

Design of an ESP32-based Intelligent Door Lock Control System

Mingyue Pang*

School of Intelligence and Electronic Engineering, Dalian Neusoft University of Information, Dalian 116023, China

*Corresponding email: pangmingyue323@163.com

Abstract

Conventional commercial smart door locks generally adopt only a single unlocking mode and rely heavily on Wireless Fidelity (Wi-Fi) for alarm transmission, which results in poor accessibility for the elderly and children and inadequate local security protection. Once the wireless connection is disrupted, remote alarm and monitoring functions become unavailable, bringing potential risks to household security. To address these drawbacks, this paper proposes a multimodal smart door lock control scheme based on the ESP32-S3 microcontroller unit (MCU). The system integrates three identity authentication methods: keypad password verification, ZW101 fingerprint recognition, and RC522 radio-frequency identification (RFID) card authentication. A SIM7600 4th Generation mobile communication technology (4G) module is deployed to realize offline short message service (SMS) alarming, while a 28BYJ-48 stepper motor driven by a ULN2003 chip performs physical locking and unlocking operations. An SSD1306 organic light-emitting diode (OLED) screen acts as the human-machine interaction terminal to display real-time system status. The whole system forms a closed-loop workflow including data acquisition, logic judgment and feedback execution. Hardware schematics and printed circuit board (PCB) layouts are designed on the Jialichuang-electronics design automation (JLC-EDA) platform, and modular firmware is developed within the Espressif Internet of Things Development Framework (ESP-IDF). Multiple encryption mechanisms are adopted for key data storage and transmission to enhance information security. Functional experiments show that the average system response time reaches approximately 1.8 s, and the fingerprint recognition accuracy exceeds 97%. When four consecutive failed authentication attempts are detected, the system triggers local alerts and sends short message service (SMS) alarm messages to designated administrators via the 4G cellular network. The stepper motor module achieves reliable positioning and stable operation. This design realizes local multimodal unlocking and network-independent security warning at low cost. It can meet the daily security requirements of households and has practical application value for residential smart home scenarios.

Keywords

Smart door lock, Multimodal unlocking, 4th Generation mobile communication technology, Remote alarm, Embedded security system

Introduction

With the rapid advancement of the Internet of Things (IoT) and embedded technologies, smart home devices have been widely adopted. As a critical household security facility, smart door locks have attracted extensive research attention from both academia and industry [1]. Traditional mechanical locks have inherent risks such as key loss and unauthorized key duplication. Most commercial smart locks support merely one unlocking method and heavily depend on Wi-Fi connectivity. Remote alarms and anomaly notifications cannot work under offline conditions. Meanwhile, complicated operation procedures degrade user experience for elderly users and children.

Overseas manufacturers including Yale and Schlage have launched high-end smart lock products equipped with biometric recognition and data encryption. Nevertheless, such commercial products usually require dedicated home gateways and come with high costs, limiting their large-scale deployment in residential environments. Relevant academic studies focus on low-cost MCU hardware design, multi-factor authentication evaluation and power consumption optimization [2]. Some solutions adopt blockchain algorithms to improve security, whereas other simplified designs reduce hardware costs at the expense of system expandability [3]. In China, the smart lock market continues to expand.

Mainstream brands such as DESSMANN, Kaadas and Xiaomi offer products covering multiple price ranges. High-end products adopt three-dimensional (3D) facial recognition and smart home interconnection, yet their price exceeds 2,000 yuan.

Mid-to-low-end products mostly combine password and fingerprint unlocking, with alarm functions relying on local Wi-Fi. Existing challenges include weak encryption capability and insufficient defense against brute-force attacks. Previous ESP32-related research has realized basic unlocking functions, but many studies ignore offline emergency communication and multi-layer anti-attack strategies [4,5].

To fill the above research gaps, this paper develops a multimodal smart door lock control system using the ESP32-S3 as the main controller. Three local authentication channels are implemented: a numeric keypad, a fingerprint sensor and an RFID card reader. The SIM7600 4G module removes Wi-Fi coverage restrictions and guarantees alarm message delivery without local wireless networks.

The system supports standalone local operation, prioritizes user-friendliness for all age groups, and balances security, cost and expandability. It provides a

feasible technical reference for low-cost embedded household security terminals [6].

System overall architecture

This paper presents a multimodal smart door lock control system based on the ESP32-S3 MCU. The system adopts a layered architecture consisting of a perception layer, control layer, actuation layer, human-machine interaction layer and communication layer. Taking the ESP32-S3 as the core controller, the system collects user identity information through a matrix keypad, ZW101 fingerprint recognition module and RC522 RFID card reader. The ESP32-S3 carries out logical identity verification and transmits control commands to actuators such as the stepper motor. An SSD1306-driven OLED screen displays real-time system status and operation prompts, and local reminders are activated upon authentication failures. The SIM7600 4G cellular module enables SMS transmission to mobile terminals. Accordingly, the system constructs a closed-loop feedback mechanism covering identity collection, identity authentication, actuator execution and security alarming. The overall functional block diagram of the proposed system is shown in Figure 1.

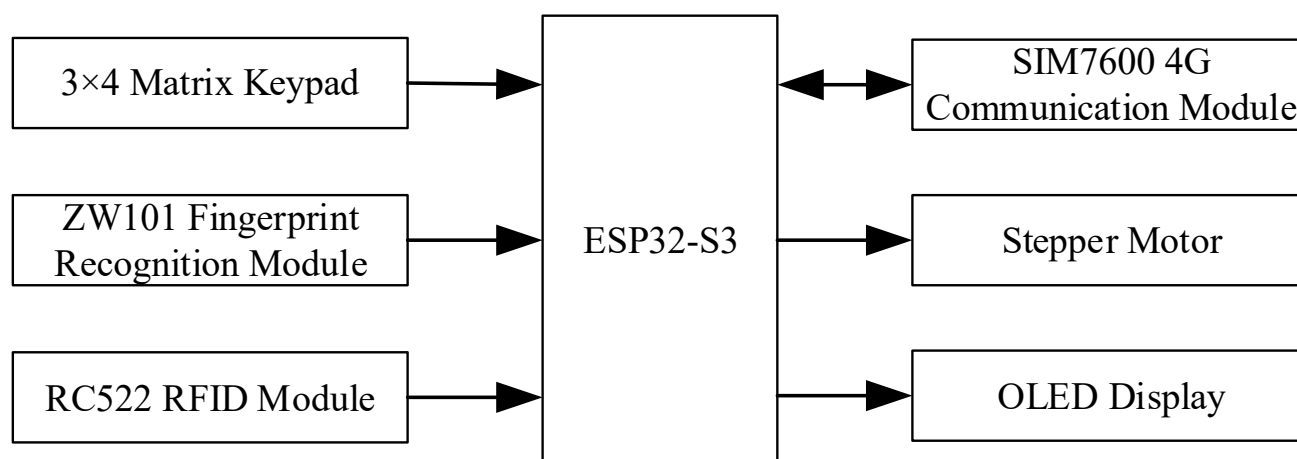


Figure 1. Overall system functional block diagram.

The system functions are divided into three core modules.

Multi-source identity perception module

This module is responsible for real-time collection of user identity authentication data for the embedded access control system. The matrix keypad captures password input from users, registering each keystroke when users manually enter their preset access passwords. The ZW101 fingerprint module collects and extracts biometric fingerprint features by scanning fingerprint ridges and valleys, converting biological information

into digital feature templates; the RC522 RFID module reads the unique identifier (UID) of contactless IC cards once the card approaches the induction area. To avoid misjudgment caused by unstable sampling and mechanical bouncing, the ESP32-S3 MCU performs software debouncing and validity verification on raw sampled data, filtering out transient noise and invalid signal interference. Verified identity data are used for local authentication comparison, administrator user management and error counting for security protection.

When authentication fails repeatedly, the system will trigger locking mechanisms to block further login attempts and reduce the risk of brute-force cracking. All processed authentication records can be temporarily cached locally for subsequent query and audit [7].

Multimodal human-machine interaction module

This module supports three unlocking interaction modes: fingerprint recognition, keypad password input and RFID card swiping to accommodate diverse user operation habits in daily access scenarios. Authentication results are fed back to users via the OLED screen with clear text prompts and simple icon display. Administrator operations including entering administrator mode, adding or deleting user credentials and configuring system parameters are supported through a guided menu workflow on the display.

The OLED screen dynamically presents the standby interface, unlocking results, error prompts and alarm status in real time during system running. Once brute-force cracking attempts are detected after consecutive failed identity verifications, the SIM7600 4G module sends intrusion warning SMS messages to preconfigured administrator mobile phones, so that administrators can promptly learn about abnormal access behaviors and take corresponding emergency disposal measures. The whole notification process relies on stable cellular network transmission to guarantee timely alarm delivery even in places without wired network coverage [8].

Intelligent lock actuation and security alarm module

This module implements two logical functions: normal locking or unlocking execution and abnormal security response. Under normal circumstances, upon successful identity authentication, the ESP32-S3 outputs pulse sequences to drive the 28BYJ-48 stepper motor through the ULN2003 chip to complete unlocking. After a preset delay, the motor rotates reversely to realize automatic door locking, which eliminates the need for manual locking operations and improves user convenience. When consecutive identity verification failures reach the preset threshold, the system triggers local alerts and activates remote SMS alarms via 4G to remind administrators of potential illegal intrusion attempts.

The operating status is synchronously refreshed on the OLED screen in real time, allowing users to directly observe system running information and fault hints [9]. The three modules cooperate to realize local multimodal

unlocking, offline 4G alarm notification, administrator user management and real-time status feedback. The design fully meets the requirements of lightweight, low-cost and high-security household smart lock terminals, and it maintains stable operation under common indoor environmental interference with simple hardware layout and fewer peripheral components.

System hardware design

Hardware layer composition

The hardware platform is divided into the perception layer, control layer, actuation layer, human-machine interaction layer and communication layer. The perception layer includes a matrix keypad, ZW101 fingerprint module and RC522 RFID module for identity information collection. The ESP32-S3 serves as the core of the control layer and executes logic judgment and task scheduling. The actuation layer comprises a ULN2003 driver and a 28BYJ-48 stepper motor to realize physical locking and unlocking. The SSD1306 OLED screen undertakes human-machine interaction, and the SIM7600 4G module transmits remote alarm messages. The AMS1117-3.3 voltage regulator converts the input 5 V supply into a stable 3.3 V supply for the MCU and peripherals.

Main control minimum system circuit

The ESP32-S3 minimum system contains an oscillator circuit, reset circuit, power filter capacitor circuit and download-debug serial port, forming the core hardware foundation for the whole smart lock control unit. All general-purpose input/output (GPIO) pins are led out to pin headers for peripheral expansion, which facilitates convenient connection with external functional modules such as fingerprint sensors, matrix keypads and RFID readers during hardware assembly and testing.

The USB interface supports firmware downloading and online debugging, enabling developers to quickly update program codes and troubleshoot runtime faults. Moreover, the on-chip hardware encryption module of ESP32-S3 is enabled to encrypt locally stored passwords, fingerprint templates and RFID whitelist data to prevent unauthorized access and illegal data dumping, further reinforcing the confidentiality of sensitive identity information inside the embedded access control device.

Identity verification module circuit

The ZW101 fingerprint module communicates via a universal asynchronous receiver or transmitter (UART)

interface. Its TX and RX pins are connected to GPIO15 and GPIO7 of ESP32-S3, respectively. The interrupt request (IRQ) interrupt pin is connected to GPIO16 for wake-up control. The module is powered by a 5 volts direct current (VDC) supply and can automatically detect the placement of fingers to trigger fingerprint collection and feature extraction.

The RC522 RFID module operates under a 3.3 V power supply. The serial peripheral interface (SPI) pins of the RC522 module include master in slave out (MISO), master out slave in (MOSI), serial clock (SCK), and serial data (SDA). These pins are connected to GPIO10, GPIO11, GPIO12 and GPIO13 of the main controller. Such wiring supports card UID reading and card management operations, such as user card registration and card deletion. A 3×4 matrix keypad is adopted for password input. Four row pins and three column pins occupy seven GPIO resources in total. The main controller scans key values through the row-column scanning algorithm with internal pull-up resistors enabled, which effectively reduces external component count and captures valid keystrokes while filtering unstable bounce signals.

Actuator and human-machine interface circuit

The ULN2003 driver chip receives control signals from four GPIO ports of ESP32-S3 and outputs amplified current to drive the 28BYJ-48 stepper motor. Forward rotation corresponds to unlocking, while reverse rotation corresponds to locking.

The 0.96-inch SSD1306 OLED screen communicates via the Inter-Integrated Circuit (I²C) bus. Its SDA and SCL lines are connected to GPIO4 and GPIO5, respectively. It displays standby prompts, unlocking results and alarm warnings.

4G communication and power supply circuit

The SIM7600 4G module interacts with ESP32-S3 through UART and is configured by AT commands. Its TX and RX pins are assigned to GPIO1 and GPIO2. The module requires a stable 5 V power input for SMS transmission.

The whole system is powered by an external 5 V/2 A DC adapter. The AMS1117-3.3 linear regulator converts 5 V to 3.3 V for the ESP32-S3, RC522 and OLED modules. Filter capacitors are installed at the power input terminals to suppress voltage fluctuations and electromagnetic interference.

All hardware schematics and PCB layouts are designed in JLC-EDA. Wider copper traces are adopted for power lines and ground planes. The traces of high-speed SPI signals are shortened to improve anti-interference performance. A design rule check (DRC) is conducted before PCB fabrication.

System software implementation

Modular firmware is developed based on the ESP-IDF environment, which provides abundant underlying driver libraries and component tools for embedded program development. Tasks are scheduled across the dual cores of ESP32-S3 by calling application programming interfaces (APIs) for task creation, so that different functional tasks can run concurrently without blocking each other.

Message queues are adopted for data exchange among sub-tasks to realize asynchronous data transmission and avoid data loss or conflict. The general workflow is as follows: system power-on and peripheral initialization → waiting for user identity credential input → identity verification → unlocking execution or failure counting → triggering alarms under abnormal conditions → returning to standby state. After entering the standby state, the system keeps monitoring external triggering signals continuously and waits for the next user operation, which guarantees the cyclic and stable running of the whole smart lock system.

Main program flow

After power-on reset, the system sequentially initializes GPIO, UART, SPI, I²C and other hardware peripherals, followed by initialization of the OLED display, fingerprint unit, RFID reader, 4G module and stepper motor driver. The OLED screen shows the standby welcome interface. Multiple FreeRTOS tasks are created, including an input detection task, fingerprint processing task and main logic task. Once user input is detected, the system performs identity matching.

If authentication succeeds, the stepper motor rotates by preset steps to unlock the door. After a delay, the motor reverses to automatically lock the door. Each failed verification increments the failure counter. When the counter reaches four, the system temporarily locks local operations for 60 seconds, invokes the 4G SMS alarm function and outputs prompt messages on the OLED screen. Administrator mode supports adding and deleting fingerprint templates and RFID card entries, as well as modifying access passwords. The main program flow chart is shown in Figure 2.

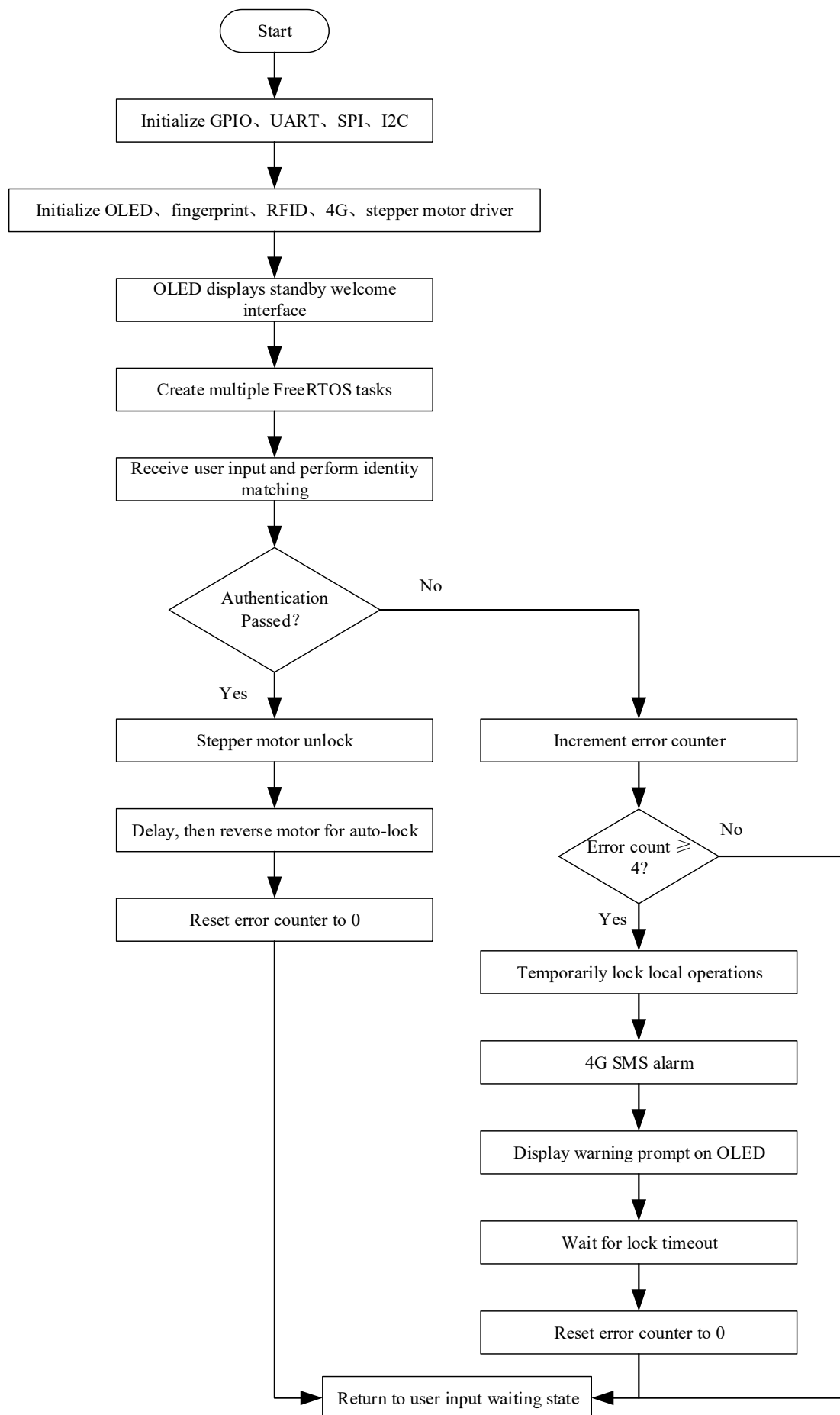


Figure 2. Main program flow chart.

Multimodal unlocking subprograms**(1) Fingerprint unlocking subprogram**

After UART initialization, the system sends configuration commands to the ZW101 module. When a finger touches the sensor, the module captures fingerprint images, performs preprocessing and feature extraction, and compares the extracted features with the

local template library. If the matching score exceeds the threshold, an unlocking command is sent to the main controller; otherwise, the failure counter increases. The administrator can start the enrollment process to collect two fingerprint samples and store the generated template into the on-chip Flash memory. The flow chart of the fingerprint recognition subprogram is shown in Figure 3.



Figure 3. Flow chart of fingerprint recognition subprogram.

(2) RFID card swiping unlocking subprogram

The software initializes the RC522 chip and activates its antenna, then continuously polls for nearby RFID cards. When an M1 card enters the 1-5 cm reading range, the system reads the card UID via SPI and compares it with the pre-stored authorized whitelist.

Unlocking is triggered upon a match; otherwise, a failure prompt is returned to users. Card registration and deletion operations can be executed under administrator privileges.

The flow chart of the RFID card swiping subprogram is shown in Figure 4.

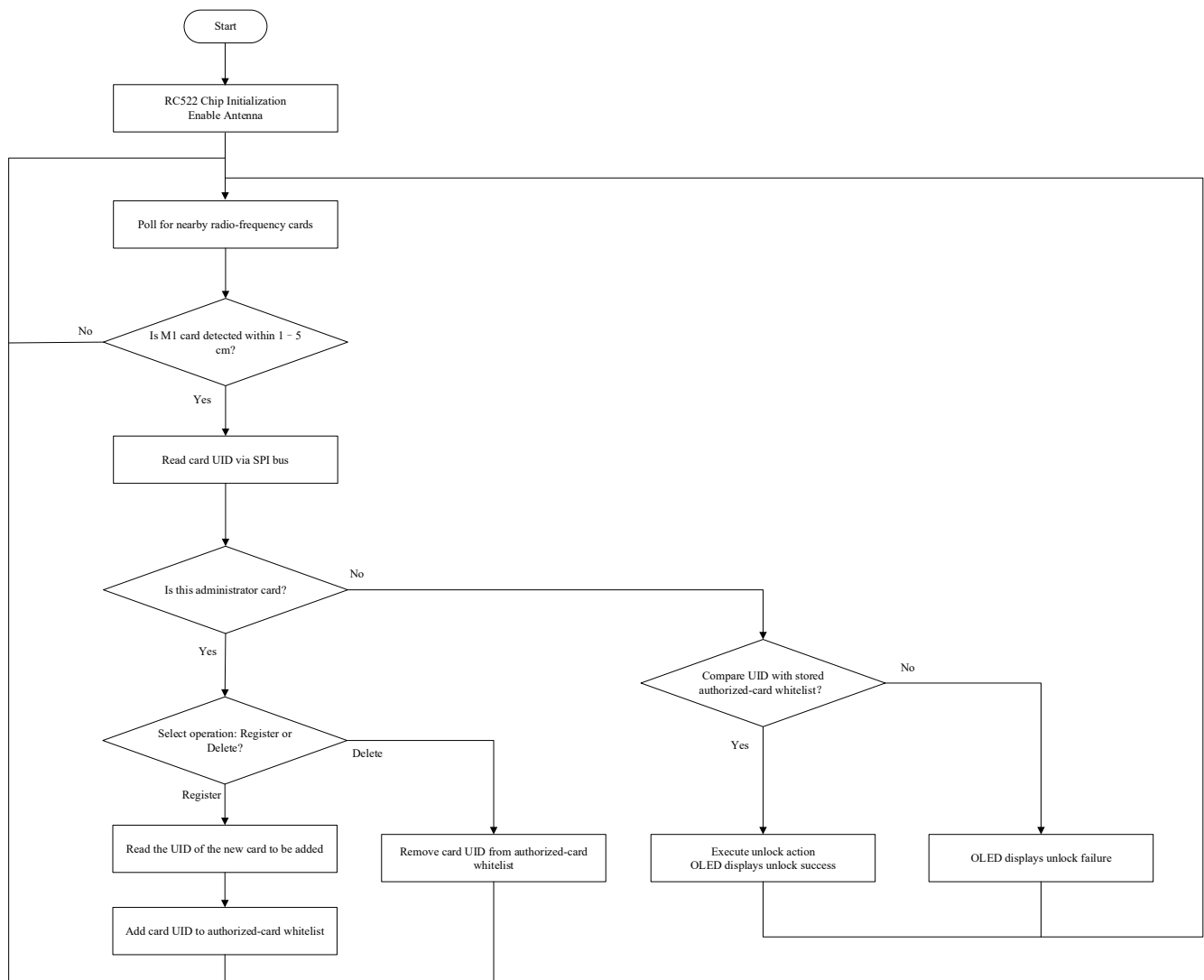


Figure 4. Flow chart of RFID card swiping unlocking subprogram.

(3) Keypad password unlocking subprogram

A row-column scanning algorithm detects keypad press events, and software debouncing is applied to input signals to filter transient jitter caused by mechanical bounce of physical keys. Users input a 6-digit access password. Input characters are displayed as asterisks on the OLED screen for privacy, preventing bystanders from peeping and capturing plaintext passwords during entry. Pressing the confirmation key submits the password for comparison with the reference value stored in Flash.

Wrong entries increment the failure counter, and repeated failed attempts will activate the system security protection mechanism. The system will temporarily limit further password trials once the preset threshold is reached, and the real-time status can be checked directly on the OLED display screen.

Password modification is available after administrator authentication, and the updated password will be written into non-volatile Flash storage for long-term preservation after verification. The flow chart of the keypad password subprogram is shown in Figure 5.

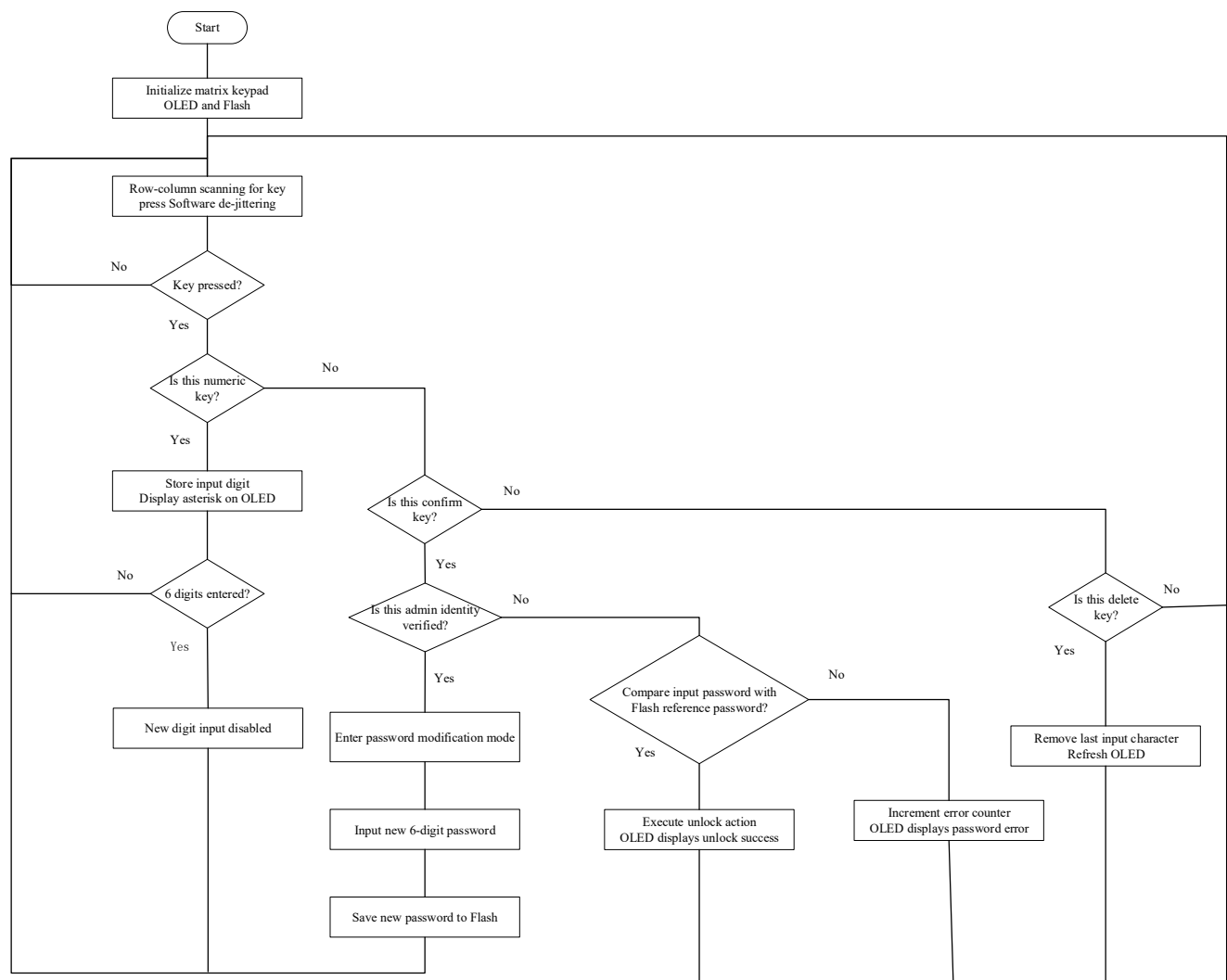


Figure 5. Flow chart of keypad password unlocking subprogram.

(4) Stepper motor driving program

An eight-step excitation sequence (A-AB-B-BC-C-CD-D-DA) is adopted for 28BYJ-48 motor control. The function “stepper-move-steps” defines rotation direction and total step count. For door unlocking, the motor rotates forward by 512 steps (approximately 90°). After a 3 s waiting interval, it rotates reversely by the same number of steps for automatic locking. Acceleration and deceleration control are introduced to reduce the risk of step loss and operating noise [10].

(5) 4G remote alarm program

The SIM7600 module is initialized through the UART driver. A set of AT commands are used to configure the baud rate, SMS text mode and service parameters. Once four consecutive invalid unlocking attempts are detected, the software assembles alarm text describing abnormal access events and sends AT commands to transmit SMS messages to pre-stored administrator phone numbers. A retransmission mechanism is implemented for transmission failures to improve message delivery

reliability.

(6) OLED display program

Based on the I²C driver for the SSD1306 controller, display functions cover the standby interface, password input interface, fingerprint management interface and alarm prompt interface. A double buffering strategy is used to eliminate screen flickering. System status, success and failure notifications and warning messages are refreshed in real time in response to system events.

System test and verification

A physical prototype is built for joint hardware and software debugging. Module-level unit tests and overall system tests are carried out to verify functional integrity, response speed and security performance.

Hardware test

Hardware testing evaluates power stability, peripheral communication reliability and actuator performance. Test items include voltage measurement of each power rail, connectivity verification of serial and bus interfaces,

OLED display quality, stepper motor positioning accuracy and SIM card detection of the SIM7600 module. Defects such as cold joints and signal interference are eliminated during debugging. All hardware modules operate stably.

Functional module test

(1) Fingerprint unlocking test

Hundreds of valid and invalid fingerprint samples are tested. Stained and dry fingerprints are used to evaluate system fault tolerance. Test cases include normal unlocking, rejection of unauthorized fingerprints and alarm triggering after repeated failures. Experimental results show that the fingerprint recognition accuracy exceeds 97%, with an average recognition time less than 1 s. Consecutive invalid fingerprint attempts activate the alarm logic.

(2) RFID unlocking test

Authorized and unauthorized IC cards are tested repeatedly. Test contents include unlocking with valid cards, rejection of unregistered cards, reading range limitation and identification of damaged cards. Valid

cards within the 1 to 5 cm detectable range trigger unlocking within 0.5 s. Removing a card UID from the whitelist revokes its access permission.

(3) Password unlocking test

Tests cover correct password input, wrong password entry, lockout and alarm triggered by four consecutive incorrect attempts, and administrator password modification. Valid password input completes unlocking within 1 s. Four successive wrong passwords trigger temporary local lockout and alarm events. Modified password data can be stored persistently.

(4) 4G offline alarm test

Brute-force attack scenarios are simulated by continuously submitting invalid authentication attempts under Wi-Fi-free conditions. The OLED screen displays the “illegal intrusion” alert, and alarm SMS messages are delivered to target mobile phones via the 4G cellular network. The SMS delivery success rate remains high, and message latency is controlled within 30 s.

(5) Comprehensive test results

The overall test results are summarized in Table 1.

Table 1. Summary of system comprehensive test results.

Test item	Performance index	Test result	Defect and optimization suggestion
Password unlocking	Response ≤ 1 s, abnormal handling effective	Passed	No obvious defect
Fingerprint identification	Accuracy $\geq 97\%$, response ≤ 1 s	Passed	Dry fingerprints occasionally cause minor recognition delay; optimize fingerprint acquisition sensitivity
RFID card unlocking	Response ≤ 0.5 s, effective reading distance 1-5 cm	Passed	No obvious defect
Stepper motor operation	Stable locking and unlocking actions	Passed	No obvious defect
4G alarm under offline environment	SMS delay ≤ 30 s	Passed	Individual test cases show minor delay; optimize AT command sending timing sequence

The prototype supports three local unlocking modes and 4G remote alarms even when Wi-Fi is unavailable. The average overall system response time is approximately 1.8 s, and the brute-force attack prevention mechanism works normally.

The system can run independently without Wi-Fi and satisfies household security requirements. Minor issues such as occasional recognition delay with dry fingerprints can be resolved by optimizing firmware parameters.

Conclusion

This paper designs and implements a multimodal smart door lock control system based on the ESP32-S3 MCU. Three identity authentication approaches are integrated: keypad password verification, ZW101 fingerprint recognition and RC522 RFID card authentication. The SIM7600 4G communication module addresses the limitation that traditional smart locks heavily depend on Wi-Fi for alarm transmission. The ULN2003-driven 28BYJ-48 stepper motor realizes mechanical lock

actuation, and the SSD1306 OLED screen provides intuitive human-machine interaction. Hardware schematic diagrams and PCB layouts are completed in JLC-EDA, and modular firmware is developed under the ESP-IDF framework.

Experimental verification demonstrates that the system supports stable local multimodal unlocking and offline 4G security alarms. Local alerts and remote SMS notifications are triggered upon continuous illegal authentication attempts. Adopting low-cost hardware components, this design accommodates operation habits of the elderly and children and can be applied in residential smart home scenarios.

For future research, infrared human detection can be added to implement anti-pry alarms. Low-power sleep strategies will be optimized to extend battery standby time. In addition, more biometric authentication modes and lightweight local encryption algorithms can be introduced to further improve system security and intelligence.

Funding

This work was not supported by any funds.

Acknowledgements

The author would like to show sincere thanks to those technicians who have contributed to this research.

Conflicts of Interest

The author declares no conflict of interest.

References

- [1] Van, A. V. (2026) Design and implementation of a smart door lock system based on Arduino mega 2560. *Thu Dau Mot University Journal of Science*, 8(2), 279-290.
- [2] Sonamoni, J. S., Sikdar, R., Akib, A. A. S., Islam, M. S., Sourov, S., Al Ahasan, M. A., Mridha, M. F. (2024) IoT-based smart remote door lock and monitoring system using an Android application. *Engineering Proceedings*, 76(1), 85.
- [3] Adiono, T., Fuada, S., Anindya, S. F., Purwanda, I. G., Fathany, M. Y. (2019) IoT-enabled door lock system. *International Journal of Advanced Computer Science and Applications*, 10(5), 445-449.
- [4] Harun, N. B., Zainal, M. S. B. (2023) Development of face recognition smart door lock system using ESP32-CAM and telegram application as media control and monitoring. *Progress in Engineering Application and Technology*, 4(2), 035-048.
- [5] Yuniarto, A. H. P., Lestiyanti, Y., Asrori, M. F., Laela, N., Nurcholis, A. (2023) Perancangan smart door lock system dengan multi sensor untuk sistem keamanan rumah. *Techné: Jurnal Ilmiah Elektroteknika*, 22(2), 333-342.
- [6] Zainuddin, A. A., Abd Rahman, A. D., Nor, R. M., Hussin, A. A. A., Mohd, N. N. M. S. N., Shamsudin, A. U., Sapuan, M. S. (2024) Innovative IoT smart lock system: Enhancing security with fingerprint and RFID technology. *Malaysian Journal of Science and Advanced Technology*, 360-365.
- [7] Bhushan, A., Misra, P. (2025) Unlocking the potential: multimodal AI in biotechnology and digital medicine - economic impact and ethical challenges. *NPJ Digital Medicine*, 8(1), 619.
- [8] Kijphitayarit, P., Poochaya, S. (2026) A data-driven multi-horizon framework for voltage alarm forecasting and persistence analysis using real-world operational 4G/5G RRU/AAU data. *Array*, 101312.
- [9] Poberezkin, E., Roozbahani, H., Alizadeh, M., Handroos, H. (2022) Development of a robust Wi-Fi/4G-based ROS communication platform for an assembly and repair mobile robot with reliable behavior under unstable network or connection failure. *Artificial Life and Robotics*, 27(4), 786-795.
- [10] Oun, A., Wince, K., Cheng, X. (2025) The role of artificial intelligence in boosting cybersecurity and trusted embedded systems performance: a systematic review on current and future trends. *IEEE Access*, 13, 55258-55276.