

# An Attendance Monitoring System Using Biometrics Authentication

Anchal V Khetan

Computer Science engg dept., Ballari Institute of Technology and Management  
Bellary-583103, India  
khetanaanchal15@gmail.com

**Abstract**— Biometric technology that involves the identification and verification of individuals by analysing the human fingerprint characteristics has been widely used in various aspect of life for different purposes, most importantly as regards this study the issue of employee attendance. The main aim of this paper is to develop an accurate, fast and very efficient automatic attendance system using fingerprint verification technique. We propose a system in which fingerprint verification is done by using extraction of minutiae technique and the system that automates the whole process of taking attendance. The study was conducted using a quantitative approach by designing a questionnaire as the data collection instrument based on fingerprint matching biometric technologies. The survey involved 6 employees based on stratified random sampling technique. The results however show that fingerprint biometric identifier was found suitable for the employee attendance management system of the organization.

**Keywords**— Biometrics, fingerprint, employee attendance, identifier, etc..

## I. INTRODUCTION

In many institutions and organization the attendance is very important factor for various purposes and its one of the important criteria that is to follow for students and organization employees. The previous approach which included manually taking and maintaining the attendance records was very inconvenient task. After having these issues in mind we develop an automatic attendance system which automates the whole process of taking attendance and maintaining it.

We already know about some commonly used biometric techniques used for objective identification , verification are like iris recognition, voice identification, fingerprint identification, DNA recognition, etc. Biometrics techniques are widely used in various areas like building security, etc.

A fingerprint is an impression of the friction ridges on all parts of the finger. A friction ridge is a raised portion of the epidermis on the palmar (palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin. These are sometimes known as

"epidermal ridges" which are caused by the underlying interface between the dermal papillae of the dermis. The term fingerprint refers impressions transferred from the pad last joint of fingers and thumbs, though fingerprint cards also typically record portions of lower joint areas of the fingers (which are also used to make identifications).

It is believed that no two people have identical fingerprint in world, so the fingerprint verification and identification is most popular way to verify the authenticity or identity of a person wherever the security is a problematic question.

The reason for popularity of fingerprint technique is uniqueness of person which arises from his behaviour; personal characteristics are like, for instance uniqueness, which indicates that each and every fingerprint is unique, different from one other. Universality, that means every person hold the individual characteristics of fingerprint.

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

- An arch is a pattern where the ridges enter from one side of the finger, rise in the centre 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. Scientists have found that family members often share the same general fingerprint patterns, leading to the belief that these patterns are inherited.

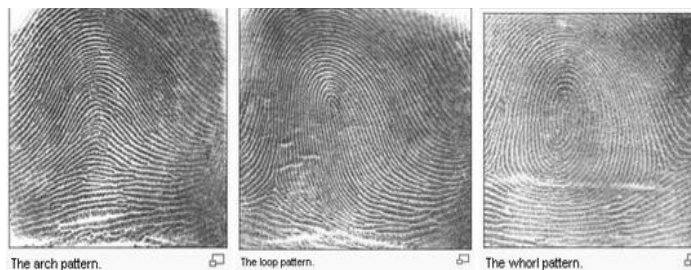


fig. 1 Fingerprint patterns

## II. HISTORY

The earliest form of Biometrics appeared on the scene back in the 1800's. Alphonse Bertillon, a Persian anthropologist and police desk clerk, developed a method for identifying criminals that became known as Bertillon age. Bertillon age was a form of anthropometry, a system by which measurements of the body are taken for classification and comparison purposes. Bertillon's system of anthropometry required numerous and precise measurements of the bony parts of a humans anatomy for identification. It also involved recording shapes of the body in relation to movements and differential markings on the surface of the body such as scars, birth marks, tattoos, etc. Bertillon estimated that the odds of duplicate records were 286,435,456 to 1 if 14 traits were used. This was the primary system of criminal identification used during the 19th century.

Bertillon's system of identification was not without fault. For example, it relied heavily on precise measurements for identification purposes, and yet two people working on measurements for the same person would record different findings. The measurements taken were also only thought to be unique and accurate in adulthood. Therefore, someone who committed a crime prior to adulthood would not have their measurements on record. Additionally, it turned out to be the case that the features by which Bertillon based his identification system were not unique to any one individual. This led to the possibility of one person being convicted of another person's crimes. This possibility became abundantly clear in 1903 when a Will West was confused with a William West. Though it would later turn out to be the case that the two were identical twins, the issues posed by the Bertillon age system of identification were clear.

Because of the amount of time and effort that went in to painstakingly collecting measurements and the overall inaccuracy of the process, Bertillon age was quickly replaced when fingerprinting emerged on the scene as a more efficient and accurate means of identification. Fingerprinting, as a means of identification, proved to be infallible. It was accepted that each individual possessed a uniquely identifiable

and unchanging fingerprint. This new system of identification was accepted as more reliable than Bertillon age.

Fingerprinting can be traced as far back as the 14th century in China. Though the use was most likely as a signature and the unique identification abilities of the fingerprint not entirely known. Fingerprints were first looked at as a form of criminal identification by Dr. Henry Faulds who noticed fingerprints on ancient pottery while working in Tokyo. He first published his ideas about using fingerprints as a means of identifying criminals in the scientific journal, *Nature* in 1880. William Herschel, while working in colonial India, also recognized the unique qualities that fingerprints had to offer as a means of identification in the late 1870's. He first began using fingerprints as a form of signature on contracts with locals. Sir Francis Galton, who had been privy to Faulds research through his uncle, Charles Darwin, would also be credited as making significant advancement to fingerprint identification. Galton ascertained that no two fingerprints were alike, not even on a set of identical twins. He noted that differentiating characteristics could be best observed in the ridge of a fingerprint and that this fingerprint would remain reliable and unchanging and could be used for identification throughout an individual's life. However, it had never been officially recognized as to which of these three men was the first to discover fingerprinting as a means of identification.

The Henry Classification system, named after Edward Henry who developed and first implemented the system in 1897 in India, was the first method of classification for fingerprint identification based on physiological characteristics. The system assigns each individual finger a numerical value (starting with the right thumb and ending with the left pinky) and divides fingerprint records into groupings based on pattern types. The system makes it possible to search large numbers of fingerprint records by classifying the prints according to whether they have an "arch," "whorl," or "loop" and the subsequently assigned numerical value. In 1901 the Henry system was introduced in England. In 1902 the New York Civil service began testing the Henry method of fingerprinting with the Army, Navy, and Marines all adopting the method by 1907. From this point on, the Henry System of fingerprinting became the system most commonly used in English speaking countries.

## III. FINGERPRINT BIOMETRIC SYSTEM

Fingerprint recognition is the technology that verifies the identity of a person based on the fact that everyone has unique fingerprints. It is one of the most heavily used and actively studied biometric technologies.

### 1. WHY FINGERPRINTS?

The cost of a fingerprint based biometric system is quite low in comparison to others like iris and face readers. Fingerprint based systems are quite strong and can be deployed across any kind of environment. This system is less intrusive than iris or retina scans. Most people find it unacceptable to have their pictures taken by video cameras or to speak into a microphone. Finger based systems are more user friendly. Besides, the ability to enrol multiple fingers makes this a very flexible option. It is a proven technology and has been in use for a long time as compared to other nascent technologies.

## 2. PRINCIPLES OF FINGERPRINT BIOMETRICS

A fingerprint is made of a number of ridges and valleys on the surface of the finger. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The ridges form so-called minutiae points, ridge endings (where a ridge end) and ridge bifurcations (where a ridge splits in two). Many types of minutiae exist, including dots (very small ridges), islands (ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges), ponds or lakes (empty spaces between two temporarily divergent ridges), spurs (a notch protruding from a ridge), bridges (small ridges joining two longer adjacent ridges), and crossovers (two ridges which cross each other).

The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. There are five basic fingerprint patterns: arch, tented arch, left loop, right loop and whorl. Loops make up 60% of all fingerprints, whorls account for 30%, and arches for 10%. Fingerprints are usually considered to be unique, with no two fingers having the exact same dermal ridge characteristics.

## 3. HOW DOES FINGERPRINT BIOMETRICS WORK

The main technologies used to capture the fingerprint image with sufficient detail are optical, silicon, and ultrasound. There are two main algorithm families to recognize fingerprints:

- a. Patterns: The three basic patterns of fingerprint ridges are the arch, loop, and whorl.

An arch is a pattern where the ridges enter from one side of the finger, rise in the centre 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. Scientists have found that family members

often share the same general fingerprint patterns, leading to the belief that these patterns are inherited.

Pattern matching compares the overall characteristics of the fingerprints, not only individual points. Fingerprint characteristics can include sub-areas of certain interest including ridge thickness, curvature, or density. During enrolment, small sections of the fingerprint and their relative distances are extracted from the fingerprint. Areas of interest are the area around a minutia point, areas with low curvature radius, and areas with unusual combination of ridges.

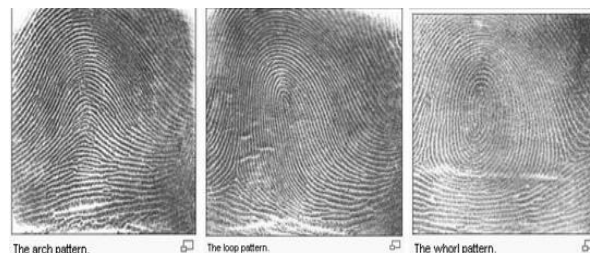


Fig. 2 Different patterns arch, loop and whorl pattern respectively

- b. Minutia features: The major Minutia features of fingerprint ridges 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. Minutia matching compares specific details within the fingerprint ridges. At registration (also called enrolment), the minutia points are located, together with their relative positions to each other and their directions. At the matching stage, the fingerprint image is processed to extract its minutia points, which are then compared with the registered template.

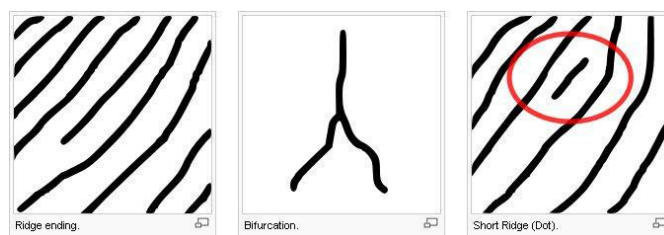


Fig. 3 Different Minutia features

- c. Issues with fingerprint systems: The tip of the finger is a small area from which to take measurements, and ridge patterns can be affected by cuts, dirt, or even wear and tear. Acquiring high-

quality images of distinctive fingerprint ridges and minutiae is a complicated task. People with no or few minutiae points (surgeons as they often wash their hands with strong detergents, builders, people with special skin conditions) cannot enrol or use the system. The number of minutiae points can be a limiting factor for security of the algorithm. Results can also be confused by false minutiae points (areas of obfuscation that appear due to low-quality enrolment, imaging, or fingerprint ridge detail). Note: There is some controversy over the uniqueness of fingerprints. The quality of partial prints is however the limiting factor. As the number of defining points of the fingerprint becomes smaller, the degree of certainty of identity declines. There have been a few well-documented cases of people being wrongly accused on the basis of partial fingerprints.

#### IV. ATTENDANCE MONITORING MODEL

Automatic attendance system using fingerprint verification technique. A fingerprint is captured by user interface, which are likely to be an optical solid state or an ultrasound sensor. Generally, there are two approaches used for fingerprint verification system among them first one is Minutiae based technique, in which minutiae is represented by ending or termination and bifurcations. Other one is Image based method or matching pattern.

- a. Minutiae-based matching: This is the most popular and widely used technique, being the basis of the fingerprint comparison made by fingerprint examiners. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Minutiae-based matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings.
- b. Pattern or Image based matching: Pattern based matching uses algorithms to compare the basic fingerprint patterns like arch, whorl or loop between a previously stored template and candidate fingerprint. For this purpose image is required to be alignment in same orientation. In matching process algorithms find a central point on the fingerprint image and centre on the image. In pattern based algorithm, the template contains the type, size and orientation of pattern within the aligned fingerprint image. The candidate fingerprint image is graphically compared with the template to determine the degree to which the match.

#### V. IMPLEMENTATION OF PROCESS

This process is complete in three phases and also phase description is mentioned below:-

- Phase 1: Fingerprint scanning and registration

Fingerprint scans convert people's fingerprints into digital codes or numerical data that can be recorded in a database. Like facial recognition software, fingerprint scanning matches an individual's code against an existing database of codes in order to confirm that individual's identity. Proponents of fingerprint scanning point to the conversion of fingerprints into digital data as a privacy protection measure.

Fingerprint scanning is already in use as an identification system that replaces cards or keys: to log onto computers. Before scanning the fingerprint everyone has to fill the registration form. These forms have some of the basic details of the individual such as name, father's name, mother's name, date of birth and so on.

Fingerprint scanning:



Fig. 4 Fingerprint enrolment



Fig. 5 Registration form

#### • PHASE-2:- Fingerprint recognition or authentication

Fingerprint recognition or 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. This article touches on two major classes of algorithms (minutia and pattern) and four sensor designs (optical, ultrasonic, passive capacitance, and active capacitance).

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.

Minutiae-based fingerprint matching algorithm has been proposed to solve two problems: correspondence and similarity computation. For the correspondence problem, use an alignment-based greedy matching algorithm to establish the correspondences between minutiae. Fingerprint recognition systems have the advantages of both ease of use and low cost.

On enrolment, a user places his or her finger on the scanner, which captures a fingerprint image. The image is sent to a PC ("client"). If the image quality is acceptable, fingerprint minutiae information is extracted, and the image is then discarded. The minutiae information is sent via a secure line to the biometric server, usually located in a secure room. This information is stored in a database on the biometric server.

The system may enrol one or up to all ten fingers. Modern one-to-many systems are capable of searching as many as 20,000 templates, even more at times, in real time, within a few seconds.

To obtain access to a facility, the user places the appropriate finger on the sensor, and the captured fingerprint is sent to the client. The client extracts the minutiae information (with the fingerprint image subsequently discarded) and sends it to the biometric server. Here, the minutiae information is run in a one-to-many mode against the entire database of stored templates. If there is a match with one of the templates, the user is granted access. Alternatively, the system may go to the next level of authentication, for example: the corresponding photo of the user whose template has been matched is retrieved from the database and displayed to the operator. If the photo matches to the individual, the user is granted access.

The system sets a default False Acceptance Rate (FAR), for example, at 0.0001, meaning that there is a one in 10,000 chance that an impostor will be accepted. The system administrator may set a system FAR to a higher (for example, one in 1,000) level in order to lower the False Rejection Rate (FRR), which is the probability that a legitimate user will be rejected.

The system is convenient for the majority of users (no need to carry cards), and prevents the problems that can undermine card systems such as, the sharing of cards with unauthorized persons. The system also tracks an individual's use of the facility, i.e. records the fact that the individual was given access and the time and date of the access.

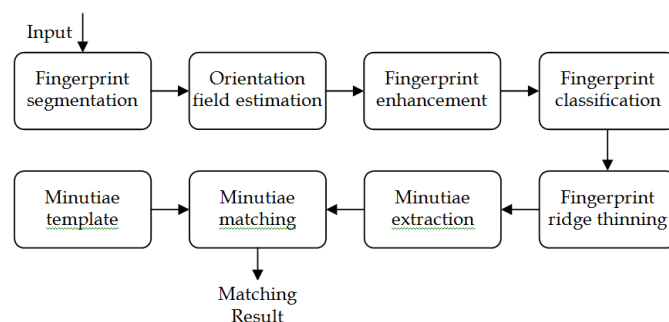


Fig. 6 Fingerprint recognition

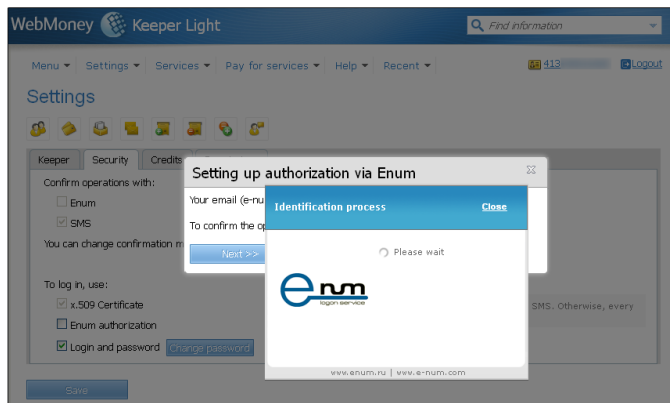


Fig. 7 Fingerprint Authorization

• Phase-3:- Attendance update:-

Employee Attendance Management software is tightly integrated with the organization's HR data. The in-time and out-time, lunch and breaks entered by the employees will help the respective authority in charge to keep in track the activities of the employees.

Employee Attendance Management System helps in keeping track of the attendance of employees based on various events like shift, late, overtime, permission, holiday working and on duty.

Single click view of all time office events like hours worked, late, permission, on duty, overtime, leave of an employee for date or month period can also be obtained from this Attendance Management system.

Employee Attendance Management Software helps to monitor the productivity of the employees and also keep a check on the Employee absenteeism which in turn helps in achieving the organization goals.

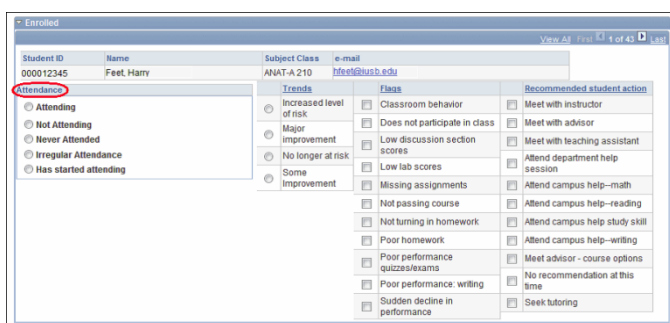



Fig. 8 Attendance updation

• Result:

The report will be generated with name of the employee matched fingerprint and stored in an attendance system. Attendance log of the month is shown in below table:



# Student Attendance List

Print

Student Name: Christina Acosta [7/7-A]

Year: 2008

H

 : Holiday

P

 : Present

A

 : Absent

W

 : Weekly Off

Month	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	P	A	
January	-	-	-	H	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	1	0	
February	-	-	-	-	-	-	-	-	-	-	-	H	-	-	-	-	-	H	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
March	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
April	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
May	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
June	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
July	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
August	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
September	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
October	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
November	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
December	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0	0
Total Present : 1 Total Absent : 0																																		

Fig. 9 Attendance list

This software not only prepare the monthly report but also shows the attendance of the individual day. It not only display the name of the present employees but it also display the employee which is absent or late on that particular day. This software also display the name of employees which is in pre plan live. The individual attendance reports is shown below:

Attendance Report				
Daniel 'Dan' Doo				
June 2012				
M	T	W	T	F
28	29	30	31	1
4	5	6	7	8
11	12	13	14	15
18	19	20	21	22
25	26	27	28	29
1.0 h	6.0 h	6.0 h	6.0 h	7.9 h
		1.0 h		1.1 h
				1.0 h
Service Type				Hours
Community				1.0
Individual Services				14.8
Occupational Therapy				4.0
Personal Care				1.1
Physical Therapy				1.0
Speech Therapy				2.0
Attendance				71.0
Total Hours				84.3
Total hours does not include overlapping service hours.				

Fig. 10 Attendance report

## VI. PRIVACY AND SECURITY ISSUES ON BIOMETRIC SYSTEMS

Since biometric data are unique and permanent characteristics of individuals, the privacy protection of biometric

authentication schemes has become a common concern of the public.

- Growing biometrics deployments and uses pose significant systemic risks to individual privacy and security
- Biometrics a lifetime permanent identifier, worse than a password (access control)
- Indiscriminate or excess collection of biometric data invites misuse
- Unauthorized secondary use of biometric data
- Poor accountability will undermine trust, acceptance and use

To achieve privacy and security we need to follow cryptographic techniques. This is called biometric encryption in this scenario.

Biometric Encryption: Rather than comparing the biometric data directly, a key is derived from these data and subsequently knowledge of this key is provided. Generate the same key from each reading of the biometric, and to make the system resilient against attacks.

#### VII. BENEFITS OF BIOMETRIC SYSTEMS

- Unique Biological Features – Biometric authentication measures a biological feature of a person like fingerprint, iris, etc. Hence it is a very effective security system and cannot be easily disguised.
- Time Saving – Unlike other identification procedures, biometric is easily accessible and time saving. Within a couple of seconds, a person's biometrics is either identified or rejected. As every office follows time management, time saving systems like biometrics have become beneficial for the office revenue
- Reduce Fraud – As biometrics cannot be shared, you cannot find anything like more than one person using the same password. This reduces fraud and provides complete security.
- Accountability - A biometric log in or entry indirectly connects the individual as responsible to any event. If there is a security breach, then the security system will provide the accurate record of who is accountable for the issue. This provides complete and true accountability and cannot be forged by others.

#### VIII. DRAWBACKS OF BIOMETRIC SYSTEMS

- False Reading – An occasional problem than occurs among biometrics is the false reading. A “false acceptance” or “false rejection” kind of technical vulnerability becomes a greatest disadvantage of biometrics.
- Copying – Nowadays, the fingerprint of a person is easily copied and used for forgeries. The biometric system scanning can also be copied and duplicated and can be controlled by another person from any corner of the world.
- Expensive – An effective biometric system is costly and is affordable only for large companies and institutions. Though biometric software is designed for complete security it is not an economically advantageous technology.
- Unreliable – Biometrics like voice recognition or iris recognition cannot be identified properly in case of sickness. If a person suffers from a throat infection or eye defect, biometrics cannot accurately identify the person and hence it is unreliable during such cases.

#### IX. APPLICATIONS

The applications of biometrics can be divided into the following three main groups.

- Commercial applications such as computer network login, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, PDA, medical records management, and distance learning.
- Government applications such as national ID card, correctional facility, driver's license, social security, welfare disbursement, border control, and passport control.
- Forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

#### X. COCLUSION AND FUTURE WORK

The proposed system will make way for perfect management of students and staff attendance and produce more accuracy. Future work on this project would include the creating of a matching algorithm that uses to mention and maintain the different type of leave such as on duty leave, leave without pay ,medical leave and soon. Also timely update the leave of the each employee when it takes leave. The efficient matching algorithm have to be developed in theory and in code so that

our goal of getting faster and more accurate matched image than with pre-existing software.

#### X11. REFERENCES

- [1] Jianjiang Feng, "Combining minutiae descriptors for fingerprint matching", Pattern Recognition, pp. 342 – 352, April 2007.
- [2] Peng Shi, Jie Tian, 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, Manisha Baswal, and Biju Gautham "Optimized Minutiae-Based Fingerprint Matching", Proceedings, 2008.
- [4] BioLink 2006. Time and attendance, Retrieved 11thDecember,2011from[http://www.m3biometrics.co.uk/Portals/2/downloads/BioTime\\_Time\\_and\\_Attendance.pdf](http://www.m3biometrics.co.uk/Portals/2/downloads/BioTime_Time_and_Attendance.pdf).
- [5] InfoTronics, Inc. 2008. Biometrics: Advantages for employee attendance verification, Michigan: Farmington Hills. Retrieved 11th November, 2011 from [www.mwtime.com/biometrics.pdf](http://www.mwtime.com/biometrics.pdf).
- [6] Jain, A., Hong, L., Pankanti, S., Bolle, R., 1997. An Identity Authentication System Using Fingerprints. Retrieved 10th June, 2012 from [http://biometrics.cse.msu.edu/Publications/Fingerprint/JainEtAlIdentityAuthUsingFp\\_ProcIEEE97.pdf](http://biometrics.cse.msu.edu/Publications/Fingerprint/JainEtAlIdentityAuthUsingFp_ProcIEEE97.pdf).
- [7] K. Asai, Y. Hoshino and K. Kiji, "Automated fingerprint Identification by minutiae-network feature- feature extraction process," IEICE transactions, Vol.J72-D-II, N0.5, pp 724-732, 1989.
- [8] Chaur-Chin Chen and Yaw-Yi Wang, "An AFIS Using Fingerprint Classification," Image and Vision Computing, 2003.
- [9] Virginia Espinosa-Dur6, "Fingerprints Thinning Algorithm," IEEE AES Systems Magazine, 2003.
- [10] U. Halici, L. C. Jain, A. Erol, "Introduction to Fingerprint Recognition,"Intelligent Biometric Techniques in Fingerprint and Face Recognition,L.C. Jain, U. Halici, I.Hayashi, S.B. Lee, S. Tsutsui (editors), CRCPress, 1999.
- [11] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S.Sandhu, "Fingerprint Verification System using Minutiae Extraction Technique," World Academy of Science, Engineering and Technology 46 2008.
- [12] Anil K. Jain, Arun Ross and Salil Prabhakar, "An introduction to biometric recognition," Circuits and Systems for Video Technology,IEEE Transactions on Volume 14, Issue 1, Jan. 2004 Page(s):4 – 20.
- [13] L. O’Gorman, "Overview of fingerprint verification technologies,"Elsevier Information Security Technical Report, Vol. 3, No. 1, 1998.
- [14]. Eric P. Kukula, Christine R. Blomeke, Shimon K. Modi, and Tephen J. Elliott, "Effect of Human Interaction on Fingerprint Matching Performance, Image Quality, and Minutiae Count", International Conference on Information Technology and Applications, pp. 771-776, (2008).