IJCSN International Journal of Computer Science and Network, Volume 4, Issue 6, December 2015
ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 0.417

FPGA Implementation of Image Steganography Using LSB and DWT

[1] Kalpana Shete, [2] Mangal Patil, [3] J. S. Morbale

[1,2,3] Dept. of Electronics, BVUCOE,
Pune, Maharashtra, India

Abstract - Steganography is one of the most influential techniques to mask the presence of concealed secret information inside a cover image. Image steganography is the important technique as digital image files are the most significant cover objects for steganography. Various algorithms and techniques such as LSB Replacement and Discrete Wavelet Transform are used for processing the secret data. Results are obtained in terms of PSNR, MSE and BER design metrics for proposed system. Intensive computations are required for embedding secret information inside images, and thus designing steganography in hardware speeds up steganography. The design when implemented with FPGA Spartan 3A kit provides a least processing time, which might give a faster, programmable & commercial hardware solution for secure communication. Proposed algorithms produces PSNR between 42-46 dB for LSB and 49-55 dB for DWT.

Keywords - *Image Steganography, Discrete Wavelet Transform, FPGA, Least Significant Bit.*

1. Introduction

The confidentiality of digital information should be maintained when being communicated precious data over the internet. In steganography, any embedding medium such as images, audio files, video files & text files can be used for hiding information. This work focuses on stenganography techniques for image files. The term steganography is defined as "covered writing" which obtained from the Greek words "Stegos" & "grafia" [1]. The steganography system contains basic three elements such as i) cover object, ii) the secret message and iii) the stego object [2]. A digital image is presented as a 2-D matrix of the color intensities at each grid point (i.e. Pixel). Generally, gray images require 8 bits, while colored images use 24 bits to describe the color model, i.e. RGB model [2, 3]. Normally concealing schemes for images are classified in: "Time and Frequency domain". The time domain embeds secret data in the least significant bit (LSB) of image pixel. The fundamental LSB technique is easy for execution but it is fragile against few attacks like low pass filtering and compression [4]. The frequency domain inserts the secret data in the frequency coefficients of images which minimizes the difficulties found in the time domain [5]. Steganalysis is the practice of sensing concealed information which is crested using steganography. Steganalysis finds stego- images by examining various image features between cover-image and stego-images [6].

Now a day, FPGA hardware is used for developing various steganography techniques. FPGA provides re-configurability, faster response as well as the robustness for the image processing [7, 8]. The rest of the paper is organized as - Section 2 describes literature review. Section 3 gives overview of image steganography. Proposed system is discussed in section 4 and section 5 shows evaluation analysis. At last, section 6 gives concluding remarks.

2. Literature Review

The image steganography technique is studied with various techniques in spatial domain and frequency domain. From these techniques, few methods are discussed here in the literature review:

P. Karthigaikumar [9] has developed new method for FPGA implementation of high speed and low area DWT based algorithm. The algorithm is implemented with Matlab and then with virtex-6 FPGA. The results obtained at maximum frequency of 344 MHz in Virtex-6 FPGA with device utility of only 1.1%.

Maya C. S. and Sabarinath [10] have proposed LSB replacement and DWT techniques to implement image steganography. The system is implemented with FPGA Spartan III kit with processing time of 13.79 ns.

FPGA implementation of LSB image steganography is presented by Bassam and Saed [1]. The results are drawn from the analysis of n-bit LSB which provides adequate values of PSNR, BER and MSE for 2 or 3 bit LSB. 2-bit LSB gives 44.1 dB PSNR while 3-bit LSB provides 37.9 dB PSNR for Baboon image.

Edgar Gomez-Hernandez, Claudia Feregrino-Uribe and Rene Cumplido [11] have developed the FPGA implementation of the ConText technique which gives improved results over Matlab implementation. The result depicted processing time difference between software and FPGA implementation. Software requires on an average 8.089 sec per image, whereas FPGA gives result within 0.0325 sec per image. Therefore, hardware runs 252 times faster over software.

With the literature review, various observations are drawn as mostly LSB and DWT techniques are employed for image steganography. From LSB method, 2 or 3- bit LSB serves adequate values for PSNR, MSE and BER. On the other hand, DWT technique is widely used due to its robustness, image quality and less processing time. Now-a-days, FPGA implementation provides excellent results than Matlab implementation in terms of processing time, power and area requirement.

3. Overview of Image Steganography

3.1 Spatial Domain Technique

Both embedding algorithms and a cover image form a stego-system [10]. Digital image have high capacity to store data and information because of its high redundancy. LSB based steganography provides the simplest way of embedding secret data into the LSBs of image pixel values.

For example, Consider the number 400 which has binary equivalent as $(110010000)_2$. After embedding these secret bits into the LSBs of cover image, the resultant pixel values are:

(0010 011**1** 1011 100**1** 0101 011**0**)
(1101 011**0** 1010 101**1** 1010 110**0**)
(1100 101**0** 01001100 00101100)
The bold bits are changed from their original value.

Also, the LSB steganography can be expanded using least n-bits to hide secret information. One can hide a large amount of information if the message to be hidden is compressed before embedding it. The resulting stego-image will look same as the cover image.

Several image metrics are used to compute the imperceptibility of the steganography. The metrics indicates the similarities or differences between the stego-image and cover image. The metrics used are:

- **Mean Square Error:** "Byte by byte comparison is performed on the cover image and stego-image to compute Mean Squared Error (MSE)" [1]. MSE is calculated as:

$$MSE = (1/M*N) \sum \sum (f_{ij} - g_{ij})^2 \quad (1)$$

where M, N are no. of rows and columns of cover image respectively, f_{ij} gives the pixel value of the cover image and g_{ij} gives the stego-image pixel value. Higher value of MSE shows deviation between cover and stego images.

- **Bit Error Rate:** "Bit error rate (BER) measures the actual number of bit position changes in the stego-image compared with the cover image" [1]. MSE and BER values should be as low as possible for good results.

- **Peak Signal-to-Noise Ratio:** "Peak signal-to-noise ratio (PSNR) computes the quality of the stego-image compared with the cover image". PSNR measured in decibels with the following equation:

$$PSNR\ (dB) = 10 \log_{10} (255^2 / MSE) \quad (2)$$

The higher PSNR better the quality. The acceptable PSNR value for images and video is noticed as between 30-60 dB [1].

3.2 Transform Domain Technique

The various transform domain techniques available such as:
1. Discrete Cosine Transform (DCT),
2. Discrete Wavelet Transform (DWT) and
3. Fast Fourier Transform (FFT)

These techniques are basically used to hide information in transform coefficients of the cover images which makes steganography system much more robust against attacks such as compression, filtering, etc [12, 13].

DWT is the mostly used compression technique in image steganography. At every decomposition level, the high

frequency and low frequency information is separated by the 1D-DWT method; thus at each level only two sub-signals are produced. 2D-DWT analysis must be used for images as images are represented by two dimensional signals that change spatially in horizontal and vertical directions. The same 'mother wavelets' as 1D-DWT is used for 2D-DWT analysis but with an extra step at each level of decomposition [14, 15]

The block diagram of 2D-DWT is shown in fig. 1demonstrates the image decomposition. Firstly, the original image of size M rows and N columns is horizontally filtered on rows with low pass and high pass filters. Thus two sub-images are produced with size M*N/2. Then, the outputs are filtered vertically to produce four sub-images of size M/2*N/2 [14].

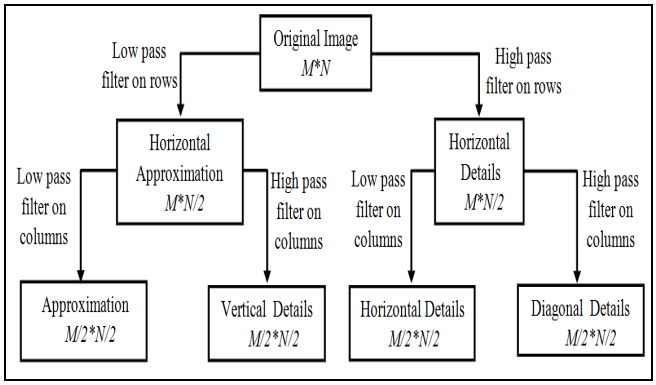

Fig. 1: Block diagram of level one 2D-DWT

3.3 Stego-System

The embedding algorithms and a cover image are combined to make the stego-system. The secret information is concealed in the cover image for transmitting it on the Internet securely [16]. The various embedding algorithms and techniques are used to form robust stego system. Thus embedding function develops the stego image from cover image and on the other hand extraction function performs reverse operation of retrieving secret information from stego image [17, 18]. Figure 2 shows the general block diagram of a stego system.

Detection of physical steganography is known as Steganalysis which requires careful physical examination. Steganalysis is the method of attacking steganography and it is achieved by applying various image processing techniques such as image filtering, cropping, rotating and translating [19, 20].

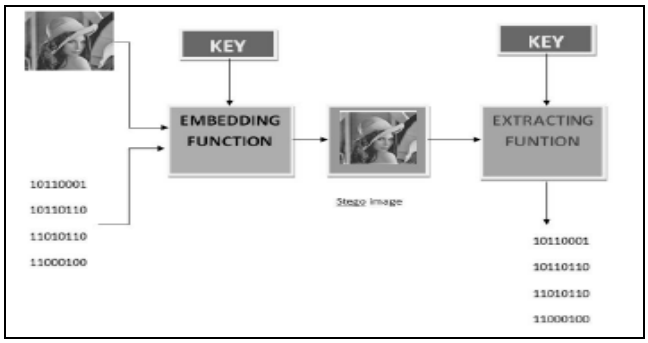

Figure 2: General Stego-system

4. Proposed System

Proposed system uses 2-bit LSB and 2 dimensional Haar DWT techniques for gray scale image steganography. 2-bit LSB algorithm is considered here as it gives desired values in terms of PSNR, MSE and BER for various image file formats e.g. .tif, .png, .bmp, etc.

In proposed paper, the image steganography technique is evaluated with 256*256 size gray scale image where each pixel is represented with 8 bits.

Using LSB technique, secret image data can be concealed into the least significant bits of the cover file. Thus, human eye can't be able to identify the hidden data in the cover image.

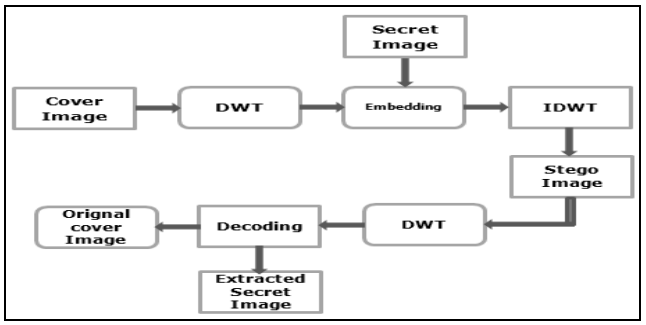

Figure 3: Block Schematic of Proposed System

With DWT, image steganography achieves improved security and robustness than LSB method. In the proposed system, 2 dimensional DWT provides better results over LSB technique in terms of PSNR, MSE, BER and processing time.

Block schematic of proposed system depicted in fig. 3 shows the embedding and extraction process of image steganography. Mainly DWT technique is employed for embedding and extracting process.

The proposed work is carried out with two techniques such as 2-bit LSB replacement and 2-D DWT with the help of Matlab and same using hardware FPGA. This system uses Spartan 3A kit to perform hardware implementation which gives faster response in terms of processing time than Matlab.

4.1 Image Steganography Embedding Process using DWT

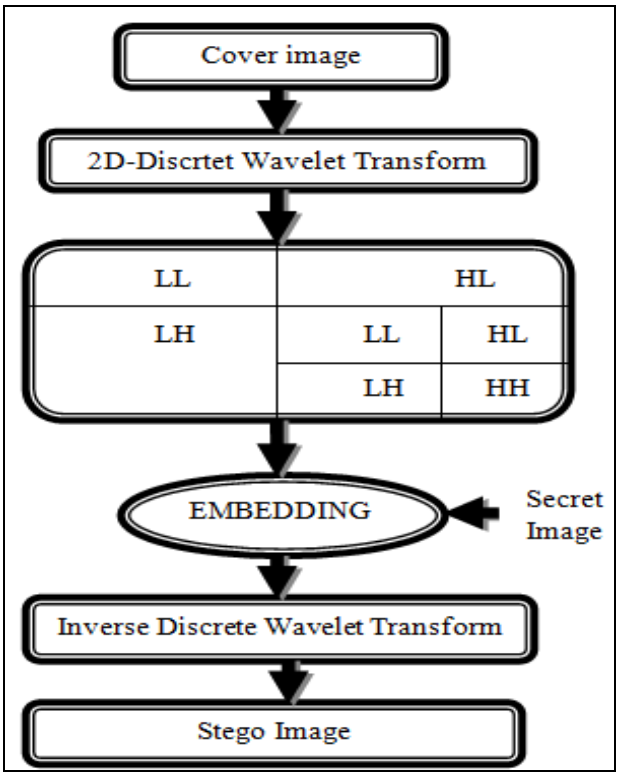

Figure 4: Flowchart of Steganography Embedding Technique using DWT

Embedding process of proposed mechanism is displayed with the help of flowchart as shown in fig. 4. DWT transformed cover image and secret image are embedded and then inverse DWT transformation is performed to get stego image. This stego image can be sent on Internet or network for transmission. At receiving side, extraction process with the use of DWT is implemented on received stego image to retrieve original secret and cover image as depicted in fig. 5.

4.2 Image Steganography Extraction Process using DWT

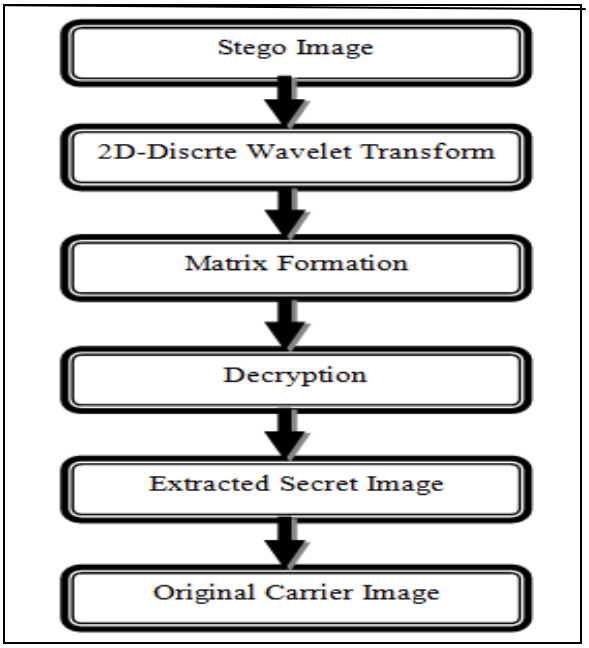

Figure 5: Flowchart of Image Steganography Extraction Technique using DWT

5. Evaluation Analysis

Evaluation analysis of the proposed work is derived for 2-bit LSB and discrete wavelet transforms on different images using Matlab 2013a.

5.1 Evaluation Results for LSB Method

Table 1 and 2 demonstrates the result of LSB and DWT respectively in terms of PSNR, MSE and BER design metrics. Results are evaluated with different cover and secret image formats.

Table 1: Result Table of 2-bit LSB

Cover Image	*Secret Image*	*PSNR (dB)*	*MSE*	*BER*
Coins.png (256*256)	Rice.png (256*256)	45.32	1.90	0.247
Hibiscus.tif (256*256)	Rice.png (256*256)	45.13	1.85	0.249
Testpat1.png (256*256)	Eight.png (256*256)	44.51	2.30	0.529
Cameraman.tif (256*256)	Goldfish.tif (256*256)	43.47	2.87	0.246
Hibiscus.tif (256*256)	Eight.tif (256*256)	43.05	3.02	0.245
Rice.png (256*256)	Hibiscus.tif (256*256)	42.91	2.18	0.248
Goldfish.tif (256*256)	Testpat1.png (256*256)	42.84	3.37	0.253

Figure 6 shows different images for LSB algorithm. Here, "Hibiscus.tif" image as carrier image and "Rice.png" image as secret image are used. LSB algorithm hides secret data into cover image and develops stego image looking same as cover image. So intruder can't get idea about secret data hidden into cover image. Finally, secret data is retrieved in the decoding process.

Figure 6: Cover, Secret and Stego Images for LSB Method

5.2 Evaluation Results for DWT Method

Table 2 gives improved DWT results over LSB results. DWT provides higher PSNR values and lower MSE, BER values and hence better visual image quality than LSB as shown in fig. 7.

Table 2: Result Table of 2D-DWT

Cover Image	*Secret Image*	*PSNR (dB)*	*MSE*	*BER*
Coins.png (256*256)	Rice.png (256*256)	54.61	0.226	0
Hibiscus.tif (256*256)	Rice.png (256*256)	54.23	0.226	0
Testpat1.png (256*256)	Eight.png (256*256)	49.91	0.673	0
Cameraman.tif (256*256)	Goldfish.tif (256*256)	50.53	0.579	0
Hibiscus.tif (256*256)	Eight.tif (256*256)	49.50	0.673	0
Rice.png (256*256)	Hibiscus.tif (256*256)	50.54	0.375	0
Goldfish.tif (256*256)	Testpat1.png (256*256)	49.59	0.693	0.003

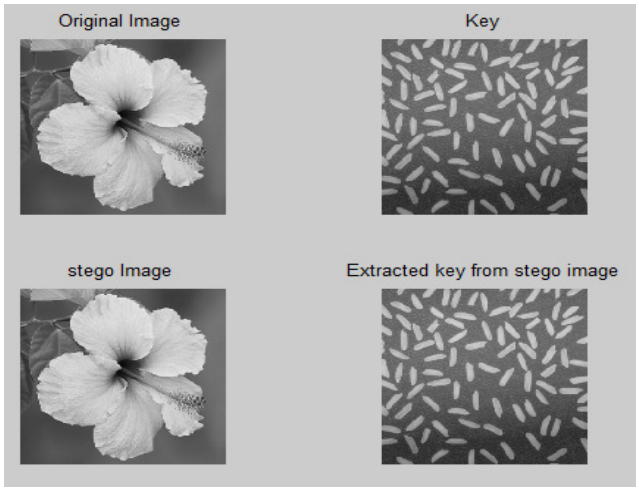

Figure 7: Cover, Secret and Stego Images for DWT Method

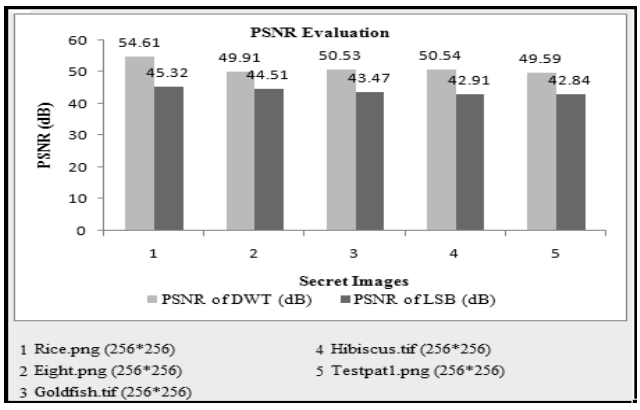

Figure 8: PSNR Characteristic for Different Images

Figure 8 and 9 depicts PSNR and MSE characteristics for DWT and LSB algorithms. DWT shows higher PSNR and less MSE for different secret images compared with LSB method.

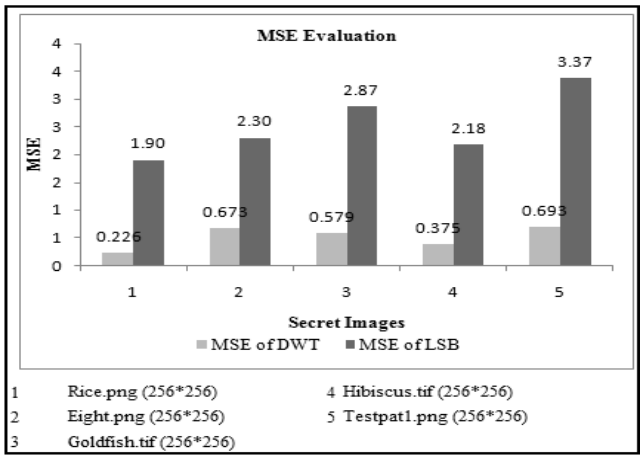

Figure 9: MSE Characteristic for Different Images

Table 3: Device Utilization Summary

Logic Utilization	*Used*	*Available*	*Utilization*
Number of Slices	42	704	5%
Number of Slice Flip Flops	64	1408	4%
Number of 4 input LUTs	64	1408	4%
Number of bonded IOBs	5	108	4%
No of GCLKs	2	24	8%

The Device utilization summary of proposed work is illustrated in Table 3. Proposed system makes use of Xilinx Spartan 3A device with target device 'XC3S50A' of target package as 'tq144' and target speed '4'.

6. Conclusion

In this paper the performance of image steganography is evaluated based on various metrics such as PSNR, MSE, BER and processing time. The proposed LSB replacement and DWT technique provides high PSNR and less MSE and BER values than previous methods. Proposed LSB algorithm produces PSNR in the range of 42-46 dB whereas DWT generates PSNR between 49-55dB. Spartan 3A development kit produces better performance in terms of processing time for same LSB and DWT algorithms. Future work should focus on hardware implementation based on various spatial and transform domain techniques to improve the robustness and image quality performance further, as well as minimizing the processing speed and power.

References

[1] Bassam Jamil Mohd, Saed Abed, Thaier Al-Hayajneh, Sahel Alounch, "FPGA Hardware of the LSB Steganography Method", IEEE Transaction on consumer Electronics, vol. 978, no. 1, 2012, PP. 4673-1550.

[2] Mrs. Manjula Y, Mr. Jagadeesha D.H, Dr. K.B ShivaKumar, "FPGA Implementation of Image Stenography Technique Using X-Box Mapping", International Journal of Computer & Organization Trends, Volume 3, Issue 6, June 2013.

[3] Deepa S. and Sarankumar S., "Implementation of Image Steganography Using FPGA", International Journal of Engineering Sciences and Research Technology, April 2014, pp. 5007-5011.

[4] K. N. Pansare and Dr. A. K. Kureshi, "A Review–FPGA Implementation of Different Steganographic Technique", International Journal of innovation Research in Science, Engineering and Technology, volume 3, special issue 4, April 2014.

[5] Shivakumar K.B., Khasim T., Raja K.B., Pattanaik S., "Dual Transform Technique for Robust Steganography", IEEE International Conference on Computational Intelligence and Communication Networks (CICN), 7-9 Oct. 2011, pp. 310 – 314.

[6] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", ELSEVIER, Signal Processing, 6th sept. 2009, pp. 727-752.

[7] Vasntha Lakshmi and B. Vidheya Raju, "FPGA Implementation of lifting DWT based LSB steganography using micro blaze processor", International journal of computer trends and technology (IJCTT), Volume 6, number 1, Dec 2013.

[8] Ankita Ganorkar and Sujata Agrawal, "Implementation of Steganography on FPGA", Ird India, Volume 2, Issue 1, January 2014.

[9] P. Karthigaikumar, Anumol, K. Baskaran, "FPGA Implementation of High Speed Low Area DWT Based Invisible Image Watermarking Algorithm", SciVerse ScienceDirect, Procedia Engineering, 30(2012), pp. 266-273.

[10] Maya C. S. and Sabarinath G., "An Optimized FPGA Implementation of LSB Replacement Steganography Using DWT", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, special issue 1, DEC 2013.

[11] Edgar Gomez-Hernandez, Claudia Feregrino-Uribe, Rene Cumplido, "FPGA Hardware Architecture of the Steganographic ConText Technique", IEEE Computer Society, 2008.

[12] Dr. Ahlam Fadhil Mahmood, Nada Abdul Kanai and Sana Sami Mohmmad, "An FPGA Implementation of Secured Steganography Communication system", Tikrit Journal of Engineering Science, vol. 19, No. 4, December 2012, pp. 14-23.

[13] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", third edition, ISBN 978-81-317-2695-2.

[14] Suhad Shakir Jaber, Hilal Adnan Fadhil, Zahereel I. Abdul Khalib and Rasim Azeez Kadhim, "Survey on Recent Digital Image Steganography Techniques", Journal of Theoretical and Applied Information Technology, Vol.66, No.3, 31st August 2014, pp. 714-728.

[15] Hala Farouk, Magdy Saeb, "Design and Implementation of Secret Key Stenographic Micro – Architecture Employing FPGA", 1530-1591/04, 2004 IEEE.

[16] Prabakaran G., Bhavani R., and Sankaran S., "Dual Wavelet Transform in Color Image Steganography Method", IEEE International Conference on Electronics and Communication Systems (ICECS), 13-14 Feb. 2014, pp. 1 – 6.

[17] Farahani M.R.D. and Pourmohammad A., "A DWT Based Perfect Secure and High Capacity Image Steganography Method", IEEE International conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), 16-18 Dec. 2013, pp. 314 – 317.

[18] Narasimmalou T. and Joseph R.A., "Discrete Wavelet Transform based steganography for transmitting images", IEEE International Conference on Advances in Engineering, Science and Management (ICAESM), 30-31 March 2012, pp. 370 – 375.

[19] Chandran S., Bhattacharyya K., "Performance analysis of LSB, DCT, and DWT for digital watermarking application using steganography", IEEE International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO), 24-25 Jan. 2015, pp. 1 – 5.

[20] Kamila S., Roy R., Changder S., "A DWT based steganography scheme with image block partitioning", IEEE 2nd International Conference on Signal Processing and Integrated Networks (SPIN), 19-20 Feb. 2015, pp. 471 – 476.