

Design and Implementation of the Intelligent Door Lock System based on STM32

Yanru Hu^{1,2,*}

¹ School of Physics and Electronic Information Engineering, Ningxia Normal University, Guyuan, Ningxia 756000, China

² Laboratory of Solid Microstructure and Function, Ningxia Normal University, Guyuan 756000, Ningxia, China

*Corresponding author email: yixing_166@qq.com

Abstract

With the continuous advancement of science and technology and the steady improvement of living standards, our daily lives have become increasingly intelligent, with smart home systems gaining widespread adoption. As a crucial component of smart homes, smart door locks meet the growing demand for home security, convenience, and intelligent functionality, gradually replacing outdated traditional mechanical locks. This paper presents a smart door lock system designed with an STM32 microcontroller as the main control unit. Through integrated hardware and software design, the system enables password verification, fingerprint recognition, and RFID identification for unlocking operations, while utilizing WIFI wireless communication technology for remote control. Equipped with a camera, the system also supports remote monitoring of the door lock. Tests demonstrate that this smart door lock offers advantages such as user-friendly operation, secure stability, and comprehensive functionality, effectively meeting users' needs for smart door locks and enhancing the intelligent experience of home living.

Keywords

STM32, Smart, Encryption, Fingerprint, RFID, WIFI, Security.

1. Introduction

With the rapid advancement of IoT technology, smart locks have become an increasingly popular security solution in modern society [1]. Traditional mechanical locks suffer from vulnerabilities such as easy prying, key loss, portability issues, and lack of remote control. To address these challenges, smart locks were developed. By leveraging computer technology, cryptography, and communication systems, they deliver efficient, intelligent, and secure features with diverse unlocking methods, making them a vital component of modern security systems [2-3].

The intelligent door lock system leverages the STM32F103C8T6 chip with ARM Cortex-M3 core, featuring high performance, low power consumption, and easy development, to deliver a more intelligent and convenient unlocking solution [4]. Additionally, it can integrate with other smart home devices to enable smarter home management, making it highly practical and valuable for real-world applications.

2. System Overall Design

This design implements an intelligent lock system based on STM32. The overall system architecture is shown in Fig. 1, with the following key functionalities:

- (1) Password-based lock unlocking: Users enter a password via a matrix keypad, and the system controls the relay to simulate the door lock's on/off state based on the password's correctness.
- (2) The fingerprint-based lock unlocking system utilizes the AS608 fingerprint recognition module to capture and verify fingerprints. By comparing the input fingerprint with the system's fingerprint database, it determines whether to open or close the lock [5].
- (3) Card-swiping lock activation: The system uses an RFID reader to scan the card, then controls the relay module to simulate the door lock's operation.
- (4) Remote monitoring: When users are away from home, the WIFI camera module allows remote monitoring of the door lock and visitor status, with the ability to control the lock remotely via a mobile app.
- (5) The OLED screen displays the door lock status and alarm notifications.

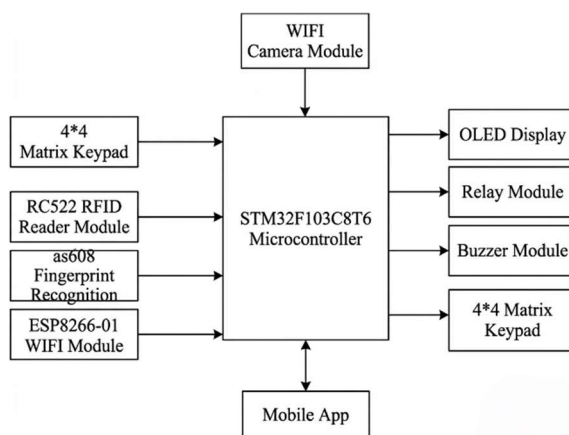


Fig. 1 Overall block diagram of the system

3. System Software Design

3.1. Digital Password Lock

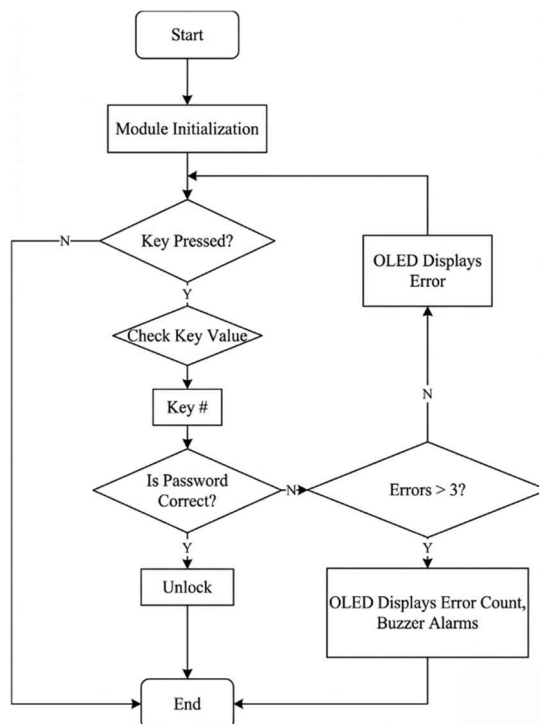


Fig. 2 Digital Password Lock Unlocking Process

The keyboard-based numeric password unlocking process is illustrated in Fig. 2 to verify user authentication. The system initiates by initializing the module, then waits for a key input command. It verifies the received key value and unlocks the device if the password matches. If the password is entered incorrectly three times, the system triggers a buzzer alarm and displays the alert on the OLED screen.

3.2. Fingerprint Recognition

Fingerprint recognition is a novel biomarker identification technology, currently the most widely adopted identification method. It is user-friendly and boasts an exceptionally high recognition rate. Having reached relative maturity, this technology has been extensively applied across various fields. Its internal working principle is as follows [6]:

(1) The fingerprint acquisition principle refers to the process of displaying fingerprint information through fingerprint sensing technology and converting the fingerprint pattern into a digital representation.

(2) Fingerprint feature extraction involves processing fingerprint images to identify key characteristics such as details, orientation, and shape. These features can be extracted through methods like filtering, enhancement, and refinement. Commonly used algorithms include Minutiae-based and Ridge-based approaches [7].

(3) Fingerprint matching refers to the process of comparing extracted fingerprint features against a pre-existing database to determine a match. Typically employing pattern recognition technology, the algorithm calculates similarity between fingerprint features. If the similarity reaches a predefined threshold, the match is deemed successful [8].

The communication protocol between the AS608 fingerprint module and the STM32 microcontroller works as follows: The AS608 first receives a data frame command from the MCU and executes the corresponding operation. Upon completion, the module sends a response data frame containing an acknowledgment code and any return parameters. During the execution of the command, the module does not automatically respond to additional commands from the host computer. Therefore, the MCU must wait for the module's response data frame to confirm the command's execution status.

The AS608 fingerprint module communicates with the STM32 microcontroller using a data frame format with one stop bit, no parity bit, and little-endian mode (high byte first, low byte last), at a baud rate of 9600.

The data frame format is analyzed as follows [8]:

The frame header consists of a fixed 2-byte identifier 0XEF01 and a 4-byte address field, with the default chip address being 0Xffffff.

The identifier has 1 byte, with the following values:

01=Command Package

02=Data packets, and some packets are still pending

08=Last data packet

Packet length: The total length of the packet content plus the checksum (excluding the packet length itself), where the checksum is the arithmetic sum of the packet identifier, packet length, and packet content. The command of the fingerprint module is shown in Table 1:

Table 1. Fingerprint Module Command Function Table

order number	code	function declaration	type	order number	code	function declaration
1	0x13	Verify password	Fingerprint processing	13	0x08	Upload features
2	0x12	Set password		14	0x09	Download features
3	0x15	Set address		15	0x06	Storage template
4	0x0e	Set system parameters		16	0x07	Download template
5	0x0f	Read system parameters		17	0x0c	Delete template
6	0x1f	Read fingerprint template index table		18	0x0d	Clear fingerprint database
7	0x1d	Number of fingerprint templates		19	0x03	compare features
8	0x01	Fingerprint image		20	0x04	Search fingerprint
9	0x0a	Upload image	Other categories	21	0x14	sampling random number
10	0x0b	Download image		22	0x18	Write in Notepad
11	0x02	Image feature transformation		23	0x19	Notebook
12	0x05	feature synthesis template				

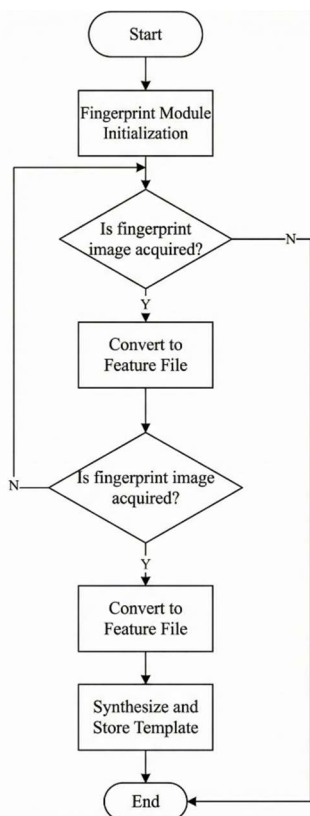


Fig. 3 Fingerprint template acquisition and storage process

Fingerprint data entry involves converting fingerprints into templates stored in a database. The process begins by converting an object image containing fingerprints into a feature data file, which is then stored in a feature data buffer. Subsequently, the feature data file is synthesized into a fingerprint template and stored in the fingerprint database [9]. The AS608 fingerprint module contains an internal FLASH storage area designated for protecting and storing fingerprint templates, also referred to as the fingerprint library. The workflow diagram for fingerprint template collection and storage is illustrated in Fig. 3.

Fingerprint recognition involves the user inputting their fingerprint data through a sensor. The system then processes the image and compares it with the stored fingerprint templates in the database to verify the user's identity. If the match is successful, the device can be unlocked. The fingerprint matching process is illustrated in Fig. 4.

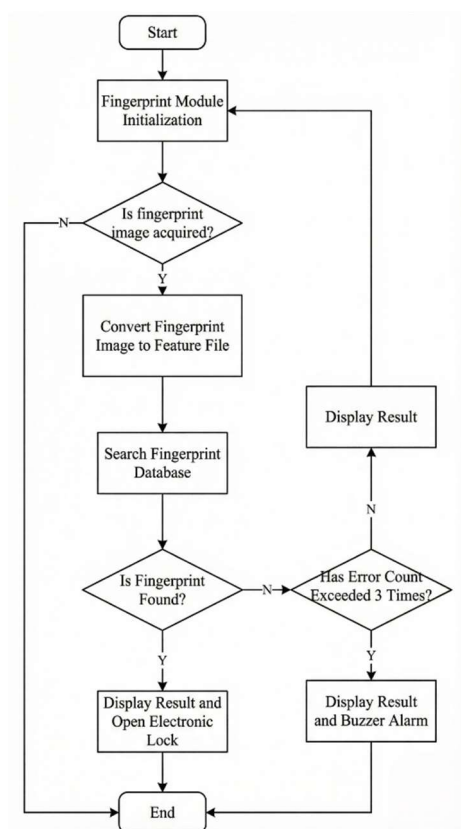


Fig. 4 Fingerprint Recognition Flow

3.3. Card Lock Unlock

The RC522 RFID identification driver module is a device designed for reading and writing RFID tags. As a radio frequency identification (RFID) technology-based device, its operational process is described as follows [10-11]:

- (1) The RC522 module first emits radio frequency signals at a specific frequency to its surroundings.
- (2) When an RFID card enters the radio frequency signal range, it receives signals transmitted by the RC522 RFID module.
- (3) Upon receiving the signal, the induction card decodes it into its unique identifier and transmits this code back to the RC522 module via radio frequency.
- (4) Upon receiving the unique identifier code transmitted by the induction card, it will be read and stored in the internal cache.

(5) The RC522 module compares the read identification code with the pre-stored codes in its internal memory. Upon successful match, it executes the corresponding operation, such as opening the door.

In summary, the RC522 RFID identification driver module operates by transmitting radio frequency signals, receiving the tag's response, decoding its unique identifier, and performing comparisons to ultimately achieve tag recognition and operation.

3.4. Relay Drive Module

The relay driver module controls the relay's on/off state to simulate unlocking operations. It receives external input signals, including switch signals and analog signals, then processes them through amplification, filtering, and logical operations to ensure signal stability and reliability.

Based on the processed input signal, the relay driver module controls the relay's on/off state to switch the circuit at the appropriate time [12-13]. Finally, the module outputs a signal that enables external devices to detect the relay's operational status.

3.5. OLED Display Driver Module

The display module controls the OLED screen to show the lock status and related information. Upon successful verification, the OLED displays "Door: Open"; if verification fails, it shows "Error" with the number of failed attempts.

3.6. WIFI Communication

The system utilizes WIFI technology to enable wireless remote monitoring via a mobile app, as illustrated in Fig. 5. The process requires the phone to connect to the WIFI module's IP address and port number, then send control characters to determine the door lock's open/closed status. During monitoring, the system connects to the camera's WIFI to achieve remote surveillance [14].

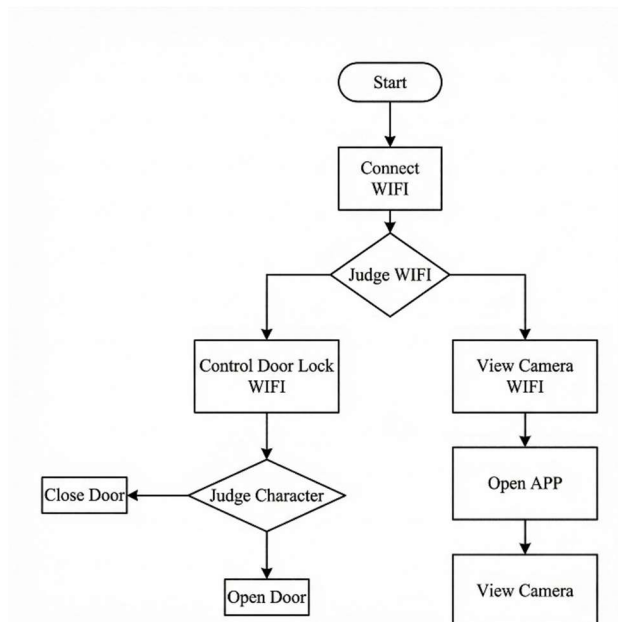


Fig. 5 WIFI Communication Flow

4. System Function Testing

The final hardware configuration is illustrated in Fig. 6. Components include: 1) the main control microcontroller STM32F103C8T6, 2) the ESP8266-01 WIFI module, 3) the AS608

fingerprint recognition module, 4) the RC522 RFID module for card-based lock unlocking, 5) the ATK-WIFI camera, 6) relays, 7) an OLED display, 8) a 4×4 matrix keyboard, and 9) an alarm buzzer..

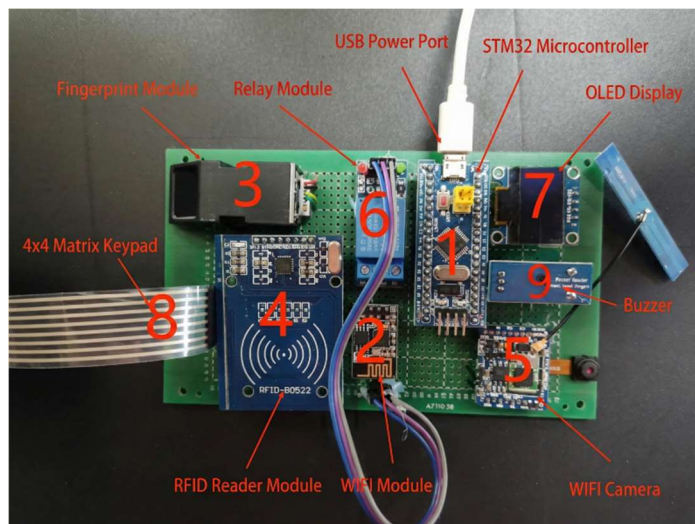


Fig. 6 Hardware Physical Image

4.1. Debugging of Digital Password Lock

Upon power-up, the OLED screen shows the door lock is locked, with the WIFI camera indicator blinking. Pressing the "#" key on the 4×4 matrix keypad and entering the correct four-digit password activates the microcontroller's blue light and the relay's green light, simulating a door open. The OLED then displays 'Door: Open' (Fig. 7).

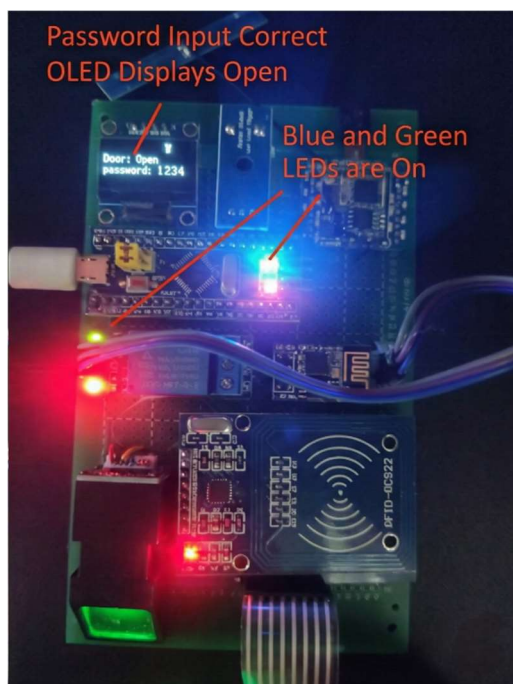


Fig. 7 Password unlock succeeded

If the password verification fails, the lock will not open. The OLED will display the error message and the number of attempts. If the error count exceeds three, the buzzer will sound an alarm, as shown in Fig. 8.



Fig. 8 Failed password unlock

4.2. Fingerprint Lock Debugging

Press the C key on the keyboard to display "Zhiwen Mode" on the screen.

When fingerprint recognition fails more than three times, the buzzer sounds as an alarm. If the fingerprint is successfully recognized, the relay activates, the microcontroller's blue light turns on, and the relay's green light turns on as an analog output, displaying 'Open'. The fingerprint lock is unlocked successfully, as shown in Fig. 9.

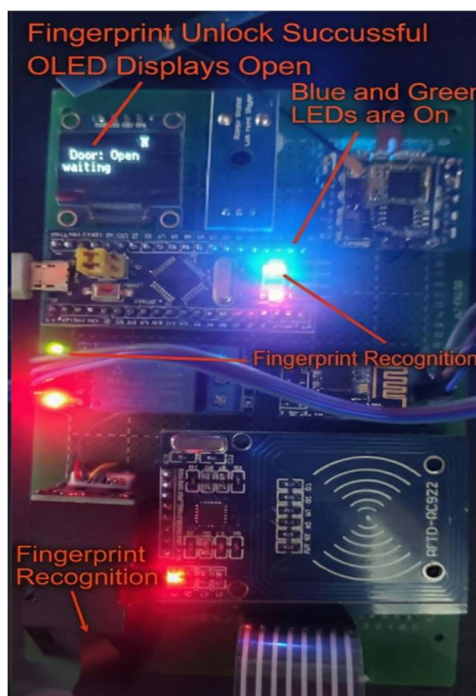


Fig. 9 Fingerprint lock opened successfully

4.3. RFID Lock Debugging

Select the access card unlocking mode by placing the RFID access card on the RC522 module. When the system detects the card, the OLED displays 'Card mode'. Upon successful card swiping, the microcontroller's blue light and the relay's green light illuminate as an analog signal, while the OLED shows 'Open' as shown in Fig. 10.

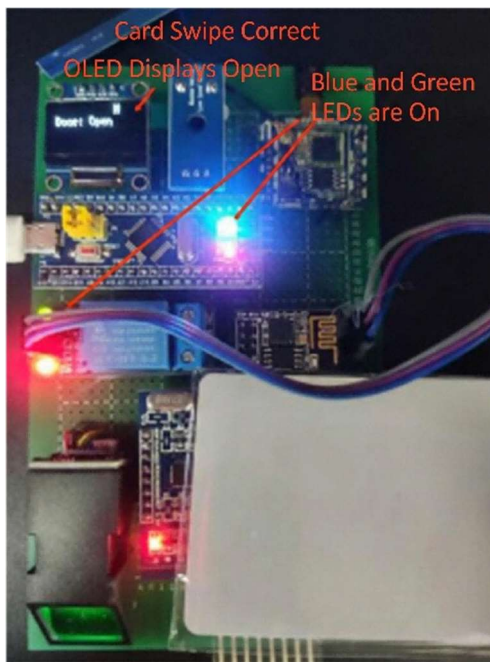


Fig. 10 Card swiped successfully

The card swiping failed, with the OLED displaying 'warning' and error counts as shown in Fig. 11.

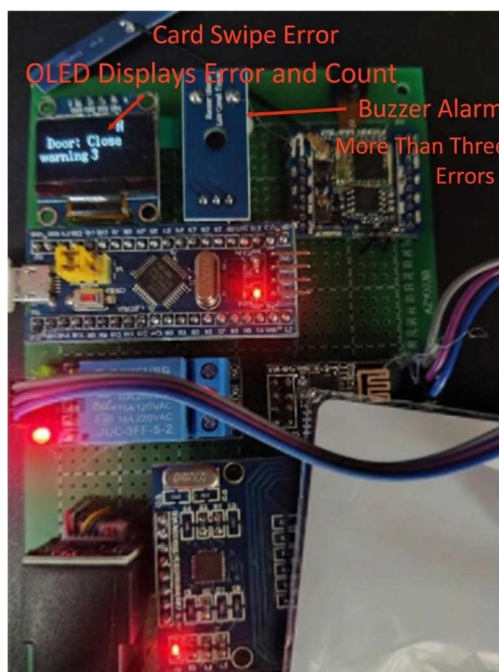


Fig. 11 Card swipe failed

4.4. Remote Monitoring

Users can remotely control the system by connecting to the corresponding WIFI. Based on the door monitoring data transmitted by the WIFI camera, they can verify visitors and perform remote lock operations via the mobile app, as shown in Fig. 12.

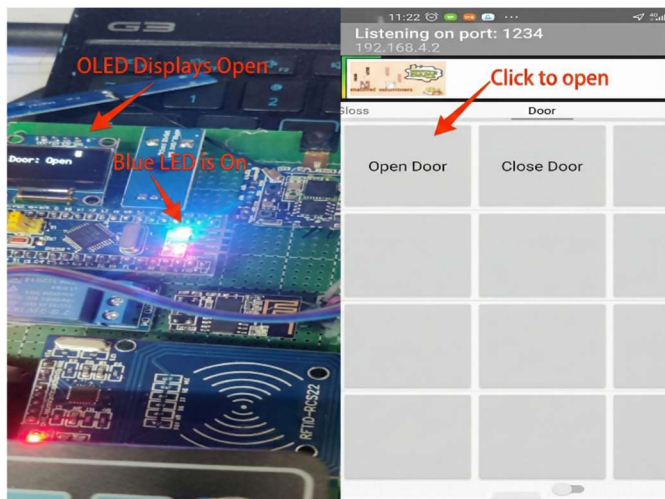


Fig. 12 Remote Control Door Lock

4.5. Administrator Module Debugging

The administrator module features functions including selecting lock unlock types, modifying passwords, adding fingerprints, and deleting fingerprints. Pressing the A key adds a fingerprint, with the OLED display showing 'add finger' and 'add ok' upon successful addition, as shown in Fig. 13.

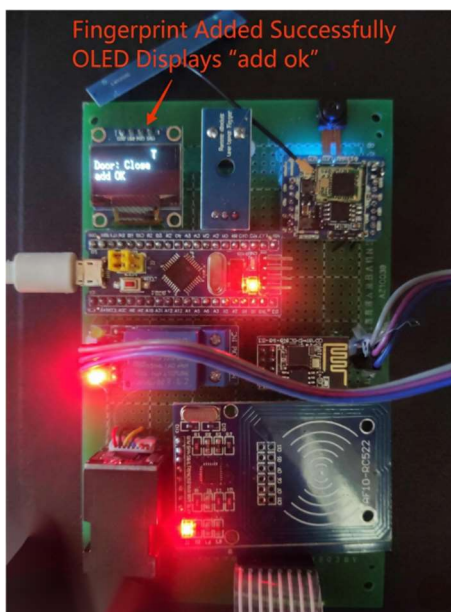


Fig. 13 Fingerprint added successfully

5. Summary

The STM32-based smart lock system enables users to remotely control the door lock via a mobile app, offering convenience and efficiency. The system supports multiple unlocking methods including digital buttons, fingerprint recognition, and RFID cards, eliminating the need for traditional keys and preventing risks of key loss or theft. Additionally, the smart lock system utilizes WIFI wireless technology for remote monitoring, allowing real-time tracking of visitors at the entrance to ensure user safety.

References

- [1] Huang Shiqi, Lin Weifeng, Yang Ying. Intelligent lock control system based on STM32 microcontroller [J]. Yangtze River Information and Communication, 2021,34(05):98-101+108.
- [2] Zhong Zhaohui. Design of a ZigBee-based wireless smart lock system [D]. Hangzhou Dianzi University, 2014.
- [3] Zhang Yun, Gao Peng. Design of Intelligent Door Lock Based on Cryptographic Recognition [J]. Electronic Design Engineering, 2018,26(3):52-54.
- [4] Wang Xiaoyan. Principles and Hardware Circuit Design of STM32 Microcontroller [J]. Southern Agricultural Machinery, 2020,51(14):163-164.
- [5] Xiao Lin Xiao, Rui Wang, Ruisong Li. Design of Intelligent Door Lock Based on Fingerprint Recognition Technology [J]. Computer Knowledge and Technology, 2019,15(29):250-251.
- [6] Zhu Xiaoqin. Design of a fingerprint recognition system for electronic reading in libraries based on microcontroller [J]. Automation and Instrumentation, 2021(11):111-115.
- [7] Wan Linfeng. A method for using an intelligent fingerprint lock based on STM32 and its intelligent fingerprint lock module. CN202211304725.0[2024-01-23].
- [8] Wang Yue. Design of a fingerprint password lock based on STC89C52 [J]. Chinese Journal of Science and Technology (Full-text Edition), Engineering Technology, 2023(4):4.
- [9] Tang Rui, Yu Juan. Design of a fingerprint password lock system based on a microcontroller [J]. Science and Technology Innovation, 2016,000(012):12-13. DOI: 10.15913/j.cnki.kjycx.2016.12.012.
- [10] Wang Zhiqiang, Wang Tingting, Wang Zuhua. Design of Intelligent Door Lock Based on RFID Identification [J]. Computer Knowledge and Technology, 2018,14(28):191-192.
- [11] Chen Ziming, Li Cheng, Cheng Huaming, et al. Design and Implementation of an Intelligent Security Interlock System Based on RFID Technology [J]. Computer Measurement and Control, 2020(011):028.
- [12] Lü Jian. Research and Implementation of Embedded Intelligent Lock Control System [D]. Tianjin: Tianjin University of Science and Technology, 2019.
- [13] Wan Lijuan, Lin Wei, Xu Yuan, Xie Rui, Shao Wenjun, Han Mingyang, Wang Lijun. Design and Implementation of a Triple Authentication Access Control System Based on STM32 Microcontroller [J]. Journal of Pingxiang University, 2022,39(06):46-49+61.
- [14] Liu Zhongbo. Application of intelligent video surveillance and analysis technology in integrated security systems [J]. Wireless Interconnection Technology, 2023,20(04):13-15..