COMPUSOFT
An International Journal of Advanced Computer Technology
ISSN:2320-0790

Secure Images for Copyright by Watermarking in Transform sphere using bidirectional Neural Network

Dharmendra Gwala[#1] and Vivek Shrivastava[*2]

[#]*Department of Information Technology, Student, ITM College Bhilwara, Rajasthan India*
[1]dharmudiwan@gmail.com
[*]*Department of Information Technology, Head of Department, ITM College Bhilwara, Rajasthan India*
[2]Vivek.sri2008@gmail.com

Abstract: Person beings knowledge a non preventable circumstances of distribution and redistribution their pictures, documents, videos etc on the internet about every week. Intruders are frequently the ones who do not desire to work hard and they maintain on somebody's original work. watermarking is the process of embedding data called a watermark into a multimedia object such that watermark can be detected or extracted later to make an declaration about the object. Watermarking is adding"ownership" information in multimedia inside to show the dependability. There are generally two most popular ways of embedding the watermark in the digital content i.e. spatial sphere and transform sphere. In spatial sphere, Least-Significant Bit (LSB), SSM Modulation-Based Technique has been developed. For DCT sphere, block based approach and for wavelet sphere, multi-level wavelet transformation technique and CDMA based approaches has been developed. Presented techniques based on spatial and occurrence domain suffer from the problems of low Peak Signal to Noise Ratio (PSNR) of watermark and image quality poverty in unreliable quantity. This paper offers a technique based on Back propagation Neural Network to instruct a given cover image to construct a preferred watermark image.

Keywords – Digital Watermarking , Transform sphere, Spatial sphere, Neural Network, PSNR, Discrete Cosine Transform (DCT).

1. Introduction

This world has knowledgeable a number of exceptional techniques of overcoming the straight troubles connected to counterfeit and illegal intrusion of digital media. There are mainly four ways of authenticating the digital media namely fingerprinting, stenography, cryptography and watermarking. The information to be surrounded in an image, audio, video signal is called a digital watermark [1]. Digital watermarking should provide the behavior like imperceptibility, strength, protection of cover image. With the increase and advances in digital communication technologies, digital images cover is converted into effortless to be delivered and exchanged. These forms of digital information can be easily derivative and dispersed during digital media [2][3]. Digital watermark also means the difference between the watermarked signal and the cover signal [1]. Thus, watermarking approach is used to make sure of the security of the figures. A digital watermark should be statistically undetectable, forceful in terms of reflexive fake and data attacks such as JPEG density, scaling, aspect part changes, alternation, cropping, row and column removal, accumulation of noise, filtering, encrypted and statistical attacks, as well as addition of other watermarks also the watermark must be extractable without much difficulty. Here we talk about the work done in the field of watermarking in spatial and transform sphere [1]. Watermarking involves embedding user information into an image. However, such watermarking is forever irretrievable, i.e. the original image cannot be recovered behind watermark extraction. Some applications, such as remedial or armed images, need to recover the original image from a watermarked image. Therefore, reversible watermarking approaches have been presented [6].

However, these techniques suffer from the problems of unsatisfactory value of imperceptibility and robustness to various attacks as discussed in these papers. These techniques also have the problems related to security. Chun–Yu-Chang [3] proposed an amazing technique of embedding the watermarks into synapses of FCNN rather than wrap image. This helped to enlarge strength and decrease imperceptibility troubles to a great size. However, this amazing work suffers from a few problems discussed in the following sections which prevent its effective use in watermarking applications [2].

It is permanently embedded into the host image. The embedded watermark may be pseudo-random binary sequence, chaotic sequence, spread spectrum sequence or binary/gray scale image. Such watermarks are used for objective detection using correlation measures. Binary or gray image is meaningful and is used for subjective detection. The examples of this type of watermark include date, serial number, logo or any other kind of identification mark [11].

1.1 Applications of Digital Image Watermarking:

There are assorted applications of image watermarking. These are listed as follows [21].

1.1.1 copyright security

When a novel effort is created, copyright information can be inserted as a watermark. In case of argument of possession, this watermark can provide facts.

1.1.2 Transmit Monitoring

This application is used to monitor illegal transmit station. It can confirm whether the content is really broadcasted or not.

1.1.3 Interfere finding

Delicate watermarks are used for interfere detection. If the watermark is cracked or corrupted, it indicates incidence of interfacing and hence digital content cannot be trusted.

1.1.5 Fingerprinting

Fingerprints are single to the holder of digital content and used to tell when an banned copy appeared.

2. Related Work

There are basically two main methods for watermark embedding namely embedding in spatial sphere and embedding in transform sphere .We present here some of the popular techniques in each of the sphere ,followed by researchers worldwide for securing the images on the digital media.

2.1 Spatial sphere Watermarking

Spatial sphere method refers to the image flat surface itself and methods in this group are based on straight exploitation of the pixels an image. Straightforward watermarks could be surrounded in the images by modifying the pixel values or the Least Significant Bit (LSB) values. Even though spatial sphere based techniques cannot maintain most of the common attacks like density, high overtake or low overtake filtering etc., researchers suggest spatial domain based schemes for the sake of time reduction and cleanness.

2.2 Transform sphere Watermarking

Ahmadi and Safabaksh [22] converted the original image into the NTSC color space for separating the grayscale information from color data followed by dividing the luminance component Y into 8X8 blocks and transforming it to DCT. To prevent tampering or unauthorized access, watermark permutation function was present.

Manimaran et al., [23] devised a unique way of encrypting the watermark by DES method after compressing it and the cover image is DCT transformed , followed by embedding. Poljicak, et al., [18] used the magnitudes of the Fourier transform for embedding. The PSNR values were chosen the means for evaluating the quality degradation. The method was robust enough to handle the print scan, print cam and the attacks from Stir Mark benchmark software. Ren [4] divided color image luminance component into 8×8 bocks for DCT transform in b r YC C Color Space, then embedded binary watermark in its middle frequency coefficients in DCT domain, therefore, the embedding and extraction of the binary watermark in color image carrier was implemented successfully. Blind extraction, to get back the watermark without original image, was also observed.

2.3 Contribution of Neural Networks in Image Watermarking

The transform sphere embedding when combines with the definitive protected and fast to instruct non-natural neural networks such as FCNN or RBF etc are unexpectedly very resourceful for the rationale of image watermarking.

Paper [19] proposed a color image watermarking algorithm based on fractal and neural networks in Discrete Cosine Transform (DCT) domain. Firstly, the algorithm utilized the fractal image coding technique to obtain the characteristic data of a gray-level image watermark signal and encrypted it by a symmetric encryption algorithm before it was embedded. Secondly, by exploiting the abilities of neural networks and considering the characteristics of Human Visual System (HVS), a Just Noticeable Difference (JND) threshold controller was designed to ensure the strength of the embedded data adapting to the host image itself entirely. Thus the watermark scheme possessed dual security characteristics. CIELab color space was chosen to guarantee the stability of the results.

Kutter [25] proposed a watermarking scheme embedding the watermark bits into the blue channel of a color image. In Kutter's system, embedded watermark bits can be extracted with a threshold by considering the neighbor pixels relation. However, the watermarking system is vulnerable since the reference information, which decides the threshold, can be easily destroyed. In order to improve the robusmess of Kutter's system, Saeed al. [9] proposed an adaptive way to decide the threshold by applying neural network. Yu et al. hide an invisible watermark into the blue channel of a color image, and then cooperate with neural network to learn the characteristics of the embedded watermark related to the watermarked image.

2.4 A Novel Approach Using FCNN for Watermarking

The above problems may be solved by using a fixed image slightly than the unique cover image at the input layer of FCNN. For embedding the cover image, first it is fixed using encoding bits and then the image is given to FCNN along with the preferred watermark at the input layer. As shown in the Fig.1, cover image is converted into Discrete Cosine Transform (DCT) block by block and encoding bits are fixed in the mean posse coefficients of the blocks. Inverse Discrete Cosine Transform (IDCT) of this embedded cover image is given to the input layer of FCNN wit the desired watermark to get watermarked cover image and the watermark images at the output layer of FCNN. For the mining of watermark from this watermarked image Fig. 2 can be referred. [2]

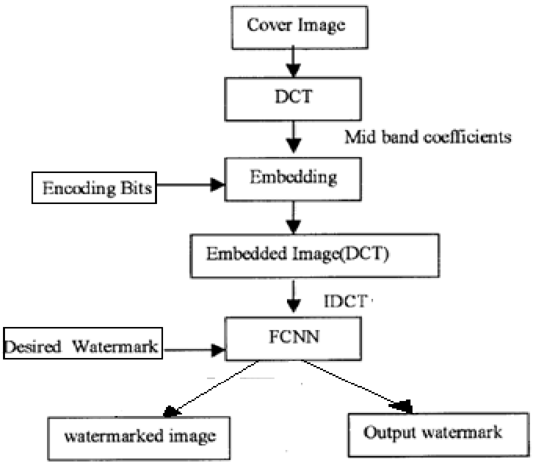

Figure 1 Block Diagram of Watermarking the encoded image using FCNN

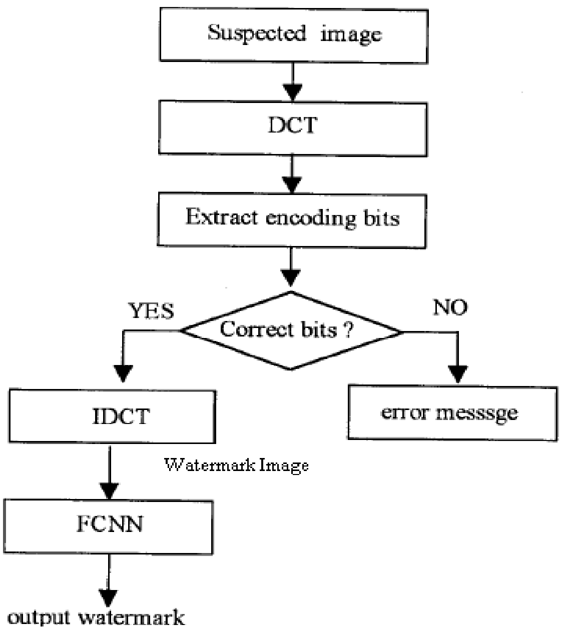

Figure 2 Block Diagram of Extracting watermark from watermarked image

3. Method of Watermark Image Insertion

In the previous techniques there were problems related to robustness and imperceptibility we have reduced the distortion to a negligible level. In the proposed approach we have Watermarking technique apply to the RGB (Red, Green, Blue) color format for select the any color the PSNR and security are changed. As the cover image is not directly exposed for embedding the secret information instead we have suggested that synapses of neural network play a better platform for the watermark insertion. There was a chance of an unauthorized person claiming his ownership by extracting watermark for an unauthenticated image. The problem was "Proprietary FCNN". A network can be trained in various ways to extract a watermark to prove ownership which is a threat to authentication.

Among every special image, the aggressive cover of the full counter propagation network chooses a victor that generate some or the other output watermark. It is quite possible that more than one input images be similar to the lightness pattern of the same neuron at the input layer. Thus, this neuron must be the victor in all the cases to produce the same watermark at the output layer for all the images. This raise trouble of 'Authenticity', when one specious image produces the correct watermark. The above problems need of an additional security against counterfeit. We have successfully encoded the cover image before actually directing it towards the actual watermark embedding phase.

The following algorithm explains each step in detail:
The cover image (color image) size is given by mc x nc mc being the no of rows and nc being number of columns. The watermark image is of size mw x nw. The blocks are of 8x8. i.e. block size = 8.The mid band matrix is chosen by user . In our algorithm it is a binary matrix of size 8x8. It will help in encoding. The midband coefficients selection matrix is given as:

Step 1- The cover image is divided into blocks of 8x8 one by one.
Step 2- Each block is then transformed into its equivalent DCT coefficient block. Lets say the block is dct_block.
Step 3- If message (k)= 0 then
{for i=1 to 8
{ for j=1 to 8
{ if (midband(i,j) =1)
{ dct_block(i,j)= pn_sequence(pos);
pos=pos+1;
}end of if }end of for }end of for }// end of if
Step 4- Now convert the dct_block back to idct i.e. inverse dct.
Step-5- Now x is incremented. If x exceeds the total number of columns, its reinitialized and next row is taken.

x= x + blocksize if (x+8)<nc
x=1 and y = y + blocksize for (x+8)>nc

Step 6- Increment k =k+1(until k=p*q ie total no of blocks in the host image) for encoding next block.
Step 7 -Go to step 1 while (k<=R)
Step 8- The encoded image is converted to column vector in the following form-
Cover_Image= [X1, X2, X3,…………..,Xmcxnc]
Where mcxnc is the total number of pixels in the cover image. Also the watermark W= [Y1, Y2, Y3,……………,Ymwxnw] Is converted to the column vector .
Step 9- The cover image and watermark are then supplied to the input layer of FCNN, followed by training the network to produce watermarked image and desired watermark at the output layer.

We have chosen Raj color images as our cover images to instruct the network.

Figure 2 Cover image

Figure 4 Watermark image

The full counter propagation network has got the following architecture:

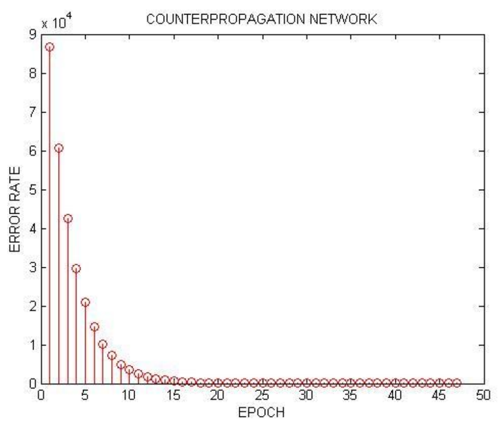

Figure 5 Architecture of Full Counter Propagation Neural Network

4. EXPERIMENT AND RESULTS

We have calculated the Peak Signal to Noise Ratio (PSNR) and Normalized Correlation (NC) which are actions of imperceptibility and toughness. To find out Peak Signal to Noise Ratio we need to calculate. Mean Square Error between the gray level versions of the original cover image and the watermarked image.

Table 1. PSNR values after performing attacks

Name of the Attack	PSNR in DB	NC
No Attack	104.18 Db	0.8476
Salt & Pepper(SP) Noise	87.82 Db	0.0013
Noise density	57.78 Db	0.0025
Speckle Noise	72.66 Db	0.0013
Compression	98 Db	0.9476

The mid band matrix of 8x8 for selecting the blocks to be encoded is
[0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
0 0 0 0 0 0 0 0
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1]
This matrix is useful in selecting the DCT block for encoding the covert message. We have chosen a value =1 i.e. if midband(i,j)=1 then only encode that individual DCT block. The idea of encoding can more be proceed for all the three channels that are red, green, and blue. We can also embed a colorful watermark in all of them. These are certain modifications in the strategy suggested here which I am working on currently.

5. CONCLUSION

The idea of conservation images with watermarking in transform sphere of image using full counter propagation neural network has confirmed its effectiveness in terms of strength, imperceptibility of watermark, ability of information thrashing and several other important parameters. With this adjustment, FCNN can be practically employed to find a successful watermarking method with better time complication, higher ability and higher PSNR. However, taught weight matrix of the FCNN is required to remove watermark from the given image. Experimental results show that the proposed scheme is forceful and protected, against a wide range of intended and unintended attacks, with NC values almost future 100%. The proposed algorithm can oppose to rotation to some level.

References

[1]. Chitralekha Dwivedi and Ashish Bansal – "Image Security achieved through Watermarking- Survey based on Spatial and Transform Domain Techniques" UACEE International Journal of Computer Science and its Applications - Volume 2: Issue 3

[2]. Bansal A and Bhadauria S.S, — "A novel approach using full counter propagation neural network for watermarking" International journal on Computer Science and Engineering,2010, Vol. 02, pp 289-296.

[3]. Chun-Yu-Chang –"The Application of a Full Counterpropagation Neural Network to Image Watermarking", 2005, IEEE.

[4]. Ren –Junn Hwand,Chuan-Ho Kao and Rong-Chi Chang, "Watermark in Color Image" in Proc. First International symposium on cyber worlds,2002 ,pp 225-229.

[5]. Chitralekha Dwivedi and Ashish Bansal – "Preventing copyrights infringement of images by Watermarking in transform domain using full counter propagation Neural Network" UACEE International Journal of Computer Science and its Applications - Volume 2: Issue 3 No.6, November 2012

[6]. Chen Chien Chang and Kao De-Sheng — "DCT Based Reversible Image Watermarking Approach", Third IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2007, pp 1-5

[7]. Bamatraf A, Rosziati Ibrahim, Mohd Salleh, Mohd Najib, "A new digital watermarking algorithm using combination of least significant bit and Inverse Bit", Journal of Computing, Vol 3, Issue 4, April, 2011,pp 1-8.

[8]. Manjunatha Prasad. R, Dr. Shivaprakash Koliwad — "A Comprehensive Survey of Contemporary Researches in Watermarking fo Copyright Protection of Digital Images", International Journal of Computer Science and Network Security (IJCSNS), Vol.9 No.4, April 2009, pp.91-102.

[9]. Saeed AL-Mansuuri and Alavi Kunhu – "Robust watermarking Technique based on DCT to Protect the Ownership of DubaiSat-I image against Attacks", IJCSNS International Journal of Computer Science and Network Security, VOL 12 NO. 6, June 2012.

[10]. Narges Ahmidi and Reza Safabakhsh – "A Novel DCT – Based Approach for Secure color Image Watermarking", ITCC 04 IEEE 2004.

[11]. Cheru Kavadia, Vishal Shrivastava and Mayank Pokharna – "Secured and High Watermarking Techniques", International Journal on Recent and Innovation in Computing and Communication Vol: 1 Issue : 1 Jan2013.

[12]. Vaishali and Dr, Sachin R. Gengaje – "Literaruture Review of Wavelet Based Digital Image Watermarking Techniques", International Journal of Computer Applications Vol : 31 No : 1 Oct-2011

[13]. R.Schyndel, A.Tirkel, and C.Osborne, "A Digital Watermark" in Proc.IEEE Int. Conf. on Image Processing,Nov. 1994 ,Vol II,pp.86-90.

[14]. Huang Song , Zhang Wei – "Blind Watermarking Scheme Based on Neural Network", Proceedings of the 7th World Congress on Intelligent Control and Automation , Chongqing, China , 25 – 27 june, 2008,5985- 5989.

[15]. Hussein J A – "Spatial Domain Watermarking Scheme for colored images based on log Average Luminance", Journal of computing, Vol 2, Issue 1, Jan 2010,pp 100-103.

[16]. Yang W, Zheng Jin – "An Algorithm for Color Image Watermarking Based On the Combination of DWT and DCT", Journal of Central South Univers ty of Forestry & Technology, December,2008, pp 139 143.

[17]. Surekha B and Swamy G.N, — "A spatial domain public image watermarking‘‘, international journal of Security and its applications ,Jan 2011,Vol 5.

[18]. Sengupta M , Mandal J.K – "Self Authentication of Color Images through Discrete Cosine Transformation (SADCT)", IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 ,832-836.

[19]. Zheng jiang bin,Zhang Yan ning, Feng Da Gan, Zhao Reng chun, — "Color Image Watermarking Based on DCT-Domains of Color Channels", Proceedings of IEEE TENCON02, pp 281-284.

[20]. Poljicak A, Mandic L, Agic D — "Discrete Fourier transform–based watermarking method with an optimal implementation radius", Journal of Electronic Imaging, Vol 20, Aug 2011.

[21]. Vidyasagar M. Potdar, Song Han, Elizabeth Chang, "A Survey of Digital Image Watermarking Techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN), 2005, pp.709-713.

[22]. Ahmidi N. Safabaksh R. (2004)"A Novel DCT Based Approach for Secure Color Image Watermarking " in Proc. ITCC 2004 International Conference Information Technology:Coding and computing,vol 2,pp 709-713.

[23]. Manimaran V, Raja S.P, Narayanan Prasanth N, Francis J,, Princess S.P, (feb 2010)"Image watermarking by using DCT '',Proceedings of the International Conference on Information Science and Applications,pp 221-224

[24]. Mao Li, Fan Yang-yu, Lv Guo-yun, Wang Hui qin,"Adaptive Color Image Watermarking Algorithm based on Fractal and Neural Networks", 2009.

[25]. Kutter M, Jordan F, Bossen F, (1998) Digital watermarking of color images using amplitude modulation, J Electron Imaging 7(2) pp 326-332.