ISSN: 0976-9102(ONLINE)
DOI: 10.21917/ijivp.2011.0042

REGION OF NON-INTEREST BASED DIGITAL IMAGE WATERMARKING USING NEURAL NETWORKS

Bibi Isac[1], V. Santhi[2] and Arunkumar Thangavelu[3]
[1,2,3]*School of Computing Science and Engineering, VIT University, Vellore, India*
E-mail: [2]vsanthinathan@gmail.com and [3]arunkumar.thangavelu@gmail.com

Abstract

Copyrights protection of digital data become inevitable in current world. Digital watermarks have been recently proposed as secured scheme for copyright protection, authentication, source tracking, and broadcast monitoring of video, audio, text data and digital images. In this paper a method to embed a watermark in region of non-interest (RONI) and a method for adaptive calculation of strength factor using neural network are proposed. The embedding and extraction processes are carried out in the transform domain by using Discrete Wavelet Transform (DWT). Finally, the algorithm robustness is tested against noise addition attacks and geometric distortion attacks. The results authenticate that the proposed watermarking algorithm does not degrade the quality of cover image as the watermark is inserted only in region of non-interest and is resistive to attacks.

Keywords:

Digital Watermarking, Invisible Watermarking, Neural Networks Based Watermarking Technique, Transform Domain Watermarking, Region of Non-Interest Based Watermarking

1. INTRODUCTION

The rapid development of digital media provides a great convenience for adopting, using or modifying the information. The development in computer network communications make information transmission relatively simple and quick and at the same time the rate of exposure to attack is also very high [1]. A digital watermark is a distinguishable piece of information that is adhered to any data which is required to be protected. The data in which the watermark embedded is called the cover data or cover signal and the embedded data is called watermark. Since watermarking could be carried out on various types of cover data like digital images, digital video and audio, the imperceptibility constraint will take different forms, depending on the properties of the recipient. In addition to imperceptibility, robustness of the watermark should also be maintained. As watermarking is used to protect the copyrights of cover data, it should not be easily removable from the watermarked objects either through normal signal processing operations which may be intentional or unintentional or through any statistical process [2]. Applications of digital watermarking include copyright protection, covert communication, broadcast monitoring, content authentication, content description, and copy control [3].

Digital watermarking can be classified into two types as visible watermarking and invisible watermarking [4]. In visible watermarking, the information is embossed in such a way that the inserted information is perceptible to easily recognize the owner of an image or video but in invisible watermarking, inserted information cannot be perceived. The hidden information can be detected to some extent with much effort [5]. The information to be inserted may be a text data or a logo which identifies the owner of the media. As mentioned earlier, based on the host signal in which the watermark is embedded, watermark may be classified as digital image watermark, video watermark and audio watermark [6][7].

Once the host signal is selected, the watermarking can be done either in the spatial domain by modifying pixel intensity values or in the frequency domain by transforming images using Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) or Discrete Wavelet Transform (DWT)[8].

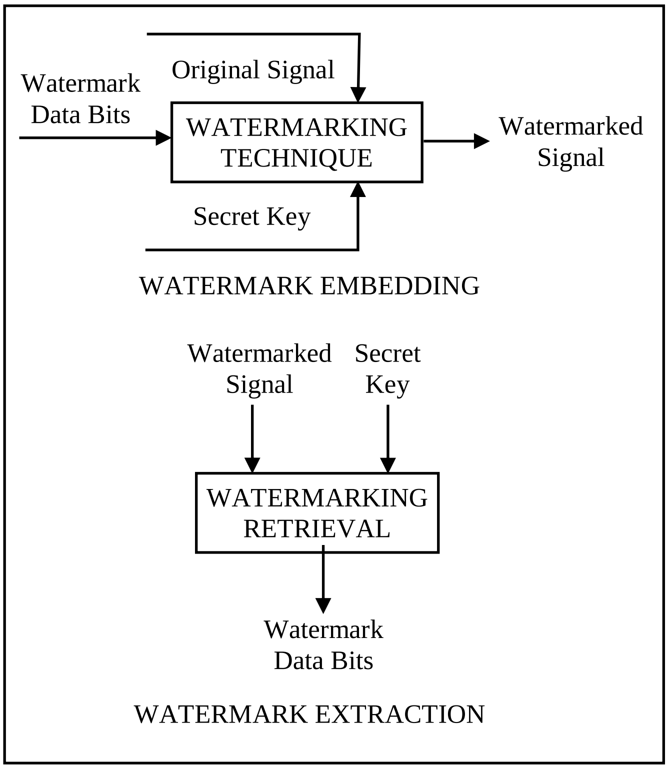


Fig.1. Basic Watermarking Process

P.T. Yu et al. [9] proposed a novel digital watermarking technique which hides an invisible watermark into a color image and uses a neural network concept to learn the relationship between the embedded watermark and the watermarked image. The relationship learnt by the neural network is then used as a digital signature in the extraction process. Multiple embedding is adopted in this technique to improve the performance. Due to the flexibility and adaptability of the neural network, the watermarking technique outperforms the conventional techniques against several attacks. Chang et al. [10] presented a specifically designed full counter-propagation neural network for digital image watermarking. Different from the traditional methods, the watermark is embedded in the synapses of the FCNN (Full Counter-Propagation Neural Network) instead of the cover image. The quality of the watermarked image is almost same as the original cover image. Since the watermark is stored in the synapses, most of the attacks could not degrade the quality of the extracted watermark image.

A novel watermarking method for an image is proposed by Jun Zhang [11], in which the logo watermark is embedded into a novel transform domain called multi-wavelet transform domain. Since the differences between the corresponding coefficients in two sub-blocks in the coarse level of the multi-wavelet domain are small, the embedding strategy could ensure the quality of the image. A BPN (Back Propagation Network) model is used to learn the relationship between the watermark and the watermarked image. Wang et al [12] presented a novel blind digital watermarking scheme based on neural networks in the multi-wavelet domain. The watermark is embedded into the coefficients selected based on the weight factors calculated by exploiting the HVS characteristics. The neural network was fused properly with watermarking process to enhance the performance of conventional watermarking techniques. In [13], a digital watermarking scheme using neural networks is proposed in which the original image is divided into blocks, and then a neural network is used to decide adaptively different embedding strengths according to different textural features and luminance value of each block. As it is embedded adaptively based on luminance value and textural features, the resulting watermarked image is extremely robust to image compression attack. In [14], artificial neural network (ANN) is used to model the HVS to decide the watermark strength of DCT coefficients and watermark bits are embedded into the DCT coefficients adaptively. It shows that an ANN can better model human visual system and that the watermarking strength calculated using ANN is much better than conventional methods without causing visual degradation of watermarked images. This results in making the watermark more robust.

Based on the literature it is found that neural network is used to calculate watermark strength adaptively for the entire region of an image. If watermark is embedded in the entire region of an image the quality of watermarked image would be degraded, instead region which is not important (RONI) is altered to insert watermark to maintain the quality of important region. Thus the region based watermarking using neural network is proposed in this paper. Moreover to make the watermark more robust it is embedded in wavelet domain.

The rest of the paper is organized as follows. In section 2 preliminaries of neural networks, basics of discrete wavelet transformation and importance of region based watermarking are briefly given. In section 3 the proposed work is presented in detail. Results and discussion are given in section 4. Section 5 concludes the work.

2. BASICS OF RELATED THEORIES

In this section, the basic concepts of the artificial neural networks and discrete wavelet transform used are described. In addition, the concept of RONI has been introduced.

2.1 ARTIFICIAL NEURAL NETWORKS

The study of neural networks was developed from the theories of how the human brain works. Many modern scientists believe the human brain is a large collection of interconnected neurons. These neurons are connected to both sensory and motor nerves. Scientists believe, that neurons in the brain fire by emitting an electrical impulse across the synapse to other neurons, which then fire or don't depending on certain conditions [15-16].

The structure of a feed forward neural network employed in this work is shown in Fig.2. In this experimental work, Back propagation algorithm is applied for learning the samples, Tan-sigmoid and log-sigmoid functions are applied in hidden layer and output layer respectively, Gradient descent is used for adjusting the weights as training methodology.

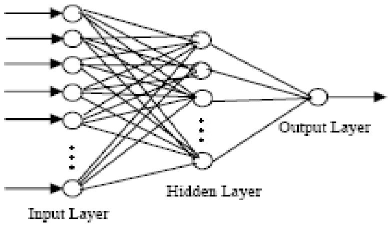


Fig.2. Architecture of a Feed Forward Neural Network

2.2 DISCRETE WAVELET TRANSFORMATION

Discrete wavelet transform (DWT) is a technique used to represent an image in a new time and frequency scale by decomposing the image into low, middle and high frequency bands. The value of low frequency band is the averaging value of the filter whereas the high frequency coefficients are wavelet coefficients or detail values.

2.3 REGION OF NON-INTEREST (RONI)

A region of non-interest (RONI) is a selected subset of samples within a dataset identified for a specific purpose. An RONI is defined by creating a binary mask, which is a binary image of same size as the image to be watermarked with pixel values that define the RONI set to 0 and all other pixels set to 1. A particular image can have more than one area that may be used as region of non-interest for embedding watermark. Among the available regions suitable region of watermark size is selected for insertion of watermark. The regions can also be defined by a range of intensities [17-18].

3. PROPOSED WORK

In this paper the region of non-interest based watermarking algorithm in transform domain is proposed. The entire region of an image could be used for inserting watermark but the visual quality of important region would be degraded. To insert the watermark and in order to retain the quality of interested regions, the selection is made from the regions which are not important. Furthermore the inserted watermark should be robust to normal image/signal processing attacks. To achieve more robustness the watermark is embedded in transform domain. If the watermark strength is increased the visual quality of the watermarked image would be degraded. Similarly if the watermark strength is very low the fidelity of the inserted watermark would be very less. In order to maintain both the quality of cover image and fidelity of inserted watermark the embedding strength should be selected by taking the tradeoff between above said requirements. The embedding strength of watermark image is calculated by training a neural network using the first level of results. The procedure for embedding and extracting watermark into/from an image is given in subsequent sections.

3.1 WATERMARK EMBEDDING ALGORITHM

In the embedding process, the region of non-interest part of an image is transformed using discrete wavelet transform. As the low frequency band of a cover image is robust to compression attack watermark is inserted in the low frequency band of an image. Once watermark insertion is carried out in region of non-interest then the region of interest is merged to get the final watermarked image. To test the proposed work a sample gray scale image of size 256×256 is considered as cover data and a small identity image of size 128×128 is used as watermark. The process of embedding watermark is given in Fig.3.

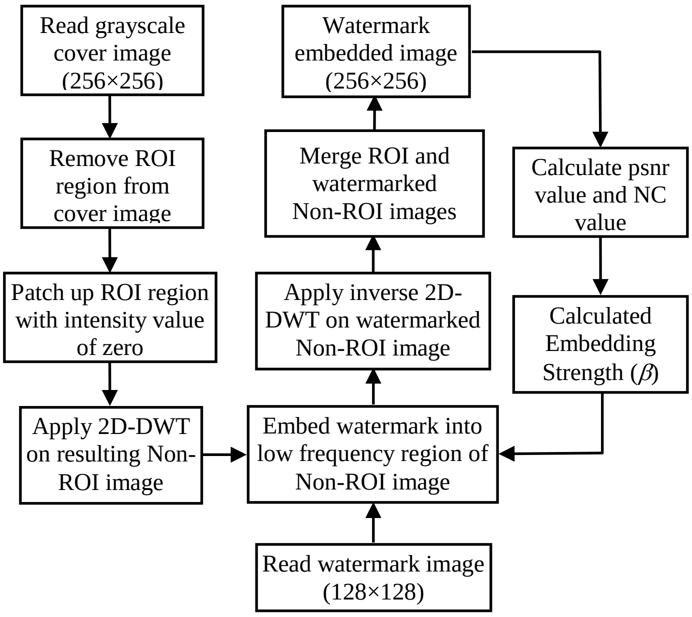

Read grayscale cover image (256×256)
Remove ROI region from cover image
Patch up ROI region with intensity value of zero
Apply 2D-DWT on resulting Non-ROI image
Embed watermark into low frequency region of Non-ROI image
Read watermark image (128×128)
Apply inverse 2D-DWT on watermarked Non-ROI image
Merge ROI and watermarked Non-ROI images
Watermark embedded image (256×256)
Calculate psnr value and NC value
Calculated Embedding Strength (β)

Fig.3. Watermark Embedding Process

Insertion Algorithm

1. Read a grayscale cover image *I* and the watermark image *W*
2. Remove the region of interest (ROI) from an image using masking operation
3. Apply 2D-DWT on the region of non-interest part of an image.
4. Calculate the embedding strength β by using the initial quality measures such as peak signal to noise ratio and correlation coefficient of original and extracted watermark
5. Insert watermark in low frequency region of the DWT transformed image using the following equation

$$I' = I + \beta W \quad (1)$$

6. Apply inverse DWT in order to get the watermarked non-region of interest in an image
7. Combine extracted ROI part with watermarked non-region of interest of an image to get the final watermarked image

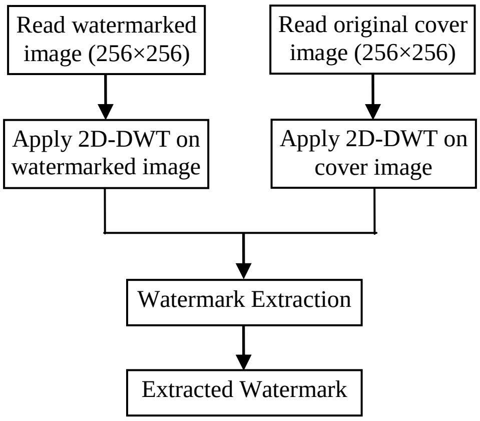

Read watermarked image (256×256)
Read original cover image (256×256)
Apply 2D-DWT on watermarked image
Apply 2D-DWT on cover image
Watermark Extraction
Extracted Watermark

Fig.4. Watermark Extraction Process

3.2 WATERMARK EXTRACTION ALGORITHM

The procedure for extracting the watermark from the watermarked image is given in Figure 4. To extract watermark from the watermarked image, the region of interest is cropped and the remaining region is subjected to wavelet transformation. As this algorithm is classified as non-blind watermarking algorithm the original image is also required to extract watermark from low frequency band.

Extraction Algorithm:

1. Apply 2D-DWT on both the watermarked image and original cover image
2. Let the low frequency region of the watermarked image be LL1 and the low frequency region of the cover image be LL.
3. Extract the watermark using the following equation:

$$W = \left(I' - I\right) / \beta \quad (2)$$

4. RESULTS AND DISCUSSION

The performance of our proposed algorithm is analyzed by embedding watermark in non-region of interest of an image in frequency domain. The quality of the watermarked image can be measured either subjectively or objectively and it is observed that both subjective and objective quality of watermarked image is good. The PSNR is the objective criteria used to measure the quality of the watermarked image. The formula for measuring PSNR and NC values are given in Eq.(3), Eq.(4) and Eq.(5).

$$\text{PSNR} = 10\log_{10}\left(\frac{255}{MSE}\right) \quad (3)$$

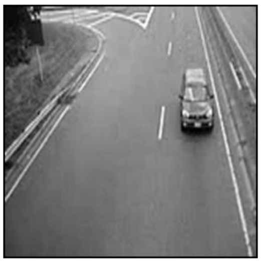
$$\text{MSE} = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}\left(f(i,j) - f'(i,j)\right)^2 \quad (4)$$

$f(i,j)$ and $f'(i,j)$ represent the pixel values of original host image and the watermarked image respectively and parameters *m*, *n* specify row and column size of an image.

The quality of the watermarked image is measured through normalized correlations (NC) using Eq.(5), which is used to measure the similarity between original watermark and extracted watermark [10].

$$\text{NC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w(i,j) * w_e(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w^2(i,j)}\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n} w_e^2(i,j)}} \tag{5}$$

Initially the watermark is embedded with embedding strength β = 0.0001. The embedding factor value 0.0001 gives good subjective quality of watermarked image. Feed-forward neural network is trained by giving initial embedding strength and obtained normalized correlation value. Based on the value of the normalized correlation, further iterations are performed. If NC value is equal to 1, the iteration is stopped. If obtained NC value is not very closer to 1 then the embedding strength is incremented by an amount of 0.001 for every iteration. The watermark embedding and extraction procedure are carried out for the new embedding strength value and the process continues till the NC value is close to 1 or reaches the saturation level i.e., maintain the same value for many iterations. A sample grayscale image and a watermark image are shown in Fig.5(a) and 5(b) respectively. The peak signal to noise ratio and normalized correlation values are calculated in order to estimate the quality of the watermarked image and the extracted watermark respectively.



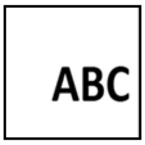


Fig.5(a). Cover Image Fig.5(b). Watermark Image

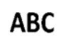
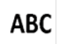
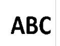
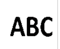
The best embedding strength found to be 0.007 for this test image and the obtained PSNR value 40. 6523 dB and NC value is 0.9593 which shows very good objective quality of watermarked image and extracted watermark under no attacks condition. Keeping this value of embedding strength constant, the algorithm is tested with various attacks such as addition of salt and pepper noise, Gaussian noise, Poisson noise and speckle noise and results are tabulated. A special type of Gaussian noise called white Gaussian noise, in which the values at any pairs of times are statistically independent that is uncorrelated. Gaussian noise is most commonly used as additive white noise and its probability density function is given in Eq.(9),

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \tag{6}$$

where, μ represents the mean and σ represents the standard deviation. In Table.1 the normalized correlation value and extracted watermark are given by keeping μ = 0 and varying the value of σ. In Fig.6 the graphical representation of noise density versus obtained normalized correlation is given.

Salt and pepper noise is randomly occurring white and black pixels. The corrupted pixels are either set to the maximum value or have single bits flipped over. In some cases, single pixels are set alternatively to zero or to the maximum value, giving the image a 'salt and pepper' like appearance. The noise is usually quantified by the percentage of pixels that are corrupted [19]. In Table.2 the extracted watermark and calculated normalized correlation is given after applying salt and pepper noise. Similarly the relation between noise density and extracted watermark is given in Fig.7.

Table.1. Extracted Watermark and obtained Normalized Correlation after Gaussian Noise attack

Variance	Normalized Correlation	Extracted Watermark
0.01	0.95098	
0.05	0.94988	
0.08	0.94956	
0.1	0.94938	

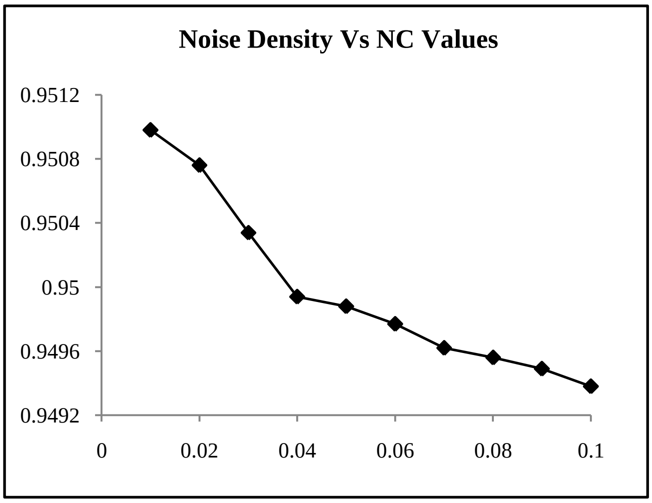
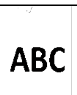
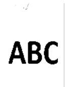
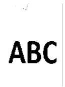
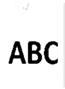


Fig.6. Relation between obtained NC and Gaussian Noise with various densities

Speckle noise is a granular noise that inherently exists in and degrades the quality of the active radar and synthetic aperture radar (SAR) images. Speckle noise in conventional radar results from random fluctuations in the return signal from an object. It increases the mean grey level of a local area [19]. In Table.3 the extracted watermark and normalized correlation value after speckle noise attack are given. Fig.8 shows the relation between speckle noise density and obtained normalized correlation values. The resistivity of proposed algorithm for different types of noise attack is shown in Fig.6, Fig.7 and Fig.8.

Another important type of attack is called geometric attack which includes rotation, translation and scaling. A rotation is a circular movement of an object around a *center* (or *point*) *of rotation*. That common point lies within the axis of that motion. The axis is 90 degrees perpendicular to the plane of the motion. The algorithm is tested with rotational attack and result is tabulated in Table.4. The relation between amount of rotation and normalized correlation of extracted watermark is shown in Fig.9.

Table.2. Extracted Watermark and Normalized Correlation after Salt and pepper noise attack

Noise Density	Normalized Correlation	Extracted Watermark
0.01	0.95017	
0.05	0.94972	
0.08	0.94912	
0.1	0.94886	

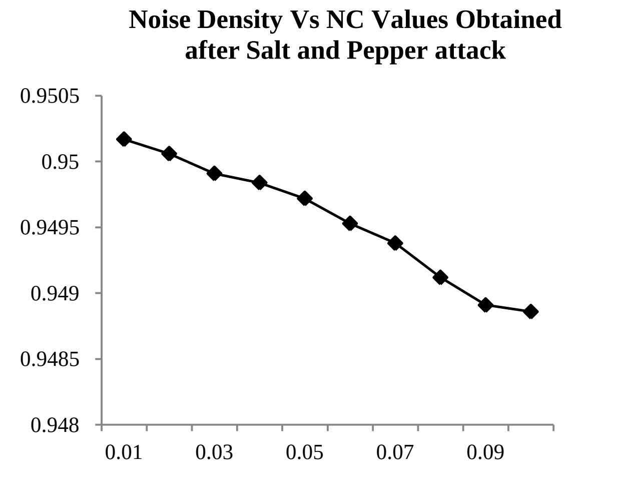
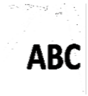
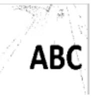
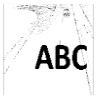


Fig.7. Relation between obtained NC and salt and pepper noise with various densities

Table.3. Extracted Watermark and Normalized Correlation after Speckle noise attack

Variance	Normalized Correlation	Extracted Watermark
0.001	0.94921	
0.004	0.94753	
0.008	0.94614	

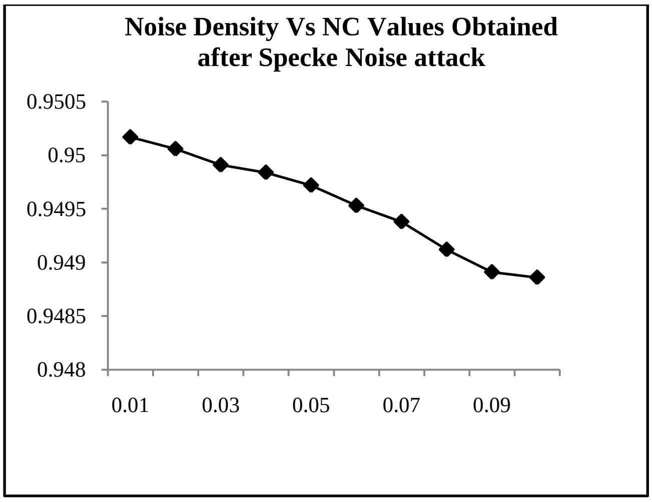
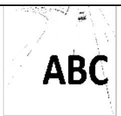
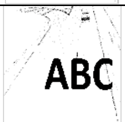
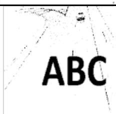


Fig.8. Relation between obtained NC values and with various Speckle noise variance

Table.4. Extracted Watermark and Normalized Correlation after Rotation attack

Degree of Rotation	Normalized Correlation	Extracted Watermark
15	0.94278	
45	0.94158	
90	0.93847	

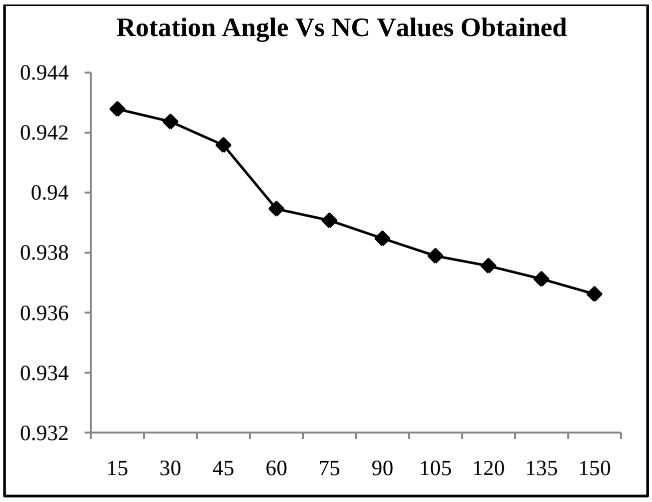
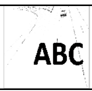
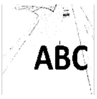
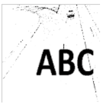


Fig.9. Relation between obtained NC Values after rotation attacks

In geometry attack, scaling is a linear transformation technique that enlarges or shrinks objects by a scale factor that is the same in all directions. Scaling can be done uniformly as well as non-uniformly. In uniform scaling, the object is scaled uniformly on every axis. In non-uniform scaling, different scale factors are applied on different axes of the object. Non-uniform scaling changes the shape of the object. The algorithm is tested with rotational attack and result is tabulated in Table.5. The relation between scaling factor and normalized correlation of extracted watermark is shown in Fig.10.

A translation moves every point of an image by the same amount in a given direction. It is one of the rigid motions a translation can also be interpreted as the addition of a constant vector to every point, or as shifting the origin of the coordinate system. The results obtained with various translation factors is given in Table.6. The graphical representation of extracted watermark and calculated normalized correlation is given in Fig.11.

Table.5. Extracted Watermark and Normalized Correlation after Scaling attack

Scale Factor	Normalized Correlation	Extracted Watermark
10%	0.94278	
40%	0.94158	
80%	0.93847	

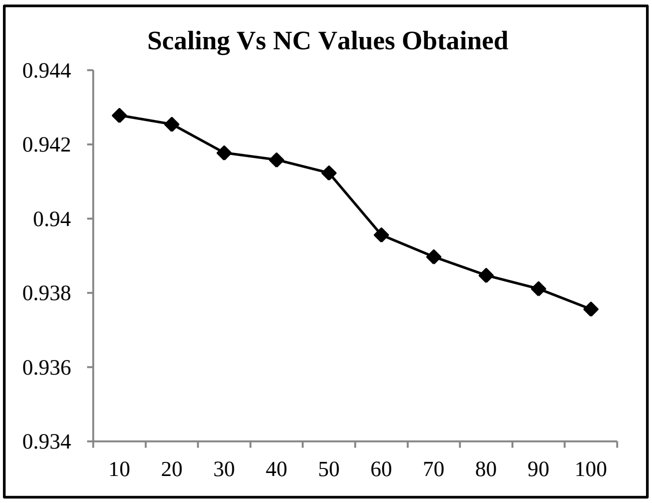
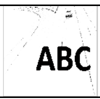
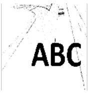
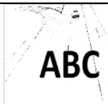


Fig.10. Relation between obtained NC Values and with scaling factor

In this work the proposed algorithm is tested against two types of attacks namely noise addition and geometric. As per the results obtained this algorithm is performing well for all kinds of noise addition attacks as various geometric attacks. As the proposed algorithm is inserting watermark in selected frequency band of wavelet decomposed image implements resistivity to different images processing attacks.

Table.6. Extracted Watermark and Normalized Correlation after Translation attack

Translation Factor	Normalized Correlation	Extracted Watermark
10	0.94278	
40	0.94158	
80	0.93847	

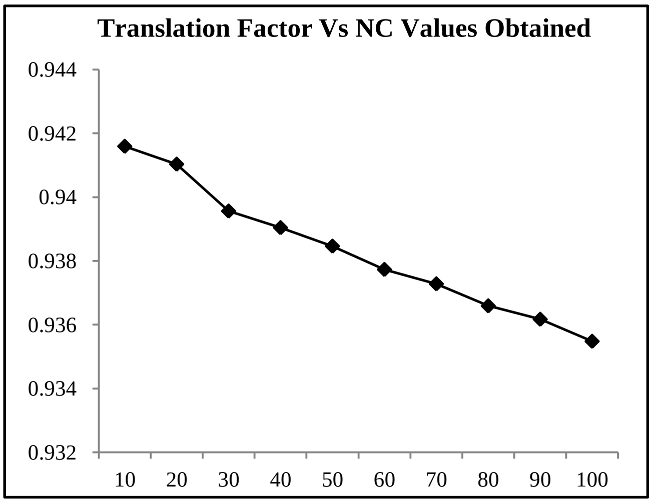


Fig.11. Relation between obtained NC Values and with various speckle noise densities

5. CONCLUSION

Digital watermarks have been dominantly used as scheme for copyright protection of digital images, video, audio and text data. This paper describes a method to embed watermark in region of non-interest (RONI) and also a method for adaptive calculation of strength factor using neural network. The embedding and extraction processes are carried out in the transform domain by using Discrete Wavelet Transform (DWT). Finally, the algorithm robustness is tested against noise addition attacks and geometric distortion attacks. The results obtained show that the algorithm is more robust to geometric attacks and noise addition attack. The calculated peak signal to noise ratio prove that the objective quality of watermarked image good. As the proposed algorithm is inserting watermark in selected frequency band of wavelet decomposed image provides resistivity to different image/ signal processing attacks. The proposed algorithm could also be extended to video sequences for inserting watermark in transform domain.

REFERENCES

[1] Kutter M, Bhattacharjee S. K and Ebrahimi, T, “Towards Second Generation Watermarking Schemes”, *Proceedings*

of International Conference on Image Processing, Vol. 1, pp. 320-323, 1999.

[2] Cox I. J, Kilian J, Leighton T and Shamoon T, “A secure, robust watermark for multimedia”, *Information Hiding*, Vol. 1174, pp. 185–206, 1996.

[3] Khan A and Mirza A. M, “Genetic perceptual shaping: Utilizing cover image and conceivable attack information during watermark embedding”, *Information Fusion*, Vol. 8, No. 4, pp. 354-365, 2007.

[4] Macq B and Quisquater J, “Cryptology for digital TV broadcasting”, *Proceedings of the IEEE*, Vol. 83, No. 6, pp. 944–957, 1995.

[5] Tanaka K, Nakamura Y and Matsui K, “Embedding secret information into a dithered multi-level image”, *Proceedings of IEEE Military Communications Conference*, Vol. 1, pp. 216–220, 1990.

[6] Hernandez J. R, Perez-Gonzalez F, Rodriguez J. M and Nieto G, “Performance analysis of a 2-D-Multipulse Amplitude Modulation scheme for data hiding and watermarking of still images”, *IEEE Journal on selected Areas in Communications*, Vol. 16, No. 4, pp. 510–524, 1998.

[7] Cachin C, “An information-theoretic model for steganography”, *Journal on Information and Computation*, Vol. 192, No. 1, pp. 41-56, 2004.

[8] Dittmann Jana, Megias David, Lang Andreas and Herrera-Joancomarti Jordi, “Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity”, *Transactions on Data Hiding and Multimedia Security I*, pp. 1-40, 2006.

[9] Yu Pao-Ta, Tsai Hung-Hsu and Lin Jyh-Shyan, “Digital watermarking based on neural networks for color images”, *Journal on Signal Processing – Special section on digital signal processing for multimedia communications and services*, Vol. 81, No. 3, pp 663-671, 2001.

[10] Chang Chuan-Yu and Su Sheng-Jyun, “The Application of a Full Counterpropagation Neural Network to Image Watermarking”, *Proceedings of IEEE Networking, Sensing and Control*, pp. 993-998, 2005.

[11] Jun Zhang, Nenchao Wang, Feng Xiong, “Hiding a Logo Watermark into the Multiwavelet Domain using Neural Networks”, *Proceedings of the 14th IEEE International Conference on Tools with Artificial Intelligence*, pp. 477-482, 2002.

[12] Wang Zhenfei, Wang Nenchango and Shi Baochang, “A Novel Blind Watermarking Scheme based on Neural Networks in the Multiwavelet Domain”, *Proceedings of the 6th World Congress on Intelligent Control and Automation*, Vol. 1, pp. 3024-302, 2006.

[13] Cong Jin and Shihui Wang, “Applications of a Neural Network to estimate Watermark Embedding Strength”, *8th International Workshop on Image Analysis for Multimedia Interactive Services*, pp. 68-68, 2007.

[14] Shi-chun Mei, Ren-hou Li, Hong-mei Dang and Yun-kuan Wang, “Decision of Image Watermarking strength based on Artificial Neural Networks”, *Proceedings of the 9th International Conference on Neural Information Processing*, Vol. 5, pp. 2430-2434, 2002.

[15] Fausett Laurene V, “*Fundamentals of Neural Networks: Architectures, Algorithms, and Applications*”, Prentice-Hall Inc., 1994.

[16] Bishop Christopher M, “*Pattern Recognition and Machine Learning*”, Springer-Verlag NY, Inc. Secaucus, 2006.

[17] Dashun Que, Li Zhang, Ling Lu and Liucheng Shi, “A ROI Image Watermarking Algorithm Based on Lifting Wavelet Transform”, *Proceedings of International Conference on Signal Processing*, Vol. 1, No. 1, 2006.

[18] Alan C. Bovik, “*Handbook of Image and Video Processing*”, Elsevier Science, 2005.

[19] Cherifi D, Smara Y, “Refined Adaptive Speckle Filtering for SAR images”, *19th Symposium Remote sensing in the 21st century: economic and environmental applications*, 1999.