I.J. Engineering and Manufacturing, **2017, 2, 50-63**
Published Online March 2017 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijem.2017.02.05

Available online at http://www.mecs-press.net/ijem

A LL Subband Based Digital Watermarking in DWT

Kamaldeep Joshi [a], Rajkumar Yadav [a]

[a] *University Institute of Engineering and Technology, Maharshi Dayanand University, Rohtak, Haryana, India*

Abstract

Digital watermarking is a technique which allows an individual to add hidden copyright notices or other verification messages to digital audio, video, image and documents in such a way that the watermark cannot be removed against different attacks. Digital Watermarking is a process to prevent the unauthorized access and modification of data. It ensures that the communication between two parties' remains secure. Digital watermarking can be performed in spatial and frequency domain. In the spatial domain, the watermark is embedded in the very existence of the pixel. In frequency domain, the transformation of any kind is applied and then information is embedded. In this paper, we proposed an approach to watermarking in frequency domain using DWT technique. The gray scale host image is divided into four sub bands: LL, HL, LH, HH and the watermark are inserted in the LL sub band using DWT technique. As the image is divided into four sub bands, a watermark of equal size of the LL sub band is inserted and the results are analyzed on the bases of different parameters such as PSNR and MSE. LL represents the average component of the host image which contains the maximum information of the image. In this approach the watermark is inserted in LL sub band using XOR operation. As the table IV shows, the imperceptibility of this method is quite good. Also, it shows good results when compared with existing methods.

Index Terms: Watermarking, Discrete Wavelet Transform, XOR, Embedding, Extraction, Steganography.

1. Introduction

Digital watermarking is the best approach to prevent assets from the unauthorized access. Digital watermarking is the act of hiding a message related to digital data (i.e. Audio, video, images) within signal itself [1]. It is nearly similar to steganography because both hide a secret message in a digital data. However, what separates them is their goal. Digital watermarking is a technique for inserting information (the watermark) into an image (visible or invisible) for authentication, while steganography is used to embed the message within another object known as cover media for secret communication, by changing its properties [2].

Digital watermarking may also be used to hide the information in cover media to protect the software for

* Corresponding author.
E-mail address:

copyright. For insertion of the watermark, we need to embed the watermark in images using the insertion algorithm. After embedding the watermark, the extraction algorithm is used to extract the watermark [3].

Extraction of watermark technique divided into three steps:

- Non-Blind technique:-In this technique, cover image and secret key are required.
- Blind technique:-In this technique, watermark and secret key are required.
- Semi blind: - In this technique, key is required.

Digital watermarking technique is divided into two parts:

1.1. Spatial Domain Technique

In the spatial domain, the watermarking is embedded through direct altered the pixel value of the cover image. LSB is one of the popular techniques in spatial domain. Watermark insertion can be 1 bit, 2 bit, and 3bit of least significant bit into a pixel of the cover image. In this method, the least significant bits of the cover media's are used to conceal the message. This method is based on masking of the bits and watermark. This method is originally applied on gray scale images, but extended to color images by considering each color plane as a single plane in which data is inserted in the LSBs. The Watermark can be extracted if the position of LSBs used in embedding process is known [4]. These methods have high message carrying capacity, but high vulnerable to the attacks.

1.2. Frequency Domain Technique

In Frequency domain, a watermark is inserted into the host image using various transformations like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT). It shows better robustness when compared to the spatial domain technique [5].

1) Discrete Cosine Transform: In the DCT watermarking scheme, firstly original images divided into 8×8 blocks of pixels to hide the secret data. It divides the image into high, low and medium frequency domain if any changes occur in single coefficient then it can affect the all 64 blocks pixel. Coefficients of middle frequency range are picked from the DCT coefficients and modified to their relative values encode a one or zero in order to embed the watermark bits. Watermark image is then obtained by performing the inverse of DCT of each block. The DCT coefficient is used for image compression [6].

The following equation can use for DCT coefficient:

$$F(u,v)=\frac{1}{4}\ C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (1)$$

For u=0, ……….7 and v=0……….7

Where C(k)= $1/\sqrt{2}$ for k=0 1 otherwise

Inverse DCT

$$F(u,v)=\frac{1}{4}\ \sum_{u=0}^{7}\sum_{v=0}^{7} C(u)C(v)f(u,v)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2y+1)v}{16}\right] \quad (2)$$

For x=0, ……….7 and y=0……….7

Middle frequency range coefficient is taken from DCT coefficients and changes the value encode a one or zero in order to embed the bits. For extraction, performs the inverse DCT on each block.

2) Discrete Wavelet Transform: DWT is one of the best techniques in Frequency domain. It has good capacity and robustness than other technique. It takes less time for Computation. DWT, perform multi-resolution decomposition on images using wavelet function. It has own space frequency property. DWT provides spatial and frequency spread of watermark in the cover image. DWT divide the signal into high and low frequency. The high part contains edge component and low part again divide into low and high part. It divides the frequency in four sub bands. These sub bands can be decomposed further to acquire the next coarser scaled wavelet coefficient. To perform second level decomposition, the DWT is applied to LL band which decomposes the LL band into four sub-bands: LL1, LH1, HL1 and HH1 [7].

DWT decomposes the signal into mutually orthogonal. This is the main difference between continuous wavelet transform (CWT) and discrete wavelet transforms (DT-CWT). Some mathematical condition in DWT is given follows: e.g. Dilation equation

$$\phi(x) = \sum_{-\infty}^{\infty} ak\, \phi(s_x - k)z \tag{3}$$

Where s is scaling factor and *ak* is finite set of coefficient, which define the scaling function and wavelet.

$$\int_{-\infty}^{\infty} \phi(x)\, \phi(x+l)dx = \delta_0\, , l \tag{4}$$

DWT is superior transformation because it has two main features: multi-resolution & best image localization.

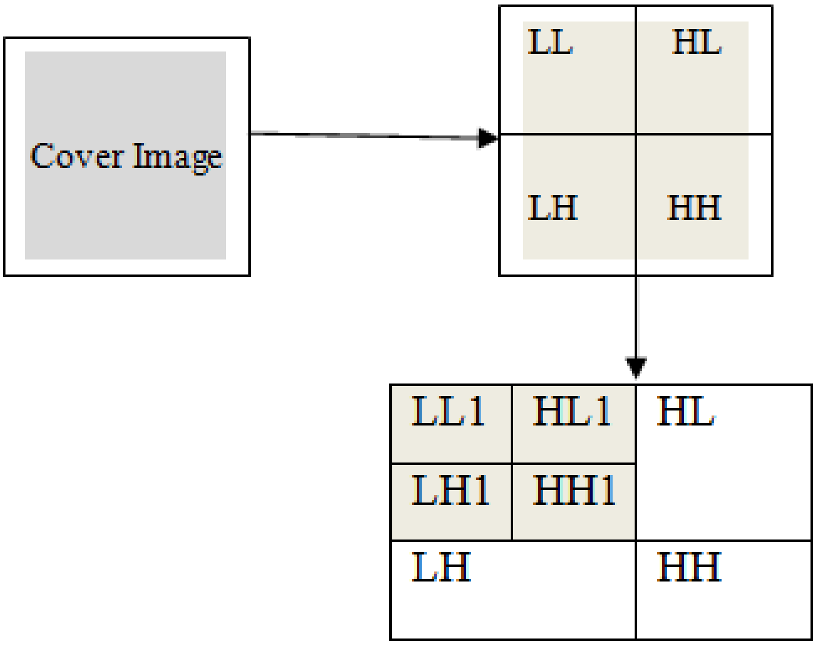


Fig.1. First and Second Level Decomposition of Host Image

3) Discrete Fourier Transform: The Discrete Fourier transform is used for getting the frequency component for each pixel of the cover image. In Fourier transform, output image produced in complex number value which could be displayed in two images with real and imaginary part or with magnitude and phase. The two dimensional DFT is performed on real numbers. When watermark is embedded in the phase component with high redundancy; a malicious attacker would cause unacceptable damage to the quality of the image to remove the watermark [8].

The Discrete frequency domain used for getting the frequency component for each pixel of the cover image. The DFT of Spatial value F (u, v) for image size M × N is defined by the following equation for their frequency domain [15].

$$F(u, v) = \frac{1}{\sqrt{MN}} \sum_{U=0}^{M-1} \sum_{v=0}^{N-1} F(x, y) e^{-12\pi \frac{UX}{M} + \frac{VY}{M}} \quad (5)$$

In inverse discrete frequency transformation, convert the frequency Component into the spatial domain using this equation:

$$F(x, y) = \frac{1}{\sqrt{MN}} \sum_{U=0}^{M-1} \sum_{v=0}^{N-1} F(u, v) e^{12\pi \frac{UX}{M} + \frac{VY}{M}} \quad (6)$$

In Fourier transform, output image produced in complex number value which could be displayed in two images with real and imaginary part or with magnitude and phase. The two dimensional DFT is performed in real number and DFT of an image results in the magnitude and phase representation of the image.

2. Literature Survey

Singh et al. [9] proposed method to insert multiple watermarks in spatial and frequency domain to make assets secure and dividing the host image into two regions: region A and region B. In region A, owner information is inserted with the help of LSB technique and region B is used to insert the watermark with additive technique DCT-DFT. Singh et al. [10] proposed method Robust Deinterlacing multiple image watermarking technique in DWT. In this method, deinterlacing process on sub band of image according to even and odd row pixel value is applied. Chen et al. [11] proposed a new steganography technique which embeds the secret message in frequency domain. Muhammad et al. [12] proposed a technique new robust digital image watermarking which was based on singular value decomposition and discrete wavelet transform for protection real property rights. Raval et al. [13] analyzed the performance of multiple watermark images in the low and high frequency sub-band of 2nd level of DWT by inserting 2 different binary watermarks using an additive scaling method by taking strength factor of watermark 0.10. Ranjan et al. [14] proposed a method which is based on securing non blind based watermark by inserting a binary watermark into last pixel of each bock after applying one level of DWT and DCT of block size 8*8. Sridhar et al. [15] applies multiple watermarking on a single host image. In this, their proposed method decomposes host image by using DWT technique after the image is divided into even and odd number of rows and then embed two different gray image as watermark into these divided images. After embedding inverse DWT is applied on sub-bands of the host image and watermarked image is generated. Durge et al. [16] introduces digital image watermarking algorithm based on singular value decomposition. Digital watermarking can be utilized for authentication of data, copyright protection and communication process. Keshri et al. [17] focuses on the security of watermarking image. In his paper the concept of dual watermarking was implemented. For insertion of the message two techniques were used. First, spatial domain technique and second frequency domain technique was used. Tao et al. [18] proposed a technique for securing multiple watermark images in DWT up to two level by inserting four same watermarks at 1st and 2nd level of DWT in all sub bands and analyzing the performance of all watermark.

3. Proposed Work

Singh The proposed technique hides a watermark (W) of size Wm* Wn into gray scale host image (H). We apply DWT transformation on host image which result four sub band LL, HL, LH and HH. Now, we select the LL sub band to insert the watermarking using XOR operation. In extraction process of watermark, apply reversing process as used in embedding process. In this proposed work we followed two step i.e.

Step 1: Apply 1 level DWT for image decomposition into four sub band

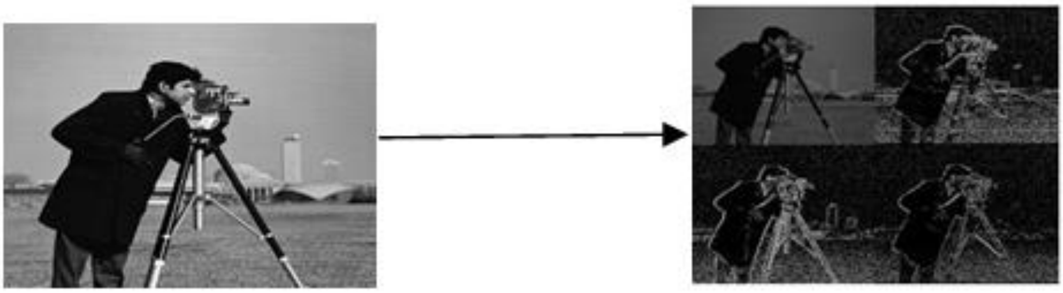


Fig.2. First level DWT Image Decomposition

In step 1, we apply DWT transformation which results in four sub bands. We select the LL Sub band for embedding the watermark.

Step 2: Embed the Watermark into LL sub band

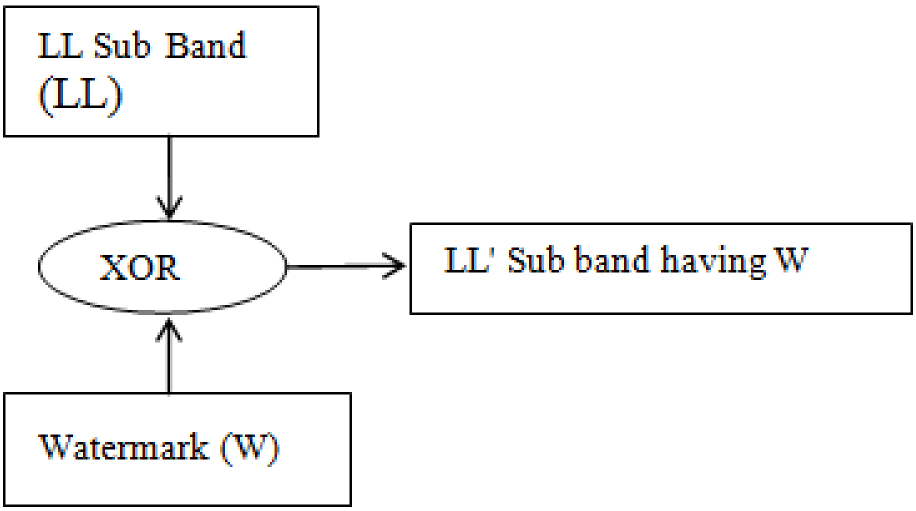


Fig.3. Watermarking Process

3.1. Watermark Embedding algorithm

Steps for Embedding Process are:

Step 1: Read the host image (H) and Watermark image (W)

$$H= \{h_{ij} \mid h_{ij} = \sum h_{ijx}$$

Where $h_{ijx} \in$ {host Image} and $\forall\, h_{ijx} \in (0, 1…255)$

Step 2: Applying DWT transformation of host image and we got four sub band LL,HL, LH and HH with four different frequencies called approximation, vertical, horizontal and diagonal respectively

Step 3: Select LL sub band and insert the watermark in LL sub band

$$W= \{W_{mn} \mid 0 \leq m < LL_r , 0 \leq n < LL_c \}$$

Where LL_r *and* LL_c are the dimensions of LL sub band after image transformation in frequency domain.

Step 4: Watermark embedding can be done as:

$$S_{mn} = H_{mn} \oplus W_{mn}$$

Step 5: Where S_{mn} stego pixel of LL sub band of stego image is obtained after applying inverse DWT transformation and represented as:

$$S= \{s_{ij} \mid s_{ij} = \sum s_{ijx}$$

Where $s_{ijx} \in$ {Watermarked Image} and$\forall\, s_{ijx} \in (0, 1….255)$

3.2. Watermark Extraction Algorithm

Steps for Extraction Process are:

Step 1: Read the stego image(S_{mn}) and host image (H).

$$S= \{s_{ij} \mid s_{ij} = \sum s_{ijx}$$

Where $s_{ijx} \in$ {Watermarked Image} and $\forall\, s_{ijx} \in (0, 1, 2……255)$

Step 2: Applying DWT transformation of host image and Watermarked image, we got four sub bands LL, HL, LH and HH with four different frequencies called approximation, vertical, horizontal and diagonal respectively.

Step 3: Select the LL sub band of host image and Watermark image

Step 4: Watermark extraction can be done as:

$$W_{mn} = S_{mn} \oplus h_{mn} \mid 0 \leq m < LL_r , 0 \leq n < LL_c$$

$$\text{And } W = W_{mn} | W_{mn}$$

Step 5: Apply inverse DWT transformation to get host image.

$$H= \{h_{ij} \mid h_{ij} = \sum h_{ijx}$$

Where $h_{ijx} \in$ {Host image} and $\forall\, h_{ijx} \in (0, 1, 2\ldots\ldots255)$

A. Flow Chart

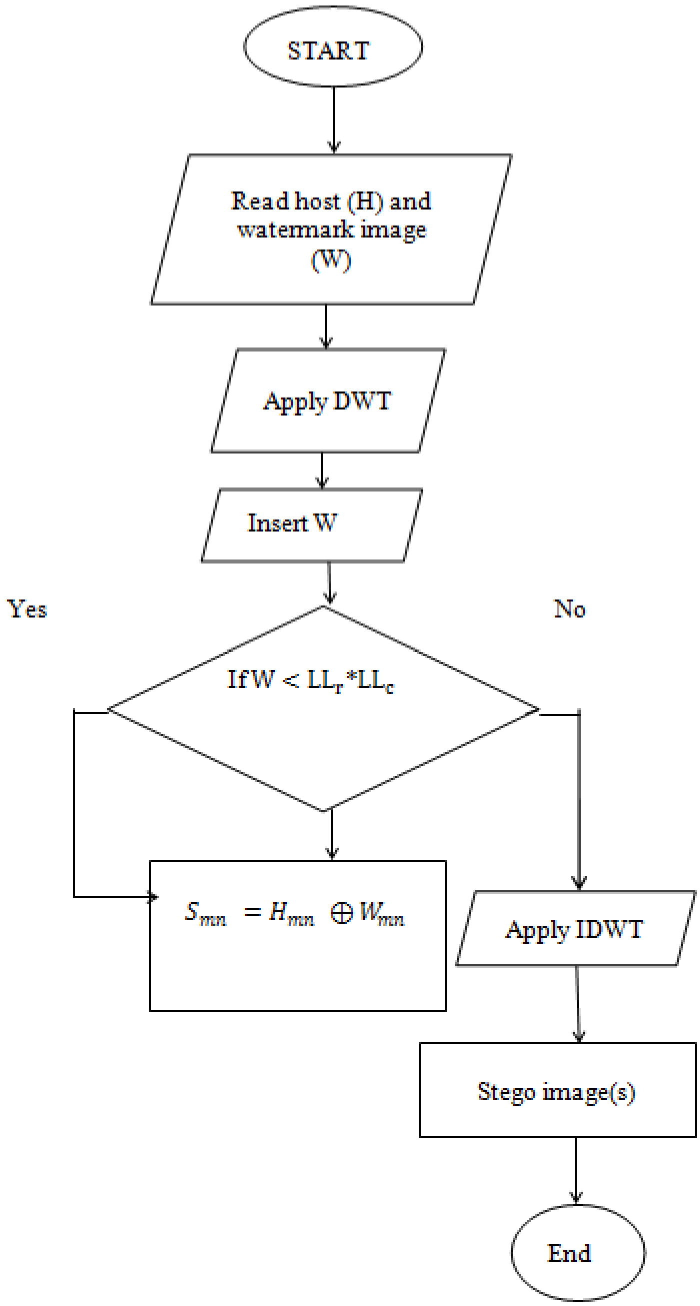


Fig.4. Flow Chart of Embedding Process

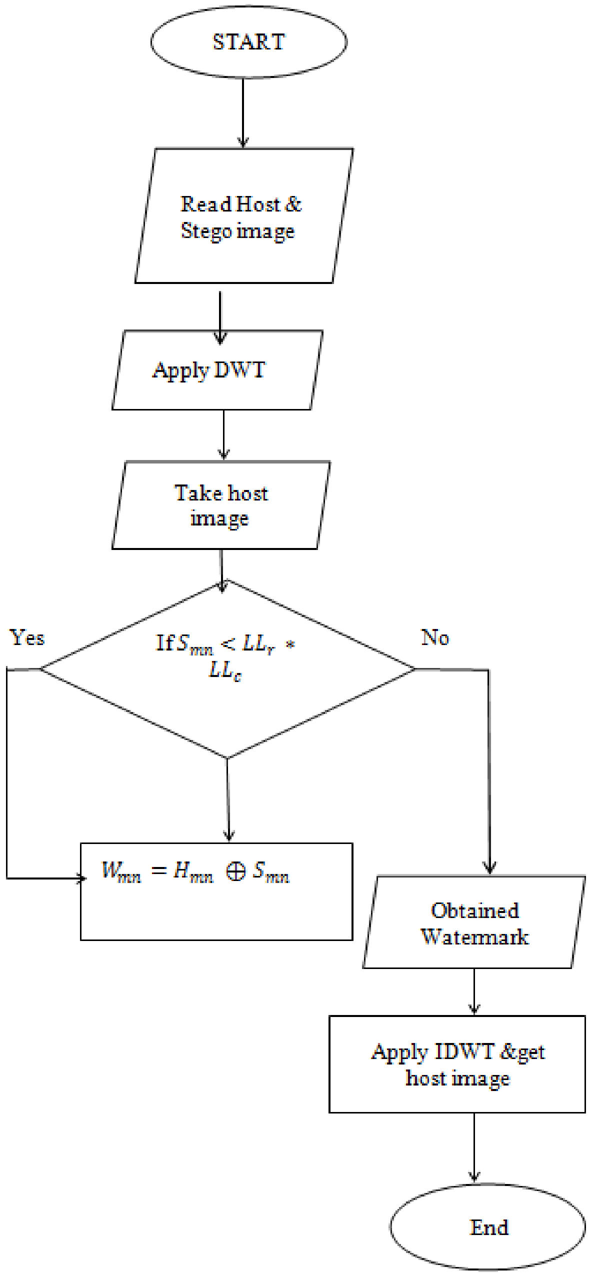


Fig.5. Flow Chart of Extraction Process

4. Result and Analysis

Singh The proposed technique hides a watermark (W) of size Wm* Wn into gray scale host image (H). We apply DWT transformation on host image which result four sub band LL, HL, LH and HH. Now, we select the LL sub band to insert the watermarking.

Table 1. Original and Extracted Watermark

Image Name	Original Watermark	Extracted Watermark
1		
2		
3		
4		
5		

Table 2 PSNR, MSE and MAXERR value

Image name	PSNR	MSE	MAXERR
1	54.7834	0.2158	0.9325
2	53.7897	0.2270	0.9330
3	54.7990	0.2137	0.9337
4	55.8870	0.2030	0.9369
5	55.6890	0.2075	0.9359
Average of 50 images	54.2332	0.2150	0.9330

Table 3. Host Image and Watermarked Image

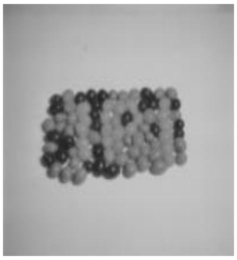
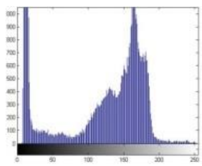
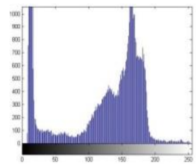
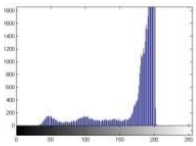
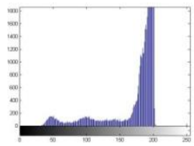
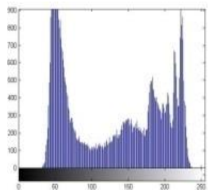
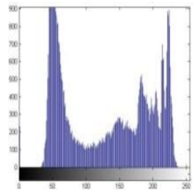
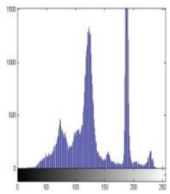
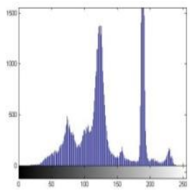
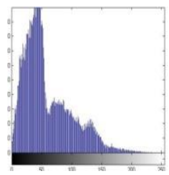
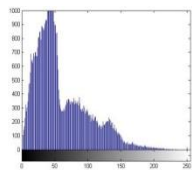
Image name	Original Image	Watermarked-Image
1		
2		
3		
4		
5		

Table 4. Host Image and Watermarked Image Histogram

Image name	Original image histogram	Stego image histogram
1		
2		
3		
4		
5		

5. Comparison

Singh T Comparison of Sridhar et al. and Singh et al. methods with our proposed method on image Lena, Goldhill and Boat having size 512*512 is given by the following tables. We consider infinite value of PSNR as max (100db).

Table 5. PSNR Comparison Table of Watermarked Image of Sridhar's and Singh method with Proposed Method

Images	Attacks	Shiridhar method	Singh's method	Proposed Method
LENA	**Without Attack**	**21.5**	**45.76**	**52.34**
	Salt and pepper	19.81	34.80	51.34
	Gaussian	**19.11**	**30.11**	**50.12**
	Speckle	19.30	38.41	52.23
GOLDHILL	**Without Attack**	**21.50**	**45.76**	**55.32**
	Salt and pepper	19.81	35.51	51.43
	Gaussian	**19.11**	**29.92**	**50.34**
	Speckle	19.30	35.85	51.67
BOAT	**Without Attack**	**21.50**	**45.76**	**54.34**
	Salt and pepper	19.81	35.40	50.35
	Gaussian	**19.11**	**29.92**	**49.76**
	Speckle	19.30	34.93	50.11

Table 6. PSNR comparison Table of Extracted Watermarked Image of Sridhar's And Singh Method with Proposed Method

Images	Attacks	Shiridhar method	Singh's method	Proposed Method
LENA	**Without Attack**	**28.49**	**Inf**	**Inf**
	Salt and pepper	27.03	75.19	77.23
	Gaussian	**27.80**	**52.56**	**55.23**
	Speckle	27.18	57.95	60.56
GOLDHILL	**Without Attack**	**28.49**	**inf**	**Inf**
	Salt and pepper	27.03	75.46	77.23
	Gaussian	**27.80**	**52.68**	**55.23**
	Speckle	27.18	55.37	60.56
BOAT	**Without Attack**	**28.49**	**inf**	**Inf**
	Salt and pepper	27.03	74.93	77.23
	Gaussian	**27.80**	**52.67**	**55.23**
	Speckle	27.18	54.58	60.56

6. Conclusion

In this paper, a new approach proposed using DWT is being proposed. The aim of watermarking algorithms is to make watermark secure and invisible to human eye. In order to improve the security, we have taken the benefit of XOR operation for embedding and extraction of the watermark. The method is analysed on the basis of PSNR, MSE and MAXERR the results are show in the tables. In this work, fifty images were tested and it is found that the proposed method provides good imperceptibility as the extracted image of watermark is same as original image. Also the average PSNR, MSE, and MEXERR are 54.2332 dB, 0.2150 and 0.9330 respectively. These values show that the proposed method shows promising result over the existing methods.

References

[1] Christian R., Dugelay J.L.,"A Survey of Watermarking Algorithms for Image Authentication", EURASIP Journal on Applied Signal Processing, 6,613-621, 2002.

[2] Jiang X., "Digital Watermarking and Its Application in Image Copyright Protection" International Conference on Intelligent Computation Technology and Automation, 2, 114 – 117, 2010.

[3] Singh V. "Digital Watermarking: A tutorial" In Cyber Journals: Multidisciplinary journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), 2, 10-21, 2011.

[4] Joshi K, Yadav R, Allwadhi S., "PSNR and MSE based investigation of LSB" IEEE Proceding on International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 280 - 285, 2016.

[5] Jia-Fa M., Xin-Xin N., Gang X., Wei-Guo, S., Na-Na, Z. "A steganalysis method in the DCT domain" Multimedia Tools and Applications, 75, 5999–6019, 2016.

[6] Karri S., Sur A., "Steganographic algorithm based on randomization of DCT kernel" Multimedia Tools and Applications, 74, 9207–9230, 2014.

[7] Chen P., Lin, H., "A DWT Based Approach for Image Steganography" 4, 275–290, 2006.

[8] Singh I., Khullar S , Laroiya S.C., "DFT Based Image Enhancement and Steganography" International Journal of Computer Science and Communication Engineering,2 ,2013

[9] Shalu Singh S., "Region Based Undetectable Multiple Image Watermarking Technique in DWT" IEEE Proceding on 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 141 - 144, 2016.

[10] Shalu Singh "A Robust Deinterlacing Multiple Image Watermarking Technique in DWT" IEEE Proceding on 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 8-13, 2016.

[11] Chen, P., & Lin, H. "A DWT Based Approach for Image Steganography", International Journal of Applied Science and Engineering, 4, 275–290, 2006.

[12] Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., Baik, S. W., "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image", Multimedia Tools and Applications, 1-27, 2015.

[13] Raval and PP Rege. (2003) "Discrete wavelet transform based multiple watermarking scheme", in the procedding of IEEE conference on convergent technologies for the Asia-Pacific Region. In tencon.vol.3, 2003, pp.935-938.

[14] Arya R.K., Singh S., Saharan R., "A secure Non-blind block based digital Image Watermarking technique usin DWT and DCT" In the Procedding of IEEE on Advances in computing communication and informatics (ICACCI), 2015 pp.2042-2048.

[15] Sridhar B., Arun C., "On secure multiple image watermarking technique using DWT", IEEE Third national conference on computing Communication & networking technologies (ICCENT), 1-4, 2012

[16] Durge A., Jaiswal A., "Increase Security of images from Attacks Using Watermarking Technique" In International Journal of Scientific & Engineering Research 3, 1-6, 2016.

[17] Sudhir K., Gopal M., "Dual watermarking based on multiple parameter fractional fourier transform and LSB technique" IEEE International Conference on Image information Processing, 1-5, 2011.

[18] Tao P. and Eskicioglu A.m., "A robust Multiple Watermarking Scheme Discrete wavelet transform Domain" Internet Multimedia management System, proceeding of SPIE, 133-144, 2004.

Authors' Profiles

Kamaldeep Joshi, he received the M.Tech degree in Computer Science and Engineering from Maharishi Dayanand University, Rohtak, and Haryana (INDIA). He is currently working as assistant professor in department of Computer Science and Engineering Department at University Institute of Engineering & Technology (M.D. University Rohtak, Haryana) India. His research interest includes Steganography, Watermarking, and Neural Network.

Rajkumar Yadav, he received the PhD degree in Computer Science and Engineering from Maharshi Dayanand University, Rohtak, and Haryana (INDIA) in 2011.He is currently working in Computer Science and Engineering Department at University Institute of Engineering & Technology (M.D. University Rohtak, Haryana) India. His research interest includes Information Hiding Techniques, Network Security and Biometrics.

How to cite this paper: Kamaldeep Joshi, Rajkumar Yadav,"A LL Subband Based Digital Watermarking in DWT", International Journal of Engineering and Manufacturing(IJEM), Vol.7, No.2, pp.50-63, 2017.DOI: 10.5815/ijem.2017.02.05