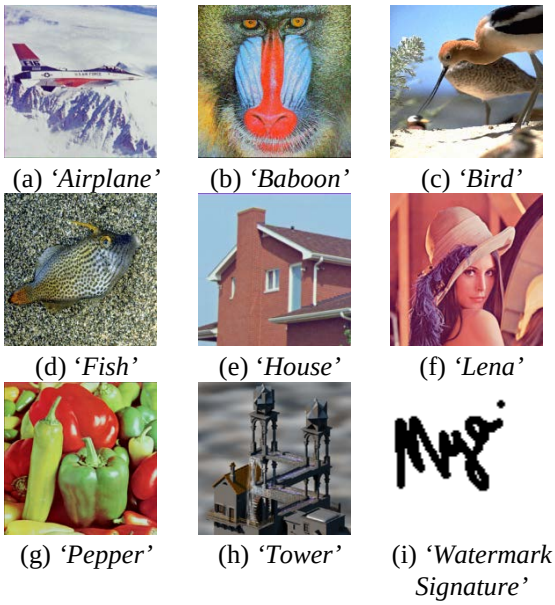
In this section, the detail performance analyses and the robustness against various attacks of the two transformed techniques are presented.

*A. Experimental Setting*

In the experiments, we used eight standard color images that are different characteristics, 'Airplane', 'Baboon', 'Bird', 'Fish', 'House', 'Lena', Pepper', and 'Tower' as the original host images. A two colors black & white image containing a sign was used as a watermark signal and shown in the following Figure.

To measure the quality of the watermarked image the quality of the retrieved watermark, Peak Signal to Noise Ratio (PSNR) and Normal Correlation (NC) are evaluated and determined by equation (5) and (6).

$$PSNR\,(\mathrm{dB}) = 20\log_{10}\frac{255\sqrt{3MN}}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(B'(i,j)-B(i,j))^2}} \qquad (1)$$



(a) *'Airplane'* (b) *'Baboon'* (c) *'Bird'*

(d) *'Fish'* (e) *'House'* (f) *'Lena'*

(g) *'Pepper'* (h) *'Tower'* (i) *'Watermark Signature'*

Fig.8:Testing images and watermark

$$NC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j)w'(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} w(i,j)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N} w'(i,j)^2}} \quad (2)$$

From these equations, M and N are the numbers of row and column of the images; w(i,j) and w'(i,j) are the original watermark bit and the retrieved watermark bit at coordinate (i,j). Note that higher NC value, the retrieved watermark will be more correctly.

*C.Performance Comparisons*

To measure the retrieval performance of the proposed methods, average NC values are evaluated from various images with the nearly the same PSNR values. The evaluation results are described as the following table.

TABLE I
RECOVERY PERFORMANCE OF PERFORMANCE OF PROPOSED SCHEME

| Images | Recovery Performance | |
|---|---|---|
| | PSNR | NC |
| Lena | 46.09381 | 0.925883 |
| Baboon | 45.72594 | 0.958418 |
| Bird | 45.13921 | 0.924608 |
| House | 44.98003 | 0.936041 |
| Pepper | 45.01686 | 0.937993 |
| Tower | 44.86638 | 0.976817 |
| Fish | 42.74961 | 0.867583 |
| Average | 44.93883 | 0.932478 |

We will continue analyze and compare the performance against image processing attacks such as JPEG compression, blurring, contrasting and sharpening, noises such as Gaussian noise and salt and pepper noise, and finally evaluate performance on geometrical attacks, image cropping and resizing. In all experiments against on the attacks such as JPEG, Blurring, Contrast, Brightness, Sharpening, Gaussian noise, Salt & Pepper noise, Cropping and Resizing, the values of performance are estimated in *PSNR* value of 40 ± 0.01 dB. The performance comparisons are expressed as following table.

TABLE II
AVERAGE NC VALUES OBTAINED FROM VARIOUS ATTACKS AT A GIVEN SIGNAL STRENGTH

| No | Type of attack | Strength | NC of DCT |
|---|---|---|---|
| 1 | JPEG | 90% | 0.85635 |
| 2 | Blurring | 20% of image pixel | 0.93486 |
| 3 | Contrast | 160% | 0.96537 |
| 4 | Brightness | 100% | 0.96340 |
| 5 | Sharpening | 90% | 0.95670 |
| 6 | Gaussian noise | 0.01 variance | 0.86155 |
| 7 | Salt & Pepper | 0.06 density | 0.92603 |
| 8 | Cropping | 30% | 0.90719 |
| 9 | Resizing | 75% | 0.89540 |

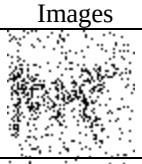
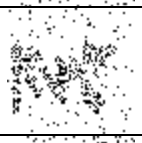
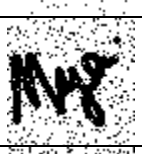
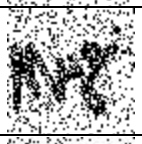
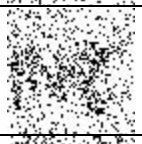
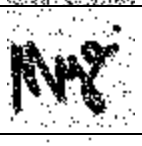
| Types of Attack | Recovery Images |
|---|---|
| Salt & Pepper 0.03 density |  |
| Gaussian variance = 0.01 |  |
| Cropping 30% |  |
| Resizing 0.75 of original image |  |
| JPEG 100% |  |
| Blurring 20% of image pixel |  |
| Brightness 100% |  |
| Contrast 160% |  |

Fig. 9 Recovery watermark of DCT in various attacks

## V. Conclusion

In this paper, we have presented a new combined scheme of block based DCT and Neural Network watermarking. To improve imperceptibility, DCT block based transformed is used and recognition power of Neural Net is for extraction performance. Experimental results point out better performances and robustnesses of our proposed scheme. Although frequency domain based digital watermarking techniques are usually better in perceptibility but weak in against geometrical attacks, the proposed techniques can rather against the geometrical attacks. Using Neural Network is one of the interesting approaches in digital watermark so our future research will continue to intelligence based digital watermarking.

## References


[1] T.K.Tewari and V.Saxena, "An Improved and Robust DCT based Digital Image Watermarking Scheme," Internal Jurnal of Computer Application, vol. 3, pp. 272-277, June 2010.

[2] I.J. Cox, M.L. Miller, and J.A. Bloom, "Digital wateramrking and Steganography," Morgan Kaufmann Publishers, 2002.

[3] I.J Cox, J. Kilian, F.T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia" in IEEE Transactions on Image Processing, vol. 6, no. 12, pp:1673 -1687, Dec.1997. http://dx.doi.org/10.1109/83.650120

[4] Huang, J, Shi, YQ & Shi, "Embedding Image Watermarks in DC Components", IEEE Transactions on Circuits and System for Video Technology, vol. 10, no. 6, pp. 974-979, 2000.

[5] M. A. Suhail and M. S. Obaidat, "Digital Watermarking based DCT and JPEG model," IEEE Trans. instrumentation and measurement, vol. 52, no. 5, pp.1640-1647, October 2003. http://dx.doi.org/10.1109/TIM.2003.817155

[6] Zhao, Y., Campisi, P., Kundur, D., "Dual Domain Watermarking for Authentication and Compression of Cultural Heritage Images", in *IEEE Transactions on Image Processing*, vol. 13, no. 3, pp. 430-448, March 2004. http://dx.doi.org/10.1109/TIP.2003.821552

[7] Y. H. Zhang, "A Blind Digital Watermarking Algorithm Based on HVS and RBF Neural Network," Proceeding of the 3rd WSEAS International Conference on Computer Engineering and Applications, vol. 09, no. 2, pp. 202-205, February 2002.

[8] Prof. A. Bansal and S. S. Bhadauria, "A Nobel Approach using Full Counterpropagation Neural Network for Watermarking", International Journal on Computer Sceience and Engineering (IJCSE), vol. 02, no. 02, pp. 289-296, 2010.

[9] S. Majumder, T. S. Das and S. K. Sarkar, "BPNN and SVD based Watermarking Scheme," Int. J. of Recent Trends in Engineering and Technology, vol. 4, no. 1, pp. 44-47, Nov. 2010.

[10] S. Oueslati, A. Cheris and B. Solaimane, "Adaptive Image Watermarking Scheme Based on Neural Network International Journal of Engineering Science and Technology (IJEST), vol. 3, no. 1, pp. 748-756, Jan. 2011.

[11] D. T. Meva and A. D. Kothari , "Adoption of Neural Network Approach in Steganography and Digital Watermarking for Convert Communication and Copyright Protection," International Journal of Information Technology and Knowledge Management, Vol.4, no. 2, pp. 527-529, July. 2011.

[12] N. Bansal and P. Pathak, "A Review of Applications of Neural Network in Digital Watermarking," Proceedings published in International Journal of Computer Applications (IJCA), Vol.2, no. 1, pp. 127-132, December,2011.