文章编号:1671-4598(2021)02-0222-07 DOI:10.16526/j.cnki.11—4762/tp.2021.02.043 中图分类号:TP520.60 文献标识码:B

基于身份证和人脸双重识别技术的智能门禁系统设计

郭伟洁，植凯吉，白瑀皓，王 兴
（太原科技大学 计算机科学与技术学院，太原 030024）

摘要：针对智能门禁系统实名制管理及安全性问题，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；经实验结果表明，该智能门禁系统可实现网络化管理以及实名化开锁，可以应用于门禁系统、政府公租房、长短租公寓、民宿网约房、家庭联网门锁、写字楼等多领域。

关键词：门禁系统；身份证；人脸识别；射频识别；电子锁

Design of Intelligent Access Control System Based on ID Card and Face Dual Recognition Technology

Guo Weijie, Zhi Kaiji, Bai Yuhao, Wang Xing
(College of Computer Science and Technology, Taiyuan University of Science and Technology, Taiyuan 030024, China)

Abstract: Aiming at the real name management and security problems of intelligent access control system, an intelligent access control system based on ID card and face dual recognition technology is designed. Face recognition is realized by width learning convolution neural network algorithm, The communication instruction of intelligent access control system is designed. The experimental results show that the intelligent access control system can realize network management and real name unlocking, and can be applied to the access control system, government public rental housing, long and short rent apartments, home accommodation network, home network door locks, office buildings and other fields.

Keywords: access control system; ID card; face recognition; RFID (radio frequency identification); electronic lock

0 引言

伴随着科学技术的不断发展，智能门禁系统作为安全防护领域不可或缺的一个组成部分，工厂、酒店、小区等领域已经广泛应用。而市场是保障出入口安全防范管理的有效解决方式，因而得到人们越来越广泛的关注。当前智能门禁系统在一些生活场景上大多数的解锁方式安全性较低、不易管理，且无法实现实名制管理。针对该问题，研究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，利用身份证的唯一性、权威性、安全性以及可存储性等特点，采用RFID射频识别技术实现实名制开锁。通过宽度学习卷积神经网络算法，对人脸进行图像识别特征值的采集，解决人脸识别过程中的快速跟踪和快速识别问题。研制后台云管理系统，实现远程无线监控管理。此智能门禁系统可自动完成人员身份识别，随时记录各类人员的出入情况并进行图像监控，有效地保护控制区域内各项财产不受非法侵犯，并对异常情况进行报警处理。用户可采用密码、身份证、人脸识别、机械钥匙应急开锁、APP临时密码下发等多种开锁方式。

1 智能门禁系统设计方案

1.1 智能门禁系统工作原理

系统在设计上，主要由系统服务端、门禁管理服务端、电子锁等组成，其中电子锁为核心部分，由门锁、身份证阅读器、门禁控制器、网络摄像头、蜂鸣器及备用电源等组成。而门禁控制器主要实现身份证信息的读取、人脸识

收稿日期:2020-12-02； 修回日期:2021-01-06。
基金项目:国家自然科学基金面上项目(41372350);山西省高等学校大学生创新创业训练计划项目(2020342);太原科技大学大学生创新创业训练项目(XJ2020167)。
作者简介:郭伟洁(1999-),女,山西省襄垣县人,大学本科,主要从事物联网工程方向的研究。
王 兴(1981-),男,山西省太原市人,博士研究生,副教授,主要从事物联网工程,计算机技术方向的研究。
引用格式:郭伟洁,植凯吉,白瑀皓,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.

别、报警处理以及开门处理。该门禁系统由身份识别单元部分、处理与控制单元部分、电子锁与执行单元部分、传感与报警单元部分、线路及通讯单元部分、管理与设置单元部分组成。系统工作原理如图 1 所示。

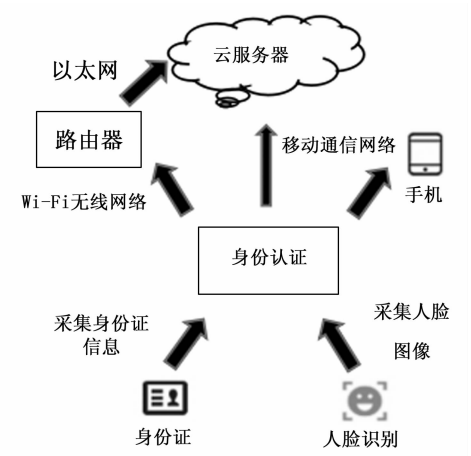

图 1　系统工作原理示意图

针对不同的应用场景可采取不同的认证方式，在较为固定的场所，可将用户的人脸信息提前录入，进行人脸识别从而加快通过效率。而对于用户不固定、流动性较大的场所则采用身份证和人脸双重识别。双重识别一方面可有效提高用户的通过效率，另一方面可实现系统的实名制管理，有效地解决了常规门禁系统的安全性问题。在对用户进行身份证识别的过程中，识别成功则进行开门处理，显示错误信息该系统则会自动进行报警处理。而在人脸识别的过程中，识别成功进行开门处理，若识别失败将进行身份证识别，最终若任然显示错误信息则进行报警处理。软件主程序流程如图 2 所示。

1.2　门禁系统工作流程

该门禁系统体系结构总体划分为感知层、接入层、应用层、平台层、基础设施层共 5 个层次。1）感知层可实现门禁系统的控制以及摄像头的监控管理；2）接入层可使用 WiFi、蓝牙、3G/4G/5G 等方式实现无线连接；3）应用层是面向功能的一个平台，在本系统中主要是通过 INTERNET 实现门禁系统管理端与手机客户端连接。从而使管理员实现远程后台管理，如权限管理、用户管理、区域管理、安全管理、后台审核、系统监控等；4）平台层是应用层与基础设施层之间的桥梁，是为服务提供开发、运行和管控环境的一个中间件功能层次。它利用基础设施层的能力面向上层应用提供服务，基于基础设施层的资源管理能力提供一个高可用、可伸缩且易于管理的与中间件平台；5）基础设施层则主要解决资源的虚拟化和自动化管理问题，将经过虚拟化的计算资源、存储资源和网络资源以基础设施的方式通过网络提供给用户使用和管理。智能门禁系统体系结构如图 3 所示。实际实验效果如图 4 所示。

1.3　管理端设计

该门禁系统对管理员进行权限分配，实现多级管理。

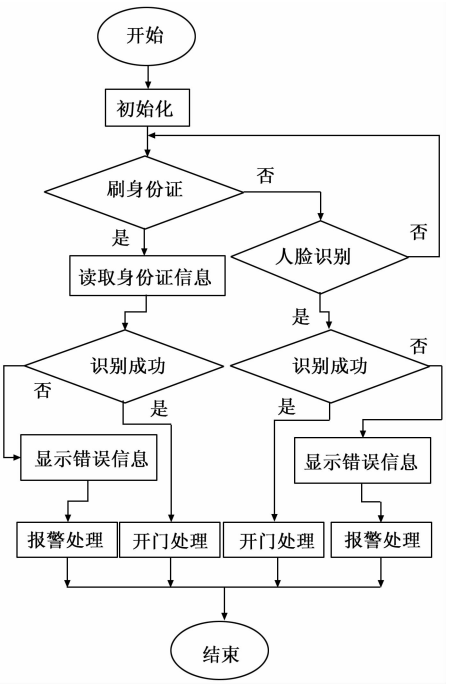

图 2　软件主程序流程

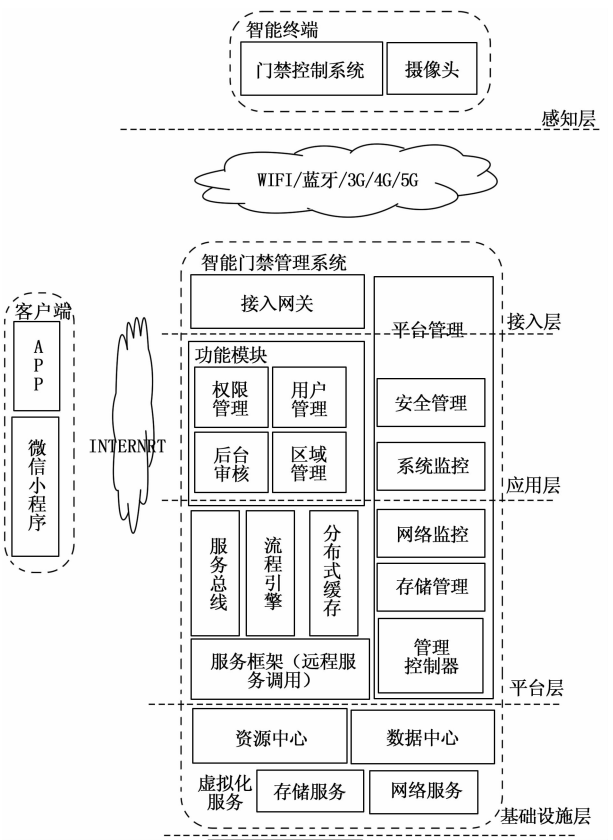

图 3　智能门禁系统体系结构

用户无需自建平台，通过 Web 即可访问云平台，登录管理员账号实现对门禁、人员信息等的统一管理，降低用户成本。

智能门锁相关参数如下：

(a) 整体外观 (b) 人脸识别 (c) 身份证识别

图 4 实际实验效果照片

1) 智能门禁控制器相关参数配置，系统初始化时，控制主板会逐一检查网络模块、RFID 读写器工作、安全模块供电参数（3.3 V/5 V）←（是否正常，若不正常，发出低电压警报）。网络模块初始化，配置 SSL 的秘钥及公钥。使用 https 通信（wifi：连接 AP 自动输入 密码连接 AP 连通网络；有线网络：查询路由器是否正常，其次由路由器分配网络 ip，连接 tcp 服务器或者直接连接服务器。ping 通后，建立心跳包 保持长久连接 及实现网络通讯。由路由器配置 ip 地址 * * . * * . * * . * * 服务器访问端口为 8 080。网络请求参数初始化 Lockld = RO014&type = 1&content = ORDER

Lockld：控制器唯一 id type：网络获取命令类型 content：请求内容

所有网络请求均以这请求格式和请求参数。系统复位断开所有的逻辑线路，完全重新连接逻辑线路初始化相同（硬件复位）。

网络初始化成功后会获取服务器系统时间保证门禁控制器时钟与服务器同步。

2) 智能门禁控制器输Ⅳ输出端口的设置，控制器的串口配置网络模块。单片机与网络模块由串口通信。

当从服务器收到 * * * 信息时开启（继电器）电机实现开锁、关锁。

互锁条件：低压警告、主动锁定、设备强破互锁。

3) 人员属性信息的配置，如用户身份证的效期、合法性、权限以及用户所属时段等。

2 身份识别设计

2.1 身份证识别模块

2.1.1 RFID 技术

RFID 是一种利用射频信号的空间耦合实现无接触信息传输并通过所传输的信息进行目标识别的自动识别技术，是本门禁系统的核心技术之一。身份证识别电子标签是近距离识别，即使用耦合方式进行无线传输信息。该门禁系统的 RFID 模块主要由身份证、身份证读写设备以及管理系统组成。读取个人身份信息的设备将自动读取刷卡人身份证信息，并将采集到的信息上传至门禁控制板。门禁控制设备安装于电子锁门附近，用来接收用户身份证信息和后台管理端的指令并执行，对用户身份证信息鉴权是否开门，存储刷卡人记录，上报主机用户信息。系统服务端用作控制门禁控制板，实时监控用户身份证信息，同时也可以依照用户的不同要求设置好门禁权限等开门的相关参数设置，如果需要查看进出门记录时也可以选择连接本系统的后台服务端。

2.1.2 身份证识别防碰撞算法

本门禁系统的 RFID 系统由身份证、身份证信息处理器和电子锁管理系统共同组成。FID 读写器正常情况下，一个时间点只能对磁场中的一张 RFID 卡进行读写操作，但在实际应用场景中经常有多张身份证同时进入读写器的射频场，导致一个读写器多个应答器，无法正确识别出一个应答器的情况，即产生碰撞现象，出现通信方面的冲突产生碰撞导致传输失败，致使门禁系统无法正常工作。为此，必须采用防碰撞算法来防止碰撞的产生。

门禁系统使用二进制树防碰撞算法来有效解决多张身份证识别过程中的碰撞问题，该算法基于树分叉搜索算法实现，目的在于从多个电子标签中筛选出所需电子标签。

二进制树型搜索算法核心原理为把会发生碰撞的电子标签进行逐次的划分，不断地缩将要识别的数量范围，最终达到仅剩唯一一个回应的情况。识别方式是阅读器向作用区域内所有电子标签发送带有某一限制条件的询问命令，所有符合条件的电子标签进行响应并向阅读器返回信息，若相应不唯一则发生了碰撞。阅读器分析所有符合条件的电子标签的返回信息，若发生碰撞，则检测所有碰撞位置，并根据返回信息修改限制条件，再次发送询问命令。重复发送询问命令，重复进行识别过程，直至有且唯一有一个电子标签进行响应，既无碰撞发生。

在该算法的使用中，需要阅读器能够检测出所有碰撞的比特的确切位置，而 Manchester 编码刚好能做到这点，若多个电子标签同一时间发送不同的数位，即收到的上升沿和下降沿将会互相抵消，不发生变化的情况不允许发生，否则会被作为错误信号。采用此方式可以依照位来追踪到冲突的发生。所以在二进制搜索算法中选用 Manchester 编码，如图 5 所示。

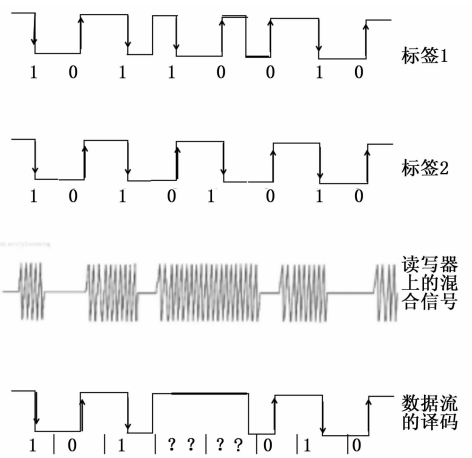

图 5 Manchester 编码

通过二进制搜索算法识别 X 个电子标签所用的次数与编码值和标签间发生碰撞的位置均相关。最少的搜索次数

为 $2X-1$，最多的搜索次数为 $2X+1$，即搜索次数 Y 满足如式（1）所示：

$$2X-1 \leqslant Y \leqslant 2X+1 \tag{1}$$

而平均次数 M 与读写器作用区域内电子标签总数 N 相关如式（2）所示：

$$M(N)=N+1 \tag{2}$$

假设算法执行效率为 α，在算法执行过程中，一共 Ln 个时隙，识别 n 个应答器。

表示算法的执行效率。因此二进制树防碰撞算法可以在短时间内有效解决多张身份证进入一个身份证阅读器导致碰撞的问题。

算法流程如下：

1）把位于冲突电子标签拆分为两不部分用 0 和 1 表示。

2）先对 0 进行检查，如果没有出现冲突情况，就将其标记为正确情况，如果出现冲突情况就进行再划分，将 0 划分为 00 以及 01。

3）依次类推，通过此种算法即可查询出 0 的所有情况，然后按照上述的步骤检查 1。

模型图如图 6 所示。

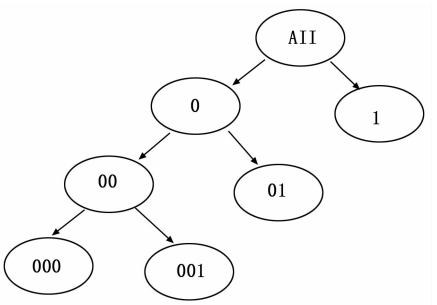

图 6　算法模型图

2.2　人脸识别模块

卷积神经网络拥有良好的图像识别能力，通过权值共享来训练神经网络。同时，其采用的算法不同于普通人工神经网络，故在图像识别方面，卷积神经网络相比于其他人工神经网络正确率明显高出许多。卷积神经网络采用池化操作进行特征提取，由于池化具有平移不变性，所以可以最大限度保留图像特征，同时降低了计算量。

本系统采用一种基于卷积神经网络的学习系统，对被测人的姿势、神态和背景环境等因素不敏感，而且该模型训练时间短、计算量小，不需要大量的训练数据便可以达到较高的识别精度。对人脸图像的处理中，卷积的操作本质上是一种滤波操作，定义以下参数：$\boldsymbol{W}$ 为权重，p 为偏置，h 代表激活函数则在数字图像处理中所用到的离散卷积公式如式（3）所示：

$$y_n m = g\left(\sum_{j=0}^{J-1}\sum_{i=0}^{I-1} X_{m+i,n+j}\boldsymbol{W}_{ij}+b\right)$$
$$(0 \leqslant m < M, 0 \leqslant n < N) \tag{3}$$

卷积原理如图 7 所示。

卷积操作完成后，对图像新提取的特征进行池化操作，其目的在于对卷积提取的图像特征进行降维操作，使得特征精简化，有助于获得更优秀的性能，图 8 为最大值池化及其结果，池化尺寸为 2×2，步长为 2。

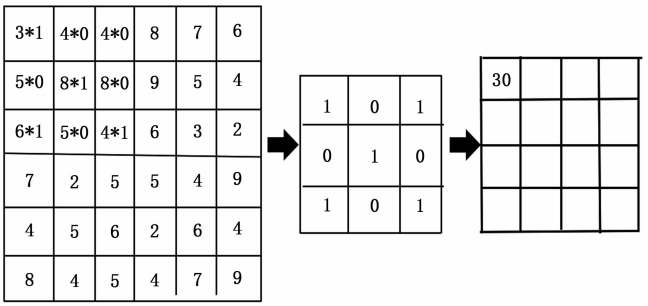

图 7　卷积原理图

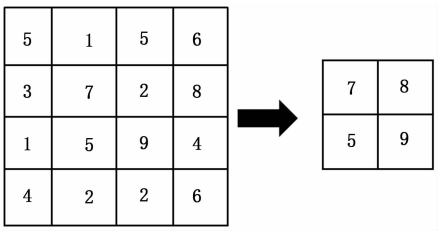

图 8　最大池化及其结果

在人脸识别处理过程中，对人脸图像进行描述的方式一般为提取图像特征点，但每个特征点又需要描述该特征点的 128 维的向量，就导致一幅人脸识别图像中特征点所需的存储量过于大，所以要对人脸图像进行降维操作。降低原始输入维度，其中一种方式是最小化输入 x 和它的重构 $r(x)$ 之间的距离，如式（4）、（5）所示：

$$\boldsymbol{W}^* = \arg\min_{w}\sqrt{\sum_{i,j}(x_j{}^i - r(x^i)_j)^2} \tag{4}$$

$$\text{s.t.}\,\boldsymbol{W}^T\boldsymbol{W}=D, \tag{5}$$

其中：$r(x)=\boldsymbol{W}\boldsymbol{W}^T X$，$i$ 表示第 i 个样本，j 表示第 j 个特征，主成分由 $X^T X$ 的特征向量给出，所以得出公式（6）：

$$X^T X = \boldsymbol{W}\Lambda\boldsymbol{W}^T$$
$$\boldsymbol{W}=[\omega_1,\cdots,\omega_n]$$
$$\Lambda=\begin{bmatrix}\lambda_1 & 0 & 0\\ 0 & \vdots & 0\\ 0 & 0 & \lambda_n\end{bmatrix},\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n \geqslant 0 \tag{6}$$

其中：ω_1 表示第 k 个主成分，λ_k 则表示对应 ω_k 的相关度，通过计算输入数据所占的百分比 l 来确定 k 如式（7）所示：

$$l=\frac{\sum_{i=1}^{k}\lambda_i}{\sum_{i=1}^{n}\lambda_i} \tag{7}$$

系统学习的正交和线性变换矩阵 $\boldsymbol{W}$ 将输入数据 x 的投影结果用 z 来表示。因此，采用 PCA 算法作为降维方法，尽可能地保留数据中的信息。采用岭回归方法，通过求最小值，进而求出网络的输出层权重如式（8）所示：

$$\boldsymbol{W}^* = \arg\min_{w}\| X\boldsymbol{W}-Y\|_2{}^2+\gamma\|\boldsymbol{W}\|_2^2 \tag{8}$$

其中：γ 表示对输出层权重 $\boldsymbol{W}$ 平方和的约束．当 $\gamma=0$ 时，则该问题变为最小二乘法问题，若 $\gamma\to\infty$，那么权重则近似为零．故可得出权重的计算公式如式（9）所示：

$$\boldsymbol{W}=(\gamma D+XX^T)^{-1}X^TY \tag{9}$$

本文基于卷积神经网络宽度学习系统，输入图像通过宽度学习系统方法映射到特征向量 x 中，同时采用 PCA 来学习映射矩阵。而后利用输入图像映射，采取卷积与最大池化操作提取增强神经节点。将 PCA 应用于合并后的特征图，提取增强特征。多次重复此过程，可以得到更深层次的特征。本文采用随机生成的卷积核与最大池化操作，通过岭回归方法更新权重 $\boldsymbol{W}$。

2.3 异常情况报警处理

当门禁控制器检测到异常情况时，如被检测用户身份异常、强制开门、门禁控制器或读写器防拆除线断开等，则会发出警报信号并上传管理端。门禁报警系统还会对身份证的合法性、权限、时段、有效期、是否为挂失卡等进行判断，只有符合条件的身份证才会开门，同时会将有关信息记录在后台的管理系统。

将安装门磁或探测器。一旦门被异常打开时，探测器或门磁探测到动作，立即立即输出信号产生报警，联动报警设备或现场警号，并在总站管理系统上会有明显显示所在各门锁的报警信息。

3 系统通信及命令设计

3.1 通信方式

本系统采用 5G Wi－Fi 通信，传统无线路由器只有 2.4 G频段的 WIFI 信号，因为目前大多数设备多使用 2.4 G 频段，用户较多时，干扰较大，不能保障足够的稳定性，会直接影响该系统之间的通信。5G 作为即将普及的新一代无线通信技术，具有高带宽、高可靠、低时延等优点，5G Wi－Fi 信号频带宽、无线环境干净、干扰少、网速稳定、能够保障传输质量，将其用于该系统能够让通信性能提高。

3.2 通信协议

超文本传输协议 HTTP 是互联网上使用最为广泛的一种网络协议，具有通信开销小、简单快速、成本低、使用灵活、节省传输时间等优点，但是传输的数据都是明文传输的，未加密，因此采用 HTTP 协议传输信息容易被监听、被伪装、被篡改，为了保证传输信息的安全性，本系统采用由网景公司设计的 SSL（Secure Sockets Later）协议用于对 HTTP 协议传输的数据进行加密，也就是使用 HTTPS 协议，该协议能够让信息加密，防监听、防伪装、防篡改，提高了本系统信息传递过程的安全性。该门禁系统通信原理如图 9 所示。

3.3 服务端配置

3.3.1 服务器系统配置

本系统根据所需要的程序、数据库类型、性能好坏、操作熟悉的程度等情况采取了一般电脑普遍采用的 Windows 系统。为了承载更多锁并发请求，拟采用服务器 CPU

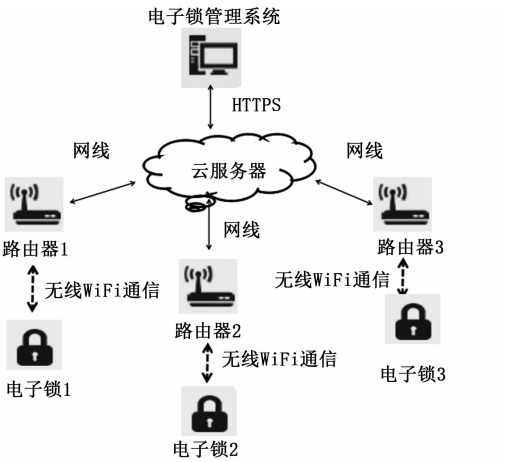

图 9 门禁系统通信原理图

芯数 4 核、4 g 内存、500 G 硬盘，10 Mbps 带宽，这样的服务器配置可容纳并发量是 500，完全可以解决锁并发请求问题。

3.3.2 服务器环境配置

本系统选择 wed 服务器，在所选操作系统安装云服务器之后，根据本系统的需求配置所需的运行环境，对 Tomcat、mysql 等进行安装与配置。

3.3.3 服务器 HTTPS 访问设计

对 HTTPS 访问请求进行设计，利用系统的 ip 地址 73.28.81.45 和采用的端口号 433 设计 URL 为：https：//73.28.81.45：433/网页的相对路径，具体实例如下：https：//94.45.27.46：443/eletronicLock/index.htm。

为访问请求设计 3 个请求参数，lockid 用来表示锁的 ID 号，type 用来表示请求的类型，content 用来表示请求的内容，例子如下：

lockid＝L0001&type＝1&content＝ORDER

电子锁功能指令集如表 1 所示。

表 1 电子锁功能指令集

序号	指令名称	功能码	目标端
1	设置管理员开锁身份证号	A	电子锁
2	设置管理员开锁密码	B	电子锁
3	设置入住人员开锁身份证号、开锁密码、入住时间	C	电子锁
4	取消管理员开锁信息	D	电子锁
5	取消入住人员开锁信息	E	电子锁
6	网络连接恢复出厂设置	1	电子锁
7	远程开锁	2	电子锁
8	远程屏蔽信息	3	电子锁
9	解除远程屏蔽	4	电子锁
10	发送电子锁开锁信息	5	服务器
11	发送低电量报警	6	服务器
12	发送错误代码	7	服务器
13	.....		

具体服务器端访问设计如表 2 所示。

3.3.4　命令说明

（1）获取命令

https：//ip：port/lock/index.htm? type = 1&id = L0001&content=ORDER

命令信息帧格式如表 3 所示。

说明：返回字符串，按顺序执行。

＋命令数目＋命令 1｜命令 2｜命令 3｜.....　｜命令 n＋@返回的例子：00510000001L0001A510183199911032222X00000000000000｜10000002L0001 B000000000000000000012345600000000｜10000003L00011000｜10000004L00012000

该字符串说明如表 4 所示。

表 2　请求及参数说明表

请求类型	参数说明	备注
获取命令	type:1 id:锁号(例如:L0001) content:ORDER	获取当前电子锁接收到的还未执行的命令,返回多条结果
命令写回	type:2 id:锁号(例如:L0001) content:执行成功的命令 id(例如:10000001)	执行成功的命令 id 为获取命令中的命令 id
开门日志	type:3 id:锁号(例如:L0001) content:开门情况 0＋密码或 1＋身份证(例如:0654321 或 151018319991103222X)	通过两种获取指定锁号电子锁的开门情况,0 表示用密码开锁,1 表示用身份证开锁
低电压报警	type:4 id:锁号(例如:L0001) content:LOWVATTERY	获取电子锁的带点状态,LOWVATTERY 表示低电量

表 3　命令信息帧格式

	长度/Byte	说明
起始字符	1	用 1 个“$”字符表示
总命令数量	3	表示获取到的总的命令数量
命令 id	8	表示需要执行的命令的 id 号
锁号	5	表示需要执行命令的锁号
功能码	1	表示该锁需要执行的功能
数据信息	101 或 0	表示命令数据信息内容
空余字节	3	用于冗余
结束字符	1	用 1 个“@”字符表示

（2）命令写回：

https：//ip：port/lock/index.htm? type = 2&id = L0001&content=10000001

说明：写回成功执行的命令，返回错误码。

（3）开门日志：https：//ip：port/lock/index.htm? type=3&id=L0001&content=0654321（0＋密码方式）https：//ip：port/lock/index.htm? type = 3&id = L0001&content=151018319991103222X（1＋身份证号方式）

说明：获得对应电子锁的开门情况，无返回值。

（4）低电量警报：https：//ip：port/lock/index.htm? type=4&id=L0001&comtent=LOWVATTERY

说明：对应锁已低电压，报警，无返回值。

表 4　命令示例说明

字符	格式	命令解读
$		起始字符 $
004	3 位十进制数	当前未执行的命令数目为 4
10000001L0001A510183199911032222X00000000000000	命令 id＋锁 id 号＋功能码＋身份证号＋000000＋00000＋000	执行命令 10000001,对锁号为 L0001 的锁设置管理员开锁身份证号
10000002L0001B000000000000000000012345600000000	命令 id＋锁 id 号＋功能码＋身份证号＋000000＋00000＋000	执行命令 10000002,对锁号为 L0001 的锁设置管理员开锁密码
10000003L00011000	命令 id＋锁 id 号＋功能码＋000	执行命令 10000003,对锁号为 L0001 的锁网络连接恢复出厂设置
10000004L00012000	命令 id＋锁 id 号＋功能码＋000	执行命令 10000004,对锁号为 L0001 的锁远程开锁
@		结束字符@

4　调度方法设计

门禁系统作为一种实时系统，要求在一定的时间范围内确保最后结果的可靠性和准确性，而调度算法的设计对整个门禁系统的性能来说起着至关重要的作用，它决定着在多任务环境下任务执行的顺序以及获得 CPU 资源后能够执行的时间长度。根据不同的优先级分配方法，基于优先级的调度算法可分为静态优先级调度算法和动态优先级算法。静态调度较简单但缺乏灵活性，不利于系统扩展；动态调度有足够的灵活性处理系统的变化，但需要消耗更多的资源。但不论是静态调度还是动态调度系统都将优先执行优先级别比较高的任务。如果在进行基于优先级的调度时只按照优先级别的高低进行处理，则会存在突发高优先级的情况，这样低优先级的任务则会等待很长时间。

所以本文提出一种基于优先级的周期性多任务调度算法，对门禁系统中处于不同优先级的任务选取恰当的时间片作为周期，以相应固定的时间片为一个基本单位从而进行周期性的调度，通过这种调度方法既可以保证实时响应性能，也可以使处于较低优先级的任务有机会尽快执行，

从而提高了实时多任务系统的整体控制性能，保障整个门禁系统的实时性要求。

当用户接收到请求时，通过网络发送至缓冲队列当中，进而分类器对其进行分类并划分好优先级，最终由解调器进行整体的调度。具体的工作原理如图 10 所示。

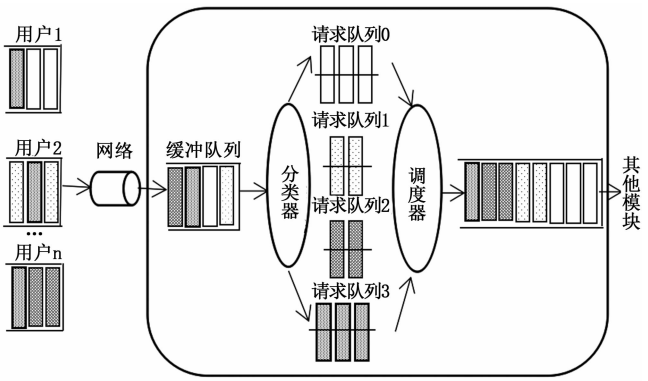

图 10 周期性调度算法

在周期性多任务调度算法中，多个任务的优先级是不同的，将会按照所划分的时间片周期性的对这多个任务进行调度。通过周期性多任务调度算法可以有效地使低优先级的任务得到尽快执行的机会，缩短了执行过程中的延迟时间，提高了低优先级任务的执行效率，从而保障了整个门禁系统控制的有效性。

5 实验结果与分析

本系统对人脸识别模块进行了测试，验证不同条件下人脸识别功能的识别率。

在人脸有遮挡的测试中，选取 30 名同学进行实时人脸遮挡测试，分别遮挡眼睛与下巴，每个人检测 5 次（每遮挡眼睛一次和下巴一次，同时检测到面部并保持 3 s 记作一次有效检测），测试结果如表 5 所示。

表 5 人脸遮挡测试结果

	眼睛遮挡	下巴遮挡
测试次数	150	150
测试时间/s	0.65～0.91	0.55～0.81
误检次数	5	3
误检率/%	5	3

对上述实验结果分析可知，本文所设计智能门禁系统的人脸识别功能可以对绝大部分侧脸和遮挡人脸正确验证，在识别时间上可以控制到 0.5～1 s 之间，速度快且精度高，契合门禁系统的安全性与高效性需求。

同时通过实物操作，对本系统的通信与调度方法进行了测试，验证指令类型与运行状态如图 11 所示。

对各指令进行了依次验证，同时本系统测试过程中系统通信正常，验证了本系统的可行性，符合门禁系统所需的通信高效性与稳定性。

图 11 验证指令类型与运行状态

6 结束语

本文设计了一种智能门禁系统，利用 RFID 射频识别技术，可实现对身份证个人信息采集，从而有效地解决身份证刷卡开锁的问题，并结合宽度卷积神经网络算法，对人脸进行图像识别特征值的采集，解决人脸识别过程中的快速跟踪和快速识别问题，实现双重认证实名制开锁。通过构建物联网电子锁云管理平台，可实现远程无线对电子锁的网络化管理，可连接手机 APP、微信小程序、公安系统等。提出一种基于优先级的周期性多任务调度算法，有效的提高实时多任务系统的整体控制性能，切实保障整个门禁系统的实时性。最终实验结果表明，该智能门禁系统可实现网络化管理以及实名化开锁，并广泛应用于银行、酒店、公寓以及校园等多领域应用。

参考文献：

[1] 王 兴，宋 琦，杨 帆，等. 疫情下的智能身份识别及消毒预警门禁系统研究 [J]. 测试技术学报，2020，34 (5)：425－430.

[2] 王 兴，侯礼宁，白 雪. 基于 RFID 技术的身份证识别门禁系统开发 [J]. 高技术通讯，2019，29 (6)：539－545.

[3] 程玉娟，姚健东，王宜怀. 基于二代身份证的 RFID 门禁考勤系统 [J]. 计算机应用与软件，2011，28 (3)：44－46.

[4] 付志梅，智能云门禁系统的设计与实现 [D]. 南昌：南昌大学，2019.

[5] 陆 璐，物联网中 RFID 智能门禁系统研究 [J]. 信息技术，2013，37 (7)：87－90.

[6] 焦双健，王志远. 卷积神经网络的人脸识别门禁系统设计 [J]. 新器件新技术，2020：47－50.

[7] 王俊昌，王 振，付 雄. 基于无锁数据结构的 FIFO 队列算法 [J]. 计算机工程，2018，44 (8)：315－320.

[8] 孙 伟，刘晓敏，王浩宇，等. 基于三重人脸识别身份验证的门禁管理系统设计 [J]. 计算机测量与控制，2016，24 (2)：225－227.