VISUAL CRYPTOGRAPHY AND ITS USE IN BIOMETRIC AUTHENTICATION

Asst. Prof. Ruchi Bathla

Assistant Professor | Department of Computer Science & Application | Geeta Degree College, Shera (Panipat)

***Abstract*:** Today, we live in information age because of advances in information & computer technology (ICT). Increasing concern over personal information in computer system has increased interest in data security. This paper reviews and applies the visual cryptography on the biometric authentication. The concept of visual cryptography is divide the secrete images into random shares. Here the encryption technique divide the image into a number of parts i.e., k-n secret sharing schema is used. Decryption is used to decrypt the shares into the secret image. In this paper, I have purposed a new k-n secret sharing schema for black & white image and apply them to biometric data such as finger print image for the purpose of user authentication.

Keywords: **Visual Cryptography, 2-out-of-2 Secret Image Sharing Scheme, Multiple Secret Images Sharing Scheme, Application of Visual Cryptography: Biometrics Authentication**

I INTRODUCTION

Now a day, increasing use of internet has a great impact in human beings. They become more dependent on the computer system and networks. This dependency has brought many threats to the network security. Due to this reason, we need a secure mechanism which protects our information through unauthorized access. Biometric authentication system is example of the technologies which widely used in various applications like ID cards, banking etc.

Biometrics is a technical terms which measure and calculate body. It is used in computer science to indentify the individual. It have unique physical characteristics (such as fingerprints, eyes, face) or behavioural characteristics (such as signature, voice etc,) for the purpose of identification and authentication [1]. Biometrics method has more advantage over the traditional password method. For example – password can be easily forgotten, stolen and difficult to remember. Easy password can easily guess and complex password is difficult to remember. But biometrics can be more reliable as compare to traditional password method. Biometric data are changed according to physical or emotional condition of the owner at the time of authentication.

This paper provides an overview of visual cryptography and also discusses its application in biometric authentication.

II VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic technique which allows visual information which is in the form of pictures, text etc. It hides the information in such a way it can't be retrieve by human visual system. In visual secret sharing schema, the decryption process decrypt the encrypt data using human visual system (HVS) without any complex computation.

Visual cryptography was invented by Moni Naor and Adi Shamir in 1994 at Eurocrypt conference [2][8]. Image sharing is a subset sharing where secrets are concealed images. Each secret is treated as number which allowed a specific encoding scheme supply for each source of the secrets. The number may not be interpreted correctly to represent the true meaning of the secrets. In (k, n) image sharing, the image is split into n shares and decryption is unsuccessful unless at least k shares are collected and superimposed. Naor and Shamir's initial implementation assume that the image is collection of black and white pixel (here black pixel show by 1 binary value and white pixel show by 0 binary value). Each pixel handled uniquely. Here white pixel show transparency.

In this paper, an algorithm [3] is described to divide a digital image into a number of shares (minimum k shares) which are sufficient to reconstruct the image again. If k shares are taken then remaining shares are (n-k) shares. If position of pixel in the image is 1 then (n-k+1) number of shares in that position of the pixel is 1 otherwise 0.

The algorithm which converts the image into the shares is as follow

```
Algorithm (Img)

/* Img is the image on which the visual cryptography will be applied */

{

    1.  Divide the image into N sub images
    2.  Obtain K bit value from N sub images to define the data sequence
    3.  Now K bit data will represent the information
    4.  Now split the information into two sub block of size k/2
    5.  If (pixel = white)
        {
    6.  Set the new random sequence for the pixel
        }
    7.  Else
        {
    8.  Set other bit sequence for that pixel
        }
    9.  Reconstruct the pixel at gray level analysis under the contrast specification for reconstruct the
        image.
    10. Return Image;

}
```

Here the secret image is taken as input from the user and create number of shares using encryption algorithm. Here each share has a equal length and width as the original image. Now the bitwise OR operation perform among the pixel of shares and final pixel value store in an array.

The decryption algorithm as follow:

```
Algorithm (Image)

/* Image is the encrypted image taken as input for decryption*/

{

  1.  For I = 1 to Size(Image)
      {
  2.  Px = GetPixel(Image(i)
      [read pixel from Image]
  3.  Divide the Pixel in N sub block called Px1, Px2, ……………,PxN
  4.  Process each Pixel under the binary value analysis
  5.  If (Px > Threshold)
      {
  6.  Set Px=Black
      }
  7.  Else
      {
```

```
    8.  Px=White
        }
    9.  If (Count(Black)> Count(White))
        {
    10. Generate the sub image to black
        }
    11. Else
        {
    12. Generate the sub image to white
        }
    13. Reconstruct the result Pixel Image
    14. Return Image

}
```

According to their algorithm, the secret image convert into n shares and the secret is revealed if any k of them stacks together.

The number of pixel should be as small as possible, in contrast of the difference between the maximum value of a hamming weight for a black pixel and the minimum value of hamming weight for white pixel is maximum as possible. Some researcher focuses on contrast degradation and introduced the methods to improve the reconstruct of the secret images. Many study have been done to support gray scale by apply the visual cryptography and also create the natural image with meaningful shares called extended visual cryptography.

III 2-OUT-OF-2 SECRET IMAGE SHARING SCHEME

In this scheme [1], every secret pixel is converted into two shares and recovered by stacking two share together by applying OR operations between the shares. Due to the pixel expansion, one pixel from original image converts into 4 pixels in the following manner:

1. If the pixel of original image is white, pick the same pattern of four pixel for both shares
2. If the pixel of original image is black, pick a complementary pair of patterns

Visual representation of the different types of share shown in figure 1

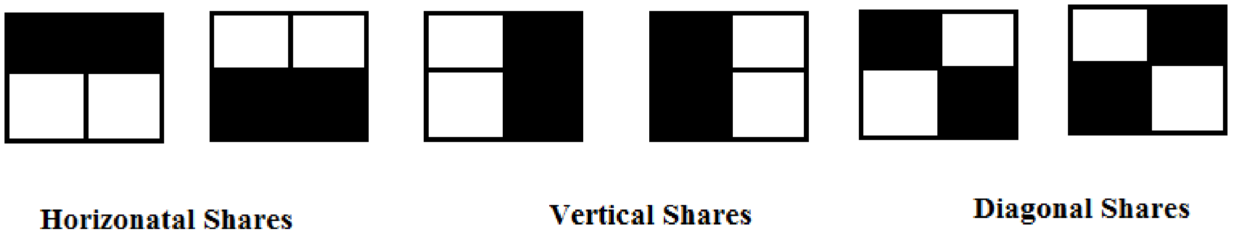
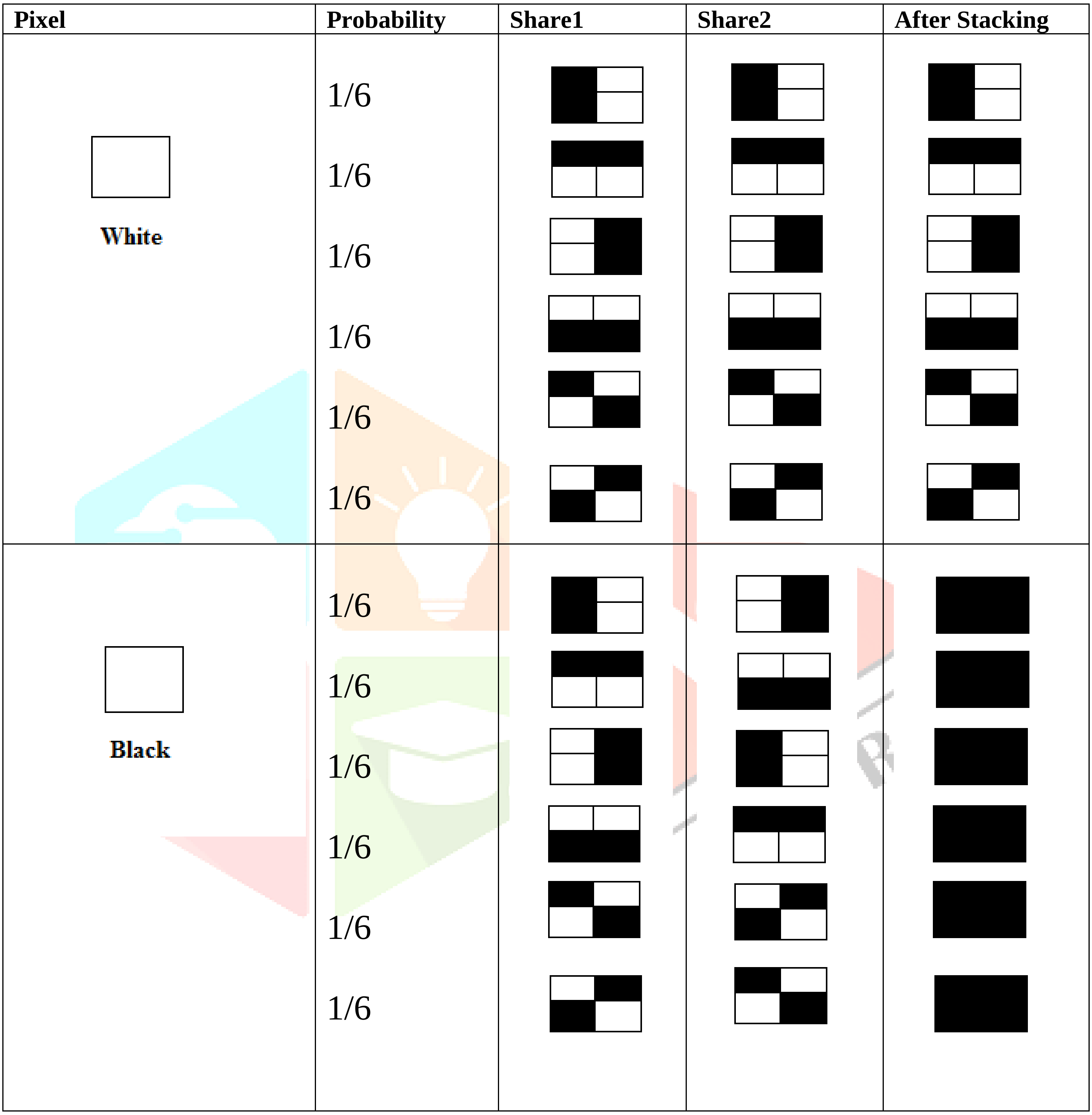


Figure 1: The various type of shares

In 2-out-of-2 schema, every secrete image is converted into two shares and recovered by stacking two share together by using OR operation between shares. As illustrate in table 1, 1 pixel covert into 4 sub pixels in such a way 2 sub pixels represent white and other two represent by black. Te selection of pixel is randomly from each pattern. It is easily see that one share doesn’t reveal the other share.

Table 1

Illustration of 2-out-of-2 secret image sharing scheme with 4 sub pixels



Pixel	Probability	Share1	Share2	After Stacking
White	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
Black	1/6			
	1/6			
	1/6			
	1/6			
	1/6			
	1/6			

An example of applying the 2-out-of-2 with 4 sub pixels layout visual secret sharing scheme is shown in figure 2. It shows the share images are 2 times larger than the original image. As illustrated in figure 1 (a) is the secret image, (b) and (c) are the share image, and (d) show the reconstructed image which generated from share images in figure 2.

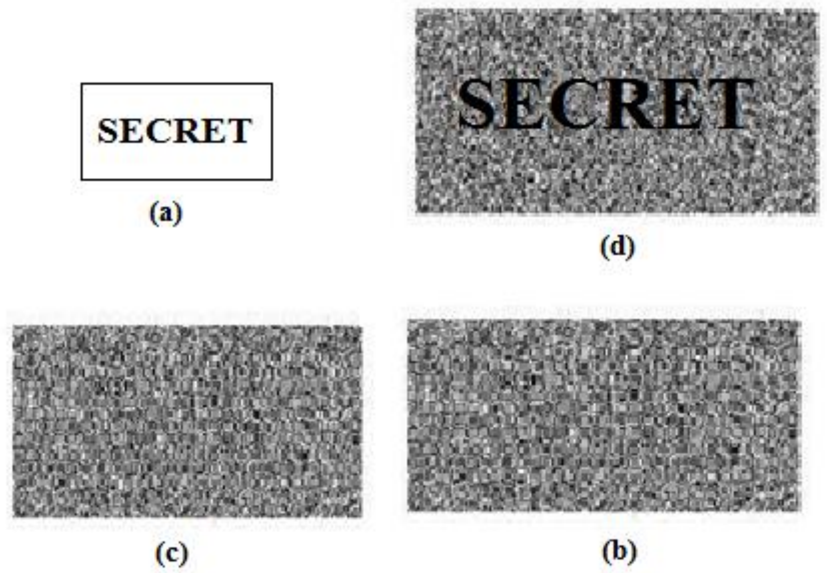


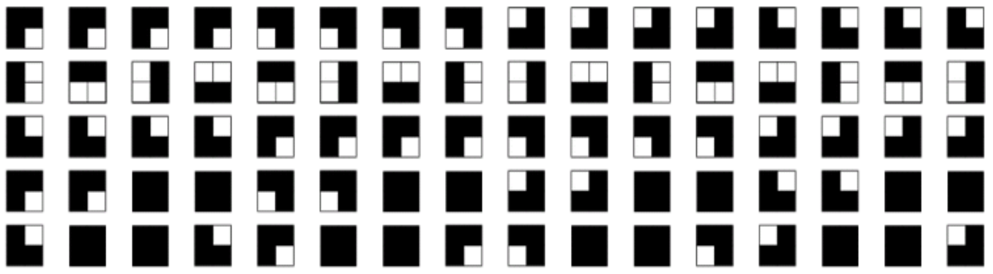
Figure 2: 2-out-of-2 secret sharing schemes

IV MULTIPLE SECRET IMAGES SHARING SCHEME

In 1998, Chen and Wu developed Naor and Shamir's schemes and proposed a multiple secret image sharing scheme [4]. One disadvantage's in previous scheme is that only one secret image is constructed at a time. So, Chen and Wu proposed a schema that that could encrypt two secret images at the same time by using rotation technique. The first secret image become visible by stacking first and second shares and second secret image is created by rotating first share by ɵ (where ɵ is 0^o, 90^o, 180^o, 270^o) and stacking with second share. Wu and Chen's encoding scheme is shown in table. In this table, the share 3 is rotate by 90^o. Table 2 [7] summarized Wu and Chen's encoding scheme for visual two secret sharing in two shares

Table 2

Illustration of visual two secret image sharing scheme

Pixel of the first secret image	W	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B
Pixel of the second secret image	W	B	B	W	W	B	B	W	W	B	B	W	W	B	B	W
S1 S2 S3 S1 stack S2 S3 stack S2																

V APPLICATION OF VISUAL CRYPTOGRAPHY TO BIOMETRIC AUTHENTICATION

Biometrics [1] is a technical terms which measure and calculate body. It is used in computer science to indentify the individual. It have unique physical characteristics (such as fingerprints, eyes, face) or behavioural characteristics (such as signature, voice etc,) for the purpose of identification and authentication. Biometrics method has more advantage over the traditional password method. For example – password can be easily forgotten, stolen and difficult to remember. Easy password can easily guess and complex password is difficult to remember. But biometrics can be more reliable as compare to traditional password method. Biometric data are changed according to physical or emotional condition of the owner at the time of authentication.

The fingerprint is the most common used for human authentication. Comparing fingerprint by other biometrics traits, it show that the fingerprint high value in factor like distinctiveness, performance, universality, durability etc. while using hand written signature, it show lower value. Biometric system requires the process of enrolment, verification and identification for improving security, reducing the fraud and enhancing the user convenience.

In enrolment, the biometric template store in database for eligible users. Verification is the process authentication of the given biometric sample. Identification is the process in which indentify the biometric sample to the biometric data in the database. For protection of the biometric sample from vulnerable attacks, data hiding techniques such as visual cryptography is used. The authors [5] substitute the OR operation with XOR operation to improve the quality.

Figure 3 show the encryption and decryption process of fingerprint image [6] using 2-out-of-2VCS with XOR operation

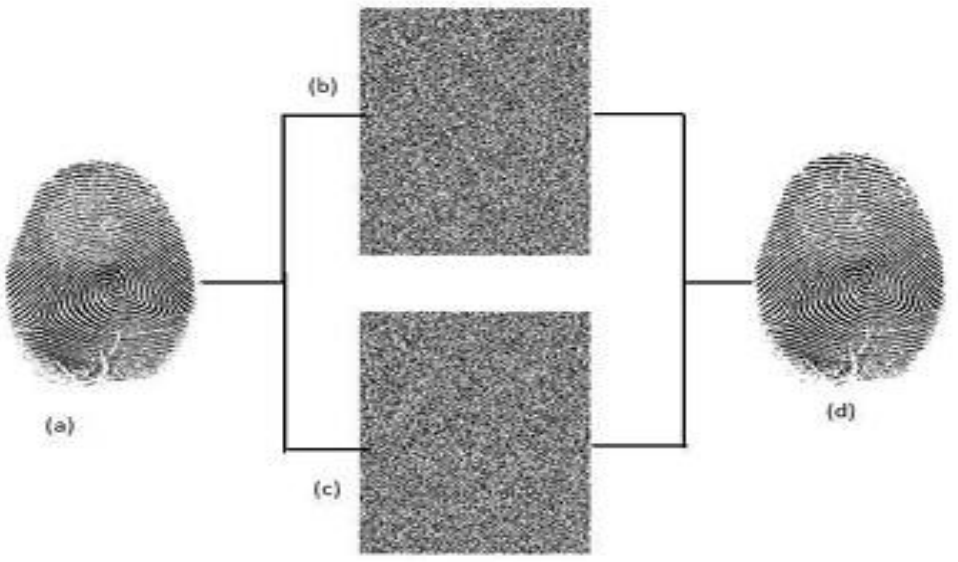


Figure 3: Example of a 2-out-of-2 secret sharing scheme: (a) Secret fingerprint image (b) First Share (c) Second share (d) Reconstruct secret fingerprint image

The fingerprint of each eligible is collected by the system administrator and random shares are created using the encryption visual cryptography system. One of the shares is stored in database and other share is store in the form of unique ID card. For verification, user insert the ID card in the system then corresponding share which store in the database matched with ID card. Thus system identify user.

One of the disadvantage of this method is that the limitation of the biometric samples. The ID card request one secret shares for each biometric sample. Fingerprint authentication system have a thousand of user and it wants the minimize cost to store the shares in the database.

This problem is overcome by multiple secret image sharing algorithms. As describe by Chen and Wu's, it need two shares to represent secret images. For example: Consider an id card with two fingerprints belong to same person. For storing two fingerprints, we use multiple secret sharing algorithms. Here first share related to ID card, second share store in database and the third share derived from second share by rotating the share. Figure 4 show the multiple secret sharing schemes.

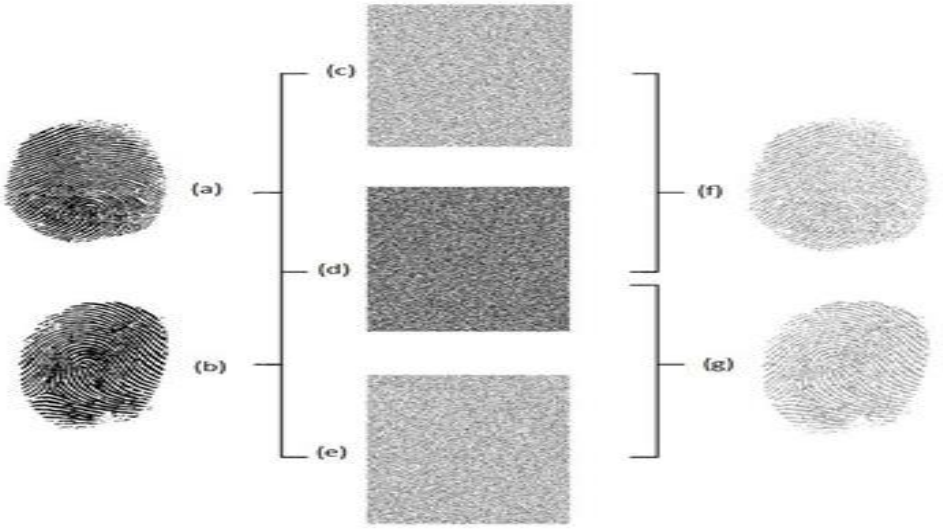


Figure 4: Example of a multiple secret sharing scheme: (a) First secret sharing fingerprint image (b) second secret sharing fingerprint image (c) Share A (d) Share B (e) Share C (f) Reconstruct secret 1 sharing fingerprint image (g) Reconstructed secret 2 sharing fingerprint image

VI .CONCLUSION

Biometric method have unique physical characteristics (such as fingerprints, eyes, face) or behavioural characteristics (such as signature, voice etc,) for the purpose of identification and authentication. Biometrics method has more advantage over the traditional password method. For example – password can be easily forgotten, stolen and difficult to remember. Easy password can easily guess and complex password is difficult to remember. But biometrics can be more reliable as compare to traditional password method. Biometric data are changed according to physical or emotional condition of the owner at the time of authentication.

In this paper, I describe visual cryptography and its schema. Chen and Wu's multiple secret sharing image schemes are used to store the two fingerprints template in the database. It enhances the security of the secret information. It is beneficial in term of cost of storage, database capacity and bandwidth. The authentication is achieved by comparing the user's fingerprint with secret fingerprint that are derived from visual cryptography algorithm. This approach can easily extend to other biometric traits such as facial image.

VII REFERENCES

[1] A. k. Jain and A. Ross, "*Biometrics: a tool for information security*". IEEE transaction of information forensics and security; vol. 1; 2006

[2] Jonathan Weir; WeiQi Yan, "*Visual cryptography and its applications",* Jonathan Weir and WeiQi Yan & ventus publishing ApS; ISBN 978-87-403-0126-7; 2012; pp. 9-11

[3] Aruna Tomar and Sunita Malik, "*A key Division Scheme to improve Visual Cryptography on Half Tone Image*"; IJCSMC Vol. 3,Issue 6; 2014; pp. 438-443

[4] J. B Feng and G. C. Wu and C.S. Tsai and Y.F. Chang and Y.P. Chu, "*Visual secret sharing for multiple secrets*", Pattern Recognition, Vol. 41; 2008; pp. 3572-3581

[5] T. Monoth and B.A. P, "*Tamperproof of transmission of fingerprints using visual cryptography schemes*", Procedia Computer Science; Vol. 2; 2010; pp. 143-148

[6] http://education.vetmed.vt.edu/Curriculum/VM8054/labs/lab14/NOTE

[7] S.J. Shyu and S. Y. Huang and Y.k.Lee and R.Z. Wang and K. Chen, "*Sharing multiple secrets in visual cryptography*", Pattern Recognition, Vol. 40, no. 12; 2007; pp. 3633-3651

[8] M. Naor and A. Shamir, "*Visual Cryptography: improving the contrast via the cover base*", IACR Eprint archive; 1996