Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 3, March 2016, pg.776 – 781

Visual Cryptography: An Efficient Technology for Securing Data

Dipawali Gabhane[1], Sanchiti Gupta[2], Renuka Rajgure[3], Pinki Verma[4], Dipika Mande[5], Shaikh Phiroj[6]

[1,2,3,4,5]Student, Computer Technology & RTMNU, India

[6]Asst. Prof., Dept. Of Computer Technology, PCE, Nagpur, India

[1]mailtogabhane@gmail.com; [2] sg171093@gmail.com; [3] steffyrajgure@gmail.com
[4] pinki.verma17.pv@gmail.com; [5] dipikamande48@gmail.com, [6] sheikh.feroz@gmail.com

Abstract—Visual cryptography is a cryptographic technique which allows visual information i.e. picture or text to be encrypted in such a way that decryption becomes a job of the person to decrypt via sight reading. There are various techniques has been established for visual cryptography. In this research the image can be sliced first and then encrypted by using the encrypted factor. To decrypt an image the user wants the correct encryption factor. By using this technique colour image also convert into gray scale image.

Keywords— Visual cryptography, Extended visual cryptography, Gray scale, Encryption factor, Decryption, Data Security.

I. INTRODUCTION

Visual cryptography is the concept in which an image can decrypt without using any algorithm. No need of any image decryption algorithm for seeing an image to the client side. The Visual Cryptography concept comes under the Data security. When an user wants to send the secret data to an another person securely, then various methods can apply for securing that data such as Caesar cipher, playfair etc. Just like that, the user wants to send any secret image securely, then the concept was arises that is called as "Securing data by using Visual Cryptography".

The Gray scale concept was arise when it is impossible to send colour image. The concept of gray scale is important for sending the colour image because the gray scale has luminous intensity. The luminous intensity factor of colour image cannot be same and to convert this luminous intensity factor of colour image into same factor, we need gray scale conversion concept.

After converting colour image into gray scale image, the image get sliced horizontally or vertically into number of parts. The sliced image needs to maintain its original size. The number of sliced get increases to create complexity for attacker. The attacker gets confused if the number of slices is more. The attacker cannot identify the image even if he/she get the details of image. The original image was only known to the authorized person.

After slicing an image into number of parts, the slices wants to encrypt by using the encryption factor. Before processing and after slicing we need to set the encryption factor. That encryption factor is also called as threshold value. By using this threshold value, every slice of an image get encrypted. Even if the attacker gets the details of an image, still attacker cannot find an original image. The attacker can see only encrypted data not original data. The encryption factor is nothing but a key which wants to encrypt the data.

In this project one concept is implemented i.e. Adding cover image. This concept was arise to remove the problem of "pixel expansion" by adding an extra pixels in the image. It is a function which is call at the time of merging slices at the receiver side. Because of this concept an image which is received at receiver side seen clearly. The adding cover image means nothing more than adding extra pixel in the original pixels.

The receiver can receive an image, by entering the threshold value. There is no need of extra algorithm to decrypt an image. The slices were merging and form an original image. The threshold value is nothing but encryption factor. If this factor enters correctly then receiver can see the image.

II. Literature Review

Most type of different algorithms are already define for visual cryptography have been proposed. The most of the attacks by a hacker would like to attack on an images. A survey and comparison of this techniques is given in this paper presents.

1. The Secret Sharing Scheme proposed by the Adi Shamir in 1979.

It refers to method for distributing a secret amongst a group of participant‘s, each of whom is allocated a share of the secret. The secret can be reconstructed only when sufficient number of shares is combined together; individual shares are of no use on their own.

2. Encrypting an image by random grids (RGs) was first introduced by Kafri and Keren in 1987.

A binary secret image is encoded into two noise-like transparencies with the same size of the original secret image, and stacking of the two transparencies reveals the content of the secret.

Comparing RGs with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded. The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme is not based on the basis matrices. The recent studies include the RG for color image.

3. The visual cryptography scheme was introduced by Naor & Shamir in 1994. It is a secret sharing scheme with good security for binary image. In [2] Wu et al have proposed a visual cryptography schemes to share two secret images in two shares. In the hidden two secret binary images into two random Shares,

for namely A and B, such that the first secret can be seen by stacking the two shares.

III. Proposed Plan

A. Architecture

In System Architecture, the working of project can be explained. An image is sending from sender to receiver are explained. In the sender side, an encryption process can be perform and in receiver side decryption process can be perform.

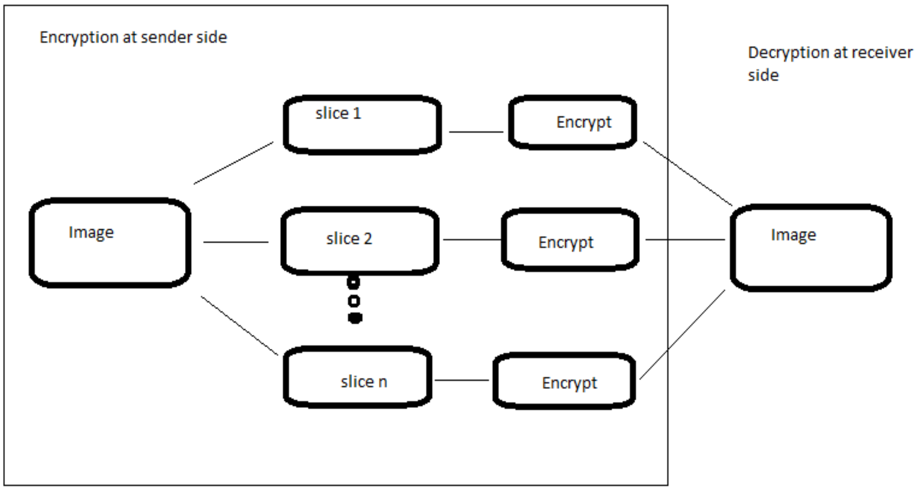
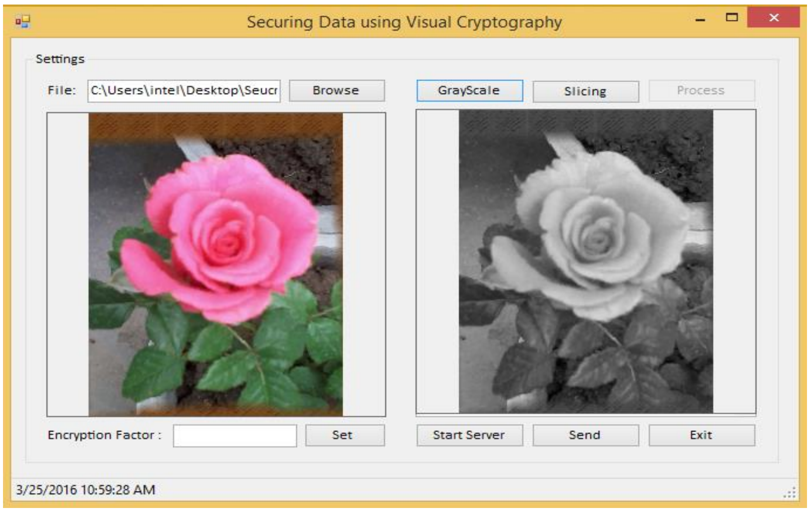


Fig. System Architecture

Fig.1 System Architecture

1. Gray Scale Conversion

In gray scale conversion, the colored image can be converted into the gray image. Gray image is nothing but the black and white image. In gray scale conversion the dark color is turned into black color and light color turn into white color. The need of conversion of gray scale is to send colored image from sender to receiver. The intensity of colored image is different at every pixel hence to maintain the intensity of image we need to convert an image into gray scale.



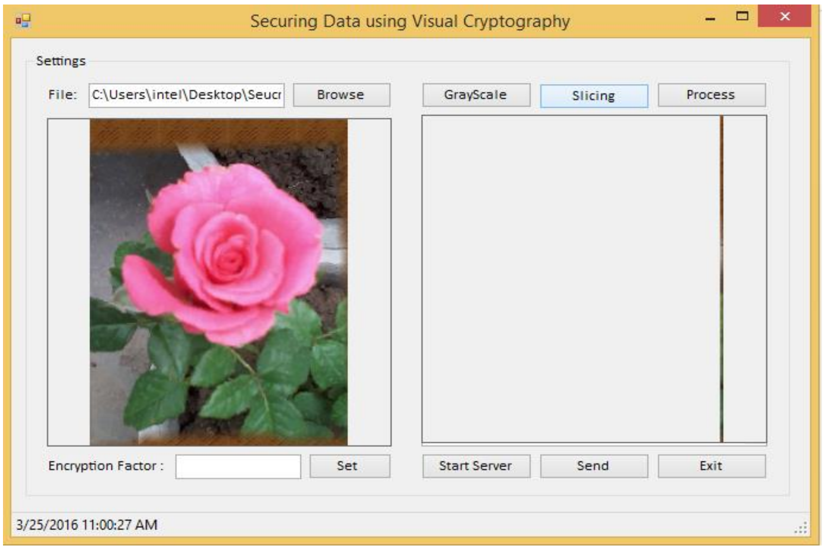
File: C:\Users\intel\Desktop\Seucr

3/25/2016 10:59:28 AM

Fig.2 Gray Scale Conversion image

2. Slicing

In this module, the image get sliced and forms a shares. The size of sliced image is converted into the size of original image .The maximum number of slice hence the security get increase. The attacker get confused because of maximum number of slices. The slicing was done either horizontal or vertical it depends. The maximum number of slices creates maximum confusion.



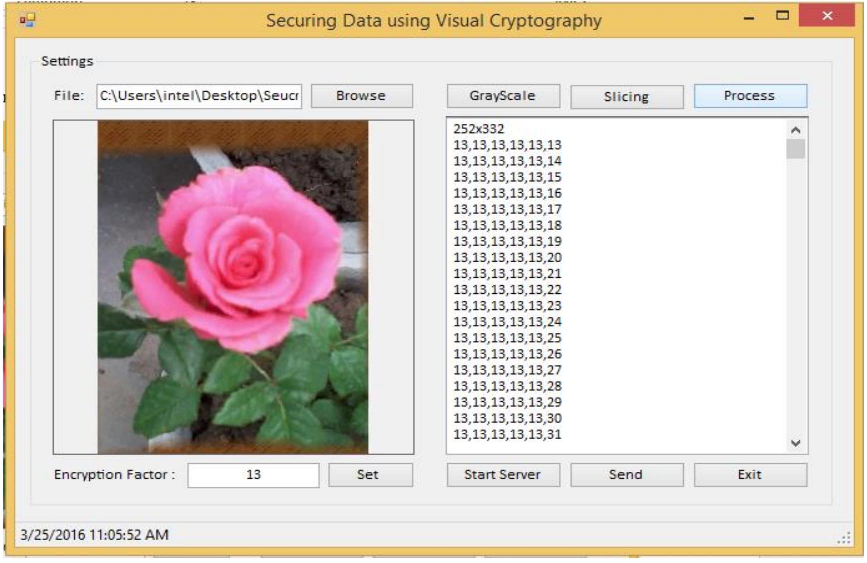
File: C:\Users\intel\Desktop\Seucr

3/25/2016 11:00:27 AM

Fig.3 Slicing Conversion image

3. Encryption

In encryption process, each slice or image get encrypted separately. Each slice can be encrypted by adding, subtracting, multiplying by a particular number. This number which is used to encrypt an image is called as Encryption factor or also called as Threshold value. By using this factor the pixels get converted into the encrypted form. This is the very simplest technique to encrypt an image. Because of this process, even if the attacker trap the details of an image then the image not original image.



Securing Data using Visual Cryptography

Settings

File: C:\Users\intel\Desktop\Seucr

Encryption Factor : 13

```
252x332
13,13,13,13,13,13
13,13,13,13,13,14
13,13,13,13,13,15
13,13,13,13,13,16
13,13,13,13,13,17
13,13,13,13,13,18
13,13,13,13,13,19
13,13,13,13,13,20
13,13,13,13,13,21
13,13,13,13,13,22
13,13,13,13,13,23
13,13,13,13,13,24
13,13,13,13,13,25
13,13,13,13,13,26
13,13,13,13,13,27
13,13,13,13,13,28
13,13,13,13,13,29
13,13,13,13,13,30
13,13,13,13,13,31
```

3/25/2016 11:05:52 AM

Fig.4 Encrypted Data image

4. *Adding Cover Image*

This concept was arise to remove a problem of pixel expansion. This method is called as extended visual cryptography. When the image decrypted, it not get cleared image. To increase the clarity of an image, the adding cover image was implement. When the image get merge at the receiver side the extra pixels are added into the original pixel. This method helps us to improve the clarity of an image.

5. *Decryption*

The Decryption is nothing but form an original image at the receiver side. There is no need of any algorithm to decrypt an image. The decryption is perform by visualizing the image by human eye. Hence this is the advantage of this research. The encryption factor is used to receive an original image.

B. *Working*

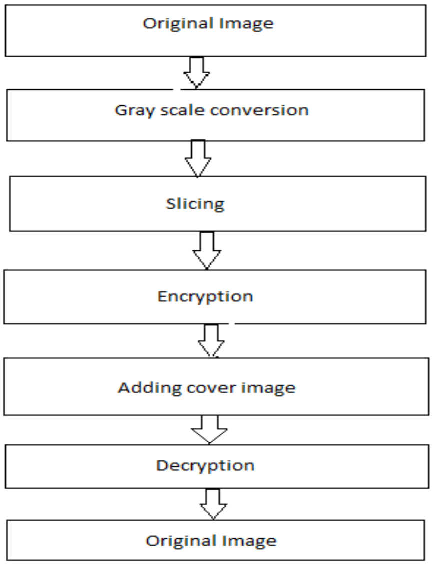


fig: data flow diagram

Fig.5 Data Flow Diagram

Original image is an input of this project which can be converting into gray scale image by using gray scale conversion. Then that gray scale image can be divided into slices, this slices can be encrypted by using Encryption technique. After Encryption, Adding cover image technique can be used. Then this image can be receive by receiver and receiver gets image in original size. In this way project is wok.

C. Code for Gray Scale

```
Bitmap bm=new Bitmap();
Bitmap bm=image.fromfile(“ “);
For(I=0;to bm.width){
   For(j=0; to bm.height)
       {
        Color c=bm.getpixel(I,j);
        Color d=newColor();
         d.R=c.R*0.3;
          d.G=c.G*0.3;
         d.B=c.G*0.3;
        dm.setpixel(I,j,d);
}
}
```

D. Users of System

1. Client

The client can send the request to the server for connecting the server. The client can receive the details of an image. If the client is authorized person then he/she enter the correct threshold value and receive the decrypted image .The IP address and port number required to connect the server with client.

2. Server

Server can give the response to the client. The encrypted image can be send to the client side. The original image can encrypt in server side by entering the encryption factor. This encryption can be entering by the user.

E. Advantages

1. In Decryption method, the slices are decrypted by giving the threshold value hence it is more efficient.

2. No need of decryption algorithm. The image can be visualized by human sight.

3. The traditional cryptosystems need much time to directly encrypt the image data hence the visual cryptography is helpful in this method.

F. Applications

1. Transmission is secure

2. Storage of data can be secure

3. Integrity in Transmission

4. Integrity in Storage

5. Authentication of Identity

6. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc.

IV. CONCLUSIONS

Visual Cryptography is an important technology for providing security to an images secending from sender to receiver. In this research paper the modules which are implementing practically are explained in detail. In this research paper only the practical implementation can be explained. Also explain why we use the above techniques for securing the data or image. The process of securing data can be helpful to share the data or image securely to another person.

REFERENCES

[1] Nagaraj V. Dharwadkar , B.B. Ambedker, S.R. Joshi, "*Visual Cryptography for Color Image using Color Error Diffusion*", ICGST-GVIP Journal ,volume 10, issue 1,February 2010.

[2] Young-Chang Hou, "*Visual cryptography for color images*", Pattern Recognition 36 (2003), 1619-1629.

[3] Masakazu Higuchi, Shuji Kawasaki, Jonah Gamba, Atsushi Koike, Hitomi Murakami "*A Fundamental Conception to Formulate Image Data Hiding Scheme Based on Error Diffusion from Stochastic Viewpoint*", International journal of mathematics and informatics, Issue 1, Volume 6, 2012.

[4] M. Naor and A. Shamir, "*Visual cryptography*" in Proc.AdvancesinCryptography(EUROCRYPT'94), vol. 950, LNCS, pp. 1–12.Stinson D.R. Cryptography Theory and Practice, CRC Press Inc., 1995.

[5] M. Sukumar Reddy, S. Murali Mohan, "Visual Cryptography scheme for Secret image retrieval" in IJCSNS Journal, volume 14, no 6, june 2014.

[6] Sian Jheng Lin and Wei Ho Chung "*A Probabilistic model of (t,n) Visual Cryptography Scheme with Dynamic group*", ieee transactions of information forensics and security, vol 7, no 1, feb-2012.