

人脸解锁及其信息注册方法和装置、设备、介质

本公开要求在 2017 年 09 月 07 日提交中国专利局、申请号为 CN201710802146.1、发明名称为“人脸解锁及其信息注册方法和装置、设备、程序、介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本公开涉及人工智能技术，尤其是一种人脸解锁及其信息注册方法和装置、设备、程序、介质。

背景技术

在信息化时代，各种终端应用（APP）层出不穷，每个用户使用各种应用时，都需要注册用户信息以保留和保护用户数据。另外，随着互联网技术的发展，终端设备可以为用户提供越来越多的功能，例如通信、照片存储、安装各种应用等，很多用户会对自己的终端设备进行锁定以防其中的用户数据泄漏。因此，保护终端设备中的应用中的私密数据逐渐成为关注焦点。

随着人工智能技术的发展，计算机视觉技术已在安全监控、金融、乃至无人驾驶等领域都具有巨大的应用价值。

发明内容

本公开实施例提供一种人脸解锁的技术方案。

根据本公开实施例的一个方面，提供一种人脸解锁方法，包括：

对图像进行人脸检测；

对检测到人脸的图像进行人脸特征提取；

基于存储的人脸特征对提取到的人脸特征进行认证；其中，所述存储的人脸特征至少包括对应同一标识 ID 的至少二个不同角度人脸图像的人脸特征；

至少响应于所述提取到的人脸特征通过认证，进行解锁操作。

根据本公开实施例的另一个方面，提供一种人脸解锁信息注册方法，包括：

输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息；

对获取到的图像进行人脸检测；

对检测到各角度人脸的图像进行人脸特征提取；

存储提取到的各角度人脸图像的人脸特征、以及所述各角度人脸图像的人脸特征与所述同一 ID 之间的对应关系。

根据本公开实施例的又一个方面，提供一种人脸解锁装置，包括：

人脸检测模块，用于对图像进行人脸检测；

特征提取模块，用于对检测到人脸的图像进行人脸特征提取；

认证模块，用于基于存储的人脸特征对提取到的人脸特征进行认证；其中，所述存储的人脸特征至少包括对应同一标识 ID 的至少二个不同角度人脸图像的人脸特征；

控制模块，用于至少响应于所述提取到的人脸特征通过认证，进行解锁操作。

根据本公开实施例的再一个方面，提供一种电子设备，包括：

处理器和本公开任一实施例所述的人脸解锁装置；

在处理器运行所述认证装置时，本公开任一实施例所述的人脸解锁装置中的单元被运行。

根据本公开实施例的再一个方面，提供一种电子设备，包括：

存储器，存储可执行指令；

一个或多个处理器，与存储器通信以执行可执行指令从而完成本公开任一实施例所述方法中各步骤的操作。

根据本公开实施例的再一个方面，提供一种计算机程序，包括计算机可读代码，当所述计算机可读代码在设备上运行时，所述设备中的处理器执行用于实现本公开任一实施例所述方法中各步骤的指令。

根据本公开实施例的再一个方面，提供一种计算机可读介质，用于存储计算机可读的指令，所述指令被执行时实现本公开任一实施例所述方法中各步骤的操作。

基于本公开上述实施例提供的人脸解锁及其信息注册方法和装置、设备、介质，可以通过注册流程预先存储对应同一 ID 的至少二个不同角度人脸图像的人脸特征，进行人脸解锁时，对图像进行人脸检测，对检测到人脸的图像进行人脸特征提取，并基于存储的人脸特征对该提取到的人脸特征进行认证，

在该提取到的人脸特征通过认证后，进行解锁操作，从而实现了基于人脸的认证解锁，本公开实施例的解锁方式操作简单，便利性较高，且安全性较高；并且，由于本公开实施例通过注册流程预先存储对应同一 ID 的至少二个不同角度人脸图像的人脸特征，可以在获取到上述同一 ID 对应用户与存储的人脸特征对应的任一角度人脸图像时，均可成功实现基于该用户的人脸解锁，提高了人脸解锁的成功率，降低了由于同一用户认证时人脸角度与注册时人脸角度的差异而导致认证失败的可能性。

下面通过附图和实施例，对本公开的技术方案做进一步的详细描述。

附图说明

构成说明书的一部分的附图描述了本公开的实施例，并且连同描述一起用于解释本公开的原理。

参照附图，根据下面的详细描述，可以更加清楚地理解本公开，其中：

图 1 为本公开人脸解锁方法一个实施例的流程图。

图 2 为本公开人脸解锁方法另一个实施例的流程图。

图 3 为本公开人脸解锁方法又一个实施例的流程图。

图 4 为本公开人脸解锁信息注册方法一个实施例的流程图。

图 5 为本公开人脸解锁信息注册方法另一个实施例的流程图。

图 6 为本公开人脸解锁信息注册方法又一个实施例的流程图。

图 7 为本公开人脸解锁信息注册方法再一个实施例的流程图。

图 8 为本公开人脸解锁装置一个实施例的结构示意图。

图 9 为本公开人脸解锁装置另一个实施例的结构示意图。

图 10 为本公开电子设备一个实施例的结构示意图。

具体实施方式

现在将参照附图来详细描述本公开的各种示例性实施方式。应注意到：除非另外可选说明，否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本公开的范围。

以下对至少一个示例性实施方式的描述实际上仅仅是说明性的，决不作为对本公开及其应用或使用的任何限制。

对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为说明书的一部分。

应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步讨论。

本公开实施例可以应用于终端设备、计算机系统、服务器等电子设备，其可与众多其它通用或专用计算系统环境或配置一起操作。适于与终端设备、计算机系统、服务器等电子设备一起使用的众所周知的终端设备、计算系统、环境和/或配置的例子包括但不限于：个人计算机系统、服务器计算机系统、瘦客户机、厚客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任何系统的分布式云计算技术环境，等等。

终端设备、计算机系统、服务器等电子设备可以在由计算机系统执行的计算机系统可执行指令（诸如程序模块）的一般语境下描述。通常，程序模块可以包括例程、程序、目标程序、组件、逻辑、数据结构等等，它们执行特定的任务或者实现特定的抽象数据类型。计算机系统/服务器可以在分布式云计算环境中实施，分布式云计算环境中，任务是由通过通信网络链接的远程处理设备执行的。在分布式云计算环境中，程序模块可以位于包括存储设备的本地或远程计算系统存储介质上。

图 1 为本公开人脸解锁方法一个实施例的流程图。如图 1 所示，该实施例的人脸解锁方法包括：

102，对图像进行人脸检测。

在一个可选示例中，该操作 102 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的人脸检测模块执行。

104，对检测到人脸的图像进行人脸特征提取。

在一个可选示例中，该操作 104 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的特征提取模块执行。

106，基于存储的人脸特征对提取到的人脸特征进行认证。

其中，本公开各实施例中，存储的人脸特征至少包括对应同一标识（ID）的至少二个不同角度人脸图像的人脸特征。其中的 ID 表示对应于存储人脸特征的用户信息，例如可以是用户姓名、编号、昵称等。

在本公开各实施例的一个可选示例中，上述对应同一 ID 的至少二个不同角度人脸图像例如可以包

包括但不限于对应上述同一 ID 的以下二个或二个以上角度的人脸图像：正面的人脸图像，仰头的人脸图像，低头的人脸图像，左转头的人脸图像，右转头的人脸图像，等等。

在一个可选示例中，该操作 106 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的认证模块执行。

108，至少响应于提取到的人脸特征通过认证，进行解锁操作。

在一个可选示例中，该操作 108 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的控制模块执行。

基于本公开上述实施例提供的人脸解锁方法，可以通过注册流程预先存储对应同一 ID 的至少二个不同角度人脸图像的人脸特征，进行人脸解锁时，对图像进行人脸检测，对检测到人脸的图像进行人脸特征提取，并基于存储的人脸特征对该提取到的人脸特征进行认证，在该提取到的人脸特征通过认证后，进行解锁操作，从而实现了基于人脸的认证解锁，本公开实施例的解锁方式操作简单，便利性较高，且安全性较高；并且，由于本公开实施例通过注册流程预先存储对应同一 ID 的至少二个不同角度人脸图像的人脸特征，可以在获取到上述同一 ID 对应用户与存储的人脸特征对应的任一角度人脸图像时，均可成功实现基于该用户的人脸解锁，提高了人脸解锁的成功率，降低了由于同一用户认证时人脸角度与注册时人脸角度的差异而导致认证失败的可能性。

在本公开人脸解锁方法各实施例的一个可选示例中，操作 108 中基于存储的人脸特征对提取到的人脸特征进行认证，可以通过如下方式实现：

获取提取到的人脸特征与至少一个存储的人脸特征之间的相似度；

响应于提取到的人脸特征与任一存储的人脸特征之间的相似度大于设定阈值，确定提取到的人脸特征通过认证。

否则，若提取到的人脸特征与存储的所有角度的人脸特征之间的相似度均不大于设定阈值，则确定提取到的人脸特征未通过认证。

基于本实施例，可以逐一比对提取到的人脸特征与存储的各角度的人脸特征之间的相似度，只要提取到的人脸特征与存储的任一角度的人脸特征之间的相似度大于设定阈值，即可确定提取到的人脸特征通过认证，即：本实施例可能只比对提取到的人脸特征与存储的一个角度或部分角度的人脸特征之间的相似度便可确定提取到的人脸特征通过认证，便无需再比对提取到的人脸特征与存储的其余角度的人脸特征之间的相似度，从而有利于提升认证效率。

或者，在本公开人脸解锁方法各实施例的另一个可选示例中，操作 108 中基于存储的人脸特征对提取到的人脸特征进行认证，还可以通过如下方式实现：

分别获取提取到的人脸特征与多个存储的人脸特征之间的相似度；

响应于提取到的人脸特征与多个存储的人脸特征之间的多个相似度中的最大值大于设定阈值，确定提取到的人脸特征通过认证。

其中，上述多个存储的人脸特征可以是存储的所有角度的人脸特征或者其中部分角度的人脸特征。上述多个存储的人脸特征是存储的部分角度的人脸特征时，在提取到的人脸特征与该部分角度的人脸特征之间的多个相似度中的最大值大于设定阈值时，即可确定提取到的人脸特征通过认证，便无需再比对提取到的人脸特征与其余角度的人脸特征之间的相似度，从而有利于提升认证效率。在提取到的人脸特征与该部分角度的人脸特征之间的多个相似度中的最大值不大于设定阈值时，确定提取到的人脸特征未通过认证，可以从存储其余角度的人脸特征中再选取多个角度的人脸特征，采取类似方式，获取再选取的多个角度的人脸特征与该提取到的人脸特征之间的多个相似度中的最大值大于设定阈值，直至获取到的多个相似度中的最大值大于设定阈值，确定提取到的人脸特征通过认证，或者完成提取到的人脸特征与存储的所有角度的人脸特征之间的相似度的比对，均不存在最大值大于设定阈值的相似度，则确定提取到的人脸特征未通过认证。

图 2 为本公开人脸解锁方法另一个实施例的流程图。如图 2 所示，该实施例的人脸解锁方法包括：202，获取图像。

在一个可选示例中，该操作 202 可以由处理器调用摄像头执行，也可以由被处理器运行的一个接收模块执行。

204，对获取到的图像进行光线均衡调整处理。

在本公开各实施例的一个可选示例中，可以直接执行该操作 204，对获取到的图像进行光线均衡调整处理。

或者，在本公开各实施例的另一个可选示例中，也可以在该操作 204 之前，先确定获取到的图像的质量是否满足预定的人脸检测条件，在图像的质量不满足预定的人脸检测条件时再执行该操作 204，对图像进行光线均衡调整处理，而对于质量满足预定的人脸检测条件的图像不再执行操作 204、而直接通

过操作 206 对图像进行人脸检测,该实施例可以对质量满足预定的人脸检测条件的图像不再执行光线均衡调整处理操作,从而有利于提升人脸解锁的效率。

其中,预定的人脸检测条件例如可以包括但不限于以下至少一项:图像的像素值分布不符合预设分布范围,图像的属性值不在预设数值范围内,等等。其中,图像的属性值例如图像的色度、亮度、对比度和饱和度等属性值。

在一个可选示例中,该操作 204 可以由处理器调用存储器存储的相应指令执行,也可以由被处理器运行的光线处理模块执行。

206,对光线均衡调整处理后的图像进行人脸检测。

本公开各实施例中,若从图像中未检测到人脸,可以选择性地返回执行操作 202,即继续执行获取图像的操作。若从图像中未检测到人脸,执行操作 208。

在一个可选示例中,该操作 206 可以由处理器调用存储器存储的相应指令执行,也可以由被处理器运行的人脸检测模块执行。

208,对检测到人脸的图像进行人脸进行特征提取。

在一个可选示例中,该操作 208 可以由处理器调用存储器存储的相应指令执行,也可以由被处理器运行的特征提取模块执行。

210,基于存储的人脸特征对提取到的人脸特征进行认证。

其中,本公开各实施例中,存储的人脸特征至少包括对应同一 ID 的至少二个不同角度人脸图像的人脸特征。

在一个可选示例中,该操作 210 可以由处理器调用存储器存储的相应指令执行,也可以由被处理器运行的认证模块执行。

212,至少响应于提取到的人脸特征通过认证,进行解锁操作。

在基于本实施例的一个可选实施例中,若提取到的人脸特征通过认证,还可以获取该提取的人脸特征对应的 ID 并显示,以使用户知晓当前通过认证的用户信息。

若提取到的人脸特征未通过认证,不执行解锁操作。或者,在本公开人脸解锁方法的一个可选实施例中,也可以输出人脸解锁失败的提示消息。

在一个可选示例中,该操作 212 可以由处理器调用存储器存储的相应指令执行,也可以由被处理器运行的控制模块执行。

在实际情况中,经常会遇到逆光、强光、暗光等复杂场景,例如夜晚在外背后射来灯光或是室内光线昏暗等情况,此时对拍摄到的图像中人脸进行检测,背景过于突出而引起人脸检测的困难,或者即使检测到人脸,从图像中提取的人脸特征非常模糊。相比于一般场景的人脸检测,暗光场景的像素值集中在较低的数值区域,纹理梯度较小,图像整体的信息特征都十分模糊,要检测出有效信息尤其是人脸比较困难;而逆光、强光场景相对于一般场景而言,虽然整体亮度差不多,但是由于背景光线非常亮,导致人脸部分的轮廓和细节纹理等都十分模糊,从而导致人脸特征提取具有较高的难度。

本公开人通过研究发现,对于逆光、强光、暗光等复杂光照场景,这些场景的图像中,其像素值分布往往会有有一定的局域性不符合预设分布范围,和/或图像的属性值不在预设数值范围内。例如在暗光场景中,像素值往往都集中在较低数值的区域,此时图像的对比度、色度等都会很低,检测器很难处理这些图像中的人脸或是会产生误报的情况。

在图 2 所示实施例的一个可选示例中,操作 204 中,对获取到的图像进行光线均衡调整处理,可以包括:获取图像的灰度图;至少对该图像的灰度图进行直方图均衡化处理,使图像的灰度图的像素值分布能够均匀的扩展到整个像素值空间,同时保留原图像像素值的相对分布,以便对经过直方图均衡化处理的图像的灰度图执行后续操作。

在图 2 所示实施例的另一个可选示例中,操作 204 中,对获取到的图像进行光线均衡调整处理,可以包括:至少对图像进行图像光照变换,以将图像变换为满足预设光照条件的图像。

本公开实施例的一个可选示例中,对获取到的图像的质量进行检测,在图像的质量不满足预定的人脸检测条件时,例如在图像的亮度不满足预设亮度条件时,对图像的灰度图进行直方图均衡化处理,即:首先对图像的灰度图在像素值上进行直方图均衡化,使图像的灰度图的像素值分布能够均匀的扩展到整个像素值空间,同时保留原图像像素值的相对分布,对经过直方图均衡化处理的图像再进行人脸检测,进行过直方图均衡化处理的图像的灰度图中特征更加明显,纹理更加清晰而易于检测人脸;或者,对图像进行图像光照变换,将图像变换为满足预设光照条件的图像,再进行人脸检测,从而易于检测人脸。本公开实施例遇到暗光、逆光等极端的光照条件下,依然能够较为准确地检测到图像中的人脸,尤其对于实际场景中那些室内或是夜晚光照非常暗几乎接近全黑的情况,或是在夜晚背景光照强烈,人脸昏暗纹理模糊的情况下也都能够检测出人脸,从而使得本公开可以更好的实现人脸解锁应用。

另外，在基于本公开上述各实施例的人脸解锁方法的又一个实施例中，还可以包括：对获取到的图像进行活体检测。相应地，在该实施例中，响应于提取到的人脸特征通过认证、且该图像通过活体检测，进行解锁操作。

示例性地，本公开各实施例的人脸解锁方法中，可以在获取图像之后，对图像进行活体检测；或者，也可以响应于从图像中检测到人脸，对该检测到人脸的图像进行活体检测；或者，还可以响应于提取到的人脸特征通过认证，对提取到的人脸特征通过认证的图像进行活体检测。

在本公开各实施例的一个可选示例中，对图像进行活体检测，可以包括：

利用神经网络，对图像进行图像特征提取，检测提取的图像特征是否包含至少一种伪造线索信息；基于该至少一种伪造线索信息的检测结果，确定图像是否通过活体检测。若提取的图像特征未包含任何一种伪造线索信息，该图像通过活体检测；否则，若提取的图像特征包含任何一种或多种伪造线索信息，该图像未通过活体检测。

示例性地，本公开各实施例中的图像特征，例如可以包括但不限于以下任意一项或多项：局部二值模式（LBP）特征、稀疏编码的柱状图（HSC）特征、全景图（LARGE）特征、人脸图（SMALL）特征、人脸细节图（TINY）特征。实际应用中，可以根据可能出现的伪造线索信息对需要提取的图像特征包括的特征项进行更新。

其中，通过 LBP 特征，可以突出待检测图像中的边缘信息；通过 HSC 特征，可以更明显的反映待检测图像中的反光与模糊信息；LARGE 特征是全景图特征，基于 LARGE 特征，可以提取到待检测图像中最明显的伪造线索（hack）；人脸图（SMALL）是待检测图像中人脸框若干倍大小（例如 1.5 倍大小）的区域切图，包含人脸、人脸与背景切合的部分，基于 SMALL 特征，可以提取到反光、翻拍设备屏幕摩尔纹与模特或者面具的边缘等伪造线索；人脸细节图（TINY）是取人脸框大小的区域切图，包含人脸，基于 TINY 特征，可以提取到图像 PS（photoshop 编辑）、翻拍屏幕摩尔纹与模特或者面具的纹理等伪造线索。上述各项特征中包含的伪造人脸的伪造线索，可以预先通过训练神经网络，被神经网络学习到，之后包含这些伪造线索的图像输入神经网络后均会被检测出来，就可以判断该图像是伪造人脸图像，否则为真实人脸图像，从而实现人脸的活体检测。

示例性地，本公开实施例中的上述至少一种伪造线索信息，例如可以包括但不限于以下任意一项或多项：2D 类伪造线索信息、2.5D 类伪造线索信息和 3D 类伪造线索信息，可选可以根据可能出现的伪造线索信息对该多个维度伪造线索信息进行更新。

本公开实施例中的伪造线索信息能被人眼观测到。伪造线索信息的维度可以划分为 2D 类、2.5D 类和 3D 类伪造线索。其中，2D 类伪造人脸指的是纸质类材料打印出的人脸图像，该 2D 类伪造线索信息一般包含纸质人脸的边缘、纸张材质、纸面反光、纸张边缘等伪造信息。2.5D 类伪造人脸指的是视频翻拍设备等载体设备承载的人脸图像，该 2.5D 类伪造线索信息一般包含视频翻拍设备等载体设备的屏幕摩尔纹、屏幕反光、屏幕边缘等伪造信息。3D 类伪造人脸指的是真实存在的伪造人脸，例如面具、模特、雕塑、3D 打印等，该 3D 类伪造人脸同样具备相应的伪造信息，例如面具的缝合处、模特的较为抽象或过于光滑的皮肤等伪造信息。

基于本公开上述实施例，可以从多个维度来检测图像是否伪造人脸图像，可以检测出不同维度、各种类型的伪造人脸图像，提高了伪造人脸检测的精确度，有效避免了活体检测过程中不法分子利用待验证用户的照片或视频进行伪造攻击；此外，通过神经网络进行人脸防伪检测，可以针对各种伪造人脸方式的伪造线索信息进行训练学习，在出现新的伪造人脸方式时，基于新的伪造线索信息对神经网络进行训练、微调即可快速更新神经网络，而无需改进硬件结构，从而可以快速有效的响应新的人脸防伪检测需求。

图 3 为本公开人脸解锁方法又一个实施例的流程图。本公开实施例中，以在获取图像之后对图像进行活体检测为例对本公开实施例进行说明，本领域技术人员根据本公开的记载可以知晓，响应于从图像中检测到人脸，对该检测到人脸的图像进行活体检测的实现方案；以及响应于提取到的人脸特征通过认证，对提取到的人脸特征通过认证的图像进行活体检测的实现方案，此处不再赘述。如图 3 所示，该实施例的人脸解锁方法包括：

302，获取图像。

之后分别执行操作 304 和 308。

在一个可选示例中，该操作 302 可以由处理器调用摄像头执行，也可以由被处理器运行的一个接收模块执行。

304，识别获取到的图像是否满足预设质量要求。

其中，可以预先设置质量要求的标准，以选取高质量的图像进行活体检测。其中的质量要求的标准例如可以包括以下任意一项或多项：人脸朝向是否正面朝向、图像清晰度的高低、曝光度高低等，依据

相应的标准选取综合质量较高的图像进行活体检测。

响应于图像满足预设质量要求, 针对该图像执行操作 306。否则, 响应于图像不满足预设质量要求, 重新执行操作 302 获取图像。

在一个可选示例中, 该操作 304 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的光线处理模块执行。

306, 对获取到的图像进行活体检测。

之后, 执行操作 314。

在一个可选示例中, 该操作 306 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的活体检测模块执行。

308, 对获取到的图像进行人脸检测。

可选地, 该操作 308 可以包括: 在获取到的图像的质量不满足预定的人脸检测条件时, 先对图像进行光线均衡调整处理, 然后再对光线均衡调整处理后的图像进行人脸检测。若获取到的图像的质量满足预定的人脸检测条件时, 可以直接对该图像进行人脸检测。

在一个可选示例中, 该操作 308 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的人脸检测模块执行。

310, 识别是否从图像中检测到人脸。

响应于从图像中检测到人脸, 执行操作 312。否则, 响应于从图像中未检测到人脸, 可以继续执行操作 302, 即重新获取图像并进行后续流程。

在一个可选示例中, 该操作 310 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的人脸检测模块执行。

312, 对检测到人脸的图像进行特征提取, 并基于存储的人脸特征对提取到的人脸特征进行认证。

其中, 本公开各实施例中, 存储的人脸特征至少包括对应同一 ID 的至少二个不同角度人脸图像的人脸特征。

在一个可选示例中, 该操作 312 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的特征提取模块执行。

314, 确定提取到的人脸特征是否通过认证, 以及获取到的图像是否通过活体检测。

响应于提取到的人脸特征通过认证、且获取到的图像通过活体检测, 执行操作 316。否则, 响应于提取到的人脸特征未通过认证和/或获取到的图像未通过活体检测, 不执行本实施例的后续流程, 或者, 可选地执行操作 318。

在一个可选示例中, 该操作 314 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的认证模块执行。

316, 进行解锁操作。

可选地, 在本公开另一实施例中, 响应于提取到的人脸特征通过认证, 还可以从预先存储的对应关系中获取该通过认证的人脸特征对应的 ID 并显示。

在一个可选示例中, 该操作 316 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的控制模块执行。

之后, 不执行本实施例的后续流程。

318, 输出认证失败的提示消息和/或者认证失败原因提示消息。

其中, 认证失败原因例如可以是未检测到人脸、人脸特征未通过认证、未通过活体检测 (例如, 检测为照片等), 等等。

在一个可选示例中, 该操作 318 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的认证模块或者交互模块执行。

另外, 在本公开又一实施例的人脸解锁方法中, 还可以包括:

响应于提取到的人脸特征未通过认证, 获取预先设置的允许重复次数信息, 对本次人脸解锁方法流程中的认证次数进行累计, 并识别当前累计的认证次数是否达到允许重复次数;

若未达到允许重复次数, 提示用户是否重新认证;

响应于接收到用户发送的重新认证请求, 返回执行操作 102、202 或 302, 继续获取图像, 重新执行本实施例的人脸解锁流程;

响应于当前累计的认证次数达到允许重复次数, 执行输出认证失败的提示消息或者认证失败原因提示消息的操作。

本公开各实施例的人脸解锁方法可以应用于电子设备屏幕解锁、应用程序 (APP) 的解锁、应用程序中的人脸解锁等一切需要解锁的场景, 例如, 在移动终端启动时可以采用本公开各实施例的人脸解锁

方法解锁屏幕，在移动终端的 APP 中可以通过本公开各实施例的人脸解锁方法进行应用程序的解锁，在支付应用程序中通过本公开各实施例的人脸解锁方法进行人脸解锁等。由此，本公开各实施例的人脸解锁方法可以响应于接收到用户发送的刷脸认证请求，或者响应于接收到应用或操作系统发送的刷脸认证请求等，触发执行。解锁之后，可以正常操作设备、应付程序等，或者正常进行后续流程。例如，需要进行人脸解锁的电子设备解锁后可以正常使用、操作电子设备（例如移动终端等）；需要进行人脸解锁的 APP（例如各种购物客户端、银行客户端、终端中的相册等）在解锁后可以进入该 APP，正常使用该 APP；在各种 APP 的支付环节需要进行人脸解锁时，解锁成功后可以完成支付等等。

本公开上述各实施例的人脸解锁方法流程之前，还可以包括：通过人脸解锁信息注册流程获取存储的对应同一 ID 的至少二个不同角度人脸图像的人脸特征。

示例性地，上述人脸解锁信息注册流程可以通过本公开以下各实施例的人脸解锁信息注册方法实施例实现。

图 4 为本公开人脸解锁信息注册方法一个实施例的流程图。如图 4 所示，本实施例的人脸解锁信息注册方法包括：

402，输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息。

在一个可选示例中，该操作 402 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的交互模块执行。

404，对获取到的图像进行人脸检测。

在一个可选示例中，该操作 404 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的人脸检测模块执行。

406，对检测到各角度人脸的图像进行人脸特征提取。

在一个可选示例中，该操作 406 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的特征提取模块执行。

408，存储提取到的各角度人脸图像的人脸特征、以及各角度人脸图像的人脸特征与上述同一 ID 之间的对应关系。

其中，本公开各实施例中，存储的人脸特征至少包括对应同一 ID 的至少二个不同角度人脸图像的人脸特征。其中的 ID 表示对应于存储人脸特征的用户信息，例如可以是用户姓名、编号等。

在本公开各实施例的一个可选示例中，上述对应同一 ID 的至少二个不同角度人脸图像例如可以包括但不限于对应上述同一 ID 的以下二个或二个以上角度的人脸图像：正面的人脸图像，仰头的人脸图像，低头的人脸图像，左转头的人脸图像，右转头的人脸图像，等等。

在一个可选示例中，该操作 408 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的存储模块执行。

基于本公开上述实施例提供的人脸解锁信息注册方法，可以通过注册流程预先存储对应同一 ID 的至少二个不同角度人脸图像的人脸特征，以便后续基于该对应同一 ID 的至少二个不同角度人脸图像的人脸特征进行人脸解锁，有利于提高人脸解锁的成功率，降低了由于同一用户认证时人脸角度与注册时人脸角度的差异而导致认证失败的可能性。

图 5 为本公开人脸解锁信息注册方法另一个实施例的流程图。如图 5 所示，本实施例的人脸解锁信息注册方法包括：

502，输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息。

在一个可选示例中，该操作 502 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的交互模块执行。

504，获取图像。

在一个可选示例中，该操作 504 可以由处理器调用摄像头执行，也可以由被处理器运行的人脸检测模块执行。

506，对获取到的图像进行光线均衡调整处理。

在本公开各实施例的一个可选示例中，可以直接执行该操作 506，对获取到的图像进行光线均衡调整处理。

或者，在本公开各实施例的另一个可选示例中，也可以在该操作 506 之前，先确定获取到的图像的质量是否满足预定的人脸检测条件，在图像的质量不满足预定的人脸检测条件时再执行操作 506，对获取到的图像进行光线均衡调整处理；对于质量满足预定的人脸检测条件的图像不再执行操作 506，直接通过操作 508 对图像进行人脸检测，该实施例可以对质量满足预定的人脸检测条件的图像不再执行光线均衡调整处理操作，从而有利于提升人脸解锁的效率。

其中，预定的人脸检测条件例如可以包括但不限于以下至少一项：图像的像素值分布不符合预设分

布范围, 图像的属性值不在预设数值范围内, 等。其中, 图像的属性值例如图像的色度、亮度、对比度和饱和度等属性值, 等等。

在本实施例的一个可选示例中, 操作 506 中, 对获取到的图像进行光线均衡调整处理, 可以包括: 获取图像的灰度图; 至少对该图像的灰度图进行直方图均衡化处理, 使图像的灰度图的像素值分布能够均匀的扩展到整个像素值空间, 同时保留原图像像素值的相对分布, 以便对经过直方图均衡化处理的图像的灰度图执行后续操作。

在本实施例的另一个可选示例中, 操作 506 中, 对获取到的图像进行光线均衡调整处理, 可以包括: 至少对图像进行图像光照变换, 以将图像变换为满足预设光照条件的图像。

在一个可选示例中, 该操作 506 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的光线处理模块执行。

508, 对获取到的图像进行人脸检测。

在一个可选示例中, 该操作 508 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的人脸检测模块执行。

510, 识别是否从图像中检测到人脸。

响应于从图像中检测到人脸, 执行操作 512。否则, 响应于从图像中未检测到人脸, 返回执行操作 504, 重新获取图像。

在一个可选示例中, 该操作 510 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的人脸检测模块执行。

512, 对检测到各角度人脸的图像进行人脸特征提取。

在一个可选示例中, 该操作 512 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的特征提取模块执行。

514, 存储提取到的各角度人脸图像的人脸特征及其与上述同一 ID 之间的对应关系。

在一个可选示例中, 该操作 514 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的人脸检测模块执行。

本公开实施例中, 先对获取到的图像进行光线均衡调整处理, 再进行人脸检测, 从而易于检测人脸, 遇到暗光、逆光等极端的光照条件下, 依然能够较为准确地检测到图像中的人脸, 尤其对于实际场景中那些室内或是夜晚光照非常暗几乎接近全黑的情况, 或是在夜晚背景光照强烈, 人脸昏暗纹理模糊的情况下也都能够检测出人脸, 从而使得本公开可以更好的实现人脸解锁应用。

图 6 为本公开人脸解锁信息注册方法又一个实施例的流程图。如图 6 所示, 与图 5 所示实施例相比, 本实施例的人脸解锁信息注册方法中, 在操作 514 之前, 例如可以在操作 512 之前、之后或同时, 执行如下操作:

602, 检测图像包括的人脸的角度。

在一个可选示例中, 该操作 602 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的存储模块执行。

604, 确定检测出的角度与提示信息对应的角度是否相匹配。确定检测出的角度与提示信息对应的角度相匹配时, 执行操作 512 对检测到各角度人脸的图像进行人脸特征提取、或者 514 存储提取到的各角度人脸图像的人脸特征、以及各角度人脸图像的人脸特征与上述同一 ID 之间的对应关系。

可选地, 在另一实施例中, 响应于检测出的角度与提示信息对应的角度不匹配, 还可以输出表示重新输入该角度的人脸图像的新提示信息, 以便调整人脸角度, 重新执行本公开实施例的人脸解锁信息注册方法流程。

在一个可选示例中, 该操作 604 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的存储模块执行。

在图 6 所示实施例的一个可选示例中, 操作 602 检测图像包括的人脸的角度, 可以包括:

对人脸进行关键点检测;

根据检测到的关键点计算人脸角度, 例如人脸的左右角度和上下角度;

根据计算出的人脸角度, 确定检测出的角度与提示信息对应的角度是否相匹配。

本公开实施例中, 后续可以基于在人脸解锁信息注册流程中保存的人脸特征对用户进行人脸解锁, 为了避免后续进行人脸解锁时由于参与人脸解锁的人脸角度与注册时不同而人脸解锁失败, 提高人脸解锁的成功率, 本公开实施例可以针对同一用户存储多个角度 (例如五个角度) 人脸图像的人脸特征。其中, 不同角度的人脸例如可以是正面、仰头、低头、左转头、右转头五种角度的人脸。本公开实施例中, 可以人脸 (即: 人头) 的左右角度和上下角度表示人脸角度, 可以设定正面人脸时, 人脸的左右角度和上下角度均为零。

相应地，在图 6 所示实施例的另一个可选示例中，操作 502 中，输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息，可以包括：根据预先设置的多角度参数，选取一预设角度并提示用户录入该一预设角度的人脸图像。其中的多角度参数包括需要获取的人脸图像的多个角度信息。相应地，该示例中，存储该一预设角度人脸图像的人脸特征及其与上述同一 ID 之间的对应关系之后，还可以包括：识别是否选取完多角度参数对应的所有预设角度；响应于未选取完多角度参数对应的所有预设角度，选取下一预设角度并针对该下一预设角度执行上述图 5 或图 6 所示实施例。若选取完多角度参数对应的所有预设角度，则完成该本次人脸解锁信息注册。

可选地，响应于选取完多角度参数对应的所有预设角度或者每次提取到一个角度的人脸特征后，还可以输出用于提示用户输入所述同一 ID 的提示信息。相应地，存储提取到的各角度人脸图像的人脸特征及其与上述同一 ID 之间的对应关系，包括：存储提取到的至少二个角度人脸图像的人脸特征与用户输入的 ID，并建立该 ID 和上述至少二个角度人脸图像的人脸特征之间的对应关系。

基于上述示例，实现了针对同一用户存储多个不同角度人脸的人脸特征。

在本公开上述各实施例的人脸解锁信息注册方法中，还可以包括：对图像进行活体检测。相应地，在本公开上述各人脸解锁方法实施例中，响应于该图像通过活体检测，执行上述存储提取到的各角度人脸图像的人脸特征及其与上述同一 ID 之间的对应关系的操作。

示例性地，本公开各实施例的人脸解锁方法中，对图像进行活体检测，可以在获取图像之后，对获取到的图像进行活体检测；或者，也可以对检测到各角度人脸的图像进行活体检测；或者，响应于检测到的人脸的角度与预设角度匹配，对图像进行活体检测；或者，还可以对人脸进行特征提取之后，对图像进行活体检测。

本公开各人脸解锁信息注册方法实施例中对图像进行活体检测的实现方式，可以参考本公开上述各人脸解锁方法实施例中对图像进行活体检测的实现方式，此处不再赘述。

图 7 为本公开人脸解锁信息注册方法再一个实施例的流程图。本公开实施例中，以在获取图像之后对图像进行活体检测为例对本公开实施例进行说明，本领域技术人员根据本公开的记载可以知晓，对检测到各角度人脸的图像进行活体检测、响应于检测到的人脸的角度与预设角度匹配对图像进行活体检测、检测到各角度人脸的图像进行人脸提取之后对图像进行活体检测的实现方案，此处不再赘述。如图 7 所示，本实施例的人脸解锁信息注册方法包括：

702，输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息。

在一个可选示例中，该操作 702 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的交互模块执行。

704，获取图像，并对获取到的图像进行活体检测。

响应于该图像通过活体检测，执行操作 706。否则，若该图像未通过活体检测，不执行本实施例的后续流程。

在一个可选示例中，该操作 704 可以由处理器调用摄像头和存储器存储的相应指令执行，也可以由被处理器运行的活体检测模块执行。

706，对获取到的图像进行人脸检测。

在一个可选示例中，该操作 706 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的人脸检测模块执行。

708，识别是否从图像中检测到人脸。

响应于从图像中检测到人脸，执行操作 710。若从图像中未检测到人脸，继续执行操作 702，或者继续获取图像并执行操作 704。

在一个可选示例中，该操作 708 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的人脸检测模块执行。

710，检测图像包括的人脸的角度。

在一个可选示例中，该操作 710 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的存储模块执行。

712，确定检测出的角度与提示信息对应的角度是否相匹配。

响应于检测出的角度与提示信息对应的角度相匹配，执行操作 714。否则，若检测出的角度与提示信息对应的角度不匹配，重新执行操作 702。

在一个可选示例中，该操作 712 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器运行的存储模块执行。

714，对检测到各角度人脸的图像进行人脸特征提取。

在一个可选示例中，该操作 714 可以由处理器调用存储器存储的相应指令执行，也可以由被处理器

运行的特征检测模块执行。

716, 存储提取到的各角度人脸图像的人脸特征、以及各角度人脸图像的人脸特征与上述同一 ID 之间的对应关系。

另外, 作为本公开人脸解锁信息注册方法的又一实施例, 在图 7 所示实施例的操作 704 中, 可以识别获取到的图像是否满足预设质量要求; 响应于图像满足预设质量要求, 对图像进行活体检测; 否则, 响应于图像不满足预设质量要求, 继续执行操作 702 或 704。

在一个可选示例中, 该操作 716 可以由处理器调用存储器存储的相应指令执行, 也可以由被处理器运行的存储模块执行。

本公开上述实施例可以从多个维度来检测图像是否伪造人脸图像, 可以检测出不同维度、各种类型的伪造人脸图像, 提高了伪造人脸检测的精确度, 有效避免了活体检测过程中不法分子利用待验证用户的照片或视频进行伪造攻击, 确保人脸解锁信息注册时的图像即为真实的用户图像; 此外, 通过神经网络进行人脸防伪检测, 可以针对各种伪造人脸方式的伪造线索信息进行训练学习, 在出现新的伪造人脸方式时, 基于新的伪造线索信息对神经网络进行训练、微调即可快速更新神经网络, 而无需改进硬件结构, 可以快速有效的响应新的人脸防伪检测需求。

本公开上述各实施例的人脸解锁信息注册方法, 可以响应于接收到用户发送的录入人脸请求开始执行, 或者响应于接收到应用或操作系统发送的录入人脸请求开始执行。

本公开实施例提供的任一种人脸解锁方法和人脸解锁信息注册方法可以由任意适当的具有数据处理能力的设备执行, 包括但不限于: 终端设备和服务器等。或者, 本公开实施例提供的任一种人脸解锁方法和人脸解锁信息注册方法可以由处理器执行, 如处理器通过调用存储器存储的相应指令来执行本公开实施例提及的任一种人脸解锁方法和人脸解锁信息注册方法。下文不再赘述。

本领域普通技术人员可以理解: 实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成, 前述的程序可以存储于一计算机可读存储介质中, 该程序在执行时, 执行包括上述方法实施例的步骤; 而前述的存储介质包括: ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

图 8 为本公开人脸解锁装置一个实施例的结构示意图。该实施例的人脸解锁装置可用于实现本公开上述各方法实施例。如图 8 所示, 该实施例的人脸解锁装置包括: 人脸检测模块, 特征提取模块, 认证模块和控制模块。其中:

人脸检测模块, 用于对图像进行人脸检测。

特征提取模块, 用于对检测到人脸的图像进行人脸特征提取。

认证模块, 用于基于存储的人脸特征对提取到的人脸特征进行认证。

其中, 存储的人脸特征至少包括对应同一 ID 的至少二个不同角度人脸图像的人脸特征。示例性地, 上述对应同一 ID 的至少二个不同角度人脸图像例如可以包括但不限于对应同一 ID 的以下二个或二个以上角度的人脸图像: 正面的人脸图像, 仰头的人脸图像, 低头的人脸图像, 左转头的人脸图像, 右转头的人脸图像, 等等。

控制模块, 用于至少响应于提取到的人脸特征通过认证, 进行解锁操作。

在其中一个可选示例中, 认证模块用于获取提取到的人脸特征与至少一个存储的人脸特征之间的相似度; 以及响应于获取到任一相似度大于设定阈值, 确定提取到的人脸特征通过认证。在另一个可选示例中, 认证模块用于分别获取提取到的人脸特征与多个存储的人脸特征之间的相似度; 以及响应于获取到的多个相似度中的最大值大于设定阈值, 确定提取到的人脸特征通过认证。

本公开实施例提供的人脸解锁装置, 对图像进行人脸检测, 对检测到人脸的图像进行人脸特征提取, 并基于存储的人脸特征对该提取到的人脸特征进行认证, 在该提取到的人脸特征通过认证后, 进行解锁操作, 从而实现了基于人脸的认证解锁, 本公开实施例的解锁方式操作简单, 便利性较高, 且安全性较高; 并且, 由于本公开实施例通过注册流程预先存储对应同一 ID 的至少二个不同角度人脸图像的人脸特征, 可以在获取到上述同一 ID 对应用户与存储的人脸特征对应的任一角度人脸图像时, 均可成功实现基于该用户的人脸解锁, 提高了人脸解锁的成功率, 降低了由于同一用户认证时人脸角度与注册时人脸角度的差异而导致认证失败的可能性。

图 9 为本公开人脸解锁装置另一个实施例的结构示意图。如图 9 所示, 与图 8 所示实施例相比, 该实施例的人脸解锁装置还包括: 获取模块和光线处理模块。其中:

获取模块, 用于获取图像。该获取模块例如可以是一个摄像头或其他图像采集设备。

光线处理模块, 用于在对图像进行光线均衡调整处理。

相应地, 人脸检测模块用于对光线均衡调整处理后的图像进行人脸检测。

在其中一个可选示例中, 光线处理模块用于获取图像的灰度图, 以及至少对图像的灰度图进行直方图均衡化处理。在另一个可选示例中, 光线处理模块用于至少对图像进行图像光照变换, 以将图像变换

为满足预设光照条件的图像。在又一个可选示例中，光线处理模块用于确定图像的质量不满足预定的人脸检测条件，对图像进行光线均衡调整处理。其中，预定的人脸检测条件例如可以包括但不限于以下至少一项：图像的像素值分布不符合预设分布范围，图像的属性值不在预设数值范围内。

进一步地，再参见图 9，在本公开人脸解锁装置的又一个实施例中，还可以包括：交互模块和存储模块。其中：交互模块，用于输出表示获取上述同一 ID 的至少二个不同角度的人脸图像的提示信息。存储模块，用于存储特征提取模块提取到的各角度人脸图像的人脸特征及其与上述同一 ID 之间的对应关系。

在其中一个可选示例中，存储模块用于检测图像包括的人脸的角度；以及确定检测出的角度与提示信息对应的角度相匹配，存储特征提取模块提取到的各角度人脸图像的人脸特征及其与同一 ID 之间的对应关系。

在另一个可选示例中，存储模块检测图像包括的人脸的角度时，用于对图像进行人脸关键点检测；以及根据检测到的人脸关键点计算图像包括的人脸的角度。

另外，在本公开人脸解锁装置的再一个实施例中，存储模块还可用于在检测出的角度与提示信息对应的角度不匹配时，请求交互模块输出表示重新输入该角度的人脸图像的新提示信息。

在又一个可选示例中，存储模块用于识别是否存储完成同一 ID 的至少二个不同角度的人脸图像的人脸特征；响应于未存储完成同一 ID 的至少二个不同角度的人脸图像的，请求交互模块输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息的操作；响应于存储完成同一 ID 的至少二个不同角度的人脸图像的人脸特征，请求交互模块输出用于提示用户输入同一 ID 的提示信息；存储提取到的至少二个角度人脸图像的人脸特征与用户输入的同一 ID，并建立同一 ID 和至少二个角度人脸图像的人脸特征之间的对应关系。

进一步地，再参见图 9，在本公开人脸解锁装置的再一个实施例中，还可以包括：活体检测模块，用于对图像进行活体检测。相应地，该实施例中，控制模块用于至少响应于提取到的人脸特征通过认证、且图像通过活体检测，进行解锁操作。

在其中一个可选示例中，活体检测模块，用于响应于图像满足预设质量要求，对图像进行活体检测。

在另一个可选示例中，活体检测模块可以通过神经网络实现。该神经网络用于：对图像进行图像特征提取；检测提取的图像特征是否包含至少一种伪造线索信息；以及基于至少一种伪造线索信息的检测结果，确定图像是否通过活体检测。

其中，利用神经网络对图像提取的图像特征例如可以包括但不限于以下任意一项或多项：LBP 特征、HSC 特征、LARGE 特征、SMALL 特征、TINY 特征。

上述至少一种伪造线索信息例如可以包括但不限于以下任意一项或多项：2D 类伪造人脸信息、2.5D 类伪造人脸信息和 3D 类伪造人脸信息。

其中，2D 类伪造人脸信息包括纸质类材料打印人脸图像的伪造信息；和/或，2.5D 类伪造人脸信息包括载体设备承载人脸图像的伪造信息；和/或，3D 类伪造人脸信息包括伪造人脸的信息。

本公开实施例还提供了一种电子设备，包括：本公开上述任一实施例的人脸解锁装置。

另外，本公开实施例还提供了另一种电子设备，包括：

处理器和本公开上述任一实施例的人脸解锁；

在处理器运行该人脸解锁时，上述任一实施例的人脸解锁中的模块被运行。

另外，本公开实施例还提供了又一种电子设备，包括：

存储器，存储可执行指令；

一个或多个处理器，与存储器通信以执行可执行指令从而本公开上述任一实施例的人脸解锁方法或者人脸解锁信息注册方法步骤的操作。

另外，本公开实施例还提供了一种计算机程序，包括计算机可读代码，当该计算机可读代码在设备上运行时，设备中的处理器执行用于实现本公开上述任一实施例的人脸解锁方法或者人脸解锁信息注册方法中步骤的指令。

另外，本公开实施例还提供了一种计算机可读介质，用于存储计算机可读取的指令，该指令被执行时实现本公开上述任一实施例的人脸解锁方法或者人脸解锁信息注册方法中步骤的操作。

图 10 为本公开电子设备一个实施例的结构示意图。下面参考图 10，其示出了适于用来实现本申请的实施例的终端设备或服务器的电子设备的结构示意图。如图 10 所示，该电子设备包括一个或多个处理器、通信部等，所述一个或多个处理器例如：一个或多个中央处理单元（CPU）801，和/或一个或多个图像处理器（GPU）813 等，处理器可以根据存储在只读存储器（ROM）802 中的可执行指令或者从存储部分 808 加载到随机访问存储器（RAM）803 中的可执行指令而执行各种适当的动作和处理。通信部 812 可包括但不限于网卡，所述网卡可包括但不限于 IB（Infiniband）网卡，处理器可与只读存储器 802

和/或随机访问存储器 803 中通信以执行可执行指令,通过总线 804 与通信部 812 相连、并经通信部 812 与其他目标设备通信,从而完成本申请实施例提供的任一方法对应的操作,例如,对图像进行人脸检测;对检测到人脸的图像进行人脸特征提取;基于存储的人脸特征对提取到的人脸特征进行认证,其中,所述存储的人脸特征至少包括对应同一标识 ID 的至少二个不同角度人脸图像的人脸特征;至少响应于所述提取到的人脸特征通过认证,进行解锁操作。或者,输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息;对获取到的图像进行人脸检测;对检测到各角度人脸的图像进行人脸特征提取;存储提取到的各角度人脸图像的人脸特征、以及各角度人脸图像的人脸特征与所述同一 ID 之间的对应关系。

此外,在 RAM 803 中,还可存储有装置操作所需的各种程序和数据。CPU801、ROM802 以及 RAM803 通过总线 804 彼此相连。在有 RAM803 的情况下,ROM802 为可选模块。RAM803 存储可执行指令,或在运行时向 ROM802 中写入可执行指令,可执行指令使中央处理单元 801 执行上述方法对应的操作。输入/输出 (I/O) 接口 805 也连接至总线 804。通信部 812 可以集成设置,也可以设置为具有多个子模块(例如多个 IB 网卡),并在总线链接上。

以下部件连接至 I/O 接口 805:包括键盘、鼠标等的输入部分 806;包括诸如阴极射线管 (CRT)、液晶显示器 (LCD) 等以及扬声器等的输出部分 807;包括硬盘等的存储部分 808;以及包括诸如 LAN 卡、调制解调器等网络接口卡的通信部分 809。通信部分 809 经由诸如因特网的网络执行通信处理。驱动器 810 也根据需要连接至 I/O 接口 805。可拆卸介质 811,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器 811 上,以便于从其上读出的计算机程序根据需要被安装入存储部分 808。

需要说明的,如图 10 所示的架构仅为一种可选实现方式,在可选实践过程中,可根据实际需要对上述图 10 的部件数量和类型进行选择、删减、增加或替换;在不同功能部件设置上,也可采用分离设置或集成设置等实现方式,例如 GPU813 和 CPU801 可分离设置或者可将 GPU813 集成在 CPU801 上,通信部可分离设置,也可集成设置在 CPU801 或 GPU813 上,等等。这些可替换的实施方式均落入本公开公开的保护范围。

特别地,根据本公开的实施例,上文参考流程图描述的过程可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括有形地包含在机器可读介质上的计算机程序,计算机程序包含用于执行流程图所示的方法的程序代码,程序代码可包括对应执行本申请实施例提供的方法步骤对应的指令,例如,对图像进行人脸检测;对检测到人脸的图像进行人脸特征提取;基于存储的人脸特征对提取到的人脸特征进行认证,其中,所述存储的人脸特征至少包括对应同一标识 ID 的至少二个不同角度人脸图像的人脸特征;至少响应于所述提取到的人脸特征通过认证,进行解锁操作。或者,输出表示获取同一 ID 的至少二个不同角度的人脸图像的提示信息;对获取到的图像进行人脸检测;对检测到各角度人脸的图像进行人脸特征提取;存储提取到的各角度人脸图像的人脸特征及其与所述同一 ID 之间的对应关系。

本说明书中各个实施例均采用递进的方式描述,每个实施例重点说明的都是与其它实施例的不同之处,各个实施例之间相同或相似的部分相互参见即可。对于系统实施例而言,由于其与方法实施例基本对应,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

可能以许多方式来实现本公开的方法和装置、设备。例如,可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本公开的方法和装置、设备。用于所述方法的步骤的上述顺序仅是为了进行说明,本公开的方法的步骤不限于以上可选描述的顺序,除非以其它方式特别说明。此外,在一些实施例中,还可将本公开实施为记录在记录介质中的程序,这些程序包括用于实现根据本公开的方法的机器可读指令。因而,本公开还覆盖存储用于执行根据本公开的方法的程序的记录介质。

本公开的描述是为了示例和描述起见而给出的,而并不是无遗漏的或者将本公开限于所公开的形式。很多修改和变化对于本领域的普通技术人员而言是显然的。选择和描述实施例是为了更好说明本公开的原理和实际应用,并且使本领域的普通技术人员能够理解本公开从而设计适于特定用途的带有各种修改的各种实施例。