

一种身份验证方法、系统、装置及设备

技术领域

[01] 本说明书涉及信息技术领域，尤其涉及一种身份验证方法、系统、装置及设备。

背景技术

- 5 [02] 目前，基于人脸识别的身份验证技术方兴未艾。在实际应用中，可以在超市、地铁站等场所布置可采集人脸图像的身份验证系统，身份验证系统用于对进入验证区域的用户进行身份验证。

- [03] 具体地，以用户乘坐地铁的场景为例，可以在地铁站布置身份验证系统，用户若想要乘坐地铁，则需要进入验证区域，身份验证系统会采集用户的人脸图像以及获取用户
10 出示的账户标识，然后判断采集的人脸图像和预先存储的对应于该账户标识的人脸图像是否匹配，若是，则确定用户通过身份验证并指令地铁闸机开启，允许用户进站乘车。

[04] 基于现有技术，需要一种更为便捷的身份验证方法。

发明内容

- [05] 本说明书实施例提供一种身份验证方法、系统、装置及设备，以解决现有的身份验证方法存在的对用户而言不够便捷的问题。
15

[06] 为解决上述技术问题，本说明书实施例是这样实现的：

[07] 本说明书实施例提供一种身份验证方法，包括：

[08] 获取位于验证区域外的用户的实时人脸图像，并存储获取到的实时人脸图像；

[09] 获取进入验证区域内的用户提供的身份标识；

- 20 [10] 根据获取到的身份标识，获取所述身份标识对应的预存人脸图像；

[11] 根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[12] 本说明书实施例提供的另一种身份验证方法，包括：

[13] 服务器通过采集设备获取并存储位于验证区域外的用户的实时人脸图像；

[14]所述服务器接收所述采集设备发送的身份标识；所述身份标识是进入验证区域内的用户提供给所述采集设备的；

[15]所述服务器根据所述身份标识，获取所述身份标识对应的预存人脸图像；

5 [16]所述服务器根据存储的各实时人脸图像和确定的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[17]本说明书实施例提供的另一种身份验证方法，包括：

[18]采集设备采集位于验证区域外的用户的实时人脸图像；

[19]采集设备将获取的实时人脸图像发送给服务器进行存储；

[20]采集设备获取进入验证区域内的用户提供的身份标识；

10 [21]采集设备将获取的身份标识发送给服务器，以使所述服务器根据接收到的身份标识，获取所述身份标识对应的预存人脸图像，进而根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。本说明书实施例提供的一种身份验证系统，包括：包括采集设备和服务器；

15 [22]所述采集设备，获取实时人脸图像或实时图像，并将获取的实时人脸图像或实时图像发送给所述服务器，所述实时人脸图像是位于验证区域外的用户的实时人脸图像，所述实时图像是验证区外的实时图像；以及，获取进入验证区域内的用户提供的身份标识，并将获取的身份标识发送给所述服务器；

[23]所述服务器，接收并存储所述采集设备发送的实时人脸图像，或接收所述采集设备发送的实时图像，从所述实时图像中提取人脸图像，作为实时人脸图像并存储；以及，
20 接收所述采集设备发送的身份标识，根据所述身份标识获取所述身份标识对应的预存人脸图像，根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[24]本说明书实施例提供的一种身份验证装置，包括：

[25]第一获取模块，通过采集设备获取并存储位于验证区域外的用户的实时人脸图像；

25 [26]接收模块，接收所述采集设备发送的身份标识；所述身份标识是进入验证区域内的用户提供给所述采集设备的；

[27]第二获取模块，根据所述身份标识，获取所述身份标识对应的预存人脸图像；

[28]身份验证模块,根据存储的各实时人脸图像和确定的预存人脸图像,对所述进入验证区域内的用户进行身份验证。

[29]本说明书实施例提供的一种服务器,包括一个或多个处理器及存储器,所述存储器存储有程序,并且被配置成由所述一个或多个处理器执行以下步骤:

5 [30]通过采集设备获取并存储位于验证区域外的用户的实时人脸图像;

[31]所述服务器接收所述采集设备发送的身份标识;所述身份标识是进入验证区域内的用户提供给所述采集设备的;

[32]所述服务器根据所述身份标识,获取所述身份标识对应的预存人脸图像;

10 [33]所述服务器根据存储的各实时人脸图像和确定的预存人脸图像,对所述进入验证区域内的用户进行身份验证。

[34]本说明书实施例提供的另一种身份验证装置,包括:

[35]第一获取模块,获取位于验证区域外的用户的实时人脸图像;

[36]第一发送模块,将获取的实时人脸图像发送给服务器进行存储;

[37]第二获取模块,获取进入验证区域内的用户提供的身份标识;

15 [38]第二发送模块,将获取的身份标识发送给服务器,以使所述服务器根据接收到的身份标识,获取所述身份标识对应的预存人脸图像,进而根据存储的各实时人脸图像和获取的预存人脸图像,对所述进入验证区域内的用户进行身份验证。

[39]本说明书实施例提供的一种采集设备,包括:图像采集器、身份标识采集器、通信单元;

20 [40]所述图像采集器,采集位于验证区域外的用户的实时人脸图像;

[41]所述身份标识采集器,获取进入验证区域内的用户提供的身份标识;

[42]所述通信单元,将获取的实时人脸图像和获取的身份标识发送给服务器,以使所述服务器存储接收到的实时人脸图像,以及根据接收到的身份标识,获取所述身份标识对应的预存人脸图像,进而根据存储的各实时人脸图像和获取的预存人脸图像,对所述进入验证区域内的用户进行身份验证。

25

[43]由以上本说明书实施例提供的技术方案可见,在本说明书实施例中,在用户进入验证区域之前,身份验证系统就可以获取并存储用户的实时人脸图像;待用户进入验证区

域之后，身份验证系统只需获取到用户提供的身份标识，即可根据获取到的身份标识获取该身份标识对应的预存人脸图像，进而根据存储的实时人脸图像和获取的预存人脸图像，对用户进行身份验证。如此一来，用户进入验证区域后，身份验证系统只要获取到用户提供的身份标识，就可以很快完成对用户的身份验证，无需再耗费时间采集用户的实时人脸图像。也就是说，用户进入验证区域后，等待较短时间即可完成身份验证。

附图说明

[44]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例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，下面描述中的附图仅仅是本说明书中记载的一些实施例，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。

- [45]图 1 是现有技术中对进站乘车的用户进行身份验证的示意图；
- [46]图 2 是本说明书实施例提供的身份验证方法流程图；
- [47]图 3 是本说明书实施例提供的进站乘车的场景下验证区域与指定有限区域的位置关系示意图；
- 15 [48]图 4 是本说明书实施例提供的在乘车进站的场景下，用户排队进入验证区域的示意图；
- [49]图 5 是本说明书实施例提供的一种身份验证系统示意图；
- [50]图 6 是本说明书实施例提供的另一种身份验证方法流程图；
- [51]图 7 是本说明书实施例提供的另一种身份验证方法流程图；
- 20 [52]图 8 是本说明书实施例提供的一种身份验证装置示意图；
- [53]图 9 是本说明书实施例提供的一种服务器示意图；
- [54]图 10 是本说明书实施例提供的另一种身份验证装置示意图；
- [55]图 11 是本说明书实施例提供的一种采集设备示意图；
- [56]图 12 是本说明书实施例提供的布置采集设备的示意图。

具体实施方式

[57]在现有的基于人脸识别的身份验证方法中，通常采用“身份标识+实时人脸图像”的方式对用户进行身份验证，其目的在于判断用户是否为其提供的身份标识的实际拥有者。其中，所述身份标识可以唯一标识用户的身份，所述身份标识具体可以是账户标识、
5 账号、手机号、身份证号等；所述实时人脸图像是身份验证系统针对要进行身份验证的用户所采集的人脸图像。

[58]可见，针对待验证的每个用户，对该用户进行身份验证的前提是获取到该用户提供的“身份标识+实时人脸图像”组合。实践中，通常会预先划定用于进行身份验证的指定区域（本文将之称为验证区域），要求用户进入验证区域内，向身份验证系统一并提供
10 供自己要使用的身份标识和自己的实时人脸图像（通常由身份验证系统实时采集得到）。

[59]具体而言，针对进入验证区域的每个用户，身份验证系统一方面要采集该用户的实时人脸图像，另一方面要获取用户出示的身份标识，然后，身份验证系统会对采集的该实时人脸图像和对应于该身份标识的预存人脸图像（即该身份标识的实际拥有者的人脸图像）进行比对，若二者匹配，则确定该用户是其出示的身份标识的实际拥有者，该用
15 户可通过身份验证。

[60]图 1 是现有技术中对进站乘车的用户进行身份验证的示意图。如图 1 所示，用户若想要进站乘车，需要站在验证区域内，向身份验证系统出示证件（具体可以是车票、身份证等），并配合身份验证系统采集自己的实时人脸图像。

[61]但是，如图 1 所示，身份验证系统采集用户的实时人脸图像需要耗费一定的时间（通常需要几秒），倘若用户进入验证区域后并未立刻面向摄像头，导致无法进行人脸图像的采集，那么身份验证系统采集用户的实时人脸图像所耗费的时间会更长。可见，在身份验证系统采集到用户实时人脸图像之前，用户不得不在验证区域内等待，这对用户而言并不便捷。尤其是，在图 1 所示的进站乘车的场景下，有时会有很多用户排队进站，若队列中的每个用户进入验证区域后对需要等待几秒，则会明显拖慢进站队列的前进速度。
25 度。

[62]而在本说明书实施例中，在用户进入验证区域之前，身份验证系统可以获取并存储用户的实时人脸图像；待用户进入验证区域之后，身份验证系统只需获取到用户提供的身份标识，即可对用户进行身份验证。通过本说明书实施例，用户进入验证区域后，不必配合身份验证系统采集实时人脸图像并等待较长时间，仅需要出示身份证和车票，即

可快速完成身份验证后进站，这对用户而言更为便捷。并且，当有很多用户排队等待进站时，进站队列的推进速度也大为提升。

[63]为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书一个或多个实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，
5 显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。通过本说明书实施例，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，都应当属于本说明书保护的范围。

[64]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[65]图 2 是本说明书实施例提供的身份验证方法流程图，包括以下步骤：

10 [66]S200: 获取位于验证区域外的用户的实时人脸图像，并存储获取到的实时人脸图像。

[67]本说明书实施例所应用的场景为在线下的业务现场对用户进行身份验证，以判断用户是否为其出示的身份标识的实际拥有者。例如，在移动支付的场景下，通过身份验证的用户可以使用其出示的身份标识（具体是账户标识）对应的账户进行支付。又如，在进站乘车的场景下，用户通过身份验证后，可以使用其持有的车票进站乘车。更具体地，
15 本发明所应用的场景可以是多个用户排队，依次进入验证区域进行验证，如排队进站乘车、在超市排队结算等场景。为了描述的方便，后文主要以进站乘车的场景为例说明。

[68]本方法的执行主体可以由一个或多个装置组成的身份验证系统。

[69]在本说明书实施例中，身份验证系统仅会对进入验证区域的用户进行身份验证，对身份验证系统而言，进入所述验证区域的用户即是需要接受身份验证的用户。位于所述
20 验证区域外的用户可以是等待进入验证区域接受身份验证的用户，也可以是无意接受身份验证的用户。

[70]在本说明书实施例中，位于验证区域外等待进入验证区域的用户可以配合身份验证系统进行实时人脸图像的采集。由于位于验证区域外的用户通常处于等待进入验证区域的状态，因此，对这些用户进行实时人脸图像的采集，并不会额外耗用户的时间。

25 [71]此外，在现有技术中，针对进入验证区域的每个用户，通常会要求该用户配合身份验证系统进行实时人脸采集，如图 1 所示，用户需要面对摄像头进行实时人脸采集。而在本说明书实施例中，身份验证系统获取验证区域外的用户的实时人脸图像的方式可以是获取验证区域外的实时图像，从所述实时图像中提取人脸图像，作为位于所述验证区域外的用户的实时人脸图像。

[72]其中，所述实时图像通常是身份验证系统对验证区域外进行监控得到的，也就是说，所述实时图像显示的画面反映的是位于验证区域外的用户的实时状态。

[73]在本说明书实施例中，用户的实时状态通常是较为随意的状态（用户有时面向摄像头，有时并不面向摄像头），因此，为了确保所述实时图像可以记录到位于验证区域外的各用户的人脸，可以布置多个摄像头，从多个方向对验证区域外进行拍摄。如此，哪怕位于验证区域外的用户的状态是较为随意的，用户的人脸总会在某个瞬间被某个摄像头捕捉到，用户的人脸就会被所述实时图像记录下来，身份验证系统就可以从所述实时图像中提取到该用户的实时人脸图像。

[74]在本说明书实施例中，所述实时图像实际上是包含连续的若干帧画面的视频。其中，每帧画面记录了验证区域外某个瞬间的图像。身份验证系统实际上是从实时图像包含的每帧画面中提取人脸图像，作为实时人脸图像。因此，只要验证区域外的用户在某个瞬间被摄像头捕捉到人脸，身份验证系统就可以从实时图像中提取到该用户的实时人脸图像。如此，在验证区域外等候验证的用户可以无需花费注意力配合摄像头进行人脸图像的采集，身份验证系统依然可以采集到位于验证区域外的用户的实时人脸图像。这对用户而言也更为便利。

[75]进一步地，身份验证系统可以对所述验证区域外的指定区域进行监控，得到实时图像。所述指定区域的尺寸、所述指定区域与所述验证区域的位置关系都可以根据需要指定。举例来说，如图3所示，在进站乘车的场景下，所述指定区域可以是在进站队列前进方向的反方向上，距离所述验证区域1m的矩形区域（可称等待区域），所述等待区域的宽为所述验证区域的宽，所述等待区域的长为10m。进站队列中的用户会先经过所述等待区域，随后再进入验证区域。

[76]S202：获取进入验证区域内的用户提供的身份标识。

[77]在本说明书实施例中，进入验证区域的用户可以采用各种方式向身份验证系统提供身份标识。例如，用户可以向身份验证系统出示二维码，由身份验证系统通过扫描该二维码获取该用户提供的身份标识，用户也可以通过身份验证系统提供的输入装置（如输入面板、触摸屏、键盘等）输入身份标识。

[78]此外，身份验证系统从进入验证区域内的用户所携带的射频识别（Radio Frequency Identification, RFID）标签或近场通信（Near Field Communication, NFC）芯片中读取身份标识。也就是说，所述验证区域可以是射频识别感应区或近场通信感应区，用户进

入验证区域后，无需主动出示身份标识，身份验证系统可以通过阅读器从用户携带的RFID 标签或 NFC 芯片中读取身份标识，这可以进一步加快身份验证的速度。

[79]S204：根据获取到的身份标识，获取所述身份标识对应的预存人脸图像。

5 [80]S206：根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[81]在本说明书实施例中，所述身份标识对应的预存人脸图像是预先存储的所述身份标识的实际拥有者的人脸图像。

10 [82]身份验证系统可以判断存储的各实时人脸图像是否存在与获取的预存人脸图像相匹配的实时人脸图像；若是，则确定所述用户通过身份验证；否则，确定所述用户未通过身份验证。

15 [83]通过图 2 所示的身份验证方法，在用户进入验证区域之前，身份验证系统可以获取并存储用户的实时人脸图像；待用户进入验证区域之后，身份验证系统只需获取到用户提供的身份标识，即可根据获取到的身份标识获取该身份标识对应的预存人脸图像，进而根据存储的实时人脸图像和获取的预存人脸图像，对用户进行身份验证。如此一来，用户进入验证区域后，身份验证系统只要获取到用户提供的身份标识，就可以很快完成对用户的身份验证，无需再耗费时间采集用户的实时人脸图像。也就是说，用户进入验证区域后，等待较短时间即可完成身份验证。

20 [84]此外，图 4 是在乘车进站的场景下，用户排队进入验证区域的示意图。如图 4 所示，进站队列中的用户离摄像头越近，身份验证系统采集的该用户的人脸图像的尺寸就越大，进站队列中的用户离摄像头越远，身份验证系统采集的该用户的人脸图像的尺寸就越小。例如，在实时图像包含的某一帧画面中，用户 1 的人脸图像的尺寸大于用户 2 的人脸图像的尺寸，用户 2 的人脸图像的尺寸大于用户 3 的人脸图像的尺寸，以此类推。可见，对于实时人脸图像过小的用户，该用户进入验证区域还需要较长时间，为了避免身份验证设备后续需要比对的实时人脸图像过多，提升后续的验证效率，可以不从实时图像中提取尺寸过小的人脸图像；对于实时人脸图像过大的用户，该用户可能已经进入或即将进入验证区域，身份验证系统之前很可能已经存储了该用户的实时人脸图像，因此，同样基于提升后续的验证效率的考虑，可以不从实时图像中提取尺寸过大的人脸图像。

[85]基于上述说明，身份验证系统可以从所述实时图像中提取尺寸落入指定尺寸范围内

的人脸图像,作为实时人脸图像。所述指定尺寸范围可以根据所述指定有限区域的大小、所述指定有限区域与所述验证区域的位置关系、摄像头的拍摄参数等确定。如此,不提取尺寸过大或过小的实时人脸图像,可以使存储的实时人脸图像数量较少,后续可以有效提高身份验证的效率。

5 [86]还需要说明的是,在进站乘车的场景下,由于进站队列中的每个用户需要花费一定的时间从验证区域外进入验证区域,因此,身份验证系统获取的验证区域外的实时图像也会记录下用户从验证区域外进入验证区域的整个过程。如图4所示,实时图像会记录下进站队列中的每个用户从通过指定有限区域的整个过程。这就会导致身份验证系统从所述实时图像的各帧画面中提取的人脸图像中可能存在大量重复的情况,为了避免这种情况,身份验证系统从所述实时图像中提取人脸图像的方式可以是:根据预设的抽取规则,从所述实时图像中抽取若干帧画面,然后针对抽取的每帧画面,从该帧画面中提取人脸图像。所述抽取规则可以是每当指定周期(如200ms)经过时,从所述实时图像中抽取当前显示的画面。

15 [87]进一步地,身份验证系统可以从存储的实时人脸图像中删除指定时间段以前获取的实时人脸图像,也即,所述身份验证系统存储的实时人脸图像总是最近指定时间段内获取的实时人脸图像。在进站乘车的场景下,身份验证系统不需要存储已经经过身份验证的用户的实时人脸图像。所述指定时间段可以根据需要指定,使得身份验证系统删除的指定时间段以前获取的实时人脸图像尽可能是已经经过身份验证的用户的实时人脸图像,身份验证系统存储的最近指定时间段内获取的实时人脸图像尽可能是未进行身份验证的用户的实时人脸图像。这样,可以减少步骤S206中需要比对的实时人脸图像的数量,提升身份验证系统的验证速度。

20 [88]图5是本说明书实施例提供的一种身份验证系统示意图,包括采集设备501和服务

器502;

[89]所述采集设备501,获取实时人脸图像或实时图像,并将获取的实时人脸图像或实时图像发送给所述服务器,所述实时人脸图像是位于验证区域外的用户的实时人脸图像,所述实时图像是验证区外的实时图像;以及,获取进入验证区域内的用户提供的身份标识,并将获取的身份标识发送给所述服务器;

[90]所述服务器502,接收并存储所述采集设备发送的实时人脸图像,或接收所述采集设备发送的实时图像,从所述实时图像中提取人脸图像,作为实时人脸图像并存储;以及,接收所述采集设备发送的身份标识,根据所述身份标识获取所述身份标识对应的预

存人脸图像，根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[91]也就是说，图 2 所示的身份验证流程的执行主体可以是所述采集设备和所述服务器。其中，所述采集设备通常布置于线下，可以在现场获取位于验证区域外的用户实时人脸图像，以及获取进入验证区域的用户提供的身份标识。

[92]图 6 是本说明书实施例提供的另一种身份验证方法流程图，包括以下步骤：

[93]S600：服务器通过采集设备获取并存储位于验证区域外的用户的实时人脸图像；

[94]S602：所述服务器接收所述采集设备发送的身份标识；所述身份标识是进入验证区域内的用户提供给所述采集设备的；

10 [95]S604：所述服务器根据所述身份标识，获取所述身份标识对应的预存人脸图像；

[96]S606：所述服务器根据存储的各实时人脸图像和确定的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[97]图 6 所示的方法的执行主体是服务器。具体地，在步骤 S600 中，服务器可以接收采集设备发送的位于验证区域外的用户的实时人脸图像，也可以接收采集设备发送的验证区域外的实时图像，从所述实时图像中提取人脸图像，作为位于验证区域外的用户的实时人脸图像。

[98]图 7 是本说明书实施例提供的另一种身份验证方法流程图，包括以下步骤：

[99]S700：采集设备获取位于验证区域外的用户的实时人脸图像。

[100] S702：采集设备将获取的实时人脸图像发送给服务器进行存储。

20 [101] S704：采集设备获取进入验证区域内的用户提供的身份标识。

[102] S706：采集设备将获取的身份标识发送给服务器。

[103] 图 7 所示的方法的执行主体是采集设备。在步骤 S706 中，采集设备将获取的身份标识发送给服务器，以使所述服务器根据接收到的身份标识，获取所述身份标识对应的预存人脸图像，进而根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[104] 进一步地，在步骤 S700 中，采集设备可以采集验证区域外的实时图像，从所述实时图像中提取人脸图像，作为位于验证区域外的用户的实时人脸图像。

[105] 基于图 6 所示的身份验证方法, 本说明书实施例对应提供一种身份验证装置, 如图 8 所示, 包括:

[106] 第一获取模块 801, 通过采集设备获取并存储位于验证区域外的用户的实时人脸图像;

5 [107] 接收模块 802, 接收所述采集设备发送的身份标识; 所述身份标识是进入验证区域内的用户提供给所述采集设备的;

[108] 第二获取模块 803, 根据所述身份标识, 获取所述身份标识对应的预存人脸图像;

[109] 身份验证模块 804, 根据存储的各实时人脸图像和确定的预存人脸图像, 对所述进入验证区域内的用户进行身份验证。

10 [110] 所述第一获取模块 801, 接收采集设备发送的位于验证区域外的用户的实时人脸图像; 或接收采集设备发送的验证区域外的实时图像, 从所述实时图像中提取人脸图像, 作为位于验证区域外的用户的实时人脸图像。

[111] 基于图 6 所示的身份验证方法, 本说明书实施例还对应提供了一种服务器, 如图 9 所示, 包括一个或多个处理器及存储器, 所述存储器存储有程序, 并且被配置成由

15 所述一个或多个处理器执行以下步骤:

[112] 通过采集设备获取并存储位于验证区域外的用户的实时人脸图像;

[113] 接收所述采集设备发送的身份标识; 所述身份标识是进入验证区域内的用户提供给所述采集设备的;

[114] 根据所述身份标识, 获取所述身份标识对应的预存人脸图像;

20 [115] 根据存储的各实时人脸图像和确定的预存人脸图像, 对所述进入验证区域内的用户进行身份验证。

[116] 基于图 7 所示的身份验证方法, 本说明书实施例还对应提供了一种身份验证装置, 如图 10 所示, 包括:

[117] 第一获取模块 1001, 获取位于验证区域外的用户的实时人脸图像;

25 [118] 第一发送模块 1002, 将获取的实时人脸图像发送给服务器进行存储;

[119] 第二获取模块 1003, 获取进入验证区域内的用户提供的身份标识;

[120] 第二发送模块 1004, 将获取的身份标识发送给服务器, 以使所述服务器根据接

收到的身份标识，获取所述身份标识对应的预存人脸图像，进而根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

[121] 所述第一获取模块 1001，获取验证区域外的实时图像；从所述实时图像中提取人脸图像，作为位于验证区域外的用户的实时人脸图像。

5 [122] 基于图 7 所示的身份验证方法，本说明书实施例还对应提供了一种采集设备，如图 11 所示，包括：图像采集器、身份标识采集器、通信单元；

[123] 所述图像采集器，采集位于验证区域外的用户的实时人脸图像；

[124] 所述身份标识采集器，获取进入验证区域内的用户提供的身份标识；

10 [125] 所述通信单元，将获取的实时人脸图像和获取的身份标识发送给服务器，以使所述服务器存储接收到的实时人脸图像，以及根据接收到的身份标识，获取所述身份标识对应的预存人脸图像，进而根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。

15 [126] 所述图像采集器包括至少两个摄像头；各摄像头分别安装于不同的位置，用于从不同方向对所述验证区域外进行拍摄，具体可以图 12。如图 12 所示，针对每个地铁闸机，可以在该地铁闸机处布置两个采集设备，每个采集设备上安装有一个摄像头，摄像头的高度、拍摄方向以及角度可以根据需要调整。

20 [127] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于图 10 所示的服务器而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

25 [128] 在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array, FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成

电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language, HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、

5 AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言

10 稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[129] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读存储介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit, ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌

15 入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[130] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字符助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

25

[131] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

30

[132] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[133] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[134] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[135] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[136] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和计算机可读存储介质。

[137] 计算机可读存储介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机可读存储介质的例子包括，但不限于相变内存（PRAM）、静态随机存取存储器（SRAM）、动态随机存取存储器（DRAM）、其他类型的随机存取存储器（RAM）、只读存储器（ROM）、电可擦除可编程只读存储器（EEPROM）、快闪记忆体或其他内存技术、只读光盘只读存储器（CD-ROM）、数字多功能光盘（DVD）或其他光学存储、磁盒式磁带、磁带磁磁盘存储或其他磁性存储设备或任何其他传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读存储介质

不包括暂存电脑可读媒体（transitory media），如调制的数据信号和载波。

[138] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[139] 本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

权利要求书

- 1、一种身份验证方法，包括：

获取位于验证区域外的用户的实时人脸图像，并存储获取到的实时人脸图像；

获取进入验证区域内的用户提供的身份标识；
- 5 根据获取到的身份标识，获取所述身份标识对应的预存人脸图像；
- 根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证。
- 2、如权利要求 1 所述的方法，获取位于验证区域外的用户的实时人脸图像，具体包括：
- 10 获取验证区域外的实时图像；
- 从所述实时图像中提取人脸图像，作为位于所述验证区域外的用户的实时人脸图像。
- 3、如权利要求 2 所述的方法，从所述实时图像中提取人脸图像，具体包括：
- 从所述实时图像中提取尺寸落入指定尺寸范围内的人脸图像。
- 15 4、如权利要求 1 所述的方法，所述方法还包括：
- 从存储的实时人脸图像中删除指定时间段以前获取的实时人脸图像。
- 5、如权利要求 1 所述的方法，获取进入验证区域内的用户提供的身份标识，具体包括：
- 从进入验证区域内的用户所携带的射频识别 RFID 标签或近场通信 NFC 芯片中读取
- 20 身份标识。
- 6、如权利要求 1 所述的方法，根据存储的各实时人脸图像和获取的预存人脸图像，对所述进入验证区域内的用户进行身份验证，具体包括：
- 判断存储的各实时人脸图像是否存在与获取的预存人脸图像相匹配的实时人脸图像；
- 25 若是，则确定所述用户通过身份验证；
- 否则，确定所述用户未通过身份验证。
- 7、一种身份验证方法，包括：
- 服务器通过采集设备获取并存储位于验证区域外的用户的实时人脸图像；
- 所述服务器接收所述采集设备发送的身份标识；所述身份标识是进入验证区域内的
- 30 用户提供给所述采集设备的；
- 所述服务器根据所述身份标识，获取所述身份标识对应的预存人脸图像；

根据存储的各实时人脸图像和确定的预存人脸图像,对所述进入验证区域内的用户进行身份验证。

8、如权利要求 7 所述的方法,服务器通过采集设备获取位于验证区域外的用户的实时人脸图像,具体包括:

- 5 服务器接收采集设备发送的位于验证区域外的用户的实时人脸图像;或
服务器接收采集设备发送的验证区域外的实时图像,并从所述实时图像中提取人脸图像,作为位于验证区域外的用户的实时人脸图像。

9、一种身份验证方法,包括:

- 采集设备获取位于验证区域外的用户的实时人脸图像;
10 采集设备将获取的实时人脸图像发送给服务器进行存储;
采集设备获取进入验证区域内的用户提供的身份标识;
采集设备将获取的身份标识发送给服务器,以使所述服务器根据接收到的身份标识,获取所述身份标识对应的预存人脸图像,进而根据存储的各实时人脸图像和获取的预存人脸图像,对所述进入验证区域内的用户进行身份验证。

- 15 10、如权利要求 9 所述的方法,采集设备获取位于验证区域外的用户的实时人脸图像,具体包括:

采集设备采集验证区域外的实时图像;
采集设备从所述实时图像中提取人脸图像,作为位于验证区域外的用户的实时人脸图像。

- 20 11、一种身份验证系统,包括采集设备和服务器;

所述采集设备,获取实时人脸图像或实时图像,并将获取的实时人脸图像或实时图像发送给所述服务器,所述实时人脸图像是位于验证区域外的用户的实时人脸图像,所述实时图像是验证区外的实时图像;以及,获取进入验证区域内的用户提供的身份标识,并将获取的身份标识发送给所述服务器;

- 25 所述服务器,接收并存储所述采集设备发送的实时人脸图像,或接收所述采集设备发送的实时图像,从所述实时图像中提取人脸图像,作为实时人脸图像并存储;以及,接收所述采集设备发送的身份标识,根据所述身份标识获取所述身份标识对应的预存人脸图像,根据存储的各实时人脸图像和获取的预存人脸图像,对所述进入验证区域内的用户进行身份验证。

- 30 12、一种身份验证装置,包括:

第一获取模块,通过采集设备获取并存储位于验证区域外的用户的实时人脸图像;

接收模块,接收所述采集设备发送的身份标识;所述身份标识是进入验证区域内的的用户提供给所述采集设备的;

第二获取模块,根据所述身份标识,获取所述身份标识对应的预存人脸图像;

身份验证模块,根据存储的各实时人脸图像和确定的预存人脸图像,对所述进入验证区域内的的用户进行身份验证。

13、如权利要求 12 所述的装置,所述第一获取模块,接收采集设备发送的位于验证区域外的用户的实时人脸图像;或接收采集设备发送的验证区域外的实时图像,从所述实时图像中提取人脸图像,作为位于验证区域外的用户的实时人脸图像。

14、一种服务器,包括一个或多个处理器及存储器,所述存储器存储有程序,并且被配置成由所述一个或多个处理器执行以下步骤:

通过采集设备获取并存储位于验证区域外的用户的实时人脸图像;

接收所述采集设备发送的身份标识;所述身份标识是进入验证区域内的的用户提供给所述采集设备的;

根据所述身份标识,获取所述身份标识对应的预存人脸图像;

15 根据存储的各实时人脸图像和确定的预存人脸图像,对所述进入验证区域内的的用户进行身份验证。

15、一种身份验证装置,包括:

第一获取模块,获取位于验证区域外的用户的实时人脸图像;

第一发送模块,将获取的实时人脸图像发送给服务器进行存储;

20 第二获取模块,获取进入验证区域内的的用户提供的身份标识;

第二发送模块,将获取的身份标识发送给服务器,以使所述服务器根据接收到的身份标识,获取所述身份标识对应的预存人脸图像,进而根据存储的各实时人脸图像和获取的预存人脸图像,对所述进入验证区域内的的用户进行身份验证。

16、如权利要求 15 所述的装置,所述第一获取模块,获取验证区域外的实时图像;从所述实时图像中提取人脸图像,作为位于验证区域外的用户的实时人脸图像。

17、一种采集设备,包括:图像采集器、身份标识采集器、通信单元;

所述图像采集器,采集位于验证区域外的用户的实时人脸图像;

所述身份标识采集器,获取进入验证区域内的的用户提供的身份标识;

所述通信单元,将获取的实时人脸图像和获取的身份标识发送给服务器,以使所述服务器存储接收到的实时人脸图像,以及根据接收到的身份标识,获取所述身份标识对应的预存人脸图像,进而根据存储的各实时人脸图像和获取的预存人脸图像,对所述进

入验证区域内的用户进行身份验证。

18、如权利要求 17 所述的采集设备，所述图像采集器包括至少两个摄像头；各摄像头分别安装于不同的位置，用于从不同方向对所述验证区域外进行拍摄。