American Journal of Computing Research Repository, 2014, Vol. 2, No. 1, 8-14
Available online at http://pubs.sciepub.com/ajcrr/2/1/2

DOI:10.12691/ajcrr-2-1-2

Biometric-based Attendance System: LASU Epe Campus as Case Study

O. Shoewu[1,*], N.T. Makanjuola[1], S.O. Olatinwo[2]

[1]Department of Electronic and Computer Engineering, Lagos State University, Lagos, Nigeria
[2]Department of Computer Engineering, Moshood Abiola Polytechnic, Ogun State, Nigeria
*Corresponding author: engrshoewu@yahoo.com

Received December 02, 2013; Revised December 12, 2013; Accepted January 09, 2014

Abstract In this paper, we propose a biometric-based attendance system for course lecture. The proposal system takes attendance during lecture periods automatically using student identification method. Efforts in this work recorded 94% success rate for eight students who participated in the study. Biometrics based attendance system produced approximately 3.8 seconds execution time on the average while the manual method of attendance produced approximately 17.8 seconds execution time on the average. Results of the biometric based attendance system confirm improved performance as compared to the manual method of attendance. Continuous observation improved the performance.

Keywords: *biometric, technology, automated, RFID, register*

Cite This Article: O. Shoewu, and N.T. Makanjuola, "Biometric-based Attendance System: LASU Epe Campus as Case Study." *American Journal of Computing Research Repository* 2, no. 1 (2014): 8-14. doi: 10.12691/ajcrr-2-1-2.

1. Introduction

The use of biometric technology in attendance management cannot be overemphasized. Biometric is an automated of recognizing a person based on physiological or behavioral characteristics. Many biometrics can be used for some specific systems but however the same. From literature it is known that biometrics is used for objective identification and verification.

Every Nigerian university has the obligation to record and take student attendance during lecture periods every semester. The accuracy of this record of attendance as important as it is have been marred by many challenging problems which ranges from the cumbersome nature of the paper sheets used in recording, manipulation of the attendance record by fraudulent students, emplacement of the attendance records after taking them and so on. It therefore becomes very difficult for the regular management and update of such records which have been previously taken. Also the calculation of the percentage of attendance to ascertain the qualification of student to write a particular examination may not be achieved. For the stated reasons, a biometric based attendance system is developed and designed to overcome the problems associated with the attendance system. Biometric-based systems are particularly used for one of the two identified objectives which include verification and identification. Identifications suggests a match between the query biometric belongs to the claimed identity or not. Previously biometric techniques were used in many areas such as credit cards, passport control, criminal investigations, ATM and security services.

This biometric based system we proposed in this work uses finger prints technique. It has been observed in literature that human beings have been using fingerprints for recognition for a long time, due to its simplicity and accuracy. The developed system makes it possible to estimate automatically whether each student is present or absent and also generate the percentage on order to determine eligibility for examination in a particular course.

Advantages of Biometrics include:

- **Accuracy and Security:** tokens such as papers, keys, magnetic stripe cards can be lost, stolen or duplicated; passwords could be shared. On other hand, biometric verification involves the physical presence of the user.
- **Screening:** in biometrics, users can not assume multiple identities and thus it helps to screen the users [1].
- **Non-repudiation:** with other security models, perpetrators can deny committing a particular action. Biometrics [2] completely eliminates the problem of repudiation.
- **Universality:** everyone has a biometric feature and it is thus universal to everybody.
- **Environment friendly:** it reduces paper and other resource requirement and does not cause any negative impact to the environment.

The various biometric modalities can be categorized as

- Behavioural Biometrics: these involve measuring the manner in which a user acts, reactions and the aggregate of the responses or movements made by the user. This includes signature, gait, keystroke dynamics, speech et.c
- Physical Biometrics: these involve all forms of physical measurements and body characteristics that

differ from person to person such as facial recognition, fingerprints, hand geometry, iris recognition et.c

- Chemical Biometrics: this is an emerging field of biometric and it involves measuring cues such as the chemical composition of human perspiration, body odour et.c

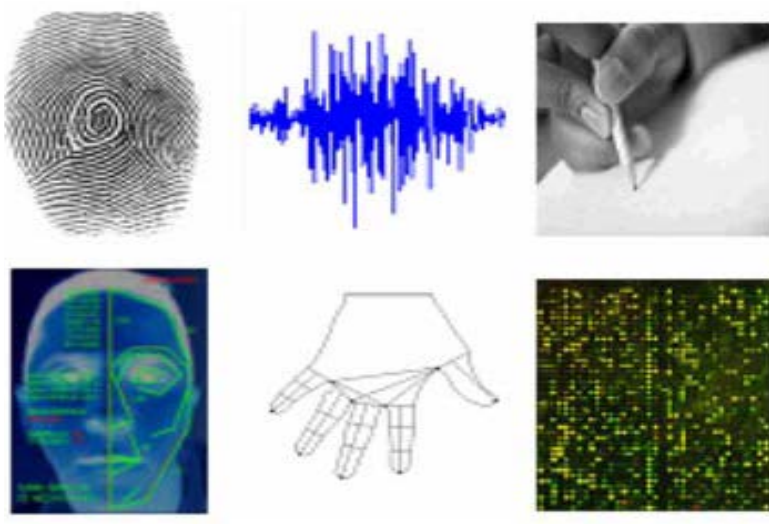

Figure 1. Various biometric modalities: Fingerprints, Speech, Handwriting, Facial Recognition, Hand Geometry and Chemical Biometrics

A biometric system can either be an identification system or a verification system (authentication) system, depending on the application [3]. Identification and Verification can be defined as [4]:

- **Identification-One to Many:** identification involves determining a person's identity by searching through the database for a match (In essence, the system tries to answer the question, "Who am I?"). For example, identification is performed in a list to find if the query image matches with any of the images in the list; it is also used by law enforcement agencies for criminal identification initiatives to link a suspect to an unsolved crime or identify the person suspected of committing a crime.
- **Verification-One to One:** verification involves determining if the identity which the person is claiming is correct or not (In essence, the system tries to answer the question, "Am I whom I claim to be?"). Examples of verification include access to an ATM; it can be obtained by matching the features of the claimed identity in the database (a user might claim to be matric no 050210057 by presenting his identity using his fingerprint). It is not required to perform match with complete database.

There are two major types of biometric systems: unimodal and multimodal systems. Unimodal biometric systems are only one characteristic or feature for recognition such as face recognition, fingerprint recognition, and iris recognition. Multimodal biometric systems typically use multiple information obtained from more than one biometric modality, such as fusing information from face and fingerprint.

1.1. Fingerprints as a Biometric

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 minutia 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, tended arch, left loop, right loop and whorl as shown in Figure 2. 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. Fingerprints have several advantages over other biometrics, such as the following:

1. High Universality: a large majority of the human population has legible fingerprints and therefore be easily authenticated. This exceeds the extent of the population who possess passports, ID cards or any other form of tokens.
2. Easy to collect: the process of collecting fingerprints has become very easy with the advent of online sensors. These sensors are capable of capturing high resolution images of the finger surface within a matter of seconds [6]. This process requires minimal or no user training. In contrast, other accurate modalities like iris recognition require considerable learning curve in using the identification system.
3. High Performance: fingerprints remain one of the most accurate biometric modalities available to date with jointly optimal FAR (false accept rate) and FRR (false reject rate). Forensic systems are currently capable of achieving FAR of less than 5% [9].
4. High Permanence: the ridge patterns on the surface of the finger are formed in the womb and remain invariant until death except in the case of severe burns or deep physical injuries.

5. High distinctiveness: even identical twins who share the same DNA have been shown to have different fingerprints, since the ridge structure on the finger is not encoded in the genes of an individual. Thus, fingerprints represent a stronger authentication mechanism than other types of biometrics. There are also mathematical models [8] that justify the high distinctiveness of fingerprint patterns.

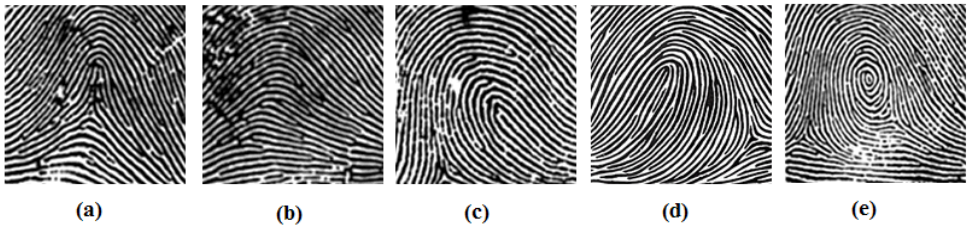

Figure 2. Fingerprint Classes: (a) Tended Arch (b) Arch (c) Right Loop (d) Left Loop (e) Whorl

Other advantages of using fingerprints include widespread public acceptance and reliability. It takes little time and effort to acquire one's fingerprint with a fingerprint identification device, and so fingerprint recognition is considered among the least intrusive of all biometric verification techniques. Ancient officials used thumbprints to seal documents thousands of years ago, and law enforcement agencies have been using fingerprint identification since the late 1800s [5]. Fingerprints have been used so extensively and for so long, there is a great accumulation of scientific data supporting the idea that no two fingerprints are alike i.e. have the exact same dermal ridge characteristics.

2. Methodology

The proposed attendance management system uses fingerprint identification. In identification, the system recognizes an individual by comparing his/her biometrics with every record in the database. In general, biometric identification consist of two stages

i Enrolment and
ii Authentication

During enrolment, the biometrics of the user is captured (using a fingerprint reader, which are likely to be an optical, solid state or an ultrasound sensor or other suitable device) and the unique features are extracted and stored in a database as a template for the subject along with the student ID. The objective of the enrolment module is to admit a student 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 student, formulating the process of authentication. The enrolment process is carried out by an administrator in the attendance system.

During authentication, the biometrics of the user is captured again and the extracted features are compared (using a matching algorithm) with the ones already existing in the database to determine a match. The identification accuracy of a biometric system is measured with the false (impostor) acceptance rate (FAR) and the false (genuine individual) reject 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. However, as it becomes more complex the computational cost increases which leads to undesirable high processing times. Thus, the overall performance of the identification system should be evaluated in terms of FAR/FRR, computational cost and other factors such as security, size and cost. A brief flowchart is shown in Figure 3.

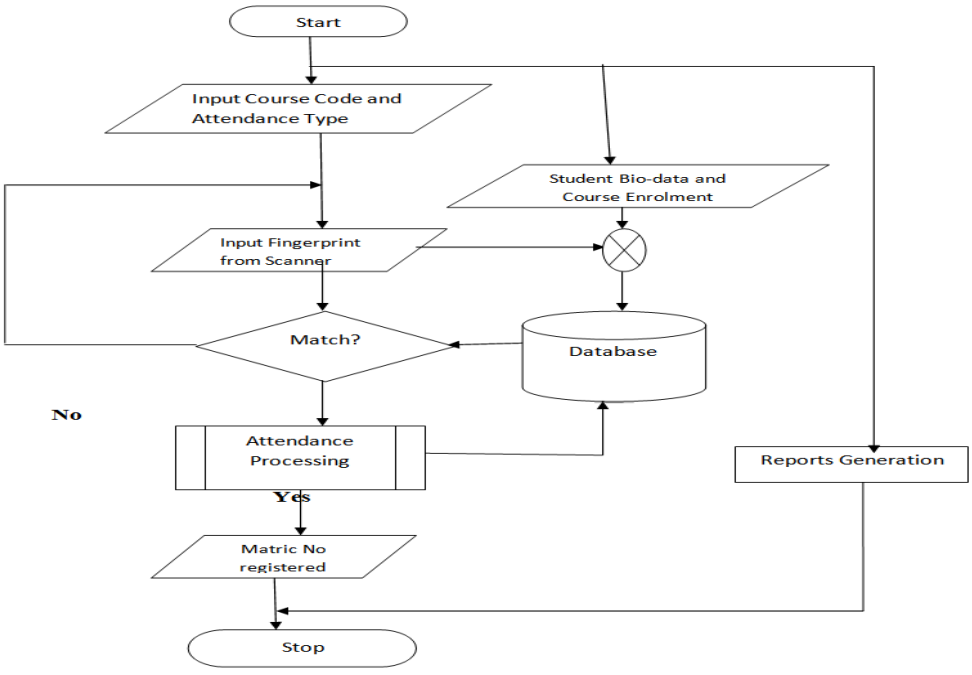

Figure 3. Flowchart for Attendance management system

3. Implementation

The implementation of the application involves the fingerprint reader and the PC. The fingerprint reader acquires the fingerprint and the PC consists of the windows forms that simulate the attendance application. The functionality of the Attendance management system can be broken down into the following blocks. These are:

i Administrative interface
ii Attendance system
iii Reports generation

3.1. Forms

The forms in the program are:

- Attendance Portal
- Courses
- Student
- Exams
- Lecturers
- Reports

Note: the courses, student, exams and lecturers form are administrative forms that can only be accessed by the administrator.

All the forms are connected to the database and all transactions carried out on the form are stored in the database.

3.1.1. Attendance Portal

This form is used by the student to enrol for lecture attendance, mid-semester exam attendance and exam attendance.

Figure 4. Attendance form

3.1.2. Courses

This form is used to create, edit and delete courses.

Figure 5. Administrative course form

3.1.3. Students

This form is used to enrol students and also to capture the fingerprint for each student into the database.

Figure 6. Student Registration form

3.1.4. Exams

This form provides the functionality to create, edit and delete courses.

Figure 7. Exam form

3.1.5. Lecturers

This form provides the functionality to create, edit and delete lecturers.

Figure 8. Lecturers Registration form

3.1.6. Report

This form is used for reports generation. The reports were created using reports in visual basic 2010.

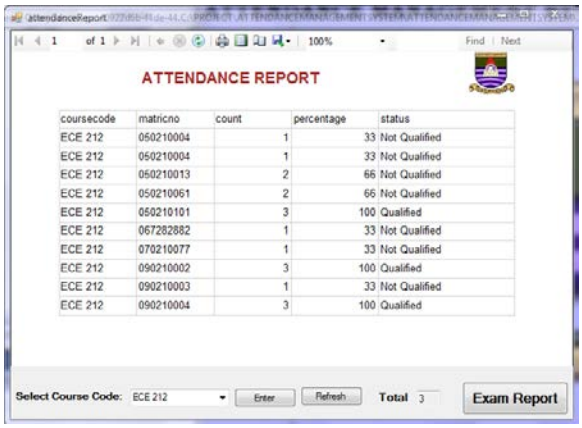

Figure 9. Attendance Report Form

4. Results

All sections of the system were tested starting with the administrative part of the attendance. The test results shows that the system is effective and it has a fast response. There was no false identification of students, few cases of false reject which was later accepted and only pre-registered students were authenticated. The matric of the identified students were enrolled for attendance automatically.

The system was tested using the bio-data and fingerprints collected from eighty (80) students of the department of Electronics and Computer Engineering, Lagos State University, Epe, Lagos State, Nigeria. In the test, there was no false acceptance i.e. a person that was not pre-registered was not falsely enrolled for attendance. There were a few false rejections during the test in which the system failed to identify some pre-registered users. The false rejects could be attributed to improper placement of the finger on the scanner and fingers that have been slightly scarred due to injuries. The 80 candidates are divided into 8 groups of 10 students and a success rate of over 94% was obtained from the tests carried out. The results of the test are shown below in the chart (Figure 10).

Table 1. Comparison of Success and Failure Rate

Groups	1	2	3	4	5	6	7	8
Success (%)	100	90	100	100	80	100	90	100
Failure (%)	0	10	0	0	20	0	10	0

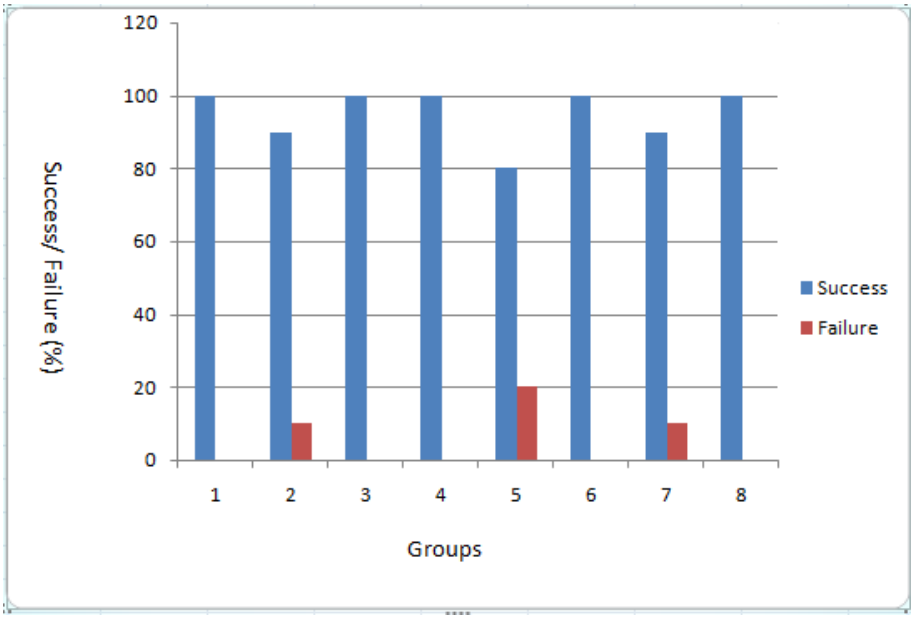

Figure 10. Comparison of Success and Failure Rate

4.2. Test Results

There are 3 phases of operation:

4.2.1. Enrolment and Registration Phase

The enrolment and registration phase is an administrative phase in which the administrator needs to log in. The user fingerprint as well as the other bio-data is stored for the first time into the database for student registration. The courses, lecturers and exams are also registered at this phase. All data and information required for the proper recording of attendance are enrolled.

4.2.2. Normal Attendance Usage

The lecturer selects the course code and the attendance type, then the student places his/her fingerprint on the fingerprint reader; the finger recognition unit compares the fingerprint features with those stored in the database. The possible cases are:

Figure 11. Attendance Form (Match of fingerprint)

- Match (of Fingerprint): captured user fingerprint features are matched with stored fingerprint templates. The user is automatically recorded for that lecture/mid-semester test/semester exam. A message box pops up for a short interval to show that the user has been recorded for the attendance. Figure 11 shows a snapshot of the program.
- Non-match (of fingerprint): the user is not accepted for attendance and a message is shown in the textbox that fingerprint is not found. The interface is shown in Figure 12.

Figure 12. Attendance form (Non-match of fingerprint)

4.2.3. Report Phase

Reports are generated for each course and the total number of students for each attendance is listed and their corresponding status. An example is shown in Figure 9.

4.3. Execution Time

The fingerprint identification, in which the comparison and shifting of the fingerprint image is done many times, is completed within a short time. The total period to register a new user i.e. sense the fingerprint and input the bio-data is about 1minute 20seconds.

For the actual attendance collection process, the total time taken to sense the fingerprint, identify the user and record the attendance for that particular course is less 5 seconds. Thus it can be effectively implemented in classes with large population.

4.4. Comments

These experimental results confirm that the system tallied with the design expectations and the proposed system is suitable for attendance collection. The system can also be adapted for other institutions.

4.5. Comparison with Manual Attendance

The manual attendance system average execution time for eighty (80) students is approximately 17.83 seconds as against 3.79 seconds for the this automatic attendance management system using fingerprint identification. Reports generation for the attendance system takes approximately 30s.

It can be shown in the graph below and thus, it can be seen that the automatic attendance management system using fingerprint authentication is better and faster than the use sheets of paper.

Table 2. Comparison of the execution time of Manual Attendance and Attendance Management System

Student	Manual Attendance	Attendance System
1	22.78	3.81
2	12.82	3.43
3	19.65	4.12
4	11.38	3.63
5	12.65	2.53
6	16.24	2..49
7	14.66	2.72
8	15.23	3.35
9	15.03	4.01
10	16.31	4.21
11	14.97	4.31
12	15.16	3.85
13	15.18	4.32
14	16.54	4.78
15	16.59	4.23
16	16.92	3.55
17	16.95	4.34
18	17.61	5.11
19	17.72	3.36
20	17.78	4.57
21	18.01	3.12
22	18.25	3.31
23	18.62	3.1
24	19.19	2.92
25	19.34	2.83
26	19.67	4.47
27	19.72	5.05
28	19.85	3.34
29	19.89	3.42
30	20.52	3.81
31	20.91	4.92
32	22.03	3.58
33	23.16	4.31
34	23.19	5.19
35	24.21	5.52
36	10.68	3.72
37	15.37	4.33
38	15.68	3.58
39	11.92	4.87
40	19.23	3.53
41	20.86	2.12
42	14.17	2.34
43	17.75	3.89
44	15.99	3.75
45	27.69	3.53
46	25.39	2.38
47	24.46	2.41
48	19.87	4.11
49	15.24	3.08
50	20.05	2.98
51	17.45	3.67
52	13.67	3.52
53	21.15	3.71
54	19.08	4.05
55	14.44	5.00
56	13.67	3.97
57	19.9	2.56
58	15.28	3.45
59	12.76	3.42
60	23.75	3.54
61	12.34	4.21
62	15.43	4.07
63	17.32	4.93
64	20.52	4.91
65	14.89	4.05
66	17.6	3.99
67	16.43	4.04
68	18.75	5.14
69	19.32	3.85
70	19.3	3.79
71	15.68	3.62
72	18.92	2.87
73	19.23	4.52
74	17.41	4.09
75	18.43	4.26
76	18.52	3.99
77	19.8	3.54
78	15.87	2.87
79	19.42	2.34
80	17.62	3.71

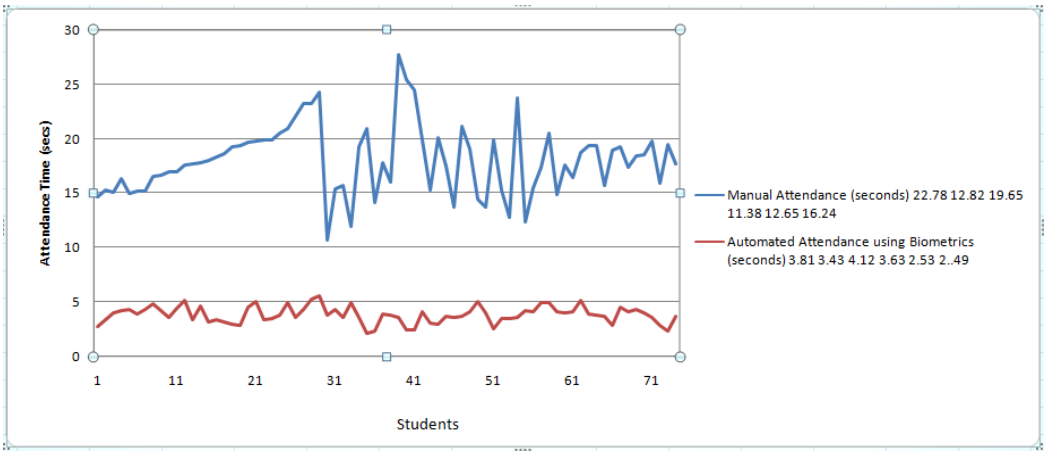

Figure 13. Comparison of Manual Attendance with Attendance Management System

5. Conclusion

The system successfully simulated attendance recording both at lectures and examinations. The prototype successfully captured new fingerprints to be stored in the database; scanned fingerprints placed on the device sensor and compared them against those stored in the database successfully. The performance of the system was acceptable and would be considered for full implementation especially because of its short execution time and reports generation. Everyone who tested the system was pleased and interested in the product being developed for use in schools.

References

[1] Christopher James Jenkins. The weakly identifying system for doorway monitoring. PhD thesis, Duke University, USA, 2007.

[2] Sharat S. Chikkerur. Online Fingerprint Verification System. MSc thesis, SUNY, Buffalo, USA. 2005.

[3] Richa Singh, Mayank Vasta, Phalguni Gupta. Biometrics. West Virginia University, USA and Indian Institute of Technology, India.

[4] Jain et al., 1999, 2004; Ross, Nandakumar, & Jain, 2006.

[5] Andrew S. Patrick. Fingerprint Concerns: Performance, Usability and Acceptance of Fingerprint Biometric Systems

[6] T. Jea, V. K. Chavan, V. Govindaraju, and J. K. Schneider. Security and matching of partial fingerprint recognition systems. In Proceeding of SPIE, number 5404, pages 39-50, 2004.

[7] Anil k. Jain. Handbook of Fingerprint Recognition, Springer-Verlag, 2003.

[8] Rishabh Mishra, Prashant Trivedi. Student Attendance Management System based on fingerprint recognition and one-to – many matching.

[9] T. Matsumoto, H. Matsumoto, K.Yamada, and S. Hoshino. Impact of artificial gummy fingers on the fingerprint systems. In the proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques IV, volume 8577, 2002.