

ISSN 2090-4304

Journal of Basic and Applied

Scientific Research

www.textroad.com

# A Novel Digital Watermarking Scheme Using Neural Networks with Tamper Detection Capability

## Mohamad Vafaei, and Homayoun Mahdavi-Nasab

Department of Electrical Engineering, Najafabad Branch, Islamic Azad University, Isfahan, Iran

#### ABSTRACT

In this paper, a novel watermarking method based on wavelet coefficient quantization using artificial neural networks is proposed. Imperceptibility and robustness are known as the main contradictory requirements of every watermarking scheme. In the proposed method, better compromises are achieved applying neural networks to adjust the watermark strength. Every four non-overlapped wavelet coefficients of the host image are grouped into a block and the differences of appropriately selected coefficients are quantized according to the watermark bit. A binary image is used as the watermark and embedded repetitively into the selected wavelet coefficients. The proposed method also improves the tamper detection in the watermarked image. Experimental results demonstrate simultaneous good imperceptibility and high robustness of the method against several types of attacks, such as Gaussian and salt and pepper noise addition, median filtering, and JPEG compression; in addition to capability of detecting even minor changes in the watermarked.

**KEYWORDS:** Digital watermarking, Discrete wavelet transform, Neural network, Tamper detection

#### 1- INTRODUCTION

Together with the modern developments in widespread communications and digital multimedia, many researches are led toward issues such as copyright protection, image authentication and ownership proof. Digital watermarking is one of the proposed solutions, in which a specified hidden signal (watermark) is embedded in digital data that can be detected or extracted later for authentication purpose [1-3]. Two well-known contradictory requirements of digital image watermarking are imperceptibility and robustness against any modifications, noise, and manipulations.

Tamper detection is used to disclose any change or manipulation made into an image. This can be achieved through the use of "fragile/semi-fragile watermark" with low robustness to the modifications of the host image [4-8]. In [4] a method for tamper detection using semi-fragile data hiding is presented that aims at achieving high perceptual quality of images even after malicious modifications.

Many digital watermarking algorithms have been proposed in spatial and transform domains. The techniques in spatial domain still show relatively low capacity and are not robust enough to loss image compression and other image processing operations [9, 10]. On the other hand, frequency domain techniques although more complex, can embed more bits as watermark and are more robust to attacks. Transforms such as discrete Fourier [11, 12] discrete cosine [13, 14] and Discrete Wavelet Transform (DWT) [15-20] are generally used in the frequency domain.

The implication of watermark embedding may be classified into two categories [21]: spread spectrum [22] and quantization based watermarking [16-18]. The spread spectrum methods add a pseudorandom pattern into host image. This watermark can be detected by correlating with the same pattern or by applying other statistics to the watermarked image. In quantization watermarking a set of features extracted from the host image are quantized so that each watermark bit is represented by a quantized feature value. This technique improves the robustness to JPEG compression, and other typical attacks [17].

In recent years, neural networks pave the way for the further development of watermarking techniques by imitating the learning ability of brain. Neural networks are applied either to improve watermark extraction or to determine the watermark strength [23-25].

As two examples, Mei proposed a method for deciding the watermark strength using DCT coefficients [24], and Davis proposed a method to implement an automated system of creating maximum-strength watermarks [25]. The differences between our work and related works lie in the more elaborate selection of wavelet coefficients for watermark embedding, the block selection process and Artificial Neural Network (ANN) inputs.

In this paper, a watermarking method based on Feed-forward Neural Networks (FNN) is proposed. We embed the watermark in the components of the second and third decomposition layers of the DWT of host image. The scientific contributions of this paper can be summarized as follows:

1) The quantization watermark embedding is used to improve the robustness to JPEG compression, and other typical attacks.

- 2) ANNs are successfully applied to balance the two requirements of watermark, robustness and imperceptibility, by adaptively determining the watermark strength.
- 3) The embedding in the second decomposition layer is done by dividing it into 4 equal blocks to improve detection of changes and regions where the changes take place in the image.

The rest of this paper is organized as follows: in section 2, the preliminaries including DWT, neural network in digital watermarking, and watermark embedding based on quantizing the wavelet coefficients are briefly provided. Section 3 describes the proposed watermarking approach. In section 4 we describe how to detect watermark and tamper. The experimental results and performance comparisons are given in section 5. Finally, a conclusion is drawn in section 6.

### 2-PRELIMINARIES

#### 2-1 Discrete Wavelet Transform (DWT)

The basic idea of DWT is to split a signal into two parts, usually high and low frequency bands. The edge components of the signal are largely confined in the high frequency. The low frequency part is split again into two parts. This process is continued until the signal has been entirely decomposed or stopped before by the application at hand. The original signal can be reconstructed using the inverse DWT (IDWT).

For a two dimensional signal x(m, n), the DWT and IDWT can be similarly defined by implementing one dimensional transforms for each dimension, m and n, separately as:

$$DWT(x[m,n]) = DWT_n[DWT_m[x[m,n]]]$$
 (1)

This way, an image is decomposed through a pyramid structure with various band information such as low-low (LL), high-low (HL), low-high (LH), and high-high (HH) frequency bands [26, 27]. An example of three levels decomposition is shown in Figure 1.

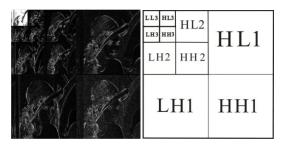


Figure 1: The pyramidal three level decomposition of an image

### 2-2 Neural Networks in Digital Watermarking

ANNs are powerful tools that provide an optimization procedure with high-speed computation. ANN may be classified to feed-forward and recurrent (feedback), and supervised or unsupervised for training of each group [28].

Back Propagation Feed-forward Neural Network (BPNN) is the most widely used among FNN. It is a supervised learning neural network that uses steepest descent method to approximate arbitrary non-linear relations between input and output. Many different variations of BPNN have been proposed including gradient descent with momentum, adaptive learning rate, resilient BP, conjugate gradient, quasi-Newton, and Levenburg-Marquardt (LM) algorithms.

The LM algorithm is used to increase the training speed and make the training avoid getting into local minimum. It acts as a compromise between the steepest-descent method with stable but slow convergence and the Gauss-Newton method with opposite characteristics [29].

To achieve a robust watermark while remaining imperceptible to the human eye usually involves generating a watermarked image using a given power; increasing the power until the watermark seems visible. ANN may be applied here to detect the desired watermarking power automatically, based on the presented past experiences.

In [25], a wavelet-based watermarking technique was introduced, in which the watermark was added to the coefficients of all the sub-bands except the low pass. The embedding is based on the following equation:

$$c_i' = c_i (1 + \alpha . m_i) \tag{2}$$

Where  $\alpha$  is the watermark strength,  $c_i$  is the DWT coefficients of the host image,  $m_i$  is the watermark to be added following a normal distribution [0, 1], and  $c_i'$  is the watermarked image coefficient. To limit the inputs to the neural network, each image is subdivided into blocks of 64×64. The resulting DWT coefficients of each image are considered as the ANN inputs. The FNN (with a (4096-512-1) structure) is used to automatically

control and select the watermark strength. The ANN is trained using the scaled conjugate gradient algorithm until the MSE is less than 5e-5.

#### 2-3 Watermarking Based on DWT Quantization

A host image is transformed into wavelet coefficients using k-level DWT, generating  $(3\times k)+1$  subbands. The  $LL_k$  sub-band cannot be used for embedding as it contains important low frequency information and any minor change in this band leads to major perceptual distortion.  $HH_k$ ,  $HH_{k-1}$ ,  $HH_1$  bands are not suitable for embedding as they are very susceptible to compression.

In [16], the host image was decomposed using 3-level DWT. The watermark was embedded into HL3 and LH3 sub-bands. Every seven non-overlap wavelet coefficients of the host image were grouped into a block. The differences between local maximum and local second maximum values were modified to the watermark bit as visualized in Figure 2. In [17], every six non-overlap wavelet coefficients were grouped into a block. In [18], to achieve the secrecy of watermark, variable block size was used for embedding a watermark bit using different sub-bands.

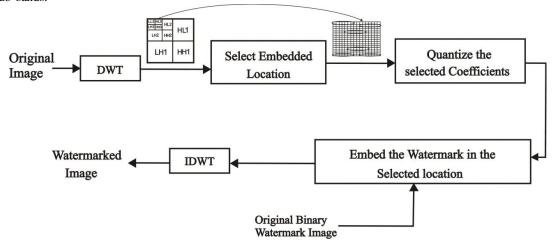


Figure 2: Watermark embedding algorithm of [16]

# 3-THE PROPOSED WATERMARKING METHOD

In this work, the watermark is embedded by appropriately modifying the values of wavelet coefficients. Neural networks are used to automatically control and create the maximum image-adaptive watermark strength. Figure 3 demonstrates the block diagram of the proposed embedding method.

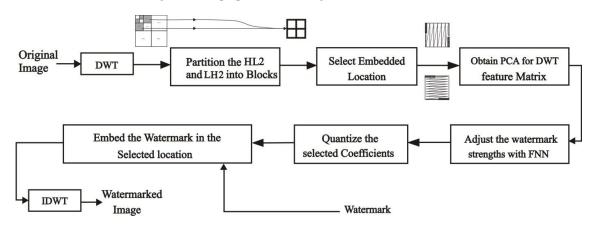


Figure 3: Block diagram of the proposed watermarking embedding scheme

#### 3-1 Wavelet TransformFunction

Due to the linear phase, compact supported and favorable signal reconstruction properties of Cohen-Daubechies-Feauveau-9/7 (CDF-9/7) [30], it seems qualified for the watermark embedding. Thus, this biorthogonal wavelet was employed for analyzing the host image.

#### 3-2 The Embedding Algorithm

In the proposed method, the host image of size 512×512 is decomposed using 3-level DWT. Increasing the number of levels improves the robustness. But it may reduce the payload capacity. As mentioned earlier, the LL3 and HH3, HH2 sub-bands are not suitable for watermark embedding. Here, LH3, HL3, LH2, and HL2 are utilized (Figure 1).

In contrast to quantization methods of [16-18], we propose modifying the second and third maximum values of the small block coefficients (Figure 4) to embed the watermark bits. This way, the host image seems to be less manipulated and better preserved.

The HL3 sub-band is subdivided into non-overlapping small blocks along the columns from top to bottom and then left to right. Block size choice is a trade-off between capacity and robustness. Considering blocks of smaller size will increase the capacity at the cost of robustness. Block size of  $4\times1$  appear to satisfy the requirements for host images of size  $512\times512$ .Since the host image is considered  $512\times512$ , the HL3 sub-band size will be  $64\times64$ , and one bit of watermark is embedded in 4 pixels of each small block as visualized in Figure 4. Therefore the watermark size can be  $32\times32$  bits at maximum; which is taken here for maximum performance. LH3 sub-band is also subdivided into  $1\times4$  blocks and one bit of watermark is embedded in each block (Figure 4). Considering  $C_i$ , i=1...4 as the increasingly sorted positive values of the coefficients, the distance between  $C_I$  and  $C_4$  may be defined as [31]:

$$\Delta_1 = \frac{C_4 - C_1}{2} \times \alpha_1 \tag{3}$$

Where  $\alpha_1$  is the strength of watermark. The distance between  $C_2$  and  $C_3$  is quantized according to  $\Delta_1$ :

$$d = \frac{C_3 - C_2}{\Delta_1} \tag{4}$$

And d is modified to its closest even or odd integer according to the value of current watermark bit  $w_i$ :

$$d' = \begin{cases} \lfloor d \rfloor + (1 \stackrel{\frown}{\oplus} w_j) & \text{if } \lfloor d \rfloor \text{ is even} \\ \\ \lfloor d \rfloor + (1 \stackrel{\frown}{\oplus} w_j) & \text{if } \lfloor d \rfloor \text{ is odd} \end{cases}$$
 (5)

Where  $\lfloor . \rfloor$  is the lower integer truncating, and  $\oplus$  and  $\overline{\oplus}$  are the XOR and XNOR operators. This way, d' is the closest even or odd integer to d. A zero watermark bit (wj) results to an even, and a one bit to an odd value of d'.

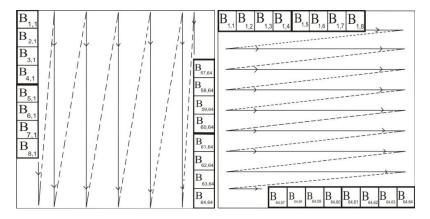


Figure 4: Location of the 4 coefficients in HL3, and LH3 respectively

To change the value of  $C_3$  – $C_2$ , both  $C_2$  and  $C_3$  are modified by the same value for keeping constant the sum of 4 coefficients. This is:

$$C_2' = C_2 - \frac{d' - d}{2} \times \Delta_1 \tag{6}$$

$$C_{3}' = C_{3} + \frac{d' - d}{2} \times \Delta_{1} \tag{7}$$

Selecting higher amounts of  $\alpha_1$  causes an increase in the watermark robustness against attacks. On the contrary, when  $\alpha_1$  decreases, host image quality will be more likely preserved. However, the watermark would be more vulnerable to noise as it is weaker. Thus, there is a tradeoff for  $\alpha_1$  between the robustness and imperceptibility.

In order to detect the tampering in watermarked image, a semi-fragile watermark is embedded in HL2 and LH2 sub-bands [4]. But in HL2 and LH2 at first the sub-bands are divided into 4 equal blocks. In each of these blocks, the watermark is embedded at least once. This redundancy assures embedding the watermark in all important parts of the sub-band in order to be able to detect the manipulations on the watermarked image. Each block is subdivided into non-overlapping small blocks as mentioned earlier. In each block values of the 4 coefficients are sorted in increasing order, named  $C_i$ , i=1...4. Again, we define:

$$\Delta_2 = \frac{C_4 - C_1}{2} \times \alpha_2 \tag{8}$$

Where  $\alpha_2$  is the strength of the fragile watermark. Higher amounts of  $\alpha_2$  causes an increase in robustness, but also more demotion in image quality. The distances of  $C_2$  and  $C_4$  and  $C_4$  and  $C_3$  are quantized according to  $d_1$  and  $d_2$ , as follows:

$$d_1 = \frac{C_2 - C_1}{\Delta_2} \tag{9}$$

$$d_2 = \frac{C_4 - C_3}{\Delta_2} \tag{10}$$

 $d_1$ , and  $d_2$  are modified to its closest even or odd integer according to the value of current watermark bit  $w_i$ :

$$d_{1}' = \begin{cases} \lfloor d_{1} \rfloor + (1 \oplus w_{j}) & \text{if } \lfloor d_{1} \rfloor \text{ is even} \\ \\ \lfloor d_{1} \rfloor + (1 \stackrel{\frown}{\oplus} w_{j}) & \text{if } \lfloor d_{1} \rfloor \text{ is odd} \end{cases}$$

$$(11)$$

$$d_{2}' = \begin{cases} \lfloor d_{2} \rfloor + (1 \oplus w_{j}) & \text{if } \lfloor d_{2} \rfloor \text{ is even} \\ \\ \lfloor d_{2} \rfloor + (1 \oplus w_{j}) & \text{if } \lfloor d_{2} \rfloor \text{ is odd} \end{cases}$$

$$(12)$$

Where  $d'_1, d'_2$  are the closest even or odd integers to  $d_1$ ,  $d_2$ . A zero watermark bit (wj) results to an odd  $d'_1$  and even  $d'_2$ , and a one bit results to an even  $d'_1$  and odd  $d'_2$ . Only  $C_2$  and  $C_3$  are modified to adjust the values of  $C_2 - C_1$  and  $C_4 - C_3$ . This is:

$$C_2' = C_2 + (d_1' - d_1) \times \Delta_2$$
 (13)

$$C_3' = C_3 - (d_2' - d_2) \times \Delta_2 \tag{14}$$

### 3-3 Maximizing the Watermark Strength

# A. Feature Extraction by Principal Component Analysis (PCA)

As mentioned above, a watermark bit is embedded into 4 coefficients of the small blocks at each sub-band of the third decomposition layer and also into small blocks at HL2, LH2 sub-bands. The differences between local maximum and local minimum values of each small block, containing the watermark bits, are calculated and stored in row vectors of size 1×1024 for each part (HL3 and LH3 sub-bands, and 64x64 blocks in HL2 and LH2) defined as *Vectordata*. The feature extraction procedure is illustrated in Figure 5.

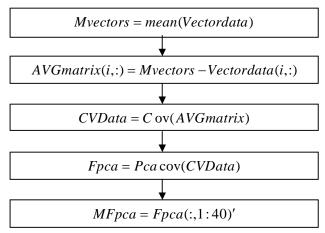


Figure 5: Feature extraction procedure

PCA is used to reduce the dimension of the DWT. Since the main features locate at the first rows or columns, we select only the first forty rows of the PCA matrix. The PCA factors of each image are obtained by multiplying the MFpca in the Vectordata.

### B. Neural NetworkTraining

Here, FNNs with three layers are used to adjust automatically the robust and fragile watermark strengths  $(\alpha_{1},\alpha_{2})$  to the most acceptable values. The resulting PCA coefficients of each image are considered as the inputs to the FNN.

A training sample set of 20 different standard grayscale images of size 512×512, such as *Elaine*, *Boat*, *Couple*, *Cat*, *Mount hood*, *House*, *Man*, *Harbour*, *Car* and *Bridge*, were considered. The training targets were obtained by exhaustive subjective experiments using many different values of  $\alpha_l$  and  $\alpha_2$ .

Before training, all the inputs and targets have to be scaled so that they always fall within a specified range. In the case of inputs (X), they are normalized in order to be in the range [-1, 1] according to equation (15). The outputs (Y) are normalized to the range [0, 1] according to equation (16)[32].

$$\bar{X}_{i} = \frac{2X_{i} - X_{\text{max}} - X_{\text{min}}}{X_{\text{max}} - X_{\text{min}}}$$
(15)

$$\overline{Y_i} = \frac{Y_i - Y_{\min}}{Y_{\max} - Y_{\min}} \tag{16}$$

To obtain the watermarked image the IDWT is carried out on the analysed sub-bands.

# 4- WATERMARK EXTRACTIONALGORITHM

The block diagram of the proposed watermark extraction is shown in Figure 6. Here, the same calculations as in the watermark embedding stage are carried out for  $\Delta_1$  and din HL3 and LH3 sub-bands to calculate the closest integer to d. With regard to being even or odd, the intended one or zero bit is specified. Since each bit of the watermark is embedded in 2 different locations of these sub-bands, two values of d are obtained for each bit of watermark. Suppose there are 2 different quantities  $d_i$ , i=1, 2 for each bit of watermark. An appropriate method should be adopted in order to make decision between these 2 quantities.

We use fuzzy mean [33] of  $d_1$ , and  $d_2$ . The  $\hat{B}_i$  value is calculated as:

$$\hat{B}_{i} = 1 - 2 \times |d_{i} - round(d_{i})| = 1, 2$$
 (17)

Where  $\hat{B}_i$  represents the fuzzy membership of each evidence. The vote of each evidence is calculated as:

$$V_{i} = \begin{cases} -1 & \text{if round } (d_{i}) \text{ is even} \\ \\ +1 & \text{if round } (d_{i}) \text{ is odd} \end{cases}$$
 (18)

Where round is used for rounding the nearest integer of its argument. The decision criteria is computed as:

$$\sigma = \sum_{i=1}^{2} (\hat{B}_i \times V_i) \tag{19}$$

Ultimately the value of  $w_j$  bit is specified according to equation 20.

$$w_{j} = \begin{cases} 0 & if \sigma < 0 \\ 1 & if \sigma > 0 \end{cases}$$
 (20)

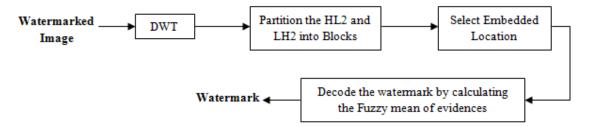


Figure 6: Block diagram of the proposed watermark extraction method

Since each 4×4 block in a watermarked image is corresponding to just one pixel of HL2 and LH2 subbands, the detection of image manipulation is executed on these blocks. Each of these pixels is placed in the vertical and horizontal quantized aforementioned small blocks.

Two values of  $\Delta_2$  are obtained from HL2 and LH2, named  $\Delta_{2,\nu}$  and  $\Delta_{2,h}$ , respectively. In addition there are two values of d,  $(d_1, d_2)$  for each of these sub-bands. Totally 4 values of d, as  $d_{1,h}$ ,  $d_{2,h}$ ,  $d_{1,\nu}$  and  $d_{2,\nu}$  are obtained. To check that a 4×4 block is tampered or not, the membership of the each evidence for that block is obtained as:

$$B_{i,n} = 1 - 2 \times |d_{i,n} - round(d_{i,n})| = 1, 2, n = h, v$$
 (21)

The vote of each evidence is calculated as:

$$V_{i,n} = \begin{cases} -1 & \text{if round } (d_{i,n}) \text{ is odd} \\ \\ +1 & \text{if round } (d_{i,n}) \text{ is even} \end{cases}$$
 (22)

Ultimately the fuzzy mean for each 4×4 block j of watermarked image is calculated as:

$$\sigma_{j} = \sigma \times \sum_{i,n} (V_{i,n} \times B_{i,n})$$
(23)

A negative value for  $\sigma_j$  indicates manipulations present in each block, while a positive  $\sigma_j$  confirms no manipulations.

### 5-EXPERIMENTAL RESULTS

The proposed watermarking method is implemented in MATLAB. Five gray scale images, "Lena", "Baboon", "Airplane", "Barbara", "Goldhill" are used as test images. All test images are of size  $512 \times 512$  and the watermark is a  $32 \times 32$  binary image. Table 1 depicts the watermark and watermarked image of the original images.

Evaluation of the watermarked image quality is based on Peak Signal to Noise Ratio (PSNR); given as:

$$PSNR = 10\log_{10} \frac{255^2}{MSE}$$
 (24)

Where MSE is the mean-square error between the watermarked and original images; defined as:

MSE = 
$$\frac{1}{M \times N} \sum_{i=1}^{i=M} \sum_{j=1}^{j=N} (I(i, j) - IW(i, j))^2$$
 (25)

Where M and N are the rows and columns of host image, I(i, j) and IW(i, j) represent the original and watermarked images.

Since the watermarks are embedded in 2 sub-bands of HL3, LH3 and different locations blocks specified in HL2 and LH2, we may use an FNN for each part (sub-band or block) and calculate the average of FNN outputs to determine the robust and fragile watermark strengths. Each estimator is a three-layer FNN. The numbers of neurons in hidden and output layers are 40 and 1 respectively. 20 samples are used for training each part estimator. Levenberg-Marquardt training algorithm was selected to train the networks. Training continues until the MSE is less than 5e-5. The hidden layer transfer function is considered to be sigmoid, and linear for the output layer.

	Table1: Original, Water	nark, and <mark>V</mark>	Watermarke	ed test images		
		Waterma	rk Image			
Image	original	Image	Size	Watermarked		
Size	Image	-		Image		
	H					
512×512	The state of the s		32×32	star nes		
		K				

Table 2 shows the robust and fragile watermark strengths ( $\alpha_1,\alpha_2$ ) obtained for the five different test images along with their respective PSNR values.

Table 2: Watermark strength with their respectivePSNR Values

Image	$\alpha_1$	α2	PSNR(db)
Lena	0.43	0.2	45.76
Baboon	0.76	0.39	41.45
Airplane	0.57	0.28	43.75
Barbara	0.46	0.24	45.25
Goldhill	0.67	0.32	42.23

We tested the watermarked images under the attacks of JPEG compression, median filter, and noise addition. The quality of watermark extracted from embedded image is evaluated by the Normalized Correlation (NC)between the embedded W(i,j) and extracted watermark  $\hat{W}(i,j)$  defined as:

$$NC = \frac{\sum_{i} \sum_{j} W(i, j).\hat{W}(i, j)}{\sum_{i} \sum_{j} [W(i, j)]^{2}}$$
(26)

The robustness against JPEG compression with different quality factors and median filter attacks are shown in Table 3.

Table 3: NC values after attacked by JPEG compression with the quality factor (QF) (25, 40, 60, 80, 90, 100), and median filter (3×3, 5×5, 7×7)

	JPEG compression				Median filter				
Image	QF=25	QF=40	QF=60	QF=80	QF=90	QF=100	(3×3)	(5×5)	(7×7)
Lena	0.756	0.952	0.957	0.983	0.991	1	0.994	0.842	0.655
Baboon	0.841	0.964	0.971	0.992	0.997	1	0.921	0.681	0.463
Airplane	0.711	0.916	0.938	0.966	0.971	0.982	0.965	0.772	0.548
Barbara	0.773	0.954	0.959	0.985	0.992	0.995	0.982	0.823	0.661
Goldhill	0.815	0.958	0.968	0.988	0.995	1	0.941	0.716	0.497

Figures 7 and 8 demonstrate the ability of the proposed method in tamper detection.



Figure 7: (a) Baboon was tampered, (b) Detected tampering image

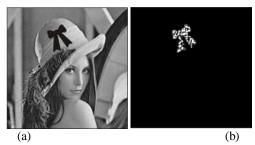


Figure 8: (a) Lena was compressed with Q=70 then was tampered, (b) Detected tampering image

Finally the proposed method is compared with the methods presented in [16-18], which also apply wavelet quantization for blind watermarking, using the Lena image. The results are shown in Table 4. The proposed method gains a better PSNR for the watermarked image and is more capable of resisting several attacks; especially filtering attacks such as median and adding noises.

Table 4: Comparing watermark NC values of the proposed method with the methods presented in [16-18] for various attacks.

· · · · · · · · · · · · · · · · · · ·						
Attack	Ref. [17]	Ref. [16] (PSNR=44.25)	Ref. [18] (PSNR=42.02)	Proposed method (PSNR=45.76)		
Median filter (3×3)	NA	0.88	0.90	0.99		
Median filter (5×5)	NA	0.74	0.76	0.84		
Median filter (7×7)	NA	0.57	0.53	0.65		
JPEG(QF=25)	NA	0.80	0.74	0.76		
JPEG(QF=60)	0.99	0.99	0.95	0.96		
JPEG(QF=80)	1	1	0.99	0.98		
JPEG(QF=100)	1	1	1	1		
Gaussian Noise	0.89	NA	0.81	0.90		
Salt-pepper	0.88	NA	NA	0.88		

#### 6- CONCLUSION

A digital watermarking algorithm based on feed-forward neural networks was presented. The host image was decomposed into wavelet domain. The wavelet coefficients were grouped into different blocks and watermark bits embedded by changing the values of appropriately selected sub-band coefficients. It was shown that neural networks can satisfactorily maximize the watermark strength using proper trainings; in addition to being adaptive based on the knowledge of the image block features. The simulation results illustrated that the values of PSNRs of the watermarked images in the proposed method are always greater than 40 db and it can represent acceptable robustness against more frequent attacks; especially filtering attacks such as median, and also noise addition. After undergoing these attacks, the extracted watermark can still be recognized clearly. Moreover, the proposed method is capable of detecting even minor changes in the watermarked image and determining where such changes take place. The tamper detection ability of the proposed scheme was shown experimentally, besides high robustness to different types of attacks such as filtering and noise addition.

#### REFERENCES

- [1] Cox, I.J. and M.L. Miller, 1997. A Review of Watermarking and the Importance of Perceptual Modeling. In Proceedings of the International Conference on Human Vision and Electronic Imaging II, San Jose, pp. 92-99.
- [2] Moulin, P. and R. Koetter, 2005. Data-Hiding Codes. In Proceeding of the IEEE, 93(12): 2083–2126.
- [3] Langelaar, G. C., I. Setyawaan, and R. L. Lagendijk, 2000. Watermarking Digital Image and Video Data: A State-of-the-Art Overview, IEEE Signal Processing Magazine, 17(5): 20-46.
- [4]Phadikar, A., S. P. Maity, and M. Mandal, 2010. QIM Data Hiding for Tamper Detection and Correction in Digital Images Using Wavelet Transform. 23rd Canadian Conference on Electrical and Computer Engineering, pp: 1-5.
- [5] Maeno, K., Q. Sun, S. F. Chang, and M. Suto, 2006. New Semi-fragile Image Authentication Watermarking Techniques Using Random Bias and NonuniformQuantization. IEEE Transaction on Multimedia, 8(1): 32-45.
- [6] Kundur, D., and D. Hatzinakos, 1999. Digital Watermarking for Telltale Tamper Proofing and Authentication. In Proceedings of IEEE, 87(7): 1167-1180.
- [7] Lin, S. D., Y. C. Kuo, and Y. H. Huang, 2006. An Image Watermarking Scheme with Tamper Detection and Recovery. International Conference on Information and Control, Beijing, pp. 74-77.
- [8] Iwata, M., T. Hori, A. Shiozaki, and A. Ogihara, 2010. Digital Watermarking Method for Tamper Detection and Recovery of JPEG Images. International Symposium on Information and its Applications, Taichung, pp: 309-314.
- [9] Hsieh, M.S., D.C. Tseng and Y.H. Huang, 2001. Hiding Digital Watermarks Using Multiresolution Wavelet Transform. IEEE Transactions on Industrial Electronics, 48(5): 875-882.
- [10] Mukherjee, D.P., S. Maitra and S.T. Acton, 2004. Spatial Domain Digital Watermarking of Multimedia Objects for Buyer Authentication. IEEE Transactions on Multimedia, 6(1): 1-15.
- [11] Doncel, V.R., N. Nikolaidis and I. Pitas, 2007. An Optimal Detector Structure for the Fourier Descriptors Domain Watermarking of 2D Vector Graphics. IEEE Transactions on Visualization and Computer Graghics, 13(5): 851-863.

- [12] Rosa, A. D., M. Barni, F. Bartolini, V. Ceppellini, and A. Piva, 1999. Optimum Decoding of Non-additive Full Frame DFT Watermarks, In Proceedings of the International Conference on Information Hiding, Germany pp: 159-171.
- [13] Cox, I.J., J. Kilian, F.T. Leighton, and T. Shamoon, 1997. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transactions on Image Processing, 6(12): 1673-1687.
- [14] Hernandez, J. R., M. Amado, and F. P. Gonzalez, 2000. DCT-domain Watermarking Techniques for Still Images: Detector Performance Analysis and a New Structure. IEEE Transaction on Image Processing, 9(1): 55-68.
- [15] Bao, P. and X. Ma, 2005. Image Adaptive Watermarking Using Wavelet Domain Singular Value Decomposition. IEEE Transactions on Circuits and Systems for Video Technology. 15(1): 96–102.
- [16] Lin, W.H., S.J. Horng, T.W. Kao, P. Fan, C.L. Lee, Y. Pan, 2008. An Efficient Watermarking Method Based on Significant Difference of Wavelet Coefficient Quantization. IEEE Transactions on Multimedia, 10(5): 746-757.
- [17] Patel, D. and S. Patnaik, 2011. Robust Image Watermarking Based on Average and Significant Difference. In Proceedings of the World Congress on Engineering and Computer Science, San Francisco, pp. 495-498.
- [18] Lin, W. H., Y. R. Wang, S. J. Horng, T. W. Kao, and Y. Pan, 2009. A Blind Watermarking Method Using Maximum Wavelet Coefficient Quantization. International Journal of Expert Systems with Applications, Elsevier, 36(9): 11509-11516.
- [19] Me, L., and G.R. Arche, 2001. A Class of Authentication Digital Watermarks for Secure Multimedia Communication. IEEE Transaction on Image Processing, 10(11): 1754-1764.
- [20] Bazargani, M., H. Ebrahimiand R. Dianat, 2012. Digital Image Watermarking in Wavelet, Contourlet and Curvelet Domains. Journal of Basic and Applied Scientific Research, 2(11): 11296-11308.
- [21] Wu, M. and B. Liu, 2003. Data Hiding in Image and Video .I. Fundamental Issues and Solutions. IEEE Transactions on Image Processing, 12(6): 685–695.
- [22] Mairgiotis, A.K., N.P. Galatsanos, and Y.Yang, 2008. New Additive Watermark Detectors Based on A Hierarchical Spatially Adaptive Image Model. IEEETransactions on Information Forensics and Security, 3(1): 29–37.
- [23] Yang, Q.T., T.G. Gao and L. Fan, 2010. A Novel Robust Watermarking Scheme Based on Neural Network. International Conference on Intelligent Computing and Integrated Systems. Guilin, pp: 71-75.
- [24] Mei,S.C., R.H. Li, H.M. Dang, Y.K. Wang, 2002. Decision of Image Watermarking Strength Based on Artificial Neural-networks.In Proceedings of the 9<sup>th</sup> International Conference on Neural Information Processing, pp: 2430-2434.
- [25] Davis, K.J. and K. Najarian, 2001. Maximizing Strength of Digital Watermarks Using Neural Networks. International Joint Conference on Neural Networks. Washington DC, pp. 2893-2898.
- [26] Xia, X., C. Boncelet, and G. Arce, 1998. Wavelet Transform Based Watermark for Digital Images. Optics Express, 3(12): 497-511.
- [27] Shensa, M.J., 1992. The Discrete Wavelet Transform: Wedding the A Trous and Mallat Algorithms. IEEE Transactions on Signal processing, 40(10): 2464-2482.
- [28]Qianhui, Yi. and K. Wang, 2009.An Improved Watermarking Method Based on Neural Network for Color Image. International Conference on Mechatronics and Automation. Changchun, pp. 3113-3117.
- [29] Hagan, M.T. and M.B. Menhaj, 1994. Training Feedforward Networks with the Marquardt Algorithm.IEEE Transactions on Neural Networks. 5(6): 989-993.
- [30] Cohen, A., I. Daubechies and J.C. Feauveau, 1992. Biorthogonal Base of Compactly Supported Wavelets. Communications on Pure and Applied Mathematics, 45(5): 485-560.
- [31] Xie, L. and G.R. Arce, 1998. Joint Wavelet Compression and Authentication Watermarking. International Conference on Image Processing, pp: 427-431.
- [32] Frank, H.L.L., Z.Y. Chen, L. Tang, 2005. Novel Perceptual Modeling Watermarking with MLF Neural Networks. International Journal of Information Technology, 1(1): 40-43
- [33] Myeongsu, K., T.H. Linh, K. Yongmin, H.K. Cheol, K.J. Myon, 2011. Image Watermarking Using A Dynamically Weighted Fuzzy C-means Algorithm. Optical Engineering, 50(10): 1-9.