Secure Biometric Authentication using Visual Cryptography

Vinay Chutake
Department Of Computer Engineering, PCCOE

Nikhil Hatiskar
Department Of Computer Engineering, PCCOE

Avinash Dhas
Department Of Computer Engineering, PCCOE

Miss. Harshada Mhaske
Faculty of Computer Dept., PCCOE

***Abstract*— Nowadays there is increase in the use of biometric devices for authentication processes, as they are simple to use and there is no need to remember any password or to carry any card. But as the use of biometric devices is increased there is increased need for security to the system. In the proposed paper we use Visual Cryptography technique for enhancing the security in the biometric authentication system at the database level, as we divide the template image into two shares out of which one is on the ID card of the user and other is stored in the database. At the time of authentication user has to provide his fingerprint and ID card, so by using visual cryptography technique on a share of ID card and share in database we create template image to match with the fingerprint he has provided. This system enhances security as there we have not stored template image directly, so even if anyone hacks into database he will not get the original template image. It also reduces time and space complexity, as we have stored only one image in the database results into lowering the cost of large database i.e. lowered space complexity and as we match provided fingerprint image with only one template image instead of matching with number of images that are stored in the database in the conventional biometric authentication systems, which results in lowered time complexity.**

***Index terms*— Visual Cryptography, Image Processing, Minutiae Extraction, Biometric Authentication, Fingerprint Matching**

I. INTRODUCTION

Security has become important issue over the network, internet and in the any system, applications. As the technology is advancing there is increase in threats also. There are various application where personal identification is required such as computer login control, secure electronic banking, bank ATM, credit cards, border crossing, airport, mobile phones, military services, health and social services, etc. So for automated personal identification we use biometric authentication. Biometrics is a technology that uses physiological or behavioral characteristics to authenticate identity of persons.

Requirements for security have evolved significantly over the past decade. This project can be great deal for customer as they can demand the biometric authentication services on regular basis and on the other hand users will feel secure.

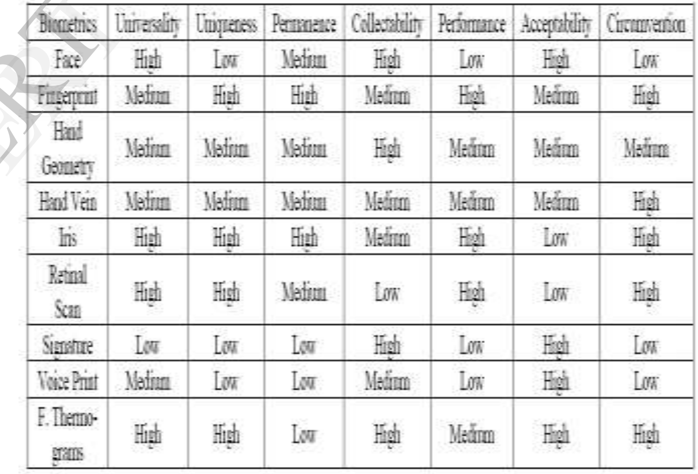
The biometric authentication system which are itself created for the security need security for itself. So to enhance the security in the biometric authentication system we can use the visual cryptography technique to encrypt the template image. In visual cryptography we divide the image in number of shares such that individual share is not understandable for the naked eyes.

II. OVERVIEW

There are various concepts are used in this project, these are explained below.

2.1 Biometric Authentication

Biometrics is the detailed measurements of the human body. It deals with automated methods of identifying a person or verifying the identity of a person based on physiological or behavioral characteristics. A comparison of some biometric techniques made by A. Jain et al. in 1997 is provided in following figure 1. [2]



Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	Medium	Low	Low	Medium	Low	High	Low
F. Thermo-grams	High	High	Low	High	Medium	High	High

Fig. 1: Comparison of different biometric techniques

Based on above comparison chart, we can see that it is effective to use finger print and iris for the security reasons. As we can use this project to encrypt template image of any biometric authentication system, it may be iris or finger print. But there are many existing devices are available for finger print recognition for biometric authentication than the iris recognition. So it is efficient to use fingerprint authentication. As per the study done for the number of existing devices on the biometric authentication, there are more number of finger print authentication system than any other type of biometric device. This shown in following graph in figure 2. [4]

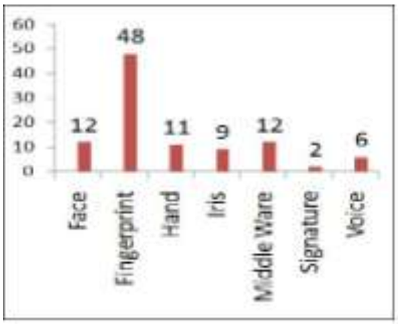


Fig. 2: Comparison of different techniques used in Biometric devices (in percentage)

Although, these biometric devices are used for security but they need security as well. Existing biometric authentication devices are vulnerable to many attacks. These attacks can be shown in following figure 3. [1]

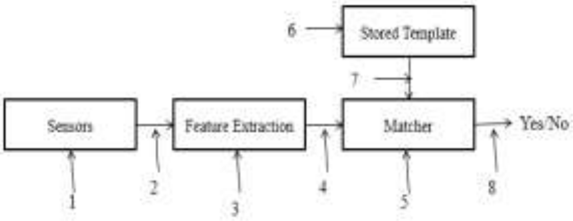


Fig. 3: Possible attacks on existing biometric devices

As we can see in figure above there are 8 positions where attacks can be done. As Nalini K. Ratha et al[3] pointed out that the stored template in the database attacker may try to alter result in authorization for a unauthorized users, or denial of service for the authenticated user related with the corrupted template. In proposed system we are enhancing the security by introducing the visual cryptography technique to the stored template.

2.2 Visual Cryptography

Visual cryptography (VC) is a secret-sharing scheme that uses the human visual system to perform the computations. Naor and Shamir introduced Visual Cryptography (VC) in 1994 [1] .Examination of one share should reveal no information about the image. Naor and Shamir devised the scheme that specifies how to encode a single pixel, and it would be applied for every pixel in the image to be shared. This scheme is illustrated in the figure 4 given below.

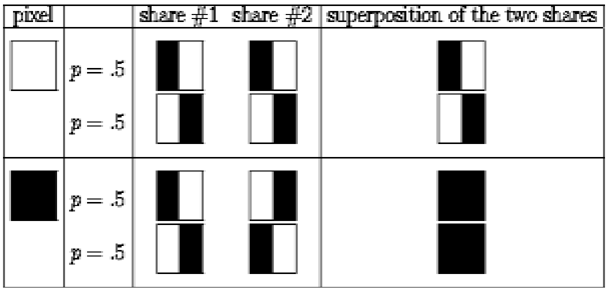


Fig. 4: Pixel transformation in encryption using Visual Cryptography technique

A pixel P is split into two sub pixels in each of the two shares. If P is white, then a coin toss is used to randomly choose one of the first two rows in the figure above. If P is black, then a coin toss is used to randomly choose one of the last two rows in the figure above. Then the pixel P is encrypted as two sub pixels in each of the two shares, as determined by the chosen row in the figure. Every pixel is encrypted using a new coin toss.

Suppose we look at a pixel P in the first share. One of the two sub pixels in P is black and the other is white. Moreover, each of the two possibilities "black-white" and "white-black" is equally likely to occur, independent of whether the corresponding pixel in the secret image is black or white.

Thus the first share gives no clue as to whether the pixel is black or white. The same argument applies to the second share. Since all the pixels in the secret image were encrypted using independent random coin flips, there is no information to be gained by looking at any group of pixels on a share, either. This demonstrates the security of the scheme.

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). It involves breaking up the image into n shares so that only someone with all n shares could decrypt the image by overlaying each of the shares over each other.

As we can see in the figure below, original image is encrypted into the two shares by using visual cryptography and as we can see these shares are not understandable to the naked eyes but by decrypting them we can again get the original image.

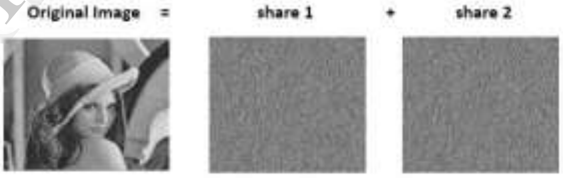


Fig. 5: Image transformation using visual cryptography technique

2.3 Minutia Extraction

Minutiae means small or precise meaning of something, Here that something is fingerprint. We are extracting the required information from the fingerprint which is needed in the matching process of two fingerprints. We are referring that information as minutiae points in fingerprint. These minutiae points are shown in figure 6.

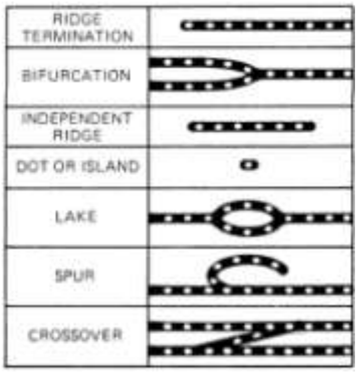


Fig. 6: Minutiae points in fingerprint

In minutiae matching process we intend to match the two fingerprint by matching the minutiae of that images. Following figure 7 shows the marked minutiae in the fingerprint image.

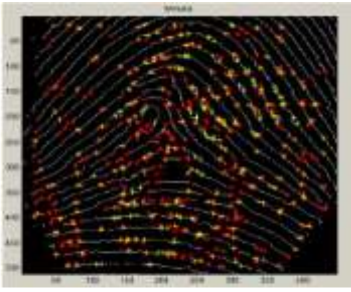


Fig. 7: Minutiae marking on fingerprint

III. PPROPOSED SYSTEM

The proposed system is mainly divided into two parts. First is enrollment, in which admin creates shares by enrolling employees fingerprints. And the second part is related to the authentication which is required to be done by employee. These two parts are explained below.

3.1 Enrollment

In the enrollment part, the administrator will collect the eye image of the eligible users those are having access to secure resource. The enrolled eye image is required to be processed so characteristic fingerprint features can be extracted and are divided in to two shares. Among these shares first share is stored on the user's identity card and other is saved in the database. So next time when user comes for authentication he need to provide his ID card and finger print as he is already enrolled in the system.

Data flow diagram for the enrollment part is shown in the figure 8 below.

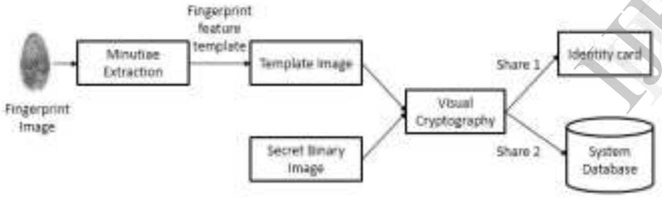


Fig. 8: Data flow diagram of enrollment process in proposed system

As we can see in the figure above, Minutia extraction module is used to extract the feature and by using visual cryptography technique we created the shares and stored on ID card and database.

3.2 Authentication

Authentication part of the proposed system is related to the each time authentication done by the enrolled user of system or employee. In this he has to provide ID card allocated to him and his fingerprint in order to complete authentication. As there is one share saved on ID card and other is in the database when user provides ID card, By using the share on the ID card and other share in the database we create the temporary image which have the features from the original image which was provided during the enrollment of user. This temporary image is then matched with the fingerprint which is provided in the authentication. Which then provides result as either authenticated or not.

The data flow diagram for authentication part is shown in figure 9 given below. In which we have used visual cryptography and minutiae extraction technique.

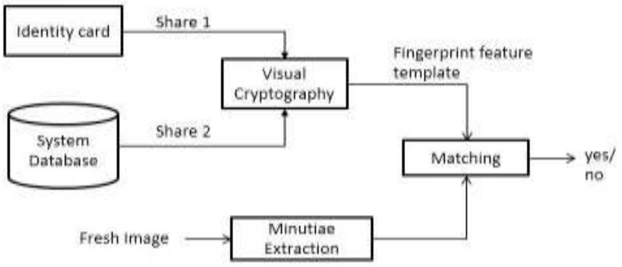


Fig. 9: Data flow diagram of authentication process in proposed system

IV. PRODUCT FEATURES AND CONCLUSION

Proposed system will provide certain advantages such as reduced time complexity, reduced space in database, security enhancement which are explained below.

4.1 Security enhancement

In the existing biometric authentication system there are many vulnerabilities and possible attacks. So in the proposed system we are using the visual cryptography technique so instead of original image only one share is saved in the database. Even if there is attack on the database, attacker will not get original image instead he will get share of image which is not understandable to the naked eyes.

If attacker successful to penetrate system and he tries to change the share in the database, this will result in the crash of system. As there is only one share in database and for every user to successfully authenticate it is required that his share on ID card should combine with share on database. If that share is changed by attacker then no one will get authenticated resulting into recognition of attack. Thus security is enhanced.

4.2 Reduced time for authentication

In existing biometric authentication system there is need to match fingerprint image with all existing images in the database. But In the authentication process of proposed system we are matching the fingerprint which is provided at the time of authentication with the temporary image which is created using visual cryptography. Here we need to match fingerprint with only one image instead of matching with the all images. So time for authentication is reduced.

4.3 Reduced storage space

In the existing biometric authentication systems, there is need to save all the fingerprint images of all users in the database for matching process but in the proposed system we are storing only one image of share. So results in reduced space for storage.

REFERENCES

[1] P. S. Revenkar, Anisa Anjum, W. Z. Gandhare "Secure Iris Authentication Using Visual Cryptography" (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No.3, 2010.

[2] Moni Naor and Adi Shamir, "Visual cryptography" .In Proceedings of the advances in cryptology– Eurocrypt, 1-12,1995.

[3] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle, "An Analysis of Minutiae Matching Strength". In Proceedings of the 3rd AVBPA, Halmstad, Sweden,223-228 ,June 2001.

[4] Moses Okechukwu Onyesolu, Ignatius Majesty Ezeani "ATM Security Using Fingerprint Biometric Identifer : An Investigative Study". (IJACSA) International Journal of Advanced Computer Science and Applications,Vol. 3, No.4, 2012.

[5] Le Hoang Thai and Ha Nhat Tam “Fingerprint recognition using standardized fingerprint model” IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010.

[6] Roli Bansal, Priti Sehgal and Punam Bedi “Minutiae Extraction from Fingerprint Images - a Review” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, September 2011.

[7] Sonali Patil, Kapil Tajane, Janhavi Sirdeshpande “SECRET SHARING SCHEMES FOR SECURE BIOMETRIC AUTHENTICATION” International Journal of Scientific & Engineering Research, Volume 4, Issue 6, June-2013.

[8] Philippe Parra “Fingerprint minutiae extraction and matching for identification procedure” University of California, San Diego La Jolla, CA 92093-0443.

[9] Smital D.Patil and Shailaja A.Patil “Fingerprint recognition using minutia matching” World Journal of Science and Technology 2012, 2(4):178-181 ISSN: 2231 – 2587.