2009 International Conference on Machine Learning and Computing
IPCSIT vol.3 (2011) © (2011) IACSIT Press, Singapore

Robust and Imperceptible Image Watermarking using Full Counter Propagation Neural Networks

Summrina Kanwal Wajid[1 +], M. Arfan Jaffar[2], Wajid Rasul[3], Anwar M. Mirza[4]

[1]Alyamamah University, Riyadh, Saudia Arabia, [2,4]National University of Computer and Emerging Sciences (FAST) Islamabad, Pakistan, [3]Quaid-i-Azam University, Islamabad, Pakistan.

summrina@gmail.com, arfan.jaffar@nu.edu.pk, wajidrasul@gmail.com, anwar.m.mirza@nu.edu.pk

Abstract. Digital Media is the main source of communication now a days. A drastic change emerged with the access of internet to everyone, which made it possible to copy and distribute the digital content illegally. Digital Watermarking/Steganography has been used for digital media protection. Many techniques have been developed for effective watermarking. However, there is always a tradeoff between robustness and imperceptibility features of watermarking offered by these techniques. In this paper, we have proposed a method based on Full Counter Propagation Neural Network (FCPN) to train multiple grey or color cover images to produce a desired watermark image. We have used grey, binary and color images as watermarks. The results have proved the higher imperceptibility and robustness of this scheme when compared with the other available watermarking techniques.

Keywords: watermarking, full counter propagation neural network, PSNR

1. Introduction

A drastic change emerged with the access of internet to everyone, which made it possible to copy and distribute the digital content illegally. Work has been done continually to solve these problems and provide copyright protection and proof of ownership. Watermarking is one of them, where metadata is created containing some information about the digital content (cover work), which is to be protected, and hide into the digital content. The watermark embedded should be robust enough to survive through even distortion caused by malicious attacks.

A watermark can be embedded into spatial as well a s frequency domain. In case of spatial domain watermarking watermark is embedded by directly modifying the pixel values. Caronni proposed a tagged method for watermark embedding in spatial domain, in which he manipulated pixel blocks of N by N size [2]. Tirkel proposed another method to embed PN signal in the least significant bits (LSB) of an image pixel, in another approach PN noise is added to the LSB [3].Bender et al. proposed a method called "Pathwork" [4] in which he selected pair of pixels X_i, Y_i in an image then for each pair he added a value K to X_i while subtracting it from Y_i if the bit to embed is one (leaving pair unchanged otherwise). The extraction is processed by calculating the sum of the difference between respectively X_i, $Y_i$in the watermarked and the original image. A sum equals to 2K determines that the recovered bit is to be set to one, while otherwise to zero.

In DCT domain watermarking, image is first expressed in terms of a sum of cosine functions. Koch et al. in [5], [6] proposed watermarking scheme based on jpeg compression scheme which manipulates DCT of an image for watermarking. Tao and Dickinson in [7] proposed an adaptive DCT based watermarking scheme following JPEG compression table and claimed to resist JPEG compression down to 5% as well as random noise [7]. Der-Chyuan et al. suggested a non blind DCT domain watermarking scheme in which they embedded visually recognizable pattern of black and white pixels [8]. Xiaoyun Wu et al. suggested another method of watermarking based on Integer Wavelet Transform with Parameters [9]. Emir Ganic et al. [10]

+ Corresponding author. Tel.: +966568008095; fax: +996 1 224 1111. *E-mail address*: summrina@gmail.com.

suggested a hybrid scheme based on Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD).

Many techniques of image watermarking based on neural network have been proposed because of the fact that neural networks have best capability for pattern mapping and classification. In case of embedding and extracting water mark, they automatically select system parameter and recover watermark. Hwang et al. used back propagation neural network to design the water marking scheme [11]. Jun Zhang et al. proposed a scheme of hiding logo into an image [12]. The scheme hides logo into the multi wavelet domain using back propagation neural network (BPN). Wang Zhenfei, Zhai Gvangun, Wang and Nengchao proposed an effective blind digital watermarking algorithm based on neural network [13].

In this paper a novel scheme of image watermarking has been proposed which is based on Full Counter Propagation Network (FCPN). The specialty of this technique is its lesser complexity and easy apprehension.

Full Counter Propagation Network is the extension of Forward only Counter Propagation network with bidirectional mapping which was developed by Hecht-Neilsen and it works as a self-adapting optimal lookup table, which provides mapping between input and output layer. The architecture consist of three layers: 1. Input layer. 2. Hidden layer also called Kohonen layer as the weights between input and this layer are trained by self organizing kohonen rule. 3. Output layer is called Grossberg layer.

2. Methodology

The methodology integrates the watermark embedding and extraction into a FCPN. The algorithm has the ability to embed watermark into multiple cover images at a time, where the images and the watermark are presented into the network simultaneously. The same FCPN is used for watermark extraction too.

The s-th two-dimensional cover image Xs and watermark image Y can be written in vector form as:

$$X^s = \{x_1^s, x_2^s \ldots\ldots x_N^s\},\ Y = \{y_1, y_2, \ldots\ldots\ldots y_M\}$$

where N is the number of pixels of the s-th cover image Xs and M is the number of pixels of the watermark image Y. The input vectors Xs and Y are connected to neuron Z_i with weights W and U respectively.

$$W = \{ w_{11}, w_{12}, w_{13} \ldots w_{Nn}\}$$
$$U = \{u_{11}, u_{12}, u_{13} \ldots, u_{Mi} \}$$

where wN_i denotes the weight between N-th input xN and i-th neuron. Similarly, uM_i denotes the weight between M-th input and i-th neuron.

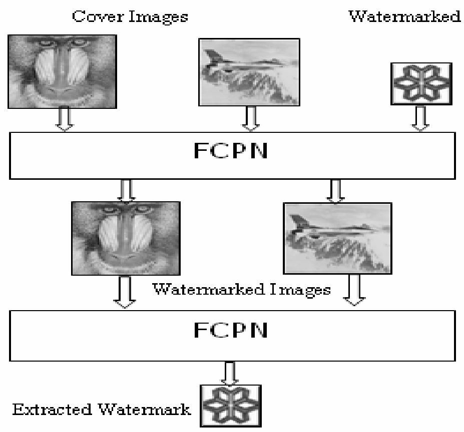


Fig. 1: The schematic block diagram of the FCPN embedding and extracting procedure.

similarly the synaptic weights can be written in a vector form as:

$$V = \{v_{11}, v_{21}, v_{31}, \ldots\ldots, v_{Ni}\} \text{ and } T = \{ t_{11}, t_{12}, t_{13} \ldots\ldots\ldots\ldots, t_{Mi}\}$$

where N and M are the number of pixels of the cover image X and watermark image Y respectively.

The neuron output Γi for the hidden layer is computed as :

$$\Gamma_j = \begin{cases} 1 & \text{if } Z_j \text{ is the smallest for all j} \\ 0 & \text{otherwise} \end{cases} \qquad (1)$$

where

$$Z_j = \sum_{k=1}^{N}(x_k - w_{kj})^2 + \sum_{k=1}^{M}(y_k - u_{kj})^2 \quad (2)$$

The neuron with weight closest to the input layer wins and its output is set to 1 where rest is assigned 0. After the winner is found the output layer is computed using equation below:

$$x_n^{s^*} = \sum_{j=1}^{J} v_{jn}\Gamma_j, n = 1, \ldots, N \quad (3)$$

and

$$y_m^* = \sum_{j=1}^{J} t_{jm}\Gamma_j, m = 1, \ldots, M \quad (4)$$

Weight between input and the hidden layer is updated using equations:

$$w_{kj}(n+1) = [1-\alpha(n)]w_{kj}(n) + \alpha(n)x_k^s, k = 1,.., N.j = 1, \ldots, J \quad (5)$$

$$u_{kj}(n+1) = [1-\alpha(n)]u_{kj}(n) + \alpha(n)y_k, k = 1,.., M.j = 1, \ldots, J \quad (6)$$

and learning rate by equation:

$$\alpha(n) = \alpha(0)exp\left(\frac{-n}{n_0}\right) \quad (7)$$

where w_{jk} is the weight between input x_k and the winning neuron Γj, and u_{kj} is the weight between input y_k and neuron Γj, and α (n) is gradually decreasing learning rate and α (0) is the initial learning rate. Weights between hidden and output layer is trained by equations:

$$v_{ji}(n+1) = v_{ji} + \beta(n)[xg_i - v_{ji}(n)]\Gamma_j, j = 1, \ldots, J.i = 1, \ldots, N \quad (8)$$

$$t_{ji}(n+1) = t_{ji} + \beta(n)[yg_i - t_{ji}(n)]\Gamma_j, j = 1, \ldots, J.i = 1, \ldots, M \quad (9)$$

where v_{ji} and tji is the weight between Γj and the output x_i, yi respectively.

After calculating the outputs X^{s^*} and Y* the output error of FCPN can be calculated as:

$$xE_i = |x_i^{s^*} - xD_i^s|, i = 1 \ldots N \quad (10)$$

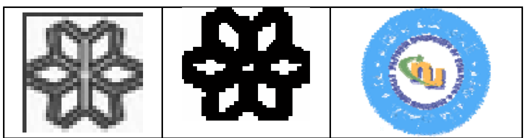
$$yE_i = |y_i^* - yD_j|, j = 1..M \quad (11)$$

where xDi is the i-th pixel value of desired watermarked image (input cover image) and yDj denote the j-th pixel value of desired watermark image (input watermark image). If the output error is less than a predefined threshold, the network converges. Otherwise, the input weight vectors W and U are updated

3. Experiments, Results and Discussion

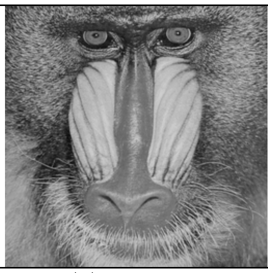
To demonstrate robustness, authenticity and imperceptibility of this technique gray scale cover images including Jet, Baboon and Couple are used where the image size is 256× 256 in each case shown in Fig. 3. In addition, the grayscale, binary and color watermark images have been used with image size 32×32 shown in Fig. 2.

The Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) were used to evaluate the quality of watermarked image and extracted watermark. The higher the value of PSNR and NC ,the more similar watermarked image and the cover image are. For further analysis of the current scheme two more metrics, Universal Image Quality Index (IQI) and Structural Similarity Metric (SSIM) which are based on HVS, has been used [14].



(a)Gray (b)Binary (c)Color

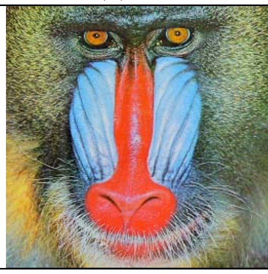
Fig. 2: Watermarked Images



(a) Baboon

(b) Jet

(c) Couple



(d) Color Baboon

Fig. 3: Cover Images

3.1. Imperceptibility

The initial learning rates α and β were set to 0.7 and 0.5 respectively. The number of neurons is taken as 64 and constant k0 was set to 10. We have calculated experimentally threshold value and that is close to 0.01.

Watermarked Image	Jet	Baboon	Couple	Extracted Watermark
PSNR	43.79	45.74	44.11	44.06
IQI	0.98	0.99	0.99	0.98
SSIM	0.99	0.99	0.98	0.99

Table 1: PSNR and IQI and SSIM of Watermarked Images after embedding grey watermark

The higher PSNR value suggests that the cover and watermarked image are quite similar. The NC value lies within the rage of 0 and 1, where in this case NC value lies near 1 suggests that the extracted watermark is very near to the original one. Image Quality Index and Structural Similarity Index guarantee the accuracy of the results. These two objective measures are based on Human Visual System(HVS). The value lying near 1 suggests that watermark is highly invisible since that difference between watermarked and cover image is small. Results are shown in Table 1.

3.2. Binary Image Watermarking

To experiment with binary watermarking, the following binary watermark has been embedded in the cover images in Fig. 3. In case of binary watermarking the PSNR value shows even better reults , meaning that watermark embedding is highly imperceptible as well as the extracted watermark is very much similar to the original one as shown in Table 2.

Watermarked Image	Jet	Baboon	Couple	Extracted Watermark
PSNR	43.79	45.74	44.11	44.06
QI	0.98	0.99	0.99	0.98
SSIM	0.97	0.99	0.98	0.99

Table 2: PSNR and IQI and SSIM of Watermarked Images after embedding binary watermark

3.3. Robustness Testing

In robustness test, we attack watermarked Jet by

1. crop right-top ¼

2. 3x3 Laplacian mask,
3. 3x3 averaging filter
4. median filter
5. Gaussian Noise
6. 2x2 mosaic and
7. JPEG compression(Q=80%)

The result had shown that still the watermark was extracted with accuracy when compared with other proposed watermarking methods. Results are shown in Table 3.

Attack	PSNR	NC
Cropped	44.7571	0.9979
Median filter	44.1576	0.9978
Sharpened	44.1576	0.9977
Blurred	44.1576	0.9975
Gaussian Noise	43.3379	0.9980

Table 3: PSNR and NC of Watermarked Images by attacking different methods

These results show that different attacks on the watermarked image do not harm the embedded watermark and we can still get the watermark very much similar to the original one.

3.4. Colored Image Watermarking

The scheme was experimented by

1. Embedding colored watermark into grayscale images.
2. Embedding grayscale watermark into colored images.
3. Embedding colored watermark into colored image.

For experimentation 24-bit colored images were used after converting them to HSV (Hue, Saturation, and Value) Model.

3.5. Colored Watermark Watermarking

For embedding colored watermark, FAST_NU logo has been taken as a watermark, which has been split into HSV channels. Watermark is embedded into the cover images shown in Fig. 3(a), (b) and (c).Each individual channel/image is then embedded into the cover images. While extracting the watermark, each individual channel image is extracted from the cover image and then the three H, S, V channel images are concatenated to get the image. Results are shown in Table 4.

Watermarked Image	Jet	Baboon	Couple	Extracted Watermark
PSNR	44.72	46.64	45.22	45.36
QI	0.99	0.99	0.99	0.98
SSIM	0.99	0.99	0.98	0.99

Table 4: PSNR and NC of Watermarked Images by embedding color watermark

The results had shown the higher imperceptibility of this algorithm since PSNR and NC values indicate the similarity between the original and watermarked image which had made embedded watermark highly imperceptible. Again in case of any attack to the watermarked image, still the extracted watermark is very similar to the original one. The results further indicate that the algorithm is rather more effective and imperceptible in case of colored image watermarking, since PSNR value is higher for watermarked image in this case, when we compare it with grayscale image watermarking. This shows that the algorithm is more suitable for colored watermarking.

3.6. Colored Watermark embedding into Colored Cover Images

For experimentation colored baboon image and colored FAST-NU logo has been used. Both cover and watermark images are first split into HSV channels and embedding of corresponding channels has been done. The result is shown in the Table 5. In case of colored images the PSNR has been calculated using following equation:

$$PSNR(dB) = 10log_{10}\left[\frac{255^2}{\frac{MSE(H)+MSE(S)+MSE(V)}{3}}\right] \quad (12)$$

where MSE is the mean square error given as:

$$MSE = \left(\frac{1}{nm}\sum_{i=1}^{n}\sum_{i=1}^{m}[x(i,j)-z(i,j)]^2\right) \quad (13)$$

Watermarked Image	PSNR	Extracted Watermark	NC	PSNR
Baboon	56.15	From Baboon	0.9986	54.10

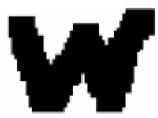
Table 5: The PSNR of the watermarked image and the Normalized correlation & PSNR of the extracted Watermark.

Similarly grayscale watermark can also be embedded into colored images

3.7. Binary Watermark embedding to Colored Cover Images

Fig. 4(a) and (b) shows the colored image and the binary watermark which has been used for this experimentation, and the results are compared with the algorithm by Bhupendara Verma et al. [15]. Bhupendara Verma et al. suggested a method in spatial domain. The blue channel of the colored images has been used for watermark embedding, which is divided into 8 by 8 blocks.

(a)Autumn



(b) Watermark Image

Fig. 4: Cover image and watermark image.

No.	Image Processing Operation	NCC Value By [15]	NCC Value.
1	Straight	1.0000	1.000
2	Wiener Filter	1.0000	1.000
3	Median Filter	1.0000	1.000
4	Scaled Down 0.75	1.0000	1.000
5	Jpeg 100	1.0000	1.000
6	Jpeg 80	1.0000	1.000
7	Cropped	0.8665	1.000
8	Rotate 17 degree	1.0000	1.000

Table 5: The Normalized correlation of the extracted Watermark after attacks on cover image

Corresponding to each bit to be inserted, the pixel intensity of the corresponding block pixels is modified according to certain rules. The watermark is extracted using non-Blind probability. Both methods results are compared below.

4. Conclusion & Future Work

The proposed watermarking algorithm is different from traditional watermarking methods as

- The watermark was embedded in the synapses of FCPN instead of the cover image.
- The network is experimented to embed multiple images with one watermark simultaneously.

- The method integrates embedding and extracting process in the same network which simplifies the task.

The proposed scheme is based on spatial domain processing, if the same scheme is used with frequency domain analysis, it might be able to improve the watermarking further.

We can further

- Do quantitative Analysis of the scheme.
- Use other type of neural networks for watermarking.
- Use other metrics instead of euclidean normal metric for cluster forming

5. References

[1] Chuan-Yu Chang , Sheng-Jyun Su, A Neural-Network-Based Robust Watermarking Scheme, *IEEE International Conference*, Volume 3, no. 10-12, pp. 2482 – 2487, October 2005.

[2] G. Caronni, Ermitteln unauthorisierter Verteiler von Maschinenlesbar Daten. ETH, Zuruch, Switzerland, *TechnicalReport*, August 1993.

[3] A.Z.Tirkel, et al., Electronic Watermarking, Proc. of Digital Image Computing Technology and Applications, Sydney, *Australia*, 1993, pp.666-672.

[4] W. Bender, D. Gruhl, N. Morimoto, Techniques for data hiding , Proc. SPIE, vol. 2420, San Jose, February 1995.

[5] E. Koch, J. Rindfrey, J. Zhao, Copyright protection for multimedia data, *Digital Media and Electronic Publishing*, 1996.

[6] Kundur. D., Hatzinakos, D., Digital Watermarking using Multiresolution Wavelet Decomposition, in Proc. IEEE Int. Conf On Acoustics, Speech and Signal Processing, Seattle,Washington, vol. 5, May 1998, pp. 2969-2972.

[7] B. Tao, B. Dickinson, Adaptive watermarking in the DCT domain. Proc. Int. *Conference Image Processing*, Lausanne, Switzerland, September 1996.

[8] L. Der-Chyuan; L. Jiang-Lung; C. Ming-Chang, Digital watermarking using multi resolution wavelet transform Security Technology, Proceedings, *IEEE 37th Annual 2003 International Carnahan Conference*, October, 2003 pp. 370-377.

[9] Xiaoyun Wu, Junquan Hu, Zhixiong Gu, Jiwu Huang, Conferences in Research and Practice in Information Technology Series; Vol. 108 archive, Proceedings of the 2005 Australasian workshop on Grid computing and e-research,- Volume 44, Newcastle, New South Wales, *Australia* pp.75– 80.

[10] Emir Ganic, Ahmet M. Eskicioglu, Robust DWT-SVD domain image watermarking: embedding data in all frequencies, International Multimedia Conference Proceedings of the 2004 workshop on Multimedia and security, Magdeburg, *Germany*, 2004, pp. 166 - 174.

[11] M.S.Hwang, C.C.Chang, and K.F.Hwang, Digital watermarking of images using neural networks, *Journal of Electronic Imaging*, 2000, 9(4)pp. 548-555.

[12] Jun Zhang, Nengchao Wang, Feng Xiong, Hiding a Logo Watermark into the Multi wavelet Domain Using Neural Networks, *Proceedings of the 14th IEEE International Conference on Tools with Artificial Intelligence (ICTAI'02)*, 2002.

[13] Wang Zhenfei, Zhai Gvangun,Wang Nengchao, Digital watermarking algorithm based on wavelet transform and neural network, in IEEE Trans. *On circuit and system for Video Technology,* vol. 9, no. 4, June 1999, pp: 545-550.

[14] Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli, Image quality assessment: From error visibility to structural similarity, *IEEE Transactions on Image Processing* , April. 2004, vol. 13, no. 4, pp. 600-612.

[15] Bhupendra Verma, Sanjeev Jain, D.P.Agarwal, Amit Phadikar, A New Color Image Watermarking Scheme, *Department of Information Technology Samrat Ashok Technological Institute Vidisha (M.P.)*, India.

[16] Imran Usman, A. Khan, Asad Ali, and Tae-Sun Choi, Reversible Watermarking based on Intelligent Coefficient Selection and Integer Wavelet Transform, *International Journal of Innovative Computing, Information and Control (IJICIC)* , 2009, Vol.5, No.12.