IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 1, Ver. III (Jan. 2014), PP 32-37
www.iosrjournals.org

Secured Employee Attendance Management System Using Fingerprint

Chiwa, Musa Dalah
Yobe State University, Department of Mathematics & Statistics, Damaturu, Nigeria

Abstract: *In this paper an effective employee attendance management system using fingerprint is introduced. It is used to managed the attendance of employees in any organization. All organizations and institutions are established to achieve specific objectives or goals. The identification and authentication of employee is very necessary for achieving any objective or goal. To identify and authenticate the identity of an individual employee by their names, ID numbers and signatures only are not enough, because any one can misuse other's identity and this type of problem occur very often. Fingerprint can be applied for recognizing any person, because human fingerprints are unique to each person and can be regarded as some sort of signature, certifying the person's identity. This method of employee identification and authentication will improve the attendance of employees thereby improving security, productivity and skill which will in turn improve the progress of organizations.*
Keywords: *Employee, Attendance, Fingerprint Matching.*

I. Introduction

In any organization, employee management is very important. It is an aspect widely practiced in all workplaces. Employee Identification and personal verification technologies are becoming a great concern to organizations because of increase in security breaches and transaction fraud. Here the paper has looked into an efficient employee management system using fingerprint. For this purpose the employees necessary information such as name, sex, ID number and fingerprints are compiled and stored in the Database. When attendance is calculated, the daily fingerprints are matched with the stored fingerprint by using the scanner. If fingerprint is matched, then attendance is accepted otherwise it is rejected. Fingerprints, are impression of the ridges on the end of our fingers and thumbs. Human beings have used fingerprints for personal identification for centuries, and they have used them for criminal investigations for more than 400 years. The validity of fingerprints as a basis for personal identification is thus well established. Therefore, no two persons have exactly the same arrangement of pattern, and the patterns of any one individual remain unchanged throughout life. Using fingerprint for identification and authentication is very important because of it's unique nature. No two person's fingerprint are the same and this will overcome the limitations of the existing system where one person can sign for another. Using this system, No one can thump print for another. In the paper, Section II is on some related concepts on fingerprint, section III is on proposed work using fingerprint. Section IV is on experimental results and section V is the conclusion.

II. Related Concepts

FINGERPRINT

Human fingerprint has been discovered on a large number of archaeological artifacts and historical items. It is widely accepted by the public and law enforcement agencies as a reliable means of human identification and verification. Fingerprint biometric is an automated digital version of the old ink-and-paper method used for more than a century for identification, primarily by law enforcement agencies (Malton, 2003). The biometric device requires each user to place a finger on a plate for the print to be read. Fingerprint biometric currently has three main application areas: large-scale Automated Finger Imaging Systems (AFIS), generally used for law enforcement purposes; fraud prevention in entitlement programs; and physical and computer access. A major advantage of finger imaging is the long-term use of fingerprints and its wide acceptance by the public and law enforcement communities as a reliable means of human recognition. Others include the need for physical contact with the optical scanner, possibility of poor-quality image due to residue on the finger such as dirt and body oils (which can build up on the glass plate), as well as eroded fingerprints from scrapes, years of heavy labour or mutilation. Sir William H, decided to capture the fingerprint of an individual while preparing a contract, instead of using his signature. Herschel's objective was not to authenticate the contractor, but to frighten him. Some years later, he discovered that the fingerprints characteristics remained immutable. This was may be the first observation to the fingerprints persistence. Personal contact with the document, they believed, made the contract more binding than if they simply signed it. Thus, the first wide-scale, modern-day use of fingerprints was predicated, not upon scientific evidence, but upon superstitious beliefs. As his fingerprint

collection grew, however, Herschel began to note that the inked impressions could, indeed, prove or disprove identity. While his experience with fingerprinting was admittedly limited, Sir William Herschel's private conviction that all fingerprints were unique to the individual, as well as permanent throughout that individual's life, inspired him to expand their use. Henry (2009), the British Surgeon-Superintendent of Tsukiji Hospital in Tokyo, Japan, took up the study of "skin-furrows" after noticing finger marks on specimens of "prehistoric" pottery. Sir Francis Galton published his book, "Fingerprints", establishing the individuality and permanence of fingerprints. The book included the first classification system for fingerprints. Francis's primary interest in fingerprints was as an aid in determining heredity and racial background. While he soon discovered that fingerprints offered no firm clues to an individual's intelligence or genetic history, he was able to scientifically prove what Herschel already suspected: that fingerprints do not change over the course of an individual's lifetime, and that no two fingerprints are exactly the same. Hertfordshire (2008), in United Kingdom, the fingerprint Bureau contacted experts throughout the UK and began organization of that country's first professional fingerprint organization, the National Society of Fingerprint officers. The Organization initially consisted of only UK experts, but quickly expanded to international scope and was renamed The Fingerprint Society in 1977. The initial F.F.S. behind a fingerprint expert's name indicates they are recognized as a Fellow of the Fingerprint Society. The Society hosts annual educational conferences with speakers and delegates attending from many countries. During the past three decades, Certified Latent Print Examiners (CLPE) status has become a prerequisite for journeyman fingerprint expert positions in many US state and federal government forensic laboratories. International Association for Identification (IAI) Certified Latent Print Examiners (CLPE) status is considered by many identification professionals to be a measurement of excellence. As of May 2012, the Unique Identification Authority of India operates the world's largest fingerprint system, with over 200 million fingerprint, face and iris biometric records. Unique Identification Authority of India (UIAI) plans to collect as many as 600 million multi-modal record by the end of 2014. India's Unique Identification project is also known as Aadhaar, a word meaning "the foundation" in several Indian languages. Aadhaar is a voluntary program, with the ambitious goal of eventually providing reliable national ID documents for most of India's 1.2 billion residents. (Helma & Pallavi, 2012)

UNIQUE FEATURES OF THE FINGERPRINT

According to Francis (2009), fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the epidermis on the palmar, that is palm and fingers or plantar (sole and toes) skin, consisting of one or more connected ridge units friction ridge skin. These ridges are sometimes known as "dermal ridges" or "dermal papillae".

Fingerprint Pattern

There are a number of different strategies through which fingerprint identification can be done, among which verification through minutia points is the most simple and easy. According to the current most widely used Galton–Henry system, the fingerprint is divided into five classifications.

(i) Arch: Fingerprint lines start from side of the finger and end at the other side, do not return and on the core points and delta point.
(ii) Tented Arch: Like an arch fingerprint, but graphic Center upward rise in the vertical direction, equivalent to a core and a delta on the same vertical line.
(iii) Left Loop: Circular pattern that is fingerprint lines access from one direction then back from the same direction after a rotation around. To the left is Left Loop. There is a core and a delta at the lower left.
(iv) Right Loop: To the right is Right Loop. There is a Core and a delta at the lower right.
(v) Whorl: At least one fingerprint stripe rotate into a closed curve around the center, there are two core points in center, a triangular point on each side when the cores are not in the same vertical line, here will form a double helix.

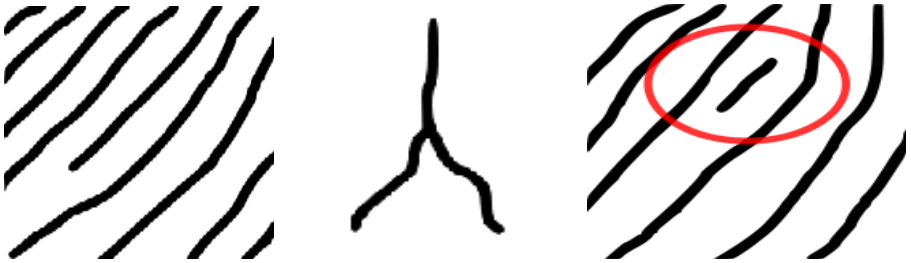
Fig. 1: Example of a fingerprint recognition (Francis, 2009).

The minutia based algorithm is widely used for fingerprint authentication. It focuses on the endings of ridges and bifurcations. Consequently the central area in fingerprint image is very important and this algorithm keenly

relies on the quality of the input images. Global and local characteristics of fingerprints are used for identification of individuals (as shown in figure 1). Global features are the ones that can be seen with naked eye like ridges, pattern area and delta while local characteristics are the minutia points.

Minutiae 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. (as depicted in Fig 2, a, b and c respectively). Minutiae and patterns are very important in the analysis of fingerprints since no two fingers have been shown to be identical.



(a) Ridge ending (b) bifurcation (c) short ridge

Fig. 2: a, b and c (Francis, 2009)

The minutia based algorithm is widely used for fingerprint authentication. It focuses on the endings of ridges and bifurcations. Consequently the central area in fingerprint image is very important and this algorithm keenly relies on the quality of the input images. Global and local characteristics of fingerprints are used for identification of individuals. Global features are the ones that can be seen with naked eye like ridges, pattern area and delta while local characteristics are the minutia points. Fingerprint ridges are not continuous as there are a number points at which ridges change and end and these points are called minutia points. The unique identifying features are provided by these minutia points. A raw image is taken from the sensor and algorithms are implemented on the image to enhance it and further extract the minutia points directly from this representation. This procedure provides a much more efficient and reliable result as compared to other methods of fingerprint verification.

FINGERPRINT MATCHING

According to Francis (2009), Fingerprint matching is the process used to determine whether two sets of fingerprint come from the same finger. One fingerprint is stored into the database and other is employee's current fingerprint, as shown in Figure 3.

Fig. 3: Fingerprint Matching. (Francis, 2009)

The use of fingerprint for human identification and verification has been in use for a long time, because of its unique features. Many scientists have researched and proved that each individual has his own unique fingerprint and therefore the best means of human identification and verification.

III. Proposed Work

LIMITATION OF THE EXISTING SYSTEM

The limitations of the existing system is that it does not capture the fingerprint of the employees, their images and voices, that is why, one employee can sign for another, employees can come to work late and leave early. The usual use of attendance register and physical supervision are not able to solve the problem adequately. These problems can be overcome by capturing individual's fingerprint as a means of identification and verification, because of the unique nature of individual's fingerprint.

PROCEDURE

The employee's necessary information such as name, sex, ID number, fingerprint are compiled and stored in the database. When attendance is calculated, the daily fingerprints are matched with the stored fingerprint by using the scanner. If fingerprint is matched, then attendance is accepted otherwise it is rejected.

IV. Experimental Results

The requirements of this system are:-

- The software will record staff information and their fingerprints.
- The software allows users to sign in and out during working hours.
- The software stops recording information once closing time is due.
- Those staff that are absent are recorded. When a staff is absent without genuine reason for:
  - 15 day, a verbal warning is issued.
  - 29 days, a written warning is issued.
  - 45 days, query/termination of appointment.
- The software should have a Database Management System (DBMS) so that staffs information can be Searched, Deleted, Added or Modified.
- In addition to the DBMS the software should be able to generate a comprehensive report of the staff and those on each category of penalty.

V. Results

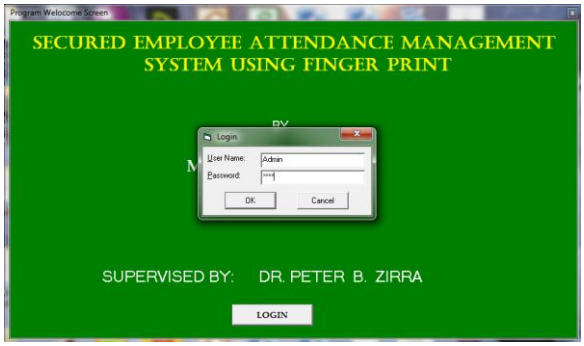


Fig 4.: Login Window

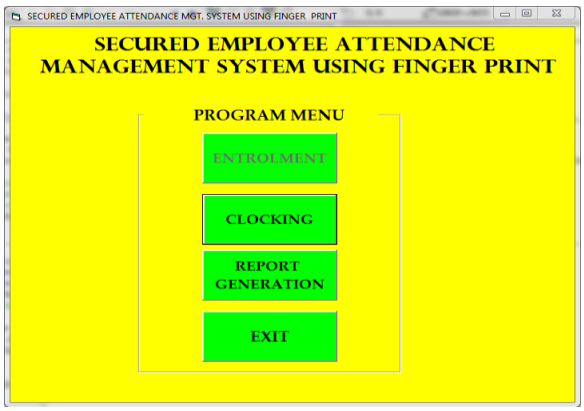


Fig.5: Program Menu

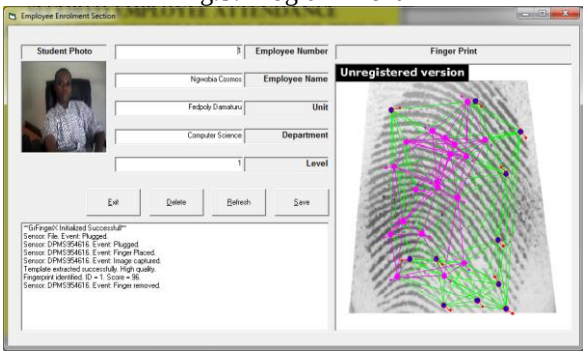


Fig. 6: Employee Enrolment

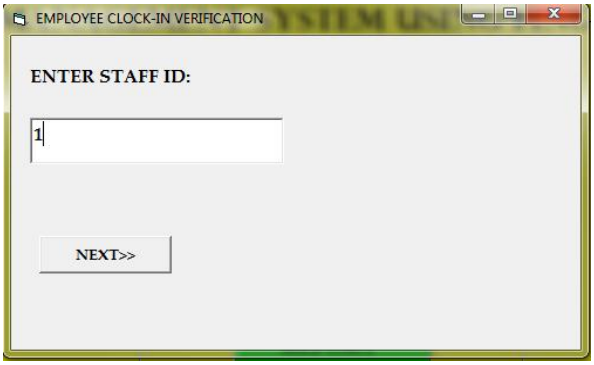


Fig. 7: Employee Clock- in Verification

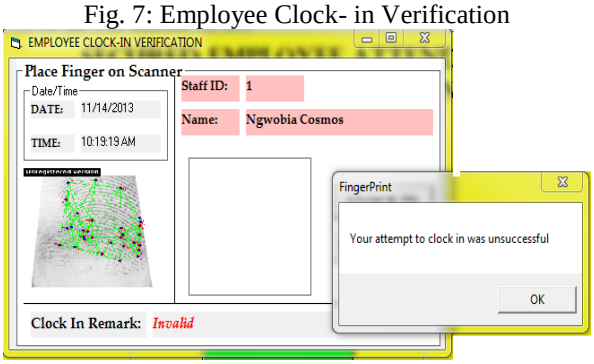


Fig.8: Employee Invalid Clock- in Window

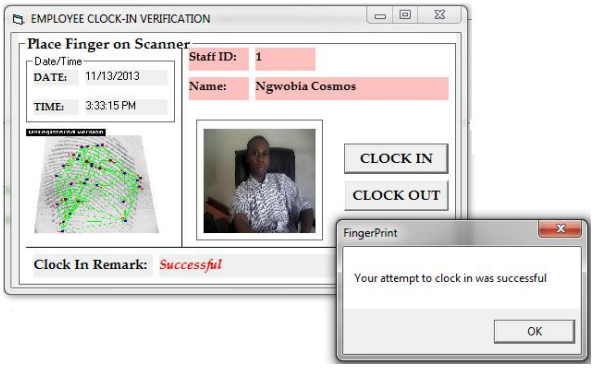
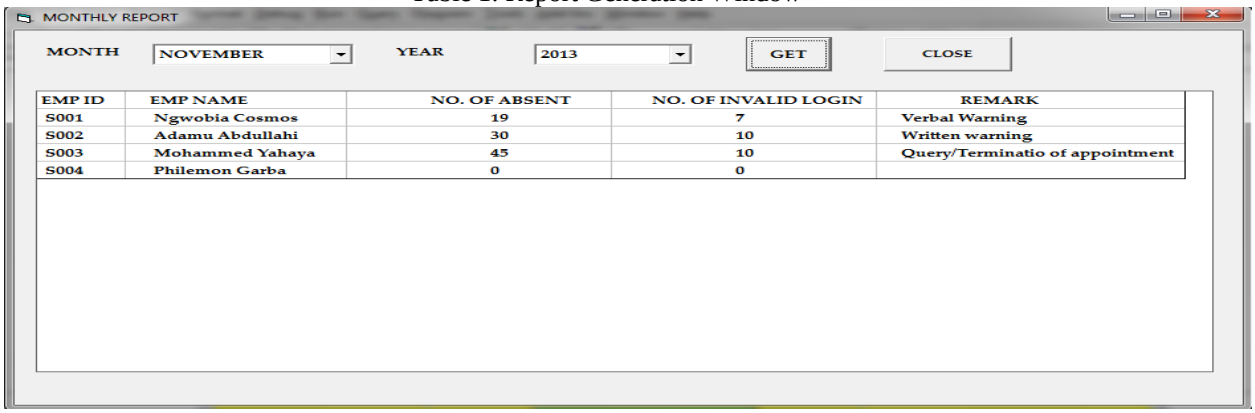


Fig. 9: Employee Successful Clock- in Window

Table 1: Report Generation Window



VI. Analysis of Results

Fig. 4. is the login window where the user will be prompted to put his username and password in order to login.
Fig. 5. is the program menus which consist of:

- Enrolment Button
- Employee Clock-in/Clock-out Button

- Report Generation Button
- Program Exit Button

Fig. 6. is the employee enrolment where a new employee will be registered given his/her ID number, Name, Department, Level, Passport and Fingerprint will be captured.
Fig. 7. is the clock-in/clock-out verification window for taking the time an employee sign-in and sign-out from duty.
Fig. 8. and 9. are the responses for valid and unsuccessful clock-in/clock-out.
Finally Table 1 is the report generation window which is the section that analysis the performance of the employees over a period of time of duties. It track the number of times an employee was absent from duty as well as invalid login attempts. The program at this point uses this information to draw the type of penalty to be given to the defaulted employee. The penalties are categorized as follows:

i Verbal warning: which is given as result of an employee absents for more than fourteen (15) times in a month.
ii Written warning: which is given as result of an employee absents for more than twenty nine (29) times in two months.
iii Written Query/Termination of Appointment: which is as result of the employee being absent from duty for more than forty- five (45) times. This may lead to termination of employee's appointment if he/she fails to give a cogent reason(s) for being absent from duty.

FINDINGS

The results have indicated that attendance of employees can be managed by this system. The thump print of employees can be enrolled and verified by using the system. No one can thump print for another. Absentees can be easily identified and necessary measured can be taken to improve attendance. The thump print can serve as a check because if an employee/person attempt to thumb print for another employee, the system will disallow and record invalid entry for that employee after displaying unsuccessful clock-in/clock-out message.

VI. Conclusion

The development of any organization depends highly on the effective attendance management of its employees. This will provide the necessary security and skills that is required for the progress of the organization. Different techniques are been applied for managing the attendance of employees but they have been found not to solve the problem of employee attendance. Employees come to work late and leave early, some sign attendance for others and some does not come to work but still receive wages/salaries. These problems can be solve by using biometric authentication technology using fingerprint since a person's biometric data is undeniably connected to its owner, is non-transferable and unique for every individual. The system has been integrated using fingerprint biometric technology that will efficiently enable organizations manage the attendance of their employees which will greatly improve the progress of organizations.

References

[1]. Hemlata, P. and Pallavi, A. International Journal of Electrical, Electronics and ComputerEngineering 1: 37-40, 2012
[2]. Henry, F. Study of fingerprint identification. McGraw-Hill Books. Inc: USA, 2009
[3]. Francis, G. Fingerprint recognition McGraw-Hill Books. Inc: USA, 2009
[4]. Griaule, B. American Libraries, Journal of fingerprint in United State of America, 354(3):
[5]. 23-25, 2008
[6]. Chikkeru, S. Ratha, N.K., Connel, j. & Bolle, R.M. Generating cancelable fingerprint templates IEEE Transaction on pattern analysis and machine intelligence. 29(4), 2007
[7]. Hertforshire, N. Fingerprint notification, McGraw-Hill Books Inc: USA, 2008
[8]. Hide, S. overview of fingerprint verification technologies, Elsevier information Security Technological Report, 3(1), 2007
[9]. Abdalla, U. A. Information systems design and programming. National Open University Pamma press, Akure, Nigeria, 200-2001, 2006
[10]. Malton, D. Handbook of fingerprint recognition, Springer New York, 2003
[11]. IAI, Techniques for students research information design and application, Prentice Hall: USA, 2000
[12]. William, C. Information Security (Dictionary of Concepts Standards and Terms), McMillan Publishers Limited; U.S.A, 1996