THE SYSTEM OF AUTHENTICATING ATTENDANCE BASED ON FINGERPRINT

Otaboyeva Munisa Ollabergan qizi
Master's degree student of Urgench branch of Tashkent University of Information Technologies named after Muhammad al-Khwarazmi
https://doi.org/10.5281/zenodo.7880134

Abstract. *This study aims to design and develop an automated student attendance system based on fingerprint recognition that will be hassle-free management of records in student attendance for conducting the classes.*
Keywords: *fingerprint recognition, student attendance, hassle-free management, system.*

Introduction.

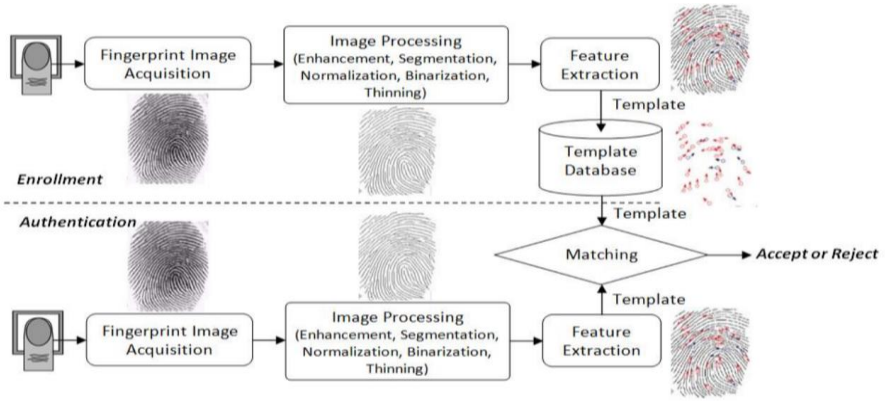
The modern world is the revolutionary time of Information and Computer Technology. Most of the works in daily life depends on computer applications. The traditional student attendance includes all the hassles of roll calling and the very time-consuming of the students and teachers for conducting the classes in an institute. This time-consumed process is very boring for the students and teachers. Thus, a new and innovative approach is required to handle this issue. It motivates us to design a reliable system for student attendance. The biometric authentication systems are widely utilized for the unique identification of people, like students, especially for the verification and identification of individuals. Also, the use of biometric features in the student attendance management system is a secure approach. A biometric system could be either an identification system or a verification (authentication) system. Several biometric features are used in user authentication systems. These include DNA sequence (chemical biometric), ear (visual biometric) , eyes (iris or retina recognition) , face recognition (visual biometric) , fingerprint recognition (visual biometric), gait (behavioral biometric), signature recognition (visual/behavioral biometric), speech and speaker recognition (auditory biometric) . Designing a trustworthy student attendance system based on face detection and recognition is considered the faster and optimal way to manage the records for students' attendance in institutes. Furthermore, any business organization or educational institution has to maintain the attendance of students or employees for effective functioning of business records.

Main Part.

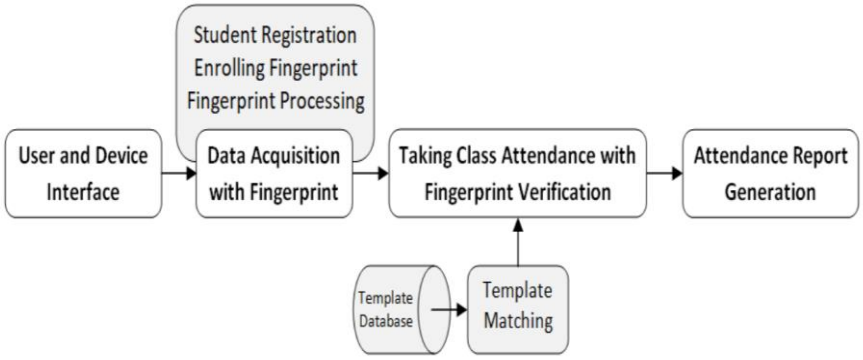
Fingerprints are meant to be the best and fastest method for biometric identification. They are safe to use, unique for everyone, and do not change in one's lifetime. A fingerprint recognition system operates either in authentication mode or in identification mode. Automated fingerprint identification is the process of automatically matching one or many unknown fingerprints against a database of known and unknown prints. Automatic fingerprint authentication is a related technique used in applications, such as attendance and access control systems. On the contrary side, these types of systems determine identity based on fingerprints. Therefore, the biometric matching algorithm plays a vital role in a fingerprint recognition system. Matching algorithms are used to compare previously stored fingerprints templates against candidate fingerprints for authentication purposes. In fingerprint authentication, two majorly used algorithms are image-based algorithms and minutiae feature-based algorithms. Pattern-based algorithms compare the basic fingerprint patterns between a previously stored template and a candidate fingerprint. Other

algorithms use minutiae features from the fingerprint images. The major minutia features are ridge ending, bifurcation, and short ridge. 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 are ridges that are significantly shorter than the average ridge length on the fingerprint. Minutiae and patterns are crucial in analyzing fingerprints since no two fingers are identical. The minutia feature-based algorithm matches the fingerprint templates in the proposed attendance system.

Generally, a typical biometric fingerprint authentication system consists of five modules: biometrics acquisition, image processing, feature extraction, template database, and matching procedure. The acquisition module using the sensor acquires the biometrics image. Then, it continues several preprocessing steps. After the preprocessing, the fingerprint image is enhanced, normalized, segmented, binarized, thinned, and then the fingerprint image is ready for feature extraction or detection of minutiae information. A set of minutiae features is extracted from the acquired biometric image by the feature extraction module. The extracted features (are stored in a database as template data. Finally, the matching module compares the query biometrics data and template data to reach a match or non-match verdict. During the matching process, each input minutiae point is compared with the template minutiae point. In each case, template and input minutiae are selected as reference points for their respective data sets. The reference points are used to convert the remaining data points to polar coordinates. Matching an input image with a stored template involves computing the differences using distance measures techniques. The matching score obtained from the minutiae-based method defines the successful match with the template.

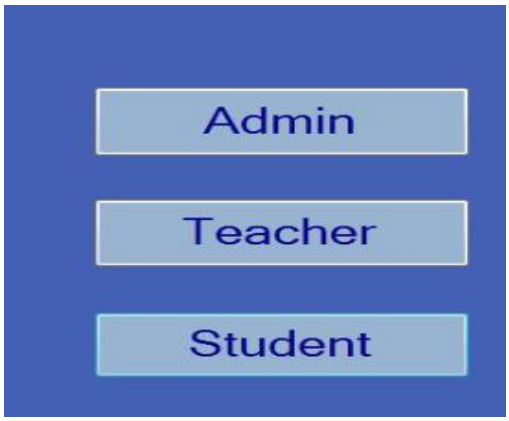


The block diagram in the pictures the methodological steps for developing the proposed attendance system. The proposed approach has five major components, such as (i) user and device interface, (ii) data acquisition with fingerprints, (iii) fingerprint processing, (iv) taking class with fingerprint verification, and (v) attendance report generation.



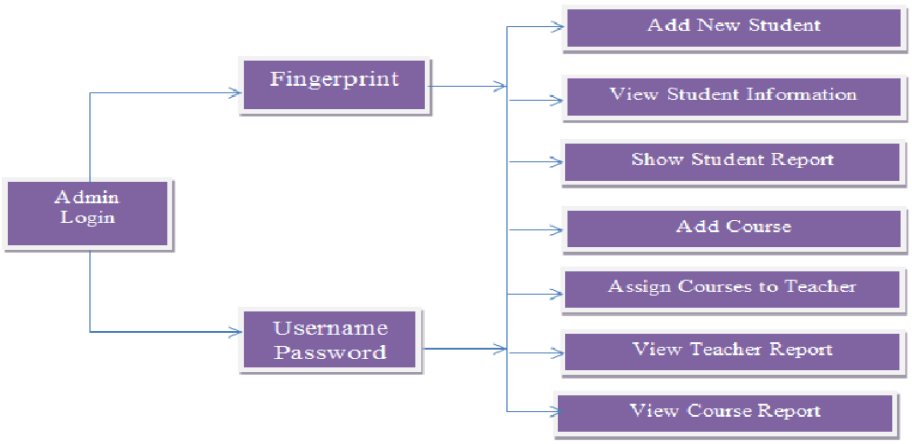
The block diagram of the proposed attendance system.

User Interface is the communication between a user and the system. There are three panels in the designated system: admin, teacher, and student Admin has to log in to the system in two ways. One is by providing the admin's fingerprint, and another way is to provide the username and password. Admin can add a student's information with fingerprints, add syllabus and course information, assign courses to the teacher, generate the student and teacher report, and view the system's information at any time. The user interface also includes two registration forms that are used to get student and teacher information and their fingerprints. All the information about the student and teacher are taken through these forms.



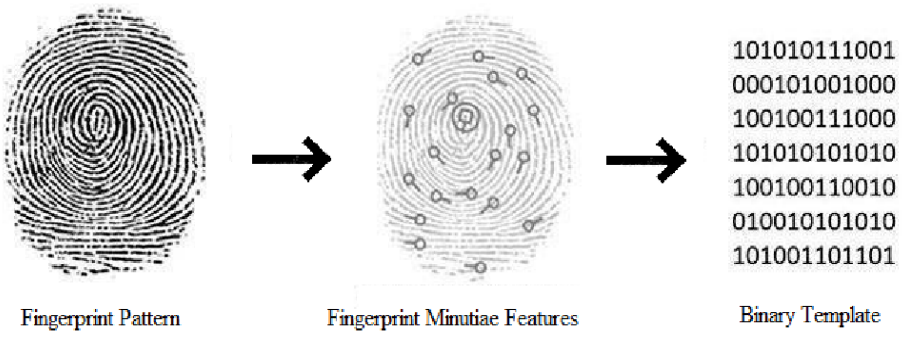
In the teacher panel, every teacher gets a profile after registration. This profile shows all the basic information about the teacher. Admin assigns different courses to the various teachers by the decision of the academic committee. When a course is set to a teacher, then it appears in their profile. Then the teacher can take class attendance on this course through student's fingerprint authentication. In the student panel, a student can only verify themselves by scanning their fingerprints. When a student enrolls their finger, the device collects the fingerprint template and matches it with the entire stored reference templates. If the template matches with any template, then they are authenticated students, otherwise not. The system successfully connected fingerprint devices with the computer referred to as fingerprint device interface. The device can be connected with the computer in three ways: TCT/IP communication, serial port communication, and USB client communication. The fingerprint device was connected with the PC by using a TCP/IP communication port in this work.

The picture below highlights activities in admin panel.



The system received the student's information by filling in the registration form and the student's fingerprints from the fingerprint scanner as input. The fingerprint scanner can read fingerprints of any or more fingers of both hands. The basic information was stored in the student profile table, and the fingerprints were stored in the template data table. In this template table, the key field is the student roll number, and all the templates have differed by this roll number.

When a student enrolls their finger on the device's scanner sensor, the machine scans the edge and ridge of the finger. Then it set some values from the position of the ridges and edges and combines them. Finally, from this point of fingerprint minutiae features, the device creates a binary template, known as fingerprint template. The proposed system used these templates for the further steps in the fingerprint authentication phase, such as student identification and verification. Student identification is made after enrolling student's fingers in the device. For identification, the device acquires the fingerprint minutiae features and creates a fingerprint template. The proposed system searches all the templates stored in the system database and matches the enrolled template with each reference template. If the templates match the existing template, the student is authenticated. However, if the template is not matched with any existing template, the system notifies that the user is not a valid student of the department. The teacher can take the student's attendance through the fingerprint verification process.



The teacher can log in to the system by scanning their fingerprint or by entering username and password. The courses assigned by the admin are appeared in their profile. Then the teacher can take attendance to each class through student's fingerprint authentication. The student attendance is automatically tick marked by enrolling the student's finger on the device. The entire process is automated with fingerprint verification. The verified and present student attendance is stored in the attendance database for further usage. They can also take attendance manually by clicking the checkbox from the list of students. Finally, the student attendance report is generated from the attendance table. The proposed attendance system generates two types of reports; one is a short report containing the only date by date of student attendance. Another is a detailed attendance report including the date-by-date attendance with the total present, total absent, percentage, and the marks. These reports are used for the internal semester evaluation of the students in the department.

Conclusion.

The paper has revealed the advantages of establishing student attendance system based on fingerprint, as they are fast, non-invasive and easy to use. There are some limitations of fingerprint technology. These are the inability to enroll some users for poor fingerprints. For these cases, one needs to consider other biometric features. Also, it can suffer some minor changes along the time. The system may be necessary to re-enroll the fingerprint and/or use multiple fingerprint

enrollments to overcome this problem. The system needs to deploy specialized devices for fingerprint enrollment. The future works can be extended to store fingerprint databases on the remote server that can be used worldwide, and a dedicated website will be hosted on the cloud server for online access to attendance reports This system prevents fake attendance of students, as fingerprint system is much harder to fake, they also change very little over a lifetime, so the data remains current for much longer than photos and passwords. No more struggling to remember students' last password or being locked out due to leaving their photo ID at home. Non-transferable side of fingerprint system, it allows for more accurate tracking of workforce and provides additional security against the theft of sensitive materials. From a technology management perspective, fingerprint recognition is now a cost-effective security solution. Small hand-held scanners are easy to set up and benefit from a high level of accuracy.

REFERENCES

1. Study on Introducing Biometric Fingerprint Authentication in Automated Student Attendance System. Md. Mijanur Rahman1* DOI: 10.9734/bpi/nvst/v4/4580F 2. Integrated System for Monitoring and Recognizing Students During Class Session. Article *in* The International journal of Multimedia & Its Applications · December 2015 DOI: 10.5121/ijma.2013.5604
2. Yuan L, Mu Z, Xu Z. Using ear biometrics for personal recognition. International Workshop on Biometric Person Authentication, Springer. 2005;221-228.
3. Mock K, Hoanca B, Weaver J, Milton M. Real-time continuous iris recognition for authentication using an eye tracker. Proceedings of the 2012 ACM conference on Computer and communications security. 2012;1007-1009.
4. Zulfiqar M, Syed F, Khan MJ, Khurshid K. Deep face recognition for biometric authentication. 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE). 2019;1-6. IEEE.