

Multi Factor Bio Metric Access Control System For Secure Physical Document Using Fingerprint and Dwelltime Authentication

Kavya G. R¹, Dr. Swapna Pavan²

^{1,2}Department of studies in Computer Science (M.Sc.), Davangere University, Shivagangotri, Davangere-577007, Karnataka, India.

Abstract

Protecting confidential physical documents is essential in organizations and institutions where unauthorized access can lead to information loss and security breaches. This paper presents a Multi-Factor Biometric Access Control System for Physical Documents using an Arduino Uno and a fingerprint sensor for secure authentication. The system verifies the user's fingerprint before actuating a servo motor to unlock the document storage unit. An OLED display provides real-time system status and user guidance, while visual and audible indicators enhance usability and security. The proposed system eliminates the need for traditional keys and passwords, reducing the risk of theft, duplication, and unauthorized access. It is designed to be portable, cost-effective, and energy-efficient for standalone operation. Experimental testing demonstrated reliable authentication, fast response time, and stable lock control. The proposed solution provides a practical and scalable approach for protecting confidential physical documents and can be extended with future security enhancements such as IoT connectivity and remote monitoring.

KeyWords: Fingerprint Authentication, Biometric Access Control, Arduino Uno, Document Security, Embedded System, Servo Motor, Access Control System, Physical Document Protection.

I. INTRODUCTION

The security of confidential physical documents is a major concern in government organizations, educational institutions, financial sectors, and corporate offices. Conventional security methods, such as mechanical locks and key-based systems, are vulnerable to key duplication, lock picking, and unauthorized access. These limitations highlight the need for a more secure and reliable access control mechanism to protect valuable documents. Biometric authentication has emerged as an effective solution for secure access control due to its accuracy and uniqueness. Among various biometric techniques, fingerprint recognition is widely adopted because every individual possesses unique fingerprint patterns, making it highly reliable for user authentication. Fingerprint-based systems eliminate the need for physical keys and passwords while improving security and user convenience. This paper presents the design and development of a Biometric Access Control System for Physical Document Security using an Arduino Uno, an optical fingerprint sensor, a servo motor, and an OLED display. The system authenticates users through fingerprint verification and automatically unlocks the document storage unit for authorized users while denying unauthorized access. The proposed solution is portable, cost-effective, energy-efficient, and suitable for securing

confidential physical documents in offices, institutions, and residential environments.

Problem Statement: The protection of confidential physical documents remains a significant challenge in organizations, educational institutions, banks, and government offices. Conventional security mechanisms, such as mechanical locks and key-based systems, are vulnerable to key duplication, lock picking, loss of keys, and unauthorized access. Password-based systems also suffer from security issues such as password sharing, guessing, and misuse. These limitations reduce the reliability of traditional document protection methods and increase the risk of information theft and document tampering.

To overcome these challenges, there is a need for a secure, portable, and cost-effective access control system that authenticates users based on their unique biometric identity. The proposed system addresses this problem by employing fingerprint-based biometric authentication using an Arduino Uno, optical fingerprint sensor, servo motor, and OLED display. By allowing access only to authorized users, the system enhances the security of physical documents while providing an efficient and user-friendly locking mechanism.

Objectives:

- To design and develop a secure access control system for protecting confidential physical documents using fingerprint-based biometric authentication.
- To implement an embedded authentication mechanism using an Arduino Uno microcontroller for real-time fingerprint verification.
- To develop an automated locking and unlocking mechanism using a servo motor, allowing access only to authorized users.
- To provide real-time user interaction and authentication status through an OLED display and visual/audible indicators.
- To develop a portable, cost-effective, and energy-efficient document security solution suitable for offices, educational institutions, and residential environments.
- To improve the security of physical document storage by eliminating the limitations of conventional key-based locking systems and preventing unauthorized access.

II. RELATED WORK:

[1] F. M. Salama and A. Shokry (2022) proposed a secure biometric access control framework using fingerprint authentication with encrypted fingerprint templates. The system improved template security and user authentication.

Drawback: The encryption process increased computational complexity and required additional processing resources.

[2] Sharmin Yasmin (2023) developed a Fingerprint Door Lock System Using Arduino Uno with a fingerprint sensor, relay module, and solenoid lock. The system successfully authenticated authorized users and prevented unauthorized access. Drawback: The design was intended for door security and did not provide document-specific protection or user status display.

[3] Muhammad Afif and Rahmat Rasyid (2023) designed an Arduino Uno-based bag security system using a fingerprint sensor, PIR sensor, and limit switch. The proposed system improved the protection of personal belongings through biometric authentication. Drawback: The system required multiple sensors, increasing hardware complexity.

[4] I Wayan Agus Edi Saputra et al. (2023) proposed a computer laboratory door security system using an Arduino Uno, fingerprint sensor, buzzer, LCD, and solenoid lock. The system replaced conventional locks with biometric authentication. Drawback: The implementation was limited to door access control and required fixed installation.

[5] Siddhartha Bhowmick, Aman Kumar, and Sai Manas (2023) presented a Fingerprint Door Lock using Arduino UNO R3 that enhanced security through biometric authentication and discussed integrating advanced encryption techniques. Drawback: The system mainly focused on door locking rather than protecting physical document storage.

[6] Navneet Kaur, Nidhi Ahirwar, Mohini Prasad, Ankit Sharma, and Chetan Bhaisare (2023) evaluated an Arduino-integrated fingerprint locker security system for banking applications. The study demonstrated the effectiveness of fingerprint authentication in securing lockers. Drawback: The proposed system was designed specifically for banking environments and did not emphasize portability.

III. METHODOLOGY

The proposed biometric document security system is designed to provide secure access to confidential physical documents through fingerprint authentication. The system integrates an Arduino Uno microcontroller, an optical fingerprint sensor, a servo motor, an OLED display, LEDs, and a buzzer to achieve reliable and automated access control. The overall methodology consists of requirement analysis, system design, hardware implementation, software development, system testing, and maintenance planning.

3.1 Requirement Analysis

The initial phase focuses on identifying the functional and security requirements of the proposed system. The primary objective is to protect confidential physical documents from unauthorized access while providing a user-friendly authentication mechanism. The system requirements include fingerprint-based user authentication, automatic locking and unlocking, real-time status display, low power consumption, portability, and reliable operation. The hardware and software

requirements are analyzed to ensure efficient integration and stable performance.

3.2 System Design

Based on the identified requirements, the overall system architecture is designed. The Arduino Uno functions as the central controller, communicating with the fingerprint sensor to verify user identity. Upon successful authentication, the Arduino activates the servo motor to unlock the document storage box. An OLED display provides real-time messages such as "Place Finger," "Access Granted," and "Access Denied," while LEDs and a buzzer provide visual and audible feedback. The system design emphasizes simplicity, security, and ease of implementation.

3.3 Software Development

The embedded software is developed using the Arduino IDE and Embedded C programming language. The program initializes all hardware modules, enrolls and stores fingerprint templates, performs fingerprint matching, controls the servo motor, updates the OLED display, and manages LED and buzzer notifications. The software continuously monitors authentication requests and ensures secure access control by allowing only authorized users.

3.4 Hardware Implementation

The hardware implementation involves integrating the Arduino Uno with the optical fingerprint sensor, servo motor, OLED display, LEDs, buzzer, and power supply. Proper wiring and serial communication are established to ensure accurate fingerprint verification and smooth operation of the locking mechanism. After assembling all components, the prototype is tested under different operating conditions to verify functionality and reliability.

3.5 Testing and Validation

The developed prototype is tested using multiple fingerprint authentication attempts to evaluate system performance. The testing process verifies successful authentication, unauthorized access rejection, servo motor operation, OLED display functionality, and automatic re-locking. Performance parameters such as response time, authentication reliability, and operational stability are analyzed to ensure the system meets the intended security requirements.

3.6 Maintenance and Future Enhancement

The proposed system requires periodic maintenance to ensure reliable operation of the fingerprint sensor, servo motor, and other hardware components. Future enhancements may include battery backup, IoT-based remote monitoring, encrypted access logs, GSM alert notifications, and multi-user access management to further improve system security and functionality.

ARCHITECTURE DIAGRAM

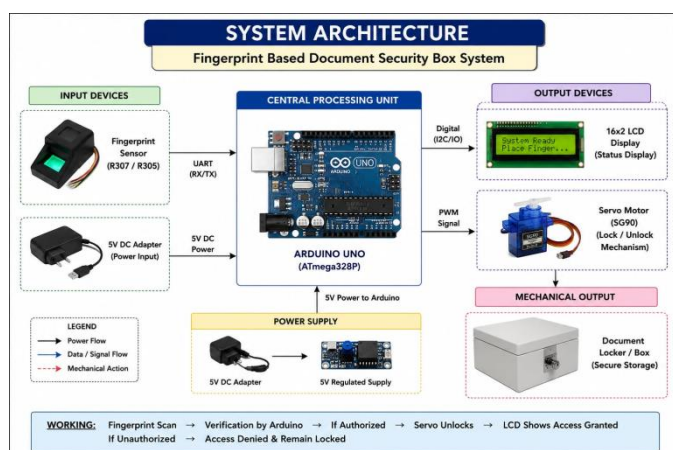


Fig 1: System Architecture

The proposed Multi-Factor Biometric Document Locker System consists of five main modules: User Input, Central Controller, Output Devices, Document Locking Mechanism, and Power Supply. The user provides authentication through a fingerprint sensor (with optional keypad and RFID modules for multi-factor authentication). The Arduino Uno acts as the central controller, processing the authentication data and making access decisions. If the user is successfully authenticated, the Arduino activates the servo motor to unlock the document locker and displays "Access Granted" on the OLED display. If authentication fails, the locker remains locked, the OLED displays "Access Denied," and the buzzer generates an alert. The entire system is powered by a regulated 5V power supply, ensuring reliable and secure operation for protecting confidential physical documents.

IV. APPLIED TECHNOLOGY

The proposed Multi-Factor Biometric Access Control System for Physical Documents combines embedded hardware and software technologies to provide secure and reliable access control. The following technologies are used in the implementation of the system.

4.1 Arduino Uno

Purpose: Central controller of the system.

Use in Project: The Arduino Uno (ATmega328P) processes fingerprint authentication data, controls the servo motor, manages the OLED display, and activates the buzzer during unauthorized access attempts. It serves as the main processing unit for the entire system.

4.2 Fingerprint Sensor (R307/AS608)

Purpose: Biometric user authentication.

Use in Project: The optical fingerprint sensor captures the user's fingerprint, compares it with stored fingerprint templates, and sends the authentication result to the Arduino Uno for access control.

4.3 Servo Motor (SG90)

Purpose: Automatic locking mechanism

Use in Project: The servo motor performs the locking and unlocking of the document storage box based on the authentication result received from the Arduino Uno.

4.4 OLED Display

Purpose: User interface.

Use in Project: The OLED display provides real-time status messages such as "Place Finger," "Access Granted," and "Access Denied," improving user interaction and system usability.

4.5 Arduino IDE

Purpose: Software development environment.

Use in Project: The Arduino IDE is used to write, compile, debug, and upload the Embedded C program to the Arduino Uno. It also supports serial monitoring for testing and troubleshooting.

4.6 Embedded C Programming

Purpose: Embedded software development.

Use in Project: Use in Project: Embedded C is used to implement fingerprint authentication, servo motor control, OLED display communication, buzzer operation, and overall system control logic.

4.7 Power Supply

Purpose: Power management.

A regulated 5V DC power supply provides stable power to the Arduino Uno and all connected peripherals, ensuring reliable system operation.

4.8 Communication Interfaces

Purpose: Hardware communication.

Use in Project:

- UART (Serial Communication): Used for communication between the fingerprint sensor and Arduino Uno.
- I²C Communication: Used to interface the OLED display with the Arduino Uno.
- PWM (Pulse Width Modulation): Used to control the rotation angle of the servo motor.

V. RESULTS AND DISCUSSION

5.1 Hardware Prototype

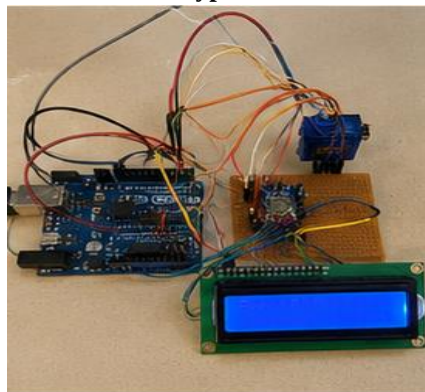


Fig 2: Hardware prototype of the proposed biometric document security system

5.2 Fingerprint Authentication Process



Fig 3: Fingerprint Enrollment Process

Access Denied



Fig 6: Unauthorized Authentication



Fig 4: Fingerprint Verification Process

5.3 Document Locker Operation

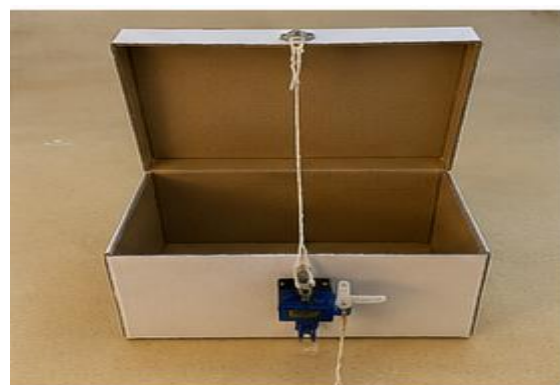


Fig 7: Locker Opened



Fig 5: Successful Authentication

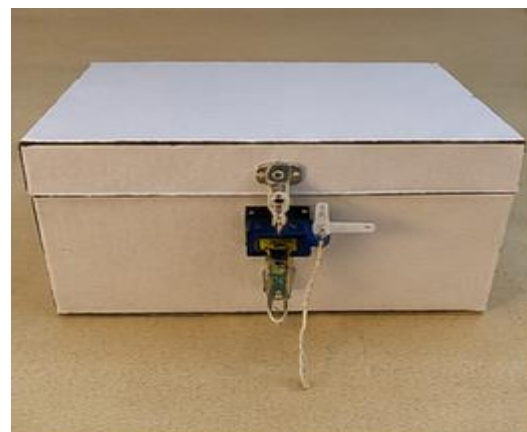


Fig 8: Locker Locked for Unauthorized user

5.4 Experiment Results

Test Case	Description	Expected Result	Actual Result	Status
TC1	Fingerprint Enrollment	Store fingerprint	Successful	Pass
TC2	Authorized Finger	Unlock locker	Successful	Pass
TC3	Unauthorized Finger	Deny access	Successful	Pass
TC4	Servo Operation	Open/Close locker	Successful	Pass
TC5	LCD/OLED Display	Display status	Successful	Pass

5.5 Discussion

The experimental results demonstrate that the proposed biometric document security system operates reliably under different authentication scenarios. The fingerprint sensor successfully enrolled and verified authorized users, while unauthorized fingerprints were rejected. The Arduino Uno effectively controlled the servo motor to lock and unlock the document locker based on authentication results. The LCD/OLED display provided clear user feedback throughout the process. These results indicate that the proposed system is suitable for protecting confidential physical documents in educational institutions, offices, and residential environments.

VI. CONCLUSION

This paper presented a Multi-Factor Biometric Access Control System for Physical Documents that provides secure and reliable protection for confidential physical files using fingerprint-based authentication. The proposed system integrates an Arduino Uno, optical fingerprint sensor, servo motor, LCD display, and buzzer to implement an automated document locking mechanism. Experimental results demonstrated that only authorized users could successfully unlock the document locker, while unauthorized access attempts were denied, thereby enhancing the security of physical document storage. The developed prototype is simple, cost-effective, portable, and suitable for applications in educational institutions, offices, banks, and residential environments. The proposed system offers an efficient and practical solution for improving the security of physical document access.

REFERENCE

- [1] A. K. Jain, K. Nandakumar, and A. Ross, "50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities," *Pattern Recognition Letters*, vol. 79, pp. 80–105, 2016.
- [2] I. Velásquez, A. Caro, and A. Rodríguez, "Authentication Schemes and Methods: A Systematic Literature Review," *Information and Software Technology*, vol. 94, pp. 30–37, 2018.
- [3] P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A Survey on Adaptive Authentication," *ACM Computing Surveys*, vol. 52, no. 4, Article 80, 2019.
- [4] W. Yang, S. Wang, M. Shahzad, and W. Zhou, "A Cancelable Biometric Authentication System Based on Feature-Adaptive Random Projection," *Journal of Information Security and Applications*, vol. 58, p. 102704, 2021.
- [5] M. Nappi, S. Ricciardi, and M. Tistarelli, "Context Awareness in Biometric Systems and Methods: State of the Art and Future Scenarios," *Image and Vision Computing*, vol. 76, pp. 27–37, 2018.
- [6] T. J. Neal and D. L. Woodard, "You Are Not Acting Like Yourself: A Study on Soft Biometric Classification, Person Identification, and Mobile Device Use," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 2, pp. 109–122, 2019.
- [7] N. Solayappan and S. Latifi, "A Survey of Unimodal Biometric Methods," in *Proceedings of the International Conference on Security and Management*, 2006, pp. 57–63.
- [8] X. Zhang, L. Yao, C. Huang, T. Gu, Z. Yang, and Y. Liu, "DeepKey: A Multimodal Biometric Authentication System via Deep Decoding Gaits and Brainwaves," *ACM Transactions on Intelligent Systems and Technology*, vol. 11, no. 4, Article 49, 2020.
- [9] F. Roli, L. Didaci, and G. L. Marcialis, *Adaptive Biometric Systems That Can Improve with Use*. London, U.K.: Springer, 2008.
- [10] K. Z. C. Tun and S. M. M. Zaw, "Gait-Based Human Identification Through Intra-Class Variations," in *Proceedings of the 6th International Conference on Inventive Computation Technologies (ICICT)*, IEEE, 2021, pp. 564–571.
- [11] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, and N. Karimian, "ECG Biometric Authentication: A Comparative Analysis," *IEEE Access*, vol. 8, pp. 117853–117866, 2020.
- [12] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. New York, NY, USA: Springer, 2006.
- [13] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[14] R. C. Gonzalez and R. E. Woods, Digital Image Processing, 4th ed. Pearson Education, 2018.

[15] Arduino, "Arduino Uno Rev3 Technical Specifications."
Available: <https://docs.arduino.cc/hardware/uno-rev3>