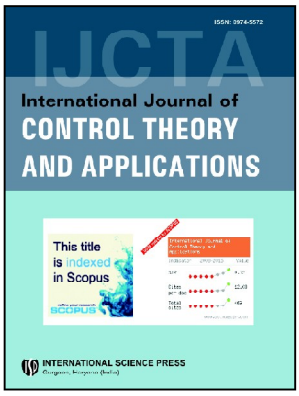


International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 10 • 2017

Distributed Approach Based Image Steganography Using Double Thresholding for High Speed Hardware Applications

Avdash Bhatt[1] and Rinkesh Mittal[2]

CEC Landran, Mohali / ECE Dept, Chandigarh, 140307, India
E-mail: [1]avdeshbhatt29@gmail.com; [2]hod.coeece@cgc.edu.in

Abstract: Image processing and signal processing implementation of hardware resources like FPGA is a current area of research in recent years. Many techniques have been implemented in recent times and their results are compared with the existing approaches. Image and data security through steganography is an important aspect of research and many new designs have been evolved for efficient and fast implementation and processing of images. In this work distributed technique is used for increasing the speed of implementation at the cost of hardware resources. All the unit work in parallel and produces an output file four times faster than the usual method. Canny edge detector is used for detection of edges of the image. It utilizes double thresholding technique for the detection of edges. LSB steganography technique is used for hiding the image inside another image. The PSNR value of the design comes out to better as compared to the basic approach.

Keywords: Steganography, FPGA.

I. INTRODUCTION

Steganography is a technique of hiding information within the information or hiding one form of information into another form of information. It is a method in which secret message can be transmitted. Steganography is a state of art for sending secret information over secret communication. In this technique, new and real files may be expressed as cover text, or it can be expressed as cover image if file is in image format. Also, it may refer as cover audio/video, if the original file will be an audio/video. When the secret information or message is inserted then it will be expressed as stego medium. In order to hide the process to control the detection and extraction, then stego-key is used. Additionally, steganography may be defines as the method of hiding the secret message or data in such manner that the existence of message is not visible. Inthis method, sender should choose the suitable message carrier before the hiding process and then it chooses efficient secret information as well as password. The usefuland suitable Steganography algorithmshouldbechosenwhich is capable toinstructthe message and then sender will transfer the stego medium file by email, or by any other technique. This stego file contains information with secret message. At the receiver end, message cam be received and then it decodes by using the extracting algorithm and password which is known to sender.

Mostly, in steganographicprocesses, even though merely the irrelevant components are distorted, most of the analytical methodsmaydisclosethe existence of the secreted message by finding statistical difference among the cover and stego objects.

For developing the steganographic methods, two measures should be taken: 1. avoid prominent parts while inserting the messages into cover. 2) Increase the embedding efficiency.

Capacity, Imperceptibility and Robustness are three parameters known as magic triangle. Capacity is also known as embedding payload, and it is calculated by secret a bit which is inserted in every cover pixel. More secret data is allowed to be inserted into the cover image when the capacity is high. Imperceptibility is generally determined by PSNR. The PSNR value is high, when the difference between the cover image and the stego image is small. Hence it may be said that eminence of stego image is betterwhen the imperceptibility is high. Robustness helps to protect the secret message from being attacked.

II. RELATED WORK

Chen, Wen-Jan*et al.* [1] In this paper, High payload steganography method has been presented using hybrid edge detector. The result indicated that presented approach attains high capacity but also increases the eminence of stego image with the help of edge detection method.

Ioannidou, Anastasia *et al.* [2] proposed approach for image steganography depending on high payload and edge detection. In this paper, hybrid edge detector is utilized for steganography. Furthermore, combination of two approaches produces a new steganography algorithm. The results demonstrated that proposed approach attains high peak signal to noise ratio.

Arora, Sneha *et al.* [3] presented an image steganography using edge detection method. The presented approach helps to conceal the message into color images and edge of an image can be detected by scanning which uses 3*3 windows. The results show that presented method attains higher capacity and high image quality.

Mohamed, Marghny H. *et al.* [4] proposed High Capacity Image Steganography Technique.The major objective of the proposed technique is to enhance the capacity and increase the image quality. The result indicates that presented technique performs well in comparison to other traditional methods or techniques in terms of capacity, quality and noise ratio. The efficiency of proposed method is evaluated from the hidden information and image quality of cover image

Kaur, Amanpreet, and Sumeet Kaur *et al.* [5] in this work, 2k correction method & edge detection method has been presented. This approach shows better results as compared with earlier techniques. The proposed algorithm gives better PSNR values.

Charan, Gunda Sai, *et al.* [6] presented a image steganography with multi-level encryption. In this work, a new technique has been presented which encrypts the plain text into cipher text and inserting it into a color image.

Tseng, Hsien-Wen *et al.* [7] presented anfuzzy logic-based approach and extends the real design to block-based design. The result indicates that the presented approach attains higher payload and also having minimal distortion.

Singla Deepali, Mamta Juneja *et al.* [8] proposed image steganography technique depending on the Hybrid Edge Detection. The proposed approach can be used for color images. Hybrid edge detection is the combination of canny and fuzzy edge detector. Embedding is done accordingly after detecting edges.

Al-Dmour, Hayat *et al.* [9] proposed anovel image steganography method. The presented scheme uses the sharp section of the image. The results indicate that the presented scheme has attained good results as compared with other traditional approach. Moreover, in this work, the proposed approach sustains the better security in comparison to other schemes.

Mohapatra, Chandan *et al.* [10] presented a survey on image steganography. In this paper, several kind of steganography has been studied and discussed. Here, the significance can be given to the Image spatial

domain, image frequency domain and to adaptive method. Yet there is a lot of scope and chances to analyze and employed more an efficient scheme for steganography.

Singh, Saurabh *et al.* [11]presented a hash based approach utilizes canny edge detection method. It can follow the encoding and decoding process. Edge detection is done by canny method and then hash function is used to embed text data in the image. Matlab 2010a version is used for simulating the results. the results indicates that canny edge detection performs better.

Maheswari, S. Uma *et al.* [12] presented an frequency domain steganography algorithm. The result analysis indicates that PSNR ratio is produced by the proposed algorithm is around 49dB. This ratio of noise is higher among all other data hiding approaches which are discussed in this paper.

Hariri, Mehdi, Ronak Karimi *et al.* [13] in this paper, different types of steganography considering the cover data has presented. As the first step, text steganography and investigate its details is provided. Then, image steganography and its techniques will be investigated. Some techniques including Least Significant Bits, Masking and filtering and Transformations will be subjected during image steganography.

Zaidan, A. [14] in this paper, a new concepts on Steganography which is "multi-cover steganography" using remote sensing image; Remote sensing Image is an image taken from the satellite in a manner of three shots, engagimgthese images generate one false color image, this type of image has been proposed in this research. The second concepts is general recursion neural cryptosystem, this approach has been designed and implemented to defeat the problem of exchange cryptography keys through the network, the new cryptosystem exchange the keys through trine the neural network data which later on used to decrypt the data, this powerful cryptosystem merged with the multi-cover steganography to produce the third novel concept. The fourth concept is designing irregular encoding method base on LSB algorithm. The new way of encoding has approved the security of data hidden.

III. PROPOSED METHODOLOGY

For the implementation of steganography in hardware platform, there are various stages which must be followed by the hardware. The stages are discussed in the following section. These stages include buffering of image into the hardware, smoothening using the Gaussian Filter, and then the edge detection using the canny edge detector. These steps are:

Row Buffering

In row buffering operation, a 3X3 window is used for buffering the image and loaded into the FPGA. The device has a limited storage and can be used to store the values of the pixels in real time basis. Partial row buffering is used to store and import the image to the FPGA and can be used for further processing performed on the pixels of the image. Figure 1 indicates the partial buffering of the image with the help of 3X3 window.

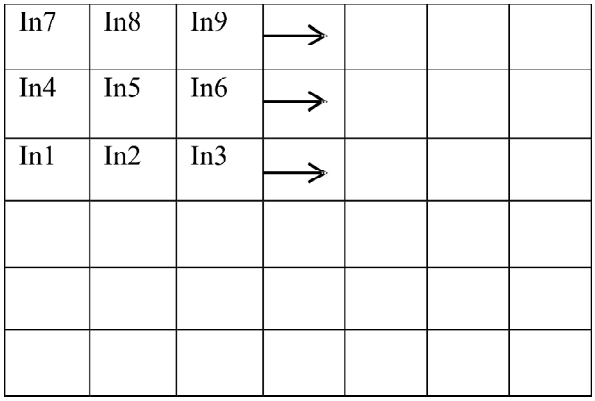


Figure 1: Window Operation

Smoothing

All the images contain some amount of noise; the first target is to reduce that noise otherwise it is mistaken for edges. To decrease the noise Gaussian Filter is used with standard deviation of 1.4. is the matrix shown in equation 1 which must be multiplied with the window for smoothing the image.

$$B = \frac{1}{159}\begin{bmatrix} 2 & 4 & 5 & 4 & 2 \\ 4 & 9 & 12 & 9 & 4 \\ 4 & 12 & 15 & 12 & 5 \\ 4 & 9 & 12 & 9 & 4 \\ 2 & 4 & 5 & 4 & 2 \end{bmatrix} \tag{1}$$

Sobel Operator

Canny Edge Detector detects the images by finding the gradients of the image in the x and y direction. Gradients are calculated using the matrices for x and y direction are:

$$K_X = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \tag{2}$$

$$K_Y = \begin{bmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix} \tag{3}$$

The gradient magnitude is calculated as the sum of the gradients in the x and y direction which is given by the equation 4.

$$|G| = |G_X| + |G_Y| \tag{4}$$

Double Thresholding

This operation is used to find the pixel value which is finally written into the output file. For the application of the canny edge detection algorithm the target pixels upper, lower, left and right pixel value is also selected.

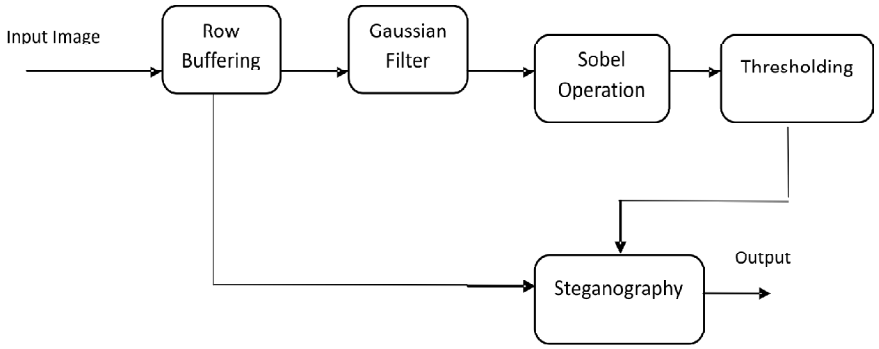


Figure 2: LSB Steganography

Double threshold value is applied i.e. if the pixel value is greater than the higher threshold is considered to be strong, lower than the low threshold is suppressed and the one lies between the thresholds are considered as weak.

Steganography

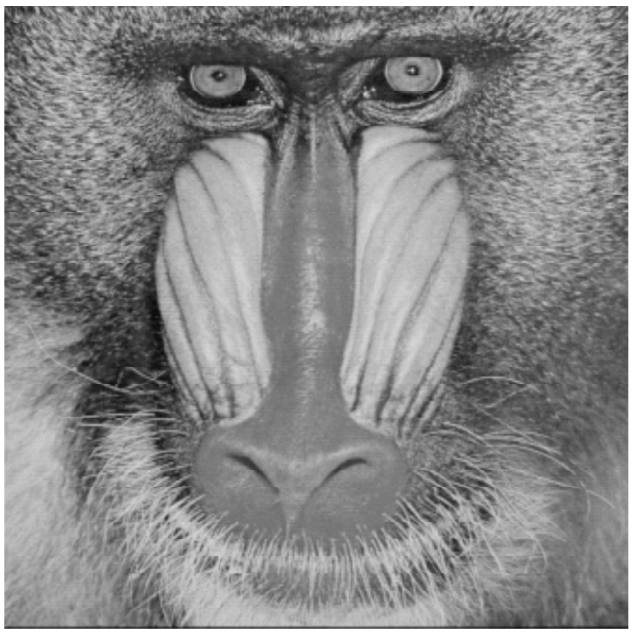
It is a process of hiding an image inside an edged image. The method used for hiding the image is termed as LSB steganography. In this type of steganography if the LSB bit of the edged image and the stego image are equal then the pixel value remains same otherwise it must be complimented. The process of steganography is shown in figure 2.

Distributed Technique

In order to increase the speed of detection of edges and the steganography, the image is distributed into four equal parts. Parallel processing is performed on all the selected parts. The image distribution and then combining to get the original image is performed on MATLAB and performance parameters are also calculated using the MATLAB.

IV. RESULTS AND DISCUSSIONS

The proposed design is implemented using the Xilinx Virtex 6 FPGA with VHDL Language. The image taken for the simulation of hardware is of size and can be divided into four equal parts each. The image is then given to the FPGA for the processing of the proposed design. Figure 3 and 4 shows the original image and steganography image (which must be hidden).



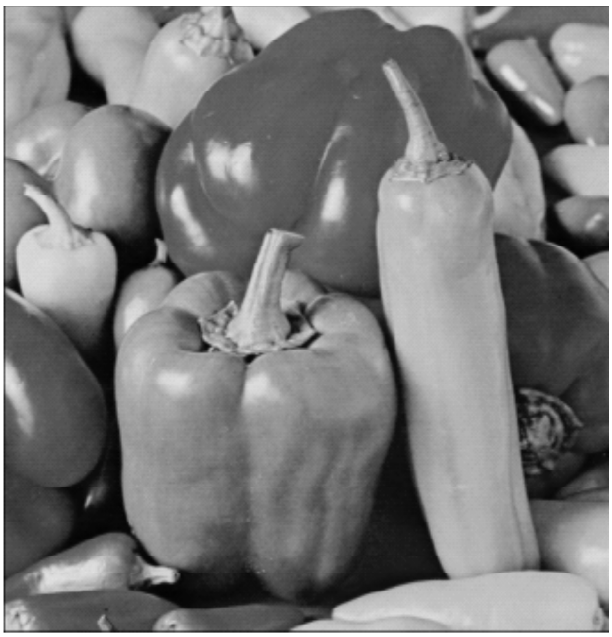


Figure 3 & 4: Original Image & Steganography Image

figure 5a-5d shows the conversion of image four parts into the edged image of the original image while figure 6a-6d shows the steganography image divided into 4 equal parts.

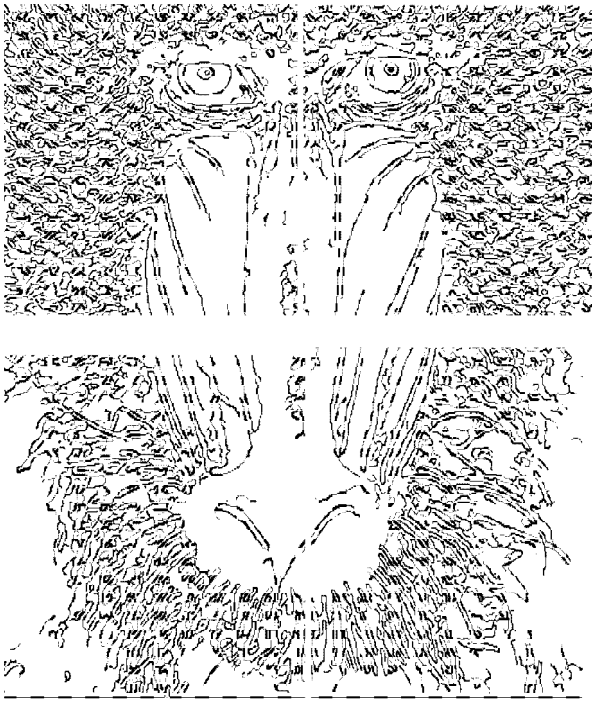


Figure 5a- 5d: Edged version of the original image

Figure 6a- 6d: Steganography Image

Now if the figure 4 is edged and the original image figure 3 remains the original image and the figure 4 image is first converted into edges and then it must be hidden in the original image. Figure 7a-7d shows the edges of the steganography image and figure 8a-8d shows the image after steganography operation is performed.

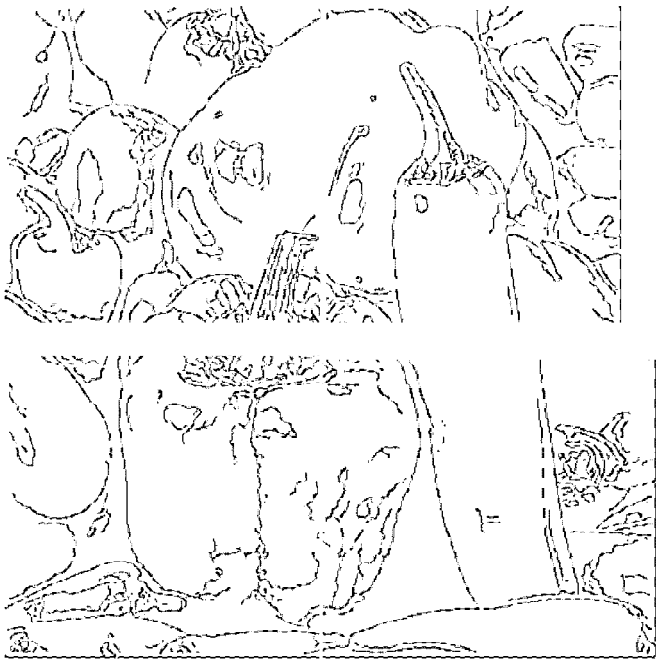


Figure 7a- 7d: Edged version of second image

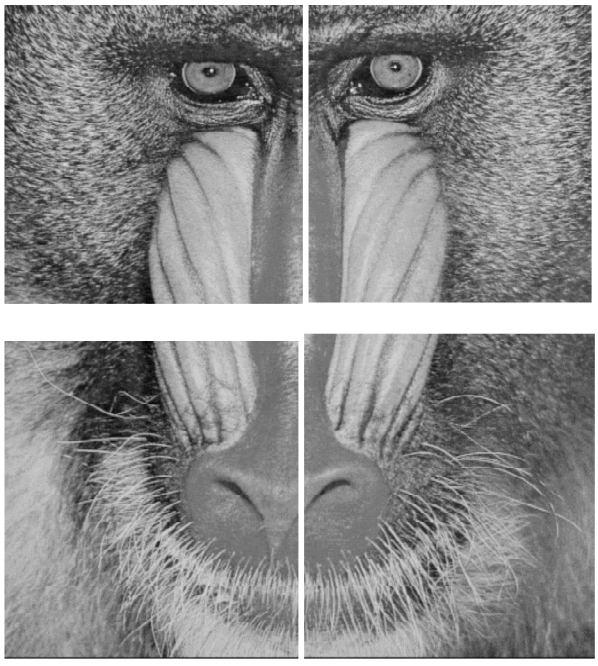


Figure 8a-8d: Image after Steganography

The PSNR value of the steganography image comes out to be 51.2344 db while in the base paper the PSNR value is 31.882 db. Table 1 shows the resources utilized by the device while implementation of the proposed design. Number of resources are the measure of area utilized by the device in terms of number of slices, number of slice LUTs and number of Flip-Flop pairs.

Table 1
Resource Utilization

Parameters	*Centralized Approach*	*Proposed Approach*
Number of Slice LUTs	16947	194181
Number of Slice Registers	276	1223
Number of Fully Used LUT-FF pairs	166	693
Number of Block RAM	66	136
Number of BUFG/BUFGCTRLs	3	3
Total Time (ns)	2621440	65536

Fig. 9-12 shows the above results in the tabular form which explains the improvement in proposed approach over centralized approach.

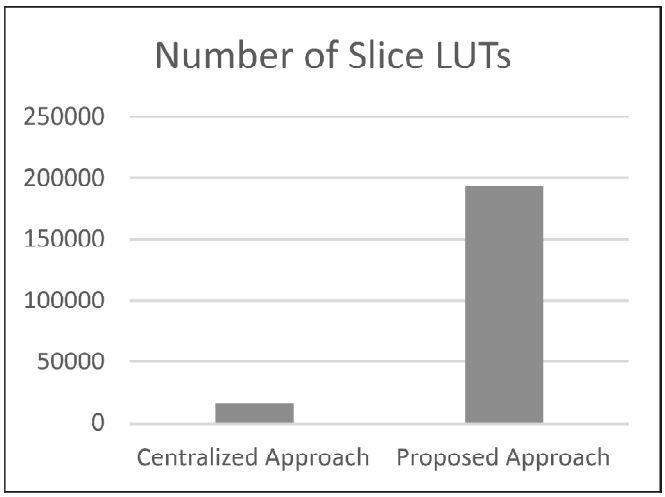


Figure 9: Slice LUTs Comparison

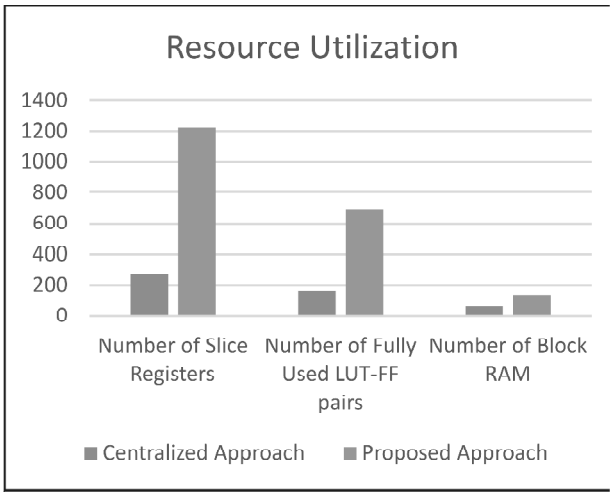


Figure 10: Resource Utilization Comparison

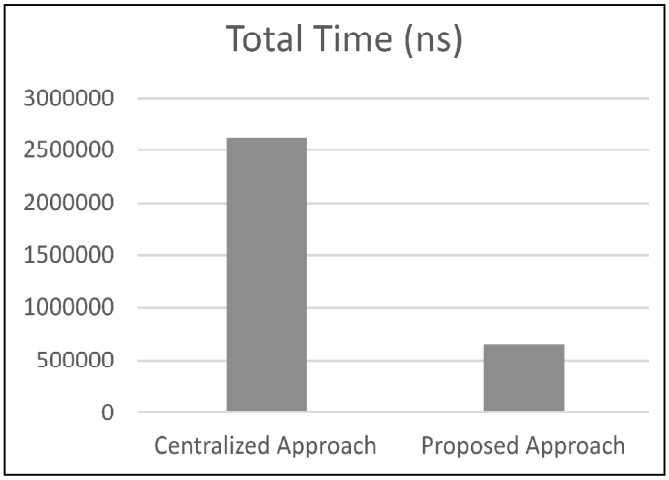


Figure 11: Total Time Comparison

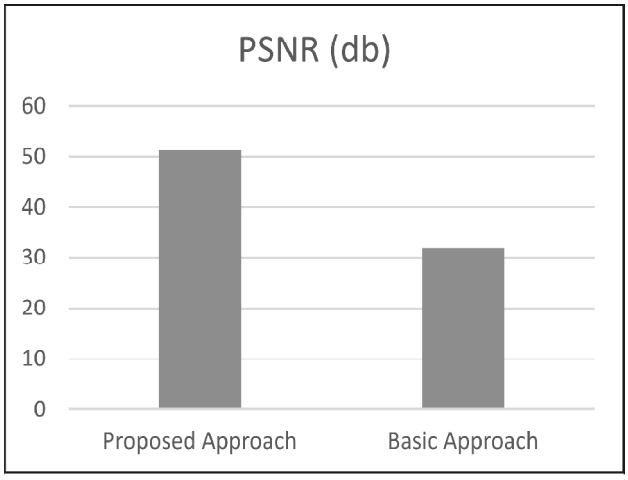


Figure 12: PSNR Comparison

ACKNOWLEDGMENT

Authors would like to thank Chandigarh Engineering College (CEC) Landran, Mohali (India) for important and timely help in research. The work we present in this paper is completely supported by CEC, Landran.

CONCLUSION

The implementation of image processing application on FPGA is an important area of research to make them fast and area efficient. The present work uses distributed approach to the implementation. In distributed approach the image is divided into 4 equal parts and can be processed in parallel. The whole system uses buffering operations in order to save the memory for saving the pixels instead it takes a pixel at a time. PSNR value for the same number of pixels comes out to be better as compared to the basic approach and the speed of operation is increased by 4 times at the cost of the number of resources of the FPGA. In future other image processing application must be implemented on FPGA and compare their results with the existing approaches.

REFERENCES

[1] Chen, Wen-Jan, Chin-Chen Chang, and T. Hoang Ngan Le. "High payload steganography mechanism using hybrid edge detector." *Expert Systems with applications* 37, no. 4 (2010): 3292-3301.

[2] Ioannidou, Anastasia, Spyros T. Halkidis, and George Stephanides. "A novel technique for image steganography based on a high payload method and edge detection." *Expert systems with applications* 39, no. 14 (2012): 11517-11524.

[3] Arora, Sneha, and SanyamAnand. "A Proposed Method for Image Steganography Using Edge Detection." *International Journal of Emerging Technology and Advanced Engineering* 3, no. 2 (2013): 296-297.

[4] Mohamed, Marghny H., and Loay M. Mohamed. "High Capacity Image Steganography Technique based on LSB Substitution Method." *Applied Mathematics & Information Sciences* 10, no. 1 (2016): 259.

[5] Kaur, Amanpreet, and SumeetKaur. "Image steganography based on hybrid edge detection and 2 k correction method." *International Journal of Engineering and Innovative Technology (IJEIT)* 1, no. 2 (2012).

[6] Charan, GundaSai, S. S. V. Nithin Kumar, B. Karthikeyan, V. Vaithiyanathan, and K. Divya Lakshmi. "A novel LSB based image steganography with multi-level encryption." In *Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on*, pp. 1-5.IEEE, 2015.

[7] Tseng, Hsien-Wen, and Hui-Shih Leng. "High-payload block-based data hiding scheme using hybrid edge detector with minimal distortion." *Image Processing, IET* 8, no. 11 (2014): 647-654.

[8] Singla, Deepali, and MamtaJuneja. "Hybrid Edge Detection-Based Image Steganography Technique for Color Images." In *Intelligent Computing, Communication and Devices*, pp. 277-280. Springer India, 2015.

[9] Al-Dmour, Hayat, and Ahmed Al-Ani. "A steganography embedding method based on edge identification and XOR coding." *Expert Systems with Applications* 46 (2016): 293-306.

[10] Mohapatra, Chandan, and ManjushaPandey. "A Review on current Methods and application of Digital image Steganography." *International Journal of Multidisciplinary Approach & Studies* 2, no. 2 (2015).

[11] Singh, Saurabh, and AshutoshDatar. "Improved Hash Based Approach for Secure Color Image Steganography using Canny Edge Detection Method."*International Journal of Computer Science and Network Security (IJCSNS)*15, no. 7 (2015): 92.

[12] Maheswari, S. Uma, and D. Jude Hemanth. "Frequency domain QR code based image steganography using Fresnelet transform." AEU-International Journal of Electronics and Communications 69, no. 2 (2015): 539-544.

[13] Hariri, Mehdi, RonakKarimi, and MasoudNosrati. "An introduction to steganography methods." World Applied Programming 1, no. 3 (2011): 191-195.

[14] Zaidan, A. A., B. B. Zaidan, Y. AlaaTaqa, M. Kanar Sami, GaziMahabubulAlam, and A. Hamid Jalab. "Novel multi-cover steganography using remote sensing image and general recursion neural cryptosystem." International Journal of Physical Sciences 5, no. 11 (2010): 1776-1786.