Academia International College

Tribhuvan University

Institute of Science and Technology

Project Report

On

"Adi Shamir's visual secret sharing and its comparison with Ceaser cipher Algorithm for image encryption"

Submitted To:

Department of Computer Science and Information Technology

Academia International College

In partial fulfillment of the requirement for Bachelor Degree in Computer Science and Information Technology

Submitted By:

Nikhil Maharjan (10829/073)
Nirmal Maharjan (10830/073)
Sachin Maharjan (10836/073)
Sujan Raj Tuladhar (10845/073)

Nov 04 2020

ABSTRACT

In this paper, we have studied the Adi Shamir's visual secret sharing scheme which is different from conventional cryptography, visual cryptography is an image cryptographic technique proposed by Naor and Shamir. Visual cryptography schemes allow the encoding of a secret image into shares, which is distributed to the participants. The requirement for minimum threshold shares ultimately leads to the confidentially of secret. (k, n) visual secret sharing uses threshold scheme by using the concept of Lagrange's polynomial interpolation. Also, we have compared it with the Caesar Cipher encryption with image. Then we have calculated the efficiency of the encryption in terms of the NPCR and UACI. In Caesar cipher we have key which is used to encrypt and decrypt the image color pixel values. We had the existing pixel value with the key for encryption and subtract the encrypted pixel values with key for decryption again. From our study average value of NPCR for Shamir's Secret Share is 99.9993. Also, the average NPCR value of the Caesar cipher algorithm is 100. Similarly the average value of UACI for Shamir's Secret Share is 65.9841. Also, average UACI value of the Caesar cipher algorithm is 97.66. Hence based on NPCR and UACI the Caesar cipher seems to be better algorithm but the key used in the encryption can be guessed easily. Since, shares are distributed and threshold shares are necessary to reveal original image it is visual secret sharing is quite stronger algorithm in image encryption.

Keywords: *cryptography, (k, n) visual secret sharing, Caesar Cipher algorithm*

ACKNOWLEDGEMENT

We would like to express our sincere gratitude towards to our project mentor Mr. Krishna Bikram Shah for guiding and helping us to complete project in the topic “Adi Shamir’s visual secret sharing and its comparison with Ceaser cipher Algorithm for image encryption”. From him we had gained lot of benefits from his experience in the computer science and information technology field. We would also like to express our gratitude towards our colleges’ team leader Ms. Shristi Awlae for support and encouragement during the project duration.

Sachin Maharjan
Nikhil Maharjan
Nirmal Maharjan
Sujan Raj Tuladhar

TABLE OF CONTENTS

LIST OF FIGURE

LIST OF TABLE

ABBREVIATION

VSS	Visual Secret Sharing
NPCR	Number of Pixel change Rate
UACI	Unified Average Change Intensity

1. INTRODUCTION

1.1 Visual Secret Sharing

Cryptography is a technique of securing information through the use of codes so that only those for whom the information is intended can read and process it. Cryptography has four main objectives. They are confidentiality, integrity, non-repudiation and authentication. Confidentiality means the information cannot be understood by anyone for whom it was intended. If information could not be altered in storage or transit between sender and intended receiver then we can say integrity of information is maintained. Non-repudiation means the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information. Authentication is maintained when sender and receiver can confirm each other's identity and the origin/destination of the information.

Till now lots of the cryptographic techniques and algorithms has developed such as AES (Advanced Encryption Standard), RSA (Rivest, Shamir, Adelman), Diffie-Hellman, DES (Data Encryption Standard), Blow Fish, MD5, SHA and many other. But these all algorithms depends upon the secret key. Imagine we encrypt our important files with one secret key and if such a key is lost then all the important files will be inaccessible. Keyed cryptographic techniques provide various way to protect secret information but most of them requires highly complex encryption and decryption. 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 the multiple intended 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 [1]. Thus confidentiality can be achieve without complex computation.

Visual cryptography is a cryptographic technique which allows visual information (pictures, images etc.) to be encrypted in such a way that the decryption can be performed by the human visual system. In this algorithm the given data is portioned into multiple shares. Then we define minimum threshold number of shares which when gathered form shared participants can reveal the secret. Suppose the data 'D' is divided into N shares. Then 'D' can be constructed from 'K' shares out of 'N'. Complete knowledge of k-1 shares reveals no information about 'D'. 'K' of 'N' shares is necessary to reveal secret data. Visual cryptography was pioneered by Moni Naor and Adi Shamir in 1994 at Eurocrypt. Visual cryptographic schemes are used to secure visual data based on authentication techniques that contain sensitive data such as military surveillance, satellite images, medical records etc. Visual cryptographic scheme also provide secure way to transfer images on the internet [2].

Caesar cipher we have key which is used to encrypt and decrypt the image color pixel values. We add the existing pixel value with the key for encryption and subtract the encrypted pixel values with key for decryption again.

1.2. Problem Statement

The general idea of the traditional visual cryptography model is to split a secret image into multiple random shares which separately reveals no information about the secret image other than the size of the secret image. The secret image can be reconstructed by superimposing the threshold number of the shares.

But in Adi Shamir's visual cryptographic scheme there is use of geometrical and mathematical functions that provides the secure way to transfer the secret data on the internet. To maintain confidentiality of the encrypted image it provides shares available only to selected people. Shamir's (k, n) visual secret sharing uses threshold scheme by using the concept of Lagrange's polynomial interpolation. The original image can be generated without loss and without complex mathematical calculation. Also there are lot of drawbacks in the traditional visual secret sharing schemes. Some of them are listed below:

- **Much time consumption for encryption and decryption:** In the traditional visual secret sharing scheme such as Region Incremental Visual Cryptography (RIVC) consist of division of images into regions which lead to high security. But as algorithm is applies to all the separate regions of the image. So it takes huge memory and takes lot of encryption and decryption time [3].

- **The decrypted images has low quality:** In a basic 2-out-of-2 scheme 2 share images are produced from an original image and share must be stacked to reproduce the original image. In this scheme original pixel is changed into 2*2 block of sub Pixels. As shown in Table 1 if the original pixel is white it can be combination of the six combinations of share pixels that is randomly created. Similar, the possible share combination for black pixels is also shown. After stacking the shares with white transparent and black opaque, the original secret image will be revealed. Here the resulting share images contain 4 times more pixels than the original image (since each pixel of the original image was mapped to four sub pixel). So the recovered image has degraded visual quality [4].

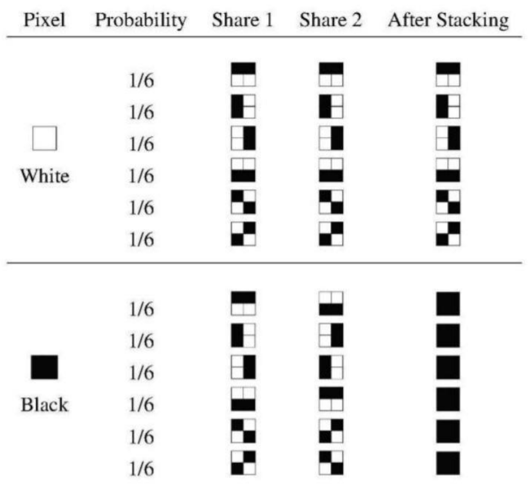


*Figure 1: Pixel combinations in 2*2 schemes*

- **The overlapping had to be done correctly:** In traditional visual secret sharing schemes the share images must be overlapped correctly to reveal the secret which is quite a difficult task. But in Shamir's visual cryptographic schemes we use Lagrange's interpolation formula for reconstruction of the secret image.

1.3 Objectives

The main objectives of research project are:

- To understand how the share construction and secret image reconstruction happens in the Naor Shamir’s visual cryptographic scheme.
- To implement the visual secret sharing by using Naor Shamir’s scheme and study the performances.
- To compute Adi Shamir’s Visual Secret Sharing algorithm and Ceaser Cipher Algorithm and provide conclusion based on result obtained.

1.4 Scope and Limitation

1.4.1 Scope of project

Visual secret Sharing can be used extensively in areas where very confidential data are need to be stored and transferred over insecure network such as internet in a authenticated way. The visual cryptographic techniques can be used in crucial data such as military surveillance, satellite images, medical records, financial transactions, maps, cloud data, biometrics, watermarking etc.

1.4.2 Limitations of the system

Although visual cryptography provides security and confidentiality, it has also got some flaws. There are many things that are not considered in secret sharing. The following are some limitations of study for this system.

- The decryption of the image totally depends upon human visual system. Therefore people with eye problem (blind people) cannot use it.
- The visual secret sharing involves sharing of encrypted images to all participants. So, it is difficult to reveal original message if the participants live in different geographical area.

2. METHODOLOGY

Visual cryptography is one of the best cryptographic scheme as it embodies both the idea of perfect secrecy and a very simple mechanism for decrypting the secret without complex mathematical computation.

The methodology includes implementing the Naor Shamir's secret sharing algorithm and Caesar Cipher algorithm for image encryption. The secret and cover images are standard images. To share the secret among 'n' participants we first extract R, G and B values of the image pixels. Then apply Shamir (k, n) visual secret sharing algorithm.

2.1 Literature Review

In 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 [2].

In 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 sub pixel, the four-pixel colors will be treated as an average color [3].

The visual cryptography schemes to share two secret images in two shares presented in 1998. 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° [4].

In [5], 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.

Zhi Zhou, Gonzalo R.Arc, and Giovanni D Crescenzo proposed the concept of visual cryptography [6]. In this method, a secret binary pixel is encoded into an array of sub-pixels in each of the n-shares. These sub pixels are called halftone cells. Visually halftone shares can be obtained by using halftone cell with an appropriate size. The halftone share carries significant visual information to the viewers, such as landscape, building etc. The above method can be applied in a number of visual secrets sharing application which required high-quality visual images, such as watermarking, electronics cash etc.

In progressive visual secret sharing scheme proposed by Jin, W.Q. Yan and M.S. Kankanhalli, when more shares are stacked progressively, the recovery of secret image will be clearer and clearer [7]. Only sketch will be reveled when few shares are being staked and more detailed will be recovered when more shares are being used.

Young-chang Hou developed an additive and subtractive model which is commonly used to describe the structure of colors [8]. Three primary colors red, red, green and blue (R, G, B) are used in the additive mode. All the desired colors are obtained by making these RGB components. For calculating the intensity of red/green/blue in the compound light can be adjusted. The television is the great example of the additive model. In the subtractive model, color is represented by applying the combinations of colored-lights reflected from the surface of an object. This model uses Cyan(c), magenta (m), and yellow(y) color components and produce a wide range of colors. The color printer is an example of subtraction model. Hou’s scheme utilizes principle of halftone technique an color decomposition. Halftoning is the process of using patterns of pixel of varying size and color to give illusions of various shades. In this method, the color secret shades. In this method, the color secret image is decomposed into three separate images that are respective cyan(c), magenta (m) and yellow(y). The three-color images are translated into halftone image using the halftone technique. A color halftone image is finally generated containing the three halftone images.

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 [9], 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.

2.2 Adi Shamir’s visual secret Sharing

We construct the n shares using polynomial equation of degree k-1 where k is a threshold. Similar, we reconstruct original image using LaGrange's interpolation equation.

We take inputs n as total shares and k as minimum number of require threshold to recover secret. Then generate polynomial equation of degree (k-1) as $q(x) = a_0+a_1x+ \dots +a_{k-1}x_{k-1}$ mod p, where a0 = pixel value and $a_0, a_1, \dots , a_{k-1}$ are coefficients < p, p is large prime.

Then for decryption, Apply Lagrange's Interpolation with minimum required threshold shares as:

$Y = q(x) = \sum_{i=0}^{n} yi\ \ li\ (x) \bmod p$ where $l_i\ (x) = \prod_{j=0\ i\neq j}^{n} \frac{(x-xi)}{(xi-xj)}$

2.3 Caesar cipher algorithm for image encryption

In Caesar cipher algorithm for encryption we used to add the key to the color pixel value of the original image.

Mathematically,

$I_e = I_o + key$

Similarly, for decryption we subtract the color pixel of encrypted image with the key.

Mathematically,

$I_d = I_e - key$

3. REQUIREMENT ANALYSIS

Software requirement is a functional or non-functional need to be implemented in system. Functional means providing particular service to the user. For example, in context to banking application the functional requirement will be when customer selects “View Balance” they must be able to look at their latest account balance. Software requirement can also be a non-functional, it can be performance requirement. For example, a non-functional requirement is where every page of the system should be visible to the user within 5 seconds.

3.1 Functional Requirements

Functional requirement means providing particular service to user. We have implement our comparison system in python programming language using jupyter notebook. Also we use anaconda environment which automatically provides necessary dependencies to run our project. In our project the main requirement of our system is when user defines shares and threshold the system should able to generate the decrypted images which is uploaded by user. Also when user upload threshold amount of the decrypted image, the original image should be produced.

3.2 Non Functional Requirements

Non-functional requirements specifies the quality attributes of a software system. They judge the software system based on responsiveness, usability, security, portability and other non-functional standards that are critical to success of the software system. Some of the non-functional requirements of our project are:

- Encryption and decryption process should be fast as much possible.
- The system should be secured.
- Other user should not know encryption details such as encryption image, threshold and number of participant involved.
- Every unsuccessful attempt by a user to decrypt image should be recorded for security purpose
- The application should be easy to use. Even non-technical people should easily use it.

4. SYSTEM DESIGN

4.1 System Architecture

We construct the n shares using polynomial equation of degree k-1 where k is a threshold. Similar, we reconstruct original image using LaGrange's interpolation equation.

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) = $a_0+a_1x+ \dots +a_{k-1}x_{k-1}$ mod p, where a0 = pixel value and $a_0, a_1, \dots , a_{k-1}$ are coefficients < p, p is large prime.

Reconstruction

Step 1: Apply Lagrange's Interpolation with minimum required threshold shares as:

Y = q (x) = $\sum_{i=0}^{n} yi \;\; li\,(x)$ mod p where l_i (x) = $\prod_{j=0\; i\neq j}^{n} \frac{(x-xi)}{(xi-xj)}$

4.1.1 Process Flow Chart:

In Adi Shamir' algorithm we first input secret image in the system. Then we divide the image into 'n' shares, where n is number of participants.

Similarly, for decryption (image reconstruction) we input 'k' number of shares in the algorithm to get original image.

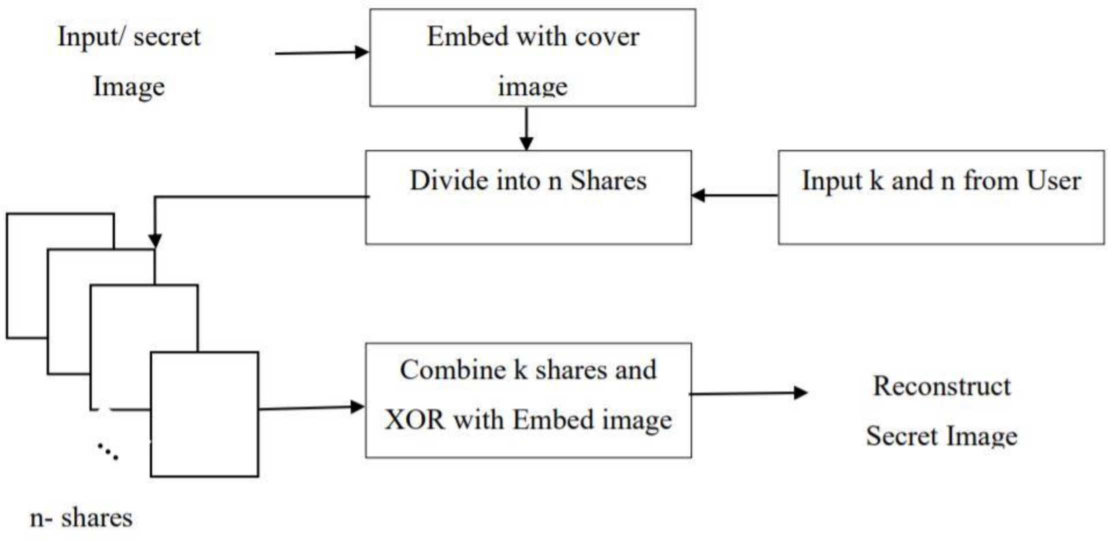
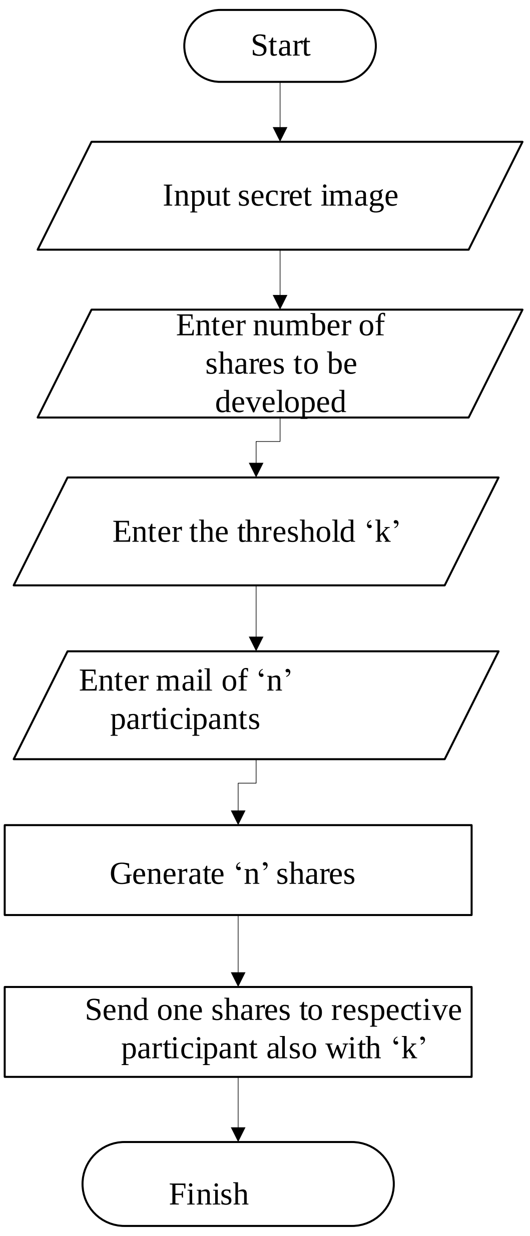


Figure 2: Shamir's Visual Secret Sharing Scheme

4.1.2 Flow chart of share generation in Adi Shamir's VSS



Start
Input secret image
Enter number of shares to be developed
Enter the threshold 'k'
Enter mail of 'n' participants
Generate 'n' shares
Send one shares to respective participant also with 'k'
Finish

Figure 3: Flow chart of encryption of secret image in proposed system

4.1.3 Flow chart of decryption of image in Adi Shamir’s VSS

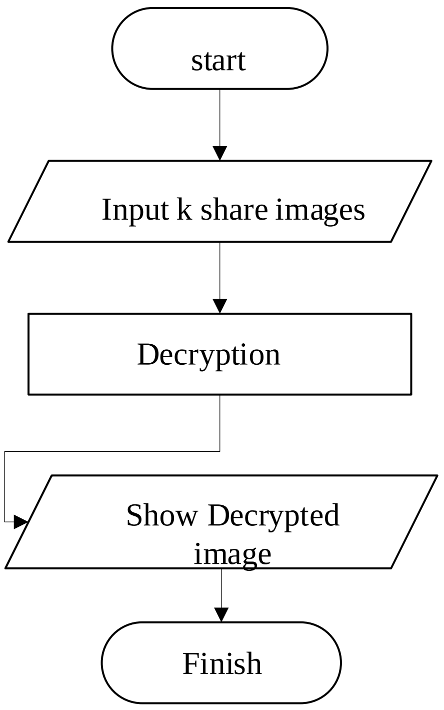


Figure 4: Flow chart of decryption of secret image in proposed system

4.2 Approaches of Algorithm Comparison

NPCR

NPCR stands for Number of Pixel Change Rate. Human eye cannot separate tiny change on the light intensity of the image pixel. Even though two different image looks same does not mean their pixel intensity are also same. Even small number of bit changes on key does not reveal the original secret. So, to distinguish how many pixels are changed 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 images' pixels.

Mathematically, NPCR is defined as:

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

Where D(i, j) = $\begin{cases} 0, if\ Io(i,j) = Ishare(i,j) \\ 1,\ ifIo(i,j) \neq Ishare(i,j) \end{cases}$

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

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

UACI

Unified Average Change Intensity (NPCR) determines the average intensity of differences between the two images. It is better to have a high UACI value to be considered as good results.

Mathematically UACI is defined as

UACI = $[\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|Io(i,j) - Ishare(i,j)|}{F}] * \frac{100\%}{T*C}$

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.

5. IMPLEMENTATION AND TESTING

5.1 Implementation Tools

All the implementation is done in python programming language using Visual Studio Code text editor. For converting the image to matrix, we used the Pillow and Numpy. Furthermore, for sending share image to the participants we used the django SMTP backend. We also have made simple system to demonstrate how to use visual secret sharing can be used in the commercial apps for authentication.

Also we used to show quick algorithm implementation using python in jupyter notebook. Jupyter notebook is a interactive python IDE which runs on the browser. Jupyter notebook is open source and part of ipython (interactive python) which is mostly used by data scientist and AI researchers.

After implementing Adi Shamir's' visual secret sharing algorithm and the Caesar cipher algorithm for image encryption, we perform the NPCR and UACI test.

5.1.1 Tools and Technology

Backend programming language: python 3

Python is a general-purpose, interpreted, high-level programming language. Python allows programmers to use different programming styles to create simple or complex programs get quicker results and write code almost as if speaking in a human language.

Modules and Framework

Django

Django is an open-source python web framework used for rapid development, pragmatic, maintainable, clean design, and secures websites. A web application framework is a toolkit of all components need for application development. The main goal of the django framework is to allow developers to focus on components of the application that are new instead of spending time on already developed components.

Numpy

Numpy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays.It is the fundamental package for scientific computing with python.It consists of many different features.

Some of them are listed below:

- Powerful N-dimensional array object.
- Sophisticated (broadcasting) functions.
- Tools for integrating C/C++ and FORTRAN code.
- Useful for calculating linear algebra, Fourier transforms, and random number capabilities.

Pillow

Pillow is a python Imaging Library (PIL), which adds support for opening, manipulating and saving images. The current version identifies and reads a large number of formats.

5.2 Testing

Testing is the process of evaluating a system or its component(s) with the intent to find whether it satisfies the specified requirements or not. Testing is executing a system in order to identify any gaps, errors, or missing requirements in contrary to the actual requirements.

An early start to testing reduces the cost and time to rework and produce error free software that is delivered to the client. However, in Software Development Life Cycle (SDLC), testing can be started from the Requirements Gathering phase and continued till the deployment of the software. It also depends on the development model that is being used.

5.2.1 Objectives of Testing

The objectives of testing are:

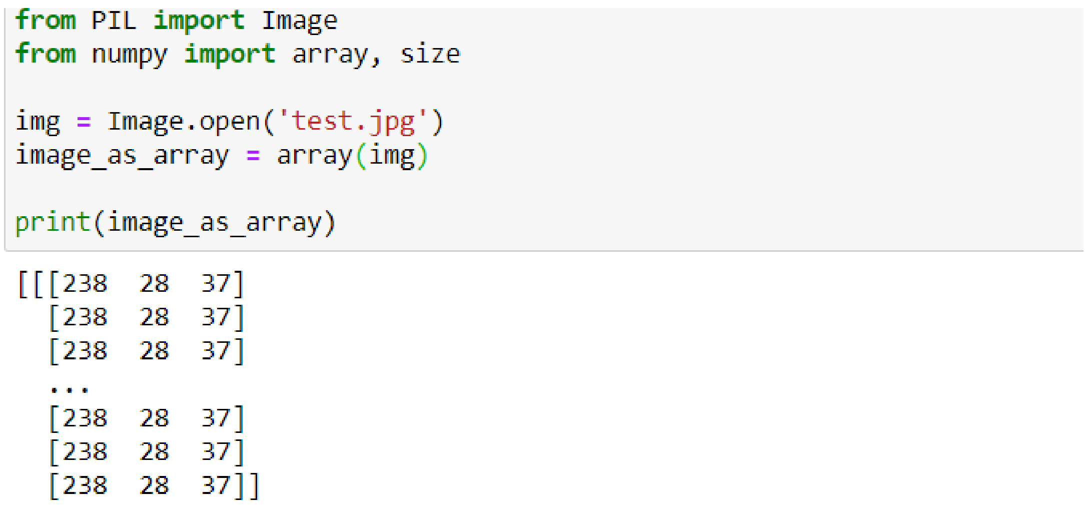
- Testing is a process of executing a program with the intent of finding errors.
- A Successful test case is one that uncovers an as-yet-undiscovered error**.**

5.2.2 Purpose of testing

System testing is a stage of implementation, which is aimed at ensuring that the system works accurately and efficiently as per the user need before the live operation commences. As stated, before testing is vital to the success of a system. System testing makes a logical assumption that if all parts of the as system are correct, the goal will be successfully achieved. A series of tests are performed before the system is ready for the user acceptance test.

5.2.3 Testing Image to Matrix Transform

Testing for the image to NumPy array are done in following ways to visualize if the image is correctly transformed in to required matrix form or not**:**



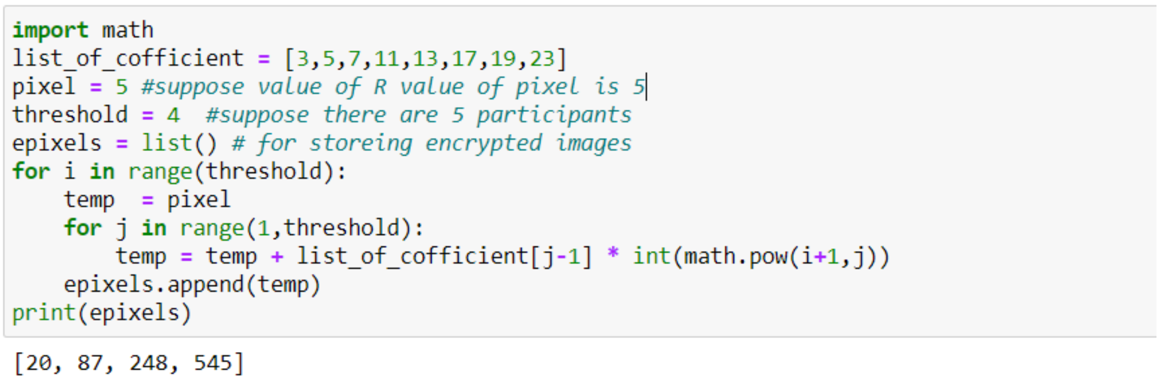
```python
from PIL import Image
from numpy import array, size

img = Image.open('test.jpg')
image_as_array = array(img)

print(image_as_array)
```

```
[[[238  28  37]
  [238  28  37]
  [238  28  37]
  ...
  [238  28  37]
  [238  28  37]
  [238  28  37]]
```

Figure 5: Image to Matrix

5.2.4 Testing the encryption of color pixel value

During share generation we should determine that each individual color value of each pixel are generated according to LaGrange interpolation or not:



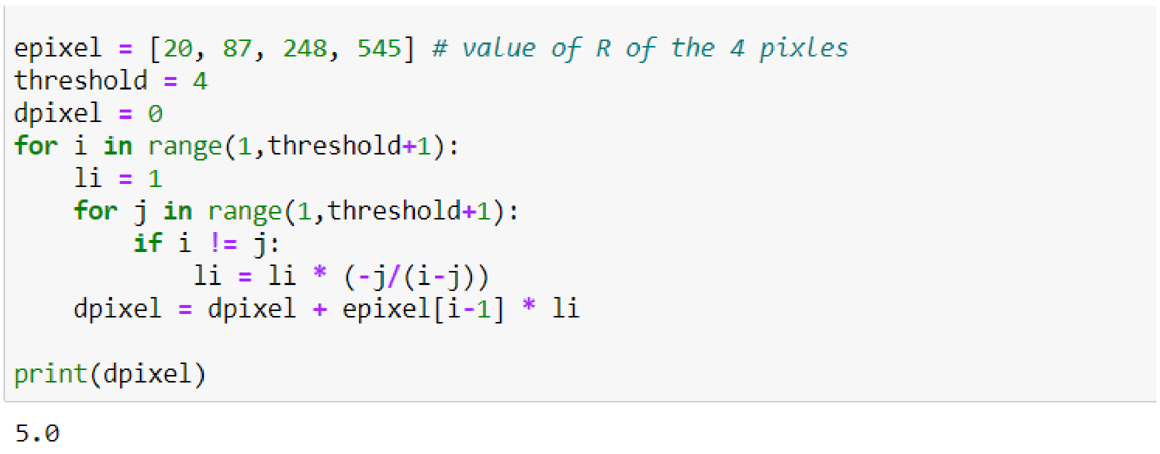
```
import math
list_of_cofficient = [3,5,7,11,13,17,19,23]
pixel = 5 #suppose value of R value of pixel is 5
threshold = 4  #suppose there are 5 participants
epixels = list() # for storeing encrypted images
for i in range(threshold):
    temp  = pixel
    for j in range(1,threshold):
        temp = temp + list_of_cofficient[j-1] * int(math.pow(i+1,j))
    epixels.append(temp)
print(epixels)
```

```
[20, 87, 248, 545]
```

Figure 6: Encryption of color pixel

5.2.5 Testing the decryption of color value

As in share generation we should also check that original value is correctly generated from shares or not.



```
epixel = [20, 87, 248, 545] # value of R of the 4 pixles
threshold = 4
dpixel = 0
for i in range(1,threshold+1):
    li = 1
    for j in range(1,threshold+1):
        if i != j:
            li = li * (-j/(i-j))
    dpixel = dpixel + epixel[i-1] * li

print(dpixel)
```

```
5.0
```

Figure 7: Decryption of color value

6. RESULT OBTAINED AND CONCLUSION

6.1 Result Obtained

The result of NPCR obtained from the both algorithm area:

Table 1 NPCR Result

S.No	**(Threshold(k), Total Shares(n) and p=257)**	**Shares**	**NPCR (%)**	
			Visual secret Sharing	**Caesar Cipher**
1	(2,3)	1	100	100
		2	100	
		3	100	
2	(3,5)	1	100	
		2	100	
		3	100	
		4	99.9967	
		5	100	
3	(4,6)	1	100	
		2	99.9943	
		3	100	
		4	100	
		5	99.9943	
		6	100	
4	(7,7)	1	100	
		2	100	
		3	100	
		4	100	
		5	100	
		6	100	
		7	100	
Average			99.9993	100

The average value of NPCR for Visual Secret Sharing scheme is 99.9993 whereas the NPCR of the same image with Caesar Cipher Algorithm is 100. Both algorithms generate good result. But in case of NPCR the result of Caesar Cipher is quite better.

The result of UACI obtained from the both algorithm area:

Table 2: UACI Results

S.No	**(Threshold(k), Total Shares(n) and p=257)**	**Shares**	**UACI (%)**	
			Visual secret Sharing	**Caesar Cipher**
1	(2,3)	1	98.4435	97.66
		2	97.2726	
		3	96.1089	
2	(3,5)	1	96.4980	
		2	89.4941	
		3	78.5990	
		4	63.8132	
		5	45.1361	
3	(4,6)	1	93.774	
		2	67.7042	
		3	5.0583	
		4	88.7959	
		5	3.50192	
		6	31.9066	
4	(7,7)	1	77.8210	
		2	11.6731	
		3	81.7120	
		4	88.7959	
		5	88.7959	
		6	50.5836	
		7	30.3501	
Average			65.9841	97.66

The average value of UACI of secret shares using visual secret sharing is 65.9841. For same image the UACI of Caesar Cipher is 97.66. Clearly Ceaser Cipher has good result in case of UACI test.

The execution time of visual secret sharing algorithm and caser cipher algorithms according to the total number of shares and threshold are given below:

Table 3 Time consumption to share generation and image reconstruction

S.No.	**(Threshold, participants)**	**Share generation time in microseconds**	**Shares reconstruction time in microseconds**
1	(2,3)	811756	536379
2	(3,5)	390484	21839
3	(4,6)	719020	782960
4	(7,7)	862300	880284

6.2 Future Work

The project is about demonstrating how visual secret share can be used in the part of authentication in the different types of modern application. And also show comparison it with simple Caesar cipher algorithm for image encryption.

During our project we have problem to get correct result while using JPG images. We only get expected result in PNG format of image. So, we need extra time for researching the different image compression formats and relation with visual secret sharing.

6.3 Conclusion

The project presents the approach to demonstrate how the visual secret can be applied in the modern applications and also comparison of the visual secret sharing with the Caesar Cipher algorithm for image encryption. We found that there are different types of image encryption technology and one of the most popular one is visual secret sharing. Similarly the Caesar Cipher algorithm is one of the primitive algorithm for message encryption. In addition, there are many other algorithms for share generations. We find that many scholars in the different universities have done more research in the field of image encryption techniques. The main goal is to discover effective and efficient algorithm for image encryption that can be used to secure digital medias such as image specially. The finding highly secure which cannot be rebuild easily by intruders is the ultimate goal of this project.

We have computed the NPCR and UACI of the both algorithm. The value of NPCR and UACI lies between 0 to 100. The higher the NPCR and UACI value higher will be the secured. In terms of the NPCR and UACI the Ceaser Cipher algorithm for image encryption has the best result. We conclude that NPCR and UACI only define the difference between original image and encrypted image. So by using different techniques it is very difficult to generate old original image. Also we have to consider that the Cesar Cipher algorithm use only one key. So guessing the key will be easy and if the any intruder gets the key then he/she can easily decrypt the encrypted image and get original image.

Although NPCR and UACI value of Visual secret sharing is not so good. It is the strong technique because we need threshold number of shares to decrypt. So, we conclude this project by recommending the Visual Secret Sharing scheme is secure algorithm although it is weak in terms of NPCR an UACI.

References

[1] A. D. B. a. A. D. Santis, "Secret Sharing and Visual cryptography schemes," Dipartimento di Informatica ed Applicazioni, Università di Salerno,, 84081 Baronissi (SA), Italy.

[2] M. N. A. Shamir, "Visual Cryptography," Department of Applied Math and Computer Science, Weizmanu Institute, Rehovot, 1995.

[3] M. Quist-Aphetsi Kester, "A cryptographic Image Encryption technique," *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* Vols. Volume 2,, no. Issue 2,, ,January 2013.

[4] D. K. S. Ashish Sharma, "A Comprehensive View on Encryption Techniques of Visual," *International Journal of Recent Research and Review,* Vols. , Vol. VII,, no. Issue 2,, June 2014.

[5] V. V. T. R. J. Tamilarasi, "Improving Image Quality In Extended Visual," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH,* Vols. VOLUME 3, , no. ISSUE 4,, APRIL 2014.

[6] M. I. G. R. A. F. I. a. G. D. C. Zhi Zhou, "Halftone Visual Cryptography," AUGUST 2006.

[7] Z.-Y. Q. a. C.-F. T. Young-Chang Hou1, "Progressive Visual Cryptography with Friendly and size invariant shares," The International Arab Journal of Information Technology, Tamkang, Tiwan, March 2018.

[8] Y.-C. Hou∗, "Visual cryptography for color images," pergamon, Jung Li, Taiwan, Received 6 June 2002; accepted 26 August 2002.

[9] S. J. H. k. a. M. y. Amir hergberg, "Proactive secreat sharing or how to cope with perpetual leakage," IBM TJ Watson Research Center, York Town Heights, New York.

Appendix A

1. Gantt chart

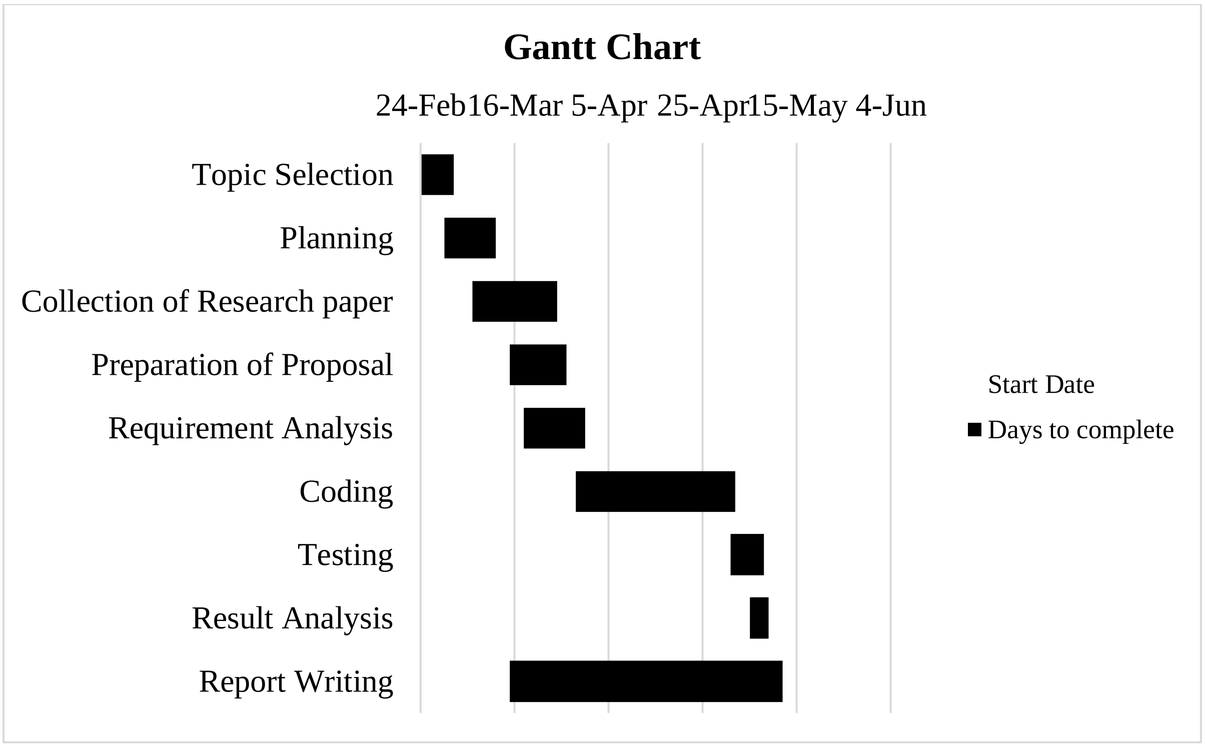
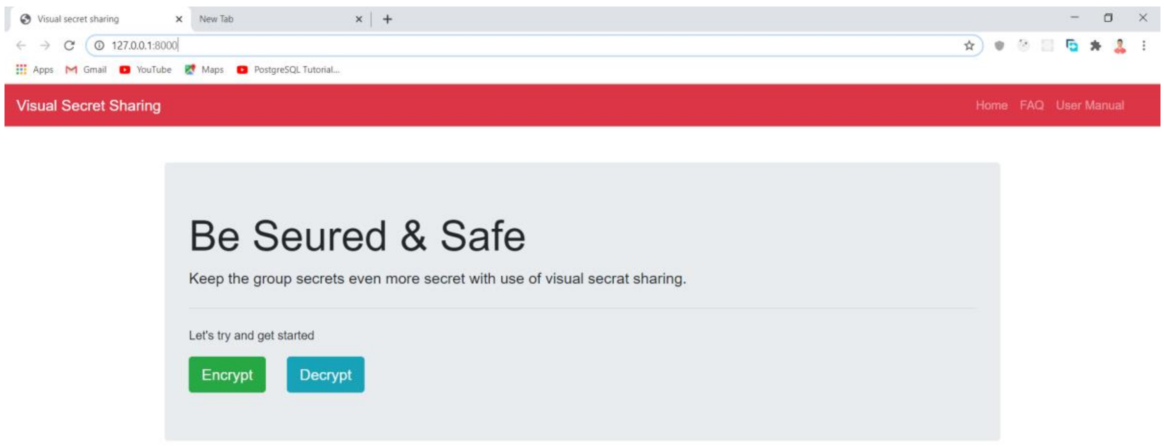


Figure 8: Gantt Chart

Appendix B

1. Screenshots

1. Home View



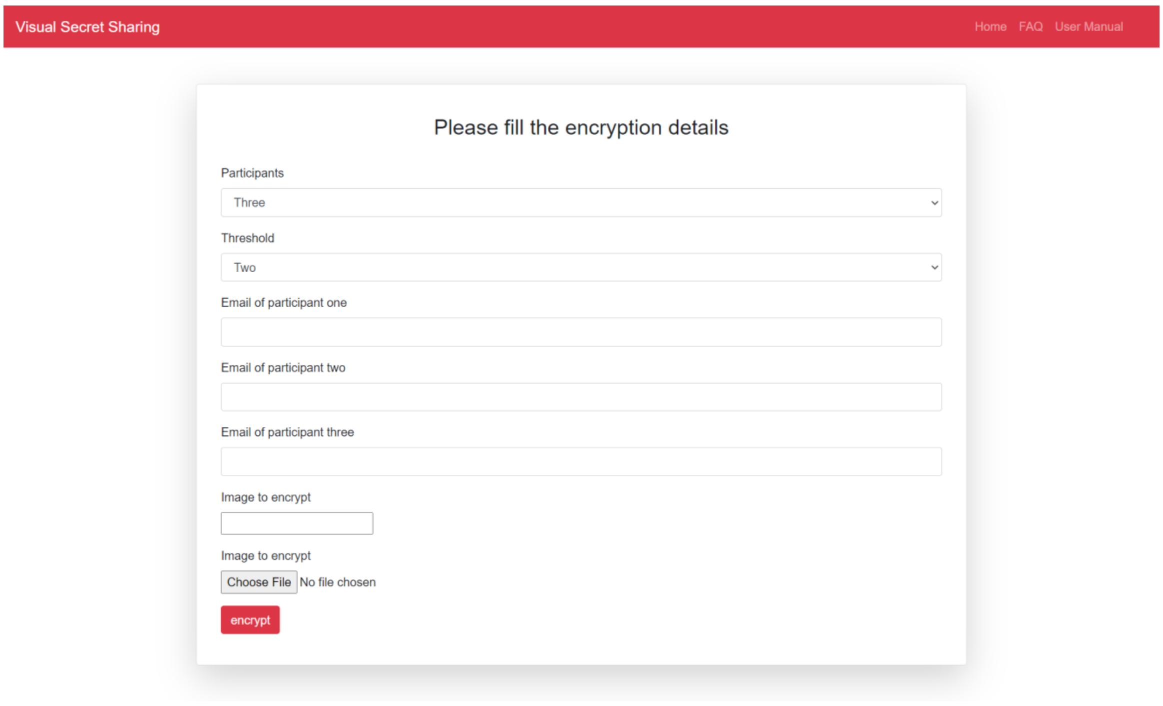
Be Seured & Safe

Keep the group secrets even more secret with use of visual secrat sharing.

Let's try and get started

Figure 9: Home View

2. Encryption Form



Please fill the encryption details

Participants: Three

Threshold: Two

Email of participant one

Email of participant two

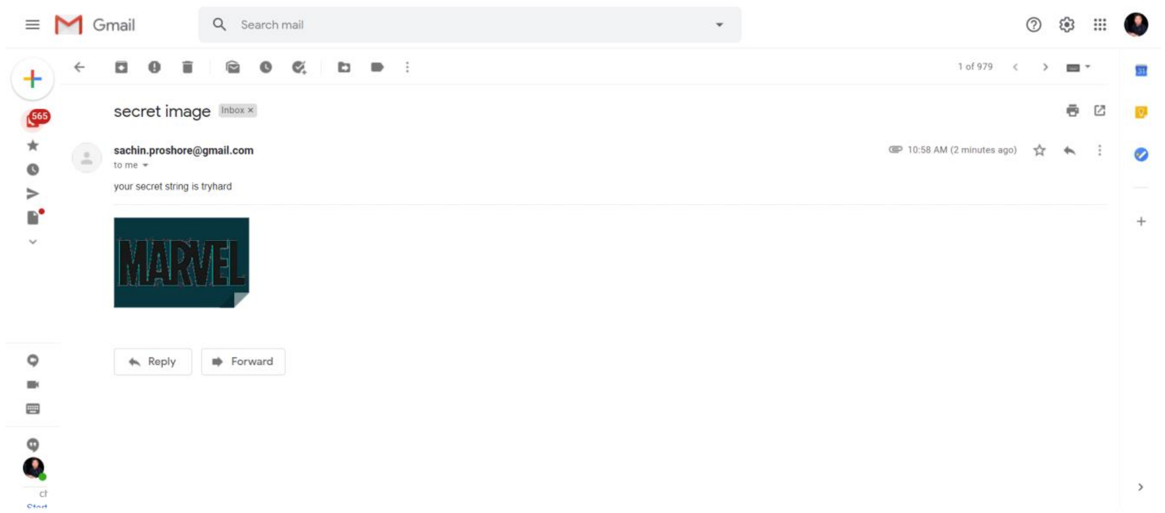
Email of participant three

Image to encrypt

Image to encrypt

Figure 10: Encryption Form

3. Share image in the Gmail



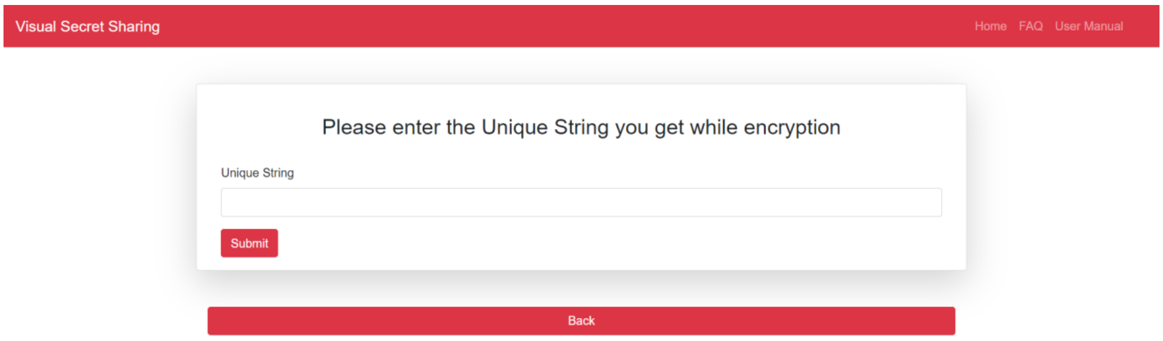
secret image

sachin.proshore@gmail.com
to me
10:58 AM (2 minutes ago)

your secret string is tryhard

Figure 11: Share image in Gmail

4. Decryption verification

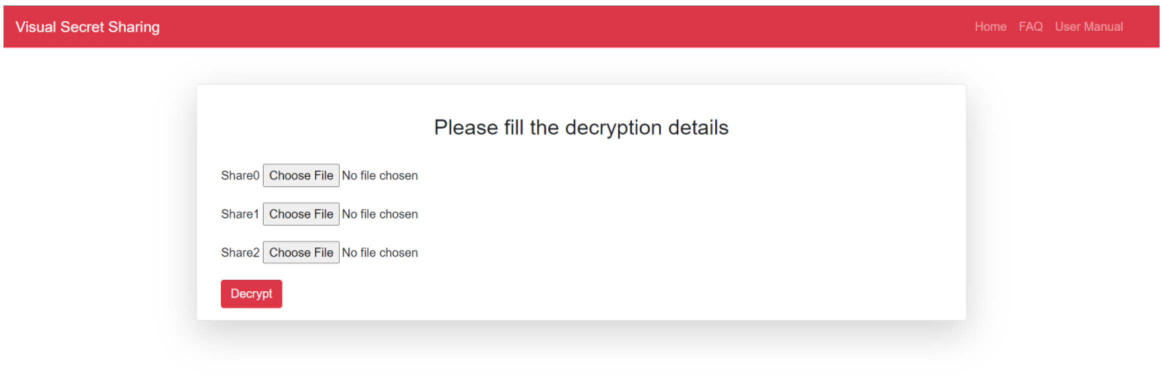


Please enter the Unique String you get while encryption

Unique String

Figure 12: Decryption Verification

5. Decryption Form


Visual Secret Sharing
Home FAQ User Manual

Please fill the decryption details

Share0 Choose File No file chosen

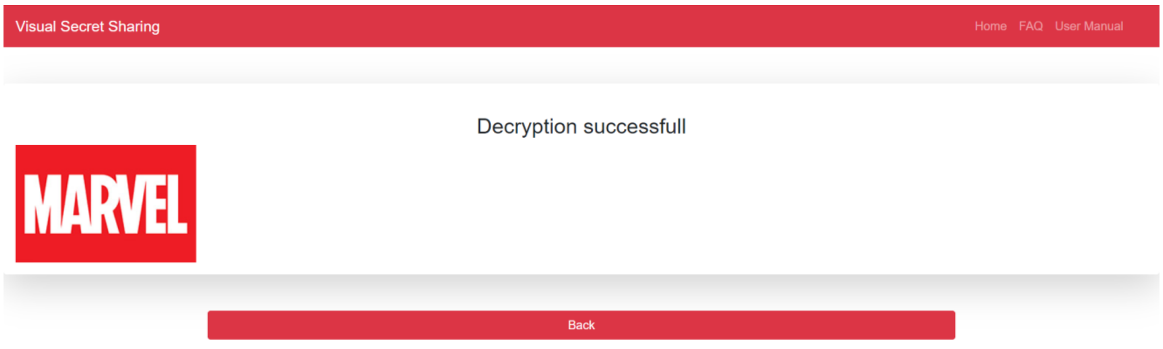
Share1 Choose File No file chosen

Share2 Choose File No file chosen

Decrypt

Figure 13: Decryption Form

6. Decryption Result


Visual Secret Sharing
Home FAQ User Manual

Decryption successfull

Back

Figure 14: Decryption Result

7. Shamir’s Secret Share Scheme (n=4, k=6)

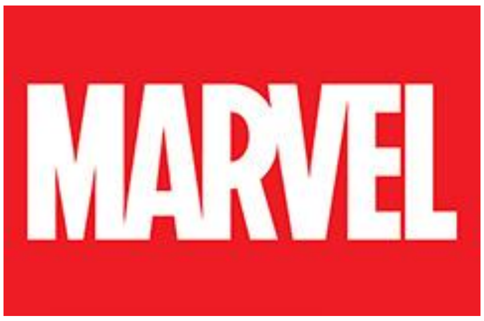


Figure 15: Original Secret Image

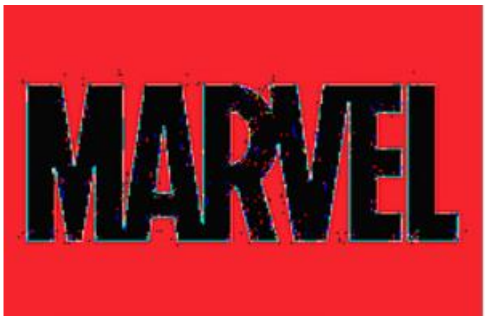


Figure 16: Share 1

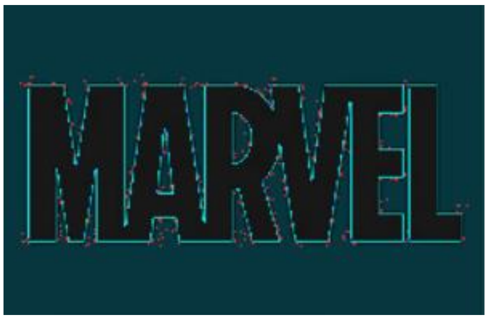


Figure 17: Share 2

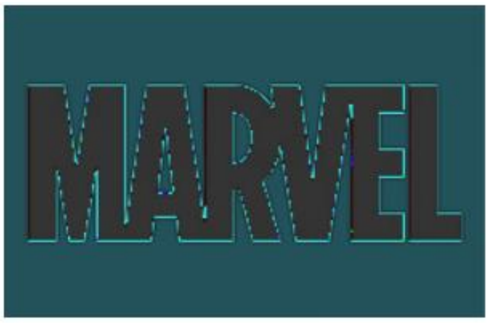


Figure 18: Share 3

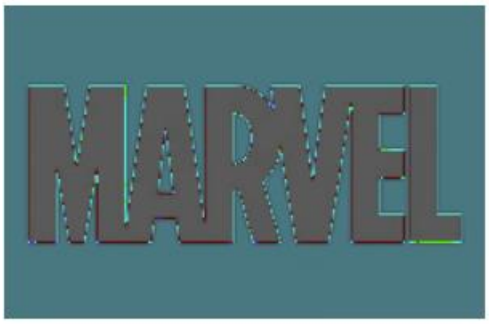


Figure 19: Share 4

8. Encryption using Caesar Cipher (key=5)

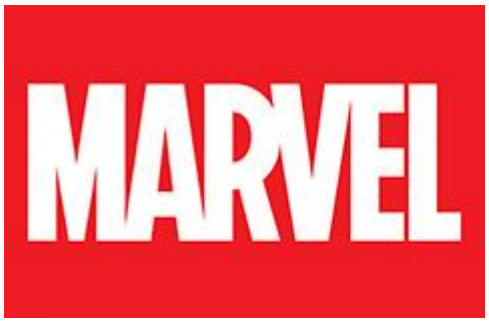


Figure 20: Original Image

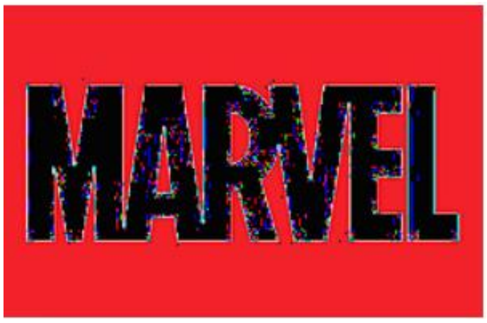


Figure 21: Encrypted Image

Appendix C

Source code

Code for visual secret Sharing

```
# Required Modules

from PIL import Image

from NumPy import array, size

import math

# Configuration Variables

total_Shares = 4

threshold = 3

list_of_cofficient = [3,5,7,11,13,17,19,23]

# function to chnage image to numpy array (Matrix)

def changeImageToMatrix(imagename):

    img = Image.open(imagename)

    image_as_array = array(img)

    return image_as_array

# function to encrypt the single color value of each pixel

def encryption(pixel):

    epixels = list() # for sotring the shares
    for i in range(total_Shares):

        temp = pixel

        for j in range(1, threshold):

            temp = temp + list_of_cofficient[j-1] * int(math.pow(i+1, j))



        epixels.append(temp % 257)

    return epixels

# function to decryt the images to original image

def decryption(epixel):

    dpixel = 0

    for i in range(1, threshold + 1):

        li = 1

        for j in range (1, threshold + 1):

            if i != j:

                li = li * (-j/(i-j))



        dpixel = dpixel + epixel[i-1] * li

    return dpixel



# code for generating the share
```

```
image = changeImageToMatrix('test.jpg')

image = list(image)

encrypted_images = list()

for b in range(total_Shares):

    encrypted_images.append(image)

encrypted_images = array(encrypted_images)



for i in range(len(image)):

    for j in range(len(image[i])):

        for k in range(len(image[i][j])):

            encrypt = encryption(image[i][j][k])

            for b in range(total_Shares):

                encrypted_images[b][i][j][k] = encrypt[b]

# displaying the encrypted image

for b in range(total_Shares):

    encrypted_images[b] = array(encrypted_images[b])

    Image.fromarray(encrypted_images[b], 'RGB').show()

# code for generating the original image from share

decrypted_image = array(image)

for i in range(len(image)):
    for j in range(len(image[i])):
        for k in range(len(image[i][j])):
            row = []
            for b in range(threshold):
                row.append(encrypted_images[b][i][j][k])
            colorpixel = decryption(row)
        decrypted_image[i][j][k] = colorpixel


Image.fromarray(decrypted_image,"RGB").show()
```

Code for calculationg NPCR and UPCR for VS

```
# code for calculating NPCR
m = size(array(image), axis=0)
n = size(array(image), axis=1)


d = 0
for i in range(len(image)):
    for j in range(len(image[i])):
        if list(image[i][j]) != list(encrypted_images[0][i][j]):
            d += 1
npixel_change = (d / (m * n)) * 100
print("NPCR : ",npixel_change)
#code for calculating UACI
m = size(image, axis=0)
n = size(image, axis=1)
original_image = array(image)
total_diff = 0
for i in range(len(image)):
    for j in range(len(image[i])):
        for k in range(len(image[i][j])):
            total_diff = total_diff + (original_image[i][j][k] - encrypted_images[3][i][j][k])
# f= 257, t = M *N, c = 3 s
diff_intensity = (total_diff/257) * (100 / (m * n * 3))
print("UACI : ", diff_intensity)
```

<u>Program to demonstrate ceaser Cipher Algorithm</u>

```
# configurariton variable
key = 5
```

```
def cencryption(pixel):
    return (pixel + key)


def cdecryption(pixel):
    return pixel – key
# encryption
image = changeImageToMatrix('test.jpg')
image  = list(image)
encrypted_image = array(image)
for i in range(len(image)):
    for j in range(len(image[i])):
        for k in range(len(image[i][j])):
            encrypted_image[i][j][k] = cencryption(image[i][j][k])
print("Encrypted Image")
Image.fromarray(encrypted_image,"RGB").show()


# decryption
decrypted_image = array(image)
for i in range(len(image)):
    for j in range(len(image[i])):

        for k in range(len(image[i][j])):

            decrypted_image[i][j][k] = cdecryption(encrypted_image[i][j][k])



print("Decrypted Image")

Image.fromarray(decrypted_image,"RGB").show()
```

Calculating NPCR and UACI for Caesar Cipher

```
# NPCR for ceaser cipher

m = size(array(image), axis=0)

n = size(array(image), axis=1)



d = 0

for i in range(len(image)):

    for j in range(len(image[i])):

        if list(image[i][j]) != list(encrypted_image[i][j]):

            d += 1

npixel_change = (d / (m * n)) * 100

print("NPCR : ",npixel_change)

# UACI for Caesar cipher

m = size(decrypted_image, axis=0)

n = size(decrypted_image, axis=1)

original_image = array(image)

total_diff = 0

for i in range(len(image)):

    for j in range(len(image[i])):

        for k in range(len(image[i][j])):
```

```
        total_diff = total_diff + (original_image[i][j][k] - encrypted_image[i][j][k])

# f= 256, t = M *N, c = 3 s

diff_intensity = (total_diff/257) * (100 / (m * n * 3))

print("UACI : ", diff_intensity)
```