Design and Implementation of Visual Cryptography System for Transmission of Secure Data

Guru Prasad M Bhat
Assistant Professor, Department of ECE
Jyothy Institute of Technology
Bengaluru, India
guruprasad.bhat@jyothyit.ac.in

Nayana G Bhat
Assistant Professor, CIIRC
Jyothy Institute of Technology
Bengaluru, India
nayana.gb@ciirc.jyothyit.ac.in

***Abstract*—** In recent period of time security of the transmitted data is most critical problem, as network technology is greatly advanced and heaps of information is transmitted via net. Visual cryptography strategy is one of the most secure technique for privacy auspices, that allow the encryption of secret image or data by transferring it into the secure percentage and such a strategy is able to recover the secret image or data. This behavior makes visual cryptography especially useful for the low computation load requirement.

In this paper, we are providing the information regarding information security by using Visual Cryptography scheme by making use of exclusive new technique of splitting of images along with their pixels rotation with the help of generated random number. We also have made an attempt to overcome some of the disadvantages of preexisting techniques of encryption and decryption.

Finally, successful transmission of the message from transmitting end to receiving end without any interception was done. Most importantly, it is very difficult to hack by use of any professional hacking techniques as the message is encrypted twice. Hence the data is highly secured under transmission path.

Keywords- *visual cryptography scheme, privacy protection, steganography*

*****

I. INTRODUCTION

Visual Cryptography scheme is used in many real-time applications such as transmitting passwords, authentication, and Information forensics and many more. The security issues pertaining to secured images has to be considered, as security hackers may find the way to unleash the image. As of recent proposed schemes, they require more rounds of communications between different phases of encryption and decryption. And if the file or hard drive is crashed, it is hard to recover. To overcome some of these demerits of pre-existing techniques, we propose to design & implement visual cryptography system for transmission of secured data to increase the security of the data by pre-and post-transmission methods of encryption and decryption, using a technique called Visual Cryptography to make it 'hack proof' by introducing the 'Rotation of images' concept, and developing circuits for the receiving end.

II. RELATED WORK

Securing data in the form of images is increasing in various real-time applications. Abhisek Parakh et. al [1] has worked on Visual Cryptography, in which two pixels are combined using Boolean functions in random way, and each share contains some information of secret image. They have shown that using image pixels, secret can be secured for further real-time applications. Shiuh-Jeng Wang et. al [2] proposed VCM watermarking with frequency-domain watermarking technique and visual cryptography, in image processing. In this proposed system, watermark is generated for embedded portion only. Himanshu Sharma, Neeraj Kumar, et. al, [3] proposed new algorithm called Cover Image Share Embedded security algorithm (CISEA), which provide better security compared to visual cryptography using watermarking techniques.

Piyush Marwaha, Paresh Marwaha [4] has used traditional cryptographic techniques to achieve data encryption and visual steganography algorithms to hide the encrypted data. Pahlavi V. Chauvin et. al, [5] proposed sharing scheme, where they have shared the secret in to group of participants, and each participant contain one share of secret.

Mrs.G.Prema, S.Natarajan [6] proposed to secure data by dividing the image into two shares based on some threshold value, to achieve this, they have used steganographic technique using Genetic Algorithm and visual Cryptography. Anil C et. Al [7] have discussed about various techniques to secure secret messages, and concluded that combination of stenography and cryptography would lead to more secure than previous techniques. Souvik Roy, P. Venkateswaran [8] have worked on text steganographic technique to encrypt the secret, as it consumes less memory and easy communication. Siddaram Shetty, Minu P Abraham, [9] generated secret shares for documents, handwritten -text, images using RSA algorithm of Public Key Cryptography.

III. PROPOSED WORK

Proposed work includes the concept of creating images for letters and numbers initially. The methodology of the proposed work is in Fig1 and Fig2.

The secret message can include numbers, alphabets and space. The input message is then split into two images individually. The split images undergo rotation at the pixel level with the help of generated random number.

 ISSN: 2321-8169
718 – 721

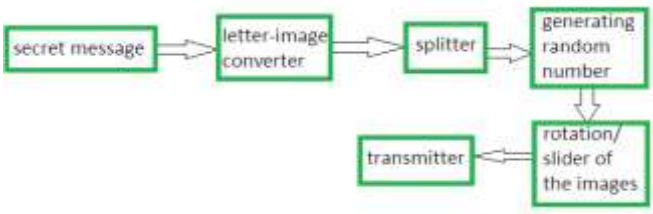

Fig 1

These rotated images along with the size of the message and random number is sent to the receiving end through email. This email message is encrypted in such a way that no interception is possible.

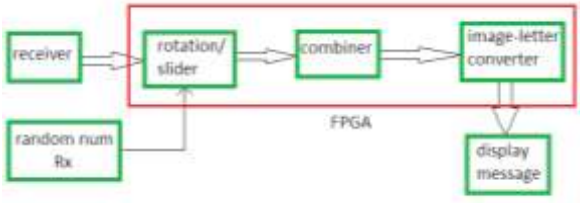

Fig 2

At the receiving end, the images are re-rotated with the help of received random number will be combined at the combiner. Then these images are converted back to the letters and will be displayed on the screen and also the message will be displayed on the MATLAB interface.

The circuits for receiving end are developed in Simulink. This is implemented using FPGA Spartan 3e, the only FPGA chip which interfaces with MATLAB function used in circuit designing.

Finally, the images will be displayed along with the message on MATLAB interface.

IV. PROPOSED METHOD

Our proposed system will be consisting of four phases as:

1. Letter to Image Conversion
2. Splitting of an image
3. Random number Generation & Rotation
4. Transmission

A. *Letter To Image Conversion:*

Before converting each letter into images, images are created for each letter and pre-assigned for those letters. Each letter typed is then compared with the pre-assigned letter and the respective image is read and displayed.

For displaying each letter in the whole message, firstly the size of the message is computed and the comparison is looped according to the size of the message.

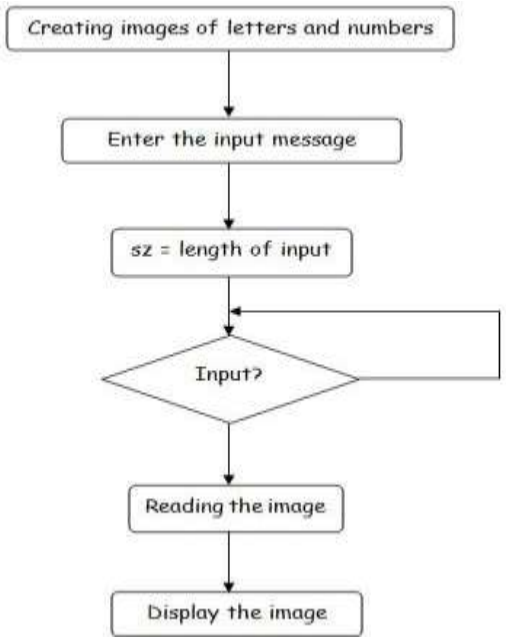

Fig 3

B. *Splitting of an image:*

Each letter converted to the respective images is split into two shares i.e., two new images are formed. One image of 16 pixels is split into two images of 16 pixels each. This

process of splitting the image manually is explained previously in chapter 4 in detail. The converted image of each letter is split into two shares according to the designed pattern. Then those two shares of an image are also displayed if required. This comes under the basic concept of visual cryptography. These steps are explained in the flowchart given in Fig 4

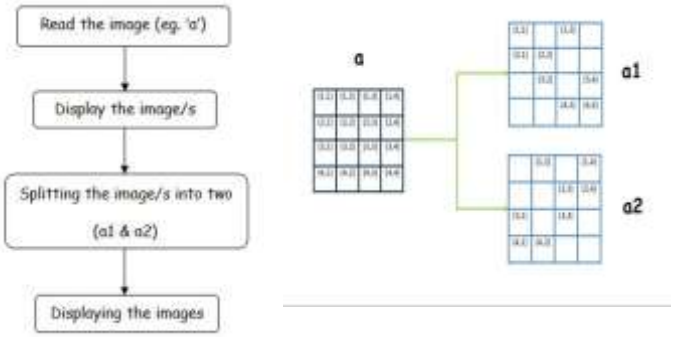

Fig 4

C. *Random number Generation & Rotation:*

The Random number generation is explicit to the process of encryption. It needs the maximum and minimum values i.e., the range in which the number has to be generated.

After the generation of Random number explicitly, the rotation of split images is carried out in MATLAB. The implementation of this stage is shown in the fig 5

The split images and the Random number are given as input almost at the same time to the Rotation block. In the rotation block the outer most pixels are rotated in anti-clockwise and the inner most pixels are rotated in clockwise.

 ISSN: 2321-8169
718 – 721

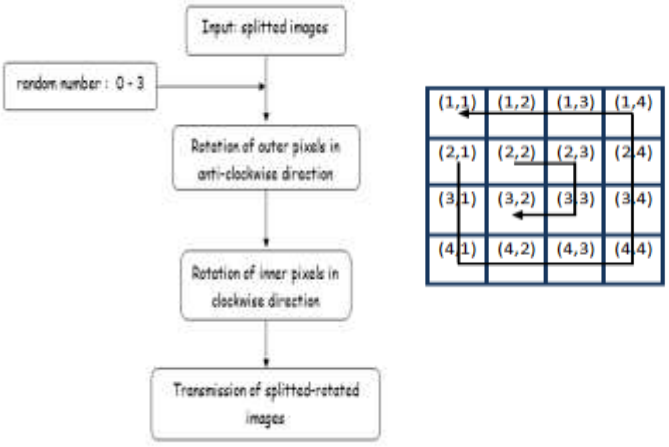

Fig 5

D. Transmission:

Once the images are rotated they need to be made ready for transmission or sending those images to the receiver end. As the images cannot be directly sent as it is, few initial preparations are need to be done, which is in fig 6

The pixels of the rotated image of the first split image are concatenated with the same for the whole message to form a single dimensional array, say 'sk'. Similarly the pixels of the rotated images of the second split image are also concatenated to form another single dimensional array, say 'sl'.

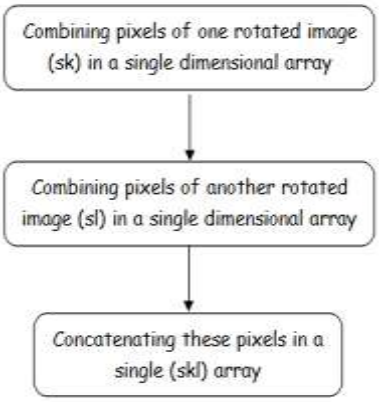

Fig 6

Both of these arrays are then concatenated into a single array, say 'skl' which will contain every pixel of the data to be sent. Now this array is sent to the receiver who needs the message through email.

Before emailing the pixels, another round of encryption is done which is readily available in MATLAB which is designed on AES technique. This process of encryption is in Fig 7

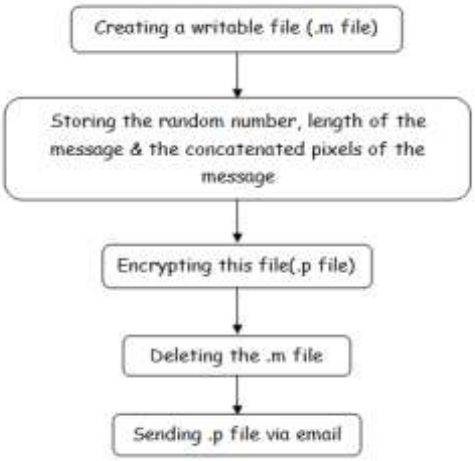

Fig 7

Initially a MATLAB file i.e., .m file is created, inside which the random number generated, the size of the input entered and the final single dimensional array containing all the pixels of the input data is written.

This .m file is then encrypted to a .p file which is a protected file built based on AES encryption technique [10]

After encryption, the .m file is deleted for more security purpose and the .p file is sent via email to the desired receiver.

V. RESULTS AND ANALYSIS

To implement the proposed scheme, using Simulink, 'mdl' file is created in which circuits for the receiver part is designed using different blocks from the library.

E. The received array of pixels is formed into its images as sent by the sender which is given as input to the MATLAB function block. Another input is the random number received. The output of the MATLAB function block is the display of the letter in the message and hence the whole message.

F. The final output using Simulink , Xilinx ISE Simulator and FPCA- Spartan 3e for the alphanumeric input 'user 123' can be viewed in the below fig 8.

Fig 8

VI. CONCLUSION AND FUTURE SCOPE

This proposed scheme is designed with Visual cryptography system specially to avoid interception along the whole transmission path. This project involves an exclusive new technique of splitting of images along with their pixels rotation with the help of generated random number.

We also have made an attempt to overcome some of the disadvantages of preexisting techniques of encryption and decryption. This scheme makes use of some concepts of AES to cover up the disadvantages of some encryption techniques. It also includes FPGA implementation for whole receiving process. The circuits for the receiving part are developed using Simulink whereas the transmission is shown with the help of MATLAB interface.

Finally, the proposed scheme successfully transmits the message from transmitting end to receiving end without any interception. Most importantly, it is very difficult to hack by use of any professional hacking techniques as the message is encrypted twice. Hence the data is highly secured under transmission path.

In this proposed scheme, 4*4 matrices are used for the easier implementation of each step. Improvisation can be made by using higher order matrices. If it is designed for higher order images or matrices it can be used for real time applications. The images which are developed in our project are only for images and alphabets. No images are created for special characters. If the images are created for all the special characters, then the input message can also include special characters in them.

REFERENCES

[1] AlfreJo De Santk, "Visual Cryptography Schemes", ITW Killarney, Ireland, 1998.

[2] Shiuh-Jeng Wang, Jian-Yi Lin, Hung-Jui Ke,et al, "Targeted Secret Disclosures in Visual-based Watermarking Concealment Systems", International Conference on Multimedia and Ubiquitous Engineering(MUE'07) 0-7695-2777-9/07, 2007.

[3] Himanshu Sharma, Neeraj Kumar, et. al, "Enhancement of security in Visual Cryptography system using Cover Image share embedded security algorithm (CISEA)" 978-1-4577-1386-611, IEEE, 2011.

[4] Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in Images", Infosys Technologies Limited, India. Second International conference on Computing, Communication and Networking Technologies, 2010.

[5] Pahlavi V. Chauvin and Dr. Mohammad Antique, "Design of Hierarchical Visual Cryptography", 978-1-4673-1719-1/12/, IEEE, 2013.

[6] Mrs.G.Prema, S.Natarajan, "An Enhanced Security Algorithm for Wireless Application using RSA and Genetic Approach", 4th ICCCNT, 2013.

[7] Anil C, Anuradha S, Arpita V, Murthy, Sridevi S, Guruprasad M. Bhat , "Securing Secret Messages: A Review", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 5, May 2016.

[8] Souvik Roy, P. Venkateswaran, "Online Payment System using Steganography and Visual Cryptography", IEEE Conference, 2014.

[9] Siddaram Shetty, Minu P Abraham,"A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Issue 4, April 2015.

[10] Vikas kumar, et. Al, "Efficient Implementation of AES", IJARCSSE , Volume 3, Issue 7, July 2013.