Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 2; Issue 2; March 2025; Page No. 99-110.

Development of a Fingerprint-Biometric Expert System for Student Class Attendance Monitoring

Odulaja, G.O.
Department of Computer and Information Science, College of Science and Information Technology, Tai Solarin University of Education, Ijagun, Nigeria.

Corresponding author email: odulajago@tasued.edu.ng

Abstract
Over the years, flaws such as impersonation, multiple entry, manipulation and mutilation of attendance records by unscrupulous students in various forms associated with the manual taking of class attendance for coursework and examination often compromise the accuracy and reliability of the records, thereby defeating the purpose of the exercise in Nigerian tertiary institutions. A Fingerprint-Based Student Attendance Monitoring System, FiBSAMS, was developed to mitigate against this problem in this study. An Atmega328P microcontroller, five fingerprint RS305 scanner modules, a liquid crystal display (LCD), RGB light emitting diodes, and a laptop computer were used to uniquely capture and validate fingerprints of 100 student candidates for populating the knowledge base of the expert system. With pattern matching algorithms, the inference engine (microcontroller) was configured and trained to validate every fingerprint input for acceptance or rejection. For 2 academic semesters, attendance was taken manually in the first semester and biometrically with FiBSAMS in the second semester. Results showed that the biometric attendance system had 95% successful valid and accurate identifications and 30% increase in class attendance relative to manual attendance records. Besides, manipulation of attendance records reduced significantly. Compared with manual attendance system, FiBSAMS' performance amounted to a significant improvement in accuracy and reliability.

Keywords: Atmega328P Microcontroller, FiBSAMS, Biometric, Fingerprint, RS305 Scanner Module

Introduction

Biometric identification is the process of automatically identifying and verifying an individual based on unique behavioural and psychological traits they naturally possess. Such traits can include his retina, fingerprint, facial or iris features. Because of the stronger binding offered by biometric technologies over traditional identification approaches such as passwords, signatures and cards, they have become the preferred means of identification and verification even on highly sensitive systems (Anil et al., 2025). For authentication, verification and identification purposes, biometrics technologies measure and analyze human body characteristics. Biometric Measurement is the process of measuring unique physical features such as fingerprints, hand geometry, or retinal scans for security purposes by comparing them to previous samples for authentication (ScienceDirect.com). However, fingerprints which is more accurate, unique and immutable have become much more widely accepted than any other biometric systems.

Many organizations and institutions relying on the data gathered from attendance for performance, punctuality and efficacy of their employees, have found obtaining and keeping accurate attendance a significant problem. Attendance has proved over time to be an integral indicator of an individual's eligibility for promotion, awards, recognition, timeliness, and devotion to a cause, in an institution or association (Kabir et al., 2021). It has also been used to measure one's reliability, orderliness, commitment punctuality, trustworthiness and respect for others. Incidentally, the traditional paper and pen approach to attendance taking remains the de facto method in many educational institutions to date. Leaders (teachers and association secretaries) are often seen making roll calls from a

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

prepared paper register or requesting attendees to put their names and identification details down on a provided paper.

In Tai Solarin University of Education (TASUED), Ijagun, Ogun State, Nigeria, the traditional attendance system is still in use for taking students class and non-Computer Based Tests and exam attendances. For record purpose, a lecturer will mandate the class representative to pass sheets of paper round the students present for a class lecture for them to put down their details – name, matriculation number, and signature. This traditional approach to taking attendance is prone to both intentional and unintentional flaws. It is time consuming for both the students and instructors during classes and prone to many human errors. Other problems include losses of attendance sheet, manipulation and mutilation of this record, double entry, impersonation, poor handwriting, infringing on other instructor's time, rowdiness, and inaccuracies among others. While using manual approach, the purpose of taking the attendance can easily be defeated when the attendance sheet is misplaced, destroyed or compromised, as is the case with impersonation; thus making no sense of efforts and time invested in exercise (Onyishi & Igbinoba, 2021). Finger print Biometrisc based attendance system can greatly reduce these irregularities associated with paper based manual methods and considerably cut down on the time needed for attendance verification.

Operations and Procedures for Biometric Authentication

Measuring and statistically analysing the physiological and behavioural characteristics like hand-written signatures, fingerprints, faces, irises, retinal patterns, palm prints and voice of an individual to the end of verifying his identity is all that Biometrics is about. For being more convenient compared to other popular approaches such as passwords, signature or use of ID cards, biometrics techniques are receiving more attention as the preferred means of authenticating identity. Reliance of Biometrics on unique data with life-long consistency, collected directly through contact with the candidate in question, informed its preference over other identification methods. However, for being the most unique, permanent, stable and relatively easy to acquire, adoption of fingerprint biometrics technology supersedes other biometrics approaches. It is therefore the most mature and popular biometrics technology for automatic personal identification.

Encryption of collected biometric data is significantly promotes its ease of use in averting identity theft and this has further informed its adoption by many. The process of biometric verification begins when an appropriate application software is used to isolate and capture a specific feature, spot, part or component of human physical characteristics and such is kept unaltered as a template for eventual comparative analysis. The isolated and captured feature is digitized by converting it to its numerical equivalence and stored as a reference match point in the database. Using pattern-matching algorithm, captured information is compared with every other similar entries gotten from user input through biometric scanner. If this authentication process results in a match with that of the database template up to a predetermined degree, the result is accepted as approved, otherwise, it is rejected.

Fingerprint Biometrics

Uniqueness, stability, permanency and relative ease of capture informed the choice of fingerprint biometrics for this study. Long recognised is the fact that fingerprint biometrics stands out among others in terms of maturity and popularity as the biometric of choice for automated human identification. As reported in literature, there are no two fingerprints that are alike. This is attributable to the minutiae of the fingerprint. On the palm and fingers are the characteristically minute friction ridge skin minutiae that, make it possible to uniquely identify individuals. On their fingers, should two or more people have equal number of loops, arches, or even whorls, the different minutia configurations on their fingers will still make it possible to identify them uniquely (Wilder & Wentworth, 2025).

While personal identification numbers PINs and passwords have served as means of individual identification in many important situations and places, it has been realised over time that they suffer from vulnerabilities in the face of prevailing modern technologies. There had been cases of forgetting pin number or password at the point of use (IFSEC Insider, 2025). This is not far in between in modern time because many are preoccupied with several mental, emotional and occupational challenges. Besides, with the recent increases in global terrorism, cyber stalking and sophisticated technologically organised crimes, vulnerabilities of passwords and PINs are more glaring and they often fail in adequacy as means of identity verification and security. Consequently, more advanced means of identifying and verifying individuals have become imperative and inevitable. In the light of these developments, fingerprint biometrics like other sophisticated biometric technologies stands out for identity authentication purposes (IFSEC Insider, 2025).

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

Both conventional and traditional authentication methods, like ID cards, passwords and magnetic cards, keys cannot stand up to fingerprint biometric security system. This is not unconnected to its intrinsic link to the individual involved. Consequently, cases of loss, collusion or theft do not lead to security compromise (IFSEC Insider, 2025). Integrating biometric technology has promoted e-commerce, cloud computing, internet banking and demands for products from Smartphone industries.

It is therefore not surprising that increased use of biometrics in e-commerce, internet banking, cloud computing systems and smartphones had been recorded. Integrated biometric technologies are some of the major factors driving demand for products of smartphone industries. One predictive estimate has it that by 2036, contactless cards and apps enhanced by biometric technology will be responsible for all monetary transactions conducted in London (IFSEC Insider, 2025).

Related Works

Proliferation of automated fingerprint identification systems (AFIS) in recent times had resulted in time saving staff verification and authentication. The speed at which AFIS operates informed this. As a biometric solution, AFIS consists of a computer database populated with fingerprint records, through which searches and comparisons are carried out in order to identify known or unknown fingerprints. These applications can search over a billion fingerprint records within a second with almost 100 percent accuracy (Innovatrics, 2025). Consequently, automated fingerprint identification systems have found relevance and use in crucial areas such as in criminal investigation, border patrol law enforcement and many more (Innovatrics, 2025).

To ease the challenges associated with manually managing staff and students attendance records each day, and publishing monthly and annual reports of such Kabir et al. (2021) developed a modular multi-level Smart Attendance and Leave Management System based on fingerprint recognition for Students and employees of tertiary institutions.

To mitigate abuses associated with manual attendance taking system in tertiary institutions, Onyishi and Igbinoba (2021) similarly developed a biometric students' time and attendance logging system that used fingerprint biometric for accurate student identity. Tools and techniques used include: a microcontroller, a fingerprint module, a liquid crystal display (LCD), an RGB light emitting diode and a PC, visual studio C# and MySQL2008. They simulated the attendance taking system with proteus prior to its construction and testing.

Kadry (2010) developed a wireless iris recognition attendance management system using Daugman's algorithm to solve the problem of spurious attendance on wireless network. George et al. (2012) proposed Transform Domain Fingerprint Identification Based on DTCWT. In their findings, they rated physiological biometric characteristics higher in performance than behavioral biometric for human identification. besides they also found that compared to other levels of DTCWT, level 7 recognition rate is much better.

Walia and Jain (2016) reviewed fingerprint based biometric attendance systems. They discovered that for the system to offer more functionality the required circuit will correspondingly be more complex and the supporting software, more difficult to develop. A tradeoff was found between power consumed and the speed of the system, ditto to large databases and accuracy of fingerprint matching process.

Jiang and Yau (2020) proposed a fingerprint minutia matching technique that uses local and global fingers minutiae structures for identifiction.to achieve improved matching and more reliable fingerprint comparison result that is even suitable for online processing.

Materials and Methods

Top-down software development model was adopted in designing FiBSAMS. As shown in the architectural diagram (figure1) the system is categorized significantly into three submodules namely: Admin submodule, Lecturer submodule and Student submodule;with each of the listed submodules having different user privileges.

At Admin Submodule level, users can add, delete or update records or information across he whole system. Add Course, Assign Course, Fingerprint Enrollment, Enroll Student, Enroll Lecturer and Report are some other roles assigned to the Admin in this submodule. Thus the admin has overriding permission across the entire system to add, update or delete records.

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

Unlike Admin submodule level, at the Lecturer Submodule level, privileges are limited to:

i. attendance activation,
ii. viewing a student record
iii. or marking student attendance for the courses allocated to the lecturer

This submodule is further subdivided into:

a. course b. lecture taken c. activation duration and d. profile.
(See figure 1).

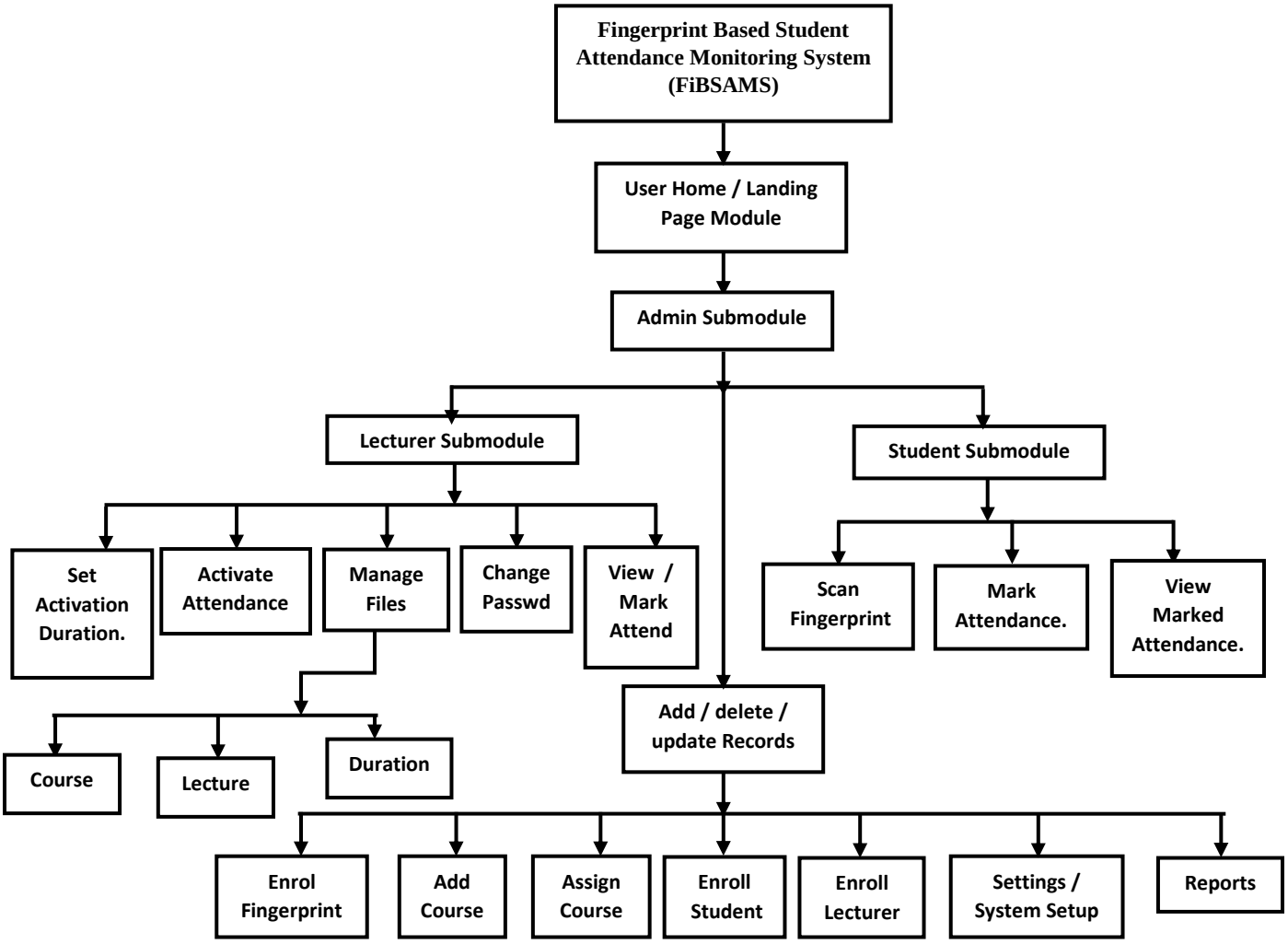


Figure 1: Architectural Model of the Fingerprint Attendance System

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

The block diagram of FiBSAMS is as shown in Figure 2. The five major components of this system are:

1. Power Control Unit
2. Microcontroller Module
3. Display Control Unit
4. Fingerprint Module and
5. Database Unit

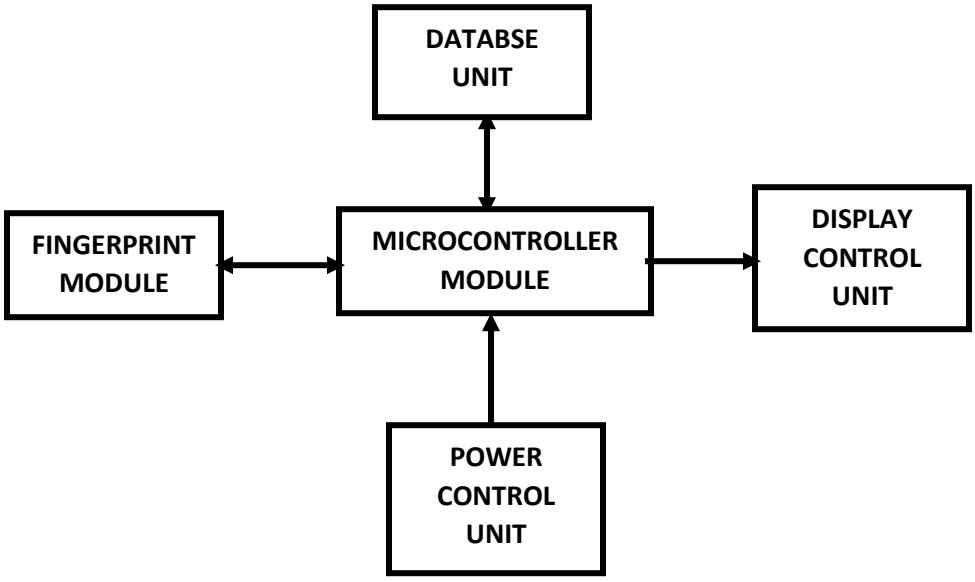


Figure 2: Block diagram of Fingerprint-Based Student Attendance Monitoring Systems, FiBSAMS

Power Control Unit

Through the UART (Universal Asynchronous Receiver Transmitter) cable to the USB (Universal Seril Bus) cable, the entire FiBSAMS circuit is duly powered from the personal computer. Of the four wires at the UART end, 2 supply the needed five volts power to the microcontroller, while the other two serve as the duplex receiver and transmitter lines. This requires that while USB terminal end is connected to the PC, it is the UART terminal end that is connected to the microcontroller.

Microcontroller Module

Central to the entire FiBSAMS system is the microcontroller because it has to interface with all the other 4 components. This 28 pin Atmega328P microcontroller has the following configurations:

i. 32 kb flash memory for program storage
ii. 2 kb Random Access Memory (RAM),
iii. 6 channels of 10-bit analog to digital converter (ADC),
iv. 1 kilobyte Electrically Erasable Programmable ROM ,
v. two 8 bits and one 16 bit timer/counter and
vi. serial communication ports for communicating with the computer using the COM port.
vii. Two 22 pF resonance capacitor and
viii. A 16MHz crystal oscillator

Interfacing roles of the microcontroller includes:

1. Controlling the display messages of the LCD,
2. Controlling display colour and timing of the RGB LED
3. Interfacing communication between the personal Computer and the RS305 fingerprint scanner.

Display Control Unit

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

The two principal components of this unit are the LED and the LCD, and both are connected to the microcontroller as shown below:

1. for the RGB LED, connection was via a 220 ohms resistors attached to pin 17, 18 and 19 of the microcontroller.
2. For the LCD, a high-density Hitachi product, HD44780 1602 LCD was used. Its Read/Write (R/W) pin is the fifth pin. Its configuration is such that
    a. if we set the R/W terminal to HIGH, a READ operation to the LCD is implied, and
    b. if we set it to LOW, a WRITE operation to the LCD is implied.
    c. This LCD operates in a 4-bit mode.

Table 1 shows the interpretations for each LCD colour display

Table 1: LCD Display Interpretations

	Colour	Implications
1	RED	No MATCH found for input fingerprint in the database
2	GREEN	A MATCH was found for input fingerprint in the database
3	BLUE	System is busy processing

For any fingerprint whose match is found, the name of the student as stored in the database is also displayed

Fingerprint Module

In this study, the scanner RS305 is adapted for two functions namely: fingerprint enrollment and fingerprint comparison. Consequently, its selection was carefully made to conform to the purpose and bring out the best result. Its configurations are

1. **Processor Model**: AS601 DSP SyncoCHIP. This processor from SynchoChip is specially designed for identifying fingerprints and its widely adopted in embedded systems.
2. **Processor Speed:** 120 MHz frequency.
3. **Peripherals**:
    i. 128 kb SRAM,
    ii. 64 kb ROM,
    iii. 4 kb OTP memory,
    iv. USB 2.0 (FS) Device,
    v. 2 × USARTs ,
    vi. Limited Optical CMOS Sensor Controller
    vii. Asynchronous Parallel Controller (APC) RSA engine,
    viii. Pseudo/True Random Number Generator(RNG), and
    ix. 37 GPIOs.

Respectively, the scanner is connected to Pin 2, Receiver-Rx pin and Pin 3, the Transmitter-Tx pin of the microcontroller.

Fingerprint Enrollment

Fingerprint enrollment stage is the stage at which the researcher obtains and registers the fingerprints of each of the students for storage in order to populate the system's knowledge base with the students' unique fingerprint templates. The fingerprint scanner was used to scan each student's fingerprints. The finger biometric template is consequently extracted from the scanned fingerprints and stored in a particular register of the scanner. Connected to the scanner, the microcontroller senses that a template has been stored, and sends a notification message signal to the Database Management System, DBMS of the database. This was repeated for all the students participating in this study.

Fingerprint Matching Mode

In the fingerprint matching mode, each student is asked to place his/her previously registered finger on the scanner. The scanner's processor scans the students fingerprint again, searches for a match in the database and uses its pattern matching algorithm to compare currently scanned students' fingerprint patterns with the enrolled fingerprint templates until a match is found or not found but the search list has been exhausted. The outcome (whatever it is) is then sent to the microcontroller.

Database Unit

The Computer database unit stores essential information about each student. The computer is connected to the microcontroller via a UART cable to USB cable. However, since the receiver -Rx and transmitter -Tx pin of the microcontroller (i.e pin 2 and pin 3) had already been used by the RS305 as mentioned above, another two I/O pins were converted to serve as Rx and Tx pins so that these can be connected to the UART side of the cable.

For every fingerprint successfully enrolled, its stored template assigned a reference name by the PC / Database Administrator. During the fingerprint matching, the microcontroller sends signals to the PC's software to indicate if a match for the fingerprint is found or not. If a match is found, the result is a **MATCH FOUND**, and the software marks the particular student present. However, if the fingerprint's match is not found in the database, result is a **NO-MATCH FOUND** and the software marks the student absent. Besides, the DBMS allows the students' particulars - name, level, course of study, gender and matriculation number to be edited as well as generate report on the number of times a student was present or absent. In order to prevent unauthorized access, the FiBSAMS requires a login password.

Implementation

The Biometric Fingerprint-Based Students Attendance Monitoring (FiBSAMS) was designed to be deployed by the concerned academic staff in Tai Solarin University of Education. It was implemented by the following logical outline:

i. The administrator (or lecturer) captured the data of all the 100 sample students offering his course to be hosted on the Window server.

ii. The Biometric Fingerprint Scanner/Reader was connected to the Computer system via its USB port.

iii. The Biometric Fingerprint-Based Attendance System FiBSAMS was installed on the Personal Computer (laptop) of the academic staff while the database was hosted on the department's LAN server.

iv. The PC and the window server are on the same networks. Figures 3 to 6 show all the forms in the system.

Results

Figure 3 shows the login form of the Student's Attendance, where the system users (the administrator (sitting HOD), lecturer, (which could be any of the academic staff of the department to whom at least a course has been allocated to handle by the HOD), and students,) provide their login details and to be validated and verify if the user is an authenticated one.

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

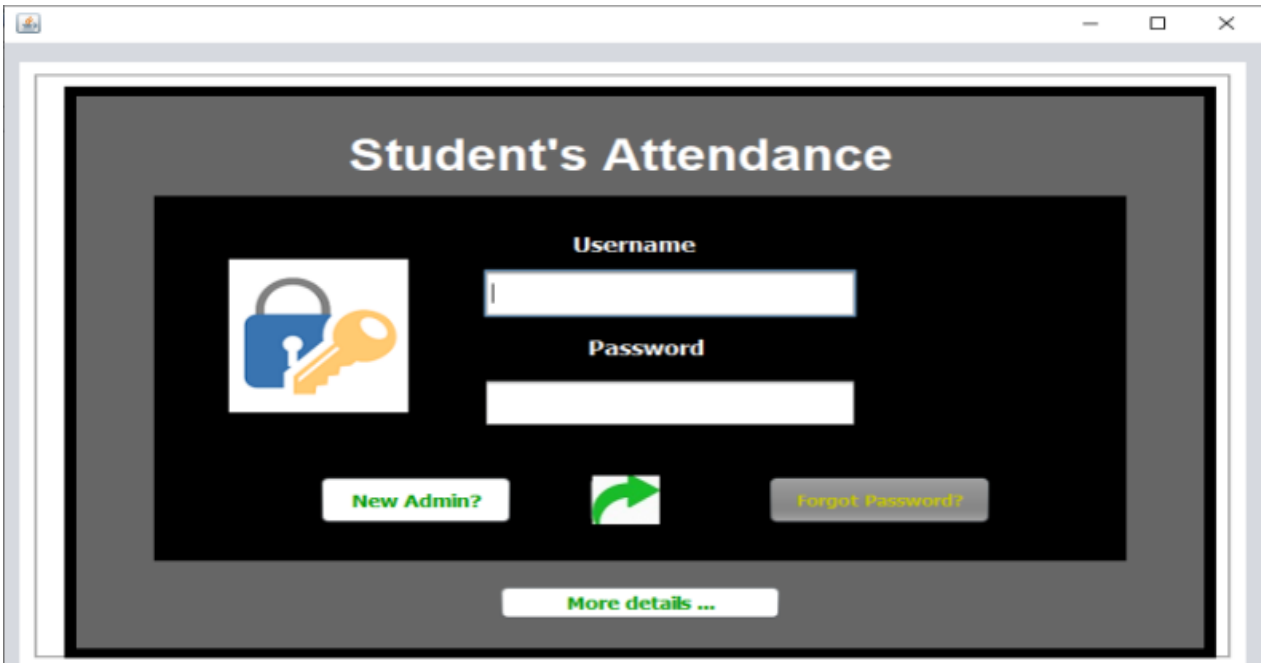
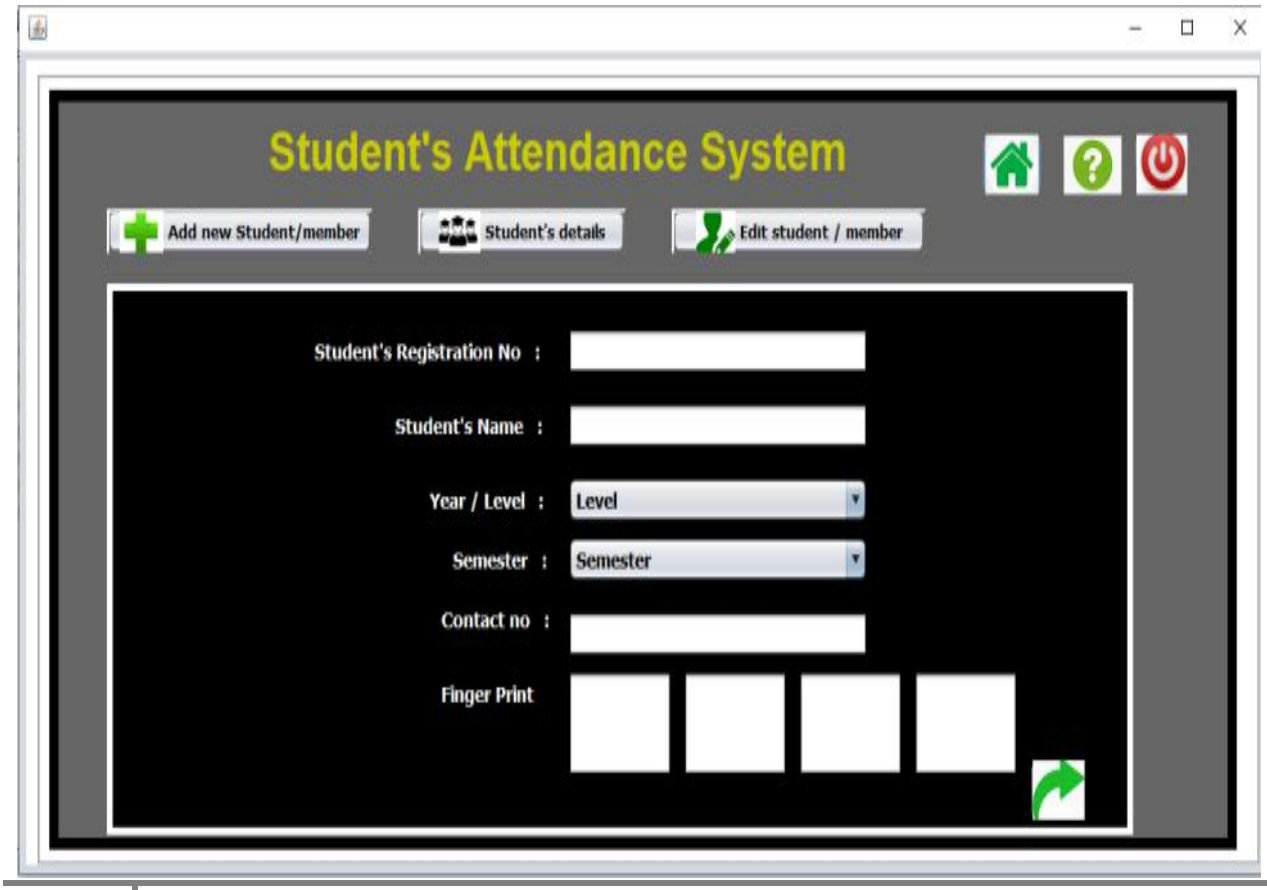


Figure 3: Login form

Figure 4 shows the student's set-up form for the Attendance system. The administrator uses the Student Set-up Form to collect and save all the required data (such as registration number, student's name etc.) about each student.



Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

Figure 4: Student Set-up Form

Figure 5 shows the Admin dashboard. It gives the administrator the privilege to work and select actions to be taken on the Attendance board. Only the designated Admin has access privilege to this Admin Dashboard page.

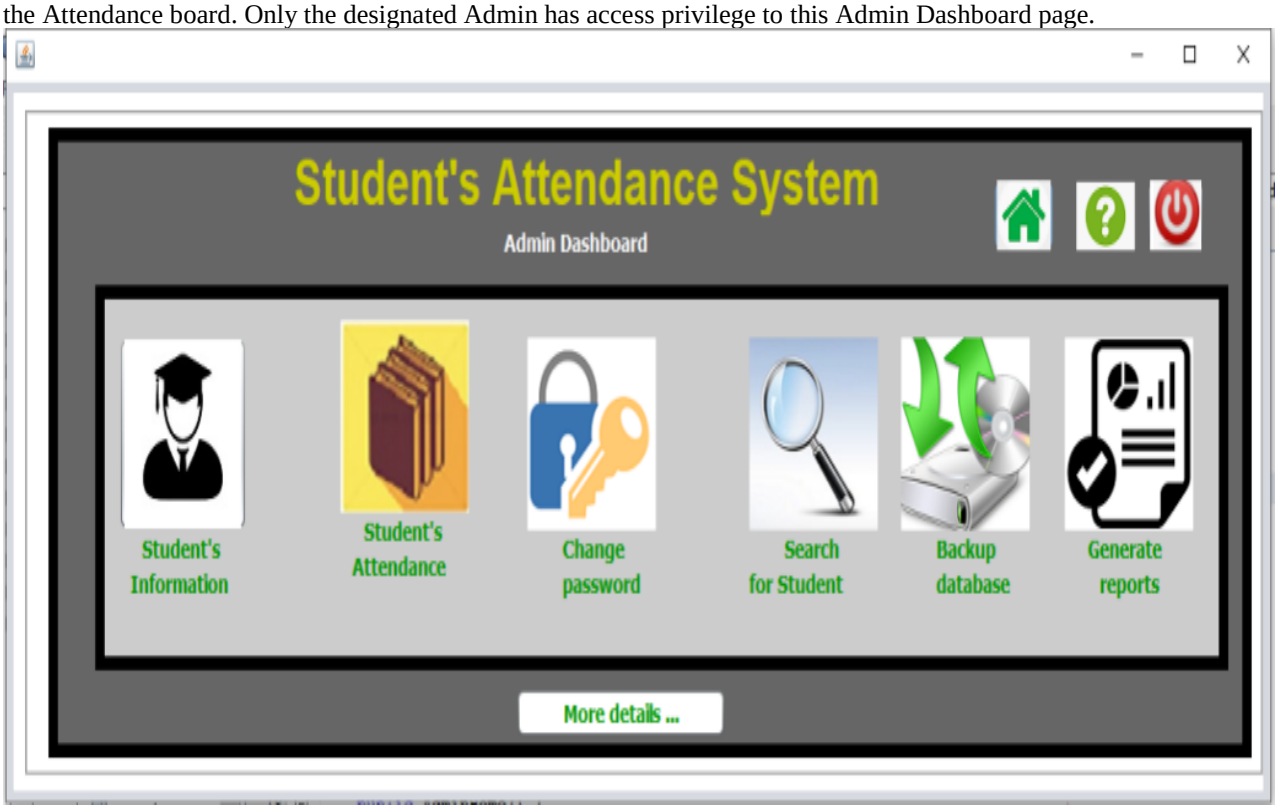


Figure 5: Admin Dashboard

Figure 6 shows the Attendance board page. This page shows the number of students whose attendance was captured in the knowledgebase.

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

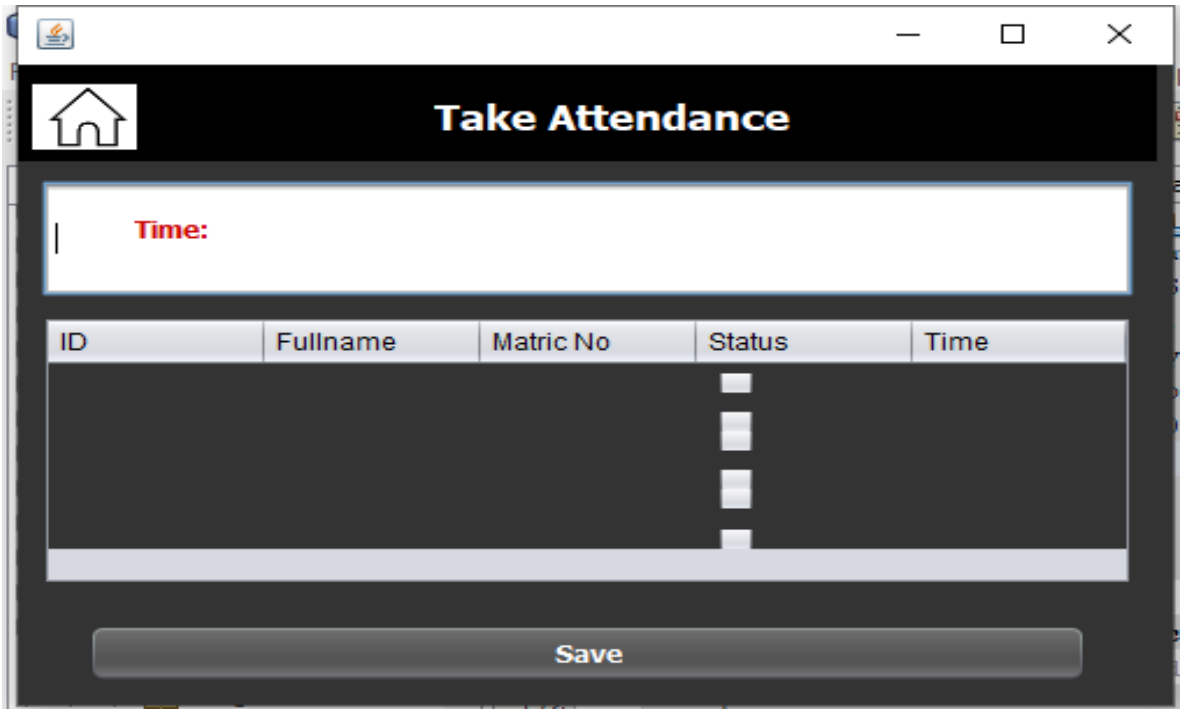


Figure 6: Attendance Board

Table 2: Table Showing Fingerprint Verification Success/Failure Percentage

Round	1	2	3	4	5	6	7	8	Cumulative%
Success (%)		100	90	100	100	80	100	90	100	95
Failure (%)		0	10	0	0	20	0	10	0	05

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

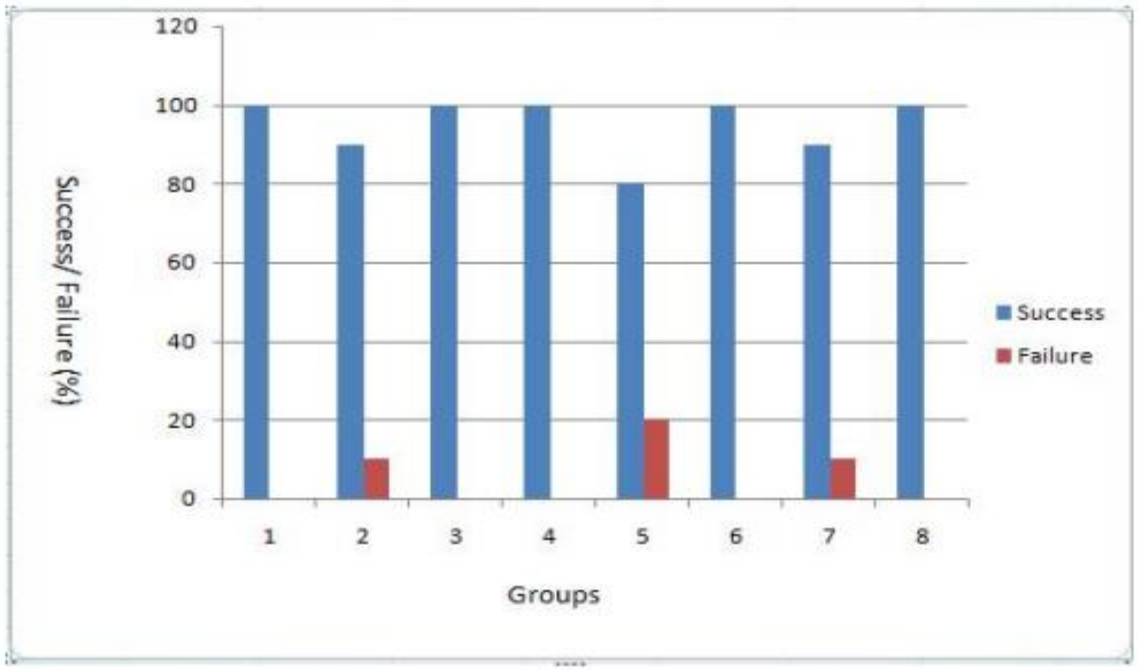


Figure 7: Graph showing percentage success/failure.

Discussion

To evaluate performance of FiBSAMS, bio-data and fingerprints templates were collected from the one hundred (100) students. This process was hitch free and without any false recognition. That means all students enrolled for attendance were the same students who had previously been registered. However, some false rejections were recorded as the system failed to identify 5 preregistered students users. These false rejections were found to have resulted from scarred fingers and an improperly placed finger on the scanner. The test of the 100 students was carried out 8 times and a success rate of about 95% was obtained from the tests carried out.

Table 2 shows the results obtained from evaluating the FiBSAMS. and Figure.7. During the test-running for evaluation process, it was found that one – time registration of a new user lasted for an average of 80 seconds while verification and identification of each previously registered candidate for a particular course is about 7 seconds on average. This implies that FiBSAMS can effectively be used in classes regardless of population size.

Conclusion

In this study, application of Fingerprint Biometric for the purpose of student attendance taking and recognition has proved to be a much better alternative to the traditional paper-based manual method of attendance management. As demonstrated in this study, the biometric attendance approach has successfully managed and controlled problems such as record mutilation, double entry, impersonation and record misplacement, associated with the manual approach. It also significantly fosters increased class attendance among the students, perhaps as a result of the awareness that the biometric attendance system cannot be compromised or manipulated, as is the case with the manual system. The uniqueness of each candidate's fingerprint nullifies attendance by proxy, as it demands each candidate to be physically present.

In conclusion, this study has demonstrated that the developed Fingerprint-Based Student Attendance Monitoring (FiBSAM) system is more reliable, more secure, and more efficient than the traditional manual system. Findings revealed that this system can be deployed in both pre and post secondary academic institutions for better student attendance management This new system promises to be cost effective with time as it replaces the stationery material with electronic apparatus and can compare several thousands of fingerprints within a second.

Cite this article as:
Odulaja, G.O.(2025). Development of a fingerprint-biometric expert system for student class attendance monitoring. *FNAS Journal of Computing and Applications*, *2*(2), 99-110.

However, the new system is limited in some few ways. To use the system requires that there be constant electric power source and backup without which the computerized FiBSAM system will not function. There must also be a competent administrator to manage and operate the system, and it also requires that the students obediently follow through with the biometric fingerprint enrollment and verification procedures. The electronic gadgets needed must be available and functional as well, thereby increasing the implementation cost in the short run. In the long run, however, this cost becomes insignificant over time when compared with the benefits.

Recommendations

1. The researcher strongly recommends the adoption of Fingerprint Based Student Attendance Monitoring (FiBSAM) system in Tai Solarin University of Education and other institutions, academic or non-academic, where candidates' attendance remains a crucial metric for performance recognition, recommendation assessment and in ascertaining punctuality, commitment and reliability without bias.

2. Secondly, fingerprint pattern verification, recognition and comparison algorithms were employed in this study. It is recommended that future research consider other biometrics features like facial recognition and iris or combinations thereof, and other relevant algorithms for batch attendance processing for more efficient and cost effective performance.

References

Anil, K., Arun, A., Kathik. N., & Thomas, S. (2025) Introduction to biometrics *google.com.ng/books/edition/Introduction-to-Biometrics.*

George, J., Abhilash, S., & Raja, K. (2012). Transform domain fingerprint identification based on DTCWT. *Int. J. Adv. Comput. Sci. Appl*. *3*(1), 190–195.

IFSEC INSIDER. (2025). *Biometric security systems: a guide to devices, fingerprint scanners and facial recognition access control.* https://www.ifsecglobal.com/global/biometric-security-systems-guide-devices-fingerprint-scanners-facial-recognition/

Innovatrics. (2025) *Automated Fingerprint Identification System* https://www.innovatrics.com/glossary/afis-automated-fingerprint-identification-system/#:~:text= Automated%20Fingerprint%20Identification %20System%20(AFIS,identify%20known%20or%20unknown%20 fingerprints.

Jiang, X., &. Yau, N. (2020). Fingerprint minutiae matching based on the local and global structures. *Proceedings of the 15th International Conference on Pattern Recognition*, *2*, 1038-1041). Nanyang: *IEEE.*

Kabir, H., Roy, S., Ahmed, T., & Alam, M. (2021). Smart attendance and leave management system using fingerprint recognition for students and employees in academic institute. *International Global Journal of Computer Science and Technology*, *10*(6), 268 -276.

Kadry, S. (2010). Wireless attendance management system based on iris recognition. *Scientific Research and Essays, 5*(12), 1428– 1435.

Onyishi, D., & Igbinoba, C. (2021). Design and Implementation of a biometric students' time and attendance logging system. *Nigerian Journal of Technology,40*(3), 484–490.

Walia, H., &. Nelu, J. (2016). Fingerprint Based Attendance Systems-A Review. *International Research Journal of Engineering and Technology*, *3*(7) 1166-1171.

Wilder, H., & Wentworth, B. (2025) *Personal Identification: Methods for the Identification of Individuals, Living Or Dead.* Boston: Richard G. Badger, The Gorham Press.