

# 基于 MM32F5270 微控制单元的 智慧门禁系统设计

林博涵, 程 仪, 朱立超, 谢迎娟

(河海大学 信息科学与工程学院, 江苏 常州 213000)

**摘要:** 传统门禁系统存在钥匙易被伪造、解锁方式单一、难以对门禁区域进行实时监控和数据分析等一系列安全性、体验性问题; 结合物联网技术, 以灵动微电子 MM32F5270 开发板作为主控, 设计了一套安全性高、智能化高、可联网的智慧门禁系统; 系统以 MindSDK 和 MircoPython 为开发平台, 由摄像头模块采集图像数据, 并交由 MM32F5270 处理后, 通过 WIFI 模块传输数据到服务器; 根据接收到的图像数据结合 LBP 算法获取人脸特征点数据, 并将其输入至卷积神经网络以实现人脸检测的目标; 实验结果表明, 该智慧门禁系统能有效解决安全性差、数据管理难和无法实时监控等问题, 提高了用户体验和系统可靠性。

**关键词:** 智慧门禁; IoT; TCP 透传; MM32F5270; OpenMV; LBP 算法

## Intelligent Access Control System Design Based on MM32F5270 Micro Control Unit

LIN Bohan, CHENG Yi, ZHU Lichao, XIE Yingjuan

(School of Information Science and Engineering, Hohai University, Changzhou 213000, China)

**Abstract:** Traditional access control systems have a series of security and experiential issues, such as easy key forgery, single unlocking method, and difficulty in real-time monitoring and data analysis of access control areas. Combining IoT technology, a smart access control system with high security, intelligence, and networking capabilities was designed using the Smart Microelectronics MM32F5270 development board as the main controller; The system is developed using MindSDK and MircoPython as platforms. Image data is collected by the camera module and processed by MM32F5270. The data is then transmitted to the server through the WIFI module. Obtain facial feature point data based on the received image data combined with the LBP algorithm. And input it into the convolutional neural network to achieve the purpose of face detection. The experimental results show that the smart access control system can effectively solve problems such as poor security, difficult data management, and inability to monitor in real time, improving user experience and system reliability.

**Keywords:** smart access control; IoT; TCP transparent transmission; MM32F5270; OpenMV; LBP algorithm

### 0 引言

在现有的门禁系统技术领域, 多种门禁管理方案被广泛应用于各类场所, 以确保区域的安全性和管理的便捷性, 门禁控制通常依赖于传统的物理媒介如钥匙、磁卡或者更先进的技术如密码输入、指纹识别以及 RFID 技术进行身份验证<sup>[1]</sup>, 此外, 部分门禁系统还引入了视频监控技术来增强安全措施。采用以上的门禁控制手段各有优势, 但主要集中在单一的身份验证方式或者将多种方式结合使用, 而较少考虑到系统的整体智能化和网络化管理。例如, 机械钥匙锁易于被撬锁和钥匙复制, 且存在钥匙易丢失难管理的问题, 尤其是在需要多人共享进出权限时。其次, 传统门锁难以对进出人员进行数据管理和监控追踪, 限制了

对人员活动的监控能力, 减少了整体的安全性。传统门禁系统无法远程操作, 且在用户验证和信息处理方面的响应时间较长, 降低了其效率和实用性。现有的智慧门禁系统研究有:

文献 [2] 设计了一种基于 STM32 的智能家庭门禁系统, 该系统能实现人脸识别开门功能、短信报警功能, 通过 WiFi 模块、云平台 and 手机 App 远程开门, 还可通过手机 App 生成一次性的加密二维码, 给予来访者扫码开门的权限。文献 [3] 设计了一种基于身份证和人脸双重识别技术的智能门禁系统, 通过 RFID 射频识别技术实现了身份证识别, 通过宽度学习卷积神经网络算法实现了人脸识别, 设计了智能门禁系统的通信指令, 提出了一种基于优先级的

收稿日期: 2024-06-11; 修回日期: 2024-06-28。

基金项目: 国家自然科学基金(61573128); 教育部产学研合作协同育人项目(220803494162012, 220603632072407); 大学生创新创业训练计划项目(202310294048Z); 河海大学创新性实验项目(河海教务[2022]49号)。

作者简介: 林博涵(2001-), 男, 大学本科生。

引用格式: 林博涵, 程 仪, 朱立超, 等. 基于 MM32F5270 微控制单元的 智慧门禁系统设计[J]. 计算机测量与控制, 2024, 32(8): 272-279.

周期性多任务调度算法, 有效地提高实时多任务系统的整体控制性能。文献 [4] 通过集成射频识别 (RFID) 卡标签系统、指纹传感生物识别安全系统和全球移动通信系统 (GSM), 将系统生成的令牌发送到授权用户的接入手机, 引入了一种具有自动传感功能的开发安全系统。该系统的精度是在模拟屏幕上虚拟测量的。文献 [5] 通过提出了一种用于访问控制系统的三维人脸识别算法。所提出的算法包括预处理、特征提取和分类阶段。所提出的访问控制系统的应用是自动滑动门、系统的控制器、基于网络的数据监测、控制和存储。

在上述研究的基础上, 本文设计基于 MM32F5270 微控制单元的智慧门禁系统。文章扩展了 LBP 算法以支持不同环境下对目标进行识别与跟踪。LBP 特征对光照变化具有鲁棒性, 它基于局部邻域的相对灰度差异而不是绝对值, 这使得它在不同光照条件下仍能保持较好的识别性能。LBP 算法能够有效提取面部的局部纹理特征, 如眼睛、鼻子、嘴巴等区域的纹理信息, 有助于对个体的准确识别。并利用卷积神经网络针对提取到的特征点实现检测的目的。

### 1 系统结构及原理

本文设计的智慧门禁系统设计采用 MM32F5270 作为主控芯片, 硬件区域由身份验证模块、门禁控制模块和远程通信模块组成。软件区域基于 LBP 的人脸特征提取进行了身份验证设计。MM32F5270 单片机作为硬件设备工作的核心; ESP32WIFI 模块作为硬件系统与服务器流的传输媒介并实现数据传输功能; 摄像头模块时刻监测并采集门禁区域的图像数据, 通过 LBP 算法和卷积神经网络实现人脸检测, 便于用户随时监视门禁系统的状态和活动。系统总体结构如图 1 所示。

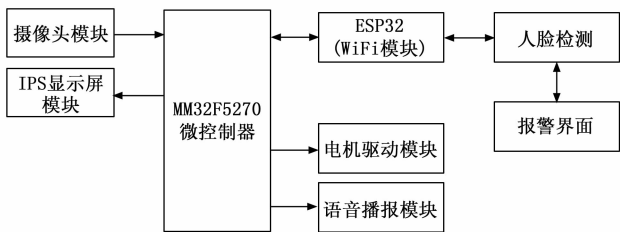


图 1 系统结构示意图

## 2 系统硬件设计

### 2.1 主控电路设计

采用 MM32F5270 微处理器作为主控芯片, 该芯片具有高性能、低功耗、丰富的外设接口等优势。MM32F5270 是智慧门禁系统的重要组成部分, 负责处理从摄像头、密码键盘和 NFC 卡识别等模块获取的数据进行处理, 从而控制驱动电机的运作; 可以控制 IPS 屏幕显示门禁状态; WIFI 模块与微处理器进行通信实现连接, 通过阿里云平台进行数据交互和远程控制。MM32F5270 单片机和电源电路、时钟电路、复位电路等构成单片机最小系统, 确保系统可靠

启动以及门禁内部各模块同步工作。

### 2.2 WIFI 模块

本系统采用 ESP32 芯片来完成 WIFI 模块的设计和开发。ESP32WIFI 模块是一种可编程的、低功耗、高性价比的无线网联芯片方案。它支持 TCP/IP 协议栈, 并可以通过串口实现与 MM32F5270 主控芯片的连接和通讯。ESP32 模块可以通过 UART (串行通信) 与主控芯片进行数据交换, 并接收传来的数据, 如云平台的指令或者门禁状态信息。主控芯片也可将采集处理的数据发送给云平台实现同步。ESP32 的主要引脚连接如下: VCC, 电源正极接口, 连接至 3.3 V 电源; RXD、TXD 串口通信引脚, 分别与 MM32F5270 主控板上的 B0 和 B1 引脚相连。在连接之后, 需要配置串口通信参数, 使用 AT 指令设置合适的波特率, 以确保数据的准确传输和接收。ESP32 模块原理如图 2 所示。

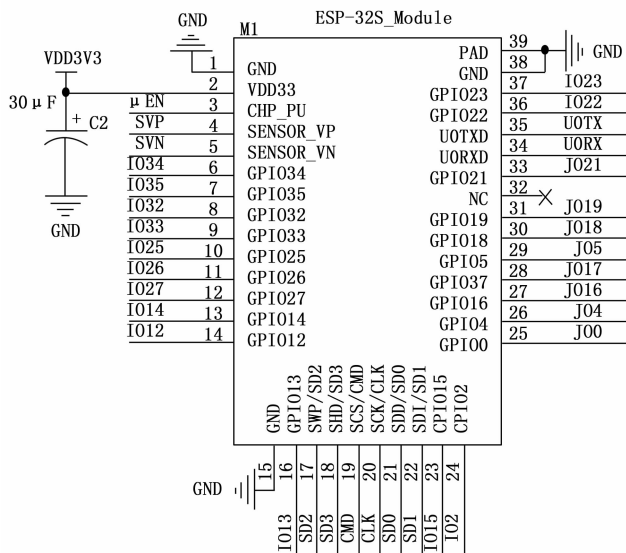


图 2 ESP32 模块原理图

### 2.3 摄像头模块

OpenMV 是一种基于 MicroPython 的开源计算机视觉平台, 专门设计用于嵌入式系统和物联网应用。它具有小巧、高效的特点, 并且集成了图像传感器、处理器和运行 MicroPython 的环境。通过 OpenMV 模块, 门禁系统可以获取门禁区域的图像数据, 并实现图像处理、人脸识别、人体感应等功能<sup>[3]</sup>。

OpenMV 摄像头模块具有全速 USB (12 Mbps) 接口, 能连接到电脑, 便于将数据传输到云服务器;  $\mu$ SD 卡槽拥有 100 Mbps 读写, 允许 OpenMV 摄像头拍摄照片, 便于存储监控图像; 具有两个异步串口总线 (TX/RX), 能与 MM32F5270 主控芯片进行通信; 两个 I/O 引脚用于舵机控制, 便于摄像头自主跟踪可疑目标, 提高安全系数。OpenMV 摄像头模块具有可拆卸、可靠性高、传输速率快等特点。

### 2.4 显示屏模块

通过将 IPS 显示屏与门禁系统集成, 可以在显示屏上

实时显示系统的状态信息。例如,显示当前时间、门锁状态(开启或锁定)、输入的密码等。通过 IPS 显示屏模块,用户可以方便地查看系统的实时状态。门禁系统可以提供实时信息展示和记录查询的功能。用户可以通过 IPS 显示屏实时查看系统状态和密码输入,为用户提供了方便、直观的界面和操作,便于用户更好地管理和监控门禁系统。显示屏模块接口的原理如图 3 所示。

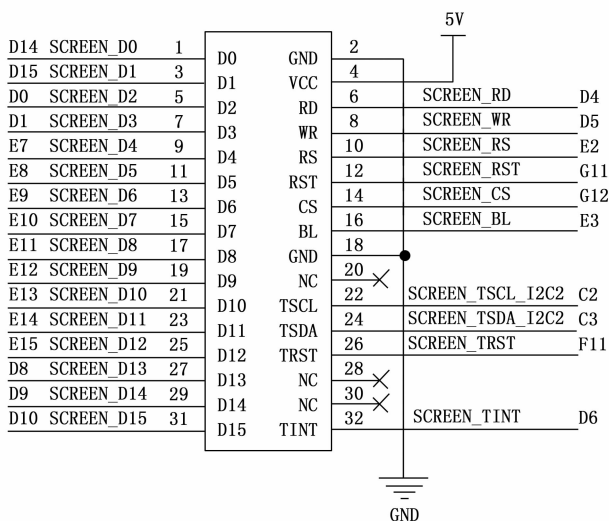


图 3 显示屏模块接口原理图

2.5 电机驱动模块

本模块使用了 LM298n 作为驱动芯片。MM32 主控芯片作为控制核心,通过给 LM298n 驱动芯片使能和输入信号,能有效控制电机的启停,从而实现门禁的开合控制。通过该驱动模块,可以实现对门禁系统的自动化管理,提高门禁系统的安全性和便利性,满足现代社会对门禁系统智能化的需求。电机驱动模块的原理如图 4 所示。

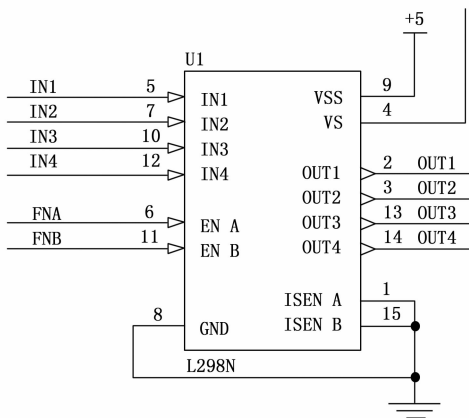


图 4 电机驱动模块原理图

2.6 语音播报模块

通过集成语音合成技术,对非法入侵行为进行语音警告。当系统检测到异常情况或未授权人员进入时,通过扬声器或喇叭发出语音提示,提醒潜在入侵者离开。本系统

使用 JQ8900 语音播报模块,通过 UART 串口通信,模块的 TXD 和 RXD 分别与主控制器的 RXD 和 TXD 连接。在使用该模块过程中,需要注意的是语音输出后要增加延时语句,即需要一定的时间让语音模块读完播放信息<sup>[4-5]</sup>。语音播报模块的主控 IC 原理如图 5 所示。

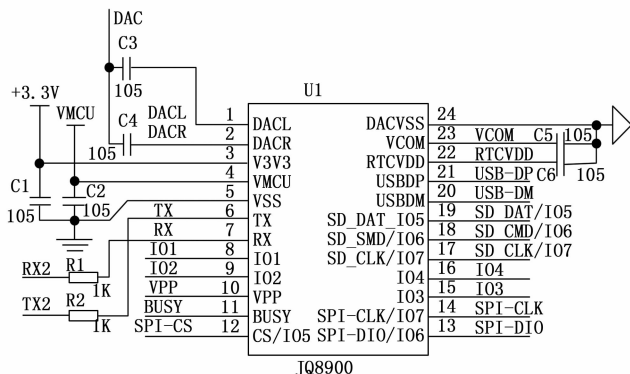


图 5 语音播报模块主控 IC 原理图

2.7 数据库设计

云端应用采用阿里云云服务器作为云端应用平台,使用 springboot 技术框架进行后端开发,通过云服务器提供的高可用性和容错机制,保证门禁系统的稳定性和可靠性<sup>[6-7]</sup>。连接 MySQL 作为持久型数据库,使用 Redis 数据库存储需要频繁改动的数据,实现对门禁系统数据的快速存储和查询。门禁系统将采集到的数据,将开门记录、警报记录、监控图像等重要信息保存在云端数据库中,用户可以随时访问和查看,并进行必要的数据分析和和管理。

3 系统软件设计

3.1 总体程序设计

系统软件总体上由核心主控程序、开门程序、行人识别程序以及人脸识别开门程序组成。

主程序在运行后,主控 MM32 控制摄像头开始识别门禁区域内的行人,通过 PID 算法实现自动跟踪。若可疑人员在门禁区域内逗留超过 10 s,则拍摄照片并保存到本地,便于用户了解门禁监控区域状态;若没有行人经过,摄像头则继续捕捉图像。当用户人脸识别成功时,则会控制电机工作开启大门;如果识别失败时,则会发出警报,并返回当前时间等信息,确保仅授权用户能够进行开锁成功的操作。

用户可以通过微信小程序控制摄像头执行人脸录入授权以及人脸识别开门的操作。系统在人脸识别时可迅速将当前人员的面部特征与事先存储的授权用户的人脸数据进行比对。软件运行总体流程如图 6 所示。

3.2 行人检测算法设计

行人检测算法的核心是使用 OpenMV 内部部署训练好的神经网络模型,进行目标检测识别。行人检测功能实现步骤如下:

- 1) 将 OpenMV 连接上位机 IDE 完成行人数据集的采

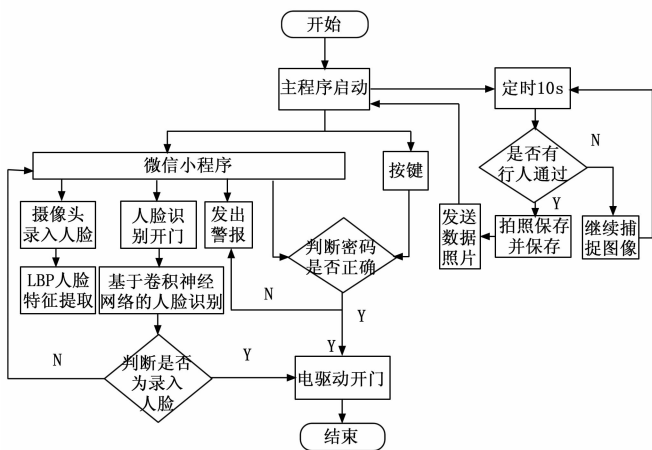


图 6 软件运行总体流程图

集, 将采集好的数据集上传至 EdgeImpulse 网站, 在标注列队对数据集进行集中标记, 框出行人目标并设置标记名称;

- 2) 设置卷积神经网络参数, 选择训练图像分辨率大小为  $96 \times 96$ , 以适用于 FOMO 模型进行神经网络模型训练;
- 3) 生成模型特征, 并进行模型训练, 对训练结果进行训练参数调整并将文件部署在 OpenMV 上;

4) OpenMV 完成初始化后, 加载训练好的行人检测模型, 调用函数不断采集图像, 对采集的图像进行识别处理, 判断图片内是否存在模型检测目标, 并对参数进行调整, 使行人检测精确度达到最优。如果检测到行人目标, 则进一步对目标行人所在像素块进行筛选, 选择有效区进行目标定位。通过 UART 串口通信方式向主控单片机发送指示信号。行人检测算法流程如图 7 所示。

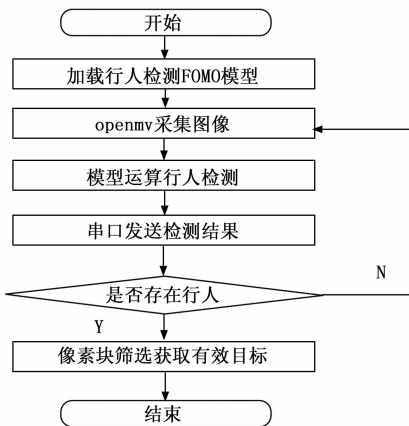


图 7 行人检测算法流程图

### 3.3 目标追踪算法设计

目标追踪算法的核心在于检测到行人目标定位后<sup>[8]</sup>, 利用 PID 算法控制云台快速稳定地自动跟随行人并进行实时追踪。提前将 PID 算法文件保存到 OpenMV 内, 并在程序前添加算法文件的声明。使用神经网络算法检测到行人目标有效区后, 计算出该有效区的中心像素点坐标并保存, 横纵坐标值  $x$ 、 $y$  分别与中心像素点坐标作差, 求出

目标点的坐标偏差, 将偏差参数进行 PID 算法处理, 获取云台打角偏量, 并改变云台打角, 进行目标追踪。所用到的摄像头功能函数如表 1 所示。目标追踪算法流程如图 8 所示<sup>[9-10]</sup>。

表 1 摄像头功能函数表

函数名称	实现功能
tf.load_builitin_model()	加载检测模型函数
sensor.snapshot()	图像采集处理函数
net.detect()	判断检测目标函数
uart_send()	串口发送函数
pan_pid.get_pid()	PID 处理函数
pan_servo.angle()	底部云台打角函数
tilt_servo.angle()	顶部云台打角函数

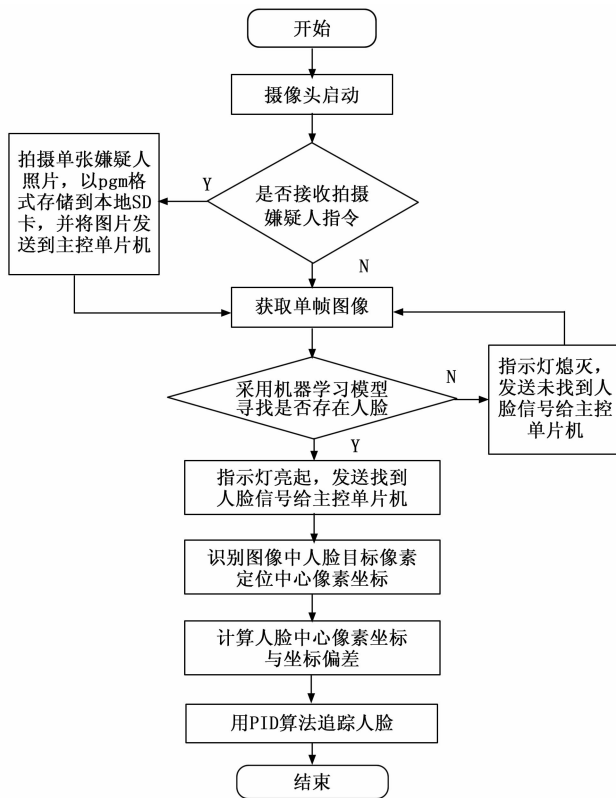


图 8 目标追踪算法流程图

### 3.4 基于 LBP 的人脸特征提取

LBP 是一种描述图像纹理特征的算子, 其核心思想在于利用中心像素的灰度值作为阈值, 通过与其相邻像素进行比较, 得到相应的二进制码来表征局部纹理特征<sup>[11-13]</sup>。

假设有一个  $3 \times 3$  的窗口, 里面的数值表示每个像素的灰度值, 如图 9 所示。

例如中心像素点的灰度值为 6, 将此中心像素点的灰度值与其周围 8 领域的像素值大小进行比较, 若大于 6, 则把右侧对应的方格置为 1, 小于 6 则置为 0。之后就得到右边的窗口, 把这些 1 和 0 按逆时针方向依次连起来就得到了所谓的 LBP 模式。然后将得到的 8 位二进制数按顺序排列,

example	thresholded	weights
6 5 2	1 0 0	1 2 4
7 6 1	1 1 0	128 32 8
9 8 7	1 1 1	64 32 16

图 9 3×3 的窗口

即为该中心像素的 LBP 值。该值反映了中心像素和其邻域的纹理信息。则根据 LBP 获取到人脸特征表达式为：

$$LBP(x_c, y_c) = \sum_{p=0}^{p-1} (p-1)2^{p-1} \quad (1)$$

式中,  $(x_c, y_c)$  为代表邻域窗口内的中心像素, 其像素值为  $i_c$ 。  $i_p$  表示邻域内其他像素值,  $p$  为邻域内像素的数量<sup>[14-15]</sup>。

### 3.5 基于卷积神经网络的人脸识别

根据上述提取到的人脸特征点信息, 通过卷积神经网络对其进行识别。卷积神经网络是一种专门针对图像和空间数据的深度学习模型。在门禁系统中, 将上述获取的特征点作为输入, 通过对这些特征的分析和学习, 可以实现对人脸的实时监控和异常检测。卷积神经网络结构如图 10 所示<sup>[16-17]</sup>。

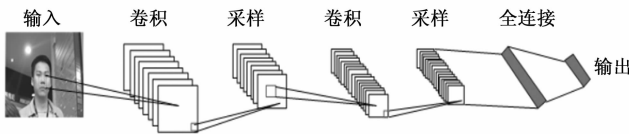


图 10 卷积神经网络结构

1) 输入层接受人脸特征点信息并将其传入网络, 以供后续的特征学习和处理使用。

2) 卷积层作为特征提取层, 通过使用卷积核与输入数据的局部区域进行卷积运算, 从图像中提取出不同的特征。每个神经元通过与其周围神经元的连接来学习不同的特征表示。通过选择不同的卷积核, 网络能够从图像中学习多种不同类型的特征, 以用于后续的任务和分析。这种方式使网络具有更轻量级和高效的特征提取能力。卷积层操作如图 11 所示。

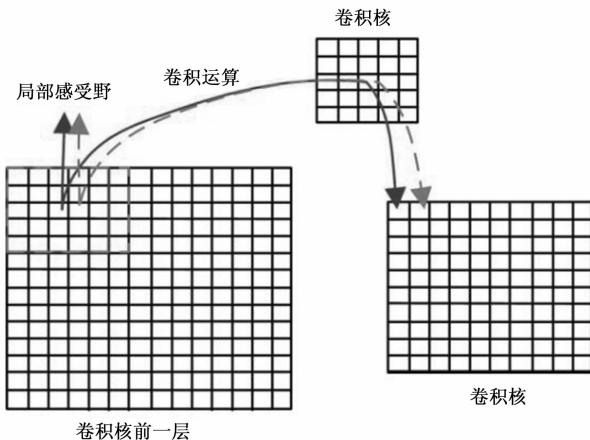


图 11 卷积层操作示意图

卷积层输出形式为：

$$A_j^{(l)} = f\left(\sum_{i \in R_j} A_i^{(l-1)} * K_{ij}^{(l)} + B_j^{(l)}\right) \quad (2)$$

式中,  $*$  为卷积运算,  $R_j$  为输入特征图的一个选择,  $A_i^{(l)}$  为第  $(l-1)$  层的第  $i$  个特征图的输出值,  $K_{ij}^{(l)}$  为第  $l$  层的第  $j$  个特征图与第  $(l-1)$  层的第  $i$  个特征图相连的卷积核,  $B_j^{(l)}$  为第  $l$  层的第  $j$  个特征图的偏置。

3) 采样层, 又称为特征映射层, 用于对卷积层所提取的特征进行处理和压缩。它的主要功能是将输入的特征图像按照一定的规则划分成不重叠的子块, 并在每个子块上进行池化操作。通过这种方式, 可以减少数据的维度和规模, 并提取出更具代表性和重要性的特征。采样层的运算帮助网络实现对特征的空间转换和缩放, 同时减少了网络的参数和计算量, 提高了计算效率<sup>[18-19]</sup>。采样层的输出形式为：

$$A_j^{(l)} = \text{down}[A_j^{(l-1)}] \quad (3)$$

式中,  $\text{down}()$  为降采样函数。

4) 全连接层对经过卷积层和采样层处理后的特征进行综合和转换。全连接层通过连接具有权重的多个神经元, 将这些特征映射到输出结果的空间中。其输出形式为：

$$a_j^{(l)} = f\left[\sum_{i=1}^{S_{l-1}} a_i^{(l-1)} W_{ij}^{(l)} + b_j^{(l)}\right] \quad (4)$$

式中,  $a_i^{(l-1)}$  为第  $(l-1)$  层的第  $i$  个神经元节点的输出值。根据上述流程实现人员识别。

### 3.6 WIFI 通信程序设计

本系统采用 TCP 透传的方式实现 WIFI 模块和服务器之间的通信。TCP 协议是智能门禁系统传输层的基础。它是互联网传输数据的核心协议, 具有可靠性和稳定性。TCP (Transmission Control Protocol) 负责在传输过程中进行数据分包、传输、重传等操作, 确保数据的完整性和准确性。WIFI 连接的步骤如下：

1) 重启模块: AT + RST, 返回 OK, 说明模块已重启。

2) 设置工作模式: AT + CWMODE = 1, 指令参数 <mode>: 1-Station 模式; 2-AP 模式; 3-AP + Station 共存模式。

设置 ESP32 的工作模式为 Station 模式 (连接到 WIFI 网络), 在 Station 模式下, ESP32 作为客户端可以连接到一个已有的 WIFI 网络, 使用 AT 指令连接成功之后, ESP32 会获得 IP 地址, 表示已成功连接到 WIFI 网络。

3) 连接 WIFI 热点: AT + CWJAP = "WiFi\_name", "pass\_word", 开启手机热点, 返回 OK, 说明成功连接。

4) 设置透传模式: AT + CIPMODE = 1, 指令参数 <mode>: 0-非透传模式; 1-透传模式。

设置 ESP32 的数据传输格式为透传模式 (Transparent Transmission Mode, TTM), 使其在串口接收数据时, 可以立即将数据通过网络发送给服务器, 避免了数据在 ESP32 上的临时存储和处理, 从而提高数据传输的效率<sup>[20]</sup>。

5) 设置连接模式: AT + CIPMUX = 0, 指令参数: <mode>; 0-单路连接模式; 1-多路连接模式。

ESP32 有多种网络传输模式, 包括单路连接模式 (Single) 和多路连接模式 (Multiple), 本次设计 ESP32 只要与一个服务器建立连接, 所以采用单连接模式, 在 AT 指令下连接到指定的服务器。

6) 建立 TCP 连接: AT + CIPSTART = “TCP”, “IP”, port, 返回 OK 则说明格式正确且连接成功。

7) 发送数据: AT + CIPSEND = <data>, 由于是在透传模式下, 所以无需规定数据长度, 如果数据发送成功, 返回 SEND OK。

至此, ESP32 已连接服务器, 并进入透传模式, 当输入单独一包 “+++” 返回指令模式。

所用到的 AT 指令如表 2 所示。

表 2 AT 指令表

AT 指令	含义
AT+RST	启动 WIFI 模块
AT+CWMODE=<mode>	设置工作模式为 Station
AT+CWJAP=“WiFi_name”, “pass_word”	连接 WIFI 热点
AT+CIPMODE=<mode>	设置透传模式
AT+CIPMUX=<mode>	设置单连接模式
AT+CIPSTART=“TCP”, “IP”, port	设置服务器类型、IP 地址和端口号
AT+CIPSEND=<data>	发送数据

若需要通过小程序控制门禁系统执行相应的功能, 则可通过云服务器向 ESP32 传输特定的字符串, 由 MM32 主控进行判断, 从而调用相应的功能函数, 实际应用如下:

1) 如果接收字符串为 “open”, 则 door\_flag 标志位置 1, 并调用 door\_control () 函数执行开门、发送开门时间等操作;

2) 如果接收字符串为 “saveFace”, 则 save\_flag 标志位置 1, 并调用 load\_proc () 函数执行人脸录用操作;

3) 如果接收字符串为 “checkFace”, 则 check\_flag 标志位置 1, 并调用 detect\_proc () 函数执行人脸识别操作。

### 3.7 微信小程序设计

微信小程序通过微信开发者工具开发, 实现与阿里云服务器的数据交互, 支持用户远程访问和控制门禁系统。用户能实时查看门禁监控数据、开门记录、警报信息, 并远程控制门禁开关、设置密码以及接收可疑人员警报。门禁设备通过 TCP 连接与阿里云服务器通信, 实现实时监控数据的上传和远程控制指令的接收。这包括开门操作、报警响应等。

微信小程序与云端服务器间的数据传输采用 HTTP 协议, 这是一种稳定且广泛使用的应用层协议, 基于请求与响应模式, 利用 URL 定位网络资源, 并通过不同请求方法操作资源。同时, 为了确保数据的简洁、轻量且易于解析,

微信小程序与服务器、WIFI 模块与服务器配网通信时均使用 JSON 格式传输数据。云应用通信设计确保了数据的实时性、安全性和用户操作的便捷性, 为门禁系统的智能化管理提供了有力支持。云应用通信设计如图 12 所示。

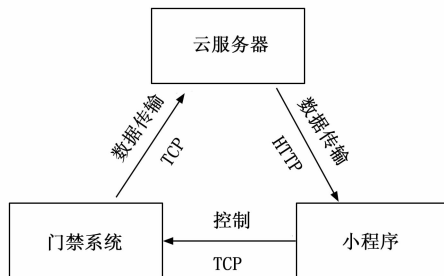


图 12 云应用通信设计图

在门禁系统中, 数据的可视化非常重要, 它可以为用户提供实时信息展示和追踪功能。微信小程序首先会与云平台建立连接, 以确保数据通信的实时性和准确性。一旦连接成功, 小程序便能够实时获取门禁系统的事件记录。无论是有人进出门禁区域, 还是其他任何门禁相关事件, 这些数据都会迅速更新并显示在小程序的界面上。

对于用户而言, 他们可以随时随地通过小程序查看门禁系统的活动记录。这些记录不仅包括了门禁的开关时间, 还涵盖了任何可能的警报事件及其发生时间。这样, 用户能够全面了解门禁系统的运行状态, 确保区域的安全。

在警报触发时, 门禁系统除了记录事件外, 还会拍摄照片作为辅助证据。这些照片将同步至云平台, 并通过微信小程序实时展示给用户。用户只需轻触小程序界面, 即可查看警报发生时的现场照片, 了解事件的具体情况, 从而做出更准确的判断和决策。此外, 微信小程序还提供了远程开锁的功能。当用户需要进入门禁区域时, 只需在小程序中输入正确的密码或进行其他身份验证, 即可远程执行开锁操作。这不仅提高了门禁系统的使用便捷性, 也增强了其安全性和灵活性。

## 4 实验结果与分析

### 4.1 系统运行测试

本文通过对基于 MM32F5270 的智慧门禁系统的硬件和软件设计进行详细分析, 提出了一个全新的智慧门禁系统方案。在该方案中, 通过硬件和软件设计搭建了一个完整的系统。为了验证系统性能, 进行了模拟用户开门和可疑人员报警的检测。

系统的测试步骤如下:

1) 系统上电, 系统程序进入初始化, 包括摄像头程序初始化和 WIFI 联网初始化;

2) 通过 WIFI 模块的 IP 地址使系统与云服务器连接, 检测联网状态是否正常;

3) 测试摄像头模块录入和识别人脸功能是否正常, 检测图片数据是否正常传输;

4) 测试门禁开关是否正常, 显示屏是否正常显示数据, 语音是否正常播报。

经多次实际测试, 摄像头拍摄图像并传输保存至云平台平均用时 3.1 s, 开门平均用时 1.7 s, 数据更新时延平均 0.6 s, 响应速度较快。人脸识别成功率高达 96.67%, 可靠性较高。

### 4.2 数据管理测试

门禁系统通过 WIFI 模块将数据传输到云服务器的数据库中, 并同步更新到微信小程序, 其中包括警报时间、开门时间以及摄像头采集的图像。这些信息的保存和检测非常关键, 可以确保门禁系统的安全性和数据完整性。当系统正常工作时, 查看数据库中时间和图像信息是否实时更新和完整保存。通过检测, 拍摄时间被全部记录, 图像数据在给定的路径 E:\test 下得到了及时完整的保存, 并通过序号 id 进行命名。数据库测试效果如表 3 所示。

表 3 数据库测试过程

id	create_time	path	file_name
1	2023-07-19 16:15:29	E:\test	1.jpg
2	2023-07-19 16:18:50	E:\test	2.jpg
3	2023-07-19 16:21:13	E:\test	3.jpg
4	2023-07-19 16:22:01	E:\test	4.jpg
5	2023-07-19 16:29:29	E:\test	5.jpg
6	2023-07-19 16:33:56	E:\test	6.jpg
7	2023-07-19 16:39:11	E:\test	7.jpg
8	2023-07-19 16:48:06	E:\test	8.jpg
9	2023-07-19 16:53:15	E:\test	9.jpg
10	2023-07-22 18:15:34	E:\test	10.jpg
11	2023-07-22 18:28:10	E:\test	11.jpg
12	2023-07-22 19:47:09	E:\test	12.jpg
13	2023-07-22 19:48:19	E:\test	13.jpg
14	2023-07-22 20:03:45	E:\test	14.jpg



图 13 用户主界面及报警界面

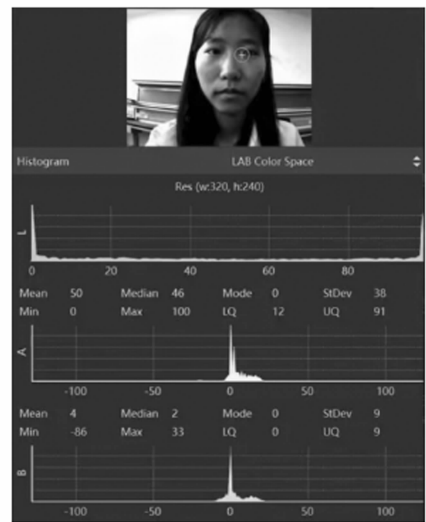


图 14 人脸识别效果图

### 4.3 小程序功能测试

测试小程序输入密码、开门、录入以及识别人脸按钮功能是否正常, 界面开门及报警时间是否实时更新。通过在摄像头前停留 10 s 模拟可疑人员, 检查摄像头是否抓拍图像并实时显示在小程序的报警界面中。经过测试, 小程序功能正常, 数据实时更新。图 13 展示了小程序的主界面以及报警界面, 用户可以通过这些界面直观地了解门禁系统的状态和操作功能。

### 4.4 人脸识别测试

随机选取六位实验人员参与人脸识别实验, 实验前, 提前录入其中两位实验人员人脸作为解锁人脸数据, 实验时, 分别采集六位实验人员人脸并记录其与已录入的两组人脸数据的差异度平均值, 每位实验人员做八组实验, 其中实验人员 1、2 人脸已提前录入。差异度平均值越小, 表明该人脸与已录入人脸越近似, 根据实验数据, 选取差异度阈值为 5 800, 则筛选效果较为理想。图 14 为人脸识别效果图。不同人脸对于 1、2 人脸的差异度如表 4 所示。

表 4 人脸差异度测试

人脸		差异度							
实验人脸 1	1	3 189	3 841	3 462	4 305	5 011	5 196	4 007	3 273
	2	7 891	7 675	7 598	6 991	6 965	7 249	7 690	7 611
实验人脸 2	1	7 689	7 416	6 948	7 457	7 479	7 570	7 422	7 644
	2	4 406	5 587	5 550	4 368	4 056	3 946	4 046	4 035
实验人脸 3	1	8 716	8 710	8 675	8 744	8 878	8 847	8 715	8 828
	2	10 363	10 263	10 382	10 308	10 349	10 325	10 195	10 269
实验人脸 4	1	7 924	7 897	7 890	7 703	7 711	7 733	7 851	7 709
	2	8 216	8 140	8 094	8 170	8 169	8 074	8 088	8 086
实验人脸 5	1	7 960	7 873	7 885	7 927	8 144	8 110	8 542	8 723
	2	9 123	9 118	9 079	9 170	9 515	9 828	10 596	10 849
实验人脸 6	1	7 713	7 756	7 635	7 770	7 880	7 628	7 732	7 819
	2	9 090	9 055	8 973	9 030	9 003	9 007	8 989	8 999

通过测试, 除了实验人脸 1 和实验人脸 2 与自身的差异值低于阈值, 其他实验人脸均高于阈值, 达到测试期望, 人脸识别安全可靠。

## 5 结束语

本文设计并开发了一种基于 MM32F5270 的智慧门禁系统, 借助 ESP32 无线 WIFI 模块和 OpenMV 摄像头模块, 智能门禁系统实现了远程监控和控制功能。用户可以通过 WIFI 模块连接至服务器, 从而控制小程序显示以及云平台的移动设备, 通过摄像头采集的图像数据实时监视门禁系统的状态和活动, 并能根据警报实时上报的时间迅速采取必要的行动。这种便利性使得门禁系统的安全性和可管理性得到了大幅提升。突破了传统门禁系统通常只基于本地服务器或控制器进行管理的局限。在后续的工作中, 我们将继续优化和完善该系统, 增加智慧门禁系统的人机交互功能, 更好地优化摄像头的算法性能, 使用户界面功能多元化, 追踪和识别更加快速高效。

### 参考文献:

- [1] 杨晶晶. 基于 STM32 的智能门禁系统的设计 [D]. 唐山: 华北理工大学, 2020.
- [2] 宋天慧, 曾建, 钱进, 等. 基于单片机的智能家庭门禁系统的设计 [J]. 电脑知识与技术, 2023, 19 (7): 98-101.
- [3] 郭伟洁, 植凯吉, 白珞皓, 等. 基于身份证和人脸双重识别技术的智能门禁系统设计 [J]. 计算机测量与控制, 2021, 29 (2): 222-228.
- [4] VALENTINE N H, AKAERUE E I, ETIDO M G, et al. A 3-factor authentication access control system using RFID, fingerprint, token and code [J]. Multimedia Tools and Applications, 2024, 83 (15): 43635-43647.
- [5] QUOC D L, TRAN T C V, TUONG Q. Application of 3D face recognition in the access control system [J]. Robotica: International Journal of Information, Education and Research in Robotics and Artificial Intelligence, 2022, 40 (7): 2449-2467.
- [6] YANG Y. Design and implementation of student information management system based on springboot [J]. Advances in Computer, Signals and Systems, 2022, 6 (6): 21-25.
- [7] 董振华, 何森. 基于 OpenMV 的行人检测系统 [J]. 科学技术创新, 2023 (24): 92-95.

(上接第 271 页)

- [19] 许延龙, 潘昊, 丁柏圆. 基于深度信念网络的属性散射中心匹配及在 SAR 图像目标识别中的应用 [J]. 液晶与显示, 2023, 38 (11): 1511-1520.
- [20] TASKIRAN M, KAHRAMAN N, ERDEM C E. Face recognition: past, present and future (a review) [J]. Digital Signal Processing, 2020, 106: 102809.
- [21] LIAO W H. Region description using extended local ternary patterns [C] //International Conference On Pattern Recognition, 2010: 1003-1006.
- [22] WANG M, DENG W. Deep face recognition: a survey [J]. Neurocomputing, 2021, 429: 215-244.
- [23] 步一凡, 王晓玲, 贺珂珂, 等. 面向身份相互关系一致性的人脸去识别化方法 [J]. 华东师范大学学报 (自然科学版),

- [8] YONG G, JUN Y, YU W, et al. Research and implementation of an OpenMV-based target edge detection and tracking system [J]. Journal of Physics: Conference Series, 2022, 2173 (1): 1-7.
- [9] 闫磊, 王萌, 朱焯繁. 双目视觉云台模糊自适应 PID 跟踪控制 [J]. 控制工程, 2022, 29 (11): 2003-2009.
- [10] 李光镐. 基于卷积神经网络的人脸识别系统研究与应用 [D]. 兰州: 兰州理工大学, 2021.
- [11] 朱兆丰, 刘静琦, 周振虎, 等. 基于 STM32 的室内环境监测系统设计 [J]. 物联网技术, 2021, 11 (6): 6-9.
- [12] 廖玥灵, 马敏耀, 令狐蓉, 等. 基于面部识别的新型智能门禁系统设计与实现 [J]. 无线互联科技, 2022, 19 (20): 49-51.
- [13] LAI X, RAU P L P. Has facial recognition technology been misused? A user perception model of facial recognition scenarios [J]. Computers in Human Behavior, 2021, 124: 106894.
- [14] 包虹璐. 网络通信中嵌入式 TCP/IP 协议单片机技术运用分析 [J]. 科技资讯, 2023, 21 (18): 48-51.
- [15] 朱扬, 杨延宁, 董晨乐, 等. 基于 STM32F103C8T6 的游乐场智能手环设计 [J/OL]. 计算机测量与控制, 1-13 [2024-03-15]. <http://kns.cnki.net/kcms/detail/11.4762.TP.20240119.1704.018.html>.
- [16] WANG F, WANG Z, CHANG K, et al. New multifunctional industrial wireless network adapter [J]. Energy Procedia, 2017, 118: 95-103.
- [17] 屈晓, 周挺, 吴楷, 等. 一种 SpringBoot 基于嵌入式设备的辅助医疗 App 的设计与实现 [J]. 电脑知识与技术, 2023, 19 (29): 55-58.
- [18] 黄赛英. 基于 Springboot 的医院档案管理系统设计 [J]. 集成电路应用, 2023, 40 (11): 384-385.
- [19] CRUZ D A M, RODRIGUES J J, LORENZ P, et al. A proposal for bridging application layer protocols to HTTP on IoT solutions [J]. Future Generation Computer Systems, 2019, 97: 145-152.
- [20] 高静, 段会川. 基于移动设备的 JSON 数据传输效率研究 [J]. 信息技术与信息化, 2011 (1): 13-16.
- [21] 高静, 段会川. 基于移动设备的 JSON 数据传输效率研究 [J]. 信息技术与信息化, 2023 (6): 49-60.
- [24] 龙慧, 张雅璐, 罗觉灵, 等. 基于 FaceNet 网络的口罩人脸识别别人流监测系统 [J]. 现代电子技术, 2023, 46 (19): 65-69.
- [25] 高锦凤, 陈玉, 魏永明, 等. 基于改进的 YOLOv3 和 Facenet 的无人机影像人脸识别 [J]. 中国科学院大学学报, 2023, 40 (1): 93-100.
- [26] TAN M, LE Q. Efficientnet: Rethinking model scaling networks for convolutional neural networks [C] //International Conference on Machine Learning, 2019: 6105-6114.
- [27] 祁春阳, 黄杰, 赵翔宇, 等. 云边协同的轻量级网络结构人脸识别方法 [J]. 东南大学学报 (自然科学版), 2023, 53 (1): 1-13.