

A Project Report
On
**“Efficient Algorithm to Share Secret Images in Visual
Cryptography and Development of plugin based Android
Application”**

*Submitted in the Partial Fulfillment of the Requirements
for the award of*

Bachelor of Technology
in
Electronics and Communication Engineering

By
Riyaz Panjwani
Ankit Kumar Saroj
Akhilesh Kumar

Under the guidance of
Dr. Shweta Tripathi
Assistant Professor



Department of Electronics & Communication Engineering
Motilal Nehru National Institute of Technology Allahabad
Allahabad – INDIA
(November, 2017)

UNDERTAKING

We declare that the work presented in the software project titled “**Efficient Algorithm to Share Secret Images in Visual Cryptography and Development of plugin based Android Application**”, submitted to the Department of Electronics & Communication Engineering, Motilal Nehru National Institute of Technology, Allahabad is our own work.

Riyaz Panjwani (20142079)

Ankit Kumar Saroj (20145137)

Akhilesh Kumar (20145087)

Department of Electronics & Communication Engineering
Motilal Nehru National Institute of Technology Allahabad
Allahabad – INDIA



CERTIFICATE

This is to certify that the work contained in the project titled **“Efficient Algorithm to Share Secret Images in Visual Cryptography and Development of plugin based Android Application”**, submitted by **Riyaz Panjwani, Ankit Kumar Saroj and Akhilesh Kumar** in the partial fulfillment of the requirement for the award of Bachelor of Technology in Electronics Communication Engineering to the Electronics Communication Engineering Department, Motilal Nehru National Institute of Technology, Allahabad, is a bonafide work of the students carried out under my supervision.

Date: 21st November, 2017

Place: Allahabad

Dr.Shweta Tripathi
Assistant Professor
ECE Department,
MNNIT Allahabad

Acknowledgements

We take this opportunity to express our deep sense of gratitude to our project supervision, **Dr. Shweta Tripathi**, Department of Electronics & Communication Engineering, **Motilal Nehru National Institute of Technology, Allahabad** for his constant guidance and insightful comments during the course of the work. We shall always cherish our association with mam for her constant encouragement and freedom to thought and action rendered to us throughout the work.

We are also grateful to **Dr. Vijaya Bhadauria (Head of the Department ECED, MNNIT Allahabad)** and other faculty member of ECED ,MNNIT Allahabad for providing there expertise and technical support in the implementation. Without their superior, knowledge and experience, the project would have lacked in quality of outcomes, and thus their support has been essential.

We are also thankful to 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.

Date: 30th November 2017

Place: Allahabad

Riyaz Panjwani (20142079)

Ankit Kumar Saroj (20145137)

Akhilesh Kumar (20145087)

Abstract

In modern era, due to everything has been Digitalized Starting from Social Media to Digital Payment. Even bio-metric verification is now being supported in many of the Mobile Phones. Mobile Phones have been the primary source of Data Traffic due to the latest improvements in Communication Technology. For Example: 4G VoLTE Services, NFC (Payments & Authentication), Mobile Wallets, Social Media etc. This lead to colossal increase in Network Traffic and has called for efficient Secret Sharing Algorithms through which private information can be safeguarded without compromising on security and keeping in mind complexity of systems. One approach to have the essential information secure not retrieved by malicious users easily is making the essential information shared among several participants. Consequently, the secret sharing schemes are proposed to be one of candidates for solving this security concern.

Visual Cryptography is a cryptographic technique which allows Visual Information (pictures, text etc.) to be encrypted in such a way that the decryption becomes the job of the person to decrypt via Human Visual System (HVS). One of the best know techniques has been credited to **Moni Naor** and **Adi Shamir**, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k -out-of- n visual cryptography.

There was a need to extent the secret sharing for multiple secret images, so that the bandwidth of the system can be effectively utilized while giving just the appropriate amount of Data to the participants, at the same time embedding this technology in an Android Application helps the developers / researchers understand the market use of this technology. The Android Application Developed by us can be used as a plugin based application (plugin the suitable VC Algorithm and it works seamlessly).

List of Figures

Fig.no.	Page no.
Fig.2.1. Illustration of concept behind traditional (2,2) VCS Scheme	6
Fig.2.2 Illustration of Encryption of Polynomial based SIS Scheme	6
Fig.2.3 Illustration of Decryption of Polynomial based SIS Scheme	7
Fig.3.1.1 Experimental results of Naor and Shamir (2,2) VCS (a)secret image (b) Share 1(c) Share 2	10
Fig.3.1.2 Illustration of working of Naor's and Shamir (2,2) VCS Scheme	11
Fig.3.2.1 Simulation results of Thein Lin Polynomial based (4,6) SIS Scheme (a)Secret Image (b)share 1(c) shares 2(d) share 3(e) share 4(f) share 5(g)share 6	13
Fig.3.3.1Simulation results of probabilistic DNA XOR VSS (a) Secret Image (b) share1 (c) share 2(d) share3	14
Fig.3.3.2 The Automata of XOR Operator for DNA Sequence	15
Fig.3.4.1 Simulation results of Multi- Secret Sharing based on Boolean Operators (a)Secret image of circuit (b)Secret image of cameraman(c) Secret image of coins (d)Share1 (e) Share 2 (f) Share 3(g) Share 4	16
Fig.3.5.1 Simulation results of RGVS for Color Image(a)Secret Image(b)R component of secret(c)G component of secret (d)B component of secret(e)R component of Share(f)G component of secret(g)B component of secret	17
Fig.3.6.1 Frames of Content Change (frame no1)	20
Fig.3.6.2 Frames of Content Change (frame no2)	21
Fig.3.6.3 Frames of Content Change (frame no3)	21
Fig.3.6.4 Halftoned Frame for Processing (Jarvis Halftone Algorithm)	22
Fig.3.6.5 Watermarking Image (cameraman)	22
Fig.3.6.6 Simulation results of secret key (using MATLAB)	23
Fig.3.6.7 Verification vector (vi)generated (simulation using MATLAB)	23
Fig.3.6.8Recovered watermark (simulation using MATLAB)	23
Fig.4.4.1 (a)Screenshot of application named "My App" (b)Zoomed icon of application	27

Fig.4.4.2(a) Encryption / Decryption Scheme(b)On – Click Encryption button	27
(c)Scan picture if not available	
Fig.4.4.3(a)Automatic Edge Detection(b)Grey Image Filter(c)Black and White Filter	28
Fig.4.4.4(a)Image after being scanned(b)Key and Cipher of Encrypted Image	28
(c)Image Cipher Stored in scanned_images folder	
Fig.4.4.5(a)Decryption Screen(b)VCS gesture movement(c)Decrypted Image	29
(The quality has been reduced intentionally – for the sake of presentation)	
Fig.5.2.1 Illustration of proposed algorithm	31
Fig.5.3.1 Simulation results (selecting the no of images)	32
Fig.5.3.2 (a) Secret image1(circuit)(b)Secret image2(cameraman)(c)Secret Image3 (Eight)	32
Fig.5.3.3 Simulation results (a)Share1 (b)Share 2 (c)Share3	33
Fig.5.3.4 Simulation results (a) Recovered image1 (b) Recovered image2	34
(c)Recovered3	
Fig.5.3.5 PSNR & MSE values of Share Image3 compared with original Secret Image	35

List of Tables

Table No.	Page No.
Table.3.3.1 Eight kinds of Schemes encoding map of DNA	15
Table.3.6.1 Rules to assign values of verification information	19

Contents

Contents	Page No.
Undertaking	i
Certificate	ii
Acknowledgement	iii
Abstract	iv
List of Figures	v
List of Tables	vi
1.Introduction	1
1.1.Motivation	1
1.2. Objective	2
2. Visual Cryptography	3
2.1. Introduction to Visual Cryptography	3
2.2 Applications of Visual Cryptography	7
3.Analysis of Various Cryptographic Schemes	9
3.1 Naor and Shamir (2,2) Visual cryptographic scheme	9
3.2 Thein Lin Polynomial based (4,6) Threshold Secret	11
3.3 Probabilistic DNA XOR Visual Secret Sharing	13
3.4 Multi Secret Sharing based on Boolean Operation	15
3.5 Extension of random grid based VCS to colored	16
3.6 Watermarking Video Content using VCS	18
4. Android Application That Implements VCS Scheme	23
4.1 Need for an Android Application	23
4.2 Feature Implements in Android Application	23
4.3 Enhancement in applied VCS Technique	24
4.4 Screen Shots of Android Application	26
5. Scheme to Share Multiple Image in VCS	29
5.1 Previous Works	29
5.2 Proposed Scheme	30
5.3 Simulation Result	31
5.4 Result and Discussion	34
5.5 Conclusion	35
References	37

Chapter 1

Introduction

1.1 MOTIVATION

Due to everything has been Digitalized Starting from Social Media to Digital Payment. Even bio-metric verification is now being supported in many of the Mobile Phones. It is now the primary source of Data Traffic due to the latest improvements in Communication Technology. For Example: 4G VoLTE Services, NFC (Payments & Authentication), Mobile Wallets, Social Media etc. This lead to colossal increase in Network Traffic and has called for efficient Secret Sharing Algorithms through which private information can be safeguarded without compromising on security and keeping in mind complexity of systems. One approach to have the essential information secure not retrieved by malicious users easily is making the essential information shared among several participants. Consequently, the secret sharing schemes are proposed to be one of candidates for solving this security concern.

According to Cisco Visual Network Index (VNI) forecast projects IP traffic to triple over the span of next 2 years. As of today, the Internet traffic is around 122 EB (Exabyte) per month. Growth of Video Streaming Sites like Netflix & You Tube account for more than 45% of the Internet Traffic in North America. On an average (Globally) 345 GB of data is generated per second. Not only the Internet, important information like military maps, nuclear codes, UN Resolutions, Financial Bonds, Collateral papers, Credit / Debit Card Information, Passwords, private data (images/videos) and many other assets which need high level of security have grown exponentially over time. Black Hat Hackers work on breaking the loopholes by various protocols, Due to inconsistent implementation or some weak password they can break into the server and steal essential information. For Large companies like Facebook, Google which store PB or more of important data cannot practically encrypt the data due to huge computation complexity while encryption and decryption.

This has led to development of alternate Cryptographic techniques which could encrypt the data efficiently and decrypt effortlessly. Visual Cryptographic Schemes have their

own flaws and strengths which we could analyse, this would lead us to develop our own Visual Cryptographic Scheme to Share Multiple Secret Images. To bridge the gap between Research and Market use of this schemes, we have developed a plugin based Android Application.

1.2 OBJECTIVE

Right to Privacy is a fundamental right and an intrinsic part of Article 21 that protects life and liberty of the citizens and as a part of the freedoms guaranteed by Part III of the Constitution. In June 2011, India passed a new privacy package that included various new rules that apply to companies and consumers. A key aspect of the new rules requires that any organization that processes personal information must obtain written consent from the data subjects before undertaking certain activities. Application of the rule is still uncertain. The Aadhar Card privacy issue become controversial when the case reached Supreme Court.

The main objective of Visual Cryptography in the context of achieving privacy is that, if an intruder gets some of the shares of the distributed shares, in other words even if some of the participants are compromised then the attacker should not be able to decrypt the secret by himself even by using the most advanced computer technology. If such a scheme is designed then, it would facilitate 100% security even over weak communication channels like WPA, HTTP or Bluetooth. Meaning, even eaves dropping or data sniffing would be useless to break the security and decipher the secret image.

The task of Visual Cryptography is particularly difficult for two reasons:

1) The recovered quality of random grid based schemes is not 100% (loss of contrast) and 2) Pixel expansions is observed when using pre-defined codebooks (suggested by Naor & Shamir) or using polynomial schemes. In addition, while using Polynomial based VSS the complexity is very high, implying that the decryption of as big as 512*512 image can take as much as 30-35 minutes in encryption process. A system for Sharing Multiple Secret Images efficiently (without compromising security and achieving optimum trade-off for contrast vs pixel expansion).

Chapter 2

Visual Cryptography

2.1 INTRODUCTION TO VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes the job of the person to decrypt via sight reading.

One of the best-known techniques has been credited to **Moni Naor** and **Adi Shamir**, who developed it in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. There are several generalizations of the basic scheme including k -out-of- n visual cryptography.

Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the ciphertext. Normally, there is an expansion of space requirement in visual cryptography. But if one of the two shares are structured recursively, the efficiency of visual cryptography can be increased to 100%. Some antecedents of visual cryptography are in patents from the 1960s. Other antecedents are in the work on perception and secure communication. Visual cryptography can be used to protect biometric templates in which decryption does not require any complex computations.

Few years later, Verheul and Tilborg developed a scheme that can be applied on colored images. The inconvenient with these new schemes is that they use meaningless shares to hide the secret and the quality of the recovered plaintext is bad. More advanced schemes based on visual cryptography were introduced in where a coloured image is hidden into multiple meaningful cover images. Chang et al. introduced in 2000 a new coloured secret sharing and hiding scheme based on Visual Cryptography schemes

(VCS) where the traditional stacking operation of subpixels and rows interrelations is modified. This new technique does not require transparencies stacking and hence, it is more convenient to use in real applications. However, it requires the use and storage of a Colour Index Table (CIT) in order to losslessly recover the secret image. CIT requires space for storage and time to look up the table. Also, if number of colours increases in the secret image, CIT becomes bigger and the pixel expansion factor becomes significant which results in severe loss of resolution in the camouflage images. Broadly Visual Cryptography can be classified into 2 categories:

1. Random Grid based VCS (RGVCS) schemes
2. Polynomial based Secret Image Sharing (Polynomial based SIS) schemes

Although the classification is not complete yet it can be used to get a broad idea in-regard to how the Secret Sharing Schemes functions under the hood.

In Random Grid based VCS, the concept of Randomness is used. It lies on the fact that, when a Random Grid technique is used the resultant accuracy cannot be 100%. Hence, we try to obtain the black pixels as they store the information and white pixels are recovered with 50% accuracy. Hence, the background is more of Black Color. This can be easily extended to Color Images where the space is divided into separate RGB or CYM components and all the Processing is done in orthogonal planes. The resultant image is formed by stacking all the orthogonal planes together.

Following is the crux of RGVCS Schemes:

- Each Pixel is divided into m (≥ 2) closely spaced sub-pixel.
- Decryption is done by Human Visual System (HVS) by stacking all the images.
- Pixel is considered:
 - Black: $H(V) \geq d$ (Threshold value)
 - White: $H(V) \leq d - \alpha * m$ (α – loss in contrast, m – loss of resolution in shared image from original)
 - $H(.)$ is the Hamming weight of “OR”ed m -vector V .















Secret pixel				
Basic matrices	$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$		
Matrix collections	$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Shadow image1				
Shadow image2				
Probability	50%	50%	50%	50%
Stacking result(OR)				

Fig 2.1 *Illustration of concept behind traditional (2,2) VCS Scheme*

In Polynomial based SIS a polynomial is constructed using the pixels of the Secret Image. Then, the values of the pixels of the Shares are obtained by substituting Random Values in the later generated Polynomial. At the Decryption end, the values of all the Shares are used to generate back the original pixel values by reconstructing the original polynomial by using various interpolation techniques like Lagrange interpolation, Newton Divided Difference or Spline Interpolation etc.

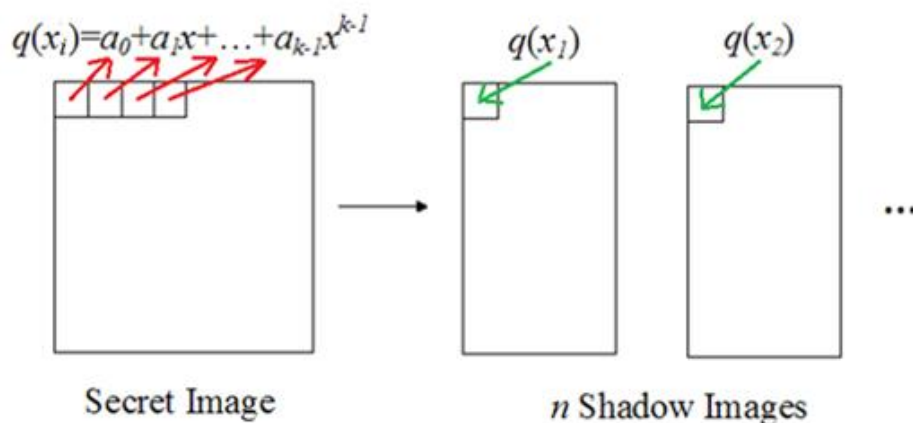


Fig 2.2 *Illustration of Encryption of Polynomial based SIS Schemes*

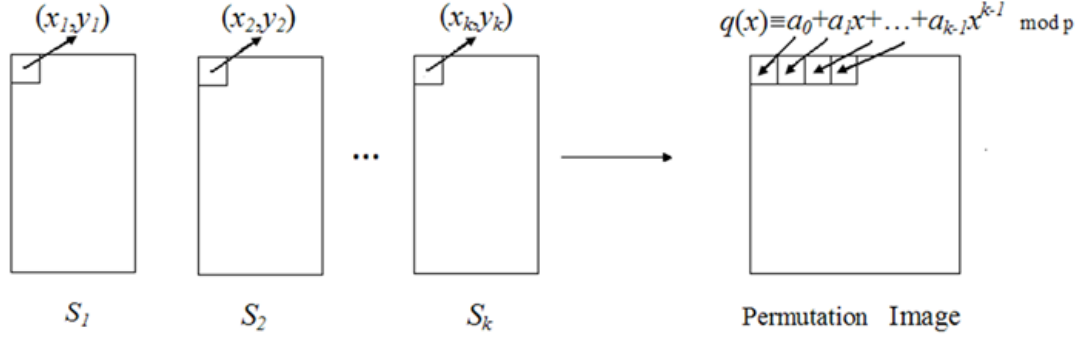


Fig 2.3 Illustration of Decryption of Polynomial based SIS Schemes

To illustrate this, consider Fig 2.2 and Fig 2.3:

- Consider a polynomial $g(x) \equiv a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \pmod{25}$ – Equation 2.1
- Select n distinct secret keys x_1, x_2, \dots, x_n .
- Deliver $(x_i, s(x_i))$ to the i th participant.
- Use Lagrange interpolation to reconstruct the image.
- There will be no loss of contrast in Image.

There is a trend to develop friendly Share images as they are less suspect able to the intruder and hence the attack is less probable. The motivation behind this is obtained from Stenography (Image Hiding) Techniques.

Now-a-days VC is also being used in Water Marking without embedding any additional data on the original image. This can be used to issue copyright and in identification of where the image (painting, document, record, transaction) is original or duplicate. A modified concept of VCS can be used to store Crypto Currency so that even if the intruder manages to get some information from the compromised system, it is of no use.

2.2 APPLICATIONS OF VISUAL CRYPTOGRAPHY

The main aim of Visual Cryptography is secure store of data. The data can be some private / confidential image or document, public keys, secret key for various encryption algorithms, video data, military codes, password, text file or some medical prescription. VCS finds its uses in many applications where a secure data has to be transmitted over a compromised / not-secure channel. The Decryption is solely through HVS (Human Visual System) or Simple Embedded System (with minimal logic).

Applications of Visual Cryptography is widespread including:

- Bio-metric Authentication
- Medical prescription authorization
- Copyright on information
- Progressive quality enhancement (video streaming)
- Identification purpose
- Cryptographic Key protection
- Chat encryption
- Storing Credit / Debit Card Information

VCS Schemes can be used in bio-metric verification. The Bio-metric of the person can be safeguarded using VCS Schemes on various servers of the organization. If an intruder manages to hack a server due to some security loop-hole. The attacker has information on the shares (some of them) but cannot recover the whole secret (fingerprint or some biometric information).

Many of us use mobile phones to save photos of Credit / Debit Cards, Password Documents or some private information (images/videos). If the information is stored without any encryption malicious trojan or application may try to hack into the gallery of the Mobile Phone and transmit all information over ftp / http channel. Since, it is time consuming to encrypt and decrypt the saved data, Visual Cryptography can be used to safeguard personal data by storing share images instead of the images themselves.

Cryptographic Schemes like AES (Advanced Encryption System) or 3- DES (Data Encryption Algorithm) uses Secret Key and Public Key to encrypt the data. Even though public key is used for identification and nothing about secret key can be obtained using Public Key, but, how can the Secret Keys themselves be protected? One of the methods is Visual Cryptographic Schemes allow to safe guard the Secret Keys.

In India, Aadhar Card is linked with Bank Account and personal information is stored in it. If an individual manages to spoof these details then it could be troublesome to the Governmental Organizations. Instead Copyright can me maintained on the Cards.

Wang and Hsu proposed a tagged VC (TVC) scheme in which more secret images can be revealed by the folding up operation. Specifically, when we fold up a share along its midline, an additional secret image is visually presented. Obviously, the folding up operation is easier for participants.

Chapter 3

Analysis of Various Cryptographic Schemes

3.1 Naor and Shamir (2,2) 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 3.1.1. 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.

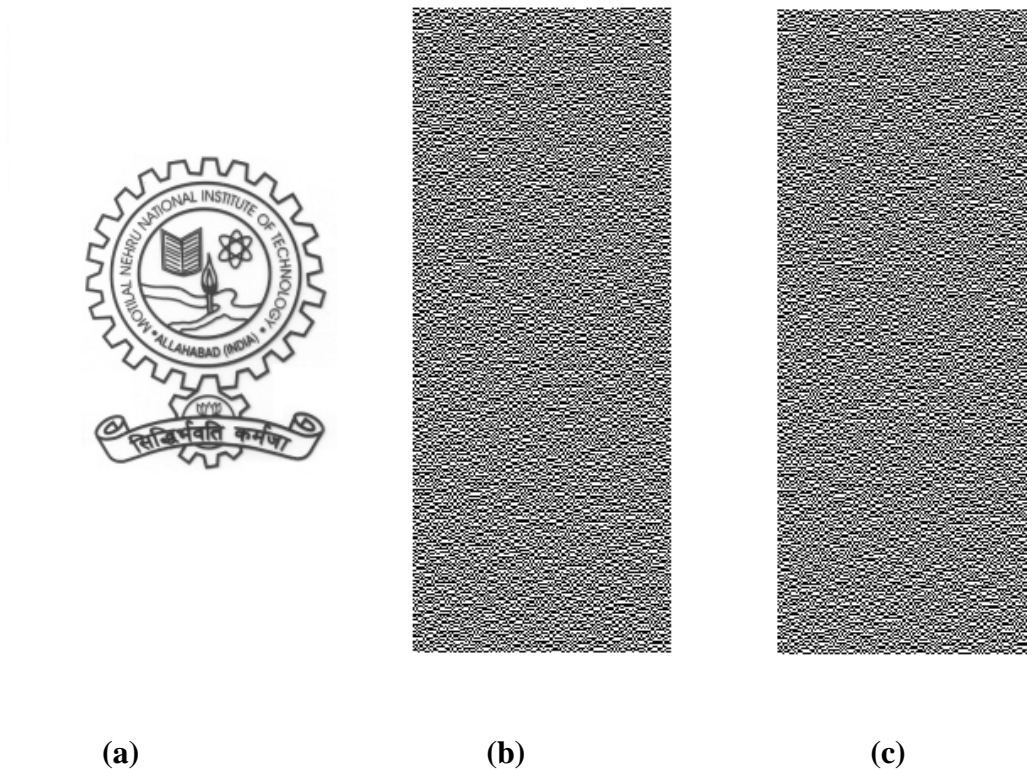


Fig 3.1.1 Experimental results of Naor and Shamir (2,2) VCS (a) Secret Image (b) Share 1 (c) Share 2

The important parameters of a scheme are:

- m , the number of pixels in a share. This represents the loss in resolution from the original picture to the shared one. We would like “ m ” to be as small as possible.
- a , the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original picture. This represents the loss in contrast. We would like a to be as large as possible.
- r , the size of the collections C_0 and C_1 (they need not be the same size, but in all of our constructions they are). $\log r$ represents the number of random bits needed to generate the shares and does not affect the quality of the picture.

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.

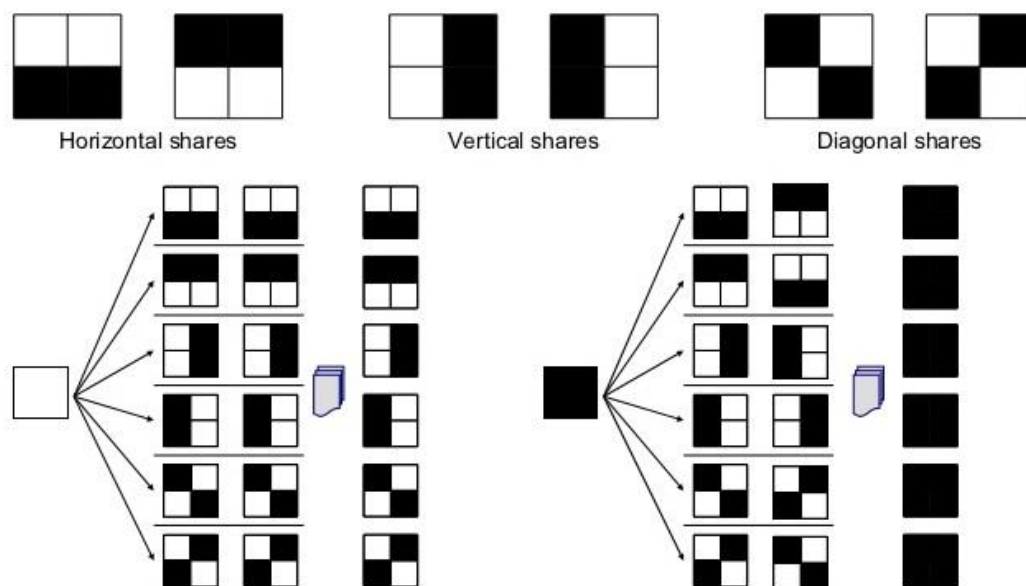


Fig 3.1.2 Illustration of working of Naor's and Shamir's (2,2) VCS Scheme, White pixel has 50% probability of recovery and black pixel has 100% probability

Pros:

- Generates Random Pixels
- Cannot be attacked by attacker
- Complexity is $O(1)$ for Encoding and Decoding

Cons:

- Suffers from loss of Contrast
- Not 100% Recovery
- Undergoes Pixel Expansion
- Cannot be applied to Multiple Secret Sharing

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

Suppose that we want to divide the secret image S into n shadow images ($S_1 \dots S_n$), and the secret image S cannot be revealed without k or more shadow images. In this method, we generate the $k-1$ -degree polynomial, by letting the k coefficients be the gray values of k pixels. Therefore, the major difference between our method and Shamir's is that we use no random coefficient. Because the gray value of a pixel is between 0 and 255, we let the prime number p be 251 which is the greatest prime number not larger than 255. To apply the method, we must truncate all the gray values 251–255 of the secret image to 250 so that all gray values are in the range 0–250. (If we do not want to change the gray values of the secret image, there is a lossless secret image sharing method which uses *Galios Field*) 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 j ; we define the following $k-1$ -degree polynomial.

$$g(x) \equiv a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1} \mod 251 \quad \text{-- Equation 3.1}$$

The possibility of obtaining the right image is only $(1/251)^{(512 \times 512)/k}$, which is pretty low.

Pros:

- Extension of Shamir's VCS that includes Polynomial based techniques
- 100% Image Recovery at Decrypting end (Lossless)

Cons:

- Applicable to only Grey Scale Images
- Cannot be extended for Multiple Images
- System hangs when applied to larger images
- Complexity at decryption end varies depending on programming language (MATLAB – {Encryption - $O(n \times k \times h \times w \times \text{complexity}(\text{polyval}))$ Decryption – $O(n \times \log^2(k))$ – Lagrange Interpolation})

- McCabe Complexity of interpolate in MATLAB is 41
- McCabe Complexity of Encryption Code is 11
- Reuse of Shares is not possible

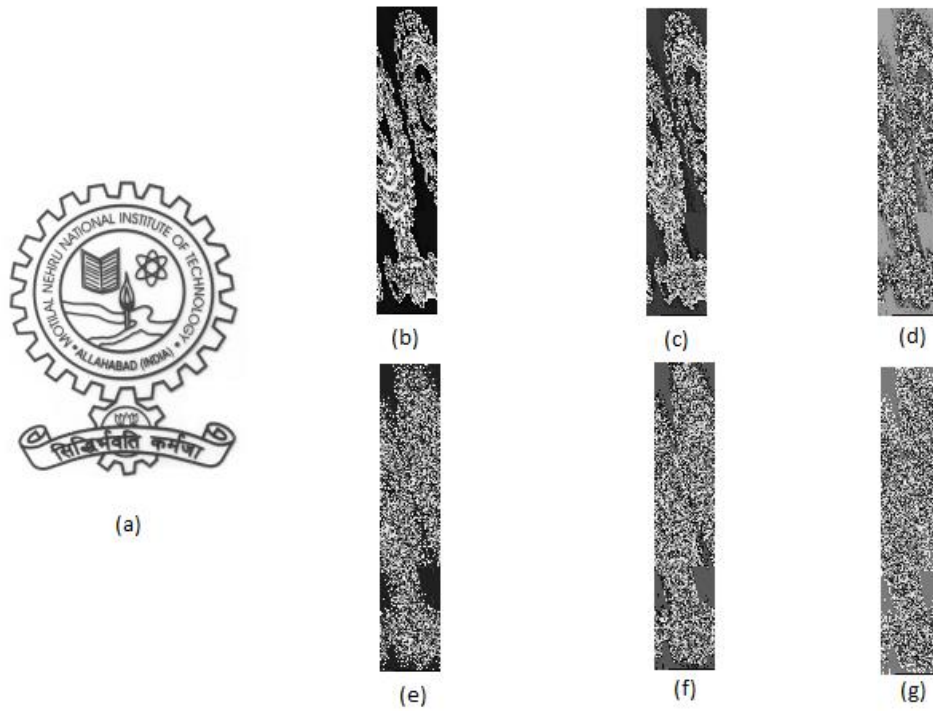


Fig 3.2.1 Simulation results of Thein Lin Polynomial based (4,6) SIS Scheme, (a) Secret Image (b) Share 1 (c) Share 2 (d) Share 3 (e) Share 4 (f) Share 5 (g) Share 6

3.3 Probabilistic DNA XOR Visual Secret Sharing Scheme.

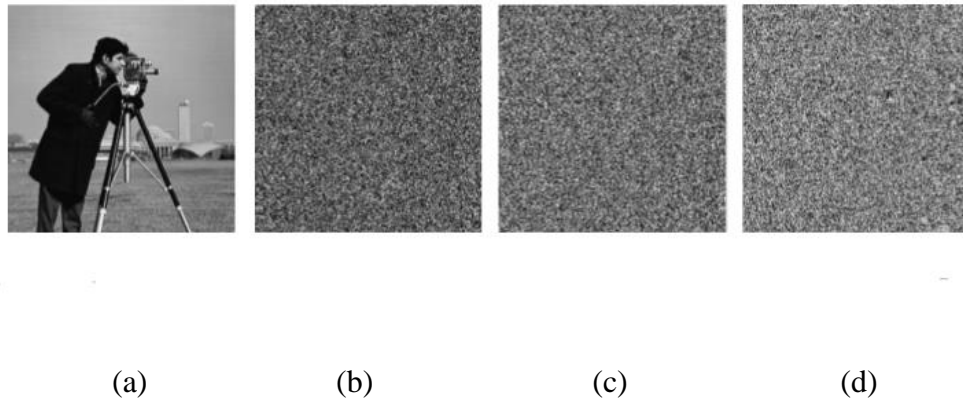


Fig 3.3.1 Simulation results of Probabilistic DNA XOR VSS (a) Secret Image (b) Share 1 (c) Share 2 (d) Share 3

Secret sharing based methods have been introduced to protect the reliability of the encryption key or data. Shamir's (k,n) threshold method is the best known of these methods. Purpose of secret sharing is to provide the key reliability. In the literature, many secret sharing based data hiding algorithms are proposed. To achieve an optimum data hiding scheme, a new probabilistic secret sharing method is proposed. The DNA XORing scheme is similar to Wang's scheme. The probabilistic DNA-XOR secret sharing scheme is applied on a test image. The test image is divided into secret shares by using the probabilistic DNA-XOR secret sharing scheme and results are given in Fig. 3.3.1.

In a DNA sequence, there are four different nucleic acids which are, A (adenine), T (thymine), C (cytosine), and G (guanine). Therefore, Watson–Crick complement rule is valid in here. Table 3.3.1 shows encoding and decoding map by using DNA sequence in this paper. The Watson–Crick complementarity rule gives fundamental information which can be transferred to daily life. Firstly, a color image is separated to RGB channels. Secondly, these RGB channels are converted to binary coding. Then, each pixel of RGB channels can be expressed as a DNA sequence. For example, the binary code of the pixel value of blue channel image is [1 1 0 1 0 0 1]. DNA sequence of this binary code is [T A G C] according to Table 3.3.1.

Table 3.3.1 Eight Kinds of Schemes encoding map of DNA

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

Pros:

- Cover Images can be used (To make the shares Friendly and less Susceptible)
- DNA XORing is used (which uses a set of 8 encoding techniques) so it is reliable.
- BER for Lena Image was found to be ~ 0.01 , PSNR (using MATLAB) was found to be 59.89dB using Lena Image.
- Payload (according to Paper using MATLAB 2013a) was around 2bpp (bit per pixel).

Cons:

- Decryption is performed at the receiver's end.
- Calculates MSE of all probabilities to ensure perfect reliability, hence computationally complex.
- Can be attacked based on studies (Likelihood approximation) if k-1 shares of given secret are found.
- SSIM was found to be 0.98 (Better schemes have 0.99)

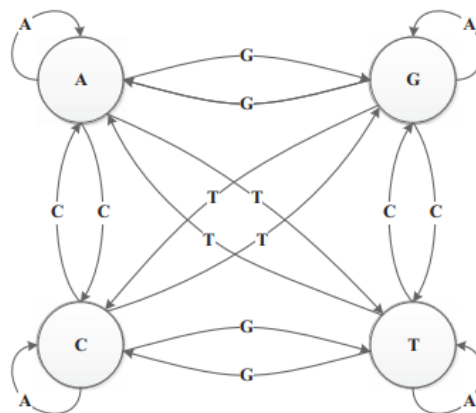


Fig 3.3.2 State Diagram of XOR Operator for DNA Sequence

3.4 Multi Secret Sharing based on Boolean Operators

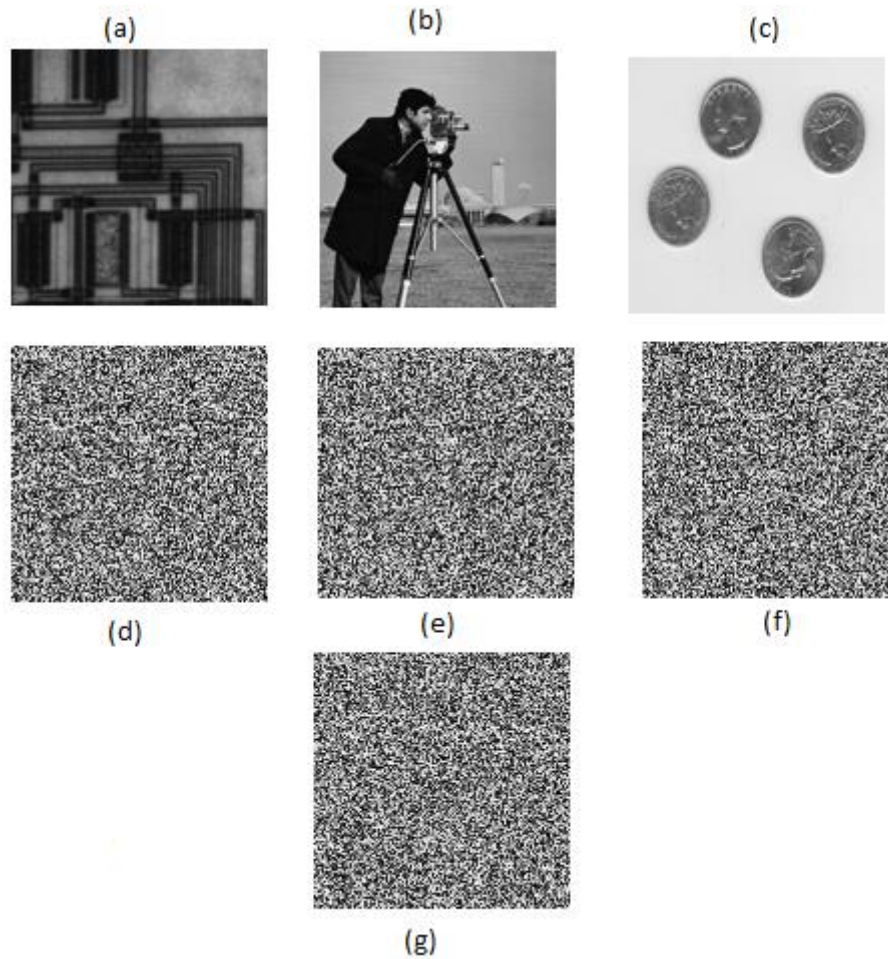


Fig 3.4.1 Simulation results of Multi-Secret Sharing based on Boolean operators (a) Secret Image of Circuit (b) Secret Image of Cameraman (c) Secret Image of Coins (d) Share 1 (e) Share 2 (f) Share 3 (g) Share 4

A new $(n+1, n+1)$ multi-secret scheme based on Boolean based VSS is analyzed to enhance the Sharing Capacity of VSS. TO begin with, the Boolean-based VSS technology, used to encode the secret images, generates n random matrices; then the n secret images, generates n random matrices, then the n secret images are encoded into $n+1$ meaningless shares. In decoding phase participants collect $n+1$ shares to obtain the recovered image.

Pros

- Can be extended for Coloured Images
- McCabe Complexity of the Code is 5 (For Encryption) $O(h*w)$ & 1 (Decryption based on ORing)
- It uses $N+1$ shares for N secret images (Lower bandwidth).
- Lossless Scheme with NO Pixel Expansion and NO Codebook at decryption end.
- Sharing Capacity = $N/(N+1)$ & Computationally Efficient.
- No Pixel Expansion and better contrast is found.

Cons

- Secret Sharing Schemes are known which uses 2 Share images to recover N images (Rotation of Stacked Image).
- Does not generate meaningful shares hence can be suspect able to attack.
- It doesn't implement threshold secret sharing.
- Shares are not friendly (Can be suspected by attacker).

3.5 Extension of Random Grid Based VCS to Coloured Images

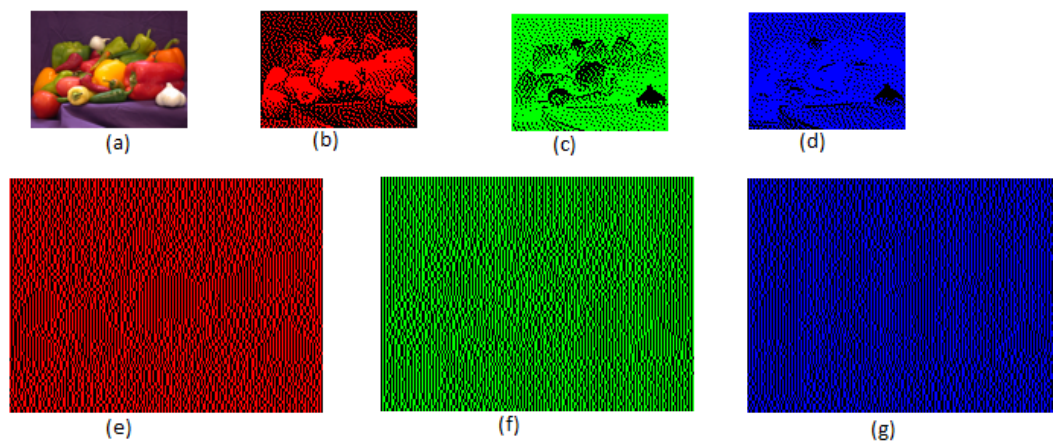


Fig 3.5.1 Simulation results of RGVS for Colour Images (a) Secret Image (b) R component of Secret (c) G component of Secret (d) B Component of Secret (e) R Component of Share (f) G Component of Share (g) B Component of Share

This scheme utilizes the fact that we can divide the given image into various components (RGB) components. It is generally more feasible to use CMY Colour model and then convert the image back to RGB model.

First, the image is segregated into its 3 dimensions. Now, the range of values of each dimension is (0, 255). Since, it is desirable to work with logical values while using Random Grid based techniques, it is necessary to convert the given pixels to Boolean values. There are 2 methods to achieve this: (a) Treat the values as grey scale values and convert each of the components to Boolean values using a threshold value (For e.g.: If $> 125 \rightarrow 1$ else 0). (b) To use halftoning for converting RGB / CMY Components to Boolean values.

We have observed that halftoning gives better results, hence we have used Jarvis Halftoning to perform Halftoning. A stacking image, which is basically a random grid is generated and used to obtain the other share. During decryption, recovered image is obtained by stacking the given images along with a stacking image which was used during the encoding process.

Pros:

- Works well for Coloured Images (Shares are Unidentifiable)
- Cannot be broken due to Randomization Nature of the Algorithm and Increased Dimensionality
- McCabe Complexity for the Encryption Code is $11(O(n*k*h*w))$ and Decryption Code is 1 ($O(1)$ -- Stacking)
- Halftoning is used (to make logical decision while forming shares) – We have implemented it using Jarvis Halftoning Algorithm (McCabe Complexity is 9)
- Can be decrypted by Human Visual System.

Cons:

- Suffers from Pixel Expansion (Size increases by 2-fold).
- Suffers from reduced Contrast in the recovered image.
- For Sharing a single secret 4 shares (3 CMY Shares and one Random Stacking Sharing) are required (Increase in bandwidth).

3.6 Watermarking Video Content using Visual Cryptography & Scene Average Image

Digital watermarking has been effectively used to protect the copyright of digital multimedia data. In digital watermarking of images, a watermark pattern is embedded on the original image to be watermarked. The watermark on the marked image can either be visible or invisible. A visible watermark is a visible translucent watermark pattern which is overlaid on the original image. Visible watermarks distort the fidelity of original images and are susceptible to direct image processing attacks. Invisible watermark methods hide the watermark pattern either in the spatial domain or in the frequency domain which are perceptible to watermark attacks. Many watermark methods have been proposed in the literature. Some of these methods are built on the concept of Visual Cryptography.

Ren-Junn Hwang proposed a novel scheme for watermarking digital images using the principles of visual cryptography. In this scheme, the owner of a digital image selects a black and white image as watermark pattern. Then, Verification Information vector (VI) is generated from the original image to be watermarked based on (2,2)-visual cryptography with the watermark pattern as the shared image. A secret key is used to generate the VI for the image and watermark combination. The secret key is one share of visual cryptography and VI is the other share. Both these shares are required to extract the watermark pattern from a suspect image that can be visually examined. Thus, rather than embedding any information into the image, information is extracted from the image by applying the principles of visual cryptography. This extracted information is used to verify the copyright of the image. The copyright holder of the image needs to register the corresponding watermark pattern and verification information with a notarial organization before releasing the image to any other person. In the event of any dispute, the copyright holder of the image needs to submit the secret key and the registration information of corresponding watermark pattern and verification information of the image. The notary will carry out the verification process and use the time stamp of the registration to establish the ownership.

3.6.1 Procedure of Watermarking

The process to generate VI for watermark pattern W of size $h \times l$ and an original 256 gray-levelled image I of size $m \times n$ is as follows:

- Select a random number S as the secret key for the image I .
- Using S as the seed, generate $h \times l$ random numbers over the interval $(0, m \times n)$. i th random number is denoted as R_i .
- Using Table 2, assign (V_{i1}, V_{i2}) of i th pair of VI.
- Construct VI by assembling all the (V_{i1}, V_{i2}) pairs.

Table 3.6.1 Rules to assign values of verification information

Colour of i^{th} pixel in W	MSB of R_i^{th} pixel of Image I	Assign (V_{i1}, V_{i2}) of VI to be
Black	1	(0,1)
Black	0	(1,0)
White	1	(1,0)
White	0	(0,1)

3.6.2 Simulation Results:



Fig 3.6.1 Frames of Content Change (Frame Number 1)



Fig 3.6.2 Frames of Content Change (Frame Number 102)

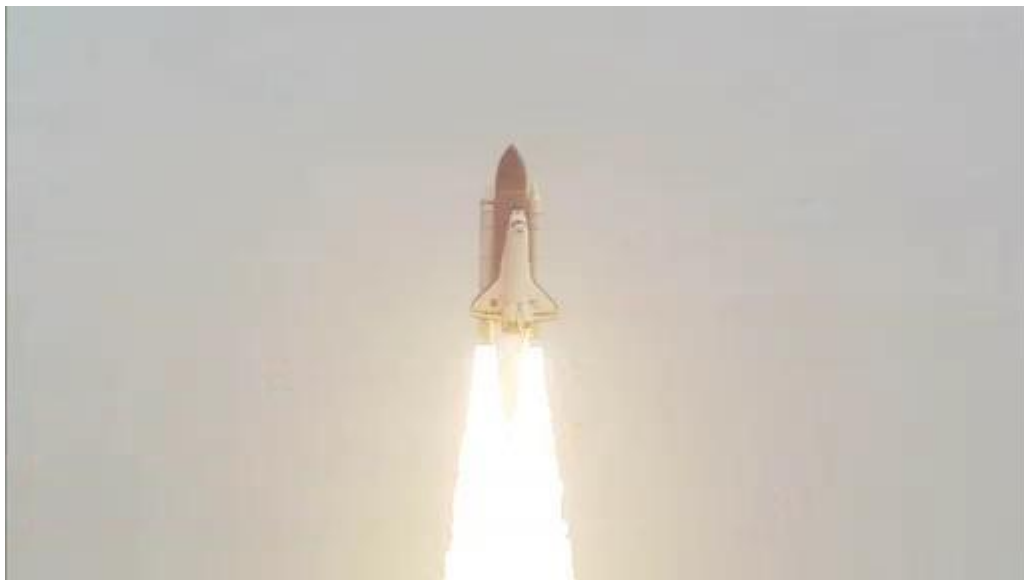


Fig 3.6.3 Frames of Content Change (Frame Number 113)

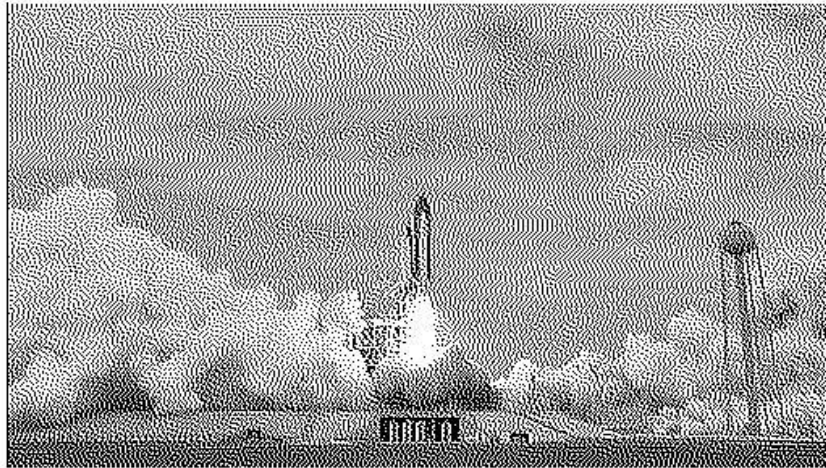


Fig 3.6.4 Halftoned Frame for processing (Jarvis Halftoning Algorithm)



Fig 3.6.5 Watermarking Image (cameraman)

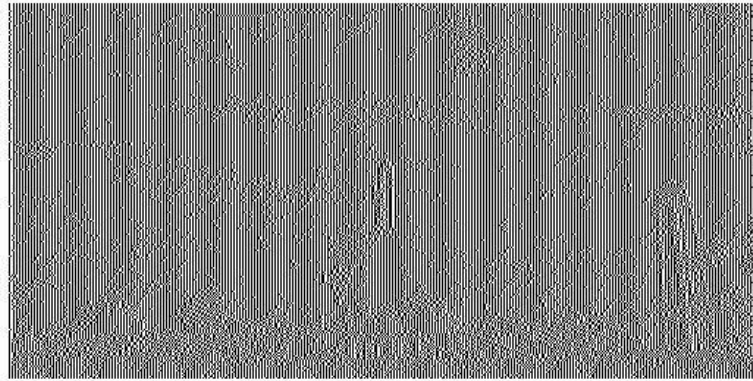


Fig 3.6.6 Simulation results of Secret Key (using MATLAB)

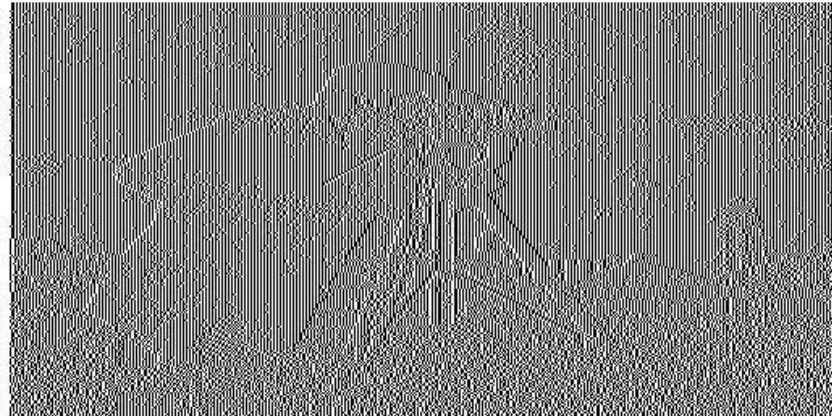


Fig 3.6.7 Verification Vector (VI) generated (Simulation using MATLAB)



Fig 3.6.8 Recovered Watermark (Simulation using MATLAB)

Chapter 4

ANDROID APPLICATION THAT IMPLEMENTS VCS SCHEMES (PLUG IN BASED)

4.1 Need for an Android Application

So far, we have analyzed various Visual Cryptography Schemes and drawn important conclusions out of them. We have analyzed various parameters by which we could compare two different schemes based on performance. The thing that is common with every scheme is that they perform encryption and decryption (mostly human visual system). We thought to implement an interface where any user with zero knowledge of cryptography can use its techniques to directly.

This would also help developers / researchers to directly use this app since it is plugin based. Meaning, you can plug in the desired algorithm and the app would work seamlessly.

Now-a-days most of the phones support Android, so we chose an android application to demonstrate. More over the attacks on Android Devices are relatively more than any other Mobile Operating System.

Implementation of App not only serves as a demonstration of various VC Schemes, it also allows for Efficient and Secure Sharing of images, even over a compromised communication channel.

4.2 Features implemented in Android Application

The following features are supported in the App designed:

- User Friendly GUI (Graphical User Interface)
- Option to SCAN Image using Camera
- Option to directly choose image from Gallery

- Option to apply filters (Change to gray, black and white & magic color)
- Option to SAVE scanned image
- Perform Edge Detection while Scanning
- Option to crop the Scanned Image (Polygonal Style)
- Option to decrypt the Selected Shares
- Use gestures to move image across so that they overlap and HVS can decrypt the image.

We have used java as our coding language, Android Studio 2.3.3

4.3 Enhancements in applied VCS technique

Traditional VCS Scheme which uses random grid are easy to implement but they suffer from loss of contrast and pixel expansion. This is because of the Random nature of the Shares which give them inherent property to be free from attacks / less susceptible to intruder. We have implemented one such scheme which utilizes the code book as given in Naor and Shamir (2,2) VCS Scheme.

Although the main purpose of this app is to facilitate the research, we thought of demonstrating one such application i.e. using the app to store important information like pics of credit / debit card or some private pics. Using the app to store the important information not only adds security but also makes it less susceptible to attacks.

We have analyzed various security attacks in Android Devices. Some of them being:

- Email Spoofing Attacks: In this type of attack, the attacker sends a spoofed email just like an original email. The email is redirected to a phishing site or makes the victim download some spoofed apk file. By, using a simple shell script the attacker can then launch attack of autorun, this would run the app in background and it may attach itself to some system file. This would make it really difficult for the OS to detect and remove it. Alternately, It may disable Antivirus Software present in the Mobile Phone and hence the mobile is now susceptible to attack.

- Trojans: Now-a-days due to the presence of lot of custom Hacking software that are equipped with designing customized Trojans. The signature of the created trojan may not be present in the database of the Anti-Virus Software, hence these are not detected and they give complete control of victim's mobile phone to the attacker.
- Software like Metasploit have excellent Network Reconnaissance and Information Gathering tools like SET (Software Engineering Toolkit). Anyone with basic knowledge of networking can plan an attack and install some malicious code in the Mobile Phones which can later transfer important information over a simple FTP or HTTP Channel.

The point of the above discussion is, with the growth of technology advanced techniques exists which can be used to plan an attack on the victim. Even some harmless data sniffing software like Wire Shark may turn harmful if no proper security is used in Transmission of the Information.

To enhance the security various protocols are designed, yet it is more logical to perform encryption at the senders end than trusting the protocols. It adds additional layer of security to Data Transmission.

We have made some changes in the existing algorithm based on the above knowledge of Security loopholes and overcoming the flaws in random grid.

By making the changes we found that the image quality was improved considerably. Giving the same pixel expansion as Random Grid VCS. The image recovered was lighter in background and the contrast was significantly improved.

4.4 Screen Shots of Android Application

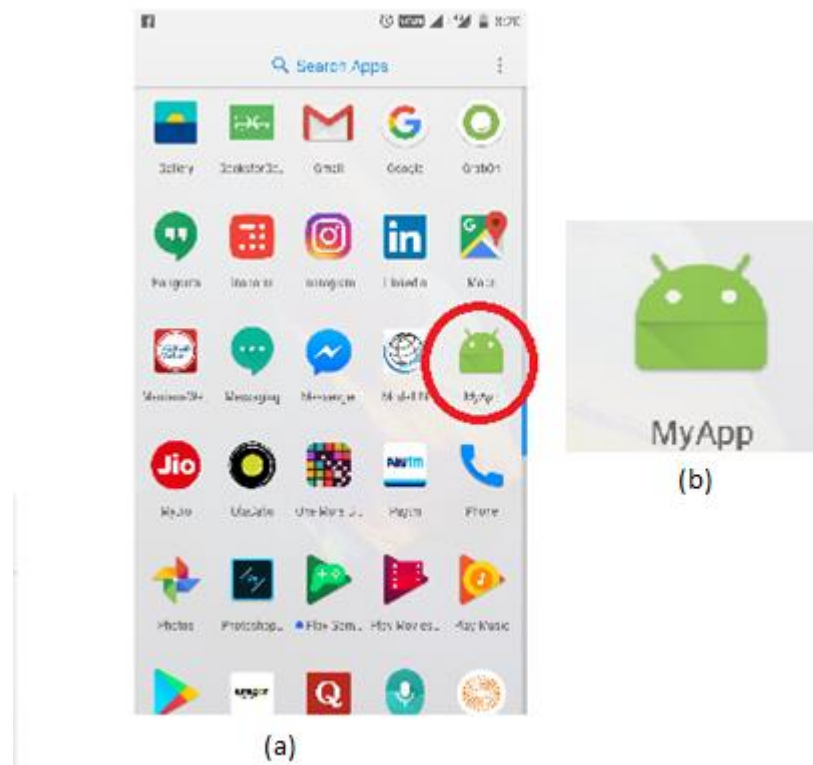


Fig 4.4.1 (a) Screen Shot of Application named “My App” (b) Zoomed Icon of Application

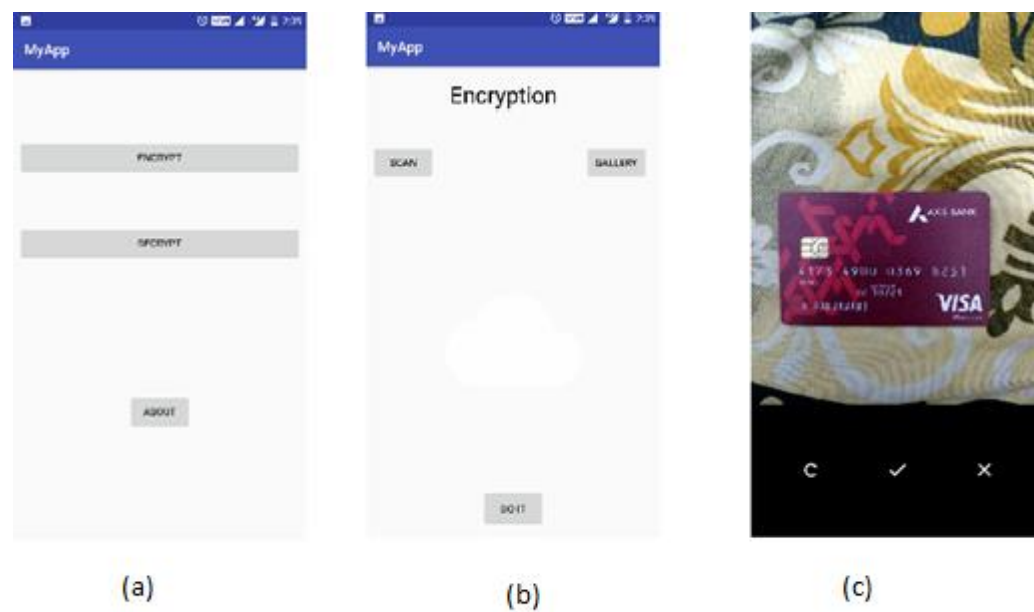


Fig 4.4.2 (a) Encryption / Decryption Screen (b) On-Click Encryption button (c) Scan picture if not available

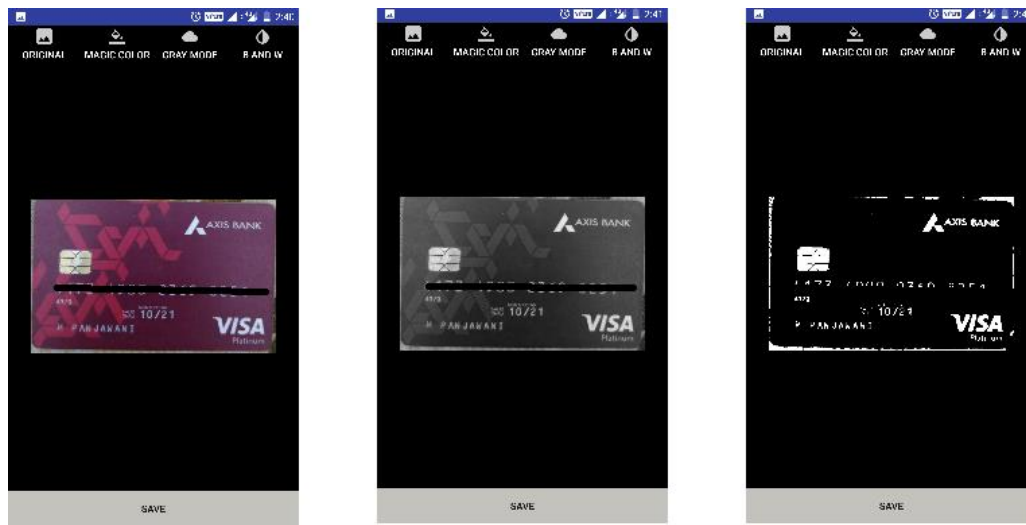


Fig 4.4.3 (a) Automatic Edge Detection (b) Grey Image filter (c) Black and White Image filter

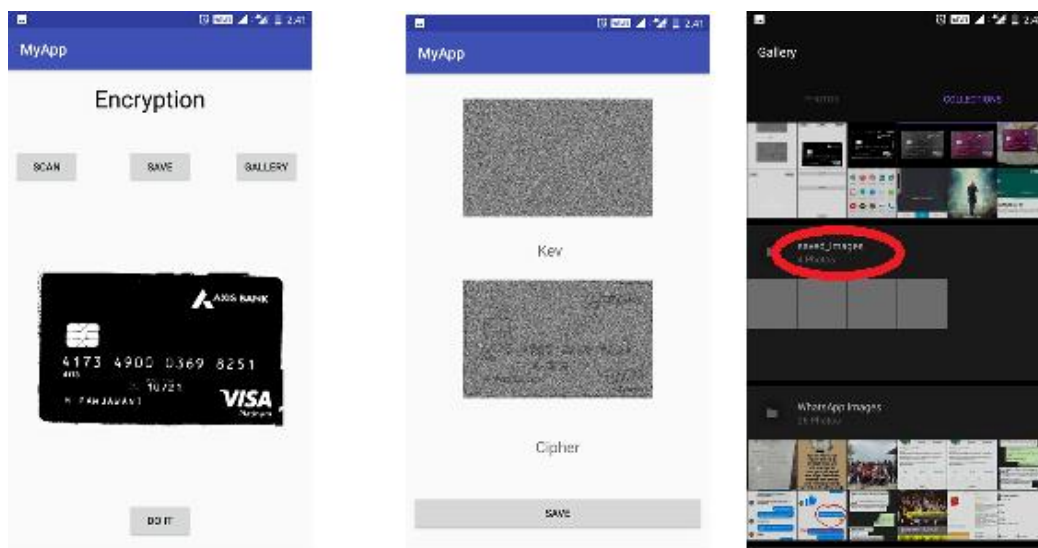


Fig 4.4.4 (a) Image after being scanned (b) Key and Cipher of Encrypted Image (c) Image Cipher Stored in scanned_images folder

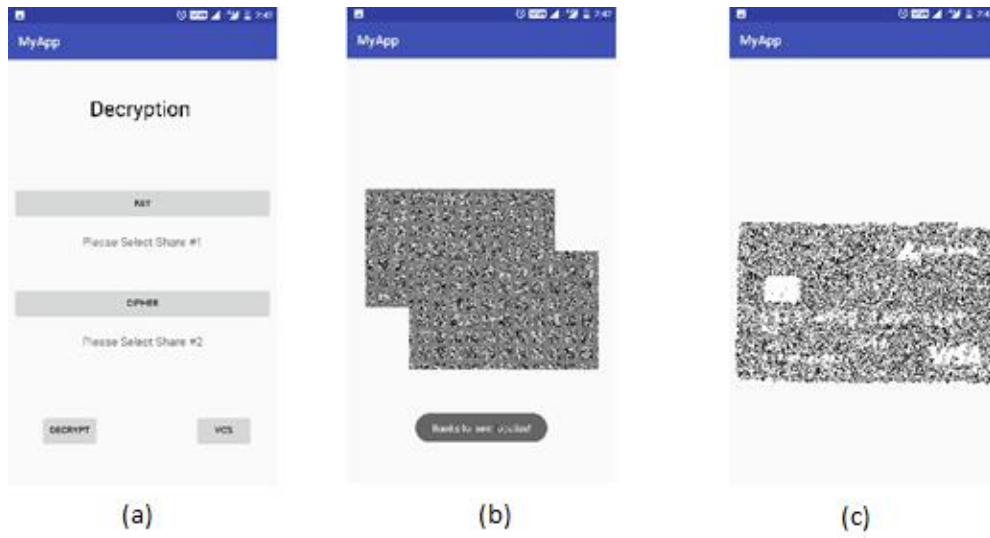


Fig 4.4.5 (a) Decryption Screen (b) VCS gesture movement (c) Decrypted image (The Quality has been reduced intentionally – For the sake of presentation)

Chapter 5

SCHEME TO SHARE MULTIPLE IMAGES IN VISUAL CRYPTOGRAPHY

5.1 Previous Works

Right from the basic model of visual cryptography, researchers have come up with many related studies. But most of these studies concentrated on sharing the single secret. Bin Yu, Xiaohui Xu, Liguang Fang solved this problem by introducing a multi secret scheme in which the combination of different shares results in different secret images. Lina Ge, Shaohua Tang gave the solution to share multi secrets based on circle properties. Later Weir, Wei Qi Yan introduced a new scheme to share multiple secrets with the help of generating master key. Zhengxin Fu, Bin Yu introduced a new concept of rotation to share multiple secrets with a method RVCS in which four secret images are encrypted into two shares and the decryption is done by combining two shares with different angles. We propose a new Visual Cryptography Scheme for multiple images using basic (2,2) scheme, which encrypts three secret images into three shares and each secret image is obtained by combining one share with the 180° anticlockwise rotation of another share. The scheme uses the basis matrices concept in basic (2, 2) scheme.

This would lead to saving spectral bandwidth as the same of Shares transmit more information. In this scheme we have n shares which reveal n secrets. For e.g. to obtain Secret1, Share1 and 180° rotation of Share2 is overlapped, similarly for Secret2, Share2 and 180° rotation of Share3 are overlapped and so on.

This is effective in a way, that it is more generalized than other Schemes meaning instead of using a fixed number of secrets any number of Secrets can be used.

5.2 Proposed Scheme

We have built a generalized Scheme which would take input as n secret and the output would be n shares. This scheme is a generalized scheme in a sense that, the value of n can be changed by the user.

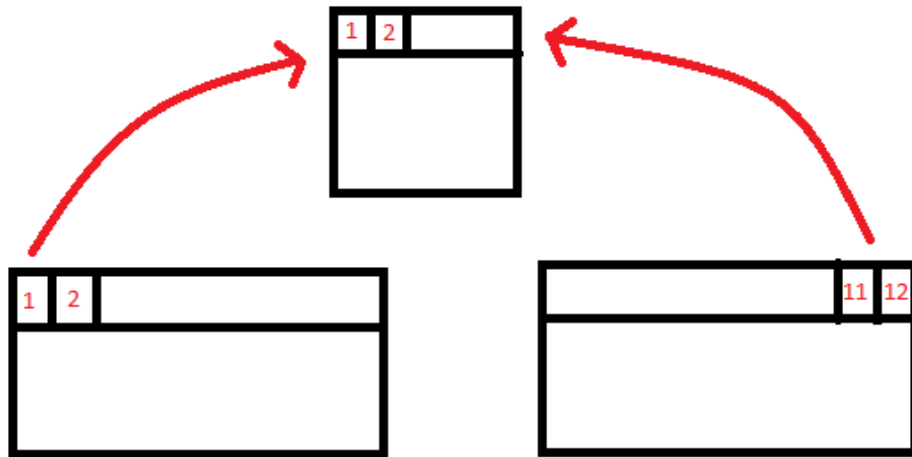


Fig 5.2.1 Illustration of proposed Algorithm

For the sake of illustration consider a Secret image with 6 pixels. The Shares have 12 pixels each. Now, in-order to decide the value of 1st and 2nd pixel of Share 1, a toss of coin is made and it is accordingly assigned a value $\{ (0,1) \text{ or } (1,0) \}$. Now, we can decide the value of last 2 pixels i.e. $2*m$ and $2*m-1$ pixel using following equation:

$$secret(i, j) = [shareA(i, 2 * j), shareA(i, 2 * j + 1)] \cup [shareB(i, 2 * m - 2 * j), shareB(i, 2 * m - 2 * j - 1)]$$

Where $i \rightarrow 0 \text{ to } n$ & $j \rightarrow 0 \text{ to } m/2$

-- Equation 5.1

Encryption:

Step 1: Iterate over each row by row all the share images.

Step 2: Fill the first 2 pixels of Share1 randomly

Step 3: Depending on the value of the first 2 pixels of Share1 decide the value of last pixels of Share2 since both have to overlap to give first 2 pixels of Secret1

Step 4: Repeat the above procedure for all other Shares and Secret images

Decryption:

Step 1: Print the images over transparency

Step 2: Overlap images (Share1 above 180⁰ rotated Share2 and so on..)

5.3 Simulation Results

First, we have to enter the number of Images, then select those images. By default, we select random images from the list of inbuilt images in MATLAB 2015 b (Grey or RGB). Then, we convert this image to Black and White format. Since we are using Random Grids. For color images we use halftoning methods like Jarvis halftoning.

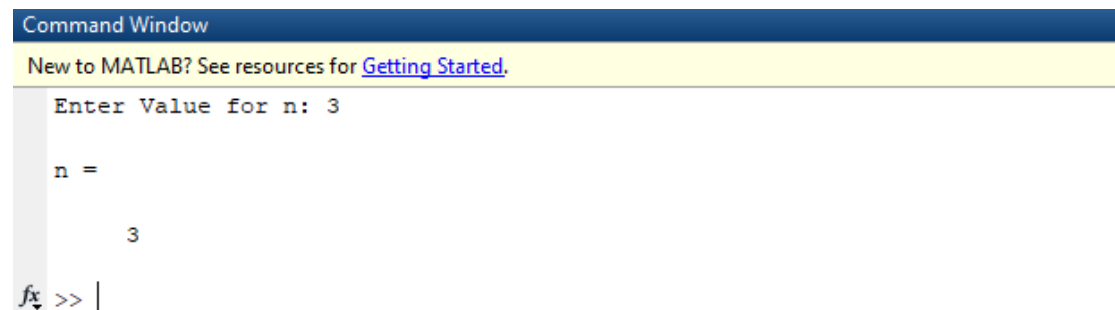
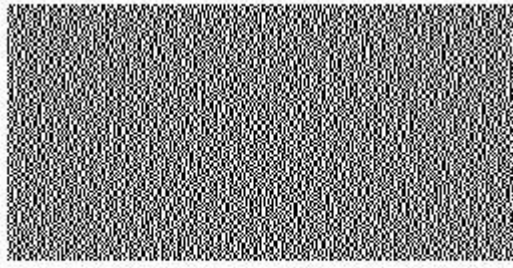


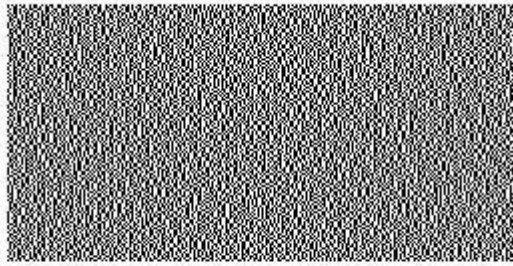
Fig 5.3.1 Simulation result (Selecting the number of images)



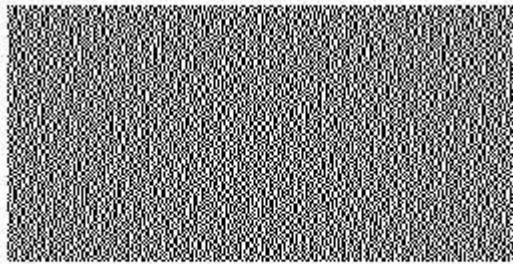
Fig 5.3.2 (a) Secret Image1 (circuit) (b) Secret Image2 (cameraman) (c) Secret3 (eight)



(a)



(b)



(c)

Fig 5.3.3 Simulation results (a) Share1 (b) Share2 (c) Share3



(a)



(b)

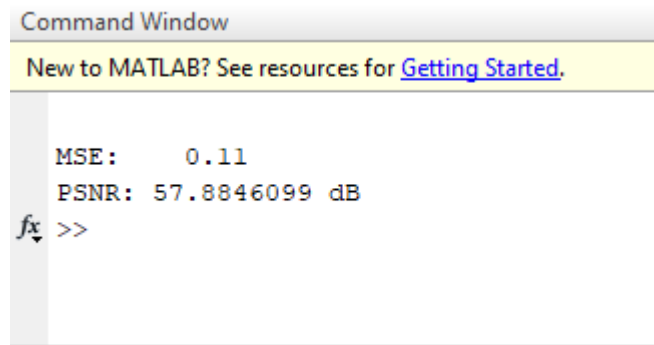


(c)

Fig 5.3.4 Simulation results (a) Recovered image1 (b) Recovered Image2 (c) Recovered Image3

5.4 Results and Discussion

This scheme works best while using even number images. This Scheme has a disadvantage that it undergoes pixel expansion.



```
Command Window
New to MATLAB? See resources for Getting Started.

MSE:    0.11
PSNR: 57.8846099 dB
fx >>
```

Fig 5.4.1 PSNR & MSE Values of Share3 image compared with original Secret Image

The McCabe complexity of the code is found to be 9. Which is significantly less than other schemes which uses more bandwidth to share multiple secret images. Our scheme is more generalized than other schemes. Our Schemes works well with even dimensional images. We have used MATLAB 2015 b for demonstrating our proof of concept. We have used JAVA 8.x for Android Development. Also, initially we used python's OpenCV libraries to understand about image processing and implemented basic schemes (as it is easy to get started).

5.5 Conclusion

We have initially invested huge amount of our time in understanding on how the existing schemes work. We implemented many research papers and analyzed the security of all the schemes. This made us appreciate the strength of Visual Cryptography and how easily we can integrate it with the modern technology. We then, changed our focus to Multiple Secret Sharing and Video Processing, we had to implement the mathematical proof of its validity and then we coded it using MATLAB. We also made an Android Application, which is easy to use, this helps the Research Scientists and Developers to bring the scheme to market directly as it is plugin based. We designed an efficient and genialized scheme to share multiple secret images. Although, we had faced a lot of difficulties, we were able to overcome by sheer determination and the interesting concepts we developed along the way.

References

- [1] N. Alon, J. Bruck, J. Naor, M. Naor and R. Roth, Construction of asymptotically good, low-rate error-correcting codes through pseudo-random graphs, *IEEE Transactions on Information Theory*, 38 (1992), 509-516.
- [2] J. Naor and M. Naor, Small bias probability spaces: efficient constructions and applications, *SIAM J. on Computing*, vol 22, 1993, pp. 838-856.
- [3] M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set equality, *Journal of Computer and System Sciences* 22, pp. 265-279 (1981).
- [4] Ren-Junn Hwang, "A digital image copyright protection scheme based on visual cryptography," *Tamkang Journal of Science and Engineering*, vol. 3, no. 2, pp. 97–106, 2000.
- [5] Akio Nagasaka and Yuzuru Tanaka, "Automatic video indexing and full-video search for object appearances," in *Proceedings of the IFIP TC2/WG 2.6 Second Working Conference on Visual Database Systems II*, Amsterdam, The Netherlands, The Netherlands, 1992, pp. 113–127, North-Holland Publishing Co.
- [6] Boon-Luck Yeo and Bede Liu, "Rapid scene analysis on compressed video," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 5, no. 6, pp. 533–544, Dec. 1995.
- [7] Moni Naor and Adi Shamir, "Visual cryptography," in *EUROCRYPT*, 1994, pp. 1–12.
- [8] C. F. Lam and Moon-Chuen Lee, "Video segmentation using color difference histogram," in *MINAR '98: Proceedings of the IAPR International Workshop on Multimedia Information Analysis and Retrieval*, London, UK, 1998, pp. 159–174, Springer-Verlag.
- [9] Robby S. Fussell, "Piracy prevention for multimedia data through digital watermarking," *The ISSA Journal*, pp. 24– 27, Dec. 2004.

- [10] Gordon W. Braudaway, Karen A. Magerlein, and Frederick C. Mintzer, "Protecting publicly available images with a visible image watermark," in Proceedings of SPIE, 1996, vol. 2659, pp. 126–133.
- [11] Amir Houmansadr and Shahrokh Ghaemmaghami, "A novel video watermarking method using visual cryptography," IEEE International Conference on Engineering of Intelligent Systems, Islamabad, Pakistan, 2006.
- [12] Min Wu and Bede Liu, "Watermarking for image authentication," in ICIP (2), 1998, pp. 437–441.
- [13] G.R. Blakley, Safeguarding cryptographic keys, in: Proceedings of the National Computer Conference, vol. 48, NJ, USA, 1979, pp. 313–317.
- [14] A. Shamir, How to share a secret, Commun. ACM 22 (1) (1979) 612–613.
- [15] C. Blundo, A. De Santis, M. Naor, Visual cryptography for gray-level image, Info. Process. Lett. 75 (2001) 255–259.
- [16] C.-C. Chang, H.-C. Wu, A copyright protection scheme of images based on visual cryptography, Imaging Sci. J. 49 (2001) 141–150.
- [17] J.-B. Feng, H.-C. Wu, C.-S. Tsai, Y.-P. Chu, A new multi-secret images sharing scheme using largrange's interpolation, J. Syst. Software 76 (2005) 327–339.
- [18] C.-S. Tsai, C.-C. Chang, A generalized secret image sharing and recovery scheme, in: Advanced in Multimedia Information Processing-PCM2001, Lecture Notes in Computer Science, Springer, Germany, vol. 2195, 2001, pp. 963–968.