DEFENSE SYSTEM DATA ENCODING USING VISUAL CRYPTOGRAPHY

***Project Reference No.:** 45S_BE_3656*

***College** : Bangalore Institute of Technology, Bengaluru*
***Branch** : Department of Information Science and Engineering*
***Guide(s)** : Mrs. S Mercy*
***Student(S)** : Mr. Pramod N*
Mr. Nikhil R Samak
Ms. Prakul Rastogi
Mr. Kumar Ayush

Introduction:

In any army a decision is not directly taken by just one commander or leader but rather that same decision is taken only after discussing about that issue and a majority agrees upon it. This had become the base idea of our paper. In this paper, the idea was to secretly transmit a secret image which can possible be any kind of important map or as such to the main people in the army and the original image can be formed only when the required number of people agree to that plan. This is done by the concept called "Visual Cryptography". Visual Cryptography deals with images. Visual cryptography is a technique which allows visual information such as images, videos etc. to be encrypted in such a way that the decrypted information appears as a visual image .In this paper we implement visual cryptography on black and white images and color images (RGB) using "(k, n) secret image sharing algorithm" .This scheme is perfectly secure and very easy to implement. We extend this algorithm in such a way that the secret image is divided into n shares and each share is sent to n different officers and only when at least k officers (k<=n) agree to see the secret and when they combine their individual share, the secret is revealed.

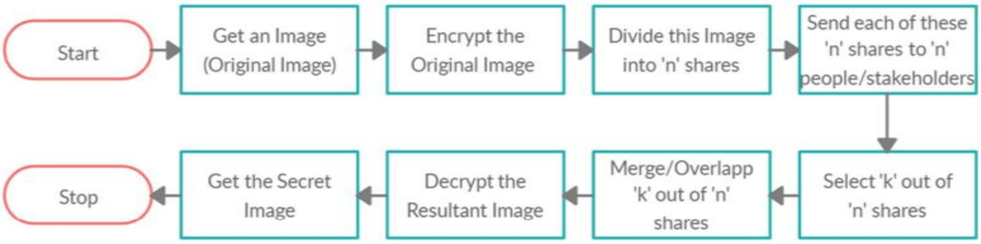
Objectives:

1. The main objective of the project is to develop a secure data sharing system which can be used effectively in the field of defense.
2. All this is achieved by using various encryption decryption algorithms along with k - n sharing scheme.
3. A higher level of security is also achieved with the help of keys used for encryption
4. E.g. If a higher military officer wants to send a photo to his juniors then first he/she encrypts the photo using basic ciphers.
5. Then in the second step uses more complex ciphers finally sends the data to n juniors using k n sharing scheme.

Methodology:

The approach has the following steps:

1. An image that is to be secretly transmitted should be selected.
2. This selected image will then be encrypted,
   2.1 First by using Caesar cipher wherein we make use of a key and compute a value. Then we add this value to all the pixels and mod it by 256.
   2.2 Then we use RSA encryption wherein we compute a pair of public and private keys. Now with this public key, we encrypt all the pixel values using RSA.
3. Then we split this encrypted image into ‘n’ shares using (k, n) secret sharing encryption algorithm.
4. Then we send each share to each individual person via mails.
5. Now, at least ‘k’ of ‘n’ shares are selected for merging.
6. Once the shares are selected, then we overlap and combine these shares using (k, n) secret sharing decryption algorithm.
7. Once we got the merged image, then it is time to carefully decrypt the merged image.
   7.1 The decryption starts by decrypting using RSA. The private key that we generated earlier is used for RSA decryption.
   7.2 Next, we make use of the key (that we earlier used for Caesar Cipher encryption) for decrypting using Caesar Cipher.


Start
Get an Image (Original Image)
Encrypt the Original Image
Divide this Image into 'n' shares
Send each of these 'n' shares to 'n' people/stakeholders
Select 'k' out of 'n' shares
Merge/Overlapp 'k' out of 'n' shares
Decrypt the Resultant Image
Get the Secret Image
Stop

The flow of the system architecture goes like this:

A secret image is selected so that it can be transmitted securely. That image is then encrypted first by using a private key or symmetric key encryption technique (Caesar Cipher) and then by a public key or asymmetric key encryption technique (RSA). Now this resultant image is then divided into ‘n’ shares by using k-n secret sharing algorithm by using a random number generator and also by using a reconstruction factor (n-k+1). Now each of these ‘n’ shares is sent to each of ‘n’ different people/shareholders via mails by the admin. Now, to reconstruct the original image, at least ‘k’ out of the shareholders has to agree to combine their shares. Now, since they have agreed to combine their shares, each of these shareholders (at least ‘k’ people) will have to send back their shares to the admin. Admin on getting the shares back, will combine the shares. Now, the admin has a resultant image which he/she will have to decrypt. In the decryption phase, the resultant image is first decrypted w.r.t RSA decryption algorithm and then by Caesar Cipher decryption algorithm with the proper keys. If all the conditions of minimum number of shares required and the use of correct keys are satisfied, the admin will have the secret image by now. Now, the secret image can be seen by the shareholders who have agreed to merge their shares directly at the admin’s system.

Conclusion:

Sharing data secretly, especially in the domain of army is very important. That data that is being transmitted is very sensitive. So, it is very important to transmit data by providing security to it. This idea not only makes it difficult for intruders to steal the data but also makes it nearly impossible as we encrypt the data before dividing into shares. Encryption provides extra security for the data in addition to that data being divided into shares. Now even if the intruder has required number of shares, he won't be able to get the original image as it is as he doesn't know the values of the key. What makes this algorithm good is that, the intruder has to get all the required number of shares at the first place and this is tough. What is tougher is that even if he has the required number of shares, he should have the key values as well. So, it's better if the value of 'k' to be closer to the value of 'n' and also have a good set of keys for encryption.

Scope for future work:

This proposed method has a compulsion that there should be only one admin and the each shareholder has to take the shares from and has to bring back the shares to that only admin. It is that person who initially takes the image to be shared secretly, encrypt the image, divide into 'n' shares, send mails, combine the accepted shares, decrypt the image, get back the secret image and maintain all the files related to that image. It can be further extended in such a way that encryption, division into 'n' shares and mailing those shares be done at one end taken care by one admin and combining 'k' shares and decryption be done at another end taken care by another admin. This makes this algorithm more feasible and robust to use and work with. Also, with the changing technologies, newer and stronger encryption algorithms can replace the ones that are used in this proposed algorithm. This same idea can be used in other fields as well like in providing authentication in Photography Contests, Online Voting Systems using Visual Cryptography, in Copyright authentication etc.