**Title:- Secret Sharing master**

J Component Project

CSE1901

Technical Answers for Real World Problems (TARP)

Summer Semester Special 2021-22



Team Meambers:-

19BCE2054 – Prayag Nikul Purani

(prayagpurani11@gamil.com)

19BCT0055 – Sathwik Gunuganti

(mailto:sathwikgunuganti6221@gmail.com)

**ABSTRACT**

**Aim:**

The aim of the topic is to encrypt the image so that image can secure from the external users.

**Objective:**

As we all know that in today’s world of networking, a secure transmission of information with the help of image encryption which can either contain some kind of information or any text information is one of the most important focuses for security. Image encryption is a useful technique of image content protection. Instead of traditional AES based encryption, with this project, we want to implement an encryption scheme for digital images based on visual cryptography using (k, n) secret sharing scheme.

➢ Here in our project we are trying to implement Lagrange polynomial based logic to achieve image encryption and decryption using secret sharing.

➢ For making encryption and decryption highly complicated we will use rule-based share generation and reconstruction.

➢ Using secret sharing, it makes it harder for someone to break the encryption, because they will have to target ‘k’ shares to decrypt the image

## Keywords

* Grayscale image
* Keys (depending on the algorithm used)
* Cryptosystems
* Random generator
* Cipher block
* Encrypted image and Decrypted image

# INTRODUCTION

# Overall Idea

A (t, n) threshold secret sharing scheme is a cryptographic primitive used to distribute a secret s to n participants in such a way that a set of t (or more) participants can recover the secret s and a set of t −1 (or fewer) participants cannot recover the secret s. A piece of shadow held by participants is called a share.

In our project, we propose a secret sharing scheme for black & white (B/W), grey-level and colour images based on Shamir secret sharing. In this scheme, the share obtained for each participant has a far smaller size than the secret image and the recovered image is the same as the original one without any loss. Thus, the scheme is very fit to be applied in the wireless network and the IC Card system for image encryption. Moreover, secret sharing schemes satisfying the additional property that unqualified subsets can gain absolutely no information about the secret are called perfect schemes.

Secret sharing schemes are very useful in some application fields, such as access control, opening a bank vault, opening a safety deposit box, or even launching missiles.

## Background

The secret usually is text data, although visuals can also be considered. Visual cryptography was the first technique for sharing images, developed by Naor and Shamir. It is based on t of n visual threshold systems, which partition the original picture into n shares. Each one is photocopied onto a transparency, and the original picture is recreated by superimposing t number of transparencies.

Furthermore, it is not recovered using any cryptographic mechanism. Its key characteristic is that it recovers the original image using human vision qualities. Only black and white photographs were appropriate for sharing due to the model's attributes. Nonetheless, not just for processing Gray-level pictures, but also for colour images, a slew of novel suggestions based on visual cryptography have appeared in recent years.

Each pixel of the secret picture is ciphered using 'h' subpixels (pixel expansion) for the 'n' shares in these visual threshold methods; as a result, the size of the shared images is substantially larger than the original. Another downside of these systems is that the contrast between the hidden picture and the restored image is much reduced.

# LITERATURE SURVEY

## Paper Overviews

1. *Secret Sharing Scheme for Image Encryption Using New Transformation Matrix.*

This paper proposes image encryption and decryption process using a new transformation matrix. The image is divided into zones. The zones are constructed from blocks of size 3 x 3 using secret keys. All the zones are combined to form a new transformation matrix and are used for encryption purposes. The sender sends the secret in the form of a polynomial function value for their ID value. The receiver reconstructs the secret from the polynomial’s function value. Then form the transformation matrix and decrypt it to get the original image. The comparison of the proposed method with the Cross Chaotic map image encryption method reveals that the proposed method is higher insecurity and superior in encryption quality and also the share to be sent is smaller.

1. *A (t, n) secret sharing scheme for image encryption.*

This paper introduces a new (t, n) secret sharing scheme for image encryption. The proposed method encrypts the secret image into two images of the same size as the original image, which one is the public image (called the encrypted image) and another is to be shared among n participants using a new secret sharing method based on the Shamir’s secret sharing. In the new secret sharing scheme, t (or more) shares secretly held by the participants could reconstruct the shared image, where the size of each share is 2(log m)t 2/m of that of the shared m m× image. Then the secret image could be recovered from the encrypted image and the shared image through simple XOR operations without any loss. Furthermore, the size of the shares can become smaller by partitioning the secret image into many smaller blocks and encrypting all these block images into a public encrypted image of the same size as the secret image. Compared with the known image encryption schemes based on secret sharing, the size of the shares in our scheme is smaller with the same size original image.

1. *Polynomial Substitution Based Image Encryption Using Shamir Scheme.*

In this paper, an efficient (𝑡, 𝑛) secret sharing is proposed for encryption of images based on polynomial substitution with Shamir secret sharing. The proposed technique enciphers the secret image as two different images: one is made public which is the enciphered image and an additional other one is secret that can be shared among the 𝑛 members. In the proposed method, 𝑡−shares are implemented.

1. *A New Technique for Image Encryption using RIJNDAEL Block Cipher Algorithms.*

This paper has proposed a block cypher Rijndael algorithm that is used to encrypt and decrypt an image with a variable key length and variable block length. The authors in this paper focused on the quality measurements such as the speed, Encryption Ratio, Correlation Coefficient and Compression encryption has no effect on the size of the JPEG image encryption with the existing bitmap image encryption. Since the JPEG files are of compressed format and the compression friendliness is measured here. It is desirable that the size of encrypted data should not increase. The result ends with the comparison of performance parameters based on the type of files formats. Hence for higher data encryption or multimedia encryption, the compressed format can be applied and it yields a higher encryption ratio.

1. *Creation of pseudo-random sequences based on chaos for forming of wideband signal.*

The aim of the paper is the development of a technique for creating pseudorandom sequences based on chaos, as well as the analysis of the correlation characteristics of pseudo-random sequences formed on the basis of a chaotic signal. Chaotic signals are inherently pseudo-random, but they are generated by deterministic systems. All computer models of chaos are approximations of mathematical chaos. Any analysis of these sequences doesn’t allow them to be reproduced and they can’t be intercepted, so they have significant advantages when used for spreading the signal spectrum and creating a pseudo-noise broadband signal. Sequence selection with an acceptable level of side lobes of the autocorrelation function is carried out by using the developed graphical interface method.

1. *A novel fuzzy encryption technique based on multiple right translated AES gray S-boxes and phase embedding.*

In this examination, they proposed a Grayscale picture encryption strategy dependent on RTSs and steganography. The proposed cryptosystem utilizes numerous RTSs and stages installing methods for the age of disarray in spatial and recurrence areas of mystery pictures. The fluffy methodology is utilized for the determination of RTSs. Investigations and correlation indicated that the proposed security framework is safer when contrasted with a few of the notable cryptosystems dependent on a single S-box and a mix of S-box and steganography. In future, the recently created calculation can be utilized for the encryption of shading pictures and information concealing reason with certain changes.

1. *Enhancing the Security in Cryptosystems Based on Magic Rectangle.*

Another encoding plan dependent on MR rather than the existing ASCII based encoding plan has been thought of and the numerals associated with MR are utilized for encryption in RSA and ElGamal open key cryptosystems. The numerals are not handily followed by the busybody in light of the fact that the enchantment total, MRS and MRT utilized in producing the MR are just known to the sender, what's more, the collector. Moreover, for a similar enchantment whole various MRS are created by exchanging columns or segments which will create various numerals at the same position without fail. This causes an extra layer of security for any cryptosystems before performing encryption and unscrambling. Further, to speed up cryptographic activities parallelism is utilized in this paper which depends on the Maui scheduler in recreated conditions with various processors.

1. *Image encryption and decryption using AES algorithm.*

In this paper, Image Encryption and Decryption utilizing the AES calculation are actualized to make sure the picture information from unapproved get to. Fruitful usage of symmetric key AES calculation is extraordinary compared to other encryption and decoding guidelines accessible in the market. With the assistance of MATLAB coding execution of an AES calculation is integrated and reenacted for Image Encryption and Decryption. The first pictures can likewise be totally reproduced with no contortion. It has demonstrated that the calculations have incredibly huge security keyspace and can withstand most normal assaults, for example, animal power assaults, figure assaults, and plaintext assaults.

1. *Encryption On Grayscale Image For Digital Image Confidentiality Using Shamir Secret Sharing Scheme.*

In this study, the Secret Sharing Method was used by employing the Shamir Threshold Scheme Algorithm on grayscale digital images with the size of 256x256 pixels obtaining 128x128 pixels of the shared image with threshold values (4,8). The resulting number of shared images were 8 parts and the recovery process can be carried out by at least using 4 shares of the 8 parts. The result of encryption on the grayscale images is capable of producing vague shared images (i.e., no perceptible information), therefore a message in the form of a digital image can be kept confidential and secure.

1. *Image encryption using separable reversible data hiding scheme.*

An epic distinguishable reversible information concealing plan is executed for picture encryption. An info picture is encoded by the substance proprietor utilizing an encryption key. Information concealing key packs the least huge pieces of the encoded picture to make space to insert information. Haar wavelet lossy pressure procedure can't recover the picture proficiently contrasted with RLC lossless pressure method for quicker transmission. The picture encryption key is utilized to recover the picture and information concealing key for information extraction. Picture encryption and information concealing keys can be utilized for concurrent extraction of the first substance by abusing the spatial relationship in a normal picture. Recreation results gotten is like the common substance. Equipment execution for encryption and decoding of 32 x 32 pictures is actualized.

1. *Non-expanded visual cryptography scheme with authentication.*

This paper combines the non-expanded scheme with the extra ability to hide confidential data to prevent the detection of information. In the proposed scheme, the secret image is divided into four regions, and share blocks are subsequently generated by using the block encoding method with non-expansion ability. A certain sequence of original regions must be followed when generating region shares. Finally, the first share image is reversed and stacked with the other share image. The extra confidential data can be revealed, and it prevents the detection of information.

1. *Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images.*

This paper proposes an encryption scheme with a new additive homomorphism based on Elliptic Curve ElGamal (EC-ElGamal) for sharing secret images over unsecured channels. The proposed scheme enables shorter keys and better performance than schemes based on RSA or ElGamal. It has a lower computation overhead in image decryption compared with the method that uses other additively homomorphic properties in EC-ElGamal. Elliptic curve parameters are selected to resist the Pohlig– Hellman, Pollard’s-rho, and Isomorphism attacks. Experimental results and analysis show that the proposed method has superior performance to RSA and ElGamal.

1. *New Cryptography Algorithm with Fuzzy Logic for Effective Data Communication.*

In this paper, people forget to care about security when data communication gets the importance of privacy most of the time. There the data theft takes place effortlessly. Many methodologies have been devised for making effective communication either over the internet or intranet. However, the hackers enrich themselves more than the new technologies whenever they are launched. As the need arises to cultivate the security key generation while secure data communication has to be ensured, we propose a new cryptography algorithm along with the fuzzy logic through this paper that materializes the secure communication possible. Firstly, we observed the flaw that causes hacking effortlessly by the intruder during the data transmission over the network. Then the evaluation part could be done with the same context without losing data because of this proposed algorithm. This algorithm concentrates on image and text data encryption using fuzzy logic and on a secured sharing theme that provides highly authenticated data transferring. The existing security algorithms had a nod in many ways only for the secure data transmission rather than the complexity in which they have when needed to be executed. Henceforth the aspirants who want to have the communication have to spend more time than the actual. Obviously, the precious algorithms should have less processing time and are highly secure in nature.

1. *Chaotic Genetic-fuzzy Encryption Technique.*

In this technique, binarize any digital data type. The main encryption stages of CGET are chaotic map functions, fuzzy logic and genetic operations. Mathematical operations and rotation are also included that increase encryption quality. Images are used for testing propose. For testing C-GET, digital images are used because they become an important resource of communication. The original and reconstructed data are identical. Experimental results show that the C-GET technique has multilayer protection stages against various attacks and powerful security based on the multi-stages, multiple parameters, fuzzy logic and genetic operations. Decrypted data is nearly random and has a negligible correlation with secret data.

1. *Overview on selective encryption of image and video: challenges and perspectives.*

In this paper it is discussed that traditional image and video content protection schemes, called fully layered, the whole content is first compressed. Then, the compressed bitstream is entirely encrypted using a standard cypher (DES, AES, IDEA, etc.). The specific characteristics of this kind of data (high transmission rate with limited bandwidth) make standard encryption algorithms inadequate. Another limitation of fully layered systems consists of altering the whole bitstream syntax which may disable some codec functionalities. Selective encryption is a new trend in image and video content protection. It consists of encrypting only a subset of the data. The aim of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security. This computation saving is very desirable, especially in constrained communications (real-time networking, high definition delivery, and mobile communications with limited computational power devices). In addition, selective encryption allows preserving some codec functionalities such as scalability. This tutorial is intended to give an overview of selective encryption algorithms. The theoretical background of selective encryption, potential applications, challenges, and perspectives is presented.

1. *An approach towards an efficient encryption-decryption of grayscale and color images.*

Can be applied to any image, especially to images with well-defined contours. The cryptographic strength of the developed modifications is provided by the RSA algorithm as well as by additional use of bitwise binary operations.  It is established that the influence of additional noise functions in the source  image does not significantly affect the results of the method. The resulting image  differs from the source one only by a small change in the brightness level.

1. *Multiple Secret Sharing with Simple Image Encryption.*

The fusion of encryption and MSS increase the stability and security required for a good MSS design. He proposed MSS method can be effectively implemented for achieving the correctness issue and high randomness of shared images.

1. *Kn secret sharing visual cryptography scheme on color image using random sequence.*

This technique needs very less mathematical calculation compared with other existing techniques of visual cryptography on color images. This technique only checks ‘1’ at the bit position and divide. that ‘1’ into (n-k+1) shares using random numbers. The main drawback of the algorithm is in its number of loops. For n=6, k=5 and a 32-bit pixel with 50% ‘1’, the number of loop operations required is 32

1. *Study on Secret Sharing Schemes (SSS) and their applications.*

This paper focuses on the major algorithms of secret image sharing. Low image quality:  The contrast of the reconstructed secret image in VSS is poor due to the stack property. The proposed methods are Single Point of Failure (SPOF) type as they use single storage mechanism and thus these two methods are not robust against loss or manipulation.

1. *An image secret sharing method.*

Its large compression rate on the size of the image shares, its strong protection of the secret image and its ability for real-time processing. Fewer image shares cannot get sufficient information to reveal the secret image.

1. *Secret sharing approach for securing cloud-based image processing.*

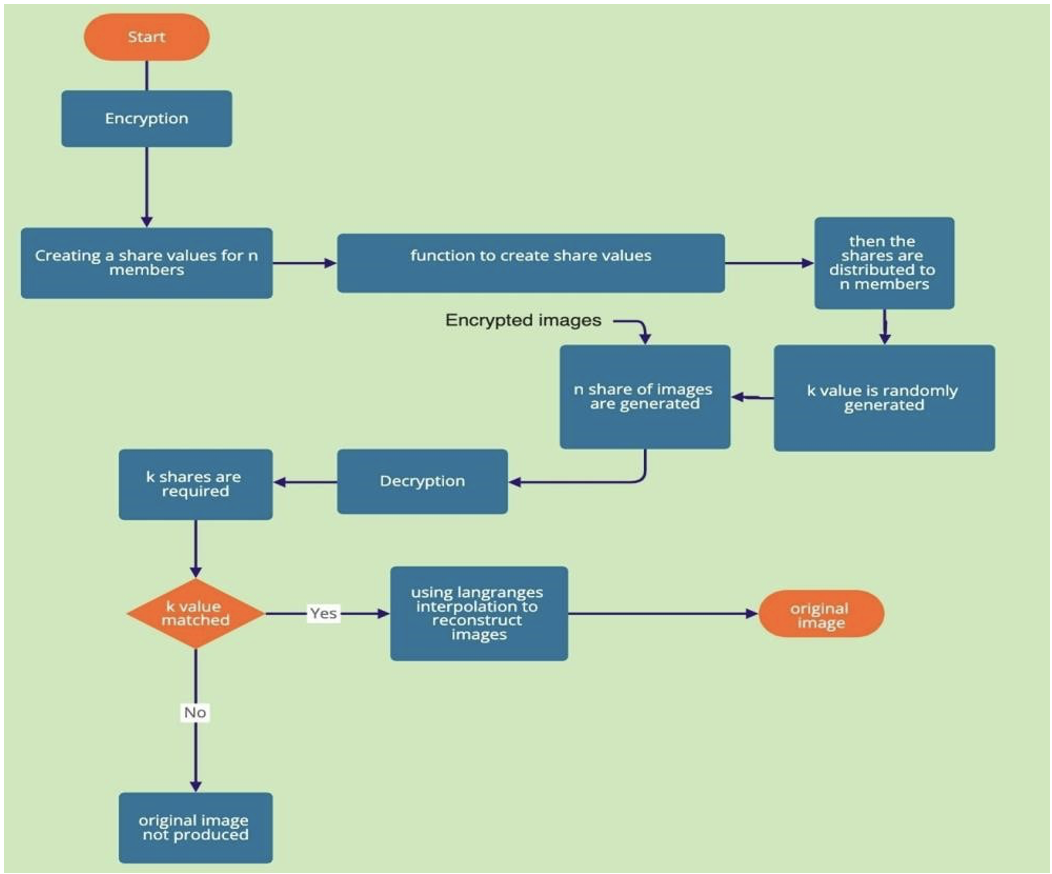
Cloud-based video storage/processing can be more advantageous than conventional serverside video storage/processing, security and privacy are the main concern.

1. *Overview on selective encryption of image and video: challenges and perspectives.*

In this paper it is discussed that traditional image and video content protection schemes, called fully layered, the whole content is first compressed. Then, the compressed bitstream is entirely encrypted using a standard cypher (DES, AES, IDEA, etc.). The specific characteristics of this kind of data (high transmission rate with limited bandwidth) make standard encryption algorithms inadequate. Another limitation of fully layered systems consists of altering the whole bitstream syntax which may disable some codec functionalities. Selective encryption is a new trend in image and video content protection. It consists of encrypting only a subset of the data. The aim of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security. This computation saving is very desirable, especially in constrained communications (real-time networking, high-definition delivery, and mobile communications with limited computational power devices). In addition, selective encryption allows preserving some codec functionalities such as scalability. This tutorial is intended to give an overview of selective encryption algorithms.

# PROPOSED ARCHITECTURE

We convert the image into an array that contains the R, G and B values for each pixel. Depending on the values of (k, n), we then generate n shares of images using the values we get by creating secret shares using Shamir’s scheme using LaGrange’s polynomial. These n shares can then be distributed through separate channels for security.



*Fig 1: Architecter Diagram*

1. First, image is being selected.
2. Then need to select a value for N to encrypt, the image.
3. After which the encryption takes place.
4. Then in the system, encrypted images will be shown depending upon the number of N.
5. Then proceed to the decryption part.
6. If the value of K matches,
7. Then using LaGrange’s, the image will be reconstructed or decrypted
8. And get the original image.
9. But if we fail to match the value of k,
10. We will receive an Error and the original image not be produced.

In this project, the Secret Sharing method put forward by Shamir will be used.

The aim is to distribute the secret data indicated by "S" to "n" people and to obtain the hidden secret by combining the "k" ones. Each person will have a share value. First of all, the function that will create the share values is determined.

f (x) = (S + ax + bx ^ 2 + cx ^ 3 + ... + zx ^ (k-1)) mod (p)

Here, the definition range of values a, b, c, z is [0, p - 1] and they are chosen randomly from this range. (While the "p" value is the prime 257 while storing the image).

Then it is calculated on the 1st share, f (1) determines the value of the 1st share. Likewise, the value of the 2nd share is calculated with f (2), after the value of "n" denominators is calculated, random "k" grain is selected. These k denominators selected are used in Lagrange's interpolation to obtain hidden data.

# ALGORITHM & MATHAMETICAL MODELS

**Lagrange Interpolation**

In Lagrange interpolation (n + 1), a function f (x) whose value (x, y) (x1, y1) (x2, y2) is known at the point (n + 1) is fitted with an L (x) polynomial whose values at these points are equal.

We convert the image into an array that contains the R, G and B values for each pixel. Depending on the values of (k, n), we then generate n shares of images using the values we get by creating secret shares using Shamir’s scheme using LaGrange’s polynomial. These n shares can then be distributed through separate channels for security. When we need to get back the original image, we require at least k shares, and using the R, G, B values from these K shares, we use LaGrange’s interpolation to reconstruct the original image.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Equation | Degree | Shape | Random Parameters | Number of points(K) needed to recover S |
| (S+RX)mod P | 1 | Line | R | 1 |
| (S+R1X+R2X)mod P | 2 | Parabola | R1,R2 | 2 |
| (S+R1X+R2X2+R3X3)mod P | 3 | Cubic | R1,R2,R3 | 3 |

Example:-

S = 1234, n = 6, k = 3

At random we obtain 2 numbers: a(1) = 166 ,a(2) = 94

Our polynomial to produce secret shares (points) is therefore:

q(x) = 1234 + 166x + 94x ^ 2

We construct 6 points from the polynomial:

(1,1494); (2,1942); (3,2578); (4,3402); (5,4414); (6,5614)

We give each participant a different single point (both x and q(x)).

Let us consider:-

(x, y) = (2,1942); (1,31)=(4,3402); (2, 2) = (5,4414)

We will compute Lagrange basis polynomials:

L0=  \* = \* =

L1=  \* = \* =

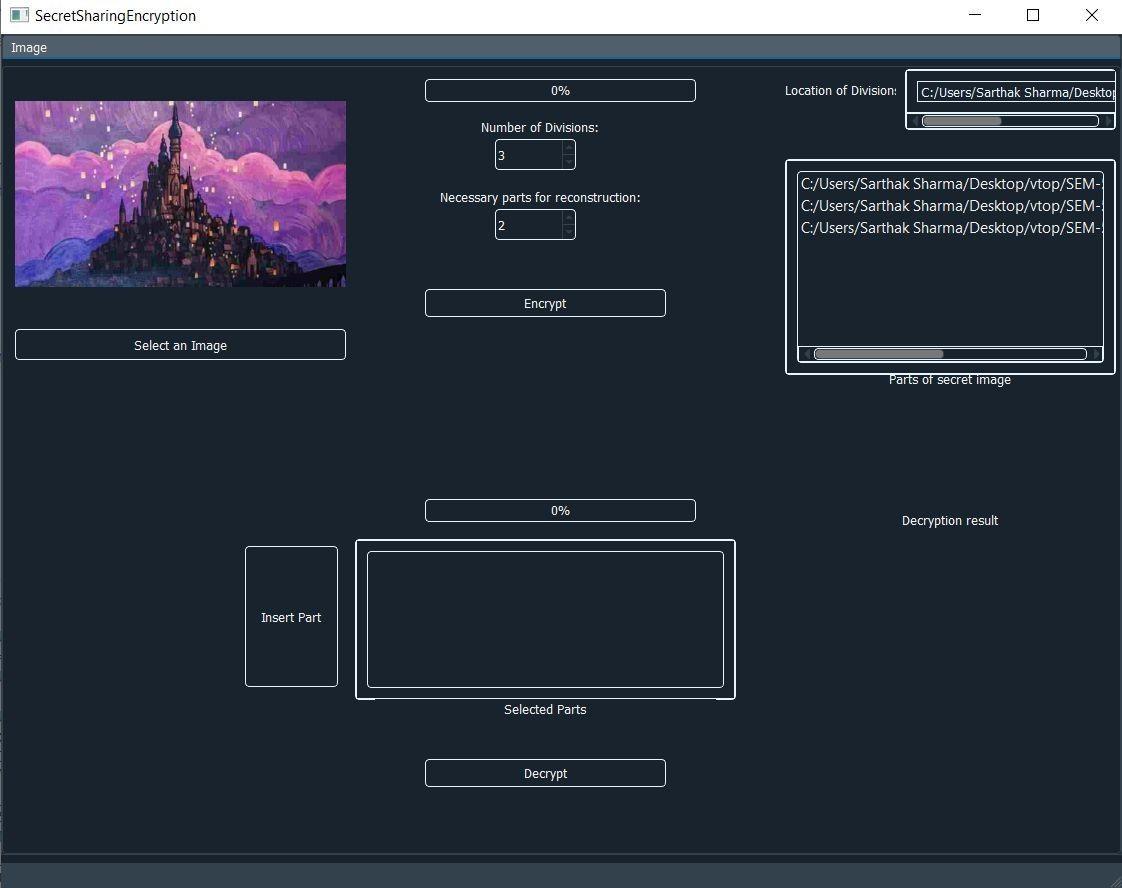
L2=  \* = \* =

F(x) =

= 1942() + 3402() + 4414()

**IMPLEMENTATION:**

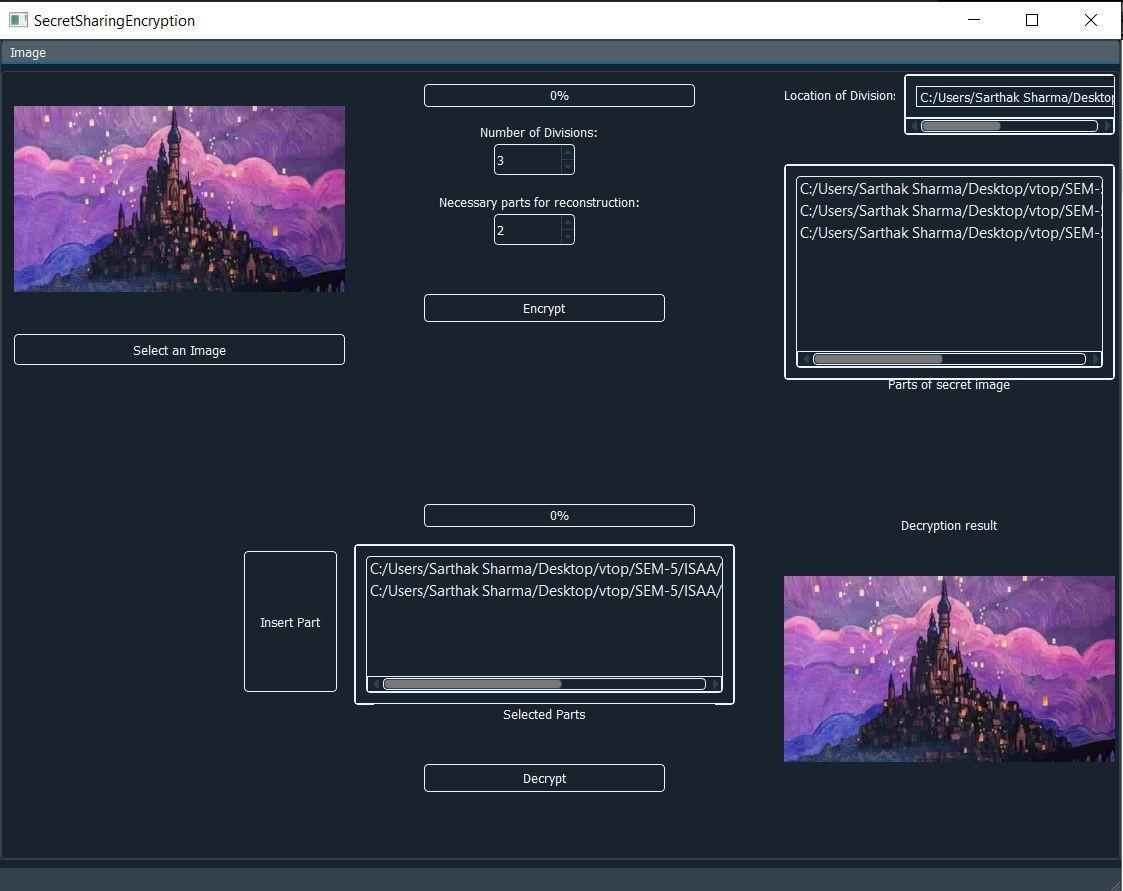
Generating 3 encrypted images using (2, 3) secret sharing scheme.



*Fig 2: Encryption Screen*



*Fig 3: Encryption image*



*Fig 4:Decryption Screen*

**CODE**

**Encryption**

def construct\_shares(self):

self.coefs.append(self.s)

values = np.polyval(self.coefs, [i for i in range(1, self.n + 1)]) % self.p

shares = {i: values[i - 1] for i in range(1, self.n + 1)}

return shares

def construct\_shares\_image(self):

self.coefs.append(self.s)

values = np.polyval(self.coefs, [i for i in range(1, self.n + 1)]) % self.p

shares = {}

for i in range(1, self.n + 1):

if int(values[i - 1]) != 256:

if int(values[i - 1]) == 0:

shares[self.n + 1] = 256

shares[i] = int(values[i - 1])

else:

shares[i] = 0

shares[self.n + 1] = 256

return shares

@staticmethod

def reconstruct\_secret(shares: dict, inputs: list, k, p):

if len(shares) < k:

raise Exception("More shares needed")

for el in inputs:

if el not in shares.values():

raise Exception("Inadequate share")

indeksi = []

for i in range(len(inputs)):

indeksi.append(int(list(shares.keys())[list(shares.values()).index(inputs[i])]))

lp = LagrangePolynomial(indeksi, [shares[ind] for ind in indeksi])

secret = lp.interpolate(0) % p

return secret

**Decryption**

def basis(self, x, i):

L = [(x - self.X[j]) / (self.X[i] - self.X[j]) for j in range(self.n) if j != i]

return np.prod(L, axis=0) \* self.Y[i]

def interpolate(self, x):

p = [self.basis(x, i) for i in range(self.n)]

return np.sum(p, axis=0)

def interpolate\_img(self, x):

p = [self.basis\_img(x, i) for i in range(self.n)]

return np.sum(p, axis=0)

def basis\_img(self, x, i):

L = []

temp = []

done = False

skip = 0

for k in range(len(self.X[i])):

if self.X[i][k] in self.temp:

skip += 1

for j in range(self.n):

if j != i:

cont = False

for k in range(len(self.X[i])):

k += skip

if k >= len(self.X[i]):

done = True

break

self.temp.append(self.X[i][k])

for m in range(len(self.X[j])):

try:

if self.X[j][m] in temp or self.X[j][m] == self.X[i][k]:

continue

calc = (x - self.X[j][m]) / (self.X[i][k] - self.X[j][m])

temp.append(self.X[j][m])

L.append(calc)

cont = True

if len(L) == self.n - 1:

done = True

break

except ZeroDivisionError:

continue

if done:

break

if cont:

break

if done:

break

if cont:

break

if done:

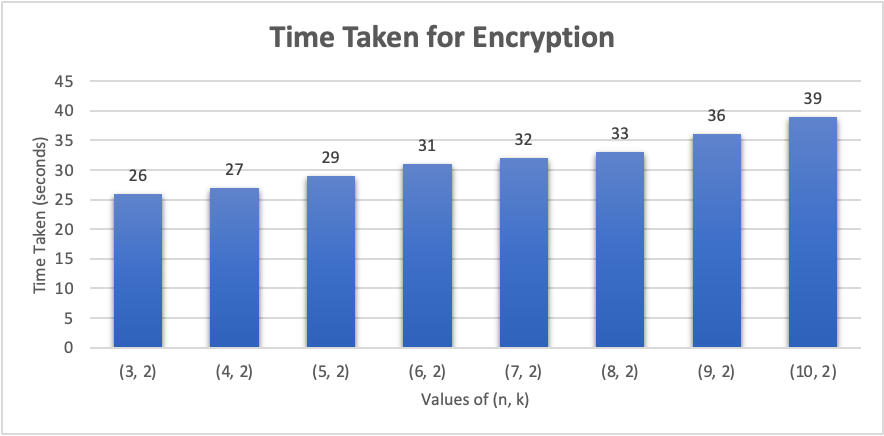
break

return np.prod(L, axis=0) \* self.Y[i]

**ANALYSIS & VISUALIZATION**

**Time Taken for Encryption**

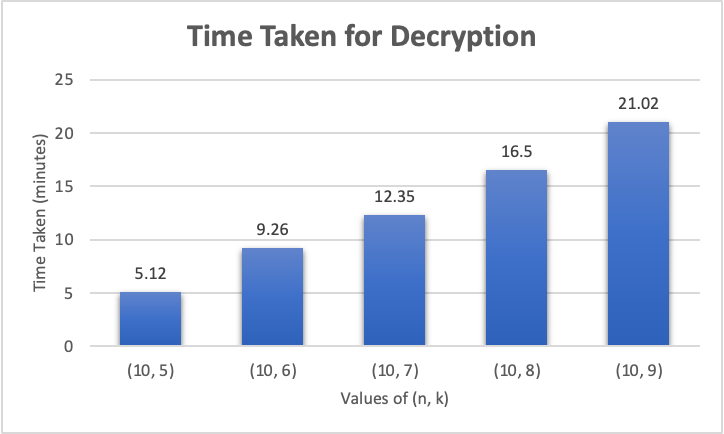
|  |  |
| --- | --- |
| **Values of (n, k);**  **k is constant** | **Time for Encryption (seconds)** |
| (3, 2) | 26 |
| (4, 2) | 27 |
| (5, 2) | 29 |
| (6, 2) | 31 |
| (7, 2) | 32 |
| (8, 2) | 33 |
| (9, 2) | 36 |
| (10, 2) | 39 |

****

*Fig 5:Graph 1 for encryption time taken*

**Time Taken for Decryption**

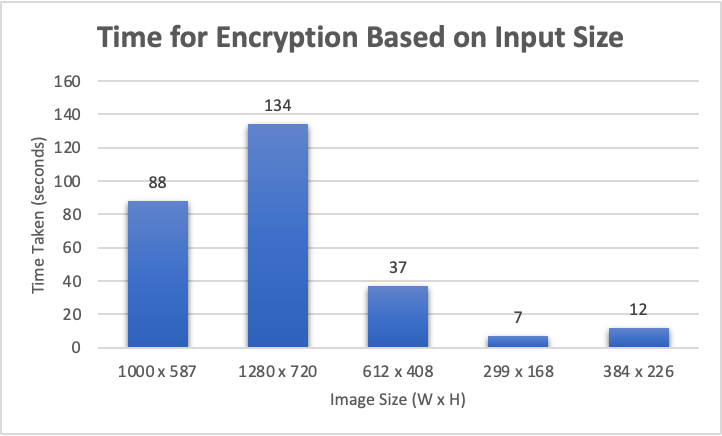
|  |  |
| --- | --- |
| **Values of (n, k);**  **n is constant** | **Time for Decryption (minutes)** |
| (10, 5) | 5.12 |
| (10, 6) | 9.26 |
| (10, 7) | 12.35 |
| (10, 8) | 16.5 |
| (10, 9) | 21.02 |

****

*Fig 6: Graph 2 for decryption time taken*

**Comparison Based on Input Size**

|  |  |
| --- | --- |
| **Image Size (W x H)** | **Time for Encryption (seconds)** |
| 1000 x 587 | 88 |
| 1280 x 720 | 134 |
| 612 x 408 | 37 |
| 299 x 168 | 7 |
| 384 x 226 | 12 |

****

*Fig 7: Graph 3 for time taken by encryption on the bases of input size*

**Comparison with Present Algorithms**

|  |  |
| --- | --- |
| **Types of Algorithm** | **Time Taken by Algorithm (seconds)** |
| AES (512 x 512) | 75 |
| RES (512 x 512) | 64 |
| DES (512 x 512) | 0.05 |
| Our Algorithm (512 x 512) | 42 |

*Fig 8:Graph 4 for the comparison between the present algorithm*

# 

# CONCLUSION AND FUTURE WORK

**Conclusion**

With traditional methods of image encryption such as AES, we need to use a key to decode the image. The problem with this approach is that even though the encryption method itself is robust, the ability of an attacker to gain access to the image due to a single point of failure (getting access to the private key) makes it an unsuitable choice for highly confidential data.

Our algorithm works for an equal number of k and n values which makes the efficiency a bit low, and for k = n = 3, it takes nearly 1-2 mins to give the output.

We thus conclude that the time taken with our approach is minimal for consecutive steps of n shares in the encryption process. However, the time taken for decryption is slightly more prominent than encryption. We see a more considerable rise in the time taken for decryption as compared to encryption.

Our algorithm bodes well compared to preexisting techniques in terms of time taken for encryption.

For future work, the decryption process can be made more efficient such that the time taken is significantly reduced. In addition, further work can be done comparing the size of the decrypted image with the original image and comparing results from different image formats.

Furthermore if we are able to include parallelism like openmp or mpi in python so furthermore the time taken for the whole process can be reduce.

# 

# REFERENCES

[1] Kalai Selvi, A., & Mohamed Sathik, M. (2010, September). Secret Sharing Scheme for Image Encryption Using new Transformation Matrix. In *International Conference on Advances in Information and Communication Technologies* (pp. 647-650). Springer, Berlin, Heidelberg.

[2] Shi, R., Zhong, H., Huang, L., & Luo, Y. (2008, May). A (t, n) secret sharing scheme for image encryption. In *2008 Congress on image and signal processing* (Vol. 3, pp. 3-6). IEEE.

[3] Vidhya, R., & Brindha, M. (2019). Polynomial Substitution Based Image Encryption Using Shamir Scheme. *International Journal of Computational Intelligence & IoT*, *2*(1).

[4] Mahalakshmi, J., & Kuppusamy, K. (2012). A New Technique for Image Encryption using RIJNDAEL Block Cipher Algorithms. *International journal of computer Applications*, *975*, 8887.

[5] Semenko, A., Kushnir, N., Bokla, N., & Kosovan, G. (2017). Creation of pseudo-random sequences based on chaos for forming of wideband signal. *Information and Telecommunication Sciences*, (2), 5-10.

[6] Azam, N. A. (2017). A novel fuzzy encryption technique based on multiple right translated AES gray S-boxes and phase embedding. *Security and Communication Networks*, *2017*.

[7] Mani, K., & Viswambari, M. (2017). Enhancing the Security in Cryptosystems Based on Magic Rectangle. *International Journal of Computer Network & Information Security*, *9*(4).

[8] Padate, R., & Patel, A. (2015). Image encryption and decryption using aes algorithm. *International Journal of Electronics and Communication Engineering & Technology*, 23-29.

[9] Anggraini, D., & Kazhimi, F. (2016, April). Encryption On Grayscale Image For Digital Image Confidentiality Using Shamir Secret Sharing Scheme. In *Journal of Physics: Conference Series* (Vol. 710, No. 1, p. 012034). IOP Publishing.

[10] Smitha, M., Jayanthi, V. E., & Merlin, A. (2013, July). Image encryption using separable reversible data hiding scheme. In *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

[11] Huang, Y. J., & Chang, J. D. (2013, February). Non-expanded visual cryptography scheme with authentication. In *2013 International Symposium on Next-Generation Electronics* (pp. 165-168). IEEE.

[12] Li, L., Abd El-Latif, A. A., & Niu, X. (2012). Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. *Signal Processing*, *92*(4), 1069-1078.

[13] GaneshKumar, K., & Arivazhagan, D. (2016). New Cryptography Algorithm with Fuzzy Logic for Effective Data Communication. *Indian Journal of Science and Technology*, *9*(48).

[14] Mousa, H. M. (2018). Chaotic Genetic-fuzzy Encryption Technique. *International Journal of Computer Network & Information Security*, *10*(4).

[15] Massoudi, A., Lefebvre, F., De Vleeschouwer, C., Macq, B., & Quisquater, J. J. (2008). Overview on selective encryption of image and video: challenges and perspectives. *Eurasip Journal on information security*, *2008*(1), 179290.

[16] Kovalchuk, A., Lotoshynska, N., Izonin, I., & Berezko, L. (2019). An approach towards an efficient encryption-decryption of grayscale and color images. *Procedia Computer Science*, *155*, 630-635.

[17] Prasetyo, H., Hsia, C. H., & Deng, J. Y. (2020). Multiple Secret Sharing with Simple Image Encryption. *Journal of Internet Technology*, *21*(2), 323-341.

[18] Kandar, S., & Dhara, B. C. (2011). Kn secret sharing visual cryptography scheme on color image using random sequence. *International Journal of Computer Applications*, *975*, 8887.

[19] Al Ebri, N., Baek, J., & Yeun, C. Y. (2011, December). Study on Secret Sharing Schemes (SSS) and their applications. In *2011 International Conference for Internet Technology and Secured Transactions* (pp. 40-45). IEEE.

[20] Bai, L., Biswas, S., Ortiz, A., & Dalessandro, D. (2006, July). An image secret sharing method. In *2006 9th International Conference on Information Fusion* (pp. 1-6). IEEE.

[21] MOHANTY, M. (2013). Secret sharing approach for securing cloud-based image processing.

[22] Massoudi, A., Lefebvre, F., De Vleeschouwer, C., Macq, B., & Quisquater, J. J. (2008). Overview on selective encryption of image and video: challenges and perspectives. *Eurasip Journal on information security*, *2008*(1), 179290.

[23] Akif, O. Z. (2012). Image encryption technique using Lagrange interpolation. *Image*, *25*(1).

[24] Liu, Y. X., Sun, Q. D., & Yang, C. N. (2018). (k, n) secret image sharing scheme capable of cheating detection. *EURASIP Journal on Wireless Communications and Networking*, *2018*(1), 1-6.

[25] Pan, H., Lei, Y., & Jian, C. (2018). Research on digital image encryption algorithm based on double logistic chaotic map. *EURASIP Journal on Image and Video Processing*, *2018*(1), 1-10.