DIGITAL WATERMARKING MODELLED AS NOISE IN COMMUNICATION CHANNEL AND OPTIMIZATION OF DESIRABLE CHARACTERISTICS USING ADAPTIVE RESONANCE THEORY (ART)

Dr.Ashish Bansal, Mrs. Neha Gupta
Symbiosis University of Applied Science, Indore

Abstract:. Digital watermarking precisely means inserting secret bits of information in a digital cover. This is analogous to the theory of a communication channel where the cover media may be regarded as the communication channel and the noise may be modelled as the digital watermark to be inserted. Many research works aiming at optimizing robustness and fidelity of watermarking are cited in the literature. Amongst such techniques, neural network ART based technique can be employed to create and reproduce watermark with reasonably high values of robustness and fidelity.

Index terms: Area-efficient, Low power, CSLA, Binary to excess one converter, Multiplexer.

I. INTRODUCTION

In this paper the concept of adaptive watermarking is introduced which investigates visual characteristics of the pixels of a cover image to decide the embedding strength of watermark. The proposed technique divides the cover image pixels into various clusters using Adaptive Resonance Theory (ART), depending on the similarity between their visual characteristics defined by parameters of Human Visual System (HVS).An iterative procedure is then used to associate each cluster with a particular embedding strength of watermark which helps in adaptive insertion of watermark into the cover image. This technique helps to preserve high fidelity of the watermarked image even with a stronger insertion of watermark.

II. APPROACH:WATERMARKING EMBEDDING

(1) All the pixels of the cover image are divided into various clusters using the visual characteristics of the pixels and ART clustering algorithm.
(2) The embedding strength for the pixels of each cluster is evaluated by an iterative procedure.
(3) The target watermark is embedded sequentially into corresponding cover image pixels with an adaptive embedding strength as decided in step 2.

WATERMARK EXTRACTION:

(1) The embedding strength of the watermark information inserted into pixels of the watermarked image are obtained according to their designated cluster as decided during the watermark embedding.
(2) The watermark embedded into the pixels are found using the embedding strength of watermark in the pixels and the intensities of the pixels before and after watermarking.
(3) The watermarks obtained from all the pixels are combined to create the complete Watermark.

III. ALGORITHM: Watermark Embeding

(1) An ART network is chosen with one cluster unit as output and four input neurons initially. A vigilance parameter is chosen for the clustering operation.
(2) For all the pixels in the cover image do the following:
(a)The four Human Visual system (HVS) parameters h1, h2, h3 and h4 depicting Entropy sensitivity, Frequency sensitivity, Luminance sensitivity and Texture Sensitivity of the pixel respectively are calculated.
(b)The four parameter values are given as inputs to the ART network.
(c)Output cluster for the pixel is obtained. New clusters are formed in the process. Pixels with similar visual characteristics are grouped under same clusters the degree of similarity between them is governed by selecting vigilance parameter of the network.
(3) First of all *m* different watermark bits of the watermark image are embedded uniformly with embedding strength α into *m* randomly selected pixels of the cover image using the formula

$$p2=p+w\times\alpha \qquad 1.1$$

Where *p*= original pixel intensity of the randomly selected pixel of the cover image. *p2*= modified pixel intensity of the randomly selected pixel of the cover image and *w* is the watermark bit to be inserted into this pixel. (*p2*, *p* and *w* are specific values for each pixel). Equation 1.1 is used for *m* pixels for inserting *m* different watermark bits.
4) The PSNR of the watermarked image is obtained referred as *old_psnr*.
5) For each new cluster of pixels the steps 6 and 7 are repeated. Initialize *max_diff* = 0.

6) For each value of *diff* from 0.01 to 0.1 in steps of 0.01 the steps from (a) to (d) are executed.
(a) All pixels of this cluster which are to be randomly selected for watermarking are identified.
(b)The original embedding strength of inserted watermark for all the watermarked pixels of this cluster is replaced by $\alpha + diff$ and the pixel intensity values are modified using the formula:

$p2=p+w\times(\alpha + diff)$ 1.2

where, w shows the watermark inserted into the pixel. p= original pixel value.
p2= Modified pixel intensity value.
(c)The PSNR of the watermarked image is Obtained referred as *changed_ psnr*
(d) If *old_ psnr< changed_ psnr* then *old_ psnr = changed_ psnr* 1.3 *max_diff = diff*. 1.4

max_diff corresponds to *diff* where maximum PSNR is obtained. This value is recorded for each cluster to be used for the watermark extraction.
This step decides the optimum embedding strength for the selected cluster.
(7) Control is sent to step 5 until all the clusters are taken.

Watermark Extraction
To extract the watermark, the following steps are done.
(1)For each randomly selected pixel which is watermarked, do the steps from 2 to 4.
(2)Note the embedding strength *max_diff* corresponding to the cluster where this pixel belongs to, as recorded in the watermark embedding stage.
(3)The watermark information (w) corresponding to the pixel is obtained by using the formula:

$w= (p2-p)/ (\alpha+max\_diff)$ 1.5

Where, p2 = changed pixel intensity of the watermarked pixel.
p = original pixel intensity value of the watermarked α = Original Embedding strength for watermark insertion.
max_diff = Modification in the original embedding strength of watermark α for the cluster of pixels to get maximum PSNR of the watermarked image as recorded during watermark embedding. The variables shown in equation (1.5) are specific for each pixel.
(4) The extracted watermark information is obtained by assembling the watermark bits embedded into all the randomly selected watermarked pixels.

IV. EXPERIMENTS CONDUCTED AND RESULTS.

Experimental setup
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 experiment, ART2 network was used. The image of Lena of size (127×128) pixels was taken as the cover image and Logo image of size (127×128) pixels was taken as the gray scale watermark to be inserted. The value of embedding strength □=0.5 and vigilance parameter = 0.05 were selected.

Generation of watermark
Algorithm given in section (6.1.3.1) has been used to insert the watermark and the algorithm given in section (6.1.3.2) has been used for the extraction of watermark. ART2 network has been used to find the embedding strength for various clusters and not for creating a watermark directly as a result of network training. Hence, the variation of PSNR of extracted watermark with vigilance parameter, training time or number of epochs used for training are not significant and are not recorded.

Experimental Results (Robustness, fidelity and payload)
The experimental results for robustness, fidelity and payload have been determined and are given below in table 1.1 and Figures 1.2 to 1.4.

Attacks:
Blurring: (3×3 averaging filter,0.5%) , Crop: (Top Left (30%), Contrast Enhanced: (3×3 Contrast enhancement filter,40%), JPEG Compression:(CR=10.75 with QF=50%), Rotation(15 degrees),Scaling (50%->(1-1/2-1),1-3-1),Gaussian noise(25%,Variance=0.1), Sharpening: (30%,3×3 Laplacian).

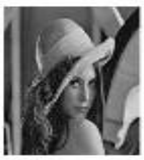
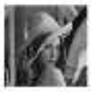
	
Lena's image	**Logo's image**

Figure 1.2 Unattacked watermarked image (Lena) and watermark (Logo)

Table 1.1
(Results observed for Fidelity-PSNR (dB)= 46.5 dB, ART vigilance parameter= 0.05)
(Adaptive watermarking using ART)

Cover Image	Watermark Image	PSNR(dB) of watermarked image(Fidelity) and NC of watermark	Size of watermark	Attack	PSNR (dB) of extracted watermark & NC of extracted watermark After attack

		extracted (no attack situation) (PSNR,NC)			
 Lena's Image	 logo's Image	46.5, 0.999	(127×128) pixels with 256 gray values	Blurred (0.5%) 3×3 averaging filter	39.8,0.912 39.54,0.915
				Cropped (30%)	43.5,0.984
				Sharpened (30%) 3×3 laplacian filter	40.75,0.954 41.23,0.953
				Compressed (CR=10.75) & (QF=50%)	44.3,0.989
				Gaussian noise (25%) Variance=0.1	43.59,0.984 42.22,0.978
				Contrast enhanced (40%) 3×3 contrast enhancement filter	40.87,0.954 40.98,0.976
				Rotated (15^0)	44.2,0.989
				Scaled (50%)(1-1/2-1) 1-3-1	43.5,0.984 43.63,0.987

Trade off (Robustness and Fidelity)

The table 1.2 given below may be referred for the tradeoff characteristics.

Table 1.2 (Tradeoff –Robustness and Fidelity)
(Adaptive watermarking using ART)

S-No	Fidelity PSNR (dB) (Watermarked Image) (Unattacked)	Normalized Correlation (Extracted Watermark) (Unattacked)	Trade off
1	46.5	.999	
2	46.9	.997	
3	47.1	.994	**YES**

The above table shows the inverse relationship between fidelity of watermarked image and the robustness of extracted watermark. Thus, there is an existence of tradeoff between the two.

V.CONCLUSION

Due to adaptive insertion of watermark, the fidelity of the watermarked image is high and varies from 46.5 to 47.1 with different embedding strengths of watermark insertion. Due to direct embedding and extraction of watermark from the cover image, the PSNR and NC of the output watermark varies with different kinds of attacks. Normalized correlation of extracted watermark (Logo) decreases with increase in the fidelity of the image. The payload of the watermark inserted is (127×128) pixels with 256 gray values which is equivalent to $(127 \times 128 \times 8)$ bits.

VI. 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 RobustGeometric Distortions", IEEE Transaction on image processing, December 2005, vol.14(12).
[4] Charkari N.M. and Chahooki M.A.Z., "ARobust 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 Yan-Wei Lee, "A RobusT Watermark Scheme for Copyright Protection" in MUE International Conference on Multimedia and Ubiquitous Engineering, 2008, pp 132-137
[7] Fredric M.Ham and Ivica Kostanic, "Principle of Neuro computing 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.