



廣東科技學院
GUANGDONG UNIVERSITY OF SCIENCE & TECHNOLOGY

葉選平

毕业设计

题目：基于视觉识别的智能门禁安全监控系统的设计与实现


姓 名： 吴诗聪
学 号： 2023303030084
层 次： 本科
二级学院： 计算机学院
专 业： 物联网工程
班 级： 23 物联网升本 2 班
指导教师： 柳子来、李明轩

2025 年 5 月

广东科技学院教务处 制

毕业论文（设计）独创性声明

本人郑重承诺：所呈交的毕业论文（设计）是本人在指导教师的指导下，独立研究所取得的成果。本人在撰写毕业论文（设计）的过程中严格遵守学术规范，尽我所知，除致谢部分外凡文中引用的他人发表或未发表的学术成果均已注明出处，除引用部分外文中所有的数据及其他引证材料均真实客观。如有学术失范行为，本人愿意承担由此造成的一切后果。

论文（设计）作者签名：

日期： 2025 年 5 月 8 日

摘要 本论文聚焦于智能门禁系统的设计与实现，旨在解决传统门禁系统在安全性和便利性方面的不足。本研究设计并实现了基于视觉识别的智能门禁安全监控系统，该系统选用 ESP32-S3-DevKitC-12 作为主控芯片，结合 K210 视觉识别模块、音频报警模块、NFC 模块等多个功能模块。通过 K210 进行实时视频流处理和人脸识别，快速识别人员身份。一旦检测到未经授权的人员，音频报警模块会立即启动，发出警报。通讯上利用 ESP32-S3-DevKitC-12 的 Wi-Fi 模块实现远程监控和数据传输，借助 Micro SD 卡实现数据存储。用户可通过简洁直观的交互界面进行操作，支持 NFC 感应解锁、手机 Wi-Fi 无接触开锁。该系统主要适用于各类住宅、办公场所、学校、商业园区等对门禁安全和便捷性要求较高的场景。实验证明，本系统成功实现远程监控门禁状态、智能化身份识别与管理，显著提升门禁系统的安全性和便捷性。

关键词 视觉识别；智能门禁；安全监控

Abstract This thesis focuses on the design and implementation of an intelligent access control system, aiming to address the deficiencies of traditional access control systems in terms of security and convenience. In this research, an intelligent access control security monitoring system based on visual recognition has been designed and implemented. This system selects the ESP32-S3-DevKitC-12 as the main control chip and combines multiple functional modules such as the K210 visual recognition module, the audio alarm module, and the NFC module. The K210 is used for real-time video stream processing and face recognition to quickly identify individuals. Once an unauthorized person is detected, the audio alarm module will be activated immediately and sound an alarm. In terms of communication, the Wi-Fi modules of the ESP32-S3-DevKitC-12 are utilized to achieve remote monitoring and data transmission, and data storage is realized with the help of a Micro SD card. Users can operate through a simple and intuitive interactive interface, and the system supports NFC sensing unlocking and contactless unlocking by pairing with a mobile phone via Wi-Fi. This system is mainly applicable to various scenarios with high requirements for access control security and convenience, such as residential buildings, office premises, schools, and commercial parks. Experiments have demonstrated that this system has successfully achieved remote monitoring of the access control status, intelligent identity recognition, and management, significantly enhancing the security and convenience of the access control system.

Keywords Visual Recognition; Intelligent Access Control; Security Monitoring;

目 录

1 绪论	1
1.1 背景和意义	1
1.2 国内外研究现状	2
1.2.1 国内发展现状	2
1.2.2 国外发展现状	3
1.3 本文主要研究内容和论文结构	3
1.3.1 主要研究内容	3
1.3.2 论文结构	4
2 开发技术简介	6
2.1 PlatformIO 开发平台简介	6
2.2 C/C++ 语言简介	6
2.3 Wi-Fi 通信技术简介	6
2.4 OpenCV 库简介	6
2.5 微信小程序开发框架简介	7
2.6 本章小结	7
3 智能门禁系统总体设计分析	8
3.1 系统总体设计	8
3.2 系统功能模块简述	9
3.2.1 ESP32-S3-DevKitC-12 主控芯片	9
3.2.2 人脸识别模块	9
3.2.3 音频报警模块	10
3.2.4 NFC 模块	11
3.2.5 数据存储模块	11
3.2.6 Wi-Fi 模块	12
3.2.7 解除/启动报警模式	12
3.2.8 移动终端模块（微信小程序）	13
4 系统硬件设计	14
4.1 硬件整体设计	14
4.2 NFC 模块电路设计	14

4.3 音频报警模块电路设计	14
4.4 数据存储模块电路设计	15
4.5 Wi-Fi 模块（射频模块）电路设计	16
4.6 人脸识别模块	17
5 系统软件设计	18
5.1 系统软件总体设计	18
5.2 Wi-Fi 子程序软件设计	19
5.3 NFC 模块子程序软件设计	20
5.4 人脸识别模块子程序软件设计	22
5.5 存储模块子程序软件设计	24
5.6 微信小程序模块程序设计	26
6 系统功能的测试分析	27
6.1 系统测试	27
6.2 系统整体分析测试总结	32
7 总结与展望	33
7.1 系统总结	33
7.2 后期展望	33
参考文献	35
致谢	37

1 绪论

1.1 背景和意义

在科技飞速发展的当下，智能化浪潮席卷各个领域，传统门禁系统在安全性与便利性方面的短板愈发凸显，难以契合现代社会的多元需求。从安全性角度来看，传统门禁系统多依赖物理钥匙或卡片。物理钥匙存在易丢失、易复制的问题，一旦钥匙落入不法分子手中，便会直接威胁到场所的安全。而门禁卡也并非绝对安全，存在被窃取、盗用的风险，且部分门禁卡加密技术有限，容易被破解。同时，传统门禁系统对于人员身份的验证方式较为单一，难以应对复杂多变的安全威胁，在面对蓄意闯入等异常情况时，缺乏有效的预警和防范机制。在便利性方面，传统门禁在人流高峰时段，人工操作的签到、放行流程繁琐，导致通行效率低下，容易造成拥堵。对于大型企业、公共场所而言，大量人员的出入管理工作繁重，传统门禁无法实现自动化、智能化的管理，管理人员需耗费大量的时间和精力在日常门禁事务上，管理成本居高不下。随着视觉识别技术、人工智能算法、无线通信技术以及嵌入式系统等相关技术的蓬勃发展，为智能门禁系统的创新升级提供了坚实的技术支撑。视觉识别技术凭借其高精度、非接触式的特点，能够快速准确地识别人员身份，极大地提升了门禁系统的安全性和便利性。深度学习算法在图像处理和模式识别领域取得了突破性进展，使得人脸识别、行为分析等功能更加精准高效。无线通信技术的不断迭代，如 Wi-Fi、蓝牙、5G 等，实现了设备之间稳定高速的数据传输，为门禁系统的远程监控和管理提供了可能。嵌入式系统的性能日益强大，体积不断缩小，功耗逐渐降低，能够将各种复杂的功能集成在小型设备中，满足智能门禁系统对硬件设备的高要求。这些技术的融合发展，为智能门禁系统的设计与实现开辟了新的路径，使其具备了更强大的功能和更广阔的应用前景。

本研究旨在打造一个基于视觉识别的智能门禁安全监控系统，该系统具有多方面的意义。在提升公共安全方面，系统通过高精度的人脸识别技术，能够准确判断进出人员的身份，有效阻止未经授权的人员进入，降低安全风险。同时，实时行为监测功能可以及时发现异常行为，如徘徊、长时间逗留、暴力闯入等，并迅速发出警报，通知相关人员进行处理，为公共场所和企业的安全提供全方位的保障。对于提高管理效率而言，智能门禁系统实现了身份验证和门禁控制的自动化，无需

人工干预，大大缩短了人员通行时间，提高了门禁通行效率。管理人员可以通过系统后台实时查看人员出入记录，方便进行人员管理和数据分析，为管理决策提供有力支持。此外，系统的远程管理功能使得管理人员可以随时随地对门禁系统进行操作和设置，进一步提升了管理的便捷性和高效性。

该系统的成功研发和应用，还将对智能家居、智能办公等领域产生积极的推动作用。在智能家居领域，智能门禁系统作为家庭安全的第一道防线，与其他智能设备互联互通，实现家庭智能化管理，为用户提供更加安全、便捷、舒适的居住体验。在智能办公领域，智能门禁系统与办公自动化系统相结合，实现员工考勤管理、权限控制等功能的智能化，提高办公效率，优化办公环境。同时，本系统的设计理念和技术方案可以为其他智能监控系统的开发提供有益的参考和借鉴，促进整个智能监控行业的发展。

1.2 国内外研究现状

1.2.1 国内发展现状

在国内，众多科研团队和企业积极投身于智能门禁系统的研发。何鑫宇提出的基于 ARM 架构的智能家居监控系统，深入探讨了 Wi-Fi 技术和嵌入式系统在智能家居领域的应用^[1]，为智能门禁系统的硬件架构设计提供了参考思路。李昌奇等人设计的基于 Android 和 Wi-Fi 的智能家居监控系统，融合了嵌入式控制技术、无线网络和 Android 技术，实现了家居环境的实时监测、远程控制和语音播报功能^[2]，展示了智能门禁系统与智能家居其他功能模块的融合发展趋势。张敏和刘佑鑫结合压缩感知理论和时序自适应网络，成功解决了家庭监控视频中的隐私泄露问题，并提高了识别准确度，为智能门禁系统的隐私保护和识别性能优化提供了新的技术手段^[3]。

黄金亮利用 LoRa 技术实现了远程监控、数据加密、访问控制等功能，为用户带来了便捷、安全的家居管理体验^[4]，拓展了智能门禁系统的通信方式和应用场景。沧澜智能科技（昆山）有限公司开发的系统，通过智能识别分析模块集成对象检测、特征提取识别及行为分析功能，显著提升了系统的预警精度和判断能力^[5]，推动了智能门禁系统向智能化、精细化管理方向发展。郭顺超等人基于人脸识别技术设计并开发的小区门禁管理系统，采用 Python 语言和 Django 框架进行编程实现，后台数据管理采用 MySQL 数据库，借助百度 AI 提供的人脸识别接口完成业主人脸的检测与识别，为小区门禁管理提供了切实可行的解决方案，具有较高的实用性和推广

价值^[6]。张斌等人设计了一套非接触式手势识别门禁装置，该系统以 STM32 单片机为主控制器，通过手势识别系统实现手势与数字密码的转换，实现门禁锁开关^[7]。陆畅等人设计了一种智能门禁系统，利用 OpenCV 视觉库和树莓派硬件，通过人脸识别技术实现安全管理。系统通过灰度化、降维和特征值计算，对人脸信息进行处理，测试结果显示该系统具有人脸识别的高成功率^[8]。徐杰等人研究了 Adaboost 与 MTCNN 算法，构建了一个人脸识别门禁系统。该系统利用 STC89C51 单片机和 OpenCV 实现人脸检测与识别，测试表明系统具有较高的识别准确率和实时性^[9]。玄冉等人设计了一套人脸识别门禁系统，利用 MATLAB 进行图像处理和 PCA 算法分析，系统能够有效识别疑似人员，测试结果显示识别准确率达到 80%^[10]。王蒙蒙等人开发了一款智能门锁系统，采用机器视觉技术和人脸识别，解决了指纹锁和门禁卡的安全隐患。系统通过 LBP 算法优化人脸识别效率，测试结果表明识别准确率超过 99%^[11]。

1.2.2 国外发展现状

在国外，智能门禁系统的研究同样活跃。Smithetal.（2021 年）设计了一种基于视频分析的智能门禁系统，能够实时识别和记录入侵者的行为，为安全管理提供了有效的支持^[12]。而 Johnson（2022 年）则探讨了将人工智能与传统门禁系统结合的方法，提升了系统的智能化水平和实用性^[13]。Husni 等（2021）提出了一种基于 Visual Studio Code 的活动监测接口，该接口旨在监控环境状况以及人类活动，如垃圾投放。根据专利 CN220647443U，提出了一种智能家居安防装置，该装置通过滑道主体和可移动的监控装置组合，实现了对监控角度的灵活调整。

Sharad 等（2021）在其论文中强调，随着微型视频传感器和计算机视觉技术的发展，视觉物联网（Visual IoT, VIoT）正逐渐成为重要的研究方向^[14]。

近年来，Sabit（2025）对智能家居中的视频监控技术进行了深入探讨，强调了视频作为输入模态在非侵入性和信息丰富性方面的潜力。研究表明，基于视频的活动检测系统能够有效地识别家庭环境中的人类活动，提升居住安全性^[15]。Si、Hao 和 Jing（2022）提出了一种基于视觉密码学的认证和识别方法，旨在解决人类用户在不依赖可信计算设备的情况下进行认证的挑战^[16]。

1.3 本文主要研究内容和论文结构

1.3.1 主要研究内容

随着人们对安全与便捷生活的追求不断提升，传统门禁系统已难以满足现代社

会的需求。本研究以视觉识别技术为核心，致力于开发一套智能门禁安全监控系统，旨在提升门禁管理的安全性和效率，为各类场所提供可靠的安全保障。

本系统将综合运用多种技术，实现对人员身份的精准识别、行为的实时监测以及门禁的智能控制。系统选用 ESP32-S3-DevKitC-12 作为主控芯片，结合 K210 视觉识别模块，进行实时视频流处理和人脸识别，确保身份验证的高效性和准确性。通过 MAX98357 音频放大器模块和 3525 腔体-8 欧姆 2W/喇叭实现音频报警功能，及时对异常情况做出响应。集成 PN532-NFC 套件，方便用户进行报警状态的设置与解除，提升系统交互性。利用 MicroSD 卡 SPI 接口插座存储监控记录，保障数据的长期保存。借助 ESP32-S3-DevKitC-12 内置的 Wi-Fi 模块，将实时监控状态传输至用户手机，实现远程监控功能。同时，使用微信小程序开发移动终端模块，为用户提供便捷的操作界面，便于用户随时随地查看监控情况、接收报警信息并进行远程控制。

对于移动终端模块设计，注重功能完善与性能优化，减少不必要的操作步骤，提高响应速度和稳定性，确保系统在长时间无人值守的情况下依然能够稳定运行，满足实际应用需求，为用户带来良好的使用体验。

1.3.2 论文结构

根据以上的研究内容，论文分为七个章节，各章节具体安排如下：

第一章：绪论：阐述本课题的研究背景和意义。通过对国内外相关研究现状的分析，明确本研究的切入点和创新点。

第二章：开发技术介绍：对本文系统在实现过程中需要的主要技术进行详细介绍，为后续系统设计与实现提供技术支撑。

第三章：智能门禁安全监控系统的总体设计：对本系统的总体需求进行深入分析，如人脸识别、音频报警、NFC 交互、数据存储、远程监控、移动终端控制等。根据需求和功能设计，对系统各个模块进行详细说明，绘制系统总体架构图，展示系统各部分之间的关系和数据流向。

第四章：系统硬件设计：主要进行硬件部分的设计工作。首先绘制硬件系统的总体框架图，清晰呈现各个硬件模块之间的连接关系，说明硬件选型的依据和设计要点。

第五章：系统软件设计：完成系统各部分软件程序的设计和编写。详细介绍人脸识别算法的实现过程。阐述功能模块的软件设计思路和实现方法，展示各类子程

序模块的设计流程和实现效果。

第六章：系统功能的测试分析：对智能门禁安全监控系统的各个模块进行功能测试，验证其是否成功运行。总结系统存在的问题和不足之处，提出相应的改进措施。

第七章：总结与展望：对系统的整体功能和研究内容进行全面总结，评估系统的实际应用价值。同时，提出改进方向和未来的研究展望。探讨智能门禁安全监控系统在未来技术发展趋势下的发展方向，如与人工智能技术的深度融合、在更多场景中的应用拓展等，为后续研究提供参考。

2 开发技术简介

2.1 PlatformIO 开发平台简介

本项目选择了 PlatformIO 作为嵌入式系统的开发工具链，PlatformIO 是一个跨平台的代码构建工具和库管理工具，并且支持像 Arduino 和 MBED 这样的平台。他们可以跨 macOS、windows 和 linux 三个平台工作的工具链、调试器和开发平台，它支持超过 200 个的开发板和超过 15 种的开发平台以及 10 中开发框架，并以 C 语言为程序语言。其丰富的库资源极大缩短开发周期，多平台适配性让开发者无需担心系统差异。借助它能轻松管理项目依赖，高效编译代码，快速实现嵌入式系统开发目标。

2.2 C/C++ 语言简介

系统开发主要采用 C/C++ 语言。C 语言作为一种高效、灵活且面向过程的编程语言，在底层硬件驱动开发和系统性能优化方面发挥着关键作用。它能够直接操作硬件资源，对内存进行精细管理，这对于实现系统中各硬件模块的驱动程序至关重要，如控制 ESP32-S3-DevKitC-12 的 GPIO 口、配置各类传感器的工作模式等。C++ 在此基础上引入面向对象编程思想，通过类和继承等特性增强代码的可维护性和扩展性。两者结合，既能高效驱动硬件，又能构建复杂软件逻辑。

2.3 Wi-Fi 通信技术简介

Wi-Fi 技术在本系统中承担着关键的数据传输任务，实现了门禁设备与移动终端之间的远程通信。其通信过程主要包括设备的扫描、连接、认证以及数据传输等环节。在扫描阶段，设备会搜索周围的 Wi-Fi 热点；连接时，通过输入正确的密码进行身份认证；认证成功后，即可进行数据的双向传输。通过加密协议保障数据传输安全，防止信息泄露。先进的加密机制保障了数据在传输过程中的安全性，降低信息被窃取风险。快速的连接与稳定的数据传输，确保门禁设备与终端实时交互，提升系统响应速度。

2.4 OpenCV 库简介

OpenCV (Open Source Computer Vision Library) 是一个用于计算机视觉任务的开源库，在本系统的视觉识别模块开发中发挥着核心作用。在人脸识别功能实现过程中，OpenCV 库提供了多种人脸检测算法。并且，OpenCV 库具有良好的跨平台性，可在多种操作系统和硬件平台上使用，方便系统的开发和部署。丰富的算法

库可根据不同场景灵活选择，提高识别精度和效率。跨平台特性使得系统能在不同设备上稳定运行，降低开发和维护成本。

2.5 微信小程序开发框架简介

微信小程序是一种无需下载安装即可使用的应用程序，在本系统中作为移动终端的用户交互平台。微信小程序开发框架为开发者提供了一套完整的开发工具和环境，通过微信小程序开发框架，开发者可以方便地调用微信提供的各种原生接口，为用户提供便捷的使用体验。庞大的微信用户基础为系统带来广泛的用户覆盖，便捷的开发工具和丰富接口加速项目开发。无需下载的特性降低用户使用门槛，提升用户参与度和满意度。

2.6 本章小结

本章详细阐述了本项目所采用的核心开发技术。PlatformIO 开发平台凭借其跨平台特性、丰富的开发板与框架支持及强大的库管理能力，为嵌入式系统开发提供了高效、便捷的工具链，显著提升了开发效率，缩短了项目周期。C/C++ 语言的结合使用，使系统既能充分发挥 C 语言对硬件的直接操控优势，实现底层驱动开发与性能优化，又能借助 C++ 面向对象的特性增强代码的可维护性与扩展性，满足复杂功能需求。Wi-Fi 通信技术作为系统数据传输的桥梁，通过标准化的扫描、连接、认证流程及加密机制，保障了门禁设备与移动终端间安全、稳定、实时的数据交互。OpenCV 库则为视觉识别模块，尤其是人脸识别功能的实现提供了关键技术支撑，其丰富的算法资源与良好的跨平台性，确保系统在不同环境下均能实现高精度的图像识别与处理。微信小程序开发框架则依托微信庞大的用户生态，以便捷的原生接口调用能力与免安装特性，构建起用户友好的交互平台，有效降低了用户使用门槛，提升了系统的易用性与推广价值。这些技术相互协作、优势互补，共同为智能门禁系统的功能实现、性能优化与用户体验提升奠定了坚实基础，确保项目在技术层面的可行性与先进性。

3 智能门禁系统总体设计分析

3.1 系统总体设计

基于视觉识别的智能门禁安全监控系统总体框架设计融合了多种先进技术，构建了一个高效、安全的门禁管理体系，主要分为感知层、处理层、传输层和应用层。

感知层负责采集各类关键信息，主要由摄像头、K210 视觉识别模块、NFC 模块等组成。摄像头用于获取人员出入的视频图像信息，为后续的人脸识别提供原始数据；K210 视觉识别模块凭借其强大的图像处理能力，对摄像头采集的视频流进行实时处理，精准识别人员面部特征；NFC 模块则用于获取用户设置或解除报警状态等交互信息，实现便捷的用户操作。

处理层以 ESP32-S3-DevKitC-12 主控芯片为核心，承担着数据处理和系统控制的关键任务。它接收感知层传来的数据，运用优化后的人脸识别算法对人脸数据进行分析比对，判断人员身份是否合法。同时，根据系统设定的规则和逻辑，控制音频报警模块、数据存储模块等执行相应操作，如在检测到异常情况时触发音频报警，将监控数据存储至 MicroSD 卡等。

传输层主要依靠 ESP32-S3-DevKitC-12 内置的 Wi-Fi 模块实现数据的远程与近程传输。该模块将处理层处理后的监控情况数据、人员出入记录等信息通过 Wi-Fi 网络传输至服务器，再由服务器将数据转发至用户的移动终端，实现远程监控功能。Wi-Fi 传输具有高速、稳定的特点，确保数据能够及时、准确地传输，使用户随时随地都能获取门禁系统的实时信息。同时，Wi-Fi 模块也可以为系统提供近程数据传输的能力。在一些特定场景下，如用户在门禁设备附近需要快速获取设备状态、进行参数配置或者进行应急操作时，它能在短距离内稳定地将门禁系统的数据传输到用户的移动设备，如手机或平板电脑。

应用层主要通过微信小程序实现。用户可以在微信小程序上了解门禁处的实时情况；接收系统发出的报警信息，及时知晓异常事件；还能进行远程控制，如远程开启或关闭门禁、设置报警参数等，实现智能化的门禁管理。系统总体框架如图 3.1 所示。

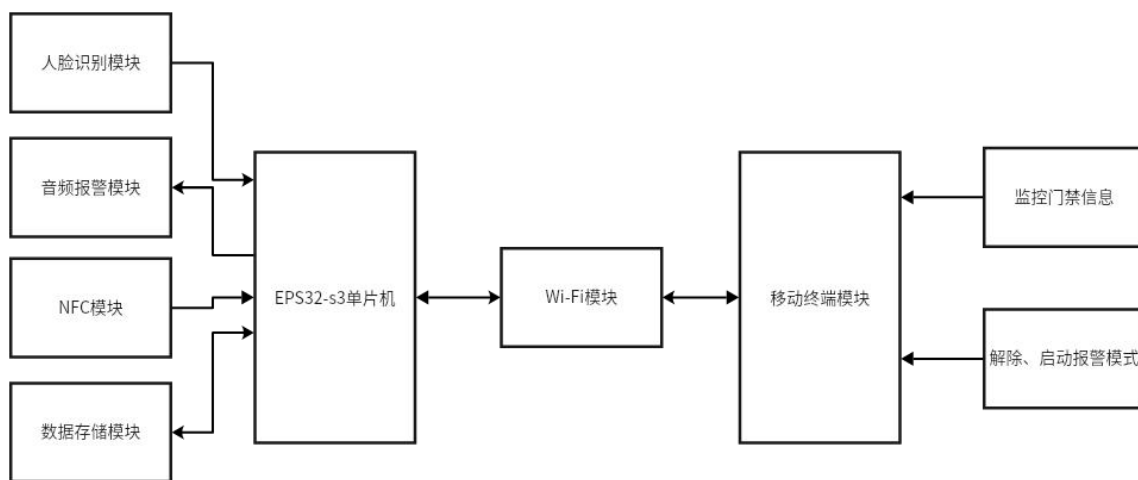


图 3.1 智能门禁控制系统总体设计图

3.2 系统功能模块简述

3.2.1 ESP32-S3-DevKitC-12 主控芯片

本设计选用 ESP32-S3-DevKitC-12 作为主控芯片，它是一款集成 Xtensa®32 位 LX7 双核微处理器的系统级芯片（SoC）。该芯片支持 2.4GHz Wi-Fi (IEEE 802.11b/g/n) 和 Bluetooth®5 (LE) 无线通信，具备强大的通信能力，能够满足系统远程监控和数据传输的需求。ESP32-S3-DevKitC-12 芯片图如图 3.2 所示。

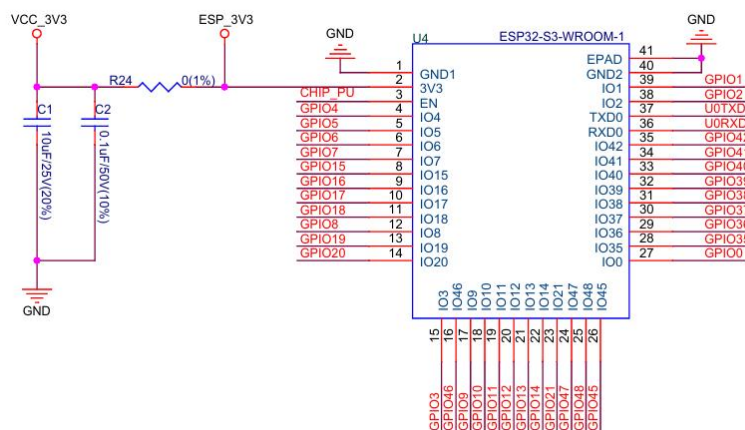


图 3.2 ESP32-S3-DevKitC-12 芯片图

3.2.2 人脸识别模块

人脸识别模块作为本系统至关重要的核心功能模块，承担着门禁系统人员身份精准识别的关键任务，主要由 K210 人脸识别模块与配套的优化算法构成。

在选择 K210 芯片时，充分考虑到了门禁系统应用场景的复杂性。门禁系统通常会面临各种各样的环境状况，光照条件更是复杂多变。白天时，阳光的直射和反射会造成光照强度的大幅波动，强光下可能出现过曝现象，而阴影处又存在光照不

足的问题；夜晚，人工照明的角度和亮度差异也会对识别造成干扰。此外，人员在进出过程中，可能会出现用手遮挡面部、佩戴帽子或口罩等部分遮挡的情况。

K210 芯片具备专门为图像处理深度优化的硬件架构，拥有强大的算力和高效的数据处理能力。它能够以极高的速度对摄像头采集的实时视频流进行处理。针对复杂光照环境，通过图像预处理技术，如自适应直方图均衡化、Gamma 校正等，能够动态调整图像的亮度和对比度，使图像在不同光照强度下都能清晰呈现面部特征。同时，优化后的算法采用了多角度特征提取和多尺度匹配技术，在人员部分遮挡的情况下，依然能够从可见的面部区域提取关键特征，并与数据库中的模板进行精准匹配，从而保持较高的识别准确率，为门禁系统的安全性提供了有力保障。实物如图 3.3 所示。

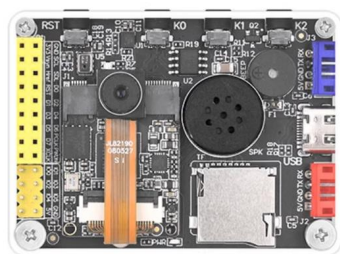


图 3.3 K210 视觉识别模块

3.2.3 音频报警模块

音频报警模块由 MAX98357 音频放大器模块和 3525 腔体-8 欧姆 2W/喇叭组成。MAX98357 音频放大器模块具备出色的低噪声放大特性，其自身引入的噪声微乎其微，有效避免了在放大报警信号过程中额外增加噪音干扰。同时，它拥有强大的功率放大能力，能够将初始的音频信号进行精准、高效的放大，确保输出足够强劲功率驱动 3525 腔体-8 欧姆 2W 喇叭。并且 MAX98357 采用了先进的节能技术，在正常工作状态下功耗较低。这使得门禁系统在长时间运行过程中，不会因为音频报警模块的高能耗而增加过多的电量消耗，有利于系统的稳定运行和降低使用成本。该模块也能够适应较宽的电源电压范围，一般为 2.7V 至 5.5V。这使得它可以灵活地与门禁系统中的其他电源模块配合使用，无论是采用电池供电还是外部电源适配器供电，都能保证音频放大器模块的正常工作，提高了系统的兼容性和适应性。

当系统检测到异常情况，如识别出未经授权的人员试图闯入、门禁长时间处于异常开启状态等，及时提醒周边人员注意异常情况，起到威慑不法分子和警示管理人员的作用。实物如图 3.4 所示。



图 3.4 MAX98357 音频放大器模块和喇叭

3.2.4 NFC 模块

NFC 模块采用 PN532-NFC 套件，为用户提供了便捷的交互方式。PN532-NFC 套件支持多达 6 种主流 NFC 标准，包括 ISO/IEC 14443 TypeA、ISO/IEC 14443 TypeB、ISO/IEC 15693 等。这使得它能够与市面上超过 90%带有 NFC 功能的设备进行通信，无论是不同品牌、型号的智能手机，还是各类 NFC 卡片、手环等，都能与之稳定连接。

用户可以通过带有 NFC 功能的设备，如手机，靠近 PN532-NFC 套件，实现设置或解除报警状态、快速授权等操作。PN532-NFC 套件支持多种 NFC 标准，兼容性强，能够与各类符合标准的设备进行通信。其操作简单、响应迅速，提升了用户使用门禁系统的便捷性和效率。实物如图 3.5 所示。



图 3.5 NFC 模块 PN532 传感器

3.2.5 数据存储模块

数据存储模块使用 MicroSD 卡 SPI 接口插座，负责存储系统运行过程中产生的各类重要数据，从成本角度来看，Micro SD 卡 SPI 接口插座方案具有显著的价格优势。对于大规模部署的门禁系统来说，Micro SD 卡的低成本使得在满足存储需求的同时，能够有效控制整体硬件成本。并且收集 NFC 特征码、人员出入信息等。方便后续查询、分析和追溯，为门禁管理提供数据支持。实物如图 3.6 所示。



图 3.6 数据存储模块

3.2.6 Wi-Fi 模块

本系统的 Wi-Fi 模块集成在 ESP32-S3-DevKitC-12 主控芯片内，选用支持高速传输的相关标准（如 802.11ac）。集成了透传功能的 Wi-Fi 模块，支持大数量的接入点，方便后台系统的管理，大大减少巡查人力，也提高产品的监管效率。特别适合智能化、大规模、低成本的现代化系统，便于应用在各种物联网系统环境。

该模块主要负责将摄像头采集的人脸信息、系统报警信息、人员出入记录等数据通过 Wi-Fi 网络传输至服务器，再由服务器转发至用户的移动终端。同时，它也接收来自移动终端的控制指令，实现远程控制功能。在实际应用中，通过优化网络设置、调整信号强度等方式，确保 Wi-Fi 信号稳定，保障数据传输的高效性和可靠性。ESP32-S3-DevKitC-1 的主要组件和连接方式如图 3.7 所示。

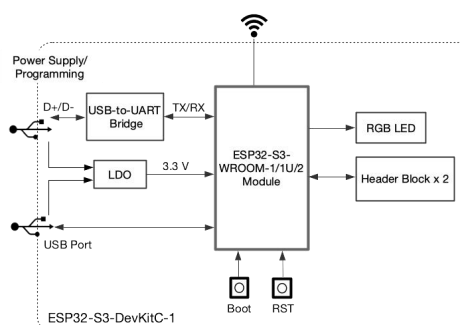


图 3.7 ESP32-S3 主要组件和连接方式

3.2.7 解除/启动报警模式

用户打开微信小程序后，进入主界面。在主界面的显眼位置，设有一个专门用于控制报警模式的文字，以醒目的颜色（如红色代表报警启动状态，绿色代表解除状态）标识，方便用户一眼识别当前报警模式并进行操作。当用户点击该按钮时，小程序会平滑地弹出一个二级确认窗口，该窗口不仅再次明确显示当前的报警状态（“当前为报警启动状态，是否确认解除？”或“当前为报警解除状态，是否确认启动？”），还以文字简要说明操作的影响，如“解除报警后，系统将暂停异常情况的主动通知，直至您再次启动”，确保用户充分知晓操作后果。解除/启动报警模式如图 3.8 所示。



图 3.8 解除/启动报警模式

3.2.8 移动终端模块（微信小程序）

移动终端模块基于微信小程序开发，为用户提供了便捷的操作界面。用户无需下载额外的应用程序，通过微信即可快速访问。在小程序界面上，用户可以接收系统推送的报警信息，及时掌握异常事件；还能进行远程控制，如远程开关门禁、设置系统参数等。小程序设计注重用户体验，界面简洁美观、操作流程简单易懂，方便不同年龄段和技术水平的用户使用。微信小程序开发者工具如图 3.9 所示。



图 3.9 微信小程序开发者工具

引脚，VCC 供电、GND 接地。

I2S_DOUT 47：I2S（Inter-IC Sound）数据输出引脚，用于输出经过处理的音频数据。在音频播放过程中，该引脚将音频数据发送到后续的音频设备（如喇叭）。

I2S_BCLK 48：I2S 位时钟引脚，为音频数据的传输提供时钟信号，保证音频数据的正确采样和传输。

I2S_LRC 15：I2S 左右声道时钟引脚，用于区分音频数据中的左右声道信息，确保音频播放的准确性。

原理图如图 4.2 所示。

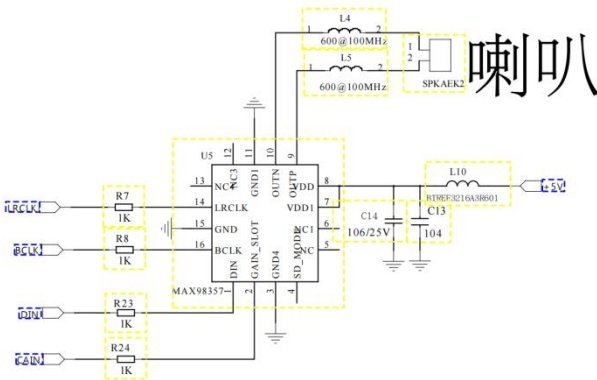


图 4.2 MAX98357 原理图

4.4 数据存储模块电路设计

SD 卡用于存储数据，如门禁系统的 NFC 标志位、人员出入记录等。引脚分别为 SD_CS、SPI_MOSI、SPI_MISO、SPI_MISO、SPI_SCK、VDD、VSS。

SD_CS 5：SD 卡片选引脚，当 ESP32 需要与 SD 卡进行通信时，通过拉低该引脚电平来选中 SD 卡，使其进入工作状态。

SPI_MOSI 9：SPI（Serial Peripheral Interface，串行外设接口）主出从入引脚，ESP32 通过该引脚将数据发送到 SD 卡。

SPI_MISO 8：SPI 主入从出引脚，ESP32 通过该引脚接收来自 SD 卡的数据。

SPI_SCK 7：SPI 时钟引脚，为 SP 通信提供时钟信号，控制数据的传输速率和时序。

原理图如图 4.3 所示。

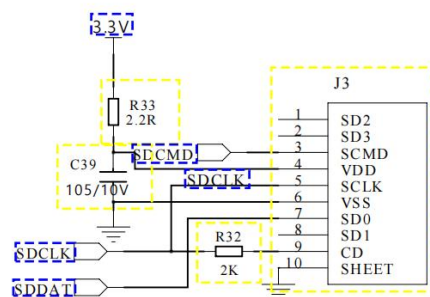


图 4.3 数据存储模块原理图

4.5 Wi-Fi 模块（射频模块）电路设计

ESP32-S3 采用低功耗 40 纳米工艺，具有超高的射频性能、稳定性、通用性和可靠性，以及超低的功耗，满足不同的功耗需求，适用于各种应用场景。ESP32-S3 的典型应用包括 Wi-Fi 模块。

ESP32-S3 系列芯片的射频电路主要由三部分组成：PCB 板射频走线、芯片匹配电路、天线及其匹配电路。各部分电路应满足以下设计规范：

- PCB 板射频走线：需进行 50 Ω 阻抗控制。
- 芯片匹配电路：请尽量靠近芯片放置，优先采用 CLC 结构。
 - ◆ CLC 结构主要用于阻抗匹配及谐波抑制，空间允许的情况下可以再加一组 LC。
 - ◆ 芯片匹配电路如图 4.4 ESP32-S3 系列芯片射频匹配电路图 所示。
- 天线及其匹配电路：为保证辐射性能，建议天线的输入阻抗为 50 Ω 左右。为保险起见，推荐在靠近天线位置增加一组 CLC 匹配电路，用于调节天线的输入阻抗。如果经过仿真可以确保天线阻抗点为 50 Ω 左右，并且空间较小，则可以不加天线端的匹配电路。

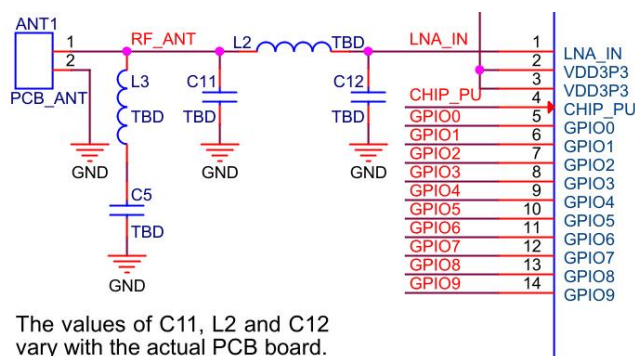


图 4.4 ESP32-S3 系列芯片射频匹配电路图

4.6 人脸识别模块

ESP32 与 K210 之间的通信是实现人脸识别和门禁控制功能协同工作的关键。采用 UART（通用异步收发传输器）通信方式，使用 TX（发送）和 RX（接收）引脚进行数据交互。

K210 的通信引脚分别为 A2 和 B11，其中 A2 作为 TX 引脚用于发送数据，B11 作为 RX 引脚用于接收数据。将 K210 的 A2（TX）引脚与 ESP32 的 RX 引脚相连，这样 K210 就能向 ESP32 发送数据；同时，将 K210 的 B11（RX）引脚与 ESP32 的 TX 引脚相连，以便 ESP32 向 K210 发送数据。

当 ESP32 需要与 K210 进行通信时，双方按照设定的 UART 通信协议：波特率设置为 115200，数据位默认是 8 位，停止位默认是 1 位，没有使用奇偶校验。开始工作。在整个通信过程中，双方持续保持数据的收发状态。当通信结束后，双方维持各自的当前状态，等待下一次通信请求。K210 原理图如图 4.5 所示。

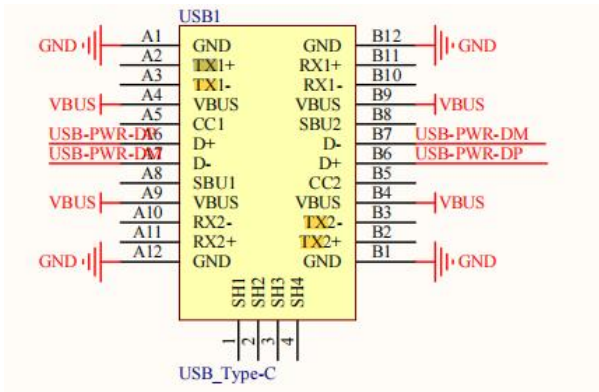


图 4.5 K210_GPIO 原理图

5 系统软件设计

5.1 系统软件总体设计

在基于视觉识别的智能门禁安全监控系统中，为实现人员身份的准确识别、门禁的智能控制以及数据的远程传输与交互，采用了多模块协同工作并结合应用程序的软件设计架构。具体如下：

系统启动后，首先进行系统初始化，涵盖人脸识别模块初始化、NFC 模块初始化以及 Wi-Fi 初始化。人脸识别模块开始采集人员面部信息，通过特定算法对采集到的图像进行处理和特征提取；NFC 模块则准备采集用户的 NFC 操作信息，如设置或解除报警状态等；Wi-Fi 模块完成初始化工作，为后续的数据传输和设备连接做准备。

这些模块采集到的数据会统一发送到应用程序。应用程序对数据进行分析处理，判断人员是否通过认证。若通过认证，门禁开启，同时音频播报通过信息，告知相关人员门禁已成功开启。

此外，系统通过 Wi-Fi 将相关数据发送至手机，用户可以通过手机选择不同的模式并控制设备，例如远程设置报警参数。若未通过认证，则不执行门禁开启操作，系统等待下一次数据采集和判断。

通过这样的软件设计，充分发挥了人脸识别、NFC、Wi-Fi 等技术的优势，实现了门禁系统的智能化、便捷化和安全可靠运行，为用户提供了高效的门禁管理体验。系统还具备完善的日志记录功能，详细记录每次人员识别和操作的时间、结果等信息，便于后续查询与审计。同时，考虑到系统的稳定性和容错性，软件设计中加入了异常处理机制，当某个模块出现故障时，系统能及时发出警报并尝试进行自我修复或切换到备用模式。此外，该软件架构还具有良好的扩展性，可方便地集成其他功能模块，如视频监控、访客管理等，以满足不同场景下日益多样化的门禁安全需求。具体软件设计框架如图 5.1 所示。

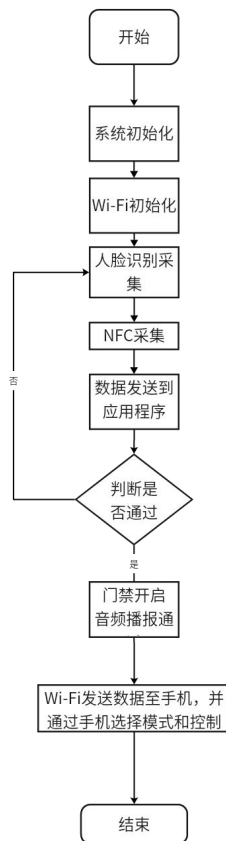


图 5.1 系统软件总体设计图

5.2 Wi-Fi 子程序软件设计

选用 ESP32 模块作为 Wi-Fi 模块。系统启动后，先通过串口向 ESP32 模块发送指令，随后开始 Wi-Fi 连接工作。一旦 Wi-Fi 连接成功，该模块便会以每 5 秒一次的频率，精准地向移动端发送包括人脸识别结果、NFC 操作信息等各类数据。这些数据能够让用户实时掌握门禁处的状况。

用户在移动端查看这些采集到的数据后，可依据实际需求，借助应用程序便捷地下达指令。比如当识别到授权人员时，用户可远程操控打开门禁；在异常情况发生时，可远程开启音频报警设备等，以此实现对门禁系统的灵活、智能控制。流程图如图 5.2 所示。

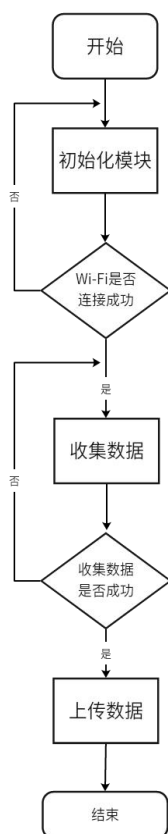


图 5.2 Wi-Fi 模块软件设计流程图

5.3 NFC 模块子程序软件设计

在智能门禁系统中，NFC 模块子程序起着关键的用户交互与信息获取作用，以下流程图展示了门禁系统从开始，经初始化模块后等待获取 NFC 卡信息并串口显示等待打印信息，判断 NFC 卡是否为已录入卡片，若是则门禁开启，流程结束的工作过程。NFC 模块子程序设计流程图如图 5.3 所示。

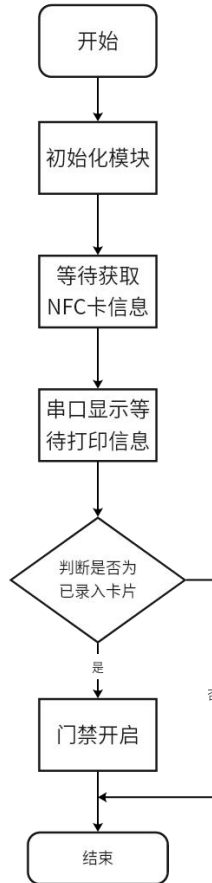


图 5.3 NFC 模块子程序设计流程图

以下基于代码进行设计阐述：系统启动后，该子程序初始化相关资源，包括初始化与 NFC 模块连接的串口通信，确保能与 PN532 芯片稳定交互，以及初始化音频模块（如 audio 对象所关联的音频播放功能），为后续可能的音频反馈做准备，同时准备好用于存储配置信息的文件对象（如 configFile），以便快速查询 NFC 卡片 UID 与操作指令的对应关系。

进入主循环后，程序持续运行并在控制台打印“Task 1 is running...”，以此表明该任务处于活跃状态。接着，它进入等待 NFC 卡片靠近的状态，并打印“Waiting for NFC card....”。当有 NFC 卡片进入感应范围时，通过 nfc.readPassiveTargetID 函数尝试读取卡片的 UID，该函数基于 PN532_MIFARE_ISO14443A 协议进行通信。若读取成功，首先将 UID 以十六进制格式打印输出，方便调试与记录，同时将读取到的 UID 字节数组转换为字符串形式（uidString），用于后续的匹配查找操作。

接下来，程序比对当前读取的 uidString 与上一次记录的 pre_uidString。若二者相同，意味着同一 NFC 设备短时间内再次触发，此时执行

audio.pauseResume() 操作，实现音频的暂停或恢复，例如在门禁场景下，如果之前有报警音频播放，再次触碰同一 NFC 设备可暂停报警，延迟 300 毫秒后继续循环等待新的 NFC 触发，避免频繁重复操作。

NFC 模块函数主要代码：

```
while (1)
{
    Serial.println("Task 1 is running...");
    uint8_t uid[] = { 0, 0, 0, 0, 0, 0, 0 }; // 存储读取到的 UID
    uint8_t uidLength; // UID 长度
    Serial.println("Waiting for NFC card...");
    // 检查是否有 nfc 卡片
    if (nfc.readPassiveTargetID(PN532_MIFARE_ISO14443A, uid, &uidLength))
    {
        // 打印 UID
        Serial.print("UID: ");
        for (uint8_t i = 0; i < uidLength; i++) {
            for (int i = 0; i < sizeof(uid); i++)
            {
                if (uid[i] < 0x10)
                {
                    uidString += "0"; // 如果元素小于 0x10，则补 0
                }
                uidString += String(uid[i], HEX);
            }
        }
    }
}
```

5.4 人脸识别模块子程序软件设计

在智能门禁系统中，人脸识别模块主要借助 K210 芯片及相关库函数来实现功能，通过与摄像头等硬件协同工作，完成人员身份的识别。以下流程图展示了门禁控制流程图。流程开始，先初始化模块，接着摄像头获取图像，然后判断是否检测到人脸，若检测到则进行人脸关键点检测，再判断关键点检测是否合格，合格就控制门禁开启，最后流程结束；若未检测到人脸或关键点检测不合格则直接结束流程。人脸识别模块子程序设计流程图如图 5.4 所示。

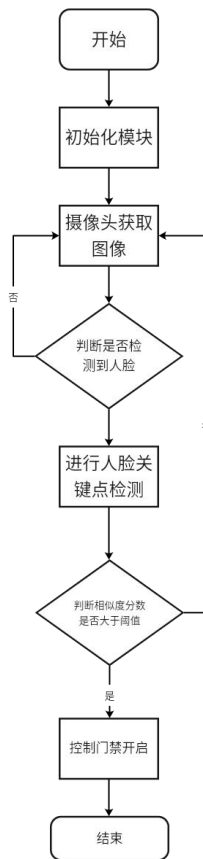


图 5.4 人脸识别模块子程序设计流程图

以下基于代码进行设计阐述：该模块首先进行初始化操作：利用 sensor 库复位并初始化摄像头，设置其输出格式为 sensor.RGB565，输出大小为 QVGA (320x240) 并等待摄像头稳定；使用 lcd 库初始化 LCD 显示屏；通过 KPU 类创建多个对象（如 kpu、ld5_kpu、fea_kpu），分别用于人脸检测、人脸关键点检测以及人脸属性检测，并加载对应的模型文件，同时完成对各模型的初始化配置，如设置人脸检测锚点、阈值等参数。此外，通过 fm、GPIO 等库对按键相关的引脚进行配置，将 board_info.BOOT_KEY 引脚注册为 GPIOHS0，配置为输入模式，并设置上升沿触发中断，中断回调函数为 set_key_state，用于在按键按下时触发特定操作。

初始化完成后，进入循环检测阶段：在每次循环中，先通过 gc.collect() 进行内存垃圾回收，查看剩余内存信息，确保系统有足够的内存资源。将获取的图像输入到用于人脸检测的 kpu 对象中进行运算，通过 kpu.regionlayer_yolo2() 进行后处理，获取检测到的人脸信息。

当检测到人脸时，对人脸框进行裁剪和处理：先通过 extend_box 函数对人脸框进行转换，从原始图像中裁剪出人脸图 face_cut，并将其调整大小为 128*128，转换为适合 AI 运算的格式。获取人脸属性特征数据 feature。

得到人脸特征数据后，将其与已记录的人脸特征数据 record_ftrs 进行比对：通过 kpu.feature_compare 函数计算相似度分数，找出最大相似度分数 max_score 及其对应的索引 index。

在循环过程中，若检测到按键 BOOT 按下（即 start_processing 为 True ），则将当前检测到的人脸特征数据 feature 添加到 record_ftrs 列表中，记录人脸特征。每次循环结束时，在图像上显示当前的帧率信息（%2.1ffps）以及提示信息（press boot key to regist face），并将处理后的图像显示在 LCD 显示屏上。

当系统结束运行时，分别对创建的 kpu、ld5_kpu、fea_kpu 对象调用 deinit 方法进行去初始化操作，释放模型占用的内存资源。通过这样的软件设计流程，实现了对门禁处人员的人脸识别功能，为门禁的开启与否提供判断依据。

获取人脸识别模块函数主要代码：

```
for l in dect :
    x1, y1, cut_img_w, cut_img_h= extend_box(l[0], l[1], l[2], l[3],
scale=0)
    face_cut = img.cut(x1, y1, cut_img_w, cut_img_h)
    # 从 img 中裁剪出人脸图 face_cut_128 = face_cut.resize(128, 128)
    ld5_kpu.run_with_output(face_cut_128, getlist=True)
    # kpu 运算并获取结果
    face_key_point = []for j in range(5):
        x = int(KPU.sigmoid(out[2 * j])*cut_img_w + x1)
        y = int(KPU.sigmoid(out[2 * j + 1])*cut_img_h + y1)
    face_key_point.append((x,y))
    T = image.get_affin_transform(face_key_point, dst_point)
    #由关键点算出变换矩阵
    image.warp_affine_ai(img, feature_img, T)
```

5.5 存储模块子程序软件设计

存储模块子程序主要负责与 SD 卡进行交互，实现将 NFC 特征码写入 SD 卡中的配置文件，以及读取和展示 SD 卡中相关文件内容和文件列表的功能。这些功能有助于系统对 NFC 特征码进行存储管理，方便后续识别验证，同时也便于用户了解

SD 卡中存储的配置信息以及文件的存储情况，进行数据管理和调试工作。流程图如下图 5.5 所示。

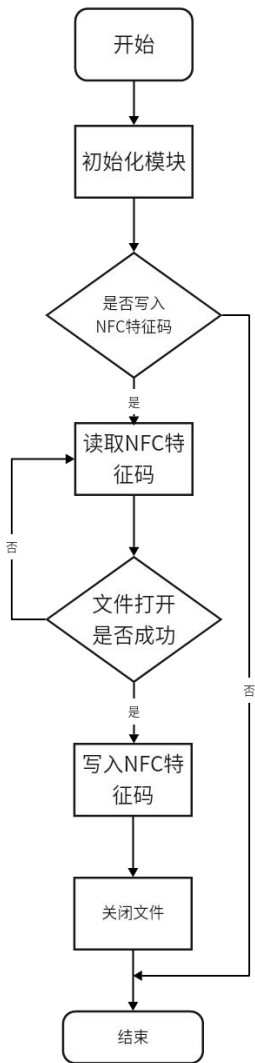


图 5.5 存储模块子程序设计流程图

以下基于代码进行设计阐述：在系统运行过程中，当读取到 NFC 特征码时，可调用 writeNfcFeatureToSD 函数将其写入 SD 卡中的配置文件，实现特征码的存储。例如，在门禁系统中，当有新的授权 NFC 设备靠近时，将其特征码存储下来以便后续识别验证。

在系统调试阶段，printWi-FiFileContents 和 printConfigFileContents 函数可用于查看存储在 SD 卡中的配置文件内容，帮助开发者确认配置信息是否正确，例如查看 Wi-Fi 配置信息或已存储的 NFC 特征码等。

listDir 函数可用于查看 SD 卡中的文件存储结构，方便用户了解文件的组织情况，例如查找特定的文件或检查文件是否正确存储在 SD 卡中。存储模块函数主要代码：

//实现将 SD 卡中的 config.txt 文件内容打印到串口的代码:

```
void printWifiFileContents() {  
  File file = SD.open("/WifiConfig.txt", FILE_READ);  
  if (file) {  
    while (file.available()) {  
      Serial.println(file.readStringUntil('\n'));  
    }file.close();} else {  
      Serial.println("Failed to open config file");}}}
```

5.6 微信小程序模块程序设计

智能门禁系统的微信小程序主要用于实现用户与门禁系统之间的交互，方便用户对门禁进行远程控制和管理，实时获取门禁相关信息。微信小程序控制界面如图 5.6 所示。



图 5.6 微信小程序控制界面

6 系统功能的测试分析

6.1 系统测试

本智能门禁系统的最终目标是实现对门禁的安全、便捷管理，准确识别人员身份，保障区域安全。

对系统的测试，首先要保证各模块的功能能够实现，需先对各模块独立测试，再进行系统整体测试。系统测试情况如下：

（1）人脸识别模块测试

人脸识别是本智能门禁系统的主要功能，用来实现人脸解锁门禁，因此人脸识别的准确性和稳定性是门禁系统的关键。本模块通过与大量已知身份的人员面部数据进行比对测试，验证其识别能力。测试方法是在不同光照条件（夜间低照度、弱光、逆光）、不同角度（正面、侧面）下，使用摄像头采集人员面部图像，然后通过 K210 视觉识别模块进行处理和识别。将识别结果与预设的人员身份信息进行对比，判断识别是否准确。同时，进行多次连续识别测试，观察识别速度和稳定性。测试数据如表 6.1 所示。

表 6.1 人脸识别模块测试测试数据表

实验序号	光照条件	角度	识别结果	准确率（置信度）	识别时间（s）	是否准确
1	正常光	正面	授权人员 A	99.62%	2	准确
2	弱光	侧面	授权人员 B	97.34%	4	准确
3	逆光	正面	授权人员	87.75%	5	准确
4	逆光	正面	未授权人员	15.35%	5	准确
5	夜间低照度	正面	授权人员 C	85.58%	7	准确
6	夜间低照度	正面	未授权人员	18.98%	9	准确

人脸识别过程如图 6.1 所示。

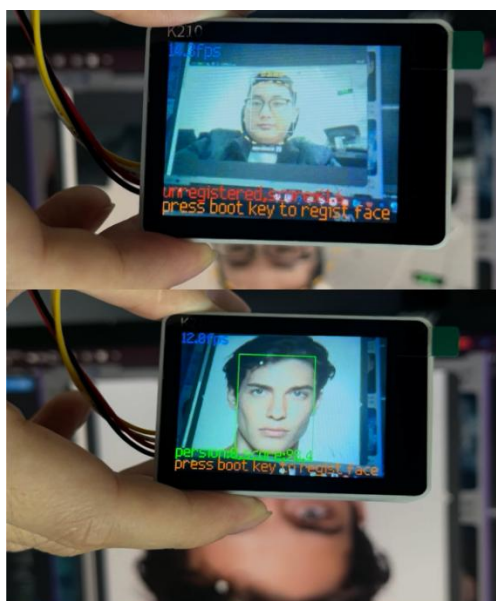


图 6.1 识别人脸过程：识别未授权人员（上）；识别已授权人员（下）

（2）NFC 模块测试

在智能门禁等系统中，NFC 模块用于实现与用户 NFC 设备的交互，测试该模块读取 NFC 设备 UID 的准确性及基 UID 执行相应操作的功能非常关键。这是因为在实际应用场景下，准确读取 UID 是系统识别用户身份、判断用户是否具备访问权限的重要前提。若读取功能出现偏差，可能会导致授权用户无法正常通行，影响用户体验；也可能使未授权用户被误判为合法用户，严重威胁系统安全。因此，对 NFC 模块进行准确性测试，从而保障整个系统的安全性和可靠性。测试数据如表 6.2 所示。

表 6.2 NFC 模块测试数据表

实验序号	NFC 设备	UID	是否为己 录入 NFC 卡	操作结果	是否准确
1	NFC 卡 1	d3f22a14000 000	是	成功	是
2	NFC 卡 2	f3fe4328000 000	是	成功	是
3	NFC 卡 3	53ee84c4610 001	是	成功	是
4	NFC 卡 4	530c8ec4610 001	否	失败	是
5	NFC 卡 5	530c9gd4610 000	否	失败	是

NFC 识别如图 6.2 所示。

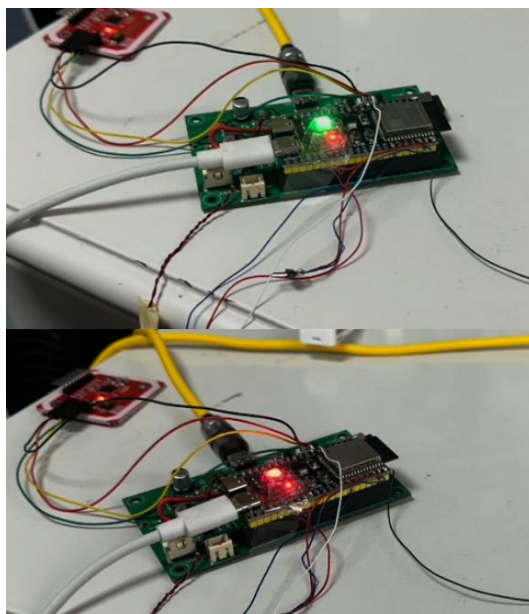


图 6.2 NFC 识别：识别已录入卡（上）；识别未录入卡（下）

（3） 音频报警模块测试。

在门禁系统这一安全防护体系里，音频报警模块承载着关键职责。门禁系统所处环境复杂多变，面临诸多潜在风险，如不法分子试图非法闯入，通过撬锁、尾随等手段避开正常授权流程开启门禁，又或是因光线不佳、人员伪装等因素致使人脸识别多次失败，这些异常状况一旦发生，若不能及时察觉并警示，将为安全防线撕开缺口。对音频报警模块展开测试意义重大。测试其是否能在正确的触发条件下发出清晰的警报声。测试方法是模拟各种异常情况，观察音频报警模块是否能及时发出警报。是否能清晰传达警示信息。进行多次测试，确保其可靠性。测试数据如表 6.3 所示。

表 6.3 音频报警模块测试数据表

实验序号	触发条件	是否发出警报	警报持续时间	警报声清晰度
1	网络中断 1 分钟	是	1 分钟	清晰
2	人脸识别失败三次	是	10 秒	清晰
3	未授权 NFC 操作	是	10 秒	清晰
4	网络中断 2 分钟	是	2 分钟	清晰
5	人脸识别失败四次	是	10 秒	清晰

音频模块如图 6.3 所示：

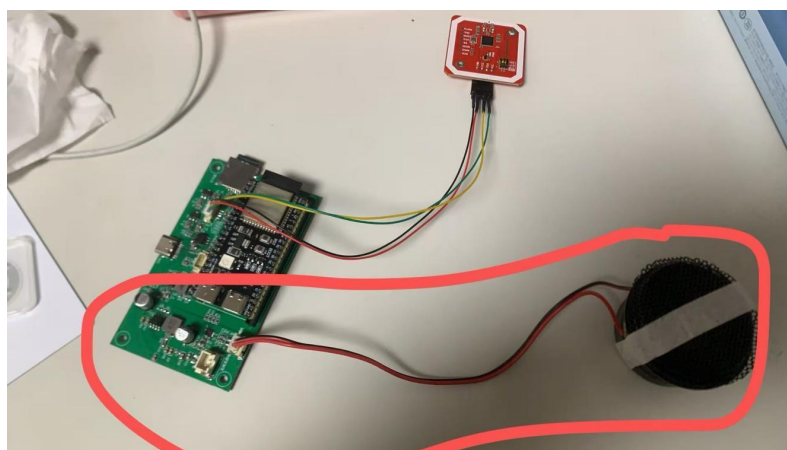


图 6.3 音频模块发出警报

（4） 微信小程序测试

微信小程序模块为用户提供了便捷的门禁管理界面。它作为直接面向用户的交互端口，极大地拓展了门禁管理的便捷性与灵活性。测试其界面的易用性、功能的完整性以及与门禁系统的交互性。测试方法是邀请不同的用户使用小程序，进行各种操作，如查看门禁状态、远程控制门禁、设置参数等。收集用户的反馈，评估界面是否简洁直观、操作是否便捷流畅。检查微信小程序模块的各项功能是否正常工作，与门禁系统的数据交互是否准确及时。测试界面如图 6.4 所示。



图 6.4 微信小程序界面

（5） Wi-Fi 通讯测试

在整个智能门禁系统架构里，Wi-Fi 通讯模块使得用户移动端与门禁主控设备之间能够实现便捷、高效的数据交互，极大提升了门禁系统的使用灵活性与智能化水平。因此，对 Wi-Fi 通讯模块进行一方面，要测试 Wi-Fi 连接的稳定性。考虑到实际使用场景复杂多样，都需要确保 Wi-Fi 设备与门禁系统之间能迅速、可靠地建立连接，并且在长时间使用过程中不会无故中断或出现频繁掉线情况。另一方面，数据传输的准确性与及时性是关键要点。测试数据如表 6.4 所示；

表 6.4 Wi-Fi 通讯模块测试数据表

实验序号	触发条件	是否成功连接（手机与门禁系统）	连接建立时长	数据传输是否准确	数据传输是否及时
1	空旷距离 5 米处尝试连接	是	2 秒	是	0.3 秒
2	空旷距离 10 米处尝试连接	是	4 秒	是	0.4 秒
3	空旷距离 15 米处尝试连接	是	7 秒	是	0.4 秒
4	连接状态下手机发送 10 组模拟开门指令	已连接，测试指令发送	—	10 组指令全部准确接收并执行	平均 0.4 秒
5	连接状态下门禁系统推送 10 组模拟门禁状态数据	已连接，测试数据推送	—	10 组指令全部准确接收并执行	平均 0.4 秒
6	保持连接 1 小时观察连接稳定性	持续连接 1 小时	连接未中断	—	—
7	模拟信号波动环境下连接并传输数据	是	连接未中断	指令全部准确接收并执行	平均 0.4 秒

测试小程序搜索 Wi-Fi 设备如图 6.5 所示。

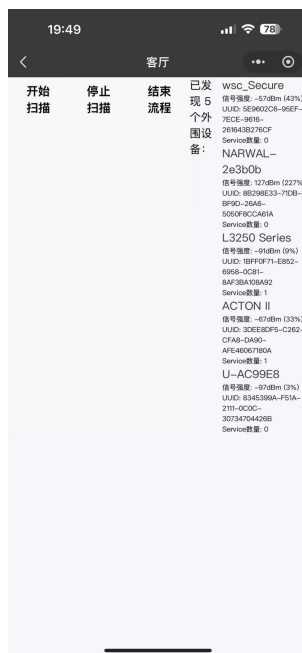


图 6.5 小程序搜索 Wi-Fi 设备 (wsc_Secure)

测试 ESP32 连接串口打印如图 6.6 所示。



图 6.6 ESP32 连接串口打印

6.2 系统整体分析测试总结

经过系统测试，当系统通电后，等待各模块初始化成功，系统的各个模块工作正常，系统整体测试正常。人脸识别模块能够在多种条件下准确识别人员身份；NFC 模块可以正确读取 NFC 设备信息并执行相应操作；Wi-Fi 模块连接稳定，数据传输准确；音频报警模块能在触发条件下及时发出警报；存储模块可准确存储和读取数据；APP 模块功能完整，用户体验良好。

通过多次测试，本系统实现了基于多模块协同工作的智能门禁系统，达到了预期要求。该系统具有安全性高（准确识别人员身份，有效防范非法进入）、便捷性强（支持远程控制和多种交互方式）、扩展性好（可根据需求添加或升级功能模块）的优点，适于进一步推广或研究，具有很强的可实施性。

7 总结与展望

7.1 系统总结

本课题聚焦于智能门禁安全监控系统的设计与构建，依托先进的物联网与嵌入式技术，以 ESP32 作为核心单片机，充分发挥其强大的数据处理与多模块协同控制能力，借助内置的 Wi-Fi 模块，搭建起稳定高效的无线通信链路，实现系统与外部设备间的无缝对接。

在硬件设计层面，运用专业的电路设计软件精心绘制原理图，对各个功能模块进行精细布局与选型，涵盖精准灵敏的人脸识别模块（K210 视觉识别模块搭配高清摄像头）、便捷实用的 NFC 模块（PN532-NFC 套件）、及时有效的音频报警模块（MAX98357 音频放大器与优质喇叭组合）、可靠稳定的数据存储模块（Micro SD 卡存储方案）等。各硬件模块间通过高速 SPI、UART 等通信接口紧密相连，确保数据的流畅交互，从底层硬件架构上为系统的稳定运行筑牢根基。

软件方面，基于嵌入式实时操作系统或高效的裸机程序架构，开发出功能完备的控制程序。其中，人脸识别算法经过大量样本训练与优化，能在复杂环境下快速、精准地识别人员身份真正实现了系统的智能化、便捷化管理。

综合来看，本设计圆满达成了预期目标，成功打造出一个集人员精准识别、门禁智能管控、安全异常报警、数据实时交互于一体的智能门禁安全监控系统，具备高可靠性、强扩展性以及出色的用户体验，在提升区域安全性、管理便捷性上成效显著。

7.2 后期展望

尽管当前系统已实现诸多核心功能，但随着技术的飞速发展与实际应用场景的日益复杂，仍有广阔的优化提升空间。

在功能拓展维度，考虑引入智能视频监控功能，通过在门禁关键位置部署高清网络摄像头，利用先进的视频编码与传输技术，将实时画面推送至云端服务器，用户即可借助手机 APP 随时随地查看门禁现场动态，不仅能实时掌握人员进出情况，在异常事件发生时还能第一时间获取直观的现场视频证据，极大增强系统的安防监控能力。同时，可深度融合人工智能技术，如基于深度学习的行为分析算法，对监控画面中的人员行为进行实时分析，提前预警潜在的异常行为，如徘徊、翻越等，将安全防范关口进一步前移。

从用户体验优化角度出发，持续改进 APP 界面设计，引入更加人性化的交互元素，如语音控制功能，用户仅需通过简单的语音指令即可完成门禁操作、查询信息等任务，彻底解放双手；加强数据可视化展示，利用图表、图形等直观形式呈现门禁使用数据、报警统计等信息，让用户一目了然。

在系统兼容性与扩展性方面，着眼于未来智能家居、智慧办公等综合生态系统的构建，预留丰富的外部接口与通信协议，使其能轻松与其他智能设备（如智能照明、空调控制系统、智能考勤机等）互联互通，实现一体化的智能管理解决方案，为用户打造更加便捷、高效、智能的生活与工作环境，助力物联网产业的蓬

参考文献

- [1]何鑫宇. 基于 ARM 的智能家居监控系统的设计与实现[D]. 2022
- [2]李昌奇, 何志琴, 周恒, 王霄. 基于 Android 和 WiFi 的智能家居监控系统设计与实现[J]. 现代电子技术, 2020, 第 43 卷(20): 67-70
- [3]张敏. 基于视觉隐私安全机制与时序自适应网络的居家视频行为识别系统设计与实现[D]. 2022
- [4]黄金亮. 融合 LoRa 通信技术的智能家居安全监控系统设计与实现[J]. 集成电路应用, 2024, 第 41 卷(6): 40-41
- [5]王建财, 王焕昱, 曾文杰. 一种基于视觉识别的智能安全监控系统[P]. 中国专利: CN118279834A, 2024. 07. 02
- [6]郭顺超, 苗雄, 元艳香. 基于人脸识别的小区门禁管理系统设计与实现[J]. 科技视界, 2024, 第 14 卷(18): 58-61
- [7]张斌, 徐榕泽, 庞昊. 基于 STM32 的非接触式手势识别门禁设计[J]. 单片机与嵌入式系统应用, 2023, 23(07): 84-87.
- [8]陆畅, 陈东焰, 俞浩. 基于 OpenCV 视觉库和树莓派的人脸识别门禁系统[J]. 科技创新导报, 2019, 第 16 卷(2): 152-154, 156
- [9]徐杰, 李捍东. 基于单片机与 OpenCV 的门禁系统[J]. 计算机时代, 2022, (5): 63-65, 69
- [10]玄冉, 姜明明, 王忠祥, 米世新, 刘涵玉. MATLAB 的疫情防控人脸门禁系统设计[J]. 南方农机, 2021, 第 52 卷(12): 187-189
- [11]王蒙蒙, 高腾腾. 基于机器视觉的智能门锁系统的设计与实现[J]. 滨州学院学报, 2020, 第 36 卷(2): 74-78
- [12]Husni N L, Sari P A R, Dewi T, et al. Visual Studio Code for Activity Monitoring Interface[C]//5th FIRST T1 T2 2021 International Conference (FIRST-T1-T2 2021). Atlantis Press, 2022: 380-386.
- [13]Hazra A. Promising role of visual IoT: Challenges and future research directions[J]. IEEE Engineering Management Review, 2023.
- [14]Sharad S ,Aparna K .An Efficient Routing Algorithm for IoT Using GWO Approach[J].International Journal of Applied Metaheuristic Computin

g (IJAMC), 2021, 12(2):67–84.

[15]Sabit H .Artificial Intelligence-Based Smart Security System Using Internet of Things for Smart Home Applications[J].Electronics, 2025, 14(3):608–608.

[16]Si S ,Jing L ,Hao G , et al.A facile way to construct highly stable PUF tags for unclonable anti-counterfeiting and authentication with computer vision[J].Colloids and Surfaces A: Physicochemical and Engineering Aspects, 2022, 648.

致谢

在智能门禁系统的设计与实现过程中，诸多人士和组织给予了我极大的支持与帮助，在此，我想向他们表达我最诚挚的感谢。

我要衷心感谢我的导师，是您的悉心指导与耐心解答，为我在项目研究的迷茫中点亮了一盏明灯。从最初的选题构思，到系统架构的搭建，再到技术难题的攻克，每一个环节都离不开您的专业建议与严谨治学态度的感染。您的一次次审阅与批注，让我不断反思、进步，为项目的顺利推进奠定了坚实基础。

感谢我的朋友们，在无数个熬夜奋战的日子里，你们给予了我陪伴与鼓励。当我为代码的错误而懊恼，为设计的瓶颈而焦虑时，是你们的欢声笑语让我暂时放下疲惫，重拾信心。你们的理解与包容，让我能全身心地投入到这项研究中。

我还要感谢那些为开源社区做出贡献的开发者们，本项目所使用的诸多技术框架、库函数，都源自你们的智慧结晶。无论是人脸识别算法的开源代码，还是 NFC、Wi-Fi 等模块的驱动程序，你们无私的分享让我得以站在巨人的肩膀上，加速了项目的开发进程，节省了大量的时间与精力。

特别感谢我的家人，你们始终是我最强坚实的后盾。在漫长的求学与研发道路上，你们默默承担了生活的琐碎，给予我物质与精神上的双重支持。你们的关心与期待，化作我前进的动力，让我在面对困难时从未轻言放弃。

同时，我也要感谢参与本项目测试的同学们，是你们不厌其烦地试用系统，提出宝贵的反馈意见，帮助我发现那些隐藏在角落里的漏洞与不足，促使我不断优化完善，最终打造出一个更加稳定、实用的智能门禁系统。

这份毕业设计的完成，不仅仅是我个人努力的成果，更是众多力量汇聚的结晶。我将带着这份感恩，继续在技术的道路上砥砺前行，用所学知识创造更多的价值。

附录 1 系统硬件设计图

