



(12) 发明专利

(10) 授权公告号 CN 109712291 B

(45) 授权公告日 2020.11.10

(21) 申请号 201811608295.5

(51) Int.Cl.

(22) 申请日 2018.12.26

G07C 9/37 (2020.01)

G07C 9/38 (2020.01)

(65) 同一申请的已公布的文献号

申请公布号 CN 109712291 A

审查员 蔡伊青

(43) 申请公布日 2019.05.03

(73) 专利权人 巽腾(广东)科技有限公司

地址 510000 广东省广州市高新技术产业
开发区科学城科学大道182号创新大
厦C2栋首层103单元

(72) 发明人 简伟明 皮爱平 黄飞鹰 梁华贵
陈秋榕

(74) 专利代理机构 北京超凡志成知识产权代理
事务所(普通合伙) 11371

代理人 苏胜

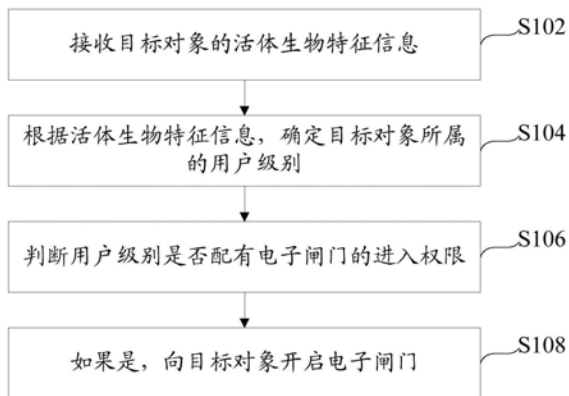
权利要求书3页 说明书9页 附图2页

(54) 发明名称

电子闸门的开启方法、装置及服务器

(57) 摘要

本发明提供了一种电子闸门的开启方法、装置及服务器,该方法包括:接收目标对象的活体生物特征信息;其中活体生物特征信息携带有账号信息,和/或,电子闸门位置信息;根据活体生物特征信息,确定目标对象所属的用户级别;其中,用户级别与账号信息,和/或,电子闸门位置信息相关;判断用户级别是否配有电子闸门的进入权限;如果是,向目标对象开启电子闸门。本发明通过采集目标对象活体生物特征信息,来判断目标对象是否配有电子闸门的进入权限,省去目标对象刷门禁卡片或者出示身份证件步骤,进而提高用户体验;另外,采用采集活体生物特征信息的方式,可以有效防止他人冒用身份证件等信息,进而提高电子闸门的安全性。



1. 一种电子闸门的开启方法,其特征在于,包括:

接收目标对象的活体生物特征信息;其中所述活体生物特征信息携带有电子闸门账号信息,和/或,电子闸门位置信息;

根据所述活体生物特征信息,确定所述目标对象所属的用户级别;其中,所述用户级别与所述电子闸门账号信息,和/或,所述电子闸门位置信息相关;

判断所述用户级别是否配有电子闸门的进入权限;

如果是,向所述目标对象开启所述电子闸门;

所述用户级别包括第一类用户、第二类用户、第三类用户和第四类用户;所述根据所述活体生物特征信息,确定所述目标对象所属的用户级别的步骤,包括:

根据所述活体生物特征信息和第一服务器内的各用户的生物特征信息,判断所述目标对象所属的用户级别是否为第一类用户;所述第一服务器为本地服务器或远程服务器;

如果否,将所述活体生物特征信息发送至第二服务器,以使所述第二服务器基于所述活体生物特征信息进行第二生物特征匹配,得到第二生物特征匹配结果,并向用户管理的终端设备发出位置请求;根据所述第二生物特征匹配结果和位置信息判断所述目标对象所属的用户级别是否为第二类用户;

如果否,将所述活体生物特征信息发送至第三服务器,所述第三服务器基于所述电子闸门位置信息查询所有在预设范围内用户,并获取所述用户所述活体生物特征信息进行第三生物特征匹配,得到第三生物特征匹配结果;根据所述第三生物特征匹配结果判断所述目标对象所属的用户级别是否为第三类用户;

如果否,确定所述目标对象所属的用户级别为第四类用户;

所述将所述活体生物特征信息发送至第三服务器,以使所述第三服务器基于所述活体生物特征信息进行第三生物特征匹配,得到第三生物特征匹配结果;根据所述第三生物特征匹配结果判断所述目标对象所属的用户级别是否为第三类用户的步骤,包括:

基于所述活体生物特征信息生成第二识别请求;其中,所述第二识别请求包括所述活体生物特征信息和所述电子闸门位置信息;

将所述第二识别请求发送至第三服务器,以使所述第三服务器获取所述电子闸门位置信息对应的第一栅格区域内的各当前用户的生物特征信息,和/或,与所述第一栅格区域相邻的第二栅格区域内的各当前用户的生物特征信息,对所述活体生物特征信息和各所述当前用户的生物特征信息进行第三生物特征匹配,并返回第三生物特征匹配结果;其中,所述第三服务器对各用户的轨迹进行跟踪,以确定处于所述第一栅格区域,和/或,第二栅格区域内的各当前用户;

当所述第三生物特征匹配结果为成功时,将所述目标对象所属的用户级别确定为所述第三类用户。

2. 根据权利要求1所述的方法,其特征在于,所述根据所述活体生物特征信息和第一服务器内的各用户的生物特征信息,判断所述目标对象所属的用户级别是否为第一类用户的步骤,包括:

获取第一服务器内的各第一类用户的生物特征信息;

对所述活体生物特征信息和各所述第一类用户的生物特征信息进行第一生物特征匹配;

当所述第一生物特征匹配成功时,将所述目标对象所属的用户级别确定为所述第一类用户。

3. 根据权利要求1所述的方法,其特征在于,所述将所述活体生物特征信息发送至第二服务器,以使所述第二服务器基于所述活体生物特征信息进行第二生物特征匹配,得到第二生物特征匹配结果;根据所述第二生物特征匹配结果判断所述目标对象所属的用户级别是否为第二类用户的步骤,包括:

基于所述活体生物特征信息生成第一识别请求;其中,所述第一识别请求包括所述活体生物特征信息和所述电子闸门账号信息;

将所述第一识别请求发送至第二服务器,以使所述第二服务器查找与所述电子闸门账号信息对应的各授权用户的生物特征信息,对所述活体生物特征信息和各所述授权用户的生物特征信息进行第二生物特征匹配,并返回第二生物特征匹配结果;

当所述第二生物特征匹配结果为成功时,向所述目标对象的关联终端发送位置确认请求;

接收所述目标对象的关联终端基于所述位置确认请求返回的位置确认信息,并将所述目标对象所属的用户级别确定为所述第二类用户。

4. 根据权利要求1所述的方法,其特征在于,所述判断所述用户级别是否配有电子闸门的进入权限的步骤,包括:

当所述用户级别为第一类用户、第二类用户或第三类用户时,确定所述用户级别配有电子闸门的进入权限。

5. 根据权利要求1所述的方法,其特征在于,所述方法还包括:

将所述目标对象所属的用户级别发送至关联终端,以使所述关联终端对应的管理人员查看所述目标对象的用户级别。

6. 一种电子闸门的开启装置,其特征在于,包括:

接收模块,用于接收目标对象的活体生物特征信息;其中所述活体生物特征信息携带有电子闸门账号信息,和/或,电子闸门位置信息;

级别确定模块,用于根据所述活体生物特征信息,确定所述目标对象所属的用户级别;其中,所述用户级别与所述电子闸门账号信息,和/或,所述电子闸门位置信息相关;

判断模块,用于判断所述用户级别是否配有电子闸门的进入权限;

权限开放模块,用于在所述判断模块的判断结果为是时,向所述目标对象开启所述电子闸门;

所述用户级别包括第一类用户、第二类用户、第三类用户和第四类用户;

所述级别确定模块,还用于:

根据所述活体生物特征信息和第一服务器内的各用户的生物特征信息,判断所述目标对象所属的用户级别是否为第一类用户;所述第一服务器为本地服务器或远程服务器;

如果否,将所述活体生物特征信息发送至第二服务器,以使所述第二服务器基于所述活体生物特征信息进行第二生物特征匹配,得到第二生物特征匹配结果,并向用户管理的终端设备发出位置请求;根据所述第二生物特征匹配结果和位置信息判断所述目标对象所属的用户级别是否为第二类用户;

如果否,将所述活体生物特征信息发送至第三服务器,所述第三服务器基于所述电子

闸门位置信息查询所有在预设范围内用户,并获取所述用户所述活体生物特征信息进行第三生物特征匹配,得到第三生物特征匹配结果;根据所述第三生物特征匹配结果判断所述目标对象所属的用户级别是否为第三类用户;

如果否,确定所述目标对象所属的用户级别为第四类用户;

所述级别确定模块,还用于:

基于所述活体生物特征信息生成第二识别请求;其中,所述第二识别请求包括所述活体生物特征信息和所述电子闸门位置信息;

将所述第二识别请求发送至第三服务器,以使所述第三服务器获取所述电子闸门位置信息对应的第一栅格区域内的各当前用户的生物特征信息,和/或,与所述第一栅格区域相邻的第二栅格区域内的各当前用户的生物特征信息,对所述活体生物特征信息和各所述当前用户的生物特征信息进行第三生物特征匹配,并返回第三生物特征匹配结果;其中,所述第三服务器对各用户的轨迹进行跟踪,以确定处于所述第一栅格区域,和/或,第二栅格区域内的各当前用户;

当所述第三生物特征匹配结果为成功时,将所述目标对象所属的用户级别确定为所述第三类用户。

7. 一种服务器,其特征在于,包括处理器和存储器;

所述存储器上存储有计算机程序,所述计算机程序在被所述处理器运行时执行如权利要求1至5任一项所述的方法。

8. 一种计算机存储介质,其特征在于,用于储存为权利要求1至5任一项所述方法所用的计算机软件指令。

电子闸门的开启方法、装置及服务器

技术领域

[0001] 本发明涉及安防技术领域,尤其是涉及一种电子闸门的开启方法、装置及服务器。

背景技术

[0002] 随着社会的不断发展,用户的安防意识也随之逐渐加强,门禁系统和电子闸门等设备应运而生。目前,现有的门禁系统或电子闸门等设备,需要刷门禁卡片进入,或者出示身份证件才允许用户进入,导致用户的进出需要经过较为繁琐的过程,从而降低了用户的体验。另外,当来访人员的数量较多时,往往需要每个用户进行身份登记才能进入,不但耗时、耗人力资源,还会进一步降低用户体验。并且当用户的门禁卡片或者身份证件丢失时,可能被他人拾取或冒用,不但将会给用户带来不便,同时还可能带来安全隐患。

发明内容

[0003] 有鉴于此,本发明的目的在于提供一种电子闸门的开启方法、装置及服务器,可以简化用户经过电子闸门时的操作步骤,进而提高用户体验;同时还可以提高电子闸门的安全性。

[0004] 第一方面,本发明实施例提供了一种电子闸门的开启方法,包括:接收目标对象的活体生物特征信息;其中活体生物特征信息携带有账号信息,和/或,电子闸门位置信息;根据活体生物特征信息,确定目标对象所属的用户级别;其中,用户级别与账号信息,和/或,电子闸门位置信息相关;判断用户级别是否配有电子闸门的进入权限;如果是,向目标对象开启电子闸门。

[0005] 结合第一方面,本发明实施例提供了第一方面的第一种可能的实施方式,其中,上述用户级别包括第一类用户、第二类用户、第三类用户和第四类用户;根据活体生物特征信息,确定目标对象所属的用户级别的步骤,包括:根据活体生物特征信息和第一服务器内的各用户的生物特征信息,判断目标对象所属的用户级别是否为第一类用户;如果否,将活体生物特征信息发送至第二服务器,以使第二服务器基于活体生物特征信息进行第二生物特征匹配,得到第二生物特征匹配结果;根据第二生物特征匹配结果判断目标对象所属的用户级别是否为第二类用户;如果否,将活体生物特征信息发送至第三服务器,以使第三服务器基于活体生物特征信息进行第三生物特征匹配,得到第三生物特征匹配结果;根据第三生物特征匹配结果判断目标对象所属的用户级别是否为第三类用户;如果否,确定目标对象所属的用户级别为第四类用户。

[0006] 结合第一方面的第一种可能的实施方式,本发明实施例提供了第一方面的第二种可能的实施方式,其中,上述根据活体生物特征信息和第一服务器内的各用户的生物特征信息,判断目标对象所属的用户级别是否为第一类用户的步骤,包括:获取第一服务器内的各第一类用户的生物特征信息;对活体生物特征信息和各第一类用户的生物特征信息进行第一生物特征匹配;当第一生物特征匹配成功时,将目标对象所属的用户级别确定为第一类用户。

[0007] 结合第一方面的第一种可能的实施方式,本发明实施例提供了第一方面的第三种可能的实施方式,其中,上述将活体生物特征信息发送至第二服务器,以使第二服务器基于活体生物特征信息进行第二生物特征匹配,得到第二生物特征匹配结果;根据第二生物特征匹配结果判断目标对象所属的用户级别是否为第二类用户的步骤,包括:基于活体生物特征信息生成第一识别请求;其中,第一识别请求包括活体生物特征信息和账号信息;将第一识别请求发送至第二服务器,以使第二服务器查找与账号信息对应的各授权用户的生物特征信息,对活体生物特征信息和各授权用户的生物特征信息进行第二生物特征匹配,并返回第二生物特征匹配结果;当第二生物特征匹配成结果为功时,向目标对象的关联终端发送位置确认请求;接收目标对象的关联终端基于位置确认请求返回的位置确认信息,并将目标对象所属的用户级别确定为第二类用户。

[0008] 结合第一方面的第一种可能的实施方式,本发明实施例提供了第一方面的第四种可能的实施方式,其中,上述将活体生物特征信息发送至第三服务器,以使第三服务器基于活体生物特征信息进行第三生物特征匹配,得到第三生物特征匹配结果;根据第三生物特征匹配结果判断目标对象所属的用户级别是否为第三类用户的步骤,包括:基于活体生物特征信息生成第二识别请求;其中,第二识别请求包括活体生物特征信息和电子闸门位置信息;将第二识别请求发送至第二服务器,以使第二服务器获取电子闸门位置信息对应的第一栅格区域内的各当前用户的生物特征信息,和/或,与第一栅格区域相邻的第二栅格区域内的各当前用户的生物特征信息,并对活体生物特征信息和各当前用户的生物特征信息进行第三生物特征匹配,并返回第三生物特征匹配结果;其中,第三服务器对各用户的轨迹进行跟踪,以确定处于第一栅格区域,和/或,第二栅格区域内的各当前用户;当第三生物特征匹配结果为成功时,将目标对象所属的用户级别确定为第三类用户。

[0009] 结合第一方面的第一种可能的实施方式,本发明实施例提供了第一方面的第五种可能的实施方式,其中,上述判断用户级别是否配有电子闸门的进入权限的步骤,包括:当用户级别为第一类用户、第二类用户或第三类用户时,确定用户级别配有电子闸门的进入权限。

[0010] 结合第一方面,本发明实施例提供了第一方面的第六种可能的实施方式,其中,上述方法还包括:将目标对象所属的用户级别发送至关联终端,以使关联终端对应的管理人员查看目标对象的用户级别。

[0011] 第二方面,本发明实施例还提供一种电子闸门的开启装置,包括:接收模块,用于接收目标对象的活体生物特征信息;其中活体生物特征信息携带有账号信息,和/或,电子闸门位置信息;级别确定模块,用于根据活体生物特征信息,确定目标对象所属的用户级别;其中,用户级别与账号信息,和/或,电子闸门位置信息相关;判断模块,用于判断用户级别是否配有电子闸门的进入权限;权限开放模块,用于在判断模块的判断结果为是时,向目标对象开启电子闸门。

[0012] 第三方面,本发明实施例还提供一种服务器,包括处理器和存储器;存储器上存储有计算机程序,计算机程序在被处理器运行时执行如第一方面至第一方面的第六种可能的实施方式任一项的方法。

[0013] 第四方面,本发明实施例还提供一种计算机存储介质,用于储存为第一方面至第一方面的第六种可能的实施方式任一项方法所用的计算机软件指令。

[0014] 本发明实施例带来了以下有益效果：

[0015] 本发明实施例提供的电子闸门的开启方法、装置及服务器，通过接收携带有账号信息或电子闸门位置信息的目标对象的活体生物特征信息，根据该活体生物特征信息以及账号信息或电子闸门位置信息确定用户所属的用户级别，然后判断该用户级别是否配有电子闸门的进入权限，如果有，则允许目标对象进入电子闸门。本发明实施例通过目标对象活体生物特征信息以及账号信息或电子闸门位置信息，判断目标对象是否配有电子闸门的进入权限，省去目标对象刷门禁卡片或者出示身份证件步骤，进而提高用户体验；另外，采用采集活体生物特征信息的方式，可以有效防止他人冒用身份证件等信息，进而提高电子闸门的安全性；同时通过位置信息配合活体生物信息进一步确认是否为为用户对象本人，还可以有效缩减搜寻的范围，从而减少硬件设备的投入和提高用户级别确认的效率。

[0016] 本发明的其他特征和优点将在随后的说明书中阐述，并且，部分地从说明书中变得显而易见，或者通过实施本发明而了解。本发明的目的和其他优点在说明书、权利要求书以及附图中所特别指出的结构来实现和获得。

[0017] 为使本发明的上述目的、特征和优点能更明显易懂，下文特举较佳实施例，并配合所附附图，作详细说明如下。

附图说明

[0018] 为了更清楚地说明本发明具体实施方式或现有技术中的技术方案，下面将对具体实施方式或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施方式，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0019] 图1为本发明实施例提供的一种电子闸门开启方法的流程示意图；

[0020] 图2为本发明实施例提供的另一种电子闸门开启方法的流程示意图；

[0021] 图3为本发明实施例提供的一种电子闸门的开启装置的结构示意图；

[0022] 图4为本发明实施例提供的一种服务器的结构示意图。

具体实施方式

[0023] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合附图对本发明的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0024] 目前，现有的门禁系统或电子闸门等设备，需要刷门禁卡片进入，或者出示身份证件才允许用户进入，导致用户的进出需要经过较为繁琐的过程，从而降低了用户的体验。另外，当来访人员的数量较多时，往往需要每个用户进行身份登记才能进入，不但耗时、耗人力资源，还会进一步降低用户体验。并且当用户的门禁卡片或者身份证件丢失时，可能被他人拾取或冒用，不但将会给用户带来不便，同时还可能带来安全隐患，基于此，本发明实施例提供的一种电子闸门的开启方法、装置及服务器，通过目标对象活体生物特征信息以及账号信息或电子闸门位置信息，判断目标对象是否配有电子闸门的进入权限，省去目标对象刷门禁卡片或者出示身份证件步骤，进而提高用户体验；另外，采用采集活体生物特征

信息的方式,可以有效防止他人冒用身份证件等信息,进而提高电子闸门的安全性。

[0025] 为便于对本实施例进行理解,首先对本发明实施例所公开的一种电子闸门的开启方法进行详细介绍,参见图1所示的一种电子闸门开启方法的流程示意图,该方法包括以下步骤:

[0026] 步骤S102,接收目标对象的活体生物特征信息。

[0027] 在一种实施方式中,可以在电子闸门上设置活体生物特征采集设备,当目标对象希望进入电子闸门时,配合活体生物特征采集设备做出相应操作,以使生物特征信息采集设备获取该目标对象的活体生物特征信息。其中,活体生物特征信息可以为活体人脸信息、活体虹膜信息、活体巩膜信息、活体眼纹信息、活体耳纹信息、活体掌静脉信息、活体指静脉信息、活体掌纹信息或者活体声纹信息等生物特征信息中的一种或多种。优选的,可以采用活体人脸采集设备作为活体生物特征采集设备,通过活体人脸采集设备对目标对象的活体人脸信息进行采集。

[0028] 进一步的,考虑到用户级别与账号信息或电子闸门位置信息相关,所以为了便于对目标对象的用户级别进行识别,上述活体生物特征信息还携带有账号信息,和/或,电子闸门位置信息,当通过活体生物特征采集设备采集到目标对象的活体生物特征信息后,即可以获取电子闸门对应的账号信息或者电子闸门位置信息。在一种实施方式中,当电子闸门应用在住宅小区时,账号信息可以为电子闸门的编号信息,优选的,因为住宅小区存在多个电子闸门,因此账号信息可以为住宅小区对应的账号信息。

[0029] 步骤S104,根据活体生物特征信息,确定目标对象所属的用户级别。

[0030] 针对不同用户类别,预先将用户划分为多个级别,将目标对象的活体生物特征信息与各用户级别内用户的生物特征信息进行匹配,以确定目标对象的用户级别。其中,用户级别与账号信息,和/或,电子闸门位置信息相关。

[0031] 在一种实施方式中,可以将配有电子闸门进入权限的用户划分为三个用户级别,第一类用户可以为小区居民、安保人员和物管人员,第一类用户的生物特征信息存储在第一服务器中,可直接将目标对象的活体生物特征信息与第一服务器中存储的各第一类用户的各生物特征信息进行匹配,如果匹配成功,则可以将目标对象确定为第一类用户;第二类用户可以为辖区警察、当地治安人员、快递员、外卖送餐员、房屋中介和临时工等经常进出小区的人员,第二类用户通过对电子闸门授权或者对电子闸门对应的住宅小区、办公楼等授权,得到第二类用户与电子闸门编号、住宅小区编号或者办公楼编号的对应关系,将目标对象的活体生物特征信息与第二类用户的各生物特征信息进行匹配,如果匹配成功,则可以将目标对象确定为第二类用户;第三类用户可以为身份未知的访客,在电子闸门对应栅格区域内的各用户均可以为第三类用户,具体的,可以获取当前在该电子闸门所处区域内的用户的生物特征信息,以判断目标对象是否为未知访客,从而确定目标对象是否属于第三类用户;并可以对同一个访客一段时期进出小区的频率进行统计,如果超过预设次数,则进行预警,以增加小区的安全性。当目标对象属于上述第一类用户、第二类用户或第三类用户中的任一类用户时,说明目标对象配有该电子闸门的进入权限。进一步的,若在上述三类用户中均未匹配到与目标对象对应的用户信息,则可以将目标对象划分为第四类用户,并且第四类用户没有进入电子闸门的权限和/或进行警报的人群。

[0032] 其中,上述电子闸门可以为智能闸机、智能通道、智能门禁、智能停车场闸门、智能

电梯等等多种设备,并且可以应用在小区大门入口、大楼入口、写字楼大厅、公共场所、展馆、商店或名牌商品店等多种场景,以提供更为安全的、便捷的和可实现电子围栏的门禁系统。

[0033] 步骤S106,判断用户级别是否配有电子闸门的进入权限。

[0034] 通过判断目标对象的用户级别,进而可以判断目标对象是否有电子闸门的进入权限。当目标对象的用户级别为第一类用户、第二类用户或第三类用户中的任一用户级别时,则说明目标对象配有电子闸门的进入权限;当目标对象的用户级别为第四类用户时,则说明目标对象没有电子闸门的进入权限。

[0035] 步骤S108,如果是,向目标对象开启电子闸门。

[0036] 可以理解的,当目标对象属于上述第一类用户、第二类用户或第三类用户中的任一用户级别时,目标对象即可以进入电子闸门,因此需要向目标对象开启电子闸门。

[0037] 本发明实施例提供的电子闸门的开启方法,通过接收携带有账号信息或电子闸门位置信息的目标对象的活体生物特征信息,根据该活体生物特征信息以及账号信息或电子闸门位置信息确定用户所属的用户级别,然后判断该用户级别是否配有电子闸门的进入权限,如果有,则允许目标对象进入电子闸门。本发明实施例通过目标对象活体生物特征信息以及账号信息或电子闸门位置信息,判断目标对象是否配有电子闸门的进入权限,省去目标对象刷门禁卡片或者出示身份证件步骤,进而提高用户体验;另外,采用采集活体生物特征信息的方式,可以有效防止他人冒用身份证件等信息,进而提高电子闸门的安全性;同时通过位置信息配合活体生物信息进一步确认是否为为用户对象本人,还可以有效缩减搜寻的范围,从而减少硬件设备的投入和提高用户级别确认的效率。

[0038] 为便于对上述实施例进行理解,本发明实施例还提供了另一种电子闸门的开启方法,参见图2所示的另一种电子闸门开启方法的流程示意图,该方法包括以下步骤:

[0039] 步骤S202,接收目标对象的活体生物特征信息。

[0040] 其中,当活体生物特征信息为活体人脸信息时,通过人脸信息采集设备获取目标对象的活体人脸信息。另外,还应预先将用户级别划分为第一类用户、第二类用户、第三类用户和第四类用户,以便于对目标对象的用户级别进行判断。

[0041] 步骤S204,根据活体生物特征信息和第一服务器内的各用户的生物特征信息,判断目标对象所属的用户级别是否为第一类用户。如果是,执行步骤S216;如果否,执行步骤S206。

[0042] 优选的,首先采用第一服务器内存储的生物特征信息进行匹配,当目标对象为第一类用户时,则无需进行后续判断,进而可以减少数据交换。其中,第一服务器可以为本地服务器或远程服务器。

[0043] 为了便于理解,本发明实施例提供了一种根据活体生物特征信息和第一服务器内的各用户的生物特征信息,判断目标对象所属的用户级别是否为第一类用户的方法,该方法包括以下步骤:

[0044] (1) 获取第一服务器内的各第一类用户的生物特征信息。

[0045] 当生物特征信息为活体人脸信息时,获取第一服务器内各第一类用户的人脸信息,以基于目标对象的活体人脸信息和各第一类用户的人脸信息判断目标对象是否为第一类用户。

[0046] (2) 对活体生物特征信息和各第一类用户的生物特征信息进行第一生物特征匹配。

[0047] 优选的,先判断目标对象的活体生物特征信息是不是直接来源于真实活体,当目标对象的活体生物特征信息不是直接来源于真实活体时,则将目标对象确定为第四类用户,并不允许目标对象进入电子闸门。

[0048] (3) 当第一生物特征匹配成功时,将目标对象所属的用户级别确定为第一类用户。

[0049] 可以理解的,当第一生物特征匹配成功,说明目标对象在第一服务器内存储有生物特征信息,从而可以将目标对象确定为第一类用户。

[0050] 对于第一类用户,因为采用活体生物特征识别来判断目标对象是否属于第一类用户,可以方便目标对象不携带手机等关联终端,便于第一类用户的进出。通过第一类用户的设置,可以最大限度提供用户的自由度,提高用户体验的同时,允许用户不带手机等设备通过闸门,大大方便了年幼和年长等用户群体自由进出小区等场所。

[0051] 步骤S206,将活体生物特征信息发送至第二服务器,以使第二服务器基于活体生物特征信息进行第二生物特征匹配,得到第二生物特征匹配结果。

[0052] 当目标对象不属于第一类用户时,继续判断目标对象是否属于第二类用户。在一种实施方式中,可以将目标对象的活体生物特征信息发送至第二服务器,由第二服务器根据该活体生物特征信息进行生物特征匹配,进而得知用户是否属于第二类用户。

[0053] 具体的,基于活体生物特征信息生成第一识别请求,其中,第一识别请求包括活体生物特征信息和账号信息,然后将第一识别请求发送至第二服务器,以使第二服务器查找与账号信息对应的各授权用户的生物特征信息,并对活体生物特征信息和各授权用户的生物特征信息进行第二生物特征匹配,得到第二生物特征匹配结果。

[0054] 通过获取账号信息对应的授权用户的生物特征信息,可以有效减少搜索用户生物特征信息的数量,进而提高身份识别速度,提高生物识别的精准度。另外,由于用户已经对该电子闸门、住宅小区或者办公楼进行授权,因此已经对用户的信息进行备案,因此可以更方便进出人员的规范化管理。

[0055] 步骤S208,根据第二生物特征匹配结果判断目标对象所属的用户级别是否为第二类用户。如果是,执行步骤S216;如果否,执行步骤S210。

[0056] 因为目标对象应当位于上述电子闸门附近,所以可以进一步判断目标对象是否与电子闸门相邻。具体的,当第二生物特征匹配成功时,向目标对象的关联终端发送位置确认请求,以使目标对象返回位置确认信息,确认目标对象位置信息与电子闸门位置相邻,此时即可将目标对象确定为第二类用户。

[0057] 对于第二类用户,同样可以采用生物特征识别的方式进行电子闸门,另外,由于仅需要将目标对象的活体生物特征信息与账号信息对应的各生物特征信息进行匹配,无需目标对象的关联终端实时发送位置信息,在提高用户体验的同时,可以有效保护目标对象的位置隐私。

[0058] 步骤S210,将活体生物特征信息发送至第三服务器,以使第三服务器基于活体生物特征信息进行第三生物特征匹配,得到第三生物特征匹配结果。

[0059] 当目标对象不属于第二类用户时,继续判断目标对象是否属于第三类用户。在一种实施方式中,可以将目标对象的活体生物特征信息发送至第三服务器,由第三服务器根

据该活体生物特征信息进行生物特征匹配,进而得知用户是否属于第三类用户。

[0060] 具体的,基于活体生物特征信息生成第二识别请求,其中,第二识别请求包括活体生物特征信息和电子闸门位置信息,然后将第二识别请求发送至第三服务器,以使第三服务器获取电子闸门位置信息对应的第一栅格区域内的各当前用户的生物特征信息,并对活体生物特征信息和各当前用户的生物特征信息进行第三生物特征匹配,当第三生物特征匹配成功时,将目标对象所属的用户级别确定为第三类用户。优选的,当在第一栅格区域内没有匹配到与目标对象对应的当前用户时,考虑到定位误差对栅格区域定位的影响,可以在获取与第一栅格区域相邻的第二栅格区域内的各当前用户的生物特征信息,并进行第三生物特征识别,得到第三生物特征匹配结果。

[0061] 另外,为了得知各用户所处的栅格区域,可以通过第三服务器对各用户的轨迹进行跟踪,以确定处于第一栅格区域和第二栅格区域内的各当前用户。

[0062] 通过获取电子闸门位置信息对应区域内的各用户的生物特征信息,同样可以有效减少搜索用户生物特征信息的数量,进而提高身份识别速度。另外,还可以使第三类用户在不填写任何资料的情况下,自由进出电子闸门,便于第三类用户的进出。优选的,可以记录第三类用户的当天或者近期进出各电子闸门的次数,对于频繁进出的用户可以进行预警,以防止发生治安事件。

[0063] 步骤S212,根据第三生物特征匹配结果判断目标对象所属的用户级别是否为第三类用户。如果是,执行步骤S216;如果否,执行步骤S214。

[0064] 当第三生物特征匹配成功时,即可将目标对象确定为第三类用户。对于第三类用户,无需目标对象在治安岗登记身份,便允许目标对象直接通过电子闸门,为目标对象提供更简单、方便和快捷的进出方式,进而提高目标对象的用户体验。

[0065] 步骤S214,确定目标对象所属的用户级别为第四类用户。

[0066] 可以理解的,当目标对象为第四类用户时,目标对象将无法进入电子闸门内,或者通过安保人员手动打开电子闸门,以允许目标对象进入。

[0067] 当用户级别为第一类用户、第二类用户或第三类用户时,确定用户级别配有电子闸门的进入权限。

[0068] 步骤S216,向目标对象开启电子闸门。

[0069] 本发明实施例提供的电子闸门的开启方法,通过活体生物特征采集设备获取目标对象的活体生物特征信息,并根据该活体生物特征信息依次判断目标对象是否属于第一类用户、第二类用户或第三类用户,如果是,则允许目标对象进入,如果不是,则将目标对象确定为第四类用户,并且不允许目标对象进入电子闸门。本发明实施例通过采集目标对象活体生物特征信息,来判断目标对象是否配有电子闸门的进入权限,省去目标对象刷门禁卡片或者出示身份证件步骤,进而提高用户体验;另外,采用采集活体生物特征信息的方式,可以有效防止他人冒用身份证件等信息,进而提高电子闸门的安全性。

[0070] 进一步的,可以将目标对象所属的用户级别发送至关联终端,以使关联终端对应的管理人员查看目标对象的用户级别,甚至保存目标对象的进出记录。另外,当目标对象属于第四类用户时,在关联终端上显示目标对象属于第四类用户,以使管理人员判断是否允许目标对象进入,若允许目标对象进入,则应到相应的值班室进行访客登记。

[0071] 进一步的,可以联动涉稳人员库,通过对目标对象的生物特征信息进行身份识别,

判断目标对象是否为涉稳人员,如果是则通知保安或者管理人员,做进一步处理。另外,还可以联动失踪人口库,通过对目标对象的生物特征信息进行身份识别,判断目标对象是否为失踪人口或者诸如精神疾病或者老年痴呆等状态异常人员,如果是则通知保安或者管理人员,做进一步处理。

[0072] 对于前述实施例提供的电子闸门的开启方法,本发明实施例还提供了一种电子闸门的开启装置,参见图3所示的一种电子闸门的开启装置的结构示意图,该装置包括以下部分:

[0073] 接收模块302,用于接收目标对象的活体生物特征信息;其中活体生物特征信息携带有账号信息,和/或,电子闸门位置信息。

[0074] 级别确定模块304,用于根据活体生物特征信息,确定目标对象所属的用户级别;其中,用户级别与账号信息,和/或,电子闸门位置信息相关。

[0075] 判断模块306,用于判断用户级别是否配有电子闸门的进入权限。

[0076] 权限开放模块308,用于在判断模块的判断结果为是时,向目标对象开启电子闸门。

[0077] 本发明实施例提供的电子闸门的开启装置,信息获取模块通过活体生物特征采集设备获取目标对象的活体生物特征信息,并由级别确定模块根据该活体生物特征信息确定用户所属的用户级别,然后判断模块判断该用户级别是否配有电子闸门的进入权限,如果有,权限开放模块则允许目标对象进入电子闸门。本发明实施例通过采集目标对象活体生物特征信息,来判断目标对象是否配有电子闸门的进入权限,省去目标对象刷门禁卡片或者出示身份证件的步骤,进而提高用户体验;另外,采用采集活体生物特征信息的方式,可以有效防止他人冒用身份证件等信息,进而提高电子闸门的安全性;同时通过位置信息配合活体生物信息进一步确认是否为为用户对象本人,还可以有效缩减搜寻的范围,从而减少硬件设备的投入和提高用户级别确认的效率。

[0078] 本发明实施例所提供的装置,其实现原理及产生的技术效果和前述方法实施例相同,为简要描述,装置实施例部分未提及之处,可参考前述方法实施例中相应内容。

[0079] 该设备为一种服务器,具体的,该服务器包括处理器和存储装置;存储装置上存储有计算机程序,计算机程序在被所述处理器运行时执行如上所述实施方式的任一项所述的方法。

[0080] 图4为本发明实施例提供的一种服务器的结构示意图,该服务器100包括:处理器40,存储器41,总线42和通信接口43,所述处理器40、通信接口43和存储器41通过总线42连接;处理器40用于执行存储器41中存储的可执行模块,例如计算机程序。

[0081] 其中,存储器41可能包含高速随机存取存储器(RAM,Random Access Memory),也可能还包括非不稳定的存储器(non-volatile memory),例如至少一个磁盘存储器。通过至少一个通信接口43(可以是有线或者无线)实现该系统网元与至少一个其他网元之间的通信连接,可以使用互联网,广域网,本地网,城域网等。

[0082] 总线42可以是ISA总线、PCI总线或EISA总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图4中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[0083] 其中,存储器41用于存储程序,所述处理器40在接收到执行指令后,执行所述程

序,前述本发明实施例任一实施例揭示的流过程定义的装置所执行的方法可以应用于处理器40中,或者由处理器40实现。

[0084] 处理器40可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器40中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器40可以是通用处理器,包括中央处理器(Central Processing Unit,简称CPU)、网络处理器(Network Processor,简称NP)等;还可以是数字信号处理器(Digital Signal Processing,简称DSP)、专用集成电路(Application Specific Integrated Circuit,简称ASIC)、现成可编程门阵列(Field-Programmable Gate Array,简称FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本发明实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本发明实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器41,处理器40读取存储器41中的信息,结合其硬件完成上述方法的步骤。

[0085] 本发明实施例所提供的工艺防错方法、装置及服务器的计算机程序产品,包括存储了处理器可执行的非易失的程序代码的计算机可读存储介质,计算机可读存储介质上存储有计算机程序,该计算机程序被处理器运行时执行前面方法实施例中所述的方法,具体实现可参见方法实施例,在此不再赘述。

[0086] 所属领域的技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统具体工作过程,可以参考前述实施例中的对应过程,在此不再赘述。

[0087] 本发明实施例所提供的可读存储介质的计算机程序产品,包括存储了程序代码的计算机可读存储介质,所述程序代码包括的指令可用于执行前面方法实施例中所述的方法,具体实现可参见方法实施例,在此不再赘述。

[0088] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用,可以存储在一个计算机可读存储介质中。基于这样的理解,本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括: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。

[0089] 最后应说明的是:以上所述实施例,仅为本发明的具体实施方式,用以说明本发明的技术方案,而非对其限制,本发明的保护范围并不局限于此,尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:任何熟悉本技术领域的技术人员在本发明揭露的技术范围内,其依然可以对前述实施例所记载的技术方案进行修改或可轻易想到变化,或者对其中部分技术特征进行等同替换;而这些修改、变化或者替换,并不使相应技术方案的本质脱离本发明实施例技术方案的精神和范围,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应所述以权利要求的保护范围为准。

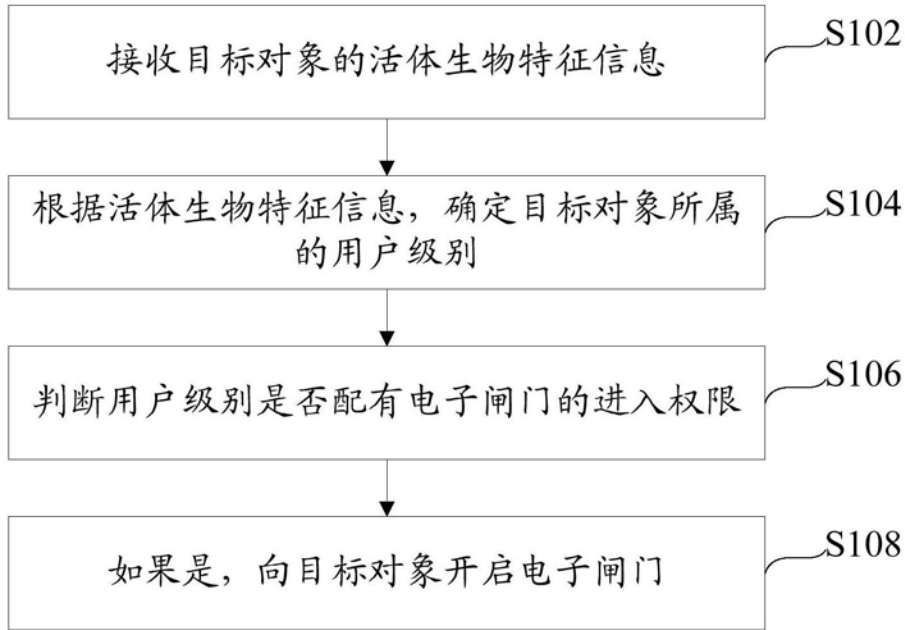


图1

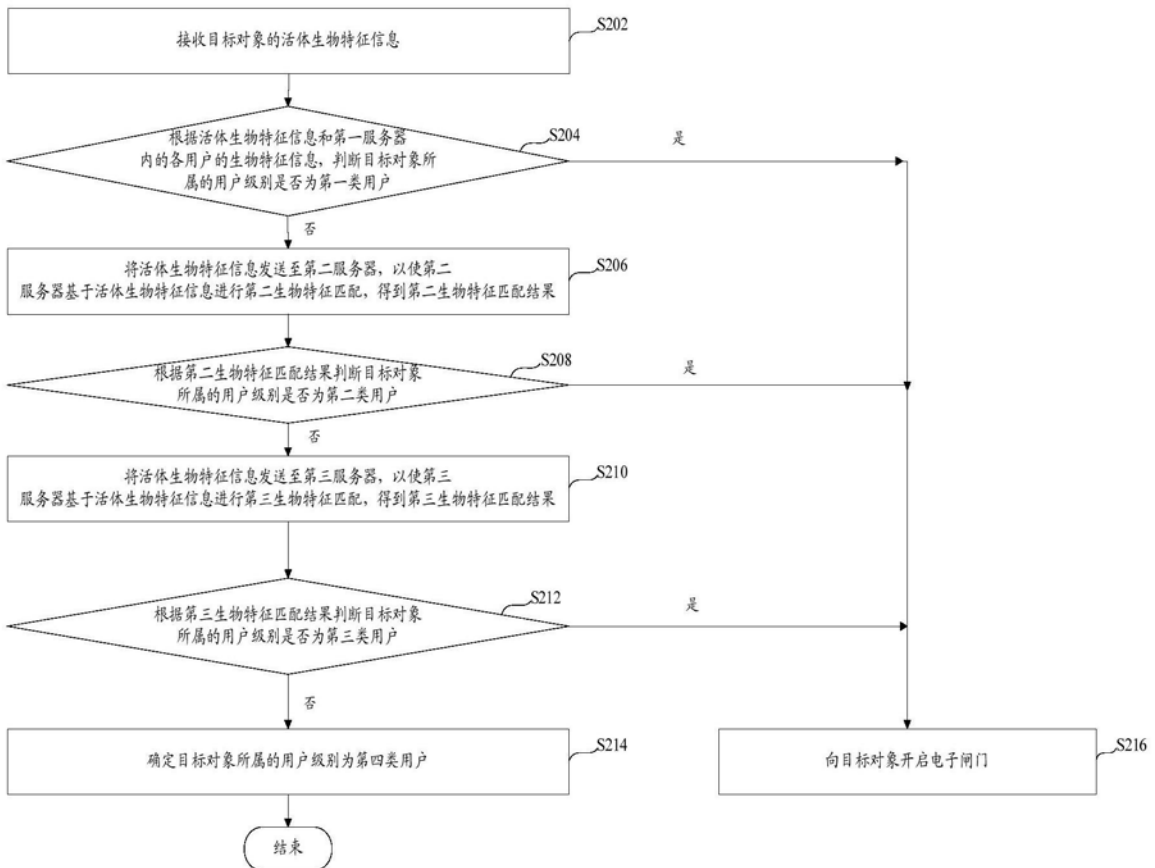


图2



图3

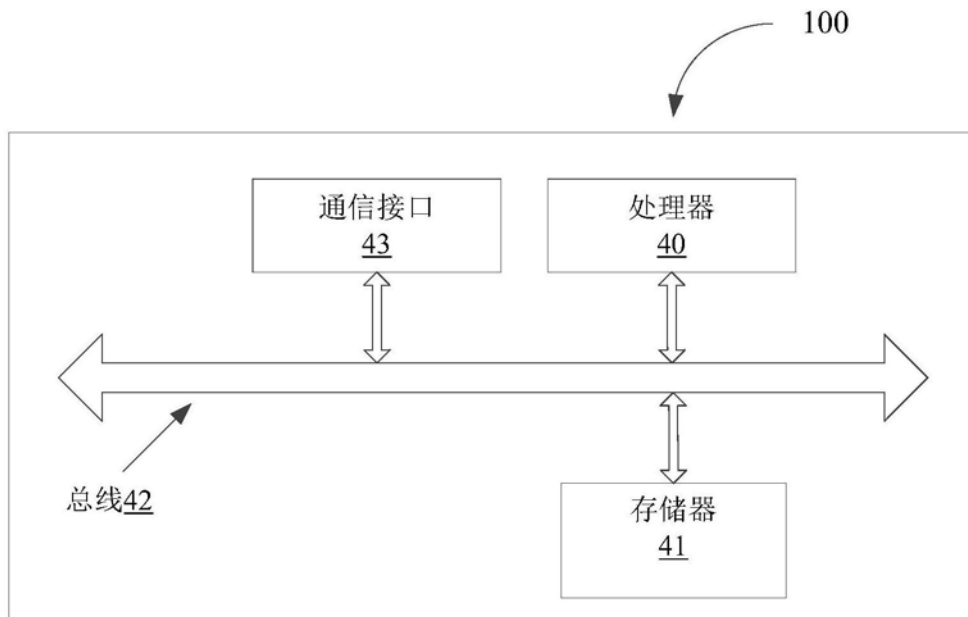


图4