Vandana Publications
IJEMR

Volume-8, Issue-3, June 2018
International Journal of Engineering and Management Research
Page Number: 112-119
DOI: doi.org/10.31033/ijemr.8.3.14

Design and Implementation of Lifting Based Wavelet and Adaptive LSB Steganography to Secret Data Sharing Through Image on FPGA

Kokila. B. Padeppagol[1] and Sandhya Rani M H[2]
[1]M. Tech in VLSI Design and Embedded Systems, Department of ECE, Sapthagiri College of Engineering, Bengaluru, INDIA
[2]Associate Professor & HOD, Department of ECE, Sapthagiri College of Engineering, Bengaluru, INDIA

[1]Corresponding Author: kokilabp9@gmail.com

ABSTRACT

Image steganography is an art of hiding images secretly within another image. There are several ways of performing image steganography; one among them is the spatial approach. The most popular spatial domain approach of image steganography is the Least Significant Bit (LSB) method, which hides the secret image pixel information in the LSB of the cover image pixel information. In this paper a LSB based steganography approach is used to design hardware architecture for the Image steganography. The Discrete Wavelet Transform (DWT) is used here to transform the cover image into higher and lower wavelet coefficients and use these coefficients in hiding the secret image. the design also includes encryption of secret image data, to provide a higher level of security to the secret image. The steganography system involving the stegno module and a decode module is designed here. The design was simulated, synthesized and implemented on Artix -7 FPGA. The operation hiding and retrieving images was successfully verified through simulations.

Keywords--- LSB, Image Steganography, DWT, Encryption and Decryption, Artix-7 FPGA

I. INTRODUCTION

Now a day, most of the data information is shared over the internet in the form of text and the media content. The internet is an open and wide channel for the communication process and the data transfer through these channels can be attacked by some stealing threat that perform unauthorized accessing action over the data to steal the information by unknown source. So, confidentiality of these digital data information should be preserve by adopting some security actions that protect the digital data from getting stolen by unauthorized user. There are some security approaches that include cryptography, watermarking and steganographic concept which secures data in such way that the original content of data cannot be noticed to third party [1]. Cryptography is concept of encryption and decryption that perform on digital image by using secrete key to secure communication with following property privacy Confidentiality, key exchange authentication and non-repudiation. Encryption is a technique that transforms plain data into encoded form (cipher text) and decryption is a technique that is used to get original data back from the encoded content [2]. Another approach for securing digital data is Watermarking technique which is the process of embedding some other content into original content of data. Watermarking technique can be used for many purposes like to hide data content, source tracking, Broadcast tracking and copyright protection. [3]

Steganography technique is an art of hiding data information in such way that original data is covered by other media such as text, image, audio or video from the and by this way it prevents from third party user.

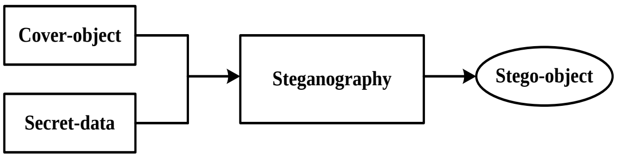


Fig.1. Steganography concept

The above figure1.1 represents the general process of Steganography technique where cover-object and Secrete-data are uses to generate stegno-object.

Image Steganography concept is mainly categorized into following techniques that are based on spatial-domain and frequency-domain. In spatial method data is hidden by modifying spatial characteristics of image and the hidden data is in the form of image pixel values. The spatial-domain consists two different methods for hiding image data that are Least Significant Bit technique (LSB) and Pixel Value Differencing technique (PVD). In frequency-domain technique both the secret message and carrier data are transformed into the frequency domain by using different transformation technique such as Discrete Fourier Transform (DFT), Discrete Wavelet Transform (DWT), Discrete Cosine

Transform (DCT) for integrating the information into image. At the decryption process the domain transformation is need to extract the original content from hidden data [4][5]. The FPGA hardware is widely used for designing various steganographic techniques because FPGA provides re-configuration feature and as well as the faster and robustness application for the image processing.

In this paper a novel design for secret image data sharing by using Adaptive LSB steganography is proposed. A DWT using lifting method is used for Image transformation and similarly, IDWT an inverse process that is used at time of decryption process to recover the original image. The proposed model is simulated and implemented on the FPGA and lastly the presented model is compared with existing models. The rest of the paper is organized as- Section-2 provides brief review of existing techniques. Section-3 presents the system design; Section-4 presents implementation operation of proposed method along with all details, Simulation results and performance analysis is present in the Section-5 and finally, Section-6 reveals the conclusion and the future work.

II. REVIEW OF LITERATURE

The work carried out by Dahiya et al. [6] have concentrated on the issue of multiplier fabrication on the chip and presented a novel multiplier-less architecture for DWT with using parallel flipping and shift adder technique that reduces problem of critical path and provides efficient implementation design and high-speed processing feature. The outcome of study shows that the presented approach achieves better performance in image and video compression.

In the study of Rao et al. [7] have studied the effect of image compression based on Haar wavelet and DSP and found the increased processing speed of image compression on digital processor when compared to general processor. The outcome of the study delivers it can be efficiently applicable on many image applications that require high transmission processing such as satellite images, HDTVs, medical images etc.

Lin et al. [8] have constructed a cell-based model for that based on the Haar DWT to mitigate the problem of imitated light-field image. The experimental result of this study achieves an efficient performance in reconstructing the blurry images with optimal bandwidth.

The work of Al-Afandy et al. [9] have offered a secure framework for data hiding by using LSB technique and cropping image steganography to enhance the security of image data information. The experimental outcomes of presented approach obtain optimal PSNR and CPU time range that is sufficient to provide more security.

The work of Sugathan [10] has tried to improve the quality features of Stego images by using LSB replacement algorithm. The outcome of presented approach achieves an improved image which is evaluated by PSNR and MSE.

The work of Juarez-Sandoval et al. [11] have studied some artifacts generated by the LSB matching steganography and presented a steganalysis algorithm to obtain compact feature vector.

Karthikeyan et al. [12] have focused on the data security management and presents an innovative concept by using data encryption algorithm. The objective of author is to provide better security while the data is transferring over the open communication channel.

Similarly, another approach for securing image data information is given by the Abood [13] in which a hybrid method of cryptography and Steganography is applied to improve the security for end-to-end data information.

In the same way another approach is proposed by the Singh and Singh [14] that have discussed various steganography techniques to provide strong security to digital data which is shared over the internet channel.

III. SYSTEM BACKGROUND

In system domain, described different methods which is used in Steganography Hardware (SH) model. The fundamentals of the Least Significant Bit (LSB) methodology of steganography, the lifting approach and the chaotic scheme for cryptography is described.

(A) LSB Techniques

In image pixel LSB is the smallest bit in the byte value. The LSB method changes some specific or more bits in a cover picture. For a 24-bit picture, 3 bits may be embedded and while in 8-bit picture one bit of secure message is secreted. The binary representation of 135 decimal number, with the LSB tinted in below [1].

1	0	0	0	0	1	1	1

Fig.2. LSB technique

(B) LSB Insertion Method

The LSB technique of embedding secure message is executed with the procedure which is shown in the figure 1. First of all, the embedded secret message is changed into binary. Then the changed message along with cover image file and stego key is proceed to the LSB encoder to achieve the stego picture as the result.

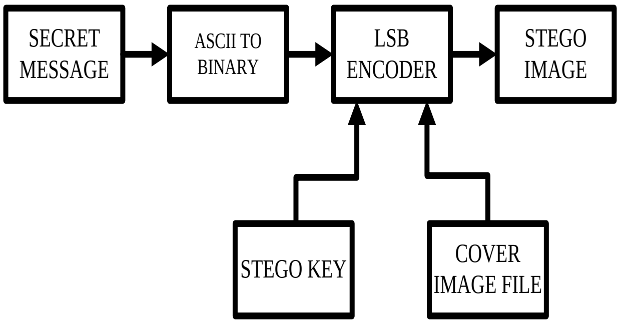


Fig.3. Procedure for stego image through LSB encoder 15]

(C) Data embedding process

In data embedding system some input is taking which is stego key, secret text and cover picture. To start with the pixels of cover picture are extracted and after that from secret text the characters are also extracted. Then from stego key characters are extracted. After these processes choosing the initial pixel and also chose the characters from stego key and place in the initial component of pixel. Next, show through end of key by insertion a terminating symbol. Thereafter attach the text character in first component of upcoming pixels by exchanging it and it is in continue until the all characters are embedded. Then insert a terminating symbol for indication of text data end. And finally acquired stego picture.

(D) Data Extraction from Stego Image

Figure 2 shows the secure data extraction by using an LSB decoder. The LSB decoder uses stego key and stego image as an input and extracts the secure data from the stego picture.

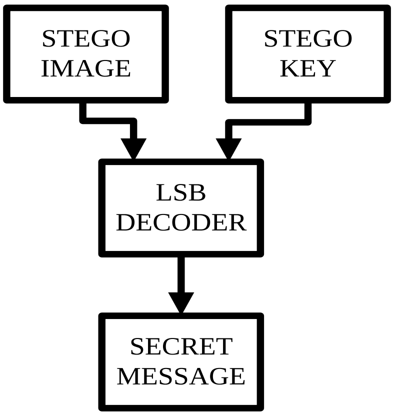


Fig.4. Data extraction using LSB decoder [1]

(E) Data Extraction Process

In data extraction procedure first of all the stego image pixels are extracted, after that start from initial pixels and extracted stego key symbols from starting component of the pixels. If the key which is entered by the receiver is correspond to the extracted key, then after move to the next stage otherwise the program is terminated. In next step the accurate key move to the next pixels and extract the secure message characters from starting component of next pixels. At last the secure message is extracted from these whole processes.

(F) Lifting Approach based on Discrete Wavelet Transform (DWT)

To implementation of DWT using lifting approach. It is an effective way to achieve multi-stage signal decomposition. The lifting method finds out the maximum and minimum frequency values through Basic Polynomial Interpolation (BPI).

Forward Wavelet Transform (FWT) contains three basic steps:

i. **Split:** The split steps distribute the signal frame into odd indexed and even indexed samples. The indexed sample provides information about the original signal recovery. [16]

ii. **Predict:** in the predict process the odd and even indexed samples are interleaved. Interpolating division is creating the predictor. To find the difference between predict value and odd samples, the wavelet coefficient is used.

iii. **Update:** the update process is essential to reduce the memory requirements.

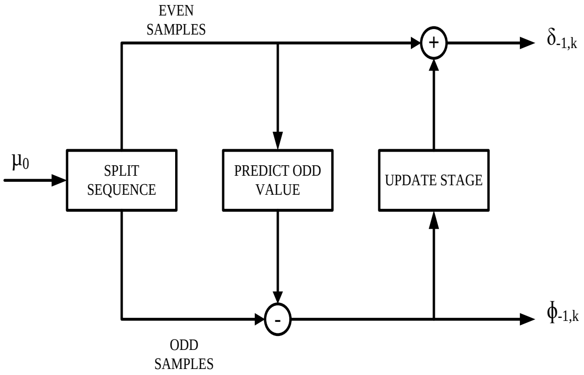


Fig.5. FWT lifting steps [2]

IV. PROPOSED METHOD

Image stenography is the most significant approach in the image processing field which hides the secret information (i.e. image) within another image (i.e. cover image). There are several methodologies which performs the image stenography process. The most adoptable approach is the spatial-domain based image-stenography. In spatial approach, LSB (i.e. Least Significant Bit) method is especially utilized for image mapping operation that maps the secret image bits into 4 distinct LSBs of cover image.

The overall implementation process of proposed Stegano-image module on FPGA is described as below.

A.Proposed Image-Steganography process

Generally, image steganographic is the method of hiding secret image into another cover image. During this process, image may be undergoing for encryption before hiding it into cover image. The pictorial representation of this process in given in the following figure: 6.

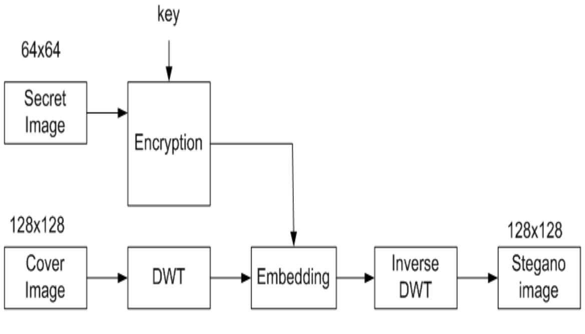


Figure: 6 Proposed Stegano Image Process

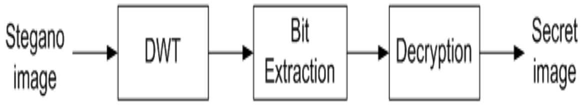


Figure 7. Decoding Operation

The system selects the (64 x 64) size of secret image and embedding with (128 x 128) size of cover image. Initially, the secret image will be encrypted by EXORed encryption operation. Then cover image is utilized and perform the lifting-based DWT operation which results the lower and higher coefficients. Then system embeds both encrypted secret image and cover image by applying LSB insertion method. This phase considers the two input images (i.e. encrypted secret image and DWT covered image). The outcome of this phase is proceeding for inverse DWT operation which obtains the Stegano image.

Next, system considers the generated Stegano image for image extraction process which is the opposite process of embedding of secret image. At this phase, Stegano image is filtered by DWT then secret image is extracted via LSB decoding process. The decoded image bits are further decoded by XORed based decryption process and finally can get the secret image.

B.Interanal architectureof Proposed Steganography module

An internal architectural view of proposed steganographic module is shown in below figure:5.

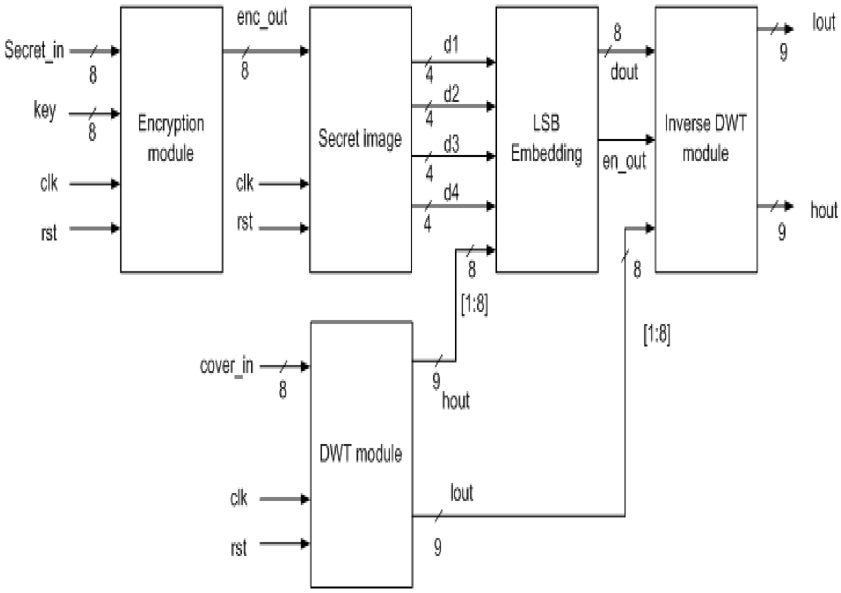


Fig. 8. Internal design of proposed Stegano module

The proposed architecture is primarily composed with five different blocks which are responsible to perform steganographic operation. Such major blocks are; 1) Encryption module, 2) Secret image splitter, 3) LSB embedding, 4) DWT module and 5) Inverse DWT module.

Initially, both secret image and cover image data are obtained from MATLAB tool which will convert those images in terms of text-based data. The MATLAB generated text-based data (i.e. 8bit secret image and 8bit cover image data) is fed for encryption and results the encrypted secret-image with secret encryption key. The encrypted image further fed into image splitter and splits the eightbits of image data into four parts (d1, d2, d3, and d4). Parallelly, system filters the cover image through DWT process and generates the "hout" (high pass) and "lout" (low pass) coefficients for that cover image. Then embedding module takes the d1, d2, d3, and d4 data and hout data as input for LSB insertion operation which inserts the d1, d2, d3, and d4 data into low-bits of hout data. The inserted data results the output in terms of 8bits dout signal. The dout and en_out signals are fed for inverse DWT operation which generates the two coefficients (i.e. hout and lout) of given image data.

While lifting based DWT module is designed which contains the 8bits din signal (i.e. cover image), clk and rst. The two 9-bits (hout and lout) output signals are extracted from input image. However, Inverse DWT module performs reverse operation of DWT module. Generally, this module considers the two input components (i.e. higher and lower frequency) and generates the two 9bits spatial domain signals.

V. RESULTS AND ANALYSIS

The tonsillitis detection system using Gabor filtering approach presented here was modeled using Verilog simulated and synthesized. The Xilinx 14.7 ISE was used here for system modeling. The simulations for the designs were carried out using Modelsim6.3f. The synthesis and the final implementation of the system design was performed on Artix 7 FPGA Board Device 7A100T-3 CSG324.

Main steganography module

The figure 9 depicts the top module design synthesized result which shows the input port and output port signals as defined in the design.

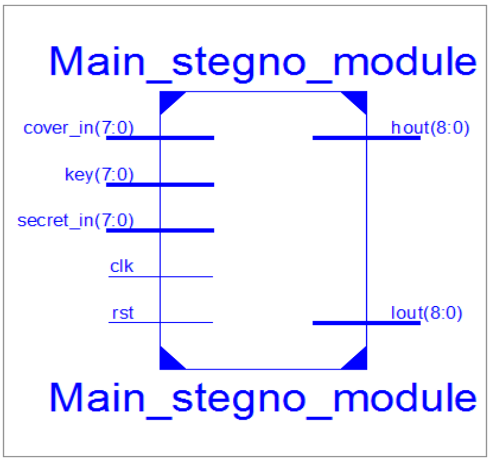
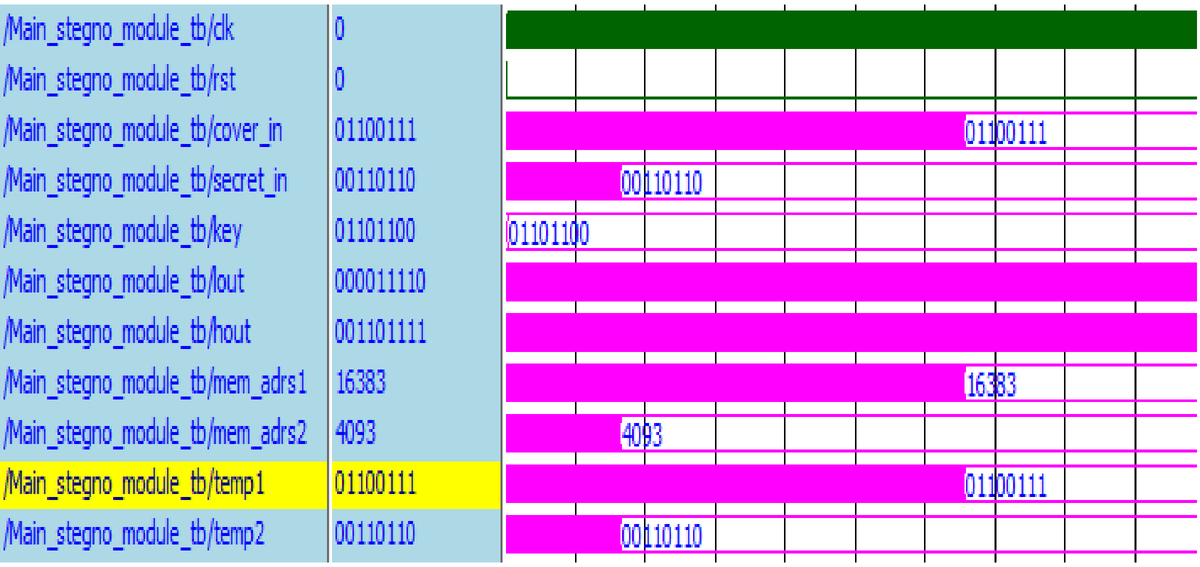


Fig. 9. Main steganography top Module

The Main stegno module simulation results as digital waveforms are displayed in figure 9.



/Main_stegno_module_tb/clk	0
/Main_stegno_module_tb/rst	0
/Main_stegno_module_tb/cover_in	01100111
/Main_stegno_module_tb/secret_in	00110110
/Main_stegno_module_tb/key	01101100
/Main_stegno_module_tb/lout	000011110
/Main_stegno_module_tb/hout	001101111
/Main_stegno_module_tb/mem_adrs1	16383
/Main_stegno_module_tb/mem_adrs2	4093
/Main_stegno_module_tb/temp1	01100111
/Main_stegno_module_tb/temp2	00110110

Fig.10. simulation waveforms for main stegano module

The waveforms show the cover image and secret image data input as 8-bit pixel data. The key input for the encryption of secret image data is selected as “01101100”. The two outputs of the module are the odd and even components of the stego image. The secret image data shown in the waveform is “00110110”.

The stego image data obtained from main stegno module simulation was used in constructing the stego image. The stego mage constructed is shown in figure 11.

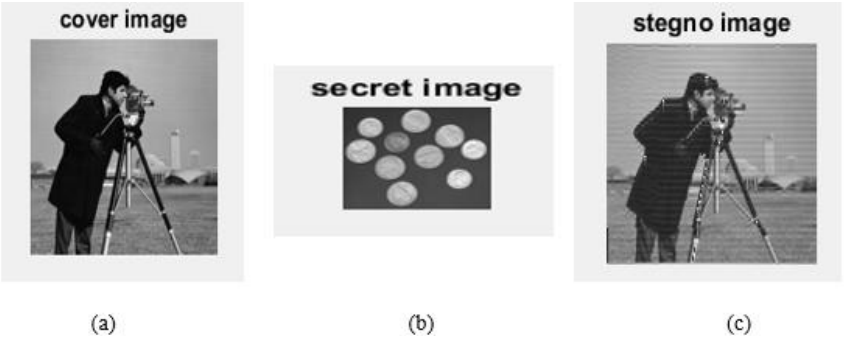


Fig.11. Main steganography Results-(a) cover image, (b) secret image (c) stego image

MAIN DECODING

The synthesized result of the top-level design for the main decoding module is shown in figure 12.

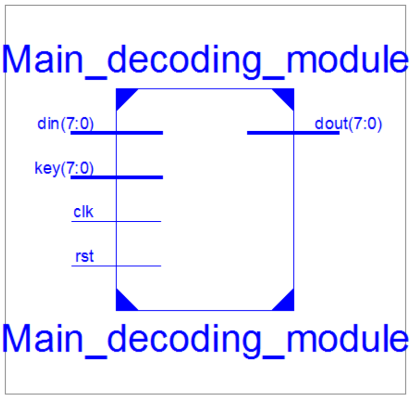
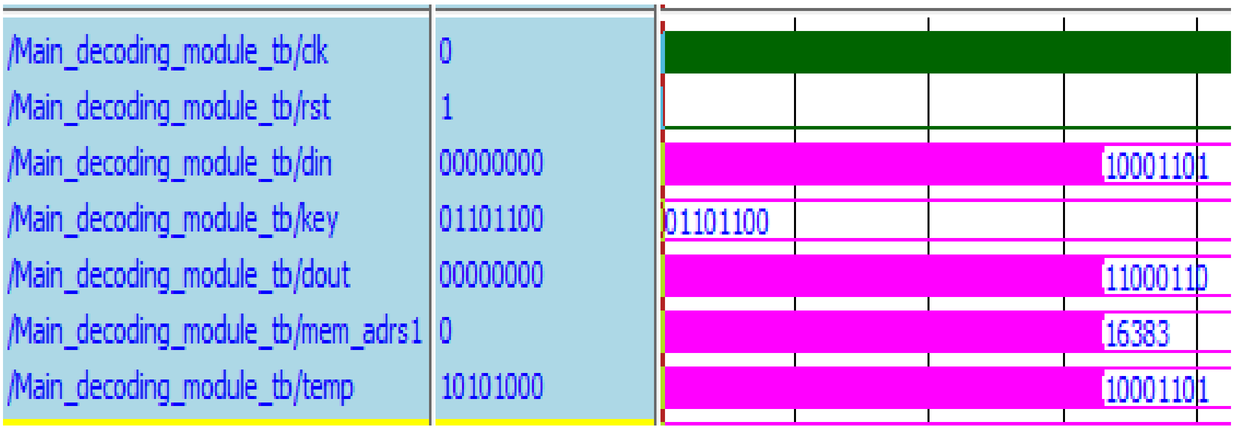


Fig.12. Main decoding top Module

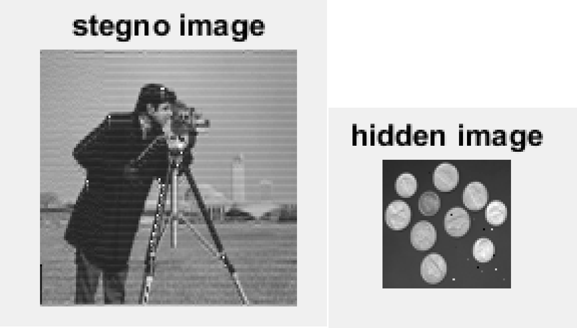
The waveform results for the main_decoding top module are shown in figure 12.



```
/Main_decoding_module_tb/clk        0
/Main_decoding_module_tb/rst        1
/Main_decoding_module_tb/din        00000000    10001101
/Main_decoding_module_tb/key        01101100    01101100
/Main_decoding_module_tb/dout       00000000    11000110
/Main_decoding_module_tb/mem_adrs1  0           16383
/Main_decoding_module_tb/temp       10101000    10001101
```

Fig.13. Main decoding Simulation Results

The data out obtained by simulating the main_decoding module was “01101100” which matches with the secret image data input to the main_stegno module. The images obtained by simulating the main decoding module are shown in figure 14.



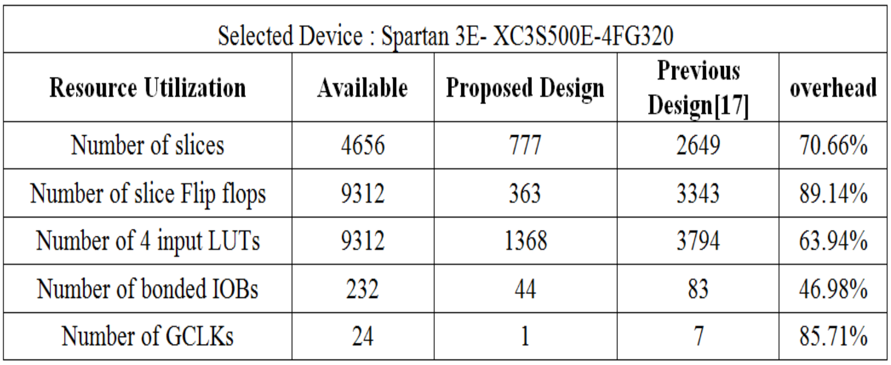
(a) (b)

Fig.14. Main decoding Results-(a) stegno image (b) hidden image

VI. COMPARISON RESULTS

A comparison of the designed stegno module and decoding module resource utilization with the existing designs of [] are shown in table 1.

Table 1: Resource utilization Comparison



Selected Device : Spartan 3E- XC3S500E-4FG320				
Resource Utilization	Available	Proposed Design	Previous Design[17]	overhead
Number of slices	4656	777	2649	70.66%
Number of slice Flip flops	9312	363	3343	89.14%
Number of 4 input LUTs	9312	1368	3794	63.94%
Number of bonded IOBs	232	44	83	46.98%
Number of GCLKs	24	1	7	85.71%

VII. CONCLUSION

An image steganography system was designed here using DWT-LSB based secret image insertion and extraction. The steganography system designed here applies encryption procedure to the secret image data before hiding the secret image inside the cover image. The DWT process is applied on the cover image to split the images as higher and lower coefficients. The coefficients were utilized to hide he secret image. The main decoder module of the steganography system was designed here to extract the encrypted hidden image data and decrypt the data to get back the secret image.

REFERENCES

[1] Sagar Kumar Nerella, Kamalendra Verma Gadi, & Raja Sekhar Chaganti. (2012, March). Securing images using color visual cryptography and wavelets. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(3), 163-168.

[2] Calabrese Thomas. (2004). *Information security intelligence: Cryptographic principles and applications*. Clifton Park, NY: Delmar Learning. Available at: https://trove.nla.gov.au/work/30183833?q&versionId=36646266

[3] Prabhishek Singh & R S Chadha. (2013, March). A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology*, *2*(9), 165-175.

[4] B. Pushpa Devi, Kh. Manglem Sing, & Sudipta Roy. (2012, July). Dual image watermarking scheme based on singular value decomposition and visual cryptography in discrete wavelet transform. *International Journal of Computer Applications*, *50*(12), 7-12.

[5] M. Tayel, H. Shawky & A. E. S. Hafez. (2012). *A new chaos steganography algorithm for hiding multimedia data*. 14th International Conference on Advanced Communication Technology, IEEE, 208 – 212. Available at: file:///C:/Users/DST/Downloads/20120277_finalpaper.pdf

[6] Usha Bhanu. N, & Dr. A.Chilambuchelvan. (2012, April). A detailed survey on vlsi architectures for lifting based dwt for efficient hardware implementation. *International Journal of VLSI design & Communication Systems*, *3*(2), 143-164.

[7] Pritee Singh & Mr. Faseeh Ahmad. (2017, June). Hardware implementation of MAC using matlab simulink and FPGA. *GRD Journals- Global Research and Development Journal for Engineering*, *2*(7), 38-44.

[8] Yi-Hsing Lin , Yu-Yao Hsu , Sih-Wei Wang , & Yu-Cheng Fan. (2016). *Imitated light field image architecture based on Haar discrete wavelet transform*.

Instrumentation and Measurement Technology Conference Proceedings (I2MTC), IEEE International. Available at: https://ieeexplore.ieee.org/abstract/document/7520356/

[9] Al-Afandy, Khalid A., et al. (2016). High security data hiding using image cropping and LSB least significant bit steganography. *World Academy of Science, Engineering and Technology International Journal of Computer and Information Engineering*, *10*(3), 659-662.

[10] C.T. Li & F.M. Yang. (2003). One-dimensional neighborhood forming strategy for fragile watermarking‖. *Journal of Electronic Imaging, 12*(2), 284-291.

[11] A.D.Ker. (2005). Steganalysis of LSB matching in grayscale images. *IEEE Journals & Magazines*, *12*(6), 441-444.

[12] O. Dabeer, K. Sullivan, U. Madhow, S. Chandrasekaran, & B. S. Manjunath. (2004). Detection of hiding in the least significant bit. *IEEE Transactions on Signal Processing*, *52*(10), 3046–3058.

[13] Anil Kumar & Rohini Sharma. (2013). A secure image steganography based on RSA algorithm and hash-lsb technique. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(7), 363-372.

[14] Mohammad A. Ahmad, Dr. Imad Alshaikhli, & Sondos O. Alhussainan. (2012). Achieving security for images by lsb and md5. *Journal of Advanced Computer Science and Technology Research, 2*(3), 127-139.

[15] Nicholas Hopper, Luis von Ahn, & John Langford. (2009). Provably Secure Steganography. *IEEE Transactions on Computers, 58*(5), 662–676.

[16] Jing-Ming Guo & Thanh-Nam Le. (2010). Secret communication using jpeg double compression. *Signal Processing Letters*, *IEEE*, *17*(10), 879–882.

[17] Min-Wen Chao, Chao-hung Lin, Cheng-Wei Yu, & Tong-Yee Lee. (2009). A high capacity 3d steganography algorithm. *IEEE Transactions on Visualization and Computer Graphics*, *15*(2), 274-284.