# Public Key Encryption in Visual Cryptography

Sarita K.[1], Nilashree W.[2]
Department of Electronics & Telecommunication
Navi Mumbai, Maharashtra, India

***Abstract*—The visual cryptography scheme is a secured method of encrypting a secret document or image by breaking it into shares. A typical property of visual cryptography scheme is that one can visually decode the secret image by superimposing shares without computation. Third person can easily retrieve the secret image by taking the advantage of this property if shares are passing in sequence over the network. In this project visual cryptographically generated image shares are obtained and Public Key Encryption is used. RSA algorithm is used for encryption and decryption so that it will provide security of secret document or image. The scheme provides more secure secret shares that are tough against a number of attacks. This method of visual cryptography will be providing a strong security for the handwritten text, images and printed documents over the public network.**

***Keywords*—Visual cryptography; security;encryption; decryption; shares***

## I. INTRODUCTION

Nowadays information sharing and transfer has increased rapidly. With advance technology, multimedia data is transmitted over the internet easily. Various data such as military maps and commercial identification are transmitted over the internet. Security has become an inseparable issue as information technology is ruling the world now. To solve security problems of secret images, we should develop some secure algorithm by which we can transfer data over the internet securely. With the help of visual cryptography, visual information (pictures) can be more secure over the internet.

Visual cryptography is technology which allows visual information (for example printed text, handwritten notes and picture) to be encrypted in such ways that the decryption can be performed by the human visual system without utilize computers [1]. Visual cryptography is introduced by first in 1994 Noar and Shamir [2]. In this method original image is breaking up into n shares and if someone has all n shares could decrypt the image by over laying each of the shares over each other. In their technique n-1 shares could not reveals information about original image. Shares are binary images presented in transparencies. Original image can be recovered bystacking sufficient number of shares. Visual Cryptographic(VC) technique is being used for secretly transfer of images in army, hand written documents, financial documents, text images, internet- voting etc.

VC shares are transmitted in actual form over network. It is not possible for third person to retrieve information with single share but if hackers are able to collect all shares over the network then there is possibility of retrieval. To overcome this issue and enhance the security of shares we have used public key cryptography in addition to visual cryptography, to prevent hackers to retrieve original secret without private key.

The basic model of visual cryptography proposed by Naor and Shamir [2] accepts binary image 'I' as secret image, which is divided into 'n' number of shares. Each pixel of image 'I' is represented by 'm' sub pixels in each of the 'n' shared images.

The resulting structure of each shared image is described by Boolean matrix 'S' Where S= [$S_{ij}$ ] an [n x m] matrix $S_{ij}$ =1 if the jth sub pixel in the ith share is black $S_{ij}$ =0 if the $j^{th}$ sub pixel in the $i^{th}$ share is white. When the shares are stacked together secret image can be seen but the size is increased by 'm' times.

The proposed method combines visual cryptography and public key cryptography. This method enhances the security of visual cryptography shares by encrypting with public key [3], which provides the better security to the transfer of secret information in form of images, text and hand written material.

## II. REVIEW OF RELATED TOPICS

To enhance the security and visual quality of secret image, different methods have been used. Different types of visual cryptography schemes and the theoretical information about visual cryptography established byNeeima G. et al. [4].

Chandramathi S. et al. [5] provided an overview of visual cryptography in 2010. They concluded from the overview of all visual cryptography that with increasing security, expansion and number of shares is increasing but that affects the resolution of image. To increase security, researchers should focus on quality of reconstructed image with minimum pixel expansion.

A novel visual cryptography scheme is suggested by Debashis Jena et al. [1]. They implemented Data Hiding in Halftone images using Conjugate Ordered Dithering (DHHCOD) algorithm. They used this algorithm for generating the shares. Generated halftone image of cover image was the first share. Some noise added to secret image and converted into binary image that was second share. Revealed image is simple AND operation of share 1 and share 2.

YogeshBani et al. [6] suggested watermarking approach for visual photography and they used Data Hiding by Conjugate Error Diffusion (DHCED) algorithm. Two shares has been generated and then embedded into cover image by using watermarking. After overlapping of share 1 and share

2, secret image and cover image has been revealed. Cover image require extra storage space.

B. Padmavathi et al. [7] proposed a novel scheme for mutual authentication and cheating prevention in visual cryptography using image processing. They generated shares using visual cryptography (2, 2) scheme. This scheme provides authentication for VC shares and also makes these shares invisible by embedding them into cover images. Extraction process was used to extract shares from embedded images. Secret image revealed by overlapped both shares. In this method two cover images have been used to hide the shares which require extra memory space.

Design and implementation of a (2, 2) and a (2, 3) visual cryptographic scheme proposed by UjjwalChoudhary et al. [8]. In (2, 2) scheme, they considered 4 pixels of input image at a time and generated 4 output pixels in each share. In (2, 3) scheme, considered 2 pixels 2 pixels of input image at a time and generated 3 output pixels in each share. Then the revealed image dimension is increased by 1.5 times in horizontal direction and in vertical direction remains same.

Wei-Qi-Yan et al. [9] suggested visual cryptography for print and scan applications. They provided solution for superimposition of two shares and employed the Walsh transform to embed marks in both of shares to find the alignment position of these shares. Without exact alignment retrieval is not possible.

Shyamalendukandar et al. [10] proposed k-n secret sharing visual cryptography scheme for color image using random sequence. They divided image into n number of shares. Image reconstructed using k shares. If k numbers of shares are used then remaining shares are n-k. If certain position of pixel in an image is 1, then in (n-k) +1 is number of shares of that pixel in that position will be 1. In that position of pixel remaining shares will be 0. For identify those (n-k) +1 number of shares, random number generator is used. Secret image can be retrieve Secret is not properly hidden if someone is able to get information about randomness.

Mizuho Nakajima et al. [11] proposed extended visual cryptography for natural images. This system has been taken three pictures as an input. One picture is secret image and remaining two for encryption. During encryption in determining the arrangement of transparent sub pixels on two images according to pixel transparencies, t1, t2 and tT. Transparency of secret image is tT. Printing two images on transparencies and stacking them together, secret image is generated. The problem of this method poor quality of reconstructed image and network overloaded due to two extra images.

An improved pixel sieve method for visual cryptography suggested by VaibhavChoudhary et al. [12]. They used additional sieve to generate shares. Using these scheme secret is hidden properly but result of retrieval image have not been shown in this paper.

P. S. Revenkar et al. [13] developed survey of visual cryptography schemes. They evaluated the performance of various visual cryptography schemes according to the available bandwidth or color of secret image or level of security required. To evaluate the performance of schemes have been used following parameters-

- No of secret image
- Pixel expansion
- type of shares generated
- Image format

In some cases cover images are used which is an extra overloaded on network.

## III. PROPOSED SCHEME

Proposed scheme is divided into 4 phases. Figure1 shows the methodology of proposed scheme.

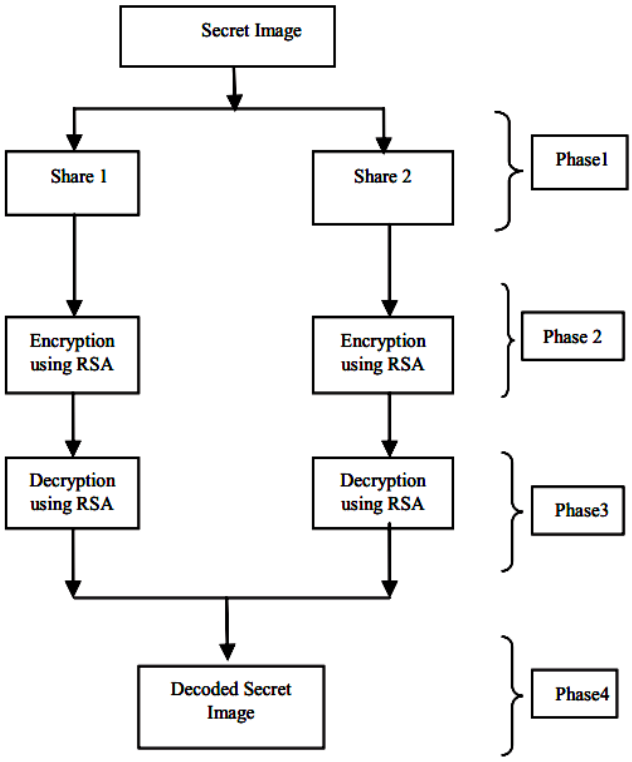


Fig.1 Methodology of proposed scheme [8]

In proposed scheme, visual cryptography shares are generated using basic visual cryptography model. Then encryption of VC shares is performed using RSA algorithm of public key cryptography. During the decryption, secret shares are extracted using RSA algorithm and stacked the shares to reveal the secret image.

PHASE-1. This is first phase of our method. Shares of secret image are generated. Visual cryptography (2, 2) scheme[7][8][2] is used to generate shares from secret image. The secret image is converted into binary image then each pixel of secret image is divided into 8 sub pixel, 4 pixels for each share by selecting the random pixel encoding scheme. Pixel encoding scheme is given in Figure2.

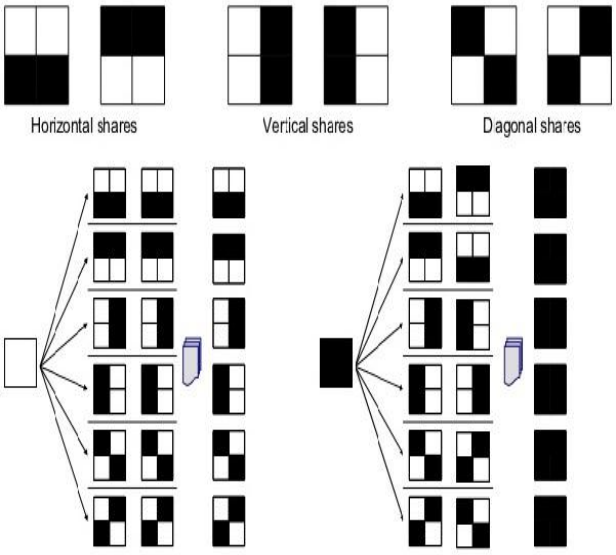


Fig.2 Pixel encoding schemes [2][14]

PHASE-2.This is second phase of our method. Generated shares are encrypted. Shares generated from the first phase are encrypted using RSA algorithm. First the key for RSA is generated then the encryption is performed. Output of this phase is encrypted shares.

PHASE-3.Shares are decrypted using RSA. At the destination, this process will take place. Output of this phase is decrypted shares.

PHASE-4. This is last phase of our method. We have decoded original secret image by applying simple binary XOR operation on both decrypted shares. Output of this phase is original secret image.

## IV. RESULTS

Proposed method has been implemented in MATLAB 2009b. The minimum hardware configuration is required to run this scheme. The experiments have been run in Window 7 on Dell INSPIRON laptop with Intel Duo Core(TM)2 2.20GHZ processor.A number of results have been obtained to analysis the performance of this scheme by using different images, image sizes and keys for RSA algorithm. Every time the recovered image was having good quality. Some experiments results are shown in Fig.3 (a)-(h), Fig.4 (a)-(h) and Fig.5 (a)-(h).

Fig.3 (a) Binary Input Image1

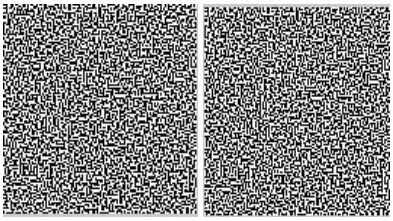

Fig.3(b) Share1 of Image1Fig. 3(c) Share2 of Image1

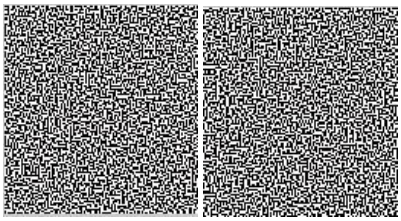

Fig.3(d) Encrypted share1 of Image1 Fig.3(e) Encrypted share2 of Image1

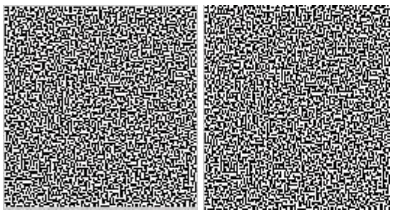

Fig.3(f) Decrypted share1 of Image1Fig.3(g) Decrypted share2 of Image1

Fig.3(h) Revealed image from decrypted shares

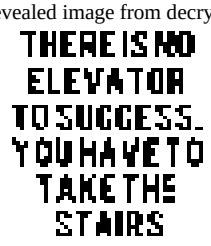


Fig.4(a) Binary Input Image2

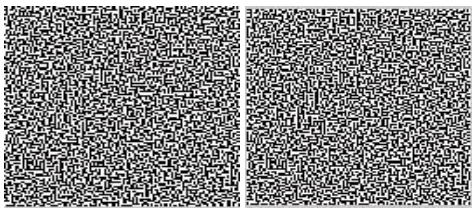

Fig.4(b) Share1 of Image2 Fig.4(c) Share2 of Image2

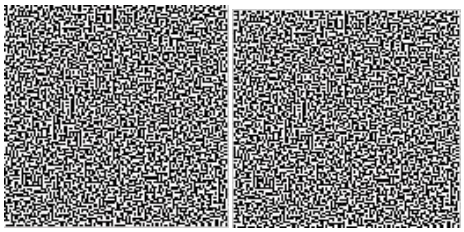

Fig.4(d) Encrypted share1 ofImage2 Fig.4(e) Encrypted share2 of Image2

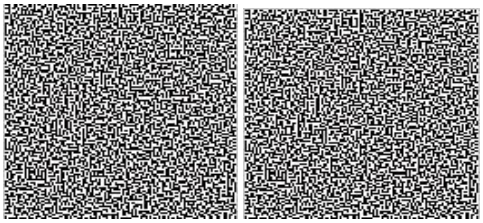

Fig.4(f) Decrypted share1 of Image2 Fig.4(g) Decrypted share2 of Image2


Fig.4(h) Revealed image from decrypted shares

Input images as shown in Figures 3(a), 4(a) and 5(a) were used for image1, image2 & image3 respectively. Figures 3(b), 4(b) and 5(b) show share1 of image1, image2 and image3


Fig.5(a) Binary Input Image3

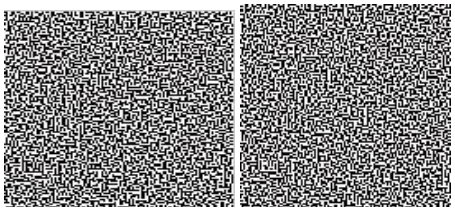

Fig.5(b) Share1 of Image3 Fig.5(c) Share2 of Image3

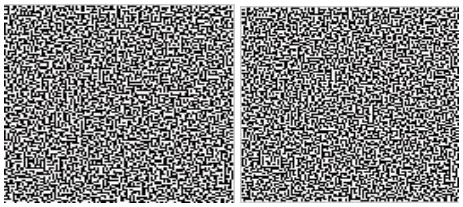

Fig.5(d) Encrypted share1Fig.5(e) Encrypted share2 ofImage3of Image3

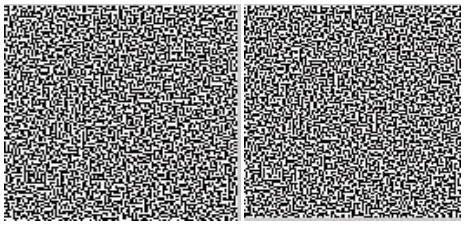

Fig.5(f) Decrypted share1Fig.5(g) Decrypted share2 ofImage3of Image3


Fig.5(h) Revealed image from decrypted shares

respectively. Figures 3(c), 4(c) and 5(c) show share2 of image1, image2 and image3 respectively. Shares are generated usingpixel encoding scheme [8][14]. Figures 3(d), 4(d) and 5(d) show the encrypted share1 & Figures 3(e), 4(e) and 5(e) show the encrypted share2 for image1, image2 and image3 respectively.

Encrypted share1 and encrypted share2 are output of phase-2. Visual cryptography shares are encrypted using RSA algorithm. Figures 3(f), 4(f) and 5(f) show decrypted share1 and 3(g), 4(g) and 5(g) show decrypted share2. These are result of phase-3. Finally Figures 3(h), 4(h) and 5(h) show original secret image recovered by performing XOR operation of decrypted share1 and decrypted share2of image1, image2 and image3 respectively. Table1 shows the system with altering size of input and random selection of key.

TABLE1. SYSTEM PERFORMANCE

| Input image (size) In pixels | Public key (e, n) | Private key (d, n) | Recovered after stacking decrypted shares |
|---|---|---|---|
| (67×65) | (5, 1264463) | (75325,1264463) | Yes |
| (64×62) | (5,343403) | (205229,343403) | Yes |
| (63×63) | (11, 188771) | (188771, 2079527) | Yes |

## V. CONCLUSION

We have tested this scheme on different types of input images with change in size of the image and keys of RSA. And the entire time secret image is retrieved. This method is simple to implement which has lower computational cost of secret image as it is recognized only by human eyes and not computed cryptographically. The confidentiality of shares can also test by super imposing the encrypted shares before reaching to the destination. And 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.Presently we have generated shares of binary image but in future instead of binary we can use color image and then generate the shares using visual cryptography.

## REFERENCES

[1] D. Jena and S. Jena "A novel visual cryptography Scheme". 978-07695-3516-6/08 © 2008 IEEE DOI 10.1109/ICACC.2009.109.

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

[3] Behrouz A. Forouzon, "Cryptography & network security" 4th Edition.

[4] Néelima. Guntupalli et al, "An introduction to different types of visual cryptography schemes", International Journal of Science and Advanced Technology (ISSN 2221-8386), Volume 1 No 7 September 2011, PP 198-205.

[5] 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.

[6] Y. Bani, Dr. B. Majhi and R. S. Mangrulkar, 2008. A novel approach for visual cryptography using a watermarking technique. In Proceedings of 2nd National Conference, IndiaCom 2008.

[7] B. Padhmavati, P. Nirmal Kumar, M. A. DoraiRangaswamy "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.

[8] UjjwalChakraborty 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.

[9] Wei-Qi Yan, Duo Jin, Mohan S Kankanhalli "Visual Cryptography for print and scan applications" School of Computing, National University of Singapore 117543.

[10] ShyamalenduKandar&ArnabMaiti "K-N secret sharing visual cryptography scheme for color image using random number". International Journal of Engineering Science and Technology (IJEST), ISSN 0975-5462, Vol. 3 No. 3 Mar 201,PP 1851-1857.

[11] M. Nakajima and Y. Yamaguchi "Extended visual cryptography for natural images". Department of Graphics and Computer Sciences, Graduate School of Arts and Sciences, the University of Tokyo 153-8902, Japan.

[12] VaibhavChoudhary "An improved pixel sieve method for visual cryptography" International Journal of Computer Applications, (0975 –8887) Volume 12– No.9, January 2011.

[13] P. S. Revenkar, AnisaAnjum, W. Z. Gandhare "Survey of visual cryptographic schemes". International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[14] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm (last accessed on 15.10.2014).