Arzoo Singh et al. 2019, 7:5
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science,
Engineering and Technology

An Open Access Journal

An Digital Image Watermarking Using DWT and Chaotic Function

Arzoo Singh, Prof. Abhishek Sharma

Department Electronics and Communication
Bhopal ,, M.P. India
Sagar Institute of Science and Technology

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 focuses on image watermarking in a image. Here DWT low frequency band was used for embedding watermark information. Binary water mark information was hiding in the image and this hided vectors are utilized to robust by chaotic shuffling function. Extraction of watermark was done at receiver end from rounded chaotic function. Use of this kind of embedding combination of frequency and LSB techniques increase robustness of the hided data against various types of attacks. Experiment was done on real 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 cameras with no particular additional equipment's fundamental building..

AlifaD'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.

SawiyaKiatpapan, 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. 1 entire inserting work piece graph is clarified.

Pre-Processing

Image is an 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 a 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 obtain by filtering the image rows from the low pass filter then pass same to the low pass filter but here column are filter for the analysis. This block contain 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 sensitive for attacks.

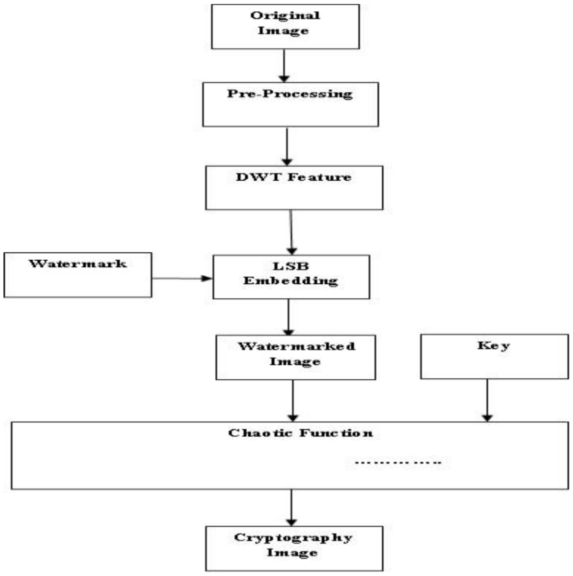


Figure1: Block diagram of proposed work.

LSB Embedding

Here as image is combination of numeric value then conversion of that value into its equivalent binary values is done at first level then replacement of that binary value into last four bit of the selected pixel position of low frequency band of DWT feature is done. Here number of data hiding characters or numbers positions should be less as compare to selected pixel positions. In this work whole image maintain large amount of original values.

Block: As work is done on color image so embedding is done on the red matrix of the image, so whole operation of embedding is done this red matrix. Whole red matrix is divide into 2x2 blocks for embedding the message into image. As after canny algorithm each image pixel value is divide into two regions first is edge and other is non-edge. So for embedding following steps are taken.

For a non edge pixel in a block embed „x‟ bits of message XOR with „x‟ MSBs of the pixel by LSB substitution. To maintain the quality of the embedded image, the value of x here is 1.

For an edge pixel in a block, embed „y‟ bits of message XOR with „y‟ MSBs of the pixel by LSB substitution. The value of „y‟ is generated randomly for each pixel using chaotic map. To maintain the quality of stego image, the value of y is 3.

Now combined all 2x2 blocks into single red matrix. Now combine this embedded red matrix with other blue and green matrix, which give embed image.

Chaotic Encryption

In this step original image from the database is jumble by utilizing the chaotic matrix where each pixel position is multiply by the matrix, then new position is obtain for the pixel value. In similar fashion all pixels of the image is randomize.

Chaotic Matrix = $\begin{vmatrix} 1 & 1 \\ \lambda & \lambda+1 \end{vmatrix}$

CM (Chaotic Matrix), λ is variable range from 1,2………n.

$$\begin{vmatrix} 1 & 1 \\ \lambda & \lambda+1 \end{vmatrix}$$

Let P is matrix represent [row, column], then multiple CM and p, will give N matrix which is a new pixel position of the older pixel.
N=CM*P

Extraction steps
In next module of this step encrypted image obtain is decrypt first by running remaining cycle of the chaotic function to get the watermarked image. It depends on the image dimension and chaotic parameter that how many numbers of iterations are required. After this DWT feature is extract from the image where LL band is used for extraction of watermark information from the image.

Now block LL band into 2*2 size. First pixel gives Edge and non edge region while other 3 pixel of block gives watermark data. So if LSB of first pixel is 101than second and fourth pixel are edge region while third pixel is non edge.Hence1 watermark bit is extract from non edge pixel and 3 watermark bit is extract from edge pixel. By repeating above steps for remaining 2*2 blocks of LL band, watermark data is obtained.

Proposed Embedding Algorithm
Input: OI, W// OI Original Image, W Watermark

```
• OutPut: CI Chaotic Embedded Image
• [Non-Edge Edges]   Edge_Detection(O)
• B Block(O, m) // B blocks of image in mxm size

• Loop 1:B
• Loop n = 1: Edge
• Binary   Edge(n)
• x   XOR(Binary(MSB), M) // MSBt
• Binary(LSB)   x
• EI   Binary
• EndLoop
• Loop n = 1: Non-Edge
• Binary   Non-Edge(n)
• x   XOR(Binary(MSB, M) // MSB one bits
• Binary(LSB)   x
• EI   Binary
• EndLoop
• EndLoop
• While CI Not Equal EI
• CI   Chaotic_Shuffling(EI)
• If c= Embedding_position
• Break Loop
• EndIf
• Endif
• Endloop
```

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, Cup, 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.

Evaluation Parameter:
Peak Signal to Noise Ratio

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

Signal to Noise Ratio

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

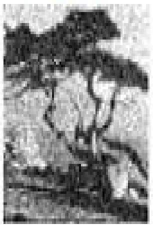
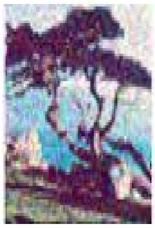
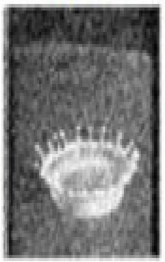
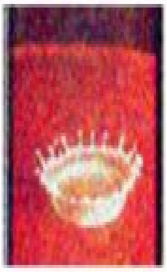
Extraction Rate

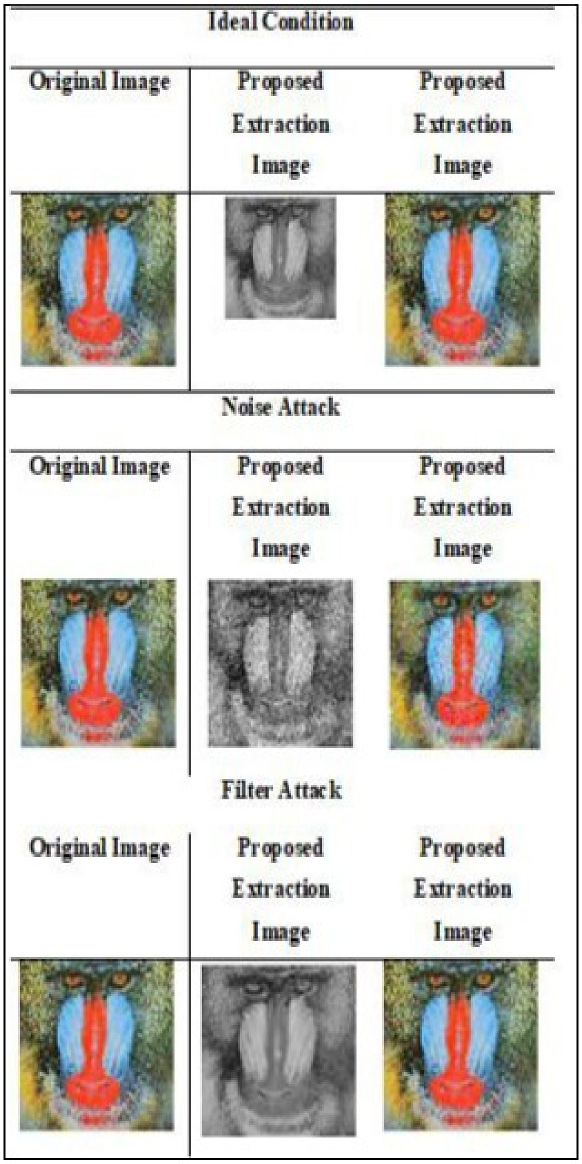
$$\eta = \frac{n_c}{n_a} \times 100$$

Here nc is number of pixels which are true.
Here na is total number of pixels present in Data Hiding.

Results:

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

Ideal Condition		
Original Image	Proposed Extraction Image	Proposed Extraction Image
Noise Attack		
Original Image	Proposed Extraction Image	Proposed Extraction Image
		
Filter Attack		
Original Image	Proposed Extraction Image	Proposed Extraction Image
Original Image	Proposed Extraction Image	Proposed Extraction Image
Noise Attack		
Original Image	Proposed Extraction Image	Proposed Extraction Image
		
Filter Attack		
Original Image	Proposed Extraction Image	Proposed Extraction Image


Ideal Condition
Original Image
Proposed Extraction Image
Proposed Extraction Image
Noise Attack
Original Image
Proposed Extraction Image
Proposed Extraction Image
Filter Attack
Original Image
Proposed Extraction Image
Proposed Extraction Image

PSNR Based Comparison		
Images	Proposed Work	Previous Work
Cup	85.0953	52.3594
Tree	85.79	50.5478
Mandrilla	87.0298	52.1584

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, LSB and Chaotic 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.

SNR Based Comparison		
Images	Proposed Work	Previous Work
Cup	71.0027	3.38207
Tree	70.5523	35.4064
Mandrilla	69.8405	3.60298

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, LSB and Chaotic algorithm has regenerate images in color format only so this parameter is high as compare to previous value.

Table -3: PSNR Based Comparison between proposed and previous work in different Attack.

Filter and Noise Attack Based PSNR Comparison				
Images	Filter Attack		Noise Attack	
	Proposed Work	Previous Work	Proposed Work	Previous Work
Cup	27.8531	52.3006	49.5037	52.3021
Tree	16.3473	50.4433	50.762	50.5096
Mandrilla	29.7668	52.0796	50.8878	52.1078

Table -4: SNR Based Comparison between proposed and previous work in different Attack.

Filter and Noise Attack Based PSNR Comparison				
Images	Filter Attack		Noise Attack	
	Proposed Work	Previous Work	Proposed Work	Previous Work
Cup	11.826	3.36683	33.4766	3.32474
Tree	31.585	3.34628	35.5243	3.41257
Mandrilla	13.6478	3.52418	34.7688	3.55244

Table -5: Extraction rate comparison between proposed and previous work in different attack.

Filter and Noise Attack Based PSNR Comparison				
Images	Filter Attack		Noise Attack	
	Proposed Work	Previous Work	Proposed Work	Previous Work
Cup	54.1667	43.75	59.1837	36.8056
Tree	47.7273	43.75	51.0638	40.9722
Mandrilla	42.8571	42.3611	38.7755	43.0556

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

V. CONCLUSION

In this work proposed neural network based hiding has effectively hide data in the carrier image. As combination of frequency and spatial feature works well at sender side while extraction of data. Hence security of the data increases as intruder should know embedded image and chaotic matrix 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, SNR, extraction rate evaluation parameters. In future, work can be improve 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]. AlifaD‟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.

[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 IEEE.

[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]. SawiyaKiatpapanandToshiakiKondo, "SawiyaKiatpapan 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 IEEE.

[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.