

Visual Cryptography

Rajkumar Kushwaha^[1] Ankit Gajakosh^[2] Prasanna More^[3] Manjusha Shelke^[4] Nilima Patil^[5]
¹Engineering Student, ²Engineering Student, ³Engineering Student, ⁴Assistant Professor, ⁵Assistant Professor
¹Computer Engineering Department,
¹K. C. College of Engineering and Management Studies and Research, Mumbai, India

Abstract : The visual cryptography scheme is an encryption technique that uses the human visual system to recover a secret image and it not require any complex calculation. However, the contrast of the recovered image could be quite low. The scheme visual cryptography is used to encrypt a secret image or text by breaking into two shares. The secret image can be recovered by stacking both the shares obtained; but we will get nothing if any share is missing. In order to take the advantage of this property, the unauthorized user can recover the secret image if the shares of secret image are passing in sequence over a network. This project approach is to encrypt generated image shares of visual cryptography using public key encryption. We apply RSA algorithm to provide the double security of the image or document. Hence, shares of secret image are not accessible for unauthorized person to make alteration. The proposed scheme provides shares that are more secure and robust against number of attacks. This scheme also provides strong security for the documents, handwritten-text, images etc. that exists in the public network.

IndexTerms - Visual Cryptography, Encryption, Decryption, Shares.

I. INTRODUCTION

Now days, File or information sharing through the internet is rapidly increase. Therefore, there is high chance for unauthorized user accessing secret file or information has been an ever existing concern for the data communication experts. Many secure and confidential data items like military maps and commercial identifications are sent over the internet. While sending secret documents (images, text etc.) over the network, the security is the measure issue, since hackers can steal secret information in weak network. Hence we are in the need of algorithm to secure are document. With the help of Visual Cryptography, the secret information can be securely sent over the internet. The proposed scheme combines the advantages of both visual cryptography as well as Public Key cryptography. Which provides the strong security to transfer the secret information in form of images, printed text and hand written material. These technique was first proposed by Moni Naor and Adi Shamir in 1994. According to them Visual Cryptography is a technique of encrypting a secret image into shares such that stacking a sufficient shares of secret image reveals the original image. Shares are usually binary images presented in transparencies. Unlike, when compared to existing traditional cryptographic methods, Visual Cryptography needs no complicated computation for recovering the secret image. The decryption method is to simply stacking the shares and view the original (secret) image that appears on the stacked shares. It uses the human visual system for decryption. The shares of Visual Cryptography exist in their normal form during transmission in sequence over the network. However, hackers cannot predict secret information with only one share, but there is a chance of recovering the secret image if hackers are able to collect all the shares that are passing in sequence over the network. Due to same reason we have used both Public Key Cryptography and Visual Cryptography so that even if hackers are able to get all the shares but they cannot retrieve the original secret without the access of private key.

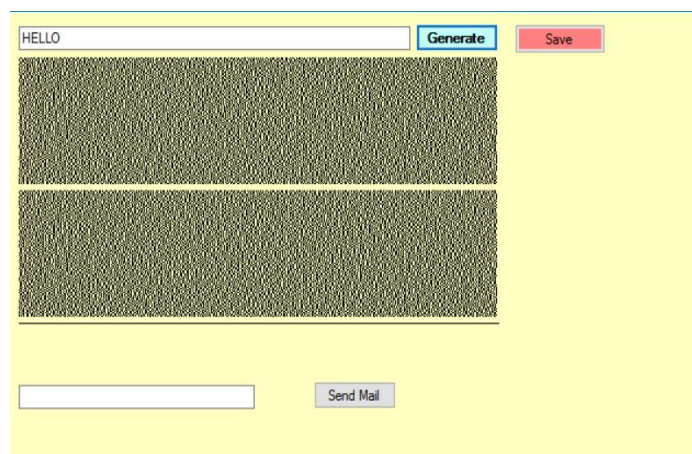


Fig:- Encrypted text



Fig:- Decrypted text

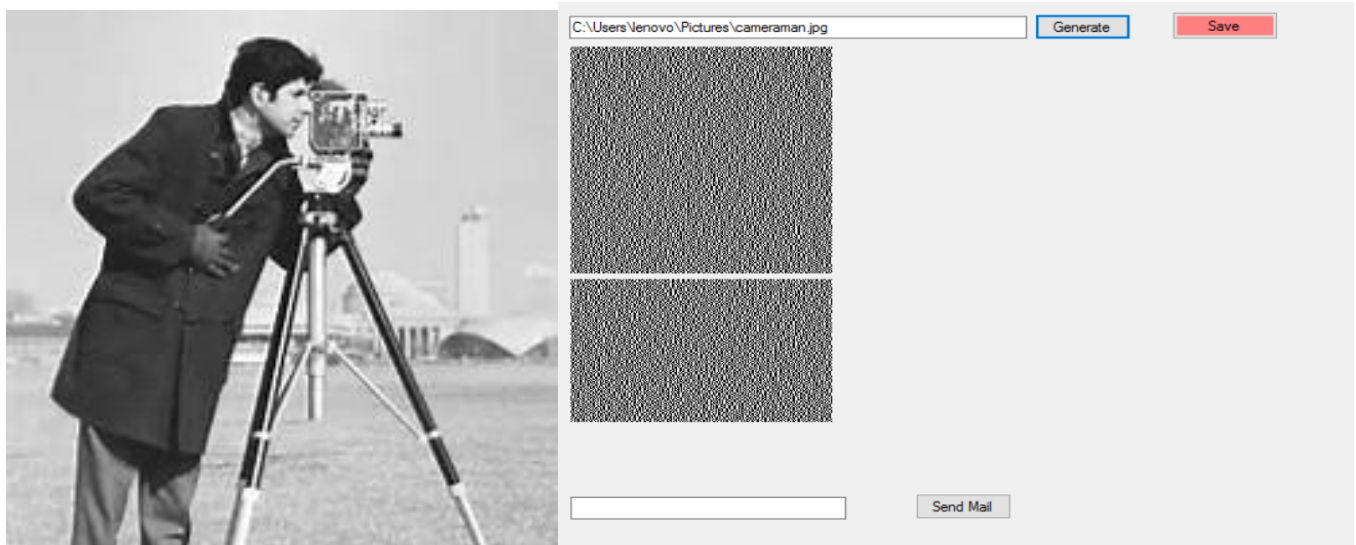


Fig:- Original image

Fig:- Encrypted image



Fig:- Decrypted image

II. LITERATURE SURVEY

1. In 2012, Mr. John Justin.M and Alagendran.B and Mr. Manimurugan.S.

A Survey on Various Visual Secret Sharing Schemes with an Application: different kinds of encryption and decryption techniques with the aim of the experimental study of implementations of various available visual secret sharing techniques and its study extends to an application of the visual secret sharing scheme that embeds an extra confidential image with key pair structure with no pixel expansion and everyday .

2. In 2016, Miss A.A Naphade and Dr.R.N.khobaragade and Dr.V.M.Thakare

In their article Survey on multiple share image using random grid and XOR-based Visual Cryptography :In this Techniques develops Visual Cryptography is a new technique for protect the visual information like picture, text etc. In the process of Visual Cryptography the images are divided into two encoded image called shares. These shares are distributed among the several people and their encryption can be done by decrypting them by overlapping the shares to get original image. At first there are various measures on which performance of visual cryptography schemes depends, such as pixel expansion, visual quality, image quality, contrast, security, quality of shares, size, computational complexity.

3. In2016,Akashatha A shenoy, Jaipriya k,Pooja

In their article Survey on Secured encryption and decryption for image transformation using Visual Cryptography: in this image are divided in two shares and then transfer the share to the other user and the other user decrypt the image by performing the XOR operation into received shares after the performing the operation user get the original image.

III. SYSTEM DESIGN

The proposed scheme generates the shares of Visual Cryptography using basic Visual cryptography method but hackers can generate original image if shares are transmitted on internet in sequence. Hence we encrypt the shares generated using RSA algorithm, so that if hackers get all the shares they cannot generate original image without public key.

1. Generating the Shares of Secret Image: In this phase implementation of Visual Cryptography is done. It involves dividing the shares into two parts. First the secret image is converted into binary image by using Floyd-Steinberg algorithm. Then each pixel is divided into eight pixel four in each shares.

2 . Encrypting the generated Shares: In these stage shares generated is encrypted using RSA algorithm. First the keys are generated and then each shares is encrypted using public key.

3.Decrypting the Shares using RSA: At the receiver side decryption is done. Participants at receiver side uses RSA decryption algorithm for getting back original shares which were encrypted at sender side.

4.Visual Cryptography decryption: In these stage actual decryption of visual cryptography is performed. Here by applying the binary XOR operation, on both decrypted shares, we are going to get back the original secret image.

IV. IMPLEMENTATION

A. PROCESS OF THE ENCRYPTION

1. Select the image or enter the text.
2. Apply Floyd-Steinberg Dithering on secret image and generate the share.
3. Apply RSA algorithm on the generated share.
4. Send the shares generated and private key to participants.

B. PROCESS OF THE DECRYPTION

1. Enter the private key received.
2. Select the both the share you received or take the print of both the shares.
3. Put the both the paper together or use XOR method to get the original image.

V. CONCLUSION

Providing much security to the secret data that is shared in day to day life is one of the important issues in real life. In the scheme of Visual cryptography, we can decrypt the secret images without need of cryptographic computations. The proposed scheme is more secure and it is very easy to implement with low computation cost. In this proposed scheme, very first the secret image is taken and then it is divided into shares after converting it into binary image, next the shares of binary image are encrypted and decrypted by using RSA algorithm, because of this even if the unauthorized person, once getting all the shares, he/she can't get back the original secret image without availability of the private key. We can implement this type of system in various fields like

Military, Defence, and other places where the confidentiality of the data is must. We can notice that there are many future extensions exist as the visual quality and size of the retrieved image.

VI. REFERENCES

- i. Multiple share images using random grids and XOR-Based visual cryptography Miss A. A. Naphade, Dr.R.N.khobaragade,Dr.V.M.Thakare (NCRTCSIT-2016) IOSR Journal of Computer Engineering (IOSRJCE)
- ii. A Secure Visual Cryptography Scheme for Sharing Secret Image using RSA Siddaram Shetty¹, Minu P Abraham² PG Scholar, Dept. of CSE, NMAMIT, Nitte, Udupi, Karnataka, India¹ Asst. Professor, Dept. of CSE, NMAMIT, Nitte, Udupi, Karnataka, India² April 2015 International Journal of Innovative Research in Computer and Communication Engineering Nidhi "Image Processing and Object Detection" International Journal of Applied Research ,2015
- iii. Visual Cryptography Scheme for Secret Image Retrieval M. Sukumar Reddy[†], S. Murali Mohan June 2014 IJCSNS International Journal of Computer Science and Network Security, VOL.14 No.6
- iv. A Survey on Various Visual Secret Sharing Schemes with an Application John Justin.M Alagendran.B Manimurugan.S March 2012 International Journal of Computer Applications (0975 – 8887) Volume 41– No.1
- v. Digital Image Encryption Based on RSA Algorithm Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834,pISSN: 2278-8735.Volume 9, Issue 1, Ver. IV (Jan. 2014), PP 69-73
- vi. www.wikipedia.org
- vii. www.ieeeexplore.com

