International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 10, October-2014, pp: (145-154), Impact Factor: 1.252, Available online at: www.erpublications.com

A New Robust Digital Image Watermarking Based on Statistical Information of Wavelet Coefficients Transform and Back-Propagation Neural Network

Ayoub Taheri
Group of IT Engineering, Payam Noor University, Broujen , Iran

ABSTRACT: A new digital image watermarking algorithm based on the statistical Information and relations between wavelet coefficients of image and Back-Propagation neural network (BPNN) is proposed. The BPNN is a type of supervised learning neural networks. It is a very popular in neural networks. Using improved BPNN, the watermark can be embed into Discrete Wavelet Transform (DWT), which can reduce the error and improve the rate of the learning, the trained neural networks can recover the watermark from the watermarked images. The BPNN, gains statistical information of wavelet coefficients that is important for robustness and transparency of watermarking algorithm. The proposed method has good imperceptibility on the watermarked image and superior in terms of Peak Signal to Noise Ratio (PSNR). The implementation results show that the watermarking algorithm has very good robustness to all kind of attacks.

KEYWORDS: Digital Image Watermarking, Discrete Wavelet Transform, Back-Propagation Neural Network

1. INTRODUCTION

Digital watermarking is an important and useful technology for protecting the copyright of content and for preventing misuse of multimedia that increases with the rapid development of the internet. This technology embeds a signal (called a watermark) which identifies specific information of a copyrighter or owner in content itself without distortion of the quality. This content may be a text, audio, and video, but most of the time watermarking is applied to still images. The watermarking applications are authentication, finger printing, integrity verification, copyright protection, copy protection, and broadcast monitoring. Watermarking has several properties such as invisibility, robustness, and security. The inserted watermark must be imperceptible is Invisibility. The watermark intentional or unintentional removal should be impossible without damaging the original data is robustness. Security means extraction must be impossible for any unauthorized person even if the insertion algorithm is public. The digital watermarks can be divided into three different types according to perceptibility of watermark are as follows; A watermark which is quite visible is known as visible watermark, A watermark which is invisible but robust in nature is known as invisible-Robust watermark. A watermark is invisible and not robust to noise is known as invisible- Fragile watermark. The image watermarking algorithms can be classified into two categories: spatial-domain techniques and frequency-domain techniques [2]. The spatial-domain techniques directly modify the intensity values of some selected pixels while the frequency domain techniques modify the values of some transformed coefficients. The watermarking scheme based on the frequency domains can be further classified into the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT) and Discrete Wavelet Transform (DWT) domain methods [8]. The watermark is embedded in transformed coefficients of the image such that the watermark is invisible and more robust for some image processing operations [3].

2. SCHEME DESIGN

Scheme design is organized as follows; Scrambling Watermark is given in section A. DWT techniques are discussed in section B. The training of BPNN is described in section C. The Watermark embedding process is presented in section D. The Watermark extracting process is shown in section E.

A. Watermark Scrambling

Original watermark is the logo of company or institute where is a black-white image with size 64×64; the entries of this image are zero and one values. Scrambling can be implemented in both spatial domain such as color space, position space, and frequency domain of a digital image, which is regarded as a cryptographic method to an image, allows rightful users to choose proper

algorithm and parameters easily. As a result, the illegal decryption becomes more difficult, and security of the watermark more strengthened. Scrambling image in spatial domain is to change correlation between pixels, leading to the image beyond recognition, but maintain the same histogram. In a practical application, the scrambling algorithm with small computation and high scrambling degree is needed. This paper applies the famous toral Auto orphism mapping, Arnold transformation [4], which was put forward by V. I .Arnold when he was researching ring endomorphism, a special case of toral Auto orphism. Arnold transformation is described as the following formula:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 64 \qquad (1)$$

Where x,y is the coordinates of a point in the plane, and x',y' is the ones after being transformed. The constant, 64 is relevant to original watermark image size. Arnold transformation changes the layout of an image by changing the coordinates of the image, so as to scramble the image. Furthermore, the transformation with a periodicity like T, the watermark image goes back to its original state after T transformations. In the recovering process, the transformation can scatter damaged pixel bits to reduce the visual impact and improve the visual effect, which is often used to scramble the watermark image. In this paper, the periodicity T is for 24, scrambling process is displayed as the following Figure 1(a) ~ (d), which are original watermark image, 6, 12, and 24 Arnold transforming effect. For T, here is for 24, the 24 transforming is equivalent to the recovering effect. Let T=k1+k2, Scrambling the watermark image k1 times before embedding it, then after extracting scrambled watermark form watermark image, k2 times of transformation can recover the original extracted watermark, where k1, and k2 are secret keys. After scrambling watermark image, it is arranged to one dimensional array W (k), where k=1, 2… 64×64

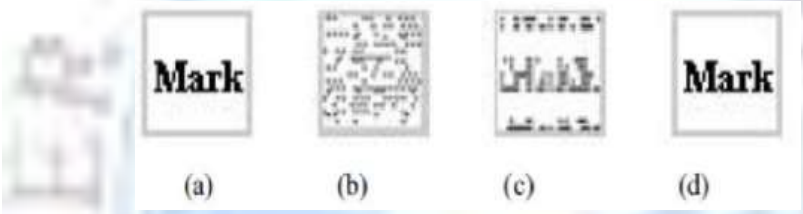

Figure 1: Image effect after being Arnold transformed

B. Discrete Wavelet Transform

The wavelet transform is based on small waves. It was in 1987 when the wavelets became the base of the multi-resolution analysis. In two-dimensional DWT, each level of decomposition produces four bands of data, one corresponding to the low pass band (LL), and three other corresponding to horizontal (HL), vertical (LH), and diagonal (HH) high pass bands. The decomposed image shows an approximation image in the lowest resolution low pass band, and three detail images in higher bands. The low pass band can further be decomposed to obtain another level of decomposition. **Error! Reference source not found.** shows three levels of decomposition. Watermark data inserted into low frequencies is more robust to image distortions that have low pass characteristics like filtering, loss compression, and geometric manipulations but less robust to changes of the histogram such as contrast/brightness adjustment, gamma correction, and cropping [9], [11]. On the other hand, watermark data inserted into middle and high frequencies is typically less robust to low-pass filtering, loss compression, and small geometric deformations of the image.

The proposed method uses the wavelet domain in frequency domain techniques. Because, compared to DCT and DFT the wavelet transform is performed a multi resolution analysis is good localization in frequency domain and DWT is higher flexibility. The watermark is embedded only into the following sub bands: HL3, LH3, HH3, HL2, LH2, HH2, HL1, and LH1. In our scheme, scaling coefficients LL3 and coefficients in HH1 are not used for embedding the watermark since embedding in LL3 will degrade the watermarked image while embedding the watermark in sub band HH1 will make the watermark more susceptible [1]. These selected sub bands are divided into non-overlapping 3-by-3 blocks and then scanned to arrange into a sequence of blocks with the sub band order that mentioned above. The relationship between wavelet coefficients and its neighborhoods in a 3-by-3 block is memorized by a given BPNN for watermark embedding and extracting processes**.**

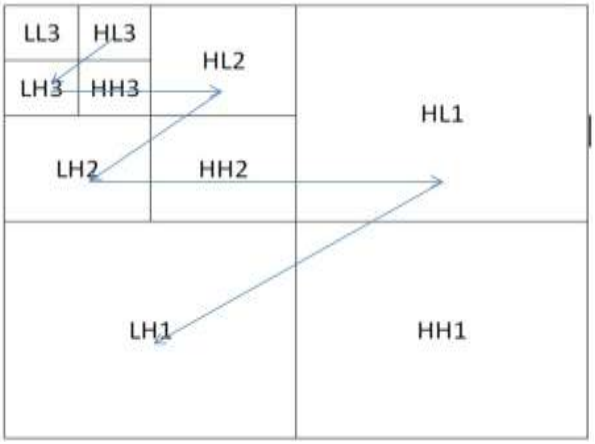

Figure 2: Three level decomposition of 2-D DWT coefficients

The method to select a position of embedding watermark was as following: Calculate the variance of each block, and arrange the variance in ascending order, then choose the block center coefficient, which the first Lw variance corresponding to, as an embedding position, where Lw indicated the size of the watermark sequence (i.e. 64×64). The position of embedding watermark must be known first when extract the watermark, so It is necessary to save the position matrix as a file by using the save command in MATLAB. The position matrix saves as a secret key K for further use in watermark extracting process. The organization of coefficients block is shown in Figure 3.

$S_{i-1,j-}$	$S_{i-1,j}$	$S_{i-1,j+}$
$S_{i,j-1}$	$S_{i,j}$	$S_{i,j+1}$
$S_{i+1,j-}$	$S_{i+1,j}$	$S_{i+1,j+}$

Figure 3: 3×3 coefficients block of wavelet

The average formula for each block is:

$$mean = \frac{1}{9} \sum_{u=-1}^{u=1} \sum_{v=-1}^{v=1} s(i+u, j+v) \qquad (2)$$

The formula of computing variance for each block is:

$$Var = \frac{1}{8} \sum_{u=-1}^{u=1} \sum_{v=-1}^{v==1} (s(i+u, j+v) - mean)^2 \qquad (3)$$

$s(i+u\ j+v)$ represent the wavelet coefficients of each block; $s(i, j)$ represent the wavelet coefficients of the center position in each block. Variable; u, v is the variation that other coefficients relative to the center position.

C. The training of BPNN

The BPNN is one type of supervised learning neural networks. It is a very popular modal and most frequently used learning techniques in neural networks.

Figure, shows the general types of Neural Network. As a widely used feed-forward neural network, order to obtain minimum mean squared error between expected outputs and actual outputs, BPNN can fix the network weights by using mean squared error and gradient descent methods. A variety of watermarking techniques have been come up recently, many

of which are based on neural networks [5], [6], [10].

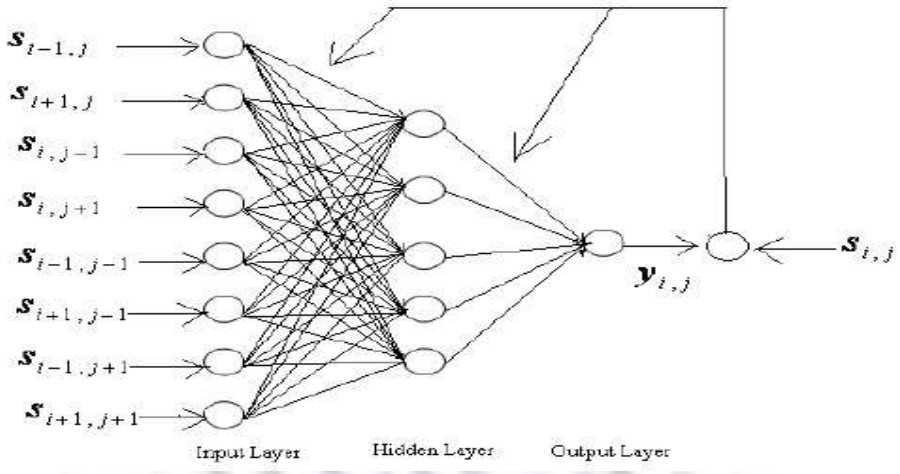

Figure 4: The BPNN structure

A typical BPNN architecture with three layers is depicted in Fig. 4, which consists of an input layer, hidden layer, and output layer. Each layer has one or more neurons and each neuron is fully connected to its adjacent layers. Two neurons of each adjacent layer are directly connected to one another, which is called a link. Each link has a weighted value, representing the relational degree between two neurons. The numbers of input nodes and output neurons of neural network can be easily determined according to the practical problem. The wavelet coefficients of selected blocks, based on max variance except center coefficient, are considered as input vector that is an array with 8 elements, so the number of input neurons is 8. The desired output is the value of center coefficient of each selected block. The training process performs for each block separately. By selecting these values for input vector and desired output, the final output of BPNN has the statistical information of center coefficient relative to adjacent coefficients in each selected block, which is very important for robustness and transparency of watermarking algorithm. The input vector is represented as x, the initial weights of back propagation neural network are initialized at x values. The number of hidden neurons is calculated by following relation:

$$N = \sqrt{nm + 1.7n + 1} \qquad (4)$$

Where n is the number of input neurons, and m is the number of output neurons. In this paper, n=8, m=1, N =4.7, taking N=5. Find the output of hidden unit (h_j) and the output unit (a) by using activation functions.

$$h_j = \sum_{i=1}^{8} x_i g_{ij} \qquad (5)$$

$$a = f\left(\sum_{j=1}^{5} h_j m_j\right) \qquad (6)$$

Here g_{ij} and m_{jk} are input and hidden synaptic weights in neural network. Activation function f is sigmoid, which is given as:

$$f(x) = \frac{1}{1 + e^{-x}} \qquad (7)$$

Calculating the error (e) which is the different between the actual output (a) and the desired output (d) is easily measured at the output layer by using equation:

$$e = (d - a) f'\left(\sum_{j=1}^{5} h_j m_j\right) \qquad (8)$$

Calculating the error correction term, updating the weight between the output layer and hidden layer is measured by using equation:

$$\Delta(m_j) = \alpha.e.h_j \qquad (9)$$

The modified weight can be calculated as follows:

$$m_j(new) = m_j(old) + \Delta(m_j) \qquad (10)$$

The error information term (e_j) is calculated as follows:

$$e_j = e.m_j f'\left(\sum_{i=1}^{8} x_i g_{ij}\right) \qquad (11)$$

On the basis of e_j, update the weight between the hidden layer and input layer is measured by using equation:

$$\Delta(g_{ij}) = \alpha e_j x_i \qquad (12)$$

The modified weight can be calculated as follows:

$$g_{ij}(new) = g_{ij}(old) + \Delta(g_{ij}) \qquad (13)$$

After change the weight, check reaches the closured output. Otherwise repeat the step until actual output equal the desired output. The BP neural network in order to speed the convergence to an optimal weight assignment, introduce momentum coefficient [7]. The leaning rate (α) affects the convergence of BPNN. A large value of a may speed up the convergence but result is overshooting, smaller value of α has vice-versa effect. The large learning rate leads to rapid learning but there is oscillation of weights, so avoid there problem any adding a momentum factor to the normal gradient descent learning rate. Then weights updating formula

$$\begin{aligned} m_j(t+1) &= m_j(t) + \alpha e h_j \\ &+ \eta[m_j(t) - m_j(t-1)], \\ g_{ij}(t+1) &= g_{ij}(t) + \alpha e_j x_i \\ &+ \eta[g_{ij}(t) - g_{ij}(t-1)] \end{aligned} \qquad (14).$$

Here η is called the momentum factor. It ranges from

$0<\eta<1$.

D. Watermark embedding process

The flowchart of embedding process is shown in

Figure. The watermark bits after being scrambled with a secret key are entered to the embedding process to be embedded into the selected block center coefficients according to

$$S_w(i,j) = \bar{S}(i,j) + \beta(2W(k) - 1) \qquad (15)$$

Where β is the watermarking factor, and can be altered to obtain the imperceptibility and robustness. If β is small, we get the higher quality of watermarked image, but lower level of robustness, and vice versa. This is a trade- off between the qualities of the watermarked image with the robustness of watermark. We apply β= 18 (which is really large for other

alternative techniques, but works well in our method) to receive a high transparency of the watermarked image and the robustness of the watermark. *W (k)* is the k^{th} watermark bit in the sequential watermark bits. $S_w(i,j)$, the watermarked coefficient, is obtained by replacing the central coefficient *S(i,j)* by the combination of the final output of BPNN $\overline{S}(i, j)$ and the watermark bit *W(k).* After embedding, an inverse DWT is performed to get the watermarked image.

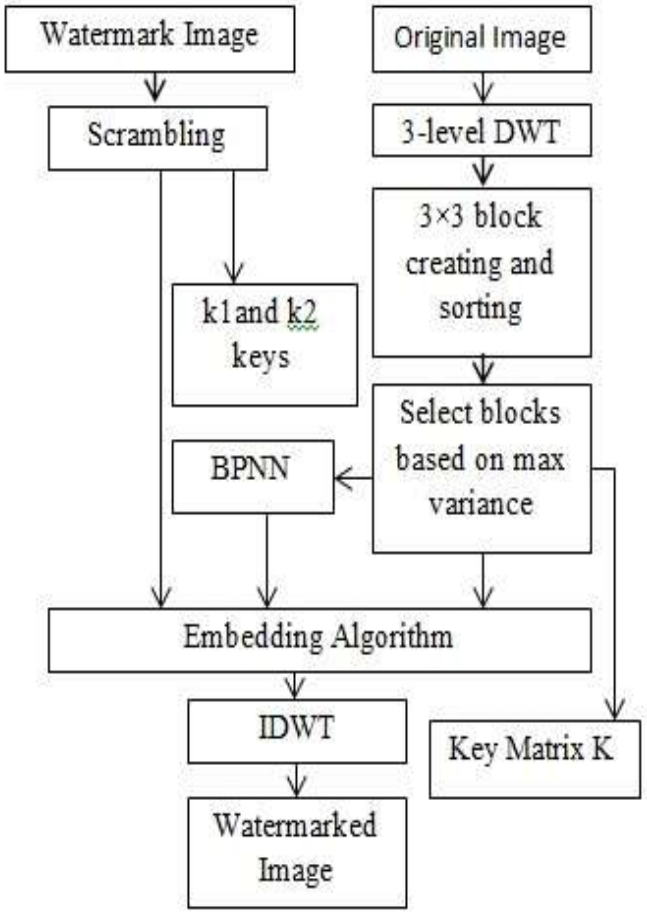

Figure 5: Watermark embedding flowchart

E. Watermark extracting process

The flowchart of process is shown in
Figure. The extraction process is the inversion of embedding process. First, the watermarked image is decomposed by 3-level DWT. The wavelet coefficients are also grouped into 3-by-3 blocks and arranged into the ordering sequence as described in Sec. B. From detected blocks based on secret key K that is saved previously, we set up input vector x and desired output d for each detected block as discussed in Sec. C.

The BPNN is used to extract the scrambled watermark. For each input vector x the BPNN produces the output $\overline{S_w}(i, j)$; the scrambled watermark bit extraction is performed by

$$W'(k) = \begin{cases} 1 & S_w(i, j) \geq \overline{S_w}(i, j) \\ 0 & otherwise \end{cases} \qquad (16)$$

Where, $S_w(i,j)$ is the center coefficient of detected block for watermarked image, $W'(k)$ is the scrambled watermark bit, after obtaining all of watermark bit, W' is the scrambled watermark sequence, then it is descrambled using the secret key k_2 to obtain the extracted logo watermark.

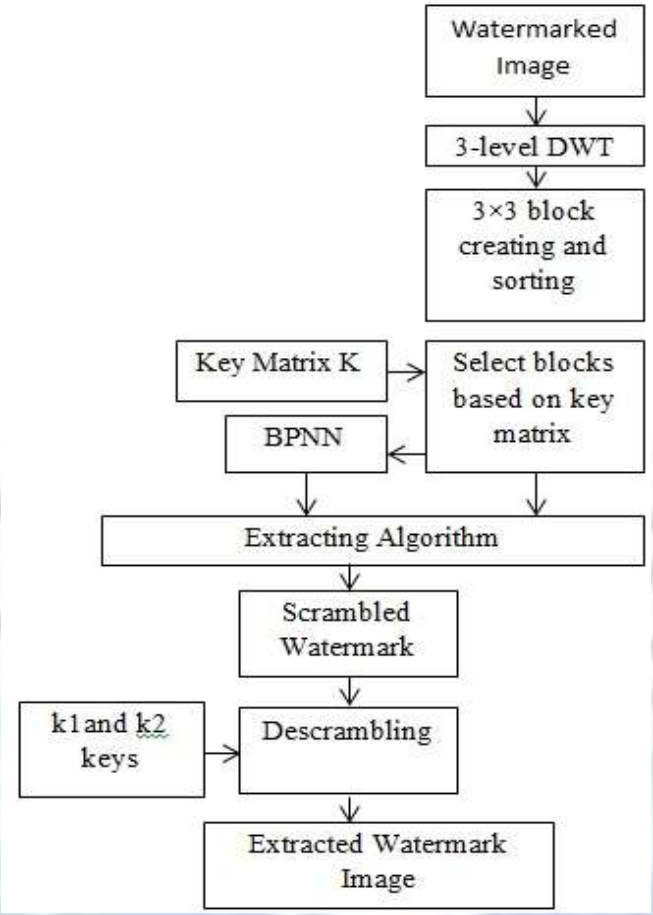

Figure 6: Watermark extracting flowchart

3. IMPLEMENTATION RESULTS

The original and watermarked images have been shown in
Figure and Figure. Cameraman, images has been used to implement the watermarking algorithm. Original Watermark is a binary image and its size is 64 × 64. The original watermark image is shown in Figure.

Figure 7: Original Cameraman image.

Extracted watermarks after some kind of attack on mentioned watermarked images have been shown in Figure. The performed attacks on the watermarked images are as follows: Gaussian noise; median filtering 3*3; low pass filtering; and resizing 1/5 the image; jpeg compression with quality factors of 10, 25, 50, and 90 and finally jpeg 2000 compression with bit rate 3 .

Figure 8: Watermarked Cameraman image.

The estimate of similarity between the extracted watermark image and the original watermark image according to relation (17), along the peak signal to noise ratio (PSNR) of watermarked image and Original image, to relation (18), were calculated having performed each one of the mentioned attacks on the watermarked image, and results have been integrated in table (1).

$$SIM(W,W') = \frac{W.W'}{W.W} \qquad (17)$$

$$PSNR = 10\log\left(\frac{255}{\sum_{i,j} I(i,j) - I_w(i,j)}\right)^2 \qquad (18)$$

In relation (17) W is the original watermark and W' is the Extracted logo watermark image. Dot operation in this relation is explanatory sum of product of respective entries between matrix W and W'. Square operation is explanatory sum of product of each entry of matrix W with itself.

Figure 9: Original Watermark

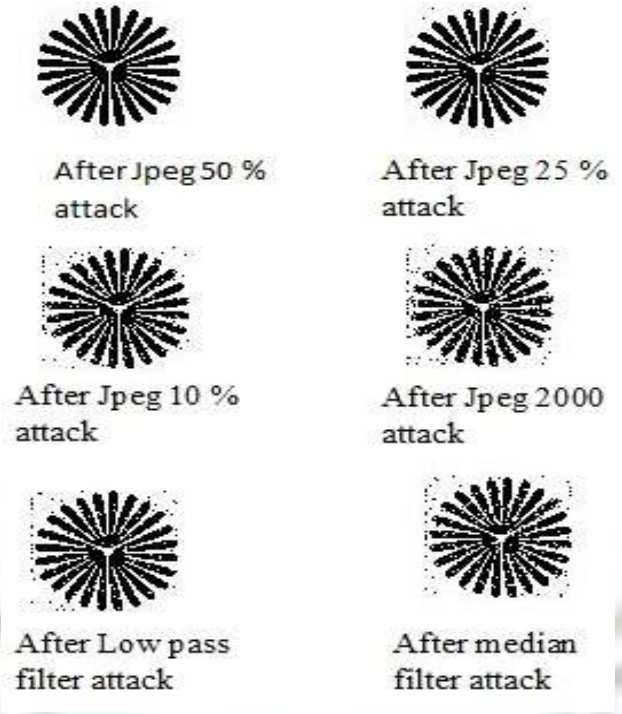

Figure 10: Extracted logo watermarks after some kinds of watermarking attack on the watermarked image.

TABLE 1: IMPLEMENTATION RESULTS AND COMPARISONS

Kind of attack	Our method		Method in [12]	
	SIM	PSNR	SIM	PSNR
Gaussian Noise	94.4	32.15	93.5	31.44
Low Pass Filter	92.5	31.0	-	-
Median Pass Filter	88.1	30.7	85.95	32.7
Scaling 1/5	84.5	27.3	88.1	28.5
JPEG 90%	96.0	38.2	91.2	37.7
JPEG 50%	93.7	37.2	89.4	33.5
JPEG 25%	90.0	33.0	86.3	29.8
JPEG 10%	87.2	24.2	81.2	24.1
JPEG 2000 with bit rate 3	83.7	22.0	-	-

REFERENCES

Periodicals:

[1]. Wang Hongjun; Li Na, "An algorithm of digital image watermark based on multiresolution wavelet analysis, " VLSI Design and Video Technology, 2005. Proceedings of 2005 IEEE International Workshop on Volume , Issue , Page(s): 2**Books:**
, 28-30 May 2005.

Books:

[2]. uCox, M.L. Miller, J.A.Bloom, "Digital Watermarking", Morgan Kaufinann, 1999.
[3]. P.Ramana Reddy, DR.Munaga.V.N.K.Prasad, DR D.Sreenivasarao "Robust Digital Watermarking of Images using Wavelets," International Journal of Computer and Electrical Engineering, Vol. I, No. 2, June 2009, pp. 1793-8163.
[4]. D.K. Arrowsmith and C.M.Place, "An Introduction to Dynamical systems", Cambridge Univ. Press 1990.

Papers Presented at Conferences (Unpublished):

[5]. Z. F. Wang, N. C. Wang, B. C. Shi, "A Novel Blind Watermarking Scheme Based on Neural Network in Wavelet Domain, "Proceedings of the 6th World Congress on Intelligent Control and Automation, Dalian, China, June 21-23, 2006.
[6]. Song Huang, Wei Zhang, Wei Feng and Huaqian Yang "Blind Watermarking Scheme Based on Neural Network", Proceedings of the 7th World Congress on Intelligent Control and Automation, Chongqing, China, June 25 - 27, 2008.
[7]. Qianhui Yi and Ke Wang, "An Improved Watermarking Method Based on Neural Network for Color Image," Proceedings of the IEEE International Conference on Mechatronics and Automation, Changchun, China, August 9 - 12, 2009.

Papers from Conference Proceedings (Published):

[8]. U.Cox, lKilian, T.Leighton, T.G.Shamoon, "Secure spread spectrum watermarking for multimedia ", In Proceedings of the IEEE International Conference on Image Processing, lCIP '97, volume 6, pages 1673 - 1687, Santa Barbara, California, USA, 1997.
[9]. P. Tao and A. M. Eskicioglu, "A Robust Multiple Watermarking Scheme in the Discrete Wavelet Transform Domain," Optics East 2004 Symposium, Internet Multimedia Management Systems Conference V, Philadelphia, PA, USA, Oct. 25-28, 2004.
[10]. Zhang, J., Wang, N.C., Xiong, F: A Novel Watermarking for Images Using Neural Networks, International Conference on Machine Learning and Cybernetics, 3(2002) 1405-1408.
[11]. Ghouti, L. Bouridane, A, "Towards a Universal Multi resolution-based Perceptual Model," Image processing, IEEE international Conference. On page(s): 449-452, 2006.
[12]. Qun-ting Yang, Tie-gang Gao, Li Fan, "A Novel Robust Watermarking Based on Neural Network," Intelligent Computing and Integrated Systems, International Conference On page(s): 71-75, 2010.