Indian J.Sci.Res. 17(2): 108 - 110, 2018 ISSN: 0976-2876 (Print)
ISSN: 2250-0138(Online)

HUMAN BEING PHYSIOLOGICAL CHARACTERISTICS IN BIO-METRIC SECURITY SYSTEM

[1] Kanchanapally Anil Kumar
[1] Software Developer, ICRISAT, Patancheru, Hyderabad.

Abstract - Biometric technology that involves the identification and verification of individuals by analyzing the human Physiological characteristics has been widely used in various aspect of life for different purposes, most importantly as regards this study the issue of employee attendance and security in organization. The main aim of this paper is to develop an accurate, fast and very efficient automatic attendance system using Human Physiological characteristic verification technique. We propose a system in which Human physiological characteristics verification is done by using extraction of minutiae, Iris, Palm Scanning technique and the system that automates the whole process of taking attendance. The Biometric Security based on human Physiological characteristics identifier was found suitable for the employee attendance management system of the organization.

***Keywords*:** Biometric, Physiological Characteristic, minutiae, Iris and Palm.

I.Introduction

Recently, biometricfeatures have been widely used in many personal authenticationapplications because they possess the following physiologicalproperties: universality,uniqueness, permanence, collectability, performance, acceptability, and circumvention. According to the aboveproperties,manyaccesscontrolsystemsabiometricfeatu retoreplacethedigitbasedpassword and registers…etc.

Biometric Security system is playing an important role where security, accuracy is crucial. Based on Human being's physiological characteristics now a day's latest biometric devices are manufacturing. Human being characteristics like

- Fingerprint,
- Iris / Retina,
- Palm.

Below we can know about Physiological characters:

1. Fingerprint Identification

Fingerprints are made of a series of ridges and furrows on the surface of the finger and have a core around which patterns like swirls, loops, or arches are curved to ensure that each print is unique.An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the other side of the finger. The loop is a pattern where the ridges enter from one side of a finger, form a curve, and tend to exit from the same side they enter. In the whorl pattern, ridges form circularly around a central point on the finger.

The ridges and furrows are characterized by irregularities known as minutiae, the distinctive feature upon which finger scanning technologies are based. The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.

Fig 1: Types of fingerprints

There are five stages involved in finger-scan verification and identification:

- Fingerprint Image Acquisition.
- Image Processing.
- Locating Distinctive Characteristics.
- Template Creation.
- Template Matching.

A sensor takes a mathematical snapshot of the user's unique pattern, which is then saved in a fingerprint database. A fingerprint enhancement algorithm is included

[1]Corresponding Author

in the minutiae extraction module to ensure that the performance of the system is not affected by variations in quality of fingerprint images.One of the main difficulties in the minutiae-based approach is that it is very difficult to reliably extract minutiae in a poor quality fingerprint image.

The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is not entirely genetically determined and thus even identical twins do not share a similar pattern.

The human retina is a thin tissue composed of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is not entirely genetically determined and thus even identical twins do not share a similar pattern.The iris pattern of a person's eyes are first scanned, and then registered in the iris recognition system database. Since the iris pattern of eyes is almost terrible to forge or otherwise duplicate, the identification created on iris recognition system is almost safe and exact.

When human being placed his eye in front of Retina scanner, scanner will scan the retina and check with databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second, and with infinitesimally small False Match rates.

In many companies, security administrators use iris acknowledgement system to identify the individuals before they are allowable to access classified information. Many millions of persons in several countries around the world have been enrolled in iris recognition systems, for convenience purposes such as passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to False Matches, is the stability of the iris as an internal, protected, yet externally visible organ of the eye.

Features-Iris Recognition Time Attendance Software

- Rapid and accurate iris identification.
- Robust recognition, even with gazing-away eyes or narrow eyelids.
- The algorithm is able to detect irises under various difficult conditions, like visual noise, lightning reflections or obstructions in eye images. Gazing-away eyes and eyes with narrowed eyelids are accepted.
- A number of iris capture cameras and multi-modal face-iris devices are supported by software.
- Reasonable prices, flexible licensing.

2. Palm Identification

Palm Identification is very suitable in many network-based applications. The authentication system consists of enrollment and variation stages. In the enrollment stage, the training samples are collected and processed by the pre-processing, feature extraction, and modeling modules to generate the matching templates. In the variation stage, a query sample is also processed by the pre-processing and feature extraction modules, and then is matched with the reference templates to decide whether it is a genuine sample or not. The region of interest (ROI) for each sample is, first obtained from the pre-processing module. Then, the palm-print features are extracted from the ROI by using Sobel and morphological operations. The reference templates for a specific user are generated in the modeling module. Last, we use the template-matching and the backpropagation neural network to measure the similarity in the verification stage.

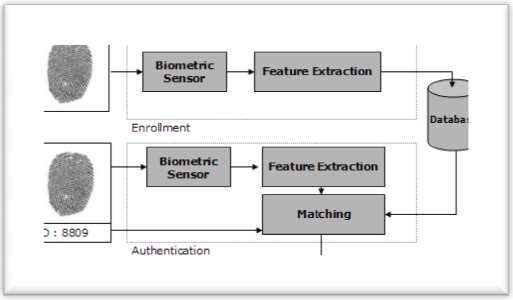

Fig 2: Biometric Attendance scan and verification (Authenticating)

II. System Structure

The system consists of Human being Physiological Character Scanner, GPRS modem, Database.

- Scanner will have used for capture the characteristic.
- GPRS modem is used to send the attendance information of human to the database for permanently storing the user information.
- Database will store the user details like employee name, ID, in time and out time of a day, biometric device location. Database will get from the device by using GPRS network as data transfer medium. In our paper SQL Server database is used for storing the data.
- When an employee placed his finger or palm on the scanner, the scanner will scan the employee attendance

record and send to the Server over the internet. From the Server, this application will retrieve the data and generate the reports and display in the webportal.

III.System Software Design

Database GUI:

SQL Server Management Studio is used for making the database of the system. SQL Server will maintain database tables for store the employees details, fingerprint ID. Every time user used the Biometric device, user attendance record will send to database table with time. In the Database table we can store use in time, out time, late time, time period of present session, employee leave information, Biometric Device Serial number, Biometric Device location.

Database Design:

Database is for storing user information, for that, first we need to design our database structure with a number of database interrelated tables. Like Users, Department, Device logs, Devices, Employees Leaves, Holidays, Shifts…etc.

Each and every database table will store its specific data related to Biometric Device and employee information.

Report GUI:

In this Application we used SQL Server Reporting Services (SSRS) for displaying the attendance. ADO.Net, Entity framework are used as Object Relational Mapping tool for Database connectivity.

IV. Conclusion & Future Work

The proposed system will make a way for perfect management of students and staff attendance and produce more accuracy. In Future we are going propose a system for Human being Behavioral characteristics basedbiometricSecurity System and a mobile application. Behavioral characteristics are like Voice Recognition and signature.

References

[1] JianjiangFeng, “Combining minutiae descriptors for fingerprint matching”, Pattern Recognition, pp. 342 – 352, April 2007.

[2] Peng Shi, JieTian, Qi Su, and Xin Yang, “A Novel Fingerprint Matching Algorithm Based on Minutiae and Global Statistical Features”, IEEE Conference, 2007.

[3] Neeta Nain, Deepak B M, Dinesh Kumar, ManishaBaswal, and BijuGautham “Optimized Minutiae–Based Fingerprint Matching”, Proceedings, 2008.

[4] R. Clarke, Human identification in information systems: Managementchallengesandpublicpolicyissues, Information Technology. People 7 (4) (1994) 6–37.

[5] A.K. Jain, R. Bolle, S. Pankanti, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, Dordrecht, 1999.

[6] L. O’Gorman, Fingerprint verification, in: A.K. Jain, R. Bolle, S. Paukauti (Eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, Dordrecht, 1999, pp. 43–64.

[7] M. Golfarelli, D. Miao, D. Maltoni, on the error-reject trade-oDinbiometricverificationsystems,IEEE Transfer Pattern Anal. Mach. Intell. 19 (7) (1997) 786–796.

[8] R.L. Zunkei, Hand geometry based verification, in: A.K. Jain, R. Bolle, S. Pankanti (Eds.), Biometrics: Personal Identification in Networks Society, Kluwer Academic Publishers, Dordrecht, 1999, pp. 87–101.