Secret sharing & Visual Cryptography

Raj Dharmendra

What is the shamir Secret Sharing Scheme:-

In cryptography, a **secret sharing scheme** is a method for distributing a secret amongst a group of participants, each of which is allocated a *share* of the secret. The secret can only be reconstructed when a certain number of shares(Threshold scheme) are combined together; individual shares are of no use on their own.

For distributing shares among the participants, We use a polynomial function of N-1 degree(N= number of participants). We assign a point in 2-D plane(x-y coordinate) each point represent a participant who has share.

For obtaining our secret back we used lagrange interpolation (wiki-link) function.

Mathematical Modeling Of Secret Sharing:-

Actually Shamir secret sharing scheme work on a mathematical polynomial function
Let's start from very beginning:

Suppose we have a secret(secret maybe anything like a password that we want share, or any information), Let's take it in another way, we have a share bank locker account mean more than two people share this locker and an individual locker can not open this account. To open this account we need minimum number of lockers holder.
Shamir scheme work in this ways exactly.
Let's understand this by taking bank locker example. In a bank there is a shared locker and 5 people shared this locker. And bank issue a password for this locker but not given the password direct to any locker holders. Rather bank gave them another number and told them that if minimum 3 locker holder together can open the lock but less than 3 they can not open a lock.
Means after combining 3 locker holders number then the original password will generated.

For encrypting the password, bank use a mathematical formula.
Let's bank decide that this locker can be share between 5 people and to open this locker minimum 3 people will require.
N=5 // total number of locker holders
K=3 // minimum number of locker holder require to open the locker.
(N,K)= this is called Threshold scheme

Now bank splits this password into 5 parts in different numbers and give each part to each locker holder by using a polynomial function.
The degree of the polynomial function will be decided on the base of minimum locker holder to open. If minimum locker holder to open the locker is K then degree of a polynomial will be K-1.
So in this example we will use 2 degree polynomial function because here K=3.

Secret=S

Y=$F(x) = a1x + a2x^2$ +S   this is the polynomial function degree 2 and we are going to split our secret in the form of this polynomial.
So we want to share this secret in the form of 5 locker holders so we will evaluate this function for 5 times.
Like x=1, x=2, x=3, x=4, x=5
For each corresponding value of x there will be a value of Y.
Locker1Holder = Y1, Locker2Holder=Y2, Locker3Holder=Y3, Locker4Holder=Y4, Locker5Holder=Y5.
So with the help of this polynomial function we split our secret(S) into 5 locker holder.

And the condition for getting secret back is we need at least 3 locker holders value.

Pseudo-Code for Encryption:

Step 1: define the degree of polynomial(K-1) and generate the random values for the polynomial coefficients(a1, a2, … ak-1)

```
Step2: Now run a loop for N time(total number of locker holder)
    i=1;
    while(i<=N)
        Do:
            For every value of x get a corresponding value of Y.
            Y=$F(x) = a1x + a2x^2$ +S
```

Step 3: Give the value of each Y to each locker holder

For Decryption the original password(secret) we use the lagrangian function:
We takes any 3 locker holders value(Minimum locker holder need) and by using lagrangian function we get a polynomial and the constant term in this polynomial will be our password(secret)

Pseudo-code for Decryption:

Lets we take(x1,y1), (x2,y2), (x3,y3) locker holders value.

Now find the a polynomial for each locker holders.

$$L1(x1) = x - x2/x1 - x2 \ * \ x - x3/x1 - x3$$

$$L2(x2) = x - x1/x2 - x1 \ * \ x - x3/x2 - x3$$

$$L3(x3) = x - x2/x3 - x2 \ * \ x - x1/x3 - x1$$

Now get a single polynomial function after combining these all polynomial functions

$$Y \ = f(x) = \sum_{j=1}^{k} \ yj.Lj(xj)$$

This is the our final polynomial and the Constant term in this polynomial will be our password(Secret).

What is Visual Cryptography:-

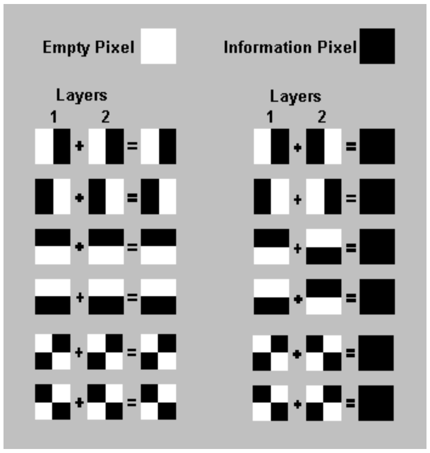
Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

How Visual Cryptography works:-

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks.

In the table on the blow we can see that a pixel, divided into four parts, can have six different states.If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black.



Source- google

The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.
If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

Advantage and disadvantage of this technique:-

1. A key exchange protocol enables parties to share a common key for encrypting a large amount of data.
2. Authentication is an essential requirement prior to the key exchange process in order to prevent man-in-the-middle attack.
3. Mostly use in cryptography algorithms

References:

1. Link1

2 Link2