Development of Biometric User Identification and Access Control System

Cookey Iyen
Department of Pure and Applied Physics,
Federal University Wukari, Taraba State, Nigeria

Abel Jacob
Department of Pure and Applied Physics,
Federal University Wukari, Taraba State, Nigeria

Ayoola Oluwasegun
Department of Pure and Applied Physics,
Federal University Wukari, Taraba State, Nigeria

ABSTRACT:
Safeguarding digital and physical premises against unauthorized entry is increasingly crucial in an era characterized by fast technological advancements and escalating security risks. Biometric security devices for controlling entry employ distinct form and behavioral attributes to authenticate persons and regulate access, hence offering innovative solutions. This paper offers a comprehensive review of the utilization of fingerprint recognition methods in the creation of an entry authorization device with biometrics. The material and methods section provides a detailed description of the hardware components used, including the Arduino UNO and fingerprint scanner module (SM 630), as well as an in-depth explanation of the construction process and performance evaluation. The text provides detailed explanations of the registration and operating methods, specifically emphasizing the gathering of biometric information, generation of templates, user registration, and the decision-making processes for controlling entry. This paper advocates for the utilization of fingerprint authentication for access control technology as crucial tool for improving safety and mitigating risks in different operational environments. It recommends a systematic approach that involves preparation, construction, testing, deployment, and future planning.

Keywords: Biometric system, Access control, Fingerprint, Arduino UNO, SM-630.


INTRODUCTION
With the continued advancement of technology, there has been a rise in the incidence of impersonation in both private and public realms [1,2,3]. To counter this, biometric security recognition and entry management has grown as a innovative fix that harnesses unique physical and interactive qualities to authenticate, identify and manage access to systems, facilities, and devices [4,5,6]. Unlike earlier approaches, such as passwords or access cards, biometric authentication is exceedingly secure and hard to copy or mimic [7,8]. This makes it a trustworthy and simple identifying mechanism, crucial in an era marked by technological innovation and rising security concerns [9,10,11]. Biometric security access control systems have become vital in safeguarding digital and physical regions, playing a revolutionary role in security paradigms across sectors, including banking, healthcare, government, and critical infrastructure [12,13]. By simplifying access and insuring accountability by full documentation of access activities, biometrics provides a practical and
effective solution to enhance security and reduce susceptibility to counterfeit credentials [14,15]. Fingerprint Scanners by collecting and analyzing unique patterns in a user's fingerprints, may give access only to authorized users [16]. This technology delivers high precision and ease of use, because consumers just need to touch the fingerprint sensor in order to access their devices. There are several sorts of biometric characteristics that may be utilized for identification and access control and they include: facial recognition technology [17,18] use sophisticated algorithms to examine facial characteristics, like the spacing between the eyes, nose, and mouth, in order to generate a distinct biometric profile. While face recognition offers convenience, it has drawn attention addressing privacy and accuracy challenges, specifically concerning apparent biases in detection algorithms. Iris biometrics [19,20] is another form of biometric electronic devices which delivers a high degree of precision and security, as iris patterns are particularly distinctive and difficult to fake. Nevertheless, the adoption of iris scanners has been constrained as a consequence of issues such as prices and the requirement for specialized equipment.

Another type of biometric technology is the voice recognition [21,22] biometrics which analyzes an individual's unique vocal characteristics to verify their identity. While less common than fingerprint or facial recognition, voice recognition can be integrated into devices for tasks such as voice authentication for unlocking devices or authorizing transactions. Behavioral Biometrics [23,24] is a type of biometric technology employed by some devices to continuously authenticate users according to their distinct behavior patterns, such as typing speed and touchscreen interactions. This passive authentication method adds an extra layer of security without requiring explicit user action.

In the current era of technology, it is crucial to prioritize the establishment of safe entry to locations that contain confidential information. This applies to a variety of industries, including government facilities, business settings, and private buildings. Conventional means for gaining access, which include keys and passwords, are being gradually substituted with more advanced biometric verification technique because of their improved security and simplicity. The recognition of fingerprints is considered to be one of the most dependable and extensively used ways for person identification among other biometric technologies.

This study explores the organizing and execution of a biometric identification and entry management system that utilizes fingerprint technology. The device is constructed by combining microcontroller-based hardware, primarily Arduino, with a top-notch fingerprint scanner which is the SM630 fingerprint scanner. Through the combination of these components, our objective is to develop a resilient and effective access control system that guarantees both safety and user ease.

The Arduino platform [25-29], serves as the basis for the hardware architecture of our system. The variety, simplicity of programming, and cost-effectiveness of Arduino make it an excellent option for creating embedded systems, such as biometric applications. By using Arduino, we can develop a versatile and adaptable system that can connect with different peripheral devices, such as fingerprint scanners, transistors and relays to perform switching operations using biometric identification.

An essential component of our system is the integration of a cutting-edge fingerprint scanner SM-630 fingerprint scanner. The captured fingerprints are saved as templates to the flash memory of the Arduino board. The SM-630 IDE software allows for already captured finger template data to be imported. This makes it possible to easily transfer already captured data from system to system or to integrate them through networks using a number of fingerprint scanners This device serves as the principal way of obtaining and processing fingerprint pictures, allowing accurate and reliable identification of people. Leveraging developments in sensor technology, current fingerprint scanners provide high-resolution imaging capabilities and sophisticated feature extraction algorithms, therefore boosting the accuracy and security of biometric identification systems.

This work offers a thorough investigation of the planning and execution of a fingerprint-based biometric identification and access control system. Our goal is to provide a reliable, effective, and easy-to-use solution for safe access management in a variety of settings by using microcontroller-based hardware, the Arduino platform, and cutting-edge fingerprint scanning technologies. By doing this study, we want to further the development of biometric authentication systems and encourage their broad use in protecting confidential data and assets.
MATERIAL AND METHOD

Material Used
Various materials were utilized during the research process, including a Direct Current (D.C.) power supply source, an Arduino UNO showcased in Figure 2 below, a fingerprint scanner module (SM 630) displayed in Figure 1 below, a display screen, a breadboard for testing and organization, 220Ω resistors, soldering lead, a jumper wire kit (male and female), a 10kΩ variable resistor, LEDs, and a Vero-Board for permanent soldering.

![Figure 1. SM 630 Fingerprint Scanner](image1)

![Figure 2. Arduino UNO Board](image2)

Method Used
To implement a reliable biometric security access control system, a combination of hardware and physical components is necessary. As shown in the figure below, the fingerprint scanner captures the attributes of the finger that is placed on it and saves it as a template together with the name of the individual that is being captured. The implementation process comprises of two stages, the first stage is the registration of individuals into the system while the second stage is the identification and authentication of registered users to grant access. In the case of registration of new users, the new user places his/her finger on the scanner, the scanner scans the fingerprint and saves it to the arduino flash memory together with the name of the individual which is saved together with the template. For the user authentication, recognition and access control part of the setup, the template of fingerprint placed on the scanner is collected then it is searched for in the database in the arduino memory, if the individual is found in the database, the person's name is displayed on the LCD and the person is allowed access by writing a digital pin on the arduino to logic 1 however if the person's finger template is not found in the database, the person is denied access figures 4 and 5 show the flowchart used for writing the arduino codes for user registration and access control respectively.
CONSTRUCTION AND PERFORMANCE EVOLUTION

Figure 3. Working Diagram for the Project

Figure 4. Flowchart for the Arduino Program for Registration of New Users
PROJECT DESCRIPTION

This section provides an in-depth look into the construction methodology and performance evolution of the biometric security access control system. It outlines the steps taken during its construction and the iterative improvements made to enhance its performance over time.

Enrollment and Working Process
The enrollment and working process of the biometric security access control system involves the following steps to ensure accurate authentication and efficient access control [30,31,32]:

**Enrollment Process**

User Registration: Users provide and select the biometric modality for enrollment.

Biometric Data Capture: Users present their biometric traits to the designated sensor.

Template Generation: Specialized algorithms process the captured biometric data to extract unique features and create a template representation.

Template Storage: The generated templates are securely stored in the Arduino system’s database, associated with the corresponding user’s identification details.

**Working Process**

Authentication Request: Individuals initiate an authentication request by presenting their biometric trait to the designated fingerprint scanner sensor [32].

Biometric Data Capture: The sensor captures a fresh sample of the individual's biometric trait and converts it into a digital representation [33].

Template Comparison: Matching algorithms compare the captured biometric data against the stored templates in the database [34].

**Access Control Decision**

Based on the comparison results, the system makes an access control decision [35,36]. If the captured biometric trait matches any stored template within acceptable thresholds, access is granted. If there is no match or the match falls below the specified thresholds, access is denied [37-42].

![Completed Schematic Of A Biometric Access Control System](image)

**Figure 6. Completed Schematic Of A Biometric Access Control System**
Figure 7. Testing the Sub-circuits on a Breadboard

Figure 8. Construction Process

Figure 9: The Completed and Packaged Work
CONCLUSION

In conclusion, this research study has provided valuable insights into the implementation of biometric access control system [43], improving user experience, cost effectiveness and efficiency. Future research should focus on addressing Data privacy concern, environmental Limitation maintenance and support and exploring Biometric fusion techniques, Continuous authentication, Privacy-preserving biometrics and Behavioral biometric [7,23,44,45].

RECOMMENDATION

Combining multiple biometric modalities reduces the likelihood of false positives or false negatives associated with individual biometric traits [5, 46-48]. For example, if facial recognition fails due to poor lighting conditions, fingerprint authentication can serve as a backup, ensuring reliable identification. Multi-modal systems leverage the strengths of each biometric trait while compensating for their respective weaknesses [33, 49-51]. This results in more accurate and reliable authentication, even in challenging environments or under varying conditions.

REFERENCE


42. Y.X.M. Tan, A. Iacoavazzi, I. Homoliak, Y. Elovici, A. Binder, “Adversarial attacks on remote user authentication using behavioural mouse dynamics,” In 2019 International Joint Conference on Neural Networks (IJCNN) (pp. 1-10). IEEE, 2019. DOI: 10.1109/IJCNN.2019.8852414


