

A Review of Image Processing Applications Implementation on FPGA

Avdash Bhatt, Mr. Paramveer Singh Gill

M.Tech VLSI 4th SEM, Assistant Professor

Avdeshbhatt29@gmail.com, paramveer.ece@cgic.edu.in

CEC Landran, Mohali

Abstract: Digital Image processing applications on digital systems have become an important area of research in recent years. Many image processing applications have been implemented on hardware and compared with their software counterparts. Researchers have proposed many techniques for the implementation on FPGA platforms and other processing hardware. Encryption and decryption of images on images or text on images is an ever booming area of research and new techniques have been evolved for their implementation on hardware. In the present work different techniques of steganography available in the literature have been compared and the advantages and disadvantages of the same are discussed.

Keywords: Steganography, FPGA

I. INTRODUCTION

Steganography is a technique which is used to transmit a secret message under the cover of digital media such as images. Steganography is a technique of hiding information within the information or hiding one form of information into another form of information. Steganography is the art and science of secret communication [1]. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data. Steganography is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible [2]. In this scenario, before the hiding process, the sender must select the appropriate message carrier and select the effective secret messages as well as the robust password. The effective and appropriate Steganography algorithm must be selected that able to encode the message in more secure technique. Then the sender may send the Stego file by email chatting, or by other modern techniques. The Stego file is the carried message with the secret information. After receiving the message by the receiver, he can decode it using the extracting algorithm and the same password used

by the sender [3]. An effective steganography scheme should not cause any perceptible distortion and have to achieve high capacity as well. In most steganographic techniques, although only the most insignificant components are changed, many analytical techniques can reveal existence of the hidden message by detecting statistical difference between the cover and stego objects [4]. The following two measures may be taken in developing steganography schemes to combat steganalysis:

- (1) Avoid conspicuous parts when embedding messages into the cover.
- (2) Improve embedding efficiency, i.e., embed more information per modification to the cover data.

In the fields of information hiding, there is a visual requirements model, which is called magic triangle, having following requirements [5]:

1. Capacity
2. Imperceptibility.
3. Robustness.

1. Capacity:

Capacity is also known as embedding payload, and it is calculated by the number of secret bits embedded in each cover pixel. A higher capacity allows much more the secret data to be inserted into the cover image.

2. Imperceptibility

Imperceptibility is generally determined by peak signal-to-noise ratio (PSNR). The PSNR value is high, when the difference between the cover image and the stego image is small. Hence it can be said that quality of stego image is good with the imperceptibility is high.

3. Robustness

Robustness helps to protect the secret data from being attacked or stolen.

II. LITERATURE SURVEY

Chen, Wen-Janet al. [1] In this paper, High payload steganography mechanism has been presented using hybrid edge detector. The result indicated that

presented approach attains high capacity but also increases the quality 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 used for steganography. Moreover, combination of two approach produce a new steganography algorithm. The results demonstrated that proposed approach attains high peak signal to noise ratio.

Arora, Sneha et al. [3] presented a image steganography using edge detection method. The presented approach helps to hide the text data into color images and edge of an image can be detected by scanning which uses 3*3 window. The results show that proposed scheme attains high embedding capacity and high quality of encoded image.

Mohamed, Marghny H. et al. [4] proposed High Capacity Image Steganography Technique. The main goal of the presented method is to increase the embedding capacity and improve the image quality of the stego-image. The experimental results show better performance of the proposed method compared to the corresponding methods, in terms of PSNR and the capacity. The effectiveness of the model is estimated from the viewpoint of both the amount of data hidden and the image quality of the 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. This paper proposes a novel approach of encrypting the plain text into cipher text and embedding it into a color image.

Tseng, Hsien-Wen et al. [7] fuzzy logic-based algorithm has been proposed in this paper and extends the original design to block-based design. The result indicates that the proposed method attains higher payload and also having minimal distortion.

III. CONCLUSION

In this paper different image encryption techniques have been reviewed. Many researchers have proposed various techniques and compared their merits and demerits with the existing approaches. In one technique high payload steganography is proposed which shows significant improvement in the results in terms of quality of stego image. Few other

techniques use Hybrid Edge Detector for edge detection and a sliding window is used for scanning the image pixels. The techniques are compared in terms of the peak signal to noise ratio and other performance parameters. In the end hardware implementation of the technique remains a challenge and can be solved using fast and area efficient techniques.

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 Sanyam Anand. "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 Sumeet Kaur. "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, Gunda Sai, S. S. V. Nithin Kumar, B. Karthikeyan, V. Vaithyanathan, 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.