A Study on Biometric Authentication

B. R. Swetha[1] Dr. S. Venkatesh Kumar[2]
[1]Student [2]Associate Professor
[1,2]Department of Computer Application
[1,2]Dr.SNS Rajalakshmi College of Arts & Science, Coimbatore-641049, India

Abstract— Biometric is a technical term related to human uniqueness. It is a term that describes about the body measurements and calculations of individual person. Biometrics is predefined set of technique used for identifying a particular person based on their physiological and behavioral characteristics. Face, fingerprint, hand geometry, iris, retinal, signature and voice are the various features measured for the authentication purpose. Biometric authentication is becoming the foundation for safe identification and personal confirmation. As the intensity of protection breach and business scam increase, the need for very safe identification and particular verification technology is becoming evident.

Key words: Recognition, Facial, Iris, Voice

I. INTRODUCTION

Biometrics allows a person to be recognized and authenticated based on a set of identifiable and verifiable data, which are unique and specific to them. Biometric encompasses:

1) Biometric authentication
2) Biometric identification
3) Physiological measurements
4) Behavioral measurements
5) Access control

Biometric authentication refers to the use of different physiological characteristics of a human like fingerprint identification, face recognition, retinal scanning, hand geometry recognition, iris recognition, etc. and behavioral characteristics such as voice recognition, giat recognition, signatu recognition etc. They are called the biometric identifiers or biometrics. For authentication purpose these features are used in computer based security system. The recognition of a person is becoming very essential as the ID cards, username, secret password and PIN which are used for the personal identification need to be secured. The ID can be stolen by someone and the PIN Number can be forgotten but the biometric techniques can overcome all these issues. The biometric authentication method offers a range of advantages over conventional authentication system. The problem of information security gives protection of information ensuring only authorized users are able to access the information. This methodology requires the person being authentic to be present at the point of authentication .Thus biometric authentication methods are the most secure methods.

II. TECHNIQUES

The purpose of biometrics system is to uniquely identify or verify an individual person through the characteristics of their body. There are several biometric technique used for identification purpose which are mainly divided into two category i.e.

– Physiological characteristics

1) Fingerprint Recognition
2) Iris Recognition
3) Retinal Recognition
4) Facial Recognition
5) Hand Geometry

– behavioral characteristics

1) Voice Recognition
2) Signature Recognition

A. Fingerprint Recognition

Fingerprint recognition is a methodology where an individual's fingerprint is defined by a combination of patterns like lines, arches, loops and whorls. In this technique the image of a person's fingertips is taken and its characteristics are recorded. In this process the user presses his finger on a small reader surface. The time of verification is less than 5 seconds and the size of reader is about 2 inch square. The computer is the reader and it takes the information from the scanner and sends it to the database and it compares with the information searching for matches.
If no matches are found then the user is authenticated.

B. IRIS Recognition

Iris scans the coloured tissue surrounding the pupil. In this technique, the user places him so that he can see the reflection of his own eye on the device. Unlike the retinal scanner, the iris scanner can be placed 12 to 18 inches apart from the person who is using it. The Verification time is generally less than 5 seconds as the user only need to look into the device for a couple of moments. In comparison this is stored version of the user's iris pattern stored on the user's identification card or in a central database. This database is a collection of images which contain iris region of the eye and the images are stored by sensor that operates in visible spectrum. If match occurs then user is authenticated.

C. Retinal Scanning

Retinal scanning examines the layer of blood vessels at the back of the eye. Scanning involves a low-intensity light source and an optical coupler and can read the patterns at a great level of accuracy. In this technique, the user looks through a small opening in the device at a small green light and requires the user to remove glasses, place their eye close to the device. After doing this the user has to focus on a certain point for few seconds during that time period the device will verify his identity. Then this profile is compared to a profile stored on the central database. If match occurs then user is authenticated.

D. Facial Recognition

Facial recognition technique analysis the uniqueness of a person's face images using a digital video camera. It measures the complete facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are saved in the database and used as a comparison when a user

stands before the camera. This technique is now used in verification systems only with a good deal of success. In this technique, the user faces the camera by standing about two feet away from it. The user's face is located by the system and then match is performed against the claimed identity or the facial database.

E. Voice Recognition

Voice recognition systems use characteristics of the voice like pitch, tone, frequency, etc. This method mainly focus on the difference which are resultant from the shape of vocal tract and learned speaking habits.

In this technique, the user should speak a specific word into a microphone attached to the system. Software examines his or her voice and extracts significant quantity on roughly twenty parameters like pitch, speech, energy density, waveforms, etc. This live profile is correlated against a profile stored on a central database where whole data is stored. If a good match occurs then user is authenticated. Voice recognition is easy to use and it is one of the simplest technique.

F. Signature Recognition

Signature recognition is one of the least effective biometric authenticator. The text involved in a signature is continuous and regular in nature. In this methodology the user signs on a tablet or on the paper which is placed over a sensor tablet. The device records the signature of the user and compares it to its database and the verification takes about 5 seconds. The technology is promoted by low-cost, writing tablet and this technology significantly improves the cost efficiency of this biometric without suffering an adequate loss in the capacity of the biometric to carry out at an high accuracy levels. This technology is very cheap, non-intrusive, high user acceptance and require low training but it changes over time and has low distinctiveness.

G. Hand Geometry

In this technique, the user places the palm of his hand on a metal surface, positions his or her fingers according to a set of pins on the device and waits approximately for 1.2 seconds. The hand is properly aligned so that the device can read the hand attributes. Then the database is checked by the device where whole information of the user is stored for verification of the user. This process usually takes less than 5 seconds. This technique becomes popular in small organizations because of its low cost and high performance.

EXAMPLE: Biometric Security Techniques for IRIS Recognition System

III. METHODOLOGY

1) Iris features and process.
2) Capturing the image.
3) Iris localization.
4) Polar Transformation.
5) Matching Process

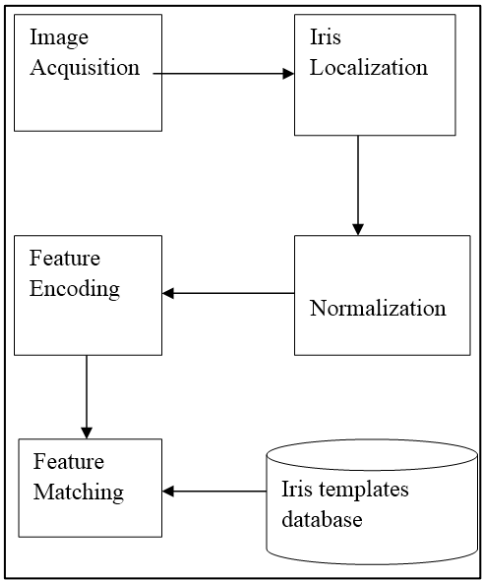

Fig. 1:

A. IRIS Features & Process

The iris recognition technology has a range of features that helps us to make a distinction between one iris from another. One of the most important evident feature is called the trabecular meshwork. This is a tissue that gives an appearance of isolating the iris in a radial fashion that is eternally formed in the eighth month of gestation. The reality of this technology is that the iris is sheltered behind the eyelid, aqueous humor and cornea which means that, unlike other biometrics such as fingerprints, face recognition the possibility of scratch and/or scrape is said to be minimum. The important feature of iris is the effects of aging which means it remains in a constant form from concerning the age of one until their death. It has little consequence of the use of glasses and contact lens on the representation of the iris and hence does not get in the way with the detection technology.

B. Capturing the Image

To capture the iris of a person the human eye should be placed 9 cm far away from the camera. The halogen lamp should be in a fixed position to get the similar illumination result over all the images, thus not including the illuminated part from the Iris. Getting the Iris Code is easier to obtain more comprehensible images through a CCD camera and it also minimizes the cause of the reflected lights caused by the surrounding illumination, we place two halogen lamps as the surrounding lights and the two halogen lamp should be in front of the eye.

1) IRIS Localization

Both the inner boundary and the outer boundary of a typical iris can be considered as circles for iris localization. But the two circles are usually not co-centric. Compared with the other part of the eye, the pupil is much darker. We detect the inner boundary between the pupil and the iris by means of thresholding. It is more difficult to detect the outer boundary of the iris because of the low contrast between the two sides of the boundary. The outer boundary of the iris can be detected by maximizing the changes of the perimeter-normalized by the sum of the gray level values along the circle. The technique is said to be resourceful and valuable.

C. Polar Transformation

After iris localization the localized iris part from the image should be changed into polar coordinates system. Locating iris in the image delimit the circular iris zone of examination by its own inner and outer boundaries. The Cartesian to polar reference convert authorizes equivalent rectangular illustration of the zone of interest as shown in the figure. This way how we compensate the stretching of the iris quality as the pupil changes in size, and we unfold the frequency information controlled in the circular texture in order to smooth the progress of next features extraction. Moreover this new representation of the iris breaks the no eccentricity of the iris and the pupil.

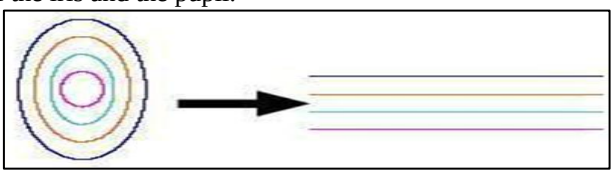

Fig. 2: Polar Transformation

D. Matching Process

To measure the variation between the Iris Code recorded from the presented iris and each Iris Code recorded in the databases, calculation of Hamming Distance (HD) is used.
Let Aj and Bj be two iris codes to be compared, then the Hamming distance function can be calculated as:

$$HD = \frac{1}{87}\sum_{j}^{87}(A_j \oplus B_j)$$

(The exclusive-OR is a Boolean operator that equals one if and only if the two bits Aj and Bj are different

IV. Conclusion

Biometric authentication is an automated identification of persons based on their behavioral and biological individuality. It relies on the assumption that individuals are physically and behaviorally unique in a number of ways.

Biometric system are considered to be useful to distinguish individuals and control access to physical spaces, information, services and to other rights or benefits, including the ability to cross international restrictions. The motivation for using biometric authentication technology is diverse and often has common characteristics. The convenience and also the efficiency of regular access transactions, reducing fraud and enhancing public safety and national safety is increased by the use of biometric authentication.

Biometric systems are essentially useful for authentication purpose and hence naturally perfect. The chance of error can be made small but cannot be eliminated. System designers and operators should anticipate and plan for the accuracy of errors, even if errors are expected to be infrequent.

References

[1] Alessandra Lumini and Loris Nanni "when Fingerprint are Combined with Iris- A case Study: FVC2004 and CASIA" published in the proceeding of Network Security, Vol.4, No.1, PP.27-34, Jan. 2007.
[2] Srinivasulu Asadi, Dr. Ch. D. V. Subba Rao, V. Saikrishna "A Comparative Study of Face Recognition with Principal Component Analysis and Cross – Correlation Techniques" published in the proceeding of international journal of computer application, Vol. 10, NO-8, November 2010, ISSN 0975-8887.
[3] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," IEEE Transactions on Computers, vol. 55, pp. 1081-1088, 2006.
[4] A.K. Jain, A. Ross and U. Uludag, "Biometric template security: Challenges and solutions", Proceedings of 13th European Signal Processing Conference (EUSIPCO), 2005.
[5] G. Kee, Y. Byun, K. Lee and Y. Lee, "Improved Techniques for an Iris Recognition System with High Performance" Lecture Notes Artificial Intelligence, LNAI 2256, pp. 177-181,2001.
[6] G.O. Williams, "Iris Recognition Technology" IEE Aerospace and Electronics Systems Magazine, vol. 12, no. 4, pp. 23-29,1997.
[7] J.G Daugman, "Biometric Personal Identification System based on Iris Analysis" U.S. patent 5, 291,560, March 1, 1994.

