(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 212256412 U
(45)授权公告日 2020.12.29

(21)申请号 202021100036.4
(22)申请日 2020.06.15
(73)专利权人 安徽理工大学
地址 232001 安徽省淮南市山南新区泰丰大街168号
(72)发明人 朱奥强 张顺香 朱广丽 孟楠 徐新燕 张延 朱海洋 许汗清 张梦瑶 张标 尹畅 余宏斌
(51)Int.Cl.
G07C 9/25(2020.01)
G07C 9/27(2020.01)
G07C 9/37(2020.01)
G07C 9/38(2020.01)
G07C 9/00(2020.01)
H04N 7/18(2006.01)
G08B 21/00(2006.01)
G08B 3/10(2006.01)

(ESM)同样的发明创造已同日申请发明专利

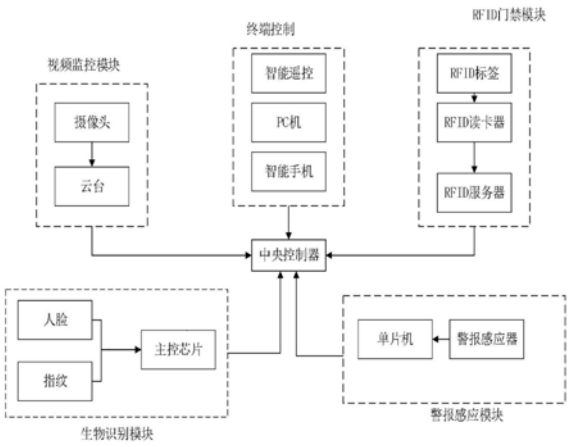
权利要求书1页 说明书3页 附图5页

(54)实用新型名称

基于RFID和生物识别的物联网门禁系统

(57)摘要

本发明专利公开了一种基于RFID和生物识别的物联网门禁系统，包括RFID门禁模块、生物识别模块、视频监控模块、警报感应模块、单片机、中央控制器、控制终端；所述RFID门禁模块和生物识别模块与中央控制器连接，通过RFID读卡器RFID标签的匹配、指纹识别和红外人脸识别，后台设置控制进门时需要验证的特征组合，可单选或多选，匹配成功后中央控制器根据匹配数据智能开门，并在多次匹配失败后开启摄像头采集图像并向后台发送告警信息；视频监控模块通过网络摄像头实现门外环境的实时监控和人脸图像的采集；警报感应模块以一单片机作为传感器信息处理核心控制板，一旦有任何异常，门禁系统能立即向后台发布报警信息，保证门禁系统安全。



CN 212256412 U

1.一种基于RFID和生物识别的物联网门禁系统,其特征在于:包括RFID门禁模块的RFID标签和RFID读卡器、生物识别模块的人脸识别和指纹识别、视频监控模块的网络摄像头和云台、警报感应模块的报警感应器和单片机、中央控制器的无线传输、控制终端的PC机移动手机和智能遥控,RFID门禁模块和生物识别模块与中央控制器连接,通过RFID读卡器和RFID标签的信息匹配、指纹识别和红外人脸识别的信息匹配共同控制门禁系统开关,后台设置控制进门时需要验证的特征组合,可单选或多选,视频监控模块通过网络摄像头与PC和智能手机实现门外附近环境的实时监控和人脸图像的采集,警报感应模块以一块单片机作为传感器信息处理核心控制板,与各传感器、按键、喇叭和指示灯构成报警系统。

2.根据权利要求1所述的基于RFID和生物识别的物联网门禁系统,其特征在于:所述RFID门禁、指纹识别和红外人脸识别控制门禁开关,通过后台设置,可控制进门时需要验证的特征组合,可单选或多选,在单选RFID或指纹识别开门时,RFID或指纹识别不匹配,自动转为人脸识别。

3.根据权利要求1所述的基于RFID和生物识别的物联网门禁系统,其特征在于:所述核心控制板为STM32芯片,还用于当RFID或指纹匹配失败时将采集的人脸图像与所储存器预存的人脸模板进行人脸匹配并在人脸匹配成功时控制锁芯开锁。

4.根据权利要求1所述的基于RFID和生物识别的物联网门禁系统,其特征在于:所述RFID门禁模块的RFID芯片采用Philips公司生产的一款典型的非接触式RFID电子标签Mifare1S50。

5.根据权利要求1所述的基于RFID和生物识别的物联网门禁系统,其特征在于:所述指纹识别和人脸识别包括,通过指纹和人脸采集器对用户指纹和人脸进行录入,将每个采集到的数据存储至服务器,当用户进门时触发指纹或人脸比对模块进行指纹或人脸对比。

6.根据权利要求1所述的基于RFID和生物识别的物联网门禁系统,其特征在于:所述视频监控模块为通过中央控制器和无线通讯与PC和智能手机相连。

7.根据权利要求1所述的基于RFID和生物识别的物联网门禁系统,其特征在于:所述报警感应器,以一块SPCE061A单片机作为传感器信息处理核心控制板,与各传感器、按键、喇叭和指示灯构成报警系统。

8.根据权利要求1所述的基于RFID和生物识别的物联网门禁系统,其特征在于:所述智能遥控,为无线遥控器,可直接控制门禁的开关。

基于RFID和生物识别的物联网门禁系统

技术领域

[0001] .本发明属于门禁设备领域,具体基于RFID和生物识别的物联网门禁系统。

背景技术

[0002] .传统机械锁的打开方式较为单一,开锁过程简易方便,随着社会的发展与进步,传统的机械锁在某些地方已经无法满足人们的安全需求。利用门禁卡通过射频识别技术识别身份信息后控制开锁,开锁方式简单方便,但由于门禁卡容易丢失,只需携带门禁卡即可开门,存在较大的安全隐患。单一固定的解锁方式在安全性和方便性方便都有所欠缺,并且现有的门禁系统无法在多次验证失败时获取图像信息并向后台发送报警,也无法快速验证用户身份,智能开门,导致现有锁具的安全性、使用便捷性和用户体验不佳。

发明内容

[0003] .本发明的目的在于针对上述存在的问题和不足,提出一种结构简单、安装方便、安全可靠、开锁方便的基于RFID和生物识别的物联网门禁系统,通过双重验证开锁,安全系数高。

[0004] .为了实现上述目的,本发明采用的技术方案是:一种基于RFID和生物识别的物联网门禁系统,其特征在于:包括RFID门禁模块的RFID标签和RFID读卡器、生物识别模块人脸识别和指纹识别、视频监控模块的网络摄像头和云台、警报感应模块的报警感应器和单片机、中央控制器的无线传输、控制终端的PC机移动手机和智能遥控,RFID门禁模块和生物识别模块与中央控制器连接,通过RFID读卡器RFID标签的匹配、指纹识别和红外人脸识别,后台设置控制进门时需要验证的特征组合,可单选或多选,视频监控模块通过网络摄像头与PC和智能手机实现门外附件环境的实时监控和人脸图像的采集,警报感应模块以一块单片机作为传感器信息处理核心控制板,与各传感器、按键、喇叭、指示灯等构成报警系统。

[0005] .进一步的,所述RFID门禁、指纹识别和红外人脸识别控制门禁开关,通过后台设置,可控制进门时需要验证的特征组合,可单选或多选,在单选RFID或指纹识别开门时,RFID或指纹识别不匹配,自动转为人脸识别。

[0006] .进一步的,所述主控芯片为STM32芯片,还用于当指纹匹配失败时将采集的人脸图像与所储存器预存的人脸模板进行人脸匹配并在人脸匹配成功时控制锁芯开锁。

[0007] .进一步的,所述RFID门禁模块的RFID芯片采用Philips公司生产的一款典型的非接触式RFID电子标签Mifare1S50。

[0008] .进一步的,所述指纹识别和人脸识别包括,通过指纹和人脸采集器对用户指纹和人脸进行录入,将每个采集到的数据存储至服务器,当用户进门时触发指纹或人脸比对模块进行指纹或人脸对比。

[0009] .进一步的,所述视频监控模块为通过中央控制器和无线通讯与PC和智能手机相连。

[0010] .进一步的,所述报警感应器,以一块SPCE061A单片机作为传感器信息处理核心控

制板，与各传感器、按键、喇叭、指示灯等构成报警系统。

[0011] .进一步的，所述智能遥控，为无线遥控器，可直接控制门禁的开关。

[0012] .本发明的有益效果：本发明通过RFID读卡器RFID标签的匹配、指纹识别和红外人脸识别匹配共同控制门禁的开关，不用担心丢失门禁卡带来的安全隐患，提高了安全性能。通过射频检测模块验证RFID标签内的身份信息、触摸感应模块识别指纹触摸信号，以人脸识别的多重验证方式来开锁，并在多次匹配失败后开启摄像头采集图像并向后台发送告警信息，不用担心丢失门禁卡带来的安全隐患，提高了安全性能。并设置有报警系统，当感应到异常信息时会把信息传到控制中心，提醒用户处理，并报警。视频监控模块通过中央控制器和无线通讯与PC和智能手机相连，建立无线通讯网络连接实时监控门锁信息。提升了门禁系统的安全性、便捷性和用户体验。

附图说明

[0013] .图1是本发明所述基于RFID和生物识别的物联网门禁系统总体结构图；

[0014] .图2是本发明的RFID射频和生物识别门禁流程图；

[0015] .图3是本发明的单选RFID射频门禁流程框图。

[0016] .图4是本发明的单选指纹识别门禁流程框图。

[0017] .图5是本发明的单选人脸识别射频门禁流程框图。

具体实施方式

[0018] .为使本发明的内容更加清楚，下面结合附图，对本发明的具体实施方式作进一步详细描述。

[0019] .本发明提供的基于RFID和生物识别的物联网门禁系统，如图1所示，包含RFID门禁模块的RFID标签和RFID读卡器、生物识别模块人脸识别和指纹识别、视频监控模块的网络摄像头和云台、警报感应模块的报警感应器和、中央控制器的无线传输、控制终端的PC机移动手机和智能遥控；RFID门禁模块和生物识别模块与中央控制器连接，通过RFID读卡器RFID标签的匹配、指纹识别和红外人脸识别，后台设置控制进门时需要验证的特征组合，可单选或多选，视频监控模块通过网络摄像头与PC和智能手机实现门外附件环境的实时监控和人脸图像的采集，警报感应模块以一块单片机作为传感器信息处理核心控制板，与各传感器、按键、喇叭、指示灯等构成报警系统；

[0020] .各模块和中央控制器通过无线传输网络实现，信息的传送和控制，选定WiFi来实现无线传感网络，具有安全可靠、低成本、短延时和方便快捷的特点；

[0021] .云台可根据不同需要，远程控制来调整网络摄像头的角度；

[0022] .警报感应模块的警报感应器包括：人体红外传感器、震动传感器和蜂鸣器，以一块SPCE061A单片机作为传感器信息处理核心控制板，与各传感器、按键、喇叭、指示灯等构成报警系统。

[0023] .如图2所示，为本发明的RFID射频和生物识别门禁流程图，具体方式为：通过RFID技术将用户信息纳入到物联网的范围之内，RFID标签卡片给予人员身份信息，并能通过读卡器进行识别，当RFID电子标签进入读卡器的射频区域内时，RFID电子标签通过读卡器的射频场获得激活能量，再向读卡器发送数据，之后对比加密信息，如果加密信息匹配，再通

过指纹和人脸识别验证生物信息，如果指纹和人脸为注册信息，门禁将开启，不是注册信息，则提示验证错误，再多次验证错误后，讲存储指纹和人脸信息备案，后台通知用户并开启警报系统；

[0024] .用户可通过主程序对系统进行控制。通过设备采集器采集合法用户的指纹、人脸等信息，并录入服务器。通过后台设置，可控制进门时需要验证的特征组合，可单选或多选。

[0025] .如图3所示，为本发明的单选RFID射频门禁流程框图，具体方式：RFID标签进入读卡器的射频区域内，通过读卡器进行识别，识别成功控制锁芯开锁，识别失败，将采集的人脸图像与所储存器预存的人脸模板进行人脸匹配并在人脸匹配成功时控制锁芯开锁。多次匹配失败后经储存人脸信息备案，并通知后台用户，同时主控芯片输出门铃音频，启动警报系统。

[0026] .如图4所示，本发明的单选指纹识别门禁流程框图，具体方式和单选RFID射频门禁方式相同，指纹识别成功控制锁芯开锁，识别失败，启动人脸识别，识别成功控制锁芯开锁，多次识别失败后储存人脸信息备案，并通知后台用户，启动警报系统。

[0027] .图5所示，本发明的单选人脸识别射频门禁流程框图，具体方式：处于待机状态的系统，检测到人脸图像时，采集的人脸图像与所储存器预存的人脸模板进行人脸匹配并在人脸匹配成功时控制锁芯开锁。多次匹配失败后经储存人脸信息备案，并通知后台用户，同时主控芯片输出门铃音频，启动警报系统。

[0028] .除了以上门禁系统开锁方式之外，本发明所述基于RFID和生物识别的物联网门禁系统，还可将RFID射频和指纹识别、RFID射频和人脸识别、指纹识别和人脸识别进行组和构成本门禁系统的开门方式。所选开门方式均可通过后台设置，控制进门时需要验证的特征组合。并且本系统设置的智能遥控装置可在室内一键开门，实现门禁系统更加安全、高效、便捷。

[0029] .以上仅表达了本发明的实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干组合、变形和改进，这些都属于本发明的保护范围。

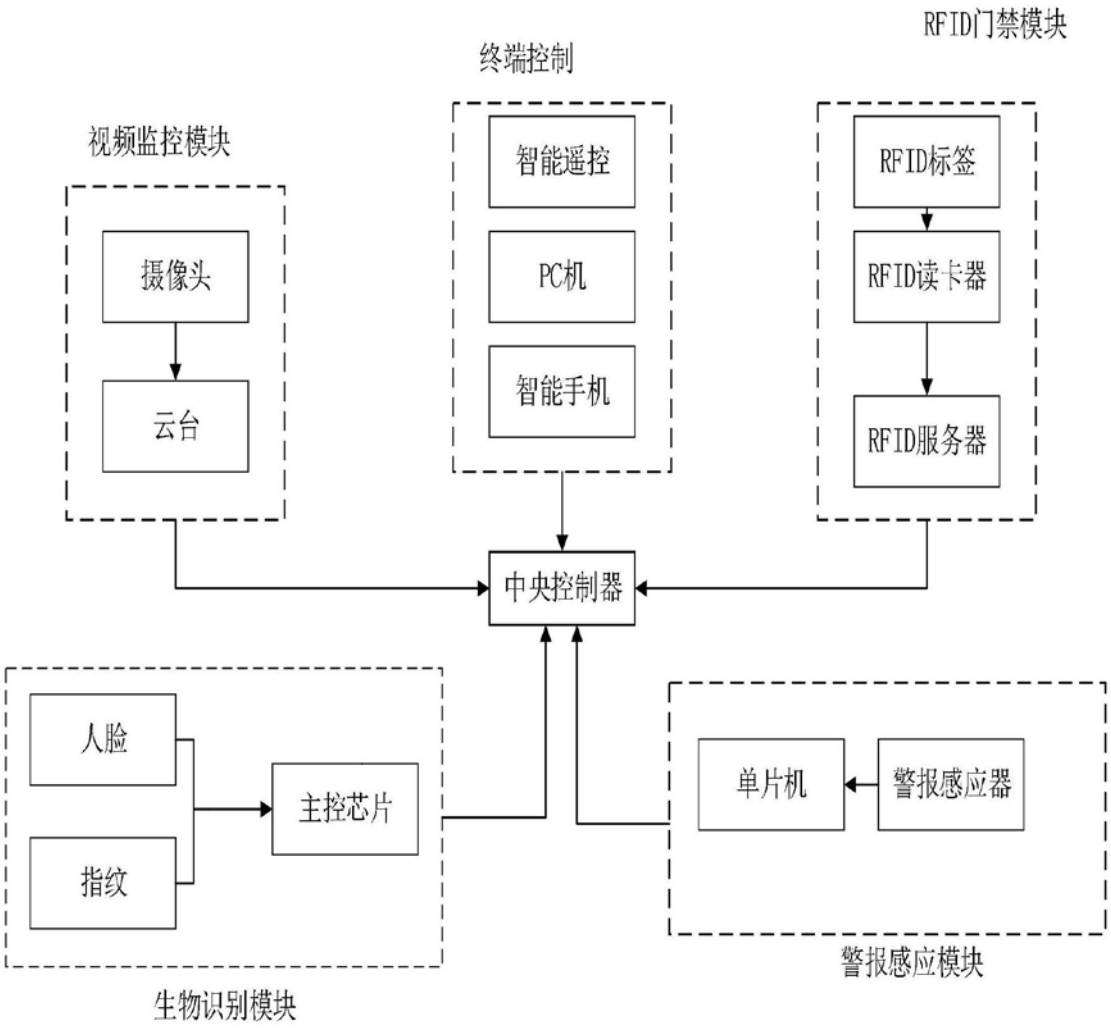

RFID门禁模块
终端控制
视频监控模块
智能遥控
RFID标签
摄像头
PC机
RFID读卡器
云台
智能手机
RFID服务器
中央控制器
人脸
单片机
警报感应器
主控芯片
指纹
警报感应模块
生物识别模块

图1

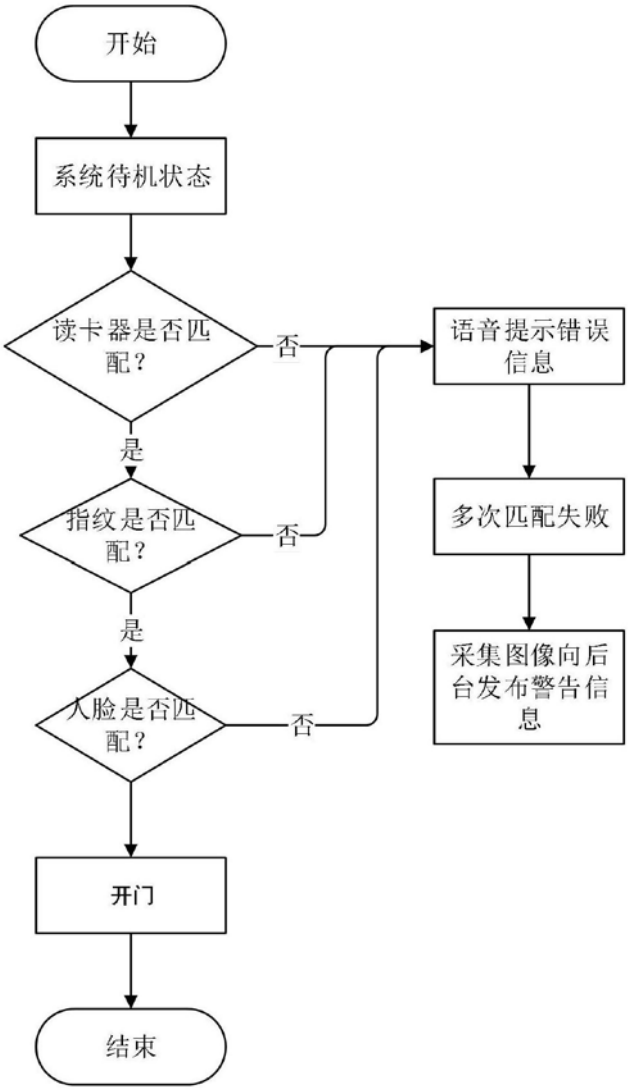

开始
系统待机状态
读卡器是否匹配？
否
是
指纹是否匹配？
否
是
人脸是否匹配？
否
开门
结束
语音提示错误信息
多次匹配失败
采集图像向后台发布警告信息

图2

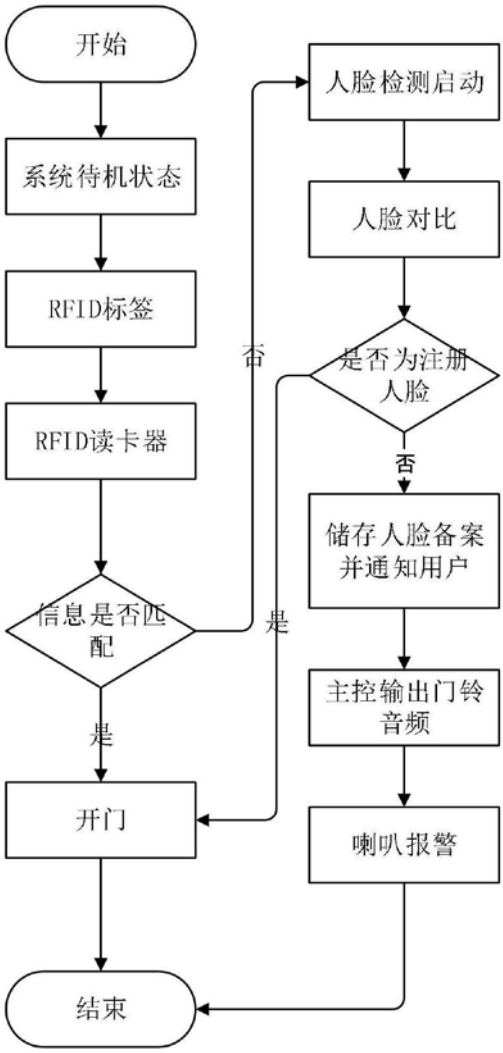

开始
系统待机状态
RFID标签
RFID读卡器
信息是否匹配
否
是
开门
结束
人脸检测启动
人脸对比
是否为注册人脸
否
是
储存人脸备案并通知用户
主控输出门铃音频
喇叭报警

图3

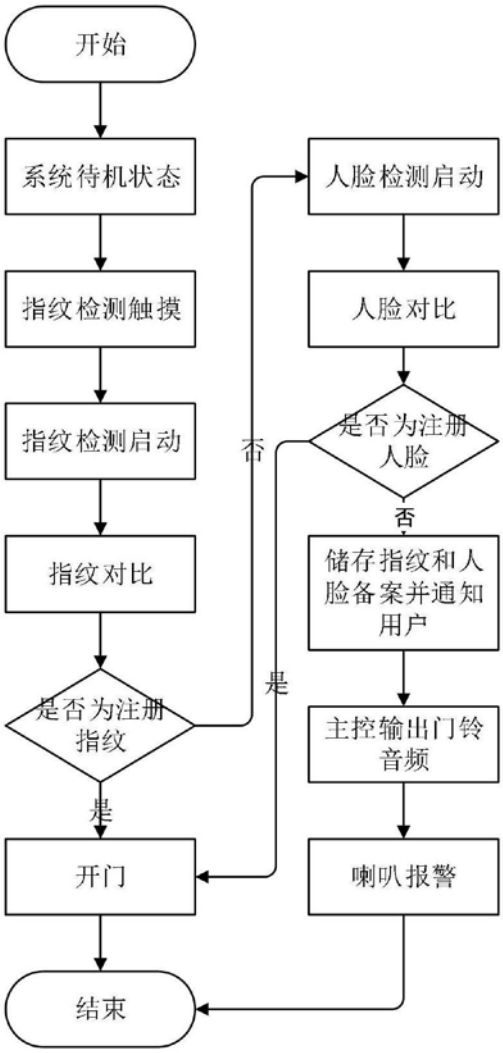

开始
系统待机状态
指纹检测触摸
指纹检测启动
指纹对比
是否为注册指纹
否
是
人脸检测启动
人脸对比
是否为注册人脸
否
储存指纹和人脸备案并通知用户
主控输出门铃音频
喇叭报警
是
开门
结束

图4

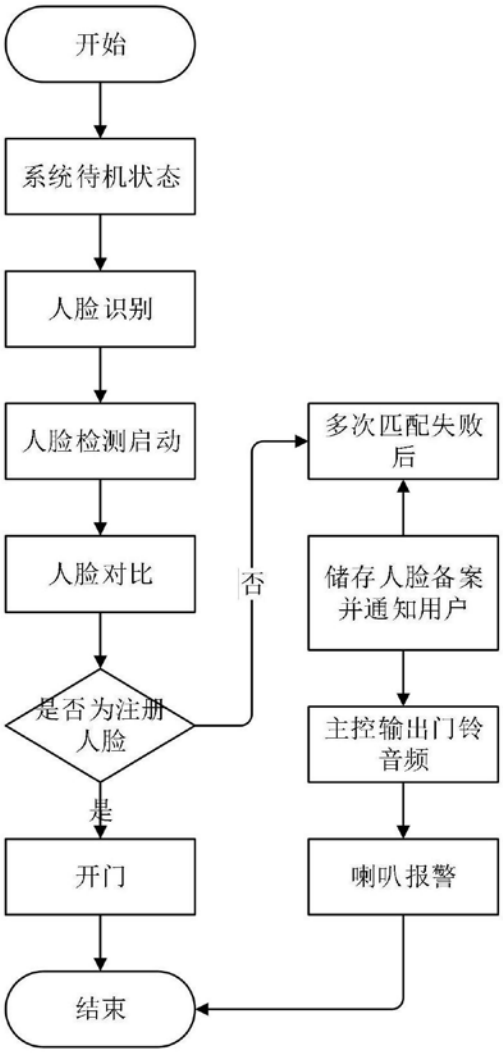

开始
系统待机状态
人脸识别
人脸检测启动
人脸对比
是否为注册人脸
否
是
开门
结束
多次匹配失败后
储存人脸备案并通知用户
主控输出门铃音频
喇叭报警

图5