I.J. Image, Graphics and Signal Processing, **2016, 6, 48-56**
Published Online June 2016 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijigsp.2016.06.06

Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA

Kalpana Sanjay Shete
Dept. of Electronics BVUCOE Pune, India
Email: shete.kalpana4@gmail.com

Mangal Patil and J. S. Chitode
Dept. of Electronics BVUCOE Pune, India
Email: mvpatil@bvucoep.edu.in, j.chitode@gmail.com

Abstract—Steganography is the science that deals with conveying secret information by embedding into the cover object invisibly. In steganography, only the authorized party is aware of the existence of the hidden message to achieve secret communication. The image file is mostly used cover medium amongst various digital files such as image, text, audio and video. The proposed idea of this research work is to develop the robust image steganography. It is implemented using Least Significant Bit and Discrete Wavelet Transform techniques for digital image signal to improve the robustness & evaluate the performance of these algorithms. The parameters such as mean square error (MSE), bit error rate (BER), peak signal to noise ratio (PSNR) and processing time are considered here to evaluate the performance of the proposed work. In the proposed system, PSNR and MSE value ranges from 42 to 46 dB and 1.5 to 3.5 for LSB method respectively. For DWT method these results are further improved as it gives higher PSNR values between 49 to 57 dB and lower MSE values 0.2 to 0.7.

Index Terms—Discrete Wavelet Transform, Field Programmable Gate Array, Image Steganography, LSB Replacement, Security

I. Introduction

An ideal steganographic technique deals with concealing a large amount of information such that the modified object is visually seems to be exactly the original object [1]. Steganography basically came into existence from “Greek” and meaning that "protected writing", such that Steganos refers to “covered or protected” and graphei means “writing” [2]. Steganography uses various types of digital cover medium for concealing the secret information such as: Image, Video, Text, Audio and Protocol [3]. The digital files have redundant bits that can be changed without knowing the modification easily. The image file is mostly used cover medium because it has more redundant bits which can be replaced with secret information bits with minimum suspicion [4]. Also, images are commonly used through Internet in websites or an e-mail attached so it achieved the attention of developers. Therefore, this paper focuses on the image steganography approach using two primary groups as spatial domain and transform domain [5].

Steganography is used to achieve high capacity, robustness and security. As shown in fig. 1, three features represent a triangle in information hiding systems that are used to determine the system performance.

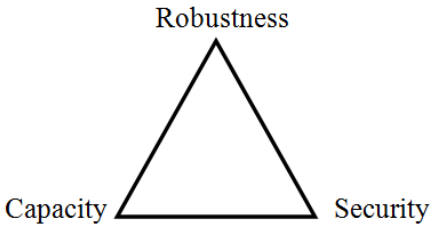


Fig.1.The Competing Factors in Hiding Information System

The recent image steganography techniques are [5]:

- Spatial (image) domain: LSB replacement, LSB matching, etc.
- Compressed domain based on vector quantization (VQ).
- Transform domain: DCT, DWT and FFT methods
- Spread spectrum.
- Statistical technique
- Distortion technique

In this approach we have implemented two techniques such as “LSB replacement” from spatial-domain and “DWT” from transform domain techniques. Hence it will balance secret data size and the imperceptibility of the system as well as it will provide strong secrecy.

Steganography provides best option in secure communications in cases where the use of cryptography can’t give proper solution or raises suspicion [6]. One of these applications is military and intelligence mediators which gives a high priority for saving a mediator’s life.

Additionally, steganography can be used for the protection of data modification, in companies for the safe circulation of secret data, and in accessing the control systems for digital content distribution [5, 7].

The rest of paper is arranged as follows– Section II explains related works regarding various steganography methods. Section III illustrates system overview of digital image steganography. Then section IV discusses proposed methodology and implementation results are shown in section V. At last, section VI gives concluding remarks.

II. Related Works

The review of the image steganography algorithms is carried out in time domain as well as in frequency domain. Among the large number of techniques, few techniques are reviewed in the literature:

Suhad Shakir Jaber, Hilal Adnan Fadhil, Zahereel I. Abdul Khalib and Rasim Azeez Kadhim[5] have presented survey on recent digital image steganography techniques. According to this paper, three approaches such as spatial domain, compressed domain based on VQ and transform domain are mostly used techniques in steganography. After comparing various methods author has observed that spatial domain has a simple implementation and high capacity with low robustness against signal processing techniques. Compressed domain based on VQ is more robust than the spatial domain but the hiding capacity is low. Transform domain based on DCT or DWT is the most robust among the others in that it has high resistance to signal processing techniques while the hiding capacity is low.

Maya C. S. and Sabarinath [8] intend to provide an overview of image steganography. In this research the secret data is embedded in gray image and image compression is done with DWT on hardware. By comparing the processing time of implementation on Matlab and Xilinx FPGA, it is remarked that hardware implementation gives much reduction in processing time than obtained with Matlab. The observed processing time is 0.446 sec on MATLAB while 13.79ns on FPGA. Thus this work reduced the operation time.

Bassam and Saed [9] have innovated LSB steganography using FPGA implementation. The proposed research has analyzed n-bit LSB. From the analysis, PSNR of 2-bit and 3-bit LSB are 44.1dB and 37.9dB for Baboon image respectively. For Baboon image, 2/3- LSB gives good performance i.e. 37.9dB which is between 2-bit and 3-bit LSB.

In paper [10], Elham Ghasemi has presented application of image steganography using wavelet domain and genetic algorithm. A genetic algorithm is used for embedding data in DWT coefficients of the cover image. After embedding message, an optimal pixel adjustment method is used. Author has employed wavelet transform for improving robustness of steganography. Simulation outcomes show that this scheme based on wavelet transform performed better in adaptive steganography system in terms of PSNR and capacity, 39.94 dB and 50% correspondingly.

Abbas Cheddad [11] has presented analysis on recent schemes of digital image steganography algorithm. The conclusion is that the new techniques such as adaptive steganography, DCT and DWT are strong against attacks. As these are the transform domain techniques in which coefficients are changed, so that image distortion is kept at minimum but transform domain methods have a lower payload than spatial domain.

Vasntha Lakshmi and B. Vidheya Raju [12] have presented the technique of FPGA implementation of lifting DWT based LSB steganography using micro blaze processor. Lifting based DWT split the image into ‘trends’ i.e. original signal and ‘details’ i.e. noise or high frequency data. The Haar lifting scheme is employed in this paper.

Ankita Ganorkar and Sujata Agrawal [13] have published the implementation of Steganography on FPGA using 2/3-LSB technique. 2/3-LSB system design offers good image quality and makes easy memory access. The result viewed that stego image gives better peak signal to noise ratio and less error results for LENA image in 2/3-LSB system.

The technique developed by Dr. Ahlam Fadhi Mohmmed [14] is more secure against attacks. Author has used adaptive LSB method and LFSR techniques in this paper. To preserve the statistical and visual features in cover images, the proposed method has embedded the secret message into the less sensitive regions adaptively according to sensitivity of the human visual system. According to results, the proposed reversible scheme provides a higher capacity of the performance of multilayer embedding and achieves better image quality for steganography images. Also the computational cost of the proposed scheme is less.

In the paper [15], Edgar Gomez-Hernandez has developed the ConText technique using FPGA architecture. This technique has drawn a better enhancement over Matlab realization. The result shows that the software implementation requires on an average 8.089 sec per image. On the other hand, the hardware architecture requires only 0.0325 sec per image. Thus, hardware solution gives timing efficiency.

K. N. Pansare and Dr. Kureshi [16] have presented some steganographic techniques which are proposed on FPGA. Mostly the image domain and wavelet transform methods are considered for analysis. It is observed that FPGA provides the best results in the case of image steganography. Furthermore with the help of appropriate hardware implementation the LSB domain could be developed for better performance.

Ravinder Reddy [17] has employed LSB method for encoding and decoding of image steganography. This paper has analyzed the various steganography algorithms such as spatial domain (LSB) and frequency domain and developed stenographic application for good security. It is shown that the message embedded into image provides negligible change in resolution and also the image is

protected with the personal password. Hence, secret data remained protected from unauthorized personnel.

Sujay Narayana [18] has proposed two novel ways for image steganography using cryptographic practices and type conversions. Combination of cryptography and steganography concept is introduced here. In this paper the image pixels (R,G,B) were encrypted using S-DES algorithm with 10 bit key and then converted to text i.e. cipher text. By using another steganographic approach this cipher text hide in another image. The proposed method achieved a higher similarity between the cover and stego image with better imperceptibility. The paper concluded that steganography when combined with encryption provides more security for secret communication.

From the literature evaluation, it is concluded that the LSB technique from spatial domain and various wavelet transforms from frequency domain are widely used. Thus 2 or 3 bit LSB technique provides better results in terms of BER, MSE and PSNR. Frequency domain steganography technique gives more robustness and security against spatial domain. Also it is observed that hardware implementation of steganography gives excellent performance over software implementation for any method [19, 20].

III. System Overview

The system overview covers the basic concept of digital image steganography along with LSB and DWT technique.

A. Digital Image Steganography

Concealing secret information in cover medium is the skill of hiding the presence of communication. Steganographic technique hides important messages inside of cover images such that the messages are invisible to a casual viewer [21]. The main objective of steganography is to achieve protection of data and high payload. Modifications to the cover medium may destroy hidden information as it is often fragile [22]. The general information hiding system for steganography is depicted in fig. 2.

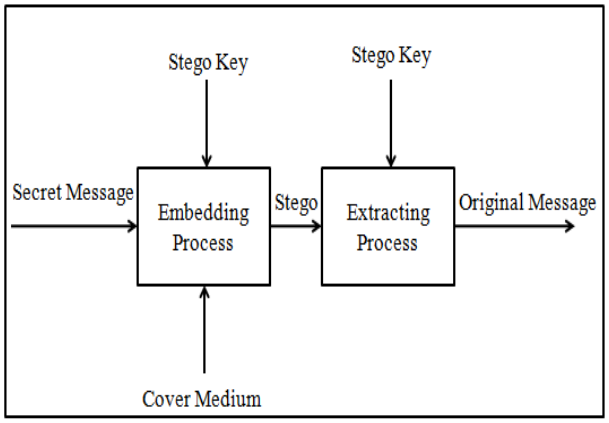


Fig.2. General Hiding Information System

B. Least Significant Bit Technique

Image or spatial domain system contain bit-wise methods which concern LSB insertion and noise manipulation. The spatial domain is based on embedding message in the least significant bit (LSB) of image pixel [23]. The basic LSB method is simple for implementation with high capacity. However there is possibility of detecting it by steganalysis easily. Both embedding algorithms and a cover image form a stego-system [8, 24]. Digital image have high capacity to store information. LSB algorithm is implemented in gray scale images to reduce the complexity of the system. In this research, the technique evaluated using 8-bitgray scale images of size 256*256 in which each pixel value is represented with 8 bit representation.

E.g. Consider the cover image has the following two pixel values:

(10101001 01011101 01110100)
(10111011 010011011100 0111)

Also, consider the secret bits are: $(101011)_2$.

The resultant pixel values by embedding the secret bits are:

(1010100**1**0101110**0**01110101)
(1011101**0**0100110**1**1100 011**1**)

The underlined bits are changed from its original value. On an average approximately half of the bits of cover image will change during embedding the secret message.

C. Performance Measures

The proposed system performs evaluation of results with design metrics such as MSE, PSNR and BER as shown below:

1) MEAN SQUARED ERROR (MSE):

It is calculated by comparing byte by byte performance of cover image and stego image. The MSE is calculated with the formula as below:

$$MSE = \frac{1}{M*N} \sum_{1}^{M} \sum_{1}^{N} (fij-gij)^2 \quad (1)$$

Where M = no. of rows and N = no. of columns in the cover matrix, f_{ij}= pixel value of the cover, and g_{ij}= pixel value of the stego-image. The value of MSE should be as small as possible because it indicates the dissimilarity between the cover and stego images [9].

2) PEAK SIGNAL TO NOISE RATIO (PSNR):

The quality of stego image compared with cover image is measured by Peak Signal to Noise Ratio (PSNR) in decibels. The higher value of PSNR gives the better image quality. The PSNR for an image is computed as follows:

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

It is observed that the human vision cannot identify any distortions in stego-images having PSNR beyond 36 dB for gray scale images [25]. Thus, appropriate PSNR value is between 30-60dB for images and video media.

3) BIT ERROR RATE (BER):

It measures the changes in actual number of bit positions of the stego image compared with cover image. BER also should be kept small. The error metrics such as MSE and BER increases with the increase in the value of least significant bit [9].

D. Discrete Wavelet Transform

The group of transform domain tools involves manipulation of algorithms and image transforms such as:

- Discrete wavelet transform (DWT),
- Discrete Cosine Transform (DCT)and
- Fast Fourier Transform (FFT).

The discrete wavelet transform is useful for compressing, transmitting as well as analyzing the images [26]. It is based on wavelets i.e. small waves which have short duration and variable frequency [27]. Discrete wavelet transform (DWT) performs excellent operation for image coding.

The discrete wavelet transform (DWT) is a multi-resolution analyzing tool with tremendous characteristics in the time as well as frequency domains [28]. With DWT, signals can be divided into different sub-bands with time and frequency information. This technique supports reliable coding efficiency and better image restoration quality compared with the traditional discrete cosine transforms [29]. Also, it gives a high compression ratio. Fig. 3 demonstrates "a one level decomposition using the two-dimensional DWT".

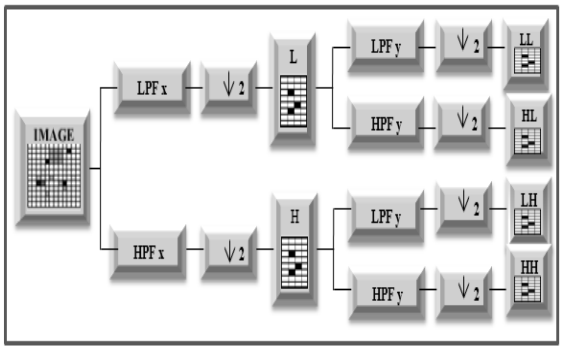


Fig.3. One-level decomposition using the Two - dimensional DWT

DWT separates component into four frequency bands given below:

LL –Horizontal and vertical low pass
LH – Horizontal low pass and vertical high pass
HL - Horizontal high pass and vertical low pass
HH - Horizontal and vertical high pass
The proposed work uses the Haar DWT.

E. Haar Discrete Wavelet Transform (HDWT)

Haar wavelet works on information with performing manipulations as sums and differences of neighboring components. The HDWT performs operation first on adjacent horizontal components and then takes into consideration the adjacent vertical elements. Haar wavelet transform has one excellent feature as the transform and its dual are same. Every transform determines the data energy of the top left hand corner. The Lena image after one HDWT is shown in fig. 4. The dimension of the block which holds the principal data is decreased by a factor of 4 after performing each transformation [10].

Fig.4. The Lena image after one Haar wavelet transforms

IV. Proposed Methodology

In proposed work, the embedding and extraction process on cover and secret image is achieved with LSB and DWT techniques. LSB algorithm is used to insert the bits of the secret image into the LSB of the cover image pixels. Proposed system uses 2-bit LSB technique which gives adequate results in terms of PSNR, MSE and BER. Thus the secret image bits are hidden into two-least significant bits of the cover image.

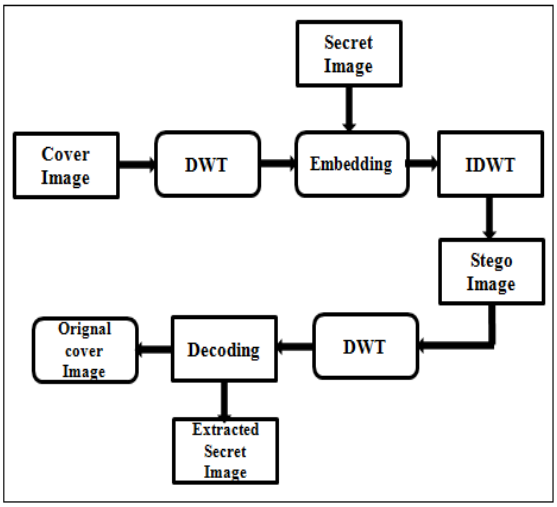


Fig.5. Block Diagram of Proposed System

In the DWT method, 2-dimensional Haar wavelet is used. It is observed that 2D-DWT gives better results than LSB and all other hiding methods. Embedding and extraction processes of LSB and DWT are performed on cover and secret images. Embedding process produces stego image whereas extraction process retrieves secret image back as shown in fig. 5.

A. Image Steganography Embedding Process Using DWT Method

DWT is applied to the original cover image so that it divides image into four sub-bands. It follows by encryption process using secret image. Then secret image is embedded into processed cover image. Finally inverse 2D-DWT is performed on this embedded output to get stego-image.

Embedding process for proposed scheme using DWT is as follows:

Step 1: Read the cover image to hide the secret message and resize it.

Step 2: Read the secret image for hiding into cover image and also resize it. Then compute 2D-wavelet transform of cover image. This operation produces four sub-bands as LL, LH, HL and HH respectively.

Step 3: Select LL sub-band for embedding process and encryption is performed using formula:

$$\boldsymbol{Y = y + c * key} \quad (3)$$

Where **Y** = Encrypted value, **y** = DWT matrix of cover image, **c** = weight of steganography and **key** = secret image.

Step 4: Embed the secret image into processed cover image.

Step 5: Perform inverse discrete wavelet transform to get stego image. Thus, in embedding process 'stego-image' is produced.

B. Image Steganography Extraction Process Using DWT Method

The stego image is then processed to extract the original secret image and cover image. 2D-Discrete wavelet transformation is performed to form the matrix. Then decryption is performed to extract the secret and original carrier image.

Extraction process for proposed scheme is as follows:

Step 1: Compute 2D-DWT of stego image to generate the matrix for retrieving the secret image back.

Step 2: Perform the decryption process using following formula,

$$N1 = n1 - y \quad (4)$$

Where $\mathbf{N_1}$= Decrypted value, $\mathbf{n_1}$= DWT matrix of stego image and **y** = DWT matrix of cover image. Thus, original secret and cover image is retrieved back from stego image.

This paper introduces the implementation of LSB steganographic technique and discrete wavelet transform with Matlab as well as FPGA.

The proposed system performs hardware implementation of image steganography using "Spartan 3A" kit. FPGA kit receives cover and secret images using GUI through USB to serial converter. It performs operation on it and displays results back on Matlab GUI window. Thus, FPGA provides better results than Matlab in terms of processing time and quality of image.

V. Implementation Results

Various results for LSB and DWT algorithms are evaluated with different cover and secret images. This section gives MATLAB and FPGA results in terms of different design metrics.

A. Implementation Results for LSB method

Table 1 shows the various design metrics for n-bit LSB. It shows that the PSNR value decreases if more number of least significant bits is used to hide secret information. Hence it is concluded that maximum up to 2 or 3 bits gives optimum results for data hiding.

Table 1. n-bit LSB Results

n-bit LSB	Cover Image	Secret Image	PSNR (dB)	MSE	BER (%)	Elapsed Time
1-bit	Cameraman.ti (256*256)	Rice.png (256*256)	51.07	0.5	0.49	11.71
2-bit	Cameraman.ti (256*256)	Rice.png (256*256)	45.38	1.85	0.25	11.69
3-bit	Cameraman.ti (256*256)	Rice.png (256*256)	38.47	9.09	0.12	11.66
4-bit	Cameraman.ti (256*256)	Rice.png (256*256)	32.28	38.13	0.06	11.60
5-bit	Cameraman.ti (256*256)	Rice.png (256*256)	26.32	150.34	0.03	11.55
6-bit	Cameraman.ti (256*256)	Rice.png (256*256)	20.16	621.54	0.015	11.68
7-bit	Cameraman.ti (256*256)	Rice.png (256*256)	13.42	2933.7	0.0077	11.55
8-bit	Cameraman.ti (256*256)	Rice.png (256*256)	8.36	9408.6	0.004	11.65

It is seen that visual quality of stego image varies with hiding secret image within different bit planes of cover image. Here, PSNR and hence image quality of "Cameraman.tif" stego image started degrading from 4th bit plane onwards as visualize in fig. 6.

1-bit 2-bit

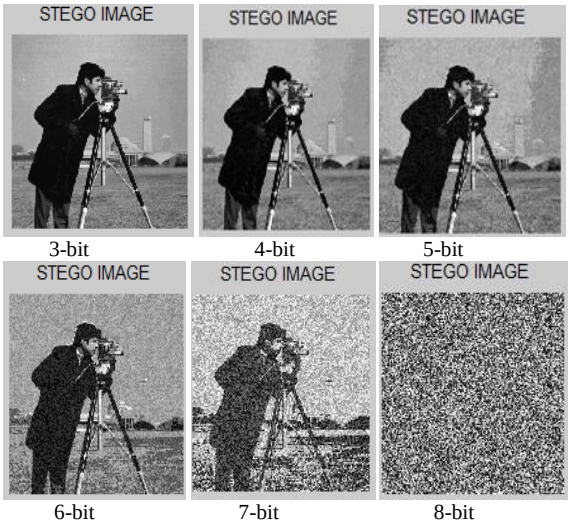


Fig.6. Variations in Stego Images for Different Bit Planes

Table 2 gives the results for various images of different formats e.g. .tif, .png etc. The parameters such as PSNR, MSE and BER vary for different images.

Table 2. 2-bit LSB Results for Different Images

Cover image	Secret Image	PSNR (dB)	MSE	BER (%)	Elapsed Time (Sec)
Testpat1.png (256*256)	Rice.png (256*256)	43.50	2.9	0.08	8.74
Cameraman.tif (256*256)	Rice.png (256*256)	45.40	1.8	0.25	8.87
Testpat1.png (256*256)	Cameraman.tif (256*256)	42.90	3.2	0.12	8.64
Cameraman.tif (256*256)	Hibiscus.tif (256*256)	44.80	2.1	0.24	8.68
Hibiscus.tif (256*256)	Goldfish.tif (256*256)	43.24	2.8	0.24	8.26
Cameraman.tif (256*256)	Eight.tif (256*256)	43.45	3.0	0.24	8.81
Hibiscus.tif (256*256)	Testpat1.png (256*256)	42.57	3.3	0.24	8.54

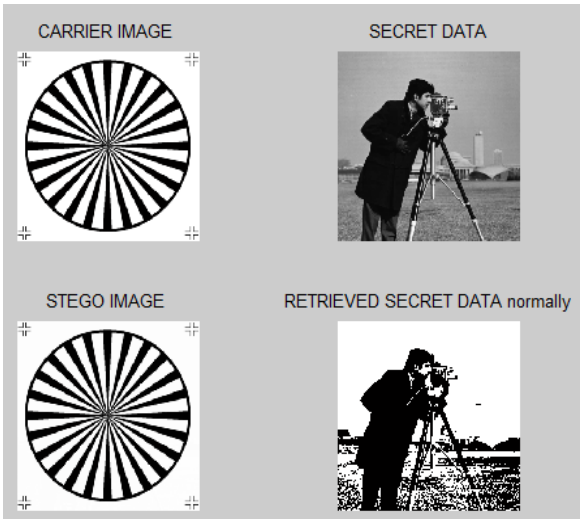


Fig.7. Carrier and Stego Images Using LSB Method for "Testpat1.png" as carrier image and "Cameraman.tif" as secret image

In fig. 7, the various images such as carrier and secret images are shown. Here, secret data is hidden into cover image to form stego image. At destination, this stego image is received and decoded to get secret data.

B. Implementation Results for DWT Method

DWT provides better results over LSB substitution method which is shown in table 3. DWT gives higher PSNR and less MSE values with good image quality than LSB method.

Table 3. DWT Results for Different Images

Cover image	Secret Image	PSNR (dB)	MSE	BER (%)	Elapsed Time (Sec)
Testpat1.png (256*256)	Rice.png (256*256)	54.63	0.226	0	0.79
Cameraman.tif (256*256)	Rice.png (256*256)	54.60	0.226	0	0.79
Testpat1.png (256*256)	Cameraman.tif (256*256)	53.61	0.286	0	0.78
Cameraman.tif (256*256)	Hibiscus.tif (256*256)	52.43	0.375	0	0.78
Hibiscus.tif (256*256)	Goldfish.tif (256*256)	50.15	0.579	0	0.79
Cameraman.tif (256*256)	Eight.tif (256*256)	49.90	0.673	0	0.77
Hibiscus.tif (256*256)	Testpat1.png (256*256)	49.37	0.693	0.004	0.76

Fig. 8 depicts the better stego and retrieved image quality using DWT over LSB technique.

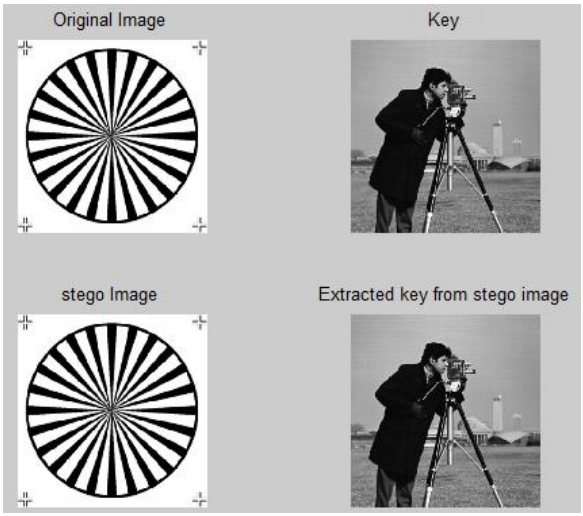
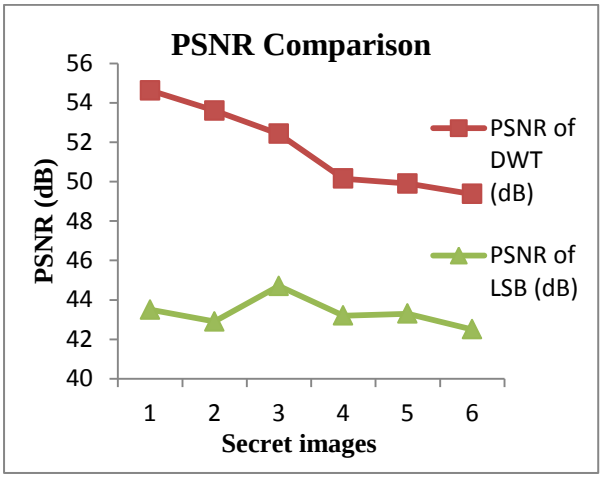


Fig.8. Carrier and Stego Images Using DWT Method for "Testpat1.png" as carrier image and "Cameraman.tif" as secret image

C. Performance Analysis of PSNR and MSE for LSB and DWT Methods

Performance analysis of PSNR with different secret images is done by comparing PSNR values of DWT and LSB methods as shown in fig. 9. DWT shows better PSNR performance than LSB algorithm.

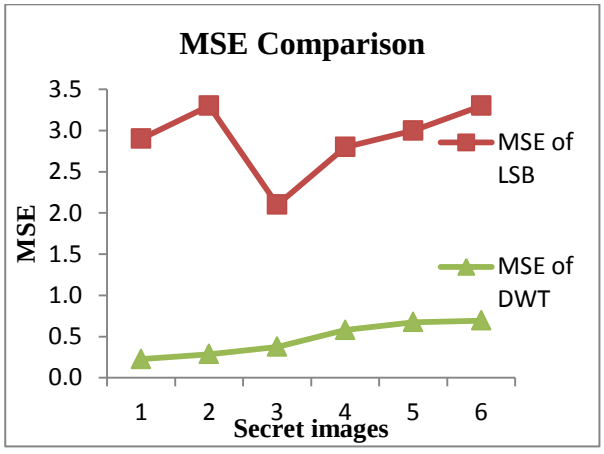


Note: X- Axis numbers represents secret images as below.

1	Rice.png	4	Goldfish.tif
2	Cameraman.tif	5	Eight.tif
3	Hibiscus.tif	6	Testpat1.png

Fig.9. Performance Analysis of PSNR for Different Secret Images

Fig. 10 does the performance analysis of MSE for DWT and LSB. This comparison shows less MSE values for DWT algorithm than LSB. Hence DWT is preferred over LSB method for several design metrics such as PSNR, MSE, image quality and processing time.



Note: X- Axis numbers represents secret images as below.

1	Rice.png	4	Goldfish.tif
2	Cameraman.tif	5	Eight.tif
3	Hibiscus.tif	6	Testpat1.png

Fig.10. Performance Analysis of MSE for Different Secret Images

Fig. 11 shows GUI window for FPGA results. Cover image and Secret image from MATLAB is given to FPGA Spartan 3 kit using GUI through USB to serial converter. Then converted images in the hardware are received back in the MATLAB GUI window.

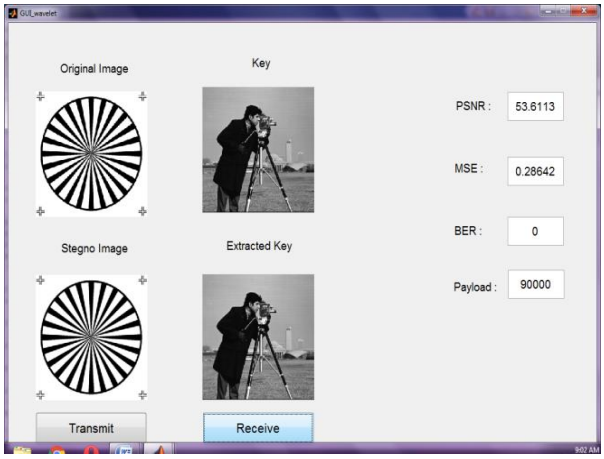


Fig.11. GUI window of FPGA result

Table 4. FPGA 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%

Table 4 depicts the device utilization summary of proposed system. Proposed system uses Xilinx Spartan 3A device:

Target Device: XC3S50A
Target Package: tq144
Target Speed: -4

- Timing Summary:
- Minimum period: 5.442ns (Maximum Frequency: 183.756MHz)
- Minimum input arrival time before clock: 2.853ns
- Maximum output required time after clock: 5.642ns

Table 5 shows the comparison of device utilization by different target FPGA device. Proposed Spartan device has done appropriate utilization of available logic.

Table 5. Comparison of FPGA Device Utilization for Different Xilinx Spartan Devices

Logic Utilization	**Used**			**Available**			**Utilization**		
FPGA Devices	**Xilinx Spartan - 2 Device**	**Xilinx Spartan - 3A Device**	**Proposed Xilinx Spartan 3A Device**	**Xilinx Spartan - 2 Device**	**Xilinx Spartan - 3A Device**	**Proposed Xilinx Spartan 3A Device**	**Xilinx Spartan - 2 Device**	**Xilinx Spartan - 3A Device**	**Proposed Xilinx Spartan 3A Device**
Number of Slices	1195	22	42	1200	23872	704	99%	0%	5%
Number of Slice Flip Flops	N/A	42	64	N/A	47744	1408	N/A	0%	4%
Number of 4 input LUTs	N/A	35	64	N/A	47744	1408	N/A	0%	4%
Number of bonded IOBs	43	30	5	92	469	108	46%	6%	4%
No of GCLKs	2	2	2	4	24	24	50%	8%	8%

VI. Conclusion

This paper performs operation of hiding secret image into 8-bit gray scale cover image using Least Significant Bit and Discrete Wavelet Transform. From results it is observed that DWT technique provides improved PSNR, MSE, BER and quality of image with minimum processing time than LSB. In the proposed system, PSNR value ranges from 42-46 dB for LSB method and for DWT it gives higher values between 49-57 dB. Thus, proposed mechanism provides average PSNR of 44 dB using LSB technique and 52 dB using DWT method. In addition, hardware implementation of same method using "Spartan 3A" kit provides better results than Matlab results in terms of processing time. Proposed FPGA design requires 5.4 ns for implementation whereas Matlab performs operation within 0.7-8 sec.

Future work can be performed with FPGA implementation on color image and can be extended to video processing also.

Acknowledgment

This paper is fully supported by the Bharati Vidyapeeth University College of Engineering, Pune, India.

References

[1] Manoj Gowtham G.V, Senthur T, Sivasankaran M, Vikram M4 and Bharatha Sreeja G, "AES based steganography", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 1, pp. 382-389, January 2013.

[2] Mrs. Manjula Y, Mr. Jagadeesha D.H, Dr. K.B Shiva Kumar, "FPGA Implementation of Image Stenography Technique Using X-Box Mapping, "International Journal of Computer & Organization Trends – ISSN:2249-2593, Volume 3, Issue 6, June 2013.

[3] Prabakaran G., "A modified secure digital image steganography based on Discrete Wavelet Transform", IEEE International Conference on Computing, Electronics and Electrical Technologies (ICCEET), ISBN: 978-1-4673-0211-1, pp. 1096 – 1100, 21-22 March 2012.

[4] Narasimmalou T., Joseph R.A., "Discrete Wavelet Transform based steganography for transmitting images", IEEE International Conference on Advances in Engineering, Science and Management (ICAESM), ISBN: 978-1-4673-0213-5, pp. 370 – 375, 30-31 March 2012.

[5] 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, pp. 714-728, 31st August 2014.

[6] Prabakaran G.,Bhavani R., Sankaran S., "Dual Wavelet Transform in Color Image Steganography Method", IEEE International Conference on Electronics and Communication Systems (ICECS), ISBN: 978-1-4799-2321-2, pp. 1 – 6, 13-14 Feb. 2014.

[7] 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), ISBN: 978-1-4799-7676-8, pp. 1 – 5, 24-25 Jan. 2015.

[8] Maya C S, 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.

[9] Bassam Jamil Mohd, Saed Abed, Thaier Al-Hayajneh, Sahel Alounch, "FPGA Hardware of the LSB Steganography Method", IEEE Transaction on consumer Electronics, 978-1-4673-1550-0/12 © 2014 IEEE.

[10] Elham Ghasemi, Jamshid Shanbehzadeh, NimaFassihi, "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", IMECS 2011, March 16-18, 2011.

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

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

[13] Ankita Ganorkar, Sujata Agrawal, "Implementation of Steganography on FPGA", Ird India, ISSN (Online):2347-2812, Volume-2, Issue-1, January -2014.

[14] 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, pp. 14-23, December 2012.
[15] Edgar Gomez-Hernandez, Claudia Feregrino-Uribe, Rene Cumplido, FPGA Hardware Architecture of the Steganographic ConText Technique", IEEE Computer Society, 0-7695-3120-2/08 © 2008 IEEE.
[16] K.N. Pansare, Dr. A.K. Kureshi, "A Review–FPGA Implementation of Different Steganographic Technique", International Journal of innovation Research in Science, Engineering and Technology, ISSN (print):2347-6710, volume 3, special issue 4, April 2014.
[17] Ravinder Reddy Ch, Roja Ramani A, "The Process of Encoding and Decoding of Image Steganography using LSB Algorithm", IJCSET, Vol. 2, Issue 11, pp.1488-1492, November 2012.
[18] Sujay Narayana, Gaurav Prasad, "Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions", Signal & Image Processing: An International Journal (SIPIJ) Vol.1, No.2, pp.60-73, December 2010.
[19] Hala Farouk, MagdySaeb, "Design and Implementation of Secret Key Stenographic Micro – Architecture Employing FPGA" 1530-1591/04, 2004 IEEE.
[20] P Karthigaikumar, Anumol, K Baskaran, "FPGA Implementation of High Speed Low Area DWT Based Invisible Image Watermarking Algorithm", Sci-Verse Science-Direct, Procedia Engineering pp. 266-273, 2012.
[21] 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), ISBN: 978-1-4799-5990-7, pp. 471 – 476, 19-20 Feb. 2015.
[22] NielsProvos, Peter Honeyman, "Detecting Steganographic Content on the Internet", Center for Information Technology Integration.
[23] 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), ISBN: 978-1-4577-2033-8, pp. 310 – 314, 7-9 Oct. 2011.
[24] Deepa S, Sarankumar S, "Implementation of Image Steganography Using FPGA", International Journal of Engineering Sciences and Research Technology, pp. 5007-5011, April, 2014.
[25] Sushil Kumar, S.K. Muttoo, "A Comparative Study of Image Steganography in Wavelet Domain", IJCSMC, Vol. 2, Issue 2, pp. 91- 101, February 2013.
[26] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", third edition, ISBN 978-81-317-2695-2, pp. 484-542.
[27] Farahani M.R.D, 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), ISBN:978-1-4799-2418-9, pp. 314 – 317, 16-18 Dec. 2013.
[28] N. Ajeeshvali, B.Rajasekhar, "Steganography Based on Integer Wavelet Transform and Bicubic Interpolation", International Journal of Image, Graphics and Signal Processing, pp. 26-33, November 2012.
[29] Jyoti, Md. Sabir, "Genetic Algorithm Based Image Steganography for Enhancement of Concealing Capacity and Security", International Journal of Image, Graphics and Signal Processing, pp. 18-25, June 2013.

Authors' Profiles

Kalpana Shete has received B.E. degree in Electronics and Telecommunication from Pune University, Maharashtra, India in 2011. Now she is pursuing M-Tech Electronics (VLSI) from Bharati Vidyapeeth University College of Engineering, Pune, India. Her research interests include multimedia, digital image processing and VLSI design.

M. V. Patil has obtained the B.E degree in Electronics Engineering from Shivaji University, Kolhapur, Maharashtra, India in 1999. She received M.E. degree from the Bharati Vidyapeeth Deemed University College of Engineering at Bharati Vidyapeeth Deemed University, India in 2006. Currently pursuing Ph.D. (Electronics Engg.) from Bharati Vidyapeeth Deemed University College of Engineering, Pune.

She has more than 12 years of teachingexperience. She has been serving as a faculty member in the Department of Electronics Engineering at Bharati Vidyapeeth Deemed University College of Engineering, Pune.

Dr. J. S. Chitode is a professor received the B.E. degreein Industrial Electronics Engineering from Bharati Vidyapeeth University, Pune, Maharashtra, india in 1991. He received M.E. degree from College of Engineering (COEP), Pune at University of Pune from Maharashtra, India in 1995. He has received Ph.D. degree in Electronics from Bharati Vidyapeeth Deemed University, India in 2009.

Currently he is a professor in the Bharati Vidyapeeth Deemed University College of Engineering, Pune (India). His research interest includes Signal processing, Speech Synthesis, Digital Communication, etc.

Dr. Chitode is actively participating as a member of different professional research societies, like IEEE, ISTE, etc.

How to cite this paper: Kalpana Sanjay Shete, Mangal Patil, J. S. Chitode,"Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA", International Journal of Image, Graphics and Signal Processing(IJIGSP), Vol.8, No.6, pp.48-56, 2016.DOI: 10.5815/ijigsp.2016.06.06

