**I J C T A**, 9(16), 2016, pp. 8341-8347
© International Science Press

# Secret sharing of message using grey scale images

**Niharika Prajapati* and G. Sujatha****

**ABSTRACT**

The E-mail is the most popular program on the internet and different users exchange the messages . The visual cryptography scheme is very secure method that encrypts the message or an image by breaking it into the shares first. In Secret sharing of message using grey scale images, the message which needs to be send is first converted into grey scale image. Then (3, 3) visual cryptographic shares are created from that grey scale image . Public key encryption is used to encrypt the shares. By using public key cryptography the secret shares are more secure because those shares are protected from malicious user. The scheme is more secure, the secret shares that are vigorous against a number of attacks and the system provides the security for text, image and other document over the network. One out the three VC share is send to the server and other is send to the recipient's mail box. The shares are transmitted through 2 different medium so the man in the middle attack is not possible. If the malicious user has one of the three shares then he has no information about the message . at the receiver's side all the shares fetched, decrypted and stacked to generate the grey scale image and from that image message can be reconstructed.

***Keyword:*** Visual cryptography, VC Shares, grey scale image, Public key encryption, encrypt/decrypt, man in the middle attack.

## 1. INTRODUCTION

It is age of information, information sharing and transfer has increased .The threat of an intruder to access the secret data has been a concern for communication experts. With the rapid growth of network topology, multimedia information is transmitted over the network suitably . Various confidential information such as protected health information, personal information, business confidential information and military maps are transmitted over the network. The proposed approach combines both visual cryptography and public key cryptography. This scheme increase the security of VC shares by encrypting with Public Key Cryptography [11][12] which provides the extreme security to the transfer of secret information in form of images, printed text The technique was proposed by Moni Naor and Adi Shamir [6] in 1994 According to them Visual Cryptography is a method of encrypting a secret image into shares such that stacking a sufficient number of shares reveals the secret image. The idea of (3,3) Visual Cryptography is to split secret 'a' into 3 pieces called shares. VC shares exist in their actual form during the transmission over network. Although, directly unauthorized person cannot guess the secret message with any share, but there are chances of retrieval if hackers are able to collect all the shares passing in sequence over the network. Therefore to clear out this problem, we need to enhance the security of shares. For this purpose we are using Public Key Cryptography with Visual Cryptography so that even if hackers are able to get all the shares but they will unable to retrieve the original secret without the access of private key and the shares are transmitted through different mediums. If an adversary has only one out of the three shares, then he has no information about the secret message. The shares are encrypted using public cryptography. One of the shares is send to a

* Student, Information security and cyber forensics, Department of information Technology, SRM University, Chennai, India, *Email: niharikaprajapati92@gmail.com*

** Information security and cyber forensics, Department of information Technology, SRM University, Chennai, India, *Email: sujatha.g@ktr.srmuniv.ac.in*

server and the other share is send to the recipient's mail box. The three shares are transmitted through two different transmission medium. If an adversary has only one out of the three shares, then he has no information about the message. At the receiver side the shares are fetched (one from the server and the other from the mail box), decrypted and stacked to generate the grey scale image. From the grey scale image the message is reconstructed.

## 2. RELATED WORK

Various researches have been carried out to increase the security in this area & visual quality of the secret image. Some of them are as follows:

1) Pei-Fang Tsai, Ming-Shi Wang presented a paper on (3, 3)-Visual Secret Sharing Scheme for Hiding Three Secret Data. In this paper authors proposes an improved (3, 3)-visual secret sharing scheme, which uses three shares to embed three secret messages and improve security. First, the first main share image is develop randomly and other two share images are based on the first share image and the two coding tables are also designed in this paper.

   Figure 1 and 2 shows the proposed encoding process. The share A and share Temp are generated from the three secret messages that are passed through the first coding process .From the share temp share B and C are generated in second coding process. Share A, share B, and share C are transmitted. Share B and share C are logic XORed to create a temporal image-share Temp after getting the three shares for decoding process.

2) Sandeep Katta proposed a method Visual Secret Sharing Scheme using Grayscale Images. First of all each pixel value in a grey scale block is transformed into binary representation in this proposed approach. Go for different combination of each binary block and try to design the block into different shares.

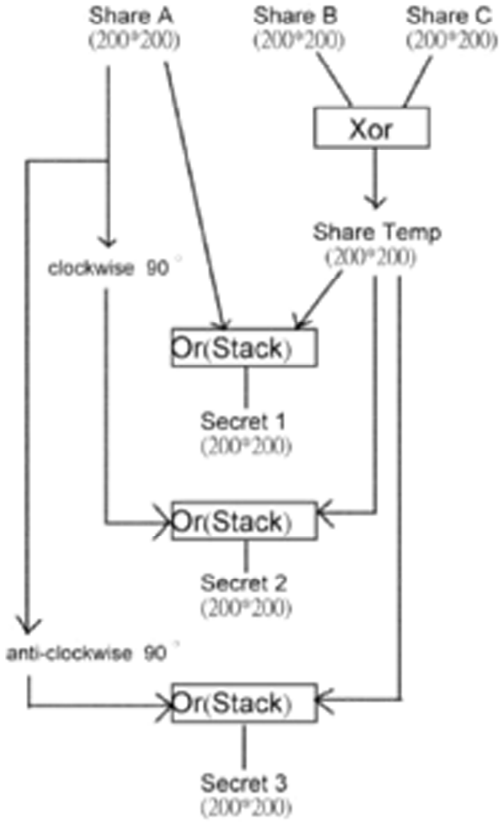


**Figure 1:**

3) B. Padhmavati, P. Nirmal Kumar, M. A. Dorai Rangaswamy [2] generated shares first by Visual Cryptography VC (2, 2) scheme. With the help of watermarking both the share were embedded into cover images. To extract the shares from the embedded images and to reveal the secret message, the extraction process was used. At last both shares were overlapped and revealed the secret image.

4) Ujjwal Chakraborty et al [13] proposed two schemes for (2, 2) and (2, 3) visual cryptographic encryption. The first scheme generates 4 output pixels in each share and considers 4 pixels of input image at a time. The second scheme generates 3 output pixel in each share and considers 2 pixels (1 block) of input image at a time. The dimension of revealed image is increased by 1.5 times in horizontal direction and remains same in vertical direction.

5) P. S. Revenkar, Anisa Anjum and W. Z Gandhare [15] evaluated the performance of various Visual Cryptographic Schemes, which help in choice of best scheme according to the available bandwidth or color of secret image or level of security required.

   Following parameters have been used to evaluate the performance:

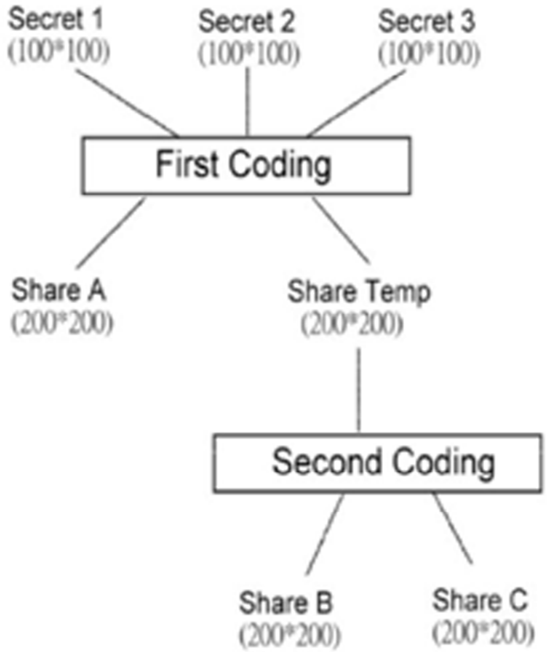


**Figure 2:**

   No. of Secret images

   Pixel Expansion Image Format

   Type of shares generated

6) Pretty Good Privacy (PGP)[3] is a popular program used to encrypt and decrypt e-mail over the Internet. It used to send an encrypted digital signature that verifies receiver’s and the sender’s identity and know that the message was not changed route. PGP[1] messages are encapsulated in packets. A PGP packet has two section one is header and a data section. The header holds information such as the packet type and length, among other things. The data section contains the payload of the packet, which is dependent on the packet type.

A random “session-key” K is generated, encrypted with the recipient’s public key pk, and encapsulated in a public-key encrypted session key packet(PKESKP). The output can be represented as follows:

<PKESKP HEADER, Epk(K)>:

Message M is encapsulated in a literal data packet (LDP), resulting in:

LDP = <LP HEADER, M>:

The LDP is compressed using the deflate algorithm [4], and becomes the payload of a compressed data packet (CDP):

CDP = <CP HEADER, DEFLATE(LDP)>:

The CDP is encrypted with a symmetric-key encryption algorithm (i.e., block cipher) and key K, using cipher feedback (CFB) mode (described below). This gives ciphertext C1, C2, C3, . . . The ciphertext is encapsulated in a symmetrically encrypted data packet (SEDP) as follows:

<SEDP HEADER, C1, C2, C3, . . .>:

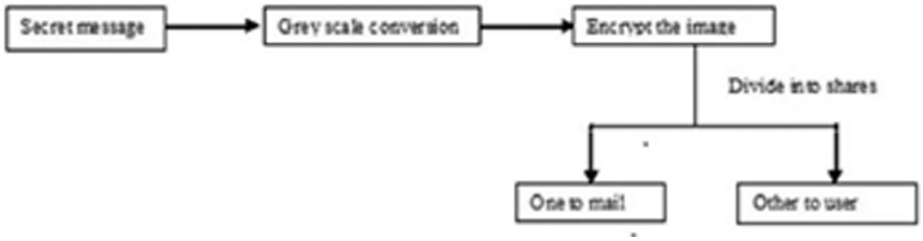
The following message is sent to the recipient:

<PKESKP HEADER, Epk(K)><SEDP HEADER,
C1, C2, C3, . . .>:

## 3. PROPOSED SYSTEM

The proposed scheme generates the VC shares using Visual Cryptography and then encrypt both shares using Public Key Cryptography so that the secret shares will be more secure and shares are protected from the malicious user who may alter the bit sequences to create the fake shares. During the decryption phase, secret shares are extracted by decryption algorithm & stacked to reveal the secret image.

**Sender's side:**



**Receiver's side:**

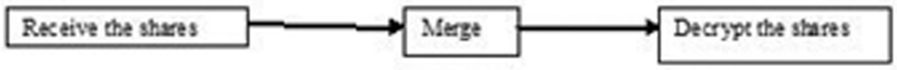


**Figure 3: Methodology of proposed syste**

Complete scheme is divided into following four steps:

### A. Encrypting the generated Shares

This is the first phase of our approach in which the image generated will encrypt. We are using public key encryption in this step. First we generate the key and then perform the encryption. Encrypted shares are the result of this phase.

### B. Generating shares of secret image:

First of all each pixel value in a grayscale block is transformed into binary representation. For example take a grayscale block and transform into binary block.

$$\begin{matrix} 111 & 159 & 20 \\ 254 & 10 & 198 \\ 40 & 215 & 100 \end{matrix}$$

Its corresponding binary blocks are as follow 01101111 10011111 00010100 11111110 00001010 11000110 00101000 11010111 01100100

Take each binary block and go for different possible combinations of that block, and design the block into different shares. For example take a binary block

254[1 1 1 1 1 1 1 0]

and divide it into shares.

Share 1 = 1 1 1 1

Share 2 = 1 1 1 0

1 1 1 1 1 1 1 0 = 254

Combining the two shares will give the exact bit and by doing the same procedure for the whole grayscale block gives the perfect high quality image when reconstructed without any loss of contrast.

**Image-conversion**

**Input:** .jpg image/.bmp image/.png image

**Output:** BIN_IMG IMG=read ()

BIN_IMG=Convert_to_binary (IMG) [R_size C_size]=Cal_size (BIN_IMG)

Image Conversion

**Share_generation**

**Input:** BIN_IMG, R_size, C_size

**Output:** SHARE1

```
SHARE2
For i=1 TO R_size
Do
For j=1 TO C_size
Do
Pix_enc_scheme=Rand_select()
SHARE1=Pix_enc_scheme(BIN_IMG(i,j))
SHARE 2=Pix_enc_scheme(BIN_IMG(I,j))
Done
Done
```

Share Generation

**C. Transmission of Shares**

One share is send to the recipient’s mail box and the second share is send to server. The two shares are transmitted through two different transmission medium so man in the middle attack is not possible. If an adversary has only one out of the two shares, then he has absolutely no information about the message.

### D. Decryption of Shares

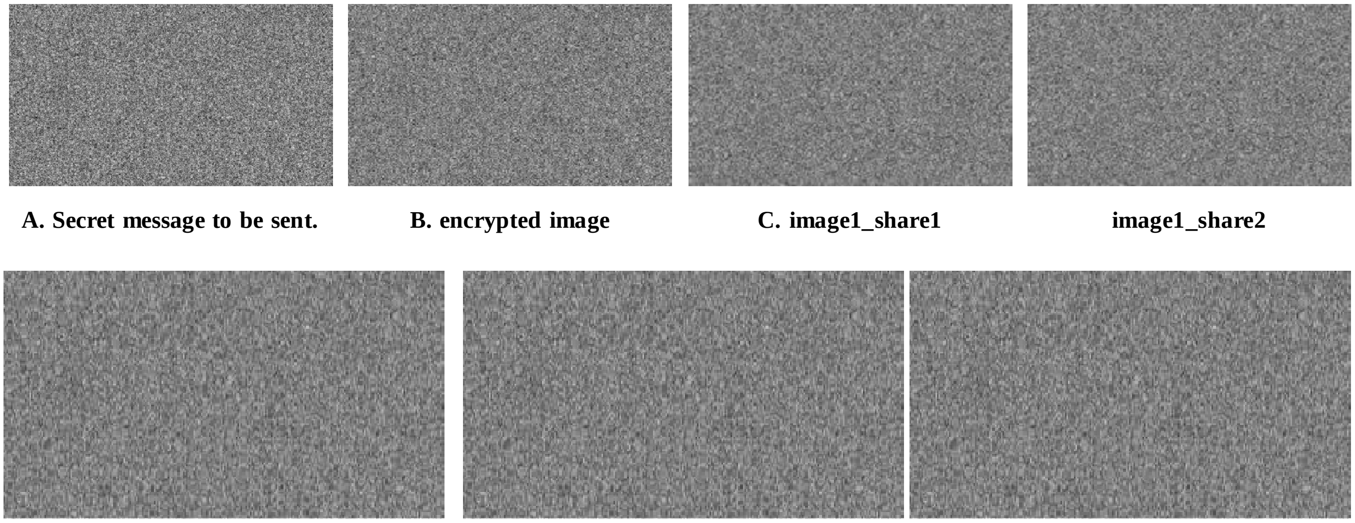
At the receiver side the two shares are fetched one from the server and the other from the mail box. After that the two shares are stacked to generate the grey scale image. From the grey scale image the message is reconstructed.

## 4. EXPERIMENTAL RESULT

Proposed scheme has been implemented in ECLIPS. To run this scheme minimum hardware configuration is required with no extra specifications. The experiments have been run in Windows 7 on a Sony VAIO laptop with Intel i3. Number of experiment has been conducted to test the performance of this scheme with different image sizes and types.

Result of some experiment is shown in figure 4.1

ABCMDFKJHKH



**A. Secret message to be sent.** **B. encrypted image** **C. image1_share1** **image1_share2**

**image1_share3** **D.image1_decrypted _share1** **image1_decrypted_share2**

**Figure 4: Experiment 1**

image1_decrypted_share3

ABCMDFKJHKH

### E. revealed image from decrypted shares

## 5. CONCLUSION

We have tested this scheme on different types of input images with change in size of the image and keys. But the entire time secret image is retrieved with good visual quality. The confidentiality of shares is also tested by super imposing the encrypted shares before reaching to the destination. In all the cases it has been observed that if any intruder will be successful to get the encrypted shares from network, he or she cannot retrieve the original secret image without availability of private key.

## REFERENCES

[1] Kahil Jallad1 and Jonathan Katz and Jena J. Lee and Bruce Schneier *Implementation of Chosen-Ciphertext Attacks against PGP and GnuPG*, International Journal of Computer Science and Network Security.

[2] B. Padhmavati, P. Nirmal Kumar, M. A. Dorai Rangaswamy “A Novel Scheme for Mutual Authentication and Cheating Prevention in Visual Cryptography Using Image Processing”. Department of Computer Science & Engineering, Easwari Engineering College, Chennai, DOI: 02, ACS.2010.01.264, 2010 *ACEEE*.

[3] P Zimmerman, *The Official PGP User's Guide*, MIT Press, 1995.

[4] Sandeep Katta, *Visual Secret Sharing Scheme using Grayscale Images*, Department of Computer Science, Oklahoma State University Stillwater, OK 74078.

[5] Secure mail using visual cryptography 5th ICCCNT 2014 July 11- 13, 2014, Hefei, China

[6] M. Naor and A. Shamir "Visual Cryptography". Advances in Cryptology EUROCRYPT '94. Lecture Notes in Computer Science, (950):1–12,1995.

[7] Securing visual cryptographic shares using public key encryption 978-1-4673-4529-3/12/$31.00_c 2012 IEEE

[8] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S. "An overview of visual cryptography" *International Journal of Computational Intelligence Techniques*, ISSN: 0976–0466 & E-ISSN: 0976– 0474Volume 1, Issue 1, 2010, pp. 32-37

[9] William Stallings, *Cryptography and Network Security*, Pearson Education Inc publishing as Prentice Hall.

[10] Secret Image / Message Transmission through Meaningful Shares using (2, 2) Visual Cryptography IEEE-International Conference on Recent Trends in Information Technology, ICRTIT 2011 MIT, Anna University, Chennai. June 3-5, 2011

[11] Behrouz A. Forouzon, "Cryptography & Network Security" 4th Edition.

[12] http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html

[13] Ujjwal Chakraborty et al, "Design and Implementation of a (2, 2) and a (2, 3) Visual Cryptographic scheme" International conference [ACCTA-2010], vol.1 issue 2, 3, 4, pp. 128-134.

[14] P. S. Revenkar, Anisa Anjum, W. Z. Gandhare "Survey of Visual Cryptographic Schemes". *International Journal of Security and Its Applications* Vol. 4, No. 2, April, 2010.