(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 111931153 B
(45)授权公告日 2021.02.19

(21)申请号 202011108276.3
(22)申请日 2020.10.16
(65)同一申请的已公布的文献号
申请公布号 CN 111931153 A
(43)申请公布日 2020.11.13
(73)专利权人 腾讯科技(深圳)有限公司
地址 518000 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 罗朝 白琨
(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 李文渊
(51)Int.Cl.
G06F 21/32(2013.01)
G06K 9/00(2006.01)

(56)对比文件
CN 106156578 A,2016.11.23
CN 106570489 A,2017.04.19
CN 111340013 A,2020.06.26

审查员 黄彰

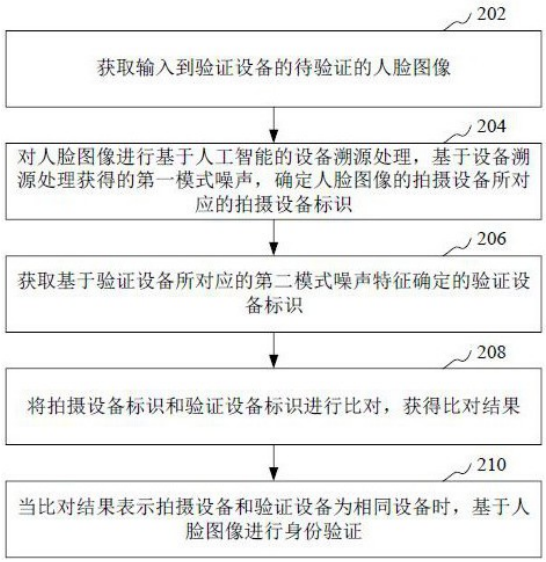
权利要求书3页 说明书16页 附图8页

(54)发明名称

基于人工智能的身份验证方法、装置和计算机设备

(57)摘要

本申请涉及一种基于人工智能的身份验证方法、装置、计算机设备和存储介质。所述方法包括:获取输入到验证设备的待验证的人脸图像;对人脸图像进行基于人工智能的设备溯源处理,基于设备溯源处理获得的第一模式噪声,确定人脸图像的拍摄设备所对应的拍摄设备标识;获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识;将拍摄设备标识和验证设备标识进行特征比对,获得比对结果;当比对结果表示拍摄设备和验证设备为相同设备时,基于人脸图像进行身份验证。采用本方法能够提高身份验证的准确率,确保身份验证的安全性。



CN 111931153 B

1.一种基于人工智能的身份验证方法,其特征在于,所述方法包括:

获取在进入的身份验证界面中,通过即时拍摄或本地上传输入到验证设备的待验证的人脸图像;

对所述人脸图像进行基于人工智能的设备溯源处理,基于所述设备溯源处理获得的第一模式噪声特征,确定所述人脸图像的拍摄设备所对应的拍摄设备标识;

查询所述验证设备的设备属性信息,从所述设备属性信息中,提取得到基于所述验证设备所对应的第二模式噪声特征确定的验证设备标识;

根据所述第一模式噪声特征和所述第二模式噪声特征之间的相似度,得到所述拍摄设备标识和所述验证设备标识之间的相似度,根据所述拍摄设备标识和所述验证设备标识之间的相似度,得到所述拍摄设备标识和所述验证设备标识进行特征比对的比对结果;

或查询预设的设备标识格式,根据所述设备标识格式定义的映射规则,将所述第一模式噪声特征和所述第二模式噪声特征映射为对应的字符串,根据所述第一模式噪声特征和所述第二模式噪声特征映射分别对应的字符串之间的比对结果,得到所述拍摄设备标识和所述验证设备标识之间的字符比对结果,根据所述字符比对结果,得到所述拍摄设备标识和所述验证设备标识进行特征比对的比对结果;

当所述比对结果表示所述拍摄设备和所述验证设备为相同设备、确定所述人脸图像由所述验证设备拍摄得到时,基于所述人脸图像进行身份验证;

当所述比对结果表示所述拍摄设备和所述验证设备为不同设备、确定所述人脸图像非所述验证设备拍摄得到时,指示所述验证设备展示验证失败提示消息,并指示所述验证设备展示描述所述人脸图像为非法图像的提示信息。

2.根据权利要求1所述的方法,其特征在于,所述特征比对的步骤包括:

确定所述第一模式噪声特征和所述第二模式噪声特征之间的余弦相似度;

根据所述余弦相似度得到所述拍摄设备标识和所述验证设备标识的比对结果。

3.根据权利要求2所述的方法,其特征在于,所述根据所述余弦相似度得到所述拍摄设备标识和所述验证设备标识的比对结果,包括:

当所述相似度大于相似度阈值时,得到表示所述拍摄设备和所述验证设备为相同设备的比对结果;

当所述相似度小于或等于所述相似度阈值时,得到表示所述拍摄设备和所述验证设备为不同设备的比对结果。

4.根据权利要求2所述的方法,其特征在于,所述对所述人脸图像进行基于人工智能的设备溯源处理,基于所述设备溯源处理获得的第一模式噪声特征,确定所述人脸图像的拍摄设备所对应的拍摄设备标识,包括:

对所述人脸图像进行至少一次的卷积操作,获得所述人脸图像的图像卷积特征;

对所述图像卷积特征进行非线性映射,得到第一模式噪声特征;

基于所述第一模式噪声特征,确定所述人脸图像的拍摄设备所对应的拍摄设备标识。

5.根据权利要求4所述的方法,其特征在于,所述基于所述第一模式噪声特征,确定所述人脸图像的拍摄设备所对应的拍摄设备标识,包括:

将所述第一模式噪声特征按照设备标识格式映射为字符串,得到所述人脸图像的拍摄设备所对应的拍摄设备标识;

所述特征比对的步骤包括：

对所述拍摄设备标识和所述验证设备标识进行字符比对，得到比对结果。

6.根据权利要求1所述的方法，其特征在于，所述设备溯源处理基于设备溯源网络模型实现，所述设备溯源网络模型通过模型训练步骤生成，所述模型训练步骤包括：

获取携带设备标识标签的训练图像；

通过待训练的设备溯源网络模型对所述训练图像进行至少一次的卷积操作，获得所述训练图像的训练卷积特征；

通过所述设备溯源网络模型对所述训练卷积特征进行非线性映射，得到训练模式噪声特征；

通过所述设备溯源网络模型根据所述训练模式噪声特征确定所述训练图像的拍摄设备所对应的预测设备标识；

根据所述设备标识标签和所述预测设备标识调整所述设备溯源网络模型的参数后继续进行训练，直至训练结束得到训练完成的设备溯源网络模型。

7.根据权利要求6所述的方法，其特征在于，所述根据所述设备标识标签和所述预测设备标识调整所述设备溯源网络模型的参数后继续进行训练，包括：

获得所述设备标识标签和所述预测设备标识之间的距离损失；

确定所述距离损失的梯度参数；

根据所述梯度参数对所述设备溯源网络模型的参数进行调整，并通过参数调整后的设备溯源网络模型继续进行训练。

8.根据权利要求1所述的方法，其特征在于，确定所述验证设备标识的步骤包括：

获取由所述验证设备拍摄得到的参考图像；

对所述参考图像进行基于人工智能的设备溯源处理，基于所述设备溯源处理获得的第二模式噪声特征，确定所述验证设备所对应的验证设备标识。

9.根据权利要求1至8任意一项所述的方法，其特征在于，所述基于所述人脸图像进行身份验证，包括：

获取验证标准图像；

将所述人脸图像与所述验证标准图像进行人脸比对，得到人脸比对结果；

根据所述人脸比对结果得到所述人脸图像的身份验证结果。

10.根据权利要求1至8任意一项所述的方法，其特征在于，所述验证失败提示消息和描述所述人脸图像为非法图像的提示信息在验证结果界面中展示。

11.一种基于人工智能的身份验证装置，其特征在于，所述装置包括：

人脸图像获取模块，用于获取在进入的身份验证界面中，通过即时拍摄或本地上传输入到验证设备的待验证的人脸图像；

设备溯源处理模块，用于对所述人脸图像进行基于人工智能的设备溯源处理，基于所述设备溯源处理获得的第一模式噪声特征，确定所述人脸图像的拍摄设备所对应的拍摄设备标识；

验证设备标识获取模块，用于查询所述验证设备的设备属性信息，从所述设备属性信息中，提取得到获取所述验证设备所对应的第二模式噪声特征确定的验证设备标识；

标识比对模块，用于根据所述第一模式噪声特征和所述第二模式噪声特征之间的相似

度，得到所述拍摄设备标识和所述验证设备标识之间的相似度，根据所述拍摄设备标识和所述验证设备标识之间的相似度，得到所述拍摄设备标识和所述验证设备标识进行特征比对的比对结果；或查询预设的设备标识格式，根据所述设备标识格式定义的映射规则，将所述第一模式噪声特征和所述第二模式噪声特征映射为对应的字符串，根据所述第一模式噪声特征和所述第二模式噪声特征映射分别对应的字符串之间的比对结果，得到所述拍摄设备标识和所述验证设备标识之间的字符比对结果，根据所述字符比对结果，得到所述拍摄设备标识和所述验证设备标识进行特征比对的比对结果；

身份验证处理模块，用于当所述比对结果表示所述拍摄设备和所述验证设备为相同设备、确定所述人脸图像由所述验证设备拍摄得到时，基于所述人脸图像进行身份验证；

验证结果展示模块，用于当所述比对结果表示所述拍摄设备和所述验证设备为不同设备、确定所述人脸图像非所述验证设备拍摄得到时，指示所述验证设备展示验证失败提示消息，并指示所述验证设备展示描述所述人脸图像为非法图像的提示信息。

12.根据权利要求11所述的装置，其特征在于，所述标识比对模块包括：

相似度确定模块，用于确定所述第一模式噪声特征和所述第二模式噪声特征之间的余弦相似度；

比对结果获得模块，用于根据所述余弦相似度得到所述拍摄设备标识和所述验证设备标识的比对结果。

13.根据权利要求12所述的装置，其特征在于，所述设备溯源处理模块包括：

卷积特征提取模块，用于对所述人脸图像进行至少一次的卷积操作，获得所述人脸图像的第一图像卷积特征；

噪声特征获得模块，用于对所述第一图像卷积特征进行非线性映射，得到第一模式噪声特征；

拍摄设备标识确定模块，用于基于所述第一模式噪声特征，确定所述人脸图像的拍摄设备所对应的拍摄设备标识。

14.一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，其特征在于，所述处理器执行所述计算机程序时实现权利要求1至10中任一项所述的方法的步骤。

15.一种计算机可读存储介质，存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现权利要求1至10中任一项所述的方法的步骤。

基于人工智能的身份验证方法、装置和计算机设备

技术领域

[0001] 本申请涉及计算机技术领域，特别是涉及一种基于人工智能的身份验证方法、装置、计算机设备和存储介质。

背景技术

[0002] 随着计算机技术的发展，越来越多的业务应用场景中需要进行实名身份验证，如互联网金融、个人征信、远程开户等业务，一般需要基于人脸识别技术进行身份验证。具体地，在身份验证时，需要用户通过移动端上传拍摄的人脸图像，再将人脸图像与用户的证件照片进行比对，判断上传的人脸图像与证件照片是否为同一人，从而实现实名身份验证。

[0003] 然而，目前在线进行身份验证的过程中，存在使用不真实的人脸图像，如从网络盗取的人脸图像进行验证的风险，影响了身份验证的准确率，导致身份验证的安全性存在隐患。

发明内容

[0004] 基于此，有必要针对上述技术问题，提供一种能够提高身份验证准确率，确保身份验证安全性的基于人工智能的身份验证方法、装置、计算机设备和存储介质。

[0005] 一种基于人工智能的身份验证方法，所述方法包括：

[0006] 获取输入到验证设备的待验证的人脸图像；

[0007] 对人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理获得的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识；

[0008] 获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识；

[0009] 将拍摄设备标识和验证设备标识进行特征比对，获得比对结果；

[0010] 当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证。

[0011] 一种基于人工智能的身份验证装置，所述装置包括：

[0012] 人脸图像获取模块，用于获取输入到验证设备的待验证的人脸图像；

[0013] 设备溯源处理模块，用于对人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理获得的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识；

[0014] 验证设备标识获取模块，用于获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识；

[0015] 标识比对模块，用于将拍摄设备标识和验证设备标识进行特征比对，获得比对结果；

[0016] 身份验证处理模块，用于当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证。

[0017] 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现以下步骤：

[0018] 获取输入到验证设备的待验证的人脸图像；

[0019] 对人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理获得的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识；

[0020] 获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识；

[0021] 将拍摄设备标识和验证设备标识进行特征比对，获得比对结果；

[0022] 当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证。

[0023] 一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现以下步骤：

[0024] 获取输入到验证设备的待验证的人脸图像；

[0025] 对人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理获得的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识；

[0026] 获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识；

[0027] 将拍摄设备标识和验证设备标识进行特征比对，获得比对结果；

[0028] 当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证。

[0029] 上述基于人工智能的身份验证方法、装置、计算机设备和存储介质，对输入到验证设备的人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理得到的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识，在拍摄设备标识与基于验证设备所对应的第二模式噪声特征确定的验证设备标识的比对结果表示拍摄设备和验证设备为相同设备时，确定输入验证设备的人脸图像是真实可靠的，并基于人脸图像进行身份验证。通过对输入到验证设备的人脸图像进行基于人工智能的设备溯源处理，根据基于模式噪声得到的人脸图像的拍摄设备所对应的拍摄设备标识与验证设备的验证设备标识进行特征比对，在确定人脸图像的拍摄设备为验证设备时，基于人脸图像进行身份验证，确保了输入到验证设备的人脸图像的真实性和可靠性，从而提高了基于人脸图像进行身份验证的准确率，确保了身份验证的安全性。

附图说明

[0030] 图1为一个实施例中基于人工智能的身份验证方法的应用环境图；

[0031] 图2为一个实施例中基于人工智能的身份验证方法的流程示意图；

[0032] 图3为一个实施例中身份验证界面的界面示意图；

[0033] 图4为一个实施例中设备溯源处理的流程示意图；

[0034] 图5为一个实施例中参考图像上传界面的界面示意图；

[0035] 图6为一个实施例中验证结果界面的界面示意图；

[0036] 图7为另一个实施例中基于人工智能的身份验证方法的流程示意图；

[0037] 图8为一个实施例中网络训练的流程示意图；

[0038] 图9为图8所示实施例中全连接层的结构示意图；

[0039] 图10为一个实施例中基于人工智能的身份验证装置的结构框图；

[0040] 图11为一个实施例中计算机设备的内部结构图。

具体实施方式

[0041] 为了使本申请的目的、技术方案及优点更加清楚明白，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。

[0042] 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。

[0043] 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。

[0044] 其中，机器学习(Machine Learning, ML)是一门多领域交叉学科，涉及概率论、统计学、逼近论、凸分析、算法复杂度理论等多门学科。专门研究计算机怎样模拟或实现人类的学习行为，以获取新的知识或技能，重新组织已有的知识结构使之不断改善自身的性能。机器学习是人工智能的核心，是使计算机具有智能的根本途径，其应用遍及人工智能的各个领域。机器学习和深度学习通常包括人工神经网络、置信网络、强化学习、迁移学习、归纳学习、式教学习等技术。

[0045] 随着人工智能技术研究和进步，人工智能技术在多个领域展开研究和应用，例如常见的智能家居、智能穿戴设备、虚拟助理、智能音箱、智能营销、无人驾驶、自动驾驶、无人机、机器人、智能医疗、智能客服等，相信随着技术的发展，人工智能技术将在更多的领域得到应用，并发挥越来越重要的价值。本申请实施例提供的方案涉及人工智能的机器学习技术在身份验证场景中的应用，具体通过如下实施例进行说明：

[0046] 本申请提供的基于人工智能的身份验证方法，可以应用于如图1所示的应用环境中。其中，终端102通过网络与服务器104进行通信。终端102对输入到终端102的人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理得到的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识，在拍摄设备标识与基于终端102所对应的第二模式噪声特征确定的验证设备标识的比对结果表示拍摄设备和终端102为相同设备时，确定输入终端102的人脸图像是真实可靠的，并从服务器104获取证件图像，以基于证件图像与人脸图像进行身份验证。此外，进行身份验证的证件图像也可以直接输入到终端102，从而由终端102单独实现基于人工智能的身份验证方法。另外，也可以由服务器104进行身份验证，即由服务器104获取输入到终端102的人脸图像，并对人脸图像进行基于人工智能的设备溯源处理，根据基于模式噪声得到的人脸图像的拍摄设备所对应的拍摄设备标识与验证设备的验证设备标识进行特征比对，在确定人脸图像的拍摄设备为验证设备时，由服务器104基于人脸图像和证件图像进行身份验证，其中，证件图像可以由服务器104从本地数据库中获取或由服务器104从终端102获取。其中，终端102可以但不限于是各种个人计算机、笔记本电脑、智能手机、平板电脑和便携式可穿戴设备，服务器104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、CDN(Content Delivery Network,内容分发网络)、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。终端可以是智能手机、平板电脑、笔记本电脑、台式计算机、智能音箱、智能手表等,但并不局限于此。终端102以及服务器104可以通过有线或无线通信方式进行直接或间接地连接,本申请在此不做限制。

[0047] 在一个实施例中,如图2所示,提供了一种基于人工智能的身份验证方法,以该方法应用于图1中的终端为例进行说明,包括以下步骤:

[0048] 步骤202,获取输入到验证设备的待验证的人脸图像。

[0049] 其中,验证设备可以为用户发起进行身份验证的终端设备,人脸图像是需要进行验证的包含用户人脸部位的图片,人脸图像可以是需要验证身份的用户的人脸照片,从而可以基于人脸图像进行身份验证,如可以判断人脸图像是否与证件图像一致,实现实名认证。

[0050] 具体地,验证设备获取输入的待验证的人脸图像,人脸图像可能是验证设备拍摄得到的,也可能是非该验证设备拍摄的,而是从网络上盗取的,若人脸图像是从网络上盗取并输入验证设备,那么若基于该人脸图像进行身份验证,身份验证的安全性存在风险,身份验证的准确率有限。

[0051] 在具体实现时,如图3所示,在正常使用场景下,用户可以在验证设备进入的身份验证界面中上传人脸图像或拍摄人脸照片,以上传到身份验证界面中预览区域确认无误,提交后即可以根据人脸图像进行身份验证,以确保验证设备操作用户的身份。如图3中,在正常使用场景下,若用户通过立即拍照控件触发验证设备进行照片拍摄,则验证设备在预览区域展示验证设备当前拍摄的照片,此时可继续执行后续流程,以基于当前拍摄的照片进行身份验证。若用户通过上传人脸图像控件触发上传人脸图像,则可以从验证设备本地存储的图像中选择人脸图像在预览区域进行展示,而此时如果选择的人脸图像不是验证设备拍摄的,比如是从网络上获取的,则在执行后续的流程后,无法通过身份验证。在非法使用场景下,黑客可能通过一些计算机侵入方式,在验证设备输入非法获取的照片,企图利用该照片通过后续的身份验证,但采用本申请提供的方案,在这种非法使用场景下黑客将无法顺利通过身份验证。

[0052] 步骤204,对人脸图像进行基于人工智能的设备溯源处理,基于设备溯源处理获得的第一模式噪声,确定人脸图像的拍摄设备所对应的拍摄设备标识。

[0053] 其中,设备溯源是指追溯图像的拍摄设备的过程,如判断一张图片由何种设备拍摄;又如在同一类型拍摄设备中,判断图片由哪一台拍摄设备拍摄。通过人脸图像进行设备溯源处理,可以确定人脸图像的拍摄设备,如可以获得人脸图像的拍摄设备所对应的拍摄设备标识。第一模式噪声特通过对输入到验证设备的人脸图像进行设备溯源处理提取得到,第一模式噪声特征反映了人脸图像的拍摄设备的模式噪声,将第一模式噪声特征可以作为拍摄设备的拍摄设备标识,以对各设备进行准确区分。其中,模式噪声是具备拍摄功能的设备的固有属性,具体地,一般相机的传感器感光面由能够存储信号电荷的光刻单元组成,而由于光刻单元对光感应的不均匀性以及相机传感器制造工艺的不足使每个相机都会存在系统噪声,即模式噪声,且每个相机的模式噪声都不同,但有唯一的对应关系,因相机个体而异,如同人的指纹特征一样,从而也可以将反映模式噪声的模式噪声特征作为各种

设备的标识，以对各种具有拍摄功能的设备进行区别。拍摄设备标识用于区分各种拍摄设备，如可以为拍摄设备的ID(Identity document，身份标识号)、拍摄设备的特征等能够用于区分拍摄设备的信息。

[0054] 具体地，在验证设备输入待验证的人脸图像后，验证设备基于人工智能技术，如通过预训练的神经网络模型对人脸图像进行设备溯源处理，从而基于设备溯源处理得到的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识，通过拍摄设备标识可以区别不同图像对应的拍摄设备，从而确定人脸图像的拍摄来源。

[0055] 步骤206，获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识。

[0056] 其中，第二模式噪声特征反映了验证设备的模式噪声。第二模式噪声特征可以通过对由验证设备拍摄的图像进行设备溯源处理提取得到。验证设备标识用于区别各种验证设备，不同验证设备对应于不同的验证设备标识，具体可以为验证设备的模式噪声特征或模式噪声特征经过映射后得到的字符串等能够用于区分设备的信息。对模式噪声特征按照一定的映射规则进行映射处理，可以将模式噪声特征映射为可读性更强的字符串，可以将该字符串作为验证设备标识，以通过该字符串对各验证设备进行区分。

[0057] 具体地，验证设备进一步获取基于自身所对应的第二模式噪声特征确定的验证设备标识。在具体实现时，验证设备所对应的验证设备标识可以存储在设备属性信息中，从而从设备属性信息中提取得到验证设备标识；此外，验证设备标识也可以通过对由验证设备拍摄的图像进行基于人工智能的设备溯源处理得到。

[0058] 步骤208，将拍摄设备标识和验证设备标识进行特征比对，获得比对结果。

[0059] 得到人脸图像的拍摄设备所对应的拍摄设备标识和验证设备的验证设备标识后，验证设备比对拍摄设备标识和验证设备标识，如对设备的模式噪声特征映射后的字符串进行特征比对，或对模式噪声特征进行特征比对，得到比对结果。特征比对的比对结果反映了输入到验证设备的人脸图像的拍摄设备与验证设备的关系，根据比对结果可以确定输入到验证设备的人脸图像是否由验证设备拍摄得到。

[0060] 步骤210，当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证。

[0061] 得到比对结果后，若比对结果表示拍摄设备和验证设备为相同设备时，如拍摄设备标识和验证设备标识相同时，则可以确定输入到验证设备的人脸图像由验证设备拍摄得到，验证设备基于人脸图像进行身份验证处理，具体如可以将人脸图像与验证标准图像进行人脸比对，得到身份验证结果。其中，验证标准图像可以为用户的证件照片等可以用于身份验证的参考图像。此外，若比对结果表示拍摄设备和验证设备为不同设备，即输入到验证设备的人脸图像并非由该验证设备拍摄，则存在该人脸图像为网络盗取图像的风险，则可以不进行身份验证，或得到身份验证失败的验证结果，以提示验证设备的用户重新提交具有可信度的真实人脸图像，从而确保进行身份验证的人脸图像的真实性和可靠性，提高了身份验证的准确率，确保了身份验证的安全性。

[0062] 上述基于人工智能的身份验证方法中，对输入到验证设备的人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理得到的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识，在拍摄设备标识与基于验证设备所对应的第二模式噪声特征确定的验证设备标识的比对结果表示拍摄设备和验证设备为相同设备时，确定输入验证设备

的人脸图像是真实可靠的，并基于人脸图像进行身份验证。通过对输入到验证设备的人脸图像进行基于人工智能的设备溯源处理，根据基于模式噪声得到的人脸图像的拍摄设备所对应的拍摄设备标识与验证设备的验证设备标识进行特征比对，在确定人脸图像的拍摄设备为验证设备时，基于人脸图像进行身份验证，确保了输入到验证设备的人脸图像的真实性和可靠性，从而提高了基于人脸图像进行身份验证的准确率，确保了身份验证的安全性。

[0063] 在一个实施例中，拍摄设备标识基于从人脸图像提取的第一模式噪声特征得到，验证设备标识基于验证设备所对应的第二模式噪声特征得到；将拍摄设备标识和验证设备标识进行特征比对，获得比对结果，包括：确定第一模式噪声特征和第二模式噪声特征之间的相似度；根据相似度得到拍摄设备标识和验证设备标识的比对结果。

[0064] 其中，第一模式噪声特从输入到验证设备的人脸图像中提取得到，具体可以通过对人脸图像进行设备溯源处理提取得到，第一模式噪声特征反映了人脸图像的拍摄设备的模式噪声，将第一模式噪声特征可以作为拍摄设备的拍摄设备标识，以对各设备进行准确区分。同样的，第二模式噪声特征反映了验证设备的模式噪声。第二模式噪声特征可以通过对由验证设备拍摄的图像进行设备溯源处理提取得到。相似度表征了人脸图像的拍摄设备与验证设备之间的相似程度，相似度越高，则人脸图像的拍摄设备与验证设备越相似，人脸图像越可能是由验证设备拍摄的。

[0065] 具体地，拍摄设备标识可以包括从人脸图像提取的第一模式噪声特征，验证设备标识可以包括验证设备所对应的第二模式噪声特征。在比对拍摄设备标识和拍摄设备标识，验证设备确定第一模式噪声特征和第二模式噪声特征之间的相似度，具体可以为第一模式噪声特征和第二模式噪声特征间的余弦相似度，余弦相似度通过计算第一模式噪声特征和第二模式噪声特征的夹角余弦值来度量两者间的相似性。得到第一模式噪声特征和第二模式噪声特征之间的相似度后，验证设备基于该相似度得到拍摄设备标识和验证设备标识的比对结果。具体地，可以将相似度与预设的相似度阈值进行比较，在相似度超过相似度阈值时，认为第一模式噪声特征和第二模式噪声特征的相似度较高，则人脸图像的拍摄设备与验证设备为相同设备，否则人脸图像的拍摄设备与验证设备为不同设备。

[0066] 本实施例中，通过第一模式噪声特征和第二模式噪声特征之间的相似度来度量人脸图像的拍摄设备与验证设备之间的相似程度，从而得到拍摄设备标识与验证设备的比对结果，能够有效利用具有拍摄功能的设备固有的模式噪声特征，对人脸图像进行准确的设备溯源，从而对人脸图像的真实性和可靠性进行准确的判定，确保了身份验证的准确率。

[0067] 在一个实施例中，根据相似度得到拍摄设备标识和验证设备标识的比对结果，包括：当相似度大于相似度阈值时，得到表示拍摄设备和验证设备为相同设备的比对结果；当相似度小于或等于相似度阈值时，得到表示拍摄设备和验证设备为不同设备的比对结果。

[0068] 本实施例中，根据第一模式噪声特征和第二模式噪声特征之间的相似度与预设的相似度阈值的大小关系，确定表示拍摄设备和验证设备之间关系的比对结果。其中，相似度阈值可以根据实际需求进行灵活设置，如设置为80%。

[0069] 具体地，得到第一模式噪声特征和第二模式噪声特征之间的相似度后，验证设备获取预先设定的相似度阈值，比较相似度和相似度阈值，若相似度大于相似度阈值，则拍摄设备和验证设备的相似程度较高，可以认为人脸图像的拍摄设备与验证设备为相同设备，即输入到验证设备的人脸图像是由验证设备拍摄得到的，从而得到表示拍摄设备和验证设

备为相同设备的比对结果。另一方面，若相似度小于或等于相似度阈值，则表明拍摄设备和验证设备的相似程度较低，可以认为人脸图像的拍摄设备与验证设备为不同的设备，即输入到验证设备的人脸图像不是由验证设备拍摄得到的，而是其他设备拍摄的，则可能是从网络中非法盗取的人脸图像，则得到表示拍摄设备和验证设备为不同设备的比对结果。

[0070] 本实例中，通过第一模式噪声特征和第二模式噪声特征之间的相似度与预设的相似度阈值的大小关系确定比对结果，从而有效利用具有拍摄功能的设备固有的模式噪声特征，对人脸图像进行准确的设备溯源，从而对人脸图像的真实性和可靠性进行准确的判定，确保了身份验证的准确率。

[0071] 在一个实施例中，如图4所示，对人脸图像进行基于人工智能的设备溯源处理，基于所述设备溯源处理获得的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识，包括：

[0072] 步骤402，对人脸图像进行至少一次的卷积操作，获得人脸图像的图像卷积特征。

[0073] 其中，卷积操作可以通过卷积神经网络模型的卷积层实现，以对人脸图像进行特征提取，得到获得人脸图像的图像卷积特征。其中，卷积神经网络模型的卷积层由若干卷积单元组成，每个卷积单元的参数都是通过反向传播算法最佳化得到的，卷积运算的目的是提取输入的不同特征，第一层卷积层可能只能提取一些低级的特征如边缘、线条和角等层级，更多层的网路能从低级特征中迭代提取更复杂的特征。通过对人脸图像进行至少一次的卷积操作，可以从人脸图像提取得到与对应拍摄设备的模式噪声相关的图像卷积特征。

[0074] 具体地，验证设备或服务器对人脸图像进行设备溯源处理时，对人脸图像进行至少一次的卷积操作，得到图像卷积特征，图像卷积特征可以表征人脸图像的拍摄设备的模式噪声。

[0075] 步骤404，对图像卷积特征进行非线性映射，得到第一模式噪声特征。

[0076] 得到人脸图像的图像卷积特征后，验证设备或服务器对图像卷积特征进行非线性映射，具体可以先对图像卷积特征进行池化处理，再通过激励函数对池化的输出结果进行非线性映射，得到表征人脸图像的拍摄设备的模式噪声的第一模式噪声特征。

[0077] 步骤406，基于第一模式噪声特征，确定人脸图像的拍摄设备所对应的拍摄设备标识。

[0078] 得到第一模式噪声特征后，验证设备或服务器基于第一模式噪声特征确定人脸图像的拍摄设备所对应的拍摄设备标识。例如，验证设备或服务器可以直接将得到的第一模式噪声特征作为人脸图像的拍摄设备所对应的拍摄设备标识，也可以将第一模式噪声特征进行标签映射，如通过全连接层进行标签映射，将第一模式噪声特征映射到对应字符串，根据该字符串得到设备ID标签，并将得到的设备ID标签作为拍摄设备标识。

[0079] 本实施例中，依次通过至少一次的卷积操作对人脸图像进行特征提取，并对提取得到的图像卷积特征进行非线性映射，基于得到的第一模式噪声特征，确定人脸图像的拍摄设备所对应的拍摄设备标识，从而基于人工智能实现对人脸图像的设备溯源处理，能够有效提高设备溯源的准确度，从业确保了身份验证的准确率。

[0080] 在一个实施例中，基于第一模式噪声特征，确定人脸图像的拍摄设备所对应的拍摄设备标识，包括：将第一模式噪声特征按照设备标识格式映射为字符串，得到人脸图像的拍摄设备所对应的拍摄设备标识。

[0081] 本实施例中，将第一模式噪声特征映射为字符串，并根据得到的字符串获得人脸图像的拍摄设备所对应的拍摄设备标识。具体地，在得到人脸图像对应的第一模式噪声特征后，验证设备查询预设的设备标识格式，设备标识格式定义了将模式噪声特征映射为字符串的映射规则，根据设备标识格式可以将模式噪声特征映射为可读性更高的字符串，模式噪声特征对应于不同的字符串，从而可以将该字符串作为对应设备的标识。确定设备标识格式后，验证设备按照该设备标识格式将第一模式噪声特征映射为字符串，并根据该字符串得到人脸图像的拍摄设备所对应的拍摄设备标识，如直接将该字符串作为拍摄设备标识。

[0082] 进一步地，将拍摄设备标识和验证设备标识进行特征比对，获得比对结果，包括：对拍摄设备标识和验证设备标识进行字符比对，得到比对结果。

[0083] 在拍摄设备标识和验证设备标识包括按照设备标识格式映射处理得到的字符串，则将拍摄设备标识和验证设备标识进行特征比对时，验证设备可以对拍摄设备标识和验证设备标识进行字符比对，如可以将字符串中各字符进行一一比对，得到比对结果。具体地，若字符比对时各对应字符相同，则可以确定人脸图像的拍摄设备与验证设备为相同设备，否则人脸图像的拍摄设备与验证设备为不同设备。

[0084] 本实施例中，将模式噪声特征按照设备标识格式映射为字符串，可以提高拍摄设备标识和验证设备标识的可读性，同时通过对拍摄设备标识对应的字符串和验证设备标识对应的字符串进行字符对比，可以对拍摄设备标识和验证设备标识进行准确的比对，得到准确的比对结果，从而确保身份验证的准确率。

[0085] 在一个实施例中，设备溯源处理基于设备溯源网络模型实现，设备溯源网络模型通过模型训练步骤生成，模型训练步骤包括：获取携带设备标识标签的训练图像；通过待训练的设备溯源网络模型对训练图像进行至少一次的卷积操作，获得训练图像的训练卷积特征；通过设备溯源网络模型对训练卷积特征进行非线性映射，得到训练模式噪声特征；通过设备溯源网络模型根据训练模式噪声特征确定训练图像的拍摄设备所对应的预测设备标识；根据设备标识标签和预测设备标识调整设备溯源网络模型的参数后继续进行训练，直至训练结束得到训练完成的设备溯源网络模型。

[0086] 本实施例中，通过训练图像训练设备溯源网络模型，并通过训练完成的设备溯源网络模型实现对人脸图像的设备溯源处理，从而基于人工智能技术对人脸图像进行设备溯源，能够有效提高设备溯源处理的处理效率和准确率。

[0087] 具体地，设备溯源处理基于设备溯源网络模型实现，设备溯源网络模型可以为卷积神经网络(Convolutional Neural Network，CNN)、循环神经网络(Recurrent Neural Network，RNN)或深度神经网络(Deep neural network，DNN)等各种神经网络模型。

[0088] 进一步地，设备溯源网络模型通过模型训练步骤生成，在训练设备溯源网络模型时，训练设备端，如验证设备或服务器等获取携带设备标识标签的训练图像。设备标识标签记载了训练图像的拍摄设备的拍摄设备标识。训练设备端通过待训练的设备溯源网络模型对训练图像进行设备溯源处理，具体通过待训练的设备溯源网络模型对训练图像进行至少一次的卷积操作，获得训练图像的训练卷积特征；再通过设备溯源网络模型对训练卷积特征进行非线性映射，得到训练模式噪声特征，训练模式噪声特征反映了设备溯源网络模型对训练图像进行设备溯源处理而获得的训练图像拍摄设备的模式噪声。训练设备端通过设

备溯源网络模型根据训练模式噪声特征确定训练图像的拍摄设备所对应的预测设备标识，预测设备标识即为待训练的设备溯源网络模型对训练图像进行设备溯源处理的结果。训练设备端根据设备标识标签和预测设备标识调整设备溯源网络模型的参数后继续进行训练，如根据设备标识标签和预测设备标识之间的差异对设备溯源网络模型的参数进行调整，并进行重复训练，直至训练结束得到训练完成的设备溯源网络模型，如在设备标识标签和预测设备标识之间的差异维持不变或差异小于预设的差异阈值时结束训练，得到训练完成的设备溯源网络模型。

[0089] 在一个实施例中，根据设备标识标签和预测设备标识调整设备溯源网络模型的参数后继续进行训练，包括：获得设备标识标签和预测设备标识之间的距离损失；确定距离损失的梯度参数；根据梯度参数对设备溯源网络模型的参数进行调整，并通过参数调整后的设备溯源网络模型继续进行训练。

[0090] 本实施例中，在根据设备标识标签和预测设备标识之间的差异对设备溯源网络模型的参数进行调整时，可以根据设备标识标签和预测设备标识之间的距离损失确定梯度参数，并通过梯度参数对设备溯源网络模型的参数进行调整。其中，距离损失表征设备标识标签和预测设备标识之间的距离，距离损失越大，表明设备标识标签和预测设备标识相差越大，即设备溯源网络模型的效果越差。距离损失具体可以采用均方误差损失，即通过设备标识标签和预测设备标识之间的平方距离得到。梯度参数可以通过随机梯度下降算法确定，随机梯度下降算法是一种机器学习优化算法，用于训练过程中最小化训练代价函数，能够寻找机器学习模型的最优参数。

[0091] 具体地，在根据设备标识标签和预测设备标识调整设备溯源网络模型的参数后继续进行训练，训练设备端获得设备标识标签和预测设备标识之间的距离损失，如可以根据设备标识标签和预测设备标识之间的平方距离计算得到距离损失。训练设备端确定距离损失的梯度参数，如基于随机梯度下降算法计算得到距离损失的梯度参数，训练设备端根据梯度参数对设备溯源网络模型的参数进行调整，并通过参数调整后的设备溯源网络模型继续进行训练。

[0092] 在一个实施例中，获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识，包括：获取由验证设备拍摄得到的参考图像；对参考图像进行基于人工智能的设备溯源处理，基于设备溯源处理获得的第二模式噪声，确定验证设备所对应的验证设备标识。

[0093] 本实施例中，通过对由验证设备拍摄得到的图像进行基于人工智能的设备溯源处理，从而基于设备溯源处理得到的第二模式噪声确定验证设备所对应的验证设备标识。具体地，验证终端获取由自身拍摄得到的参考图像，如可以触发验证设备进行拍摄，得到参考图像，参考图像经过验证设备拍摄得到，从而可以对参考图像进行设备溯源处理，基于设备溯源处理得到的第二模式噪声，确定验证设备所对应的验证设备标识。进一步地，验证设备对获得的参考图像进行基于人工智能的设备溯源处理，设备溯源处理与对人脸图像的设备溯源处理相同，如通过预训练的设备溯源网络模型对参考图像进行基于人工智能的设备溯源处理，得到验证设备所对应的验证设备标识。验证设备标识可以用于区别各种验证设备。

[0094] 在具体实现时，如图5所示，在上传人脸图像后，可以进一步进入上传参考图像的界面，通过该界面可以触发验证设备进行拍照，并在预定的预览区域展示验证设备拍摄得到的参考图像，在触发提交后可以对参考图像进行基于人工智能的设备溯源处理，获得验

证设备所对应的验证设备标识。

[0095] 本实施例中，通过对由验证设备拍摄得到的图像进行基于人工智能的设备溯源处理，从而可以准确得到验证设备所对应的验证设备标识，以便根据验证设备标识与拍摄设备标识进行特征比对，判断输入到验证设备中的人脸图像的真实性和可靠性，从而确保了身份验证的准确率。

[0096] 在一个实施例中，基于人脸图像进行身份验证，包括：获取验证标准图像；将人脸图像与验证标准图像进行人脸比对，得到人脸比对结果；根据人脸比对结果得到人脸图像的身份验证结果。

[0097] 本实施例中，通过作为身份验证标准图像的验证标准图像与人脸图像进行人脸比对，并根据人脸比对结果得到身份验证结果。具体地，验证设备获取验证标准图像，验证标准图像为身份验证的标准图像，如可以为用户的证件照片。验证标准图像可以通过验证设备输入，也可以从服务器中获取得到。验证设备将人脸图像与获得的验证标准图像进行人脸比对，如基于计算机视觉对人脸图像中的人脸与验证标准图像中的人脸进行比较，得到人脸比对结果。验证终端根据人脸比对结果得到人脸图像的身份验证结果。如人脸比对结果表明人脸图像与验证标准图像包含同一用户的人脸，则身份验证结果可以为验证通过；否则，身份验证结果可以为验证不通过。

[0098] 本实施例中，在确定人脸图像为验证设备拍摄得到的，而不是从网络非法盗取的图像后，基于人脸图像与验证标准图像进行人脸比对，从而实现身份验证，可以有效避免利用非法盗取的人脸图像进行身份验证的风险，确保了身份验证的准确率。

[0099] 在一个实施例中，基于人工智能的身份验证方法还包括：当比对结果表示拍摄设备和验证设备为不同设备时，指示验证设备展示验证失败提示消息，并指示验证设备展示描述人脸图像为非法图像的提示信息。

[0100] 本实施例中，若拍摄设备标识和验证设备标识的比对结果表明人脸图像的拍摄设备与验证设备不同，即输入到验证设备的人脸图像确不是验证设备拍摄获得的，而可能是通过网络非法盗取的图像时，则可以通过验证设备展示验证失败提示消息，并展示人脸图像为非法图像的提示信息。

[0101] 具体地，验证设备将拍摄设备标识与验证设备标识进行特征比对，得到比对结果后，若比对结果表示拍摄设备和验证设备为不同设备，即输入到验证设备的人脸图像不是由验证设备拍摄的，其真实性和可靠性有限，则验证设备展示验证失败提示消息，并展示描述人脸图像为非法图像的提示信息，以提示用户重新进行人脸图像上传。在具体应用中，如图6所示，可以在身份验证的验证结果界面展示验证失败提示消息和验证失败提示消息，以提示用户重新上传真实可靠的人脸图像进行身份验证。

[0102] 本实施例中，在确定人脸图像的拍摄设备和验证设备为不同设备，通过展示验证失败提示消息和验证失败提示消息，以提示用户重新上传真实可靠的人脸图像进行身份验证，可以确保身份验证的准确率。

[0103] 在一个实施例中，如图7所示，提供了一种基于人工智能的身份验证方法，包括以下步骤：

[0104] 步骤702，获取输入到验证设备的待验证的人脸图像。

[0105] 验证设备为用户发起进行身份验证的终端设备，人脸图像输入到验证设备中，人

脸图像包含用户人脸部位，通过对人脸图像中的人脸部位进行识别，可以对人脸图像进行身份验证。人脸图像输入到验证设备进行身份验证，若人脸图像为非法盗取的图片，会影响身份验证的准确率，导致身份验证的安全性存在隐患。

[0106] 步骤704，对人脸图像进行至少一次的卷积操作，获得人脸图像的图像卷积特征。

[0107] 卷积操作通过卷积神经网络模型的卷积层实现，以对人脸图像进行特征提取，得到可以表征人脸图像对应拍摄设备模式噪声的图像卷积特征。

[0108] 步骤706，对图像卷积特征进行非线性映射，得到第一模式噪声特征。

[0109] 对获得的图像卷积特征进行非线性映射，具体可以先对图像卷积特征进行池化处理，再通过激励函数对池化的输出结果进行非线性映射，得到表征人脸图像的拍摄设备的模式噪声的第一模式噪声特征。

[0110] 步骤708，基于第一模式噪声特征，确定人脸图像的拍摄设备所对应的拍摄设备标识。

[0111] 具体地，可以直接将得到的第一模式噪声特征作为人脸图像的拍摄设备所对应的拍摄设备标识，也可以将第一模式噪声特征进行标签映射，如通过全连接层进行标签映射，将第一模式噪声特征映射到对应字符串，根据该字符串得到设备ID标签，并将得到的设备ID标签作为拍摄设备标识。

[0112] 步骤710，获取由验证设备拍摄得到的参考图像。

[0113] 参考图像经过验证设备拍摄得到，从而可以对参考图像进行设备溯源处理，得到验证设备所对应的验证设备标识。参考图像可以为验证设备出厂时预存的参考图像，如可以为验证设备在出厂时，于安全存储中预先存储的仅可读不可更改的由该验证设备拍摄获得的参考图像，从而可以从验证设备的安全存储中获取该参考图像，并确保了该参考图像为验证设备拍摄获得。此外，参考图像也可以为与人脸图像对应拍摄的无人脸的背景图像。进一步地，参考图像也可以为官方认证的由验证设备拍摄得到的图像，如可以由官方工作人员对参考图像进行认证，从而确保参考图像由验证设备拍摄得到。

[0114] 步骤712，对参考图像进行基于人工智能的设备溯源处理，获得验证设备所对应的验证设备标识；验证设备标识基于验证设备所对应的第二模式噪声特征得到。

[0115] 具体可以通过预训练的设备溯源网络模型对参考图像进行基于人工智能的设备溯源处理，得到验证设备所对应的验证设备标识，验证设备标识用于区别各种验证设备。

[0116] 步骤714，确定第一模式噪声特征和第二模式噪声特征之间的相似度。

[0117] 相似度表征了人脸图像的拍摄设备与验证设备之间的相似程度，相似度越高，则人脸图像的拍摄设备与验证设备越相似，人脸图像越可能是由验证设备拍摄的。具体可以确定第一模式噪声特征和第二模式噪声特征间的余弦相似度，余弦相似度通过计算第一模式噪声特征和第二模式噪声特征的夹角余弦值来度量两者间的相似性。

[0118] 步骤716，根据相似度得到拍摄设备标识和验证设备标识的比对结果。

[0119] 基于第一模式噪声特征和第二模式噪声特征之间的相似度得到拍摄设备标识和验证设备标识的比对结果。具体地，将相似度与预设的相似度阈值进行比较，在相似度超过相似度阈值时，认为第一模式噪声特征和第二模式噪声特征的相似度较高，则人脸图像的拍摄设备与验证设备为相同设备，否则人脸图像的拍摄设备与验证设备为不同设备。

[0120] 步骤718，当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行

身份验证。

[0121] 具体地，验证设备获取验证标准图像，验证标准图像为身份验证的标准图像，如可以为用户的证件照片。验证标准图像可以通过验证设备输入，也可以从服务器中获取得到。验证设备将人脸图像与获得的验证标准图像进行人脸比对，如基于计算机视觉对人脸图像中的人脸与验证标准图像中的人脸进行比较，得到人脸比对结果。验证终端根据人脸比对结果得到人脸图像的身份验证结果。如人脸比对结果表明人脸图像与验证标准图像包含同一用户的人脸，则身份验证结果可以为验证通过；否则，身份验证结果可以为验证不通过。

[0122] 本实施例中，对输入到验证设备的待验证的人脸图像进行至少一次的卷积操作，对得到的图像卷积特征进行非线性映射，得到第一模式噪声特征，并基于第一模式噪声特征确定人脸图像的拍摄设备所对应的拍摄设备标识。另一方面，获取由验证设备拍摄得到的参考图像，对参考图像基于人工智能的设备溯源处理，得到基于验证设备所对应的第二模式噪声特征生成的验证设备标识。计算第一模式噪声特征和第二模式噪声特征之间的相似度，根据该相似度判定拍摄设备与验证设备的关系，得到比对结果，若比对结果表示拍摄设备和验证设备为相同设备时，表明输入到验证设备的人脸图像由验证设备拍摄得到，人脸图像为真实可信的，则基于人脸图像进行身份验证。通过对输入到验证设备的人脸图像进行基于人工智能的设备溯源处理，根据得到的人脸图像的拍摄设备所对应的拍摄设备标识与验证设备的验证设备标识进行特征比对，在确定人脸图像的拍摄设备为验证设备时，基于人脸图像进行身份验证，确保了输入到验证设备的人脸图像的真实性和可靠性，从而提高了基于人脸图像进行身份验证的准确率，确保了身份验证的安全性。

[0123] 本申请还提供一种应用场景，该应用场景应用上述的基于人工智能的身份验证方法。具体地，该基于人工智能的身份验证方法在该应用场景的应用如下：

[0124] 在验证设备基于人脸图像进行身份验证时，获取输入到验证设备的人脸图像，人脸图像可能是验证设备拍摄，或由其他各种拍摄设备拍摄得到的电子图片，对人脸图像进行缩放处理，将人脸图像缩放到224*224像素，将缩放后的人脸图像输入到预训练的CNN网络，以通过预训练的CNN网络来提取人脸图像的拍摄设备的传感器的模式噪声特征，得到图片拍摄设备ID，并通过该图片拍摄设备ID判断人脸图像是否由验证设备拍摄得到。一般地，不同拍摄设备的图像获取传感器在制造过程中会产生传感器模式噪声，不同设备的传感器模式噪声不同，表现在图片上，就是不同设备拍摄的图片在像素上存在差异。根据这种差异，可以根据图片来区分不同的设备，从而获取设备ID，从而实现对图像的拍摄设备ID溯源。

[0125] 其中，在训练CNN网络时，如图8所示，包括：

[0126] 步骤802，获取训练图像，训练图像携带设备ID。

[0127] 训练图像为由各种拍摄设备拍摄的电子图片，设备ID为各训练图像对应的真实拍摄设备的标识。

[0128] 步骤804，对训练图像进行预处理。

[0129] 具体将训练图像统一缩放到224*224像素。

[0130] 步骤806，CNN网络进行特征提取。

[0131] 通过CNN网络的卷积层对缩放后的训练图像进行特征提取，CNN网络为从原始数据提取其特征表示的多层前馈人工神经网络，CNN网络可以通过滑动卷积提取图片对应的特

征。

[0132] 步骤808,对提取的CNN特征进行映射处理。

[0133] 对于步骤806提取得到的特征进行最大池化,并通过激励函数RELU进行映射处理,以增强特征的表示能力。

[0134] 步骤810,获得模式噪声特征。

[0135] 根据步骤808中映射处理结果得到训练图像对应的模式噪声特征。在具体实现时,步骤806和步骤808可重复叠加进行多次,以提取训练图像中更深层次的特征。

[0136] 步骤812,通过全连接层进行标签映射,获得预测设备ID。

[0137] CNN是一个多层神经网络,经过多层的特征提取-特征处理操作,将得到一个1*256维的设备噪声模式特征,该特征经过一个全连接层,预测输入图片的设备ID,即输出标签。全连接层的结构图如图9所示,其中,输入256个节点表示256维噪声模式特征,输出n个节点表示有n个设备ID,可以取输出节点中值最大的节点作为当前输入图片对应的设备ID。

[0138] 步骤814,根据设备ID和预测设备ID计算标签损失。

[0139] 比较设备ID和预测设备ID的距离,该距离越大,损失越大,表明预测设备ID与真实设备ID差异越大。如可以采用均方误差损失,均方误差是反映估计量和被估计量之间差异程度的一种度量,具体可以计算设备ID和预测设备ID的平方距离得到标签损失。

[0140] 步骤816,计算损失的梯度。

[0141] 基于设备ID和预测设备ID确定标签损失的梯度。具体地,可以采用梯度下降计算标签损失的梯度,梯度下降在机器学习中应用十分的广泛,不论是在线性回归还是Logistic回归中,它的主要目的是通过迭代找到目标函数的最小值,或者收敛到最小值。进一步地,确定获得的标签损失的梯度,按照梯度相反的方向,确定局部最小值,按照预定的步长进行梯度下降的迭代计算,得到标签损失的最小值。

[0142] 步骤818,根据梯度更新CNN参数并继续进行训练,直至训练结束。

[0143] 按照标签损失的梯度更新CNN参数并继续进行训练,直至训练结束,如设备ID和预测设备ID的损失一致或者距离不变,即得到训练完成的CNN,该CNN网络可以对输入的图片进行设备溯源处理,得到输入的图片的拍摄设备的拍摄设备标识。

[0144] 另一方面,获取人脸验证设备ID。人脸验证设备ID的获取处理与图片拍摄设备ID的获取原理相同,不同之处在于由验证设备拍摄一张无人脸的背景图片,然后将拍摄的背景图输入CNN中进行设备溯源处理,获取当前执行人脸验证设备的模式噪声特征,并根据该模式噪声特征确定人脸验证设备ID。

[0145] 得到图片拍摄设备ID和人脸验证设备ID后,对图片拍摄设备ID和人脸验证设备ID进行比较,如可以计算在设备溯源处理中获取的256维模式噪声特征的余弦相似度,如果相似度大于一定阈值,则认为两个ID代表同一台设备,则可以基于人脸图像进行身份验证处理;如果相似度小于一定阈值,则认为两个ID代表不同设备,表明当前用于人脸验证的图片不是当前执行人脸验证设备所拍摄,为盗用图片,从而可以输出验证失败的身份验证结果。通过CNN网络对人脸图像进行设备溯源处理,判断该人脸图像是否由验证设备拍摄,可以确保人脸图像的真实性和可靠性,从而提高身份验证的准确率。

[0146] 应该理解的是,虽然图2、4、7-8的流程图中的各个步骤按照箭头的指示依次显示,但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明,这些

步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，图2、4、7-8中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

[0147] 在一个实施例中，如图10所示，提供了一种基于人工智能的身份验证装置1000，该装置可以采用软件模块或硬件模块，或者是二者的结合成为计算机设备的一部分，该装置具体包括：人脸图像获取模块1002、设备溯源处理模块1004、验证设备标识获取模块1006、标识比对模块1008和身份验证处理模块1010，其中：

[0148] 人脸图像获取模块1002，用于获取输入到验证设备的待验证的人脸图像；

[0149] 设备溯源处理模块1004，用于对人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理获得的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识；

[0150] 验证设备标识获取模块1006，用于获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识；

[0151] 标识比对模块1008，用于将拍摄设备标识和验证设备标识进行特征比对，获得比对结果；

[0152] 身份验证处理模块1010，用于当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证。

[0153] 在一个实施例中，标识比对模块1008包括相似度确定模块和比对结果获得模块；其中：相似度确定模块，用于确定第一模式噪声特征和第二模式噪声特征之间的相似度；比对结果获得模块，用于根据相似度得到拍摄设备标识和验证设备标识的比对结果。

[0154] 在一个实施例中，比对结果获得模块包括第一比对结果模块和第二比对结果模块；其中：第一比对结果模块，用于当相似度大于相似度阈值时，得到表示拍摄设备和验证设备为相同设备的比对结果；第二比对结果模块，用于当相似度小于或等于相似度阈值时，得到表示拍摄设备和验证设备为不同设备的比对结果。

[0155] 在一个实施例中，设备溯源处理模块1004包括卷积特征提取模块、噪声特征获得模块和拍摄设备标识确定模块；其中：卷积特征提取模块，用于对人脸图像进行至少一次的卷积操作，获得人脸图像的第一图像卷积特征；噪声特征获得模块，用于对第一图像卷积特征进行非线性映射，得到第一模式噪声特征；拍摄设备标识确定模块，用于基于第一模式噪声特征，确定人脸图像的拍摄设备所对应的拍摄设备标识。

[0156] 在一个实施例中，拍摄设备标识确定模块包括字符串映射模块，用于将第一模式噪声特征按照设备标识格式映射为字符串，得到人脸图像的拍摄设备所对应的拍摄设备标识；标识比对模块1008还用于对拍摄设备标识和验证设备标识进行字符比对，得到比对结果。

[0157] 在一个实施例中，设备溯源处理基于设备溯源网络模型实现，设备溯源网络模型通过模型训练装置生成，模型训练装置包括训练图像获取模块、卷积训练处理模块、映射训练处理模块、设备标识预测模块和参数更新模块；其中：训练图像获取模块，用于获取携带设备标识标签的训练图像；卷积训练处理模块，用于通过待训练的设备溯源网络模型对训练图像进行至少一次的卷积操作，获得训练图像的训练卷积特征；映射训练处理模块，用于

通过设备溯源网络模型对训练卷积特征进行非线性映射，得到训练模式噪声特征；设备标识预测模块，用于通过设备溯源网络模型根据训练模式噪声特征确定训练图像的拍摄设备所对应的预测设备标识；参数更新模块，用于根据设备标识标签和预测设备标识调整设备溯源网络模型的参数后继续进行训练，直至训练结束得到训练完成的设备溯源网络模型。

[0158] 在一个实施例中，参数更新模块包括损失确定模块、梯度确定模块和参数调整模块；其中：损失确定模块，用于获得设备标识标签和预测设备标识之间的距离损失；梯度确定模块，用于确定距离损失的梯度参数；参数调整模块，用于根据梯度参数对设备溯源网络模型的参数进行调整，并通过参数调整后的设备溯源网络模型继续进行训练。

[0159] 在一个实施例中，验证设备标识获取模块1006包括参考图像获取模块和验证设备溯源模块；其中：参考图像获取模块，用于获取由验证设备拍摄得到的参考图像；验证设备溯源模块，用于对参考图像进行基于人工智能的设备溯源处理，基于所述设备溯源处理获得的第二模式噪声，确定验证设备所对应的验证设备标识。

[0160] 在一个实施例中，身份验证处理模块1010包括标准图像获取模块、人脸比对模块和验证结果获得模块；其中：标准图像获取模块，用于获取验证标准图像；人脸比对模块，用于将人脸图像与验证标准图像进行人脸比对，得到人脸比对结果；验证结果获得模块，用于根据人脸比对结果得到人脸图像的身份验证结果。

[0161] 在一个实施例中，还包括验证结果展示模块，用于当比对结果表示拍摄设备和验证设备为不同设备时，指示验证设备展示验证失败提示消息，并指示验证设备展示描述人脸图像为非法图像的提示信息。

[0162] 关于基于人工智能的身份验证装置的具体限定可以参见上文中对于基于人工智能的身份验证方法的限定，在此不再赘述。上述基于人工智能的身份验证装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0163] 在一个实施例中，提供了一种计算机设备，该计算机设备可以是终端，其内部结构图可以如图11所示。该计算机设备包括通过系统总线连接的处理器、存储器、通信接口、显示屏和输入装置。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机程序。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的通信接口用于与外部的终端进行有线或无线方式的通信，无线方式可通过WIFI、运营商网络、NFC(近场通信)或其他技术实现。该计算机程序被处理器执行时以实现一种基于人工智能的身份验证方法。该计算机设备的显示屏可以是液晶显示屏或者电子墨水显示屏，该计算机设备的输入装置可以是显示屏上覆盖的触摸层，也可以是计算机设备外壳上设置的按键、轨迹球或触控板，还可以是外接的键盘、触控板或鼠标等。

[0164] 本领域技术人员可以理解，图11中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

[0165] 在一个实施例中，还提供了一种计算机设备，包括存储器和处理器，存储器中存储有计算机程序，该处理器执行计算机程序时实现上述各方法实施例中的步骤。

[0166] 在一个实施例中，提供了一种计算机可读存储介质，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各方法实施例中的步骤。

[0167] 在一个实施例中，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各方法实施例中的步骤。

[0168] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器(Read-Only Memory，ROM)、磁带、软盘、闪存或光存储器等。易失性存储器可包括随机存取存储器(Random Access Memory，RAM)或外部高速缓冲存储器。作为说明而非局限，RAM可以是多种形式，比如静态随机存取存储器(Static Random Access Memory，SRAM)或动态随机存取存储器(Dynamic Random Access Memory，DRAM)等。

[0169] 以上实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0170] 以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

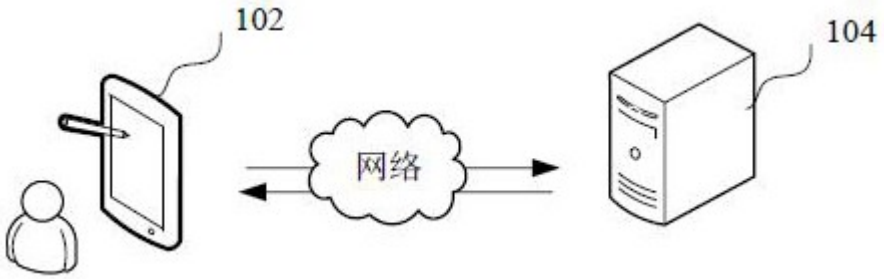

102
104
网络

图1

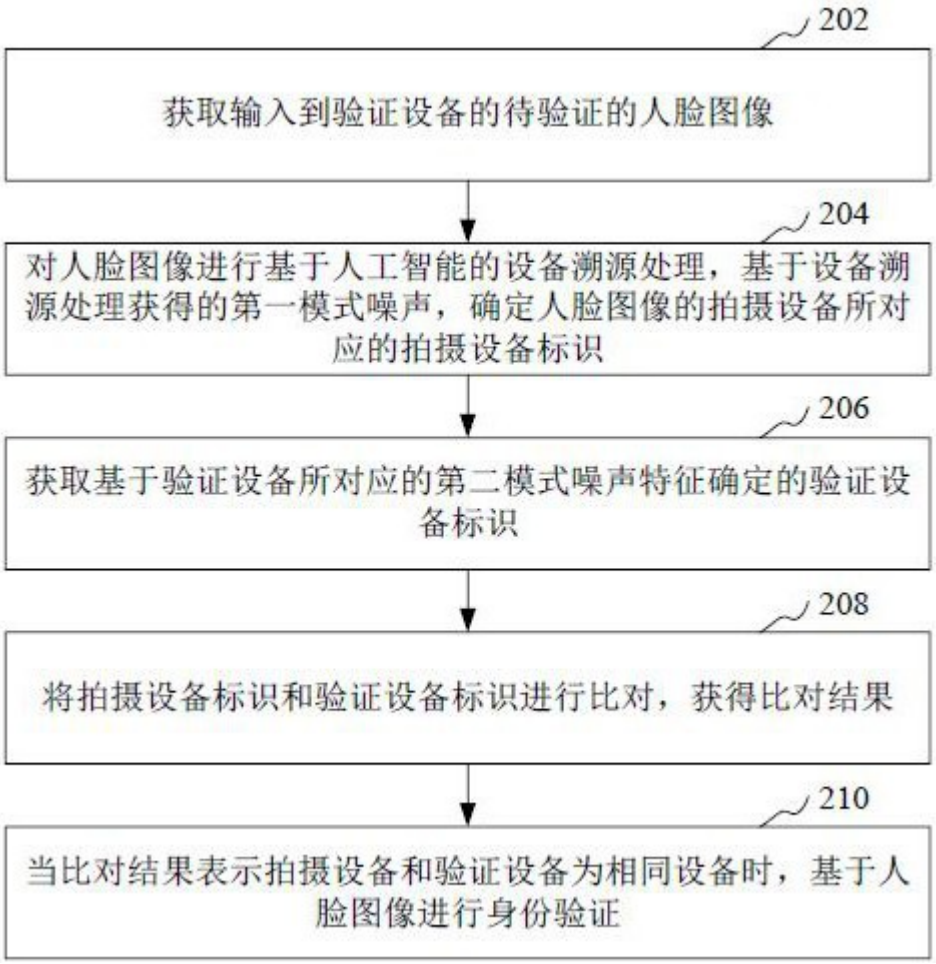

202
获取输入到验证设备的待验证的人脸图像
204
对人脸图像进行基于人工智能的设备溯源处理，基于设备溯源处理获得的第一模式噪声，确定人脸图像的拍摄设备所对应的拍摄设备标识
206
获取基于验证设备所对应的第二模式噪声特征确定的验证设备标识
208
将拍摄设备标识和验证设备标识进行比对，获得比对结果
210
当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证

图2


返回
人脸图像上传
人脸图像预览
上传人脸图像
立即拍照
提交

图3

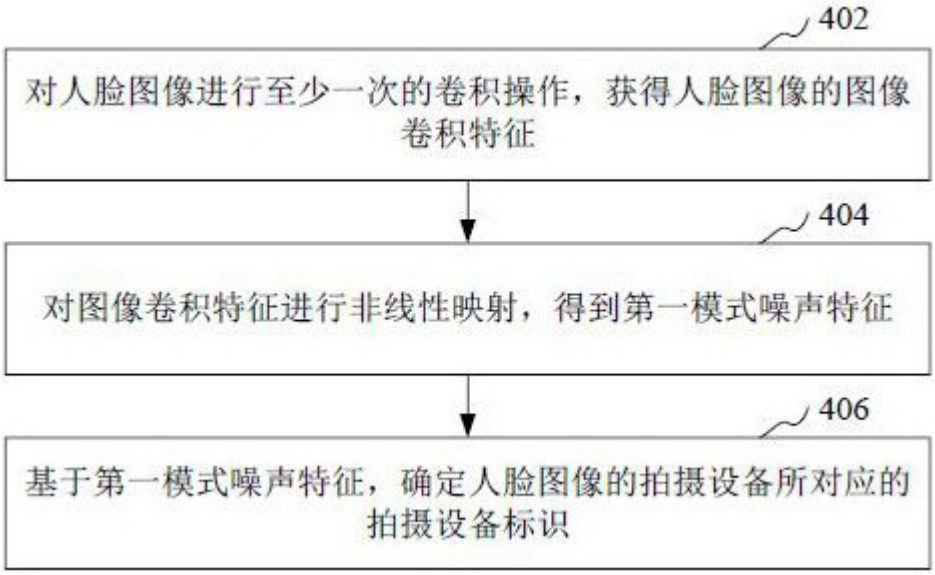

402
对人脸图像进行至少一次的卷积操作，获得人脸图像的图像卷积特征
404
对图像卷积特征进行非线性映射，得到第一模式噪声特征
406
基于第一模式噪声特征，确定人脸图像的拍摄设备所对应的拍摄设备标识

图4

图5

图6

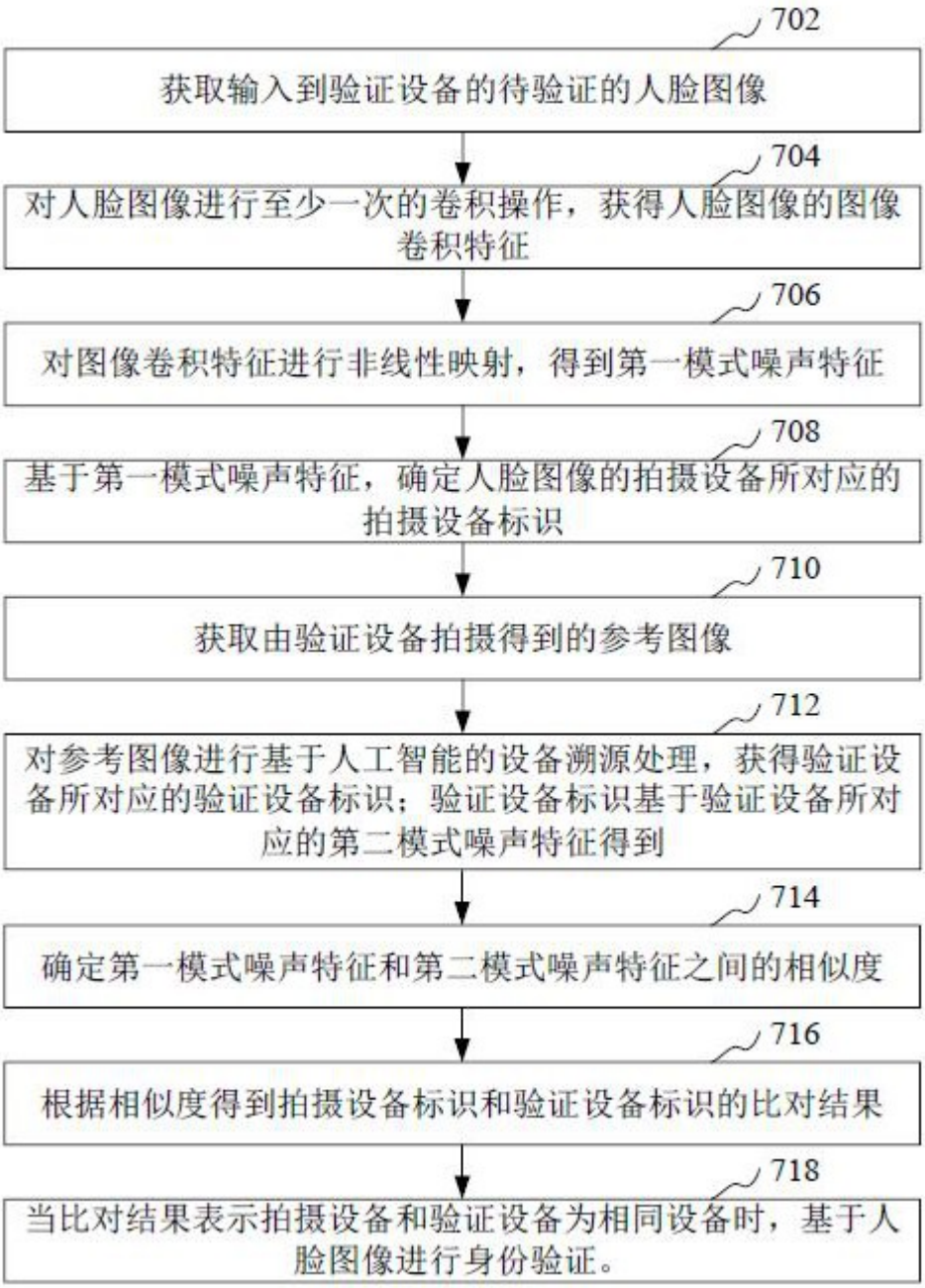

702
获取输入到验证设备的待验证的人脸图像
704
对人脸图像进行至少一次的卷积操作，获得人脸图像的图像卷积特征
706
对图像卷积特征进行非线性映射，得到第一模式噪声特征
708
基于第一模式噪声特征，确定人脸图像的拍摄设备所对应的拍摄设备标识
710
获取由验证设备拍摄得到的参考图像
712
对参考图像进行基于人工智能的设备溯源处理，获得验证设备所对应的验证设备标识；验证设备标识基于验证设备所对应的第二模式噪声特征得到
714
确定第一模式噪声特征和第二模式噪声特征之间的相似度
716
根据相似度得到拍摄设备标识和验证设备标识的比对结果
718
当比对结果表示拍摄设备和验证设备为相同设备时，基于人脸图像进行身份验证。

图7


802
获取训练图像，训练图像携带设备ID
804
对训练图像进行预处理
806
CNN网络进行特征提取
808
对提取的CNN特征进行映射处理
810
获得模式噪声特征
812
通过全连接层进行标签映射，获得预测设备ID
814
根据设备ID和预测设备ID计算标签损失
816
计算损失的梯度
818
根据梯度更新CNN参数并继续进行训练，直至训练结束

图8

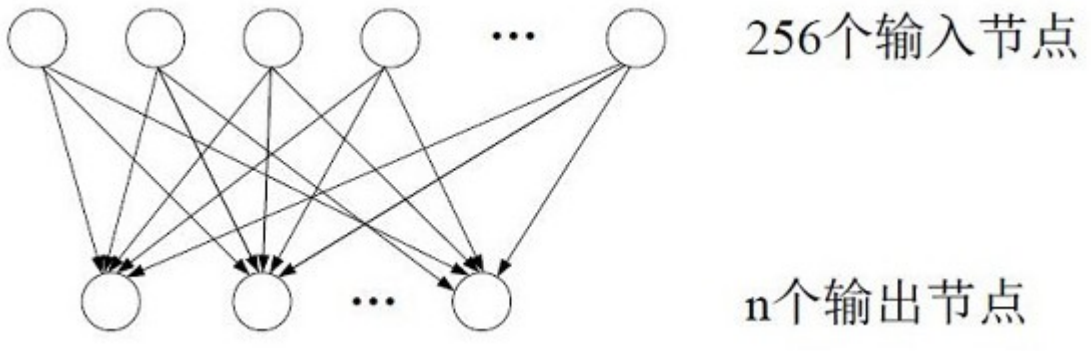

256个输入节点
n个输出节点

图9

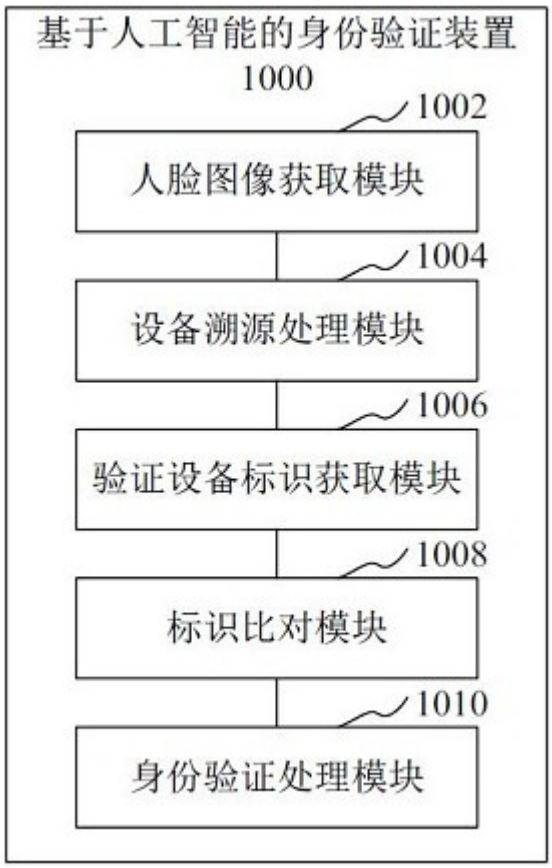

基于人工智能的身份验证装置
1000
1002
人脸图像获取模块
1004
设备溯源处理模块
1006
验证设备标识获取模块
1008
标识比对模块
1010
身份验证处理模块

图10

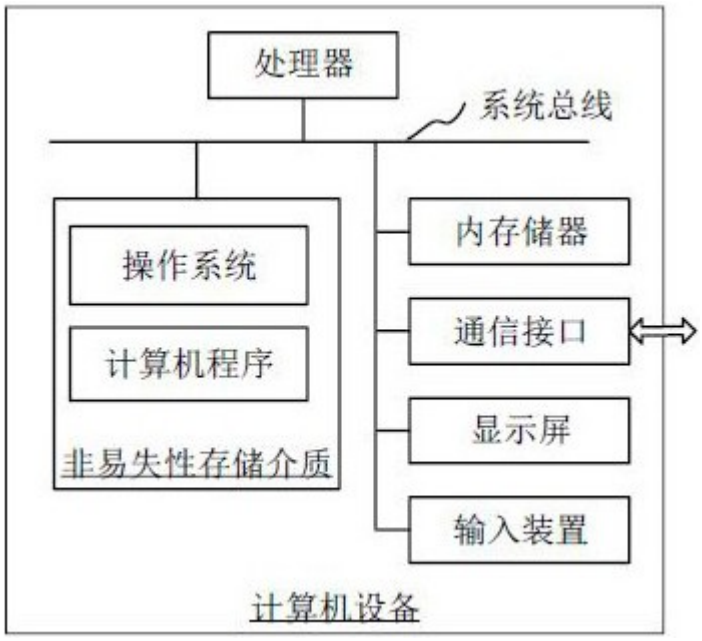


图11