Fingerprint-Based Attendance Management System

[1]Sangeetha.J, [2]Sivaranjani.S, [3]Shalini.J
[1, 2, 3] Student, Department of CSE, Panimalar Institute of Technology
Chennai, Tamil nadu, India

***Abstract*— In recent time, there has been high level of impersonation experienced on a daily basis in both privateand public sectors, the ghost worker syndrome which has become a menace across all tiers of government, employers concerns over the levels of employee absence in their workforce and the difficulty in managing student attendance during lecture periods. Fingerprints are a form of biometric identification which is unique and does not change in one's entire lifetime. This paper presents the attendance management system using fingerprint technology in a university environment. It consists of two processes namely; enrolment and authentication. During enrolment, the fingerprint of the user is captured and its unique features extracted and stored in a database along with the users identity as a template for the subject. The unique features called minutiae points were extracted using the Crossing Number (CN) method which extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhoods of each ridge pixel using a 3 x 3 window. During authentication, the fingerprint of the user is captured again and the extracted features compared with the template in the database to determine a match before attendance is made. The fingerprint-based attendance management system was implemented with Microsoft's C# on the. NET framework and Microsoft's Structured Query Language (SQL) Server 2005 as the backend. The experimental result shows that the developed system is highly efficient in the verification of users fingerprint with an accuracy level of 97.4%. The average execution time for the developed system was 4.29 seconds as against 18.48 seconds for the existing system. Moreover, the result shows a well secured and reliable system capable of preventing impersonation.**

***Keywords* — fingerprint, attendance management, enrolment, authentication, Crossing Number, minutiae score**)

I. INTRODUCTION

It is expected today that an individual who wants to authenticate himself for a service must have a token and/or password for example identity card, ATM card, driving license, health card and so on. Carrying different cards and remembering passwords for different services is a significant issue for individuals and organizations. A secure and effective identity management system plays an important role in the successful deployment of an attendance management system. To make the identity management system more secure and reliable for authentication, biometrics data are integrated in the attendance management systems [1].

Biometrics technologies verify identity through characteristics such as fingerprints, faces, irises, retinal patterns, palm prints, voice, hand -written signatures, and so on. These techniques, which use physical data, are receiving attention as a personal authentication method that is more convenient than conventional methods such as a password or ID cards because it uses data taken from measurements and such data is unique to the individual and remains so throughout one's lifetime [2].

In these technologies, fingerprint becomes the most mature and popular biometrics technology used in automatic personal identification. The reason for the popularity of fingerprint verification is that fingerprints satisfy uniqueness, stability, permanency and easily taking [3].

In this paper, an attempt was made to look at the prevalence in the high level of impersonation experienced on a daily basis in both private and public sectors, the ghost worker syndrome which has become a menace across all tiers of government, employers concerns over the levels of absence in their workforce and difficulty in managing student attendance during lecture periods. Sequel to this, a fingerprint-based Attendance Management System was developed to provide a faster, more secure, and more convenient method of user verification than passwords and tokens can provide for a reliable personal identification.

II. ATTENDANCE MANAGEMENT

Attendance management is the act of managing attendance or presence in a work setting to minimize loss due to employee downtime. Attendance control has traditionally been approached using time clocks and timesheets, but attendance management goes beyond this to provide a working environment which maximizes and motivates employee attendance [4].

Attendance management is a major part of today's human resource systems; take organization towards better human resource practice, systems and excellence, hence regular attendance and punctuality are expected of all employees or candidates in a work setting. Unsatisfactory attendance caused by unscheduled absences and tardiness cause a disruption in work, affects productivity, and creates morale problems when workloads are shifted to other employees [5].

Moreover, in many institutions, and academic organizations, attendance is also a very important criteria which is used for various purposes. These purposes include record keeping, assessment of students, and promotion of optimal and consistent attendance in class. In developing countries, a minimum percentage of class attendance is required in most institutions and this policy has not been adhered to, because of the various challenges the present method of taking attendance presents. This traditional method involves the use of sheets of paper or books in taking student attendance. This method could easily allow for impersonation and the attendance sheet could be stolen or lost. Taking of attendance is time consuming and it is difficult to

ascertain the number of students that have made the minimum percentage and thus eligible for exam. Thus, there is a need for a system that would eliminate all of these trouble spots.

Types of Attendance Management System

Attendance Management falls into two categories namely: Conventional and Automated methods.
Conventional methods include time sheet, attendance register and time clock. Time sheets are documents, electronic or otherwise that record what time was spent by the employee on what tasks. Attendance register is an official list of people who are present at an institution or organization. Time clock which is a mechanical (or electronic) time piece used to assist in tracking the hour worked by an employee of a company.
Automated methods include Barcode system attendance system, magnetic stripe attendance system, Radio Frequency Identification (RFID) and the biometric attendance system [6].

The barcode attendance system requires that every employee is issued a badge/card in which there is a barcode. In order to check into or out of the company, the badge/card is swapped on the time clock, and the data is captured by the clock. In the magnetic stripe attendance system, data is encoded in the magnetic stripe of the employee card. When the card, is swiped through the employee time clock, the information in the card's magnetic stripe is recorded by the time clock. This system reads one card at a time and also requires contact with the reader. Radio-frequency identification (RFID) is a technology that uses radio waves to transfer data from an electronic tag, called RFID tag or label, attached to an object, through a reader for the purpose of identifying and tracking the object. The ID cards of the employees is embedded with RFID tag which is read by a reader. This RFID system is interfaced to a database through a computer. Each employee uses an RFID card and the reader records the data when the employee enters or exits. In biometric Attendance system, there is attendance

Software that is paired with a time clock for employees which uses biometric technology for authentication purposes. When these systems are in use, the employees can use their biometric data such as finger prints for clocking in and clocking out. This method has the great benefit that the entire process is easy as well as quick. Other advantages include elimination of the cost previously incurred in getting the employees cards.

III. RELATED WORKS

[7] proposed an embedded computer-based lecture attendance management system where a single-chip computer based subsystems (an improvised electronic card and the card reader) were interfaced serially to the serial port of the digital computer. The electronic card is a model of a smart card containing the student identity (ID-Name, Matriculation Number and five pin encrypted code). The student ID is authenticated by the card reader which compares the entrance code with the encrypted code on the card swiped through the card reader. The student is granted and/or denies specific lecture attendance based on the result of the comparison by the backend software system running on the PC to which the card reader is serially interfaced. The system though provided a simplified, low cost embedded computer based system solution to the management of lecture attendance problem in developing countries but does not eliminate the risk of impersonation. The system is devise-based in which students have to carry RFID cards and also the RFID detectors are needed to be installed.

[8] proposed a real time computer vision algorithms in automatic attendance management systems using Computer vision and face recognition algorithms and integrating both into the process of attendance management. The system eliminates classical student identification such as calling student names, or checking respective identification cards, but still lacks the ability to identify each student present in class thereby providing a lower recognition rate because facial images are subject to change between the time of enrolment and time of verification and also poses a bigger financial burden during installation and does not offer any privacy protection.

In [2], a wireless attendance management system based on iris recognition was proposed using Daugman's algorithm. The system uses an off-line iris recognition management system that can finish all the process including capturing the image of iris recognition, extracting minutiae, storing and matching but it is difficult to lay the transmission lines where topography is bad.

IV. SYSTEM OVERVIEW

This proposed system introduces a new automatic attendance management system, which integrates fingerprint authentication into the process of attendance management for both staff and student. It is made up of two processes namely; enrolment and authentication. During enrolment, the biometrics of the user is captured and the minutiae data are extracted and stored in a database as a template for the subject along with the user's ID. The objective of the enrolment module is to admit a user using his/her ID and fingerprints into a database after feature extraction. These features form a template that is used to determine the identity of the user, formulating the process of authentication. The enrolment process is carried out by an administrator of the attendance management system. During authentication, the biometrics of the user is captured again and the extracted features are compared with the ones already existing in the database to determine a match. After a successful match, attendance is marked against the user's id used in matching the templates.

The work utilized a fingerprint reader as the input to acquire images, developed program that has fingerprint recognition and identification system as well as database to store user's information. The database comprises the fingerprint templates and other bio-data of the users together with the attendance records made by the users. Figure 1 shows the architecture of the proposed attendance management system.

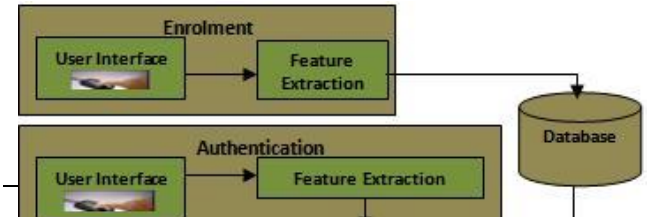

Figure 1. Architecture of the proposed fingerprint-based attendancemanagement system

V. SYSTEM ARCHITECTURE

The design of the fingerprint-based attendance management system is made up of the following:

i. Enrolment module
ii. Authentication Module
iii. System database.

Enrolment module

The task of enrollment module is to enroll users and their fingerprints into the system database. During enrolment, the fingerprint and other bio-data of the user is captured and the unique features are extracted from the fingerprint image and stored in a database as a template for the subject along with the user's ID. Staff bio data to be captured includes: employee number, surname, other names, sex, position, staff type, phone number, email, department and passport photograph. Student bio data includes: matriculation number, surname, other-names, sex, department, level, studentship, phone number and passport photograph. To improve the quality of a captured image during enrolment/registration, two image samples per fingerprint used are captured for a higher degree of accuracy.

When the fingerprint images and the user name of a person to be enrolled are fed to the enrollment module, a minutiae extraction algorithm is first applied to the
fingerprint images and the minutiae patterns (features) are extracted. These features form a template that is used to determine the identity of the user, formulating the process of authentication. The enrolment process is carried out by an administrator of the attendance management system. The enrolment and registration phase is an administrative phase. The user fingerprint as well as other bio-data is stored for the first time into the database for registration. The courses, practicals, tests, lecturers and exams are also registered at this phase. All data and information required for the proper recording of attendance are enrolled in this module.

The most commonly employed method of minutiae extraction is the Crossing Number (CN) [9] upon which this research is based. It involves the use of the skeleton image where the ridge flow pattern is eight-connected. The minutiae are extracted by scanning the local neighborhood of each ridge pixel in the image using a 3 *x* 3 window. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight- connectivity neighborhood. The CN for a ridge pixel P is given by

$$CN = 0.5\sum_{i=1}^{8} |P_i - P_{i+1}| \qquad P_9 = P_1 \qquad (1)$$

where P_i is the pixel value in the neighborhood of P.

Authentication module

The task of the authentication module is to validate the identity of the person who intends to access the system. The person to be authenticated indicates his/her identity and places his/her finger on the fingerprint scanner. The fingerprint images captured is enhanced and thinned at the image processing stage, and at feature extraction stage, the biometric template is extracted. It is then fed to a matching algorithm, which matches it against the person's biometric template stored in the system database to establish the identity. During authentication, for staff attendance, a staff supply his/her department and name, then places his/her finger over the fingerprint reader, the fingerprint recognition unit compares the fingerprint features with those stored in the database, after a successful match, the staff's employee number is sent to the database alongside the time of making such an attendance and update the status (either present/absent) of user's attendance for the day. Staff attendance is captured twice a day for both arrival and departure time.

For student attendance, the lecturer (or a designated personnel as the case may be) selects his/her department, level, course code, attendance type (for example lecture, practicals etc) and the attendance ID, then the student places his/her fingerprint on the fingerprint reader; the fingerprint recognition unit compares the fingerprint features with those stored in the database, after a successful match, the student's matriculation number is sent to the database alongside the time of making such attendance and update the status (either present/absent) of student's attendance for the class. Student attendance is captured only once for each attendance type.

Fingerprint matching approaches includes minutiae-based matching, ridge-based matching and the correlation matching approaches. However, it is believed that minutiae -based matching approach, upon which this work is based facilitates the design of a

robust, simple, and fast verification algorithm while maintaining a small template size. Minutiae-based representation is commonly used, primarily because forensic examiners have successfully relied on minutiae to match fingerprints for more than a century, minutiae-based representation is storage efficient, and expert testimony about suspect identity based on mated minutiae is admissible in courts of law [10].

Most common minutiae matching algorithms consider each minutiae as a triplet m = {x, y, θ} that indicates the (x, y) minutiae location coordinates and the minutiae angle θ [11]. Extracted minutiae from the fingerprint are together forming a point pattern in plane. Therefore matching two minutiae point patterns with each other are considered as a 2D point pattern problem. The point patterns are constructed only on positions (x, y) of minutiae in the plane. Since point patterns are based on positions of minutiae in fingerprint they form distinctive patterns. With enough points in each pattern the positions (x, y) of the minutiae are the only information that is needed for good matching results.

Let T and I be the representation of the template and input fingerprint, respectively. Let the minutiae sets of the template be given as:

$$T = \{m_1, m_2, \ldots m_m\}\ m_i = \{x_i, y_i, \vartheta_i\}\ i = 1 \ldots m \quad (2)$$

and the minutiae sets of the input fingerprint be given as :

$$I = \{m_1, m_2 \ldots m_m\}\ m_j = \{x_j\ y_j \vartheta_j\}\ j = 1 \ldots m \quad (3)$$

A minutia m_j in I and a minutia m_i in T are considered to be matched if their spatial and orientation differences are within specified thresholds r_o and θ_o. For efficient matching process, the extracted data is stored in the matrix format [12] as follows.

Number of rows: Number of minutiae points. Number of columns: 4

Column 1: Row index of each minutiae point. Column 2: Column index of each minutiae point. Column 3: Orientation angle of each minutiae point.

Column 4: Type of minutiae. (A value of '1' is assigned for termination, and '3' is assigned for bifurcation).

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. The reference points are used to convert the remaining data points to polar coordinates. The Equation 4 is used to convert the template minutiae from row and column indices to polar coordinates.

$$\begin{bmatrix} r_k^T \\ \gamma_k^T \\ \varphi_k^T \\ \theta_k^T \end{bmatrix} = \begin{bmatrix} \sqrt{(row_k^T - row_{ref}^T)^2 + (col_k^T - col_{ref}^T)^2} \\ \tan^{-1}\left(\frac{row_k^T - row_{ref}^T}{col_k^T - col_{ref}^T}\right) \\ \theta_k^T - \theta_{ref}^T \end{bmatrix} \quad (4)$$

Where for a template image,

r_k^T = radial distance of k^{th} minutiae.

γ_m^I = radial angle of k^{th} minutiae.

θ_k^T = orientation angle of k^{th} minutiae.

row_{ref}^T, col_{ref}^T = row index and column index of referencepoints currently being considered. row_k^T and col_k^T represents row index and the column index of the k^{th} minutiae. Similarly the input matrix data points are converted to polar coordinates using the Equation 5.

$$\begin{bmatrix} r_m^I \\ \gamma_m^I \\ \varphi_m^I \\ \theta_m^I \end{bmatrix} = \begin{bmatrix} \sqrt{(row_m^I - row_{ref}^I)^2 + (col_m^I - col_{ref}^I)^2} \\ \tan^{-1}\left(\frac{row_m^I - row_{ref}^I}{col_m^I - col_{ref}^I}\right) \\ \theta_k^I - \theta_{ref}^I \end{bmatrix} + rotatevalues(k,m) \quad (5)$$

Where for an input image,
$\phi^{r}{}_{m}^{I}$= radial distance of mthminutiae.
$_{m}^{I}$= radial angle of mth minutiae.
θ_{m}^{I}= orientation angle of mth minutiae.
row_{ref}^{I}, col_{ref}^{I}= row index and column index of reference points currently being considered. *Rotate values (k, m)* represents the difference between the orientation angles of
$T_k$and I_m. $row^{I}$and col^{I}represents row index and the
m m
column index of the mth minutiae. T_k and I_m represent the extracted data in all the columns of row k and row m in the template and input matrices, respectively.

The database

The attendance management system database consists of tables that stores records, each of which corresponds to an authorized person that has access to the system. Each record may contain the minutiae templates of the person's fingerprint and user name of the person or other information such as pin no as an index to the template. The database design for the system implements relational data model which is a collections of tables in which data are stored. The database was implemented in Microsoft SQL Server database (Sql Server, 2005). SQLServer is fast and easy, it can store a very large record and requires little configuration.

VI. SYSTEM PERFORMANCE AND EVALUATION

Given a fingerprint matcher, one would like to assess its accuracy and speed performance in a realistic setting. Unlike passwords and cryptographic keys, biometric templates have high uncertainty. There is considerable variation between biometric samples of the same user taken at different instances of time. Therefore the match is always done probabilistically. This is in contrast to exact match required by password and token based approaches. The inexact matching leads to two forms of errors namely: False (impostor) Acceptance Rate (FAR) and the False (genuine individual) Rejection Rate(FRR). The FAR/FRR ratios depend, among other factors, on the type of difficulty of the algorithms used in the fingerprint extraction. Usually, algorithms with high- medium complexity lead to acceptable low FRR/FAR [13].

***False Accept*:** An impostor may sometime be acceptedas a genuine user, if the similarity with his template falls within the intra-user variation of the genuine user. The FAR normally states, either in a percentage or a fraction, the probability of someone else matching as you. FAR is defined by the formula:

$$FAR = \frac{FA}{N} * 100 \qquad (6)$$

Where FA is the number of false accept and N is the total number of verification.

***False Reject*:** When the acquired biometric signal is ofpoor quality, even a genuine user may be rejected during authentication. This form of error is labelled as a 'false reject'. If you fail to match against your own template, then you have been falsely rejected. The probability of this happening is referred to as the false rejection rate, or FRR. Thus, the higher the probability of false rejection, the greater the likelihood you will be rejected. FRR is defined by the formula:

$$FRR = \frac{FR}{N} * 100 \qquad (7)$$

Where FR is the number of false reject and N is the total number of verification.

The system may also have other less frequent form of error such as:

- **Failure to enroll(FTE)** It is estimated that nearly 4%of the population have illegible fingerprints. This consists of senior population, laborers who use their hands a lot and injured individuals. Due to the poor ridge structure present in such individuals, such users cannot be enrolled into the database and therefore cannot be subsequently authenticated. The FTE normally states, either in a percentage or a fraction, the possibility of someone failing to enroll in a system.

$$FTE = \frac{FE}{N} * 100 \qquad (8)$$

Where FE is the total number of Failure Enroll and N is the total number of verification.

For performance analysis, the application developed was tested using the bio-data and fingerprints collected from One hundred and seventeen (117) users out of which 30 were staff and 87 were students of the department of computer science, the Federal University of Technology, Akure, Nigeria using a live-scan method. The fingerprints were taken from any of the ten fingers of a respective member of the group in which each person must remember the exact finger that was used for the purpose of verification. The reason for this is to allow alternate finger should any of the fingers fails to enrol due to the poor ridge structure present in such fingers. The reason for interest in the use of students and staff of the above mentioned department and school

respectively is easy accessibility and their readiness to provide their biometric data for research purposes.
The minutiae data were extracted from the fingerprint images and stored in a database as a template for the subject along with the user's ID. During authentication, the biometric of the user is captured again and minutiae data are also extracted forming the test template which is matched against the already stored template in the database. In each case, if the matching score is less than the threshold, the person is rejected otherwise the person is accepted. Using equation 6-8, Table 1 gives the respective values for the false Acceptance rate (FAR) and False Rejection Rate (FRR) and for the test that was carried out.
In the test, the false acceptance rate was zero meaning that there were no cases of false acceptance (FAR) i.e. a person that was not pre-registered was not falsely enrolled for attendance. There were a few false rejections (FRR) during the test in which the system failed to identify some pre-registered users. These could be attributed to improper placement of the finger on the scanner and fingers that have been slightly scarred due to injuries.

Table 1. Values of the FAR and FRR from the Test

FAR	FRR
0.0%	2.56%

The above values of FAR and FRR implies an accuracy of 97.4% considering the genuine acceptance rate. Tables 2a and 2b show the details.

Table 2a. Details of the evaluation

	Successful Verification	Unsuccessful Verification
Staff	30	0
Student	84	3
Total	114	3

Table 2b. Details of the evaluation

No of Attendee	Successful Verification	Unsuccessful Verification	Accuracy
117	114	3	97.4%

Table 3. Time taken for Verification

Type of system	No of attendee	Total time in seconds	Total time in minutes	Average Execution Time in seconds
Fingerprint-Based Attendance System	117	502.41	8.37	4.29
Manual Attendance System	117	2161.55	36.02	18.48

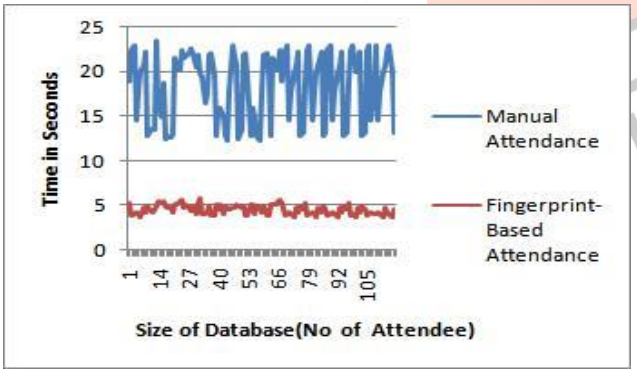

Figure 2. Comparison of the Manual Attendance System with the Fingerprint-based Attendance Management System.

The developed fingerprint-based attendance management system was compared with the existing manual attendance system (use of paper sheet/attendance register) and the time of taking both attendance was recorded. The manual attendance system average execution time for one hundred and seventeen (117) attendees is approximately 18.48 seconds as against 4.29 seconds for the fingerprint-based attendance management. Table 3 shows the time taken for verification. Figure 2 shows the comparison of the manual system with the Fingerprint-based Attendance Management System.

VII. CONCLUSION

In this paper, we have presented a fingerprint-based attendance management system. The developed system is an embedded system that is part of a fingerprint recognition/authentication system based on minutiae points. The system extract the local characteristic of a fingerprint which is minutiae points in template based. Templates are matched during both registration

and verification processes. For improved quality control during the registration or verification process, a matching score was used to determine the success of the operation. The matching score was specified so that only sets of minutiae data that exceed the score will be accepted and data below the score will be rejected. Therefore, Fingerprint Recognition using Minutia Score Matching method was used for matching the minutia points before attendance is recorded.

The developed system is very helpful in saving valuable time of students and lecturers, paper and generating report at required time. The system can record the clock in and clock out time of students and workers in a very convenient manner using their fingerprint to prevent impersonation and reduce level of absence. Also, it reduces most of the administrative jobs and minimizes human errors, avoids proxy punching, eliminates time-related disputes and helps to update and maintain attendance records.

References

[1] EPIC-Electronic Privacy Information Centre (2002):"National ID Cards," http://www.epic.org/privacy/id_cards/. accessed January, 2012.

[2] Kadry S. and Smaili M. (2010): Wireless Attendance Management System based on Iris Recognition. Scientific Research and Essays Vol. 5(12), pp. 1428-1435, 18 June, 2010.

[3] Khan B., Khan M. K. and Alghathbar K. S. (2010): Biometrics and identity management for homeland security applications in Saudi Arabia. African Journal of Business Management Vol. 4(15), pp. 3296-3306, 4 November, 2010.

[4] Bevan S and Hayday S. (1998): Attendance Management: a Review of Good Practice" Report 353, Institute for Employment Studies.

[5] McKeehan D.A. (2002): Attendance Management Program, The City of Pleasanton, Human Resources.

[6] Ononiwu G. C and Okorafor G. N (2012): Radio Frequency Identification (RFID) Based Attendance System With Automatic Door Unit, Academic Research International. Vol 2, No 2, March, 2012.

[7] Shoewu O., Olaniyi O.M. and Lawson A. (2011): Embedded Computer-Based Lecture Attendance Management System. African Journal of Computing and ICT. Vol 4, No. 3. P 27- 36, September, 2011.

[8] Shehu V. and Dika A. (2011): Using Real Time Computer Vision Algorithms in Automatic Attendance Management Systems. Proceedings of the ITI 2010 32nd Int. Conf. on Information Technology Interfaces, June 21-24, 2010, Cavtat, Croatia.

[9] Mehtre, B. M. (1993): Fingerprint image analysis for automatic identification. Machine Vision and Applications 6, 2 (1993), 124-139.

[10] Jain A. K., Maio D., Maltoni D., and Prabhakar S. (2003): Handbook of Fingerprint Recognition, Springer, New York, 2003.

[11] Maltoni D. and Cappelli R. (2008): Fingerprint Recognition, In Handbook of Biometrics, Springer Science + Business Media, U.S.A.

[12] Ravi. J. K., Raja .B. and Venugopal.K. R.(2009): Fingerprint Recognition Using Minutia Score Matching, International Journal of Engineering Science and Technology Vol.1(2), 2009, 35-42.

[13] Sharat S. Chikkerur(2005): Online Fingerprint Verification System, A Meth Thesis, Department of Electrical Engineering, Faculty of the Graduate School of the State University of New York at Buffalo.