Tribhuvan University

Institute of Science and Technology

"Comparative Analysis of Visual Secret Sharing Cryptography Scheme: Shamir's Secret Sharing and Proactive Secret Sharing "

Dissertation

Submitted To

Central Department of Computer Science & Information Technology

Institute of Science and Technology

Tribhuvan University, Kathmandu, Nepal

In partial Fulfillment of the Requirements

For the degree of Master of Science in Computer Science & Information Technology

By

Bikash Regmi

T.U Registration No.: 5-2-33-19-2010

T.U Examination Roll No.: 307/073

Date (November, 2019)

Supervisor

Mr. Bikash Balami

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Student's Declaration

I hereby declare that I am the only author of this thesis work and that no sources other than the mentioned here have been used.

…….

Bikash Regmi

Date: November, 2019

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Date.…….

Supervisor's Recommendation

I hereby recommend that this dissertation prepared under my supervision by **Mr. Bikash Regmi** entitled "**Comparative Analysis of Visual Secret Sharing Cryptography Scheme: Shamir's Secret Sharing and Proactive Secret Sharing"** be accepted as in fulfilling partial requirement for the completion of Master's Degree of Science in Computer Science & Information Technology.

……

Asst. Prof. Bikash Balami

Central Department of Computer Science and Information Technology

Tribhuvan University, Kirtipur, Kathmandu, Nepal

Date: November, 2019

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Date:……

LETTER OF APPROVAL

We certify that we have read this dissertation work and in our opinion it is sufficient for the scope and quality as a dissertation in the partial fulfillment of the requirements of Master's Degree in Computer Science & Information Technology.

Evaluation Committee

Asst. Prof. Nawaraj Paudel **Head of Department** Central Department of Computer Science & Information Technology Tribhuvan University	**Asst. Prof. Bikash Balami** Central Department of Computer Science & Information Technology (TU) (Supervisior)
(External Examiner)	**(Internal Examiner)**

ACKNOWLEDGEMENT

First of all, I would like to express my sincere gratitude to my respected teacher as well as my dissertation supervisor, Mr. Bikash Balami, Assistant Professor, Central Department of Computer Science & Information Technology (CDCSIT), Tribhuvan University for his cooperation, encouragement and strong guidelines throughout this thesis work. With his expertise knowledge and ideas, he always provides me necessary guidelines and motivations to tackle the problem raised during preparation of this work.

I am also indebted to the Head of Central Department of Computer Science & Information Technology, Asst. Prof. Nawaraj Paudel for his suggestions encouragement, valuable directions and for providing me favorable environment in conducting the research.

I would like to extend sincere acknowledgement to the entire group of Professors, Lecturers of the Department for their valued inspiration. I would like to express my sincere thanks to my colleagues Mr. Bhoj Raj Adhikari, Kshitiz Bhatt, Sushil Banstola and all my well-wishers who directly and indirectly helped me to complete this work.

Last but not least i must express my very profound gratitude to my parents and to my Brother Bishwas Regmi for providing me with unfailing support and continuous encouragement through the process of writing this thesis. This would not have been possible without them. Thank you.

Bikash Regmi

CDCSIT, TU

Abstract

Visual secret share scheme plays an important role in area of information security. Different from conventional cryptography, visual cryptography is an image cryptographic technique proposed by Naor and Shamir which encodes a secret image into multiple shares. When defined minimum threshold number of shares are gathered from shared participant's share can reveal the secret image. This phenomenon is also known as (k, n) threshold secret share scheme. Visual cryptography schemes allow the encoding of a secret image into shares, which are distributed to the participants. The requirement for minimum threshold share ultimately leads to the confidentiality of secret. (k, n) visual secret sharing uses threshold scheme by using the concept of Lagrange's polynomial interpolation. Applying XOR operation with cover image leads to authentication of secret. The reconstruction of the original image without loss of information can be generated from shared shares using the concept of Lagrange's polynomial interpolation. In this study visual secret share scheme by using Shamir's Secret Share Scheme and Proactive Secret Share Scheme are implemented and analyzed with different parameter like NPCR, UACI, correlation-coefficient, performance speed measures. The average value of NPCR for Shamir's Secret Share and Proactive Secret Share are 99.99990463 and 99.99985165 respectively. The average value of UACI for Shamir's Secret Share and Proactive Secret Share are 30.60813355 and 32.15971784 respectively. The average correlation-coefficient value of Shamir's and Proactive scheme are -0.018559263 and -0.123933789 respectively. The average share generation time of Shamir's Secret Share and Proactive Secret Share are 30400.3 and 32392.9 Millisecond respectively. Similarly, average share reconstruction time for Shamir's and Proactive scheme are 2150.3 and 2097.9 millisecond respectively. Hence based on UACI and correlation-coefficient Proactive Secret Share scheme has better performance whereas based on the NPCR and Computational time Shamir's Secret Share scheme showed better performance.

Keywords: Share Generation, Share Reconstruction, Shamir's Secret Share / (k, n) Threshold Scheme, Proactive Secret Share Scheme.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ARGB	Alpha, Red, Green, Blue
CC	Correlation–Coefficient
GB	Giga Bytes
IDE	Integrated Development Environment
NPCR	Number of Pixel Change Rate
RAM	Random Access Memory
UACI	Unified Average Change Intensity
VC	Visual Cryptography
VSSS	Visual Secret Sharing Scheme
SSSS	Shamir's Secret Sharing Scheme

Chapter 1

Introduction

1. 1 Introduction

Imagine you encrypt your important files with one secret key and if such a key is lost then all the important files will be inaccessible. Thus, secure and efficient key management mechanisms are required. Instead of providing secret key for one individual it is better idea to distribute secret key among multiple person so we can prevent damage that can happen if the key is lost or prevent any misuses. Secret sharing scheme is one of them that split the secret into several parts and distribute them among selected parties. The secret can be recovered once these parties collaborate in some way [24].

Visual secret sharing schemes are used to manage image data protection as well as image based authentication techniques that contain sensitive data such as military surveillance, satellite images, medical records, financial transactions, electronic voting systems, maps, encrypted data etc. Visual secret shares scheme (VSSS) provides one of the secure ways to transfer images on the Internet. It offers efficient solutions for controlling private data and images that are made available only to selected people. The advantage of traditional visual cryptography is that it exploits human eyes to decrypt secret images. To ensure the authenticity, integrity and availability of data transmission over the internet, VSSS uses the threshold schemes so that the original massages will discovered only when intended number of shares are available.

Secret Sharing Schemes (SSS) is one of the key management or establishment schemes invented separately in 1979 by both Shamir and Blakley as a solution to safeguard cryptographic keys. Since its invention many different secret share schemes have emerged, such as Verifiable Schemes, Proactive Schemes, Multiple Schemes, Visual Schemes, Chinese Remainder Schemes, Quantum Schemes, Rational Schemes, Online Schemes, and etc. In 1995 Naor and Shamir proposed the process of visual secret sharing scheme namely visual cryptography as (k, n) thresholds share, which can encode a secret image into n transparencies, where each pixel is expanded m times. One transparency is distributed to each participant. When any k or more shares are stacked together the

image will begin to emerge as the contrast between the black and white pixels becomes sufficient for human eye to recognize the secret image without computational devices. Naor and Shamir's presents VSSS with (2,2) scheme for black and white pixels' image in their paper [8, 24].

Traditional techniques of cryptography provide numerous means of protecting secret information, but most of these techniques requires complex computation for encryption as well as decryption. To avoid the complexity of traditional cryptographic schemes, a human vision system visual cryptography (VC) is possibly best alternative solution for cryptographic scheme [4]. The Security of the digital media has become an important field. The media used for visual Data exchanged over the Internet is unreliable and insecure. Because it can be copied and modified easily. To exchange images through any unsecured medium Naor and Shamir proposed Visual Cryptography (VC) so that a user can identify confidential data with required threshold shares without any complex computation [5].

1.2 Problem Definition

Visual secret shares scheme (VSSS) provides one of the secure ways to transfer secret data on the Internet. To manage the security issues of secret data, encrypted data etc. it offers efficient solutions for controlling private data and images that are made available only to selected people.

Traditional visual secret share scheme is a kind of secret sharing scheme which allows the encoding of a secret image into transparencies shares distributed to participants, such that human eye can recover the secret/original image by overlapping the minimum required transparencies shares without any computation. Through encryption one can prevent a third party from understanding raw data during signal transmission. Visual cryptography schemes allow the encoding of a secret image into shares, which are distributed to the participants. The condition for minimum threshold share requirement ultimately leads to the Confidentiality of secret. Shamir's (k, n) visual secret sharing uses threshold scheme by using the concept of Lagrange's polynomial interpolation. The reconstruction of the original image without loss of information can be generated from shared shares without complex mathematical calculation.

1.3 Objective:

The main objective of thesis is:

- To know the function of secret sharing scheme to distribute the shares among multiple parties and reconstruct the secret that has been shared as shares among parties with at least minimum required threshold shares/parties bring together.
- To implement the visual secret sharing scheme by using Shamir's and Proactive secret sharing scheme performance of both scheme on visual secret.
- To analyze the performance, pixels change rate, unified average change Intensity and correlation coefficient of the generated shares with the secret variation of shares threshold number.

1.4 Thesis organization

The organization of thesis is as follows:

Chapter 1 describes the introduction, problem statement and objectives.

Chapter 2 describes about the background study for the research and literature review of the related work by different authors.

Chapter 3 describes the overview of the algorithms and methodology of Visual Secret sharing Cryptography Scheme: Shamir's secret Sharing and Proactive Secret Sharing.

Chapter 4 contains the implementation overview of Visual Secret sharing Cryptography Scheme: Shamir's secret Sharing and Proactive Secret Sharing in Java platform along with analysis of different performance parameter of methodology.

Chapter 5 concludes the main theme of thesis work.

Chapter 2

Background Study and Literature Review

2. 1 Background Study

2.1.1 Shamir's Secret Sharing Scheme

In 1979, Shamir Adi [16] published an article titled *"How to share a secret"*. In this article, the following example was used to describe a typical secret sharing problem:

"Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry? The minimal solution uses combination of 462 locks (6 from 11) and 252 keys (5 from 10) per scientist.

***Theorem**: Let D be the secret to be shared among n parties. A (k, n)-threshold scheme is a way to divide D into n pieces $D_1, \cdots, D_n$ that satisfies the conditions:*

1. Knowledge of any k or more D_i pieces makes D easily computable;

2. Knowledge of any $(k-1)$ or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely)

i.e when defined minimum threshold number of shares are gathered from shared participant's share can reveal the secret image. This phenomenon is also known as Shamir (k, n) secret share scheme, which aim to distribute a secret to a group of participants such that certain conditions must be met for them to be able to solve for the secret without complex computation.

2.1.2 Proactive Secret Sharing Scheme

In 1995, Herzberg et. al. proposed a proactive secret sharing scheme which renews the shares of all users forming a group periodically, so that, any share compromised by an adversary during onetime period, becomes useless from the next. Proactive secret sharing schemes first share a

secret among the users, using a traditional secret sharing scheme, and then divide the entire lifetime of the scheme into a number of time periods. During each period, the shares of the users are renewed, so that the shares obtained by an adversary during onetime period are rendered useless from the next time period [14].

The need to maintain the confidentiality of any data within an organization as well as to prevent it from becoming corrupted or inaccessible due to single point failure, has grown considerably, with rapid increase in computer crime. *Proactive* secret sharing (PSS) schemes are designed for settings where long-term confidentiality of secrets has to be guaranteed. Secret sharing is a foundational primitive in cryptography, especially in secure computation. A secret sharing scheme typically consists of a protocol for sharing a secret (or multiple secrets) and a protocol for reconstructing the shared secret(s).

2.2 Literature Review

In [13], a technique for encryption of visual data by generating the share from a binary image into two shares Share1 and Share2 in a perfectly secure way which can be decoded directly by the human visual system. The black and white pixel are expanded with different possibilities of transparency. The original encryption problem can be considered as a 2 out of 2 secret sharing problem. The shares(secret) are printed transparency. The original image is revealed by placing the 2 shares transparency by stacking with each other. The generated shares are random noise transparency i.e. obtained by pixel expansion of white '1' and black '0' each having 2 possibilities for individual shares.

Proactive secret sharing scheme which renews the shares of all users forming a group periodically, so that, any share compromised by an adversary during onetime period, becomes useless from the next. In [14], initially all the users obtain their secret shares by any traditional threshold secret sharing. To renew a secret share a set of polynomials, having their free coefficients equal to 0 (i.e. $\delta(0) = 0$ where q is the polynomial) is used. Each such polynomial is sent to any user, by one of the other users. This scheme depends on all users in a group to renew the share of any one user.

In [7], a visual cryptography approach for color images has been proposed. In their approach, each pixel of the color secret image is expanded into a 2×2 block to form two sharing images. Each 2×2

block on the sharing image consists of red, green, blue and alpha, respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. There would be 4! possible combinations according to the permutation of the 4 colors. Because human eyes cannot detect the color of a very tiny subpixel, the four-pixel colors will be treated as an average color. When stacking the corresponding blocks of the two shares, there would be 242 variations of the resultant color for forming a color image.

In [20], introduced the first color visual cryptography which produce the meaningless shares. The idea behind this scheme is using a concept of arcs that can be shared with colored secret images to construct a colored visual cryptography scheme. One pixel is process into m sub pixels, and each sub pixel is divided into c color regions. In each sub pixel contains exactly one colored region, and all remaining color regions are black. The pixel's color depends on the interrelations between the stacked sub pixels. The pixel expansion m is c x 3 for a colored visual cryptography scheme with c colors.

The visual cryptography schemes to share two secret images in two shares presented in 1998 [17]. Two binary secret images hidden into two random Shares, namely s1 and s2, such that by stacking the two shares the first secret can be visible, denoted by s1$\otimes$ s2 and by first rotating s1 by some angle (Θ°) anti-clock wise the second secret can be obtained. They designed the rotation angle Θ to be 90°.

In 1999 for generating a meaningful secretes of color image and sharing a secret color image, anticipated color visual cryptography scheme was developed [17]. Two significant color images are selected as cover images for a secret color image, size are the same as the secret color image. On the basis of predefined Color Index Table, the secret color image will be hidden into two camouflage images. However, this scheme has disadvantage that it required extra space to accumulate the Color Index Table, because of more colors in the secret image requires larger size of shares.

In [2], the strategy of steganography introduced to generate meaningful share images in visual cryptography by adding the secrets bits of pixel or text message on the cover image's LSB bit to generate shares in 2001. Which means combine one image's MSB with other image's LSB. Extracting the covers LSB bit will reproduced the original message.

In 2005 [17], spatial-domain image hiding schemes has been proposed. Hidden a binary image into two meaning full shares by embedded these two secret shares into two gray level cover images. Embedding images can be superimposed to decrypt the hidden information. The secret images pixels are embedded with the i^{th} LSB of the cover images. i.e the original massage is hiding inside the cover images [3]. The disadvantage is only that one set of confidential messages can be embedded, so several shares have to be generated to share large amounts of confidential messages.

In [21], a visual cryptographic technique to secure image shares has proposed. Working basically into 3 phases. First, each pixel in the secret image is broken into four sub pixels. A white pixel is shared into two identical blocks of four sub-pixels. A black pixel is shared into two complementary blocks of four sub-pixels. These shares can be either Vertical or Horizontal or Diagonal Share. The visual secret sharing scheme assumes that the message consists of a collection of black and white pixels and each pixel is handled separately. Secondly, shares images are embedded into some cover images using digital watermarking. Result of this phase will be different meaningful shares consist some cover image. Discrete cosine transformation (DCT) is used to divides the image into distinct frequency bands which makes it easy to embed the watermark in the desired area of the image. At last the binary watermarked shares extracted from the host images.

Visual cryptography for color images in 2012 proposed [1]. The idea is that binarized secret images and apply XOR operation with the R, G, B shares from host images so that (2,2) shares will generate. The secret will recover after mixing 2 shares and applying XOR with host images.

In [11], a cryptographic Image Encryption technique based on the RGB Pixels shuffling has been proposed in 2013. No pixel's bit has been changed during encryption and decryption because of no pixel expansion. Instead the numerical values are transposed, reshaped and concatenated with the RGB values shifted away from its respective positions and the RGB values interchanged in order to obtain the cipher image. The RGB values are shifted out of its native pixel and interchanged within the image boundaries by the algorithmic process. The shuffling of the image will be done by displacing the RGB pixels and also interchanging the RGB pixel values.

In [8], a new scheme is proposed which can encrypt a secret image into two meaningful share-images. Participants can recognize the contents of the cover-image on each share image, but nobody can uncover any clue about the secret image on them. If superimposing these two share-images, the contents of the cover-image will be disappeared and, on the contrary, the contents of

the secret image will be revealed on the stacked image. The main concept is to take some pixels from the secret image and some pixels from the cover image to generate the needed share images. i.e embed the information of the secret image into odd locations on the cover share images.

In [9], binary image visual cryptography is proposed. The shares are obtained by dividing the original image and thus obtaining small shares in the total number of shares that the combination of them equals the size of the original image. The recovered image is similar to the original image without any data loss. The generated shares are random and the intruder cannot retrieve the original image or predict its content. The major drawback of this approach is that it requires a large storage space and increasing the time it takes to send shares to the receiver.

In [5], proposed an extended visual cryptography technique (EVCT) for true color images in 2017 as (3, 3) and (2, 3) -EVCT techniques to share the color images. First either generate three RGB shares as R, G, B shares for (3, 3)-EVCT or RG, GB, RB shares for (2,3) EVCT and embedded cover images into these shares to make them meaningful. Shares are now ready to send over any insecure communication medium. As decryption procedure the effect of cover images is nullified from three RGB shares. The shares are overlapped to get a matrix. This matrix is used to get the original secret image back.

Chapter 3

Methodology

3. 1 Methodology

Visual cryptography is a new type of cryptographic scheme that focuses on solving the problem of secret sharing. Visual cryptography is a desirable scheme as it embodies both the idea of perfect secrecy and a very simple mechanism for decrypting/ decoding the secret without complex computation.

The methodology includes implementing the Shamir's and Proactive Secret Sharing scheme algorithms applied in pixel value of secret image after embedding(XORed) with cover images. The secret and cover images are standard images. The details of data collection are discussed in section 4.3. The reason for using Shamir secret share scheme is to generate shares from the secret so that when applied minimum threshold shares reveal the secret. Proactive secret shares will generate updates shares periodically to prevent from intruder's access to the secret. Each pixel from original image works as secret. To share this secret among n participants first extract A, R, G and B component of image pixels. Then apply Shamir (k, n) visual secret sharing where each individual components becomes secret to share.

Table 1: Table representation of pixel structure

ALPHA								RED								GREEN								BLUE							
31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0

3.2 Algorithms:

The Shamir's secret sharing and Proactive Secret sharing are used to share secrets among parties. Both the Shamir's and Proactive secret sharing scheme uses threshold scheme. These scheme deals with the confidentiality of the secret but not the authentication of secret that has been shared. To

make the shared secret confidential as well as authentic, Secret image's pixel is embedding (XOR) with Cover image's pixels bitwise and apply Shamir and Proactive scheme on generated result of XORed operation to share this secret information as shares. The visual secret will be reveal only when minimum number of shares are available defined while constructing the shares for the reconstruction and apply bitwise XOR operation with cover image's pixels to reveal the secret/key image. The only condition is that both the sender and receiver should have same cover image.

3.2.1 Shamir (k, n) Threshold Scheme Share Generation and Reconstruction

Secret sharing using allows each party to keep a portion of the secret and provides a way to know at least part of the secret. Encryption using multiple keys is a possible solution for secret sharing. However, this solution requires a large number of keys, therefore the management of such a scheme becomes troublesome, as demonstrated by Shamir.

A secret sharing scheme enables distribution of a secret amongst n parties, such that only predefined authorized sets will be able to reconstruct the secret. Threshold schemes are ideally suited to applications in which a group of mutually suspicious individuals with conflicting interests must cooperate. By properly choosing the k and n parameters we can give any sufficiently large majority the authority to take some action while giving any sufficiently large minority the power to block it [16].

Lagrange interpolation is used to reveal the secret from generated shares with minimum number of required shares. It is the problem of constructing function which goes through a given set of data points [22]. Lagrange gave the following interpolation polynomial q(x) of degree n given at (n+1) points (x_i, y_i) i=0,1,…,n. such that :

$y = q(x) = \sum_{i=0}^{n} y_i \, l_i(x)$ ……..Eq(1).

where, y_i is shared value same as D_i defined by Adi shamir [12,16].

Where $l_i(x)$ is Lagrange basic polynomial defined by

$l_i(x) = \prod_{\substack{j=0 \\ i \neq j}}^{n} \frac{(x - x_i)}{(x_i - x_j)}$ ……..Eq(2).

Share Generation:

Step 1: Take inputs n as total shares and k as minimum number of require threshold to recover secret.

Step 2: Generate polynomial equation of degree (k-1) as $q(x)=a_o+a_lx+ \ldots +a_{k-1}x^{k-1}$ mod p, where a_o=pixel value and $a_o, a_1, \ldots, a_{k-1}<p$, p is large prime.

Secret Reconstruction:

Step 1: apply Lagrange interpolation with minimum required threshold shares as:

$y = q(x) = \sum_{i=0}^{n} y_i \, l_i \, (x) \mod p$ ……..Eq(3).

Process Flow chart:

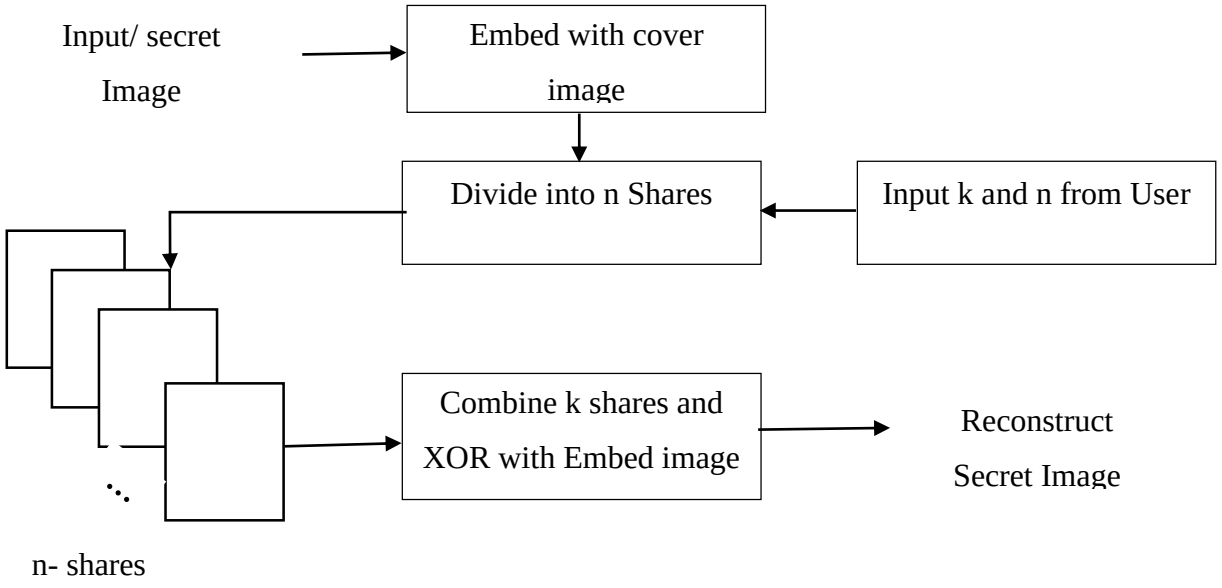


Figure 1: Shamir's Visual Secret Sharing Scheme

3.2.2 Proactive (k, n) secret sharing scheme Share Generation and Reconstruction

In [6], Herzberg et al introduced Proactive secret shares scheme using simplified version of the update protocol presented by Ostrovsky and Yung. The original secret's shares are generated as Shamir's secrets shares. When x is (distributively) stored as a value $f^{(t-1)}(0)=x$ of a k degree

polynomial $f^{(t-1)}(.)$ in Z_q, this polynomial can be update by adding it to a k degree random polynomial $\delta(.)$, where $\delta(0) = 0$, so that $f^{(t)}(0)=f^{(t-1)}(0)+\delta(0)=x+0=x$. by the linearity of the polynomial evaluation operation we get the renewal of the shares $x_i^{(t)}=f^{(t)}(i)$ according to :

$f^{(t)}(.) \leftarrow f^{(t-1)}(.)+\delta(.) \pmod p \Leftrightarrow f^{(t)}(i)=f^{(t-1)}(i)+\delta(i) \pmod p$ ……Eq(4).

for this system $\delta(.)=(\delta_1(.)+\delta_2(.)+\ldots+\delta_n(.)) \pmod p$, where each polynomial $\delta_i(.)$, $i \in \{1,\ldots n\}$ is of degree k and is picked independently and at random by the i^{th} server subject to the condition $\delta_i(0)=0$. The share renewal protocol for each server δ_i, $i \in \{1,\ldots n\}$, at time period t is as follows:

Shares Generation:

$Step$ 1: δ_i picks k random number $\{\delta_{im}\}_{m \in \{1,\ldots k\}}$ from Z_q. these number define a polynomial $\delta_i(z)= \delta_{i1}z^1+ \delta_{i2}z^2+\ldots+ \delta_{ik}z^k$ in Z_q, whose free coefficient is zero and hence $\delta_i(0)=0$.

Step 2: For all other servers/Shares δ_j , δ_i secretly sends $u_{ij}= \delta_i(j) \pmod p$ to δ_j.

Step 3: After updating u_{ji}, $\forall\ j \in \{1,\ldots n\}$, δ_i computes its new share $x_i^{(t)} \leftarrow x_i^{(t-1)} +(u_{1i}+ u_{2i}+\ldots+u_{ni}) \pmod p$ and erases all the variables it used except of its current secret key $x_i^{(t)}$.

Share Reconstruction:

Step 1: apply Lagrange interpolation with minimum required threshold shares as:

$y = q(x) = \sum_{i=0}^{n} \delta_i\ l_i\ (x) \pmod p$

Where $l_i(x)$ are Lagrange basic polynomials defined by

$l_i(x) = \prod_{\substack{j=0 \\ i \neq j}}^{n} \frac{(x-x_i)}{(x_i-x_j)}$

Process Flowchart

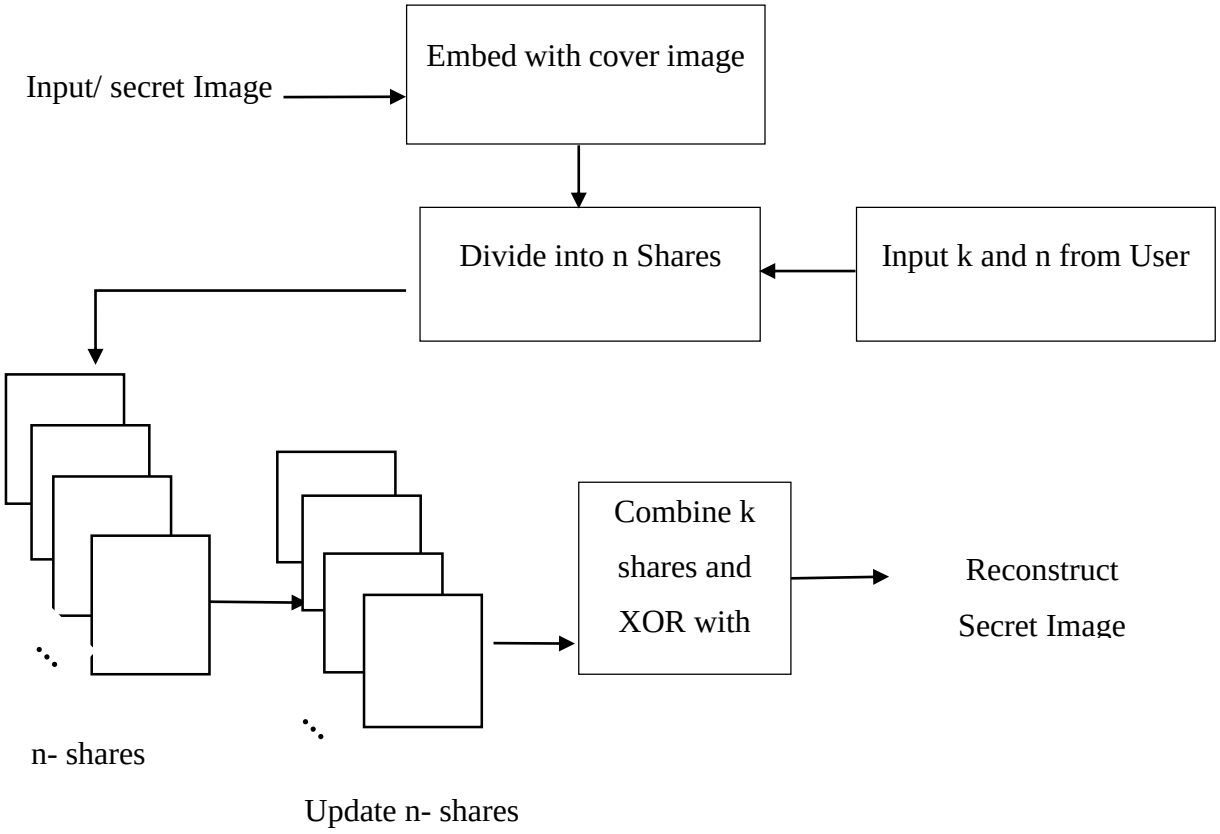


Figure 2: Proactive Visual Secret Sharing Scheme

To Generate Shamir's Visual Secret Shares:

Step 1: Take Secret Image.

Step 2: Embed (XOR- bitwise) Secret image's pixels with another Cover image's pixel.

Step 3: Define big prime (p) number.

Step 4: Take inputs n as total shares and k as minimum number of require threshold to recover secret.

Step 5: Generate polynomial equation of degree (k-1) as $q(x)=a_o+a_1x+ \ldots +a_{k-1}x^{k-1} \bmod p$, where a_o=image's pixels which shares has to be generated taken as A, R, G, B component of pixel and $a_o<p$, p is large prime.

Step 6: Take random number value of a_1, $a_{2,\ldots},a_{k-1}<p$ as co-efficient of polynomial equation.

Step 7: Generate shares q(x). where x=1,2…n.

To Generate Proactive Visual Secret Shares:

Step 1: Repeat step 1-7 of Shamir Visual Secret Share generation.

Step 2: To update shares all parties (total number of shares/parties) need to construct random polynomial of degree k-1 with free coefficient 0 as $\delta_i(z)= \delta_{i1}z^1{}_+ \delta_{i2}z^2{}_{+\ldots+} \delta_{ik}z^k \pmod p$.where $\delta_{i1}, \delta_{i2},.. \delta_{ik}<p$. and share some information with other parties as $u_{i,j}= \delta i(j)$.

Step 3: Each player update their shares as $x_i^{t+1}=x_i^t+u_{1,i}^t+u_{2,i}^t+\ldots.u_{n,i}^t$. where x_i =q(x) shares value.

To Reconstruct Secret from Shamir's and Proactive Secret Shares:

Step 1: Enter minimum number of shares to be combined and there shares id to reconstruct.

Step 2: Apply Lagrange Interpolation.

Step 3: Embed(XOR-bitwise) with cover image.

Chapter 4

Implementation and Analysis

4. 1 Implementation Tools

All the implementation is done in Java programming language using Eclipse ide 2018-09. For reconstruction of Shamir's and Proactive share secret BigInteger modInverse library is used.

4.1.1 Eclipse IDE 2018-09

Eclipse is an integrated development environment (IDE) used in computer programming originally created by IBM in November 2001. In 2004, the Eclipse Foundation was founded to lead and develop the Eclipse community. Eclipse is written mostly in Java and C. Its primary use is for developing Java applications. The Eclipse platform can be used to develop rich client applications, integrated development environments, websites and web services. It includes code editor and has integrated debugger.

Eclipse provide built-in languages such as Ada, ABAP, C, C++, C#, JavaScript, Perl, PHP, Prolog, Python, R, Ruby, Rust, XML, HTML, CSS etc. Users can extend its abilities by installing plugins written for the Eclipse Platform, such as development toolkits for other programming languages, and can write and contribute their own plug-in modules.

4.1.2 Java programming Language

Java was originally developed by James Gosling at Sun Microsystems and has been acquired by Oracle Corporation and released in 1995 as a core component of Sun Microsystems' Java platform. The language derives much of its syntax from C and C++, but it has fewer low-level facilities than either of them.

Java is a popular general-purpose programming language and computing platform. It is fast, reliable, and secure. Java is one of the most popular and widely used programming language in use particularly for client-server web applications. It is also a platform that helps to develop

run programs written in any programming language. The Java™ Programming Language is a general-purpose, concurrent, strongly typed, class-based object-oriented language.

4.2 Testing Environment

Hardware Specification:

- Device : Laptop
- System : intel(R) Core(TM) i5-3210M @2.50GHz
- Hard Disk : 500 GB.
- RAM : 4 GB.

Software Specification:

- Operating system : Windows 8.1 Enterprise N
- Coding Language : Java
- Tools : Eclipse ide 2018-09

4.3 Data Collection

The inputs data are standard image being used for image processing are taken from Kodak image database as mountain chalet ref# SK0090[1] as secret image to share and two macaws ref# JN1033[2] as cover image both having 768*512 resolution in PNG format. Applying Shamir's and Proactive Scheme intended only for confidentiality propose of visual secret works for all type of images. Although to achieve authentication on secret being send by applying embedding technique for both Shamir's and Proactive Scheme; the image format should be lossless like PNG, TIF, GIF.

[1] http://r0k.us/graphics/kodak/kodim24.html[online].[Accessed:1st April 2019].
[2] http://r0k.us/graphics/kodak/kodim23.html[online].[Accessed:1st April 2019].

4.4 Analysis

In this part, comparative analysis of implemented algorithm is performed on the basis of different parameter like mathematical computation, Unified Average Change Intensity (UACI), Number of Pixel Change Rate (NPCR), Computational time and Correlation-Coefficient analysis. Here the polynomial coefficients are used as randomly.

4.4.1 Number of Pixel Change Rate(NPCR)

Human eye cannot distinguish small change on light intensity of the image pixel. Although two image looks similar does not mean their pixel intensity are also the same. It is beneficial when image is used as key or shared as a secret. Even small number of bit changes on key does not reveal the original secret. So to distinguish how many pixels are changed/different from original image with shared images number of pixel change rate (NPCR) is used.

It gives the total number of different pixels that are different from original image's pixels. Consider two images, whose corresponding plain images and shared images, be denoted by I_o and I_{shrare}. The pixel value at grid (i,j) in I_o and I_{share} are denoted as $I_o(i,j)$ and $I_{share}(I,j)$. A bipolar array, D with the same size as images I_o and I_{share} is defined. Then, D(i,j) is determined by $I_o(i,j)$ and $I_{share}(i,j)$ [18, 23].

Mathematically, NPCR is defined as:

$$NPCR = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{D(i,j)}{T} * 100\% \quad \text{.....Eq(5)}$$

Where $D(i,j) = \begin{cases} 0, if\ I_o(i,j) = I_{share}(i,j) \\ 1, if\ I_o(i,j) \neq I_{share}(i,j) \end{cases}$

And T=(M*N) is total number of pixels.

The NPCR measures the percentage of different pixel numbers between plain/original image with the shares image. A high NPCR value is interpreted as high resistance to differential attacks.

Table 2: NPCR Measures

S.No	(Threshold(k), Total Share(n) and p=257)	Shares	NPCR(%)	
			Shamir's Secret Sharing Scheme	Proactive Secret Sharing Scheme
1	(2,3)	Shares 1	99.99974568684897	100.0
		Shares 2	99.99949137369791	99.99949137369791
		Shares 3	100.00	99.99898274739584
2	(3,5)	Shares 1	100.0	100.0
		Shares 2	99.99923706054688	99.99923706054688
		Shares 3	100.0	100.0
		Shares 4	100.0	100.0
		Shares 5	100.0	100.0
3	(4,7)	Shares 1	100.0	99.99974568684897
		Shares 2	100.0	100.0
		Shares 3	100.0	100.0
		Shares 4	100.0	100.0
		Shares 5	100.0	100.0

		Shares 6	100.0	100.0
		Shares 7	100.0	99.99974568684897
4	(9,9)	Shares 1	100.0	99.99974568684897
		Shares 2	99.99974568684897	99.99974568684897
		Shares 3	100.0	100.0
		Shares 4	100.0	100.0
		Shares 5	99.99974568684897	100.0
		Shares 6	99.99974568684897	100.0
		Shares 7	100.0	99.99974568684897
		Shares 8	100.0	100.0
		Shares 9	100.0	100.0
Average			99.99990463	99.99985165

The average value of NPCR for Shamir's Secret sharing scheme and Proactive Secret Sharing Scheme are 99.99990463 and 99.99985165 respectively. Although both the scheme generates good results Shamir's Secret Sharing has better results than Proactive Secret Sharing Scheme due

to slightly high NPCR Value. A high NPCR value is interpreted as high resistance to differential attacks.

4.4.2 Unified Average Change Intensity (UACI):

Unified Average Change Intensity determines the average intensity of differences between the two images. It is better to have high UACI value to be consider as good results [18].

Mathematically UACI is Defined as:

$$UACI = \left[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|I_o(i,j)-I_{share}(i,j)|}{F}\right] * \frac{100\%}{T*C} \quad \text{.....Eq(6).}$$

Where T=M*N is the total number of pixels. F is the largest supported pixel value and C is the total number of color component of image.

Table 3: UACI Measures

S.No	(Threshold(k), Total Share(n) and p=257)	Shares	UACI(%)	
			Shamir's Secret Sharing Scheme	**Proactive Secret Sharing Scheme**
1	(2,3)	Shares 1	27.40620465579895	31.801848234953706
		Shares 2	34.98121972177543	34.98121972177543
		Shares 3	32.48756691261574	32.94341025652699
2	(3,5)	Shares 1	32.39115796058007	33.766218862762116
		Shares 2	32.62385283160573	32.62385283160573

		Shares 3	31.93519775124677	29.69702394439764
		Shares 4	25.80041856287871	25.80041856287871
		Shares 5	33.85132002155246	32.16905747623485
3	(4,7)	Shares 1	25.779884022565184	34.52437024750221
		Shares 2	31.114107684632014	30.96467394195091
		Shares 3	33.34692994493804	33.34692994493804
		Shares 4	29.525469611672793	32.95131542064526
		Shares 5	34.31292963962929	34.31292963962929
		Shares 6	34.87724786230682	34.87724786230682
		Shares 7	31.53185177472682	32.11768322780501
		Shares 1	33.47066708899272	26.47351632710376
4	(9,9)	Shares 2	28.29864501953125	33.93342726630583
		Shares 3	26.15725149516187	33.6970453532433
		Shares 4	25.80041856287871	31.669150624659586
		Shares 5	25.998452047377107	33.6970453532433

		Shares 6	25.998452047377107	34.39786225362541
		Shares 7	32.315668841592625	25.87993912707227
		Shares 8	34.84621367942793	33.766218862762116
		Shares 9	29.744077528743706	31.44082229381553
Average			30.60813355	32.15971784

The average value of UACI for Shamir's Secret Share and Proactive Secret Share are 30.60813355 and 32.15971784 respectively. Proactive secret share has good results than Shamir's secret share in terms of UNCI value. A high UACI value is interpreted as high resistance to differential attacks.

4.4.3 Mathematical Performance analysis:

Shamir's scheme of secret sharing uses the polynomial f(x) of degree t-1 to share the secret where $f(0)=a_o$ is the secret. Since each share are generated by substituting I in the polynomial to get f(i) which does not reveal about a_o. also proactive secret sharing scheme adopts the Shamir's scheme it has the same security approach.

Assume there are t-1 shares instead of t-shares, to solve a polynomial system with t-1 equations with t unknowns [15, 19]:

$$\begin{pmatrix} 1 & ID_1 & \dots & ID_1^{t-1} \\ 1 & ID_2 & \dots & ID_2^{t-1} \\ \vdots & \vdots & \dots & \vdots \\ 1 & ID_{t-1} & \dots & ID_{t-1}^{t-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} f(ID_1) \\ f(ID_2) \\ \vdots \\ f(ID_{t-1}) \end{pmatrix}$$

It is impossible to solve this system of equation unless a t-th term is available. Thus we need at least t points to interpolate the polynomial. Hence t-1 shares do not reveal any information about secret. So both the scheme is mathematically secure.

4.4.4 Correlation- Coefficient

Correlation-Coefficient (CC) describe the degree of probability that establish a linear relationship exists between pixels in an image. If CC=1, that means the original image and its shares are identical. If CC=0, the generated shares are completely different from the original image. i.e. good secret shares generations. If CC=-1, that means the generated shares are negative of the original (secret) images [10].

Correlation Coefficient is calculated as:

$$CC = r_{xy} = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - (\sum x_i)^2}\sqrt{n\sum y_i^2 - (\sum y_i)^2}} \quad \text{.....Eq(7).}$$

Where, r_{xy} is the correlation coefficient between pixels' x and pixel y.

n is sample size. i.e. total number of pixels.

x_i, y_i are the individual pixel of two image index at i^{th} position.

Table 4: Correlation-Coefficient Measures

S.No	(Threshold, Total shares)	Shares	Correlation Coefficient	
			Shamir's Secret Sharing Scheme	**Proactive Secret Sharing Scheme**
1	(2,3)	Shares 1	0.06945623726216789	0.03752209940463833
		Shares 2	-0.40385800819840156	-0.40385800819840156
		Shares 3	-0.05539531175939599	0.1502498933814922
2	(3,5)	Shares 1	-0.041819241076399304	-0.24054419482922787

		Shares 2	-0.07603310806639312	-0.07603310806639312
		Shares 3	0.02544599802743423	0.21150114862047295
		Shares 4	0.3057233523525209	0.3057233523525209
		Shares 5	-0.25019619724148645	-0.01255367304013418
3	(4,7)	Shares 1	0.31759752004783903	-0.3364504541242564
		Shares 2	0.09776799074729052	0.1104885670401905
		Shares 3	-0.37162888603430916	-0.37162888603430916
		Shares 4	0.22440200087269382	-0.15307379524068365
		Shares 5	-0.3070037504353272	-0.3070037504353272
		Shares 6	-0.4337673488741702	-0.4337673488741702
		Shares 7	0.061544953560074445	-0.005321556397196287
		Shares 1	-0.3776893665740551	0.178382488588857
4	(9,9)	Shares 2	-0.005264463121888006	-0.2598918413289188
		Shares 3	0.22295941106056474	-0.3867446620086043
		Shares 4	0.3057233523525209	0.049377013847060024

		Shares 5	0.3970910818310121	-0.3867446620086043
		Shares 6	0.3970910818310121	-0.415306894725362
		Shares 7	-0.03133270674596812	0.27459614111696046
		Shares 8	-0.38411078818745104	-0.24054419482922787
		Shares 9	-0.1321261121516813	-0.2627846182865279
	Average		-0.018559263	-0.123933789

The average correlation value of Shamir's secret share and Proactive secret share are -0.018559263 and -0.123933789 respectively and Proactive secret share gives less correlation value than Shamir's secret share. So the generated shares by Proactive scheme is less correlated than Shamir's scheme with original images. The success of encryption of secret sharing process means smaller values of CC. Hence, Proactive secret share scheme is better than Shamir's secret share on the basis of Correlation-Coefficient.

4.4.5 Computational Time Analysis

It is the analysis of the time taken by the algorithms to generate and reconstruct secret. Also called as execution time. It is used to measure the computational performance for different number of shares(n) and threshold(t) with variation of prime(p) number in microsecond. Which ultimately help us to determine the good approach for secret share scheme.

Table 5: Computational Time Measures

S.No.	Threshold Shares(K), Total Share(N), Prime Number(P)	Shares Generation Time		Shares Reconstruct Time	
		Shamir's Secret Sharing	Proactive Secret Sharing	Shamir's Secret Sharing	Proactive Secret Sharing
1	(3,5,257)	17162	22163	1905	1744
2	(4,7,257)	20917	30621	2160	2623
3	(4,5,461)	22202	30881	1922	1783
4	(5,5,461)	24947	25936	1892	1936
5	(4,8,593)	31184	38288	2555	2363
6	(6,6,593)	36940	37015	2074	2040
7	(4,7,256)	36226	28700	2657	2150
8	(8,8,256)	65919	68532	2386	2395
9	(3,5,997)	17391	18245	2045	2081
10	(5,5,997)	31115	23548	1907	1864
Average		30400.3	32392.9	2150.3	2097.9

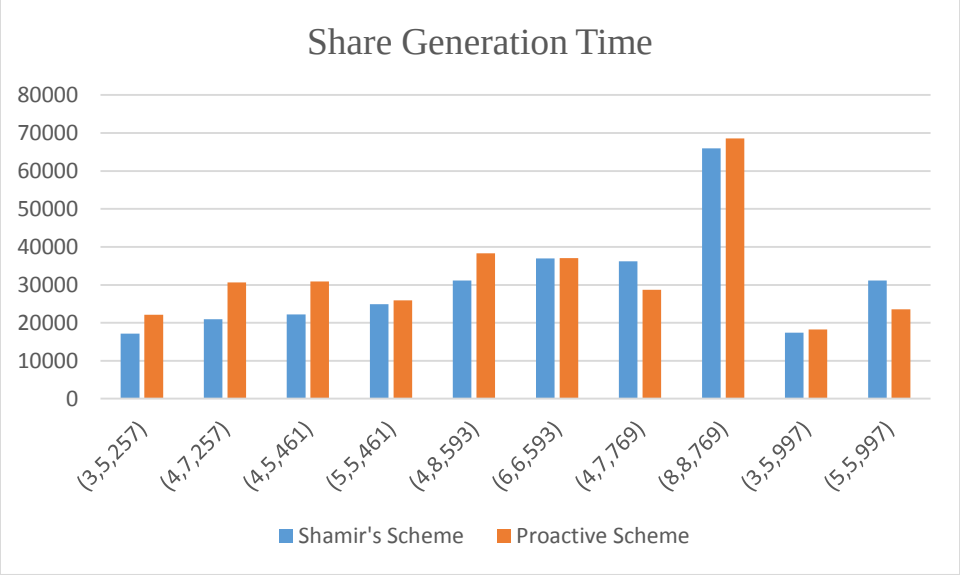


Figure 3: Shares Generation Time Measurement (millisecond)

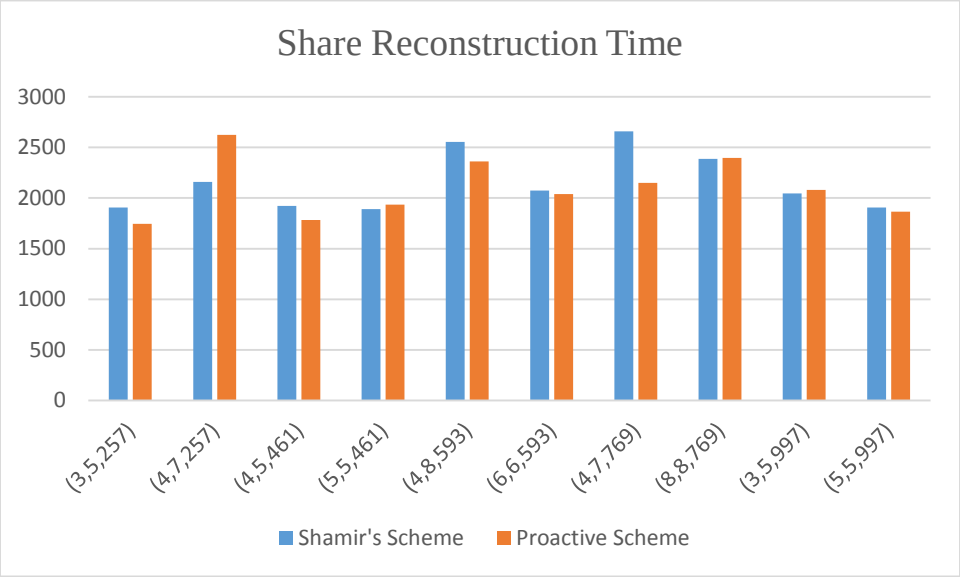


Figure 4: Share Reconstruct Time Measurement (millisecond)

4.5 Results

From table 1, Number of Pixel Change Rate ranges from 99-100% for both the secret share scheme. While NPCR measures the percentage of different pixels that change in two image. Which means measurement of changed pixel from the generated results by applying some sort of encryption algorithm or secret sharing scheme with the original/secret images. So both the scheme is very good for the secret sharing scheme. However, applying some experiments shows that Shamir's Secret Share Scheme gives higher value than Proactive secret share scheme. Which means Shamir's Secret Share Scheme has good differential analysis value which helps to protect from attackers. Although both the scheme is able to hide the significant information of image data.

From table 2, the Unified Average Intensity Value for Proactive Secret Share Scheme is 32.15971784 and for Shamir's secret share is 30.60813355. UACI shows the average differences of intensity between images and higher the UACI value has less chance of differential attack. So from the UACI value it can be said that Proactive Secret Share Scheme is better than Shamir's Secret Share Scheme.

From Correlation-Coefficient table 3, the average correlation value for Shamir's Secret Share Scheme and Proactive Secret Share Scheme are -0.018559263 and -0.123933789 respectively. Proactive Secret Share Scheme gives less correlation value than Shamir's Secret Share Scheme. So it can be said that shares generated by Proactive scheme are less correlated i.e. more different than the shares generated by Shamir's scheme with the secret image.

From the computational time analysis, Shamir's Share generation are faster than Proactive Share generation process by 1992.6 millisecond on average but the share reconstruction time of Proactive Scheme are faster than Shamir's Scheme by 52.4 millisecond. Overall computation time of Proactive Secret Share Scheme are higher than that of Shamir Generation. It is due to the factor that this scheme updates the share to prevent the secret from possible attack.

Chapter 5

Conclusion and Future Recommendation

5.1 Conclusion

The study of visual secret share scheme that is Shamir's Secret Share Scheme and Proactive Secret Share Scheme have been completed and implemented as well. The image data sets are chosen randomly one as secret image and other as Embedding (XOR) image for the authentication process in the PNG format tested with implemented algorithm with variation of different thresholds, total shares and prime number. The algorithms are implemented and analyzed with different parameters to test the strength of the Secret Share Scheme. Although from the result obtained both the scheme Shamir's Secret Share and Proactive Secret Share are strong enough to generate secret's shares without revealing the information being sent and are able to holds confidentiality of Secret. Also applying XOR help the scheme to achieve the authentication of the secret being sent. With little variation on results obtained it is found that Shamir's Secret Share Scheme has high NPCR which proves it has strong diffusion mechanism. In case of UACI analysis Proactive Secret Share Scheme has higher value than Shamir's Secret Share Scheme. A high NPCR/UACI value is interpreted as high resistance to differential attacks. The Correlation Coefficient value of Proactive Secret Share is low. So with regarding the CC the Proactive Secret Share Scheme is better. That means the generated shares are more different than secret image as compared to Shamir's Scheme. Since the computational time of Shamir's Secret Share Scheme is less than Proactive Secret Share Scheme it is computationally efficient compared to Proactive Scheme.

5.2 Future Recommendation

In this work, XOR operation is applied for the authentication process in 2D images. So in future different authentication operation can be applied such as DES, AES or Hash function on secret image and apply secret share scheme. Also thorough study for the cryptanalysis and preventing mechanism from submission of fake shares should be analyzed.

References

[1] Ao, A., Visual Cryptography For Color Images, *International Journal of Electrical and Electronics Engineering (IJEEE)*, vol. 2, no. 1, 2012.

[2] Ateniese, G. Blundo, C. et. al, Visual Cryptography for General Access Structures, *Information and computation 129, article no. 0076,* 1996.

[3] Chang, C-C. Chung, J-C. and Lin, P-Y., Sharing a Secret Two-Tone Image in Two Gray-Level Images, *Proceedings of the 2005 11th International Conference on Parallel and Distributed Systems (ICPADS'05), the Computer Society,* 2005.

[4] Chang, J-J-Y. Huang, B-Y. and Juan S-T.J., A New Visual Multi-Secrets Sharing Scheme by Random Grids, *Department of Computer Science and Information Engineering, National Chi Nan University Nantou 54561,* 17 September 2018.

[5] Dhiman, K. and Kasana S-S., Extended Visual Cryptography Techniques For True Color Images, *Elsevier, Computer Science and Engineering Department,* Thapar University, Patiala, Punjab-147004, India, 19 September 2017.

[6] Hergberg, A. Jarecki S. et.al., Proactive Secret Sharing or: How to Cope With Perpetual Leakage, *IBM T.J. Watson Research Center Yorktown Heights*, NY 10598.

[7] Hou, Y-C., Visual Cryptography For Color Images, *The journal of the pattern recognition society*, vol. 36, p. 1619 – 1629, 26 August 2002.

[8] Hou, Y-C. Quan, Z-Y. Liao, H-Y., New Designs for Friendly Visual Cryptography Scheme, *International Journal of Information and Electronics Engineering,* vol. Vol. 5, no. No. 1, January 2015.

[9] Ismaiel, Y-H. and Khether, M-M., Binary Image Visual Cryptography, *International Journal of Computer Applications (0975 – 8887)*, vol.177, no.6, November 2017.

[10] Kaur, A. Kaur, L. and Gupta, S., Image Recognition using Coefficient of Correlation and Structural Similarity Index in Uncontrolled Environment, *International Journal of Computer Applications (0975 – 8887)*, vol. 59– No.5, December 2012.

[11] Kester, Q-A. and MIEEE, A Cryptographic Image Encryption Technique Based on The RGB PIXEL Shuffling, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* vol. 2, no. 2, jan 2013.

[12] Krady, M-M., Extension Of Lagrange Interpolation, *International Journal Of Scientific & Technology Research,* vol. 4, no. 1, January 2015.

[13] Naor, M. and Shamir. A., Visual Cryptography, *Department of Applied Math and Computer Science, Weizmanu Institute 76100, Israel,* 1995.

[14] Naskar, R. and Sengupta I., Secret Sharing and Proactive Renewal of Shares in Hierachical Groups, *International Journal of Computer Science and Information Technology*, Vol 2, No.3, June 2010.

[15] Phiri, K-K. Ali, P.et.al., Linear (t, n) Secret Sharing Scheme based on Single polynomial, ISSN 0973-4562 vol. 13, Number 14 (2018) pp. 11600-11605.

[16] Shamir, A., How to Share a Secret, *Communications of the ACM ,* vol. 22, no. 11, November 1979.

[17] Sharma, A. and Srivastava K-D., A Comprehensive View on Encryption Techniques of Visual Cryptography, *International Journal of Recent Research and Review,* vol. vii, no. 2, June 2014.

[18] Somaraj, S. and Hussain M-A., Performance and Security Analysis for Image Encryption using Key Image, ***Indian Journal of Science and Technology,*** *Vol 8(35), DOI: 10.17485/ijst/2015/v8i35/73141, December 2015.*

[19] Tieng, G-D. and Nocon, E., Some Attacks on Shamir's Secret Sharing Scheme by Inside Adversaries, *DLSU Research Congress, De La Salle University, Manila, Philippines,* vol. 4, March 7-9, 2016.

[20] Verheul, R-E. and Van, T-H., Constructions and Properties of k out of n Visual Secret Sharing Scheme, *Designs, Codes and Cryptography,* vol. 11, p. 179–196, 1997.

[21] Verma, J. and Dr. Khemchandani, V., A Visual Cryptographic Technique to Secure Image Shares, *International Journal of Engineering Research and Applications (IJERA),* vol. 2, no. 1, p. 1121-1125, Jan-Feb 2012.

[22] Weir, J. and Yan W., A Comprehensive Study of Visual Cryptography, *Transactions on DHMS V, LNCS 6010, Springer-Verlag Berlin Heidelberg,* p. 70–105, 2010.

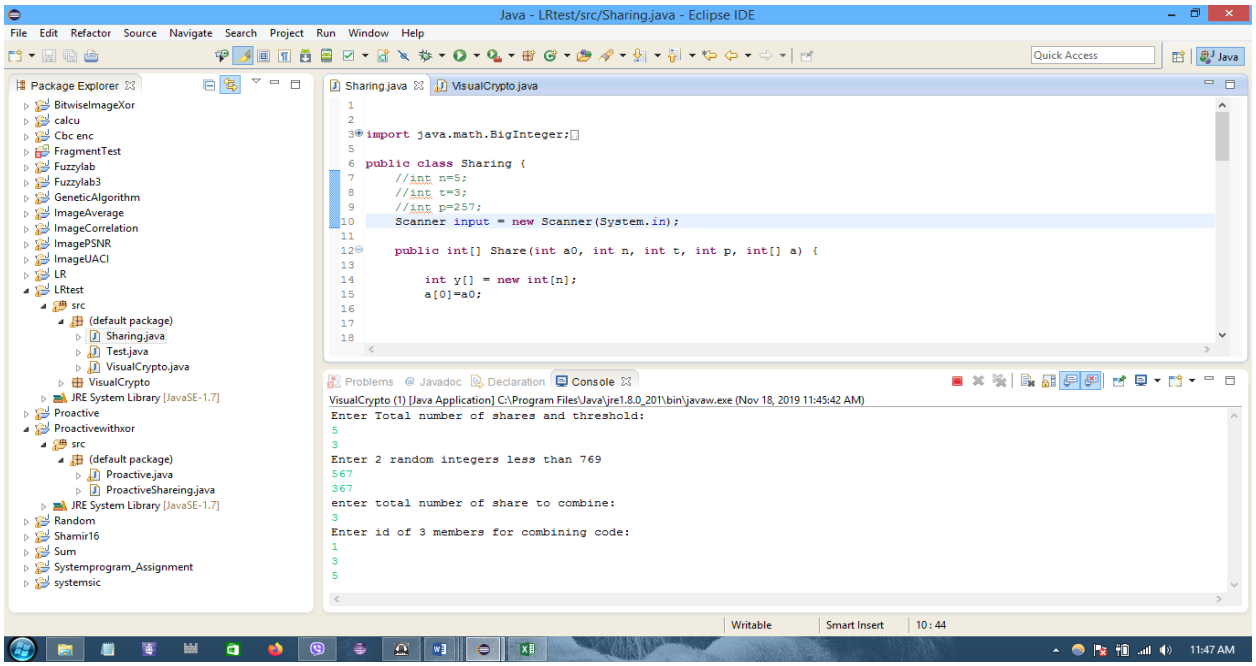
[23] Wu, Y. and Noonan, J-P., NPCR and UACI Randomness Tests for Image Encryption, *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT),* April Edition, 2011.

[24] Yeun, Y-C. Baek, J. and Ebri, A-N., Study on Secret Sharing Schemes(SSS) and Their Applications, 6th International Conference on Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirates, 11-14 December 2011.

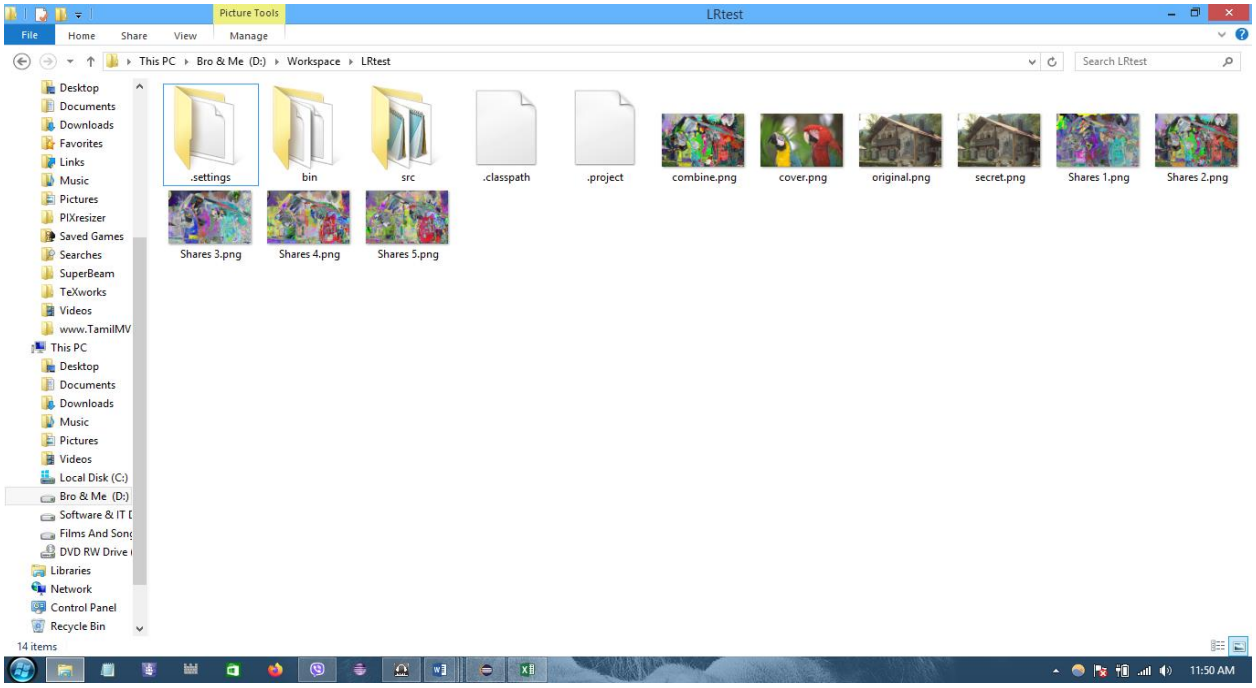
Appendix A

Screenshots

1. *Demo view*



2. *Generated Share Files and Reconstructed File Stored in Directory.*



i. Shamir's Secret Share Scheme (as k=4, n=6, p=769)

Secret Image (Mountain Chalet 768*512)

Cover Image (Two Macaws 768*512)

Share 1

Share 2

Share 3

Share 4

Share 5

Share 6

Combining Share 1, 3, 6 and XOR with Cover Image will not produce Secret Image.

Combining Share 2, 4, 6 and XOR with Cover Image will not produce Secret Image.

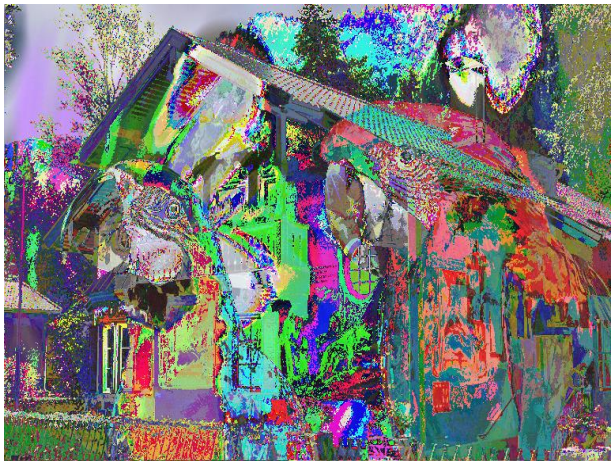
Combining Share 1,3,4,6 and XOR with Cover Image gets Secret Image.

Combining all Share and XOR with Cover Image gets Secret Image.

ii. Proactive Secret Share (as k=4, n=6, p=769)

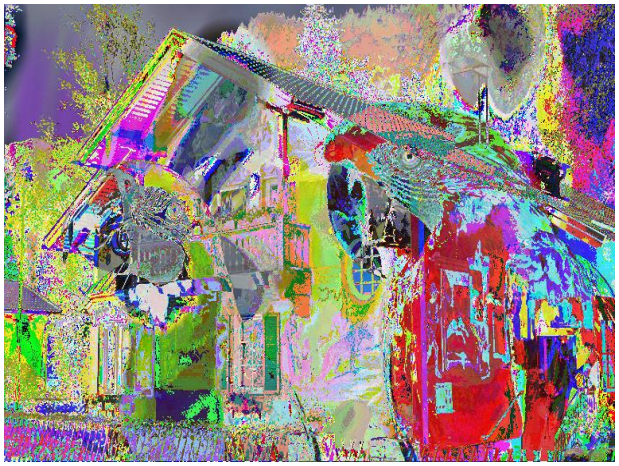
Secret Image (Mountain Chalet 768*512)

Cover Image (Two Macaws 768*512)



Share 1

Share 2

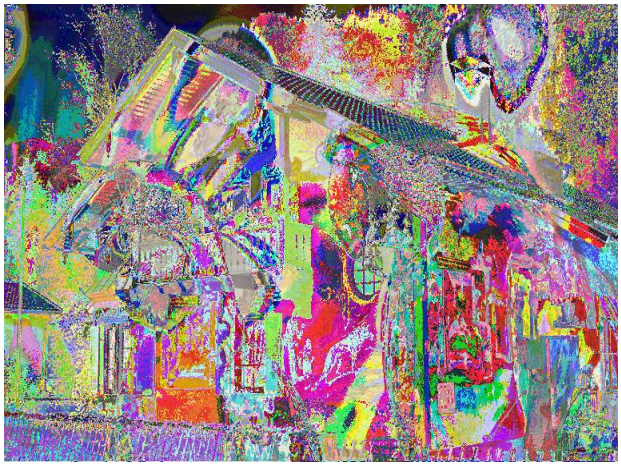


Share 3

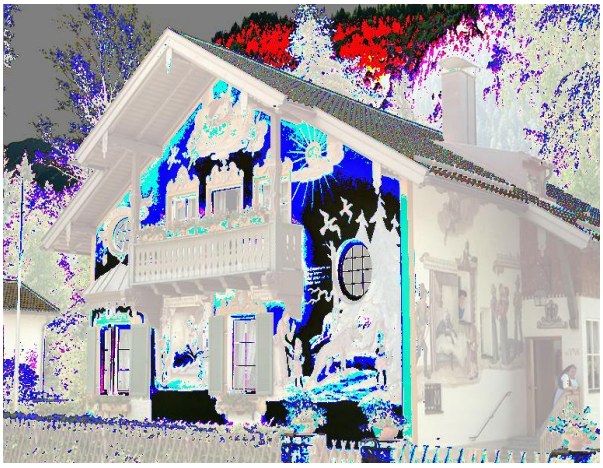
Share 4

Share 5

Share 6



Combining Share 1, 4, 6 and XOR with Cover Image will not produce Secret Image.



Combining Share 1 and 6 and XOR with Cover Image will not produce Secret Image.

Combining Share 1, 2, 5, 6 and XOR with Cover Image gets Secret Image.

Combining all Share and XOR with Cover Image gets Secret Image.

Appendix B

Source Code

Sharing.java

```
public class Sharing {
	Scanner input = new Scanner(System.in);
public int[] Share(int a0, int n, int t, int p, int[] a) {
	int y[] = new int[n];
	a[0]=a0;
	for(int i=0;i<n;i++){
			int value =0;
			for(int j=t-1;j>=0;--j){
				value=a[j]+(i+1)*value%p;
			}
			y[i]=value%p;
			if(y[i]<0){
				y[i]=p+y[i];
			}
			}
		return y;
	}
public int Combine(int q, int p, int [] a, int[] id){
			int z=0,m;
		for(int i=0;i<q;i++){
			m=1;
			for(int j=0;j<q;j++){
				int flag =0;
				if(j!=i){
				int temp = (id[j]-id[i]);
				if(temp<0){
				flag=1;
				temp =-1*temp;
					}
			BigInteger btmp = BigInteger.valueOf(temp);
			BigInteger bp = BigInteger.valueOf(p);
			BigInteger bmul = btmp.modInverse(bp);
```

```
                    int mul = bmul.intValue();
                    mul=mul%p;
                    if(flag==1)
                    mul=-1*mul;
                    m= m*(id[j])*mul%p;
                        }
                }
                z=z+a[id[i]-1]*m;
        }
                int o =  z%p;
                if(o<0){
                o=p+o;
        }
                return o;
    }
    }
```

VisualCrypto.java

```
public class VisualCrypto {
public static void main(String[] args) throws IOException {
   for (int y = 0; y <secretimage.getHeight(); ++y) {
                for (int x = 0; x <secretimage.getWidth(); ++x) {
                    int pixelA = secretimage.getRGB(x,y);
                    int pixelB = coverimage.getRGB(x,y);
                  int pixelXOR = pixelA ^ pixelB;
                  img1.setRGB(x, y, pixelXOR);
                    }
                }
        for(int i=0;i<width;i++){
                    for(int j=0;j<height;j++){
                        int p = toshare.getRGB(i,j);
                        apix[i][j] = (p>>24) & 0xff;
                        a=test.Share(apix[i][j], n, t, 256, l);
                        rpix[i][j] = (p>>16) & 0xff;
                        r=test.Share(rpix[i][j], n, t, 256, l);
                        gpix[i][j] = (p>>8) & 0xff;
                        g=test.Share(gpix[i][j], n, t, 256, l);
```

```
                    bpix[i][j] = p & 0xff;
                    b=test.Share(bpix[i][j], n, t, 256, l);
                    np=0;
                    for(int k=0;k<n;k++){

np=(a[k] & 0xff) << 24 | (r[k] & 0xff) << 16 | (g[k] & 0xff) << 8 | (b[k] & 0xff);
        bImg[k].setRGB(i, j, np);
        }
                                napix[i][j]=test.Combine(q, 256, a, id);
                                nrpix[i][j]=test.Combine(q, 256, r, id);
                                ngpix[i][j]=test.Combine(q, 256, g, id);
                                nbpix[i][j]=test.Combine(q, 256, b, id);
                        }
                }
```

ProactiveSharing.java

```
public class ProactiveShareing {
public int[] shareupdate(int [] s, int[] y, int [][] u, int p){
                        for(int i=0; i<s.length; i++){
                        for(int j=0; j<s.length; j++){
                        y[s[i]-1]= (y[s[i]-1] + u[s[j]-1][s[i]-1])%p;
                        }
                        y[s[i]-1]=y[s[i]-1]%p;
                        }
                return y;
        }
        }
```

Proactive.java

```
public class Proactive {
public static void main(String[] args) throws IOException {

for (int y = 0; y <secretimage.getHeight(); ++y) {

                        for (int x = 0; x <secretimage.getWidth(); ++x) {
                            int pixelA = secretimage.getRGB(x,y);
                              int pixelB = coverimage.getRGB(x,y);
                          int pixelXOR = pixelA ^ pixelB;
        img1.setRGB(x, y, pixelXOR);
```

```
}

}

ProactiveShareing test = new ProactiveShareing();
int [][] u = test.sharet0(n, 256, t, d);
BufferedImage noimage = new BufferedImage(width, height, BufferedImage.TYPE_INT_RGB);
for(int i=0;i<width;i++){
                                for(int j=0;j<height;j++){
                                        int p = toshare.getRGB(i,j);
                                        apix[i][j] = (p>>24) & 0xff;
                                        a=test.Share(apix[i][j], n, t, 256, l);
                                        rpix[i][j] = (p>>16) & 0xff;
                                        r=test.Share(rpix[i][j], n, t, 256, l);
                                        gpix[i][j] = (p>>8) & 0xff;
                                        g=test.Share(gpix[i][j], n, t, 256, l);
                                   bpix[i][j] = p & 0xff;
                                   b=test.Share(bpix[i][j], n, t, 256, l);
                                   int [] updatea = test.shareupdate(id, a, u, 256);
                                   int [] updater = test.shareupdate(id, r, u, 256);
                                   int [] updateg = test.shareupdate(id, g, u, 256);
                                   int [] updateb = test.shareupdate(id, b, u, 256);
                                   np=0;
                                   for(int k=0;k<n;k++){
np=(updatea[k] & 0xff) << 24 | (updater[k] & 0xff) << 16 | (updateg[k] & 0xff) << 8 | (updateb[k] & 0xff);
                                        bImg[k].setRGB(i, j, np);
                                        }
           napix[i][j]=test.Combine(q, 256, updatea, id);
           nrpix[i][j]=test.Combine(q, 256, updater, id);
           ngpix[i][j]=test.Combine(q, 256, updateg, id);
           nbpix[i][j]=test.Combine(q, 256, updateb, id);


}
}
}
```

ImgCorr.java

```
public static double SumofPix(int a){
                        double sum=0;
                        sum=sum+a;
```

```
                return sum;
        }
public static double SSofPix(int a){
                double ss=0;
                ss=ss+a*a;
                return ss;
        }
public static double ProdofPix(int a, int b){
                double sp=0;
                sp=sp+a*b;
                return sp;
        }
```