(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 107609369 B
(45)授权公告日 2022.04.12

(21)申请号 201710740996.3
(22)申请日 2012.08.06
(65)同一申请的已公布的文献号
申请公布号 CN 107609369 A
(43)申请公布日 2018.01.19
(30)优先权数据
13/247,652 2011.09.28 US
(62)分案原申请数据
201280058320.1 2012.08.06
(73)专利权人 谷歌有限责任公司
地址 美国加利福尼亚州
(72)发明人 松冈良伦
(74)专利代理机构 中原信达知识产权代理有限责任公司 11219
代理人 周亚荣 安翔
(51)Int.Cl.
G06F 21/32(2013.01)
(56)对比文件
CN 102164113 A,2011.08.24
CN 103686386 A,2014.03.26
JP 特开2003-67339 A,2003.03.07
CN 101312488 A,2008.11.26
外星人赫敏.http://dell.benyouhui.it168.com/thread-1470995-1-1.html.《http://dell.benyouhui.it168.com/thread-1470995-1-1.html》.2011,第2-4页.
审查员 吴卿

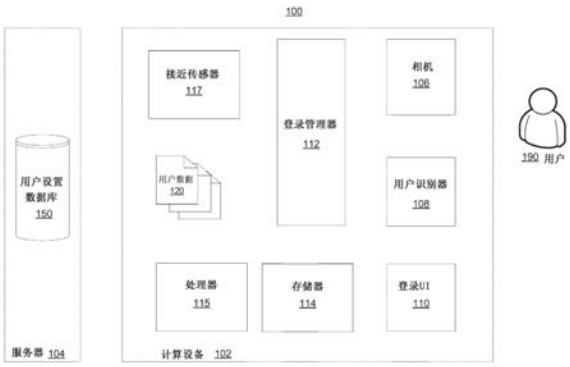
权利要求书2页 说明书19页 附图10页

(54)发明名称

基于面部识别登录到计算设备

(57)摘要

本申请涉及基于面部识别登录到计算设备。一种用于使第一用户登录到计算机设备中的方法,包括经由与该计算设备操作地耦合的相机接收第一用户的图像,并且基于所接收的图像确定第一用户的身份。如果所确定的身份与预定身份相匹配,则至少部分地基于第一用户的身份与预定身份相匹配来使第一用户登录到该计算设备中。



CN 107609369 B

1.一种计算机实现的方法,包括:

基于第一用户的第一授权水平来授权所述第一用户访问计算设备上的第一资源集合;

在所述第一用户被授权来访问所述第一资源集合的同时,由与所述计算设备相关联的成像设备捕捉第二用户的数字图像;

基于所捕捉的数字图像,识别所述第二用户的账户;

基于所述识别并且在所述第一用户被授权来访问所述第一资源集合的同时,在所述计算设备处提供用以确认所述第二用户有关所述计算设备的授权的提示;

接收对所述提示的有效响应;以及

响应于接收到所述有效响应,

确定所述第二用户访问所述计算设备上的第二资源集合的第二授权水平;以及

将当前授权水平改变为与所述第一用户的所述第一授权水平和所述第二用户的第二授权水平的交集相对应的授权水平,同时维持所述第一用户对所述计算设备的授权。

2.根据权利要求1所述的计算机实现的方法,其中,改变所述当前授权水平包括:移除在所述计算设备的显示器上显示的、与所述第一用户相关联的图形信息,以及限制由所述第二用户对所述第一资源集合中的一个或多个资源的访问。

3.根据权利要求1所述的计算机实现的方法,进一步包括:

当接收到对所述提示的所述有效响应时,禁止对所述第一资源集合的用户访问。

4.根据权利要求1所述的计算机实现的方法,进一步包括:

当接收到对所述提示的无效响应时,将所述第二用户的所述数字图像发送至所述第一用户能够访问的预定的账户或远程设备。

5.根据权利要求4所述的计算机实现的方法,其中,所述账户是所述第一用户的电子邮件账户。

6.根据权利要求1所述的计算机实现的方法,其中,所述数字图像包括多个潜在用户,并且其中,所述识别包括:

基于与由所述第二用户对所述计算设备的使用相关联的预定标准来从所述多个潜在用户当中选择所述第二用户,其中,所述预定标准包括:预定时间段、对所述计算设备的使用频率、或者所述计算设备的当前位置。

7.根据权利要求1所述的计算机实现的方法,其中,所述计算设备是移动设备并且所述成像设备是耦合至所述移动设备的相机,以及

所述识别基于由所述成像设备捕获的面部姿态。

8.根据权利要求7所述的计算机实现的方法,进一步包括:

接收作为在所述移动设备的触摸敏感区域中的触摸姿态的所述有效响应。

9.根据权利要求1所述的计算机实现的方法,其中,如果基于由所述成像设备捕捉的后续图像而检测到所述第二用户的离开,则将所述计算设备处的所述当前授权水平恢复为所述第一用户的所述第一授权水平。

10.一种计算设备,包括:

相机;

一个或多个处理器;以及

存储器,所述存储器具有存储在其上的指令,所述指令在由所述处理器执行时使得所

述设备：

基于第一用户的第一授权水平来授权所述第一用户访问由所述计算设备提供的第一资源集合；

在所述第一用户被授权来访问所述第一资源集合的同时，由所述相机捕捉第二用户的数字图像；

基于所捕捉的数字图像，识别所述第二用户的账户；

基于所述识别来提供用以确认所述第二用户有关所述计算设备的授权的提示；

接收对所述提示的有效响应；以及

响应于接收到所述有效响应，

确定所述第二用户访问所述计算设备上的第二资源集合的第二授权水平；以及

将当前授权水平改变为与所述第一用户的所述第一授权水平和所述第二用户的第二授权水平的交集相对应的授权水平，同时维持所述第一用户对所述计算设备的授权。

11.根据权利要求10所述的计算设备，其中，改变所述当前授权水平包括：移除在所述计算设备的显示器上显示的、与所述第一用户相关联的图形信息，以及限制由所述第二用户对所述第一资源集合中的一个或多个资源的访问。

12.根据权利要求10所述的计算设备，其中，所述指令在被执行时进一步使得所述设备：

当接收到对所述提示的所述有效响应时，禁止对所述第一资源集合的用户访问。

13.根据权利要求10所述的计算设备，其中，所述指令在被执行时进一步使得所述设备：

当接收到对所述提示的无效响应时，将所述第二用户的所述数字图像发送至所述第一用户能够访问的预定的账户或远程设备。

14.根据权利要求13所述的计算设备，其中，所述账户是所述第一用户的电子邮件账户。

15.根据权利要求10所述的计算设备，其中，所述数字图像包括多个潜在用户，并且其中，所述识别包括：

基于与由所述第二用户对所述计算设备的使用相关联的预定标准来从所述多个潜在用户当中选择所述第二用户，其中，所述预定标准包括：预定时间段、对所述计算设备的使用频率、或者所述计算设备的当前位置。

16.根据权利要求10所述的计算设备，其中，如果基于由所述成像设备捕捉的后续图像而检测到所述第二用户的离开，则将所述计算设备处的所述当前授权水平恢复为所述第一用户的所述第一授权水平。

17.根据权利要求10所述的计算设备，所述计算设备是移动设备，并且所述计算设备进一步包括：

接收作为在所述移动设备的触摸敏感区域中的触摸姿态的所述有效响应。

18.根据权利要求10所述的计算设备，其中，所述识别基于由所述成像设备捕获的面部姿态。

基于面部识别登录到计算设备

[0001] 分案说明

[0002] 本申请属于申请日为2012年8月6日的中国发明专利申请No.201280058320.1的分案申请。

[0003] 相关申请的交叉引用

[0004] 本申请要求于2011年9月28日提交的题为“LOGIN TO A COMPUTING DEVICE BASED ON FACIAL RECOGNITION”的美国非临时专利申请No.13/247,652的优先权并且作为其连续申请,上述申请通过引用全文合并于此。

技术领域

[0005] 本描述涉及针对计算机的用户认证,具体地涉及基于面部识别而登录到计算设备。

背景技术

[0006] 在计算机安全中,登录(也被称作登入和签入)通常是通过使用用户提供的安全证书标识用户来控制对计算机系统的个人访问的过程。用户能够登录到系统以获得对计算机系统的资源的访问并且能够在不再需要进行访问时退出(执行退出)。退出通常是为了在先前已经登录之后关闭对计算机系统的资源的访问。

[0007] 传统上,计算机或计算设备可以被锁定或者以其它方式进行保护而防止非授权或无意的使用。通常,要求用户执行一些确认动作(例如,输入密码、键入键组合、移动鼠标、将手指划过屏幕等)来对计算机进行解锁。

发明内容

[0008] 在第一个总体方面,一种使第一用户登录到计算设备中的方法包括经由与该计算设备操作地耦合的相机接收第一用户的图像,并且基于所接收的图像确定第一用户的身份。如果所确定的身份与预定身份相匹配,则至少部分地基于第一用户的身份与预定身份相匹配的来使第一用户登录到该计算设备中。

[0009] 在另一个总体方面,一种用于使第一用户登录到计算设备中的系统可以包括存储在有形计算机可读介质上并且包括指令的计算机程序产品。当该指令被执行时,它们能够使得计算机系统经由与该计算设备操作地耦合的相机接收第一用户的图像,基于所接收的图像确定第一用户的身份,如果所确定的身份与预定身份相匹配,则至少部分地基于第一用户的身份与预定身份相匹配来使第一用户登录到该计算设备中。

[0010] 在另一个总体方面,一种计算设备可以包括相机,其被配置为接收第一用户的图像;用户识别器,其被配置为基于所接收的图像确定第一用户的身份;和登录管理器,其被配置为在所确定的身份与预定身份相匹配的情况下,至少部分地基于第一用户的身份与预定身份相匹配来使第一用户登录到该计算设备中。

[0011] 实施方式可以包括以下特征中的一个或多个。例如,该相机可以在物理上与该计

算设备集成。该计算设备可以包括电话。

[0012] 使第一用户登录到计算设备中可以包括允许第一用户访问与第一用户相关联的第一资源，但是禁止第一用户访问与第二用户相关联的第二资源，并且该方法可以进一步包括使第一用户退出该计算设备，经由与该计算设备操作地耦合的相机接收第二用户的第二图像，基于所接收的第二图像确定第二用户的身份。并且然后，如果所确定的第二用户的身份与预定身份相匹配，则至少部分地基于第二用户的身份与预定身份相匹配能够使第二用户登录到该计算设备，其中使第二用户登录到该计算设备中包括允许第二用户访问与第二用户相关联的第二资源，但是禁止第二用户访问与第一用户相关联的第一资源。

[0013] 如果所确定的身份与预定身份相匹配，则能够在不要求来自用户的字母数字输入的情况下使第一用户登录到该计算设备。

[0014] 如果所确定的身份匹配不与预定身份相匹配，则可以要求第一用户输入与第一预定字母数字信息相匹配的第一字母数字信息以及与第二预定字母数字信息相匹配的第二字母数字信息，并且如果用户所输入的第一字母数字信息与第一预定字母数字信息相匹配并且第二字母数字信息与第二预定字母数字信息相匹配，则能够使第一用户登录到该计算设备上。如果所确定的身份匹配不与预定身份相匹配，则可以要求第一用户输入与第二预定字母数字信息相匹配的第二字母数字信息，但是将不要求第一用户输入与第一预定字母数字信息相匹配的第一字母数字信息。如果第二字母数字信息与第二预定字母数字信息相匹配，则能够使第一用户登录到该计算设备。该第一预定字母数字信息可以包括与第一用户相关联的用户名，并且该第二预定字母数字信息可以包括与第一用户相关联的密码。

[0015] 可以经由相机接收第一用户的多个图像，该多个图像是从相对用户脸部的不同视角拍摄的，并且基于所接收的多个图像来确定第一用户的身份。

[0016] 可以经由相机接收第一用户的多个图像，该多个图像包括用户的面部姿态，并且能够基于所接收的多个图像和基于该面部姿态来确定第一用户的身份，并且如果所确定的身份与预定身份相匹配，则能够使第一用户登录到该计算设备中。

[0017] 基于所接收的图像确定第一用户的身份可以包括基于以下中的一个或多个来确定第一用户的身份：用户的眼睛、鼻子、颧骨和/或下颌在该用户的图像中的相对位置、大小和/或形状。

[0018] 如果所确定的身份匹配不与预定身份相匹配，则要求第一用户输入与第一预定字母数字信息相匹配的第一字母数字信息作为使第一用户登录到该计算设备上的条件。然后，如果所确定的身份匹配不与预定身份相匹配，则能够接收计算设备的触摸敏感区域中的一个或多个姿态。在该触摸敏感区域中接收的姿态能够与存储在存储器中的一个或多个预定的设备姿态相比较，并且如果所接收的姿态与预定姿态相匹配则能够使第一用户登录到该计算设备上，而不需要第一用户输入字母数字信息作为使第一用户登录到计算设备上的条件。

[0019] 该方法可以进一步包括，在使第一用户登录到该计算设备中之后，经由相机接收第二用户的图像，基于所接收的第二用户的图像确定第二用户的身份，并且如果所确定的第二用户的身份不与通过第一用户的身份匹配的预定身份相匹配，则使第一用户退出该计算设备。如果所确定的第二用户的身份与预定身份相匹配，则能够至少部分基于第二用户的身份与该预定身份相匹配来使第二用户登录到该计算设备中。

[0020] 该相机可以被配置为接收第一用户的多个图像，该多个图像是从相对用户的脸部的不同视角拍摄的，并且用户识别器可以被配置为基于所接收的多个图像确定第一用户的身份。

[0021] 一个或多个实施方式的细节在附图和以下的描述中给出。其它特征将由于该描述和附图以及权利要求而是显而易见的。

附图说明

[0022] 图1是依据所公开的主题的系统的示例实施方式的框图。

[0023] 图2是依据所公开的主题的装置的示例实施方式的框图。

[0024] 图3是依据所公开的主题的系统的示例实施方式的框图。

[0025] 图4是依据所公开的主题的系统的示例实施方式的框图。

[0026] 图5A是依据所公开的主题的系统的示例实施方式的框图。

[0027] 图5B是依据所公开的主题的系统的示例实施方式的框图。

[0028] 图5C是依据所公开的主题的系统的示例实施方式的框图。

[0029] 图6是依据所公开的主题的系统的示例实施方式的框图。

[0030] 图7是依据所公开的主题的技术的示例实施方式的流程图。

[0031] 图8示出了能够用来实施这里所描述的技术的计算机设备和移动计算机设备的示例。

[0032] 同样的附图标记在各图中指示同样的要素。

具体实施方式

[0033] 图1是依据所公开的主题的系统100的示例实施方式的框图。在一个实施方式中，系统100可以包括计算设备102和服务器104。计算设备102可以包括台式计算机、膝上计算机、平板计算机、笔记本计算机、智能电话等。该计算设备102可以由用户190使用并且可以通过网络与服务器104进行通信。计算设备102可以包括相机106，所述相机可以被用来检测用户的存在并且基于面部识别技术来确定用户的身份。然后，用户的身份能够与被授权登录到计算设备102中或者被授权使用计算设备102的资源的用户的所存储信息进行比较。当在所确定的身份与所存储信息之间发现匹配时，能够使所识别的用户登录到计算设备中或者允许其使用计算设备102的资源。

[0034] 在各个实施方式中，计算设备102可以包括处理器115和存储器114。在一些实施方式中，处理器115可以执行各种软件、固件或者其组合。例如，在一个实施方式中，处理器115可以执行登录管理器112、用户识别器108和/或登录用户界面110。在这样的实施方式中，所执行软件的部分可以存储在存储器114内。

[0035] 在一个说明性实施方式中，当用户(例如用户190)靠近计算设备102时，相机106可以获取该用户的数字图像。相机106可以与计算设备102集成并且可操作地与之连接，或者相机106可以与计算设备102分离并且可操作地与之连接(例如，经由与计算设备的有线或无线连接)。处理器115或者在处理器115上执行的用户识别器108可以对用户的数字图像进行分析以确定靠近计算设备102的用户的身份。例如，用户识别器108可以分析用户的数字图像以将这样的信息确定为用户眼睛的大小、用户眼睛之间的距离、用户鼻子的大小和形

状、用户眼睛和鼻子的相对位置等等。该信息能够与所存储的与被授权使用计算设备或其资源的用户相关的信息进行比较，并且如果发现匹配，则处理器115或者在处理器上执行的登录管理器112可以使用户登录到计算设备中或者允许用户使用计算设备102的资源。

[0036] 在一个实施方式中，计算设备102可以是被多个不同用户共享的台式计算设备或笔记本计算设备。计算设备102可以包括相机106，所述相机可以被集成到计算设备中。例如，相机可以被集成到计算机设备102的显示部分的框(bezel)中并且能够定向为垂直于显示设备，使得其面向脸部位于显示设备前方的用户。

[0037] 相机106能够记录处于其视场中的对象的图像。相机106可以被配置为例如以固定速率定期记录图像，或者响应于相机前方区域中的移动而记录图像，例如响应于用户移动到相机之前的位置或者响应于来自用户的明确输入，例如用户触摸计算设备102的键盘的键。在一个实施方式中，相机106能够被配置为在相机前方的区域中没有检测到活动时以低速率记录图像，并且在该区域内检测到活动时以较高速率记录图像。这可以允许相机对坐在计算设备前方以使用该设备的用户或者从计算设备走开的用户作出快速响应，但是在用户坐在计算设备102前方时避免以高速率消耗计算资源。在一些实施方式中，相机106所记录的图像能够在自图像已经被记录之后流逝了阈值时间量(例如，5分钟)之后被丢弃，和/或相机所记录的图像能够在计算设备关机或进入低功率状态时被丢弃。

[0038] 相机106所记录的图像能够被用户识别器108接收并分析以确定其图像被记录的用户的身份。在各个实施方式中，用户识别器108可以对图像执行面部识别。例如，用户识别器108可以将如相机106所检测并且由用户识别器108所分析的用户190的面部特征与潜在用户群组的面部特征进行比较。该比较可以包括能够被用来识别用户的其他面部特征的比较。

[0039] 能够使用各种面部识别技术。例如，能够使用将脸部与相机视场中的其它特征区分开来并且随后测量脸部的各种特征的技术。每个脸部具有多个可区分的标志，以及构成面部特征的不同峰值和谷值。这些标志可以被用来定义脸上的多个节点，其可以包括与用户眼睛之间的距离、用户鼻子的宽度、用户眼窝的深度、用户颧骨的形状、用户下颌线的长度相关的信息。用户脸部的节点可以从用户脸部的一个或多个图像来确定以创建表示用户脸部的被称作面部印记(faceprint)的数字代码。

[0040] 还能够基于用户脸部的三维图像或者基于能够共同提供与用户脸部相关的三维信息的多个二维图像来执行面部识别。三维面部识别使用脸部的特色特征，例如，刚性组织和骨骼最为明显的地方，诸如眼窝、鼻子和下巴的曲线，以便识别用户并且生成用户的面部印记。用户的面部印记可以包括可量化的数据，诸如表示用户脸部的特征的数字集合。

[0041] 也可以获取相对于用户脸部的不同视点的多个二维图像并且将其用来识别用户。这也可能阻止(foil)欺骗面部识别技术的尝试，诸如通过阻挡不实际存在于计算设备102前方的用户的照片。

[0042] 在已经基于用户的一个或多个图像确定了用户身份之后，例如通过所生成的用户脸部的可量化面部印记确定了用户身份之后，用户识别器108能够将该用户的身份与一个或多个预定身份进行比较。如果在所确定的身份和预定身份之间发现了匹配，则登录管理器112可以使用户登录到计算设备102中，使得用户能够访问计算设备102的一个或多个资源。预定身份例如能够由计算设备102存储在例如一个或多个存储器114中。预定身份可以

包括用户的一个或多个图像、一个或多个用户的可量化面部印记信息或者可量化面部印记信息的子集，其中该子集不足以对用户的图像进行重构。

[0043] 针对希望利用面部识别技术来登录到计算设备102上的用户，预定身份可以根据选择加入过程而以用户的请求进行存储。例如，针对用户的缺省登录过程可以要求用户输入第一和第二字母数字串，诸如用户名和密码。然而，一旦用户已经使用缺省登录过程成功登录，该用户就可以选择使计算设备102存储与该用户相关联的预定身份，使得在未来的登录期间，该用户利用基于面部识别技术的登录过程，与输入用户名和密码相比，这可能是耗时更少并且更少干扰用户。

[0044] 在另一个实施方式中，用户可以选择使用面部识别技术减少但并不消除作为用于获得对计算设备102的资源的访问的登录过程的一部分而要求的字母数字输入的数量。例如，如果缺省登录过程要求用户输入第一字母数字信息(例如，用户名)和第二字母数字信息(例如，密码)，则用户可以选择利用面部识别技术来消除输入一条字母数字信息的要求。在一个实施方式中，如果在面部识别技术所确定的用户身份与所存储的预定身份之间存在匹配，则用户可以跳过输入第一字母数字信息的步骤并且可以继续进行以仅输入第二字母数字信息以登录到计算设备102。

[0045] 在对于登录到包括电容耦合或电阻耦合的触摸敏感输入面板的设备上特别有用的另一个实施方式中，还能够使用面部识别技术来阐明作为登录过程的一部分而需要的字母数字输入数量。例如，当在图像中接收到对应于与预定身份相匹配的身份的用户的图像时，则可以要求用户在计算设备的触摸敏感区域中输入一个或多个姿态。如果用户所输入的姿态与一个或多个预定姿态相匹配，则用户能够登录到计算设备中而并不要求用户输入字母数字信息作为登录到计算设备上的条件。然而，如果所接收到的图像对应于不与预定身份相匹配的身份，则可以要求用户输入特定字母数字信息作为登录到计算设备上的条件。通过使用面部识别技术来消除输入字母数字信息的条件，用户可以找到有保障的过程，并且在保障诸如智能电话的移动计算设备时，与需要他们输入字母数字信息以解锁移动计算设备相比麻烦更少。

[0046] 在另一个实施方式中，由处理器115、用户识别器108和登录管理器112执行的面部识别技术能够被用来有效地使不同用户登录到共享计算设备102。例如，多个用户(例如，家庭成员、同事等)可以共享计算设备102，并且每个用户可以具有存储在计算设备102上或者存储在服务器104上并且从服务器获取而使得其能够结合计算设备102使用的不同用户数据120。用户数据120可以例如包括为特定用户个人的文档、偏好、书签和收藏、设置等。使特定用户登录到计算设备102中的动作能够使得与特定用户相关联的用户数据120而不是与其它用户相关联的用户数据可被该特定用户使用。

[0047] 在一些实施方式中，用户数据120可以从保存有用户设置数据库150的服务器104获取。在这样的实施方式中，用户190可以使用多个设备(例如，计算设备102等)，并且无论使用哪个设备，他们的用户数据120都可以被使用。一旦计算设备102已经识别出用户190，计算设备102就能够请求用户190的用户数据120并随后从服务器104进行下载。

[0048] 为了促成从一个用户到另一用户的有效转换，能够使用面部识别技术。例如，基于(如面部识别技术所确定的)第一用户的身份与关联于第一用户的预定身份相匹配，第一用户能够登录到计算设备。一旦登入，第一用户就能够被允许访问存储在计算设备上并且与

第一用户相关联的第一资源(例如,用户数据120),而禁止第一用户访问与第二用户相关联的第二资源。然后,当经由相机106接收到第二用户的脸部的第二图像时,能够基于所接收的第二图像确定第二用户的身份。如果第二用户的身份与和第二用户相关联的预定身份相匹配,则第二用户能够登录到计算设备,并且第二用户能够被允许访问存储在计算设备上并且与第二用户相关联的第二资源,二禁止第二用户访问与第一用户相关联的第一资源。以这种方式,共享计算设备的多个家庭成员可以简单地将自己呈现给计算设备并且使得其个人的用户数据120被计算设备自动加载,同时还了解到其他家庭成员将不会在他们没有登录时访问到他们个人的用户数据。

[0049] 在一个实施方式中,当第一用户登录到计算设备102中并且然后接收到与预定身份相匹配的第二用户的图像时,能够提示用户来确认第一用户应当退出计算设备并且第二用户应当登录到计算设备上,使得该计算设备提供与第二用户相关联的第二资源,而不提供与第一用户相关联的第一资源。该确认可以以各种形式提供给计算设备。例如,如以上所描述的,可以要求与第二用户相关联的密码,或者可以要求键击(例如,回车键或“y”键上的敲击)。以这种方式,可以避免第一用户意外退出并使得第二用户登录。

[0050] 在另一个实施方式中,当未被授权使用计算设备102的用户试图使用计算设备时,可以捕捉该未授权用户的人的图像并且将其存储在设备中或者发送至计算设备的授权用户。例如,如果未授权用户试图登录并使用计算设备但是失败(例如,如果未授权用户输入了不正确的用户名和密码字母数字信息),则相机106能够记录未授权用户的图像并且将图像存储在存储器114中。在另一个实施方式中,所记录的图像可以被发送给授权用户。例如,所记录的图像能够从计算设备102发送至服务器104,服务器104可以将所记录的图像转发至授权用户对其进行访问的账户(例如,电子邮件账户)或设备(例如,智能电话或移动电话或其它移动设备)。然后,授权用户能够响应于未授权用户所进行的登录尝试而采取适当措施。

[0051] 在一些实施方式中,用户的存在可以将计算设备102从睡眠状态唤醒。这样的睡眠状态可以包括其中没有用户(例如,用户190)登录到设备102的状态或模式,或者其中设备102的组件或者其部分断电或关闭并且大多数操作状态被保存到设备102的存储器114的诸如睡眠模式或休眠模式的低功率模式,该存储器114为易失性存储器(例如,用于睡眠模式)或非易失性存储器(例如,用于休眠模式)。

[0052] 设备102可以被配置为在用户190接近计算设备102时检测到用户190的存在。在各个实施方式中,设备102可以包括接近传感器117,其被配置为检测用户(例如,用户190)的存在。在低功率模式中,尽管设备102的大部分处于低功率模式,但是该接近传感器或其它检测传感器106可以被供电或启动以便检测用户。在各个实施方式中,接近传感器117可以包括被配置为(例如,经由触摸等)感应用户190的存在或移动的触摸板、鼠标、电容传感器、电感传感器、红外传感器、运动检测器等。然后,在用户的存在已经将计算设备102从其睡眠状态唤醒之后,能够确定用户的身份。

[0053] 在一个实施方式中,设备102可以包括用户识别器108,其被配置为在检测到用户190存在时确定用户190的身份。用户识别器108可以包括被配置为将从相机106接收的图像的特征与关联于预定用户的特征进行比较的硬件或软件。

[0054] 在各个实施方式中,用户识别器108可以将用户190的数字图像与可能用户的列表

进行比较。用户识别器108可以从与所检测用户190最近似匹配的潜在用户的列表中选择用户。尽管在一些实施方式中用户识别器108可以被配置为在没有针对所检测用户充分近似匹配的情况下不选择潜在用户中的任何一个，其中该匹配的充分性通过预定标准进行判断。

[0055] 在没有潜在用户与所检测用户190相匹配的情况下，计算设备102可以不使任何用户登录到计算设备102。避免使所检测的用户190登录到计算设备102可以包括不将计算设备102从低功率状态移除或者使得计算设备102返回低功率状态。在另一个实施方式中，计算设备102可以整体或部分加载缺省用户设置、偏好或数据120的集合。在一个实施方式中，计算设备102可以加载访客用户设置集合。在这样的实施方式中，访客用户设置可以不提供对计算设备102上存储的数据的访问或者针对其提供有限访问。在这样的实施方式中，访客用户设置可以提供对互联网的访问或者对计算设备102以及计算设备102的能力提供以其它方式进行限制和约束的访问。

[0056] 在各个实施方式中，用户识别器108可以基于相机106记录的图像执行面部识别。在这样的实施方式中，用户识别器108可以将如相机106所检测的用户190的面部特征相对一个或多个潜在用户的面部特征进行比较。该比较可以包括其它身体特征的比较。例如，计算设备102可以基于相机所捕捉的数字图像计算用户190的身高。在另一个示例中，计算设备102可以计算用户190的眼睛或其它生理计量特征之间的距离(例如，本征脸分析等)。

[0057] 在一个实施方式中，设备102可以包括登录管理器112，其被配置为访问给定用户的设置、偏好等(共同被称作用户数据120)，并且将它们加载到设备102的存储器114中，或者以其它方式执行操作以获取对设备102的访问或者登录到设备102。在各个实施方式中，用户数据120可以包括数据，其例如指示该装置：安装各种网络驱动、打印机和/或设备；建立各种网络连接；设置某种颜色方案或图形用户界面(GUI)方案；加载书签或文件以及图标设置；音量和多媒体设置；所保存的密码或认证证书；等等。

[0058] 在另一个实施方式中，用户数据120可以包括要在用户190登录到计算设备102中时打开或执行的应用、文档、文件或标签的列表。在一些实施方式中，这些应用、文档、文件或标签在用户190先前登录到这样的计算设备102中时可能已经被打开或主动执行。在这样的实施方式中，该用户数据120可以允许或促使用户190将其工作环境跨多个机器或装置进行同步。

[0059] 在各个实施方式中，登录管理器112可以从在用户设置数据库(DB)150中存储用户数据120的远程服务器104获取用户数据120。在这样的实施方式中，如以上所描述的，远程服务器104可以被配置为将用户数据120跨多个设备(例如，计算设备102等)进行同步。在各个实施方式中，登录管理器112可以被配置为利用在用户190登录到计算设备102时发生的对用户数据120的任意改变对远程服务器104或用户设置数据库(DB)150进行更新。

[0060] 如以上所描述的，在一些实施方式中，登录过程可以要求密码或其它安全证书，其需要来自用户190的主动参与。在这样的实施方式中，设备102可以包括登录用户界面(UI)110，其被配置为针对用户190的授权证书(例如，密码等)而对其进行提示。登录管理器112可以在预期到授权或安全证书的适当存在时推测性地加载用户的用户数据120，使得如果用户输入了适当的授权证书，用户数据将已经被加载或者处于被加载的过程，从而用户将能够快速访问其用户数据。

[0061] 图2是依据所公开的主题的计算设备202的示例实施方式的框图。计算设备202可以包括台式计算机、膝上电脑、平板电脑、笔记本电脑、智能电话等，除了每一个与相应的不同用户相关联的多个用户数据(例如，用户数据220a、220b和220c等)可以在设备202内本地存储之外，计算设备202可以类似于图1的计算设备102。用户识别器108可以从与用户数据220a、220b和220c相关联的用户中选择或试图识别用户190。在这样的实施方式中，多个用户数据可以包括可被用来识别所检测用户190的数据(例如，用户190的面部特征模式、照片等)。

[0062] 在各个实施方式中，如果没有用户数据与所检测的用户190相关联，则登录管理器112可以不如以上所描述的进行预先加载或使用户190登录到设备202。在一个实施方式中，登录UI 110可以被呈现或可以向用户190显示缺省登录屏幕或UI。一旦通过该缺省登录屏幕或用户界面手工登录到计算设备202中(例如，使用用户名和密码或者根本未使用授权证书)，则登录管理器112可以为用户190创建新的用户数据集合。

[0063] 在一个实施方式中，可以在用户同意的前提下预测新的用户数据集合的创建。在这样的实施方式中，能够提示用户明确允许创建用户数据集合以及任意用户收集(例如，将用户数据存储在服务器104上等)。另外，用户可以选择加入/退出参与这样的数据收集活动。此外，所收集的数据可以在执行数据分析之前被匿名化，例如创建可以被用来创建新用户数据集合的用户数据的一般集合。例如，用户数据的一般集合可以包括所编码或加密的与用户脸部的模式和特征相关的信息，然而不允许从所编码或加密的数据构建用户的图像。

[0064] 替选地，登录管理器112可以从存储用户190的数据的远程服务器请求与用户190相关联的用户数据的集合。用户190的数据可以被添加至本地存储的用户数据集合(例如，用户数据220a、220b和220c等)并且在用户190尝试自动登录到计算设备202的后续实例中被采用。

[0065] 在一些实施方式中，可以存在分别在图1和2的设备102和202的组合。在这样的实施方式中，一些用户数据可以被本地存储而其它数据则可以远程存储。替选地，用户数据的第一部分(例如，图标置放、颜色方案等)可以本地存储，而用户数据的第二部分(例如，活动标签、打印机设置、驱动映射等)可以远程存储并且甚至在用户可以利用的各个设备之间进行同步。

[0066] 图3是依据所公开的主题的系统300的示例实施方式的框图。在一个实施方式中，系统300可以包括装置、电子设备或计算机302。计算设备302可以包括台式计算机、膝上电脑、平板电脑、笔记本电脑、智能电话等。

[0067] 同样，装置302可以类似于图2的计算设备202。然而，在图3中示出了：在一个实施方式中，用户识别器108可以被配置为从处于相机106或用户识别器108的范围内的多个可能或潜在用户(例如，用户390a和390b)中选择单个用户(例如，用户190)。

[0068] 在所图示的实施方式中，装置302可以包括由用户家中的家庭成员使用的共享计算机。在另一个实施方式中，装置302可以是工作环境中由多个雇员使用的共享计算机。在这样的实施方式中，装置302可以检测到多于一个的潜在用户并且选择潜在用户中的一个登录到装置302。

[0069] 在一个这样的实施方式中，用户识别器108可以被配置为识别与设备302最接近的

用户190。在另一个实施方式中，用户识别器108可以被配置为将计算设备202与优选的主要用户(例如用户190)或者计算设备202的主要用户相关联。如果该主要用户在多个用户之中，则可以选择该主要用户进行登录。在各个实施方式中，用户识别器108可以被配置为基于预定标准集合从多个潜在用户中选择一个用户。

[0070] 在各个实施方案中，用户190的识别可以基于用户习惯。例如，第一用户(例如用户190)可以经常在某个时间段(例如8:00pm至10:00pm)期间最频繁地登录到装置302中。第二用户(例如用户390a)可以经常在第二时间段(例如9:00am至1:00pm)期间最频繁地登录到装置302中。并且，第三用户(例如用户390b)可以经常在第三时间段(例如2:30pm至5:30pm)期间最频繁地登录到装置302中。基于用户190、390a和390b的这些习惯，装置302可以识别哪个潜在和所检测用户要被选择为主要用户。装置302可以采用其它用户习惯(例如基于位置、最近使用、使用频率等)来选择用户。还要理解的是，这样的基于识别技术的用户习惯可以仅在识别出单个用户时被采用。在这样的实施方式中，用户习惯可以提供多个可能的候选用户并且(至少在最初)减少用户候选的数量，装置302可以尝试针对所检测的用户进行匹配。

[0071] 图4是依据所公开的主题的系统400的示例实施方式的框图。在一个实施方式中，系统400可以包括装置、电子设备或计算设备402和服务器404。计算设备402可以包括台式计算机、膝上电脑、平板电脑、笔记本、智能电话等。

[0072] 所图示的实施方式中，图示了装置402可以识别用户190的另一手段。如以上关于图1、2和3所描述的，该装置可以基于生理计量信息来识别用户，诸如计算机402内本地可用或者存储在(例如，服务器104等上的)远程知识库中的用户脸部的特征。在所图示的实施方式中，识别信息可以在远程存储系统中找到。在各个实施方式中，识别信息可以以分布式方式进行存储(例如，社交媒体站点、照片共享站点等)。

[0073] 在一个实施方式中，用户识别器108可以被配置为利用存储在一个或多个服务器404内的用户标识符406来识别所检测的用户190。用户标识符406的示例可以包括来自服务器404或者与用户190相关联的站点的照片等。例如，用户识别器108可以被配置为检查与可能用户相关联的或者在预定设置中定义的公司目录、社交媒体站点或照片共享站点。用户识别器108可以将在服务器404上找到的照片与用户190等待登录到设备402中时所拍摄的用户190的照片进行比较。在各个实施方式中，用户识别器108可以被配置为仅检查可能用户的有限列表(例如，先前已经登录到设备402中的用户，公司内的用户，等等)。

[0074] 图5A是依据所公开的主题的系统500的示例实施方式的框图。在一个实施方式中，系统500可以包括用户190所使用的装置502以及服务器104。如以上所描述的，装置502可以包括处理器115、存储器114、一个或多个相机106、登录用户界面110和用户识别器108。此外，在各个实施方式中，装置502可以包括被配置为向用户190图形显示信息的显示器或监视器116。

[0075] 在各个实施方式中，相机106可以包括或具有检测区域550，相机106可以被配置为在其中进行操作。例如，在相机106嵌入在显示器116的框部分中的情况下，该相机可以具有例如距相机106大约2米的在显示器116前方以圆弧辐射的视场，或者更一般地被称作“检测区域550”。因此，相机106可以被配置为不检测相机106的检测区域550之外的事物(例如，在显示器116后的事物等)。在一些实施方式中，相机106的范围可以由用户190控制，使得相机

能够被配置为仅检测相对接近于相机的用户或者检测距离相机更远的用户。

[0076] 在所图示的实施方式中，用户190可以已经如以上所描述的被检测到并登录到装置502中。这样，如以上所描述的，用户190的用户数据120可能已经被加载到存储器114中或者以其它方式可被装置502作为登录过程的一部分而获取。在一些实施方式中，用户数据120可以已经作为用户190使用装置502的一部分被改变或编辑。例如，用户190可以已经打开或关闭各个文档或标签，改变配置设置(例如电子邮件服务器、网络设置等)或者其它形式的用户数据120。

[0077] 在所图示的实施方式中，用户190可以离开相机106的检测区域550。相机106或装置502可以检测到用户190的状态关于装置502的这一变化。在该上下文中，“用户状态变化”可以包括用户存在的变化(例如，用户已经从装置走开?等等)，用户对装置的单独或共享使用的变化(例如，用户已经单独访问了装置?多个用户共享装置?第二个人或用户能够偷听或窥探到用户的登录?等等)，或者用户对装置502的关注度的变化(例如，用户主动使用装置502还是仅是处于相机的监测区域中?等等)，等等。

[0078] 在所图示的实施方式中，用户190可以离开相机106的检测区域550。例如，用户190可以从装置502走开。在这样的实施方式中，如以上所描述的，相机106或用户识别器108可以检测到用户190的状态变化与装置550的关系。响应于用户190的状态变化，登录/授权管理器612可以对用户190的授权水平进行调节。

[0079] 例如，在一个实施方式中，响应于用户190离开相机106的检测区域550，登录/授权管理器612可以将用户190退出装置502。在此上下文中，将用户190退出装置502可以被认为是一种调节用户190使用装置502的授权的方式。在这样的实施方式中，这可以包括更新或与服务器104同步用户190的用户数据120。在这样的实施方式中，当用户190登录回到装置(例如，装置502或另一装置等)中时，更新的用户数据120可以被用来将用户190登录到装置设备中。在用户190打开用户数据120中所包括的应用、文档的实施方式中，用户190可以能够实质上就像其从未退出那样继续使用装置502(或其它装置)。

[0080] 在另一个实施方式中，响应于用户190离开相机106的检测区域550，登录/授权管理器512可以将用户190部分退出装置502。同样，在此上下文中，将用户190部分退出装置502可以被认为是一种调节用户190使用装置502的授权的方式。例如，登录UI 110可以移除经由显示器116显示的正常图形信息(例如窗口、文档等)并且替代显示要求用户190在可以经由显示器116显示正常图形信息之前对其自身进行重新认证的登录或锁定屏幕。在这样的实施方式中，用户数据120可以根据实施方式而与服务器104进行同步，或不与服务器104同步。在各个实施方式中，重新授权可以经由以上参考图1、2、3和/或4所描述的技术来自动发生。

[0081] 在另一个实施方式中，响应于用户190离开相机106的检测区域550，登录/授权管理器512可以将装置502置于或变换至功率降低的状态(例如，挂起功率状态、休眠功率状态等)。在此上下文中，将装置502置于功率降低的状态可以被认为是一种调节用户190使用装置502的授权的方式，因为在装置502处于功率降低的状态时，可以对用户可以如何使用装置502进行限制。在各个实施方式中，登录/授权管理器512可以将装置502的一部分置于或转换为功率降低的状态。例如，登录/授权管理器512可以在用户190未处于检测区域550中或者以其它方式具有与装置502相关的其中用户190不可能观看显示器116的状态(例如，用

户190的后背可能朝向装置502等)的情况下关闭显示器116或者降低其亮度。在各个实施方式中,装置502可以包括功率管理器530,其对装置502在各种功率模式中的变换进行管理。在这样的实施方式中,登录/授权管理器512可以请求功率管理器530执行这样的变换。

[0082] 相反地,如果用户190的状态变为其将可能与装置502进行交互的状态,则登录/授权管理器512可以将装置502(或者其部分)从功率降低的模式移除或者将其变换为先前的功率模式或活动功率模式(例如,工作功率模式等)。在各个实施方式中,状态改变检测和功率模式变换可以经由以上参考图1、2、3和/或4所描述的技术自动发生。

[0083] 在各个实施方式中,用户190也可以被认证为一种或多种安全方案。例如,用户190可以已经提供了认证或授权细节以便访问网络、各种文件(例如网络驱动、加密文件等)、软件或web服务(例如雇员数据库、财务网站等)。在这样的实施方式中,这些服务或文件中的每一个可以采用不同的授权方案。例如,第一服务可以允许用户190的授权直至用户190主动退出装置502;第二服务只要用户190处于装置502时就允许其授权等等。在这样的实施方式中,登录/授权管理器512可以基于多个服务所采用的相应规则系统或方案而有选择地撤销用户190的授权。例如,在以上的示例实施方式中,如相机106和/或用户识别器108所检测的,当用户190通过离开检测区域550而改变其状态时,登录/授权管理器512可以保持针对第一服务的授权(如果移出检测区域550没有被认为是主动退出装置550),但是会撤销针对第二服务的授权。

[0084] 在此上下文中,术语“安全服务”是指在那些安全服务可以被用户190使用之前要求用户190授权的一个或多个服务(例如,网站、文件访问、装置使用访问等),并且它们还可以基于用户的授权水平对用户可以使用该安全服务的方式进行约束或限制。

[0085] 在各个实施方式中,针对安全服务的这些认证或授权细节可以或已经作为如以上所描述的自动登录过程的一部分而提供。在另一个实施方式中,这些认证或授权细节可以已经由用户190手工提供或者经由其它手段自动提供(例如,web浏览器中的cookie、经由第三方认证服务的用户名/密码配对,等等)。在一些实施方式中,用户190的授权可以整体或部分由登录/授权管理器512进行管理。

[0086] 在所图示的其中登录/授权管理器512可以有选择地撤销或调整用户190有关多个安全服务的授权的实施方式中,登录/授权管理器512可以改变与那些安全服务相关联的图形信息部分如何由显示器116进行显示。例如,如果用户190使得与安全服务相关联的网站包含或显示在GUI窗口中,并且登录/授权管理器512撤销了用户190针对该安全服务的授权,则包含或显示该安全且不再授权的网站的GUI窗口可以被关闭、暗淡、模糊化、最小化,或者以其它方式从显示器116所进行的显示被遮挡或移除。同样,安全但不再被授权的文件或文档可以被关闭或加密或遮挡,使得其中所包含的信息无法被非授权的观看者(例如,如以下所描述的图5B的用户590b)所访问。

[0087] 在各个实施方式中,登录/授权管理器512可以基于一个或多个规则改变或调整用户190使用装置502的授权水平。例如,登录/授权管理器512可以基于用户190已经离开检测区550的时间量来改变或调整用户190的授权水平。在一个实施方式中,如果用户190仅从监测区域550离开相对短的时间段(例如,30秒、1分钟或2分钟),则登录/授权管理器512可以仅锁定或关闭显示器116。然而,如果用户190已经从检测区域550离开相对长的时间段(例如,5分钟、10分钟或20分钟等),则登录/授权管理器512可以将用户190退出装置502并且将

装置502置于功率降低的模式(例如,挂起功率模式、休眠功率模式等)。

[0088] 在各个实施方式中,登录/授权管理器512可以使得其调节用户190的授权水平的决策以各种因素或量度是否超过一个或多个阈值为基础。在一些实施方式中,这些影响因素或量度可以包括但不局限于:一个或多个系统资源(例如,电池电力水平、网络带宽、网络类型、处理器能力、存储器使用、存储可用性等)的可用性、一个或多个系统资源的消耗率、用户190有关装置的状态变化已经流逝的时间量、用户(例如,用户190、图5B的用户590a等)的物理位置、装置502的物理位置等。

[0089] 图5B是依据所公开的主题的系统501的示例实施方式的框图。在一个实施方式中,系统501可以包括用户190所使用的装置502b。如以上所描述的,装置502b可以包括处理器115、存储器114、显示器116、一个或多个相机106、登录/授权管理器512、登录用户界面110和用户识别器108。在各个实施方式中,如以上所描述的,相机106可以包括或具有相机106被配置为在其中进行操作的检测区域550。

[0090] 在所图示的实施方式中,如以上所描述的,用户190可以已经被检测到并且登录到了装置502b中。这样,如以上所描述的,作为登录过程的一部分,用户190的用户数据120可以已经被加载到存储器114中或者以其它方式使得可被装置502b使用。在一些实施方式中,用户数据120可以作为用户190使用装置502b的一部分而已经被改变或编辑。例如,用户190可以打开或关闭了各种文档或标签、改变了配置设置(例如电子邮件服务器、网络设置等)或者其它形式的用户数据120。

[0091] 在所图示的实施方式中,用户590a可以进入检测区域550。第二或另外用户(例如,用户590a或者用户590b,如果用户590b进入检测区域等等)的增加可以被认为是第一用户190有关装置502b的状态变化。在这样的实施方式中,登录/授权管理器512可以改变或调整第一用户190有关装置502b的授权。

[0092] 例如,在一个实施方式中,登录/授权管理器512可以调暗或关闭显示器116,使得新用户590a不会看到显示器116所显示的用户590a未被授权看到的信息。同样,音频输出或其它输出可以被限制。这些输出的限制基本上可以撤销第一用户190先前所拥有的观看显示器116、音频输出或装置502b的其它输出的授权。

[0093] 在另一个实施方式中,登录/授权管理器512可以确定第二用户590a的身份。在一些实施方式中,这可以包括访问与新用户590a相关联的用户数据520a。基于该识别,登录/授权管理器512可以确定第二用户590a所持有的授权水平。登录/授权管理器512可以将新用户590a的授权水平与第一用户190的授权水平进行比较。如以上所描述的,针对各种安全服务可以存在各种授权水平。在这样的实施方式中,登录/授权管理器512可以基于第一用户190的第一授权水平以及第二用户590a的第二授权水平来限制装置502b的使用。

[0094] 例如,在一个实施方式中,装置502b可以仅在显示器116所显示的信息未被授权由用户190和用户590a示的情况下调暗或关闭显示器116(或者其它输出设备等)。在另一个实施方式中,显示器116可以仅调暗或遮挡显示器116中包括未被授权由用户190和用户590a显示的信息的部分(例如,GUI窗口等),而可以向用户190和用户590a显示的部分则可以不变或可见。在这样的实施方式中,登录/授权管理器512可以将第一用户190的有效授权水平从用户190的实际授权水平调整为对应于监测区域550内的所有用户(例如,用户190和用户590a等)的授权水平的交集(以集合理论的说法)的授权水平。

[0095] 在另一个实施方式中，登录/授权管理器512可以将用户190的有效授权水平调整为用户190或用户590a中任一个的较高授权水平。在另一个实施方式中，登录/授权管理器512可以将有效授权水平调整为用户190和590a的授权水平的合集(同样以集合理论的说法)。在各个实施方式中，可以使用用于调整用户190的授权水平并禁止装置502b以与被调整的授权水平相符的方式被使用的其它规则或方案。

[0096] 在一个实施方式中，如果用户590a离开或者从检测区域550消失而使用户190单独留在检测区域550中，则用户190有关装置的状态可以被改变。在这样的实施方式中，登录/授权管理器512可以将用户190的授权水平返回或重新调整至用户190先前或自然的授权水平。在另一个实施方式中，如果另外的用户(例如，用户590b)进入检测区域550，用户190的状态再次可以被改变，并且登录/授权管理器512可以再次基于检测区域550内的用户(例如，用户190、590a、590b，用户190和590b，等等)对用户190的授权水平进行调节。

[0097] 在各个实施方式中，用户190有关装置502b的状态变化的检测可以由另一用户(例如，用户590a等)的检测或者另一用户的离开或存在的检测以及次要考虑因素(例如，时间元素等)触发。例如，为了生成用户190的状态变化，用户590a可以已经处于检测区域550内并且保持存在于检测区域550内达预定分钟数或秒数(例如，10秒等)。在这样的实施方式中，“错误肯定”或其它统计误差的存在可能被减少。例如，显示器116可以仅由于用户590b路过、无意进入装置502b的检测区域550就突然关闭可能会令用户190措手不及。在这样的实施方式中，登录/授权管理器512可以利用一些阈值或滞后效应来减少用户190有关装置的状态中的不期望或频繁的变化。

[0098] 图5C是依据所公开的主题的系统501的示例实施方式的框图。在一个实施方式中，系统501可以包括由用户190所使用的装置502c。如以上所描述的，装置502c可以包括处理器115、存储器114、显示器116、一个或多个相机106、登录/授权管理器512、登录用户界面110和用户识别器108。在各个实施方式中，相机106可以包括或具有相机106被配置为在其中进行感测或操作的检测区域550，如上所述。

[0099] 在所图示的实施方式中，如以上所描述的，用户190可以已经被检测到并且登录到了装置502c中。这样，如以上所描述的，作为登录过程的一部分，用户190的用户数据120可以已经被加载到存储器114中或者以其它方式而使得可被装置502c使用。在所图示的实施方式中，用户190的用户数据120可以被存储在活动用户数据522中或者被认为是活动用户数据522。在所图示的实施方式中，活动用户数据522可以包括主动登录到装置502c中的用户的用户数据。在一些实施方式中，如以上所描述的，用户数据120或522可以已经作为用户190使用装置502c的一部分而改变或编辑。

[0100] 在所图示的实施方式中，用户590a可以进入检测区域550。第二或另外用户(例如，用户590a或者用户590b，如果用户590b进入检测区域550，等等)的增加可以被认为是第一用户190有关装置502b的状态变化。在这样的实施方式中，如以上参考图5B所描述的，登录/授权管理器512可以改变或调整第一用户190有关装置502c的授权。

[0101] 然而，在所图示的实施方式中，用户190可以然后选择离开检测区550。在这样的实施方式中，用户190从检测区域550的消失可以生成用户190有关装置502c的状态变化。如以上参考图5A所描述的，登录/授权管理器512可以通过使用户190退出装置502c而改变或调整第一用户190的授权。在各个实施方式中，这可以包括将用户190的用户数据120从活动用

户数据522状态移除。在另一个实施方式中，登录/授权管理器512可以将用户190锁定在装置502c之外(例如，经由屏幕锁定、密码重新授权等)。

[0102] 在一个实施方式中，用户590a可以单独处于检测区域550中。在这样的实施方式中，如以上参考图1、2、3和4所描述的，登录/授权管理器512可以自动确定第二用户590a的身份并且使第二或新的用户590a自动登录到装置502c。在这样的实施方式中，用户590a的用户数据520a可以被认为是或形成为活动用户数据522。

[0103] 在各个实施方式中，用户190可以选择其它手段来退出装置502c或放弃其控制。例如，在一个实施方式中，用户190可以留在检测区域550中但是移动至用户590a后。例如，用户190可以从装置502c前方的座椅起身，用户590a然后可以在该座椅中坐下，并且用户190可以站在用户590a后。相反地，在一些实施方式中，如以上所描述的，用户190可以主动退出装置502c或者将其自身锁定在装置502c之外。在这样的实施方式中，登录/授权管理器512可以被配置为确定第一用户190已经将装置502的控制放弃给第二用户590b的时间。

[0104] 在各个实施方式中，登录/授权管理器512可以被配置为将活动用户数据522整体或部分替换为新的第二用户590b的用户数据520b。例如，在一个实施方式中，登录/授权管理器512可以被配置为将对装置502c的使用以及可以使用装置502c的方式进行管理的授权水平从第一用户190的授权水平变为第二用户590b的授权水平，同时保持第一用户190的配置和设置用户数据120或者其一部分作为活动用户数据522。在这样的实施方式中，具有较高或较大授权水平的管理员或用户(例如，用户590a等)可以利用其较高的授权水平临时访问或使用装置502c而无需使用户190完全退出装置502c。

[0105] 图6是依据所公开的主题的系统600的示例实施方式的框图。在一个实施方式中，系统600可以包括由用户190所使用的装置602。如以上所描述的，装置602可以包括处理器115、存储器114、显示器116、一个或多个相机106、登录/授权管理器612、功率管理器603、登录用户界面110和用户识别器108。在各个实施方式中，相机106可以包括或具有相机106被配置为在其中感测或操作的检测区域(图6中未示出)，如以上所述。

[0106] 在所图示的实施方式中，如以上所描述的，用户190可以已经被检测到并且登录到了装置602中。这样，如以上所描述的，作为登录过程的一部分，用户190的用户数据120可以已经被加载到存储器114中或者以其它方式而使得可被装置602使用。在一些实施方式中，如以上所描述的，用户数据120可以已经作为用户190使用装置602的一部分而改变或编辑。

[0107] 在一个实施方式中，相机106或用户识别器108可以被配置为监视用户190有关装置的关注度。在该上下文中，“对装置的关注度”可以包括以一定兴趣或注意力收听或观看装置(例如，显示器116等)的输出或者向装置602输入信息或指令(例如，经由键盘、鼠标、触摸屏等)。在这样的实施方式中，装置602可以包括关注监视器608，其被配置为监视用户190有关装置的关注度。在各个实施方式中，关注监视器608可以包括在相机106、用户识别器108、登录/授权管理器612或者装置602的其它组件中。

[0108] 在各个实施方式中，关注监视器608可以通过监视用户190的眼睛的位置或移动、用户头部的方位(例如，用户190是否正在观看装置602或者观看远离装置602的别处，等等)、如以上所描述的用户190的存在或消失、用户190的输入速率(例如，每个给定时间段的键击或鼠标移动等)等来测量用户190的关注度。

[0109] 在各个实施方式中，关注监视器608可以基于一个或多个规则或阈值来确定用户

190的关注度。例如，如果用户190在相对短的时间段(例如，5秒等)内看向远离装置602的别处，则关注监视器608可以确定用户190仍然关注于装置602。相反，如果用户190在相对长的时间段(例如，1分钟、5分钟等)内看向远离装置602的别处，则关注监视器608可以确定用户190不再关注于装置602。

[0110] 在一个实施方式中，用户190对装置602的关注度变化可以被认为是用户190有关装置602的状态变化。在这样的实施方式中，如以上所描述的，登录/授权管理器612可以对用户190的授权水平进行调整(例如，使用户190退出装置602，将装置602置于低功率模式等)。在各个实施方式中，登录/授权管理器612可以对用户190的授权水平进行调整，其可以包括暂停应用的执行，将用户190从一个或多个安全服务取消认证，或者将装置602的一个或多个部分置于功率降低的模式，等等。

[0111] 例如，在所图示的实施方式中，如果用户190将其头部转向远离装置602的别处，则登录/授权管理器612可以关闭显示器116。当关注监视器608检测到用户190有关装置602的状态已经通过将用户190的头部转回到装置602而再次变化时，登录/授权管理器612可以通过重新开启显示器116而调整用户190的授权水平。

[0112] 在一些实施方式中，关注监视器608可以在考虑装置602上执行的应用的同时确定用户190的关注度。例如，如果用户190正在执行与文字处理应用相对的电影应用，则以上所提到的阈值或规则可以允许更多的非关注度。在这样的实施方式中，如果用户190看向别处相对长的时间段(例如，5分钟等)但是装置602上正在播放电影，则关注监视器608可以确定用户190仍然关注于装置602。然而，如果用户190看向别处过长时间段(例如，15分钟等)并且装置602上正在播放电影，则关注监视器608可以因此确定用户190不再关注于装置602。

[0113] 例如，在另一实施方式中，登录/授权管理器612可以在用户190看向远离装置602的别处的情况下暂停视频应用的执行。但是登录/授权管理器612可以在用户190看向远离装置602的别处的情况下决定不暂停音频应用的执行。相反，登录/授权管理器612可以在用户190已经从装置602走开的情况下决定静音或暂停音频应用的执行。

[0114] 在又另一个实施方式中，登录/授权管理器612可以使得如何调节用户190的授权水平以可供装置602使用的系统资源的水平为基础。例如，登录/授权管理器612可以不关闭正在使用外部电源(例如，插入到电插口中，等等)装置602的显示器116。然而，如果装置602正在使用电池进行供电，则登录/授权管理器612可以在减少装置602的功耗方面更为积极。

[0115] 与过去利用的相比，使用面部识别技术来确定用户的存在或关注度可以允许更为动态地将设备在高功率和低功率状态之间进行切换，这会为设备602导致节能以及更长的电池寿命。例如，不同于使得将设备602从高功率切换为低功率状态的决定以预定时间段的期满为基础，设备602能够在用户190不再存在于设备前方时或者用户不再关注于设备时被切换至低功率状态。因此，如相机106或用户识别器108或关注监视器608所确定的，当用户190返回设备时或者再次关注于设备602时，该设备能够从低功率状态切换至高功率状态。

[0116] 通过使得从高功率到低功率状态的变化以用户消失或缺少关注度的自动检测为条件，能够当用户190实际上未在使用设备602时的适当时刻将设备602切换至低功率状态，而不是以预定超时的期满为条件。预定超时时段有时可以对应于用户仍然在使用设备的时间，因此干扰到用户体验，并且在其它时候可能对应于用户已经停止使用设备之后很久的时间，因此浪费能量或电池寿命。因此，基于用户消失或缺少关注度的自动检测而将设备

602自动从高功率状态切换至低功率状态，用户可以导致设备602的更高能量效率。

[0117] 类似地，使用相机106、用户识别器108和关注监视器608所提供的面部识别技术将设备602自动从低功率状态变换至高功率状态为用户提供了更好的、更无缝的体验，因为用户可以无需输入字母数字信息或者按压设备602的任何键而将设备从低功率状态变换为高功率状态。由于体验对于用户而言是更为无缝的，所以低功率状态和高功率状态之间的变换较少地打扰到用户，并且因此用户会更乐意利用设备602所提供的节能功率管理技术。

[0118] 图7是依据所公开的主题的技术的示例实施方式的流程图。在各个实施方式中，技术800可以被诸如图1、2、3、4、5、6或10的那些系统使用或产生。所要理解的是，所公开的主题并不局限于技术800所图示的动作的顺序或数量。

[0119] 在一个实施方式中，如以上所描述的，框702图示了能够经由与计算设备操作地耦合的相机接收第一用户的图像。在一个实施方式中，框704图示了能够基于所接收的图像确定第一用户的身份。在一个实施方式中，框706图示了如果所确定的身份与预定身份相匹配，则第一用户能够至少基于第一用户的身份与预定身份相匹配来登录到计算设备中。

[0120] 图8示出了可被用来与这里所描述的技术一起使用的通用计算机设备800和通用移动计算机设备850的示例。计算设备800意在表示各种形式的数字计算机，诸如膝上计算机、台式机、工作站、个人数字助理、服务器、刀片服务器、主机和其它适当计算机。计算设备850意在表示各种形式的移动设备，诸如个人数字助理、蜂窝电话、智能电话和其它类似的计算设备。这里所示出的组件、其连接和关系以及其功能仅意在是示范性的，而非意在对本文档中所描述和/或要求保护的发明的实施方式进行限制。

[0121] 计算设备800包括处理器802、存储器804、存储设备806、连接到存储器804和高速扩展端口810的高速接口808、以及连接到低速总线814和存储设备806的低速接口812。每个组件802、804、806、808、810和812使用各种总线互连，并且可以安装在共用主板上，或者以其它适宜方式进行安装。处理器802能够处理用于在计算设备800内执行的指令以在诸如耦合到高速接口808的显示器816的外部输入/输出设备上显示用于GUI的图形信息，所述指令包括存储在存储器804中或者存储设备806中的指令。在其它实施方式中，如果适宜，可使用多个处理器和/或多个总线，以及多个存储器和存储器类型。而且，可以连接多个计算设备800，每个设备提供必要操作的一部分(例如，作为服务器组、刀片服务器组或多处理器系统)。

[0122] 存储器804存储计算设备800内的信息。在一个实施方式中，存储器804是一个或多个易失性存储单元。在另一个实施方式中，存储器804是一个或多个非易失性存储单元。存储器804还可以是其它形式的计算机可读介质，诸如磁盘或光盘。

[0123] 存储设备806能够为计算设备800提供大容量存储。在一个实施方式中，存储设备806可以是或者可包含计算机可读介质，诸如软盘设备、硬盘设备、光盘设备、磁带设备、闪存或其它类似固态存储设备、或者设备阵列，包括存储域网络或其它配置中的设备。计算机程序产品可有形地实现在信息载体中。所述计算机程序产品还可包含指令，当被执行时，所述指令执行诸如以上所描述的一个或多个方法。所述信息载体是计算机或机器可读介质，诸如存储器804、存储设备806或处理器802上的存储器。

[0124] 高速控制器808管理用于计算设备800的带宽密集操作，而低速控制器812管理较低带宽密集的操作。这样的功能分配仅是示例性的。在一个实施方式中，高速控制器808耦

合到存储器804、显示器816(例如,通过图形处理器或加速器)、以及耦合到可接受各种扩展卡(未示出)的高速扩展端口810。在所述实施方式中,低速控制器812耦合到存储设备806和低速扩展端口814。可以包括各种通信端口(例如,USB、蓝牙、以太网、无线以太网)的低速控制端口814可耦合到一个或多个输入/输出设备,诸如键盘、指示设备、扫描仪、或者例如通过网络适配器的诸如交换机和路由器之类的联网设备。

[0125] 如图所示,计算设备800可以以各种不同形式来实现。例如,其可以被实现为标准服务器820,或者更多时间在这样的服务器组中。其还可以被实现为机架式服务器系统824的一部分。此外,其还可以在诸如膝上计算机822的个人计算机中实施。替选地,来自计算设备800的组件可以与诸如设备850的移动设备(未示出)中的其它组件相结合。每个这样的设备可包含一个或多个计算设备800、850,并且整个系统可由多个彼此通信的计算设备800、850所构成。

[0126] 除其它组件之外,计算设备850包括处理器852、存储器864、诸如显示器854的输入/输出设备、通信接口866和收发器886。设备850还可提供以诸如微驱动器或其它设备的存储设备以提供附加存储。每个组件850、852、864、854、866和868使用各种总线进行互连,并且若干组件可安装在共用主板上或者以其它适宜方式进行安装。

[0127] 处理器852能够执行计算设备850内的指令,包括存储在存储器864中的指令。所述处理器可被实现为包括单独且多个的模拟和数字处理器的芯片的芯片集。例如,所述处理器可提供设备850的其它组件的协同,诸如控制用户接口、设备850所运行的应用以及设备850所进行的无线通信。

[0128] 处理器852可以通过耦合到显示器854的控制接口858和显示接口856与用户进行通信。显示器854例如可以是TFT LCD(薄膜晶体管液晶显示器)显示器或OLED(有机发光二极管)显示器,或者其它适当的显示技术。显示接口856可以包括用于驱动显示器854向用户显示图形和其它信息的适当电路。控制接口858可以从用户接收命令并且对其进行转以便向处理器852提交。此外,可提供与处理器852进行通信的外部接口862,从而使得设备850能够与其它设备进行近域通信。例如,外部接口862在一些实施方式中可提供有线通信,或者在其它实施方式中提供无线通信,并且也可使用多个接口。

[0129] 存储器864存储计算设备850内的信息。存储器864可以被实施为一个或多个计算机可读介质、一个或多个易失性存储器单元或者一个或多个非易失性存储器单元。也以提供扩展存储器874并通过扩展接口872连接到设备850,所述扩展接口872例如可以包括SIMM(单列直插存储器)卡接口。这样的扩展存储器874可为设备850提供额外的存储空间,或者还可以为设备850存储应用或其它信息。特别地,扩展存储器874可以包括指令以执行或补充以上所描述的过程,并且还可以包括安全信息。例如,扩展存储器874可被提供为设备850的安全模块,并且可利用允许对设备850进行安全使用的指令进行编程。此外,可经由SIMM卡提供安全应用程序以及附加信息,诸如以不可破坏的方式在SIMM卡上放置识别信息。

[0130] 例如,如以下所描述的,所述存储器可以包括闪存和/或NVRAM存储器。在一种实施方式中,计算机程序产品有形地实现在信息载体中。所述计算机程序产品还可包含指令,当被执行时,所述指令执行诸如以上所描述的一个或多个方法。所述信息载体是计算机或机器可读介质,诸如存储器864、扩展存储器874、处理器852上的存储器或者可例如在收发器868或外部接口862上接收的传播信号。

[0131] 设备850可通过通信接口866进行无线通信，在必要情况下，所述通信接口866可以包括数字信号处理电路。通信接口866可在各种模式或协议下提供通信，除其它之外，所述模式或协议诸如GSM语音呼叫、SMS、EMS或MMS消息发送、CDMA、TDMA、PDC、WCDMA、CDMA2000或GPRS。例如，这样的通信可通过射频收发器868进行。此外，诸如使用蓝牙、WiFi或其它这样的收发器(未示出)可进行短程通信。此外，GPS(全球定位系统)接收器870可为设备850提供附加的导航和位置相关的无线数据，其可由设备850上运行的应用适当使用。

[0132] 设备850还可以使用音频编解码器860进行可听通信，所述音频编解码器860可以接收来自用户的话音信息并且将其转换为可用的数字信息。音频编解码器860同样可以诸如通过扬声器为用户生成可听声音，例如在设备850的听筒中。这样的声音可以包括来自语音电话呼叫的声音，可以包括录制的声音(例如，语音消息、音乐文件等)，并且还可以包括设备850上运行的应用生成的声音。

[0133] 如图所示，计算设备850可以以多种不同方式来实现。例如，其可以被实现为蜂窝电话880。其还可以被实现为智能电话882、个人数字助理或其它类似移动设备的一部分。

[0134] 这里所描述的系统和技术的各种实施方式可以以数字电子电路、集成电路、专门设计的ASIC(专用集成电路)、计算机硬件、固件、软件和/或其组合来实现。这些各种实施方式可以包括一个或多个计算机程序中的实施方式，所述计算机程序可在包括至少一个可编程处理器的可编程系统上执行和/或解释，所述可编程系统可以为专用或通用目的，其被耦合以从存储系统、至少一个输入设备以及至少一个输出设备接收数据和指令并且向其传送数据和指令。

[0135] 这些计算机程序(也称作程序、软件、软件应用或代码)包括用于可编程处理器的机器指令，并且能够以高级程序和/或面向对象编程语言来实施，和/或以汇编/机器语言来实施。如这里所使用的，术语“机器可读介质”、“计算机可读介质”是指用来向可编程处理器提供机器指令和/或数据的任意计算机程序产品、装置和/或设备(例如，磁盘、光盘、存储器、可编程逻辑设备(PLD))，其包括接收机器指令作为机器可读信号的机器可读介质。术语“机器可读信号”是指被用来为可编程处理器提供机器指令和/或数据的任意信号。

[0136] 为了提供与用户的交互，这里所描述的系统和技术可在具有用于向用户显示信息的显示设备(例如，CRT(阴极射线管)或LCD(液晶显示器)监视器)和用户能够通过其为计算机提供输入的键盘和指示设备(例如，鼠标或轨迹球)的计算机上实施。也可以使用其它类型的设备来提供与用户的交互；例如，提供给用户的反馈可以为任意形式的感知反馈(例如，视觉反馈、听觉反馈或触觉反馈)；并且来自用户的输入可以以任意形式接收，包括声音、话音或触觉输入。

[0137] 这里所描述的系统和技术可在计算系统中实现，所述计算系统包括后端组件(例如，作为数据服务器)，或者其包括中间件组件(例如，应用服务器)，或者其包括前端组件(例如，具有用户能够通过其与这里所描述的系统和技术的实施方式进行交互的图形用户界面或web浏览器的客户端计算机)，或者这样的后端、中间件或前端组件的任意组合。所述系统的组件可通过任意形式或介质的数字数据通信(例如，通信网络)进行互连。通信网络的示例包括局域网(LAN)、广域网(WAN)和互联网。

[0138] 所述计算系统可以包括客户端和服务器。客户端和服务器通常彼此远离并且典型地通过通信网络进行交互。客户端和服务器的关系源自于在相应计算机上运行并且彼此具

有客户端-服务器关系的计算机程序。

[0139] 已经对多个实施例进行了描述。然而将要理解的是，可以进行各种改变而并不背离本发明的精神和范围。

[0140] 此外，图中所描绘的逻辑流程并非要求所示出的特定顺序或者连续顺序才能实现所期望的结果。此外，可以提供其它步骤或者从所描述流程中消除步骤，并且可以向所描述的系统添加其它组件或者从中去除组件。因此，其它实施方式处于所附权利要求的范围内。

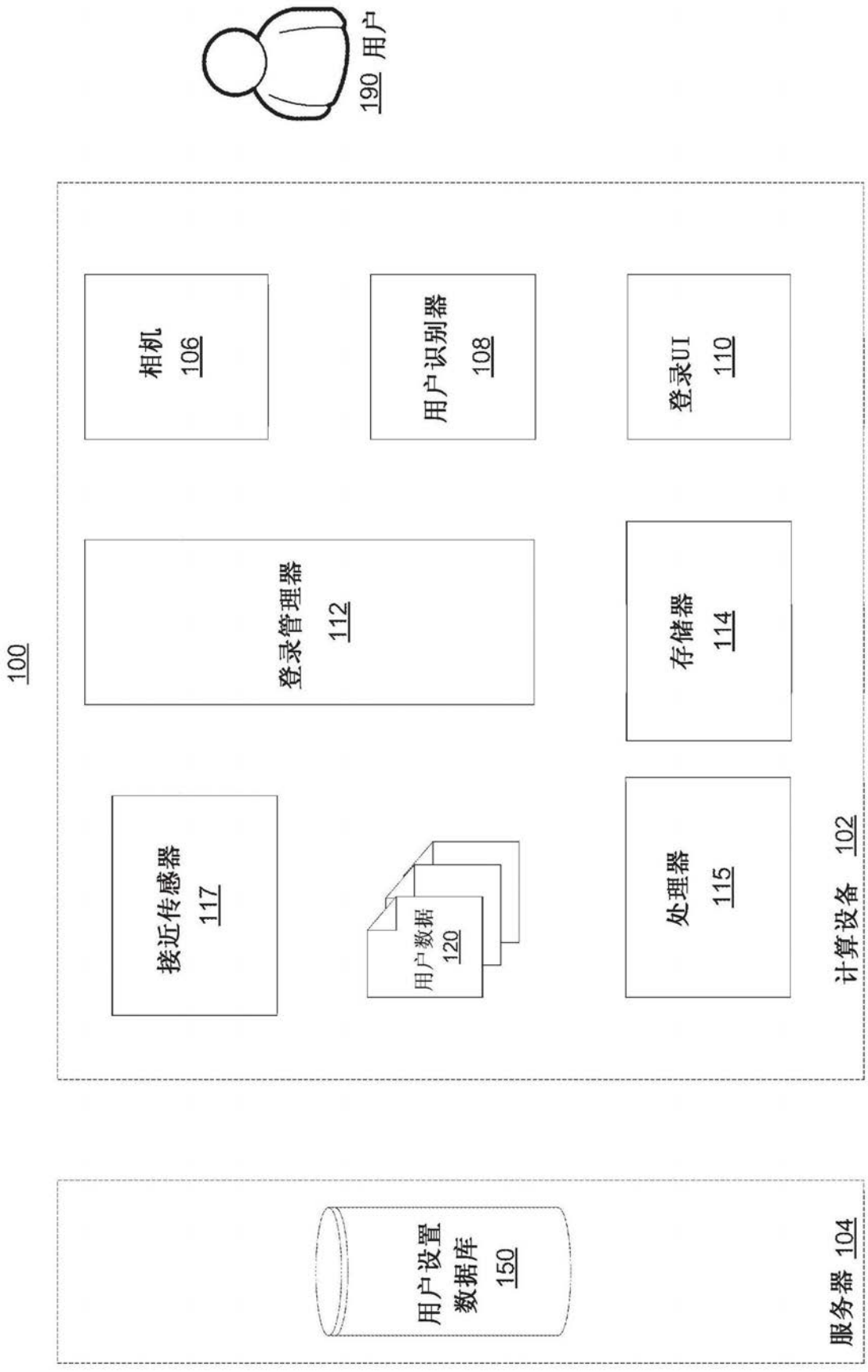

190 用户
100
相机 106
用户识别器 108
登录UI 110
登录管理器 112
存储器 114
接近传感器 117
用户数据 120
处理器 115
计算设备 102
用户设置数据库 150
服务器 104

图1

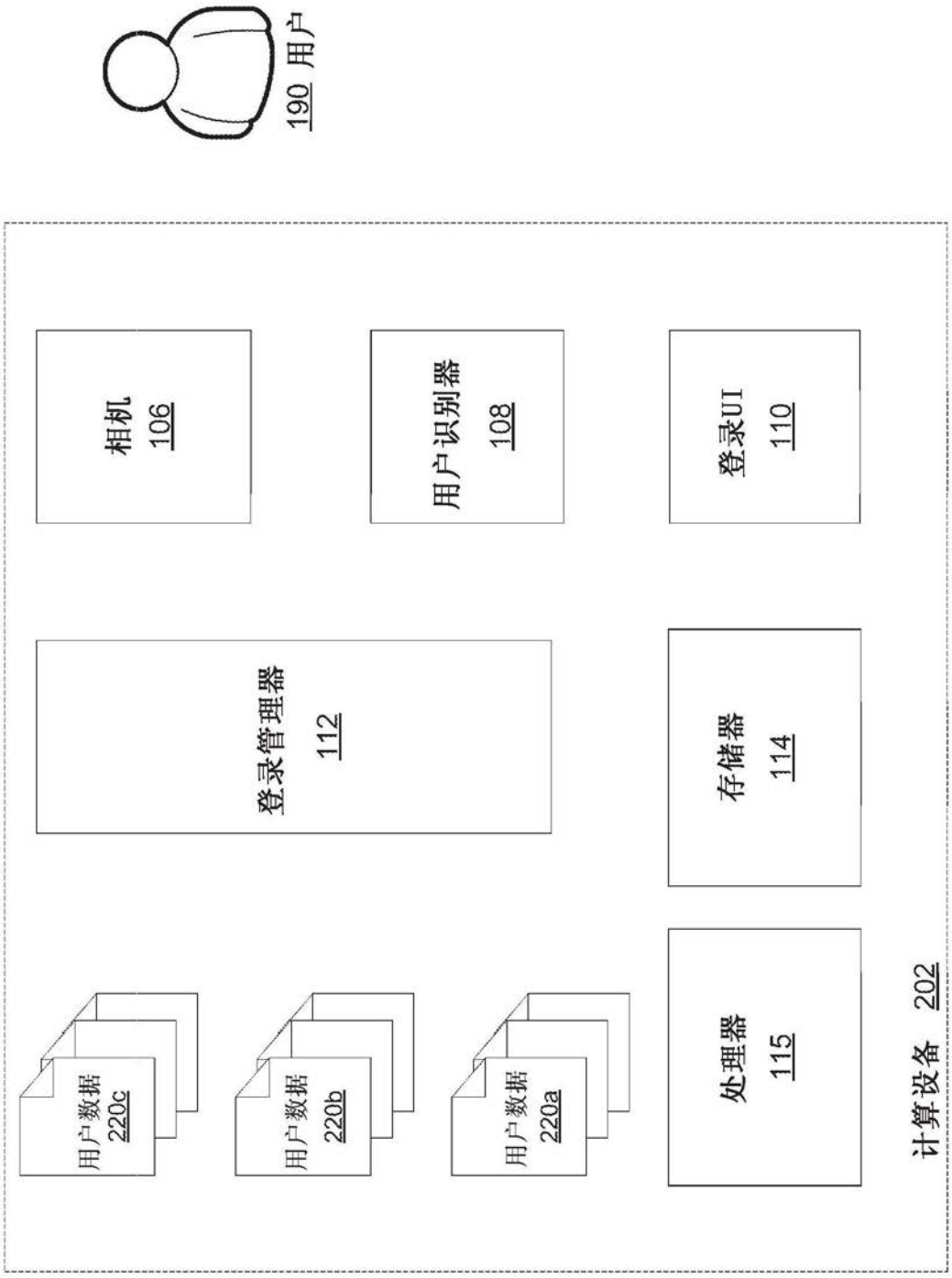

190 用户
相机 106
用户识别器 108
登录UI 110
登录管理器 112
存储器 114
处理器 115
用户数据 220c
用户数据 220b
用户数据 220a
计算设备 202

图2

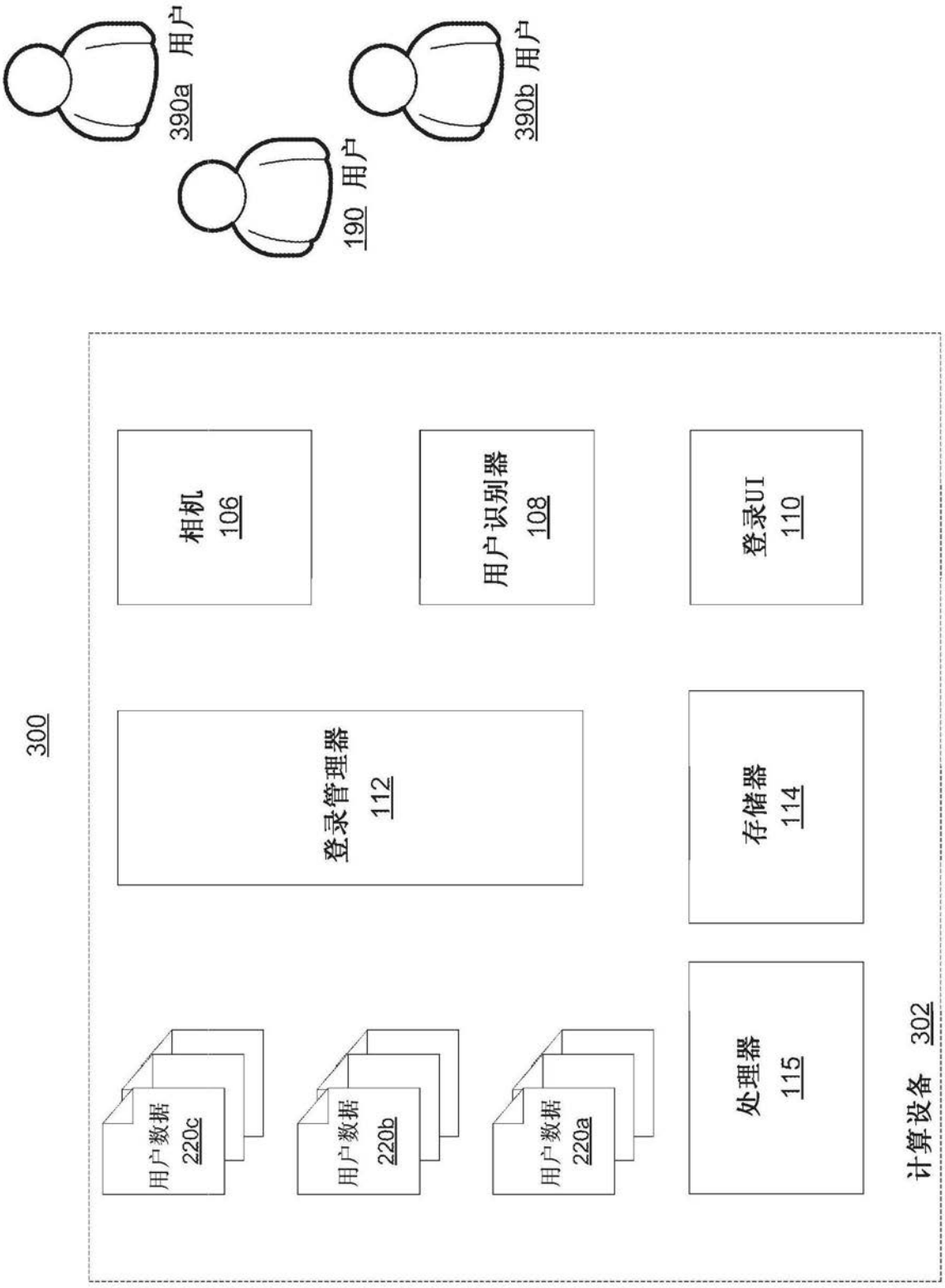

390a 用户
190 用户
390b 用户
300
相机 106
用户识别器 108
登录UI 110
登录管理器 112
存储器 114
处理器 115
用户数据 220c
用户数据 220b
用户数据 220a
计算设备 302

图3

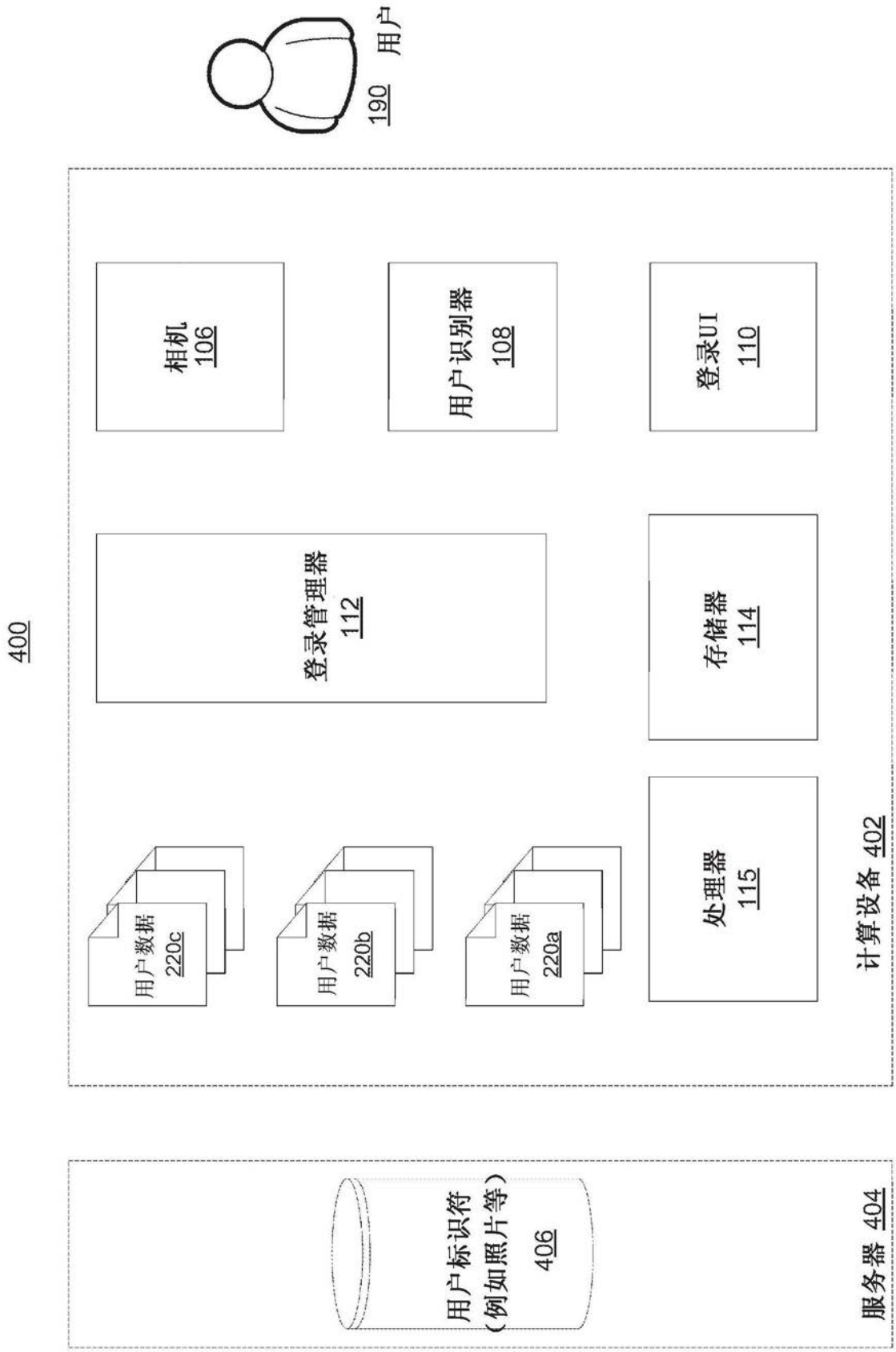

190 用户
400
相机 106
登录管理器 112
用户识别器 108
登录UI 110
存储器 114
处理器 115
用户数据 220c
用户数据 220b
用户数据 220a
计算设备 402
用户标识符（例如照片等） 406
服务器 404

图4

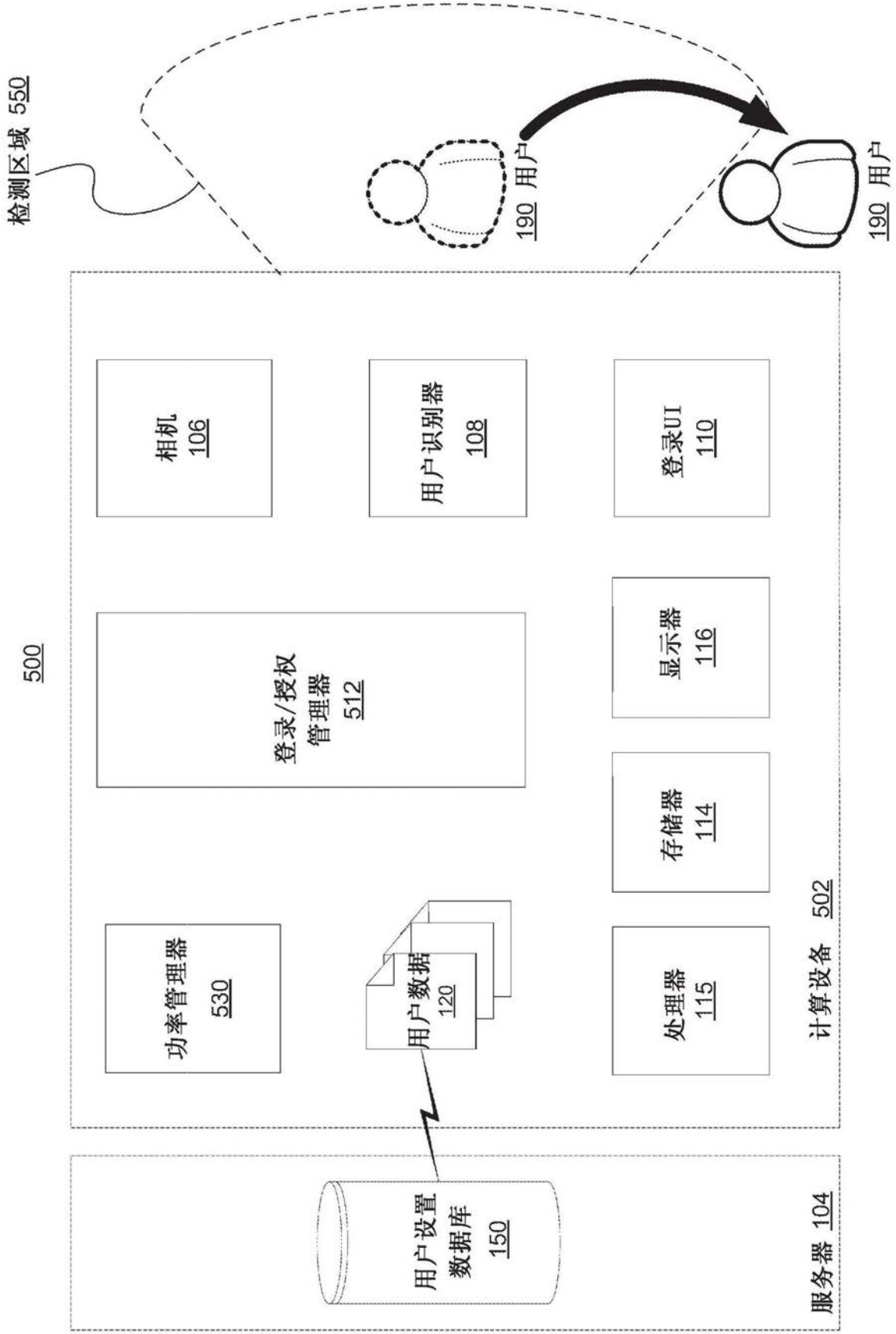

检测区域 550
190 用户
190 用户
500
相机 106
用户识别器 108
登录UI 110
登录/授权管理器 512
显示器 116
存储器 114
功率管理器 530
用户数据 120
处理器 115
计算设备 502
用户设置数据库 150
服务器 104

图5a

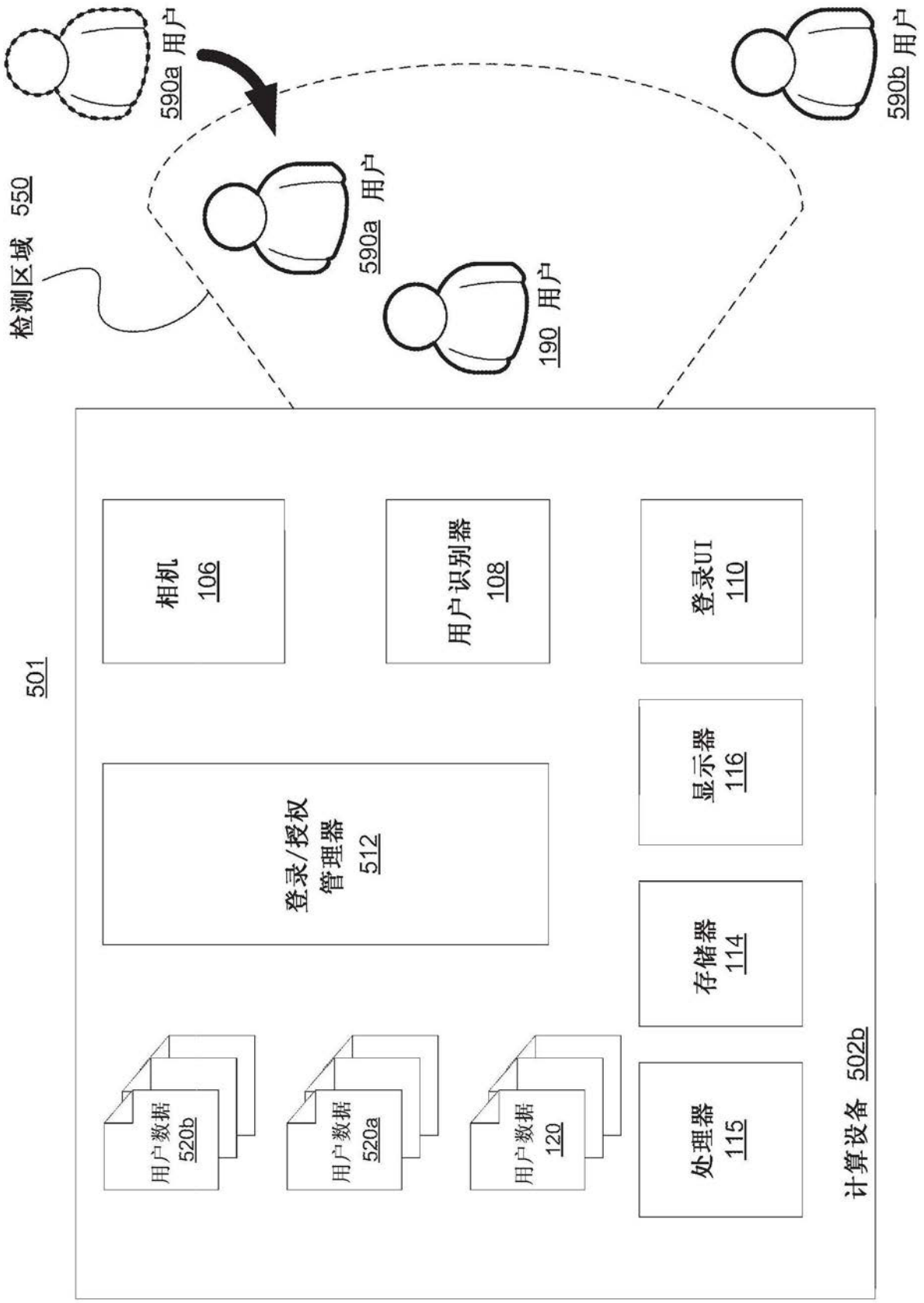

检测区域 550
590a 用户
590a 用户
190 用户
590b 用户
501
相机 106
用户识别器 108
登录UI 110
登录/授权管理器 512
显示器 116
存储器 114
处理器 115
用户数据 520b
用户数据 520a
用户数据 120
计算设备 502b

图5b

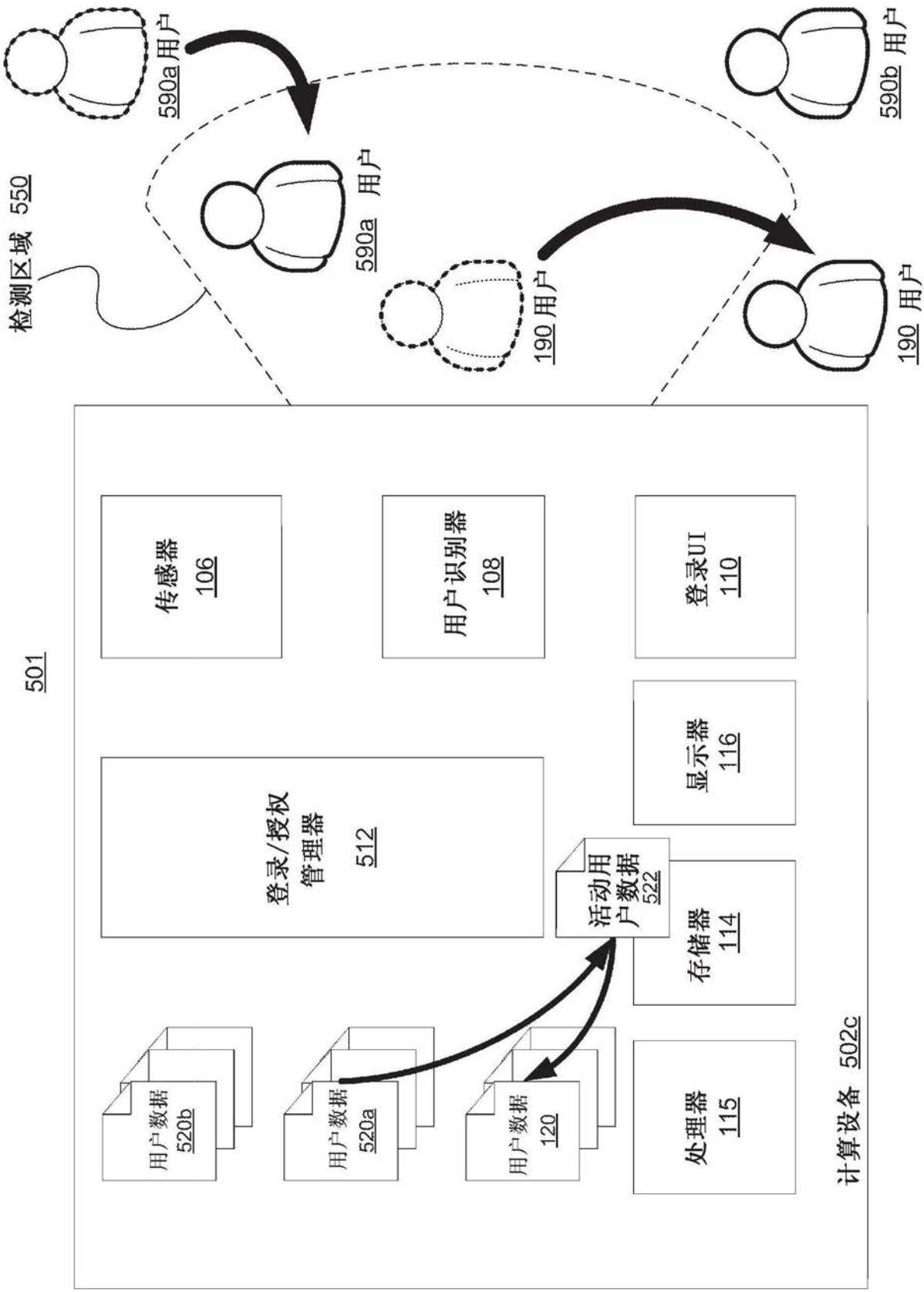

检测区域 550
590a 用户
590a 用户
590b 用户
190 用户
190 用户
501
传感器 106
用户识别器 108
登录UI 110
登录/授权管理器 512
显示器 116
活动用户数据 522
存储器 114
用户数据 520b
用户数据 520a
用户数据 120
处理器 115
计算设备 502c

图5c

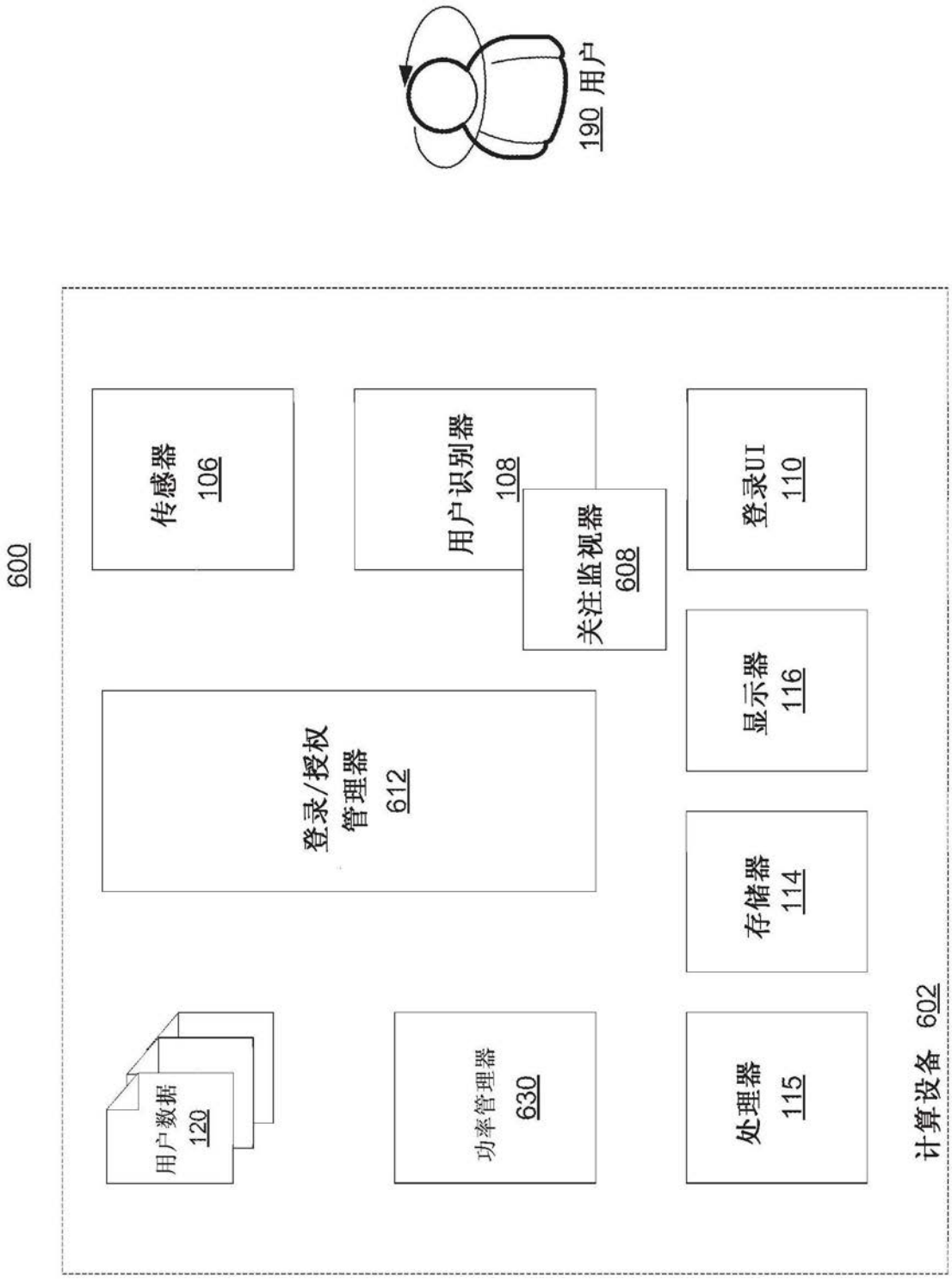

190 用户
600
传感器 106
用户识别器 108
关注监视器 608
登录UI 110
登录/授权管理器 612
显示器 116
存储器 114
用户数据 120
功率管理器 630
处理器 115
计算设备 602

图6

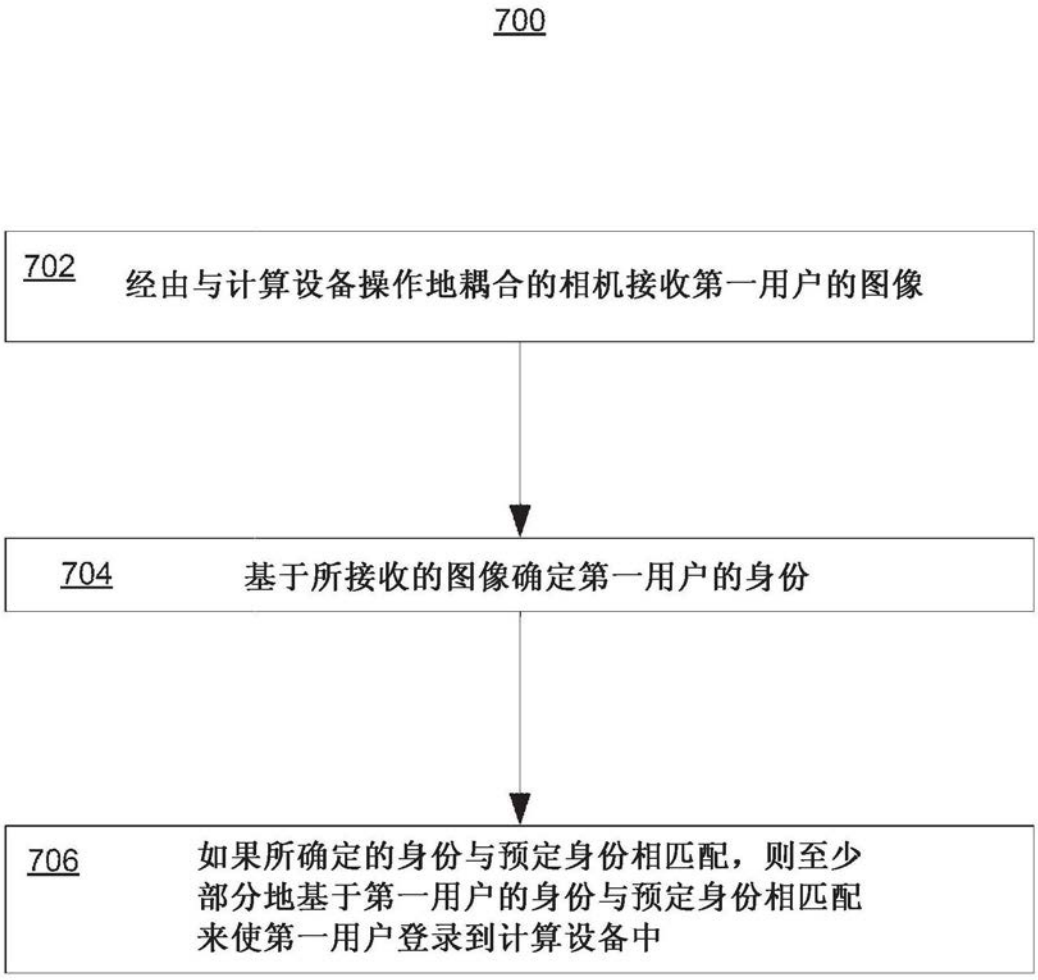

700
702
经由与计算设备操作地耦合的相机接收第一用户的图像
704
基于所接收的图像确定第一用户的身份
706
如果所确定的身份与预定身份相匹配，则至少部分地基于第一用户的身份与预定身份相匹配来使第一用户登录到计算设备中

图7

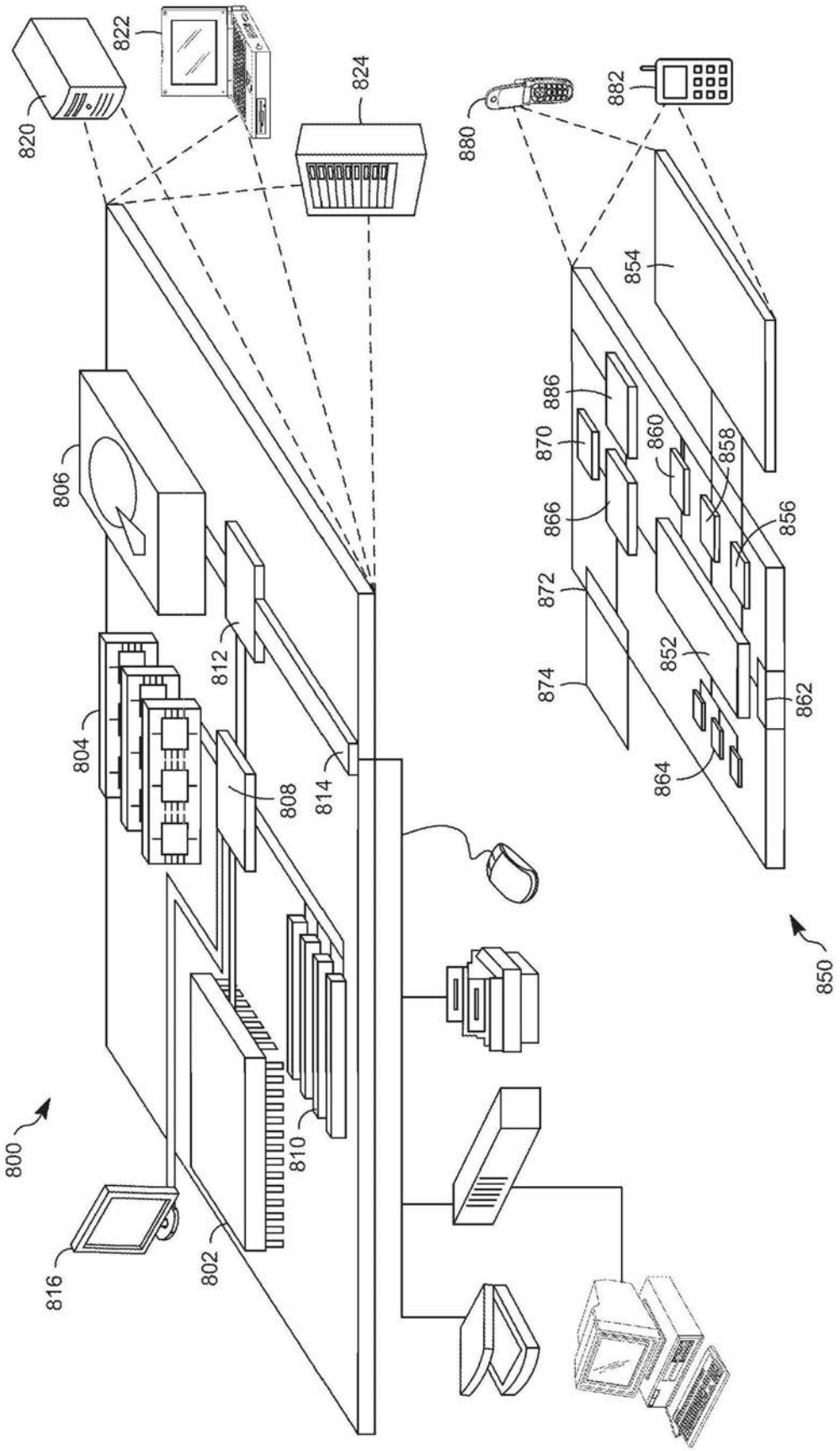

820
822
824
880
882
854
886
870
860
858
866
856
872
852
874
862
864
850
806
812
804
808
814
800
810
816
802

图8