(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112333165 B
(45)授权公告日 2022.09.23

(21)申请号 202011161221.9

(22)申请日 2020.10.27

(65)同一申请的已公布的文献号
申请公布号 CN 112333165 A

(43)申请公布日 2021.02.05

(73)专利权人 支付宝(杭州)信息技术有限公司
地址 310000 浙江省杭州市西湖区西溪路556号8层B段801-11

(72)发明人 骆希

(74)专利代理机构 北京三友知识产权代理有限公司 11127
专利代理师 阚传猛 周达

(51)Int.Cl.
H04L 9/40(2022.01)
G06F 21/32(2013.01)
G06F 21/31(2013.01)
G06K 9/00(2022.01)
G06Q 10/06(2012.01)
G06N 20/10(2019.01)

(56)对比文件
CN 108710788 A,2018.10.26
CN 106339676 A,2017.01.18
CN 105426886 A,2016.03.23
CN 108306738 A,2018.07.20
CN 106599649 A,2017.04.26
李昆仑等.基于级联支持向量机的人脸图像性别识别.《计算机工程》.2012,(第12期),

审查员 申杨

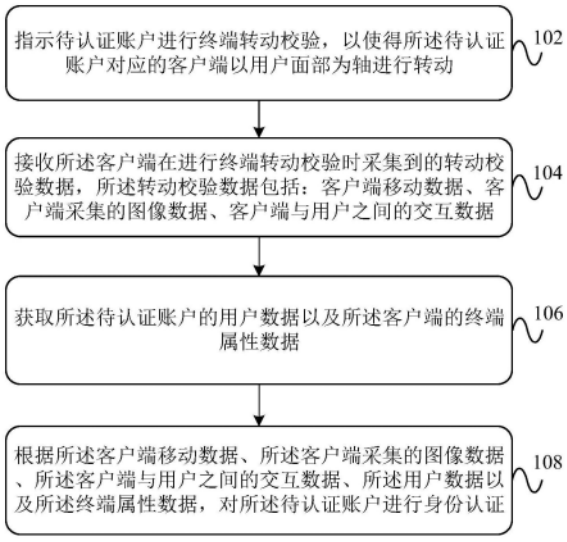
权利要求书3页 说明书16页 附图4页

(54)发明名称

身份认证方法、装置、设备及系统

(57)摘要

本说明书提供一种身份认证方法、装置、设备及系统，通过在人脸识别环节调整人脸识别终端方式进行活体检测，采用终端转动校验的方式，以一种简单易行且强感知度的方式，提升用户人脸识别参与度，加强身份认证过程中用户与终端交互，并降低虚拟视频注入和被他人诱导进行身份认证的可能性。并将终端动态校验过程中涉及的交互数据量化成风险特征，同时考虑到虚拟视频注入的可能性，参考终端系统数据，端静态特征、人静态特征、交互动态特征加入到身份认证的算法中，提升身份认证的准确性。



CN 112333165 B

1.一种身份认证方法,所述方法包括:

指示待认证账户进行终端转动校验,以使得所述待认证账户对应的客户端以用户面部为轴进行转动;

接收所述客户端在进行终端转动校验时采集到的转动校验数据,所述转动校验数据包括:客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据;

获取所述待认证账户的用户数据以及所述客户端的终端属性数据;

根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据,对所述待认证账户进行身份认证;

其中,所述根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据,对所述待认证账户进行身份认证,包括:

对所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据分别进行特征处理,获得不同类别的嵌入式向量特征,根据所述不同类别的嵌入式向量特征对所述待认证账户进行身份认证,获得所述待认证账户的身份认证分值。

2.如权利要求1所述的方法,所述获取所述待认证账户进行终端转动校验时的转动校验数据包括:

通过所述客户端中的传感器采集所述客户端在进行终端转动校验时的客户端移动数据,所述客户端移动数据包括:所述客户端的移动轨迹、所述客户端的移动速度、所述客户端的变动幅度。

3.如权利要求1所述的方法,所述客户端采集的图像数据包括图像抖动程度,所述获取所述待认证账户进行终端转动校验时的转动校验数据包括:

利用灰度投影法计算所述客户端在进行终端转动校验时采集到的用户脸部图像中帧与帧之间的位移;

根据计算出的所述用户脸部图像中帧与帧之间的位移,确定出所述客户端采集到的用户脸部图像的图像抖动程度。

4.如权利要求1所述的方法,所述客户端与用户之间的交互数据的采集方法包括:

采集所述客户端在进行终端转动校验时所述客户端与用户面部之间的距离数据,根据采集到的所述客户端与用户面部之间的距离数据获得所述客户端与用户之间的交互数据。

5.如权利要求1所述的方法,所述客户端的终端属性数据包括:所述客户端内的hook函数,所述客户端的终端属性数据的获取方法包括:

从所述客户端的视频图片模块、界面绘制模块、音频模块中获取存在风险的hook函数。

6.如权利要求1所述的方法,所述对所述待认证账户进行身份认证,包括:利用因式分解机模型基于获得的各个类别的嵌入式向量特征对所述待认证账户进行身份认证,获得所述待认证账户的身份认证分值。

7.如权利要求1所述的方法,所述对所述待认证账户进行身份认证,包括:

若所述身份认证分值大于预设阈值,则确定所述待认证账户身份认证通过;

若所述身份认证分值小于所述预设阈值,则确定所述待认证账户身份认证失败,并取消所述待认证账户的实名认证状态。

8.如权利要求1所述的方法，所述指示待认证账户进行终端转动校验之前，所述方法还包括：

接收所述待认证账户上传的身份认证信息；

获取所述待认证账户上传身份认证信息的地理位置、设备信息；

根据所述身份认证信息、所述地理位置、所述设备信息对所述待认证账户进行风险识别，若确定所述待认证账户存在风险，则指示待认证账户进行终端转动校验。

9.一种身份认证方法，所述方法包括：

接收服务器发送的终端转动校验的指示；

以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据；

将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证，其中，所述服务器对所述待认证账户进行身份认证的方法包括：对所述移动数据、所述图像数据、所述与用户之间的交互数据、所述用户数据以及所述终端属性数据分别进行特征处理，获得不同类别的嵌入式向量特征，根据所述不同类别的嵌入式向量特征对所述待认证账户进行身份认证，获得所述待认证账户的身份认证分值。

10.一种身份认证装置，包括：

转动校验指示模块，用于指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动；

转动校验数据接收模块，用于接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据；

数据采集模块，用于获取所述待认证账户的用户数据以及所述客户端的终端属性数据；

身份认证模块，用于根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证；

其中，所述根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证，包括：

对所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据分别进行特征处理，获得不同类别的嵌入式向量特征，根据所述不同类别的嵌入式向量特征对所述待认证账户进行身份认证，获得所述待认证账户的身份认证分值。

11.如权利要求10所述的装置，所述转动校验数据接收模块具体用于：

通过所述客户端中的传感器采集所述客户端在进行终端转动校验时的客户端移动数据，所述客户端移动数据包括：所述客户端的移动轨迹、所述客户端的移动速度、所述客户端的变动幅度。

12.如权利要求10所述的装置,所述客户端采集的图像数据包括图像抖动程度,所述转动校验数据接收模块具体用于:

利用灰度投影法计算所述客户端在进行终端转动校验时采集到的用户脸部图像中帧与帧之间的位移;

根据计算出的所述用户脸部图像中帧与帧之间的位移,确定出所述客户端采集到的用户脸部图像的图像抖动程度。

13.如权利要求10所述的装置,所述转动校验数据接收模块具体用于:

采集所述客户端在进行终端转动校验时所述客户端与用户面部之间的距离数据,根据采集到的所述客户端与用户面部之间的距离数据获得所述客户端与用户之间的交互数据。

14.一种身份认证装置,包括:

校验指示接收模块,用于接收服务器发送的终端转动校验的指示;

动态检验模块,用于以用户面部为轴转动,并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据;

数据传输模块,用于将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器,以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据,对待认证账户进行身份认证,其中,所述服务器对所述待认证账户进行身份认证的方法包括:对所述移动数据、所述图像数据、所述与用户之间的交互数据、所述用户数据以及所述终端属性数据分别进行特征处理,获得不同类别的嵌入式向量特征,根据所述不同类别的嵌入式向量特征对所述待认证账户进行身份认证,获得所述待认证账户的身份认证分值。

15.一种身份认证设备,包括:至少一个处理器以及用于存储处理器可执行指令的存储器,所述处理器执行所述指令时实现权利要求1-9任一项所述的方法。

16.一种身份认证系统,包括:客户端、服务器;其中,所述服务器中包括至少一个处理器以及用于存储处理器可执行指令的存储器,所述处理器执行所述指令时实现权利要求1-8任一项所述的方法,用于在确定待认证账户存在风险时,指示所述客户端进行终端转动校验,基于所述客户端的转动校验数据以及所述客户端的终端属性数据、所述待认证账户的用户数据对所述待认证账户进行身份认证;

所述客户端包括至少一个处理器以及用于存储处理器可执行指令的存储器,所述处理器执行所述指令时实现权利要求9所述的方法,用于接收所述服务器发送的终端转动校验指令,并向所述服务器上传终端转动校验过程中的转动校验数据。

身份认证方法、装置、设备及系统

技术领域

[0001] 本说明书属于计算机技术领域，尤其涉及一种身份认证方法、装置、设备及系统。

背景技术

[0002] 随着计算机互联网技术的发展，为了确保账户的安全，越来越多的账户需要身份认证后才能正常使用或者才能使用某些功能。一般的，身份认证可以采用上传身份信息以及生物图像或生物视频认证，这种身份认证，可能存在他人冒用身份或他人代操作等，不能确认是用户本人操作，是的身份认证的结果不够准确。

发明内容

[0003] 本说明书实施例的目的在于提供一种身份认证方法、装置、设备及系统，提高了身份认证的准确性。

[0004] 第一方面，本说明书实施例提供了一种身份认证方法，所述方法包括：

[0005] 指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动；

[0006] 接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据；

[0007] 获取所述待认证账户的用户数据以及所述客户端的终端属性数据；

[0008] 根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证。

[0009] 第二方面，本说明书提供了一种身份认证方法，所述方法包括：

[0010] 接收服务器发送的终端转动校验的指示；

[0011] 以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据；

[0012] 将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证。

[0013] 第三方面，本说明书提供了一种身份认证装置，包括：

[0014] 转动校验指示模块，用于指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动；

[0015] 转动校验数据接收模块，用于接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据；

[0016] 数据采集模块，用于获取所述待认证账户的用户数据以及所述客户端的终端属性数据；

[0017] 身份认证模块，用于根据所述客户端移动数据、所述客户端采集的图像数据、所述

客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证。

[0018] 第四方面，本说明书提供了一种身份认证装置，包括：

[0019] 校验指示接收模块，用于接收服务器发送的终端转动校验的指示；

[0020] 动态检验模块，用于以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据；

[0021] 数据传输模块，用于将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证。

[0022] 第五方面，本说明书实施例提供了一种身份认证设备，包括至少一个处理器以及用于存储处理器可执行指令的存储器，所述处理器执行所述指令时实现上述第一方面或第二方法所述的身份认证方法。

[0023] 第六方面，本说明书实施例提供了一种身份认证系统，包括：客户端、服务器；其中，所述服务器中包括至少一个处理器以及用于存储处理器可执行指令的存储器，所述处理器执行所述指令时实现上述第一方面所述的方法，用于在确定待认证账户存在风险时，指示所述客户端进行终端转动校验，基于所述客户端的转动校验数据以及所述客户端的终端属性数据、所述待认证账户的用户数据对所述待认证账户进行身份认证；

[0024] 所述客户端包括至少一个处理器以及用于存储处理器可执行指令的存储器，所述处理器执行所述指令时实现上述第二方面所述的方法，用于接收所述服务器发送的终端转动校验指令，并向所述服务器上传终端转动校验过程中的转动校验数据。

[0025] 本说明书提供的身份认证方法、装置、设备及系统，通过在人脸识别环节调整人脸识别终端方式进行活体检测，以一种简单易行且强感知度的方式，提升用户人脸识别参与度，加强身份认证过程中用户与终端交互，并降低虚拟视频注入和被他人诱导刷脸的可能性，同步提升刷脸感知度及虚拟视频造假门槛。并将终端动态校验过程中涉及的交互数据量化成风险特征，同时考虑到虚拟视频注入的可能性，参考终端系统数据，端静态特征+人静态特征+交互动态特征加入到人脸识别算法中，提炼本人非代操识别的特征并预测用户已知刷脸意图，重点识别用户亲自操作可能性及真实意图。

附图说明

[0026] 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性的前提下，还可以根据这些附图获得其他的附图。

[0027] 图1是本说明书实施例提供的身份认证方法实施例的流程示意图；

[0028] 图2是本说明书又一个实施例中身份认证方法的流程示意图；

[0029] 图3是本说明书一个场景示例中身份认证的流程示意图；

[0030] 图4是本说明书提供的身份认证装置一个实施例的模块结构示意图；

[0031] 图5是本说明书又一个实施例中身份认证装置的结构示意图；

[0032] 图6是本说明书一个实施例中身份认证服务器的硬件结构框图。

具体实施方式

[0033] 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，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。基于本说明书中的实施例，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，都应当属于本说明书保护的范围。

[0034] 随着网络安全越来越被重视，越来越多的账户需要进行身份认证，如：支付、转账时可能需要身份认证，有些账户也需要通过身份认证来进行实名认证。各大网络平台的账户一般均需要进行实名认证，实名认证失败或未进行实名认证的账户可能不被允许使用或被限制功能。一般的，实名认证是通过用户上传身份信息如：身份证照片，结合用户的生物图像识别如：人脸识别等，对用户进行身份认证，完成账户的实名认证过程。但是，随着计算机技术的发展，有些面部动态模拟技术可能会攻破人脸动态检验，或者有其他人代为操作进行实名认证的情况，使得账户的身份认证结果不准确，进一步可能会给账户带来风险。

[0035] 图1是本说明书实施例提供的身份认证方法实施例的流程示意图。虽然本说明书提供了如下述实施例或附图所示的方法操作步骤或装置结构，但基于常规或者无需创造性的劳动在所述方法或装置中可以包括更多或者部分合并后更少的操作步骤或模块单元。在逻辑性上不存在必要因果关系的步骤或结构中，这些步骤的执行顺序或装置的模块结构不限于本说明书实施例或附图所示的执行顺序或模块结构。所述的方法或模块结构的在实际中的装置、服务器或终端产品应用时，可以按照实施例或者附图所示的方法或模块结构进行顺序执行或者并行执行(例如并行处理器或者多线程处理的环境、甚至包括分布式处理、服务器集群的实施环境)。

[0036] 具体的一个实施例如图1所示，本说明书提供的身份认证方法的一个实施例中，所述方法可以应用在计算机、平板电脑、服务器、智能穿戴设备、车载设备等终端，所述方法可以包括如下步骤：

[0037] 步骤102、指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动。

[0038] 在具体的实施过程中，本说明书实施例主要采用终端转动校验的方式对待认证账户进行身份认证，终端转动校验可以理解为一种客户端以用户面部为轴进行转动，基于客户端转动过程中采集到的数据进行身份认证的一种身份校验方式。客户端在转动的过程中摄像头可以是打开的，客户端在转动过程中可以采集用户的脸部图像，客户端还可以采集在转动过程中客户端的移动数据以及与用户之间的交互数据等。当待认证账户需要进行身份认证如：实名认证或支付认证等时，可以向服务器发送身份认证请求，服务器在接收到身份认证请求后可以向待认证账户所在的客户端发送终端转动校验的指示，提示并引导用户进行终端转动校验。用户在客户端中看到服务器发送的终端转动校验指示后，可以手持客户端以自己的脸部为轴转动手臂，即用户头部不动，但客户端转动进行动态人脸识别。其中，客户端可以是智能手机、平台电脑、智能穿戴设备等具有拍摄功能的终端设备。

[0039] 此外，本说明书一些实施例中，在指示待认证账户进行终端转动校验之前，所述方法还可以包括：

[0040] 接收所述待认证账户上传的身份认证信息；

[0041] 获取所述待认证账户上传身份认证信息的地理位置、设备信息；

[0042] 根据所述身份认证信息、所述地理位置、所述设备信息对所述待认证账户进行风险识别，若确定所述待认证账户存在风险，则指示待认证账户进行终端转动校验。

[0043] 在具体的实施过程中，用户在对待认证账户进行身份认证时，可以先通过客户端上传身份认证信息如：身份信息或身份证照片等，服务器接收到用户上传的身份认证信息后，可以获取用户当前的地理位置以及用户上传身份认证信息的客户端的设备信息等。服务器可以基于用户上传的身份认证信息、获取到的地理位置、设备信息等，对待认证账户进行风险识别，判断待认证账户的身份认证是都存在他人冒用或他人代操作的可能，若存在，则确定待认证账户存在风险，需要进行进一步的身份认证处理，若不存在，则可以进行绑卡、人脸识别(静默识别或动态识别)等身份认证流程。其中，在对待认证账户进行风险识别时，可以采用智能学习模型或风险系统进行，如：可以根据历史风险账户进行模型的学习训练，学习存在风险的账户存在哪些特征，基于训练后的模型对待认证账户进行风险识别。一般的，可以从地理位置聚集、介质(设备、wifi、mac)聚集、身份证相似度、手机号相似度、垃圾注册账户等维度对待认证账户进行风险识别，具体风险识别的方法本说明书实施例不作具体限定。

[0044] 本说明书实施例，基于待认证账户的身份认证信息、地理位置、设备信息对待认证账户进行初步的风险筛选，对于风险高的账户，进行终端转动校验的升级认证，以确保账户的身份认证结果的安全可靠。

[0045] 步骤104、接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据。

[0046] 在具体的实施过程中，在客户端进行终端转动校验过程中，可以接收客户端在转动校验过程中采集到的转动校验数据，如：客户端移动数据、客户端采集到的图像数据、客户端与用户之间的交互数据。其中，客户端移动数据可以包括客户端转动过程中的移动轨迹、移动速度等，客户端与用户之间的交互数据可以理解为客户端终端过程中与用户之间的位置、角度等的变化数据等。

[0047] 本说明书一些实施例中，所述获取所述待认证账户进行终端转动校验时的转动校验数据包括：

[0048] 通过所述客户端中的传感器采集所述客户端在进行终端转动校验时的客户端移动数据，所述客户端移动数据包括：所述客户端的移动轨迹、所述客户端的移动速度、所述客户端的变动幅度。

[0049] 在具体的实施过程中，客户端在移动过程中，客户端中的传感器可以采集客户端的位置变化以及速度变化，基于客户端中的传感器采集到的数据，可以获得客户端在进行终端转动校验时的移动轨迹、移动速度以及客户端的变化幅度。客户端的移动轨迹可以理解为动态校验过程中，客户端转动位置点所形成的移动轨迹。客户端的移动速度可以理解为终端完成转动识别轨迹的速度，可以为平均速度，也可以为每个轨迹点对应的速度，具体可以根据实际需要而定。客户端的变化幅度可以理解为客户端陀螺仪三轴变动幅度，即客户端转动过程中，客户端的陀螺仪左右轴X，前后轴Y，纵轴Z变化幅度，即轴变化序列的标准差。通过客户端中的传感器，可以采集到客户端在进行转动校验过程中，客户端的轨迹、速

度等数据，基于采集到的数据，为确定是否是真人在操作客户端奠定了数据基础，避免面部动态模拟技术在账户的身份认证过程中被通过，导致身份认证结果不准确的问题。

[0050] 本说明书一些实施例中，所述客户端采集的图像数据包括图像抖动程度，所述获取所述待认证账户进行终端转动校验时的转动校验数据包括：

[0051] 利用灰度投影法计算所述客户端在进行终端转动校验时采集到的用户脸部图像中帧与帧之间的位移；

[0052] 根据计算出的所述用户脸部图像中帧与帧之间的位移，确定出所述客户端采集到的用户脸部图像的图像抖动程度。

[0053] 在具体的实施过程中，客户端在进行终端转动校验时，可以采集转动过程中用户的脸部图像，本说明书一些实施例可以采用灰度投影法计算客户端采集到的图像的帧与帧之间的位移，基于计算出的位移可以确定出客户端采集到的用户脸部图像的图像抖动程度。如：可以计算位移的平均值，作为图像抖动程度，或将最大位置最为图像抖动程度，或采用其他方式确定出图像抖动程度，本说明书不作具体限定。灰度投影法可以理解为一种对图像分布特征进行简化提取的一种操作，以二维图像的像素行和列为单位，将图像特征转化为沿行、列坐标的曲线，从而更容易对图像分布特征进行计算。正常情况下，若是真实用户操作客户端进行账户的身份认证，用户在转动客户端时，拍摄的视频图像会出现一定的抖动情况，基于图像抖动程度可以识别出机器操作客户端的场景，进一步识别出虚假用户进行身份认证的问题。

[0054] 本说明书一些实施例中，所述客户端与用户之间的交互数据的采集方法包括：

[0055] 采集所述客户端在进行终端转动校验时所述客户端与用户面部之间的距离数据，根据采集到的所述客户端与用户面部之间的距离数据获得所述客户端与用户之间的交互数据。

[0056] 在具体的实施过程中，客户端在进行终端转动校验时，转动的过程中可以根据客户端采集到的用户脸部图像以及用户的身位和终端的位置，推算出客户端与用户面部之间的距离。客户端在转动的过程中，计算出的客户端与用户面部之间的距离会不断变化，可以基于计算出的距离数据确定出客户端与用户之间的交互数据，如：可以将距离的标准差作为客户端与用户之间的交互数据或者将计算出的距离的平均值作为客户端与用户之间的交互数据，或者也可以将客户端在移动过程中计算出的每个轨迹点的距离数据作为客户端与用户之间的交互数据，本说明书对此不做具体限定。基于客户端与用户之间的距离数据，可以判断是否存在机器操作的可能，同时，基于距离数据和用户的个人信息如：身高等，也可以判断是否用户本人操作等，为后续账户的身份认证奠定了数据基础。

[0057] 步骤106、获取所述待认证账户的用户数据以及所述客户端的终端属性数据。

[0058] 在具体的实施过程中，接收到客户端上传的转动校验数据后，还可以获取待认证账户的用户数据如：用户年龄、身份名下认证账户数、用户所在省份、用户的身高、职业等等，此外，用户数据还可以包括待认证账户的信息如：账户注册时间、账户是否绑卡及绑卡数量、等。同时，还可以获取客户端的终端属性数据如：终端所在的地理位置、终端的mac地址、终端的历史身份认证数据等。

[0059] 本说明书一些实施例中，所述客户端的终端属性数据包括：所述客户端内的hook函数，所述客户端的终端属性数据的获取方法包括：

[0060] 从所述客户端的视频图片模块、界面绘制模块、音频模块中获取存在风险的hook函数。

[0061] 在具体的实施过程中，本说明书一些实施例中的终端属性数据主要是为了判断客户端上传的视频图像是否为虚拟视频图像，基于此，本说明书实施例主要可以获取客户端中视频图片模块、界面绘制模块、音频模块中存在风险的hook函数。其中，hook又可以叫做钩子函数，在系统没有调用该函数之前，钩子程序就先捕获该消息，钩子函数先得到控制权，这时钩子函数既可以加工处理(改变)该函数的执行行为，还可以强制结束消息的传递。

[0062] 其中，视频图片模块可以理解为libandroid_runtiome.so，该模块可以实现替换视频、图片的功能，界面绘制模块可以理解为libgui.so，该模块可以实现SurfaceView组件绘制相关的功能，音频模块可以理解为libmedia.so，该模块主要可以实现替换音频的功能。可以查询三个模块是否存在疑似hook点(目的为替换视频、图片、音频)的特征，例如：可以查看三个模块中是否存在目的为替换视频、音频、图片的hook函数，如以下hook函数：

[0063] JNICameraContext::copyAndPost，android::GLConsumer::updateAndReleaseLocked，

[0064] android::AudioRecord::set，

[0065] android::AudioRecord::read，android::AudioRecord::processAudioBuffer；

[0066] 通过对终端内的特征参数进行监控，考虑到虚拟视频注入的可能性，提升了账户身份认证的准确性。

[0067] 步骤108、根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证。

[0068] 在具体的实施过程中，在采集到客户端的转动校验数据以及用户数据、终端属性数据后，可以基于采集到的数据对待认证账户进行身份认证，如：将客户端进行终端转动校验过程中采集到的客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据以及用户数据、终端属性数据输入到预先建立的智能学习模型中，使用智能学习模型对当前的待认证账户的身份识别进行风险评估，确定出当前待认证账户的身份认证是否存在风险，若存在风险，则身份认证失败，若不存在风险，则身份认证通过。当然，还可以使用其他的方式如：专家经验、数学统计分析等方式，基于采集到的数据对待认证账户进行身份认证，本说明书实施例不作具体限定。

[0069] 本说明书一些实施例中，所述根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证，包括：

[0070] 对所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据分别进行特征处理，获得不同类别的嵌入式向量特征；

[0071] 利用因式分解机模型基于获得的各个类别的嵌入式向量特征对所述待认证账户进行身份认证，获得所述待认证账户的身份认证分值。

[0072] 在具体的实施过程中，可以先对采集到的客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据、用户数据以及终端属性数据分别进行特征处理，如：将

采集到的各个类别的数据编码成one-hot向量后，经过转化得到低维的embedding(嵌入)向量，获得不同类别数据对应的嵌入式向量特征。再将转换后的嵌入式向量特征输入到预先建立好的机器学习模型中，作为模型的入参，利用机器学习模型对当前待认证账户的身份认证过程进行风险识别，获得待认证账户的身份认证分值，基于模型输出的身份认证分值可以确定待认证账户是否认证通过。其中，若所述身份认证分值大于预设阈值，则确定所述待认证账户身份认证通过；若所述身份认证分值小于所述预设阈值，则确定所述待认证账户身份认证失败，并取消所述待认证账户的实名认证状态。本说明书实施例，在模型输出的身份认证分值小于预设阈值时，可以确定该待认证账户的身份认证过程可能是身份冒用、他人代操作等不合法行为，可以对待认证账户的身份信息进行实时身份释放，即该账户取消实名认证状态，剥离身份与账户的绑定关系，以使得真实用户后续可以重新对该账户进行身份认证，同时，可以使得待认证账户处于未实名认证状态下，限制该账户的功能，以确保账户的安全。

[0073] 本说明书实施例中的机器学习模型可以采用因式分解机模型(Factorization Machine，简称FM)对输入的嵌入式向量特征进行处理，获得待认证账户的身份认证分值。其中，因式分解机模型FM可以解决数据稀疏的情况下，特征怎样组合的问题，利用FM模型可以高效的学习特征间相互关系，对客户端在终端转动校验过程中采集到的数据进行拼接，扩充特征，以提高账户身份认证的准确性。

[0074] 此外，本说明书实施例还可以将FM模型与晚期融合模型(late fusion)相结合，如：在对采集到的数据进行特征处理时，可以使用晚期融合模型，提高特征融合的准确性，进一步提高账户身份认证的准确性。或者在对各个类别的数据进行特征处理后，利用late FM算法对转换后的特征进行融合处理，输出身份认证分值。late fusion模型可以理解为基于决策的融合，指的是特征分别进入不同的模型，然后对模型输出的特征进行连接，进而预测最终结果。

[0075] 本说明书实施例提供的身份认证方法，通过设置终端转动校验的方式对账户进行身份认证，通过终端和用户交互的方式，提升了用户进行脸部识别的感知能力，通过对终端动态检验过程中终端数据、用户数据及端人交互数据，识别人脸代操可能性，从而提升人脸攻击注入门槛、降低他人代操、身份冒用可能性，减少认证账户被转卖流入下游风险账户的量级。

[0076] 图2是本说明书又一个实施例中身份认证方法的流程示意图，如图2所示，本说明书一些实施例中可以提供一种应用在用户客户端中的身份认证方法，该客户端可以是智能手机、平板电脑或智能穿戴设备等，该客户端在身份认证过程中所执行的方法可以参考如下：

[0077] 步骤202、接收服务器发送的终端转动校验的指示。

[0078] 在具体的实施过程中，当待认证账户需要进行身份认证如：实名认证或支付认证等时，可以向服务器发送身份认证请求，服务器在接收到身份认证请求后可以向待认证账户所在的客户端发送终端转动校验的指示，提示并引导用户进行终端转动校验。用户在客户端中看到服务器发送的终端转动校验指示后，可以手持客户端以自己的脸部为轴转动手臂，即用户头部不动，但客户端转动进行动态人脸识别。

[0079] 步骤204、以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交

互数据以及拍摄的图像数据。

[0080] 在具体的实施过程中，本说明书实施例主要采用终端转动校验的方式对待认证账户进行身份认证，终端转动校验可以理解为一种客户端以用户面部为轴进行转动，基于客户端转动过程中采集到的数据进行身份认证的一种身份校验方式。客户端在转动的过程中摄像头可以是打开的，客户端在转动过程中可以采集用户的脸部图像，客户端还可以采集在转动过程中客户端的移动数据以及与用户之间的交互数据等。

[0081] 步骤206、将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证。

[0082] 在具体的实施过程中，在客户端进行终端转动校验过程中，客户端可以采集在转动校验过程中采集到的转动校验数据，如：客户端移动数据、客户端采集到的图像数据、客户端与用户之间的交互数据。其中，客户端移动数据可以包括客户端转动过程中的移动轨迹、移动速度等，客户端与用户之间的交互数据可以理解为客户端终端过程中与用户之间的位置、角度等的变化数据等。客户端将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，服务器可以根据客户端采集到的数据，结合待认证账户的用户数据、客户端的终端属性数据等，对待认证账户进行身份认证，如：采用机器学习模型对待认证账户进行身份认证打分等，身份认证的方式具体可以参考上述实施例的记载，此处不再赘述。

[0083] 本说明书实施例中客户端在进行账户的身份认证过程可以参考上述服务器侧进行身份认证过程中客户端所执行的过程，此处不作过多的赘述。

[0084] 本说明书实施例提供的身份认证方法，通过设置终端转动校验的方式对账户进行身份认证，通过终端和用户交互的方式，提升了用户进行脸部识别的感知能力，通过对终端动态检验过程中终端数据、用户数据及端人交互数据，识别人脸代操可能性，从而提升人脸攻击注入门槛、降低他人代操、身份冒用可能性，减少认证账户被转卖流入下游风险账户的量级。

[0085] 图3是本说明书一个场景示例中身份认证的流程示意图，如图3所示，该身份认证以账户的实名认证为例，下面结合图3具体介绍本说明书实施例中身份认证的过程：

[0086] 1、用户通过输入身份证信息或上传身份证正反面照片，完成公安网校验后，进入实名认证流程，判断是否存在身份冒用或代操可能性。

[0087] 身份冒用或代操可能性判断：地理位置聚集、介质(设备、wifi、mac)聚集、身份证相似度、手机号相似度、垃圾注册账户等；

[0088] 2、若存在身份冒用或代操可能性，则进入升级校验流程，若不存在身份冒用或代操可能性，则走普通实名认证流程。

[0089] 3、若进行升级校验，则进行终端转动校验(用户可感知)：用户持有人脸识别终端(如：手机)以人脸为轴心转动手臂，即人头部不动但手机转动进行动态人脸识别。

[0090] 终端在进行终端转动校验时可以采集到终端动态识别特征(即上述实施例中的转动校验数据)：

[0091] 终端转动轨迹：动态人脸识别过程中，终端转动位置点所形成的移动轨迹；

[0092] 终端移动速度：终端完成转动识别轨迹的速度；

[0093] 终端陀螺仪三轴变动幅度:转动过程中,终端陀螺仪左右轴X,前后轴Y,纵轴Z变化幅度,即轴变化序列的标准差;

[0094] 端人距离及距离变化:人脸识别过程中根据头像及身位推算出终端与人脸的距离;距离变化即动态核验过程中,端人距离的标准差。

[0095] 视频抖动程度:人脸识别过程中图像帧与帧之间会发生整体的位移,本方案计算位移采用灰度投影法,即是一种对图像分布特征进行简化提取的一种操作,以二维图像的像素行和列为单位,将图像特征转化为沿行、列坐标的曲线,从而更容易对图像分布特征进行计算;

[0096] 终端属性特征如:是否为虚拟视频:终端系统中libandroid_runtiome.so、libgui.so、libmedia.so三个模块是否存在疑似hook点(目的为替换视频、图片、音频)的特征,如查看三个模块中是否包含可以修改、替换视频、图片、音频的hook函数,具体可以参见上述实施例的记载。

[0097] 账户及身份属性特征(即用户数据):账户注册时间、账户是否绑卡及绑卡数量、用户年龄、身份名下认证账户数、用户所在省份等。

[0098] 4、身份认证:

[0099] 特征处理(late fusion):终端动态识别特征、视频录制特征及端内hook函数特征等均被编码成one-hot向量后,经过转化得到低维的embedding向量,embedding向量将作为模型的入参与模型一同训练。

[0100] 识别算法(late FM):由于终端采集数据有稀疏的特性且各类维度特征存在关联,本方案在采用late FM算法在非常稀疏的终端数据中进行合理的参数估计,最终输出数值为当前用户本人亲自操作终端进行人脸识别的可能性,即意图明确、并非他人代替操作。

[0101] 若用户完成终端动态校验且late-FM算法输出模型分高于0.8分,即该方案认为用户本人亲自操作终端进行动态检验且意图真实、没有被他人代替操作,则实名认证完成;若未通过,则需引导用户重新进入实名认证流程。

[0102] 通过终端转动校验采集转动校验数据,再进行终端转动校验的意图识别,可以识别出是否本人人脸、是否本人亲自操作,以确定身份认证的结果。

[0103] 5、若检测出身份冒用、他人代操风险,则对账户身份信息进行实时身份释放,即该账户取消实名认证状态,剥离身份与账户的绑定关系。

[0104] 此外,如图3所示,本说明书一些实施例中在实名认证成功后,还进行了异步冒用监测,可以将一些耗时较高或者不一定要在实时进行管控的策略放在异步层,在实时身份认证处理过程中或之后进行异步监测,异步监测通过后,才可以完成实名认证过程,若异步监测没有通过,则实名认证失败,进行身份释放,以便用户进行下一次的实名认证。即本说明书实施例中可以采用聚集类/冲突类策略进行实时的身份认证,同时结合准实时冒用模型对采集到的部分数据进行异步身份认证,以提高身份认证的准确性。

[0105] 本说明书实施例通过在人脸识别环节调整人脸识别终端方式进行活体检测,以一种简单易行且强感知度的方式,提升用户人脸识别参与度,加强刷脸过程用户与终端交互,并降低虚拟视频注入和被他人诱导刷脸的可能性,同步提升刷脸感知度及虚拟视频造假门槛。并将终端动态校验过程中涉及的交互数据量化成风险特征,同时考虑到虚拟视频注入的可能性,参考终端系统数据,端静态特征+人静态特征+交互动态特征加入到人脸识别算

法中，提炼本人非代操识别的特征并预测用户已知刷脸意图，重点识别用户亲自操作可能性及真实意图。

[0106] 本说明书中上述方法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考即可，每个实施例重点说明的都是与其他实施例的不同之处。相关之处参考方法实施例的部分说明即可。

[0107] 基于上述所述的身份认证方法，本说明书一个或多个实施例还提供一种用于身份认证的装置。所述系统可以包括使用了本说明书实施例所述方法的装置(包括分布式系统)、软件(应用)、模块、组件、服务器、客户端等并结合必要的实施硬件的装置。基于同一创新构思，本说明书实施例提供的一个或多个实施例中的装置如下面的实施例所述。由于装置解决问题的实现方案与方法相似，因此本说明书实施例具体的装置的实施可以参考前述方法的实施，重复之处不再赘述。以下所使用的，术语“单元”或者“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

[0108] 具体地，图4是本说明书提供的身份认证装置一个实施例的模块结构示意图，该装置可以理解为上述实施例中的服务器，如图4所示，本说明书中提供的身份认证装置可以包括：

[0109] 转动校验指示模块41，用于指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动；

[0110] 转动校验数据接收模块42，用于接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据；

[0111] 数据采集模块43，用于获取所述待认证账户的用户数据以及所述客户端的终端属性数据；

[0112] 身份认证模块44，用于根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证。

[0113] 本说明书实施例提供的身份认证装置，通过设置终端转动校验的方式对账户进行身份认证，通过终端和用户交互的方式，提升了用户进行脸部识别的感知能力，通过对终端动态检验过程中终端数据、用户数据及端人交互数据，识别人脸代操可能性，从而提升人脸攻击注入门槛、降低他人代操、身份冒用可能性，减少认证账户被转卖流入下游风险账户的量级。

[0114] 本说明书一些实施例中，所述转动校验数据接收模块具体用于：

[0115] 通过所述客户端中的传感器采集所述客户端在进行终端转动校验时的客户端移动数据，所述客户端移动数据包括：所述客户端的移动轨迹、所述客户端的移动速度、所述客户端的变动幅度。

[0116] 本说明书实施例提供的身份认证装置，通过客户端中的传感器，可以采集到客户端在进行转动校验过程中，客户端的轨迹、速度等数据，基于采集到的数据，为确定是否是真人在操作客户端奠定了数据基础，避免面部动态模拟技术在账户的身份认证过程中被通过，导致身份认证结果不准确的问题。

[0117] 本说明书一些实施例中，所述客户端采集的图像数据包括图像抖动程度，所述转动校验数据接收模块具体用于：

[0118] 利用灰度投影法计算所述客户端在进行终端转动校验时采集到的用户脸部图像中帧与帧之间的位移；

[0119] 根据计算出的所述用户脸部图像中帧与帧之间的位移，确定出所述客户端采集到的用户脸部图像的图像抖动程度。

[0120] 本说明书实施例提供的身份认证装置，基于图像抖动程度可以识别出机器操作客户端的场景，进一步识别出虚假用户进行身份认证的问题。

[0121] 本说明书一些实施例中，所述转动校验数据接收模块具体用于：

[0122] 采集所述客户端在进行终端转动校验时所述客户端与用户面部之间的距离数据，根据采集到的所述客户端与用户面部之间的距离数据获得所述客户端与用户之间的交互数据。

[0123] 本说明书实施例提供的身份认证装置，于客户端与用户之间的距离数据，可以判断是否存在机器操作的可能，同时，基于距离数据和用户的个人信息如：身高等，也可以判断是否用户本人操作等，为后续账户的身份认证奠定了数据基础。

[0124] 图5是本说明书又一个实施例中身份认证装置的结构示意图，该身份认证装置可以理解为上述实施例中的客户端，如图5所示，本说明书一些实施例中的身份认证装置，可以包括：

[0125] 校验指示接收模块51，用于接收服务器发送的终端转动校验的指示；

[0126] 动态检验模块52，用于以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据；

[0127] 数据传输模块53，用于将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证。

[0128] 本说明书实施例提供的身份认证装置，通过设置终端转动校验的方式对账户进行身份认证，通过终端和用户交互的方式，提升了用户进行脸部识别的感知能力，通过对终端动态检验过程中终端数据、用户数据及端人交互数据，识别人脸代操可能性，从而提升人脸攻击注入门槛、降低他人代操、身份冒用可能性，减少认证账户被转卖流入下游风险账户的量级。

[0129] 需要说明的，上述所述的装置根据对应方法实施例的描述还可以包括其他的实施方式。具体的实现方式可以参照上述对应的方法实施例的描述，在此不作一一赘述。

[0130] 本说明书实施例还提供一种身份认证设备，包括：至少一个处理器以及用于存储处理器可执行指令的存储器，所述处理器执行所述指令时实现上述实施例的身份认证数据处理方法，如：

[0131] 指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动；

[0132] 接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据；

[0133] 获取所述待认证账户的用户数据以及所述客户端的终端属性数据；

[0134] 根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证。

[0135] 或，接收服务器发送的终端转动校验的指示；

[0136] 以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据；

[0137] 将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证。

[0138] 本说明书实施例还提供一种身份认证系统，包括：客户端、服务器；其中，所述服务器中包括至少一个处理器以及用于存储处理器可执行指令的存储器，所述处理器执行所述指令时实现上述服务器侧执行的方法，用于在确定待认证账户存在风险时，指示所述客户端进行终端转动校验，基于所述客户端的转动校验数据以及所述客户端的终端属性数据、所述待认证账户的用户数据对所述待认证账户进行身份认证；

[0139] 所述客户端包括至少一个处理器以及用于存储处理器可执行指令的存储器，所述处理器执行所述指令时实现上述客户端侧执行方法，用于接收所述服务器发送的终端转动校验指令，并向所述服务器上传终端转动校验过程中的转动校验数据。

[0140] 需要说明的，上述所述的设备和系统根据方法实施例的描述还可以包括其他的实施方式。具体的实现方式可以参照相关方法实施例的描述，在此不作一一赘述。

[0141] 本说明书提供的身份认证装置，也可以应用在多种数据分析处理系统中。所述系统或服务器或终端或设备可以为单独的服务器，也可以包括使用了本说明书的一个或多个所述方法或一个或多个实施例系统或服务器或终端或设备的服务器集群、系统(包括分布式系统)、软件(应用)、实际操作装置、逻辑门电路装置、量子计算机等并结合必要的实施硬件的终端装置。所述核对差异数据的检测系统可以包括至少一个处理器以及存储计算机可执行指令的存储器，所述处理器执行所述指令时实现上述任意一个或者多个实施例中所述方法的步骤。

[0142] 本说明书实施例所提供的方法实施例可以在移动终端、计算机终端、服务器或者类似的运算装置中执行。以运行在服务器上为例，图6是本说明书一个实施例中身份认证服务器的硬件结构框图，该计算机终端可以是上述实施例中的身份认证服务器或身份认证装置。如图6所示服务器10可以包括一个或多个(图中仅示出一个)处理器100(处理器100可以包括但不限于微处理器MCU或可编程逻辑器件FPGA等的处理装置)、用于存储数据的非易失性存储器200、以及用于通信功能的传输模块300。本领域普通技术人员可以理解，图6所示的结构仅为示意，其并不对上述电子装置的结构造成限定。例如，服务器10还可包括比图6中所示更多或者更少的组件，例如还可以包括其他的处理硬件，如数据库或多级缓存、GPU，或者具有与图6所示不同的配置。

[0143] 非易失性存储器200可用于存储应用软件的软件程序以及模块，如本说明书实施例中的身份认证方法对应的程序指令/模块，处理器100通过运行存储在非易失性存储器200内的软件程序以及模块，从而执行各种功能应用以及资源数据更新。非易失性存储器200可包括高速随机存储器，还可包括非易失性存储器，如一个或者多个磁性存储装置、闪存、或者其他非易失性固态存储器。在一些实例中，非易失性存储器200可进一步包括相对

于处理器100远程设置的存储器，这些远程存储器可以通过网络连接至计算机终端。上述网络的实例包括但不限于互联网、企业内部网、局与网、移动通信网及其组合。

[0144] 传输模块300用于经由一个网络接收或者发送数据。上述的网络具体实例可包括计算机终端的通信供应商提供的无线网络。在一个实例中，传输模块300包括一个网络适配器(Network Interface Controller,NIC)，其可通过基站与其他网络设备相连从而可与互联网进行通讯。在一个实例中，传输模块300可以为射频(Radio Frequency,RF)模块，其用于通过无线方式与互联网进行通讯。

[0145] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[0146] 本说明书提供的上述实施例所述的方法或装置可以通过计算机程序实现业务逻辑并记录在存储介质上，所述的存储介质可以计算机读取并执行，实现本说明书实施例所描述方案的效果，如：

[0147] 指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动；

[0148] 接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据；

[0149] 获取所述待认证账户的用户数据以及所述客户端的终端属性数据；

[0150] 根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证。

[0151] 或，接收服务器发送的终端转动校验的指示；

[0152] 以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据；

[0153] 将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证。

[0154] 所述存储介质可以包括用于存储信息的物理装置，通常是将信息数字化后再以利用电、磁或者光学等方式的媒体加以存储。所述存储介质有可以包括：利用电能方式存储信息的装置如，各式存储器，如RAM、ROM等；利用磁能方式存储信息的装置如，硬盘、软盘、磁带、磁芯存储器、磁泡存储器、U盘；利用光学方式存储信息的装置如，CD或DVD。当然，还有其他方式的可读存储介质，例如量子存储器、石墨烯存储器等等。

[0155] 本说明书实施例提供的上述身份认证方法或装置可以在计算机中由处理器执行相应的程序指令来实现，如使用windows操作系统的c++语言在PC端实现、linux系统实现，或其他例如使用android、iOS系统程序设计语言在智能终端实现，以及基于量子计算机的处理逻辑实现等。

[0156] 需要说明的是说明书上述所述的装置、计算机存储介质、系统根据相关方法实施例的描述还可以包括其他的实施方式，具体的实现方式可以参照对应方法实施例的描述，

在此不作一一赘述。

[0157] 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考即可，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，对于硬件+程序类实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参考方法实施例的部分说明即可。

[0158] 本说明书实施例并不局限于必须是符合行业通信标准、标准计算机资源数据更新和数据存储规则或本说明书一个或多个实施例所描述的情况。某些行业标准或者使用自定义方式或实施例描述的实施基础上略加修改后的实施方案也可以实现上述实施例相同、等同或相近、或变形后可预料的实施效果。应用这些修改或变形后的数据获取、存储、判断、处理方式等获取的实施例，仍然可以属于本说明书实施例的可选实施方案范围之内。

[0159] 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)、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。

[0160] 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。

[0161] 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、车载人机交互设备、蜂窝电话、相机电话、智能电话、个人数字助理、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。

[0162] 虽然本说明书一个或多个实施例提供了如实施例或流程图所述的方法操作步骤，但基于常规或者无创造性的手段可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式，不代表唯一的执行顺序。在实际中的装置或终端产品执行时，可以按照实施例或者附图所示的方法顺序执行或者并行执行(例如并行处理器或者多线程处理的环境，甚至为分布式资源数据更新环境)。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、产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、产品或者设备所固有的要素。在没有更多限制的情况下，并不排除在包括所述要素的过程、方法、产品或者设备中还存在另外的相同或等同要素。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

[0163] 为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书一个或多个时可以把各模块的功能在同一个或多个软件和/或硬件中实现，也可以将实现同一功能的模块由多个子模块或子单元的组合实现等。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，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。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0164] 本发明是参照根据本发明实施例的方法、装置(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资源数据更新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资源数据更新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。

[0165] 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资源数据更新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。

[0166] 这些计算机程序指令也可装载到计算机或其他可编程资源数据更新设备上，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。

[0167] 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

络接口和内存。

[0168] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0169] 计算机可读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。计算机的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、石墨烯存储或其他磁性存储设备或任何其他非传输介质,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。

[0170] 本领域技术人员应明白,本说明书一个或多个实施例可提供为方法、系统或计算机程序产品。因此,本说明书一个或多个实施例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,本说明书一个或多个实施例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。

[0171] 本说明书一个或多个实施例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本说明书一个或多个实施例,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。

[0172] 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考即可,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,对于系统实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参考方法实施例的部分说明即可。在本说明书的描述中,参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本说明书的至少一个实施例或示例中。在本说明书中,对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且,描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外,在不相互矛盾的情况下,本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0173] 以上所述仅为本说明书一个或多个实施例的实施例而已,并不用于限制本说明书一个或多个实施例。对于本领域技术人员来说,本说明书一个或多个实施例可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等,均应包含在权利要求范围之内。

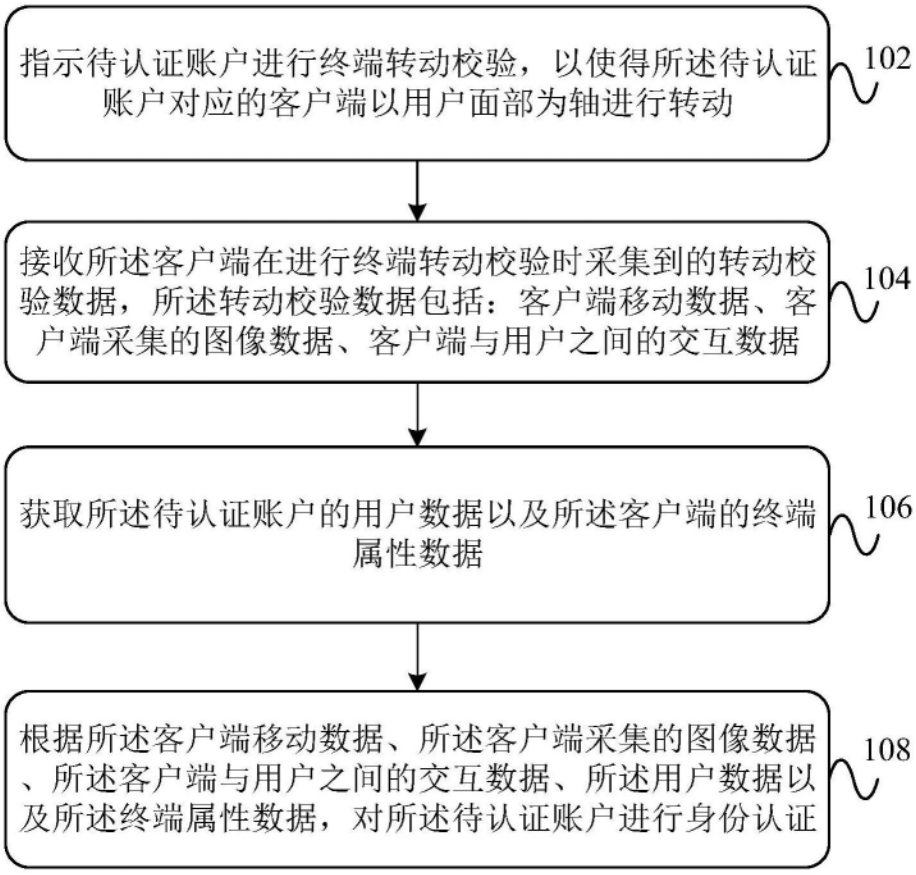

指示待认证账户进行终端转动校验，以使得所述待认证账户对应的客户端以用户面部为轴进行转动
102
接收所述客户端在进行终端转动校验时采集到的转动校验数据，所述转动校验数据包括：客户端移动数据、客户端采集的图像数据、客户端与用户之间的交互数据
104
获取所述待认证账户的用户数据以及所述客户端的终端属性数据
106
根据所述客户端移动数据、所述客户端采集的图像数据、所述客户端与用户之间的交互数据、所述用户数据以及所述终端属性数据，对所述待认证账户进行身份认证
108

图1

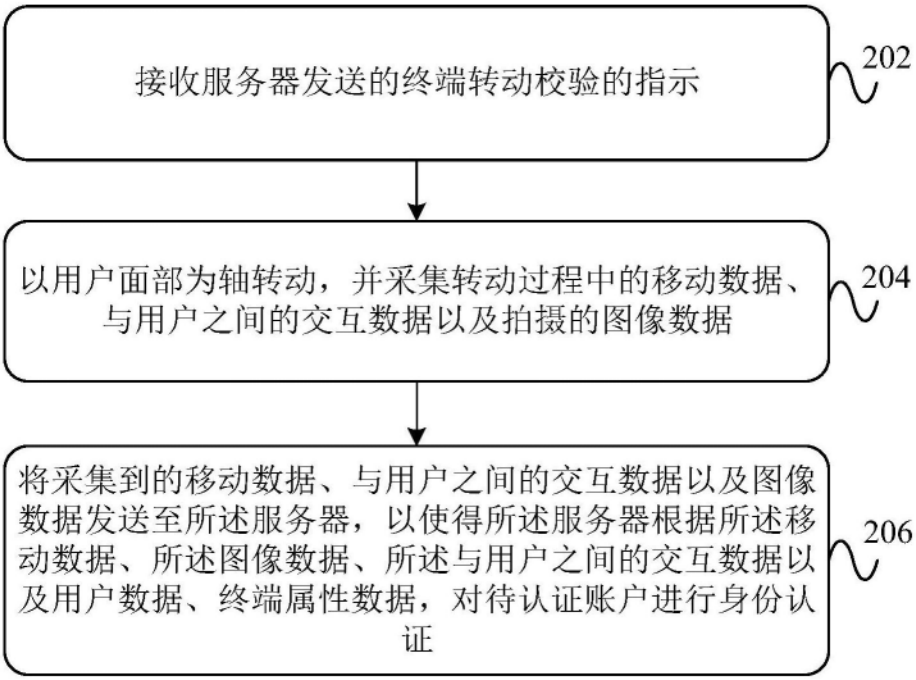

接收服务器发送的终端转动校验的指示
202
以用户面部为轴转动，并采集转动过程中的移动数据、与用户之间的交互数据以及拍摄的图像数据
204
将采集到的移动数据、与用户之间的交互数据以及图像数据发送至所述服务器，以使得所述服务器根据所述移动数据、所述图像数据、所述与用户之间的交互数据以及用户数据、终端属性数据，对待认证账户进行身份认证
206

图2

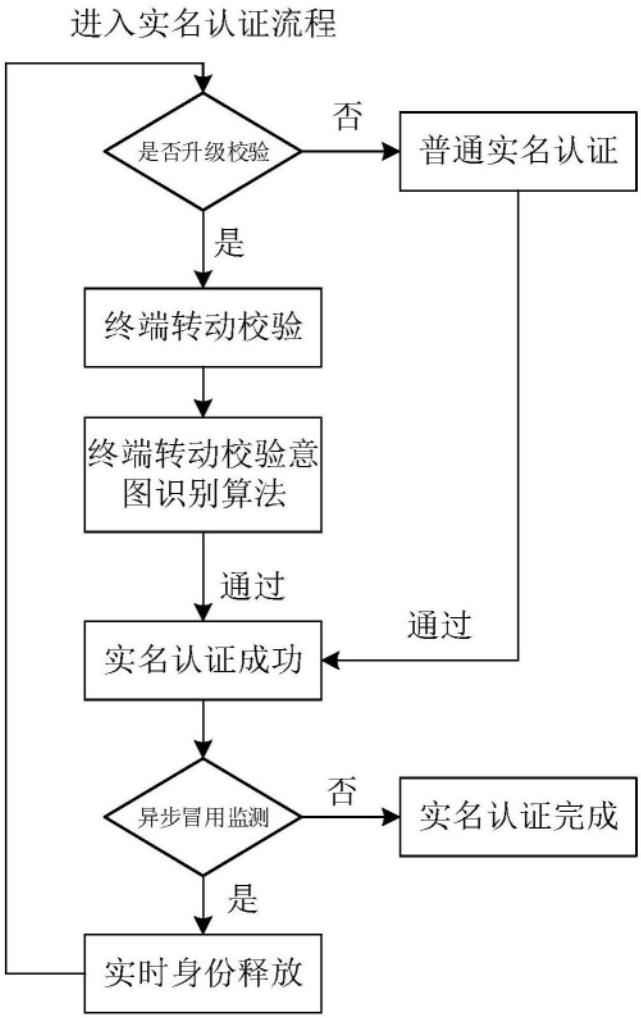

进入实名认证流程
是否升级校验
否
普通实名认证
是
终端转动校验
终端转动校验意图识别算法
通过
通过
实名认证成功
异步冒用监测
否
实名认证完成
是
实时身份释放

图3

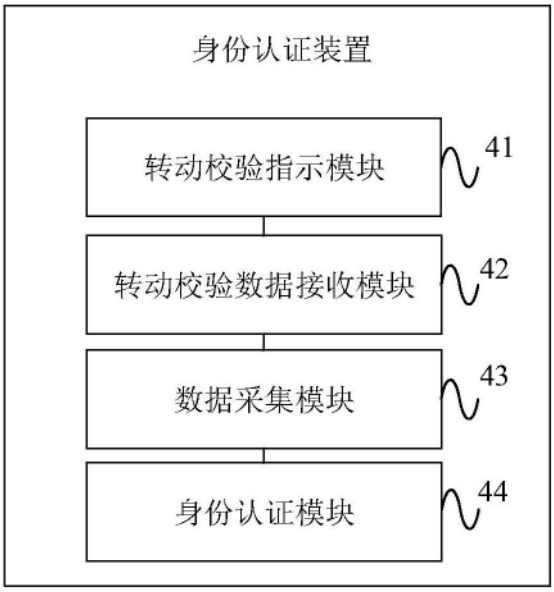

身份认证装置
转动校验指示模块
41
转动校验数据接收模块
42
数据采集模块
43
身份认证模块
44

图4

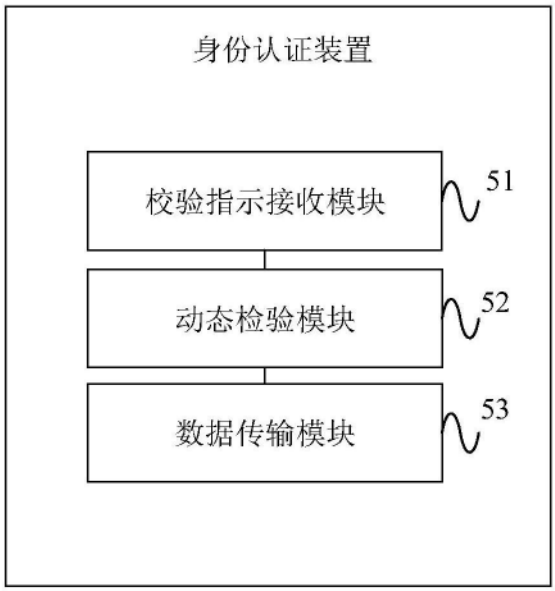

身份认证装置
校验指示接收模块
51
动态检验模块
52
数据传输模块
53

图5

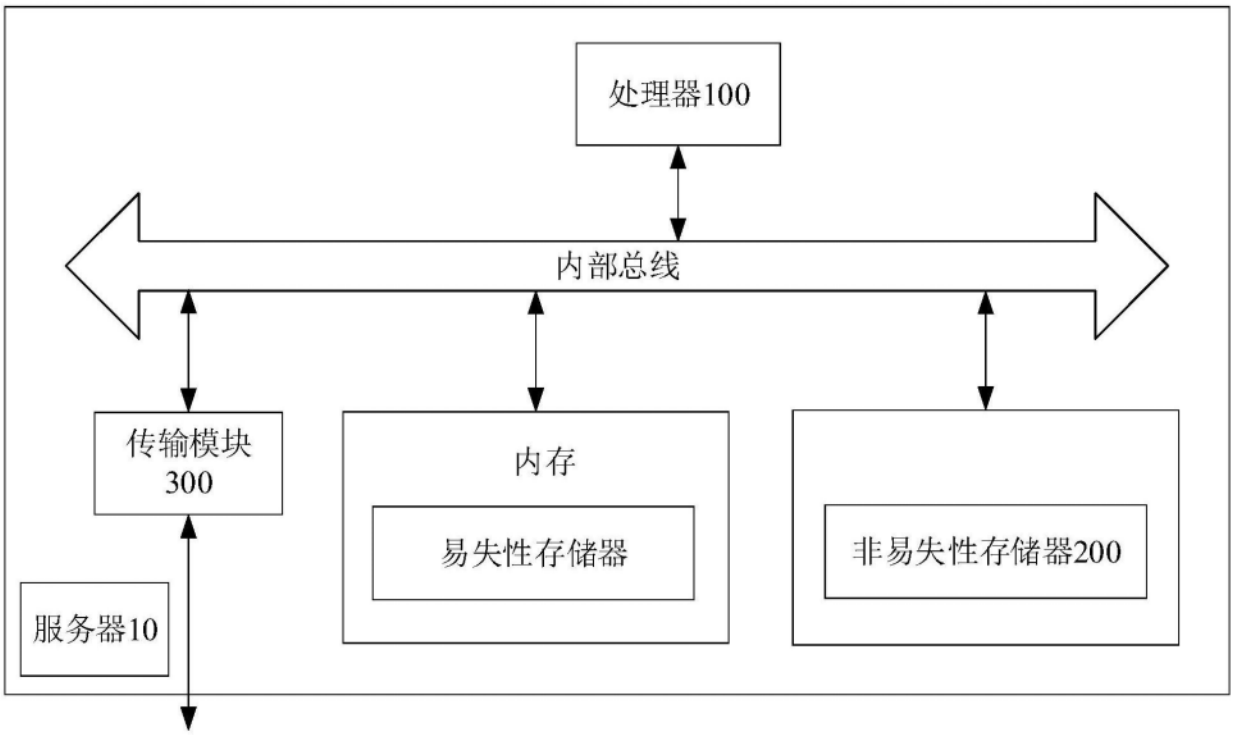


图6