



(12)发明专利申请

(10)申请公布号 CN 110706391 A

(43)申请公布日 2020.01.17

(21)申请号 201910924145.3

(22)申请日 2019.09.27

(71)申请人 恒大智慧科技有限公司

地址 518000 广东省深圳市南山区前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)

(72)发明人 郑文强

(51)Int.Cl.

G07C 9/37(2020.01)

G06K 9/00(2006.01)

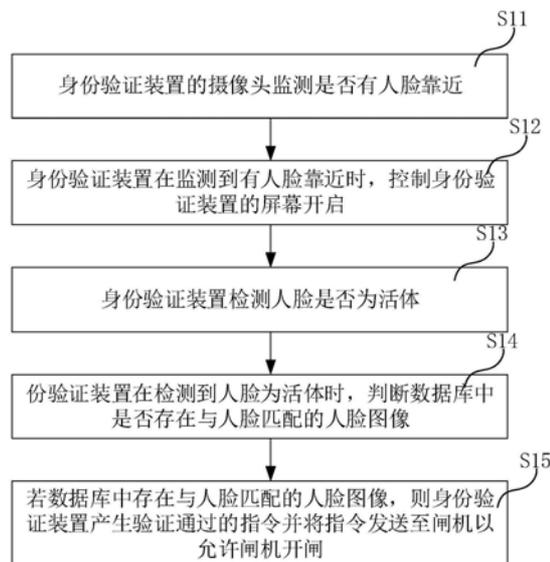
权利要求书1页 说明书5页 附图2页

(54)发明名称

人脸识别验证通行方法、身份验证装置及存储介质

(57)摘要

本申请公开了一种人脸识别验证通行方法,该方法包括:身份验证装置的摄像头监测是否有人脸靠近;身份验证装置在监测到有人脸靠近时,控制身份验证装置的屏幕开启;身份验证装置检测人脸是否为活体;身份验证装置在检测到人脸为活体时,判断数据库中是否存在与人脸匹配的人脸图像;若数据库中存在与人脸匹配的人脸图像,则身份验证装置产生验证通过的指令并将指令发送至闸机以允许闸机开闸。本申请能够提高人脸识别的通行效率。



1. 一种人脸识别验证通行方法,其特征在于,所述方法包括:  
身份验证装置的摄像头监测是否有人脸靠近;  
所述身份验证装置在监测到有人脸靠近时,控制所述身份验证装置的屏幕开启;  
所述身份验证装置检测所述人脸是否为活体;  
所述身份验证装置在检测到所述人脸为活体时,判断数据库中是否存在与所述人脸匹配的人脸图像;  
若所述数据库中存在与所述人脸匹配的人脸图像,则所述身份验证装置产生验证通过的指令并将所述指令发送至闸机以允许所述闸机开闸。
2. 根据权利要求1所述的人脸识别验证通行方法,其特征在于,所述身份验证装置的摄像头监测是否有人脸靠近的步骤,包括:  
所述身份验证装置的摄像头每间隔预定时长采集一次周围的环境图像并判断所述周围的环境图像中是否包括人脸。
3. 根据权利要求1所述的人脸识别验证通行方法,其特征在于,所述预定时长为240-260ms。
4. 根据权利要求3所述的人脸识别验证通行方法,其特征在于,所述预定时长为250ms。
5. 根据权利要求1所述的人脸识别验证通行方法,其特征在于,所述方法还包括:  
所述身份验证装置的光线传感器检测周围环境光的强度;  
所述身份验证装置根据所述周围环境光的强度调节所述身份验证装置的补光灯的亮度。
6. 根据权利要求1所述的人脸识别验证通行方法,其特征在于,所述方法还包括所述身份验证装置在监测到有人脸靠近的步骤,包括:  
在所述身份验证装置的摄像头获取的人脸图像亮度到达预设亮度阈值、人脸图像尺寸到达预设尺寸阈值、人脸图像的分辨率到达预设分辨率阈值的时间点判定为监测到有人脸靠近。
7. 根据权利要求1所述的人脸识别验证通行方法,其特征在于,所述数据库存储于所述身份验证装置。
8. 根据权利要求1所述的人脸识别验证通行方法,其特征在于,所述控制所述身份验证装置的屏幕开启的步骤之后包括:  
所述身份验证装置控制所述屏幕对所述摄像头采集的图像进行实时显示。
9. 一种身份验证装置,其特征在于,所述身份验证装置包括处理器和与所述处理器电连接的存储器,所述存储器用于存储计算机程序,所述处理器用于调用所述计算机程序以实现权利要求1-8任意一项所述的方法。
10. 一种存储介质,其特征在于,所述存储介质存储有计算机程序,所述计算机程序能够被处理器执行以实现权利要求1-8任意一项所述的方法。

## 人脸识别验证通行方法、身份验证装置及存储介质

### 技术领域

[0001] 本发明涉及智慧社区技术领域,特别是涉及一种人脸识别验证通行方法、身份验证装置及存储介质。

### 背景技术

[0002] 智慧社区是社区管理的一种新理念,是新形势下社会管理创新的一种新模式。智慧社区是指充分利用物联网、云计算、移动互联网等新一代信息技术的集成应用,为社区居民提供一个安全、舒适、便利的现代化、智慧化生活环境,从而形成基于信息化、智能化社会管理与服务的一种新的管理形态的社区。智慧社区是指充分借助互联网、物联网,涉及到智能楼宇、智能家居、路网监控、智能医院、城市生命线管理、食品药品管理、票证管理、家庭护理、个人健康与数字生活等诸多领域,把握新一轮科技创新革命和信息产业浪潮的重大机遇,充分发挥信息通信(ICT)产业发达、RFID相关技术领先、电信业务及信息化基础设施优良等优势,通过建设ICT基础设施、认证、安全等平台 and 示范工程,加快产业关键技术攻关,构建社区发展的智慧环境,形成基于海量信息和智能过滤处理的新的生活、产业发展、社会管理等模式,面向未来构建全新的社区形态。

[0003] 身份验证装置是智慧社区的一个重要组成部分,通常设置在出入口闸机出,传统智慧社区的身份验证装置采用红外感应器感应人脸的接近,然后进行人脸识别,但这种方式的检测范围小,极大影响了通行效率。

[0004] 为了身份验证装置的功耗,常规做法是在没有人使用的时候关闭屏幕或者降低屏幕亮度,有人使用的时候点亮屏幕。现有社区面板点亮屏幕是通过红外感应实现的,红外感应的缺点是感应有一定的角度,而且不同的颜色识别距离有差别,体验不是很好。

### 发明内容

[0005] 本申请主要解决的技术问题是提供一种人脸识别验证通行方法、身份验证装置及存储介质,能够提高人脸识别的通行效率。

[0006] 为解决上述技术问题,本申请实施例采用的一个技术方案是:提供一种人脸识别验证通行方法,方法包括:身份验证装置的摄像头监测是否有人脸靠近;身份验证装置在监测到有人脸靠近时,控制身份验证装置的屏幕开启;身份验证装置检测人脸是否为活体;身份验证装置在检测到人脸为活体时,判断数据库中是否存在与人脸匹配的人脸图像;若数据库中不存在与人脸匹配的人脸图像,则身份验证装置产生验证通过的指令并将指令发送至闸机以允许闸机开闸。

[0007] 其中,身份验证装置的摄像头监测是否有人脸靠近的步骤,包括:身份验证装置的摄像头每间隔预定时长采集一次周围的环境图像并判断周围的环境图像中是否包括人脸。

[0008] 其中,预定时长为240-260ms。

[0009] 其中,预定时长为250ms。

[0010] 其中,方法还包括:身份验证装置的光线传感器检测周围环境光的强度;身份验证

装置根据周围环境光的强度调节身份验证装置的补光灯的亮度。

[0011] 其中,方法还包括身份验证装置在监测到有人脸靠近的步骤,包括:在身份验证装置的摄像头获取的人脸图像亮度到达预设亮度阈值、人脸图像尺寸到达预设尺寸阈值、人脸图像的分辨率到达预设分辨率阈值的时间点判定为监测到有人脸靠近。

[0012] 其中,数据库存储于身份验证装置。

[0013] 其中,控制身份验证装置的屏幕开启的步骤之后包括:身份验证装置控制屏幕对摄像头采集的图像进行实时显示。

[0014] 为解决上述技术问题,本申请实施例采用的又一个技术方案是:提供一种身份验证装置,该身份验证装置包括处理器和与处理器电连接的存储器,存储器用于存储计算机程序,处理器用于调用计算机程序以实现上述的方法

[0015] 为解决上述技术问题,本申请实施例采用的另一个技术方案是:提供一种存储介质,该存储介质存储有计算机程序,计算机程序能够被处理器执行以实现上述的方法。

[0016] 本申请实施例通过身份验证装置的摄像头监测是否有人脸靠近;身份验证装置在监测到有人脸靠近时,控制身份验证装置的屏幕开启;身份验证装置检测人脸是否为活体;身份验证装置在检测到人脸为活体时,判断数据库中是否存在与人脸匹配的人脸图像;若数据库中存在与人脸匹配的人脸图像,则身份验证装置产生验证通过的指令并将指令发送至闸机以允许闸机开闸,能够提高人脸识别的通行效率。

## 附图说明

[0017] 图1是本申请第一实施例的人脸识别验证通行方法的流程示意图;

[0018] 图2是图1中步骤S11的一种具体步骤的流程示意图;

[0019] 图3是本申请第二实施例的人脸识别验证通行方法的部分流程示意图;

[0020] 图4是身份验证装置在监测到有人脸靠近的具体流程示意图;

[0021] 图5是本申请实施例的身份验证装置的示意图。

## 具体实施方式

[0022] 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述。可以理解的是,此处所描述的具体实施例仅用于解释本申请,而非对本申请的限定。另外还需要说明的是,为了便于描述,附图中仅示出了与本申请相关的部分而非全部结构。基于本申请中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

[0023] 本申请中的术语“第一”、“第二”等是用于区别不同对象,而不是用于描述特定顺序。此外,术语“包括”和“具有”以及它们任何变形,意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元,而是可选地还包括没有列出的步骤或单元,或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0024] 在本文中提及“实施例”意味着,结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例,也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和

隐式地理解的是,本文所描述的实施例可以与其它实施例相结合。

[0025] 请参阅图1,图1是本申请第一实施例的人脸识别验证通行方法的流程示意图。

[0026] 在本实施例中,人脸识别验证通行方法可以包括以下步骤:

[0027] 步骤S11:身份验证装置的摄像头监测是否有人脸靠近。

[0028] 身份验证装置配置了摄像头(例如身份验证装置设置有1080p摄像头),有效识别人脸的距离可以到1-2m,水平识别角度可达到150度,高度从1m到3m范围都可以识别。这就保证了大人,小孩都可以正常使用。

[0029] 摄像头改为常开,在身份验证待机情况下,摄像头也在后台运行,实时捕获人脸。通过摄像头捕捉人脸,为了降低待机功耗,可以将捕捉摄像头的采样间隔定为250ms一次,即1秒从摄像头获取4帧数据。

[0030] 步骤S12:身份验证装置在监测到有人脸靠近时,控制身份验证装置的屏幕开启。

[0031] 其中,身份验证装置在监测到有人脸靠近时,控制身份验证装置的屏幕开启,控制身份验证装置退出休眠状态,进入唤醒状态。

[0032] 步骤S13:身份验证装置检测人脸是否为活体。

[0033] 调用人脸识别算法,检测是否有人脸,如果有人脸,则判断人脸是否符合人脸识别要求,常用参数有:最小人脸尺寸、人脸水平角度,人脸垂直角度等。

[0034] 有符合人脸识别的帧之后就可以唤醒屏幕,此时用户可以看到自己,根据捕获的人脸进行活体检测。

[0035] 接下来需要做活体检测,判断是否是真人,过滤掉电子屏,照片等伪活体。

[0036] 步骤S14:身份验证装置在检测到人脸为活体时,判断数据库中是否存在与人脸匹配的人脸图像。

[0037] 其中,数据库存储于身份验证装置本地,可以提高识别速度。

[0038] 步骤S15:若数据库中存在与人脸匹配的人脸图像,则身份验证装置产生验证通过的指令并将指令发送至闸机以允许闸机开闸。

[0039] 基于以上红外感应唤醒面板的问题,提出了使用人脸识别来唤醒屏幕并快速完成人脸认证。这种方案不仅解决了上述识别角度和颜色的问题,而且加快了人脸认证的速度,真正提升了通行效率和用户体验。

[0040] 请参阅图2,图2是图1中步骤S11的一种具体步骤的流程示意图。

[0041] 在本实施例中,身份验证装置的摄像头监测是否有人脸靠近的步骤,具体可以包括:

[0042] 步骤S21:身份验证装置的摄像头每间隔预定时长采集一次周围的环境图像。

[0043] 其中,预定时长为240-260ms。可选地,预定时长为250ms。

[0044] 步骤S22:判断周围的环境图像中是否包括人脸。

[0045] 请参阅图3,图3是本申请第二实施例的人脸识别验证通行方法的部分流程示意图。

[0046] 在本实施例中,人脸识别验证通行方法还可以包括以下步骤:

[0047] 步骤S31:身份验证装置的光线传感器检测周围环境光的强度。

[0048] 步骤S32:身份验证装置根据周围环境光的强度调节身份验证装置的补光灯的亮度。

[0049] 为了夜间或光线暗的环境下正常使用,需要开启补光灯,补光灯的开启可以根据检测的周围的环境光光线强度动态调节。

[0050] 请参阅图4,图4是身份验证装置在监测到有人脸靠近的具体流程示意图。

[0051] 其中,方法还包括身份验证装置在监测到有人脸靠近的步骤,包括:

[0052] 步骤S41:在身份验证装置的摄像头获取的人脸图像亮度到达预设亮度阈值、人脸图像尺寸到达预设尺寸阈值、人脸图像的分辨率到达预设分辨率阈值的时间点判定为监测到有人脸靠近。

[0053] 每250ms从摄像头获取一帧数据(抓拍的一张图片),判断图片是否符合要求,常用参数有:图片亮度、清晰度、模糊度等。如果符合要求则进行人脸检测。

[0054] 在一种实施例中,控制身份验证装置的屏幕开启的步骤之后包括:身份验证装置控制屏幕对摄像头采集的图像进行实时显示。

[0055] 请参阅图5,图5是本申请实施例的身份验证装置的示意图。

[0056] 在本实施例中,身份验证装置50包括处理器501和与处理器501电连接的存储器502,存储器502用于存储计算机程序,处理器501用于调用计算机程序以实现上述的方法

[0057] 本申请实施例还提供一种存储介质,该存储介质存储有计算机程序,该计算机程序被处理器执行时能够实现上述任一实施例的方法。

[0058] 其中,该计算机程序可以以软件产品的形式存储在上述存储介质中,包括若干指令用以使得一个设备或处理器执行本申请各个实施方式方法的全部或部分步骤。

[0059] 存储介质是计算机存储器中用于存储某种不连续物理量的媒体。而前述的存储介质可以为:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0060] 在本申请所提供的几个实施方式中,应该理解到,所揭露的方法以及设备,可以通过其它的方式实现。例如,以上所描述的设备实施方式仅仅是示意性的,例如,模块或单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。

[0061] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施方式方案的目的。

[0062] 另外,在本发明各个实施方式中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0063] 本申请实施例通过身份验证装置的摄像头监测是否有人脸靠近;身份验证装置在监测到有人脸靠近时,控制身份验证装置的屏幕开启;身份验证装置检测人脸是否为活体;身份验证装置在检测到人脸为活体时,判断数据库中是否存在与人脸匹配的人脸图像;若数据库中存在与人脸匹配的人脸图像,则身份验证装置产生验证通过的指令并将指令发送至闸机以允许闸机开闸,能够提高人脸识别的通行效率。

[0064] 以上仅为本申请的实施方式,并非因此限制本申请的专利范围,凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术

领域,均同理包括在本申请的专利保护范围内。

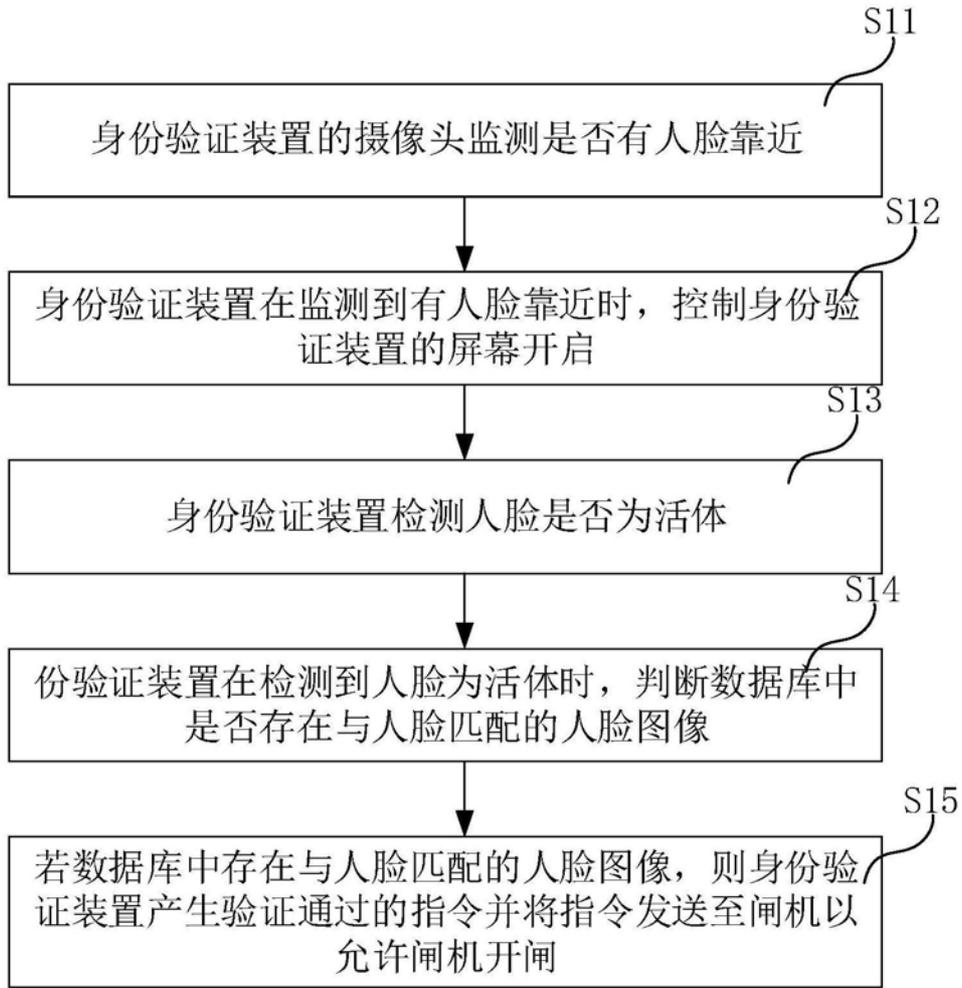


图1

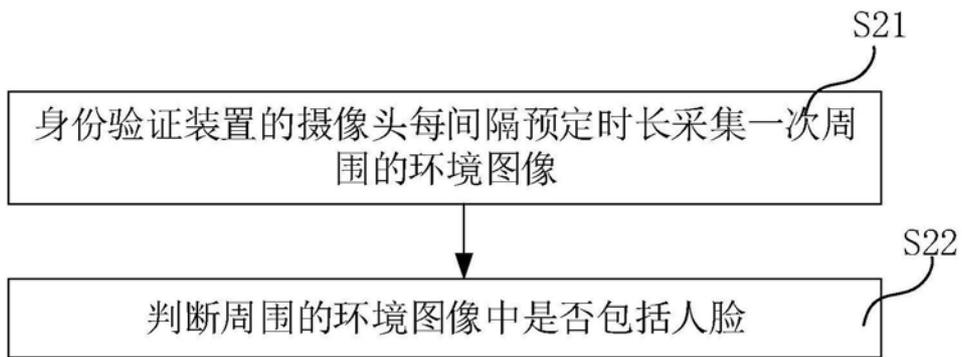


图2

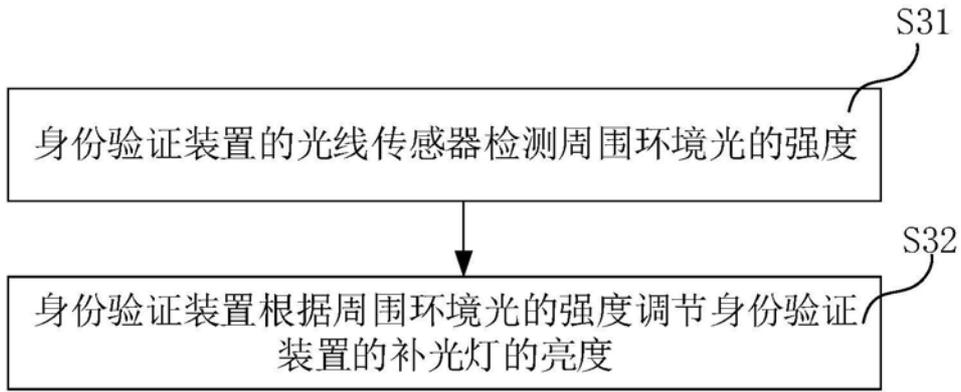


图3

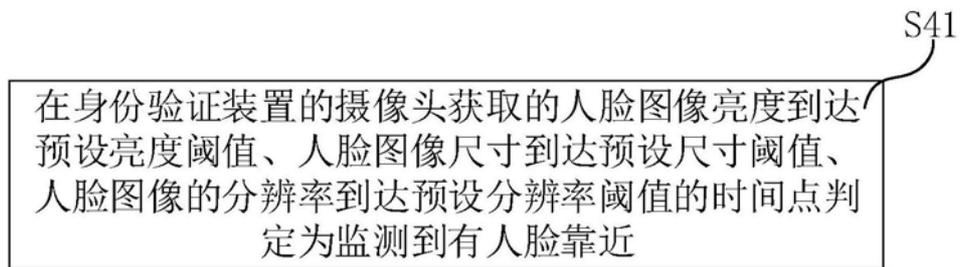


图4

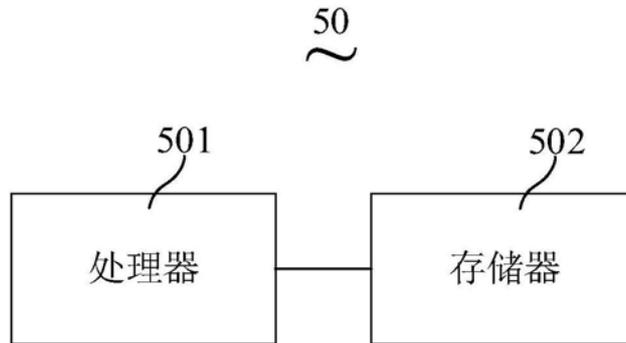


图5