Effect of Various Attacks on Watermarked Images

Nallagarla.Ramamurthy[#1] and Dr.S.Varadarajan[*2]

[#]Research Scholar, JNTUA, Anantapur, INDIA

*Professor, Dept. of ECE, S.V. University College of Eng. Tirupati, INDIA

***Abstract*— Watermarked images are affected by various attacks such as cropping, salt&pepper noise and rotation. These attacks destroy the inserted watermark, so that the copyright problem may arise. The effect of these attacks can be reduced by properly inserting the watermark with effective algorithm. In this paper, a blind transform domain based algorithm using Radial Basis Function Neural Network is introduced. The proposed algorithm is robust to cropping, salt&pepper noise and rotation attacks compared to other algorithms.**

***Keywords*— Watermark, Cropping, Salt&Pepper Noise, Rotation, Radial Basis Function Neural Network.**

I. INTRODUCTION

Due to the rapid and massive development of multimedia and the widespread use of the Internet, there is a need for efficient, powerful and effective copyright protection techniques. A variety of image watermarking methods have been proposed, where most of them are based on the spatial domain or the transform domain. However, in recent years, several image watermarking techniques based on the transform domain are developed [1].

Digital watermarking schemes are typically classified into three categories. Private watermarking which requires the prior knowledge of the original information and secret keys at the receiver. Semi private or semi blind watermarking where the watermark information and secret keys must be available at the receiver. Public or blind watermarking where the receiver must only know the secret keys [2]. The robustness of private watermarking schemes is high to endure signal processing attacks. However, they are not feasible in real applications, such as DVD copy protection where the original information may not be available for watermark detection. On the other hand, semi-blind and blind watermarking schemes are more feasible in that situation [3]. However, they have lower robustness than the private watermarking schemes [4]. In general, the requirements of a watermarking system fall into three categories: robustness, visibility, and capacity. Robustness refers to the fact that the watermark must survive against attacks from potential pirates. Visibility refers to the requirement that the watermark be imperceptible to the eye. Capacity refers to the amount of information that the watermark must carry. Embedding a watermark logo typically amounts to a tradeoff occurring between robustness visibility and capacity.

Reference [5] 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. Reference [6] presents an adaptive image watermarking algorithm which is based on synthetic human visual system characteristic and associative memory function of neural network. Reference [7] proposed a system SBS-SOM a neural network algorithm was trained to generate digital watermark values from the image. Reference [8] 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 grey image. Reference [9] presents an adaptive image watermarking scheme based on Full Counter Propagation Neural Network. Reference [10] proposed a novel approach to neural network watermarking for uncompressed video in the wavelet domain. Summrina Kanwal Wajid et al [11] proposed the robust and imperceptible image watermarking using Full Counter Propagation Neural Network, with lesser complexity and easy apprehension. Cheng-Ri. Piao et al [12] proposed a new blind watermark embedding/extracting algorithm using the RBF Neural Network. Pao-Ta.Yu et al [13] developed watermarking techniques, integrating both colour image processing and cryptography, to achieve content protection and authentication for colour images.

In this paper a blind watermarking scheme to embed the watermark into the blue plane of the cover image is presented. This technique is based on training Radial Basis Function Neural Network (RBFN) in discrete wavelet transform domain. While embedding the watermark, a secrete key is generated to determine the beginning of the watermark location. RBFN 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 cropping, rotation and salt& pepper noise.

II. DISCRETE WAVELET TRANSFORM

The Discrete Wavelet Transform (DWT) 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 [7]. 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 low-pass filter and the other is a high pass filter. The output of the low-pass filter is obtained by averaging the input, while the output of the high pass filter is obtained from the differences of the inputs [5]. 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 low-pass and high pass filters, DWT decomposes the image into sub brands of different resolutions [14]. 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. The basic idea of the DWT for 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 to LL_2, HL_2, LH_2, and HH_2. This process repeated several times, which is determined by the application at hand [15].

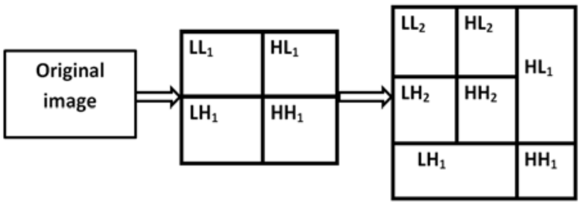


Figure (1): Discrete Wavelet Transform

III. RADIAL BASIS FUNCTION NETWORK(RBFN)

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. Radial Basis Function Neural Network is of feed forward type. The radial basis function neural network has universal approximation capability and has been successfully applied to many signal and image processing problems. A RBF network is a fully connected network and generally is used as a classification tool. In a RBF model, the layer from input nodes to hidden neurons is unsupervised and the layer from hidden neurons to output nodes is supervised. The transformation from the input to the hidden space is nonlinear, and the transformation from the hidden to the output space is linear. The hidden neurons provide a set of 'functions' that constitute an arbitrary 'basis' for the input patterns. These are the functions known as radial basis functions. Through careful design, it is possible to reduce a pattern in a high-dimensional space at input units to a low-dimensional space at hidden units. RBF neural network makes use of weighted sum of the Gaussian basis function with diagonal covariance matrix as posterior probability of training data [16].

The realization of mapping and function approximation is a common feature of the feed-forward network. RBF network with a strong input and output mapping function, and was proved the optimal network to complete the mapping function in theory. RBF neural network has been a great success in many applications, especially in the respect of Pattern Classification and function approximation and classification. for its simple network structure, the rapid process of training, the good ability of promotion, and many other advantages. Therefore, in this paper, the RBFN trained to simulate the procedure of inverse image quantification to obtain the quantitative characteristics of original image. After the watermark embedded in, neural network is used to eliminate effectively the interference from quantification procedure for image. Well trained RBF network is used to extract the watermark, to ensure watermark robustness.

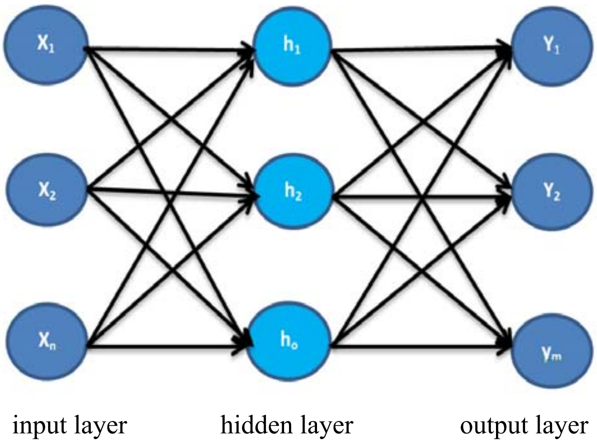


Figure (2): Radial Basis Function Neural Network

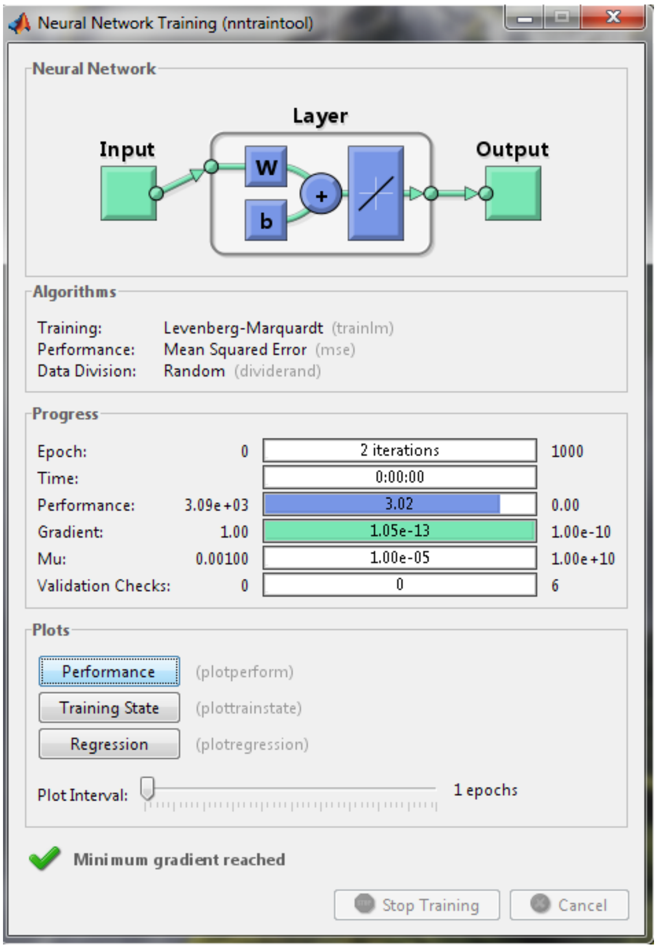
The output of the hidden layer is given by the following equation.

$$h_j(x) = exp\ (-\sum\{(x-\mu_j)^2 /2\sigma^2\})\text{-------- } (1)$$

The output of the Network is given by the following equation.

$$y_k(x) = w_{ko}+\sum w_{kj}h_j(x)\text{ ----------------}(2)$$

Where 'w_{kj}' are weights, 'σ' is the radius and 'μ'is the mean of the data points.



Algorithms

Training: Levenberg-Marquardt (trainlm)
Performance: Mean Squared Error (mse)
Data Division: Random (dividerand)

Progress

Epoch:	0	2 iterations	1000
Time:		0:00:00	
Performance:	3.09e+03	3.02	0.00
Gradient:	1.00	1.05e-13	1.00e-10
Mu:	0.00100	1.00e-05	1.00e+10
Validation Checks:	0	0	6

Plots

Performance (plotperform)
Training State (plottrainstate)
Regression (plotregression)

Plot Interval: 1 epochs

✓ Minimum gradient reached

Stop Training
Cancel

Figure (3): Neural Network Training Process

IV. WATERMARK EMBEDDING

The cover image is resized to256x256 pixels, the R, G and B planes are separated and blue plane is selected to embed watermark. The bitmap is selected as watermark and is resized to 32x32 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 Q_1=12 and Q_2=8. The radial basis function neural network is used to embed and extract watermark. The schematic diagram of 4-level wavelet transformation is shown in figure (4).

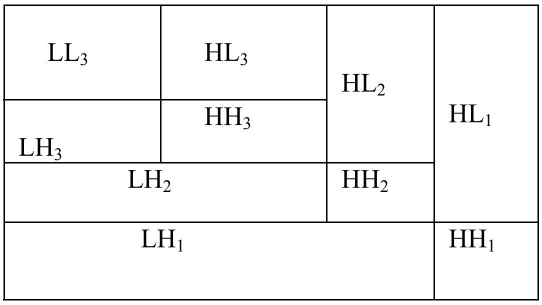


Figure (4): 3-level wavelet transformation

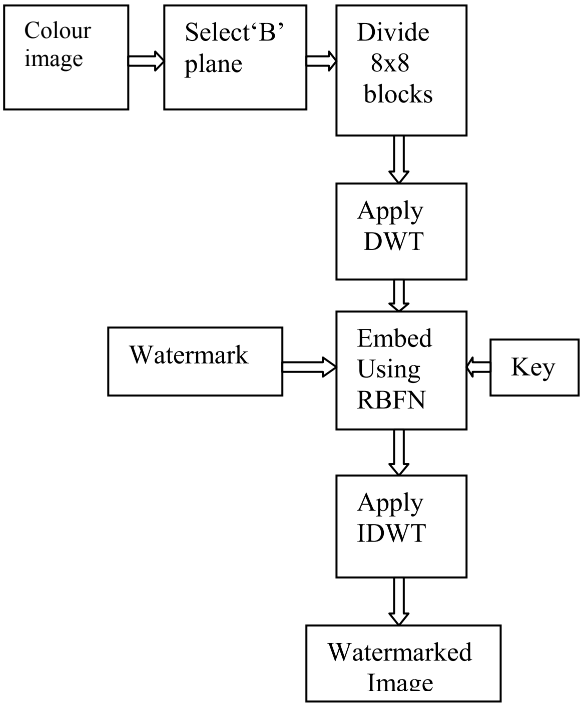


Figure (6): Watermark Embedding

To obtain the better imperceptibility and robustness, the watermark is added in transform domain using radial basis function neural network. The wavelet based watermark techniques exploit the frequency information and spatial information of the transformed data in multi resolution to gain robustness. The wavelet transform is closer to the human visual system since it splits the input image into several frequency bands that can be processed independently.

Watermark Embedding Algorithm

Step1. Read the color image of size NxN.

Step2. Resize the color image to 256x256 pixels and use it as a cover image.

Step3. Select the blue plane to embed the watermark.

Step4. The frequency subcomponents {HH1, HL1, LH1, {HH2, HL2, LH2}, {HH3, LH3, LL3}}} are obtained by computing the third level DWT of the resized color image.

Step5. Read the bitmap of size 32x32 as the watermark.

Step6. Select the beginning position of watermark using the secret key.

Step7.Initialize the weight vectors, fix the epochs, set the initial learning rate.

Step8. Quantize the DWT coefficient $T_{(j+key)}$ by Q as the input to the RBFN.

Step9. Embed the watermark using the following equation

$$T'_{(j+key)} = RBFN(round((T_{(j+key)})/Q) + x_j \ldots(3)$$

Where x_j is the random watermark sequence.

Step10. Find the difference between input values and trained values. The resultant values are accepted as watermark.

Step11. Perform IDWT on each coefficient to get the watermarked image.

V. WATERMARK EXTRACTION

The watermark extraction process is 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.

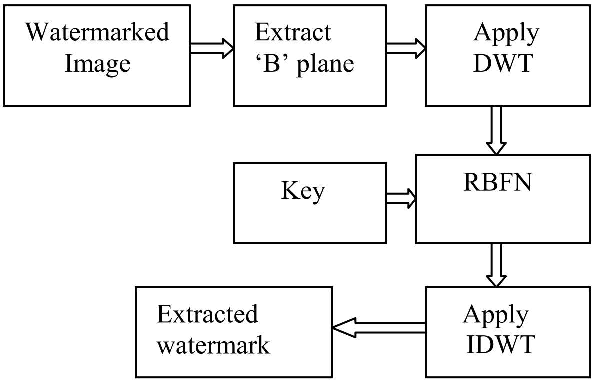


Figure (6): Watermark Extraction

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 RBFN, then get the output of RBFN as round[T''$_{(j)}$/Q].
Step 3. Extract the watermark x' using the equation
$x'_{i\,=}$ T'' (j) – RBFN (round (T''$_{(j)}$/Q)) …. (4)
where j=1 to8
Step 4. Measure the NC of the extracted watermark x' and the original watermark x.

VI. EXPERIMENTAL RESULTS

The algorithm of watermark embedding and extraction are implemented using MATLAB. onions image of size 256x256 is selected as the cover image. Gray scale bitmap image of size 32X32 Barbara is selected as the watermark. The PSNR of the watermarked image is calculated using the formula

$$PSNR = 10\log_{10}\frac{(R*R)}{MSE} \quad \dots\dots\dots \quad (5)$$

Where R= maximum fluctuation in the input image=256

$$MSE = \sum_{j=1}^{r}\sum_{k=1}^{c}\frac{[W(j,k)-W'(j,k)]^2}{rc} \quad \dots.. (6)$$

Where r = number of rows
c = number of columns

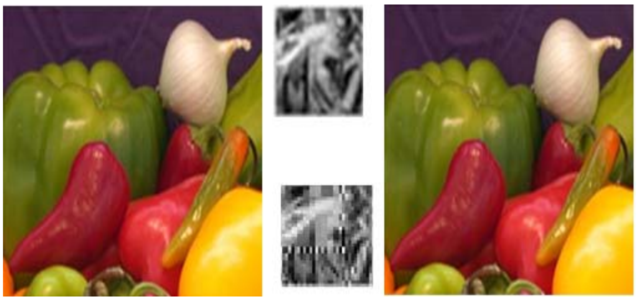
W(j,k) and W'(j,k) represent blue plane of cover image and watermarked image.

$$NC = \frac{\sum_j \sum_k W(j,k) * W'(j,k)}{\sum_j \sum_k W(j,k) * W'(j,k)} \quad \dots\dots (7)$$

The performance evaluation of the method is done by measuring imperceptibility and robustness. The normalized correlation coefficient (NCC) 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 cropping, salt & pepper noise attack, and rotation.

A. *Effect of Cropping.*

The original image onions of size 256x256, watermark Barbara of size 32x32, watermarked image (MSE of 0.4426, PSNR of 52.2154 and NCC of 0.9956) and extracted watermark without any attack are shown in figure (7). Even though the percentage of cropping is increased, there is no rapid change in the degradation of extracted watermark.



Figure(7): Cover image, Watermark, Watermarked image and Extracted watermark.

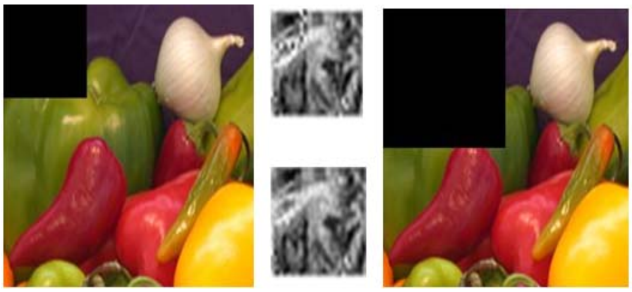


Figure (8): 10% Cropped image, Extracted watermark,25% Cropped image and Extracted watermark.

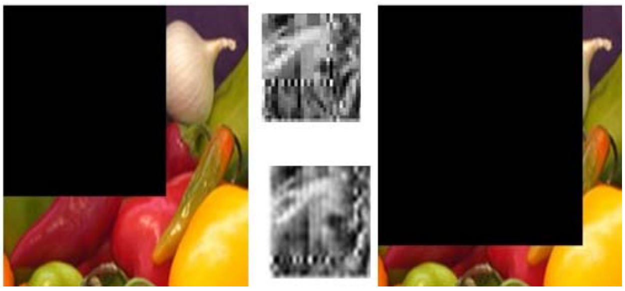


Figure (9): 50% Cropped image, Extracted watermark, 75% Cropped image and Extracted watermark.

Table 1: Comparison of cropping results

Percentage of Cropping	MSE	PSNR	NCC
10	0.4354	51.7415	0.9094
25	0.4387	51.7091	0.9465
50	0.4404	51.6922	0.8888
75	0.4236	51.8611	0.8553
90	0.4255	51.8417	0.8937

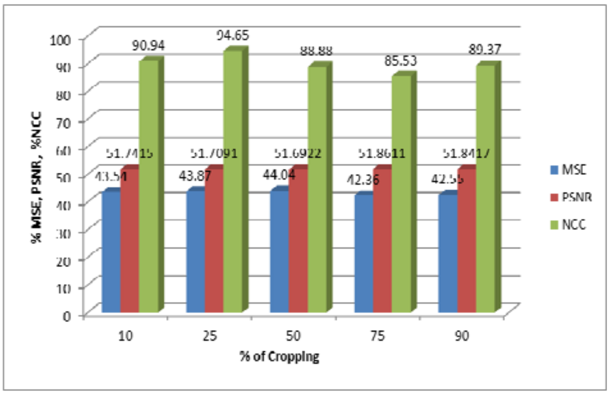


Chart (1): Comparison of Cropping Results

B. *Effect of Salt&Pepper Noise*

The effect of salt&pepper noise is greatly reduced by properly training the neural network. The MSE, PSNR and NCC values are compared for various levels of noise attack. The results show that the algorithm is robust to noise attack.

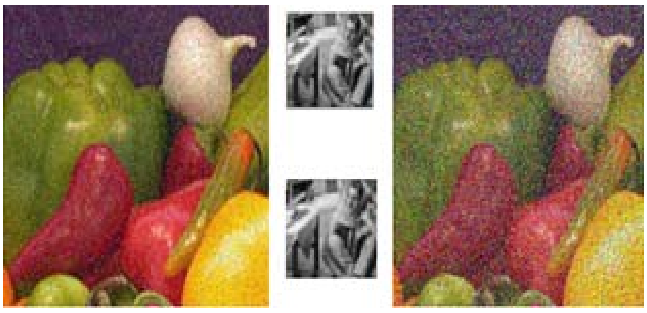
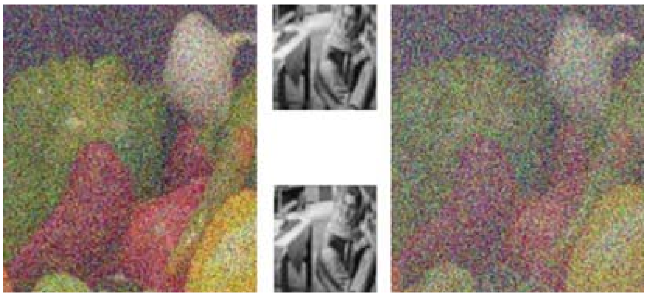


Figure (10):10% Salt&pper noise attacked image, Extracted watermark, 30% Salt&pepper noise attacked image and extracted watermark



Figure(11):50% salt&pepper noise attacked image, Extracted watermark, 70% Salt&pepper noise attacked image and Extracted watermark

Table 2: Comparison of noise attack results

Percentage of Noise attack	MSE	PSNR	NCC
10	0.4284	51.8123	0.9951
30	0.4311	51.7846	0.9948
50	0.4269	51.8727	0.9947
70	0.4282	51.8148	0.9948
90	0.4292	51.8038	0.9940

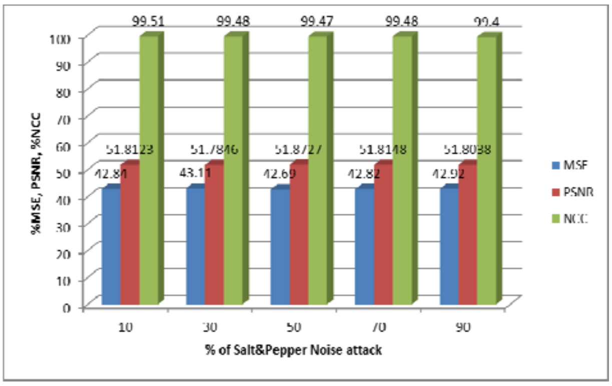


Chart (2): Comparison of Noise attack results

C. *Effect of Rotation*

The effect of rotation on watermarked images is greatly reduced by proper selection weights and learning rate .The experimental results show that the algorithm is robust to rotation attack.

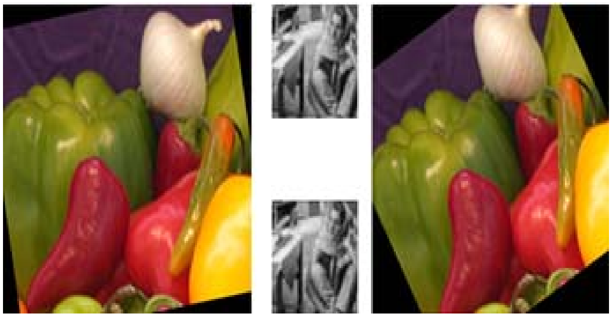


Figure (12): 10^0&30^0Rotation attacked images and the corresponding extracted watermark images

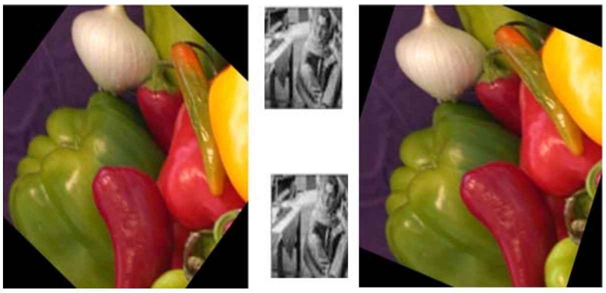


Figure (13): 50^0& 70^0 Rotation attacked images and the corresponding extracted watermark images.

Table (3): Comparison of Rotation attack results

Rotation in Degrees	MSE	PSNR	NCC
10	0.4336	51.7596	0.9953
30	0.4311	51.7847	0.9956
50	0.4288	51.8079	0.9954
70	0.4299	51.7975	0.9955
90	0.4334	51.7622	0.9957

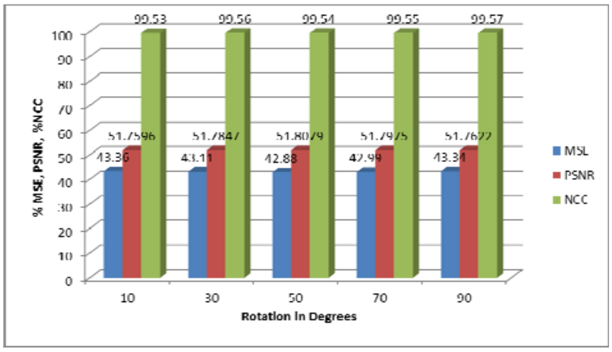


Chart (3): Comparison of Rotation attack results

VII. CONCLUSION

The experimental results show that the proposed method is robust to cropping, salt&pepper noise and rotation attacks. The robustness is better than the methods proposed in [1] and [8].This technique can also be implemented to minimize the compression attack. This algorithm can also be implemented using fuzzy logic to improve the imperceptibility.

REFERENCES

[1] G. Fahmy, M. F. Fahmy, and U. Mohammed "Nonblind and Quasiblind Natural Preserve Watermarking" Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing, Volume 2010, Article ID 452548, 13 pages

[2] Y. H.-C. Wu and C.-C. Chang, "A novel digital image watermarking scheme based on the vector quantization technique," *Computers & Security*, vol. 24, pp. 460–471, 2005

[3] Y. Wang and A. Pearmain, "Blind image data hiding based on self-reference," *Pattern Recognition Letters*, vol. 25, no. 15, pp.1681–1689, 2004.

[4] P. H. W. Wong, O. C. Au, and Y. M. Yeung, "A novel blind multiple watermarking technique for images," IEEETransactions on Circuits and Systems for Video Technology, vol.13, no. 8, pp. 813–830, 2003.

[5] Yonghong Chen and jiancong Chen, "A Novel Blind watermarking Scheme Based on Neural Networks for Image", 2010 IEEE Transactions, pp. 548-552.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] [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.

[14] 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

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

[16] P. Guo and L. Xing, "Blind Image Restoration Based on RBF Neural Networks", Proc.SPIE 5298, 2004, pp.259–266.