



(12) 发明专利申请

(10) 申请公布号 CN 114612989 A

(43) 申请公布日 2022. 06. 10

(21) 申请号 202210269733.X

G06N 3/08 (2006.01)

(22) 申请日 2022.03.18

(71) 申请人 北京明略昭辉科技有限公司

地址 100000 北京市海淀区北三环西路25号27号楼二层2020室

(72) 发明人 刘星 赵晨旭 唐大闰

(74) 专利代理机构 北京康盛知识产权代理有限公司 11331

专利代理师 高会会

(51) Int. Cl.

G06V 40/16 (2022.01)

G06V 10/764 (2022.01)

G06V 10/82 (2022.01)

G06K 9/62 (2022.01)

G06N 3/04 (2006.01)

权利要求书2页 说明书9页 附图6页

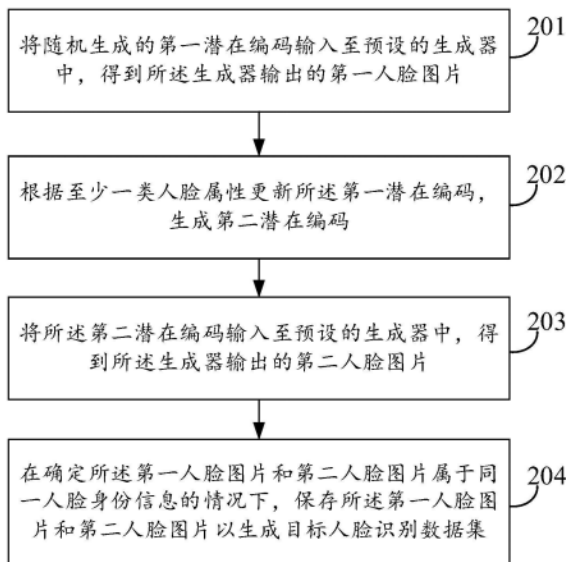
(54) 发明名称

人脸识别数据集的生成方法及装置、电子设备及存储介质

(57) 摘要

本申请涉及人脸识别技术领域,公开一种人脸识别数据集的生成方法,包括:将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片;根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码;将所述第二潜在编码输入至预设的生成器中,得到所述生成器输出的第二人脸图片;在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。该方法既节省了人力成本,又解决了人脸图像质量较差、单个人脸图片数目较少、数据集中存在重复到的人脸身份信息等各种问题。本申请还公开一种人脸识别数据集的生成装置、电子设备及存储介质。

CN 114612989 A



1. 一种人脸识别数据集的生成方法,其特征在于,包括:

将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片;

根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码;

将所述第二潜在编码输入至预设的生成器中,得到所述生成器输出的第二人脸图片;

在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

2. 根据权利要求1所述的生成方法,其特征在于,所述根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码,包括:

根据所述至少一类人脸属性中的任一人脸属性,确定修改第一潜在编码的扰动方向和扰动程度;

根据所述扰动方向和扰动程度对所述第一潜在编码进行变换,生成第二潜在编码。

3. 根据权利要求1或2所述的生成方法,其特征在于,在将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片之前,还包括:

从开源人脸识别数据集中获取多张真实的人脸图片;

根据所述多张真实的人脸图片,训练一个生成对抗网络并保留所述生成对抗网络中的生成器;

以残差网络模型为主干,训练得到一个人脸识别模型。

4. 根据权利要求3所述的生成方法,其特征在于,所述在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集,包括:

将所述第一人脸图片输入至所述人脸识别模型中,得到所述第一人脸图片对应的第一特征表达;

将所述第二人脸图片输入至所述人脸识别模型中,得到所述第二人脸图片对应的第二特征表达;

计算所述第一特征表达和第二特征表达之间的余弦相似度;

在所述余弦相似度小于相似度阈值的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

5. 一种人脸识别数据集的生成装置,其特征在于,包括:

第一图片生成模块,被配置为将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片;

扰动添加模块,被配置为根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码;

第二图片生成模块,被配置为将所述第二潜在编码输入至预设的生成器中,得到所述生成器输出的第二人脸图片;

数据集生成模块,被配置为在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

6. 根据权利要求5所述的生成装置,其特征在于,所述扰动添加模块,具体被配置为:

根据所述至少一类人脸属性中的任一人脸属性,确定修改第一潜在编码的扰动方向和

扰动程度；

根据所述扰动方向和扰动程度对所述第一潜在编码进行变换，生成第二潜在编码。

7. 根据权利要求5或6所述的生成装置，其特征在于，所述装置还包括预训练模块，所述预训练模块被配置为：

从开源人脸识别数据集中获取多张真实的人脸图片；

根据所述多张真实的人脸图片，训练一个生成对抗网络并保留所述生成对抗网络中的生成器；

以残差网络模型为主干，训练得到一个人脸识别模型。

8. 根据权利要求7所述的生成装置，其特征在于，所述数据集生成模块，被配置为：

将所述第一人脸图片输入至所述人脸识别模型中，得到所述第一人脸图片对应的第一特征表达；

将所述第二人脸图片输入至所述人脸识别模型中，得到所述第二人脸图片对应的第二特征表达；

计算所述第一特征表达和第二特征表达之间的余弦相似度；

在所述余弦相似度小于相似度阈值的情况下，保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

9. 一种电子设备，其特征在于，包括存储器和处理器，其中：

所述存储器，用于保存计算机程序；

所述处理器，用于执行所述计算机程序，以实现如权利要求1至4任一项所述的人脸识别数据集的生成方法。

10. 一种存储介质，存储有程序指令，其特征在于，所述程序指令在运行时，执行如权利要求1至4任一项所述的人脸识别数据集的生成方法。

人脸识别数据集的生成方法及装置、电子设备及存储介质

技术领域

[0001] 本申请涉及人脸识别技术领域，例如涉及一种人脸识别数据集的生成方法及装置、电子设备及存储介质。

背景技术

[0002] 目前，人脸识别系统已经应用在人们生活中点的诸多领域，例如电子识别解锁、门禁打卡和金融支付等。训练一个人脸识别模型通常需要收集大量的人脸身份信息，每个人脸身份信息需要包含同一个人的多张不同的人脸图片。同理可知，人脸识别模型的准确率非常依赖训练时用到的人脸识别数据集。通常而言，人脸识别数据集中的人脸身份信息的数目越多，每个人脸身份信息包含的人脸图片越多，那么这个人脸识别数据集就能更好地代表真实情况下的人脸特征分布。因此，如何有效地扩充人脸识别数据集的大小，对于人脸识别模型的准确率至关重要。

[0003] 在实现本申请的过程中，发现相关技术中至少存在如下问题：

[0004] 现有的人脸识别数据集，例如Glint360K和WebFace260M，通常是人工采集或者从互联网抓取得到，这种方式采集数据需要非常大的人力成本，且采集到的数据中会存在人脸图像质量较差、单个人脸图片数目较少、数据集中存在重复到的人脸身份信息等各种问题。

发明内容

[0005] 为了对披露的实施例的一些方面有基本的理解，下面给出了简单的概括。所述概括不是泛泛评述，也不是要确定关键/重要组成元素或描绘这些实施例的保护范围，而是作为后面的详细说序言。

[0006] 本申请提供了一种人脸识别数据集的生成方法及装置、电子设备及存储介质，以减少采集数据的成本并提高人脸识别数据集中的人脸图像质量。

[0007] 在一些实施例中，所述人脸识别数据集的生成方法，包括：

[0008] 将随机生成的第一潜在编码输入至预设的生成器中，得到所述生成器输出的第一人脸图片；

[0009] 根据至少一类人脸属性更新所述第一潜在编码，生成第二潜在编码；

[0010] 将所述第二潜在编码输入至预设的生成器中，得到所述生成器输出的第二人脸图片；

[0011] 在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下，保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

[0012] 可选地，所述根据至少一类人脸属性更新所述第一潜在编码，生成第二潜在编码，包括：

[0013] 根据所述至少一类人脸属性中的任一人脸属性，确定修改第一潜在编码的扰动方向和扰动程度；

- [0014] 根据所述扰动方向和扰动程度对所述第一潜在编码进行变换,生成第二潜在编码。
- [0015] 可选地,在将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片之前,还包括:
- [0016] 从开源人脸识别数据集中获取多张真实的人脸图片;
- [0017] 根据所述多张真实的人脸图片,训练一个生成对抗网络并保留所述生成对抗网络中的生成器;
- [0018] 以残差网络模型为主干,训练得到一个人脸识别模型。
- [0019] 可选地,所述在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集,包括:
- [0020] 将所述第一人脸图片输入至所述人脸识别模型中,得到所述第一人脸图片对应的第一特征表达;
- [0021] 将所述第二人脸图片输入至所述人脸识别模型中,得到所述第二人脸图片对应的第二特征表达;
- [0022] 计算所述第一特征表达和第二特征表达之间的余弦相似度;
- [0023] 在所述余弦相似度小于相似度阈值的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。
- [0024] 在一些实施例中,所述人脸识别数据集的生成装置,包括:
- [0025] 第一图片生成模块,被配置为将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片;
- [0026] 扰动添加模块,被配置为根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码;
- [0027] 第二图片生成模块,被配置为将所述第二潜在编码输入至预设的生成器中,得到所述生成器输出的第二人脸图片;
- [0028] 数据集生成模块,被配置为在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。
- [0029] 可选地,所述扰动添加模块,具体被配置为:
- [0030] 根据所述至少一类人脸属性中的任一人脸属性,确定修改第一潜在编码的扰动方向和扰动程度;
- [0031] 根据所述扰动方向和扰动程度对所述第一潜在编码进行变换,生成第二潜在编码。
- [0032] 可选地,所述装置还包括预训练模块,所述预训练模块被配置为:
- [0033] 从开源人脸识别数据集中获取多张真实的人脸图片;
- [0034] 根据所述多张真实的人脸图片,训练一个生成对抗网络并保留所述生成对抗网络中的生成器;
- [0035] 以残差网络模型为主干,训练得到一个人脸识别模型。
- [0036] 可选地,所述数据集生成模块,被配置为:
- [0037] 将所述第一人脸图片输入至所述人脸识别模型中,得到所述第一人脸图片对应的

第一特征表达；

[0038] 将所述第二人脸图片输入至所述人脸识别模型中，得到所述第二人脸图片对应的第二特征表达；

[0039] 计算所述第一特征表达和第二特征表达之间的余弦相似度；

[0040] 在所述余弦相似度小于相似度阈值的情况下，保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

[0041] 在一些实施例中，所述电子设备，包括存储器和处理器，其中：

[0042] 所述存储器，用于保存计算机程序；

[0043] 所述处理器，用于执行所述计算机程序，以实现如本申请所述的人脸识别数据集的生成方法。

[0044] 在一些实施例中，所述存储介质，存储有程序指令，所述程序指令在运行时，执行如本申请所述的人脸识别数据集的生成方法。

[0045] 本申请提供的人脸识别数据集的生成方法及装置、电子设备及存储介质，可以实现以下技术效果：

[0046] 本申请采用应用于机器学习技术领域的技术手段，通过生成对抗网络的生成器生成的第一人脸图片，然后通过图片编辑技术根据至少一类人脸属性对第一人脸图片进行修改，以通过生成器生成同一个人脸身份信息的生成的第二人脸图片，进而实现人脸识别数据集的生成，既节省了人力成本，又解决了人脸图像质量较差、单个人脸图片数目较少、数据集中存在重复到的人脸身份信息等各种问题，还能够保护采集对象的人脸生物特征隐私。

[0047] 以上的总体描述和下文中的描述仅是示例性和解释性的，不用于限制本申请。

附图说明

[0048] 一个或多个实施例通过与之对应的附图进行示例性说明，这些示例性说明和附图并不构成对实施例的限定，附图中具有相同参考数字标号的元件示为类似的元件，附图不构成比例限制，并且其中：

[0049] 图1是本申请提供的一个生成对抗网络的架构示意图；

[0050] 图2是本申请提供的一个人脸识别数据集的生成方法的示意图；

[0051] 图3是本申请提供的另一个人脸识别数据集的生成方法的示意图；

[0052] 图4是本申请提供的另一个人脸识别数据集的生成方法的示意图；

[0053] 图5是本申请提供的一个残差网络的数据结构示意图；

[0054] 图6是本申请提供的另一个人脸识别数据集的生成方法的示意图；

[0055] 图7是本申请提供的一个人脸识别数据集的生成方法具体应用示意图；

[0056] 图8是本申请提供的一个人脸识别数据集的生成装置的示意图；

[0057] 图9是本申请提供的另一个人脸识别数据集的生成装置的示意图。

具体实施方式

[0058] 为了能够更加详尽地了解本申请的特点与技术内容，下面结合附图对本申请的实现进行详细阐述，所附附图仅供参考说明之用，并非用来限定本申请。在以下的技术描述中，为方便解释起见，通过多个细节以提供对所披露实施例的充分理解。然而，在没有这些

细节的情况下,一个或多个实施例仍然可以实施。在其它情况下,为简化附图,熟知的结构和装置可以简化展示。

[0059] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的本申请的实施例。此外,术语“包括”和“具有”以及他们的任何变形,意图在于覆盖不排他的包含。

[0060] 除非另有说明,术语“多个”表示两个或两个以上。

[0061] 本申请中,字符“/”表示前后对象是一种“或”的关系。例如,A/B表示:A或B。

[0062] 术语“和/或”是一种描述对象的关联关系,表示可以存在三种关系。例如,A和/或B,表示:A或B,或,A和B这三种关系。

[0063] 术语“对应”可以指的是一种关联关系或绑定关系,A与B相对应指的是A与B之间是一种关联关系或绑定关系。

[0064] 结合图1所示,生成对抗网络(Generative Adversarial Network, GAN)

[0065] 由两个不同的机器学习模型组成,包括一个生成器(Generator)和一个判别器(Discriminator),生成器的目标是生成类似于训练图片的图片,判别器的目标是,输入一张图片并判断输入的图片是真实图片还是生成器产生的假图片。在训练过程中,生成器不断的生成更好的假图片试图骗过判别器,而判别器则在努力成为更好的鉴别者,正确的对真假图片进行分类,具体而言,生成器以随机的潜在编码(也称为潜在编码, Latent Code)作为输入生成图片输出记做 $G(z)$,而判别器输入图片并判别一张图片是不是“真实的”。它的输入参数是 x , x 代表一张图片,输出 $D(x)$ 代表 x 为真实图片的概率,如果为1,就代表是真实的图片,而输出为0,就代表不可能是真实的图片。在训练过程中,生成器的目标就是尽量生成真实的图片去欺骗判别器。而判别器的目标就是尽量把生成器生成的图片和真实的图片分别开来。这样,生成器和判别器构成了一个动态的博弈过程。在最理想的状态下,G可以生成足以“以假乱真”的图片 $G(z)$ 。对于D来说,它难以判定G生成的图片究竟是不是真实的,因此 $D(G(z))=0.5$ 。

[0066] 本申请基于生成对抗网络来生成不存在的人脸图片的算法,然后运用图片编辑技术对该张图片的人脸属性进行修改,例如修改表情、妆容、发型等不影响人脸身份信息的人脸属性,从而对同一个人脸身份信息能够得到多张不存在的人脸图片。

[0067] 结合图2所示,本申请提供一种人脸识别数据集的生成方法,包括:

[0068] 步骤201:将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片。

[0069] 在本申请的实施例中,本申请利用高斯分布随机生成一个第一潜在编码,例如 16×512 的矩阵,然后输入至预设的生成器中,生成器根据第一潜在编码输出不存在的第一人脸图片。

[0070] 步骤202:根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码。

[0071] 在本申请的实施例中,本申请根据至少一类人脸属性,例如表情、发型或妆容等,给生成第二潜在编码添加一个扰动,以生成第二潜在编码,例如 16×512 的矩阵。

[0072] 步骤203:将所述第二潜在编码输入至预设的生成器中,得到所述生成器输出的第二人脸图片。

[0073] 在本申请的实施例中,本申请将第二潜在编码输入至预设的生成器中,生成器根据第二潜在编码输出不存在的第二人脸图片。

[0074] 步骤204:在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

[0075] 在本申请的实施例中,本申请可以使用一个预训练好的人脸识别(Face Recognition,FR)模型,判断第一人脸图片和第二人脸图片是否属于同一人脸身份信息,如果是,则保留第一人脸图片和第二人脸图片作为同一个人脸身份信息包含的人脸图片;如果不是,则丢弃。这样,通过重复上述步骤就可以构建出一个包含大量人脸身份信息及其对应的人脸图片的目标人脸识别数据集。

[0076] 采用本申请提供的人脸识别数据集的生成方法,采用应用于机器学习技术领域的技术手段,通过生成对抗网络的生成器生成不存在的第一人脸图片,然后通过图片编辑技术根据至少一类人脸属性对第一人脸图片进行修改,以通过生成器生成同一人脸身份信息的不存在的第二人脸图片,进而实现人脸识别数据集的生成,既节省了人力成本,又解决了人脸图像质量较差、单个人脸图片数目较少、数据集中存在重复到的人脸身份信息等各种问题,还能够保护采集对象的人脸生物特征隐私。

[0077] 可选地,结合图3所示,所述根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码,包括:

[0078] 步骤301:根据所述至少一类人脸属性中的任一人脸属性,确定修改第一潜在编码的扰动方向和扰动程度。

[0079] 步骤302:根据所述扰动方向和扰动程度对所述第一潜在编码进行变换,生成第二潜在编码。

[0080] 在本申请的实施例中,每一类人脸属性对应一个扰动方向和扰动程度,例如微笑的尺度、发型的颜色和妆容的浓淡等,本领域技术人员能够已知的,通过给定一个人脸属性对应扰动方向和扰动程度,在不显著影响其他属性的情况下,生成引入或放大该人脸属性的图像对应的潜在编码,例如,对于人脸图像中人物头发的颜色,通过沿着头发颜色的扰动方向的正方向,可以使头发颜色变得更灰,而沿着头发颜色的扰动方向的反方向,可以产生较深的头发。同时,随着扰动程度的增加,头发颜色的会变化的更加明显。即本申请可以通过以下公式,基于第一潜在编码计算得到第二潜在编码:

[0081] $\text{latent code2}=\text{latent code1}+\lambda\times\text{direction}$

[0082] 其中,latent code 1表示第一潜在编码,latent code2表示第二潜在编码, λ 表示扰动程度,direction表示扰动方向。

[0083] 这样,能够根据不同的人脸属性对第一潜在编码进行变换,生成多种不同的第二潜在编码和第二人脸图片,提升了单个同一人脸身份信息包含的人脸图片的丰富性和多样性。

[0084] 可选地,结合图4所示,本申请提供一种人脸识别数据集的生成方法,包括:

[0085] 步骤401:从开源人脸识别数据集中获取多张真实的人脸图片。

[0086] 在本申请的实施例中,本申请使用开源人脸识别数据集,例如,从开源的Glint360K数据集(共计36万个人脸身份信息,约1700万张人脸图片)中,获取多张真实的人脸图片。

[0087] 步骤402:根据所述多张真实的人脸图片,训练一个生成对抗网络并保留所述生成对抗网络中的生成器。

[0088] 在本申请的实施例中,本申请基于Style GAN框架,使用多张真实的人脸图片,训练一个生成对抗网络,该生成对抗网络包含一个生成器和一个判别器,训练结束后保留该网络的生成器。生成器是一个神经网络,其输入称为潜在编码,例如,一个维度是 16×512 的矩阵,输出是一张人脸图片,如一张 $3 \times 512 \times 512$ 大小的RGB图片。

[0089] 步骤403:以残差网络模型为主干,训练得到一个人脸识别模型。

[0090] 在本申请的实施例中,结合图5所示,本申请以残差网络模型ResNet50为主干网络,该ResnetNet50包含50个二维卷积层,还包含四个残差块(Residual Block),以及全连接层以用于进行分类任务,ResnetNet50包含50个二维卷积操作,训练得到一个人脸识别模型,该人脸识别模型的输入为一张人脸图,输出为一个特征表达(Embedding),例如,一个512维的特征向量。

[0091] 步骤404:将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片。

[0092] 在本申请的实施例中,本申请利用高斯分布随机生成一个第一潜在编码,例如 16×512 的矩阵,然后输入至预设的生成器中,生成器根据第一潜在编码输出不存在的第一人脸图片。

[0093] 步骤405:根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码。

[0094] 在本申请的实施例中,本申请根据至少一类人脸属性,例如表情、发型或妆容等,给生成第二潜在编码添加一个扰动,以生成第二潜在编码,例如 16×512 的矩阵。

[0095] 步骤406:将所述第二潜在编码输入至预设的生成器中,得到所述生成器输出的第二人脸图片。

[0096] 在本申请的实施例中,本申请将第二潜在编码输入至预设的生成器中,生成器根据第二潜在编码输出不存在的第二人脸图片。

[0097] 步骤407:在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

[0098] 在本申请的实施例中,本申请可以上述训练好的人脸识别模型,判断第一人脸图片和第二人脸图片是否属于同一人脸身份信息,如果是,则保留第一人脸图片和第二人脸图片作为同一个人脸身份信息包含的人脸图片;若果不是,则丢弃。这样,通过重复上述步骤就可以构建出一个包含大量人脸身份信息及其对应的人脸图片的目标人脸识别数据集。

[0099] 可选地,结合图6所示,所述在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集,包括:

[0100] 步骤601:将所述第一人脸图片输入至所述人脸识别模型中,得到所述第一人脸图片对应的第一特征表达。

[0101] 步骤602:将所述第二人脸图片输入至所述人脸识别模型中,得到所述第二人脸图片对应的第二特征表达。

[0102] 步骤603:计算所述第一特征表达和第二特征表达之间的余弦相似度。

[0103] 步骤604:在所述余弦相似度小于相似度阈值的情况下,保存所述第一人脸图片和

第二人脸图片以生成目标人脸识别数据集。

[0104] 在本申请的实施例中,结合图7所示,本申请将第一人脸图片和第二人脸图片输入至预训练好的人脸识别模型中,分别得到对应的第一特征表达和第二特征表达,然后计算第一特征表达和第二特征表达之间的余弦相似度,并将余弦相似度与相似度阈值进行比较,以判断是否属于同一个人脸身份信息,如果是同一个人脸,则保留第一人脸图片和第二人脸图片为同一个人脸身份信息的不同人脸图片,如果不是同一个人脸则丢弃。

[0105] 这样,使用上述流程能够低成本的批量生成一个包含大量人脸身份信息的人脸识别数据集,并且其中的人脸图片的质量较高,单个人脸图片数目多,且同一人脸身份信息的人重复率较低。

[0106] 结合图8所示,本申请提供一种人脸识别数据集的生成装置,其特征在在于,包括:

[0107] 第一图片生成模块801,被配置为将随机生成的第一潜在编码输入至预设的生成器中,得到所述生成器输出的第一人脸图片;

[0108] 扰动添加模块802,被配置为根据至少一类人脸属性更新所述第一潜在编码,生成第二潜在编码;

[0109] 第二图片生成模块803,被配置为将所述第二潜在编码输入至预设的生成器中,得到所述生成器输出的第二人脸图片;

[0110] 数据集生成模块804,被配置为在确定所述第一人脸图片和第二人脸图片属于同一人脸身份信息的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

[0111] 可选地,所述扰动添加模块802,具体被配置为:

[0112] 根据所述至少一类人脸属性中的任一人脸属性,确定修改第一潜在编码的扰动方向和扰动程度;

[0113] 根据所述扰动方向和扰动程度对所述第一潜在编码进行变换,生成第二潜在编码。

[0114] 可选地,所述装置还包括预训练模块,所述预训练模块被配置为:

[0115] 从开源人脸识别数据集中获取多张真实的人脸图片;

[0116] 根据所述多张真实的人脸图片,训练一个生成对抗网络并保留所述生成对抗网络中的生成器;

[0117] 以残差网络模型为主干,训练得到一个人脸识别模型。

[0118] 可选地,所述数据集生成模块804,被配置为:

[0119] 将所述第一人脸图片输入至所述人脸识别模型中,得到所述第一人脸图片对应的第一特征表达;

[0120] 将所述第二人脸图片输入至所述人脸识别模型中,得到所述第二人脸图片对应的第二特征表达;

[0121] 计算所述第一特征表达和第二特征表达之间的余弦相似度;

[0122] 在所述余弦相似度小于相似度阈值的情况下,保存所述第一人脸图片和第二人脸图片以生成目标人脸识别数据集。

[0123] 采用本申请提供的人脸识别数据集的生成装置,采用应用于机器学习技术领域的技术手段,通过生成对抗网络的生成器生成不存在的第一人脸图片,然后通过图片编辑技

术根据至少一类人脸属性对第一人脸图片进行修改,以通过生成器生成同一人脸身份信息的不存在的第二人脸图片,进而实现人脸识别数据集的生成,既节省了人力成本,又解决了人脸图像质量较差、单个人脸图片数目较少、数据集中存在重复到的人脸身份信息等各种问题,还能够保护采集对象的人脸生物特征隐私。

[0124] 结合图9所示,本申请提供一种人脸识别数据集的生成装置,包括处理器(processor)900和存储器(memory)901。可选地,该装置还可以包括通信接口(Communication Interface)902和总线903。其中,处理器900、通信接口902、存储器901可以通过总线903完成相互间的通信。通信接口902可以用于信息传输。处理器900可以调用存储器901中的逻辑指令,以执行上述实施例的人脸识别数据集的生成方法。

[0125] 此外,上述的存储器901中的逻辑指令可以通过软件功能单元的形式实现并作为独立的产品销售或使用,可以存储在一个计算机可读取存储介质中。

[0126] 存储器901作为一种计算机可读存储介质,可用于存储软件程序、计算机可执行程序,如本申请中的方法对应的程序指令/模块。处理器900通过运行存储在存储器901中的程序指令/模块,从而执行功能应用以及数据处理,即实现上述实施例中人脸识别数据集的生成方法。

[0127] 存储器901可包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序;存储数据区可存储根据终端设备的使用所创建的数据等。此外,存储器901可以包括高速随机存取存储器,还可以包括非易失性存储器。

[0128] 本申请提供了一种存储介质,存储有计算机可执行指令,所述计算机可执行指令设置为执行上述人脸识别数据集的生成方法。

[0129] 上述的存储介质可以是暂态计算机可读存储介质,也可以是非暂态计算机可读存储介质。

[0130] 本申请的技术方案可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括一个或多个指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备)执行本申请所述方法的全部或部分步骤。而前述的存储介质可以是非暂态存储介质,包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等多种可以存储程序代码的介质,也可以是暂态存储介质。

[0131] 以上描述和附图充分地示出了本公开的实施例,以使本领域的技术人员能够实践它们。其他实施例可以包括结构的、逻辑的、电气的、过程的以及其他的改变。实施例仅代表可能的变化。除非明确要求,否则单独的部件和功能是可选的,并且操作的顺序可以变化。一些实施例的部分和特征可以被包括在或替换其他实施例的部分和特征。而且,本申请中使用的用词仅用于描述实施例并且不用于限制权利要求。如在实施例以及权利要求的描述中使用的,除非上下文清楚地表明,否则单数形式的“一个”(a)、“一个”(an)和“所述”(the)旨在同样包括复数形式。类似地,如在本申请中所使用的术语“和/或”是指包含一个或一个以上相关联的列出的任何以及所有可能的组合。另外,当用于本申请中时,术语“包括”(comprise)及其变型“包括”(comprises)和/或包括(comprising)等指陈述的特征、整体、步骤、操作、元素,和/或组件的存在,但不排除一个或一个以上其它特征、整体、步骤、操作、元素、组件和/或这些的分组的存在或添加。在没有更多限制的情况下,由语句“包括一

个…”限定的要素,并不排除在包括所述要素的过程、方法或者设备中还存在另外的相同要素。本文中,每个实施例重点说明的可以是与其他实施例的不同之处,各个实施例之间相同相似部分可以互相参见。对于实施例公开的方法、产品等而言,如果其与实施例公开的方法部分相对应,那么相关之处可以参见方法部分的描述。

[0132] 本领域技术人员可以意识到,结合本文中所公开的实施例描述的各示例的单元及算法步骤,能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行,可以取决于技术方案的特定应用和设计约束条件。所述技术人员可以对每个特定的应用来使用不同方法以实现所描述的功能,但是这种实现不应认为超出本申请的范围。所述技术人员可以清楚地了解到,为描述的方便和简洁,上述描述的系统、装置和单元的具体工作过程,可以参考前述方法实施例中的对应过程,在此不再赘述。

[0133] 本文所披露的实施例中,所揭露的方法、产品(包括但不限于装置、设备等),可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,所述单元的划分,可以仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例。另外,在本申请中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。

[0134] 附图中的流程图和框图显示了根据本申请的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分,所述模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这可以依所涉及的功能而定。在附图中的流程图和框图所对应的描述中,不同的方框所对应的操作或步骤也可以以不同于描述中所披露的顺序发生,有时不同的操作或步骤之间不存在特定的顺序。例如,两个连续的操作或步骤实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这可以依所涉及的功能而定。框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

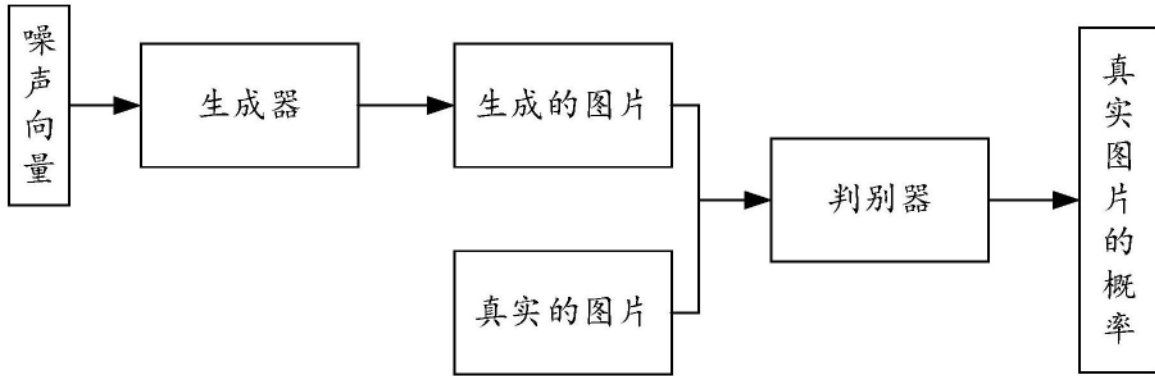


图1

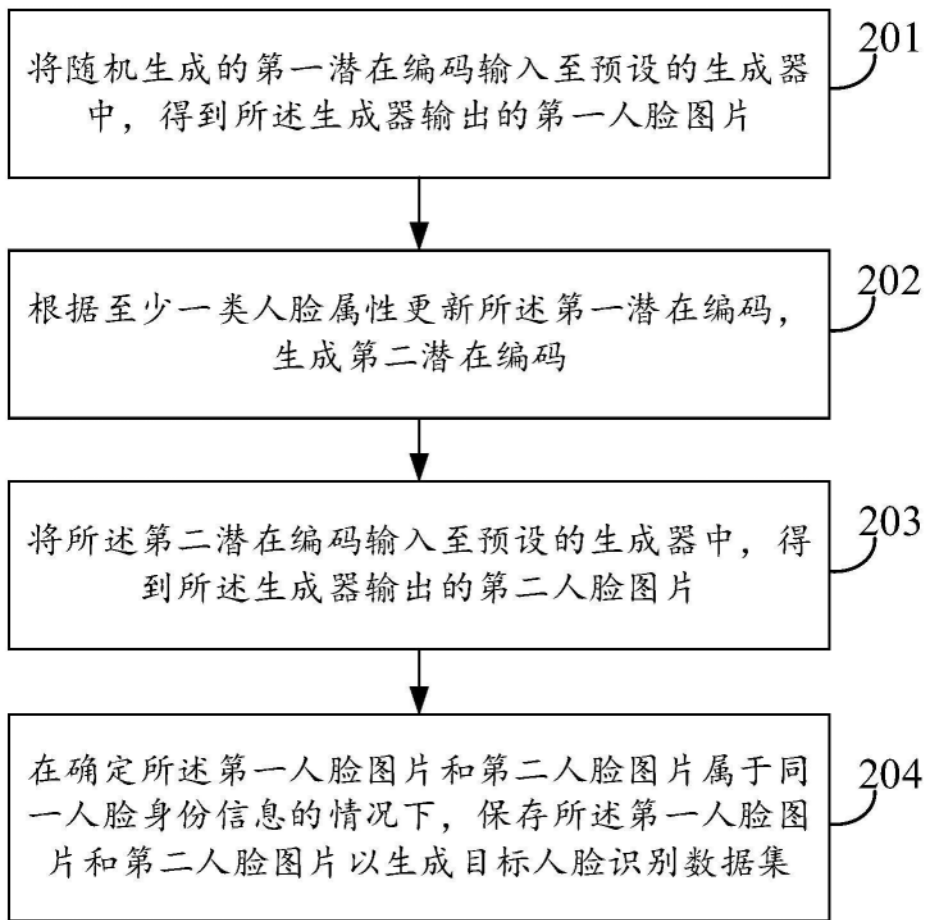


图2

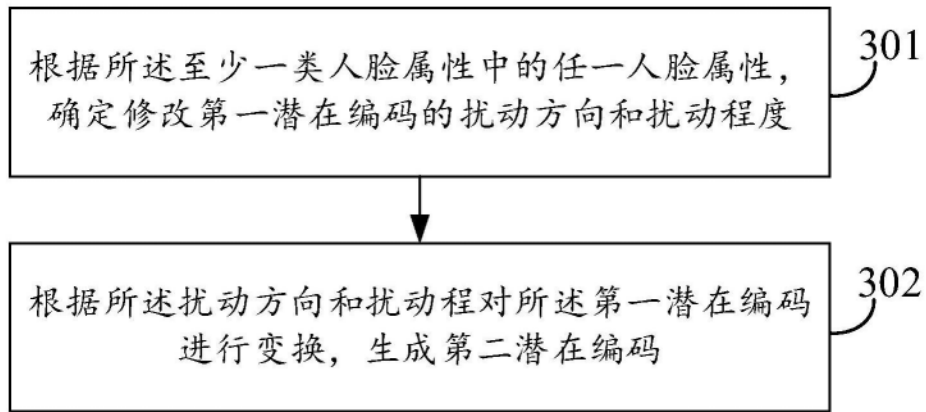


图3

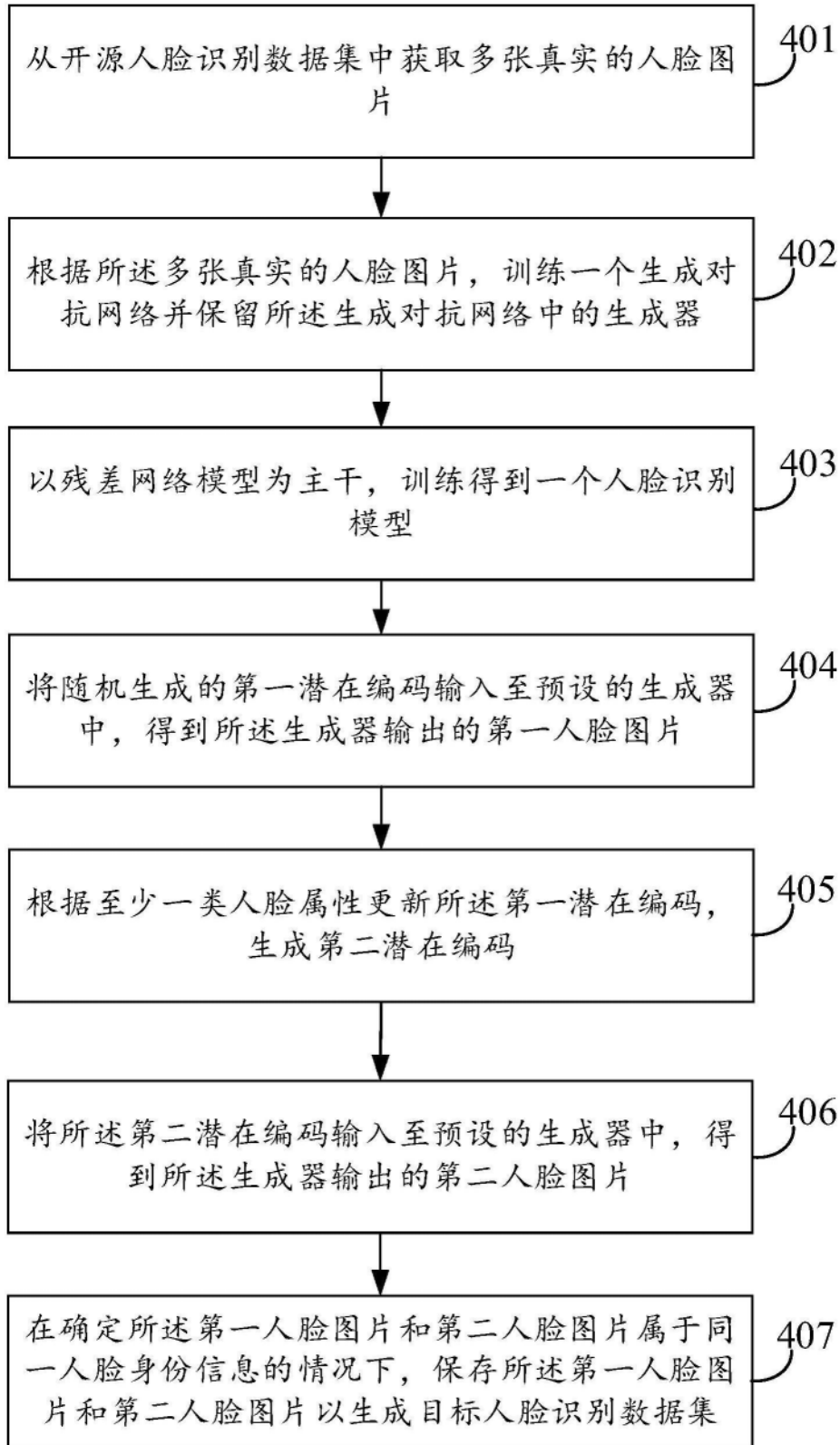


图4

layer name	output size	18-layer	34-layer	50-layer	101-layer	152-layer
conv1	112×112			7×7, 64, stride 2		
				3×3 max pool, stride 2		
conv2_x	56×56	$\begin{bmatrix} 3 \times 3, 64 \\ 3 \times 3, 64 \end{bmatrix} \times 2$	$\begin{bmatrix} 3 \times 3, 64 \\ 3 \times 3, 64 \end{bmatrix} \times 3$	$\begin{bmatrix} 1 \times 1, 64 \\ 3 \times 3, 64 \\ 1 \times 1, 256 \end{bmatrix} \times 3$	$\begin{bmatrix} 1 \times 1, 64 \\ 3 \times 3, 64 \\ 1 \times 1, 256 \end{bmatrix} \times 3$	$\begin{bmatrix} 1 \times 1, 64 \\ 3 \times 3, 64 \\ 1 \times 1, 256 \end{bmatrix} \times 3$
conv3_x	28×28	$\begin{bmatrix} 3 \times 3, 128 \\ 3 \times 3, 128 \end{bmatrix} \times 2$	$\begin{bmatrix} 3 \times 3, 128 \\ 3 \times 3, 128 \end{bmatrix} \times 4$	$\begin{bmatrix} 1 \times 1, 128 \\ 3 \times 3, 128 \\ 1 \times 1, 512 \end{bmatrix} \times 4$	$\begin{bmatrix} 1 \times 1, 128 \\ 3 \times 3, 128 \\ 1 \times 1, 512 \end{bmatrix} \times 4$	$\begin{bmatrix} 1 \times 1, 128 \\ 3 \times 3, 128 \\ 1 \times 1, 512 \end{bmatrix} \times 8$
conv4_x	14×14	$\begin{bmatrix} 3 \times 3, 256 \\ 3 \times 3, 256 \end{bmatrix} \times 2$	$\begin{bmatrix} 3 \times 3, 256 \\ 3 \times 3, 256 \end{bmatrix} \times 6$	$\begin{bmatrix} 1 \times 1, 256 \\ 3 \times 3, 256 \\ 1 \times 1, 1024 \end{bmatrix} \times 6$	$\begin{bmatrix} 1 \times 1, 256 \\ 3 \times 3, 256 \\ 1 \times 1, 1024 \end{bmatrix} \times 23$	$\begin{bmatrix} 1 \times 1, 256 \\ 3 \times 3, 256 \\ 1 \times 1, 1024 \end{bmatrix} \times 36$
conv5_x	7×7	$\begin{bmatrix} 3 \times 3, 512 \\ 3 \times 3, 512 \end{bmatrix} \times 2$	$\begin{bmatrix} 3 \times 3, 512 \\ 3 \times 3, 512 \end{bmatrix} \times 3$	$\begin{bmatrix} 1 \times 1, 512 \\ 3 \times 3, 512 \\ 1 \times 1, 2048 \end{bmatrix} \times 3$	$\begin{bmatrix} 1 \times 1, 512 \\ 3 \times 3, 512 \\ 1 \times 1, 2048 \end{bmatrix} \times 3$	$\begin{bmatrix} 1 \times 1, 512 \\ 3 \times 3, 512 \\ 1 \times 1, 2048 \end{bmatrix} \times 3$
	1×1			average pool, 1000-d fc, softmax		
FLOPs		1.8×10^9	3.6×10^9	3.8×10^9	7.6×10^9	11.3×10^9

图5

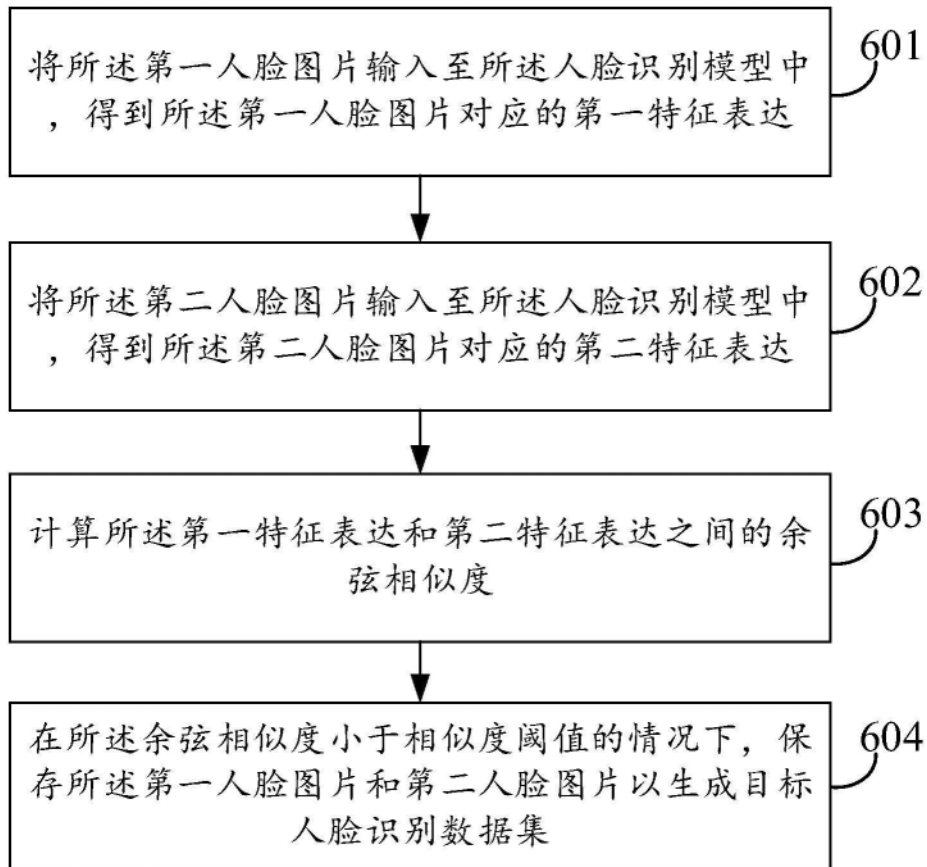


图6

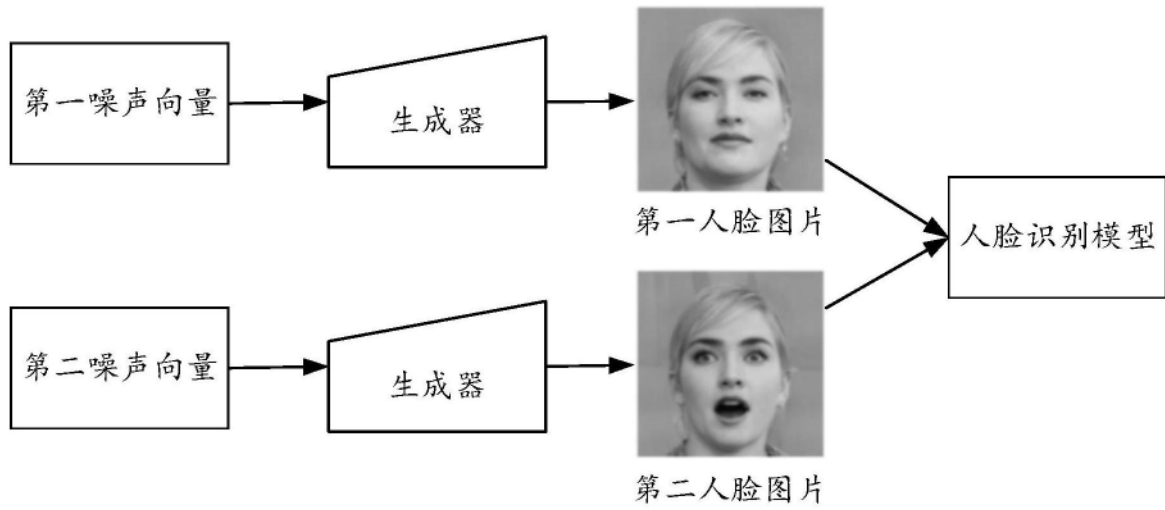


图7

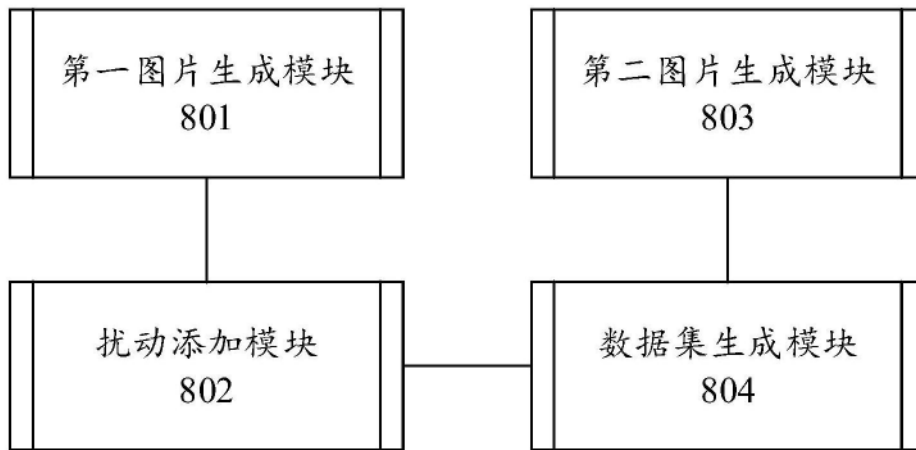


图8

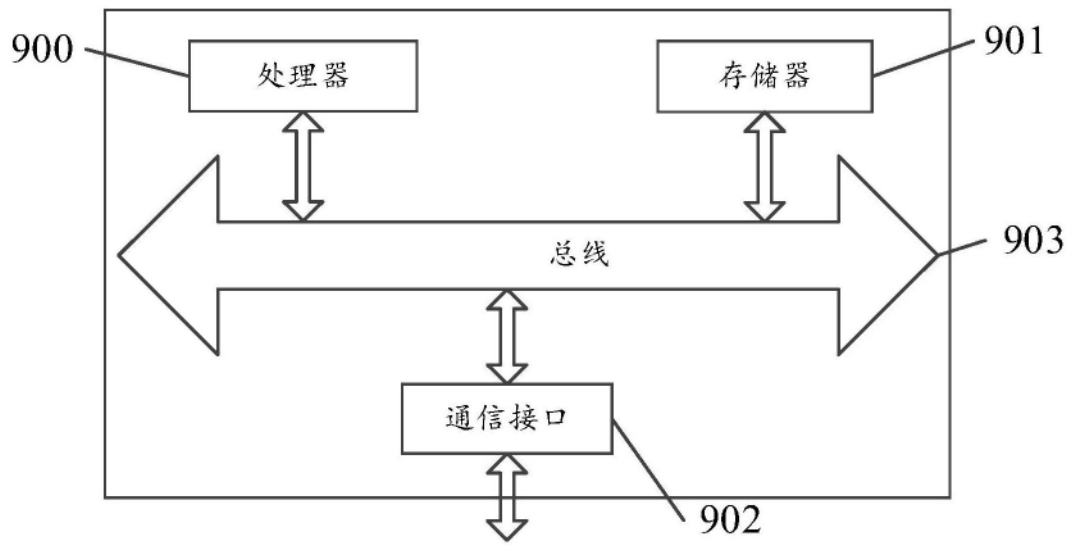


图9