Image processing Using Secret Sharing Schemes

[1]D. Boobala Muralitharan, [2]V. Krishna Kumar, [3]S. Akshay, [4]R. Akash kumar, [5]S. Arun kumar,

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Department of Computer Science and Engineering,
[1]Saranathan College of Engineering, Trichy, Tamil Nadu, India

Abstract: Secret Image Sharing allows a user to create the shared images from a secret image in such a way that an individual share does not reveal any information about the secret image, however when a specified number of shares are brought together, they can be used to reconstruct the secret image. Secret image sharing mechanisms have been widely applied to the military, ecommerce, and communications fields. This project aims to describe the design and development of a basic Secret Image Sharing System that is capable of efficiently generating shares and reconstructing the secret image from the shares. This system provides a framework which can be used as a powerful tool for Secret Image Sharing research. Efficient calculations of data make the framework an extremely powerful one. With the spread of the Internet, the speed of data spread is getting faster and faster. It benefits us a lot but also brings us many potential security problems, especially the problem of privacy leakage. For example, more and more people choose to store their private images in the cloud. Secret image sharing as a significant method has been widely applied in protecting images in the cloud, which reduces the risks of data leakage and data loss. Generally, the secret image sharing scheme would encrypt the secret image into a series of shares and then stored these shares in a cloud. However, when this cloud has been attacked, the secret may meet a risk of leakage. A solution to solve the problem is that the generated shares are distributed storage in multiple clouds. Each cloud is independent and all clouds can have a collaboration to manage the secret image

Keywords: **Secret image, Shamir's Algorithm Encryption Technique, Number of Shares, Cipher text**

I. INTRODUCTION

The effective and secure protection for important messages is a primary concern in commercial and military applications. Numerous techniques, such as image hiding and watermarking, were developed to increase the security ofthe secret. The secret image sharing approaches are useful for protecting sensitive information. The main idea of secret sharing is to transform an image into n shadow images that are transmitted and stored separately. The original image can be reconstructed only if the shadow images that participated in the revealing process from a qualified set. The (k; n)-threshold image sharing schemes were developed to avoid the single point failure. Hence the encoded content is corrupted during transmission. In these schemes, the original image can be revealed if k or more of these n shadow images are obtained. Moreover, the users who have complete knowledge of k-1 shares cannotobtain the original image. Blakley & Shamir independently proposed originalconcepts of secret sharing in 1979.

II. RELATED WORKS

The system uses whiteness to distinguish black colour from white colour. A black-and-white secret image is shared into noise-like shadows by subdividing a secret pixel into m (referred to as the pixel expansion) subpixels in each of n shadows. The shadow size is m times expanded, and thus the visual quality of a reconstructed image is degraded by this pixel expansion. Most research papers have been published to reduce the pixel expansion [5,6,7,8,9,10,11]. Some of them can even have no pixel expansion (m = 1) [5,7,10,11]. VCSs have noise-like shadows with black and white random dots, which are suspected to censors and difficult for identification and management. A VCS with meaningful shadow (oftenbeing a natural image) is referred to as extended VCS (EVCS). EVCS takes a secretimage and n original share images as inputs, and outputs n shares.

Multi secret sharing schemes can share many secret images at one time. There are many kinds of the multi secret sharing scheme using different methods. In, the paradigm of the multi secret sharing was given out by Padiya et al. and the genetic method was developed as a kind of encryption. Weir et al. proposed a scheme based on Visual Cryptography method, but the quality of the recovered secret images was very poor. Aarti et al. used the extended Visual Cryptography method and mixing method to realise multi secret sharing.

The proposed Conventional visual secret sharing scheme hides the secret image in shares, but at the time of hiding secret image in share it will arouse suspicion to hackers that there is some hidden image in shares. It will increase transmission risk problems. Natural image based visual secret sharing scheme is proposed to overcome the transmission risk problem. Natural image based visual secret sharing scheme reduces the transmission risk problem. In natural image based visual secret sharing scheme encryption and decryption algorithm is used. In the encryption process printed image and digital image is given as input along with the secret image

III. THEORETICAL FRAMEWORK

Existing System

The existing system is not automated and involves a lot of manual work to be done. Processing of various opportunities takes up considerable time and effort. Sharing of a secret image is a very tedious task. The existing system does not account for the security of these shares and they may be exploited by a hacker if they get access to the necessary number of shares Shamir developed the idea of a (k, n)-threshold based secret sharing technique (k ≤n). The technique allows a polynomial function of order (k -1) constructed using the polynomial function where the value of s0 is the secret and p is a prime number. No proper platform to utilise this amazing process. The polynomial function f(x) is destroyed after each shareholder possesses a pair of values (Xi, Yi) so that no single shareholder knows the secret value. Directly sharing shares can lead to share forgery. No information regarding hack attempt is known to anyone

Proposed System

We take the generated shares and then get a key as an input for encryption for the shares The shares are then converted from image to cipher text upon applying AES encryption. The cipher texts are then combined together to one single file and then encrypted once again to make it fool proof. The cipher text is digitally signed using JSON-web-token and shared to the receiver with a private key. JSON-web-token can be verified by the receiver and fetch back the cipher text back and by applying AES decryption the shares can be obtained, minimum shares once obtained can be combined to obtain the input image.

We hence obtain a system which has the following characteristics:

- Highly Secured system
- AES encryption and decryption shows huge impact on security aspects
- JSON-web-token is added security
- Cipher text uses less storage than images

IV. IMPLEMENTATION

The first step in the process is to enter the inputs namely number of shares,minimum number of shares and the image into the system. Then we create an empty numpy array with length, breadth of the image. Upon creating this array, we then take a random polynomial and then use the Red, Green, Blue component of the pixel of the original image as the secret.

For any n distinct point over $\mathbb{R}^2$, there is a unique polynomial $P(x) \in \mathbb{R}[x]$ of degree $n - 1$ which goes through all of them. This also means that if we have a polynomial of degree $n - 1$, we can take n points (or more) from it, and we will be able to recover the original polynomial from those n points.

We can see this starting with a line. If we are given any two points $p_0 = (x_0, y_0)$ and $p_0 = (x_1, y_1)$ from that line, we are able to recover the original line.

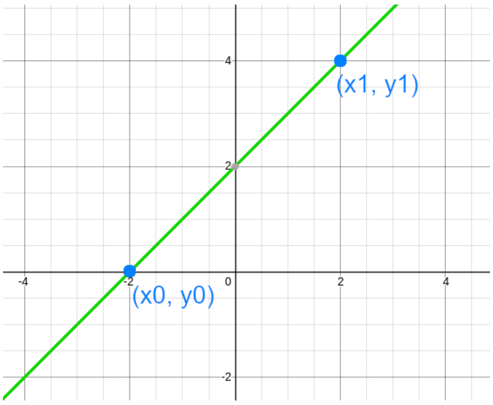

Fig 1 Plotting line using 2 points

We can map this into the previous idea, seeing that our line is a degree 1 polynomial, so, if we pick 2 points from it, we later can recover the original line.

Same happens with polynomials of degree 2. Let p(x) be a polynomial of degree 2 defined by p(x)= x^2 - 5x - 6 . We can create infinity of polynomials of degree 2 that go through 2 points, but with 3 points there is a unique polynomial degree 2 As the degree is 2, if we pick 3 points from the polynomial, we will be able to reconstruct it.

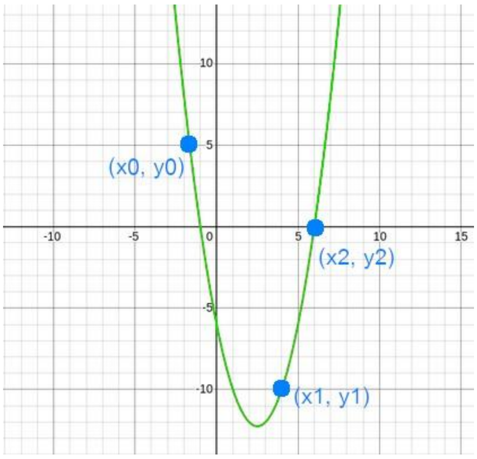

Fig 2 Plotting a Curve using 3 points

Let out secret be s = 14. We now generate out polynomial of degree n – 1 = 2, where s will be the constant coefficient: $P(x) = s + \alpha_1 x^1 + \alpha_2 x^2$. The and can be set as any random value, for example as $\alpha_1 = 4$ and $\alpha_2 = 6$ respectively. So, our polynomial will be $p(x) = 14 + 4x + 6x^2$

We can take *k* points from it using the incremental indexes for the coordinate: $p_1 = (1, p(1)), p_2 = (2, p(2)) \dots\ p_k = (k, p(k))$

$p(x) = 14 + 4x + 6x^2$
$p(1) = 14 + 4 \cdot 1 + 6 \cdot 1^2 = 24\ (mod\ 19) = 5$
$p(2) = 14 + 4 \cdot 2 + 6 \cdot 2^2 = 46\ (mod\ 19) = 8$
$p(3) = 14 + 4 \cdot 3 + 6 \cdot 3^2 = 80\ (mod\ 19) = 4$
$p(4) = 14 + 4 \cdot 4 + 6 \cdot 4^2 = 126\ (mod\ 19) = 12$
$p(5) = 14 + 4 \cdot 5 + 6 \cdot 5^2 = 184\ (mod\ 19) = 13$

So, our k points are (1,5), (2,8), (3,4), (4,12), (5,13). We can distribute these points as our secret parts. In order to recover the secret, we need at least *n* = 3 points, for example P_1, P_3, P_5 and we compute the Lagrange polynomial interpolation to recover the original polynomial over the $\mathbb{F}_{19}$

$$I(x) = \sum_{i=0}^{n} y_i l_i(x)\ where\ l_i(x) = \prod_{0<j<nj\neq i} \frac{x - x_j}{x_i - x_j}$$

$$l_1 = \frac{x-3}{1-3} \cdot \frac{x-5}{1-5} = \frac{x-3}{17} \cdot \frac{x-15}{15} = \frac{x^2 + 11x + 15}{8}$$

$$l_3 = \frac{x-1}{3-1} \cdot \frac{x-5}{3-5} = \frac{x-1}{2} \cdot \frac{x-5}{17} = \frac{x^2 + 13x + 5}{15}$$

$$l_5 = \frac{x-1}{5-1} \cdot \frac{x-3}{5-3} = \frac{x-1}{4} \cdot \frac{x-3}{2} = \frac{x^2 + 15x + 3}{8}$$

$$I(x) = y_2 l_2(x) +\ y_4 l_4(x) +\ y_5 l_5(x)$$

$$= 5 \cdot \left(\frac{x^2 + 11x + 15}{8}\right) + 4 \cdot \left(\frac{x^2 + 13x + 5}{15}\right) + 13 \cdot \left(\frac{x^2 + 15x + 3}{8}\right)$$

$$= \frac{5x^2 + 17x + 18}{8} + \frac{4x^2 + 14x + 1}{15} + \frac{13x^2 + 5x + 1}{8}$$

$$= 3x^2 + 14x + 7 +\ 18x^2 + 6x + 14 +\ 4x^2 + 3x + 12$$

$$= 6x^2 + 4x + 14$$

We can now take the constant coefficient, or just evaluate the obtained polynomial at 0, $P(0) = 6 \cdot 0^2 \rightarrow 4 \cdot 0 + 14$, and we obtain our original secret s = 14

After getting the value for each pixel by using the Red, Green and Blue component of the pixel as the secret value we then convert the list into an image. This image is then encoded using base64 format and then an AES encryption algorithm is applied on this image. The resultant cipher texts are then combined together to form a ciphertext which is again encrypted using AES encryptionalgorithm

The keys used in the algorithm are then digitally signed using a JWT token and then given to the user for future use.

In the Decryption side, the user gives the input - the cipher text file and the key fileto the system. The cipher text is decrypted to get the base64 encoded data which is then decoded to form the shares.

The original image is then reconstructed back from the shares and given as the output to the user.

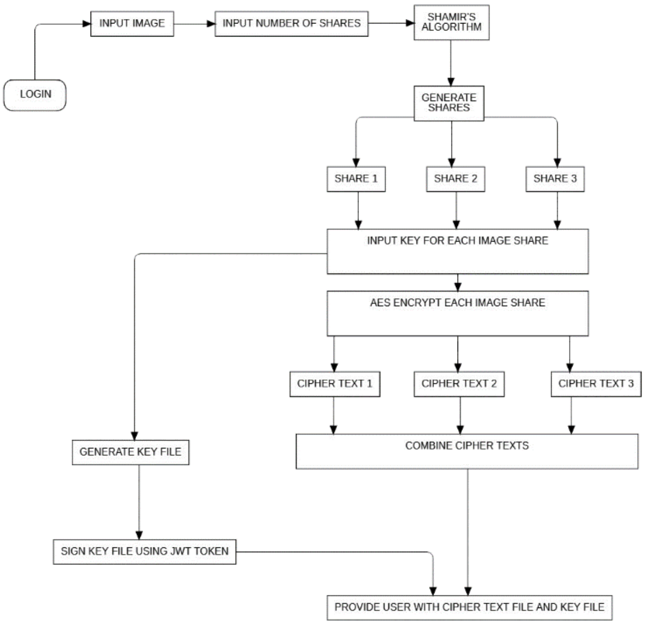

Fig 3 The Architecture Diagram for Encryption

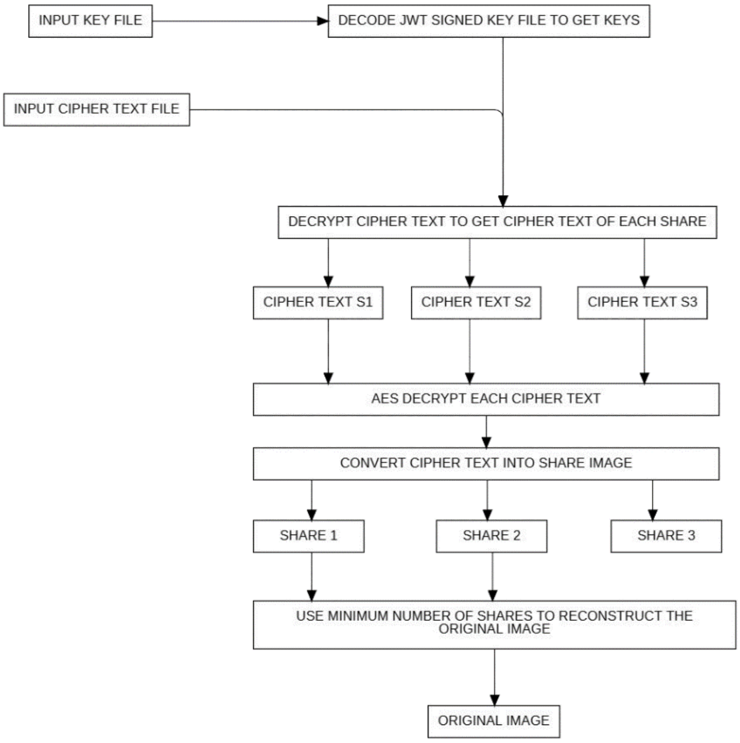
INPUT KEY FILE
DECODE JWT SIGNED KEY FILE TO GET KEYS
INPUT CIPHER TEXT FILE
DECRYPT CIPHER TEXT TO GET CIPHER TEXT OF EACH SHARE
CIPHER TEXT S1
CIPHER TEXT S2
CIPHER TEXT S3
AES DECRYPT EACH CIPHER TEXT
CONVERT CIPHER TEXT INTO SHARE IMAGE
SHARE 1
SHARE 2
SHARE 3
USE MINIMUM NUMBER OF SHARES TO RECONSTRUCT THE ORIGINAL IMAGE
ORIGINAL IMAGE

Fig 4 The Architecture Diagram for Decryption

V. CONCLUSION

In this project, an approach is proposed to share images using secret sharing schemes in security domains. Splitting images as per user input and minimum required parts for generating real images. Converting each split by encrypting and producing ciphertext and private key. Fetching the output by decrypting cipher text. All these working advantages ensure that the application is widely usable and makes it a reliable alternative for existing image sharing.

The result shows that the system is significantly better than the existing systems with respect to both reliability and ease of use and security. In future it can be hosted on a public server and then be made useful for public use and also a standalone portable desktop application can be done which is useful to ensure more data privacy. With the increased use of mobile and mobile apps, to cover the market share of the mobile users would be more fruitful. In case of any vulnerability discovery, the maintenance is easy and shall be followed if put into practical use

VI. REFERENCES

1. P. Li, X. Su and P. Ma, "Image Secret Sharing and Hiding with Authentication," in Pervasive Computing, Signal Processing and Applications,International Conference on, Harbin, China, 2010
2. R. He, S. Liu, L. Liu, W. Geng and D. Tang, "Image Secret Sharing Based onMDS Code," in 2020 International Conference on Big Data & Artificial Intelligence & Software Engineering (ICBASE), Bangkok, Thailand, 2020
3. L. Huang, R. Shi, Y. Luo and H. Zhong, "A (t, n) Secret Sharing Scheme forImage Encryption," in Image and Signal Processing, Congress on, null, 2008
4. C. Yang and T. Chen, "An Image Secret Sharing Scheme with the Capability of Previewing the Secret Image," in 2007 International Conference on Multimedia & Expo, Beijing, 2007
5. B. Chen, W. Lu, J. Huang, J. Weng and Y. Zhou, "Secret Sharing Based Reversible Data Hiding in Encrypted Images with Multiple Data-Hiders" in IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 02,