BACKPROPAGATION NETWORK USING TARGET WATERMARK AND RANDOM MATRICES

Dr.Ashish Bansal, Mrs.Neha Gupta
Symbiosis University of Applied Science, Indore, Ph.D Scholar Pacific University, Udaipur

Abstract: A new watermarking scheme may be based on generating random matrices using a seed key and training each matrix to produce parts of watermark using BPN, which can be united to generate the desired watermark and the seed key itself can be made hidden within the cover image. This scheme may bring promising fidelity and robustness results during gray scale watermarking.

Index terms: *watermarking, BPN, random matrices, seed key.*

I. INTRODUCTION

A Backpropagation Network may be successfully trained to generate watermark parts using random matrices generated from a seed key as inputs. These watermark parts can be united to obtain the original gray scale watermark again. This scheme will be promising in terms of high fidelity as it uses the minimum insertion of seed key into the gray scale cover image.

II. APPROACH:WATER MARKING APPROACH

(1) The cover image is converted into DCT domain and a 4 × 8 binary matrix for ownership identification is inserted into the mid band coefficients. Inverse DCT is taken to obtain the cover image in the spatial domain.

(2) The target watermark image is taken and divided into small fragments with two rows and four columns.

A random state key is chosen. This is used to produce a random matrix of same size as the target watermark image.

(3) The random matrix is also fragmented into 2 × 4 parts.

(4) A Backpropagation Neural Network is chosen with 1 input, 1 hidden and 1 output layer.

(5) The random matrix fragments are supplied as input to the input layer of the BPN respectively and weights of the network are adjusted to produce the corresponding target image parts at the output layer. After Backpropagation training, the random state key is saved in a file as well as in the least significant portion of the fractional part or the encoded cover image pixel value (for ex. 55.000027 to encode a value of 27) and the cover image with ownership identification bits and random state key is supplied to image corrector network as specified to be used later for the purpose of correction of attacked image. The concept of image corrector is required in situations when the watermarked image is seriously affected by image attacks. However, for minor attacks not causing appreciable changes to watermarked image, this is not required.

III WATERMARK EXTRATION

(1) The watermarked image after being subjected to various image attacks is supplied to the image corrector and the corrected watermarked image received from the image corrector is converted into DCT domain and the ownership identification matrix is recovered and verified..

(2) The watermarked image is taken and hidden random number generator state key is derived from it.

(3) This state key is used to generate exactly same random matrices of 2×4 size as in the embedding stage.

(4) The weights of the trained neural network are extracted from the files and the trained neural network as in the embedding stage is reconstructed.

(5) The random matrices are supplied at the input layer neurons of BPN and the final output matrices are produced at the output layer.

(6) The output matrices so obtained are combined together to form the original target watermark image. The block diagram of the technique is shown in figure and the algorithm for the specific implementation of watermarking with BPN is given in the section.

IV. EXPERIMENNT CONDUCTED AND THE RESULT

All experiments were conducted on genuine intel (R) CPU T-2050 @1.60GHZ, 504 MB of RAM. The operating system used was Microsoft Windows XP Home edition, Version 2002, Service Pack 2. For conducting the experiments, BPN network with one input layer, one hidden layer, one output layer and learning rate (□□=4 and momentum factor (mf) = 0.8 was used. The image of Lena was taken as the gray scale cover image and Disc image was taken as the gray scale watermark to be inserted.

V. GENERATION OF WATERMARK

First of all, the attacked watermarked image is corrected by the image corrector and then the ownership identification matrix is extracted from the DCT converted watermarked image as per procedure indicated part-I

The matrix obtained is =

$$\begin{pmatrix} 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1; \\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1; \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0; \\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1; \end{pmatrix}$$

IJCRT

This is almost same as the embedded *message* shown in assumption number 11 of section 5.3.3 with only 3 bits differing out of 32 bits of the message. Thus, the problem of ownership identification is solved.

Now, all the fragments of random matrices are generated from the key extracted from the watermarked image and are supplied as inputs to the trained Backpropagation Network respectively and the corresponding fragments of output watermark are obtained which are united to create the complete watermark. This is done for different values of error threshold.

Variation of PSNR with threshold

In the first experiment, the variation of PSNR values with respect to change in threshold value is seen. The threshold is varied from 0.4 to 0.0001 as shown in table 1.1. With the reduction in the threshold value, the PSNR goes on increasing. There is also an increment seen in training time and number of epochs required for training. The values of learning rate (α)is kept at 4 and the value of momentum factor (*mf*) is also kept constant at 0.8. The PSNR varies from 16.35 to 40.72. The best PSNR value is obtained at threshold value of 0.0001 with a training time of 321.89 seconds and number of epochs as 223469. Figure 1.11 to Figure 1.14 show the extracted watermark image corresponding to threshold values of 0.1,0.01,0.001 and 0.0001 respectively. The Figure 1.10 shows the variation of PSNR values with respect to various threshold values.

TABLE 1.1

Variation of PSNR with threshold

(BPN with random matrices α =4,mf=0.8)

α	mf	Threshold	PSNR (dB)	Training time (sec.)	Epochs
4	0.8	0.4	16.35	18.98	6466
4	0.8	0.3	17.36	21.48	8428
4	0.8	0.2	18.92	25.76	11462
4	0.8	0.1	21.85	34.10	16947
4	0.8	0.01	30.74	64.51	38875
4	0.8	0.001	37.73	126.43	83498
4	0.8	0.0001	40.72	321.89	223469

(α =4 , *mf*= 0.8)

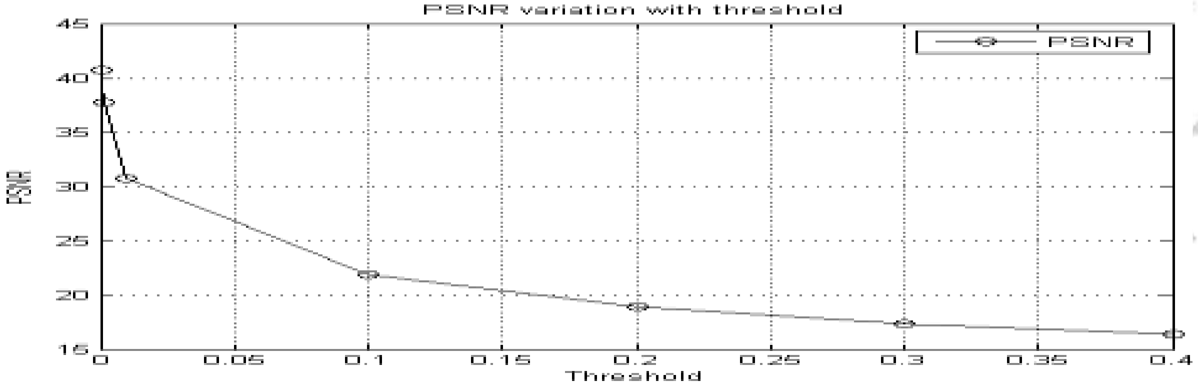

Figure 1.10 Variation of PSNR with threshold

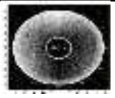	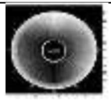	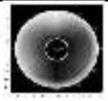	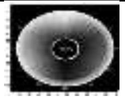
Figure 1.21 Extracted watermark at Threshold=0.1	**Figure 1.22 Extracted watermark at Threshold = 0.01**	**Figure 1.23 Extracted watermark at Threshold = 0.001**	**Figure 1.24 Extracted watermark at Threshold = 0.0001**

VI. EXPERIMENTAL RESULTS (ROBUSTNESS, FIDELITY AND PAYLOAD)

The value of PSNR varied from 21.85 to 40.72 for a variation in threshold from 0.1 to 0.0001. The best value of PSNR of watermark was recorded as 40.72. So, the training is done with a threshold value of 0.0001. When a single bit was used for ownership identification the PSNR of the 'watermarked image' was reported as 148.4780 which is also shown in the paper [A-9](Appendix-A). However, when a DCT encoded ownership identification bits matrix of a greater size , as shown in this chapter was inserted, the fidelity of the watermarked image came down to 48.63 [A-12] Appendix-A which is a practically realizable value of fidelity. The following results are with fidelity = 48.63 dB and threshold = 0.0001. The Watermarked image is subjected to various attacks and the results are shown in table 1.2.

Table 1.2(Results observed for selected Fidelity = 48.63 dB, Threshold= 0.0001)(BPN with random matrices)

Cover Image	Watermark Image	PSNR(dB) of watermarked image(Fidelity) (With DCT encoded ownership identification bits) and NC of watermark extracted (no attack situation)	Size of watermark inserted	Attack	PSNR (dB) of extracted watermark & NC of extracted watermark (post correction of watermarked image after attack)
		48.63,0.998	(117×114) pixels with 256 gray values	Blurred (0.5 %) 3×3 averaging filter	40.72,0.954 40.70,0.954
				Cropped (30%)	40.70,0.954
				Sharpened (30%) 3×3 laplacian filter	40.71,0.954 40.72,.954
				Compressed (CR=10.75) & (QF = 50%)	40.69,0.954
				Gaussian noise 25% Variance=0.1	40.69,0.954 40.87,0.957
				Contrast enhanced (40%) 3×3 contrast enhancement filter	40.60,0.952 40.62,0.953
				Rotated (15^0)	40.63,0.954
				Scaled (50%)(1-1/2-1) 1-3-1	40.66,0.954 40.66,0.952

VII. CONCLUSION

The results obtained for fidelity and robustness after performing the attacks and restoring the watermark are promising. This shows that the method involving random matrices in conjunction with BPN may be practically employed as an effective watermarking technique for digital watermarking applications on gray scale images.

VIII. REFERENCES

[1] R.Schyndel, A.Tirkel and C.Osborne, "A Digital Watermark" in Proc. IEEE International conference on Image Processing, 1994, vol.2, pp.86-92.

[2] Xia-Mu Niu and Sheng-He Sun, "Multiresolution Digital Watermarking for Still Image" in Proc. IEEE Neural Networks for Signal Processing, 2000, vol.2, pp.547-556.

[3] Ping Dong, Jovan G.Brankov, Nilolas PG alastsanos,Yongyi Yang,Franck Davoine,"Signal Compression Digital Watermarking Robust Geometric Distortions", IEEE Transaction on image processing, December 2005, vol.14(12).

[4] Charkari N.M. and Chahooki M.A.Z., "A Robust High Capacity Watermarking Based on DCT and Spread Spectrum" in IEEE International Symposium of Signal Processing and Information Technology, 2007, pp.194-197.

[5]Chu-Hsing Lin, Jung-Chun Liu, Chih-Hsiong Shihand Yan-Wei Lee, "A Robust WatermarkScheme for Copyright Protection" in MUE International Conference on Multimedia and Ubiquitous Engineering, 200 pp 132-137.

[6] Larijani H.H. and Rad G.R., "A New Spatial Domain Algorithm for Gray Scale Images Watermarking" "ICCCE International conference on computer and communication engineering", 2008, pp. 157-161.

[7] Fredric M.Ham and Ivica Kostanic, "Principles of Neurocomputing for Science & Engineering", Mc.GrawHill, Singapore, 2001, pp. 136-140.

[8] Yu,P.T., Tsai H.H., and Lin J.S., "Digital Watermarking based on Neural Networks for Color Images , Signal processing, vol.81, pp.663-671**.**

[9] J.R.Hernandez, F.Perez Gonzalez and J.M.Rodriguez, "Data Hiding for Copyright Protection of Still Images", National conference in image processing, Faislabad,2001.

[10] Hwang M.S., Chang C.C. and Hwang K.F.,"Digital Watermarking of Images using Neural Networks",Journal of electronic imaging, 2000, vol. 9,pp.548-555.

[11] CharrierM., Cruz,D.S. and Larsson M., "JPEG 2000 , the Next Millennium Compression Standard for Still Images" in Proc. IEEE International Conference on Multimedia Computing Systems, pp. 131-132.