

Image Security using Visual Cryptography

A thesis submitted in partial fulfillment of the requirements for the degree of
Bachelor of Technology

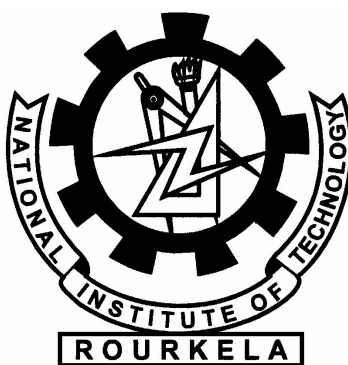
in

Computer Science and Engineering

Submitted by
Sangeeta Bhuyan
111CS0444

Under the guidance
of

Prof. R.K Mohapatra



Department of Computer Science and Engineering
National Institute of Technology Rourkela
Odisha, India, 769008

Acknowledgement

I would like to take this opportunity to extend my hearty gratitude to my guide and supervisor Professor R.K Mohapatra for his constant guidance and encouragement. I convey my regards to all the other faculty members of Department of Computer Science and Engineering, NIT Rourkela for their valuable guidance and advices at appropriate times. I would like to thank my friends for their help and assistance all through this project. Last but not the least, I express my profound gratitude to the Almighty and my parents for their blessings and support without which this task could have never been accomplished.

Sangeeta Bhuyan

Certificate

This is to certify that the work in the project entitled *Image Security using Visual Cryptography* by *Sangeeta Bhuyan* is a record of her work carried out under my supervision and guidance in partial fulfillment of the requirements for the award of the degree of *Bachelor of Technology in Computer Science and Engineering*.

Prof. R.K Mohapatra

Dept. of Computer Science and Engineering

National Institute of Technology

Rourkela - 769008

Abstract

Informations are being transferred through open channels and the security of those informations has been prime concerns. Apart from many conventional cryptographic schemes, visual cryptographic techniques have also been in use for data and information security. Visual cryptography is a secret sharing scheme as it breaks an original image into image shares such that, when the shares are stacked on one another, a hidden secret image is revealed. The Visual Cryptography Scheme is a secure method that encrypts a secret document or image by breaking it into image shares. A unique property of Visual Cryptography Scheme is that one can visually decode the secret image by superimposing shares without computation. Even to make the visual cryptography image shares more secure, public key encryption scheme is applied. Public key encryption technique makes image shares so secure that it becomes very hard for a third party to decode the secret image information without having required data that is a private key.

Declaration

I ,Sangeeta Bhuyan,hereby declare that the project entitled "Image Security using Visual Cryptography" is my original work under the supervision of Prof. R.K Mohapatra and this work has not been submitted for any degree or academic award elsewhere.

Sangeeta Bhuyan

List of Figures

1.1	General visual cryptography scheme	1
2.1	Illustration of a (2, 2) VC Scheme with 2 Subpixels	5
3.1	Illustration of a (2, 2) VC Scheme with 2 Subpixels	8
3.2	S0 and S1 matrices	8
3.3	Matrices for black and white pixels	9
4.1	Flow diagram for proposed scheme	11
5.1	Original image of Lena	13
5.2	Image of Share 1	14
5.3	Image of Share 2	14
5.4	Retrieved Image	15
5.5	Share image 1	15
5.6	Share image 2	15
5.7	Share image 3	16
5.8	Share image 4	16
5.9	Share image 5	16
5.10	Share image 6	17
5.11	Share image 7	17
5.12	Share image 8	17
5.13	Retrieved image for k out of n scheme	17
5.14	Encrypted image share	18
5.15	Encrypted image share	19
5.16	Overlapped image	20
5.17	Decrypted image share	20
5.18	Decrypted image share	21
5.19	Retrieved image	21

1	Introduction	1
1.1	Visual Cryptography	1
1.2	Literature Review	2
1.3	Objective	2
1.4	Outline of Thesis	2
2	Various Visual Cryptographic Schemes	4
2.1	k out of k visual cryptography scheme	4
2.2	k out of n visual cryptography scheme	4
2.3	Visual Cryptography Scheme for General Access Structure	5
2.4	Recursive Threshold Visual Cryptography Scheme	5
2.5	Halftone Visual Cryptography Scheme	6
2.6	Visual Cryptography Scheme for Grey images	6
3	Proposed Work	7
3.1	Basis matrices	7
3.2	Construction of 2 out of 2 VCS	8
3.3	Construction of k out of n VCS	9
4	Securing Visual Cryptographic shares using Public key encryption	10
4.1	Methodology	10
4.2	RSA algorithm	10
5	Performance Analysis	13
5.1	Implementation of 2 out of 2 VCS	13
5.2	Implementation of k out of n VCS	15
5.3	Implementation of Public key encryption	18
6	Conclusion	22
7	References	23

1.1 Visual Cryptography

Visual cryptography is a cryptographic technique which allows visual information to be encrypted in specific a way that decryption becomes a mechanical operation that does not require a computer. The idea was about producing image shares of a given secret image in a way that the image shares appear meaningless. Recovery of the image can be done by superimposing specified number of share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is a little more advantageous for implementation, while compared to conventional cryptography schemes, since the decryption process does not need any computation. Further, the image based information becomes more secure, since only the intended recipient can reveal the true meaning of the decrypted image. Suppose the data (image) D is divided into n shares. D can be constructed from any k shares out of n shares. Complete knowledge of $(k-1)$ shares reveals no information about D . So, k out of n shares is necessary to reveal secret data. For example: let 6 thieves share a bank account but they do not trust each other. The thieves split up the password for the account in such a way that any 3 or more thieves working together can have access to account, but not less than 3.

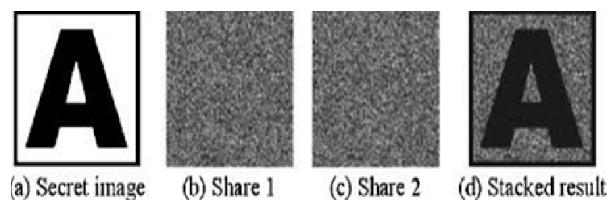


Figure 1.1: illustration of visual cryptography

1.2 Literature Review

Visual cryptography technique was introduced by Naor and Shamir in 1994 as an alternative for conventional cryptography. They demonstrated a visual secret sharing plan, where a picture was separated into n parts so that just somebody to all n shares could decode the picture, while any $n - 1$ shares uncovered no data about the first original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. At the point when all n shares were overlaid, the first picture would show up. There are a few speculations of the fundamental plan including k -out-of- n visual cryptography. Rijimen displayed another 2-out-of-2 VC plot by applying the thought of shading mixture. When two transparencies superimposed on one another with distinctive colours, they lead to raises a third blended shading.

In 2002, Nakajima predicted a new method of extended visual cryptography. This method is for regular images which are used to produce meaningful binary shares. This system works by taking three pictures as an input and generates two images which correspond to two of the three input pictures. The third picture is recreated by printing the two share pictures onto transparencies and stacking them together. By and large, visual cryptography experiences the deterioration of the image quality. In this also describes the method to improve the quality of the output image.

Binary visual cryptography scheme is proposed Hou et al. in the year 2004, which is applied to gray level images, that a gray level image is transformed into halftone images. The method that uses the density of the net dots to simulate the gray level is called Halftone and transforms an image with gray level into a binary image before processing. Halftone visual cryptography is proposed by the Zhi Zhou et al. In 2006 which produce meaningful and good high quality halftone shares, the generated halftone shares contain the visual information.

1.3 Objective

The prime objective of this project is to ensure the security of information (in this case image) transformation by creating image shares.

1.4 Outline of Thesis

The thesis consists of following chapters:

- Chapter 2: various visual cryptography schemes
In this chapter, various types of visual cryptography schemes are discussed.
- Chapter 3: Proposed Work
This chapter deals with analysis of work that is already proposed.
- Chapter 4: Securing Visual Cryptographic shares using Public Key Encryption
This Chapter deals with securing image shares using public key encryption. RSA algorithm is used for this scheme.

- Chapter 5: Performance Analysis
This Chapter deals with the implementation of proposed work.
- Chapter 5: Conclusion
This Chapter deals with conclusion of the proposed work.
- Chapter6: References
This includes the list of papers I have referenced during the work.

Various Visual Cryptographic Schemes

2.1 k out of k visual cryptography scheme

A common example of k out of k visual cryptography scheme is 2 out of 2 visual cryptography schemes. In (2, 2) Visual Cryptography Scheme, the original image is broken into 2 image shares. In original image, every pixel is represented by non-overlapping block of 2 or 4 sub-pixels in each share. If anyone is having only one share, will not be able to reveal any secret information. Both the shares are required to be superimposed to reveal the secret image.

There are many techniques for encoding the pixels of original image. In a technique, in which each pixel in original image is represented by two sub-pixels in each share, while reading the pixels in original image, if a white pixel is encountered, one of the first two rows in Figure given below is selected with probability 0.5, and the shares are assigned 2 pixel blocks as shown in the third and fourth columns in figure given below. Similarly, if a black pixel is encountered, one of the last two rows is selected with probability 0.5, from which a sub-pixel block is assigned to each share. When two shares are superimposed, if two white pixels overlap, the result will be white pixel and if a black pixel in one share overlaps with either a white or black pixel in another share, the result will be black pixel. This implies that the superimposition of the shares represents the Boolean OR function. The last column in Figure given below shows the resulting sub-pixel when the sub-pixels of both the shares in the third and fourth columns are superimposed.

2.2 k out of n visual cryptography scheme

In (2, 2) visual cryptography, both the shares are required to reveal secret information. Due to some problem if one share gets lost then the secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal the secret information and user can not afford to lose a single share. Naor and Shamir generalized basic model of visual cryptography into a visual variant of k out of n visual cryptography scheme to give













pixel		share #1	share #2	superposition of the two shares
	$p = .5$			
	$p = .5$			
	$p = .5$			
	$p = .5$			

Figure 2.1: Illustration of a (2, 2) VC Scheme with 2 Subpixels

some flexibility to user. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares superimposed, where value of k is between 2 to n . If less than k shares stacked together, secret original image cannot be revealed. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained. It also ensures the security as to know the secret information you have to have more than k shares out of n secret shares.

2.3 Visual Cryptography Scheme for General Access Structure

In (k, n) visual cryptography scheme, all n shares have equal importance. The secret information can be revealed if any k out of n shares are available. The security of system might get compromised due to this. To beat this issue, G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson extended (k, n) visual cryptography model to general access structure. In general access structure scheme, given set of n shares is divided into two subsets namely qualified and forbidden subset of shares as per the importance of shares. Any k shares from qualified subset of shares can reveal secret information, but fewer than k shares from qualified subset of shares can not reveal any secret information. Even k or more shares from forbidden set can not reveal secret information. So, Visual cryptography for general access structure improves the security of system.

2.4 Recursive Threshold Visual Cryptography Scheme

In (k, n) visual secret sharing scheme, a secret of b bits is distributed among n shares of size at least b bits each. Since only k out of n shares is needed to reveal secret, every bit of any share conveys at most $1/k$ bits of secret. It results in inefficiency in terms of number of bits of secret conveyed per bit of shares. To overcome this limitation Abhishek Parakh and Subhash Kak proposed Recursive threshold visual cryptography [7]. The basic idea behind Recursive threshold visual cryptography is recursive hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step, and thereby increasing the information, every bit of share conveys to $(n-1)/n$ bit of secret which is nearly 100

2.5 Halftone Visual Cryptography Scheme

Halftone visual cryptography uses half toning technique to create shares. Halftone is the reprographic technique. It simulates continuous tone imagery through the use of dots, which may vary either in size, in shape or in spacing. Zhi Zhou et al. proposed halftone visual cryptography. In halftone visual cryptography a secret binary pixel is encoded into an array of sub pixels, called as halftone cell, in each of the n shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. It maintains good contrast and security and increases quality of the shares[3].

2.6 Visual Cryptography Scheme for Grey images

All previous visual cryptography schemes were only limited to binary images. These procedures were fit for doing operations on just highly contrasting black and white pixels. It is not sufficient for real life applications. Chang-Chou Lin, Wen Hsiang Tsai proposed visual cryptography for gray level images. In this scheme a dithering technique is used to convert gray level image into approximate binary image. Then existing visual cryptography schemes for binary images are applied to create the shares.

3.1 Basis matrices

Any black-and-white visual cryptography scheme can be described using two $n \times m$ Boolean matrices S_0 and S_1 , called basis matrices, to describe the sub pixels in the shares. The basis matrix S_0 is used if the pixel in the original image is white, and the basis matrix S_1 is used if the pixel in the original image is black. The use of the basis matrices S_0 and S_1 can have small memory requirements (it keeps only the basis matrices S_0 and S_1), and it is efficient (to choose a matrix in C_0 or C_1) because it only generates a permutation of the columns of S_0 or S_1 .

Basically, the two basis matrices S_0 and S_1 should satisfy the following.

Definition:

1. A k -out-of- n visual cryptography scheme with parameters $1 \leq k \leq m$ and $\delta \geq 0$ can be constructed from two $n \times m$ Boolean matrices S_0 and S_1 if the following three conditions are met:
 1. The OR m -vector V of any k of the n rows in S_0 satisfies $H(V) \leq \delta \cdot m$.
 2. The OR m -vector V of any k of the n rows in S_1 satisfies $H(V) \geq \delta \cdot m$.
 3. For any set r_1, r_2, \dots, r_t , $1 \leq t \leq k$, the $t \times m$ matrices obtained by restricting S_0 and S_1 to rows r_1, r_2, \dots, r_t , are equal up to a column permutation.

where $H(V)$ is the hamming weight (the number of ones) of the m -vector V of any k of the n rows, m is the pixel expansion and δ is the relative difference. The conditions (1) and (2) related to contrast in a reconstructed image and condition (3) related to security.

Relative-Difference:

Let $H(S_0)$ and $H(S_1)$ be the hamming weight corresponding to the basis matrices S_0 and S_1 . Then relative difference (α) is defined as:

$$\alpha = (H(S_1) - H(S_0)) / m$$

Contrast:

Let α be the relative difference and m be the pixel expansion. The formula to compute contrast in different VCS is:

$$\beta = \alpha.m, \beta \geq 1$$

The basic idea of visual cryptography can be best described by considering a 2-out-of-2 VCS.

3.2 Construction of 2 out of 2 VCS

Let us consider a binary secret image S containing exactly m pixels. The dealer creates two shares (binary images), S_1 and S_2 , consisting of exactly two pixels for each pixel in the secret image. If the pixel in S is white, the dealer randomly chooses one row from the first two rows of the figure 3 given below. Similarly, if the pixel in S is black, the dealer randomly chooses one row from the last two rows of figure 3.

















Original Pixel	Pixel Value	Share1	Share2	Share1+ Share2
	0			
	0			
	1			
	1			

Figure 3.1: Illustration of a (2, 2) VC Scheme with 2 Subpixels

To analyse the security of the 2-out-of-2 VCS, the dealer randomly chooses one of the two pixel patterns (black or white) from the Table for the shares S_1 and S_2 . Randomly the pixels are selected so that the shares S_1 and S_2 consist of equal number of black and white pixels. Therefore, by reviewing a single share, one cannot distinguish the secret pixel as black or white. This technique gives flawless security. By superimposing the two shared sub pixels, the two participants can recover the secret pixel. The original pixel was black, If the superimposition results in two black sub pixels and if the superimposition creates one black and one white sub pixel, it indicates that the original pixel was white[1]. In visual cryptography, the white pixel is represented by 0 and the black pixel by 1. For the 2-out-of-2 VCS, the basis matrices, S_0 and S_1 are designed as follows:

$$S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

$$S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

Figure 3.2: S_0 and S_1 matrices

The relative difference and contrast, for the above basis matrices can be computed as:

$$\alpha = 1/2$$

$$\beta = 1$$

There are two collections of matrices, C0 for encoding white pixels and C1 for encoding black pixels. Let C0 and C1 be the following two collections of matrices:

$$C0 = \pi(S0)$$

$$C1 = \pi(S1)$$

where $\pi(S0)$ and $\pi(S1)$ represents the collection of all matrices obtained by permuting the columns of matrices S0 and S1 respectively.

That is,

To share a white pixel, the dealer randomly selects one of the matrices in C0, and to

$$C_0 = \left\{ \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\} \text{ and } C_1 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

Figure 3.3

share a black pixel, the dealer randomly selects one of the matrices in C1. The first row of the chosen matrix is used for share1(S1) and the second row for share 2 (S2).

The two shares individually do not reveal the secret message. When we merge the two shares one upon another we can reveal the secret.

3.3 Construction of k out of n VCS

In this type of VCS, we are given a secret message. We would like to generate n transparencies so that the original secret message is visible if any k (or more) of them are stacked together but totally invisible if fewer than k transparencies are stacked together. A solution to the k out of n VCS consists of two collection of $n \times m$ Boolean matrices C0 and C1. To share a white pixel, the dealer randomly chosen one of the matrices in C1. The chosen matrix defines the colour of the m sub pixels in each one of the n transparencies and likewise for black pixels. We apply 2 out of 2 VCS for every share images to create more shares[1].

Securing Visual Cryptographic shares using Public key encryption

The visual cryptography scheme is a secure method that encrypts a secret document or image by breaking it into shares. A unique property of visual cryptography scheme is that one can visually decode the secret image by superimposing shares without computation. By taking the advantage of this property, third person can easily retrieve the secret image if shares are passing in the network. This approach is for encrypting visual cryptographically generated image shares using public key encryption. RSA algorithm is used for providing the double security of secret image. This scheme provides more security to secret shares that are robust against number of attacks. This way after encryption of image shares even if a third person gets those shares while passing through the network, would not be able to reveal the secret.

4.1 Methodology

This scheme generates the VC shares using basic visual cryptography model and then encrypt the shares using RSA algorithm so that the shares will be more secure and protected from the malicious adversaries who may try to alter the bit sequence to create fake shares. During the decryption phase the secret shares are extracted by RSA decryption algorithm and stacked to reveal the secret image[6].

4.2 RSA algorithm

RSA is algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm, means there are two different keys. This is also called public key cryptography because one of them is public i.e can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of a integer is hard. RSA stands for Ron Rivest , Adi Shamir and Leonard Adleman , who first publicly described it in 1978.

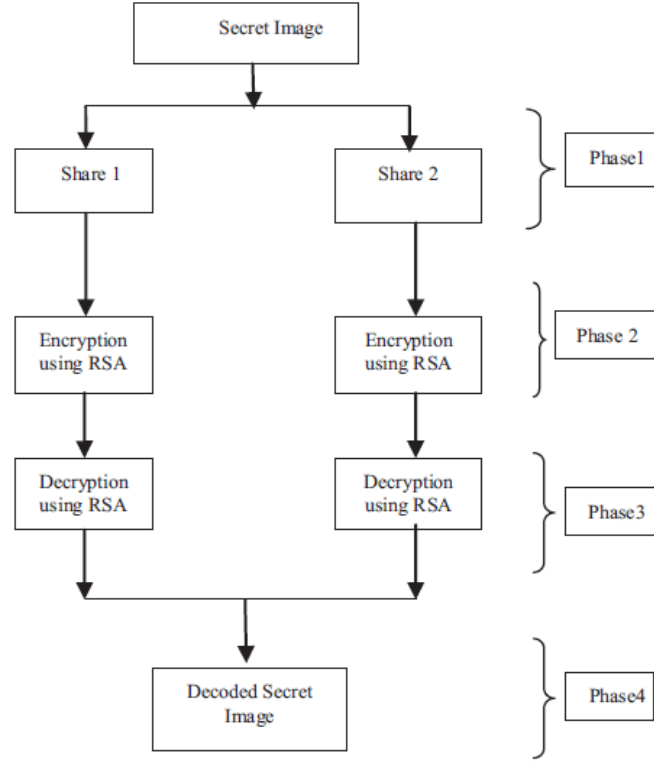


Figure 4.1: methodology for public key encryption scheme

Operation

RSA involves a public key and private key. The public key can be known to everyone, it is used to encrypt messages. Messages encrypted using the public key can only be decrypted with the private key. The keys for the RSA algorithm are generated the following way:- 1. Choose two distinctive prime numbers p and q . For security purpose, the integers p and q should be chosen at random and should be of similar bit length. Prime integers can be efficiently found using a primality test.

2. Compute $n = p * q$

n is used as the modulus for both the public and private keys. It's length usually expressed in bits, is the key length.

3. compute $\phi(n) = \phi(p) * \phi(q)$

$$= (p - 1) * (q - 1)$$

$$= n - (p + q - 1)$$

where, $\phi(n)$ is Euler's totient function.

4. Choose an integer e such that, $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$ that is e and $\phi(n)$ are coprime.

5. Determine d as $d = e^{-1} \pmod{\phi(n)}$ i.e d is the multiplicative inverse of $e \pmod{\phi(n)}$

The public key consists of the modulus n and the public(or encryption)exponent e . The private key consists of the modulus n and the private(or decryption) exponent d , which

must be kept secret.

Encryption one party transmits public key (n,e) to second party and keeps the private key d secret. The second party then wishes to send message M to first party. The second party first turns M into an integer m such that,

$$0 < m < n$$

by using an agreed upon reversible protocol known as a padding scheme. Then compute the cipher text C correspond to, $c = m^e \pmod n$

This can be done efficiently even for 500 bit numbers, using modular exponentiation. Then second party transmits C to first party.

Decryption First party can recover m from C by using private key exponent d via computing

$$m = C^d \pmod n$$

given m , first party can never recover the original message M by reversing the padding scheme.

5.1 Implementation of 2 out of 2 VCS

We have used the standard Lena image for this project. First the grey Lena image is converted to binary image and then it is ready to be used for our project.

The original image is given below:

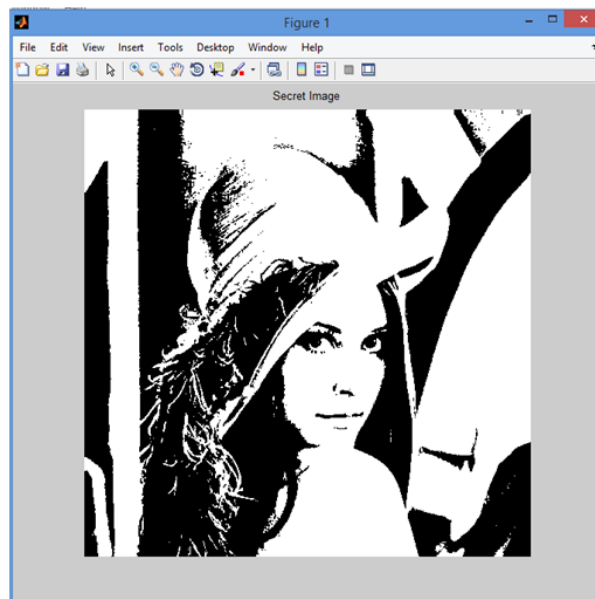


Figure 5.1: Original image of Lena

After applying 2 out of 2 VCS, we got following share images:

These share images alone could not reveal the secret image but when stacked upon on another would reveal the secret. So after stacking up we got the following image:

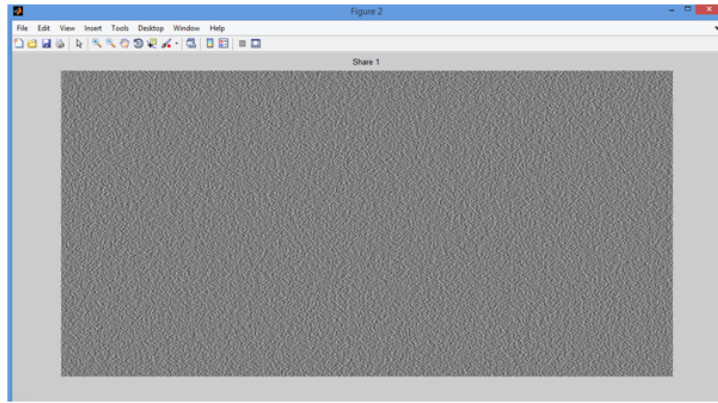


Figure 5.2: Image of Share 1

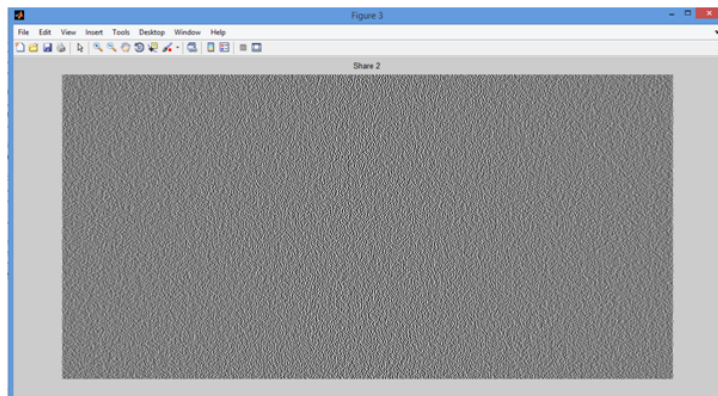


Figure 5.3: Image of Share 2

For every pixel encoded from the original image into two sub pixels and placed on each share in a horizontal or vertical fashion (here horizontal), the shares have a size of $s \times 2s$ if the secret image is of size $s \times s$. Hence there is distortion.

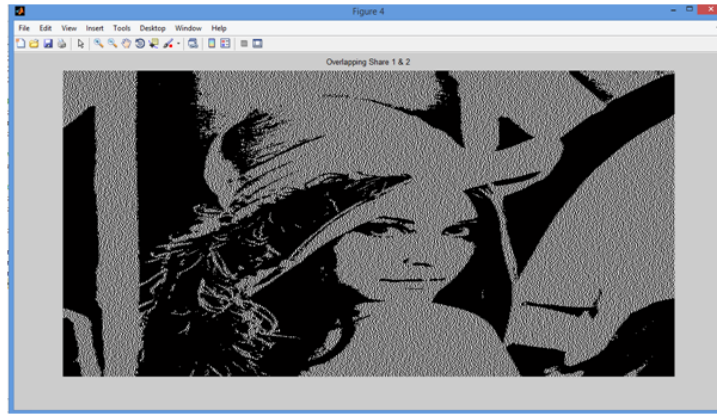


Figure 5.4: Retrieved Image after stacking share1 and share2

5.2 Implementation of k out of n VCS

We have taken 8 total transparencies that is total 8 shares are generated from original secret image($n=8$). Here, $k=4$. So, 4 or more shares would reveal the secret. Following are the 8 share images and after stacking first four or more share images, we will get the secret image revealed.

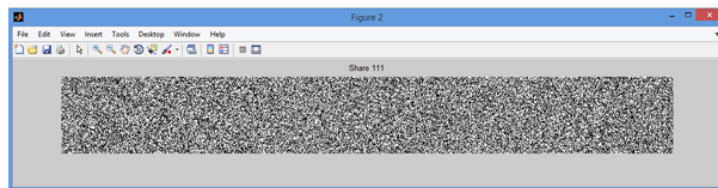


Figure 5.5: Image of Share 1



Figure 5.6: Image of Share 2

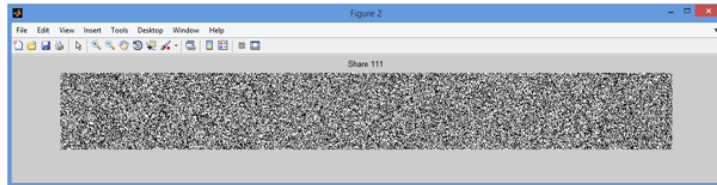


Figure 5.7: Image of Share 3



Figure 5.8: Image of Share 4



Figure 5.9: Image of Share 5



Figure 5.10: Image of Share 6

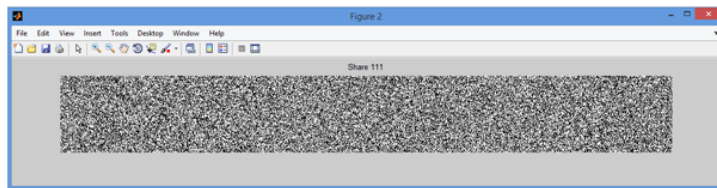


Figure 5.11: Image of Share 7

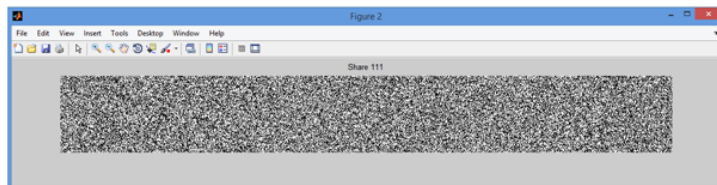


Figure 5.12: Image of Share 8

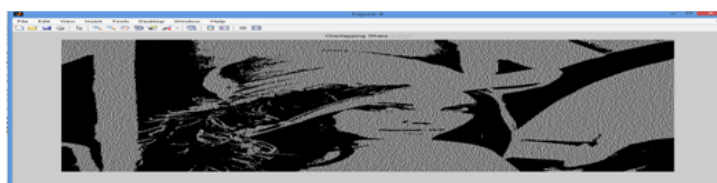


Figure 5.13: Retrieved image after stacking first 4 shares

5.3 Implementation of Public key encryption

Here, public key encryption is used for 2 out of 2 visual secret sharing scheme. First we generate image shares from the original Lena image using 2 out of 2 Visual Cryptography scheme. Then, using RSA encryption technique, the two image shares are encrypted making them more secure. Following two images are encrypted image share after applying RSA algorithm:

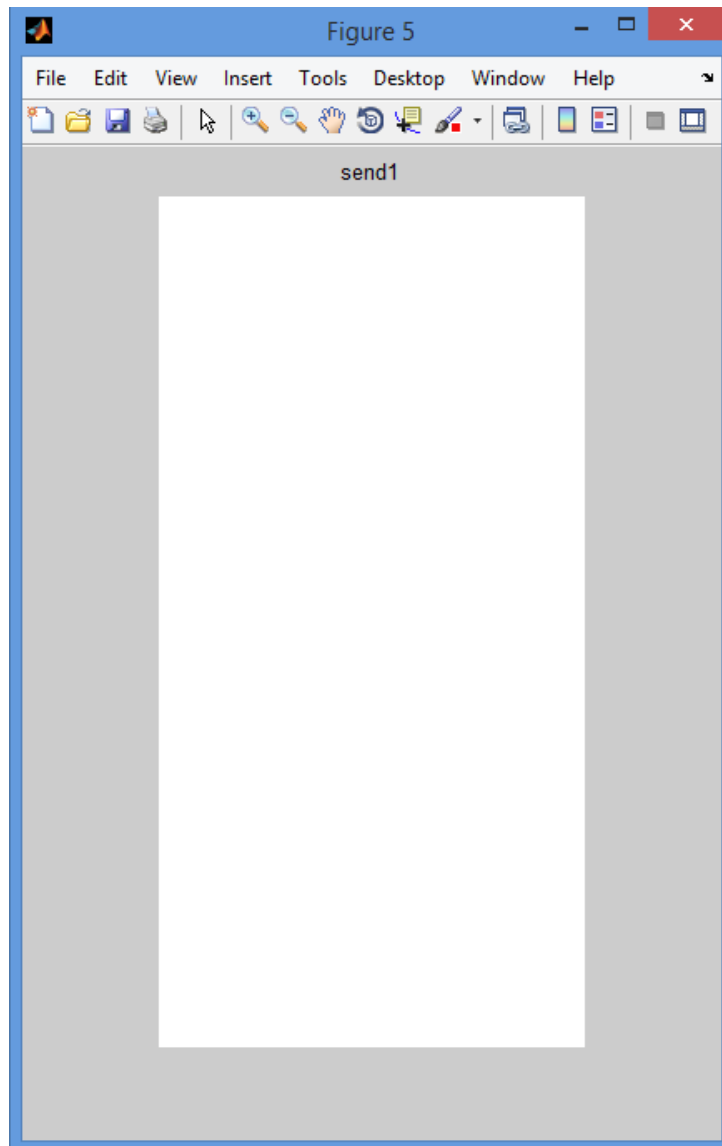


Figure 5.14: Image of Share 1 after encryption

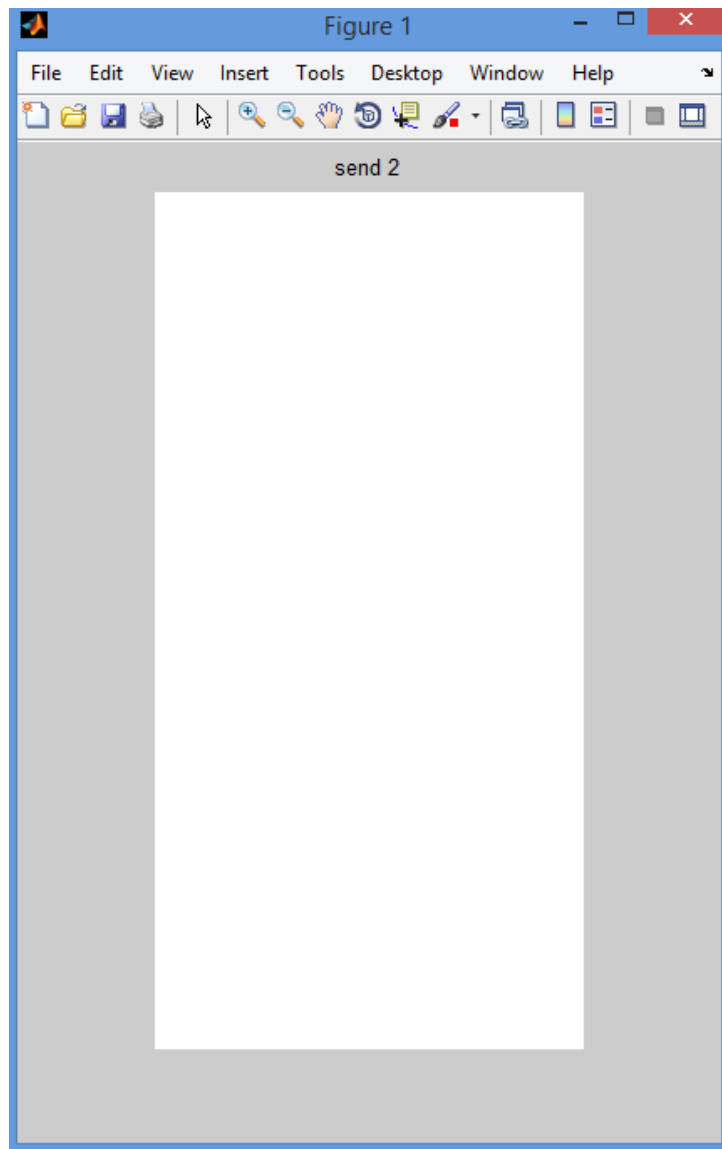


Figure 5.15: Image of Share 2 after encryption

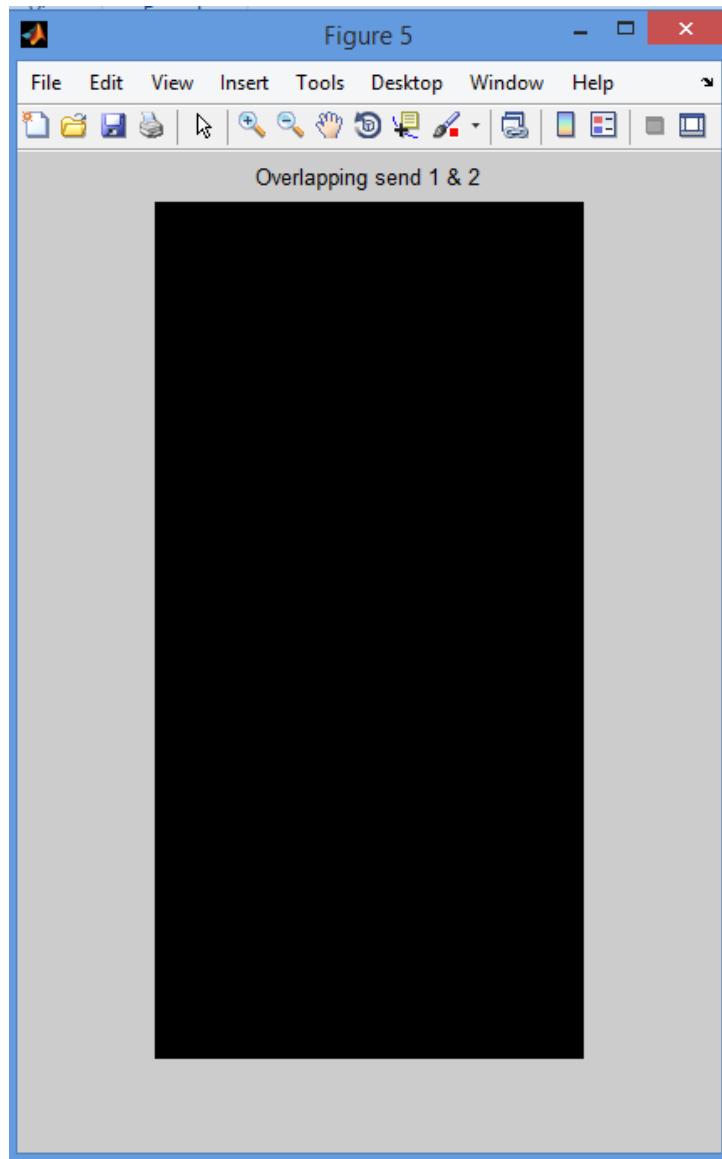


Figure 5.16: Overlapping result of encrypted shares

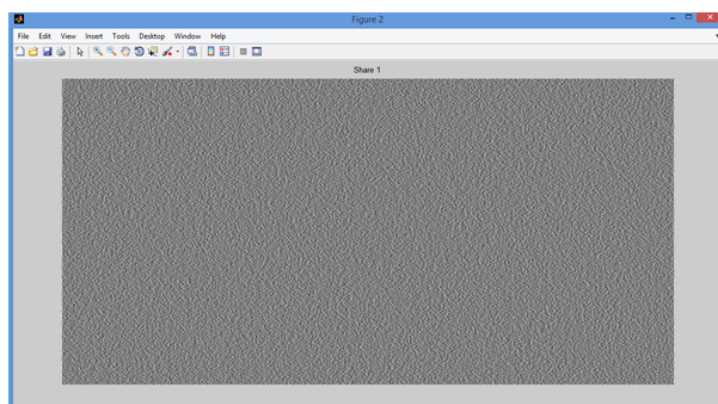


Figure 5.17: Image of Share 1 after decryption

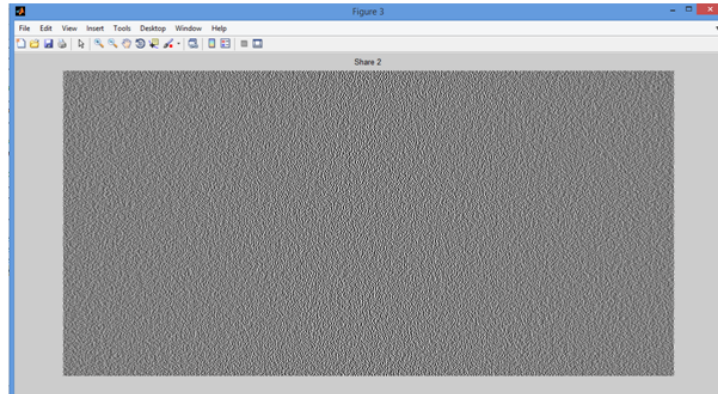


Figure 5.18: Image of Share 2 after decryption

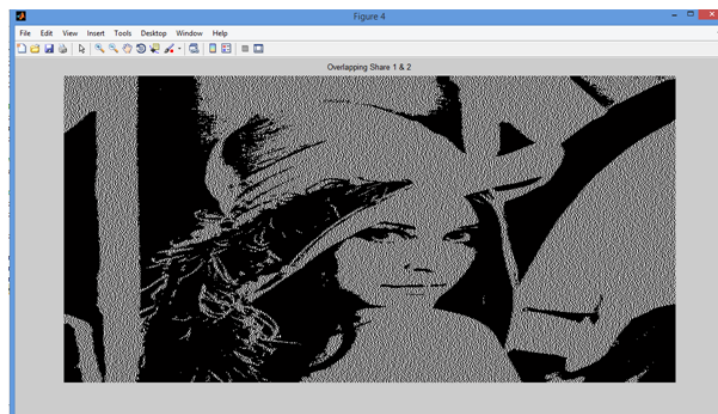


Figure 5.19: Overlapping image of decrypted shares

Conclusion

Visual cryptography is the current area of research where lot of scope exists. In this thesis, we have demonstrated the construction of basis matrices for 2-out-of-n, n-out-of-n, k-out-of-n VCS is demonstrated with examples. Also, using public key encryption, secret shares are made more secure which make secret image shares impossible to be altered by any third party. Visual secret sharing schemes with public key encryption technique ensure us for secure information transformation through a channel.

References

1. Feng Liu, Chuankun Wu, Xijun Lin. "Step Construction of Visual Cryptography Schemes". IEEE transactions on information forensics and security, vol. 5, no. 1, march 2010.
2. N. Askari, H.M. Heys, and C.R. Moloney. "an extended visual cryptography scheme without pixel expansion for halftone images". 26th annual ieee canadian conference on electrical and computer engineering year 2013.
3. Zhi Zhou, Gonzalo R. Arce and Giovanni Di Crescenzo. "Halftone Visual Cryptography". IEEE transactions on image processing, vol. 15, no. 8, august 2006.
4. Gyan Singh Yadav and Aparajita Ojha. "A Novel Visual Cryptography Scheme Based on Substitution Cipher". Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013).
5. Archana B.Dhole and Prof. Nitin J. Janwe. "An Implementation of Algorithms in Visual Cryptography in Images". International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013 1 ISSN 2250-3153.
6. Kulvinder Kaur and Vineeta Khemchandani. "Securing Visual Cryptographic Shares using Public Key Encryption". 2013 3rd IEEE International Advance Computing Conference (IACC).
7. A. Parakh and S.kak ."A Recursive Threshold Visual Cryptography Scheme ". Department of Computer Science, Oklahoma State University Stillwater, OK 74078.
8. D. Jena and S. Jena . "A Novel Visual Cryptography Scheme". 978- 07695-3516-6/08 2008 IEEE DOI 10.1109/ICACC.2009.109.
9. P. S. Revenkar, Anisa Anjum and W. Z. Gandhare. "Survey of Visual Cryptographic Schemes". International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.
10. 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.