Journal of Computer Science 1 (2): 169-174, 2005
ISSN 1549-3636

An Improved Scheme for Digital Watermarking Using Functional Link Artificial Neural Network

[1]Banshidhar Majhi and [2]Hasan Shalabi
[1]Department of Computer Science and Information Technology
(On leave from National Institute Technology, Rourkela, India-8)
[2]Department of Computer Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan

Abstract: The present study proposes a novel technique for copyright protection by utilizing digital watermarking of Images. The watermark is embedded and detected by using Functional Link Artificial Neural Network (FLANN) and Discrete Cosine Transform (DCT). The exhaustive simulation results of the proposed scheme show improved performance over the existing methods in all cases, i.e. when the watermarked image is subjected to compression, cropping, sharpening, blurring and noise. Comparative analysis with an existing neural approach shows the superiority of the proposed scheme of computational complexity and performance.

Key words: Digital Watermarking, One-way Hash Function, FLANN, MLP, DCT, JPEG Compression, Cropping

INTRODUCTION

In recent years, there has been a rapid growth of network multimedia systems and other numerical technologies. This has let to an increasing awareness of how easy it is becoming to reproduce data. The ease with which perfect copies can be made may lead to large-scale unauthorized copying, which is a great concern to the music, film, book, and software publishing industries. Because of this concern over copyright issues, a number of technologies are being developed to protect against illegal copying. One of these techniques is the use of digital watermarks. Watermarking embeds an ownership signal directly into the data [1-3].

The digital watermarking system essentially consists of a watermark embedder and a watermark detector as shown in Fig.1. The watermark embedder inserts a watermark into the cover signal and the watermark detector detects the presence of watermark signal. Note that an entity called watermark key is used during the process of embedding and detecting watermarks. The watermark key has a one-to-one correspondence with watermark signal (i.e., a unique watermark key exists for every watermark signal). The watermark key is private and known to only authorized parties and it ensures that only authorized parties can detect the watermark. Further, note that the communication channel can be noisy and hostile (i.e., prone to security attacks) and hence the digital watermarking techniques should be resilient to both noise and security attacks.

The various watermarking techniques that have been suggested till today are classified into two categories, namely, spatial domain and transform domain techniques. The first method embeds a watermark into the cover signal in spatial domain. In general, the main

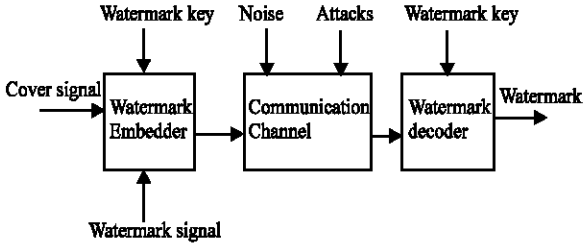


Fig. 1: Digital Watermarking System

advantage of this method is that it has a good computing performance, but the disadvantages are lower security and robustness. The transform domain methods transform the original data into the frequency domain (Fourier, Discrete Cosine, wavelet etc.) and then watermark is embedded in the frequency domain. The watermarked signal is obtained by using a corresponding inverse transform.

Schyndel *et al.* [4] generated a watermark using an m-sequence generator. The watermark is either embedded or added to the least significant bit of the original image to produce the watermarked image. The watermark is extracted from a suspected image by taking the least significant bits at the proper locations. Detection is performed by a cross-correlation of the original and extracted watermark. It has been shown that the resulting image contained an invisible watermark with simple extraction procedures. The watermark, however, is not robust to additive noise.

Cox *et al.* [5] suggested that to make the watermark more robust to attack, it must be placed in perceptually significant areas of the image. The algorithm is based

on taking 1000 random samples of a N (0,1) distribution as watermark, and then these samples are added to the 1000 largest DCT coefficients of the original image, and the inverse DCT operation is performed to generate the watermarked image. For detection, the watermark is extracted from the DCT of a suspected image. Extraction is based on knowledge of the original signal and the exact frequency locations of the watermark. The correlation coefficient is computed and compared with a predefined threshold. If the correlation coefficient exceeds the threshold the watermark is detected. This method is robust to image scaling, JPEG coding, cropping, and rescanning.

Hwang *et al.* [6] have described a DCT-based watermarking of images using neural network. Even if the method is robust against JPEG compression, sharpening, blurring and scaling, its main demerits lies in the high computational complexity and memory requirements.

Watermarking using Neural Network: Neural network is a potential tool in most of the signal processing and other application. Digital watermarking is not an exception where it finds a way to use neural network in order to make the process more secure and robust. Different models of neural network have their own merits and demerits. In this study, a FLANN and DCT based digital watermarking technique is proposed to gain in computational efficiency as well as memory requirements. The scheme is also more secure and robust. The proposed method is described below in detail.

MATERIALS AND METHODS

FLANN is a single layer neural network that is able to handle linearly non-separable tasks using the appropriately enhanced input representation. The main advantage of the FLANN is the reduced computational cost in the training stage, while maintaining a good performance of approximation [5,6]. Suppose we have a function link contains the functions $f_1, f_2, \ldots\ldots\ldots\ldots f_n$ and an input x then it will be transformed into $f_1(x), f_2(x), \ldots\ldots\ldots, f_n(x)$, which are then introduced into the network for further processing. Examples of functional link successfully applied in diverse problems are: $x, x^2, x^3 \ldots\ldots$; $x, \sin \pi x, \cos \pi x, \sin 2\pi x, \cos 2\pi x, \ldots..$; $x_1, x_1x_2, x_1x_2x_3, \ldots\ldots$ [7,8].

In this scheme, FLANN is used to learn the relationship between the DCT coefficients. DCT coefficients are used to hide the watermark signal i.e. one bit of watermark is hidden in one DCT block. The relationship among the DCT coefficients are obtained through a trained FLANN prior to embedding process and subsequently, the watermark is retrieved using the same FLANN structure. The algorithms for watermark embedding and extraction is discussed below in detail.

Algorithm for Watermark Embedding

Step 1: Obtain the DCT block (Fig. 2) of the image by some secret keys and hash function as given by Hwang's [3].

Step 2: Choose the first nine AC coefficients ($AC1_i$, $AC2_i$, ...$AC9_i$) as the input vectors and the twelfth AC coefficient i.e. $AC12_i$, as the output vector in the FLANN model for i^{th} DCT block (Fig.3). The inputs are expanded as AC_i and AC_i^2 in the functional expansion block.

DC	1	5	6	14			
2	4	7	13				
3	8	12					
9	11						
10							

Fig. 2: Coefficients in a DCT Block

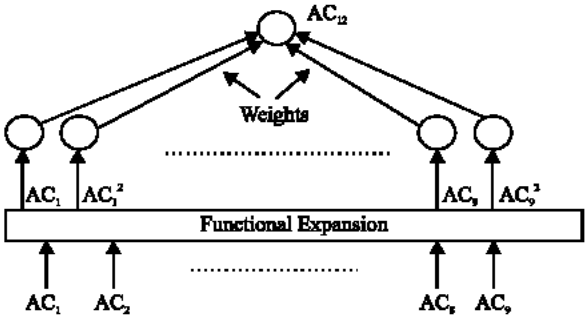


Fig. 3: FLANN Model used for Watermarking

Step 3: Train the FLANN using back propagation algorithm till the MSE is minimum or constant.

Step 4: Embed the binary watermark W_i by replacing the original $AC12_i$ with $AC12_i^{"}$, where $AC12_i^{"}$ is computed according to $AC12_i^{'}$ and W_i as follows:

$$AC12_i^{"} = \begin{cases} AC12_i^{'} - \delta & \text{if } W_i = 0, \\ AC12_i^{'} + \delta & \text{if } W_i = 1. \end{cases} \quad (1)$$

Here δ is a system parameter and is a constant, generally. A larger δ will result in a greater robustness in the watermarked image. But the distortion will be increased too. The value δ

can be determined by the applicant's requirements.

Step 5: Repeat step 4 till all the bits of the watermark are embedded.

Step 6: Take the inverse DCT to obtain the watermarked image.

Algorithm for Extracting of the Watermark: The retrieval procedure for the watermark from the watermarked image is similar to the embedding procedure.

Step 1: Introduce the secret keys to obtain the DCT blocks

Step 2: Use the $AC1_i$, $AC2_i$,..,$AC9_i$ as inputs to the FLANN structure to get the observed $AC12_i^{'}$ and then watermark retrieved using (2)

$$\tilde{W}_i = \begin{cases} 0, & \text{if } AC12_i \le AC12_i^{'}, \\ 1, & \text{if } AC12_i > AC12_i^{'} \end{cases} \quad (2)$$

Step 3: Compare the original watermark W and the extracted watermark $\tilde{W}$ as per the following quantitative measure, i.e. the Bit Correct Ratio (BCR) using (3)

$$BCR = \frac{\sum_{i=1}^{w_h \times w_w} w_i \oplus \tilde{w}_i}{w_h \times w_w} \times 100 \quad (3)$$

where, $\oplus$ denotes the EX – OR operator.

RESULTS

The algorithm is simulated using MATLAB 5.3 in a Pentium-IV processor (1.8 GHz). Standard gray scale image Lena of size 512x512 is chosen as the cover signal and binary logo (NIT) of size 32 x 64 is used as watermark signal. The MLP and FLANN is trained using conventional back propagation algorithm and the saturated weights and biases are used for retrieving the watermark from the watermarked image. Fig. 4 depicts the convergence characteristics in Mean Square Error (MSE) after 1000 epochs. In our experiment, we let δ is selected to be 20 and learning coefficient (η) as 0.1. The watermarked image is subjected to noise, blurring, sharpening and lossy JPEG compression. The watermark is retrieved from these distorted images and their corresponding PSNRs and BCRs are computed for both MLP and FLANN structure and listed in Table 1 and Table 2 respectively. The visual results from the proposed scheme are shown in the Fig. 5-8. The visual as well as the tabular results clearly indicates the robustness of the proposed scheme.

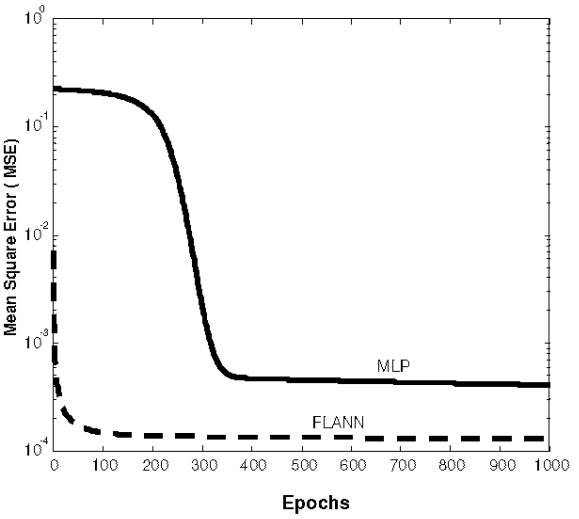


Fig. 4: Convergence Characteristics of FLANN and MLP

(a) Original Image (Lena)

(b) Watermark of NIT (33x64)

(c) Watermarked Image (PSNR = 41.36 dB)

(d) Retrieved Watermark (BCR=94.79%)

Fig. 5: Results using FLANN Structure from Watermarked Image

(a) Blurred watermarked Image (PSNR = 31.32 dB)

(b) Sharpened Watermarked Image (PSNR = 31.66 dB)

(c) Retrieved Watermark from (a) (BCR = 90.38%)

(d) Retrieved Watermark from (b) (BCR = 95.69%)

Fig. 6: Results using FLANN Structure from Sharpened and Blurred Image

(a) JPEG Compressed Watermarked Image (PSNR=35 .49dB)

(b) Cropped watermarked image (PSNR = 11.26 dB)

(c) Retrieved Watermark (BCR = 91.52%)

(d) Retrieved Watermark (BCR = 82.85%)

Fig. 7: Results using FLANN Structure from Compressed and Cropped Image

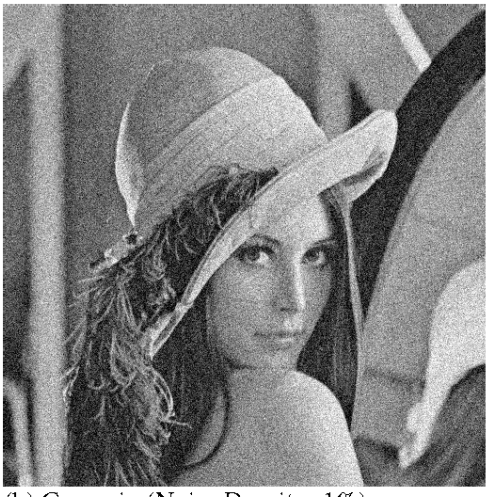
Table 1: PSNR (dB) of Different Test Images of Lena

Method	Watermarked Image Noise	JPEG compressed	Blurred Image	Sharpened Image	Noisy Image (Salt & Pepper 3%)	Noisy image Gaussian (μ=0,σ=.1)	Cropped image
MLP [6]	39.70	35.06	29.22	31.19	20.36	19.65	11.26
FLANN (Proposed)	41.36	35.49	31.32	31.66	21.40	20.40	12.26

Table 2: BCR in percentage (%)of different test images of Lena

Method	Watermarked Image Noise	JPEG compressed	Blurred Image	Sharpened Image	Noisy Image (Salt & Pepper 3%)	Noisy image Gaussian (μ=0,σ=.1)	Cropped image
MLP [6]	94.36	87.64	82.52	94.36	70.57	68.70	77.60
FLANN (Proposed)	94.79	91.52	90.38	95.69	75.86	70.35	82.85

(a) Salt & Pepper (Noise Density=3%)



(b) Gaussain (Noise Density=1%)

(c) Retrieved Watermark (BCR = 76.5%)

(d) Retrieved Watermark (BCR = 69.12.85%)

Fig. 8: Results using FLANN Structure from Noisy Images

To present the computational advantage of the proposed FLANN structure over the MLP structure [6] four basic components, i.e. the addition, the multiplication, square function and the computation of tanh (.) are considered in both cases and shown in Table 3. The total number of weights to be updated in one iteration in case MLP is 45, whereas in the proposed FLANN structure it is only 19. Since the hidden layer doesn't exist in FLANN, the computational complexity is drastically reduced in comparison to that of MLP.

Table 3: Comparison of Computational Complexity between MLP [6] and Proposed FLANN Structure

Operations	MLP	FLANN (Proposed)
Addition	90	38
Multiplication	40	18
tanh(.)	5	1
Square function	-	9

CONCLUSION

This study suggests an efficient and robust digital watermarking algorithm using neural network and DCT. A modified FLANN is used in place of conventional MLP structure, which has inherent advantage in terms of memory requirements and computational complexity. In addition, exhaustive simulation results indicate that the proposed method outperforms the existing method in terms of robustness and security.

REFERENCES

1. Anderson, R.J. and F. Petitcolas, 1998. On the limits of steganography. IEEE J. Selected Areas in Communications, 16: 474-481.
2. White Paper. Digital watermarking: A technology overview. http://www.wipro.com/dsp.
3. Sin-Joo Lee and Sung-Hwan Jung, 2001. A survey of watermarking techniques applied to multimedia. Proceedings. ISIE 2001. IEEE International Symposium on Industrial Electronics, 1: 272-277, 12-16 June.
4. Schyndel, R., A. Tirkel and C. Osborne, 1994. A digital watermark. Proc. IEEE Int. Conf. on Image Processing, 2: 86-90.
5. Cox, I., J. Kilian, F. Leighton and T. Shamoon, 1997. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 6: 1673-1687.
6. Hwang, M.S., C.C. Chang and K.F. Hwang, 2000. Digital watermarking of images using neural networks. J. Electronic Imaging, 9: 548-555.
7. Letitia Mirea and Teodor Marcu, 2002. System identification using functional link neural networks with dynamic structure. 15th Triennial World Congress, Barcelona, 2002 IFAC Spain.
8. Angel Lopez-Gomez, Shinichi Yoshida and Kaoru Hirota, 2002. Fuzzy functional link network and its application to the representation of the extended Kolmogorov theorem. Intl. J. Fuzzy Systems, 4: 2.