European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 7, Issue 07, 2020

Implementation of Zig-Zag Coded Steganography for Secured Data Transmission in FPGA

R. M. Joany[1], E. Logashanmugam[2], E. Anna Devi[3], L. Magthelin Therase[4], S. Yogalakshmi[5]

[1,2,3,4,5]Department of Electronics and Communication Engineering, Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India.

[1]mariajoany@gmail.com, [2]logu999@yahoo.com, [3]annadevimit@gmail.com, [4]ltherase@gmail.com, [5]yogalakshmi1015@gmail.com

Abstract

Steganography is defined as the knack and science of communicating in a secret way which hides some information on the existence of communication. A steganographic model helps to hide or embed the sender's secret message in an image known as carrier. For a normal view, it does not give a clue about the existence of a secret message in it. An image can be in any format which is used as a carrier. The sender's message is covered in this carrier image. The carrier is transmitted in which the message (image) is hidden. In the proposed system Zigzag coded Stenography is introduced. In the proposed scheme the image is first preprocessed using MATLAB software, Image information is converted into the grayscale format and then Binary conversion is done, after applying DCT the image is further split into multiple palettes. The preprocessed data is then provided with the stenographic step with key generation by the VLSI system and then transmitted through the channel. The reverse operation then retrieves the original information by applying IDCT and also removing noise. The proposed Zigzag coded algorithm will have a high embedding rate and embedding payload capacity, less computational complexity and at the same time maintaining the high stego-image quality compared to the existing works.

Keywords - Image Steganography, Stego-image, Discrete Wavelet Transform, FPGA, Zig Zag code.

1. INTRODUCTION

Secured means of transmission of the digital information is to be maintained when highly sensitive and precious data are communicated over the internet. The process of hiding information in any embedding medium such as images in any format, audio files and video files in any format and text files is known steganography. The term steganography is defined as "covered writing" which is derived from the Greek words "Stegos" & "grafia". The basic three elements of steganography system are the cover object, the secret message and the stego object. An image is always represented as a digital image in the form of a 2-D matrix representing colour intensities as each grid point known as a pixel. In the grayscale model, images require 8 bit for representation. For the representation of coloured images, 24 bits are required. This colour model representation is known as the RGB model. The methods for concealing data in an image are classified as Time and Frequency Domain. If the secret data

is embedded in the least significant bit (LSB) of image pixel then it is time domain. The fundamental LSB technique is easy for execution but it is fragile against few attacks like low pass filtering and compression. If the secret data is inserted in the frequency coefficients of images it is known as frequency domain. The frequency-domain insertion overcomes the difficulties and limitations in the time domain. Steg-analysis is the method of sensing concealed information. This method is carriedout by cresting using steganography. Steg-analysis examines various image features by comparing coverimage with stego-images and identifies stego-images. In recent days, various steganography techniques are developed and implemented in the FPGA. Implementation in FPGA provides optimization, reconfigurability, quick response. It is well suited for the image processing applications.

2. LITERATURE SURVEY

1. The methods suggested by Abbas Cheddad et.al. provide details about Digital Image Steganography in which survey and analysis are carriedout. This paper provides a state-of-the-art review and analysis of the different existing methods of steganography. It also suggests some common standards and guidelines to implement steganography. This paper is concluded with some recommendations and advocates for the object-oriented embedding mechanism.

2. The paper authored by E.A Elshazly provides the generalized exploiting modification direction (GEMD) steganography algorithm and it is an enhancement of the exploiting modification direction (EMD) algorithm which hides a high payload capacity but the quality of the stego-image is maintained.

3. Larged embedding capacity and imperceptible stego-images by adaptive least-significant bit (LSB) steganographic method using pixel-value differencing (PVD) was proposed by Cheng- Hsing Yang and Chi-Yao Weng.

4. An improvement of EMD embedding method for large payloads by pixel segmentation strategy by Chin- Feng Lee and Chin-Chen Chang, this paper provides data hiding method using pixel segmentation strategy is used which keeps (16-Pm) MSBs of a pixel pair unchanged and alters Pm LSBs to indicate the virtual modifications on m-dimensional pseudo random vectors for carrying the secret data.

3. OBJECTIVE

The objective of this paper is to propose an enhanced algorithm i.e. modified and efficient Zigzag coded algorithm to implement steganography. The method will have high embedding rate, high embedding payload capacity, less computational complexity. The results are to be obtained with high stego-image quality compared to the existing work. It also aims at arriving better signal to noise ratio compared to the previous work.

4. EXISTING SYSTEM

A developed GEMD image steganography algorithm is proposed in this paper. This algorithm was implemented by on an improved and modified Pixel Segmentation Strategy with Indicator Bit (PSS-IB). The proposed algorithm overcomes the limitations of the previous EMD algorithms. The proposed algorithm is implemented in two phases. In phase-1an embedding procedure is adopted. In phase-2 extracting procedure is carried out. In phase-1 of embedding procedure, the proposed algorithm segments each block of pixels of the cover

image into VCA, IB and VMA. The VCA vector of each pixel of the block is kept unchanged, the IB is flipped if required and the VMA vector is modified. The proposed algorithm assigns the overall VCA vector (the vector that contains the VCA of each pixel of the block) and generates "n" vectors to carry the secret text, where n = LVMA–1, and LVMA is the length of overall VMA vector. In phase-2 of the extracting procedure, the embedded data is extracted from the stego-image pixels.

5. BLOCK DIAGRAM OF PROPOSED STEGANOGRAPHY PROCESS

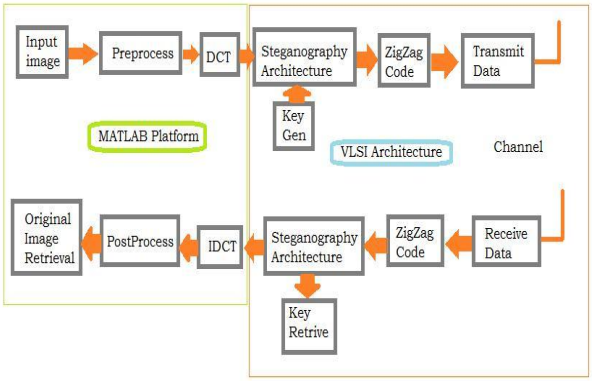

Figure No. 1: Block diagram of Zig -zag coded image steganography

The figure 1. shows the block diagram of the the proposed zig-zag coded image steganography process. The input image is preprocessed and given to a Discrete Cosine Transform block. These methods are simulated in MATLAB. The steganography architecture and zig-zag code and key generation process are done in FPGA. Thus the data is transmitted. On the receiver side, with the help of retrieving key the data is retrived and reconstructed using the Inverse Discrete Cosine Transform in MATLAB. The entire process is carriedout in four modules.

6. Proposed System

Module 1: Design of Image Preprocessing

In image processing there are various transform domain techniques available. Some of them are as follows.

1. Discrete Cosine Transform (DCT)
2. Discrete Wavelet Transform (DWT)
3. Fast Fourier Transform (FFT)

Using these techniques information can be hidden in transform coefficients to the cover images. This method makes steganography system much more robust against attacks such as compression, filtering, e.t.c [12] [13]. Discrete Wavelet Transform is the most widely used compression technique in image steganography. At every decomposition, the level is high. This module consists of image preprocessing and preparing. This module contains three important steps to be adopted. The watermarking technique is combined along with the steganography and it enhances the PSNR and provides better solution for the noise attack further [14].

- Converting into GRAYSCALE
- Apply DWT
- Split Image

In wavelet analysis, the Discrete Wavelet Transform (DWT) breaksup a signal into a set of mutually orthogonal wavelet basis functions. These functions are spatially localized hence they differ from sinusoidal basis functions, that is, nonzero over only part of the total signal length. Moreover, wavelet capacities are enlarged, interpreted and scaled forms of a typical capacity, known as the mother wavelet. Similar to the case in Fourier investigation, the DWT is invertible, with the goal that the first sign can be totally recouped from its DWT portrayal. Two of the most common are the Haar wavelets and the Daubechies set of wavelets. It is important to note the following important properties:

1. Wavelet functions are spatially localized;
2. Wavelet functions are dilated, translated and scaled versions of a common mother wavelet; and
3. Each set of wavelet functions forms an orthogonal set of basic functions DWT in one dimension.

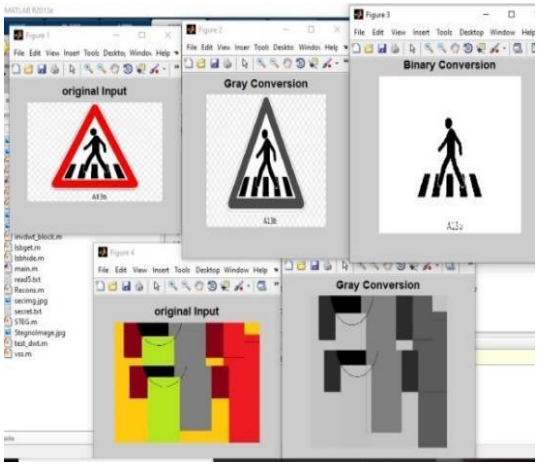

Figure No.2: Binary and Gray conversion of the input images

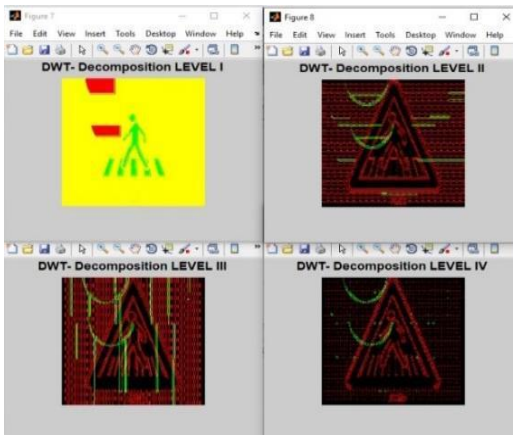

Figure No.3: Four levels of DWT Decomposition

Module 2: ZIG ZAG coding

1. This module is the core of the entire work, which contains the steganography operation such as generating the key using random generation using FPGA, Stenograph the image data with a generated key and which will generate a new Code. Further, the data is communicated through the channel.

2. The proposed steganography algorithm which is based on the proactive secret scheme and generalized exploiting modification direction embedding method is implemented in MATLAB using Simulink and Xilinx blocks. The implementation process is done in three phases. Thus the image pre-processing and image post processing phases are designed and simulated using MATLAB software and the proposed steganography algorithm is implemented in FPGA.

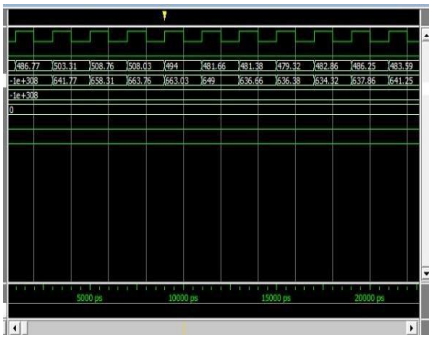

Figure No.4: Embedding the random key with the pixel values of the input image

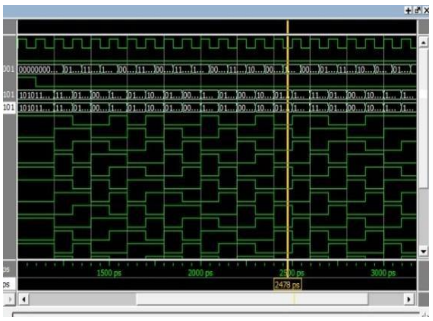

Figure No. 5: Generation of 8- bit Pseudo Random Key

Module 3: Reconstruction

The Reconstruction and Receiver part get the encrypted data and reconstruct the original image by removing the Steganography content in the image. It will check the SNR after receiving if the SNR is less than the original image is retrieved.

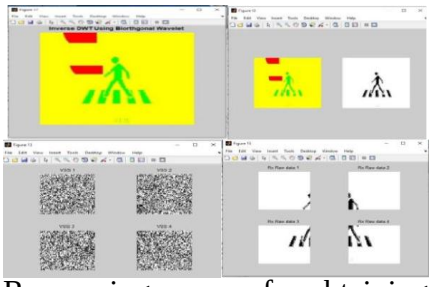

Figure No.6: Recovering process for obtaining the original images

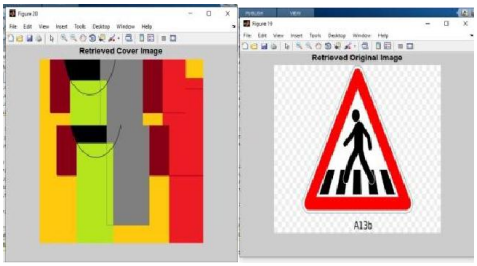

Figure No. 7: Retrieved the original input image and cover image

Module 4: Peak Signal to Noise Ratio (PSNR)

Signal to noise ratio is an error metric which is used to compare the quality of the images. The quantitative measure of the performance for restoration of image are measured in terms of Peak Signal to Noise Ratio.

$$\text{PSNR} = 10\log_{10}\frac{R^2}{MSE} \qquad (6.1)$$

R is the maximum variation in the input image data type. For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255.

Mean Square Error (MSE)

The Mean Squared Error (MSE) is estimated by the average of the squares of the errors that is, the average squared difference between the attribute which is to be estimated and the estimator.

$$\text{MSE} = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M \times N} \qquad (6.2)$$

The histogram of the input and the retrieved image is shown below. A SNR of 44.47 db is obtained.

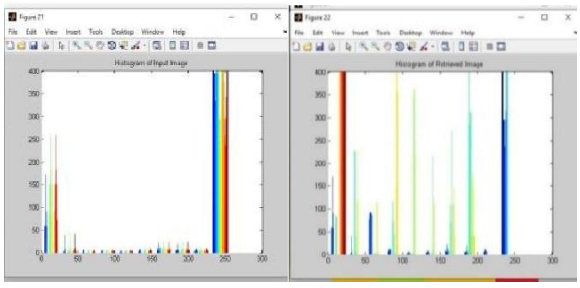

Figure No.8: Histogram of the input and the retrieved images

7. CONCLUSION

The efficient and reliable FPGA based steganographic system using Zig-zag algorithm is discussed in this paper. FPGA are reconfigurable, flexible and physically secured devices with high computational capabilities and offer a fast design cycle. It helps to solve all complex problems in terms of both security and processing speed.

Zig-zag coded algorithm has been used to perform steganography which will have good embedding rate, less computational complexity and keeping high stego-image quality compared to the existing works referred. The signal to noise ratio of 44.47 dB is obtained.

The hardware implementation based on various spatial and transforms domain techniques to develop the robustness, reconstruction of image with good quality and performance as well as optimization of the processing speed and utilization of power.

8. REFERENCES

[1] Ankita Ganorkar and Sujata Agrawal, "Implementation of Steganography on FPGA", 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.

[2] C. F. Lee, C. C. Chang, and K. H. Wang, An Improvement of EMD Embedding Method for Large Payloads by Pixel Segmentation Strategy, Image and Vision Computing, ELSEVIER, Vol. 26, No. 12, pp. 1670 – 1676, 2008.

[3] C. F. Lee, Y.R. Wang, C.C. Chang, A Steganographic Method With High Embedding Capacity by Improving Exploiting Modification Direction, Proceedings of the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP07), IEEE, pp. 497 – 500, 2007.

[4] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems, IEEE Transactions on Information Forensics and Security, Vol. 3, pp. 488 – 497, 2008.

[5] 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.Distributed Computing, Applications and Technologies (PDCAT), 16-18 Dec. 2013, pp.

[6] Dr. Ahlam Fadhil Mahmood, Nada Abdul Kanai and Sana Sami Mohmmad, "An FPGA Implementation of Secured Steganography Communication system", Tikrit.

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

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

[9] Hala Farouk, Magdy Saeb, "Design and Implementation of Secret KeyIntegrated Networks (SPIN), 19-20 Feb. 2015, pp. 471 – 476.Ird India, Volume 2,

Issue 1, January 2014. ISBN 978-81-317- 2695-2.Journal of Engineering Science, vol. 19, No. 4, December 2012, pp. 14-23

[10] K. Ntalianis and N. Tsapatsoulis, Remote Authentication via Biometrics: A Robust Video-Object Steganographic Mechanism Over Wireless Networks, IEEE Transactions on Emerging Topics in Computing, Vol. 4, Issue 1, pp. 156 – 174, March 2016.

[11] Kamila S., Roy R., Changder S., "A DWT based steganography scheme with image block partitioning", IEEE 2nd International Conference on Signal Processing.

[12] 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.

[13] 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.

[14] E. Anna Devi, R. M. Joany, S. Yogalakshmi, L. Magthelin Therase, Digital Video Steganography Technology For Security Application, IOP Conference Series: Materials Science and Engineering, 590, 2019.

[15] P. Karthigaikumar, Anumol, K. Baskaran, "FPGA Implementation of High Speed Low AreaDWTBasedInvisibleImage Watermarking Algorithm", SciVerse.

[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] Rafael C. Gonzalez, Richard E. Woods, "Digital Image Processing", third edition, ScienceDirect, Procedia Engineering, 30(2012), pp. 266-273.Society, 2008.

[18] Suhad Shakir Jaber, Hilal Adnan Fadhil, Zahereel I. Abdul Khalib and Rasim, Stenographic Micro – Architecture Employing FPGA", 1530-1591/04, 2004 IEEE.

[19] Vasantha 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.

[20] W. C. Kuo, and C. C. Wang, Data hiding based on generalized exploiting modification direction method, Imaging Science Journal, Vol. 61, No. 6, pp. 484 – 490, 2013.

[21] X. Zhang and S. Wang, Efficient Steganographic Embedding by Exploiting Modification Direction, IEEE Communications Letters, Vol. 10, No. 113, pp. 781-783, 2006.