Securing fingerprint database using Visual Cryptography

Sachin Lonkar, Prof. Shinde S.A.

Abstract— Securing tha database of biometric system is of paramount importance due to the potential threat of access by unauthorized and unknown person. Biometrics is the science and technology of measuring and analyzing biological data. In information technology, biometrics refers to technologies that measure and analyze human body characteristics, such as DNA, fingerprints, eye retinas, irises, voice patterns, facial patterns and hand measurements, for authentication purposes. Biometric authentication is the automatic identification of living individuals by using their physiological and behavioral characteristics. Negative identification can only be accomplished through biometric identification if a pin or password is lost or forgotten it can be changed and reissued but a biometric identification cannot.

Index Terms— Fingerprint, Visual Cryptography, Minutiae, Eye retinas, Eye iris, Voice pattern.

1 INTRODUCTION

Biometrics is the science and technology of measuring and analyzing biological data. Biometric systems are becoming increasing popular due to their potential applications in various information security fields. Biometric systems involve the use of various human behavioral and physical traits such as Fingerprints, Face, Iris etc. However, the Biometric databases themselves are vulnerable for security attacks. Therefore, there is need to protect the biometric database from an unauthorized user from an unauthorized access and other malicious activities.

Visual cryptography is a cryptography technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption can be performed without using any mathematical calculations. In visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any $n - 1$ shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. In enrollment process when applying the Visual Cryptography on the fingerprint image it will create the two sheet images of the original image. One of the sheets will be store on the first database server & another sheet will be store on the second database server.

Existing systems are based on the pixel expansion methods, due to this the image quality gets degraded and it in turn affects the matching process in order to find the Minutiae points from the fingerprint image. In these methods the original fingerprint image size gets large after applying the visual cryptography technique. To solve this problem without pixel expansion technique is being used. There is need to design the system without pixel expansion method and that system will be implemented in this candidate project.

In the without pixel expansion method, we take the original fingerprint image, without expanding the pixel values we just rotate the 2x2 block of the image by 90, 180, 270, and 360 degrees respectively for doing the encryption and decryption process. In encryption process two images are created named as RS and MS2 respectively. In the decryption process, we obtain the original image from the two images RS and MS2 respectively. Without pixel expansion method does not affect the quality of the original image and the size as the expansion method does that

Basically biometric systems can be used in different fields such as

1. Commercial applications, such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit cards, physical access control, cellular phones, PDAs, medical records management, and distance learning;
2. Government applications such as national ID cards, correctional facilities, driver's licenses, social security, border control, passport control, and welfare-disbursement; and
3. Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood
   determination and missing children.

The fingerprint recognition can be grouped into three subcategories: fingerprint enrollment, verification and fingerprint identification.

The authentication phase involves combining both the sheets simultaneously in order to recover the original fingerprint image by using the EX-OR operation. After getting the original fingerprint image it will be match with the registered image. Finally display the matching result. The matching process is done using the Minutiae extraction algorithm which finds the Minutiae locations on the fingerprint. After getting that image finding the Minutiae of the target image & compare the Minutiae of the target image with the Probe image & finally display the result

whether it is match or not. Existing system secure the digital biometric data but it will makes the image size larger than the original fingerprint image. So to avoid such problem, without pixel expansion technique is used. In without pixel expansion technique it will keep the original image as it is without making the change in image size.

2 Visual Cryptography

Visual Cryptography [2] is the technique in which original fingerprint image will be encrypted into the n number of sheets. In decryption process certain numbers of sheet images are required to obtain the original fingerprint image.

Suppose consider the one example, in that original fingerprint image is F, it will be divides into the n sheets, such that,

$$F=Sh_1+Sh_2+Sh_3+\ldots..+Sh_k$$

Where + is the Boolean operation, $Sh_i \in 1, 2, 3,\ldots,k$ is the sheet images, k<n and n is the number of sheet images. It is difficult to obtain the original image F using the individual Sh_i's.

1. Basic Scheme : 2 out of 2

Every pixel of the original image will be encrypted into the two sub pixels called shears.Selection choice of shares black pixel & white pixel are chosen by the randomly. A single share cannot give the any clue about the original fingerprint image since different pixels in the original fingerprint image will be encrypted using the random choices.

When applying Visual Cryptography on the fingerprint image shown in the fig.1 it will be generate the two transparency images from the original fingerprint image shown in fig.2 and 3.

Fig.1. Fingerprint Image

Value of the original pixel P can be obtained by combining the two shares. If the original pixel is a black, then we can get the two black subpixels; if the original pixel is a white, then we can obtain the one black subpixel and one white subpixel. Therefore, the size of the obtaining image will becomes the large the original image and there will be 50% loss in contrast, but reconstructed image will be visible.

1. Securing Fingerprint Images

To securing the fingerprint images two sheets of the original image are stored on two different database servers separately. If anybody want to generate the original fingerprint image, both sheet images are required at the same time. No one can generate the original image using only the single sheet image. Fig.2 shows the transparency image 1 which will be stored on the database server first.

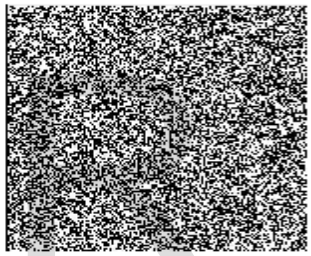

Fig.2. Transparency 1

Transparency image 2 as shown in the fig 3, it will be stored on the image database server second.

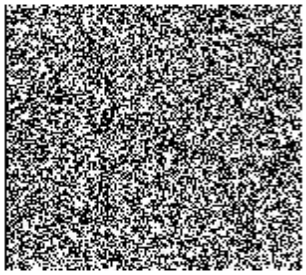

Fig. 3 Transparency 2

2. Design

The basic working of the Fingerprint recognizer System is shown in the Fig4. System takes the input as an original fingerprint image & applies the Visual Cryptography on that image. After applying the in encryption phase it will create the two sheets of the original fingerprint image.

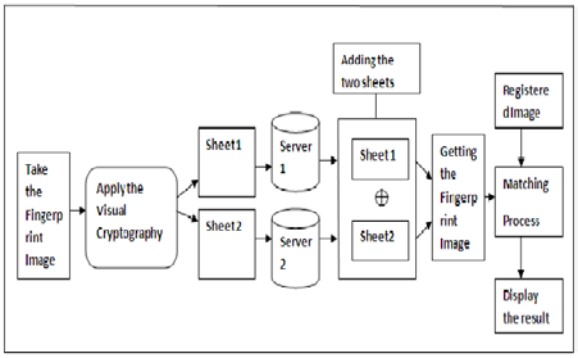

Fig.4. Architecture of Fingerprint Recognizer

Two sheets are stored on the two different database servers separately. In decryption phase it will combine the two sheets getting from the two database servers & obtain the original image. In authentication process obtained image will be matched with the registered image.

1. Minutiae Extraction

Fingerprint images are identified from the stored database on the basis of Minutiae points extracted from the fingerprint image.

Minutiae: Fingerprints are known to be unique to every individual. A Minutiae is defined as: the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings. Types of ridges:

1. Ridge endings - a ridge that ends abruptly

2. Ridge bifurcation - a single ridge that divides into two ridges.

3. Short ridges, island or independent ridge - a ridge that commences, travels a short distance and then ends.

4. Ridge enclosures - a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge.

5. Spur - a bifurcation with a short ridge branching off a longer ridge.

6. Crossover or bridge - a short ridge that runs between two parallel ridges.

Sir Francis Galton (1822-1922) was the first person who observed the structures and permanence of minutiae. Therefore, minutiae are also called "Galton details". They are used by forensic experts to match two fingerprints. Some of the Minutiae points are given in Fig5.

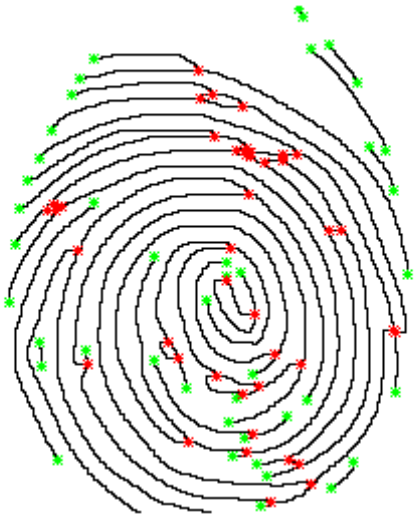

Fig.5. Minutiae Points

Minutiae have the certain number of features [10] as shown in the Fig6.

On the basis of Minutiae the fingerprint images can be matched. In matching process current fingerprint image can be matched with the registered fingerprint image. If required Minutiae count found then the matching can be found otherwise not.

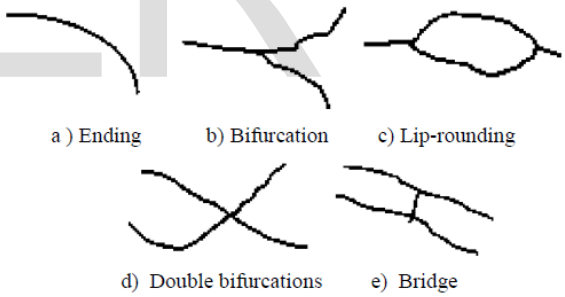

Fig.6. Minutiae Features

2. Without Pixel Expansion

In without pixel expansion technique rotating the original fingerprint image by different angles such as 90^0, 180^0 and 270^0 without doing the pixel expansions. In encryption process original image will be rotating the pixels alternately using 4x4 block of pixel that is rotate first block by 90^0 , second by 180^0 and third by 270^0 again forth by 90^0 and so on. Then convert 2x2 blocks into 2x1 blocks. If more than three pixels are black then replace block with black pixel else replace with white pixel and name that image as TEMPMS2.Then create random image RS by selecting the random pixels. Then created image MS2 by shifting the pixels of image TEMPMS2 using pixel values of RS.

In decryption process getting the pixels of MS2 and RS images from encryptions. Then shifting the pixels of MS2 image using pixel values of RS image and named it as TEMPORIGINAL. From the TEMPORIGINAL image convert block of 2x1 pixels into 2x2 pixels. If 2 pixels of block are black then replace it with black pixel block else replace it with white pixel and named it as ORIGINAL image. Then the reverse process of encryption carried out to rotate the alternate blocks of ORIGINAL image by different angles to get the decrypted image.

Some permutation combinations are given below in the Visual Cryptography. Here given the two cases:
Case 1: Fingerprint image contains 2 continues black pixels values as shown in fig7.

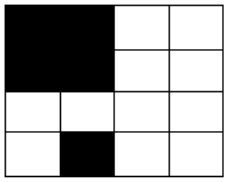

Fig.7 continues two black pixels

Fig.7 shows the original fingerprint image contains 2 continues black pixels. Applying the without pixel expansion technique on the image and generate the two transparency images. Two transparencies are combining by doing the EX-OR operation as shown in the fig. 8.

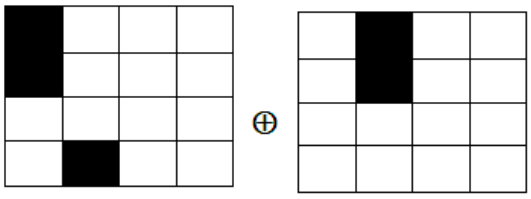

Fig.8 Output of case 1

3. RESULTS

As shown in the following fig 8, it uses the with pixel expansion technique. In this graph if we increase the number of pixels for the image encryption using the visual cryptography, automatically it increase the loss of image contrast in percentage. This increase in contrast affects the image matching process as well as to find out the minutiae points on the image. To solve the above mentioned problem using the without pixel expansion technique. This technique can remove the image matching process and reduce the loss of image contrast.

From the graph observations of both techniques pixel expansion and without

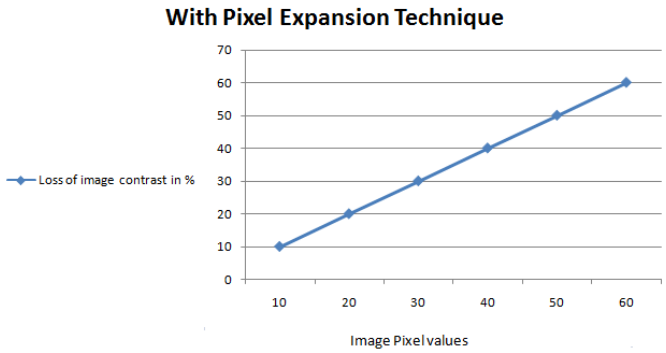

Fig: 8 With pixel expansion technique

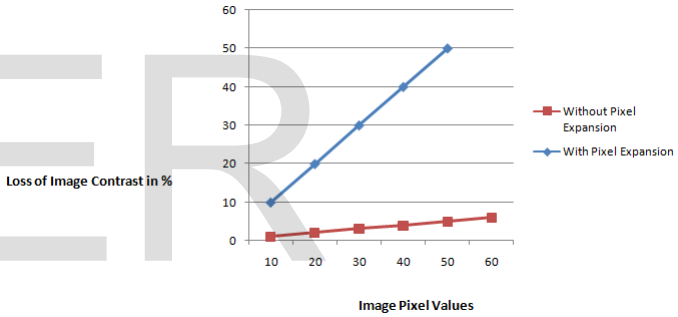

Fig: 9 Without pixel expansion technique

pixel expansion it is conclude that without pixel expansion technique is good one. Because of using the pixel expansion method we can't get the exact Minutiae points from the template image. So it will automatically affect the matching process. This issue can be solved using the without pixel expansion method. It gives us the same image quality as the original image and Minutiae points also found with greater in number for the matching process.

4. CONCLUSIONS

Biometric is the art of identifying the individuality of person on the basis of
physical and behavioral traits such as iris, face, fingerprint

and voice. General Biometric Systems works on the basis of registration, enrollment and authentication phases. The objective behind designing this system is to design the fingerprint recognizer using the without pixel expansion technique which is better one than the existing pixel expansion technique. The designed algorithm works the better in the performance and gives the better results than the existing pixel expansion technique. The implemented system gives better image quality so that fingerprint matching process becomes simple and efficient. In the pixel expansion technique image quality gets degraded due to the random pixel selection from the original image.

In the without pixel expansion technique using the 2x2 image block and rotate that block with different angles such as 90,180,270 and 360 degrees respectively. So without expanding the pixel values just rotating the pixel values that's why there is no image quality degradation and finally I get the correct fingerprint image as the original image.

5. REFRENCESES

1. Arun Ross, Asem Othman, "Visual Cryptography for Biometric Privacy," IEEE Trans, VOL.6, NO.1, March 2011.
2. Moni Naor, Adi Shamir, Visual Cryptography, Department of Math and Computer Science, Rehovot, 1994.
3. P.-C. Lin, Y.-D. Lin, Y.-C. Lai, and T.-H. Lee, Using String Matching for Deep Packet Inspection, Computer, vol. 41, no. 4.
4. W.A. Wolf and S. McKee, Hitting the Memory Wall: Implications of the Obvious, Computer Architecture News, vol. 23, no.1.
5. Z. Zhou, Y. Xue, J. Liu, W. Zhang, and J. Li, MDH: A High Speed Multi-Phase Dynamic Hash String Matching Algorithm, Proc. Ninth Int Conf. Information and Comm. Security (ICICS), pp. 201.
6. P.-C. Lin, Y.-D. Lin, Y.-J. Zheng, Y.-C. Lai and T.-H. Lee, Realizing a Sublinear Time String-Matching Algorithm with a Hardware Accelerator Using Bloom Filters, IEEE Trans. VLSI Systems, vol. 17, no. 8, pp. 1008.
7. A. Jain and U. Uludag, Hiding biometric data, IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp.1494.
8. Visual Cryptography for Biometric Privacy
Arun Ross, Senior Member, IEEE, and Asem Othman, Student Member, IEEE
9. Local Correlation-based Fingerprint Matching, Karthik Nandakumar, Anil K. Jain.
10. Minutiae Extraction from Fingerprint Images - a Review, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011
11. Yi Chen, Anil. K. Jain, Beyond Minutiae: A Fingerprint Individuality Model with Pattern, Ridge and Pore Features, June 2009.
12. ZHOU Shihai, LU Xiangjiang, Fingerprint Identification and Its Applications in Information Security Fields.
13. Yongfang Zhu, Sarat C. Dass, and Anil K. Jain, Fellow, IEEE , Statistical Models for Assessing the Individuality of Fingerprints.
14. Ching-lin Wang, Ching-Te Wang,
Meng-Lin Chiang, The Image Multiple Secret Sharing Schemes Without pixel expansion.
15. Sunny Arief SUDIRO, Michel PAINDAVOINE University of Burgundy, Dijon, France, Tb. Maulana KUSUMA Center for Multimedia Systems Gunadarma University Jakarta, Indonesia, Simple Fingerprint Minutiae Extraction Algorithm
Using Crossing Number On Valley Structure.