Implementation of Data Security Using Biometric Encryption

Himanshu Gupta [1], Yash Mangla[2]

[#] *Amity Institute of Information Technology, Amity University Uttar Pradesh, Noida, India*

[1]hgupta@amity.edu
[2]yashtruefriend@gmail.com
Noida, India

***ABSTRACT*---The logic of this paper is execution of data security using Biometric Encryption. This paper provides an overview of different biometric technique with some advantages and disadvantages. The comparison criteria for the techniques presented is limited to acceptance, accuracy, performance and cost. Single biometric encryption have many problems such as data error, spoof attack. These limitations can overcome by using multimodal biometric systems. Multimodal biometric systems is combination of two biometric traits utilize , like face, iris,retina and fingerprint. Multimodal biometric systems improve the quality and accuracy of security.**

***KEY WORDS*---- Data Security, Iris, Fingerprint, Biometric**

I INTRODUCTION

In today's environment Security is a key feature in every field. Security is also a necessary part for database. Databases also have some issues related to security. According to author these issues can be resolved by Biometric Technique. We use ID and password to gain access in a secure area. But these things can easily be hacked. A biometrical system makes personal identification by learning users physiological or behavioral characteristics. Thus biometric technologies defined as method which identify or authenticate the identity of a living person by behavioral characteristic. There are various ways which treat as biometric characteristics .In all these biometric traits some traits perform better than the other. The Accuracy of several biometric traits is measured with some experimental results. We do study of two biometric combination which make data security more secure and reliable. Two traits are used in these researches which are fingerprint and iris.

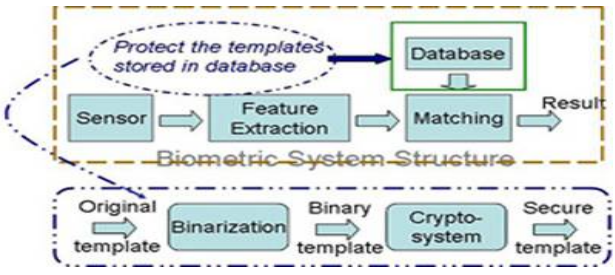

Fig. 1 Biometric Encryption process

II REVIEW OF LITERATURE

Here the author has discussed some research papers which previously discussed in the field of biometric system:

Mary Lourdes R had explained an issue for the selection of a particular algorithm which matches the fingerprint with an accuracy and good performance. Srinivasulu Asadi has discussed some face recognition techniques by some test samples. Khattab M. Ali has used histogram equalization and wavelet techniques for the implementation of iris recognition algorithm. Tiwalade O.Majekodunmi, Francis E.idachaba had explained about four biometrical traits i.e. fingerprint recognition, face recognition, iris recognition and speaker recognition with their individual advantages and disadvantages.

III MODE OF BIOMETRIC SYSTEM

Biometric authentication system has two operational modes. First mode is enrolment process and the second mode is authentication process. The authentication process is also divided into two process these are the verification process and the identification process. Further the identification process is divided into two identifications. These are positive identification and negative identification. Below we explained all these modes in detail.

ENROLMENT PROCESS

When an individual uses a biometric system first time then it is called as enrolment of user. Here biometrical information about individual is stored. And for gaining information a sensor is used which work as an interface between the real world and the system. When the information detected by sensor then it is compared with the information which are already available in the system. The second block performs several pre-processing as to remove old objects from the sensor for the

improvement of input like removing background noise. The third block extracts significant features. The third block is an important block because the correct features need to be extracted in the best way. A template is a construction of applicable characteristics which are extracted from the source. For the creation of template an image is used with particular properties. Elements which are not used in the comparison algorithm are throw away in the template to reduce the file size.

AUTHENTICATION PROCESS

The second operational mode of biometric authentication system has these two following modes. First one is verification mode and the second one is identification mode. In verification mode the system performs a one-to-one comparison between the biometric trait captured and the specific template available in biometric database for the verification of individual. Verification of individual mean the person which is declared is same or not

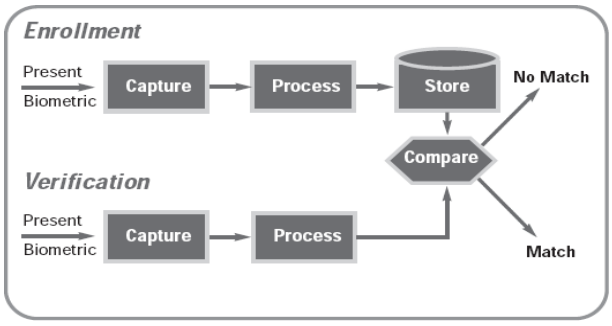

Fig. 2 Enrolment Process

IV PROPOSED SYSTEM

The biometrics technology have multiple traits available.. From these all biometric traits all have their advantages and disadvantages. Ross and Jain proposed the concept of multimodal biometric system where we use more than one biometric trait to arrive at a final decision. This helps to overcome from the unimodal system issues. In multimodal biometric system rather than binding strategies different levels of integration are also presented. Here we know whether we can achieve higher performance by the integration of face and palm print biometric traits. With the unimodal system higher performance is not possible.. With this performance increased significantly. Fusion of iris and fingerprint biometric traits are presented in this paper. At the time of iris image addition problem can generate where users have to co-operate while giving iris image. At the time of fingerprint identification a poor quality of fingerprint image may generate problem. Thus in proposed system two biometrical traits combined at score level and identification of individual person is done.

V IRIS RECOGNITION

Iris is exceptional to every person and stays steady over the life of an individual. Iris recognition is a method of biometric authentication that uses pattern recognition technique.: Iris systems have a very low False Accept Rate (FAR) compared to other biometric traits.various steps for the iris recongnition process are

1. Iris Segmentation
2. Iris Localization:
3. Normalization
4. Feature Extraction

VI IRIS SEGMENTATION

This involves first employing Canny Edge Detection to generate an edge map

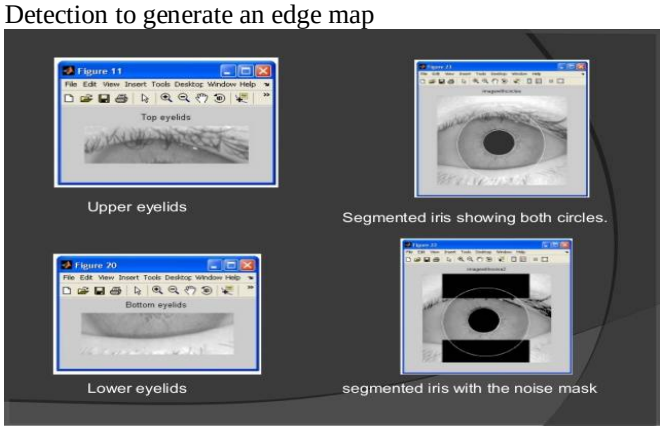

Fig. 3 Steps involved in iris segmentation

IRIS LOCALIZATION

circle detection algorithm is used in iris localization.
Circle detection has following advantages

a. recognition speed is good
b. performance recongization is good
c. Accuracy level is high
d. Simple method
e. Efficient method

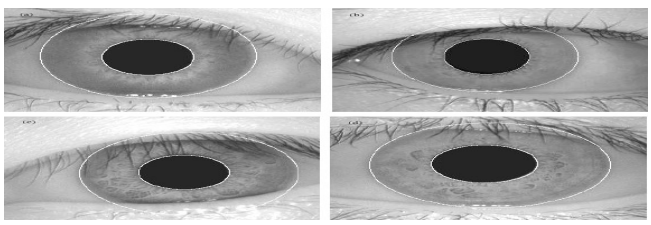

Fig. 4 Steps involved in iris localization

NORMALIZATION

Pupil size may change because of the variation in illumination and the associated elastic deformations in the iris texture may interface with the results of pattern matching. This deformation compensate is necessary for accurate texture analysis. . Mapping the iris ring to a rectangular block of texture of a fixed is easy as it detected both inner inner and outer boundaries of the iris

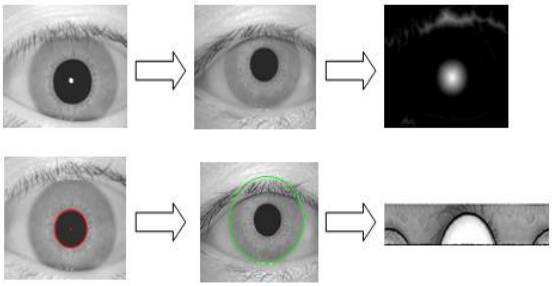

Fig. 5 Steps involved in iris preprocessing and normalization

FEATURE EXTRACTION

The primary function of features is to highlight the unique characteristics from any image. The process used to bring out the Features from the iris image is known as Haar Wavelet decomposition process in which the general procedure adopted is the decomposition of the iris image into four different coefficients-

a. Horizontal
b. Diagonal
c. Vertical
d. Approximation- on its decomposition four more coefficients are brought out.

To form a vector it is essential that certain major steps be repeated for five levels in which the last level coefficients form a vector. For practical purposes and for convenience the combined vector is binarized in form of 0 and 1. It helps in comparing between the iris codes for database and query image and also in matching module

$$IC(i) = \begin{cases} 1 & FV(i) \geq 0 \\ 0 & FV(i) < 0 \end{cases}$$

VIII FINGERPRINT RECOGNITION

It is one of the most useful and popular biometric trait for identification purpose. There are few steps for any finger recognition which are as follows-

a. Image Enhancement
b. Minutiae Extraction
c. Matching

IMAGE ENHANCEMENT

It is mainly used to improvise the quality of any fingerprint image which might have been corrupted either by some noise or any mark or holes. Such normalized fingerprint image is divided into recoverable and unrecoverable block. However the unrecoverable regions cannot be improved. The process adopted for improvisation is divided into two steps:

a. Firstly, Normalize input finger image
b. Secondly, orientation image is evaluated from the input fingerprint image
c. Thirdly, frequency image is computed

MINUTIAE EXTRACTION

$$CN = 0.5 \sum_{i=1}^{8} |P_i - P_{i+1}| \quad (4)$$

$$P_9 = P_1$$

where Pi = the pixel value in the neighborhood of P. Now the pixel can be classified by the CN value.

IX FUSION

Fusion is a very important part in biometric encryption. Fusion of two biometric traits provides more accuracy than individual traits. . In this paper the fusion of iris and fingerprint biometric traits are presented.. At the time of iris image addition problem can generate where users have to co-operate while giving iris image. At the time of fingerprint identification a poor quality of fingerprint image may generate problem. Thus in this paper two biometrical traits combined at score level and identification of individual person is done.

X MATCHING

A comparison is drawn out between iris codes (IC) and query images to understand whether the input and modal image are from the same class. For this purpose, hamming distance approach is used which mainly points out the contrasts between the bits of two codes which are then counted as well as divided by the total number of such comparisons.

.

$$MS_{Iris} = \frac{1}{N}\sum_{i=1}^{N} A_i \oplus B_i \qquad (3)$$

.

XI EXPERIMENTAL RESULTS

Apply a experiment on 200 persons where the database have record of four iris images (70×3) and two fingerprint images (70×3) per person. Acquire the iris image with the help of CCD camera by the uniform light source. However, Acquire the fingerprint images by the use of an optical fingerprint scanner.. At first level individually test both the iris and fingerprints algorithms. From the individual result design an accuracy curve as bellow in figure 1. Here iris individual score is 94.36% and fingerprint individual score is 92.06%.

To increase whole biometric system result accuracy we combine both the iris and fingerprint score at the Matching score level (MS). At the second level combine the individual biometric traits matching score and plot an accuracy graph as in figure 2.

The overall performance in terms of accuracy is increased . and result is 96.04% with FAR of 1.58% and FRR of 6.34% respectively.Accuracy graphs for individual and combined classifier are shown below

Where,
ROC= Receiver operating characteristic
GAR= Genuine acceptance rate
FAR= False acceptance rate

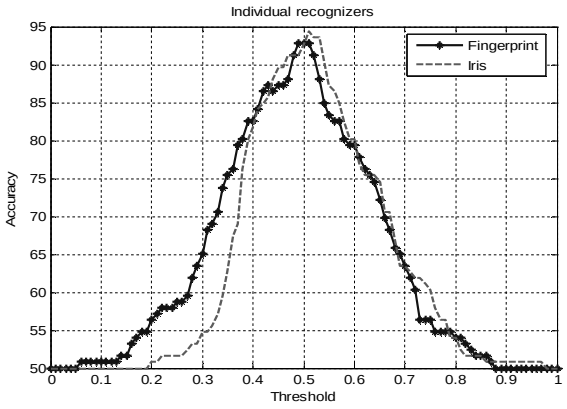

Fig 6 Accuracy plots of individual recognizers

Trait	Algorithm	Accuracy (%)	FAR (%)	FRR (%)
Iris	Haar Wavelet	94.36	4.85	6.43
Fingerprint	Minutiae Matching	92.06	3.17	12.69
Fusion	**Haar + Minutiae**	**96.04**	**1.58**	**6.34**

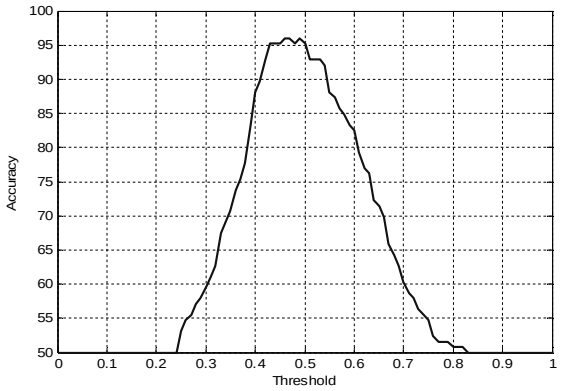

Fig. 7 Accuracy graph for combined classifier

Table 1 Figures showing individual and combined accuracy

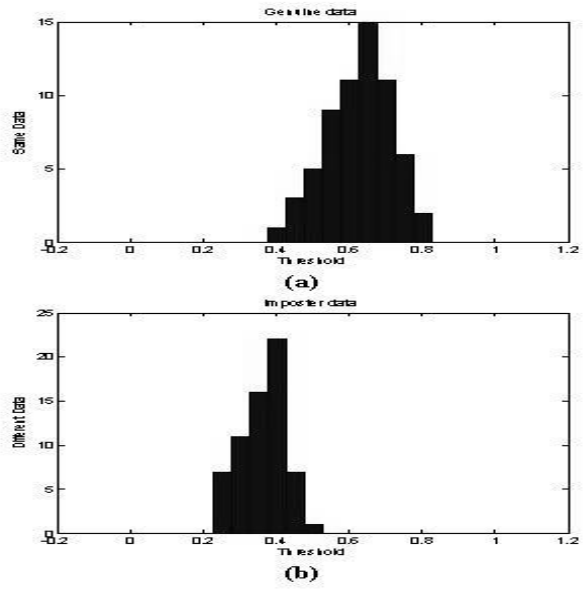

Fig. 8 ROC Curve for Fingerprint, Iris and Fusion

FIG. 9 HISTOGRAM FOR (A) GENUINE AND (B) IMPOSTER SCORES

XII CONCLUSIONS

This paper present about the data security using different biometric techniques, we studied different types of biometric techniques with their advantages and disadvantages. In this paper the primary center is given on looking at different methods of biometric as per exactness, cost, false acknowledge rate and reject rate and so on. After that we leant about the fusion of two biometric techniques to getting the best result to secure the data . We stuied about fusion of two biometric techniques which are iris and fingerprints to get the best accuracy for data security.

References

[1] A. Ross, & A. K. Jain, Information Fusion in Biometrics, Pattern Recognition Letters, 24(13), 2003, 2115-2125.

[2] W. Yunhong, T. Tan, & A. K. Jain, Combining Face and Iris Biometrics for Identity Verification, Proceedings of Fourth International Conference on AVBPA, Guildford, UK, 2003, 805-813.

[3] S. C. Dass, K. Nandakumar, & A. K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA), Rye Brook, NY, 2005.

[4] G. Feng, K. Dong, D. Hu, & D. Zhang, When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy, International Conference on Bioinformatics and its Applications, Hong Kong, China, 2004, 701-707.

[5] J. Kittler, M. Hatef, R. P. W. Duin, & J. Mates, On combining classifiers, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20(3), pp. 1998 226–239,

[6] HunnyMehrotra, AjitaRattani, Phalguni Gupta, Fusion of iris and fingerprint biometric for recognition, Indian Institute of Technology Kanpur, India – 208016

[7] Phalguni Gupta, AjitaRattani, HunnyMehrotra, Anil Kumar Kaushik, Multimodal Biometrics System for Efficient Human Recognition, Indian Institute of Technology Kanpur, India – 208016.

About Author

Himanshu Gupta is a Senior Faculty Member in Amity Institute of Information Technology, Amity University,Noida, India. He is having prestigious membership in various famous and reputed Technical and Research organizations such as CSTA (USA), Computer Society of India (India), TIFR (India), IACSIT (Singapore), UNESCO (Paris) and IEEE Computer Society (USA). With specialization in Network Security & Cryptography. He has successfully filed a patent ―A Technique & Device for Multiphase Encryption under the domain area of Network Security & Cryptography in the field of Information Technology. He has attended many National and International

Seminars, Workshops & Conferences and has been presented many research papers in the field of Information Technology. He has visited many countries as Malaysia, Singapore, Bangkok and Cambodia for the academic and research purpose. He has been delivered many technical sessions in the field of Network Security & Cryptography

Yash Mangla is a Post Graduate student pursuing Masters in Computer Application from Amity University, Noida. He is working with wipro as a Software Engineer Trainee .