PERSPECTIVE

52(252), December 1, 2016

ISSN 2278–5469 EISSN 2278–5450

Discovery

Biometric student registration and verification system

Md. Mijanur Rahman[1], Sifat Nur Rahman[2], Mahbubur Rahman[3], Firoz Haider[4]

1.Associate Professor, Dept. of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Bangladesh; Email: mijanjkkniu@gmail.com
2.Dept. of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Bangladesh; Email: sifatnur@gmail,com
3.Dept. of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Bangladesh; Email: mahbub92cse@gmail.com
4.Dept. of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Bangladesh; Email: real.cse6@gmail.com

Article History
Received: 01 October 2016
Accepted: 13 November 2016
Published: 1 December 2016

Citation
Md. Mijanur Rahman, Sifat Nur Rahman, Mahbubur Rahman, Firoz Haider. Biometric Student Registration and Verification System. *Discovery*, 2016, 52(252), 2399-2407

ABSTRACT

This project work is devoted to present a biometric identification system based on fingerprint recognition. Biometrics can be taken literally as 'life measurement' but the term is usually associated with the measurement and use of unique physiological characteristics to identify an individual person. Biometric Identification Systems are widely used for unique identification and verification of humans. At present, there are many types of biometric technology have been used; such as, fingerprint recognition, face recognition, voice recognition, iris recognition, etc. Fingerprint recognition is considered to be the best and fastest method for biometric identification. The biometric fingerprints features are secure to use, unique for every person and do not change in one's lifetime. The aim of this project is to develop a fingerprint recognition system that can accurately identify the students of the department as well as the university. The proposed system used Minutiae Matching Algorithm to identify student's fingerprints. In this project work, all the software modules were implemented using C# Software Development Kit (SDK) and tested in windows

platform. From the experimental results it can be concluded that the proposed system can effectively verify the students of the Computer Science and Engineering department at Jatiya Kabi Kazi Nazrul Islam University, Bangladesh.

Keywords: Biometric, C# SDK, Fingerprint Recognition, Minutiae Extraction, Minutiae Matching

1. INTRODUCTION

At present we are living in the age of Information Communication and Technology (ICT). From morning to night we need help of the technology. This is the revolutionary time of computer technology. Most of the works depends on computer application. In the early 1990s, the FBI in the United States, the Home Office in the United Kingdom, Paris Police in France [1], and the Japanese police initiated projects [2] to develop automated fingerprint identification systems. The trust of this research is to use electronic digital computers for classifying searching and matching fingerprints for personal identification.

The major features of the proposed Biometric Student Registration and Identification System is to register all of the students of grouped each batch and to identify all valid students. Effective time mechanism saves both time and money for the institution. 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 proposed biometric software project. To design and implement the project, ZKTeco fingerprint device [3] and its related fingerprint identification algorithm have been used. The main aim of the proposed work is to design a student identification system based on fingerprint which can effectively verify the student of the CSE department at Jatiya Kabi Kazi Nazrul Islam University, Bangladesh.

2. BIOMETRIC TECHNOLOGY

Biometrics refers to metrics related to human characteristics. Biometrics authentication is used in computer science as a form of identification and access control. Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. However, biometric identification has eventually a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction and one expects computers of the future to have the same capabilities. A number of biometric traits have been developed and are used to authenticate the person's identity [4]. The idea is to use the special characteristics of a person to identify him. By using special characteristics we mean the using the features such as face, iris, fingerprint, signature etc. Different types of biometrics are used in any identification system, such as DNA Matching (Chemical Biometric), Ear (Visual Biometric), Eyes (Iris Recognition and Retina Recognition), Face Recognition (Visual Biometric), Fingerprint Recognition (Visual Biometric), Gait (*Behavioral Biometric*), Signature Recognition **(**Visual/Behavioral Biometric**),** Voice (Speech and Speaker Recognition), etc [5].

A biometric system can be either an 'identification' system or a 'verification' (authentication) system. Biometrics can be used to determine a person's identity even without his knowledge or consent. For example, scanning a crowd with a camera and using face recognition technology, one can determine matches against a known database. Biometrics can also be used to verify a person's identity. For example, one can grant physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retinal scan.

3. AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

By the 1970s, computers were in existence, and the FBI knew it had to automate the process of classifying, searching for and matching fingerprints. The Japanese National Police Agency paved the way for this automation, establishing the first electronic fingerprint matching system in the 1980s. Their Automated Fingerprint Identification Systems (AFIS) [6], eventually enabled law enforcement officials around the world to cross-check a print with millions of fingerprint records almost instantaneously. The Automated Fingerprint Identification System (AFIS) is a computerized storage system for millions of fingerprint images. The AFIS is an effective system for identifying people and establishing the criminal history of offenders. The Automated Fingerprint Identification Systems (AFIS) includes two processes, fingerprint identification and verification. The Automated fingerprint identification is the process of automatically matching one or many unknown fingerprints against a database of known and unknown prints. The Automated fingerprint verification is a closely related technique used in applications such as attendance and access control systems. On a technical level, verification systems verify a claimed identity whereas identification systems determine identity based solely on fingerprints.

The biometric authentication is a three-step process (Capture, Process, Enroll) followed by a Verification or Identification process [7]. During Capture process, raw biometric is captured by a sensing device such as a fingerprint scanner. The second phase of processing is to extract the distinguishing characteristics from the raw biometric sample and convert into a processed biometric identifier record (sometimes called biometric sample or biometric template). Next phase does the process of enrollment. Here the processed sample is stored in a storage medium for future comparison during an authentication.

A new automated approach is needed to (i) extract each fingerprint image (ii) process each of these images to produce a reduced template of characteristic information, and (iii) search a database to automatically produce a highly reduced list of probable candidates [8].

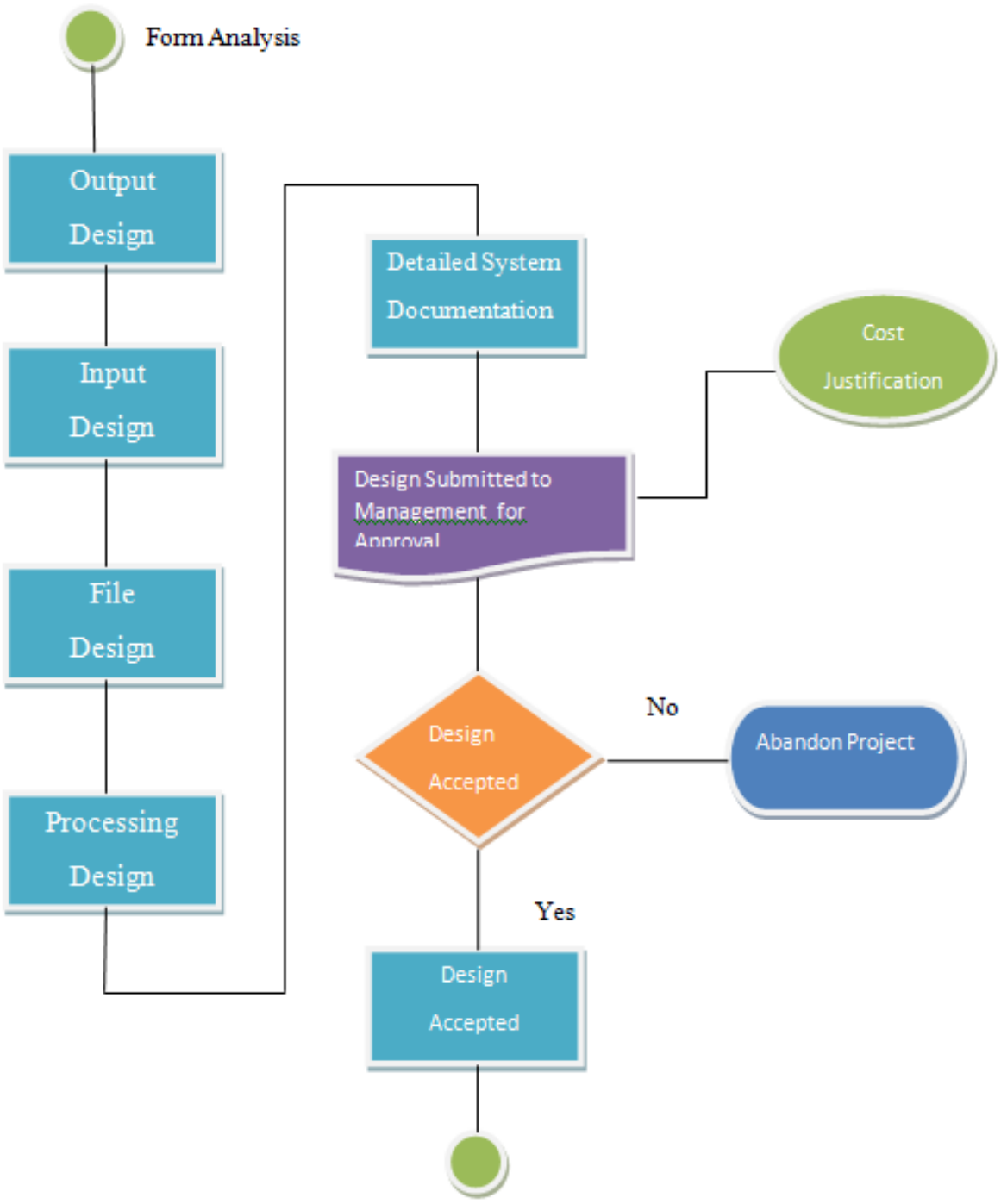

Figure 1 System Design

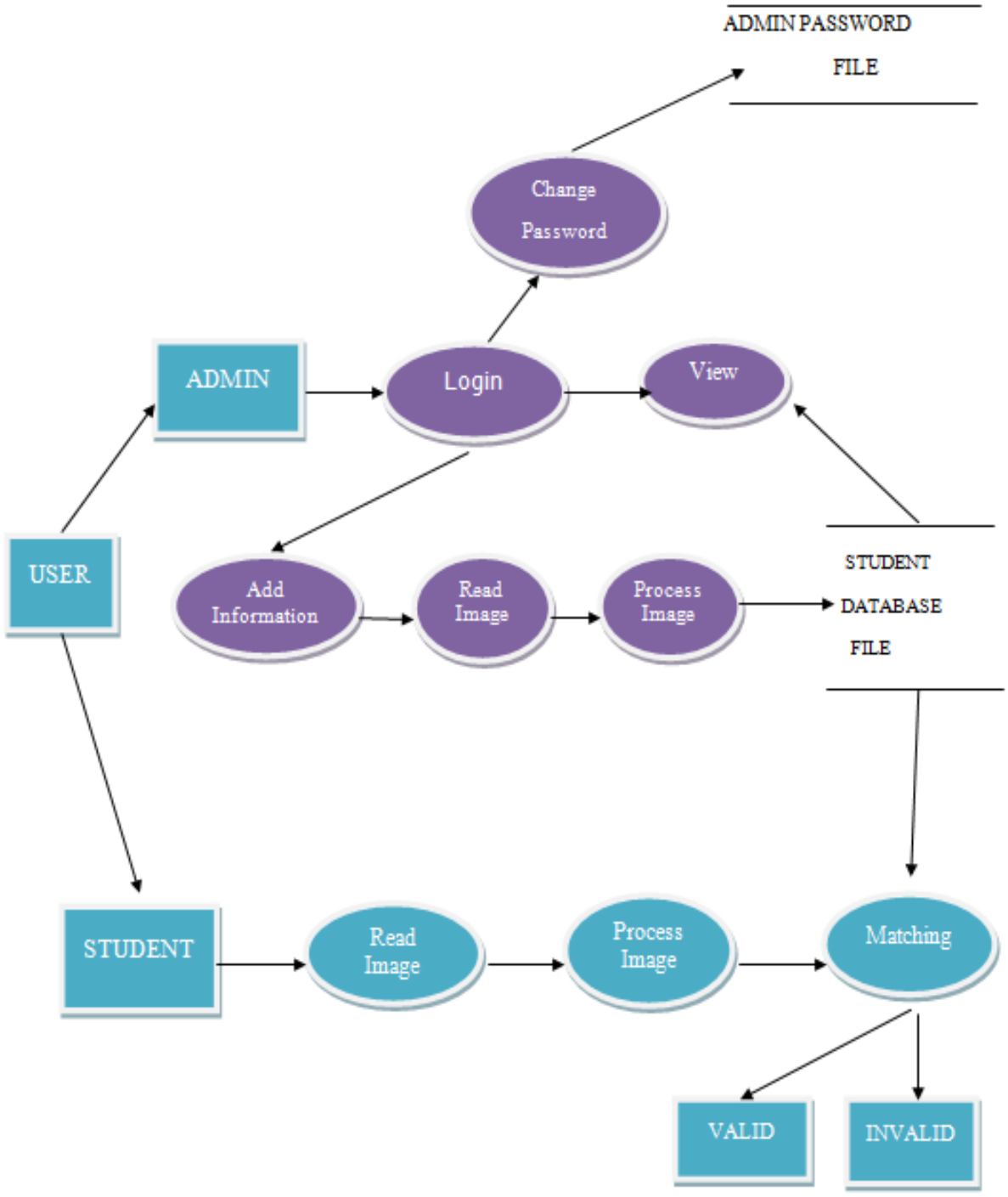

Figure 2 Data Flow Diagram

4. HARDWARE AND SOFTWARE SUPPORT

To acquire the fingerprint template of the student we need a fingerprint scanner device. This device will scan the fingerprint and also will process the data to get fingerprint template. To interface this device with computer we need some software. This software is referred as Software Development Kit (SDK). A variety of sensor types, such as, optical, capacitive, ultrasound, and thermal, are used for collecting the digital image of a fingerprint surface. Optical sensors take an image of the fingerprint, and are the most common sensor today.

The two main categories of fingerprint matching techniques are minutiae-based matching and pattern matching [9]. Pattern matching simply compares two images to see how similar they are. Pattern matching is usually used in fingerprint systems to detect duplicates. The most widely used recognition technique, minutiae-based matching, relies on the minutiae points described above, specifically the location and direction of each point.

The device should be interfaced with the system before using it. To interface the device there are some software to install. This software activated the device and controlled the device. In this project work, ZKT fingerprint device was used to capture the fingerprint template. Also several software modules, such as, ZKT Access Control, Fingerprint Driver, ZKT Timer, were installed to use the system.

5. SYSTEM ANALYSIS AND DESIGN

Analysis is a detailed study of the various operations performed by a system and their relationships within and outside of the system. The main aspect of analysis is defining the boundaries of the system and determining whether or not a candidate system should consider other related system. During analysis, data are collected on the available file, decision points, and transactions handled by the present system.

The most creative and challenging phase of the system life cycle is system design [10]. The term design describes a final system and the process by which it is developed. It refers the technical specification that will be applied in implementing the candidate system. It also includes the construction of programs and program testing. The first step is to determine how the output is to be produced and in what format. Second, input data and master files (database) have to be designed to meet the requirements of the proposed output. The operations (processing phases) are handled through program construction and testing. The steps in the system design are shown Figure-1. Also, the data flows among the steps are represented by a data flow diagram, as shown in Figure-2.

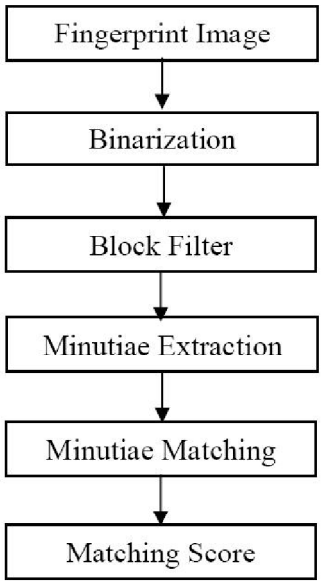

Figure 3 The block diagram of Minutiae algorithm implementation

6. MINUTIAE FEATURE EXTRACTION

The fingerprint algorithms use minutiae features on the finger. The major Minutiae features are ridge ending, bifurcation, and short ridge (or dot). The ridge ending is the point at which a ridge terminates. Bifurcations are points at which a single ridge splits into two ridges. Short ridges (or dots) are ridges which are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical. In this project, the Minutiae Feature extraction based algorithms have been used. The block diagram of the working procedure of Minutiae algorithm [11] is shown in Figure-3.

Binarization converts gray scale image into binary image by fixing the threshold value. The pixel values above and below the threshold are set to '1' and '0' respectively. It's the most critical task in the fingerprint matching system. In *Block Filter*, the binarized image is thinned using Block Filter to reduce the thickness of all ridge lines to a single pixel width to extract minutiae points effectively. Thinning preserves outermost pixels by placing white pixels at the boundary of the image, as a result first five and last five rows, first five and last five columns are assigned value of one. In *Minutiae Extraction*, the minutiae location and the minutiae angles are derived after minutiae extraction. The terminations which lie at the outer boundaries are not considered as minutiae points, and Crossing Number isused to locate the minutiae points in fingerprint image. Crossing Number is defined as half of the sum of differences between intensity values of two adjacent pixels. If crossing Number is 1, 2 and 3 or greater than 3 then minutiae points are classified as Termination, Normal ridge and Bifurcation respectively. To compare the input fingerprint data with the template data Minutiae matching is used. For efficient matching process, the extracted data is stored in the matrix format. During the *matching process*, each input minutiae point is compared with template minutiae point. In each case, template and input minutiae are selected as reference points for their respective data sets. Matching an input image with a stored template involves computing the sum of the squared differences between the two featured vectors after discarding the missing value. This distance is normalized by the number of valid feature values used to compute the distance. The *matching score* is combined with that obtained from the minutiae-based method, using the some rule of combination. If the matching score is less than a predefined threshold, the input image is said to have successfully matched with the template.

7. METHODOLOGICAL STEPS

The overall student identification process is shown in Figure-4 and Figure-5. The proposed system development includes following five modules:

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

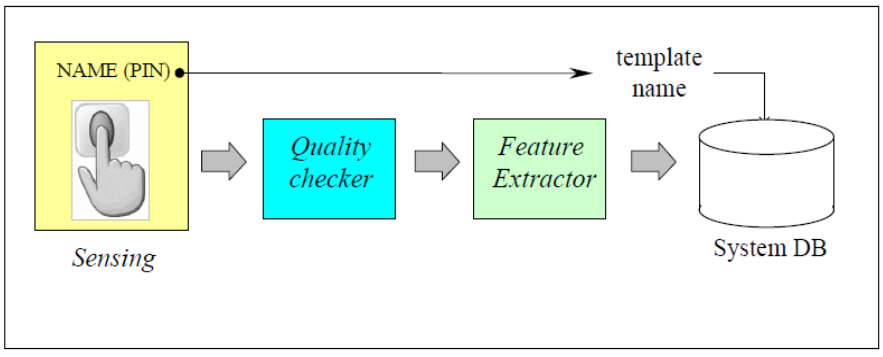

Figure 4 Fingerprint Template Generation Process

7.1. Fingerprint Interface

To work with the device first of all the device should be connected with the computer. This connection is referred as Fingerprint Interface. The device can be connected with the computer through three ways, such as, TCT/IP Communication, Serial Port Communication and USB Client Communication. In this project work, the fingerprint device is connected with the PC by using TCP/IP

communication port. There is a connecting wire to connect the device with the computer. The device is controlled by 'zkemkeeper' class. This class provides the necessary methods and property to perform the fingerprint related task. To connect the device the method Connect_Com() is used. If the device is not connect properly then it will show the error message by GetLastError() function.

7.2. Data Acquisition

The system received the student's Information by filled in the registration form and the student's fingerprint template from the fingerprint scanner (see Figure-4) as input. The basic information were stored in the student profile table and the fingerprints were in the template data table. In this template table the key field is the student roll number. By this roll number all the templates are differed from one another. The process is also known as student authentication.

7.3. Data Preprocessing and Storing

When students enroll his finger on the device scanner sensor, the device scans the edge and ridge of the finger. Then it set some value from the position of that ridges and edges and combines them. Finally from this point of finger's ridge and edge the device create binary template that is known as fingerprint template. After processing the fingerprint data the device stores the fingerprint template inside the device's internal database. The proposed system used these templates in the further steps, such as identification and verification. All the student's information and fingerprint template were stored in the system database. These templates can be accessed at any time from the system database.

7.4. Fingerprint Processing and Identification

For identification, the device scans the ridge and edge of the finger and creates a template. The system searches all the templates that are stored in the system database and matches with each saved template (see Figure-5). If the templates match with the existing template then all the information of identified student have been displayed. But if the template is not matched with any existing template then the system notifies that the user is not the valid student of the department.

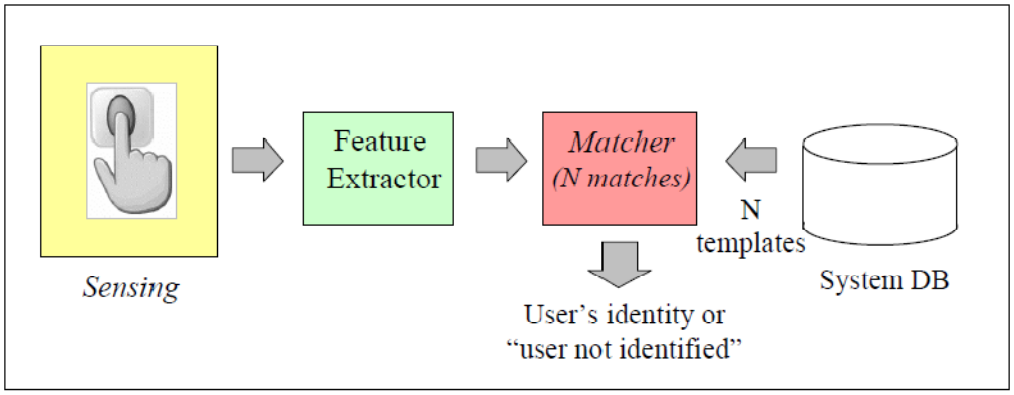

Figure 5 Fingerprint Identification Process

7.5. 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 his/her fingerprint or by providing the username and password. The admin user can add a student's information and can view all students' information at any time. The user interface also includes a registration form that is used to get student information and a fingerprint interface. All the modules of the system were integrated through this interface.

8. EXPERIMENTAL RESULTS

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. 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 (see Figure-6 and Figure-7). 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 (see Figure-8), otherwise the system notified the user was unknown in the department. All the program modules were implemented using C# Software Development Kit (SDK) and tested in windows platform.

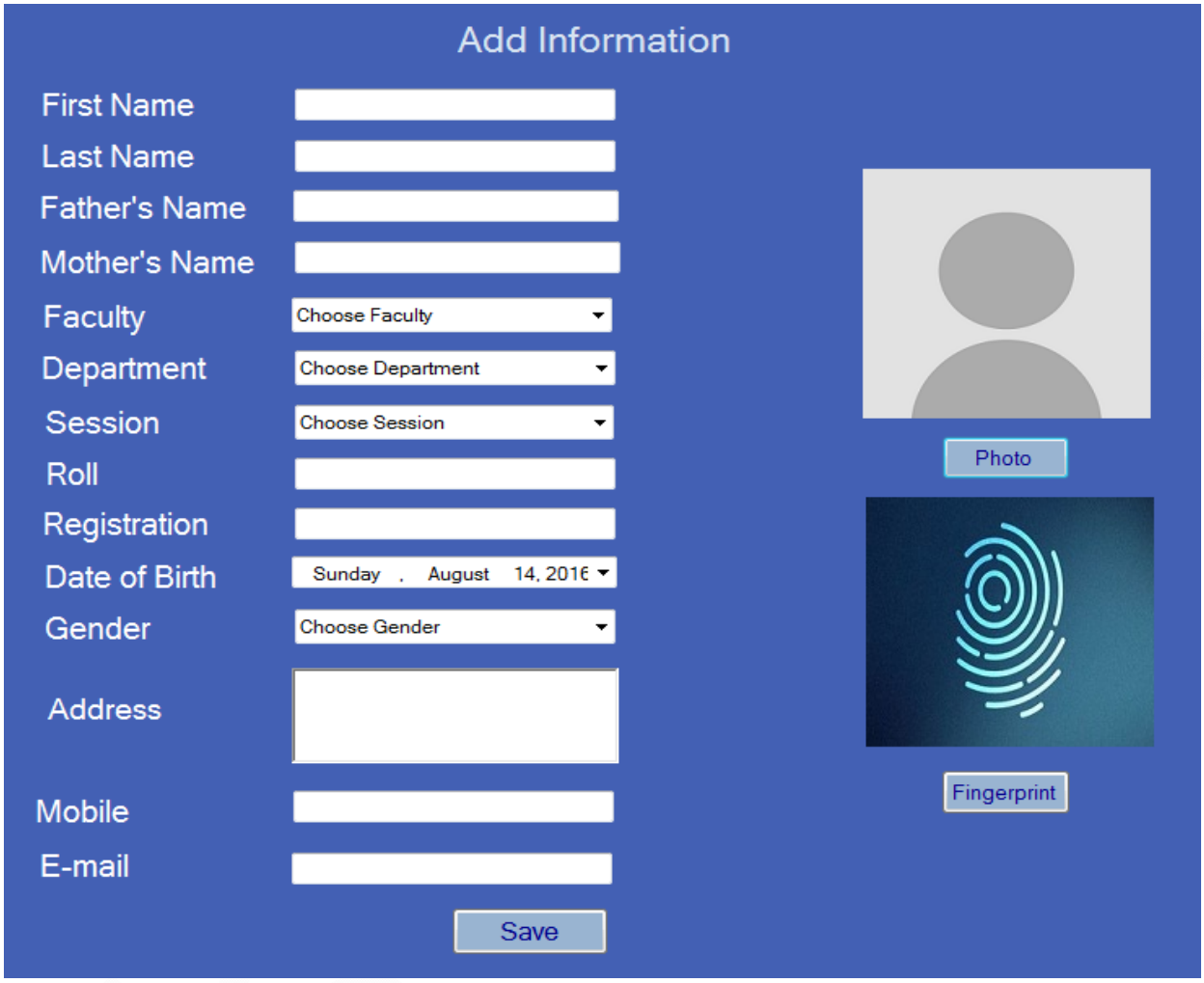

Figure 6 Student Registration Form

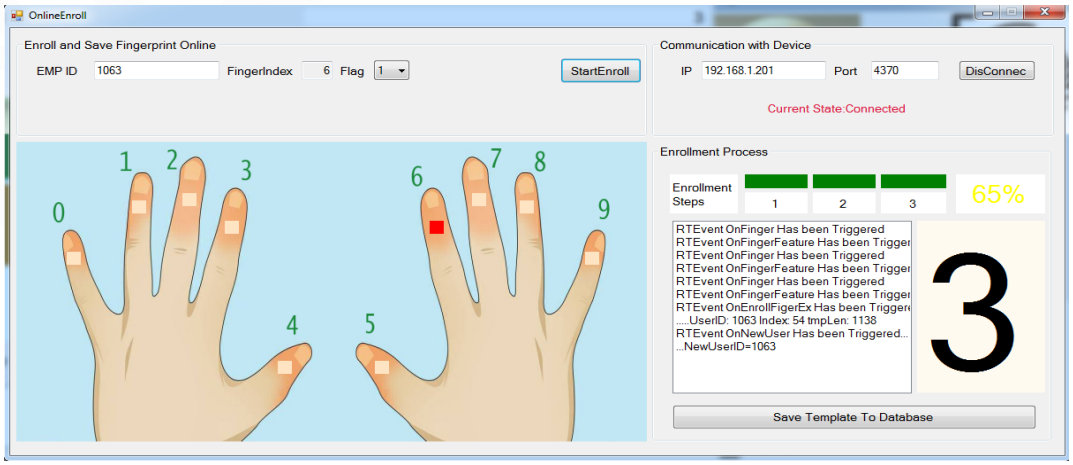

Figure 7 Fingerprint Enrollment

Figure 8 Student Verification Form

9. CONCLUSION

The aim of this project is to develop a student identification system using biometric features. The develop system is used to identify the student based on fingerprint recognition. Throughout the experiences in this project we have learned to build a reliable Embedded Fingerprint Identification System using open source software components. This was an embedded system design exercise, which involved researching existing technologies and solutions, requirement definition, project planning, system analysis and design, algorithm design, implementation, integration and testing. This system is warmly accepted to all the people as fingerprint identification is now one of the most popular technologies in the world. All the software modules were implemented using C# SDK and tested in windows platform. The major limitation of this work is that the system cannot capture the original fingerprint images from the scanner; it just receives the fingerprint templates from the device. This system will be further developed with some additional features of original fingerprint images processing in automatic student attendance system.

REFERENCE

1. Moore R. T, "Automatic Fingerprint Identification Systems. In Advances in Fingerprint Technology", 1st ed.; Lee, H. C.; Gaensslen, R. E., Eds.; Elsevier, NY, 1991; pp 163–191.
2. Kiji, K. "AFIS 30-Year History", NEC Internal Corporate Report, NEC Solutions, Tokyo, Japan, 2002.
3. http://www.zkteco.com/product/F18_248.html
4. Aleksandra Babich, "Biometric Authentication. Types of biometric identifiers", Bachelor's Thesis, Degree Programme in Business Information Technology, HAAGA-HELIA University of Applied Science, 2002.
5. Biometrics Institute Limited, "Types of Biometrics" Kingsway, London WC2B 6UN, United Kingdom, http://www.biometricsinstitute.org/pages/types-of-biometrics.html
6. Kenneth R. Moses; Peter Higgins; Michael McCabe; Salil Probhakar; Scott Swann, "Fingerprint Sourcebook - Chapter 6: Automated Fingerprint Identification System (AFIS)", PDF Document, https://www.ncjrs.gov/pdffiles1/nij/225326.pdf, 2010.
7. Sahoo, Soyuj Kumar; Mahadeva Prasanna, SR (1 January 2012). Mahadeva Prasanna, SR, Choubisa, Tarun. "Multimodal Biometric Person Authentication: A Review", IETE Technical Review, Vol 29 (1), February 2012.
8. Cole S, "Suspect Identities", Harvard University Press, Cambridge, MA, 2001.
9. James Wayman, et al, "Biometric Systems Technology, Design and Performance Evaluation", (London: Springer, 2005).
10. Elias M Awad, "System Analysis and Design", GP.
11. Lukasz Wieclaw, "A Minutiae-Based Matching Algorithm in Fingerprint Recognition Systems", Journal of Medical Informatics and Technologies, Vol 13, 2009.