**“Automated Student Attendance System using Fingerprint Recognition”**

**A MINOR PROJECT REPORT**

*Submitted by*

**Sakthi Mahalakshmi[RA2011003010363]**

**Sathya Ram[RA2011003010387]**

**Sistu Alekhya[RA2011003010388]**

**Sarthak Singh[RA2011003010332]**

*Under the guidance of*

**Dr. M. Hema**

**(Associate Professor, Department of Computing Technologies)**

*in partial fulfillment for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

*in*

**COMPUTER SCIENCE & ENGINEERING**

*of*

**FACULTY OF ENGINEERING AND TECHNOLOGY**



*S.R.M.Nagar, Kattankulathur, Chengalpattu District*

**NOVEMBER 2022**

**SRM INSTITUTE OF SCIENCE AND TECHNOLOGY**

*(Under Section3 of UGC Act,1956)*

**BONAFIDE CERTIFICATE**

Certified that minor project report titled “**Automated Student Attendance System using Fingerprint Recognition**” is the bonafide work of **Sakthi Mahalakshmi[RA2011003010363],** **Sathya Ram[RA2011003010387], Sistu Alekhya[RA2011003010388], Sarthak Singh[RA2011003010332]** who carried out the minor project work under my supervision. Certified further, that to the best of my knowledge the work reported herein does not form any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

|  |  |
| --- | --- |
| Dr. M. Hema | Dr. M. Pushpalatha |
| **Associate Professor,** | **Head of Department/Professor** |
| Dept. of Computing Technologies | Dept. of Computing Technologies |

**Table of Content**

**Chapter no. Title Page no.**

Table of content i

Abstract 1

1. An overview of biometrics 1

[2. Biometrics for Fingerprint 2](#_Toc5109)

[3. Biometric Models 3](#_Toc5110)

[3.1 Finger Scan Technology 4](#_Toc5111)

1. Biometric Applications 5
2. Conclusion 5

References 6

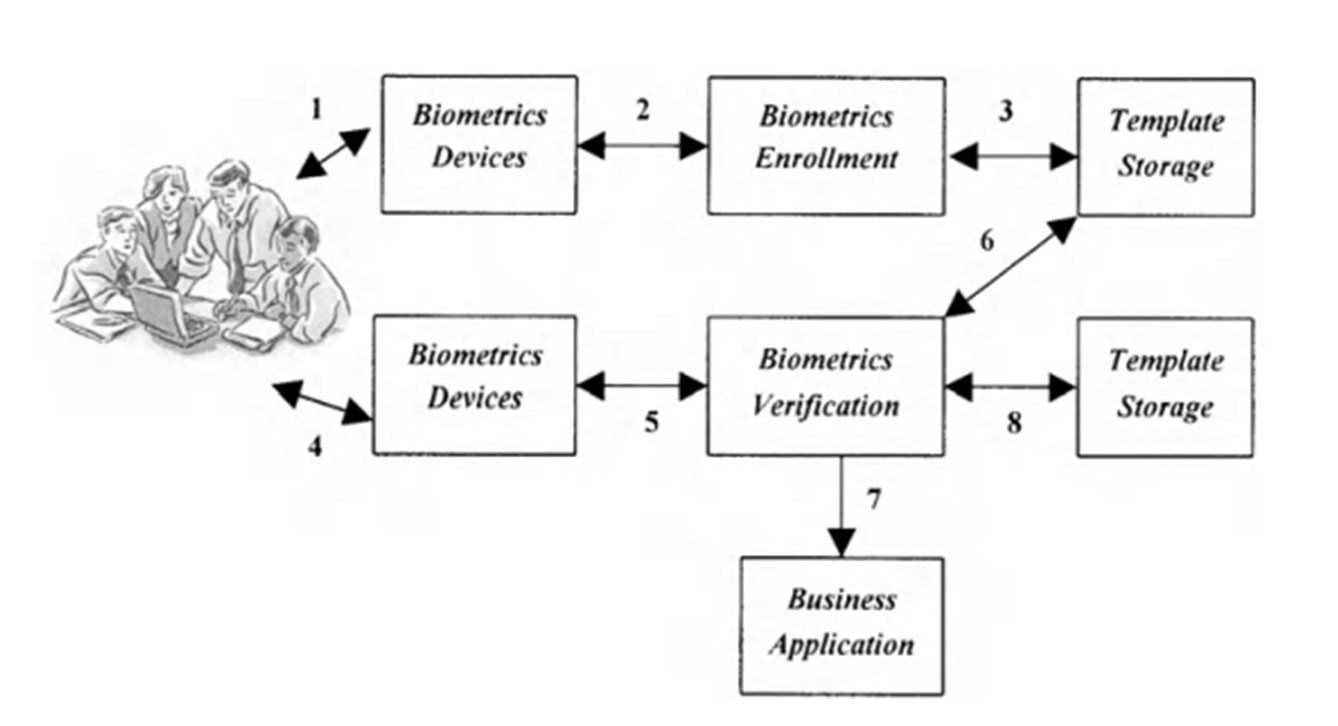
i.

**Abstract:**

* The project work aims at designing a student attendance system which could effectively manage attendance of students.
* In this project work, attendance is marked after student’s biometric identification.
* For student identification, a fingerprint recognition-based identification system is used.
* Fingerprint features are considered to be the best and fastest method for biometric identification.
* These features are more secure to use and unique for every person that don’t change in one's lifetime.
* Fingerprint recognition is a mature field today, but still identifying individual from a set of enrolled fingerprints is a time taking process.
* It was very necessary to improve the fingerprint identification system for implementation on large databases, e.g., of an institute or a country.
* In this project, the minutiae algorithm is used to develop the identification system which is faster in implementation than any other available today in the market.
* Using the fingerprint scanner does not take into consideration when a person physically changes. A person's finger changes sizes then the fingerprint scanner does not take this into consideration.

**1. An overview of biometrics:**

Biometrics has been a concern for centuries. Proving one’s identity reliably was done using several techniques. From prehistory man knew the uniqueness of fingerprints, which meant that signatures by fingerprints were sufficient to prove the identity of an individual. Indeed, two centuries before Christ, the Emperor Ts-In-She authenticated certain sealed with the fingerprint. The advance of technology is always inspired by the practical applications, and the emergence of automatic biometrics technology is rooted in the requirement for real-world security applications. Whether this new technology can last for a long time will be decided by how well it can solve security problems. Although biometric technology is at the development stage, it has been implemented in various applications and some of them work well. Along with the widespread application of biometrics technology, more funds and more attention are being given to this ascending technology. Biometrics refers to the automatic identification of a person based on his/her physiological or behavioral characteristics. Today a variety of biometric technologies are used, each with its own strengths to make it more appropriate than others for certain types of applications.

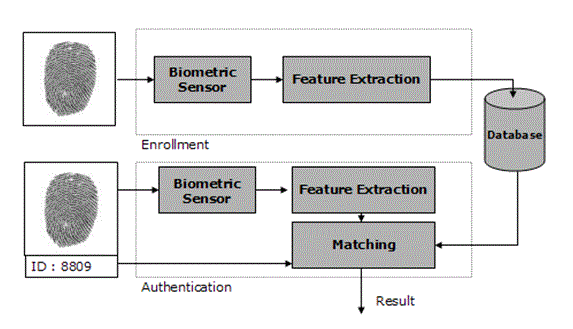


*Fig 1.1 : How biometric system works*

1

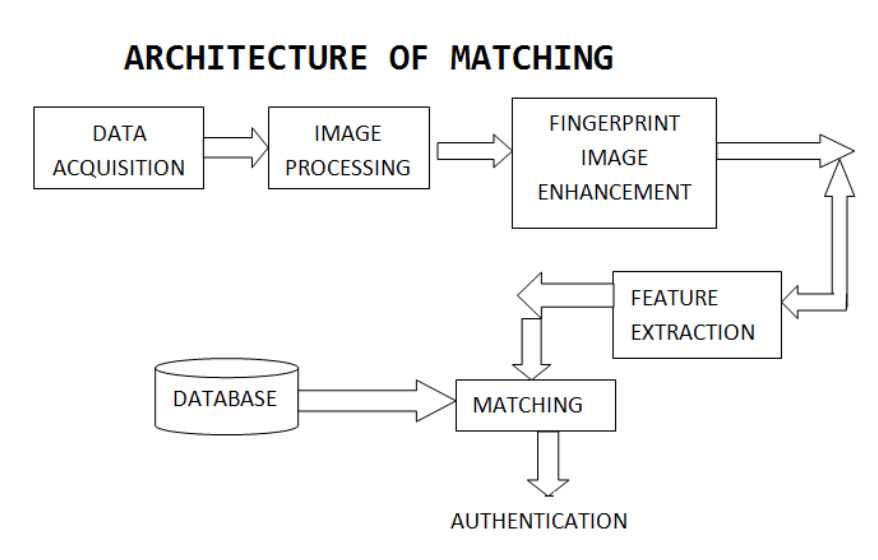
# Biometrics for Fingerprint

Biometrics are unique physical characteristics, such as fingerprints, that can be used for automated recognition. The biometric system is not new in this world. It was there, since the 14th century. At that period, China had introduced fingerprinting and had started taking fingerprints of its merchants and their children to distinguish them from all others. Fingerprinting has evolved since then. There's evidence that fingerprints were used on clay tablets during Babylonian business transactions in 500 BC. In 1969, the Federal Bureau of Investigation (FBI) pushed for automated fingerprint identification which led to the study of minutiae points to map unique patterns and ridges. By 1975, the first scanners to extract fingerprint points were prototyped, funded by the FBI. Starting in the 1990s, biometric attendance systems had commercial applications. All of these measures are put in place to protect the users from the possibility of fraud. It is the ease of use, efficiency, and time factor, which have contributed to the growth and popularity of fingerprint biometrics. According to the Anderson survey, 3% of the companies are now virtual and by 2010, 40% of the companies will be virtual. This will fingerprint all pervasive in a few years’ time and people may even not venture out to fraud. But lately spoofing have raised a few questions which need to be taken care of. The primary goal of using these technologies in businesses was to restrict access to vital assets in both a physical and logical manner. Several businesses have developed fingerprint sensors and used them in their workplaces as a means of protecting their assets and resources from unauthorized access. The security of storing a person’s fingerprints in a system is always going to be an issue because fingerprints are unique. The software’s dashboards and user interfaces (UX) must be user-friendly and should not necessitate extensive training for staff before they become comfortable with them. The software of the biometric attendance system enables organizations to ensure that data may be accessed at any time and from any location. In a biometric attendance system, there are two types of technology: fingerprint and retinal. A fingerprint picture can be captured and stored using a variety of methods, but the image-based system is the most prevalent. This form of biometric attendance system is less precise, but because the technology is simpler, it is less expensive.



*Figure 2.1: Biometric system for fingerprint scanning*

2



*Figure 2.2 : Fingerprint Enrollment and Verification System*

# Biometric Models

## Finger Scan Technology

A fingerprint refers to an impression left by the friction ridges of a human finger. They are easily deposited on surfaces like glass or metal or polished stone by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges. Human fingerprints are detailed, nearly unique, difficult to change, and remain the same over the life of an individual, making them ideal long-term markers of human identity. This is why they are used for identification purposes. Fingerprint image acquisition is the most important step in an automated fingerprint authentication system, as it assesses the final fingerprint image quality, which has a crucial impact on the overall system performance. 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. The live scan is digitally processed to come up with a unique biometric template (a collection of extracted features) which is stored and used for matching. Once this is done, there are matching algorithms that are used to compare these previously stored templates against candidate fingerprints for authentication purposes. In order to do this either the original image must be directly compared with the candidate image or certain features must be compared. Fingerprint matching techniques can be placed into two categories: minutiae based and correlation-based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties for this approach when the fingerprint is of such low quality such that accurate extraction of minutiae points is difficult Fingerprint scanning technology has several advantages. For one, it allows fast and easy one-finger access to unlock devices. As mentioned earlier, it is a good way to identify unique individuals and it is not easy to fake fingerprints and break the system. Also, unlike your signature, you can’t forget your fingerprint. The benefits include fraud protection, user confidence and retention, time/cost efficiencies, and the ability to extend services to non-local customers.

4

1. **Biometrics Applications**

* A biometric system is a system that allows the recognition of a certain characteristic of an individual using mathematical algorithms and biometric data. There are several uses of biometric systems. There are systems that require enrollment upstream of users. Other identification systems do not require this phase. Enrollment mode is a learning phase that aims to collect biometric information about who to identify.
* Several data acquisition campaigns can be carried out to ensure a certain robustness of the recognition system to temporal variations of the data. During this phase, the biometric characteristics of individuals are captured by a biometric sensor, and then represented in digital form (signatures), and finally stored in the database. The processing related to the enrollment has no time constraint, since it is performed “off-line.”
* The verification or authentication mode is a “one-to-one” comparison, in which the system validates the identity of a person by comparing the biometric data entered with the biometric template of that person stored in the system’s database. In such a mode, the system must then answer the question related to the identity of the user. Currently the verification is carried out via a personal identification number, a user name, or a smart card.
* The identification mode is a “one-to-N” comparison, in which the system recognizes an individual by matching it with one of the models in the database. The person may not be in the database. This mode consists of associating an identity with a person.
* By applying the variable score threshold to similarity scores, the pairs of false recognition rate (FRR) and false acceptance rate (FAR) can be calculated. The false recognition rate, or FRR, is the measure of the likelihood that the biometric system will incorrectly reject an access attempt by an authorized user. It is stated as the ratio of the number of false recognitions divided by the number of identification attempts. On the other hand, the false acceptance rate, or FAR, is the measure of the likelihood that the biometric system will incorrectly accept an access attempt by an unauthorized user. It is stated as the ratio of the number of false acceptances divided by the number of identification attempts

1. **Conclusion**

In this research, an attempt has been made for a technology solution based on the uniqueness of fingerprint image as a biometric, for user identification and authentication to secure the attendance. This is a very effective and robust method for preventing spoofing, and duplicate entries of users, when giving the attendance. Research leading to this application using fingerprint image as a biometric is very premature at this time. Standards are yet to be established to capture high quality fingerprint images. The Minutiae technique is a good method for processing and extraction of key features of fingerprint image and not difficult to implement compared to other feature extraction techniques like RFID etc. Complex algorithms for capturing ridges and valleys may be researched in depth. Universities and technology solutions will contribute towards this goal.

5

**References**

* 1. M. M. H. Ali , highlighted on previous studies on a basic fingerprint recognition system. In this paper, summaries of fingerprint databases with characteristics are given. "Overview of fingerprint recognition system," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, 2016
* 2. V. J. Rathod, proposed techniques like phase-based image matching in Fingerprint Recognition system designed in order to reduce the False Acceptance Rate (FAR) and False Rejection Rate (FRR) and to improve the performance of the system. In this paper gaps are also identified and an optimum approach is considered. Published in1892 in the book Finger Prints.
* 3. C. C. Liao and C. T. Chiu , proposed fingerprint matching method by combining different features like minutiae and ridge. By performing an experiment on FVC2002 database, the equal error rate (EER) is around 0.82 published in recfaces blog 18 June 2021.
* 4. R. Oulhiq , proposed a use of number of bifurcations in an image localities and also use of Artificial Neural Network (ANN) for classification. Issued in rama chellappa ,2019

6