Secure Biometric Authentication Using Recursive Visual Cryptography

Mrs.Lakshmi Madhuri.K., Mr.Viraj Thakur, Mr.Rajesh Jaiswal, Mr.Sandesh Sonawane, Mr.Rohit Nalavade

Department of Computer Engineering
Maharashtra Academy Of Engineering, Alandi
Pune, Maharashtra, INDIA

Abstract- Recursive Visual cryptography takes the idea from the basic scheme of Visual cryptography to hide multiple secrets recursively in the single image. [1] This paper proposes a scheme of recursive creation of shares using the basic scheme and embedding secrets into the shares. This results levels of share creation i.e. n- secrets equals n/2 levels. This paper also provides secured authentication for the user, using the Biometric authentication [6-7] Thus the proposed paper is implemented in any of the real time applications.

Index Terms- Recursive Visual Cryptography, Embedding secrets, Biometric authentication, Levels of shares.

I. Introduction

Internet is one of the most popular communication channels but is insecure. Since it is an open and insecure medium, malicious users can intercept data. The fast growth of online applications results in the data security problem. In order to achieve data security, users need secure communication methods for transmitting secret messages over the Internet. Encryption is well-known method for achieving data security. It transforms secret information into an encrypted form, which looks like a random message. Transformation procedure is called encryption process and the result is called cipher text. A computational device is required to perform decryption of the cipher text. Therefore, the cost or efficiency of the hardware, complex algorithms and mathematical computations increase to encrypt and decrypt the data.

Therefore, the cost increases and efficiency reduces. and mathematical computations increase to encrypt and decrypt the data.

II. DATA SECURITY

Security of data has been a major issue from many years. Using the age old technique of encryption and decryption has been easy to track for people around. Providing security to data using new technique is the need of the hour.

This project uses the technique of Visual cryptography and providing biometric authentication. Thus using the above technique Recursive Visual cryptography would be implemented.

A. *Objectives*

- To provide security in any real time application.
- To overcome and avoid cheating in real time applications.
- To store more than one secret at a time.
- To provide much more security by adding biometric authentication.

III. VISUAL CRYPTOGRAPHY

One of the best known techniques to protect data such as image is Visual cryptography. Naor and Shamir introduced the visual cryptography scheme as a simple and secure way to allow the secret sharing of images without any cryptographic computations. [1] VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. [1]

The basic scheme is referred to as the -out-of- VCS which is denoted as VCS. Given an original binary image, it is encrypted in images, such that where a Boolean operation is is an image which appears as white noise, and is the number of noisy images.[2] It is difficult to decipher the secret image using individual's. The encryption is undertaken in such a way that one or more out of the generated images are necessary for reconstructing the original image. In the case of (2, 2) VCS, each pixel in the original image is encrypted into two sub pixels called shares. [1]

The paper proposes the scheme of share creation taken from N x N share creation; we hereby propose the scheme of 2X2 Share creation proposed in this paper.

Fig. 1 denotes the shares of a white pixel and a black pixel. Neither share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. [2]When the two shares are superimposed, the value of the original pixel can be determined. If is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel. Therefore, the reconstructed image will be twice the width of the original secret image. [6]

Thus the scheme of Visual cryptography would be implemented.

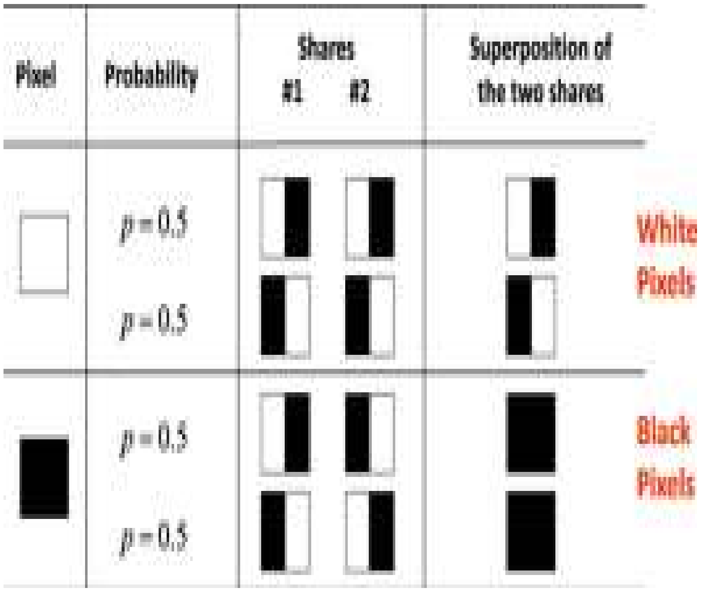

Figure 1: Pixel expansion scheme

IV. RELATED WORK

The topic of recursively hiding secrets within a share has been extensively researched. The scheme proposed in this paper applies to images and attempts to increase the efficiency of traditional VC to make it possible to hide extra secret information that serves as a steganographic channel. [2] The scheme involves recursive hiding of smaller secrets within a larger secret. It is obvious from the previous work that many thoughts have been given to the idea of recursive information hiding within visual cryptography. [2]However, the idea of embedding these types of recursive shares within the share and providing biometric security at the last level so that no previous shares would be recovered, to our knowledge, has never been considered.

V. OUR CONTRIBUTION

There are two main contributions that are discussed within this paper. The first deals with recursive creation of shares. This involves a recursive multiple resolution VC scheme which allows smaller secret to be hidden within one large share. [2]

The second contribution is providing biometric security to the last level of share, such that when the last share is authenticated the upper level of embedded secrets would be revealed. The Iris recognition algorithm would be used to provide biometric security to last level of client share.[3] The well known algorithm for Iris security the median metric algorithm would be implemented.

VI. PROPOSED MODULES

This paper proposes various modules. The models are based on the algorithm used at various stages, they are as follows:

Data storage and retrieval: For the purpose of authentication there would a server database which stores all the biometric images of the User, and the other information related to the user. The other database would store all the shares created at the runtime. [5]

This is how the data would be manipulated and the proposed modules in this paper are as:

Module 1: Image processing

Converting images to grey scale:

Naor and Shamir mentioned the extension of their scheme to grayscale images. [1] That is, to represent the grey levels of the hidden image by controlling the way how the opaque sub pixels of the sheets are stacked together. If the number of colors is increased the contrast of the images would be reduced and therefore would not be useful in recursive visual cryptography. [4] For the deployment of recursive visual cryptography scheme we need to convert color images grey scale images.

In this module we would be identifying the secrets. These would be converted in grey scale image.

Module 2: Recursive Visual Cryptography

This method put forth has a secret image. Each secret is identified, two shares are created of that secret, as in the above figure.Share1 is stored at client side and share 2 is stored at server side. In the next level the secret image 2 is taken and this secret is embedded in the application side share. The share that is stored at the application side has a secret embedded in it. Now this secret and share is converted into 2 shares and one stored at the client side and one store the server side.[1] This method is followed recursively, such that at each level a secret would be embedded in the corresponding share.[2] Thus this is the method of recursive visual cryptography.

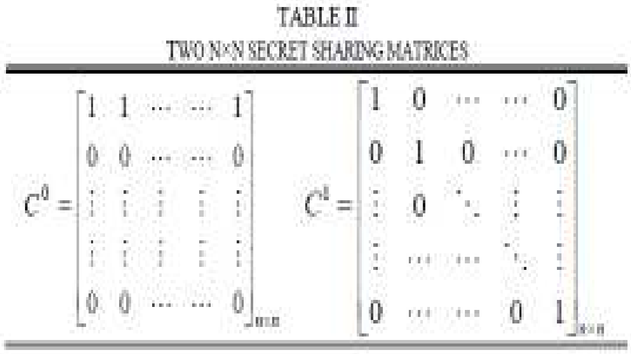

TABLE II
TWO N×N SECRET SHARING MATRICES

$$C^0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n\times n} \qquad C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$$

Fig. 2: NxN secret sharing scheme

```
Algorithm:
Input:A W x H secret image P,p(i,j) of P
Output:2 shares $S^m$ ,m=1to n;
Process:
1.Generate sharing matrices C0 and C1.
2.For each pixel p(i,j),1<i<W and 1<j<H;
3.For l as the expanded pixel 1to n;
4.For m=1 to n
    4.1: If pixelp(i,j)=0(White),the pixel value
            $S^m$ (i,j)=C0(l,m)
    4.2: If pixelp(i,j)=1(Black),the pixel value
            $S^m$ (i,j)=C1(l,m)
```

Recursive storing of secrets:

1.For each S^m, S^{m+1}=next secret,m=1to n.
2.E^m=Embedded secret in share C^m ,m=Odd share;
3.Expand E^m using the 2X2 secret sharing scheme
4.Go to step 1 of RVC for each new secret
5.Store S^m, m=Even share stored at client side,
S^m=Odd share stored at application side.

Our policy is to provide biometric authentication at the client end such that when biometric authentication is provided by the client the secret would be stacked on the application side hare and the secret would be revealed.[3]

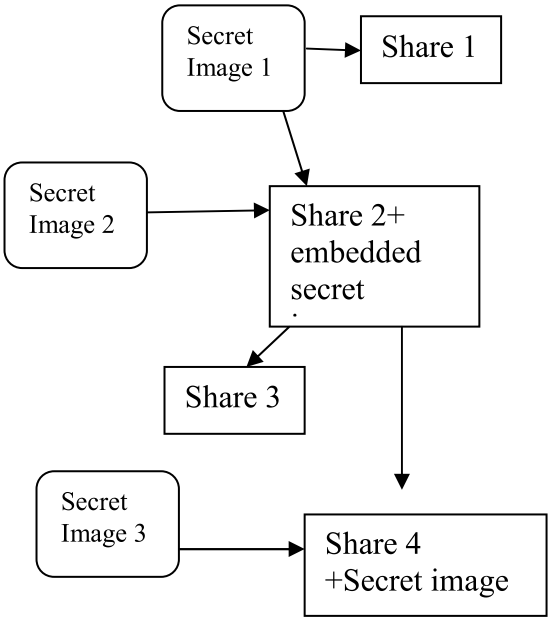

Fig. 3: Recursive Creation of shares

Module 3: Biometric Authentication

There are various techniques provided for authentication in general scheme. Biometric authentication is the scheme provided by recognizing the human visual identity recognition. We here would be implementing the iris recognition system.

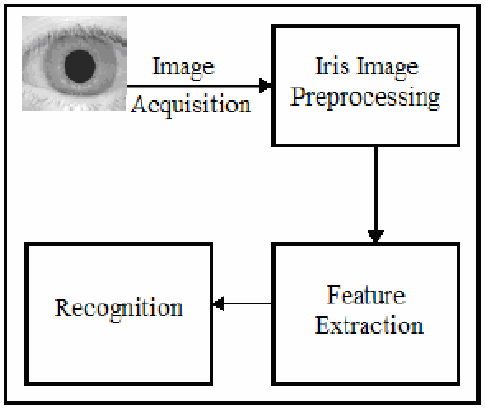

Fig. 4: Iris Recognition methodology

An efficient method for personal identification based on the pattern of human iris is proposed. [7] It is composed of image acquisition, image pre-processing to make a flat iris then it is converted into eigeniris and decision is carried out using only reduction of iris in one dimension. By comparing the Eigen irises it is determined whether two irises are similar. The results show that proposed method is quite effective.

A general iris recognition system is composed of four steps. Firstly an image containing the eye is captured then image is pre processed to extract the iris. Thirdly eigen irises are used to train the system and finally decision is made by means of matching.[8]

Methodology:

1. IMAGE ACQUISITION

In iris recognition image acquisition is an important step. Since iris is small in size and dark in colour, it is difficult to acquire good image. The colour image is captured. The image is then changed from RGB to gray level for further processing.

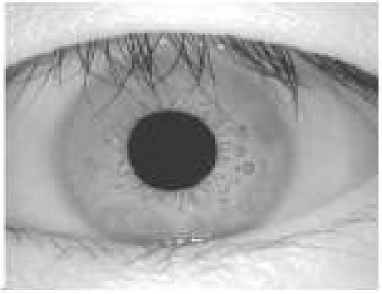

Fig. 5: Image Acquisition

First of all to separate the iris from the image the boundaries of the iris and pupil are detected. Since pupil is the darkest area in the image as shown in Figure 2; so a rough estimate of its center (Cx, *C*y) is performed using the following formula:

$$C_x = \arg\min_x \left(\sum_y I(x,y) \right)$$

$$C_y = \arg\min_y \left(\sum_x I(x,y) \right)$$

where *I(x, y)* is the iris image intensity at point (x, y). To find the exact centre of the pupil, a part of image is binarized.

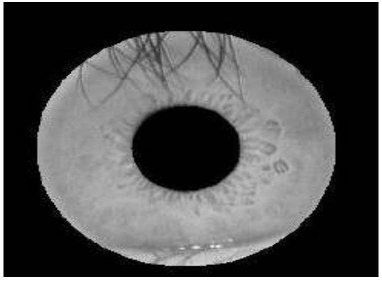

Fig. 6: Localized Iris Image

Then using the median matrix method the image pixel intensity would be calculated and median would be calculated and stored in the array. [7]

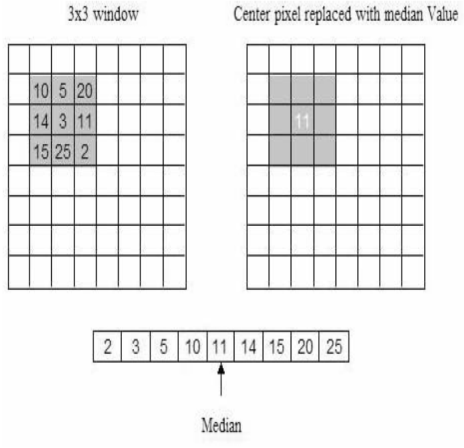

Fig7: Median matrix method

The algorithm used here is the median matrix method; here the edges of the biometric images would be detected by using edge detection algorithm.

During the authentication process the array would be attached and then customer would be authenticated.

Module 4: Decryption

After the biometric authentication is done the customer will give his part of the share. The two shares from the application side and the client side would be superimposed and if they match the secret would be revealed. [3]This would be done for each level and the embedded secrets at each level will also be revealed.

VII. Advantages

The advantages of such type of Recursive Visual cryptographic scheme are: Original image security is provided. Secure Authentication is provided. Chance of fake share creation is not possible. More than one image be kept as secret [2]. Recursive cryptography is first of the concepts to be implemented for security.

VIII. EXPERIMENTS AND RESULTS

Two shares are generated Share1 and Share2 as output of visual cryptography algorithm. One share along with username is kept by system and other is given on the user card. For authentication user provides share which is on the card. The share extracted from this card is superimposed with corresponding share that is stored in the database, generates the original image. From this Iris template image feature template is generated. Now this feature template is matched with Iris feature of newly provided eye image using hamming distance.

The most popular and commercial iris recognition system was developed by Daugman [7]. Following this many iris recognition systems are proposed by researchers [8]. As main intent of this paper is providing security to the iris template in the database, image processing algorithm for iris feature extraction are derived from [8].The working of proposed system is shown in figure 4 and 5.For enrollment a single eye image is taken from CASIA database. After performing segmentation, normalization and feature extraction feature template is generated. Iris template image (generated from feature template) and another binary image which is chosen by system administrator is given as input to the visual cryptography algorithm.

IX. CONCLUSION

We would be trying to build a secure intense project in which security would a major issue, thus making security with the intense algorithm of Recursive visual cryptography, and adding biometric authentication to it. Various approaches adopted by researchers to secure the raw biometric data and template in database are discussed here. In this paper a method is proposed to store iris template securely in the database using visual cryptography. Experimental results indicate that by applying visual cryptography techniques on iris template for more security, matching performance of iris recognition is unaffected with extra layer of authentication.

References

[1] Visual Cryptography Moni Naor and Adi Shamir EUROCRYPT -1994

[2] Resolution Variant Visual Cryptography for Street View of Google MapsJonathan ,WeirWeiQi YanQueen's University Belfast Belfast, BT7 1NN

[3] Visual Cryptography for Biometric Policy, Arun Ross & Asem Othem IEEE-Information Forensics 2011

[4] User friendly random grid based Visual Secret Sharing-Tzung Chen & Kai Hsiang Tsao, National Chiayi University, Taiwan ,ROC.

[5] Fast and Efficient Visual cryptography for Medical Images-S.Manimurugan.K.Porukumaran, Anna University Coimbatore,India.

[6] Progressive Visual Cryptography with Unexpanded shares-Young Chang Hou & Zen-Yu Quan, IEEE – Information Security and Forensics.

[7] J. Daugman. "Biometric personal identification system based on iris analysis." United States Patent, Patent Number: 5,291,560, 1994.

[8] Masood, K., D.M.Y. Javed and A. Basit, "Iris recognition using wavelet". In Proceedings of the International Conference on EmergingTechnologies-ICET, IEEE Xplore Press.

Correspondence Email – team.rvcb.1@gmail.com