(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108805005 A
(43)申请公布日 2018.11.13

(21)申请号 201810339526.0

(22)申请日 2018.04.16

(71)申请人 深圳市商汤科技有限公司
地址 518000 广东省深圳市南山区南海大道1052号海翔广场712

(72)发明人 郑桂荣 徐妙然 向许波 衷丛洪

(74)专利代理机构 北京思源智汇知识产权代理有限公司 11657
代理人 毛丽琴

(51)Int.Cl.
G06K 9/00(2006.01)
G06K 9/20(2006.01)
G06K 9/62(2006.01)

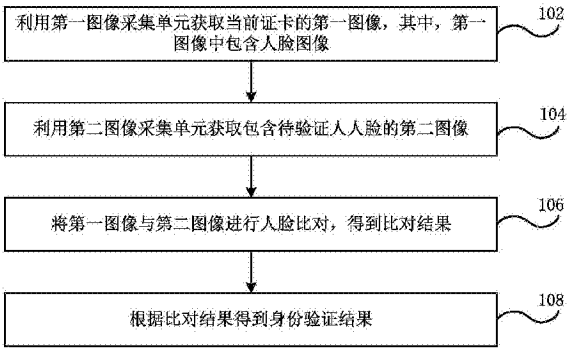
权利要求书2页 说明书14页 附图4页

(54)发明名称

身份验证方法和装置、电子设备、计算机程序和存储介质

(57)摘要

本发明实施例公开了一种身份验证方法和装置、电子设备、计算机程序和存储介质。其中，方法包括：利用第一图像采集单元获取当前证卡的第一图像，其中，所述第一图像中包含人脸图像；利用第二图像采集单元获取包含待验证人人脸的第二图像；将所述第一图像与所述第二图像进行人脸比对，得到比对结果；根据所述比对结果得到身份验证结果。本发明实施例扩大了身份验证的应用场景。



CN 108805005 A

1.一种身份验证方法,其特征在于,包括:

利用第一图像采集单元获取当前证卡的第一图像,其中,所述第一图像中包含人脸图像;

利用第二图像采集单元获取包含待验证人人脸的第二图像;

将所述第一图像与所述第二图像进行人脸比对,得到比对结果;

根据所述比对结果得到身份验证结果。

2.根据权利要求1所述的方法,其特征在于,在利用第一图像采集单元获取当前证卡的第一图像之前,还包括:

获取当前证卡的属性,所述属性包括内置芯片型证卡和非内置芯片型证卡;

当所述当前证卡的属性为非内置芯片型证卡时,利用第一图像采集单元获取当前证卡的第一图像,其中,所述第一图像中包含人脸图像。

3.根据权利要求2所述的方法,其特征在于,还包括:

当所述当前证卡的属性为内置芯片型证卡时,对所述当前证卡进行真伪识别处理;

所述当前证卡为真实证件时,利用第二图像采集单元获取包含待验证人人脸的第二图像。

4.根据权利要求3所述的方法,其特征在于,对所述当前证卡进行真伪识别处理包括:

利用第一图像采集单元获取当前证卡的第一图像,其中,所述第一图像中包含外置的人脸图像;

利用芯片识别器获取所述当前证卡的芯片信息,其中,所述芯片信息中包含内存的人脸图像;

将所述第一图像与所述芯片信息比对,得到比对结果;

根据所述比对结果确定所述当前证卡的真伪性。

5.根据权利要求1至4中任意一项所述的方法,其特征在于,还包括:

判断所述第一图像中是否包含文字部分;

当所述第一图像中包含所述文字部分时,对所述第一图像中的所述文字部分进行文字识别处理,得到所述当前证卡中的文字信息。

6.一种身份验证装置,其特征在于,包括:

第一图像采集单元,用于获取当前证卡的第一图像,其中,所述第一图像中包含人脸图像;

第二图像采集单元,用于获取包含待验证人人脸的第二图像;

图像比对单元,用于将所述第一图像与所述第二图像进行人脸比对,得到比对结果;

身份验证单元,用于根据所述比对结果得到身份验证结果。

7.一种电子设备,其特征在于,包括权利要求6所述的装置。

8.一种电子设备,其特征在于,包括:

存储器,用于存储可执行指令;以及

处理器,用于与所述存储器通信以执行所述可执行指令从而实现权利要求1至5中任意一项所述的方法。

9.一种计算机程序,包括计算机可读代码,其特征在于,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权利要求1至5中任意一项所述方法的指令。

10.一种计算机存储介质，用于存储计算机可读取的指令，其特征在于，所述指令被执行时实现权利要求1至5中任意一项所述的方法。

身份验证方法和装置、电子设备、计算机程序和存储介质

技术领域

[0001] 本发明属于计算机视觉技术领域，特别是涉及一种身份验证方法和装置、电子设备、计算机程序和存储介质。

背景技术

[0002] 人脸识别，也称为人像识别或者面部识别，是一种基于人的脸部特征信息进行身份识别的生物识别技术，是通过对包含人脸的图像或者视频流，自动检测和跟踪人脸，对检测到的人脸进行脸部的一系列相关技术。近年来，随着机器学习技术的兴起和在人脸识别领域的普及和应用，促进了人脸识别技术的发展和成熟。

[0003] 由于人的脸部特征是人本身固有的生物特征之一，因此可以将人脸识别作为一项身份鉴别技术应用于人的身份验证。

发明内容

[0004] 本发明实施例提供一种身份验证技术方案。

[0005] 根据本发明实施例的一个方面，提供一种身份验证方法，包括：

[0006] 利用第一图像采集单元获取当前证卡的第一图像，其中，所述第一图像中包含人脸图像；

[0007] 利用第二图像采集单元获取包含待验证人人脸的第二图像；

[0008] 将所述第一图像与所述第二图像进行人脸比对，得到比对结果；

[0009] 根据所述比对结果得到身份验证结果。

[0010] 可选地，在本发明上述方法实施例中，在利用第一图像采集单元获取当前证卡的第一图像之前，还包括：

[0011] 获取当前证卡的属性，所述属性包括内置芯片型证卡和非内置芯片型证卡；

[0012] 当所述当前证卡的属性为非内置芯片型证卡时，利用第一图像采集单元获取当前证卡的第一图像，其中，所述第一图像中包含人脸图像。

[0013] 可选地，在本发明上述任一方法实施例中，还包括：

[0014] 当所述当前证卡的属性为内置芯片型证卡时，对所述当前证卡进行真伪识别处理；

[0015] 所述当前证卡为真实证件时，利用第二图像采集单元获取包含待验证人人脸的第二图像。

[0016] 可选地，在本发明上述任一方法实施例中，对所述当前证卡进行真伪识别处理包括：

[0017] 利用第一图像采集单元获取当前证卡的第一图像，其中，所述第一图像中包含外置的人脸图像；

[0018] 利用芯片识别器获取所述当前证卡的芯片信息，其中，所述芯片信息中包含内存的人脸图像；

[0019] 将所述第一图像与所述芯片信息比对，得到比对结果；

[0020] 根据所述比对结果确定所述当前证卡的真伪性。

[0021] 可选地，在本发明上述任一方法实施例中，所述将所述第一图像与所述第二图像进行人脸比对，得到比对结果，包括：

[0022] 对所述第一图像中的人脸图像进行人脸特征提取，得到第一人脸特征数据；

[0023] 对所述第二图像进行人脸特征提取，得到至少一组第二人脸特征数据；

[0024] 将所述第一人脸特征数据与所述至少一组第二人脸特征数据进行比对，得到比对结果。

[0025] 可选地，在本发明上述任一方法实施例中，所述将所述第一人脸特征数据与所述至少一组第二人脸特征数据进行比对，得到比对结果，包括：

[0026] 分别计算所述第一人脸特征数据与每组所述第二人脸特征数据之间的相似度；

[0027] 将所述相似度作为比对结果。

[0028] 可选地，在本发明上述任一方法实施例中，所述根据所述比对结果得到身份验证结果，包括：

[0029] 将所述相似度大于预设阈值确定为身份验证成功；

[0030] 将所述相似度小于或等于所述预设阈值确定为身份验证失败。

[0031] 可选地，在本发明上述任一方法实施例中，所述根据所述比对结果得到身份验证结果之后，还包括：

[0032] 显示所述第一图像中的人脸图像、所述第二图像和所述身份验证结果。

[0033] 可选地，在本发明上述任一方法实施例中，所述将所述第一图像与所述第二图像进行人脸比对，得到比对结果之前，还包括：

[0034] 对所述第一图像进行处理，分离所述第一图像中的人脸图像和/或文字部分。

[0035] 可选地，在本发明上述任一方法实施例中，在所述分离所述第一图像中的人脸图像和/或文字部分之前，还包括：

[0036] 判断所述第一图像中是否包含所述人脸图像；

[0037] 当所述第一图像中未包含人脸图像时，提示用户重新放置所述当前证卡。

[0038] 可选地，在本发明上述任一方法实施例中，还包括：

[0039] 判断所述第一图像中是否包含所述文字部分；

[0040] 当所述第一图像中包含所述文字部分时，对所述第一图像中的文字部分进行文字识别处理，得到所述当前证卡中的文字信息。

[0041] 可选地，在本发明上述任一方法实施例中，所述对所述第一图像中的文字部分进行文字识别处理，得到所述当前证卡中的文字信息，包括：

[0042] 对所述第一图像中的文字部分进行特征提取，得到所述文字部分的特征数据；

[0043] 确定所述文字部分的特征数据与预设数据库中预设文字对应的特征数据之间的相似度；

[0044] 将大于相似度阈值的特征数据对应的预设文字，作为所述文字识别的结果；

[0045] 根据所述文字识别的结果得到所述当前证卡中的文字信息。

[0046] 可选地，在本发明上述任一方法实施例中，还包括：

[0047] 显示所述第一图像中的人脸图像、所述第二图像、所述身份验证结果和所述当前

证卡中的文字信息。

[0048] 根据本发明实施例的另一个方面，提供一种身份验证装置，包括：

[0049] 第一图像采集单元，用于获取当前证卡的第一图像，其中，所述第一图像中包含人脸图像；

[0050] 第二图像采集单元，用于获取包含待验证人人脸的第二图像；

[0051] 图像比对单元，用于将所述第一图像与所述第二图像进行人脸比对，得到比对结果；

[0052] 身份验证单元，用于根据所述比对结果得到身份验证结果。

[0053] 可选地，在本发明上述装置实施例中，还包括：

[0054] 属性获取单元，用于获取当前证卡的属性，所述属性包括内置芯片型证卡和非内置芯片型证卡；

[0055] 所述第一图像采集单元，用于当所述当前证卡的属性为非内置芯片型证卡时，获取当前证卡的第一图像，其中，所述第一图像中包含人脸图像。

[0056] 可选地，在本发明上述任一装置实施例中，还包括：

[0057] 真伪识别单元，用于当所述当前证卡的属性为内置芯片型证卡时，对所述当前证卡进行真伪识别处理；

[0058] 所述第二图像采集单元，还用于所述当前证卡为真实证件时，获取包含待验证人人脸的第二图像。

[0059] 可选地，在本发明上述任一装置实施例中，所述第一图像采集单元，还用于获取当前证卡的第一图像，其中，所述第一图像中包含外置的人脸图像；

[0060] 所述装置还包括：芯片识别器，用于获取所述当前证卡的芯片信息，其中，所述芯片信息中包含内存的人脸图像；

[0061] 所述真伪识别单元，用于将所述第一图像与所述芯片信息比对，得到比对结果；以及根据所述比对结果确定所述当前证卡的真伪性。

[0062] 可选地，在本发明上述任一装置实施例中，所述图像比对单元，用于对所述第一图像中的人脸图像进行人脸特征提取，得到第一人脸特征数据；对所述第二图像进行人脸特征提取，得到至少一组第二人脸特征数据；以及将所述第一人脸特征数据与所述至少一组第二人脸特征数据进行比对，得到比对结果。

[0063] 可选地，在本发明上述任一装置实施例中，所述图像比对单元，用于分别计算所述第一人脸特征数据与每组所述第二人脸特征数据之间的相似度；以及将所述相似度作为比对结果。

[0064] 可选地，在本发明上述任一装置实施例中，所述身份验证单元，用于将所述相似度大于预设阈值确定为身份验证成功；以及将所述相似度小于或等于所述预设阈值确定为身份验证失败。

[0065] 可选地，在本发明上述任一装置实施例中，还包括：

[0066] 信息显示单元，用于显示所述第一图像中的人脸图像、所述第二图像和所述身份验证结果。

[0067] 可选地，在本发明上述任一装置实施例中，还包括：

[0068] 图文分离单元，用于对所述第一图像进行处理，分离所述第一图像中的人脸图像

和/或文字部分。

[0069] 可选地，在本发明上述任一装置实施例中，还包括：

[0070] 第一检测单元，用于判断所述第一图像中是否包含所述人脸图像；

[0071] 信息提示单元，用于当所述第一图像中未包含人脸图像时，提示用户重新放置所述当前证卡。

[0072] 可选地，在本发明上述任一装置实施例中，还包括：

[0073] 第二检测单元，用于判断所述第一图像中是否包含所述文字部分；

[0074] 文字识别单元，用于当所述第一图像中包含所述文字部分时，对所述第一图像中的文字部分进行文字识别处理，得到所述当前证卡中的文字信息。

[0075] 可选地，在本发明上述任一装置实施例中，所述文字识别单元，用于对所述第一图像中的文字部分进行特征提取，得到所述文字部分的特征数据；以及确定所述文字部分的特征数据与预设数据库中预设文字对应的特征数据之间的相似度；将大于相似度阈值的特征数据对应的预设文字，作为所述文字识别的结果；以及根据所述文字识别的结果得到所述当前证卡中的文字信息。

[0076] 可选地，在本发明上述任一装置实施例中，还包括：

[0077] 信息显示单元，用于显示所述第一图像中的人脸图像、所述第二图像、所述身份验证结果和所述当前证卡中的文字信息。

[0078] 根据本发明实施例的又一个方面，提供的一种电子设备，包括上述任一实施例所述的装置。

[0079] 根据本发明实施例的再一个方面，提供的一种电子设备，包括：

[0080] 存储器，用于存储可执行指令；以及

[0081] 处理器，用于与所述存储器通信以执行所述可执行指令从而完成上述任一实施例所述的方法。

[0082] 根据本发明实施例的再一个方面，提供的一种计算机程序，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上述任一实施例所述方法的指令。

[0083] 根据本发明实施例的再一个方面，提供的一种计算机程序产品，用于存储计算机可读指令，所述指令被执行时使得计算机执行上述任一实施例所述的方法。

[0084] 在一个可选实施方式中，所述计算机程序产品具体为计算机存储介质，在另一个可选实施方式中，所述计算机程序产品具体为软件产品，例如SDK等。

[0085] 基于本发明上述实施例提供的身份验证方法和装置、电子设备、计算机程序和存储介质，通过将采集的证卡中的人脸图像，与实时采集的人脸图像进行人脸比对，可以实现在没有芯片读卡器的情况下对持证人身份的验证，从而可以有效防止人证不一致，盗用他人身份的情况。由于可以使用未内置芯片的证件进行身份验证，因此使得身份验证更加灵活，扩大了身份验证的应用场景。

附图说明

[0086] 构成说明书的一部分的附图描述了本发明的实施例，并且连同描述一起用于解释本发明的原理。

[0087] 参照附图，根据下面的详细描述，可以更加清楚地理解本发明，其中：

[0088] 图1是本发明一些实施例提供的身份验证方法的流程图；

[0089] 图2是本发明另一些实施例提供的身份验证方法的流程图；

[0090] 图3是本发明又一些实施例提供的身份验证方法的流程图；

[0091] 图4是本发明一些实施例提供的身份验证装置的结构示意图；

[0092] 图5是本发明另一些实施例提供的身份验证装置的结构示意图；

[0093] 图6是本发明又一些实施例提供的身份验证装置的结构示意图；

[0094] 图7是本发明实施例电子设备一个实施例的结构示意图。

具体实施方式

[0095] 现在将参照附图来详细描述本发明的各种示例性实施例。应注意到：除非另外具体说明，否则在这些实施例中阐述的部件的相对布置、数字表达式和数值不限制本发明的范围。

[0096] 同时，应当明白，为了便于描述，附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。

[0097] 以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本发明及其应用或使用的任何限制。

[0098] 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。

[0099] 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。

[0100] 本发明实施例可以应用于计算机系统/服务器，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。适于与计算机系统/服务器一起使用的众所周知的计算系统、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。

[0101] 计算机系统/服务器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。

[0102] 目前，电信行业营业厅、银行、酒店、网吧、机场、车站等广泛使用的身份验证一体机在进行身份验证时，大多是通过芯片识别器获取身份证内置的芯片信息，然后将芯片信息中内存的照片与摄像头现场采集的持证人的图像进行比对，来验证人证的一致性，这种身份验证一体机验证速度快，准确率高，可以有效防止人证不一致，盗用他人身份的情况。然而，在一些国家，例如：新加坡等，身份证没有内置的芯片，这样就不能通过上述的这种身份验证方式来进行身份验证。

[0103] 为了解决这一问题，本发明实施例提出了一种身份验证方法，下面将结合图1，详

细描述本发明实施例提出的身份验证方法的流程。

[0104] 应理解，图1所示的例子仅仅是为了帮助本领域技术人员更好地理解本发明的技术方案，而不应理解成对本发明的限定。本领域技术人员可以在图1的基础上进行各种变换，而这种变换也应理解成本发明技术方案的一部分。

[0105] 如图1所示，该方法包括：

[0106] 102，利用第一图像采集单元获取当前证卡的第一图像，其中，第一图像中包含人脸图像。

[0107] 可选地，证卡，是指各种证件、卡片、证照和票证的总称。例如：各种证件可以是身份证、驾照、护照、学生证、工作证等包含人脸照片的证件，证照可以是黑白或者彩色照片等。第一图像可以是采集自包含人脸照片的证卡的图像，本发明实施例对此不做限定。

[0108] 可选地，第一图像采集单元包括但不限于摄像头、扫描仪和数码相机等，因此可以先通过扫描仪对当前证卡进行扫描，或者通过摄像头/数码相机对当前证卡进行拍摄，之后通过OCR(Optical Character Recognition，光学字符识别)方式获取第一图像，本发明实施例对此不做限定。

[0109] 104，利用第二图像采集单元获取包含待验证人人脸的第二图像。

[0110] 可选地，第二图像可以是现场实时采集的图像，第二图像采集单元可以是摄像头或者数码相机等，因此可以通过摄像头或者数码相机对待验证人进行拍摄方式获取第二图像，本发明实施例对此不做限定。

[0111] 在一个可选的例子中，第一图像采集单元与第二图像采集单元可以为同一个图像采集单元。例如：可以先通过摄像头或者数码相机对当前证卡进行拍摄，之后通过OCR方式获取第一图像，再通过摄像头或者数码相机对待验证人进行拍摄方式获取第二图像。

[0112] 106，将第一图像与第二图像进行人脸比对，得到比对结果。

[0113] 可选地，可以对第一图像中的人脸图像进行特征提取，得到第一人脸特征数据，以及对第二图像进行特征提取，得到至少一组第二人脸特征数据，将第一人脸特征数据与至少一组第二人脸特征数据进行比对，得到比对结果。

[0114] 由于第二图像可以是现场实时采集的图像，在现场采集图像时，第二图像中可能仅包含待验证人人脸，也可能除了包含待验证人人脸外，还包含其他人脸。当第二图像中仅包含待验证人人脸时，对第二图像进行特征提取，会得到一组第二人脸特征数据。当第二图像中除了包含待验证人人脸外还包含其他人脸时，对第二图像进行特征提取，对于第二图像中的每一个人脸都会得到一组对应的第二人脸特征数据。

[0115] 可选地，可以分别计算第一人脸特征数据与每组第二人脸特征数据之间的相似度，将相似度作为比对结果。

[0116] 可选地，可以通过神经网络或者其他机器学习的方法对第一图像与第二图像进行人脸比对。在一个可选的例子中，神经网络可以采用卷积神经网络。可选地，也可以采用其它类型的神经网络，本发明实施例对此不做限定。

[0117] 可选地，可以通过欧氏距离或者其它相似度确定原则确定相似度，本发明实施例对此不做限定。

[0118] 108，根据比对结果得到身份验证结果。

[0119] 可选地，可以通过将相似度与预设阈值进行比较，得到身份验证结果，其中，可以

将相似度大于预设阈值的情况，确定为身份验证成功，即待验证人与当前证卡中人脸照片中的人为同一人，将相似度小于或等于预设阈值的情况，确定为身份验证失败，即待验证人与当前证卡中人脸照片中的人为不同人。其中，预设阈值可以根据统计确定或者通过其它方法确定，本发明实施例对此不做限定。

[0120] 可选地，在根据第一图像与第二图像的人脸比对结果，得到身份验证结果之后，还可以显示第一图像中的人脸图像、第二图像和身份验证结果。例如：以“验证成功/验证失败”的文字信息，或者图标标识的身份验证结果。

[0121] 在一个可选的例子中，在显示第一图像中的人脸图像、第二图像和身份验证结果的同时，还可以显示第一图像与第二图像进行人脸比对的结果，例如：以百分数的形式表示的相似度值。

[0122] 基于本发明上述实施例提供的身份验证方法，通过利用第一图像采集单元获取当前证卡的第一图像，其中第一图像中包含人脸图像，以及利用第二图像采集单元获取包含待验证人人脸的第二图像，将第一图像与第二图像进行人脸比对，得到比对结果，根据比对结果得到身份验证结果，利用采集的证卡中的人脸图像，与实时采集的人脸图像进行人脸比对，可以实现在没有芯片读卡器的情况下对持证人身份的验证，从而可以有效防止人证不一致，盗用他人身份的情况。由于可以使用未内置芯片的证件进行身份验证，因此使得身份验证更加灵活，扩大了身份验证的应用场景。

[0123] 可选地，在上述各实施例中，在利用第一图像采集单元获取当前证卡的第一图像之前，还可以获取当前证卡的属性，其中证卡的属性可以包括内置芯片型证卡和非内置芯片型证卡。当当前证卡为非内置芯片型证卡时，可以执行上述各实施例中的操作进行身份验证，即从利用第一图像采集单元获取当前证卡的第一图像，其中，第一图像中包含人脸图像，开始执行直至得到身份验证结果。通过对证卡的属性按照是否内置芯片进行区分，可以根据当前证卡的属性来确定身份验证的方式，从而提高身份验证的灵活性和通用性。

[0124] 可选地，当当前证卡为内置芯片型证卡时，还可以利用芯片识别器获取当前证卡的芯片信息，其中芯片信息中包含内存的人脸图像，然后利用第二图像采集单元获取包含待验证人人脸的第二图像，将第二图像与芯片信息中内存的人脸图像进行人脸比对，得到比对结果，根据比对结果得到身份验证结果。基于证卡的属性进行身份验证，因此使得身份验证更加灵活，扩大了身份验证的应用场景。

[0125] 可选地，当当前证卡为内置芯片型证卡时，还可以对当前证卡进行真伪识别处理，当当前证卡为真实证件时，可以通过上述方法进行身份验证。

[0126] 在一个可选地的例子中，可以分别利用第一图像采集装置和芯片识别器获取当前证卡外置和内存的信息，通过对当前证卡外置与内存的信息进行比对，来识别当前证卡的真伪。下面将结合图2，详细描述本发明实施例提出的身份验证方法利用第一图像采集装置和芯片识别器对当前证卡进行真伪识别处理的流程。

[0127] 应理解，图2所示的例子仅仅是为了帮助本领域技术人员更好地理解本发明的技术方案，而不应理解成对本发明的限定。本领域技术人员可以在图2的基础上进行各种变换，而这种变换也应理解成本发明技术方案的一部分。

[0128] 如图2所示，该方法包括：

[0129] 202，利用第一图像采集单元获取当前证卡的第一图像，其中，第一图像中包含外

置的人脸图像。

[0130] 可选地，第一图像采集单元包括但不限于摄像头、扫描仪和数码相机，因此可以先通过扫描仪对当前证卡进行扫描，或者通过摄像头/数码相机对当前证卡进行拍摄，之后再通过OCR(Optical Character Recognition，光学字符识别)方式获取外置的人脸图像。

[0131] 可选地，第一图像中除包含外置的人脸图像外，还可以包括外置的文字信息。

[0132] 204，利用芯片识别器获取当前证卡的芯片信息，其中，芯片信息中包含内存的人脸图像。

[0133] 可选地，芯片识别器可以采用非接触IC卡阅读技术，在通过内嵌的安全控制模块(Secure Access Module，SAM)以无线传输方式与卡证内专用的芯片进行安全认证后，将芯片中的信息读出。

[0134] 可选地，芯片信息中除包含内存的人脸图像外，还可以包含文字信息。

[0135] 206，将第一图像与芯片信息比对，得到比对结果。

[0136] 在本实施例中，将上述外置的人脸图像与内存的人脸图像进行比对，获取比对结果。

[0137] 可选地，当第一图像中包含外置的文字信息且芯片信息中包含内存的文字信息时，还可以将外置的文字信息与内存的文字信息进行比对，得到对应的比对结果。

[0138] 208，根据比对结果确定当前证卡的真伪性。

[0139] 可选地，若上述外置的人脸图像与内存的人脸图像一致，可以确定当前证卡为真实证件，若上述外置的人脸图像与内存的人脸图像不一致，可以向用户做出提示，例如：以语音和/或文字的形式做出提示。

[0140] 可选地，当第一图像中包含外置的文字信息且芯片信息中包含内存的文字信息时，除了将上述外置的人脸图像与内存的人脸图像进行比对，获取比对结果外，还将上述外置的文字信息与内存的文字信息进行比对，获取对应的比对结果。此时，若上述外置的人脸图像和文字信息与内存的人脸图像和文字信息均一致，可以确定当前证卡为真实证件，若上述外置的人脸图像和文字信息与内存的人脸图像和文字信息存在不一致的情况，可以向用户做出提示。

[0141] 可选地，操作204利用芯片识别器获取的当前证卡的芯片信息可以用于身份验证。即，当确定当前证卡为真实证件时，可以利用第二图像采集单元获取包含待验证人人脸的第二图像，然后将第二图像与操作204利用芯片识别器获取的当前证卡的芯片信息中的人脸图像进行人脸比对，得到比对结果，从而根据比对结果得到身份验证结果。

[0142] 基于本发明上述实施例提供的身份验证方法，通过获取内置芯片型证卡外置和内存的信息，对内置芯片型证卡外置与内存的信息进行比对，来识别内置芯片型证卡的真伪，为辨别内置芯片型证卡的真伪提供了简单有效的方法，可以防止通过伪造的证卡盗用他人身份的情况。

[0143] 可选地，在上述各实施例中，第一图像中除了包含人脸图像外，还可以包含文字部分，其中，文字部分可以是当前证卡中记载的文字内容。

[0144] 在将第一图像与第二图像进行人脸比对，得到比对结果之前，还可以对第一图像进行处理，分离第一图像中的人脸图像和/或文字部分，以将第一图像中的人脸图像与文字部分分离开来，得到第一图像中的人脸图像，从而通过将第一图像中的人脸图像与第二图

像进行人脸比对，可以得到身份验证结果。

[0145] 可选地，在分离第一图像中的人脸图像和/或文字部分之前，还可以判断第一图像中是否包含人脸图像，当第一图像中未包含人脸图像时，可以提示用户重新放置当前证卡。例如：可以通过语音形式提醒用户重新放置当前证卡。

[0146] 可选地，还可以判断第一图像中是否包含文字部分，当第一图像中包含文字部分时，可以对文字部分进行文字识别处理，得到证卡中的文字信息。下面将结合图3，详细描述在本发明实施例提出的身份验证方法中包括对当前证卡中的文字信息进行文字识别处理的流程。

[0147] 应理解，图3所示的例子仅仅是为了帮助本领域技术人员更好地理解本发明的技术方案，而不应理解成对本发明的限定。本领域技术人员可以在图3的基础上进行各种变换，而这种变换也应理解成本发明技术方案的一部分。

[0148] 如图3所示，该方法包括：

[0149] 302，对第一图像中的文字部分进行特征提取，得到文字部分的特征数据。

[0150] 304，确定文字部分的特征数据与预设数据库中预设文字对应的特征数据之间的相似度。

[0151] 306，将大于相似度阈值的特征数据对应的预设文字，作为文字识别的结果。

[0152] 308，根据文字识别的结果得到当前证卡中的文字信息。

[0153] 可选地，证卡中的文字信息可以包括但不限于姓名、性别、民族、出生日期、住址、证件号码等信息页中的个人信息。

[0154] 可选地，可以通过神经网络或者其他机器学习的方法对第一图像中的文字部分进行文字识别处理。在一个可选的例子中，神经网络可以采用卷积神经网络。可选地，也可以采用其它类型的神经网络，本发明实施例对此不做限定。

[0155] 可选地，可以通过欧氏距离或者其它的相似度确定原则确定相似度，本发明实施例对此不做限定。

[0156] 可选地，本发明实施例的方法还可以包括：显示当前证卡中的文字信息。在一个可选的例子中，可以在第一图像中的人脸图像、第二图像和身份验证结果的同时，显示当前证卡中的文字信息。

[0157] 基于本发明上述实施例提供的身份验证方法，在将当前证卡中的人脸图像与待验证人的人脸图像进行人脸比对时，通过对当前证卡中的文字部分进行识别，可以得到当前证卡中的文字信息，从而可以获得当前证卡所有人的身份信息，当待验证人的人脸图像与当前证卡中的人脸图像的人脸比对一致时，可以通过当前证卡中的文字信息进一步获得待验证人的身份信息。

[0158] 本发明实施例还提出了一种身份验证装置，图4是本发明一些实施例提供的身份验证装置的结构示意图。

[0159] 应理解，图4所示的例子仅仅是为了帮助本领域技术人员更好地理解本发明的技术方案，而不应理解成对本发明的限定。本领域技术人员可以在图4的基础上进行各种变换，而这种变换也应理解成本发明技术方案的一部分。

[0160] 如图4所示，该装置包括：第一图像采集单元401、第二图像采集单元402、图像比对单元403和身份验证单元404。其中，

[0161] 第一图像采集单元401，用于获取当前证卡的第一图像，其中，第一图像中包含人脸图像。

[0162] 可选地，证卡，是指各种证件、卡片、证照和票证的总称。例如：各种证件可以是身份证、驾照、护照、学生证、工作证等包含人脸照片的证件，证照可以是黑白或者彩色照片等。第一图像可以是采集自包含人脸照片的证卡的图像，本发明实施例对此不做限定。

[0163] 可选地，第一图像采集单元401包括但不限于摄像头、扫描仪和数码相机等，因此可以先通过扫描仪对当前证卡进行扫描，或者通过摄像头/数码相机对当前证卡进行拍摄，之后通过OCR(Optical Character Recognition，光学字符识别)方式获取第一图像，本发明实施例对此不做限定。

[0164] 第二图像采集单元402，用于获取包含待验证人人脸的第二图像。

[0165] 可选地，第二图像可以是现场采集的图像，第二图像采集单元402可以是摄像头或者数码相机等，因此可以通过摄像头或者数码相机对待验证人进行拍摄方式获取第二图像，本发明实施例对此不做限定。

[0166] 在一个可选的例子中，第一图像采集单元401与第二图像采集单元402可以为同一个图像采集单元。例如：第一图像采集单元401和第二图像采集单元402可以为同一摄像头或者数码相机。

[0167] 图像比对单元403，用于将第一图像与第二图像进行人脸比对，得到比对结果。

[0168] 可选地，图像比对单元403可以对第一图像中的人脸图像进行特征提取，得到第一人脸特征数据，以及对第二图像进行特征提取，得到至少一组第二人脸特征数据，将第一人脸特征数据与至少一组第二人脸特征数据进行比对，得到比对结果。

[0169] 可选地，图像比对单元403可以分别计算第一人脸特征数据与每组第二人脸特征数据之间的相似度，将相似度作为比对结果。

[0170] 可选地，图像比对单元403可以通过神经网络或者其他机器学习的方法对第一图像与第二图像进行人脸比对。在一个可选的例子中，神经网络可以采用卷积神经网络。可选地，也可以采用其它类型的神经网络，本发明实施例对此不做限定。

[0171] 可选地，图像比对单元403可以通过欧氏距离或者其它相似度确定原则确定相似度，本发明实施例对此不做限定。

[0172] 身份验证单元404，用于根据比对结果得到身份验证结果。

[0173] 可选地，身份验证单元404可以通过将相似度与预设阈值进行比较，得到身份验证结果，其中，可以将相似度大于预设阈值的情况，确定为身份验证成功，即待验证人与当前证卡中人脸照片中的人为同一人，将相似度小于或等于预设阈值的情况，确定为身份验证失败，即待验证人与当前证卡中人脸照片中的人为不同人。其中，预设阈值可以根据统计确定或者通过其它方法确定，本发明实施例对此不做限定。

[0174] 可选地，该装置还可以包括：信息显示单元，用于显示第一图像中的人脸图像、第二图像和身份验证结果。例如：以“验证成功/验证失败”的文字信息，或者图标标识身份验证结果。

[0175] 在一个可选的例子中，信息显示单元在显示第一图像中的人脸图像、第二图像和身份验证结果的同时，还可以显示第一图像与第二图像进行人脸比对的结果，例如：以百分数的形式表示的相似度值。

[0176] 基于本发明上述实施例提供的身份验证装置，通过利用第一图像采集单元获取当前证卡的第一图像，其中第一图像中包含人脸图像，以及利用第二图像采集单元获取包含待验证人人脸的第二图像，将第一图像与第二图像进行人脸比对，得到比对结果，根据比对结果得到身份验证结果，利用采集的证卡中的人脸图像，与实时采集的人脸图像进行人脸比对，可以实现在没有芯片读卡器的情况下对持证人身份的验证，从而可以有效防止人证不一致，盗用他人身份的情况。由于可以使用未内置芯片的证件进行身份验证，因此使得身份验证更加灵活，扩大了身份验证的应用场景。

[0177] 图5是本发明另一些实施例提供的身份验证装置的结构示意图。应理解，图5所示的例子仅仅是为了帮助本领域技术人员更好地理解本发明的技术方案，而不应理解成对本发明的限定。本领域技术人员可以在图5的基础上进行各种变换，而这种变换也应理解成本发明技术方案的一部分。

[0178] 如图5所示，与图4的实施例相比较，不同之处在于，该实施例的装置还包括：属性获取单元505。属性获取单元505用于获取当前证卡的属性，其中证卡的属性可以包括内置芯片型证卡和非内置芯片型证卡。当前证卡为非内置芯片型证卡时，第一图像采集单元501、第二图像采集单元502、图像比对单元503和身份验证单元504执行与图4实施例中相同的操作。

[0179] 可选地，如图5所示，该装置还可以包括：芯片识别器506。当当前证卡为内置芯片型证卡时，芯片识别器506用于获取当前证卡的芯片信息，其中芯片信息中包含内存的人脸图像，此时，第二图像采集单元502用于获取包含待验证人人脸的第二图像，图像比对单元503用于将第二图像与芯片信息中内存的人脸图像进行人脸比对，得到比对结果，身份验证单元540用于根据比对结果得到身份验证结果。

[0180] 可选地，如图5所示，该装置还可以包括：真伪识别单元507。真伪识别单元507用于当当前证卡为内置芯片型证卡时，对当前证卡进行真伪识别处理。

[0181] 可选地，在对当前证卡进行真伪识别时，第一图像采集单元501用于获取当前证卡的第一图像，其中第一图像中包含外置的人脸图像，芯片识别器506用于获取当前证卡的芯片信息，其中芯片信息中包含内存的人脸图像，真伪识别单元507用于将第一图像与芯片信息比对，得到比对结果，以及根据比对结果确定当前证卡的真伪性。

[0182] 可选地，芯片识别器506可以采用非接触IC卡阅读技术，在通过内嵌的安全控制模块(Secure Access Module，SAM)以无线传输方式与卡证内专用的芯片进行安全认证后，将芯片中的信息读出。

[0183] 在本实施例中，真伪识别单元507用于将上述外置的人脸图像与内存的人脸图像进行比对，获取比对结果。

[0184] 可选地，若上述外置的人脸图像与内存的人脸图像一致，可以确定当前证卡为真实证件，若上述外置的人脸图像与内存的人脸图像不一致，可以向用户做出提示，例如：以语音和/或文字的形式做出提示。

[0185] 可选地，第一图像采集单元501获取的第一图像中除包含外置的人脸图像外，还可以包括外置的文字信息。

[0186] 可选地，芯片识别器506获取的芯片信息中除包含内存的人脸图像外，还可以包含文字信息。

[0187] 可选地，当第一图像中包含外置的文字信息且芯片信息中包含内存的文字信息时，真伪识别单元507还可以将上述外置的文字信息与内存的文字信息进行比对，得到对应的比对结果。

[0188] 可选地，在真伪识别单元507将上述外置的人脸图像和文字信息与内存的人脸图像和文字信息分别进行比对，得到比对结果时，若上述外置的人脸图像和文字信息与内存的人脸图像和文字信息均一致，可以确定当前证卡为真实证件，若上述外置的人脸图像和文字信息与内存的人脸图像和文字信息存在不一致的情况，可以向用户做出提示。

[0189] 可选地，在确定当前证卡为真实证件后，可以利用芯片识别器506获取的当前证卡的芯片信息中的人脸图像，进行身份识别，此时，第二图像采集单元502用于获取包含待验证人人脸的第二图像，图像比对单元503用于将第二图像与芯片信息中内存的人脸图像进行人脸比对，得到比对结果，身份验证单元504用于根据比对结果得到身份验证结果。

[0190] 图6是本发明又一些实施例提供的身份验证装置的结构示意图。应理解，图6所示的例子仅仅是为了帮助本领域技术人员更好地理解本发明的技术方案，而不应理解成对本发明的限定。本领域技术人员可以在图6的基础上进行各种变换，而这种变换也应理解成本发明技术方案的一部分。

[0191] 如图6所示，与图4的实施例相比较，不同之处在于，该实施例的装置还包括：图文分离单元608。图文分离单元608用于对第一图像进行处理，分离第一图像中的人脸图像和/或文字部分。此时，第一图像采集单元601获取的当前证卡的第一图像中除了包含人脸图像外，还可以包含文字部分，其中文字部分可以是当前证卡中记载的文字内容。

[0192] 可选地，该装置还可以包括：第一检测单元和信息提示单元，第一检测单元用于判断第一图像中是否包含人脸图像，信息提示单元用于当第一图像中未包含人脸图像时，提示用户重新放置当前证卡。

[0193] 可选地，如图6所示，该装置还可以包括：第二检测单元和文字识别单元609，第二检测单元用于判断第一图像中是否包含所述文字部分，文字识别单元609用于当第一图像中包含文字部分时，对第一图像中的文字部分进行文字识别处理，得到当前证卡中的文字信息。

[0194] 可选地，证卡中的文字信息可以包括但不限于姓名、性别、民族、出生日期、住址、证件号码等信息页中的个人信息。

[0195] 可选地，文字识别单元609可以对第一图像中的文字部分进行特征提取，得到文字部分的特征数据，然后确定文字部分的特征数据与预设数据库中预设文字对应的特征数据之间的相似度，将大于相似度阈值的特征数据对应的预设文字，作为文字识别的结果，根据文字识别的结果得到当前证卡中的文字信息。

[0196] 可选地，文字识别单元609可以通过神经网络或者其他机器学习的方法对第一图像中的文字部分进行文字识别处理。在一个可选的例子中，神经网络可以采用卷积神经网络。可选地，也可以采用其它类型的神经网络，本发明实施例对此不做限定。

[0197] 可选地，文字识别单元609可以通过欧氏距离或者其它的相似度确定原则确定相似度，本发明实施例对此不做限定。

[0198] 可选地，如图6所示，该装置还可以包括：信息显示单元610，用于显示第一图像中的人脸图像、第二图像、身份验证结果和当前证卡中的文字信息。

[0199] 另外，本发明实施例还提供了一种电子设备，例如可以是移动终端、个人确定机(PC)、平板电脑、服务器等，该电子设备设置有本发明上述任一实施例的身份验证装置。

[0200] 本发明实施例还提供了一种电子设备，例如可以是移动终端、个人确定机(PC)、平板电脑、服务器等。下面参考图7，其示出了适于用来实现本申请实施例的终端设备或服务器的电子设备700的结构示意图：如图7所示，电子设备700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)701，和/或一个或多个图像处理器(GPU)713等，处理器可以根据存储在只读存储器(ROM)702中的可执行指令或者从存储部分708加载到随机访问存储器(RAM)703中的可执行指令而执行各种适当的动作和处理。通信部712可包括但不限于网卡，所述网卡可包括但不限于IB(Infiniband)网卡。

[0201] 处理器可与只读存储器702和/或随机访问存储器703中通信以执行可执行指令，通过总线704与通信部712相连、并经通信部712与其他目标设备通信，从而完成本申请实施例提供的任一项方法对应的操作，例如，利用第一图像采集单元获取当前证卡的第一图像，其中，所述第一图像中包含人脸图像；利用第二图像采集单元获取包含待验证人人脸的第二图像；将所述第一图像与所述第二图像进行人脸比对，得到比对结果；根据所述比对结果得到身份验证结果。

[0202] 此外，在RAM 703中，还可存储有装置操作所需的各种程序和数据。CPU701、ROM702以及RAM703通过总线704彼此相连。在有RAM703的情况下，ROM702为可选模块。RAM703存储可执行指令，或在运行时向ROM702中写入可执行指令，可执行指令使处理器701执行上述通信方法对应的操作。输入/输出(I/O)接口705也连接至总线704。通信部712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。

[0203] 以下部件连接至I/O接口705：包括键盘、鼠标等的输入部分706；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707；包括硬盘等的存储部分708；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分709。通信部分709经由诸如因特网的网络执行通信处理。驱动器710也根据需要连接至I/O接口705。可拆卸介质711，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710上，以便于从其上读出的确定机程序根据需要被安装入存储部分708。

[0204] 需要说明的，如图7所示的架构仅为一种可选实现方式，在具体实践过程中，可根据实际需要对上述图7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GPU和CPU可分离设置或者可将GPU集成在CPU上，通信部可分离设置，也可集成设置在CPU或GPU上，等等。这些可替换的实施方式均落入本发明公开的保护范围。

[0205] 特别地，根据本发明的实施例，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，本发明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，利用第一图像采集单元获取当前证卡的第一图像，其中，所述第一图像中包含人脸图像；利用第二图像采集单元获取包含待验证人人脸的第二图像；将所述第一图像与所述第二图像进行人脸比对，得到比对结果；根据所述比对结果得到身份验证结果。在这样的实施例中，该计算机程序可以通过通信部分709从网络上被下载和安装，和/或从可拆卸介质711被安装。在该计算机程序被中

央处理单元(CPU)701执行时,执行本申请的方法中限定的上述功能。

[0206] 在一个或多个可选实施方式中,本发明实施例还提供了一种计算机程序程序产品,用于存储计算机可读指令,该指令被执行时使得计算机执行上述任一可能的实现方式中的身份验证方法。

[0207] 该计算机程序产品可以具体通过硬件、软件或其结合的方式实现。在一个可选例子中,该计算机程序产品具体体现为计算机存储介质,在另一个可选例子中,该计算机程序产品具体体现为软件产品,例如软件开发包(Software Development Kit,SDK)等等。

[0208] 在一个或多个可选实施方式中,本发明实施例还提供了一种身份验证方法及其对应的装置和电子设备、计算机存储介质、计算机程序以及计算机程序产品,其中,该方法包括:第一装置向第二装置发送身份验证指示,该指示使得第二装置执行上述任一可能的实施例中的身份验证方法;第一装置接收第二装置发送的身份验证结果。

[0209] 在一些实施例中,该身份验证指示可以具体为调用指令,第一装置可以通过调用的方式指示第二装置执行身份验证,相应地,响应于接收到调用指令,第二装置可以执行上述身份验证方法中的任意实施例中的步骤和/或流程。

[0210] 应理解,本发明实施例中的“第一”、“第二”等术语仅仅是为了区分,而不应理解成对本发明实施例的限定。

[0211] 还应理解,在本发明中,“多个”可以指两个或两个以上,“至少一个”可以指一个、两个或两个以上。

[0212] 还应理解,对于本发明中提及的任一部件、数据或结构,在没有明确限定或者在前后文给出相反启示的情况下,一般可以理解为一个或多个。

[0213] 还应理解,本发明对各个实施例的描述着重强调各个实施例之间的不同之处,其相同或相似之处可以相互参考,为了简洁,不再一一赘述。

[0214] 可能以许多方式来实现本发明的方法和装置、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发明的方法和装置、设备。用于方法的步骤的上述顺序仅是为了进行说明,本发明的方法的步骤不限于以上具体描述的顺序,除非以其它方式特别说明。此外,在一些实施例中,还可将本发明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发明的方法的机器可读指令。因而,本发明还覆盖存储用于执行根据本发明的方法的程序的记录介质。

[0215] 本发明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发明限于所公开的形式。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发明的原理和实际应用,并且使本领域的普通技术人员能够理解本发明从而设计适于特定用途的带有各种修改的各种实施例。

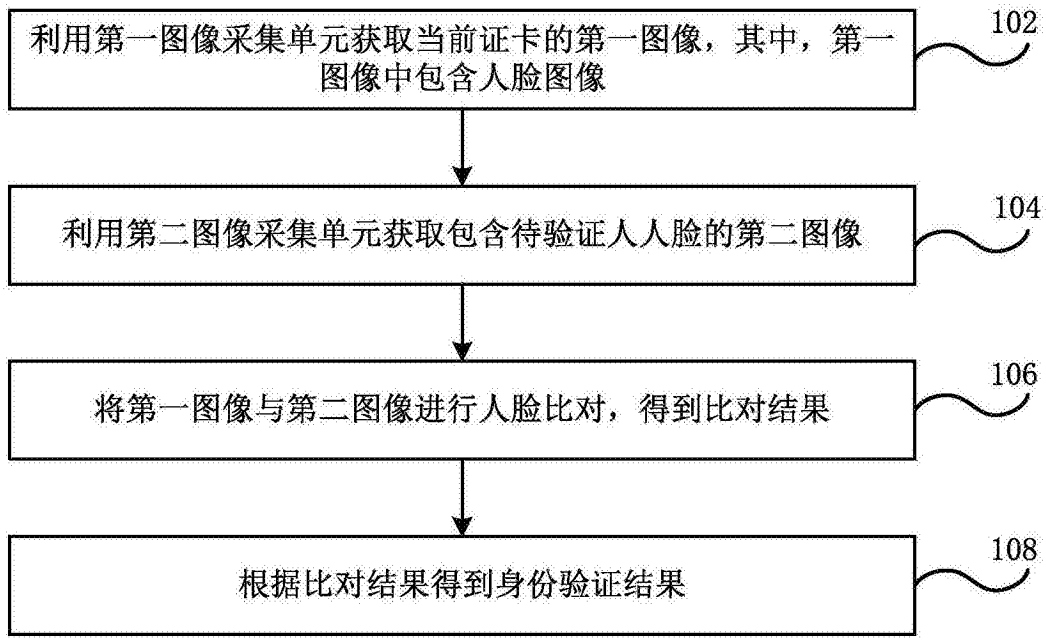

利用第一图像采集单元获取当前证卡的第一图像，其中，第一图像中包含人脸图像
102
利用第二图像采集单元获取包含待验证人人脸的第二图像
104
将第一图像与第二图像进行人脸比对，得到比对结果
106
根据比对结果得到身份验证结果
108

图1

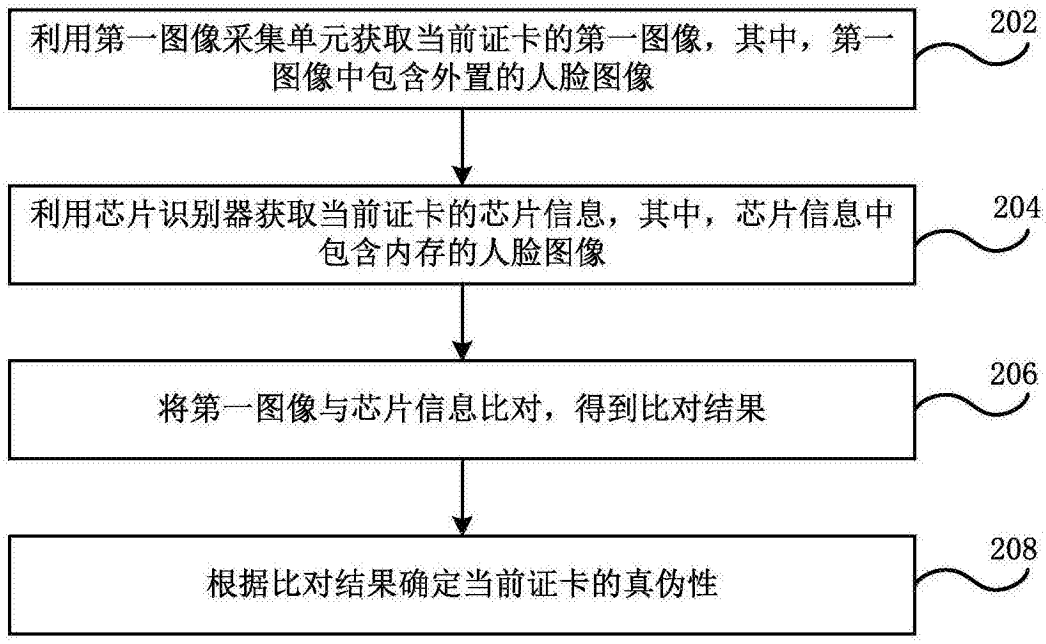

利用第一图像采集单元获取当前证卡的第一图像，其中，第一图像中包含外置的人脸图像
202
利用芯片识别器获取当前证卡的芯片信息，其中，芯片信息中包含内存的人脸图像
204
将第一图像与芯片信息比对，得到比对结果
206
根据比对结果确定当前证卡的真伪性
208

图2

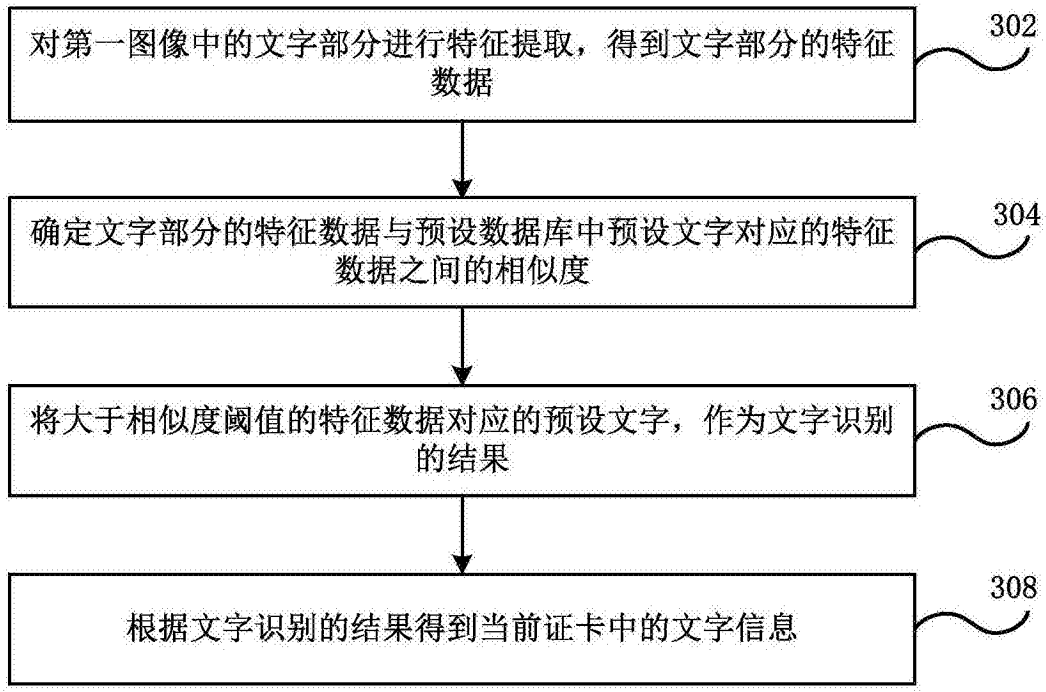

对第一图像中的文字部分进行特征提取，得到文字部分的特征数据
302
确定文字部分的特征数据与预设数据库中预设文字对应的特征数据之间的相似度
304
将大于相似度阈值的特征数据对应的预设文字，作为文字识别的结果
306
根据文字识别的结果得到当前证卡中的文字信息
308

图3

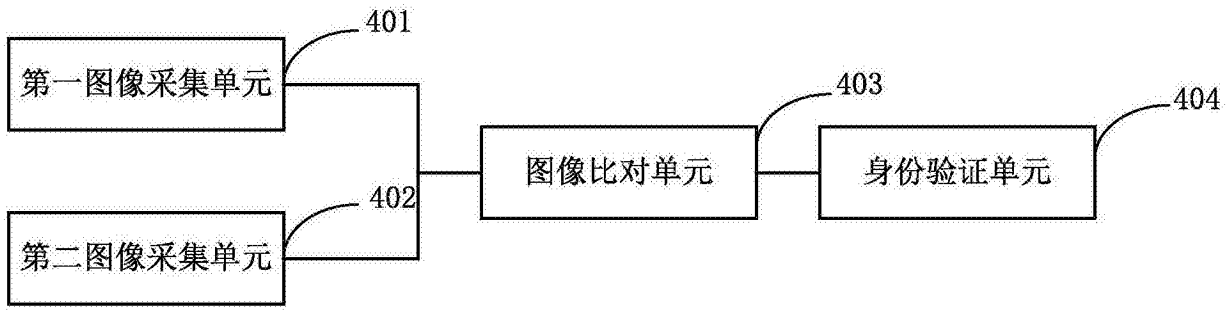

401
第一图像采集单元
402
第二图像采集单元
403
图像比对单元
404
身份验证单元

图4

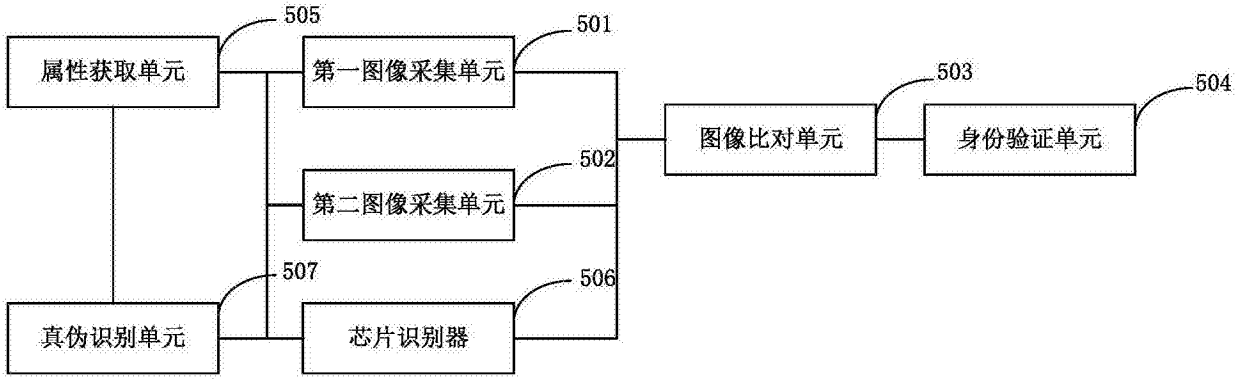

505
属性获取单元
501
第一图像采集单元
502
第二图像采集单元
503
图像比对单元
504
身份验证单元
507
真伪识别单元
506
芯片识别器

图5

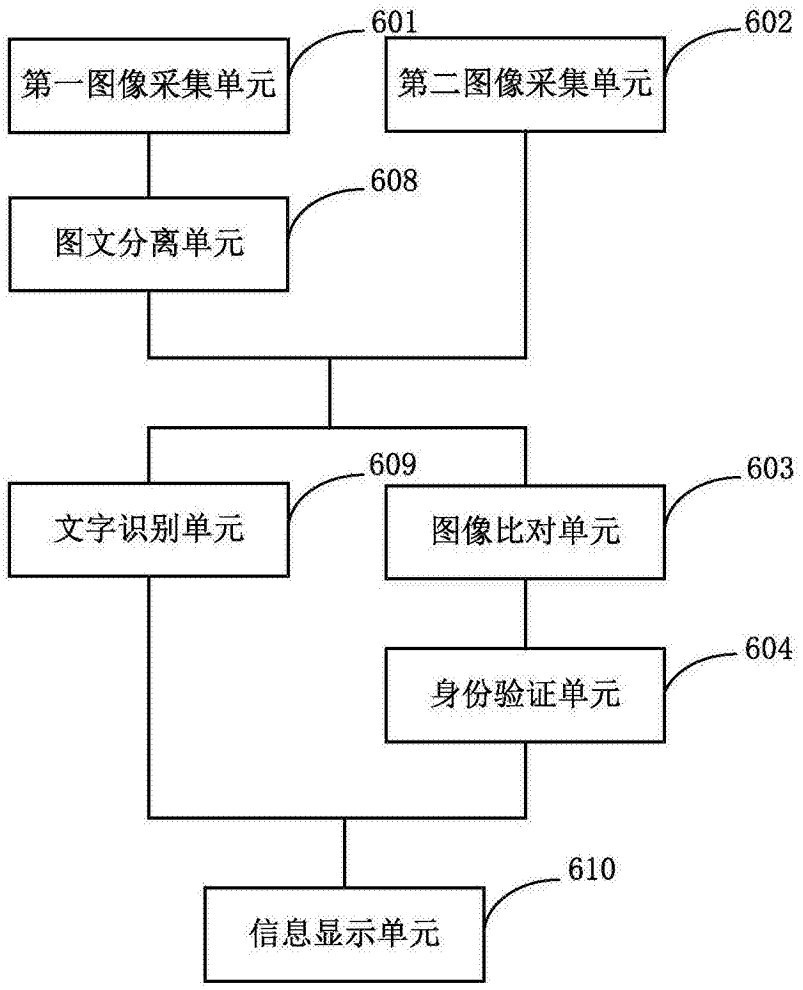

601
602
第一图像采集单元
第二图像采集单元
608
图文分离单元
609
603
文字识别单元
图像比对单元
604
身份验证单元
610
信息显示单元

图6

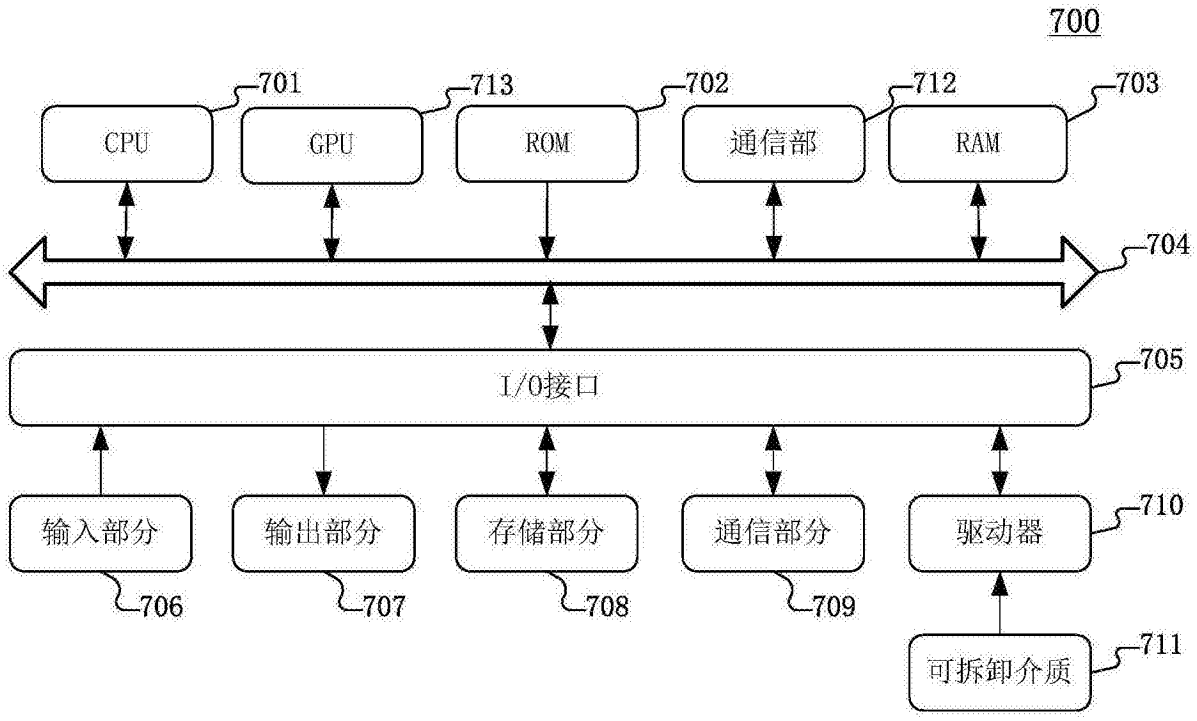

700
701
713
702
712
703
CPU
GPU
ROM
通信部
RAM
704
I/O接口
705
输入部分
输出部分
存储部分
通信部分
驱动器
710
706
707
708
709
可拆卸介质
711

图7