(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111741033 B
(45)授权公告日 2020.11.17

(21)申请号 202010874101.7
(22)申请日 2020.08.27
(65)同一申请的已公布的文献号
申请公布号 CN 111741033 A
(43)申请公布日 2020.10.02
(73)专利权人 腾讯科技(深圳)有限公司
地址 518044 广东省深圳市南山区高新区科技中一路腾讯大厦35层
(72)发明人 农燕丽 丁志敏
(74)专利代理机构 北京同达信恒知识产权代理有限公司 11291
代理人 李娟
(51)Int.Cl.
H04L 29/06(2006.01)

审查员 白生斌

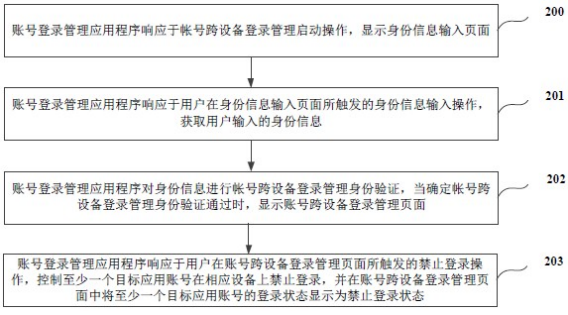
权利要求书3页 说明书21页 附图9页

(54)发明名称

一种账号跨设备登录管理的方法、装置、设备和介质

(57)摘要

本申请属于数据处理技术领域，主要涉及人工智能中的计算机视觉技术，公开了一种账号跨设备登录管理的方法、装置、设备和介质，本申请公开的一种账号跨设备登录管理的方法包括，响应于帐号跨设备登录管理启动操作，显示身份信息输入页面，响应于身份信息输入操作，获取用户的身份信息，并根据用户的身份信息，获取并显示用户关联的设备标识信息以及每一设备标识信息关联的目标应用账号信息，以及根据用户的禁止登录请求，控制指定的设备标识信息对应的设备上禁止登录指定的目标应用账号，并显示目标应用账号的登录状态。这样，可以对多个目标应用账号的登录状态进行批量处理，简化了账号跨设备登录管理的繁琐操作，提高了处理效率以及安全性。



CN 111741033 B

1.一种帐号跨设备登录管理方法,其特征在于,包括:

响应于帐号跨设备登录管理启动操作,显示身份信息输入页面;

响应于用户在所述身份信息输入页面所触发的身份信息输入操作,获取用户输入的身份信息;

对所述身份信息进行帐号跨设备登录管理身份验证,当确定帐号跨设备登录管理身份验证通过时,显示账号跨设备登录管理页面,所述账号跨设备登录管理页面中包含所述身份信息关联的至少一个设备标识信息,每个设备标识信息对应的设备关联的各个目标应用账号信息,以及每一设备标识信息关联的各目标应用账号的登录状态;

响应于用户在所述账号跨设备登录管理页面所触发的禁止登录操作,控制至少一个目标应用账号在相应设备上禁止登录,并在所述账号跨设备登录管理页面中将所述至少一个目标应用账号的登录状态显示为禁止登录状态。

2.如权利要求1所述的方法,其特征在于,还包括:

响应于账号跨设备登录管理开通操作,显示身份信息输入页面;

响应于用户在所述身份信息输入页面所触发的身份信息输入操作,获取所述用户的身份信息;

将所述身份信息发送至第三方认证平台,使得所述第三方认证平台对所述身份信息进行帐号跨设备登录管理身份验证;

接收所述第三方认证平台返回的身份验证结果,当所述身份验证结果表征验证通过时,显示设置页面;

响应于用户在设置页面所触发的目标应用关联操作,向各个应用服务器发送应用关联请求;

接收各应用服务器基于接收的应用关联请求返回的所述身份信息关联的各个目标应用账号信息以及各个目标应用账号信息分别关联的设备标识信息;

在所述设置页面上显示各个设备标识信息,以及每个设备标识信息关联的目标应用账号信息。

3.如权利要求1所述的方法,其特征在于,当确定帐号跨设备登录管理身份验证通过时,显示账号跨设备登录管理页面,包括:

分别向每一目标应用账号对应的应用服务器发送包含身份信息的登录状态请求;

接收各应用服务器基于登录状态请求返回的当前运行相应的目标应用账号的设备对应的设备标识信息;

根据获取的各设备标识信息,以及每一设备标识信息对应的设备上运行的目标应用账号信息,对所述身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的目标应用账号信息进行更新;

在所述账号跨设备登录管理页面中,显示更新后的所述身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的各目标应用账号信息。

4.如权利要求3所述的方法,其特征在于,还包括:

接收各应用服务器基于登录状态请求返回的每一设备标识信息对应的设备关联的目标应用账号的登录状态;

在所述账号跨设备登录管理页面中,还显示每一设备标识信息关联的各目标应用账号

的登录状态。

5.如权利要求1-4任一项所述的方法，其特征在于，响应于用户在所述账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录，包括：

响应于禁止登录操作，向各目标应用账号对应的应用服务器发送禁止登录请求，使得各应用服务器基于所述禁止登录请求控制各目标应用账号退出以及禁止登录关联的各设备标识信息对应的设备；或者，

响应于禁止登录操作，向各目标应用账号对应的应用服务器发送禁止登录请求，使得各应用服务器基于所述禁止登录请求控制指定的设备标识信息关联的各目标应用账号退出以及禁止登录指定的设备标识信息对应的设备；或者，

响应于禁止登录操作，向各指定的目标应用账号对应的应用服务器发送禁止登录请求，使得各应用服务器基于所述禁止登录请求控制指定的目标应用账号退出以及禁止登录指定的设备标识信息对应的设备。

6.如权利要求1-4任一项所述的方法，其特征在于，在显示账号跨设备登录管理页面之后，还包括：

响应于一键退出登录操作，向各目标应用账号对应的应用服务器发送退出登录请求，使得各应用服务器基于所述退出登录请求控制各目标应用账号从关联的各设备标识信息对应的设备上退出登录；或者，

响应于设备退出登录操作，向各目标应用账号对应的应用服务器发送退出登录请求，使得各应用服务器基于所述退出登录请求控制指定的设备标识信息关联的各目标应用账号从指定的设备标识信息对应的设备上退出登录；或者，

响应于自定义退出登录操作，向各指定的目标应用账号对应的应用服务器发送退出登录请求，使得各应用服务器基于所述退出登录请求控制指定的目标应用账号从指定的设备标识信息对应的设备上退出登录。

7.如权利要求1-4任一项所述的方法，其特征在于，还包括：

响应于一键恢复登录操作，向各目标应用账号对应的应用服务器发送恢复登录请求，使得各应用服务器基于所述恢复登录请求，执行撤销各目标应用账号禁止登录关联的各设备标识信息对应的设备的设置操作；或者，

响应于设备恢复登录操作，向各目标应用账号对应的应用服务器发送恢复登录请求，使得各应用服务器基于所述恢复登录请求，执行撤销各目标应用账号禁止登录指定的设备标识信息对应的设备的设置操作；或者，

响应于自定义恢复登录操作，向各指定的目标应用账号对应的应用服务器发送恢复登录请求，使得各应用服务器基于所述恢复登录请求，执行撤销指定的目标应用账号禁止登录指定的设备标识信息对应的设备的设置操作。

8.如权利要求1-4任一项所述的方法，其特征在于，还包括：

响应于用户在账号跨设备登录管理页面所触发的一键删除操作，删除各目标应用账号以及关联的设备标识信息；或者，

响应于用户在账号跨设备登录管理页面所触发的设备删除操作，删除指定的设备标识信息；或者，

响应于用户在账号跨设备登录管理页面所触发的自定义删除操作，删除指定的设备标识信息和指定的目标应用账号之间的关联关系。

9.如权利要求2所述的方法，其特征在于，进一步包括：

响应于用户在所述账号跨设备登录管理页面或所述设置页面所触发的设备关联操作，显示设备信息输入页面；

响应于用户在所述设备信息输入页面所述触发的设备信息输入操作，获取用户输入的设备标识信息；

将用户输入的设备标识信息，确定为所述身份信息关联的设备标识信息。

10.一种账号跨设备登录管理的装置，其特征在于，包括：

启动单元，用于响应于帐号跨设备登录管理启动操作，显示身份信息输入页面；

输入单元，用于响应于用户在所述身份信息输入页面所触发的身份信息输入操作，获取用户输入的身份信息；

显示单元，用于对所述身份信息进行帐号跨设备登录管理身份验证，当确定帐号跨设备登录管理身份验证通过时，显示账号跨设备登录管理页面，所述账号跨设备登录管理页面中包含所述身份信息关联的至少一个设备标识信息，每个设备标识信息对应的设备关联的各个目标应用账号信息，以及每一设备标识信息关联的各目标应用账号的登录状态；

控制单元，用于响应于用户在所述账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录，并在所述账号跨设备登录管理页面中将所述至少一个目标应用账号的登录状态显示为禁止登录状态。

11.一种控制设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时实现权利要求1-9任一项所述的方法的步骤。

12.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时实现权利要求1-9任一项所述方法的步骤。

一种账号跨设备登录管理的方法、装置、设备和介质

技术领域

[0001] 本申请涉及数据处理技术领域，尤其涉及一种账号跨设备登录管理的方法、装置、设备和介质。

背景技术

[0002] 用户通常会在不同的应用中注册有大量的应用账号。用户通常需要在更换设备或者设备丢失时，为避免财产损失以及信息泄露，通常会采用强制退出、冻结、挂失以及注销等方式，对应用账号的登录状态进行管理。

[0003] 例如，用户更换设备时，通常在新的设备上登录应用账号，使得该应用账号在旧设备行被强制退出登录。又例如，当用户的设备丢失时，用户需要从其它设备上登录以及冻结各应用账号，使得任何人均不能登录用户的应用账号。

[0004] 但是，实际应用中，用户通常容易忘记有多少应用账号需要处理，因此，容易遗漏。再者，用户通常需要分别登录每一应用账号以进行账号冻结，耗时较长，容易导致操作的应用账号被不法分子利用，无法保证财产和信息的安全性；进一步地，应用账号冻结时，通常需要繁琐的帐号跨设备登录管理身份验证过程，当应用账号较多时，用户需要重复的进行帐号跨设备登录管理身份验证操作，操作步骤复杂，且应用账号冻结后，包括用户在内的任何人均不能登录该应用账号，这给用户带来了不便。

[0005] 由此，在对应用账号进行账号跨设备登录管理时，需要一种账号跨设备登录管理的技术方案，以简化账号跨设备登录管理的繁琐操作，减少耗费的时长以及提高应用账号的安全性。

发明内容

[0006] 本申请实施例提供一种账号跨设备登录管理的方法、装置和存储介质，用于在进行账号跨设备登录管理时，对多个应用账号的登录状态进行统一管理，简化了账号跨设备登录管理的繁琐操作，减少了耗费的时长，以及提高了信息的安全性。

[0007] 一方面，提供一种账号跨设备登录管理的方法，包括：

[0008] 响应于帐号跨设备登录管理启动操作，显示身份信息输入页面；

[0009] 响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户输入的身份信息；

[0010] 对身份信息进行帐号跨设备登录管理身份验证，当确定帐号跨设备登录管理身份验证通过时，显示账号跨设备登录管理页面，账号跨设备登录管理页面中包含身份信息关联的至少一个设备标识信息，以及每个设备标识信息对应的设备关联的各个目标应用账号信息；

[0011] 响应于用户在账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录，并在账号跨设备登录管理页面中将至少一个目标应用账号的登录状态显示为禁止登录状态。

[0012] 一方面，提供一种账号跨设备登录管理的装置，包括：

[0013] 启动单元，用于响应于帐号跨设备登录管理启动操作，显示身份信息输入页面；

[0014] 输入单元，用于响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户输入的身份信息；

[0015] 显示单元，用于对身份信息进行帐号跨设备登录管理身份验证，当确定帐号跨设备登录管理身份验证通过时，显示账号跨设备登录管理页面，账号跨设备登录管理页面中包含身份信息关联的至少一个设备标识信息，以及每个设备标识信息对应的设备关联的各个目标应用账号信息；

[0016] 控制单元，用于响应于用户在账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录，并在账号跨设备登录管理页面中将至少一个目标应用账号的登录状态显示为禁止登录状态。

[0017] 一方面，提供一种控制设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行程序时执行上述任一种账号跨设备登录管理的方法的步骤。

[0018] 一方面，提供一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述任一种账号跨设备登录管理的方法的步骤。

[0019] 一方面，提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述任一种账号跨设备登录管理的各种可选实现方式中提供的方法。

[0020] 本申请实施例提供的一种账号跨设备登录管理的方法、装置、设备和介质中，响应于帐号跨设备登录管理启动操作，显示身份信息输入页面，响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户的身份信息，并根据用户的身份信息，获取并显示用户关联的设备标识信息以及每一设备标识信息关联的目标应用账号信息，以及根据用户的禁止登录请求，控制指定的设备标识信息对应的设备上禁止登录指定的目标应用账号，并显示目标应用账号的登录状态。这样，实现了对多个目标应用账号的跨设备批量处理，简化了账号跨设备登录管理的繁琐操作，可以快速控制指定的设备上禁止登录指定的目标应用账户，不影响目标应用账户在非指定的设备上运行，提高了处理效率以及安全性。

[0021] 本申请的其它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，或者通过实施本申请而了解。本申请的目的和其他优点可通过在所写的说明书、权利要求书、以及附图中所特别指出的结构来实现和获得。

附图说明

[0022] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0023] 图1a为本申请实施方式中一种账号跨设备登录管理开通的方法的实施流程图；

[0024] 图1b为本申请实施方式中一种设置页面的示例图；

[0025] 图2为本申请实施方式中一种账号跨设备登录管理的方法的实施流程图；

[0026] 图3为本申请实施方式中一种账号跨设备登录管理的方法的详细实施流程图；

[0027] 图4a为本申请实施方式中一种账号跨设备登录管理页面的示例图；

[0028] 图4b为本申请实施方式中一种数据结构的示例图；

[0029] 图5为本申请实施方式中一种帐号跨设备登录管理身份验证的方法的实施流程图；

[0030] 图6为本申请实施方式中一种模型处理框架的示例图；

[0031] 图7为本申请实施方式中一种账号跨设备登录管理的方法的交互流程图；

[0032] 图8为本申请实施方式中一种账号跨设备登录管理的装置的结构示意图；

[0033] 图9为本申请实施方式中一种控制设备的结构示意图。

具体实施方式

[0034] 为了使本申请的目的、技术方案及有益效果更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[0035] 首先，对本申请实施例中涉及的部分用语进行说明，以便于本领域技术人员理解。

[0036] 终端设备：可以是移动终端、固定终端或便携式终端，例如移动手机、站点、单元、设备、多媒体计算机、多媒体平板、互联网节点、通信器、台式计算机、膝上型计算机、笔记本计算机、上网本计算机、平板计算机、个人通信系统设备、个人导航设备、个人数字助理、音频/视频播放器、数码相机/摄像机、定位设备、电视接收器、无线电广播接收器、电子书设备、游戏设备或者其任意组合，包括这些设备的配件和外设或者其任意组合。还可预见到的是，终端设备能够支持任意类型的针对用户的接口(例如可穿戴设备)等。

[0037] 服务器：可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务以及大数据和人工智能平台等基础云计算服务的云服务器。

[0038] 应用程序：可以完成某项或多项业务的计算机程序，一般具有可视的显示界面，能与用户进行交互。

[0039] 人工智能(Artificial Intelligence，AI)：是利用数字计算机或者数字计算机控制的机器模拟、延伸和扩展人的智能，感知环境、获取知识并使用知识获得最佳结果的理论、方法、技术及应用系统。换句话说，人工智能是计算机科学的一个综合技术，它企图了解智能的实质，并生产出一种新的能以人类智能相似的方式做出反应的智能机器。人工智能也就是研究各种智能机器的设计原理与实现方法，使机器具有感知、推理与决策的功能。

[0040] 人工智能技术是一门综合学科，涉及领域广泛，既有硬件层面的技术也有软件层面的技术。人工智能基础技术一般包括如传感器、专用人工智能芯片、云计算、分布式存储、大数据处理技术、操作/交互系统、机电一体化等技术。人工智能软件技术主要包括计算机视觉技术、语音处理技术、自然语言处理技术以及机器学习/深度学习等几大方向。

[0041] 计算机视觉技术(Computer Vision，CV)计算机视觉是一门研究如何使机器“看”的科学，更进一步的说，就是指用摄影机和电脑代替人眼对目标进行识别、跟踪和测量等机器视觉，并进一步做图形处理，使电脑处理成为更适合人眼观察或传送给仪器检测的图像。计算机视觉研究相关的理论和技术，试图建立能够从图像或者多维数据中获取信息的人工

智能系统。计算机视觉技术通常包括图像处理、图像识别、图像语义理解、图像检索、OCR、视频处理、视频语义理解、视频内容/行为识别、三维物体重建、3D技术、虚拟现实、增强现实、同步定位与地图构建等技术，还包括常见的人脸识别、指纹识别等生物特征识别技术。

[0042] 设备标识信息：为当前运行目标应用账号的设备的标识信息。

[0043] 目标应用账号：是指用户在目标应用中注册后获得的用于登录的账号，如，手机号以及微信号等。

[0044] 目标应用账号信息：是指与目标应用账号相关的信息，如，图标以及昵称等。

[0045] 当前登录状态：目标应用账号当前在目标设备上处于登录状态。

[0046] 历史登录状态：目标应用账号在目标设备上登录过，且当前已经退出登录。

[0047] 未曾登录状态：目标应用账号从未在目标设备上登录过。

[0048] 禁止登录状态：目标应用账号被禁止登录目标设备。

[0049] 强制退出状态：目标应用账号登录目标设备后，被强制退出目标设备。

[0050] 下面介绍本申请实施例的设计思想。

[0051] 用户通常会在不同的应用中注册有大量的应用账号。用户通常需要在更换设备或者设备丢失时，为避免财产损失以及信息泄露，通常会采用：强制退出、冻结、挂失以及注销等方式，对应用账号的登录状态进行管理。

[0052] 例如，用户更换设备时，通常在新的设备上登录应用账号，使得该应用账号在旧设备行被强制退出登录。又例如，当用户的设备丢失时，用户需要从其它设备上登录以及冻结各应用账号，使得任何人均不能登录用户的应用账号。

[0053] 但是，实际应用中，用户通常容易忘记有多少应用账号需要处理，容易遗漏。再者，用户通常需要分别登录每一应用账号以进行账号冻结，耗时较长，容易导致操作的应用账号被不法分子利用，无法保证财产和信息的安全性；进一步地，应用账号冻结时，通常需要繁琐的帐号跨设备登录管理身份验证过程，当应用账号较多时，用户需要重复的进行帐号跨设备登录管理身份验证操作，操作步骤复杂，且应用账号冻结后，包括用户在内的任何人均不能登录该应用账号，这给用户带来了不便。

[0054] 显然，在对应用账号进行账号跨设备登录管理时，需要一种账号跨设备登录管理的技术方案，以简化账号跨设备登录管理的繁琐操作，减少耗费的时长以及提高应用账号的安全性。

[0055] 考虑到可以通过一个账号登录管理应用程序将用户与多个应用账号绑定，进而对用户关联的多个应用账号的登录状态进行统一控制以及批量处理，本申请实施例中提供了一种账号跨设备登录管理的技术方案，该方案中，响应于帐号跨设备登录管理启动操作，显示身份信息输入页面，响应于身份信息输入操作，获取用户输入的身份信息，并对用户的身份信息进行帐号跨设备登录管理身份验证，当用户的帐号跨设备登录管理身份验证通过时，向应用服务器发送包含身份信息的登录状态请求，并接收应用服务器返回的用户的身份信息关联的各设备标识信息以及每一设备标识信息关联的各目标应用账号信息，在账号跨设备登录管理页面，显示用户的身份信息关联的各设备标识信息以及每一设备标识信息关联的各目标应用账号信息，以及响应于用户的禁止登录操作，控制用户指定的至少一个目标应用账号在指定的设备上禁止登录，并在登录控制页面中更新指定的目标应用账号的登录状态。

[0056] 为进一步说明本申请实施例提供的技术方案，下面结合附图以及具体实施方式对此进行详细的说明。虽然本申请实施例提供了如下述实施例或附图所示的方法操作步骤，但基于常规或者无需创造性的劳动在方法中可以包括更多或者更少的操作步骤。在逻辑上不存在必要因果关系的步骤中，这些步骤的执行顺序不限于本申请实施例提供的执行顺序。方法在实际的处理过程中或者装置执行时，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。

[0057] 在对应用账号进行账号跨设备登录管理之前，先开通账号跨设备登录管理，绑定用户关联的一个或多个目标应用账号。具体的，账号登录管理应用程序响应于账号跨设备登录管理开通操作，显示身份信息输入页面，并响应于身份信息输入操作，对输入的身份信息进行验证，以及确定帐号跨设备登录管理身份验证通过时，显示账号跨设备登录管理设置页面，并响应于目标应用关联操作，获取身份信息关联的各个目标应用账号信息以及各个目标应用账号信息分别关联的设备标识信息，以及在账号跨设备登录管理设置页面上显示各设备标识信息和每一设备标识信息关联的目标应用账号信息。

[0058] 参阅图1a所示，为本申请提供的一种账号跨设备登录管理开通的方法的实施流程图。该方法的具体流程如下：

[0059] 步骤100：账号登录管理应用程序响应于账号跨设备登录管理开通操作，显示身份信息输入页面。

[0060] 具体的，账号登录管理应用程序被安装于控制设备中。账号登录管理应用程序具有可视的显示界面，可以与用户进行交互。用户可以通过控制设备的输入单元，如，键盘、触摸屏以及音视频采集单元等，与账号登录管理应用程序进行交互，使得账号登录管理应用程序执行相应的操作，以及页面跳转。

[0061] 可选的，控制设备可以为终端设备或服务器。

[0062] 本申请实施例中的操作，可以通过按键、触摸屏、语音、图像、气味、温度、控制设备的朝向等触发，在此不作限制。

[0063] 例如，用户按压账号登录管理应用程序的主页面上的登录按键时，账号登录管理应用程序响应于账号跨设备登录管理开通操作，显示身份信息输入页面。

[0064] 又例如，用户预先在设备中设置显示身份信息输入页面的快捷键，当用户点击该快捷键时，账号登录管理应用程序响应于账号跨设备登录管理开通操作，显示身份信息输入页面。

[0065] 一种实施方式中，账号登录管理显示身份信息输入页面时，可以采用以下步骤：

[0066] S1001：账号登录管理应用程序显示账号管理页面。

[0067] S1002：账号登录管理应用程序响应于用户在账号管理页面所触发的设备保护操作，显示一键开启页面。

[0068] 一种实施方式中，当用户点击设备保护的开启按键时，账号登录管理应用程序响应于开启按键触发操作，从账号管理页面，跳转至一键开启页面。

[0069] 其中，一键开启页面用于根据用户的确认指令跳转至下一页面以开启设备保护。

[0070] S1003：用户点击开启设备保护按键，账号登录管理应用程序响应于账号跨设备登录管理开通操作，显示身份信息输入页面。

[0071] 一种实施方式中，当用户点击一键开启页面中的开启设备保护按键时，账号登录

管理应用响应于账号跨设备登录管理开通操作，从一键开启页面跳转至身份信息输入页面。

[0072] 其中，身份信息输入页面用于获取以及验证用户输入的身份信息。身份信息可以包括以下任意一种或任意组合：人脸图像、声纹、指纹、虹膜以及应用账号信息等。

[0073] 这样，就可以显示身份信息输入页面。

[0074] 步骤101：账号登录管理应用程序响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户的身份信息，并对输入的身份信息进行验证。

[0075] 具体的，账号登录管理应用程序响应于身份信息输入操作，获取用户输入的身份信息，并将用户输入的身份信息，发送至控制服务器。控制服务器将身份信息发送至第三方认证平台。第三方认证平台对身份信息进行身份验证。

[0076] 其中，身份信息中至少包括人脸图像，还可以包含应用账号信息以及其它生物识别信息等。

[0077] 一种实施方式中，对身份信息进行身份验证时，采用以下步骤：

[0078] 具体的，账号登录管理应用程序响应于在第一身份信息输入页面中的第一身份信息输入操作，获取用户输入的账号登录管理应用程序账号和验证信息，并将获取的账号登录管理应用程序账号和验证信息发送至控制服务器。控制服务器接收账号登录管理应用程序发送的账号登录管理应用程序账号和验证信息，并获取存储的各应用账号和各验证信息之间的对应关系。控制服务器根据账号登录管理应用程序账号以及上述对应关系，获得账号登录管理应用程序账号对应设置的目标验证信息，若目标验证信息和接收的验证信息相同，则判定应用账号验证成功，显示第二身份信息输入页面，否则，显示帐号跨设备登录管理身份验证失败页面。

[0079] 接着，账号登录管理应用程序响应于在第二身份信息输入页面中的第二身份信息输入操作，获取用户输入的人脸图像，并将获取的人脸图像发送至控制服务器。控制服务器将人脸图像发送至第三方认证平台。第三方认证平台获取存储的包含人脸图像样本的人脸信息数据库，并将接收的人脸图像依次与每一人脸图像样本进行匹配，若获得匹配的人脸图像样本，则将匹配的人脸图像样本对应的用户身份信息，确定为人脸识别结果，获得表示验证通过的帐号跨设备登录管理身份验证结果，否则，获得表征验证失败的帐号跨设备登录管理身份验证结果，显示帐号跨设备登录管理身份验证失败页面。

[0080] 其中，第三方认证平台可以为公安系统。用户将账号登录管理应用程序账号进行实名认证后，账号登录管理应用程序可以通过第三方认证平台确定用户的身份，以及通过人脸识别对用户的身份再次确认。

[0081] 这样，就可以对用户的身份进行验证，提高账号跨设备登录管理的安全性。

[0082] 本申请实施例中，仅以将应用账号验证和人脸识别相结合的方式，进行帐号跨设备登录管理身份验证为例进行说明，实际应用中，也可以采用其它方式进行帐号跨设备登录管理身份验证，在此不作限制。

[0083] 其中，控制服务器将人脸图像发送至第三方认证平台时，可以采用以下步骤：

[0084] 步骤a：账号登录管理应用程序响应于身份信息输入操作，拍摄用户视频，并将用户视频发送至控制服务器。

[0085] 步骤b：控制服务器对用户视频进行解析，获得多个视频帧。

[0086] 步骤c:控制服务器分别对提取每一视频帧的人体关键点,并分别根据每一视频帧的人体关键点,获得每一视频帧的人脸检测框。

[0087] 若视频帧中可以提取人脸检测框,则说明该视频帧中包含人脸,否则,不包含人脸。

[0088] 步骤d:控制服务器筛选出包含人脸检测框的视频帧,并基于筛选出的多个视频帧,进行活体检测。

[0089] 其中,活体检测用于判断用户是否为真实的人类,可以采用眨眼睛,张嘴等方式。

[0090] 步骤e:控制服务器确定活体检测通过时,将筛选出的任意一张视频帧发送至第三方认证平台。

[0091] 进一步地,控制服务器对身份信息进行验证之前,还可以对账号登录管理应用程序进行鉴权,具体步骤如下:

[0092] 账号登录管理应用程序向控制服务器发送权限标识信息。控制服务器将接收的权限标识信息和存储的各权限标识信息进行匹配,若匹配成功,则控制服务器判定鉴权成功,否则,判定鉴权失败,进而拒绝账号登录管理应用程序的后续请求。

[0093] 本申请实施例中,控制服务器对账号登录管理应用程序进行鉴权,以提高数据处理的安全性。

[0094] 步骤102:账号登录管理应用程序确定帐号跨设备登录管理身份验证通过时,显示设置页面。

[0095] 具体的,账号登录管理应用程序根据帐号跨设备登录管理身份验证结果,确定帐号跨设备登录管理身份验证通过时,显示设置页面。

[0096] 其中,设置页面用于绑定用户的目标应用账号。

[0097] 进一步地,在显示设置页面之前,还可以先显示帐号跨设备登录管理身份验证通过页面,且指定时长后,跳转至设置页面。

[0098] 步骤103:账号登录管理应用程序响应于用户在设置页面所触发的目标应用关联操作,从各个目标应用对应的应用服务器中,获取身份信息关联的各个目标应用账号信息以及各个目标应用账号信息分别关联的设备标识信息。

[0099] 具体的,执行步骤103时,可以采用以下步骤:

[0100] S1031:账号登录管理应用程序响应于用户在设置页面所触发的目标应用关联操作,在设置页面中显示各应用图标。

[0101] S1032:账号登录管理应用程序响应于用户通过设置页面所触发的应用授权操作,弹出授权确认页面。

[0102] 具体的,用户点击设置页面中的一个应用的图标,控制设备根据用户选择的图标,弹出授权确认页面。

[0103] 其中,授权确认页面用于根据用户的指示,判断是否获取目标应用账号的授权标识信息。

[0104] S1033:账号登录管理应用程序响应于用户在授权确认页面所触发的允许授权操作,向各个应用服务器发送应用关联请求,并接收各应用服务器基于接收的应用关联请求返回的所述身份信息关联的各个目标应用账号信息以及各个目标应用账号信息分别关联的设备标识信息。

[0105] 具体的，用户点击授权确认页面中的确认授权按键。账号登录管理应用程序响应于允许授权操作，向控制服务器发送包含身份信息的应用关联请求。控制服务器调用目标应用对应的应用接口，向应用服务器，转发应用关联请求。应用服务器获取应用关联请求中包含的身份信息，获取身份信息对应设置的目标应用账号信息，该目标应用账号信息关联的设备标识信息以及授权标识信息。应用服务器将获取的目标应用账号信息，其关联的设备标识信息以及授权标识信息，通过应用接口以及控制服务器，返回至账号登录管理应用程序。账号登录管理应用程序建立身份信息、目标应用账号信息、设备标识信息以及授权标识信息四者之间的关联关系。

[0106] 由于随着应用实名制的实施，用户在应用中进行实名制后，应用对应的应用服务器中会建立各身份信息和各目标应用账号信息之间的关联关系。这样，应用服务器就可以通过该关联关系，获取用户的目标应用账号信息。

[0107] 进一步地，设备标识信息还可以包含历史运行过目标应用账号的设备的标识信息，以及用户输入的设备标识信息。

[0108] 其中，账号登录管理应用程序获取用户输入的设备标识信息时，可以采用以下步骤：

[0109] 步骤a：账号登录管理应用程序响应于用户在设置页面所触发的设备关联操作，显示设备信息输入页面。

[0110] 一种实施方式中，用户点击设置页面中的设备关联按键，账号登录管理应用程序响应于设备关联操作，显示设备信息输入页面。

[0111] 步骤b：账号登录管理应用程序响应于用户在设备信息输入页面所触发的设备信息输入操作，获取用户输入的设备标识信息。

[0112] 步骤c：账号登录管理应用程序将用户输入的设备标识信息，确定为身份信息关联的设备标识信息。

[0113] 具体的，账号登录管理应用程序建立用户的身份信息和用户输入的设备标识信息之间的关联关系。

[0114] 账号登录管理应用程序仅能通过应用服务器获取当前运行或者历史运行过目标应用账号的设备标识信息。因此，还可以通过设备自定义的方式，使得用户可以在账号登录管理应用程序中添加未运行过目标应用账号的设备标识信息，从而可以在后续的账号跨设备登录管理的步骤中，禁止目标应用账号在用户自定义的设备上登录。

[0115] 步骤104：账号登录管理应用程序在设置页面上显示各设备标识信息，以及每一设备标识信息关联的目标应用账号信息。

[0116] 具体的，账号登录管理应用程序按照设备标识信息，将各目标应用账号信息进行划分后显示，即依次显示每一设备标识信息以及该设备标识信息关联的目标应用账号信息。

[0117] 这样，用户就可以分别看到每一设备标识信息对应的设备上运行的目标应用账号，以便后续针对设备进行禁止登录处理。

[0118] 进一步地，账号登录管理应用程序也可以在设置页面上仅显示身份信息关联的目标应用账号信息。

[0119] 可选的，目标应用账号信息可以包括目标应用账号的图标、昵称以及应用类型等。

[0120] 例如，参阅图1b所示，为一种设置页面的示例图。图1b中更新了绑定的目标应用账号信息，新添加了社交b。

[0121] 这样，就可以绑定用户的多个目标应用账号，从而在后续的步骤中，根据用户的指示，对目标应用账号进行批量禁止登录处理。

[0122] 参阅图2所示，为本申请提供的一种账号跨设备登录管理的方法的实施流程图。该方法的具体流程如下：

[0123] 步骤200：账号登录管理应用程序响应于帐号跨设备登录管理启动操作，显示身份信息输入页面。

[0124] 步骤201：账号登录管理应用程序响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户输入的身份信息。

[0125] 步骤202：账号登录管理应用程序对身份信息进行帐号跨设备登录管理身份验证，当确定帐号跨设备登录管理身份验证通过时，显示账号跨设备登录管理页面。

[0126] 其中，账号跨设备登录管理页面中包含身份信息关联的至少一个设备标识信息，以及每个设备标识信息对应的设备关联的各个目标应用账号信息。

[0127] 步骤203：账号登录管理应用程序响应于用户在账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录，并在账号跨设备登录管理页面中将至少一个目标应用账号的登录状态显示为禁止登录状态。

[0128] 参阅图3所示，为本申请提供的一种账号跨设备登录管理的方法的详细实施流程图。该方法的具体流程如下：

[0129] 步骤300：账号登录管理应用程序响应于用户在应用保护页面所触发的帐号跨设备登录管理启动操作，显示身份信息输入页面。

[0130] 一种实施方式中，账号登录管理应用程序显示应用保护页面，用户点击应用保护页面中的控制登录状态启动按键，控制设备响应于用户触发的帐号跨设备登录管理启动操作，跳转至身份信息输入页面。

[0131] 步骤301：账号登录管理应用程序响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户输入的身份信息，并对身份信息进行帐号跨设备登录管理身份验证。

[0132] 具体的，身份信息可以包括以下任意一种或任意组合：人脸图像、声纹、指纹、虹膜以及应用账号信息等。本申请实施例中，仅以通过人脸识别的方式进行帐号跨设备登录管理身份验证为例进行说明，实际应用中，也可以采用其它方式进行身份验证，在此不作限制。

[0133] 其中，通过人脸图像进行帐号跨设备登录管理身份验证时，可以采用以下步骤：

[0134] S3011：账号登录管理应用程序响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户的多个视频帧，并分别对每一视频帧进行人脸检测。

[0135] S3012：账号登录管理应用程序对人脸检测通过的连续的视频帧进行活体检测。

[0136] 可选的，活体检测可以采用眨眼睛、张嘴、摇头，以及背景光等方式进行检测。

[0137] S3013：账号登录管理应用程序对筛选出的任意一个视频帧进行人脸识别。

[0138] 这是由于人脸识别时仅需要一个视频帧即可。

[0139] S3014：当人脸识别通过时，控制设备将身份信息发送至控制服务器。

[0140] S3015:控制服务器分别调用每一目标应用账号对应的应用接口,将身份信息发送至相应的应用服务器。

[0141] S3016:应用服务器对接收的身份信息进行验证,并通过控制服务器和对应的应用接口,向账号登录管理应用程序返回身份验证结果。

[0142] 进一步地,账号登录管理应用程序还可以将目标应用账号的授权标识信息通过控制服务器发送至相应的应用服务器。应用服务器将接收的授权标识信息与存储的授权标识信息进行匹配,确定授权标识信息匹配且身份验证通过时,向账号登录管理应用程序返回表示身份验证通过的身份验证结果,否则,向账号登录管理应用程序返回表示身份验证失败的身份验证结果。

[0143] 进一步地,为保证账号登录管理应用程序的安全性,控制服务器在进行帐号跨设备登录管理身份验证之前,还可以对账号登录管理应用程序进行鉴权,鉴权成功时,执行后续的帐号跨设备登录管理身份验证操作,鉴权的具体步骤,参见上述步骤101。

[0144] 步骤302:当确定帐号跨设备登录管理身份验证通过时,账号登录管理应用程序页面显示帐号跨设备登录管理身份验证通过页面。

[0145] 具体的,账号登录管理应用程序接收应用服务器通过控制服务器返回的帐号跨设备登录管理身份验证结果,若帐号跨设备登录管理身份验证结果表示帐号跨设备登录管理身份验证通过,则显示帐号跨设备登录管理身份验证通过页面,否则显示帐号跨设备登录管理身份验证不通过页面。

[0146] 其中,帐号跨设备登录管理身份验证通过页面和帐号跨设备登录管理身份验证不通过页面用于向用户展示帐号跨设备登录管理身份验证结果。

[0147] 这样,就实现了对用户的身份验证,确定用户的身份。

[0148] 步骤303:账号登录管理应用程序分别向每一目标应用账号对应的应用服务器发送包含身份信息的登录状态请求,并接收各应用服务器基于登录状态请求返回的当前运行相应的目标应用账号的设备对应的设备标识信息。

[0149] 具体的,账号登录管理应用程序分别针对每一目标应用账号,执行以下步骤:

[0150] S3031:账号登录管理应用程序将包含身份信息和目标应用账号的登录状态请求,发送至控制服务器。

[0151] S3032:控制服务器根据接收的登录状态请求,通过该目标应用账号对应的应用接口,将包含身份信息和目标应用账号的登录状态请求发送至相应的应用服务器。

[0152] S3033:应用服务器基于该身份信息,获取当前运行目标应用账号的设备对应的设备标识信息。

[0153] S3034:账号登录管理应用程序接收应用服务器通过控制服务器返回的设备标识信息,以及该设备标识信息对应的设备上运行的目标应用账号。

[0154] 进一步地,账号登录管理应用程序还可以从应用服务器中获取历史运行过目标应用账号的设备对应的设备标识信息。

[0155] 进一步地,账号登录管理应用程序还可以基于身份信息,从各目标应用账号对应的应用服务器中,获取每一设备标识信息对应的设备关联的目标应用账号的登录状态。

[0156] 具体的,账号登录管理应用程序分别针对每一目标应用账号,执行以下步骤:

[0157] 账号登录管理应用程序通过目标应用账号对应的应用服务器,获取目标应用账号

在关联的设备标识信息对应的设备上的登录状态。

[0158] 其中，登录状态包括：当前登录状态、历史登录状态、未曾登录状态、禁止登录状态、强制退出状态。

[0159] 目标应用账号关联的设备包括当前运行目标应用账号的设备，还可以包括历史运行过目标应用账号的设备，还可以包括用户输入的设备。

[0160] 这样，就可以获取当前运行目标应用账号的设备对应的设备信息。

[0161] 步骤304：账号登录管理应用程序根据获取的各设备标识信息，以及每一设备标识信息对应的设备上运行的目标应用账号信息，对身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的目标应用账号信息进行更新。

[0162] 具体的，执行步骤304时，可以采用以下两种方式：

[0163] 第一种方式为：账号登录管理应用程序将身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的目标应用账号信息，修改为上述获取的各设备标识信息，以及每一设备标识信息对应的设备上运行的目标应用账号信息。

[0164] 也就是说，用新获取的设备标识信息和目标应用账号信息替换旧的设备标识信息和目标应用账号信息。

[0165] 第二种方式为：账号登录管理应用程序将历史存储的设备标识信息以及每一设备标识信息对应的设备关联的目标应用账号信息，与新获取的各设备标识信息以及每一设备标识信息对应的设备上运行的目标应用账号信息合并，并将合并后的信息，更新为身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的目标应用账号信息。

[0166] 也就是说，将新的设备标识信息和目标应用账号信息，与旧的设备标识信息和目标应用账号信息合并。

[0167] 步骤305：账号登录管理应用程序在账号跨设备登录管理页面中，显示更新后的身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的各目标应用账号信息。

[0168] 其中，账号跨设备登录管理页面中包含身份信息关联的至少一个设备标识信息，以及每个设备标识信息对应的设备关联的各个目标应用账号信息。

[0169] 进一步地，账号登录管理应用程序还可以在账号跨设备登录管理页面中，显示每一设备标识信息关联的各目标应用账号的登录状态。

[0170] 其中，登录状态的显示形式可以采用以下方式中的任意一种或任意组合：文字、图标以及颜色等。

[0171] 考虑到若用户的设备丢失，则用户通常会针对丢失的设备关联的目标应用账号的登录状态进行相应的处理，因此，可以按照设备划分，依次显示每一设备关联的各目标应用账号信息和登录状态，以便用户查看和操作。

[0172] 例如，参阅图4a所示，为一种账号跨设备登录管理页面的示例图。账号跨设备登录管理页面中按照设备划分，分别显示每一设备对应的设备标识信息，即设备101和设备102，以及关联的目标应用账号信息，即游戏王者和农农，以及通过图标颜色表征登录状态。

[0173] 实际应用中，也可以按照目标应用账号进行划分，依次显示每一目标应用账号信息，以及关联的各设备标识信息和对应的登录状态。

[0174] 这样，就可以方便用户对某个目标应用账号在不同设备上的登录状态进行控制。

[0175] 实际应用中，还可以按照登录状态划分，依次显示每一登录状态下的目标应用账号信息和关联的设备标识信息。

[0176] 其中，登录状态的顺序可以根据实际应用场景中进行设置，在此不作限制。

[0177] 例如，账号登录管理应用程序先显示处于当前登录状态的各目标应用账号信息和其关联的设备标识信息，然后，显示处于历史登录状态的各目标应用账号信息和其关联的设备标识信息。

[0178] 这样，用户就可以按照登录状态，对各目标应用账号进行后续处理。

[0179] 本申请实施例中，设备标识信息以及每一设备标识信息对应的设备关联的各目标应用账号信息的显示顺序，可以按照设备标识信息、目标应用账号信息以及登录状态中的任意一个或任意组合顺序，进行划分和排序，在此不再赘述。

[0180] 步骤306：账号登录管理应用程序响应于用户在账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录。

[0181] 具体的，禁止登录操作可以实现以下几种功能：一键挂失、设备挂失以及自定义挂失。

[0182] 其中，一键挂失为：控制各目标应用账号退出以及禁止登录关联的各设备标识信息对应的设备。

[0183] 设备挂失为：控制指定的设备标识信息关联的各目标应用账号退出以及禁止登录指定的设备标识信息对应的设备。

[0184] 自定义挂失为：控制指定的目标应用账号退出以及禁止登录指定的设备标识信息对应的设备。

[0185] 可选的，执行步骤306时，可以采用以下几种方式：

[0186] 第一种方式为：账号登录管理应用程序采用一键挂失的方式，控制各目标应用账号禁止登录关联的所有设备。

[0187] 一种实施方式中，用户点击账号跨设备登录管理页面中的一键挂失按键。账号登录管理应用程序响应于禁止登录操作，弹出挂失确认页面，响应于用户在挂失确认页面所触发的确认触发操作，向各目标应用账号对应的应用服务器发送包含目标应用账号和设备标识信息的禁止登录请求。各应用服务器根据接收的禁止登录请求，控制各目标应用账号退出以及禁止登录关联的各设备标识信息对应的设备。

[0188] 例如，图4a中，账号跨设备登录管理页面中的设置有一键挂失按键。

[0189] 一种实施方式中，账号登录管理应用程序分别针对每一目标应用账号，执行以下步骤：

[0190] 步骤a1：账号登录管理应用程序向目标应用账号对应的应用服务器发送禁止登录请求。

[0191] 步骤a2：应用服务器基于禁止登录请求，获取目标应用账号信息以及关联的设备标识信息，并执行禁止登录设置操作，使得目标应用账号禁止登录关联的设备。

[0192] 步骤a3：当目标应用账号处于当前登录状态时，应用服务器向目标应用账号当前登录的设备中的目标应用程序(Application，APP)发送强制退出指示，使得目标应用账号退出当前登录的设备。

[0193] 当禁止目标应用账号登录在设备上登录时，若目标应用账号处于当前登录状态，

则仅能禁止目标应用账号在该设备上登录，并不能使得目标应用账号退出登录。这是由于目标应用账号拥有登录态(status!=0)，下次登录前仍然可以进行部分操作，因此，应用服务器向目标APP发送强制退出指示，以强制登录态过期。

[0194] 第二种方式为：账号登录管理应用程序响应于禁止登录操作，通过各指定的目标应用账号对应的应用服务器，控制指定的目标应用账号退出以及禁止登录指定的设备标识信息对应的设备。

[0195] 具体的，用户在账号跨设备登录管理页面中选中指定的目标应用账号和指定的设备，并点击批量挂失按键，账号登录管理应用程序响应于禁止登录操作，弹出挂失确认页面，响应于用户在挂失确认页面所触发的确认退出操作，向各指定的目标应用账号对应的应用服务器发送禁止登录请求。各应用服务器根据禁止登录请求，控制指定的目标应用账号退出以及禁止登录指定的设备标识信息对应的设备。

[0196] 可选的，指定的目标应用账号和指定的设备均可以为一个，也可以为多个。

[0197] 例如，图4a中，账号跨设备登录管理页面中的设置有批量挂失按键。

[0198] 这样，就可以根据用户的选择，对目标应用账号进行批量挂失。

[0199] 第三种方式为：账号登录管理应用程序采用设备挂失的方式，控制指定的设备关联的各目标应用账号禁止登录该设备。

[0200] 具体的，用户点击账号跨设备登录管理页面中的一键设备挂失按键，账号登录管理应用程序响应于禁止登录操作，向各目标应用账号对应的应用服务器发送禁止登录请求。各应用服务器根据禁止登录请求，控制指定的设备标识信息关联的各目标应用账号退出以及禁止登录指定的设备标识信息对应的设备。

[0201] 例如，图4a中，账号跨设备登录管理页面中的设置有一键设备挂失按键。这样，就可以采用设备挂失的方式，迅速禁止和退出指定设备上的所有目标应用账号。

[0202] 进一步地，账号登录管理应用程序还可以删除身份信息关联的设备标识信息以及目标应用账号。

[0203] 具体的，账号登录管理应用程序响应于关联信息删除操作，通过控制服务器，删除指定的设备关联的指定的目标应用账号。

[0204] 具体的，删除操作时，也可以采用以下几种方式：

[0205] 第一种方式为：账号登录管理应用程序响应于一键删除操作，删除各目标应用账号以及关联的设备标识信息。

[0206] 第二种方式为：账号登录管理应用程序响应于设备删除操作，删除指定的设备标识信息。

[0207] 第三种方式为：账号登录管理应用程序响应于自定义删除操作，删除指定的设备标识信息和指定的目标应用账号之间的关联关系。

[0208] 可选的，指定的设备和指定的目标应用账号均可以为一个，也可以为多个。

[0209] 例如，图4a中，账号跨设备登录管理页面中的设置有批量删除按键。

[0210] 进一步地，账号登录管理应用程序还可以控制目标应用账号从设备退出登录。

[0211] 具体的，退出登录时，也可以采用以下几种方式：

[0212] 第一种方式为：账号登录管理应用程序响应于一键退出登录操作，通过各目标应用账号对应的应用服务器，控制各目标应用账号从关联的各设备标识信息对应的设备退出

登录。

[0213] 具体的，用户点击账号跨设备登录管理页面中的一键退出按键，账号登录管理应用程序响应于一键退出登录操作，弹出退出确认页面，响应于用户在退出确认页面所触发的确认退出操作，通过各目标应用账号对应的应用服务器，控制各目标应用账号退出关联的各设备标识信息对应的设备。

[0214] 第二种方式为：账号登录管理应用程序响应于自定义退出登录操作，向各指定的目标应用账号对应的应用服务器发送退出登录请求。各应用服务器根据接收的退出登录请求，控制指定的目标应用账号从指定的设备标识信息对应的设备退出登录。

[0215] 具体的，用户在账号跨设备登录管理页面中选中指定的目标应用账号和指定的设备，并点击批量退出按键，账号登录管理应用程序响应于自定义退出登录操作，弹出退出确认页面，响应于用户在退出确认页面中触发的退出确认操作，向各指定的目标应用账号对应的应用服务器发送退出登录请求。各应用服务器根据接收的退出登录请求，控制指定的目标应用账号从指定的设备标识信息对应的设备上退出登录。

[0216] 第三种方式为：控制设备响应于设备退出登录操作，向各目标应用账号对应的应用服务器发送退出登录请求。各应用服务器控制指定的设备标识信息关联的各目标应用账号从指定的设备标识信息对应的设备退出登录。

[0217] 具体的，用户在账号跨设备登录管理页面中选中指定的设备，并点击批量退出按键。账号登录管理应用程序响应于设备退出登录操作，弹出退出确认页面，响应于用户在退出确认页面所触发的退出确认操作，向各指定的目标应用账号对应的应用服务器发送退出登录请求。各应用服务器根据退出登录请求，控制指定的设备标识信息关联的各目标应用账号退出登录指定的设备标识信息对应的设备。

[0218] 步骤307：账号登录管理应用程序在账号跨设备登录管理页面中将至少一个目标应用账号的登录状态显示为禁止登录状态。

[0219] 具体的，各目标应用账号对应的应用服务器将各目标应用账号在关联的设备上的登录状态发送至控制服务器，控制服务器将接收的各目标应用账号在关联的设备上的登录状态转发至账号登录管理应用程序。账号登录管理应用程序根据接收的各目标应用账号在关联的设备上的登录状态，更新账号跨设备登录管理页面。

[0220] 这样，若目标应用账号在关联的设备上的登录状态为禁止登录状态，则将相应的登录状态显示为禁止登录状态。若目标应用账号在关联的设备上的登录状态为强制退出登录状态，则将相应的登录状态显示为强制退出登录状态。

[0221] 进一步地，账号登录管理应用程序还可以控制目标应用账号在设备上恢复登录，具体的，可以采用以下几种方式：

[0222] 第一种方式为：账号登录管理应用程序响应于一键恢复登录操作，向各目标应用账号对应的应用服务器发送恢复登录请求。各应用服务器根据接收的恢复登录请求，执行撤销各目标应用账号禁止登录关联的各设备标识信息对应的设备的设置操作，更新账号跨设备登录管理页面。

[0223] 这样，就可以采用一键解除登录限制的方式，解除所有的目标应用账号的登录限制。

[0224] 第二种方式为：账号登录管理应用程序响应于设备恢复登录操作，向各目标应用

账号对应的应用服务器发送恢复登录请求。各应用服务器根据接收的恢复登录请求，执行撤销各目标应用账号禁止登录指定的设备标识信息对应的设备的设置操作，更新账号跨设备登录管理页面。

[0225] 这样，就可以采用一键解除设备登录限制的方式，控制某个设备关联的所有目标应用账号解除在该设备上的登录限制。

[0226] 第三种方式为：账号登录管理应用程序响应于自定义恢复登录操作，向各指定的目标应用账号对应的应用服务器发送恢复登录请求。各应用服务器根据接收的恢复登录请求，执行撤销指定的目标应用账号禁止登录指定的设备标识信息对应的设备的设置操作，更新账号跨设备登录管理页面。

[0227] 这样，就可以通过一键解除批量账号登录限制的方式，自定义解除批量目标应用账号在批量的设备上的登录限制。

[0228] 参阅图4b所示，为一种数据结构的示例图。一种实施方式中，账号登录管理应用程序通过图4b所示的数据结构，对设备信息以及目标应用账号信息进行存储以及应用。数据结构包括设备管理列表模块、设备信息模块以及目标应用账号信息模块。

[0229] 设备管理列表模块包括：增加新设备、禁止指定的设备上的所有目标应用账号登录、禁止指定的设备上的指定目标应用账号登录。设备信息模块包括：设备标识信息、是否被禁止登录、设备状态、设备图标以及设备关联应用账号列表。目标应用账号信息模块包括：目标应用账号、目标应用账号是否被禁止、目标应用账号状态、目标应用账号昵称以及目标应用账号头像。

[0230] 下面采用一个具体的实施例，对基于人脸识别的帐号跨设备登录管理身份验证的方法进行进一步具体说明。

[0231] 参阅图5所示，为一种帐号跨设备登录管理身份验证的方法的实施流程图，该方法的具体流程如下：

[0232] 步骤500：账号登录管理应用程序获取拍摄的视频。

[0233] 步骤501：账号登录管理应用程序从视频中提取多个视频帧。

[0234] 具体的，账号登录管理应用程序对视频进行解析，获得多个视频帧。

[0235] 步骤502：账号登录管理应用程序分别对每一视频帧进行人脸检测，获得人脸检测结果，并基于人脸检测结果，筛选出符合预设筛选条件的连续的视频帧。

[0236] 具体的，账号登录管理应用程序采用人脸检测模型，分别对每一视频帧进行人脸检测，获得人脸检测结果，并分别获取每一人脸检测结果表示人脸检测通过的视频帧的人脸关键点信息和人脸位置信息，以及筛选出符合预设筛选条件的连续的视频帧。当不存在符合预设筛选条件的视频帧时，账号登录管理应用程序判定身份验证不通过。

[0237] 其中，预设筛选条件为：人脸检测结果均为人脸检测通过的连续的视频帧的总数量大于指定数量。

[0238] 人脸关键点信息可以为：眼睛、鼻子以及额头等关键点的坐标。人脸位置信息可以为人脸框的尺寸和坐标。

[0239] 实际应用中，人脸关键点可以根据实际应用场景进行设置，如，人脸关键点可以为：眼睛、鼻子以及额头等，在此不作限制。

[0240] 一种实施方式中，人脸检测模型是基于目标检测算法(retinanet)和网络结构

(mobilenet v1)搭建的,并采用开源深度学习框架(ncnn)进行模型推理。

[0241] 其中,mobilenet v1具有体积小,移动设备推理速度快等优点。整个ncnn框架和模型大小在2M以内,推理速度在120ms左右,可方便部署和运行于大多数安卓(android)和苹果操作系统(iPhone Operation System,ios)设备。

[0242] 步骤503:账号登录管理应用程序根据筛选出的视频帧进行活体检测。

[0243] 具体的,账号登录管理应用程序采用活体检测模型对筛选出的视频帧进行活体检测。

[0244] 其中,活体检测可以采用眨眼睛、张嘴、摇头,以及背景光等方式检测是否为同一真实的用户。

[0245] 步骤504:账号登录管理应用程序对筛选出的任意一个视频帧进行人脸识别,获得人脸识别结果。

[0246] 具体的,账号登录管理应用程序通过第三方认证平台、控制服务器或者应用服务器,采用人脸识别模型对视频帧进行人脸识别,获得人脸识别结果。

[0247] 一种实施方式中,根据视频帧对应的人脸关键点信息和人脸位置信息,对人脸位置信息进行仿射变换矫正,并将人脸关键点信息和矫正后的人脸位置信息输入人脸识别模型中,获得表示用户的人脸特征向量,并将人脸特征向量与数据库中的各人脸特征样本向量进行匹配,以及根据匹配结果,确定人脸识别结果。

[0248] 其中,人脸识别模型可以采用卷积神经网络ArcFace变体网络训练而成。

[0249] 可选的,人脸特征向量的维度可以为512。通过两个人脸特征向量,可以判定两个人脸图像中的人脸是否为同一个人。

[0250] 其中,活体检测模型和人脸识别模型均可以部署于图形处理器(Graphics Processing Unit,GPU)的模型处理框架中。

[0251] 参阅图6所示,为一种模型处理框架的示例图。模型处理框架包括模型管理模块、预处理模块、推理引擎模块以及后处理模块。

[0252] 模型管理模块包括:用于存储模型的模型存储模块(rgw)和用于存储模型参数的配置模块(confighub)。

[0253] 预处理模块:包括读取模块、格式转换模块和尺寸缩放模块,用于对图像进行读取、格式转换、尺寸缩放等。格式转换模块用于隐藏实际推理引擎的数据格式,方便推理引擎切换和扩展。

[0254] 推理引擎模块:兼容多种模型推理引擎。

[0255] 后处理模型:用于根据模型的输出向量确定最终输出结果。

[0256] 参阅图7所示,为一种账号跨设备登录管理的方法的交互流程图。

[0257] 步骤700:控制设备响应于帐号跨设备登录管理启动操作,显示身份信息输入页面。

[0258] 需要说明的是,控制设备中安装有账号登录管理应用程序,账号跨设备登录管理的方法的执行主体为控制设备中的账号登录管理应用程序。

[0259] 步骤701:控制设备响应于身份信息输入操作,将身份信息发送至控制服务器。

[0260] 步骤702:控制服务器对身份信息进行帐号跨设备登录管理身份验证。

[0261] 步骤703:控制设备接收控制服务器返回的帐号跨设备登录管理身份验证结果。

[0262] 步骤704:当帐号跨设备登录管理身份验证通过时,控制设备向控制服务器发送登录状态请求。

[0263] 步骤705:控制服务器向应用服务器发送登录状态请求。

[0264] 具体的,控制服务器向身份信息关联的目标应用账号对应的应用服务器发送登录状态请求。

[0265] 步骤706:应用服务器获取设备标识信息和目标应用账号信息。

[0266] 具体的,控制设备基于身份信息,获取身份信息关联的至少一个设备标识信息以及每个设备标识信息对应的设备关联的各个目标应用账号信息。

[0267] 步骤707:控制服务器接收应用服务器返回的设备标识信息和目标应用账号信息。

[0268] 步骤708:控制设备接收控制服务器返回的设备标识信息和目标应用账号信息。

[0269] 步骤709:控制设备根据接收的设备标识信息和目标应用账号信息,显示账号跨设备登录管理页面。

[0270] 步骤710:控制设备响应于控制至少一个目标应用账号在对应设备上禁止登录的禁止登录操作,通过控制服务器向相应的应用服务器发送禁止登录请求。

[0271] 步骤711:应用服务器控制指定的设备标识信息对应的设备上禁止登录指定的目标应用账号。

[0272] 步骤712:应用服务器向账号登录管理应用程序返回禁止登录响应消息。

[0273] 步骤713:控制设备更新登录状态页面中的登录状态。

[0274] 具体的,控制设备在登录状态页面中将指定的设备对应的指定的目标应用账号的登录状态显示为禁止登录状态。

[0275] 本申请实施例中,通过账号登录管理应用程序对用户关联的各目标应用账号进行统一管理,可以实现批量的目标应用账号的禁止登录,且仅需要一次帐号跨设备登录管理身份验证,简化了身份认证以及批量目标应用账号禁止登录的繁琐操作,还避免了用户遗忘账号问题,再者,仅在指定的设备上禁止指定目标应用账号登录,用户仍然可以在非指定的设备上使用目标应用账号,给用户带来了便利,耗费的时间成本较少,可以避免非法分子对用户的目标应用账号的使用,保证了用户的信息和财产安全。

[0276] 基于同一发明构思,本申请实施例中还提供了一种账号跨设备登录管理的装置,由于上述装置及设备解决问题的原理与一种账号跨设备登录管理的方法相似,因此,上述装置的实施可以参见方法的实施,重复之处不再赘述。

[0277] 如图8所示,其为本申请实施例提供的一种账号跨设备登录管理的装置的结构示意图。一种账号跨设备登录管理的装置包括:

[0278] 启动单元811,用于响应于帐号跨设备登录管理启动操作,显示身份信息输入页面;

[0279] 输入单元812,用于响应于用户在身份信息输入页面所触发的身份信息输入操作,获取用户输入的身份信息;

[0280] 显示单元813,用于对身份信息进行帐号跨设备登录管理身份验证,当确定帐号跨设备登录管理身份验证通过时,显示账号跨设备登录管理页面,账号跨设备登录管理页面中包含身份信息关联的至少一个设备标识信息,以及每个设备标识信息对应的设备关联的各个目标应用账号信息;

[0281] 控制单元814，用于响应于用户在账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录，并在账号跨设备登录管理页面中将至少一个目标应用账号的登录状态显示为禁止登录状态。

[0282] 较佳的，启动单元811还用于：

[0283] 响应于账号跨设备登录管理开通操作，显示身份信息输入页面；

[0284] 响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户的身份信息；

[0285] 将身份信息发送至第三方认证平台，使得第三方认证平台对身份信息进行帐号跨设备登录管理身份验证；

[0286] 接收第三方认证平台返回的身份验证结果，当身份验证结果表征验证通过时，显示设置页面；

[0287] 响应于用户在设置页面所触发的目标应用关联操作，向各个应用服务器发送应用关联请求；

[0288] 接收各应用服务器基于接收的应用关联请求返回的身份信息关联的各个目标应用账号信息以及各个目标应用账号信息分别关联的设备标识信息；

[0289] 在设置页面上显示各个设备标识信息，以及每个设备标识信息关联的目标应用账号信息。

[0290] 较佳的，显示单元813用于：

[0291] 分别向每一目标应用账号对应的应用服务器发送包含身份信息的登录状态请求；

[0292] 接收各应用服务器基于登录状态请求返回的当前运行相应的目标应用账号的设备对应的设备标识信息；

[0293] 根据获取的各设备标识信息，以及每一设备标识信息对应的设备上运行的目标应用账号信息，对身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的目标应用账号信息进行更新；

[0294] 在账号跨设备登录管理页面中，显示更新后的身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的各目标应用账号信息。

[0295] 较佳的，显示单元813还用于：

[0296] 接收各应用服务器基于登录状态请求返回的每一设备标识信息对应的设备关联的目标应用账号的登录状态；

[0297] 在账号跨设备登录管理页面中，还显示每一设备标识信息关联的各目标应用账号的登录状态。

[0298] 较佳的，控制单元814用于：

[0299] 响应于禁止登录操作，向各目标应用账号对应的应用服务器发送禁止登录请求，使得各应用服务器基于禁止登录请求控制各目标应用账号退出以及禁止登录关联的各设备标识信息对应的设备；或者，

[0300] 响应于禁止登录操作，向各目标应用账号对应的应用服务器发送禁止登录请求，使得各应用服务器基于禁止登录请求控制指定的设备标识信息关联的各目标应用账号退出以及禁止登录指定的设备标识信息对应的设备；或者，

[0301] 响应于禁止登录操作，向各指定的目标应用账号对应的应用服务器发送禁止登录

请求，使得各应用服务器基于禁止登录请求控制指定的目标应用账号退出以及禁止登录指定的设备标识信息对应的设备。

[0302] 较佳的，控制单元814还用于：

[0303] 响应于一键退出登录操作，向各目标应用账号对应的应用服务器发送退出登录请求，使得各应用服务器基于退出登录请求控制各目标应用账号从关联的各设备标识信息对应的设备上退出登录；或者，

[0304] 响应于设备退出登录操作，向各目标应用账号对应的应用服务器发送退出登录请求，使得各应用服务器基于退出登录请求控制指定的设备标识信息关联的各目标应用账号从指定的设备标识信息对应的设备上退出登录；或者，

[0305] 响应于自定义退出登录操作，向各指定的目标应用账号对应的应用服务器发送退出登录请求，使得各应用服务器基于退出登录请求控制指定的目标应用账号从指定的设备标识信息对应的设备上退出登录。

[0306] 较佳的，控制单元814还用于：

[0307] 响应于一键恢复登录操作，向各目标应用账号对应的应用服务器发送恢复登录请求，使得各应用服务器基于恢复登录请求，执行撤销各目标应用账号禁止登录关联的各设备标识信息对应的设备的设置操作；或者，

[0308] 响应于设备恢复登录操作，向各目标应用账号对应的应用服务器发送恢复登录请求，使得各应用服务器基于恢复登录请求，执行撤销各目标应用账号禁止登录指定的设备标识信息对应的设备的设置操作；或者，

[0309] 响应于自定义恢复登录操作，向各指定的目标应用账号对应的应用服务器发送恢复登录请求，使得各应用服务器基于恢复登录请求，执行撤销指定的目标应用账号禁止登录指定的设备标识信息对应的设备的设置操作。

[0310] 较佳的，控制单元814还用于：

[0311] 响应于用户在账号跨设备登录管理页面所触发的一键删除操作，删除各目标应用账号以及关联的设备标识信息；或者，

[0312] 响应于用户在账号跨设备登录管理页面所触发的设备删除操作，删除指定的设备标识信息；或者，

[0313] 响应于用户在账号跨设备登录管理页面所触发的自定义删除操作，删除指定的设备标识信息和指定的目标应用账号之间的关联关系。

[0314] 较佳的，启动单元811还用于：

[0315] 响应于用户在账号跨设备登录管理页面或设置页面所触发的设备关联操作，显示设备信息输入页面；

[0316] 响应于用户在设备信息输入页面触发的设备信息输入操作，获取用户输入的设备标识信息；

[0317] 将用户输入的设备标识信息，确定为身份信息关联的设备标识信息。

[0318] 本申请实施例提供的一种账号跨设备登录管理的方法、装置、设备和介质中，响应于帐号跨设备登录管理启动操作，显示身份信息输入页面，响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户的身份信息，并根据用户的身份信息，获取并显示用户关联的设备标识信息以及每一设备标识信息关联的目标应用账号信息，以及根据用户

的禁止登录请求，控制指定的设备标识信息对应的设备上禁止登录指定的目标应用账号，并显示目标应用账号的登录状态。这样，实现了对多个目标应用账号的跨设备批量处理，简化了账号跨设备登录管理的繁琐操作，可以快速控制指定的设备上禁止登录指定的目标应用账户，不影响目标应用账户在非指定的设备上运行，提高了处理效率以及安全性。

[0319] 图9示出了一种控制设备9000的结构示意图。参阅图9所示，控制设备9000包括：处理器9010、存储器9020、电源9030、显示单元9040、输入单元9050。

[0320] 处理器9010是控制设备9000的控制中心，利用各种接口和线路连接各个部件，通过运行或执行存储在存储器9020内的软件程序和/或数据，执行控制设备9000的各种功能，从而对控制设备9000进行整体监控。

[0321] 本申请实施例中，处理器9010调用存储器9020中存储的计算机程序时执行如图3中所示的实施例提供的账号跨设备登录管理的方法。

[0322] 可选的，处理器9010可包括一个或多个处理单元；优选的，处理器9010可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器9010中。在一些实施例中，处理器、存储器、可以在单一芯片上实现，在一些实施例中，它们也可以在独立的芯片上分别实现。

[0323] 存储器9020可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、各种应用等；存储数据区可存储根据控制设备9000的使用所创建的数据等。此外，存储器9020可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件等。

[0324] 控制设备9000还包括给各个部件供电的电源9030(比如电池)，电源可以通过电源管理系统与处理器9010逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗等功能。

[0325] 显示单元9040可用于显示由用户输入的信息或提供给用户的信息以及控制设备9000的各种菜单等，本发明实施例中主要用于显示控制设备9000中各应用的显示界面以及显示界面中显示的文本、图片等对象。显示单元9040可以包括显示面板9041。显示面板9041可以采用液晶显示屏(Liquid Crystal Display，LCD)、有机发光二极管(Organic Light-Emitting Diode，OLED)等形式来配置。

[0326] 输入单元9050可用于接收用户输入的数字或字符等信息。输入单元9050可包括触控面板9051以及其他输入设备9052。其中，触控面板9051，也称为触摸屏，可收集用户在其上或附近的触摸操作(比如用户使用手指、触摸笔等任何适合的物体或附件在触控面板9051上或在触控面板9051附近的操作)。

[0327] 具体的，触控面板9051可以检测用户的触摸操作，并检测触摸操作带来的信号，将这些信号转换成触点坐标，发送给处理器9010，并接收处理器9010发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触控面板9051。其他输入设备9052可以包括但不限于物理键盘、功能键(比如音量控制按键、开关机按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0328] 当然，触控面板9051可覆盖显示面板9041，当触控面板9051检测到在其上或附近的触摸操作后，传送给处理器9010以确定触摸事件的类型，随后处理器9010根据触摸事件

的类型在显示面板9041上提供相应的视觉输出。虽然在图9中，触控面板9051与显示面板9041是作为两个独立的部件来实现控制设备9000的输入和输出功能，但是在某些实施例中，可以将触控面板9051与显示面板9041集成而实现控制设备9000的输入和输出功能。

[0329] 控制设备9000还可包括一个或多个传感器，例如压力传感器、重力加速度传感器、接近光传感器等。当然，根据具体应用中的需要，上述控制设备9000还可以包括摄像头等其它部件，由于这些部件不是本申请实施例中重点使用的部件，因此，在图9中没有示出，且不再详述。

[0330] 本领域技术人员可以理解，图9仅仅是控制设备的举例，并不构成对控制设备的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件。

[0331] 本申请实施例还提供了一种计算机可读存储介质，其上存储有计算机程序，该计算机程序被处理器执行时实现上述任意方法实施例中的账号跨设备登录管理的方法。

[0332] 本申请实施例还提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述任意方法实施例中的账号跨设备登录管理的方法。

[0333] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到各实施方式可借助软件加通用硬件平台的方式来实现，当然也可以通过硬件。基于这样的理解，上述技术方案本质上或者说对相关技术做出贡献的部分可以软件产品的形式体现出来，该计算机软件产品可以存储在计算机可读存储介质中，如ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台控制设备(可以是个人计算机，服务器，或者网络设备等)执行各个实施例或者实施例的某些部分的方法。

[0334] 最后应说明的是：以上实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围。

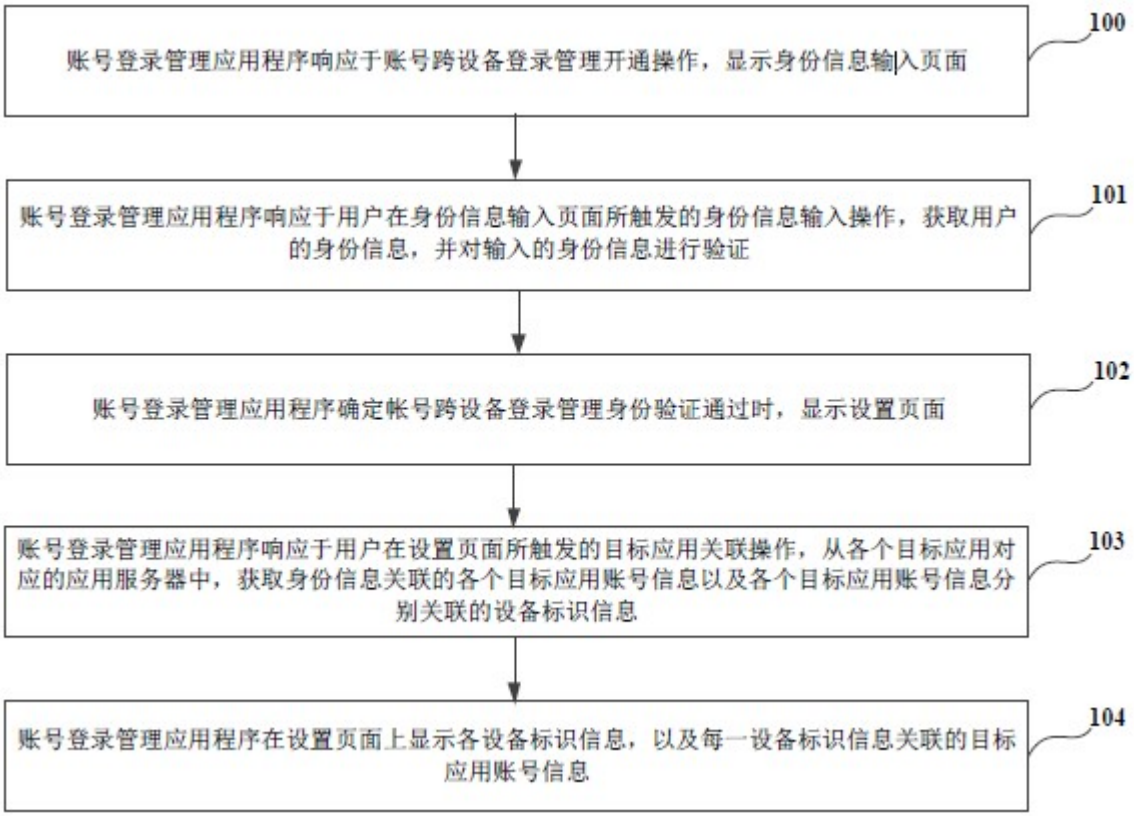

账号登录管理应用程序响应于账号跨设备登录管理开通操作，显示身份信息输入页面
100
账号登录管理应用程序响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户的身份信息，并对输入的身份信息进行验证
101
账号登录管理应用程序确定帐号跨设备登录管理身份验证通过时，显示设置页面
102
账号登录管理应用程序响应于用户在设置页面所触发的目标应用关联操作，从各个目标应用对应的应用服务器中，获取身份信息关联的各个目标应用账号信息以及各个目标应用账号信息分别关联的设备标识信息
103
账号登录管理应用程序在设置页面上显示各设备标识信息，以及每一设备标识信息关联的目标应用账号信息
104

图1a


绑定账户
可绑定账号
应用a
已绑定
社交b
已绑定

图1b

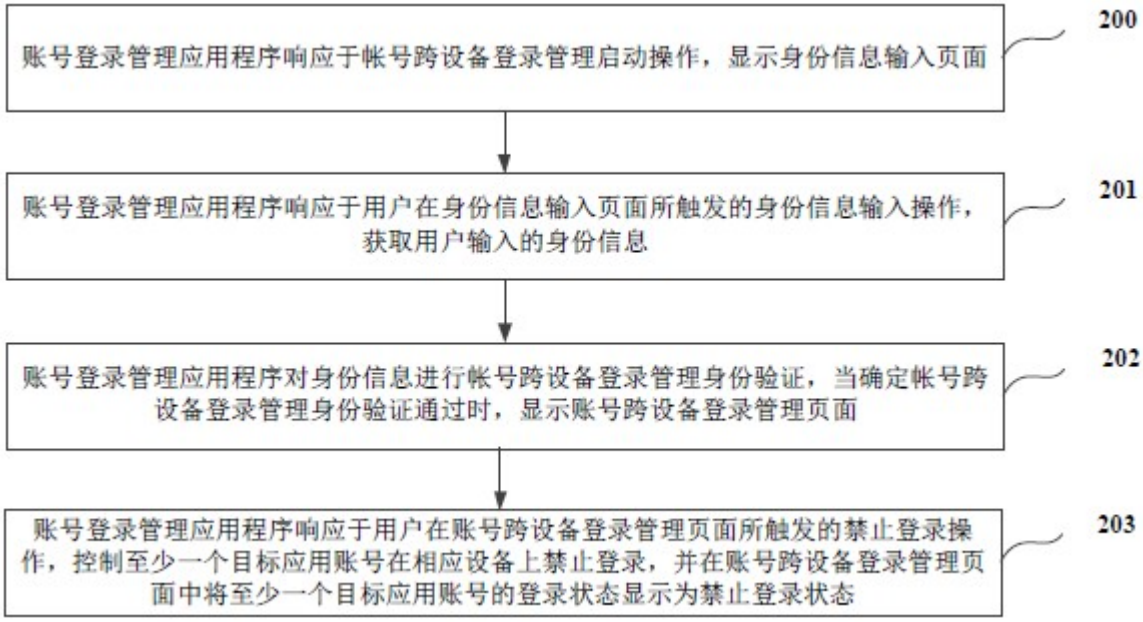

账号登录管理应用程序响应于帐号跨设备登录管理启动操作，显示身份信息输入页面
200
账号登录管理应用程序响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户输入的身份信息
201
账号登录管理应用程序对身份信息进行帐号跨设备登录管理身份验证，当确定帐号跨设备登录管理身份验证通过时，显示账号跨设备登录管理页面
202
账号登录管理应用程序响应于用户在账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录，并在账号跨设备登录管理页面中将至少一个目标应用账号的登录状态显示为禁止登录状态
203

图2

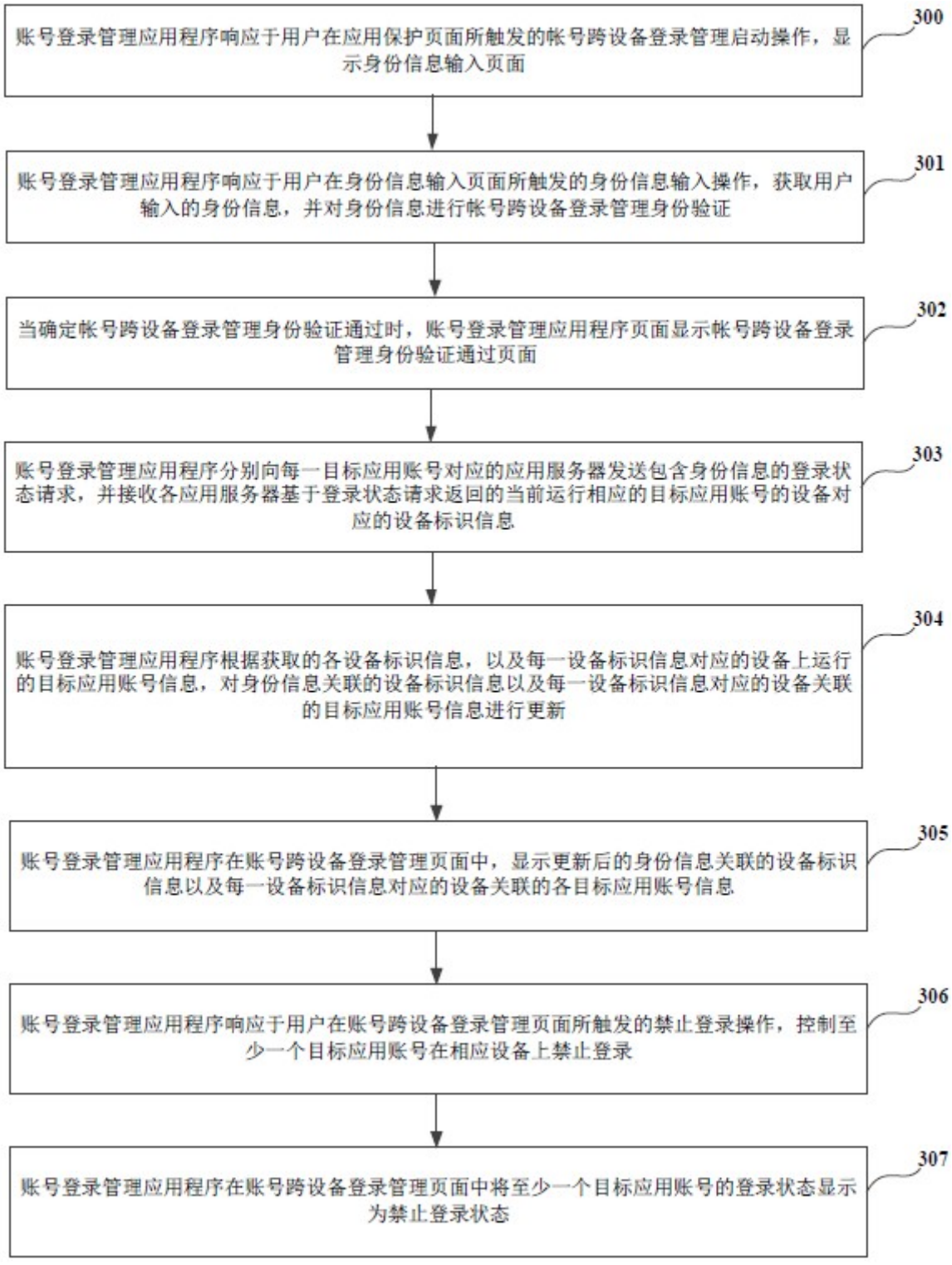

账号登录管理应用程序响应于用户在应用保护页面所触发的帐号跨设备登录管理启动操作，显示身份信息输入页面
300
账号登录管理应用程序响应于用户在身份信息输入页面所触发的身份信息输入操作，获取用户输入的身份信息，并对身份信息进行帐号跨设备登录管理身份验证
301
当确定帐号跨设备登录管理身份验证通过时，账号登录管理应用程序页面显示帐号跨设备登录管理身份验证通过页面
302
账号登录管理应用程序分别向每一目标应用账号对应的应用服务器发送包含身份信息的登录状态请求，并接收各应用服务器基于登录状态请求返回的当前运行相应的目标应用账号的设备对应的设备标识信息
303
账号登录管理应用程序根据获取的各设备标识信息，以及每一设备标识信息对应的设备上运行的目标应用账号信息，对身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的目标应用账号信息进行更新
304
账号登录管理应用程序在账号跨设备登录管理页面中，显示更新后的身份信息关联的设备标识信息以及每一设备标识信息对应的设备关联的各目标应用账号信息
305
账号登录管理应用程序响应于用户在账号跨设备登录管理页面所触发的禁止登录操作，控制至少一个目标应用账号在相应设备上禁止登录
306
账号登录管理应用程序在账号跨设备登录管理页面中将至少一个目标应用账号的登录状态显示为禁止登录状态
307

图3


登录状态控制
设备101
游戏王者
农农
一键设备挂失
设备102
游戏玩家
农农
一键设备挂失
一键挂失
批量删除
批量挂失
批量恢复

图4a


目标应用账号信息
目标应用账号
目标应用账号是否被禁止
目标应用账号状态
目标应用账号昵称
目标应用账号头像
设备信息
设备标识信息
是否被禁止登录
设备状态
设备图标
设备关联应用账号列表
设备管理列表
增加新设备
禁止指定的设备上的所有目标应用账号登录
禁止指定的设备上的指定目标应用账号登录

图4b

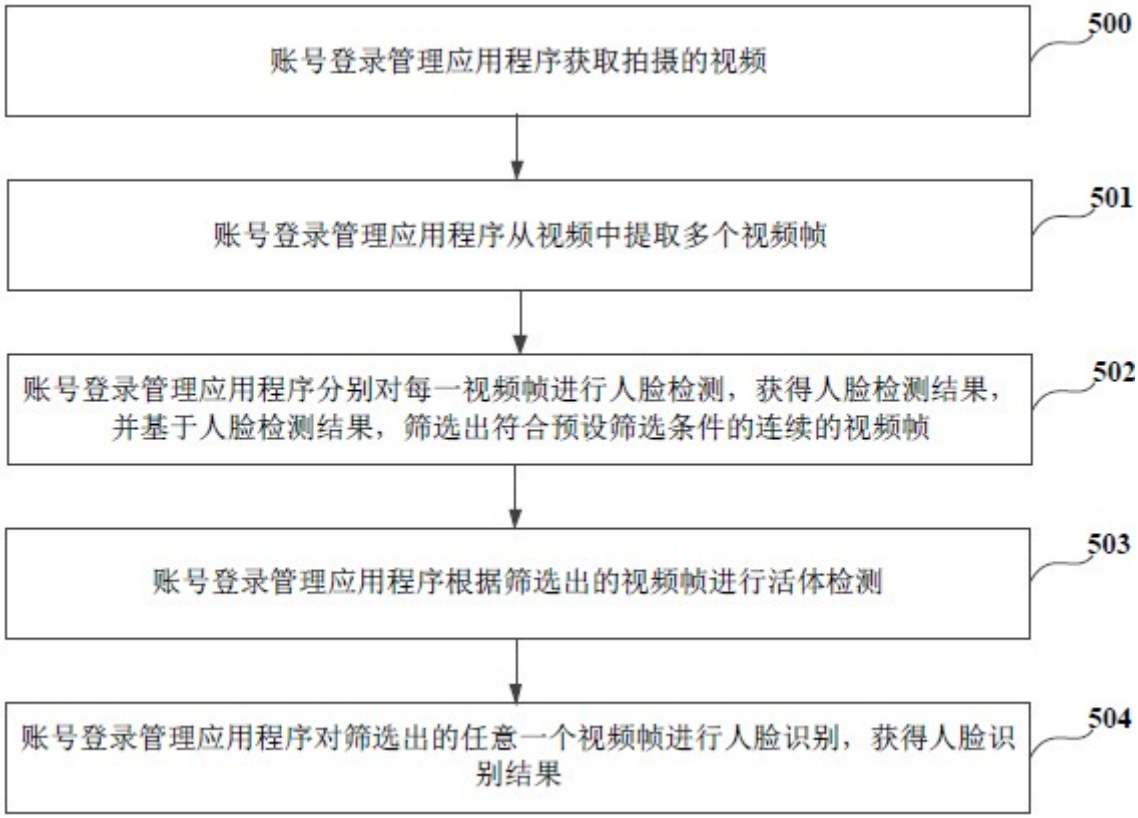

账号登录管理应用程序获取拍摄的视频
500
账号登录管理应用程序从视频中提取多个视频帧
501
账号登录管理应用程序分别对每一视频帧进行人脸检测，获得人脸检测结果，并基于人脸检测结果，筛选出符合预设筛选条件的连续的视频帧
502
账号登录管理应用程序根据筛选出的视频帧进行活体检测
503
账号登录管理应用程序对筛选出的任意一个视频帧进行人脸识别，获得人脸识别结果
504

图5

图6

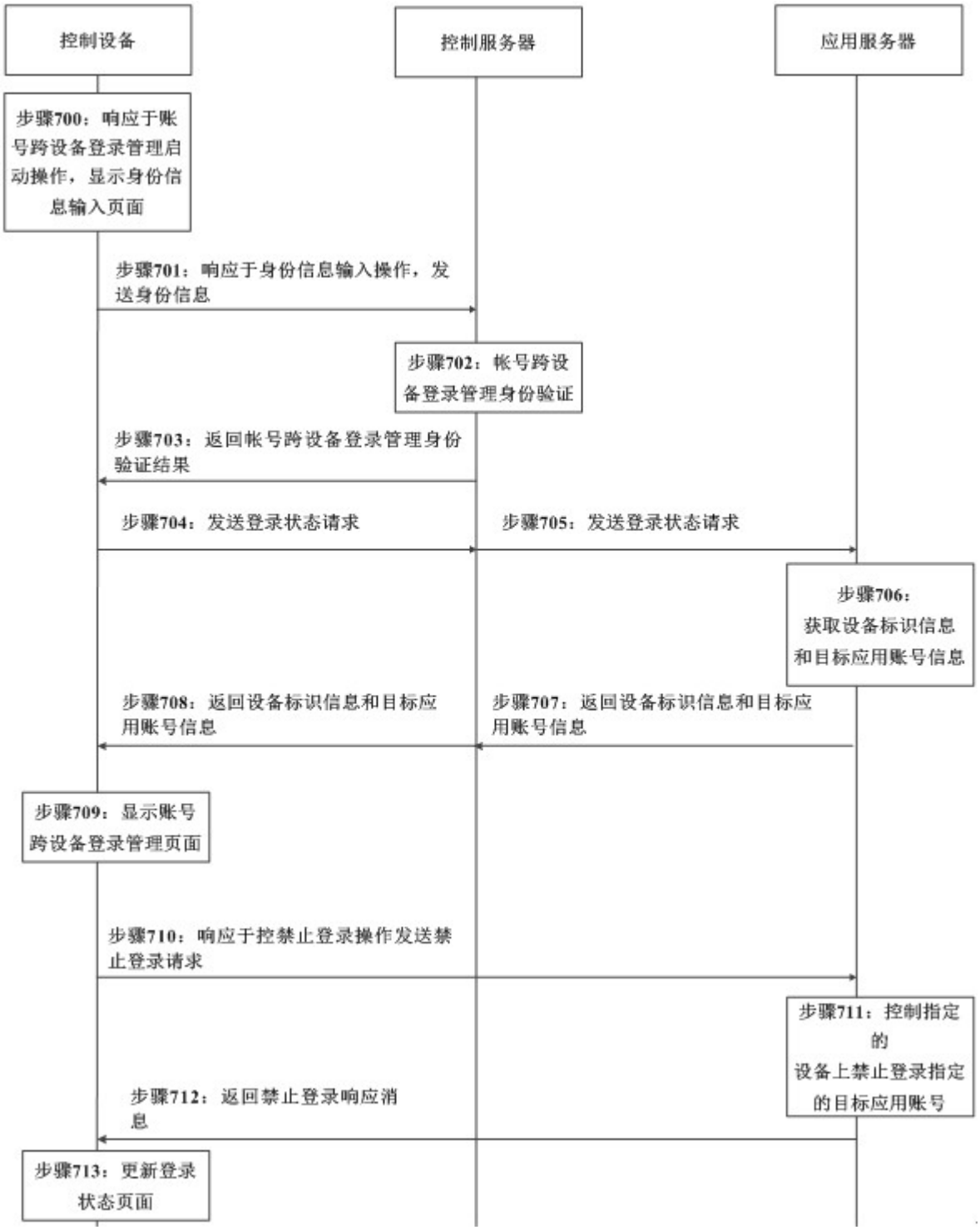

控制设备
控制服务器
应用服务器
步骤700：响应于账号跨设备登录管理启动操作，显示身份信息输入页面
步骤701：响应于身份信息输入操作，发送身份信息
步骤702：帐号跨设备登录管理身份验证
步骤703：返回帐号跨设备登录管理身份验证结果
步骤704：发送登录状态请求
步骤705：发送登录状态请求
步骤706：获取设备标识信息和目标应用账号信息
步骤708：返回设备标识信息和目标应用账号信息
步骤707：返回设备标识信息和目标应用账号信息
步骤709：显示账号跨设备登录管理页面
步骤710：响应于控禁止登录操作发送禁止登录请求
步骤711：控制指定的设备上禁止登录指定的目标应用账号
步骤712：返回禁止登录响应消息
步骤713：更新登录状态页面

图7


811
启动单元
812
输入单元
814
控制单元
813
显示单元

图8

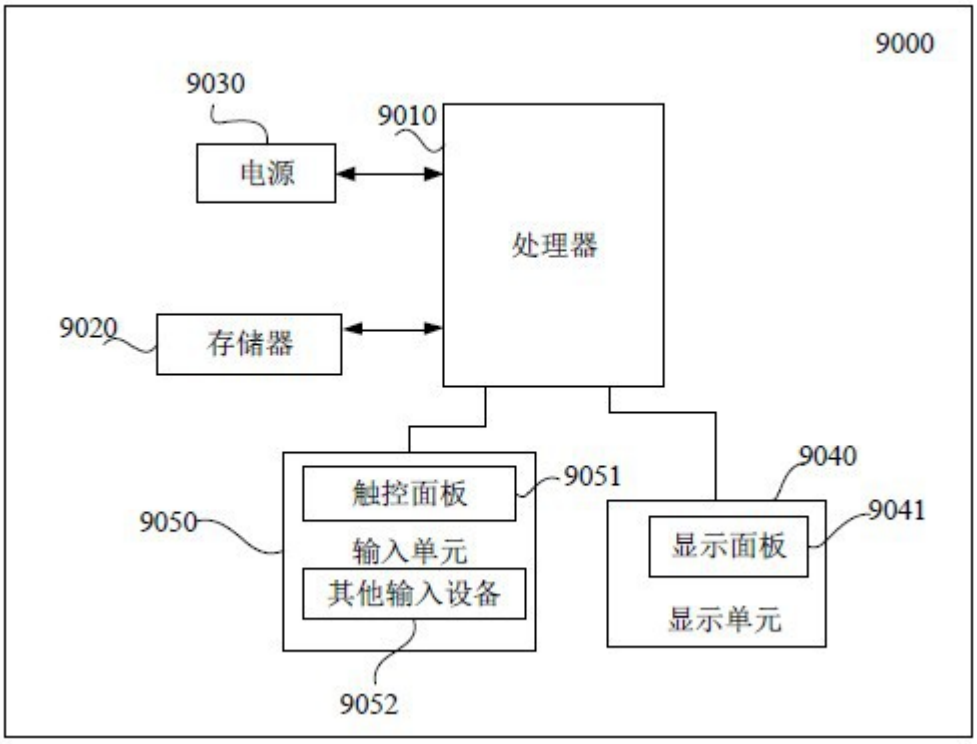

9000
9030
电源
9010
处理器
9020
存储器
9040
9051
触控面板
9050
输入单元
其他输入设备
9041
显示面板
显示单元
9052

图9