Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Engineering

Elixir Comp. Engg. 128 (2019) 52938-52941

Elixir
ISSN: 2229-712X

Student Identification Using Biometric

S.Sabitha, S.Swathi, M.Thiripurasundari and S.Praveen kumar
Department of Computer Science & Engg., E.G.S.Pillay Engineering College, Nagapattinam.

ARTICLE INFO

Article history:
Received: 15 February 2019;
Received in revised form:
15 March 2019;
Accepted: 25 March 2019;

Keywords
Biometric,
Fingerprint,
Scanner.

ABSTRACT

Bio-metric identification systems are widely used for unique identification of humans mainly is verification and identification .It is used as a form of identity access management and access control. Fingerprint identification is one of the best biometric technique. The biometric fingerprints identification are secure to use and mainly unique for every person and do not change in one's lifetime. This paper is to identify each and every student of the department as well as the college.

Introduction

There are number of students studying in a college. There is a need to identify those students all time in the campus. Managing the student information safely and efficiently is an important task. Each and every students details should be register to identify all valid students. It saves both the time and money for the institution.

This system uses the fingerprint identification terminal to collect the fingerprint information. By means of replacing the student Id card with the physiological characteristics of lifelong invariance, uniqueness, and convenience, it is the basis of student identity authentication.

In this project work, the incremental model is used to design the software project. The related information is collected from various sources to develop and test the biometric software project. To design and implement the project, software which is related to fingerprint identification have been used. The aim is to design a student identification system based on fingerprint which can effectively verify the student of the college.

Biometric Technology

Biometrics is the technical term for body measurements and calculations. It refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.

Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palmprint, handgeometry, iris recognition, retina and odour/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics to describe the latter class of biometrics. More traditional means of access control include token-based identification systems, such as a driver's license or passport, and knowledge-based identification systems, such as a password or personal identification number. Since biometric identifiers are unique to individuals, they are more reliable in verifying identity than token and knowledge-based methods; however, the collection of biometric identifiers raises privacy concerns about the ultimate use of this information**.**

Fingerprint

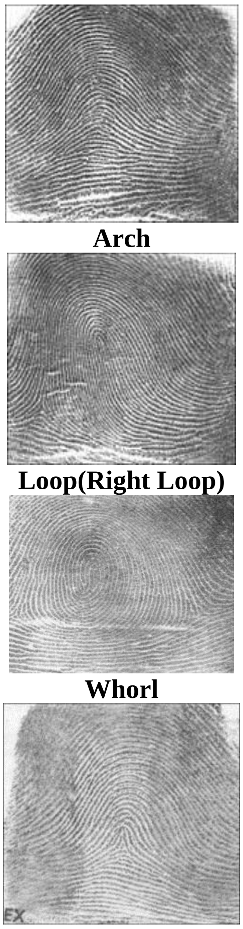
A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the glands that are present in epidermal ridges. These are sometimes referred to as "Chanced Impressions".

In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the sole of the foot can also leave an impression of friction ridges.

Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Human fingerprints are detailed, nearly unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster. Fingerprint analysis, in use since the early 20th century, has led to many crimes being solved. This means that many criminals consider gloves essential. In 2015, the identification of sex by testing the fingerprint biochemical content (rather than visual pattern) has been reported.

Tele:
E-mail address: swathi160697@gmail.com



Arch

Loop(Right Loop)

Whorl

Arch(Tented Arch)

Figure 1. Types of fingerprints.

Fingerprint Recognition

Fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies.

Pattern

The three basic patterns of fingerprint ridges are the arch, loop, and whorl:

- Arch: 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.
- Loop: The ridges enter from one side of a finger, form a curve, and then exit on that same side.
- Whorl: Ridges form circularly around a central point on the finger.

Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited.

Fingerprint processing

Fingerprint processing has three primary functions: enrollment, searching and verification. Among these functions, enrollment which captures fingerprint image from the sensor plays an important role. A reason is that the way people put their fingerprints on a mirror to scan can affect to the result in the searching and verifying process.

Regarding to verification function, there are several techniques to match fingerprints such as correlation-based matching, minutiae-based matching, ridge feature-based matching and minutiae-based algorithm. However, the most popular algorithm was minutiae based matching algorithm due to its efficiency and accuracy.

Fingerprint Matching Algorithm

Minutiae Algorithm features

Features of fingerprint ridges, called minutiae, include:

- ridge ending: The abrupt end of a ridge
- bifurcation: A single ridge dividing in two
- short or independent ridge: A ridge that commences, travels a short distance and then ends
- island or dot: A single small ridge inside a short ridge or ridge ending that is not connected to all other ridges
- lake or ridge enclosure: A single ridge that bifurcates and reunites shortly afterward to continue as a single ridge
- spur: A bifurcation with a short ridge branching off a longer ridge
- bridge or crossover: A short ridge that runs between two parallel ridges
- delta: A Y-shaped ridge meeting
- core: A circle in the ridge pattern

Pre-processing helped enhancing the quality of an image by filtering and removing unnecessary noises. The minutiae based algorithm only worked effectively in 8-bit gray scale fingerprint image. A reason was that an 8-bit gray fingerprint image was a fundamental base to convert the image to 1-bit image with value 0 for ridges and value 1 for furrows. As a result, the ridges were highlighted with black color while the furrows were highlighted with white color. This process partly removed some noises in an image and helped enhance the edge detection. Furthermore, there are two more steps to improve the best quality for the input image: minutiae extraction and false minutiae removal. The minutiae extraction was carried out by applying ridge thinning algorithm which was to remove redundant pixels of ridges. As a result, the thinned ridges of the fingerprint image are marked with a unique ID so that further operation can be conducted. After the minutiae extraction step, the false minutiae removal was also necessary. The lack of the amount of ink and the cross link among the ridges could cause false minutiae that led to inaccuracy in fingerprint recognition process.

Fingerprint Sensor

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. Many technologies have been used including optical, capacitive, RF, thermal, piezo resistive, ultrasonic, piezo electric, MEMS. This is an overview of some of the more commonly used fingerprint sensor technologies.

Optical

Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized type of digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface.

Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge-coupled device) which captures a visual image of the fingerprint.

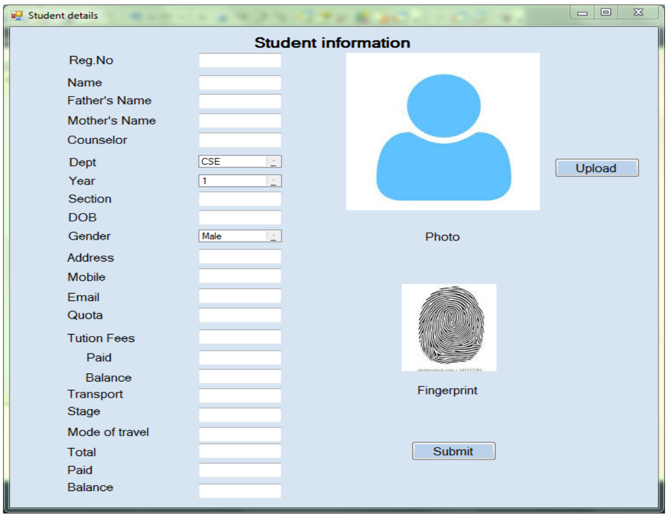
A scratched or dirty touch surface can cause a bad image of the fingerprint. A disadvantage of this type of sensor is the fact that the imaging capabilities are affected by the quality of skin on the finger. For instance, a dirty or marked finger is difficult to image properly. Also, it is possible for an individual to erode the outer layer of skin on the fingertips to the point where the fingerprint is no longer visible. It can also be easily fooled by an image of a fingerprint if not coupled with a "live finger" detector. However, unlike capacitive sensors, this sensor technology is not susceptible to electrostatic discharge damage. Fingerprints can be read from a distance.Here we use the optical sensor to scan the fingerprint.Figure2 shows optical sensor.

Figure 2. Optical sensor.

Working

The developed system is capable for identifying the students of the department. The system's first task was to insert the entire student's information in the system database. This information was obtained by the system through a registration form(Figure3:Registration form).

.



Student details

Student information

Reg.No	
Name	
Father's Name	
Mother's Name	
Counselor	
Dept	CSE
Year	1
Section	
DOB	
Gender	Male
Address	
Mobile	
Email	
Quota	
Tution Fees	
Paid	
Balance	
Transport	
Stage	
Mode of travel	
Total	
Paid	
Balance	

Figure 3. Registration form.

This registration form contains all the necessary fields about the student such as name, fathers and mother's name, session, roll, registration, address, photo and finally key information about fingerprint. The system can take one or more fingerprint templates from the ten fingers of a student. Each fingerprint was taken three times in an enrollment. Then the system saved this information into the database after proper validation of data. The student's fingerprint templates from the fingerprint scanner were stored in the fingerprint database. For identification, the fingerprint device scanned the fingerprint and created a fingerprint template

This template was matched with each saved templates in the database. If a match is found, the notified that the user was a valid student of the department and displayed the information of the student, otherwise the system notified the user was unknown in the department.

The database which is stored in the software is installed in all the computers which are placed in different places. There is a connection between these computers that automatically updates the student details when they did any works like paying fees, take and return books from library (Figure 4 : Connection diagram)

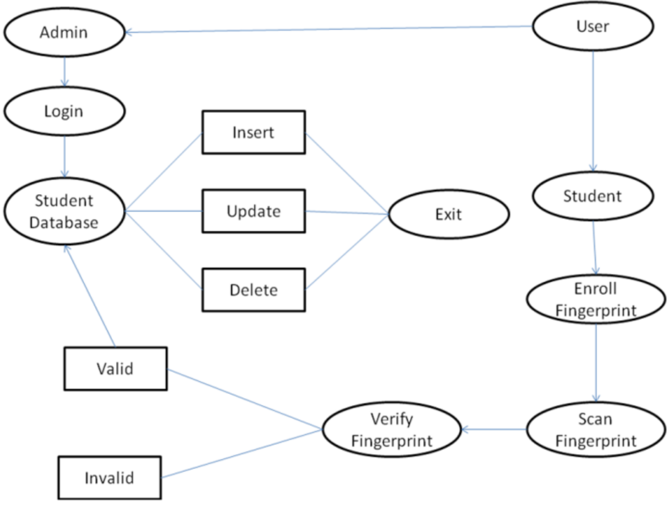


Figure 4. Data Flow Diagram.

Modules

1. Fingerprint Interface
2. Data Acquisition
3. Data Preprocessing and Storing
4. Fingerprint Processing and Identification
5. User Interface Design and Integration

Data Acquisition

The system received the student's information which filled in the form and the student's fingerprint from the fingerprint scanner. The basic information were stored in the student profile table and the fingerprints were in the fingerprint data table. The process is also known as student authentication.

Data Preprocessing and Storing

When students enroll his finger on the device, it scans the finger .Then it set some value for the particular fingerprint. After processing the fingerprint data the device stores the fingerprint inside the device's internal database. All the student's information and fingerprint were stored in the system database.

Fingerprint Processing and Identification

For identification, the device scans the finger. The system searches the all fingerprint that are stored in the system database and matches with scanned. If the fingerprint match with the existing fingerprint then all the information of identified student have been displayed. But if it is not matched with any existing fingerprints then the system notifies that the user is not the valid student of the department.

User Interface Design and Integration

User Interface is the communication between a user and the system. To access the system, a login was designed. The admin user can access the system by providing the username and password. The admin user can add a student's information and can view all student information at any time. All the modules of the system were integrated through this interface.

Conclusion

The main aim of this project is to identify the student. The system implements the verification of the student identity through the fingerprint, which can make the campus life more convenient.

Each system had the software that automatically updates the student information. Scanner scans fingerprint and identify the person. If the person is valid it shows the information about them. This project is implemented if only internet is available. This system will be further developed with some additional features and can be implement without the internet.

Reference

[1].Raymond Thai. “Fingerprint Image Enhancement and Minutiae Extraction”. Technical report, The University of Western Australia.

[2]. Kenneth Nilsson and Josef Bigun. “Localization of corresponding points in fingerprints by complex filtering”. Pattern Recognition Letters 24, page 2135 2144, October 2003.

[3].Vinod C. Nayak, Tanuj Kanchan, Stany W. Lobo, and Prateek Rastogi etc. “Sex differences from fingerprint ridge density in the Indian population”. Journal of Forensic and Legal Medicine, 17(1):84 – 86, September 2007.

[4].Mary Jane and Aliman Manalo. “Development of a Fingerprint Classification Scheme For Improved Fingerprint Identification”. Technical report, University of the Philippines, Diliman.

[5].Automated Fingerprint Identification System (AFIS)”, PDF Document.

[6].Biometrics Institute Limited, “Types of Biometrics” Kingsway, London WC2B 6UN, United Kingdom.

[7].Aleksandra Babich, “Biometric Authentication. Types of biometric identifiers”, Bachelor’s Thesis, Degree Program in Business Information Technology, HAAGA-HELIA University of Applied Science, 2002.