International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 05 Issue: 10 | Oct - 2021 ISSN: 2582-3930

Novel Approach to transmit a secret image using Visual Cryptography

Tydi Santi Swaroop[1], Vasantha murali Krishna[2]

[1] Student, Department of CSE- Avanthi Institute of Engineering and Technology Visakhapatnam
[2] Assistant Professor, Department of CSE- Avanthi Institute of Engineering and Technology Visakhapatnam

---

Abstract - In any defence authority, developer taken 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 project.
In the 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.

Key Words: Visual Cryptography, secret image sharing, Cryptography, Steganography

1.INTRODUCTION

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

Visual cryptography is the method of hiding images or documents by shadowing the original image into specific shares which are visually not recoverable. These shares when superimposed on one another would give away the concealed image which can be visually decrypted without further computation.

Naor and Shamir first introduced this cryptographic paradigm for black and white images in the year 1994.

2. Secret Sharing

In the present work is based on latest surveyed papers.

According secret sharing method contains:

1. Image is made into 'n' shares.
2. Each share is individually useless.
3. Image will be obtained only if at least 'k' shares are stacked on each other where $k \leq n$.
4. Even if there are (k-1) shares put together, the image wouldn't be formed.
5. If all the 'n' shares are put together, the image can be retrieved clearly.

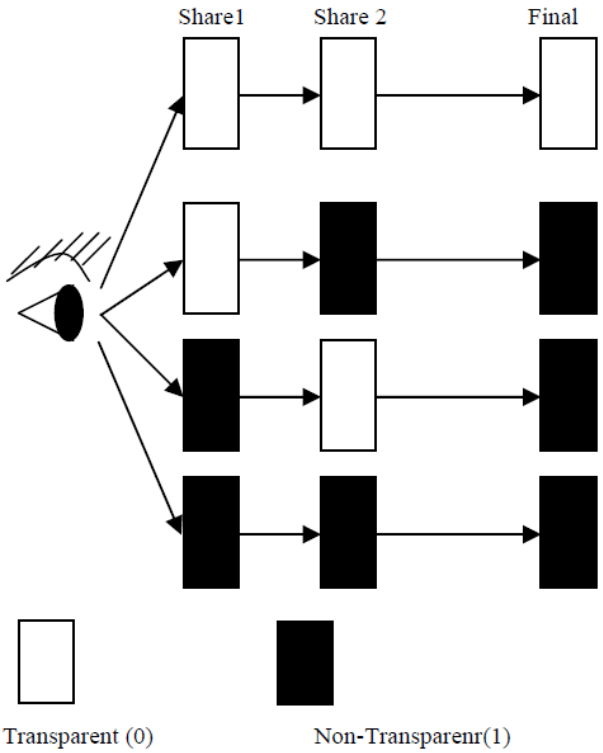


Fig 1: WORKING MODEL OF HUMAN VISUAL SYSTEM

3. RELATED WORK

Suppose we have to send a very highly confidential image data to army officers deployed near battle field, we split the image into 'n' shares and makes it compulsory for at least 'k' shares to be merged to get the original image.
Even if (k-1) agree to merge their shares, we would not be able to retrieve the original image.
We achieve this by using the concept called "VISUAL CRYPTOGRAPHY".

4. EXISTING WORK

Started by Naor and Shamir where they proposed the idea of k out of n secret sharing algorithm.

This model assumes that the secret message is a collection of black and white pixels and each pixel is handled separately.

Each original pixel can appear in 'n' modified versions called shares.

Each pixel in original image is represented by a collection both while and black sub pixels, which are printed close to each other on transparencies. This model only works for black and white images.

Later, this process was implemented by two-out-of-two secret sharing scheme where the secret image was divided into only 2 shares, and we need both of them to reconstruct the original image.

This same scheme was used to get a new color by making use of 2 different colors (the resultant color is not same as either of the 2 colors that are stacked one over the other).

5. PROPOSED WORK

Our proposed system will be having the following main modules.

Get the original image and encrypt the original image.

Split/divide this encrypted image into 'n' shares.

Send (via mail) each share to each of 'n' people/shareholders.

Collect at least 'k' shares from those 'n' people/shareholders ($k \leq n$) and merge all of them.

Decrypt the resultant image by making use of right keys.

5.1 SYTEM ARCHITECTURE

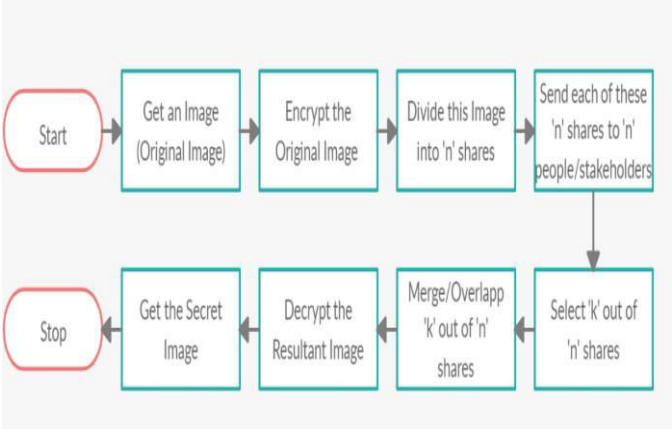


FIG 2: SYSTEM ARCHITECTURE

5.2 Module 1

At first, an image that is to be transmitted as a secret has to be selected. From there on these are the modules that are being proposed.

1. Caesar Cipher.
   The Caesar Cipher technique is one of the earliest and simplest method of encryption technique.
   In this project, the key is calculated by adding all the ASCII values of the key(text) that is entered. We get a value here which is added to each of R, G, B values of every pixel and then mod it with 256 since a value in each pixel would be in the range of 0, 1, ….., 255. By now we will have an image that is encrypted by Caesar Cipher. Since this algorithm is easy to crack, we make use of RSA as well.
   The formula used to encrypt is
   $$c(x)=(I(x) + key) \bmod 256$$
   Where,
   C is encrypted Image and I is the original Image,
   X is a specific pixel,
   Key is the sum of all ASCII values of each character in the key that is entered.
2. RSA

   RSA is algorithm used by modern computers to encrypt and decrypt messages. RSA stands for Ron Rivest , Adi Shamir and Leonard Adleman , who first publicly described it in 1978.
   The keys for the RSA algorithm are generated the following way: -
   1) Choose two distinctive prime numbers p and q
   2) Compute n = p * q
   3) Compute $\Phi(n) = \Phi(p) * \Phi(q) = (p - 1) * (q - 1) = n - (p + q - 1)$ where, $\Phi(n)$ is Euler's totient function.
   4) Choose an integer e such that, $1<e<\Phi(n)$ and $\gcd(e, \Phi(n))=1$ that is e and $\Phi(n)$ are coprime.
   5) Determine d as $d= e^{-1} \pmod{\Phi(n)}$ i.e., d is the multiplicative inverse of e(modulo $\Phi(n)$)
   The Formula used to encrypt is :
   $$c=m^e \pmod n$$

5.3 MODULE 2

DIVIDING INTO N SHARES:

Step: I: Take an image as input and calculate its width (w) and height (h).
Step II: Take the number of shares (n) and minimum number of shares (k) to be taken to reconstruct the image. k must be less than or equal to n.
Step III: Calculate recons=(n-k)+1.
Step IV: Create a three dimensional array img_share[n][w*h][32] to store the pixels of n number of shares
Step V:

```
for i=0 to (w*h-1)
 {
  Scan each pixel value of the image and convert it into
      24 bit binary string let PIX.
     for j=0 to 23
       {
    if ith position of PIX contains '1'
       call Random_Place(n, recons) for k=0 to (recons-1)
  {
```

```
        Set img_share[rand[k]][i][j] = 1
      }
    }
  }
```

Step VI: Create a one dimensional array img_cons[n] to store constructed pixels of each share.

Step VII: for k1=0 to(n-1)

```
 {
  for k2=0 to (w*h-1)
   {
 String value= " "
    for k3=0 to 23
     {
       value=value+img_share[k1][k2][k3]
     }
```

construct alpha, red, green and blue part of each pixel by taking consecutive 8 bit substring starting from 0.

Construct pixel from these part and store it into img_cons[k1].

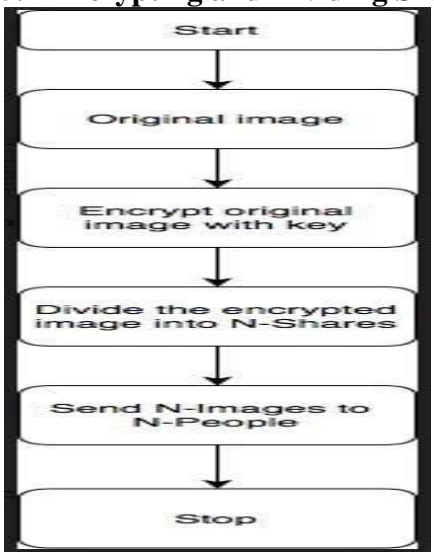
```
   }
  generate image from img_cons[k1].
 }

subroutine int Random_Place(n,recons)
 {
```

create an array rand[recons] to store the random number generated.

```
   for i=0 to (recons-1)
    {
      generate a random number within n, let rand_int.2
      if(rand_int is not in rand[recons])
        rand[i] = rand_int.
    }
   return rand[recons]
 }
```

5.4 Encrypting and Dividing Shares:

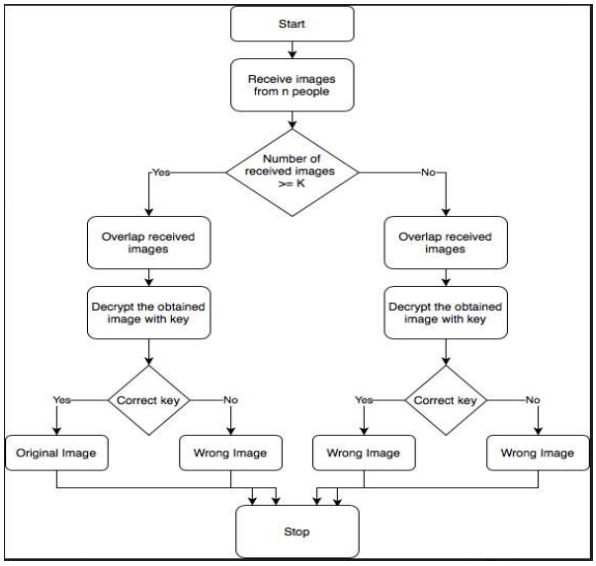


5.4 MODULE-3: SENDING 'n' SHARES TO 'n' DIFFERENT PEOPLE

Emails are sent to user's emails provided by admin. Here each user would be an army officer who are required to make a decision. The number of emails is equal to number of shares created at the first place. Now, each user will get a share of the secret image.

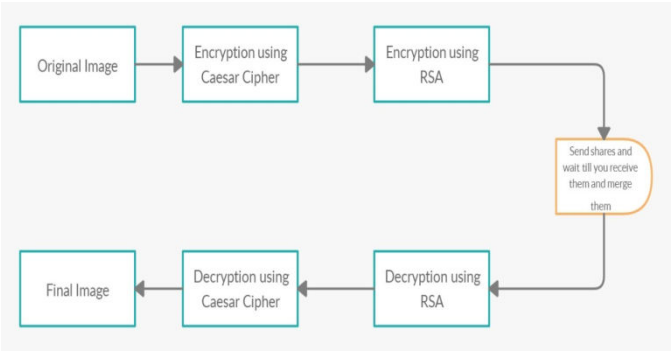
E-mails are sent directly by a python code by making use of the modules smtplib, MIMEMultipart, MIMEText, MIMEBase and by entering the e-mail ids of each shareholder after those shares are generated.

5.5 MERGING 'k' SHARES AND DECRYPTION



The heading should be treated as a 3rd level heading and should not be assigned a number.

5.6 ORDER IN WHICH ENCRYPTION AND DECRYPTION TO BE DONE



5.7 Experimental Results:

1) Overlapping K-Shares: O(K*row*column*3)

File Name	Resolution (w*h)	Encryption Time (in sec)	Decryption Time (in sec)
anits.png	200*200	0.2362	0.3569
download.jpg	225*225	0.2951	0.4969
Flower.jpg	159*119	0.1234	0.1837
god.png	450*450	1.1775	2.1045
human.jpg	208*243	0.2957	0.4895
map.jpg	300*168	0.3117	0.4938
mona.png	256*256	0.4669	0.6476
tulip.png	173*292	0.2989	0.4882

Table-1: RSA Encryption and Decryption times for images with different resolutions.

Table 1:RSA Encryption and Decryption

File Name	Resolution (w*h)	Encryption Time (in sec)	Decryption Time (in sec)
anits.png	200*200	0.1333	0.0980
download.jpg	225*225	0.1310	0.1270
Flower.jpg	159*119	0.0474	0.0677
god.png	450*450	0.6036	0.5164
human.jpg	208*243	0.1475	0.1214
map.jpg	300*168	0.1162	0.1286
mona.png	256*256	0.1364	0.1672
tulip.png	173*292	0.1157	0.1402

Table-2: Caesar Cipher Encryption and Decryption times for images with different resolutions.

Table 2: Caesar Cipher Encryption and Decryption

5.7 Results:

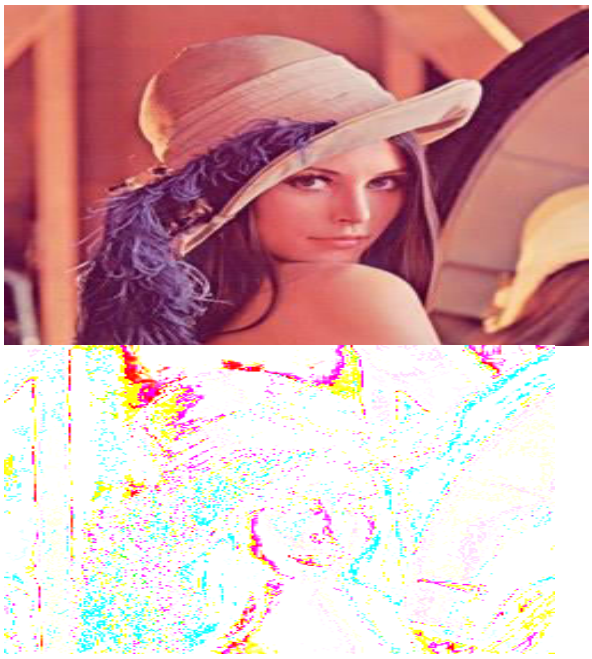


Fig 3: Input to the process and After Encryption

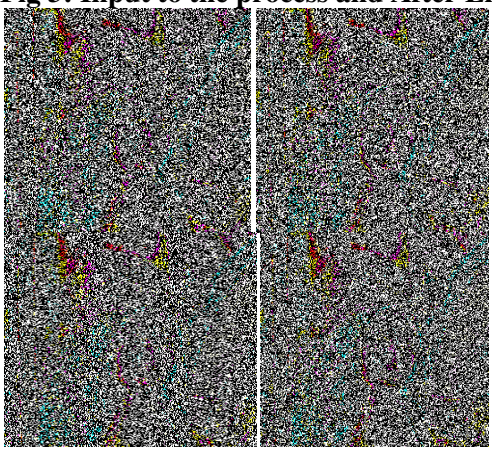


Fig 4: Four Shares

Fig 5: (AFTER MERGING k SHARES AND BEFORE DECRYPTION)

6. 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.

REFERENCES

1. Adi Shamir "Communications of the ACM: How to Share a Secret" Volume 22, Issue 11 Nov. 1979.
2. Moni Naor, Adi Shamir "Visual Cryptography" (The preliminary version of this paper appeared in Eurocrypt 94).
3. Shyamalendu Kandar, Arnab Maiti "K-N SECRET SHARING VISUAL CRYPTOGRAPHY SCHEME FOR COLOR IMAGE USING RANDOM NUMBER" International Journal of Engineering Science and Technology (IJEST).
4. J. Sharmila, Jagadish Gurrala "A Novel Approach on Secure Data Transfer for General Transactions using Secret Sharing Scheme" International Journal of Computer Applications (0975 – 8887) Volume 172 – No.8, August 2017.

BIOGRAPHIES

I am V.Murali completed B.Tech in ANITS College in 2006. I completed M.Tech - Computer science in Andhra university in 2009. I am Current working as a Assistant professor –CSE in Avanthi Engineering College, Visakhapatnam. He published many research papers in top journals like UGC,SCOPUS.

This is Swaroop, completed B.Tech in computer science and engineering. Current pursuing M.Tech –CSE in Avanthi Engineering College, Visakhapatnam.