Implementation For Data Hiding Using Visual Cryptography

Ravikumar M.Raypure[1], Prof. Vinay Keswani[2]

[1] M.Tech . IInd year, Dept. of Electronic & Communication, Vidharbha Institute of Technology, Umrer, Maharashtra, India

[2] Assistant Professor, Dept. of Electronic & Communication, Vidharbha Institute of Technology, Umrer, Maharashtra, India

---***---

Abstract - *Security and safety in each place need of protection, improvement. By this reason data transferring will secure and create need of improvement when transfer data every time. Visual cryptography with boundary steganography represent GUI (Graphical User Interface) for security improvement. This techniques gives stego image for the encryption side and destego image for decryption side. MSE (Mean square error) is very less that causes efficiency of data transfer sender to receiver also in other word we called this techniques is boundary scanning or Shamir cryptography. Boundary scanning which used the n, k for stego image and destego image .Size of image normally 128*128 depend upon the data which you want to Steganograph. Shamir techniques increase the PSNR and reduces the MSE.*

***Key Words*: *boundary*, stego image, secrete, embeded**

1. INTRODUCTION

Image processing demand more security for uses in our day today life reason is only the huge number of the requirement like social media and many more. Every time, when we think on internet services first one comes in mind security this causes progress in research and development because hacker use many techniques for decode the information. Most important is one of them is image security for fast, secure and lossless data transfer to receiver.

In this paper we are approaches data hiding techniques called as boundary scanning. Digital image is use for the hide the data in such a form of edge of image but the original image taking in 128*128 size and represent GUI (graphical user interface). Encoding and decoding time reduces when the stego image and destego image. This techniques gives robust against hackers. our focus only the hiding the data in the stego image and image divide into nth number of unnoticeable image which providing the boosting of security and purpose of communication level is only transmitting the hidden data to the receiver. Embedding process, the image compression not a problem we already use original image in the form of 128*128 size .later on the extracting process recover the same image start by encoded image .Edge or boundary of image secrete data is safe and not in complicated manner physically the data can decode decimal number with ASCII code but this visualize only sender and receiver. The data in the boundary of image in cube form for each word or symbol. They can provide security improvement such as highly confidential, military, medical field etc. Important is only in this case is image because our concentrate the data hide in the boundary of image .Number of nth parts of encoded image only reconstruct or decode by kth parts. Secret data not involve with communication channel.

2. Proposed Methodology

2.1 Block Diagram of Proposed Method

In this paper we use the Shamir techniques for image encryption and decryption fig. 1 is block diagram of proposed method.

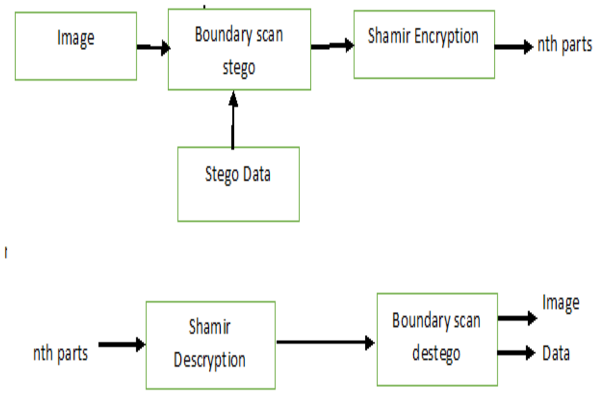


Fig -1: Block diagram of proposed method

First stage Shamir techniques is encryption original image use for the encrypted the data Boundary scanning is techniques is use for the data hide such way that cannot hackers hack the secrete data. Original image size is converted 128*128 size image or other size depends upon the size of data .For the hiding the data 128*128 image suitable for covering of data small type of data image in the form of 128*128 called as stego image .This stego image hide the data in form of boundary of image or edge. Now this encrypted form data called secrete data this place data boundary of image small square form. Secrete data encrypted ASCII form and boundary of image placed in decimal. Secret data that need to be exact parts match between two entities. Method. First read the stego image, then by preprocessed scaling convert the secrete data into stego cover image of RGB color. This Stego image is broken into number of nth parts. The compression, steganography and then encryption have best results. The main objectives of this work are to increase the security, increasing embedding capacity and lossless recovery of data. We used a stegano image divided the image into number of nth block, and embedded information. The first stage in the decryption process is the Shamir decryption stage. In the encryption process, stego image encrypted such way into nth number of parts with data hide in that image. Therefore, in the decryption process to retrieve the original image called as destego image, using n, k cryptography. n, k parts set by the sender decryption. Process nth parts recovered only when the number of kth parts should be in exact number of nth parts match and no one number is repeated this is done called destego of image. If the nth parts and kth parts repeat again the retrieved image not exact match to original image and secrete data not show. Decryption process uses the same size of image generally 128*128 we have taken in Shamir system. Decrypted image boundary show Red square form which is RGB color. Given secrete data shows red square in form of decimal number we used decode this decimal number ASCII code recovered original secrete information.

2.2 Visual cryptography System scenario Using shamir based Technique

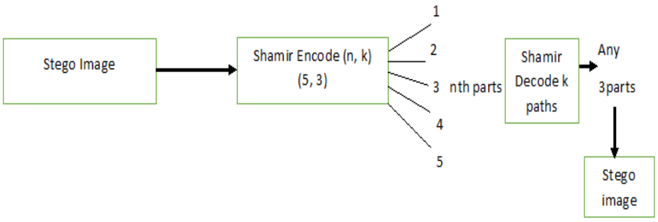


Fig -2: Visual cryptography System scenario Using shamir based Technique

In above fig. 2 stego image is divided into five parts (Shamir encode 5, 3) this five parts are unnoticeable. When decode or destego image into three parts original image and secrete data is separated. But, the encoded five parts are not repeat again for example (1-2-3-4-5) decoded parts is repeated the number one or two time (1-1-2)/ (1-3-3) in such way the image decode in unnoticeable form also the data is unavailable of that condition PNR is reduces for 11 data size 1.30dB and the 8 data size 0.50dB but effect on encoding and decoding time slightly change or same. MSE (Mean Square Error) increases 0.94458008. When the original image decode the noticeable condition that time MSE is reduces 0.00002035 and PSNR increases 93.83 for 8 and 11 size data. Below table shows noticeable and unnoticeable image.

Table -1: Noticeable and Unnoticeable image

Noticeable image	Image (n, k)	Data size	Te (Encoding Time)	Td (Decoding Time)	PSNR (dB)
	128*128(5,3)	11	6.45 s	12.21 s	93.83
	128*128(5,3)	8	8.9431s	17.5279s	93.83
Unnoticeable Image	128*128(5,3)	11	9.6672s	18.7214s	1.30
	128*128(5,3)	8	8.9431s	17.6318s	0.50

Shamir technique gives the security of data hide its possibility of image decoding is very difficult because of the hackers not all the parts hack of kth parts. The main purpose of system is not image decode by unknown authority and safely data transfer.

3. Flow Chart of Proposed Method

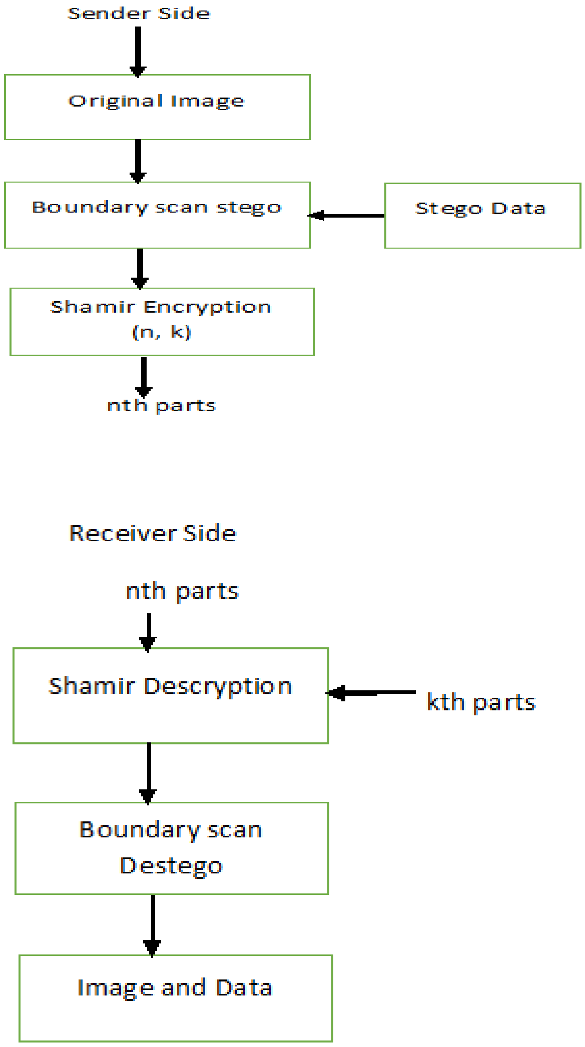
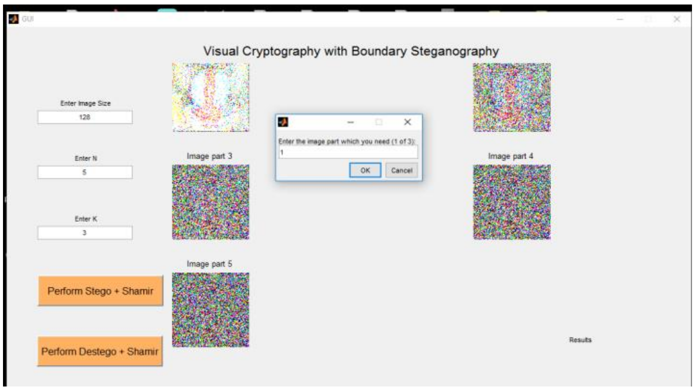


Fig -3: Flow Chart of Proposed Method

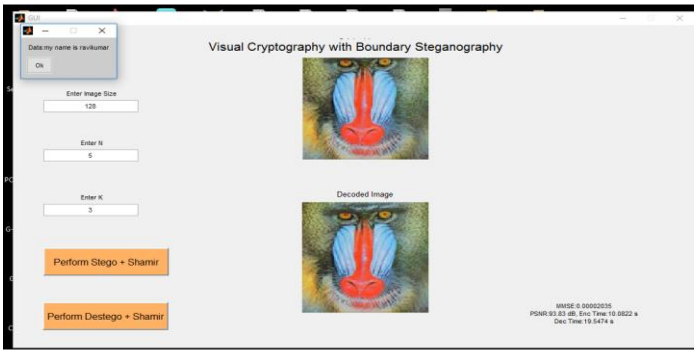
Flow chart shows the embedding and extracting the image sender side and receiver side. Stego data in the boundary of the image which is divided into nth parts and extract the receiver side image i.e. destego image by kth parts and same image found receiver. Secrete data and destego image separate from each other.

4. Simulation and Result



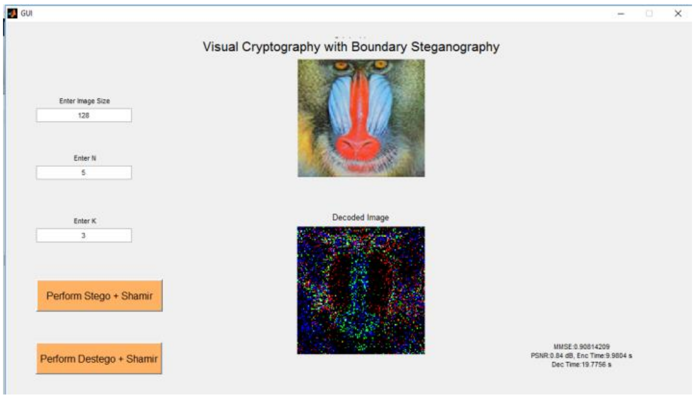
Enter Image Size: 128
Enter N: 5
Enter K: 3
Enter the image part which you need (1 of 3): 1

Fig -4: Image part 5 Baboon.jpg



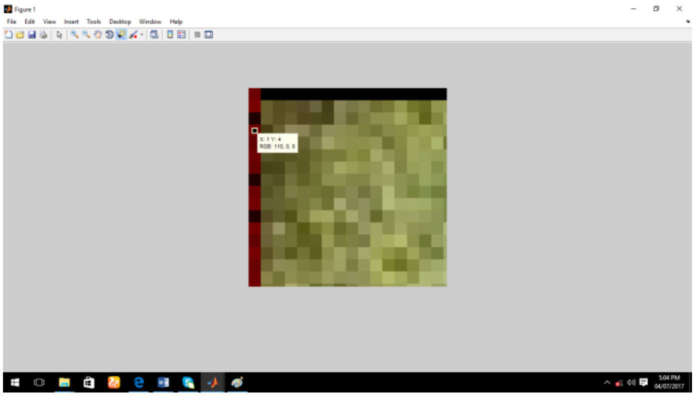
Data:my name is ravikumar
Enter Image Size: 128
Enter N: 5
Enter K: 3
MMSE:0.00002035
PSNR:93.83 dB, Enc Time:10.0822 s
Dec Time:19.5474 s

Fig -5: Image part 3 decode Baboon.jpg



Enter Image Size: 128
Enter N: 5
Enter K: 3
MMSE:0.90814209
PSNR:0.84 dB, Enc Time:9.9804 s
Dec Time:19.7756 s

Fig -6: Number repeat condition image decode unnoticeable Baboon.jpg



X: 1 Y: 4
RGB: 110, 0, 0

Fig -7: Secrete data in boundary of Baboon.jpg

5. Conclusion

In this paper, we got Shamir techniques for the data hiding in image. The original image take as 128*128 size or depend upon the size of information which we want to Steganograph. We use n, k cryptography for the data hiding and recover the data. First we can convert the image into nth parts and destego image in kth parts. Kth parts is parts from nth parts to recover the original image but kth parts similar number not repeat again otherwise decoded image not same as original one and secret data not separated from the image. In other word we use the boundary scanning techniques for the data hiding secret data is store in the edge or boundary of the image in the small square form each sentence word of secret data is separated to each other this reduces the complexity to identify the secret data but this can do only the sender and receiver only. Square form data in the boundary use RGB color but we can use only red color for the each word depend upon our size of data. We are normally identify the secret data in decimal number and this decimal number gives original data in the ASCII code. We can easily decode the decimal number using ASCII code table and actual data recover. Boundary scanning provide restriction to hackers to hack the original image because of the when increase the number of kth parts from receiver side hacker one or two parts is hack only but other parts not possible to hack. This reason the original image not decoded and this purpose our techniques provide the security improvement when the data transfer from sender to receiver. Also when encoding original image and decoding image PSNR are increases and reduces the MSE (mean square error).

6. Future Scope

We use 128*128 size image for the hiding the data and n, k cryptography to transfer the data sender to receiver this techniques gives safe transferring data but currently we performing data on image in future, we can perform processing on the videos. PSNR increases in techniques but in current system time requirement for Shamir is high we can reducing delay by using parallel processing techniques.

ACKNOWLEDGMENT

I would like to thanks my project guide Prof. Vinay Keswani (Electronics & Communication Department) whose continuous guidance and motivation helped me to achieve greater heights. I also express my gratitude to Prof. Nilesh Bodane (HOD, Electronics & Communication Department) for their constant motivation. I am also thankful to the department of Electronics Engineering, VIT for extending all the facilities for caring out this work.

References

[1] [6] M. Jiang, X. Wu, E. K. Wong, and N. Memon." Steganalysis of Boundary-based Steganography using Autoregressive Model of Digital Boundaries" Department of Electrical & Computer Engineering McMaster University Hamilton, Ontario, L8G 4K1, Canada
[2] Mrs. Bhandare Shital, Mr. Jhade Manoj, Mrs. Jadhav Angarika, "An Improved Approach for Extended Visual Cryptography Scheme for Colour Image" in International Journal of Computer Applications (0975-8887)-2011.
[3] Youssef Bassil, "A Text Steganography Method Using Pangram and Image Mediums", International Journal of Scientific & Engineering Research (IJSER), ISSN: 2229-5518, Vol. 3, No. 12, December 2012.
[4] Mr. A. Duraisamy, Mr. M. Sathiyamoorthy, Mr. S. Chandrasekar, "Protection of Privacy in Visual Cryptography Scheme Using Error Diffusion Technique" IJCSN International Journal of Computer Science and Network, Vol 2, Issue 2, April 2013.
[5] T. Rajitha, Prof P. Pradeep Kumar, V. Laxmi, "Construction of Extended Visual Cryptography Scheme for Secret Sharing" in International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 4, August 2012