International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Received in revised form, 3 March 2019, Accepted 15 March 2019, Available online 7 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

Image Watermarking by DWT and Neural Network Model

SYED IBTIHAJ HASAN*, JAYSHREE BOADHH, AKRATI SHRIVASTAVA
Department of Computer Science and Engineering, Mittal group of Institution, India
*Ibtihajhasan08@gmail.com

Abstract *In recent years image data embedding schemes techniques have been widely studied. This data watermarking schemes allow us to embed a secret message into an image. So this work focus on iris image watermarking in an image. Here DWT low frequency band was used for embedding watermark information. Binary water mark information was hide in the image and this hided vectors are utilized to train the Error Back Propagation Neural Network. Extraction of watermark was done at receiver end from trained neural network. Use of trained neural network for extraction increase robustness of the hided data against various types of attacks. Experiment was done on IRIS image dataset and compared on various evaluation parameters. Results shows that proposed work has improved the PSNR, MSE, values as compared to other previous approaches.*

Keywords—Digital data hiding, Encryption, Histogram, Image Processing.

I INTRODUCTION

Watermarking is used in various contexts depending upon their needs. There are different types of watermarking like digital image watermarking, video watermarking, audio watermarking, digital signal watermarking and text watermarking. Initially, watermarking was used to provide security especially in military applications. The signal or message sent by the sender is invisibly watermarked. The receiver has to extract the watermark and the original message separately to verify whether he has received flawless message by the correct person. Image, video and audio watermarking was used particularly to provide copyrights. Digital image watermarking helps to embed the watermark into the host image. The host image is the original image over which watermarking algorithms are applied. The watermark can be an image or a text which has to be embedded into the host image. Watermark embedding or simply watermarking is the process of applying watermarking algorithms so as to embed the watermark image into the host image to get a watermarked image. Watermark extraction or simply extraction is the process of retrieving the embedded watermark from the watermarked image. Extraction is possible only when the watermarking process is reversible. If the watermark embedded is irreversible, then extraction of the embedded watermark is impossible. Depending on the requirement, the process of watermarking can be chosen as reversible or irreversible. When watermarking is done to provide copyrights or to solve ownership issues, irreversible method of watermarking is chosen. When one needs to provide authentication, watermarking becomes reversible. Other needs for watermarking are to provide reliability, confidentiality and security. Xuehua [22] has classified watermarking process based on various parameters. Based on its characteristic property, watermarking is called robust or fragile. When watermarking is done depending upon its purpose, then it can be classified as copyright protection watermarking, tampering tip watermarking, note anti-counterfeiting watermarking and anonymous mark watermarking. If the watermark is visible, then it is called visual watermarking and when it is invisible, watermarking is called blind watermarking. It is also classified based on the attaching media-image, video, audio, text. In medical domain, large databases containing varieties of images of different persons require safe and secured storage. While indexing these databases with relevant data, the storage bandwidth reduces and the retrieval becomes easier. The main goal of watermarking the medical images is to provide integrity and to index them properly. When we watermark them using reversible technique and index them based on the patient's details, it will be easy when retrieving them at latter stages. In this paper, we discuss about the existing algorithms for watermarking.

II. Related Work

Zigang Chen, et al. (2018) [4] In this paper, we analysis a new General-NMF (General non-negative lattice factorization) founded DW conspire for duplicate insurance and respectability verification of the picture content. Moreover, the producer issue of the irregular framework and n are utilized as the keys of the analysis DW plan. New outcomes about demonstrate that the proposed DW plan can successfully oppose different attacks and altering.

Ninny Mittal, et.al. (2017) [5] In this test, we projected optical watermarking (OW) for using pictures which relies upon the mix of 5 DWT, FFT and SVD. Another point of view of this examination is to discover the life of the VW plan, which is emerge of progression that can incorporate watermarked information to address picture data carried with front line

International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Received in revised form, 3 March 2019, Accepted 15 March 2019, Available online 7 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

cameras with no particular additional equipment's fundamental building.

Alifa D'Silva, et al. (2017) [6] In this paper a hybrid method utilizing SVD and DWT is individual planned. SVD and DWT are network depend tasks, crossover technique forestalls difficulty which would somehow expend a great deal of assets. Calculation of a bigger arrangement of information happens quicker because of the utilization of SVD. This plan has been recreated in MATLAB condition.

Guang Hua, et al. (2016) [7] This paper analyzes such a dual channel scheme from the perspective of digital filtering. We show that the dual channel-based watermark extraction actually applies a high pass filter to the watermarked signal, and the performance when the filter coefficients are changed is also studied. The effectiveness of the dual channel scheme in rejecting host signal interference is confirmed via extensive experiments using both synthetic and real audio and image signals.

Jin-Xia Yang, et al. (2017) [8] In order to improve the security of dual watermark, a novel dual audio watermarking scheme based on wavelet packet analysis and ultra-chaotic encryption is proposed. First, accuracy parameters are selected to generate super chaotic sequence and ultra-chaotic binary sequence which are used to encrypt zero-watermark sequence and image watermark acquiring more evenly distribution. Finally, simulation platform is utilized to test the performance of the algorithm.

Qing Chen, et al. (2016) [9] This paper proposes an algorithm of dual watermarking based on wavelet transform for data protection in smart grid. Two different watermarks, robustness watermark and fragile watermark, are embedded in the significant coefficients of DWT to protect both copyright and integrity of data.

Jeebananda Panda, et al. (2016) [10] Digital watermarking is a technique to employ copyright protection and ensure the authenticity of the owner using a proof of ownership embedded in a multimedia file. The watermarked video is subjected to different attacks and the efficiency of the technique is measured using Correlation Factor and PSNR. The algorithm presented is robust, secure and is energy efficient with decreased payload on the host signal.

Sawiya Kiatpapan, et al. (2015) [11] This paper describes an image tamper detection and recovery method based on self embedding dual watermarking. This dual watermarking strategy ensures a robust performance in image tamper detection and recovery. This makes it possible to recover large area of tampering, such as, left, right, upper, or lower half of the cover image.

III. Proposed Methodology

Main focus of this work was to cover up digital information in the image. Entire work was done in two stages of hiding digital images and extraction of digital data from embedded image. Here it is wanted that while extraction of secret information, [7, 8] whole data remain secured. In Fig. 3 entire inserting work piece graph is clarified.

Pre-Processing

Image is a matrix of pixel value collection as per format is set in between fix range like 0-255, 0-1, 0-360, etc. So perusing pixel value of that picture lattice is done in this progression of the proposed show. As whole work focus on the image which have pixel value in the scope of 0-255. So read an image implies making a framework of the same. Measurement of the image at that point fill the matrix cell to the pixel value of the image at the cell in the grid.

DWT (Discrete Wavelet Transform)

In order to increase robustness of embedded watermark low frequency region of the DWT feature matrix was used. This block of image is obtaining by filtering the image rows from the low pass filter then pass same to the low pass filter but here column is filter for the analysis. This block contains flat region of the image which do not have any edge information, so this is term as approximate version of the image. So this work use LL band of the DWT output, this region is less.

Watermark Image

In this step watermark image is read from and pre-process into fix dimension than convert image into binary format where each pixel is either black or white.

Embedding of Watermark

As per input matrix of watermark either black pixel or 0 OR white pixel 1 is represent. So each shows one class of the watermark, now input LL matrix is resize into 8XN matrix such that 8XN=LL. Now if black pixel comes for hiding than read one row from 8XN and increase pixel values of left-hand side of four values.

In other case if white pixel comes for hiding than read next row from 8XN and increase pixel values of right-hand side of

International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Received in revised form, 3 March 2019, Accepted 15 March 2019, Available online 7 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

four values. So if watermark have 1024 pixels than total 8 X 1028. Pixel values of LL band of cover image get affected.

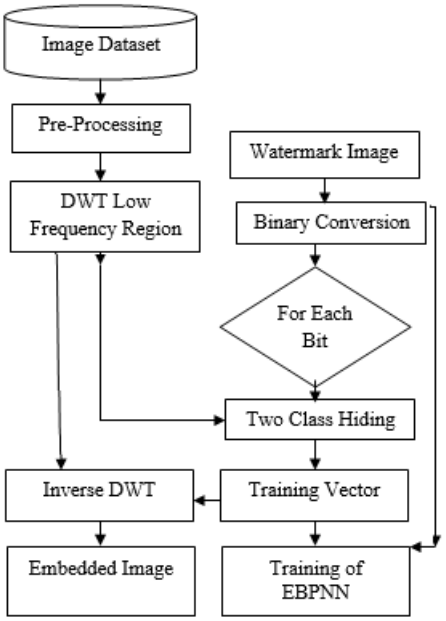

Fig.1 Block diagram of proposed work.

Training of Neural Network

Here each affected row which take part in hiding of watermark is used for training where output is corresponding watermark pixel. So this set of input and output vector is pass in the error back propagation neural network.

Embedded Image

Here after embedding the watermark in LL portion of image 8XN matrix is resize into LL dimension. Now inverse discrete wavelet transform was done by taking LH, HL, HH matrix as an input.

Extraction steps

In this extraction steps receiver can extract data from the received image and trained neural network. As done at embedding side received image is pre-process and extract DWT feature from it. Now LL matrix of that DWT feature is transforming into 8XN matrix than pass each of *X1 from 8XN into trained neural network which gives an output of 0 OR1 representing the black or white pixel values.

IV. Experiment and Result

This area exhibits the experimental assessment of the proposed procedure for protection of picture. All calculations and utility measures were executed by utilizing the MATLAB apparatus. The tests were performed on a 2.27 GHz Intel Core i3 machine, outfitted with 4 GB of RAM, and running under Windows 7 Professional.

Dataset

Analysis done on the standard pictures, for example, mandrilla, lena, tree, and so forth. These are standard pictures which are gotten from http://sipi.usc.edu/database/?volume=misc. Framework is tried on everyday pictures also.

Peak Signal to Noise Ratio

$$\text{PSNR} = 10\log_{10}\left(\frac{Max\_pixel\_value}{Mean\_Square\_error}\right)$$

Mean Square Error

$$\text{SNR} = 10\log_{10}\left(\frac{Signal}{Noise}\right)$$

Extraction Rate

$$\eta = \frac{n_c}{n_a} \times 100$$

Here n_c is number of pixels which are true.
Here n_a is total number of pixels present in Data Hiding.

Table 1. PSNR Based Comparison between proposed and previous work.

PSNR Based Comparison		
Images	**Proposed Work**	**Previous Work**
Lena	32.6517	25.6513
Mandrilla	30.439	24.6996
Tree	31.2476	25.3923

From table 1 it is obtained that under ideal condition proposed work is better as compare to previous work in [12]. under PSNR evaluation parameters. As DWT and EBPNN algorithm has regenerate images in color format only so this parameter is high as compare to previous value. From table 2 it is obtained that under ideal condition proposed work is better as compare to previous work in [12]. under MSE evaluation parameters. As DWT and EBPNN algorithm has regenerate images in color format only so this parameter is high as compare to previous value. From table 3, 4 and 5 it is obtained that under filter attack condition proposed work is

International Journal of Current Trends in Engineering & Technology
Received 1 February 2019, Received in revised form, 3 March 2019, Accepted 15 March 2019, Available online 7 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

better as compare to previous work in [12]. Extraction rate evaluation parameters. As DWT and EBPNN algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table 2. SNR based comparison between proposed and previous work.

MSE Based Comparison		
Images	**Proposed Work**	**Previous Work**
Lena	35.3107	176.991
Mandrilla	58.7728	220.356
Tree	48.7891	187.866

Table 3. PSNR Based Comparison between proposed and previous work.

Filter Attack Based PSNR Comparison		
Images	**Proposed Work**	**Previous Work**
Lena	31.2935	25.25
Mandrilla	21.9549	19.0691
Tree	29.4281	22.3579

Table 4. MSE Based Comparison between proposed and previous work.

Filter Attack Based MSE Comparison		
Images	**Proposed Work**	**Previous Work**
Lena	48.2764	193.865
Mandrilla	414.563	805.701
Tree	74.1777	377.821

Table 5. Extraction rate comparison between proposed and previous work.

Filter Attack Based Data Extraction Comparison		
Images	**Proposed Work**	**Previous Work**
Lena	62	31.1768
Mandrilla	70	32.5684
Tree	72	30.3223

V. CONCLUSION

In this work proposed neural network-based hiding has effectively hide data in the carrier image. As neural network need training so this was done at sender side while extraction of data was done at receiver side so trained neural network was send at extraction side. Hence security of the data increases as intruder should know embedded image and trained neural network parameter to get hided watermark. Proposed algorithm recovers or reverse complete data at receiver end, in ideal condition. Results shows that the proposed work was compared with previous work in [12] and it was obtained that proposed work has improved the PSNR, MSE, extraction rate evaluation parameters. In future, work can be improving for other attacks such as geometry of image.

References

[1]. Tamanna Tabassum, S.M. Mohidul Islam "A Digital Image Data Hiding Technique Based On Identical Frame Extraction In 3-Level DWT" Vol. 13, No. 7, Pp. 560 – 576, July 2003.

[2]. Frank Hartung, Jonathan K. Su, And Bernd Girod "Spread Spectrum Data Hiding: Malicious Attacks And Counterattacks". Of Multimedia Contents" International Journal Of Research In Engineering And Technology EISSN: 2319-1163 | Pissn: 2321-7308, 2005.

[3]. "CHAPTER 2. WAVELET TRANSFORMS ON IMAGES" *Sundoc. Bibliothek. Uni-Halle. De /Diss-Online/02/03H033/T4.Pdf, 2008.*

[4]. Zigang Chen, Lixiang Li, Haipeng Peng, Yuhong Liu, and Yixian Yang, "A Novel Digital Watermarking based on General Nonnegative Matrix Factorization". This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TMM.2018.2794985, IEEE Transactions on Multimedia

[5]. Ninny Mittal, Anand Singh Bisen, Rohit Gupta, "An Improved Digital Watermarking Technique Based on 5-DWT,FFT & SVD". International Conference on Trends in Electronics and Informatics ICEI 2017. 978-1-5090-4257-9/17/$31.00 ©2017 IEEE.

[6]. Alifa D'Silva, Nayana Shenvi, "Data Security Using SVD Based Digital Watermarking Technique". International Conference on Trends in Electronics and Informatics ICEI 2017, 978-1-5090- 4257-9/17/$31.00 ©2017 IEEE.

[7]. Guang Hua, Guoan Bi, Yong Xiang, "Dual Channel Watermarking – A Filter Perspective". 2016 International Conference on Progress in Informatics and Computing (PIC). 978-1-5090-3484- 0/16/$31.00 ©2016 IEEE.

Received 1 February 2019, Received in revised form, 3 March 2019, Accepted 15 March 2019, Available online 7 April 2019
www.ijctet.org, ISSN: 2395-3152
Volume: 05, Issue: 02 (March- April, 2019)

[8]. Jin-Xia Yang, Dan-Dan Niu, "A Novel Dual Watermarking Algorithm for Digital Audio". 2017 17th IEEE International Conference on Communication Technology. 978-1-5090-3944- 9/17/$31.00, 2017.

[9]. Qing Chen, Meng Xiong, "Dual Watermarking Based on Wavelet Transform for Data Protection in Smart Grid". 2016 3rd International Conference on Information Science and Control Engineering. 978-1-5090-2534-3 /16 $31.00 © 2016 IEEE.

[10]. Jeebananda Panda, Indu Kumari, Nitish Goel, "Dual Segment Video Watermarking using Energy Efficient Technique". 2016 1st India International Conference on Information Processing (IICIP). 978-1-4673-6984-8/16/$31.00 © 2016 IEEE

[11]. Sawiya Kiatpapan and Toshiaki Kondo, "Sawiya Kiatpapan and Toshiaki Kondo". 2015 12th International Conference on Electrical Engineering /Electronics, Computer, Telecommunications and Information Technology (ECTI-CON). 978-1-4799-7961-5/15/$31.00 c 2015.

[12]. Mohammed A. M. Abdullah, Satnam S. Dlay, Wai L. Woo, and Jonathon A. Chambers. "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography". IEEE Access Year: 2016, Volume: 4 Pages: 10180 – 10193.