Secret Sharing Scheme Based Technology for Visual Cryptography

A Report Submitted
in Partial Fulfillment of the Requirements
for the Degree of
Bachelor of Technology
in
Information Technology

by

Manas Abhilash Gundapuneni

Anzum Bano

Samridh Upadyay

to the

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
MOTILAL NEHRU NATIONAL INSTITUTE OF TECHNOLOGY
ALLAHABAD PRAYAGRAJ
10 July, 2020

UNDERTAKING

I declare that the work presented in this report titled "*Secret Sharing Scheme Based Technology for Visual Cryptography*", submitted to the Computer Science and Engineering Department, Motilal Nehru National Institute of Technology Allahabad, Prayagraj, for the award of the ***Bachelor of Technology*** degree in ***Information Technology***, is my original work. I have not plagiarized or submitted the same work for the award of any other degree. In case this undertaking is found incorrect, I accept that my degree may be unconditionally withdrawn.

10 July, 2020
Allahabad

(Manas Abhilash Gundapuneni)
(Anzum Bano)
(Samridh Upadhyay)

CERTIFICATE

Certified that the work contained in the report titled "*Secret Sharing Scheme Based Technology for Visual Cryptography*", by ***Manas Abhilash Gundapuneni***, ***Anzum Bano***, ***Samridh Upadhyay*** has been carried out under my supervision and that this work has not been submitted elsewhere for a degree.

(Navjot Singh)
Computer Science and Engineering Dept.
M.N.N.I.T, Allahabad

10 July, 2020

Preface

The thesis titled "*Secret Sharing Scheme Based Technology for Visual Cryptography*" is a technical document introducing an efficient algorithm for secret sharing and also provides a more renewed approach for existing methods of visual cryptography. The document introduces the readers to the foundations of visual cryptography, then discusses related work surrounding the thesis over a period of time. It is followed by the proposed work by the authors and their experimental results as well as setup leading to this outcome. The main objective of any computer science student is to get as much practical knowledge as possible. Being able to have practical knowledge by developing a project is a lifetime experience. Proper care has been taken while organising the project in order to make it comprehensible and implement various software technologies simultaneously.

Acknowledgements

The satisfaction that accompanies the successful completion of this project would be incomplete without mention of people who made it possible, because without their support, encouragement and guidance, everything would have gone in vain. We take this opportunity to thank our project supervisor, **Dr. Navjot Singh**, **Department of Computer Science and Engineering, Motilal Nehru National Institute of Technology** for his constant guidance and insightful feedback during the project. We are also grateful to the Institute for providing us this course work which helped us realise good research work is the outcome of what our teachers have taught in classes and is a good motivation to take up more research work in the future.

We are also thankful to Boddireddy Vignan Reddy for lending his mathematical insights,our colleagues and friends for their constant support. Finally; we deem it a great pleasure to thank one and all that helped us directly or indirectly in carrying out this work. Last but not the least, we wish to thank our parents for financing our studies in college as well for constantly boosting up our moral

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The thesis deals with the transmission of multimedia such as images over insecure and secure networks, secret sharing helps to mask the image from the attacker by breaking it down to shares which are not at all related in the sense of content to the original image and provide the security of only reconstructing the original image when the client has all the shares.

1.1 Visual Cryptography

Visual Cryptography deals with the multimedia information to be encrypted by means of which they cannot be decoded by visual information systems. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994[4]. Visual Cryptography uses two transparent images. One image contains arbitrary pixels and the other image contains the secret information. It is infeasible to retrieve the secret from one of the images. Both transparent images or layers are required to reveal the secret[4].

In the following years Verheul and Tilborg developed a scheme for colored images. The drawbacks of these schemes were mainly the meaningless shares being used for encryption which make the quality of the recovered secret implausible than the original secret.

Later Chang et al [3] [9] had introduced in the year 2000 a lossless scheme which used a Color Index Table(CIT) and was aberrant from the stacking mechanism of transparencies used and didn't require it, which made it easier to use in the real time applications. But as the colors present in the secret image increased the CIT became larger, pixel expansion factor became significant which increased the loss of resolution in contrast to the scheme.

Visual Cryptography can be classified into

1.Random Grid based VCS (RGVCS) schemes

2.Polynomial based Secret Image Sharing (Polynomial based SIS) schemes

Random Grid Based VCS use the concept of randomness and cannot provide 100% accuracy, whereas the Polynomial Based VCS construct a polynomial based on the pixels of the secret image.

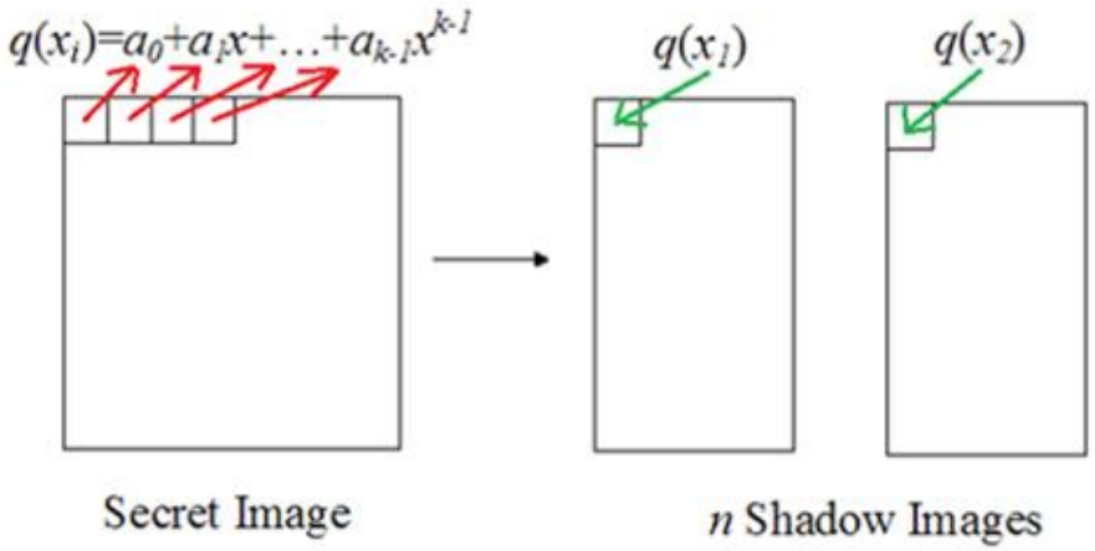


Figure 1.1.1: Internal Working of Polynomial VCS scheme

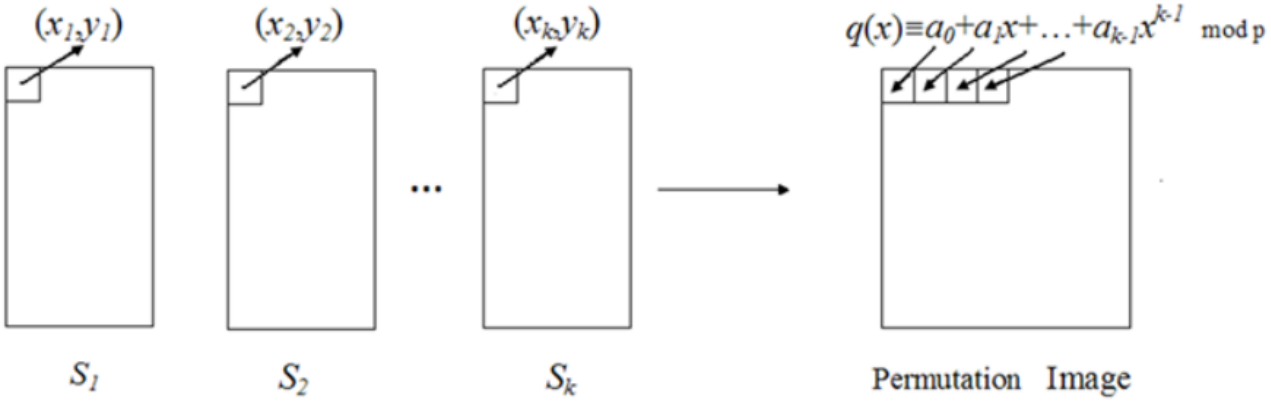


Figure 1.1.2: Internal Working of Polynomial VCS scheme Decryption

1.2 Motivation

The motivation for this type of technology is, after studying various observations in research papers it has been known that even though multimedia is encrypted using AES or any other encryption scheme, the sleuth of the image is given away meaning the outlook of the image is given away, which destroys the essence of encryption, so our project has a two-layer encryption scheme wherein, the first layer encrypts the image using any stable encryption scheme and then uses a XOR based approach to break the images into shares and transmit them over the network, making it impossible for the attacker to make sense out of the images on the wire. And we all know in computer science world, how much importance data has, and Moreover how important and critical data transmission is. It is essential to have a scheme which transfers the data from one point to another without giving any third party a chance to decode it, so this served as the motivation behind this project.

Chapter 2

Related Work

2.1 Naor and Shamir Visual Cryptographic Scheme

The basic model consists of a printed page of ciphertext (which can be sent by mail or faxed) and a printed transparency (which serves as a secret key). The original cleartext is revealed by placing the transparency with the key over the page with the ciphertext, even though each one of them is indistinguishable from random noise.The system is similar to a one-time pad in the sense that each page of ciphertext is decrypted with a different transparency. Due to its simplicity, the system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations. The best way to visualize the visual cryptographic scheme is to consider a concrete example. Consider two random looking dot patterns in Fig 3. To decrypt the secret message, the reader should photocopy each pattern on a separate transparency, align them carefully, and project the result with an overhead projector.

Shamir's Secret Sharing Scheme[6], In this a secret is divided into n parts and k serves as a threshold to recreate the original image. Here n participants are given one unique part each and any k participants collectively can recreate the image without revealing any one's key share to others. It was based on the polynomial property that in order to create a polynomial of degree 'n', n+1 unique coordinates are required and can be solved using mathematical equations, So in order to create

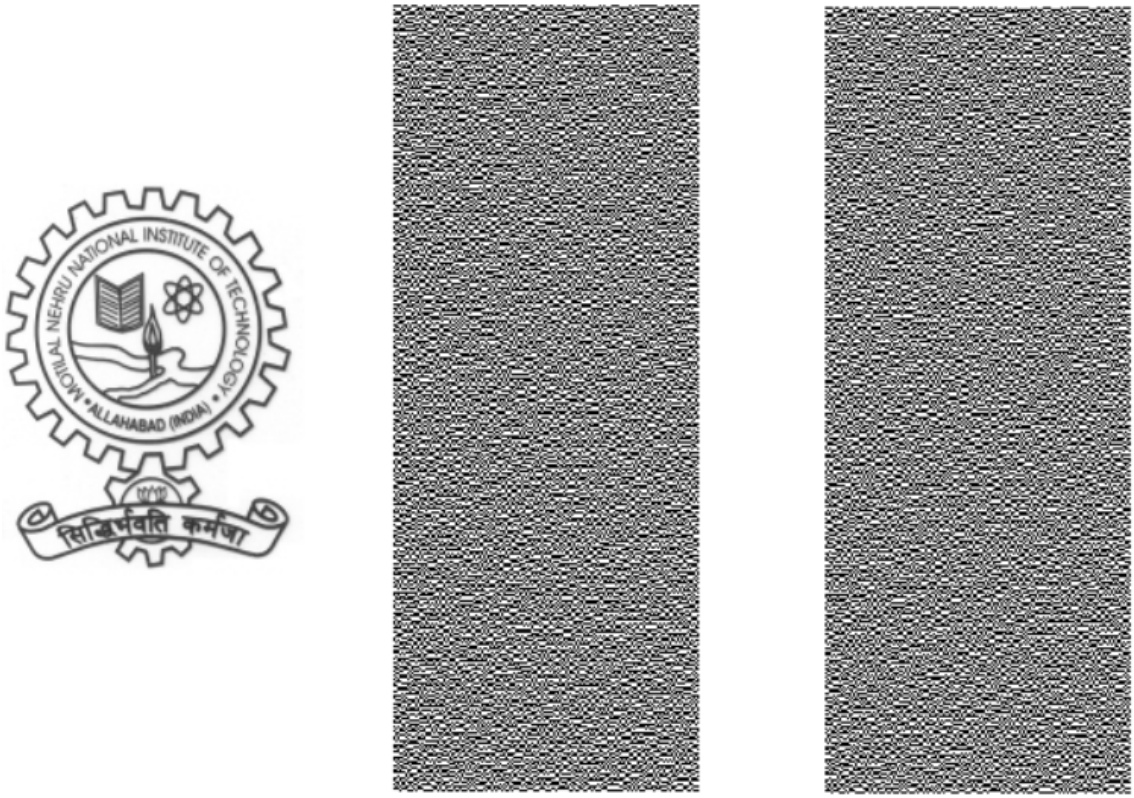


Figure 2.1.1: Naor and Shamir (2,2) VCS (a) Secret Image (b)Share 1 (c) Share 2

an image of degree k-1, 'k' shares are required. One issue with this scheme is lack of verification that shareholders are sharing honest shares and if not who is sharing the incorrect one.

This scheme is generalized to support (k,n) scheme meaning, a Secret Image can be divided into n shares such that k or more shares when overlapped can reveal the Secret Image. A combination of k or more may also reveal the secret image but with an improved quality.

The merits of this scheme, generation of random pixels, immunity from attack by attacker and complexity is O(1) for encoding and decoding.The demerits of this scheme are, loss of contrast, pixel expansion, multiple secret sharing.

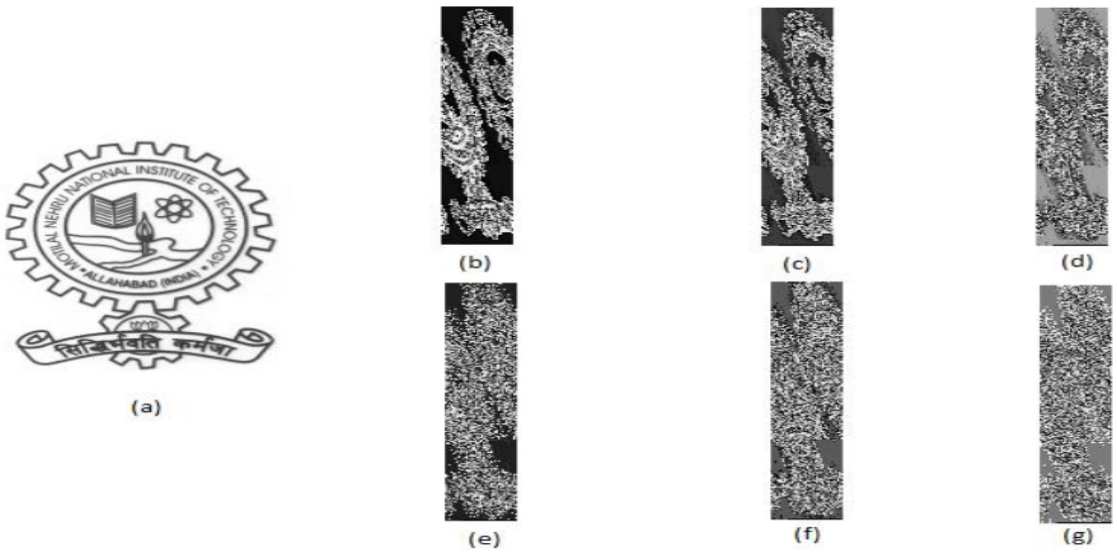


Figure 2.2.1: Thein Lin Polynomial based (4,6) SIS Scheme, (a) Secret Image (b) Share 1 (c) Share 2 (d) Share 3 (e) Share 4 (f) Share 5 (e) Share 6

2.2 Thein Lin Polynomial based (4,6) Threshold Secret Sharing

This scheme deals with dividing a secret image S into n shadow images(S1..Sn), and the secret image S cannot be retrieved without k or more shadow images. A k-1 degree polynomial is generated by letting the k coefficients be the gray values of k pixels.There is a difference in the way pixels are generated for share from the Shamir's method, as no random generation is used. The gray value of a pixel is between 0 and 255, so we let the prime number p be 251 which is the greatest prime number not larger than 255. Then, we must truncate all the gray values 251–255 of the secret image to 250, which makes all gray values translate to the range 0–250. The image is divided into several sections. Each section has k pixels, and each pixel of the image belongs to one and only one section. For each section we define the following k-1-degree polynomial.[5]

$$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_n x^{n-1} \quad mod \quad 251 \tag{1}$$

Chapter 3

Proposed Work

In this thesis, authors propose an *improved secure generalized multi transparency image multi-secret sharing* mechanism which aims to overcome the disadvantages of the existing work. This scheme is generalized i.e the shares generated can be flexible for change. A multi-secret sharing scheme gives the choice of share dynamics. A *(k,k) where k belongs to* $2 \leq k \leq n$ share scheme is used where the secret sharing is based upon Boolean operation with no reconstruction complexity. The proposed system is improved over the existing mechanisms which fail to address the color images having red, blue, green and alpha transparencies and are based on random binary assignment for the shares based upon the secret.

3.1 Architecture Design and Technical Implementation

The Architecture Design involves blue print of various modules used in coupling for the whole mechanism and are detailed for the encryption and decryption part which contain a two layer approach for increased security. The Architecture is outlined as two parts.

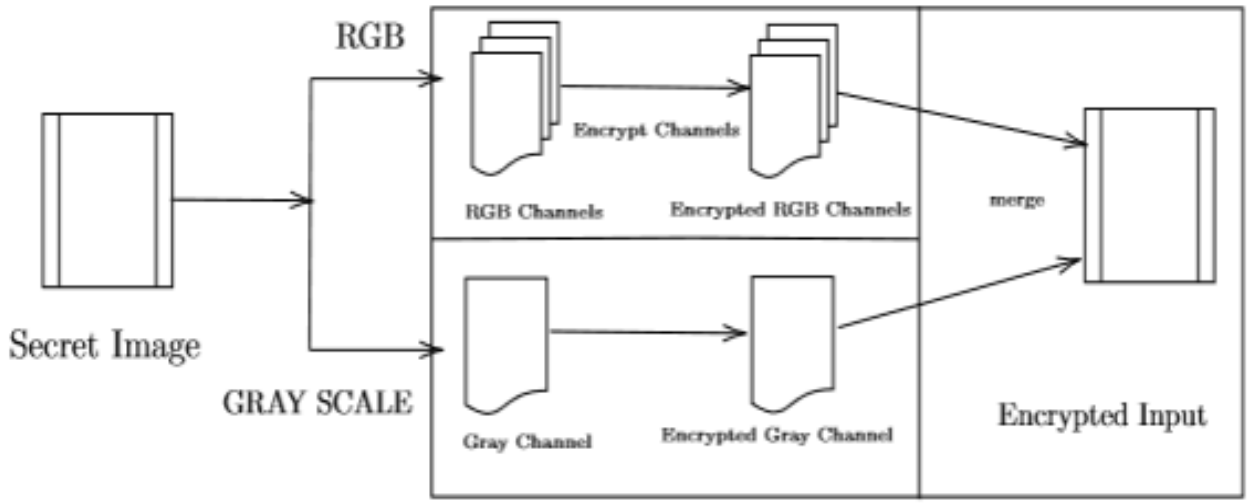


Figure 3.1.1: Layer 1 Cellular Automata based Encryption

3.1.1 Cellular Automata based Encryption Layer 1

The first part contains the standard encryption, but uses an image encryption system using one dimensional cellular automata for image encryption and decryption. Cellular automata can be corresponded with the essential cryptography properties i.e. Balance, correlation-immune, non linearity and easy to implement in hardware. CA crypto-systems can give better performances compared to classic methods that are based on computational techniques. Therefore, this technique should be most favourable for cryptography[8].

1. Encryption –

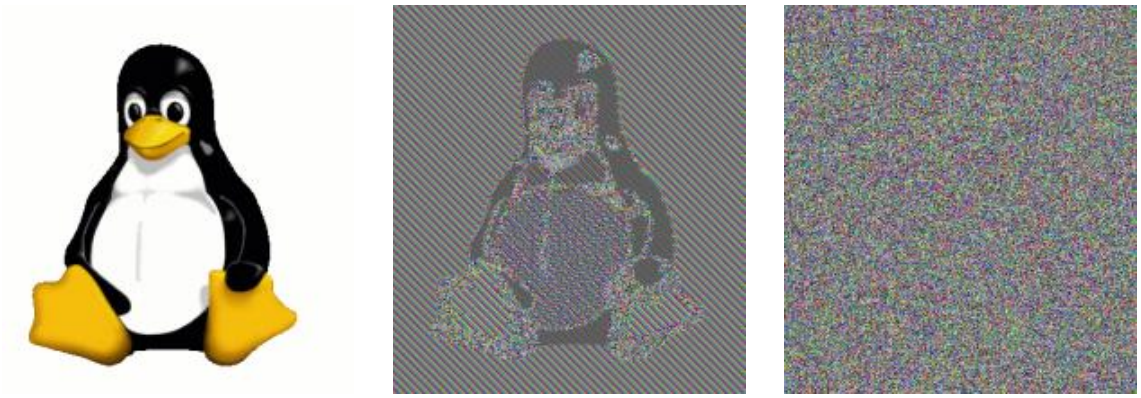
RGB: Extract individual RGB channel to encrypt each layer and merge.

Gray: Convert the given image to grayscale and use it for encryption.

2. Decryption –

Key: Use a key for each pixel for decryption process stored in a separate file.

Preset: Use predefined rules to decrypt the image.



(a) Original Linux Tux image

(b) Encrypted Tux Image using ECB

(c) Secret Sharing based Tux Image Encryption

Figure 3.1.2: Depiction of Need for Secret Sharing

3.1.2 Generalized Multi transparency Image Multi-secret Sharing Scheme Layer 2

A Boolean operated highly secure secret sharing scheme has been designed for the usage of multi secret sharing. The need for this type of sharing arises directly from the vulnerabilities faced by the modern cryptography based encryption[2]. Upon studying various works on how images have a high amount of correlation between pixels on the basis of context of the images it has been conceived that images are prone to human visual system decoding, as depicted by our study in fig 3.1.2.

The Shadow image construction procedure or the share construction from the input and the output secret re construction from the shares is given in the format of definitions and pseudo code.

A Boolean XOR based operation has been employed to create shares[7], the shares created are meaningless shares as random shares are less susceptible to human visual system crypt analysis and offer more security than meaningful shares. The Secret after entering the system is termed as the Master Share and is used to modify based on the shares being generated randomly in their respective transparencies. A *(n,n)* secret sharing scheme is used in contrast to the *(k.n)* scheme present in major works, as the later scheme increases algorithm complexity by ways of need to generate redundant shares[7] and wastes network bandwidth when incorporated.

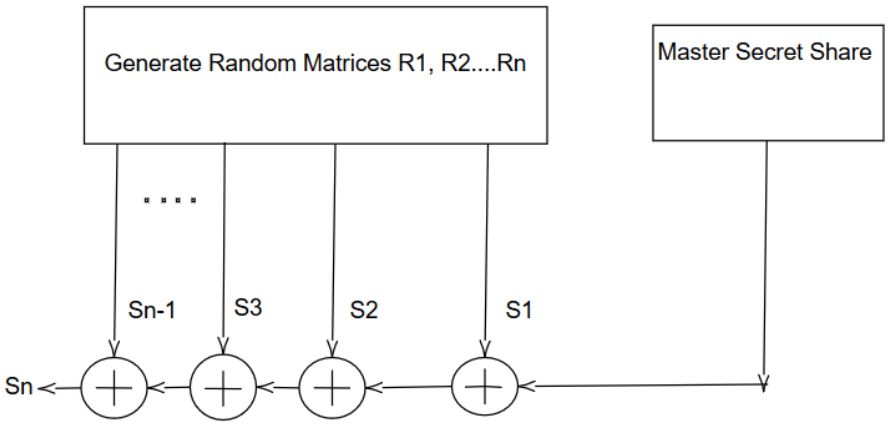


Figure 3.1.3: Proposed Secret Sharing Share Generation

Input: A Image of format PNG, JPEG or TIFF, where the said image can be having RGBA Transparencies or a Gray Scale Transparency, an integer N, where N conforms to $N \geq 2$.

Output: N meaningless shares of PNG format in the same dimensions as the secret image out of which one is the master share indistinguishable.

Construction: The secret share given in the input , is converted into it's transparencies in the form of arrays of pixels namely numpy arrays, which then undergo the Cellular Automaton Encryption at each transparency level and are merged back together. The encryption here is carried out based on rules to be can selected and order can be changed (R30, R90, R120).

Random arrays of required transparencies are generated, operated on by the Boolean operator with the master share and the newly generated share. The operations can be quantified by the following equation

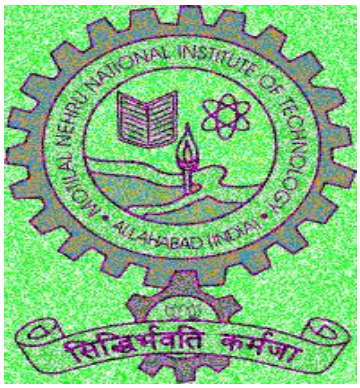
MasterShare $= Share_i \oplus MasterShare$

where $i \longrightarrow 0 \ to \ N$

where $Share_i \ is \ generated \ by \ rand_x(0, 254) * NumberofTransparencies$

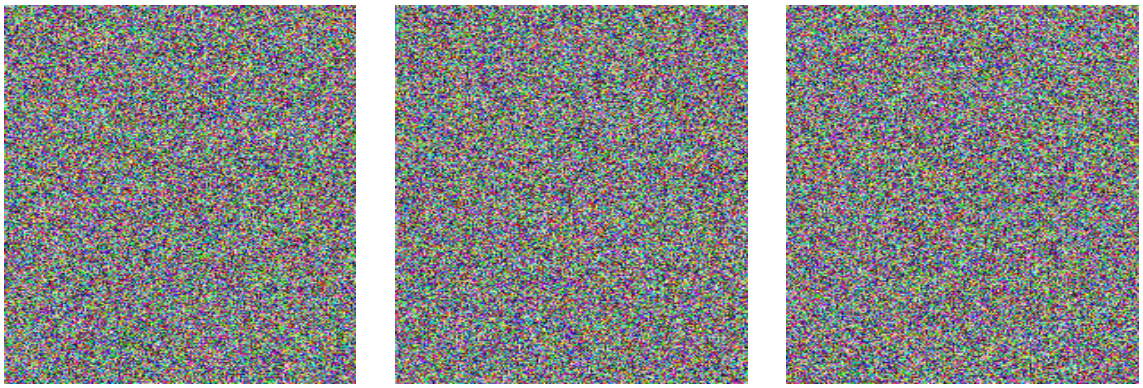
where $x \longrightarrow 0 \ to \ height * width$

(a) Input Secret Image to the proposed system



(b) After Reconstruction from Shares

Figure 3.1.4: Encryption and Decryption using proposed system



(a) Share 1 (b) Share 2 (c) Share 3

Figure 3.1.5: (3,3) Shares Generated using the proposed scheme

Revealing: The system takes as input a secret key file, N share and an integer n. The shares are then operated on by the Boolean operator for reconstructing the original secret image given as input to the system. A standard *uint8* representation is used throughout the system for the inter portability across construction and reconstruction.

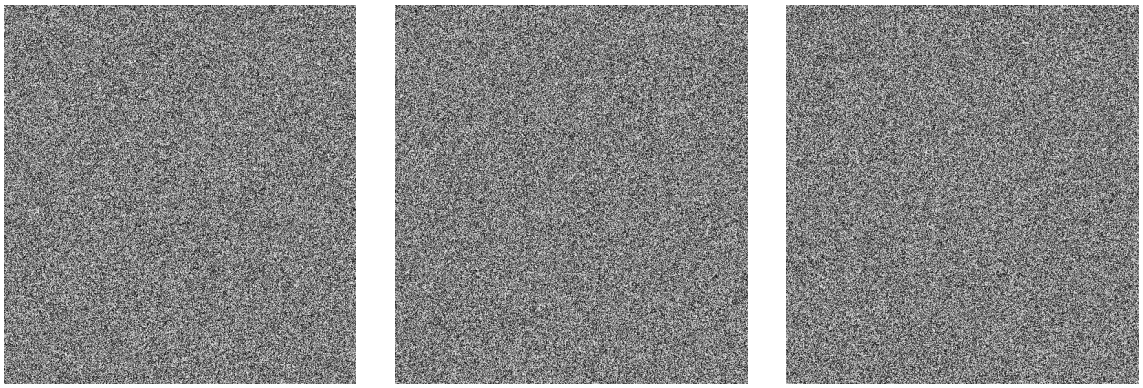
Chapter 4

Experimental Setup and Results Analysis

In this chapter we shall present the experimental results of the proposed *(n,n)* secret image sharing scheme. A (4,4) secret sharing experiment is selected to demonstrate the performance of the proposed system. The test images 'Lena', 'MNNIT Logo' are used as a secret image(input) for evaluating the systems resilience and robustness.

The 'Lena' image used for evaluation, is a gray scale image and a (4,4) scheme has been operated on it, the resultant image contained no noise or pixel expansion and was equivalent to the original image.

Figure 4.0.1: Lena Image for Secret



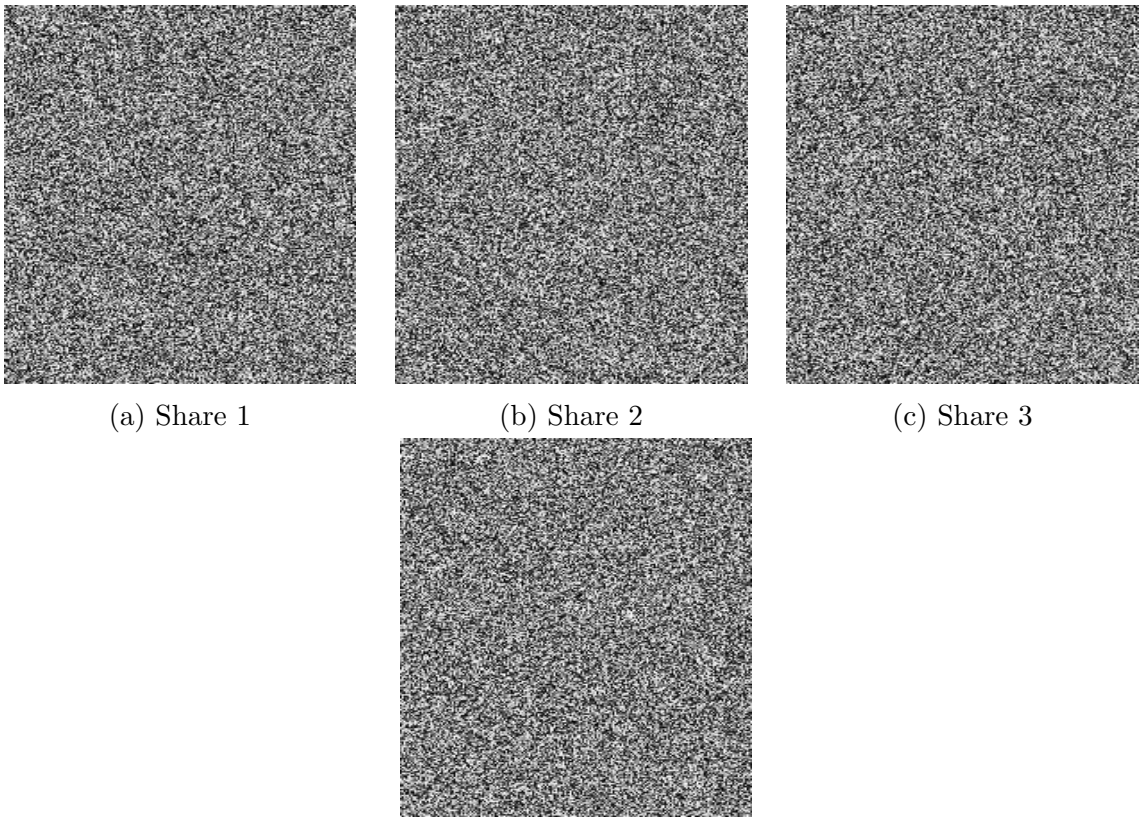
(a) Share 1 (b) Share 2 (c) Share 3

(d) Share 4

Figure 4.0.2: (4,4) Shares Generated using the proposed scheme

Figure 4.0.3: Decrypted using 4 shares 'Lena' Image

Figure 4.0.4: 'MNNIT Logo' for encryption



(a) Share 1 (b) Share 2 (c) Share 3

(d) Share 4

Figure 4.0.5: (4,4) Shares Generated using the proposed scheme

Figure 4.0.6: Decrypted using 4 shares 'MNNIT Logo' Image

4.1 Experimental System Setup

This Experiment was carried out on a personal computer.

The Hardware and Software involved are as follows.

- Intel i5-5500 2.20 Ghz dual core processor
- Fedora Linux OS 64bit
- Python 3.6 Interpreter

4.1.1 Experimental System Requirement

Processor should contain 2.2 GHz speed for better performance and System required 30GB hard disk space for the Software and Operating System and 250MB free RAM space for the application;however RAM space varies because of the image operations and image size.

4.2 Result Analysis

Peak signal-to-noise ratio is The phrase peak signal-to-noise ratio, often abbreviated PSNR, is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its

representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codecs (e.g., for image compression). The signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs it is used as an approximation to human perception of reconstruction quality, therefore in some cases one reconstruction may appear to be closer to the original than another, even though it has a lower PSNR (a higher PSNR would normally indicate that the reconstruction is of higher quality).[1]

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(I(i,j) - K(i,j))^2 \tag{2}$$

Where MSE is mean square value, PSNR is defined as

$$PSNR = 10log_{10}\frac{R^2}{MSE} \tag{3}$$

Secret & Recovered Images	PSNR	SYSTEM TICKS
MNNIT RGB Logo	9.143	0.253
MNNIT Gray Scale Logo	31.758	0.450
Lena Gray Scale	35.871	0.536

Table 1: Table Depicting the PSNR between Secret and Recovered Images

Our proposed scheme works well for gray scale and binary images, but has poorly performed on color scale, even though the PSNR is too low for the RGBA images, the visual properties of the image were retained as seen in image 3.1.4b. The performance of the scheme in comparison with the pixel expansion and co relation immunity was very good and the complexity of the scheme was on par with modern computers producing high amount of frames per second during contiguous frame encoding for secret sharing.

Image Scheme	Wang et al	Our Proposed Method
(n,n) Secret Sharing Scheme	Yes	Yes
Reconstruction Complexity	O(n)	O(n)
Tone	Binary	Binary, Gray Scale, RGBA
Lossless Secret Compression	Lossless	Lossless for Gray Scale Lossy in RGBA Color Space
Fault Tolerance Propertu	No	Yes

Table 2: Comparision between Wang et al scheme and our proposed scheme

Chapter 5

Conclusion and Future Work

A (n, n) secret sharing scheme provides for binary image, gray scale image and a RGBA image. In this paper we propose a new (n, n) secret sharing scheme, based on a bit wise XOR. In the proposed scheme even if n shares are captured or hijacked, the secret cannot be retrieved due to added cellular auomata encryption[8] at each transparency layer. XOR operations are used in the (n, n) algorithm. The proposed (2, n) scheme is probabilistic and the contrast of the recovered image is better than the existing gray scale and binary schemes. Even, the reconstruction complexity of the method proposed is O(n) due to its bit wise XOR operation.Based on the Boolean operator XOR, the proposed scheme can easily recover the reconstructed image. Experimental results confirm that our proposed scheme not only gives high reconstructed image quality with a PSNR and MES These are the main advantages of our proposed scheme compared to the existing methods. Our secret sharing can also be applied on color images but is not able to retain the transparencies.

Our future work would be focused on improving this scheme for having a loss-less share generation for the RGBA images and extend the image library to work with video encoding on the wire, using more faster hardware interfacing as Boolean operators already have custom data paths for execution and would offer better performance when improved upon.

References

[1] B, R. K., K, N. K., and G.V.S, R. K. Secret image sharing technique based on bitwise xor. *IJCSET 6*, 5 (2016), 138–143.

[2] filippo. The ECB Penguin. *Filippo.io* (Nov. 2013).

[3] Hou, Y.-C. Visual cryptography for color images. *Pattern Recognition 36* (07 2003), 1619–1629.

[4] Naor, M., and Shamir, A. Visual cryptography. In *Advances in Cryptology — EUROCRYPT'94* (Berlin, Heidelberg, 1995), A. De Santis, Ed., Lecture Notes in Computer Science, Springer, pp. 1–12.

[5] Panjwani, R. Efficient Algorithm to Share Secret Images in Visual Cryptography and Development of plugin based Android Application. Tech. rep., Motilal Nehru National Institute of Technology Allahabad, Allahabad, 2018.

[6] Shamir, A. How to share a secret. *Communications of the ACM 22*, 11 (Nov. 1979), 612–613.

[7] Shivani, S., Rajitha, B., and Agarwal, S. XOR based continuous-tone multi secret sharing for store-and-forward telemedicine. *Multimedia Tools and Applications 76*, 3 (Feb. 2017), 3851–3870.

[8] Sukhralia, L. Image encryption using cellular automata. *GeeksforGeeks* (July 2018).

[9] Youmaran, R., Adler, A., and Miri, A. An Improved Visual Cryptography Scheme for Secret Hiding. In *23rd Biennial Symposium on Communications, 2006* (May 2006), pp. 340–343.