FEDERAL UNIVERSITY OF TECHNOLOGY, AKURE
JOURNAL OF ENGINEERING AND ENGINEERING TECHNOLOGY

DESIGN AND IMPLEMENTATION OF AN ELECTRONIC ATTENDANCE AND ADMITTANCE SYSTEM WITH FINGERPRINT AUTHENTICATION USING PATTERN MATCHING

Martins, O. O., Abdulhamid, M. M., Adegoke, D. T., Omoniyi, O. E. and Gabriel, P. B.

Department of Mechatronics Engineering, Federal University, Oye-Ekiti, Nigeria
**Correspondence: oluwaseun.martins@fuoye.edu.ng*

Martins, O. O., Abdulhamid, M. M., Adegoke, D. T., Omoniyi, O. E. & Gabriel, P. B. (2024): Design and Implementation of an Electronic Attendance and Admittance System with Fingerprint Authentication Using Pattern Matching. *Journal of Engineering and Engineering Technology /18(2), 1-11*

Received Date: 12.02.23 **Accepted Date: 22.08.24**

Abstract
In the modern digital landscape, the need for effective attendance management is becoming increasingly crucial, especially within educational and corporate environments. This research introduces the design and development of an electronic attendance and admittance system that harnesses fingerprint authentication, utilizing the precision of pattern-matching algorithms. The significance of this research is evident in its potential to bolster security measures, curtail potential fraudulent activities, and simplify administrative tasks, all of which are essential in today's fast-paced world. The study is anchored on three core objectives. First, it aims to adopt the pattern-matching method for fingerprint authentication. Second, the focus shifts to the actual design and integration of an electronic attendance and admittance system. Lastly, the research seeks to critically assess the system's operational efficiency and its reliability when applied in real-world contexts. A methodical approach defines the project's blueprint. At its heart, the system is structured around three pivotal modules: the enrollment phase, the authentication process, and a comprehensive database. Essential components include a scanner, raspberry Pi, OLED display, and communication modules for seamless data transfer. The database, crafted using SQLite3, is pivotal, acting as the repository for user templates and crucial attendance records. To gauge the system's performance and reliability, a suite of evaluation techniques were employed. These include metrics like the False Acceptance Rate (FAR) and False Rejection Rate (FRR). Initial findings are optimistic, hinting at the system's potential for widespread implementation across various sectors. After evaluation, the system results in an accuracy rate of 96%, FAR of 2%, and FRR of 4% which demonstrates robustness and reliability in real-world scenarios. Conclusively, this study shows the transformative potential of integrating biometrics into attendance systems and suggests avenues for future exploration.

Keywords: *Biometric, Attendance system, Admittance system, Fingerprint authentication, Pattern Matching.*

Introduction

The rapid evolution of technology has led to the integration of biometrics into various systems to enhance security and efficiency. Among the various biometric modalities, fingerprint recognition stands out due to its uniqueness, permanence, and widespread acceptance (Alagasan et al., 2021). Traditional attendance systems, which often rely on manual entries or card-based methods, are prone to inaccuracies, inefficiencies, and fraudulent activities such as buddy-punching. These challenges underscore the need for a more reliable and secure method of recording attendance (Joshi and Raval, 2020).

The design and implementation of a fingerprint-based attendance and admittance system using pattern matching offers a solution to these challenges. Fingerprint recognition leverages the distinct ridges and valleys present in an individual's fingerprint, which are unique to each person, ensuring that the chances of two individuals having identical fingerprints are infinitesimally small (Singla et al., 2020). Pattern matching in fingerprint recognition involves comparing the minutiae points of the input fingerprint with the stored templates to determine a match. This method is known for its accuracy and speed, making it suitable for real-time applications such as attendance systems (Sharma et al., 2020).

However, like all technological systems, fingerprint-based attendance systems are not without challenges. One of the primary concerns is their vulnerability to presentation attacks, where imposters use fake fingerprints to deceive the system (Jomaa et al., 2022). Furthermore, the quality of the captured fingerprint, system errors,

and environmental factors can also impact the system's performance (Sharma and Selwal, 2021). Despite these challenges, the benefits of fingerprint-based attendance and admittance systems are undeniable. They offer a non-intrusive, fast, and efficient method of authentication. The integration of pattern matching further enhances the system's accuracy, ensuring that only registered individuals are granted access (Dargan and Kumar, 2019). Moreover, with the advent of deep learning and artificial intelligence, there are continuous improvements in fingerprint recognition techniques, making them more robust against various challenges (Joshi et al., 2020).

The significance of this study is underscored by its potential to transform attendance monitoring through the integration of fingerprint-based recognition and pattern matching. Traditional attendance systems have been plagued with inaccuracies, vulnerabilities to fraud, and security breaches (Alagasan et al., 2021; Joshi and Raval, 2020). In contrast, the proposed system addresses these challenges by leveraging the uniqueness of fingerprints, ensuring that only the registered individual can log their attendance and thereby enhancing record integrity (Jomaa et al., 2022). The incorporation of pattern matching further bolsters security by detecting variations or spoofing attempts (Sharma and Selwal, 2021). Beyond security, the system's real-time monitoring offers organizations timely insights into attendance patterns, facilitating proactive management and optimal workforce productivity (Dargan and Kumar, 2019). With its scalability and adaptability, the system can cater to various organizational contexts, from educational to corporate settings, promising a comprehensive solution to attendance monitoring challenges.

This study focuses on the design and implementation of a fingerprint-based attendance and admittance system, leveraging pattern matching for precise and secure identification. Drawing from the insights of Alagasan et al., (2021), the study acknowledges the challenges associated with traditional attendance mechanisms and aims to address these through the integration of biometric recognition. The fingerprint recognition, as emphasized by Joshi and Raval (2020) and Jomaa et al., (2022), serves as the cornerstone of the proposed system, ensuring enhanced accuracy and robust security against fraudulent attempts. While the objective is the system's development, a significant portion of the research will be dedicated to its rigorous evaluation. Using methodologies inspired by Sharma and Selwal (2021), the system's performance will be assessed in terms of accuracy, efficiency, and resilience against spoofing attempts. Beyond the technical design and evaluation, the study will also explore the broader implications of the implemented system in organizational contexts, highlighting its potential to revolutionize workforce management, boost productivity, and streamline operational processes, as suggested by Dargan and Kumar (2019). The evaluation techniques will encompass both quantitative metrics, such as error rates, and qualitative feedback from potential users and stakeholders, ensuring a holistic understanding of the system's efficacy and adaptability.

Materials and Methods

Pattern matching stands out as a pivotal technique in the domain of fingerprint recognition, primarily due to its unparalleled precision, adaptability, and efficiency. At its core, pattern matching involves the meticulous comparison of unique features extracted from a newly scanned fingerprint against those stored in a database, with the overarching aim of identifying the most congruent match. This process is facilitated by the extraction of distinct patterns, predominantly minutiae points, which are then subjected to specialized algorithms for a detailed comparison. One of the salient strengths of pattern matching is its inherent robustness, which ensures unwavering performance even in scenarios where the fingerprints might be slightly distorted or of sub-optimal quality.

When juxtaposed with other fingerprint recognition methodologies, pattern matching's merits become even more pronounced. For instance, ridge pattern analysis, although effective, might occasionally overlook some of the unique minutiae, potentially compromising the accuracy of the recognition. On the other hand, techniques like spectral analysis, while thorough, often demand substantial computational resources, making them less feasible for real-time applications. Pattern matching, in contrast, strikes an optimal balance by offering both accuracy and computational efficiency. Moreover, it ensures heightened data security by storing merely a representation of the unique fingerprint features, rather than the entire image, thereby safeguarding against potential data breaches.

As the landscape of biometric recognition continues to evolve and expand, pattern matching consistently solidifies its position as the preferred method for fingerprint recognition. Its ability to seamlessly blend reliability, accuracy, and security positions it as an indispensable tool in the ever-growing arsenal of biometric authentication techniques.

System Architecture

The fingerprint-based attendance and admittance system comprises three main components:

- Enrollment module
- Authentication Module
- System database.

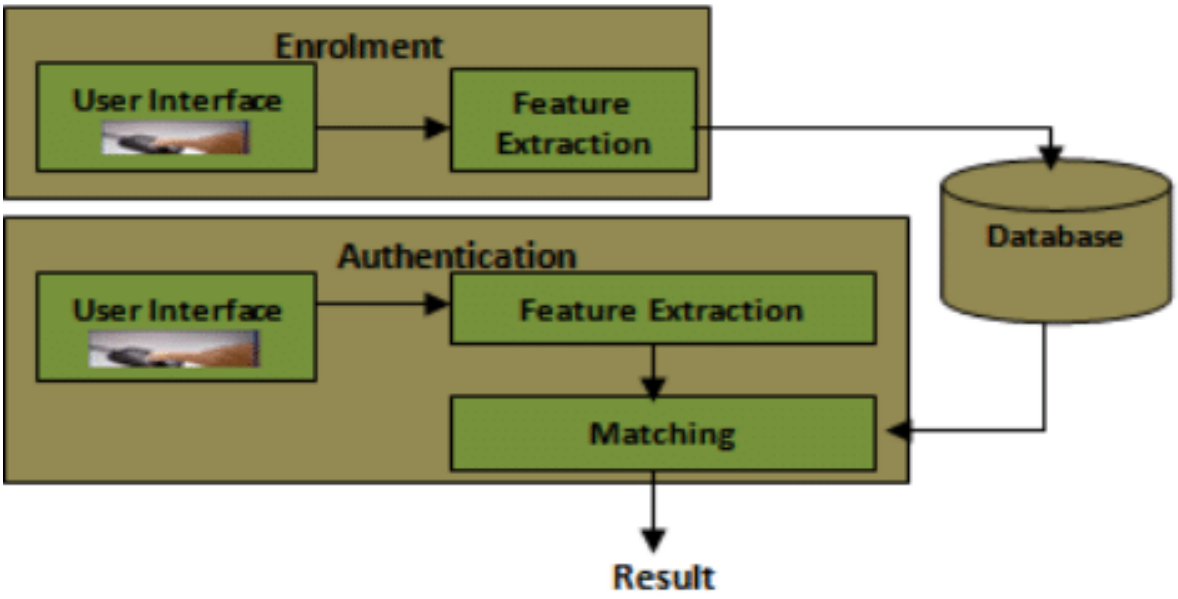

Figure 1: Shows the various modules that make up the architecture of the entire system

Enrollment Module*:* This module is responsible for registering users and their fingerprints into the system's database. During this registration phase, the system captures the user's fingerprint and other relevant details. For lecturers, details such as staff number, surname, position, contact information, etc are recorded. For students, details like matriculation number, department, contact information, etc are stored. Once the fingerprint images and user details are input into the enrollment module, a specific algorithm processes the fingerprint images to extract unique patterns. These patterns, or features, are then stored as a template linked to the user's ID. Additionally, during this phase, relevant course details are also registered.

Authentication Module: This module's primary role is to confirm the identity of an individual trying to access the system. When a person wishes to be authenticated, they provide their identity and place their finger on the fingerprint scanner. The captured fingerprint image undergoes enhancement and processing to extract its biometric template. This template is then compared with the stored templates in the system database to confirm the identity. For student attendance, a student scans their fingerprint and the system checks for a match in the database. Upon a successful match, the system records the student's attendance time and updates their attendance status for the day. Their attendance is recorded for that specific class or session.

Database: The database for the attendance management system is structured with tables, each holding records related to authorized individuals with system access. Every record might encompass the user's first name, last name, department, faculty, matric number of staff number, etc. The system's database design employs a relational data model, characterized by data storage across multiple tables. This database was developed using SQLite3. Sqlite3 is known for its speed and simplicity, capable of housing extensive records with minimal setup requirements.

Adopting Pattern Matching

To seamlessly integrate pattern matching into a fingerprint-based attendance system, a systematic approach is essential. The primary objective is to harness the power of pattern-matching algorithms to accurately identify and verify individuals based on their unique fingerprint patterns, ensuring a robust and efficient attendance system.

Fingerprint Acquisition: The first step involves capturing a high-quality image of the user's fingerprint using a specialized fingerprint module. This module is equipped with sensors that can detect and capture the intricate ridge patterns and minutiae points of the fingerprint.

Feature Extraction: Once the fingerprint image is acquired, the next step is to extract the unique features, primarily focusing on minutiae points such as ridge endings and bifurcations. These extracted features serve as the foundation for the pattern-matching process.

Database Storage: The extracted features are then stored in a secure database. It's crucial to note that only the features are stored, not the actual fingerprint image, ensuring enhanced data security.

Pattern Matching Algorithm: When an individual attempts to mark attendance, their fingerprint is scanned, and the features are extracted in real-time. These features are then compared against the stored features in the database using a pattern-matching algorithm. The algorithm calculates the degree of similarity between the newly scanned fingerprint and the stored ones.

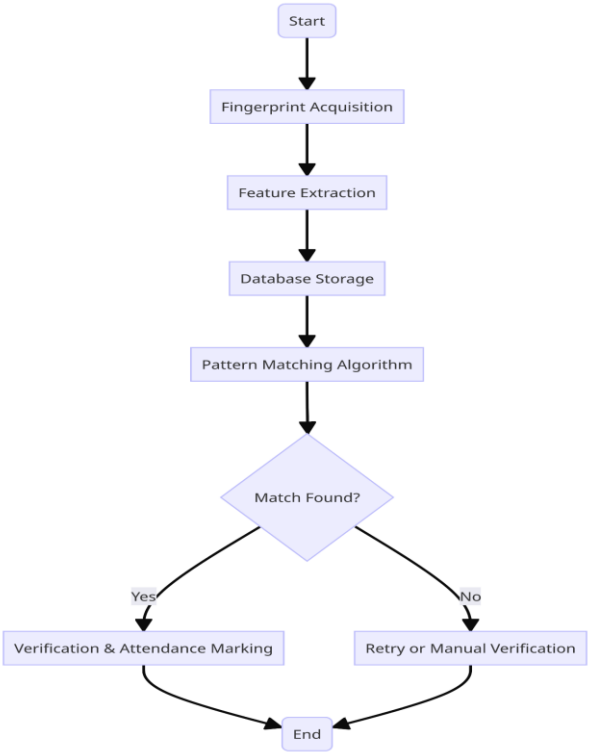

Figure 2: Flowchart for the pattern matching process

Verification and Attendance Marking: If the pattern-matching algorithm finds a match with a high degree of similarity, the individual is verified, and attendance is marked. If no match is found, access is denied, and the individual is prompted to try again or seek manual verification.

Figure 2 visually represents the entire process, starting from fingerprint acquisition to attendance marking. It provides a clear, step-by-step overview of how pattern matching is adopted and integrated into the fingerprint attendance system.

Model Integration: To ensure the seamless functioning of the system, the fingerprint module and the pattern-matching algorithm must be tightly integrated. This integration ensures real-time processing, minimizing the time taken from fingerprint scanning to attendance marking. The model also incorporates feedback mechanisms, allowing for continuous improvement based on real-world usage patterns and challenges.

Mechanical Setup for the System

Figure 3 shows the block diagram of the system setup. From the Raspberry Pi to its interaction with other components of the system.

Control Keys to Raspberry Pi: This connection establishes an interface between the user and the Raspberry Pi. The control keys allow the user to pass commands or data into the Raspberry Pi. For instance, these keys can be used to initiate the fingerprint scanning process, navigate through options, or even reset the system.

Raspberry Pi to USB to Serial Block/UART: The Raspberry Pi communicates with the "USB to Serial" block bi-directionally. This means data can flow in both directions: from the Raspberry Pi to

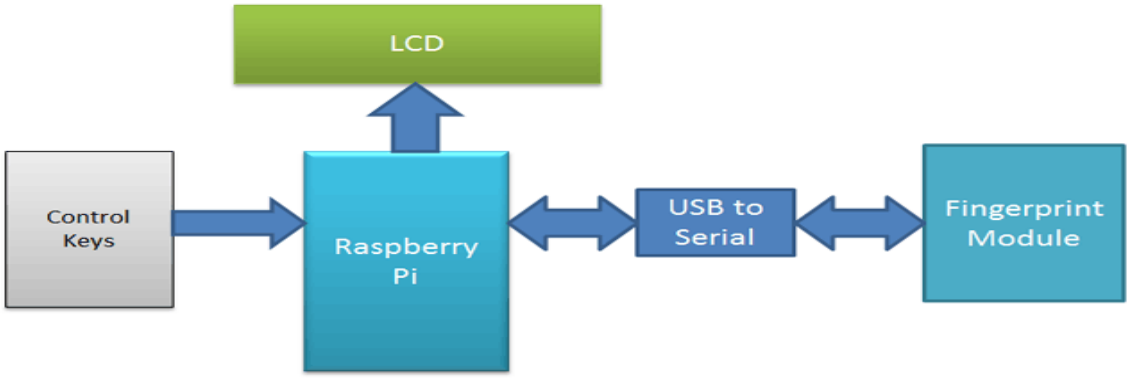

Figure 3: Block diagram of the system setup

the block and vice versa. This connection is essential because the Raspberry Pi typically communicates using digital signals, while many fingerprint modules might use serial communication. The "USB to Serial" block acts as a bridge, converting the digital signals from the Raspberry Pi into a format that the fingerprint module can understand and vice versa.

UART to Fingerprint Module: This connection facilitates the actual communication with the fingerprint module. The "USB to Serial" block sends and receives data to and from the fingerprint module. When a user places their finger on the module, the module captures the fingerprint data and sends it back through the "USB to Serial" block to the Raspberry Pi for processing.

Raspberry Pi to LCD: The Raspberry Pi sends display data to the LCD. This could be feedback messages like "Fingerprint Accepted" or "Access Denied", system status, or any other relevant information. The LCD acts as a visual interface, providing real-time feedback to the user based on the data processed by the Raspberry Pi.

Figure 4 shows the connection between the Raspberry Pi and the fingerprint module.

Pi GND to sensor GND (black wire)
Pi TX to sensor RX (white wire)
Pi RX to sensor TX (green wire)
Pi 3.3v to sensor VCC (red wire)

Pi GND to sensor GND (black wire): This

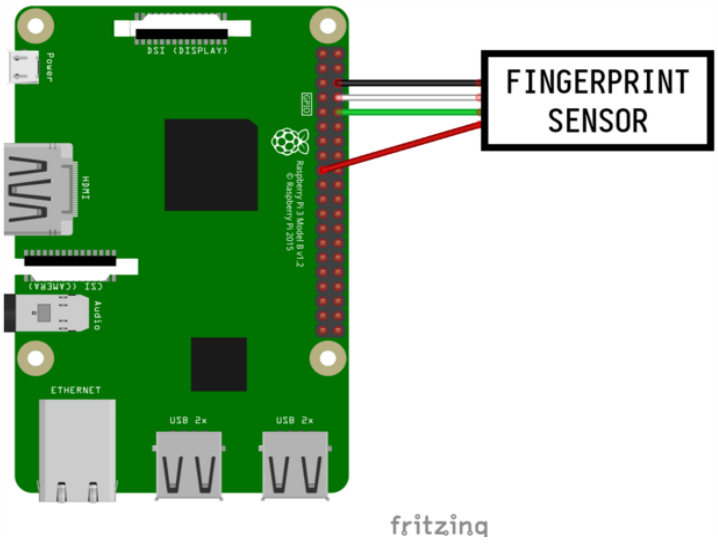

Figure 4: Connection between Raspberry Pi and fingerprint module

establishes a common ground between the Raspberry Pi and the fingerprint sensor. A shared ground is essential for ensuring that the voltage levels between the two devices are referenced to the same point, which aids in proper communication and functioning.
Color Coding: Typically, the black wire is used to denote the ground connection in electronics.

Pi TX to sensor RX (white wire): This connection is for transmitting data from the Raspberry Pi to the fingerprint sensor. TX stands for "Transmit", and RX stands for "Receive". So, the Raspberry Pi sends data out of its TX pin, and the fingerprint sensor receives this data on its RX pin.
Color Coding: The white wire is used here, but the color can vary based on the manufacturer. It's essential to ensure the TX of one device connects to the RX of the other.

Pi RX to sensor TX (green wire): This is the opposite of the previous connection. It's for the fingerprint sensor to send data to the Raspberry Pi. The sensor transmits data from its TX pin, and the Raspberry Pi receives this data on its RX pin.
Color Coding: The green wire is used in this case, but again, the colour can differ based on the manufacturer. The key is ensuring the RX of one device connects to the TX of the other.

Pi 3.3v to sensor VCC (red wire): This provides power to the fingerprint sensor. The Raspberry Pi supplies a 3.3-volt power output, which is connected to the VCC (Voltage at Common Collector) pin of the fingerprint sensor. This powers up the sensor and allows it to operate.
Colour Coding: The red wire is conventionally used to denote a positive power supply in electronics.

In summary, these connections ensure that the Raspberry Pi and the fingerprint sensor have a shared ground, can communicate bi-directionally, and the sensor receive the necessary power to operate. Proper wiring is crucial to ensure that the devices can interact without any issues.

Admittance Section of the System
Figure 5 shows the flowchart of the admittance section of the system. It shows how each step links with other steps to grant access to authenticated users.

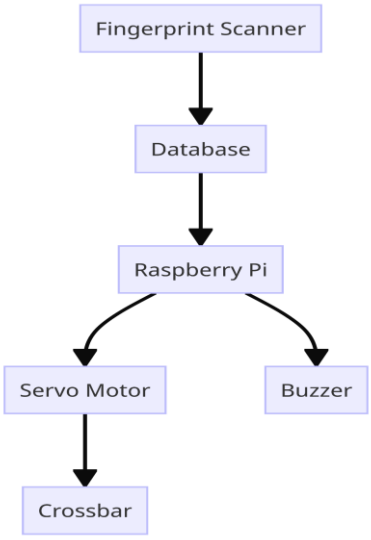

Figure 5: Block diagram for the admittance system

The admittance system is a meticulously designed mechanism that ensures a smooth and secure entry process for users. It integrates the fingerprint authentication system, the servo motor, and the buzzer to create a synchronized and user-friendly experience. Let's delve deeper into each step of this process:

Fingerprint Authentication: Everything starts when a user places their finger on the fingerprint scanner. This scanner captures the unique patterns of the fingerprint and processes it. The system then cross-references this captured data against its stored database, searching for a matching fingerprint that would confirm the user's identity.

Signal Dispatch: If a match is found, the system immediately sends a positive authentication signal to the Raspberry Pi. This signal acts as a digital nod, indicating that the user is recognized and should be granted access.

Servo Motor Actuation: Upon receiving the positive signal from the authentication system, the Raspberry Pi springs into action. It sends a command to the servo motor, which is mechanically connected to a crossbar. The motor, following this command, begins its upward motion, effectively lifting the crossbar. This movement symbolizes an open gate, granting the authenticated user access to the premises.

Buzzer Feedback: The buzzer plays a crucial role in providing real-time auditory feedback to the user. If the authentication is successful, the buzzer emits a short, single beep, serving as an auditory confirmation of successful entry. However, if the system doesn't recognize the fingerprint, the buzzer quickly emits two distinct beeps, signaling to the user that access has been denied.

Continuous Buzzer Sound: As the servo motor lifts the crossbar, the buzzer emits a continuous, low-pitched sound. This sound serves a dual purpose: it alerts the user to wait momentarily and also indicates that the crossbar is in motion. It's a gentle reminder for the user to stand by until the crossbar is fully raised.

Resetting the System: After a brief interval—just enough time for the user to pass through—the Raspberry Pi initiates the reset process. It sends a command to the servo motor to lower the crossbar back to its original position. As the crossbar descends, the buzzer sounds once more, this time indicating that the system is reverting to its initial state, readying itself for the next user.

System Ready: With the crossbar securely back in its starting position and the buzzer silent, the system is now reset and ready to authenticate the next user.

Performance Evaluation

To evaluate the performance of the proposed system, the following were used:

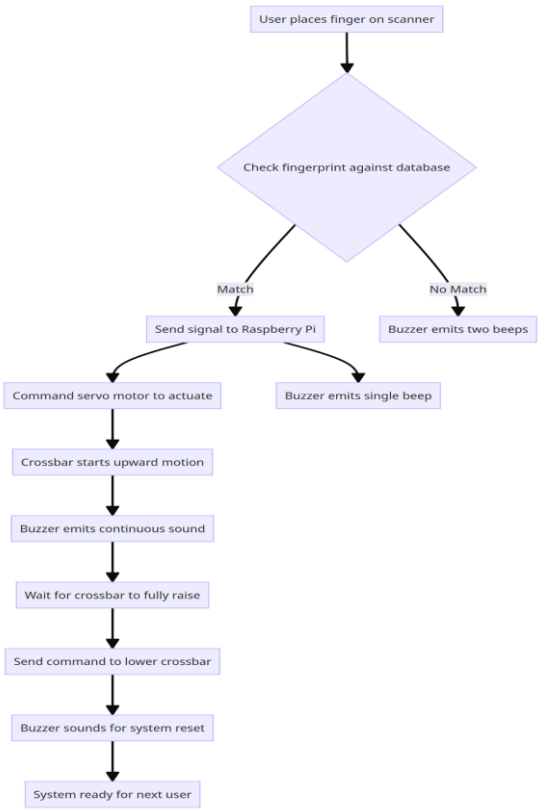

Figure 6: Admittance system flow chart

Accuracy

Accuracy is one of the most straightforward metrics used in classification problems. It

quantifies the overall correctness of the system in making predictions. In the context of fingerprint authentication, accuracy measures the proportion of instances where the system correctly identifies whether the fingerprint belongs to the claimed identity or not. As presented in Equation 1.

Mathematically, accuracy is defined as:

$$\text{Accuracy} = \frac{\text{Number of correct identifications}}{\text{Total Number of identifications}} \quad (1)$$

Equation 1 represents the Accuracy for our system, a high accuracy implies that the system is correctly identifying and authenticating users in most instances. However, it's essential to note that accuracy can sometimes be misleading, especially if the dataset is imbalanced. (Provost and Fawcett, 2013). For instance, if 95% of the inputs are genuine users and only 5% are impostors, a naive system that always predicts 'genuine' will still have a 95% accuracy. This is why, in biometric systems, we often rely on other metrics like FAR and FRR to get a more comprehensive view of the system's performance.

False Acceptance Rate (FAR)

The FAR is a critical metric in biometric systems. It quantifies the system's security by measuring the likelihood that an impostor is incorrectly authenticated as a genuine user. In simpler terms, FAR tells us how often the system makes a security error. Mathematically, FAR is given by Equation 2:

$$\text{FAR} = \frac{\text{False Acceptance}}{\text{Total Validations}} \quad (2)$$

A high FAR represented in equation 2 can be a significant security risk, especially in systems where unauthorized access can lead to severe consequences. For instance, in a high-security facility, a high FAR might allow intruders to gain access. Therefore, in such scenarios, it's crucial to minimize FAR, even if it means occasionally rejecting genuine users. It's a trade-off between security and convenience (Qin *et al.,* 2023).

False Rejection Rate (FRR)

While FAR focuses on security, the FRR represented in equation 3 is more about user convenience. FRR measures the likelihood that a genuine user is incorrectly rejected by the system. It quantifies the system's usability errors. Mathematically, FRR is defined as Equation 3:

$$\text{FRR} = \frac{\text{False Rejections}}{\text{Total Validations}} \quad (3)$$

A high FRR can be a source of frustration for users. Imagine a genuine user trying to mark attendance or access a facility, and the system keeps rejecting them. Such scenarios can lead to dissatisfaction, increased support calls, and even users abandoning the system in favor of less secure but more convenient alternatives. Therefore, while it's essential to keep the system secure (low FAR), it's equally crucial to ensure it remains user-friendly (low FRR) (Qin *et al.,* 2023).

Receiver Operating Characteristic (ROC) Curve

The Receiver Operating Characteristic (ROC) curve is a fundamental tool used in binary classification to understand the performance of an algorithm. It's a graphical representation that illustrates the diagnostic ability of a binary classifier system as its discrimination threshold is varied. The ROC curve is plotted with the True Positive Rate (TPR) against the False Positive Rate (FPR) for various threshold settings.

True Positive Rate (TPR) represented in equation 4, also known as Sensitivity or Recall, measures the proportion of actual positives that are correctly identified (Bradley, 1997). It's given by Equation 4:

$$\text{TPR} = \frac{\text{True Positives}}{\text{True Positives+False Negatives}} \quad (4)$$

False Positive Rate (FPR) as shown in equation 5 measures the proportion of actual negatives that are incorrectly identified as positives (Bradley, 1997). It's defined as presented in Equation 5:

$$\text{FPR} = \frac{\text{False Positives}}{\text{False Positives+True Negatives}} \quad (5)$$

The ROC curve provides insights into the trade-offs between the benefits (true positives) and costs (false positives). The Area Under the Curve (AUC) of the ROC represents the classifier's ability to distinguish between the positive and negative classes. An AUC of 1 indicates a perfect classifier, while an AUC of 0.5 suggests that the classifier's performance is no better than random guessing (Bradley, 1997). For instance, in our system, a ROC curve can help determine the threshold at which the balance between security (not letting unauthorized users in) and usability (not rejecting genuine users) is optimal.

Equal Error Rate (EER)

The EER is a concise metric to summarize the ROC curve. It's the point where the FAR equals the

FRR. At this point, the system is equally likely to make an error of either type. The EER provides a single measure of the system's overall error rate, and it's particularly useful when comparing the performance of different biometric systems or algorithms. A lower EER indicates a better-performing system (Qin *et al.,* 2023).

Results and Discussion

Table 1 gives the results obtained from performing the Accuracy test on the system using 50 attempts and getting an accuracy of 96% using equation 3 tells us how accurate the pattern matching method is in correctly identifying users present in the database. This shows how accurate the model is as based on this result, we can confidently project that 96 out of 100 test cases would be correctly identified.

Table 2 gives the results obtained from performing the False Acceptance test on the system using 50 attempts and getting a FAR of 2% using equation 2

Table 1: Accuracy test results

Model testing	Total number of attempts	Correct identification	Incorrect identifications	Result (%)
Accuracy Test	50	48	2	96

Table 2: False acceptance test result

Model testing	Total number of Unauthorized attempts	Unauthorized attempts granted access	Result (%)
False Acceptance Rate (FAR) Test	50	1	2

Table 3: False rejection test result

Model testing	Total number of authorized attempts	Authorized attempts denied access	Result (%)
False Acceptance Rate (FAR) Test	50	2	4

From table 1, we can see that we have a total attempt of 50 times, out of which 48 were correctly identified, and 2 incorrect identifications which

The False Acceptance test attempts to see how many times an unauthorized user would be able to access the system. From the above table, we see the results for the system. We have 50 attempts, out of

which it was only one time that an unauthorized person was able to access the system. It tells us that this system is well-secured in terms of accurately matching the fingerprints in the database.

Table 3 gives the results obtained from performing the False Rejection test on the system using 50 attempts and getting an FRR of 4% using Equation 5

The False Rejection test attempts to see how many times an authorized user would be denied access to the system. That is, the user has correctly registered and been authenticated, however, the system refuses to grant access. From the above table, we see the FRR results for the system. We have had 50 attempts, out of which it was only twice that an authorized person was denied access to the system. It tells us that this system is reliable and can be counted upon to accurately identify the users when they use the system.

Functional Testing

Functional tests were meticulously conducted to validate the operational integrity of each module within the system.

Enrollment Module: The enrollment module was rigorously tested. During these tests, for every 50 users registered, the system successfully captured both biometric data and personal details 49 times, yielding a 98% success rate.

Authentication Module: The authentication module was similarly assessed. For every 50 authentication attempts, it reliably verified users 48 times by cross-referencing the stored database records, resulting in a 96% success rate.

Evaluation Using Defined Techniques

Accuracy Testing:

Accuracy is calculated using the formula:

From equation 1, the accuracy of the system is:

$$\text{Accuracy} = \frac{48}{50} * 100 = 96\%$$

For our system, the accuracy rate was 96%.

FAR and FRR Testing:

The system's security and user convenience were evaluated using the False Acceptance Rate (FAR) and the False Rejection Rate (FRR).

From equation 2,

The FAR for the system is = $\frac{1}{50} * 100 = 2\%$

From equation 3,

The FRR for the system is = $\frac{2}{50} * 100 = 4\%$

The recorded FAR was 2%, and the FRR was 4%.

The system's adaptability was tested under various environmental conditions. A graph plotting performance against different conditions showed that the system remained consistent in its performance.

Conclusion

This article explains the design and implementation of an electronic attendance and admittance system using pattern matching. Based on the adopted pattern-matching technique for fingerprint recognition, the system was able to achieve an accuracy rate of 96% and correctly identify 48 out of 50 test cases. The electronic attendance and admittance system seamlessly integrated fingerprint authentication, despite minor processing delays. Using evaluation methods like accuracy testing, FAR, and FRR testing and analysis, the system's robust real-world performance was confirmed giving an FAR of 2% and FRR of 4%.

Acknowledgements

We acknowledge the technical input of the technical staff of the Department of Mechatronics Engineering, Federal University Oye-Ekiti.

Conflicts of Interest

No conflict of interest was declared by the author.

References

Adiraju, R. V., Masanipalli, K. K., Reddy, T. D., Pedapalli, R., Chundru,S., and Panigrahy, A. K. (2021). An extensive survey on finger and palm vein recognition systems. *Materials Today: Proceedings, 45*(2), 1804-1808.

Alagasan, K., Alkawaz, M. H., Hajamydeen, A. I., and Mohammed, M. N. (2021). A review paper on advanced attendance and monitoring systems. *2021 IEEE 12th Control and System Graduate Research Colloquium (ICSGRC)*, 195-200.

Bradley, A. P. (1997). The use of the area under the ROC curve in the evaluation of machine learning algorithms. *Pattern Recognition, 30*(7), 1145-1159.

Dargan, S., and Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. *Expert Systems with Applications, 143*, 113114

Jomaa, R. M., Islam, M. S., Mathkour, H., and Al-Ahmadi, S. (2022). A multilayer system to boost the robustness of fingerprint authentication against presentation attacks by fusion with heart-signal. *Journal of King Saud University - Computer and Information Sciences, 34*(8, Part A), 5132-5143.

Joshi, M., Mazumdar, B., and Dey, S. (2020). A comprehensive security analysis of match-in database fingerprint biometric system. *Pattern Recognition Letters,138*, 247-266.

Joshi, V. B., and Raval, M. S. (2020). Adaptive threshold for fingerprint recognition system based on threat level and system load. *Procedia Computer Science, 171*, 498-507

Nelson, J. (2020). Chapter 21 - Access control and biometrics. In L. J. Fennelly (Ed.), *Handbook of Loss Prevention and Crime Prevention (Sixth Edition)* (pp. 239-249). Butterworth Heinemann.

Provost, F., and Fawcett, T. (2013). *Data Science for Business: What you need to know about data mining and data-analytic thinking*. O'Reilly Media.

Qin, Z., Zhao, P., Zhuang, T., Deng, F., Ding, Y., and Chen, D.(2023). A survey of identity recognition via data fusion and feature learning. *Information Fusion, 91*,694-712.

Sharma, A., Arya, S., and Chaturvedi, P. (2020). A novel image compression based method for multispectral fingerprint biometric system. *Procedia Computer Science, 171*, 1698-1707

Sharma, D., and Selwal, A. (2021). FinPAD: State-of-the-art of fingerprint presentation attack detection mechanisms, taxonomy and future perspectives. *Pattern Recognition. Letters, 152*,225-252

Singla, N., Kaur, M., and Sofat, S. (2020). Automated latent fingerprint identification system: A review. *Forensic Science International, 309*, 110187.