(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114503172 A
(43)申请公布日 2022.05.13

(21)申请号 202080069809.3
(22)申请日 2020.08.07
(30)优先权数据
62/884,766 2019.08.09 US
(85)PCT国际申请进入国家阶段日
2022.04.01
(86)PCT国际申请的申请数据
PCT/US2020/045361 2020.08.07
(87)PCT国际申请的公布数据
WO2021/030178 EN 2021.02.18
(71)申请人 克利尔维尤人工智能股份有限公司
地址 美国纽约州
(72)发明人 C-H.通-萨特
(74)专利代理机构 北京市柳沈律师事务所 11105
专利代理师 胡琪
(51)Int.Cl.
G06V 40/16(2022.01)

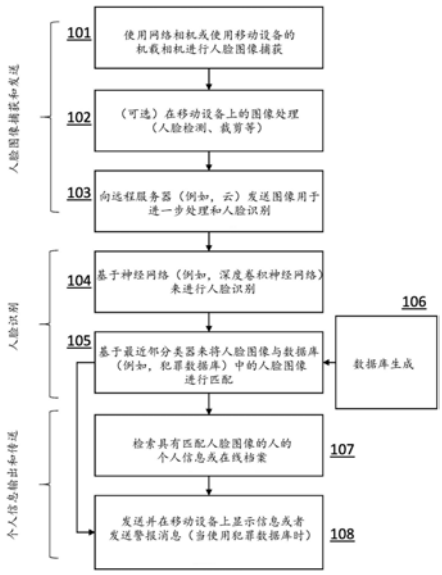
权利要求书5页 说明书16页 附图10页

(54)发明名称

基于人脸识别来提供关于人的信息的方法

(57)摘要

本公开提供了基于人脸识别来提供关于人的信息的方法以及其各种应用,包括基于人脸的登记、基于人脸的个人识别、基于人脸的身份验证、基于人脸的背景调查、人脸数据协作网络、相关人脸搜索和基于个人人脸的识别。所公开的方法能够以实时的方式提供关于人的准确信息。



CN 114503172 A

1.一种提供关于主体的信息的方法,包括:

接收从用户设备发送的人脸图像数据,所述人脸图像数据至少包括所述主体的捕获的人脸图像;

将所述人脸图像数据转换成人脸识别数据;

由服务器设备将所述人脸识别数据和与多个存储的个体人脸图像相关联的参考人脸识别数据进行比较,以识别与所述捕获的人脸图像匹配的至少一个可能的候选;

在识别出与所述捕获的人脸图像匹配的候选时,从数据库中检索与所述候选相关联的个人信息;以及

向所述用户设备发送所述个人信息,并使所述用户设备显示所述个人信息。

2.根据权利要求1所述的方法,还包括由所述用户设备预处理所述主体的图像。

3.根据权利要求2所述的方法,其中,预处理包括由所述用户设备在所述主体的图像中检测人脸图像。

4.根据权利要求2或3所述的方法,其中,预处理的步骤包括裁剪、调整尺寸、灰度转换、中值滤波、直方图均衡化或尺寸归一化图像处理。

5.根据前述权利要求中任一项所述的方法,其中,所述人脸图像由有相机功能的用户设备捕获。

6.根据权利要求5所述的方法,其中,所述用户设备被提供在具有针对所述相机的开口的定制外壳中。

7.根据前述权利要求中任一项所述的方法,其中,所述图像由网络相机捕获。

8.根据前述权利要求中任一项所述的方法,其中,所述图像是从第二用户设备导入的。

9.根据前述权利要求中任一项所述的方法,其中,所述主体是人。

10.根据前述权利要求中任一项所述的方法,其中,所述主体是罪犯。

11.根据前述权利要求中任一项所述的方法,其中,所述人脸图像数据包括所述主体的三维人脸图像。

12.根据前述权利要求中任一项所述的方法,还包括:

通过网络爬虫下载个体人脸图像和与其相关联的个人信息;以及

将所下载的人脸图像和相关联的个人信息存储在所述数据库中。

13.根据权利要求12所述的方法,其中,所述参考人脸识别数据包括通过所述网络爬虫下载的人脸图像。

14.根据权利要求12所述的方法,其中,所述参考人脸识别数据包括从互联网、职业网站、执法部门网站或机动车辆部门获得的人脸图像。

15.根据前述权利要求中任一项所述的方法,其中,所述数据库包括与存储在所述数据库中的人脸图像相关联的多个犯罪记录。

16.根据前述权利要求中任一项所述的方法,其中,所述人脸识别数据包括所述主体的所述捕获的人脸图像的向量表示。

17.根据前述权利要求中任一项所述的方法,其中,所述参考人脸识别数据包括所述数据库中存储的人脸图像的向量表示。

18.根据权利要求16或17所述的方法,其中,所述向量表示包括512点向量或1024×1024人脸数据矩阵。

19.根据权利要求16或17所述的方法,其中,比较的步骤还包括将所述主体的所述捕获的人脸图像的向量表示和与所述数据库中存储的人脸图像相关联的向量表示进行比较。

20.根据前述权利要求中任一项所述的方法,其中,比较所述人脸识别数据是由机器学习模块来执行的。

21.根据权利要求20所述的方法,其中,所述机器学习模块包括深度卷积神经网络(DCNN)。

22.根据前述权利要求中任一项所述的方法,其中,所述候选的识别通过k-最近邻算法(k-NN)来执行。

23.根据前述权利要求中任一项所述的方法,还包括检测活体姿势。

24.根据权利要求23所述的方法,其中,所述活体姿势基于第二图像相对于第一图像的偏航角和所述第二图像相对于所述第一图像的俯仰角中的至少一个,其中所述偏航角对应于以垂直轴为中心的转变,并且其中所述俯仰角对应于以水平轴为中心的转变。

25.根据前述权利要求中任一项所述的方法,其中,所述个人信息是基于所识别的候选的预定隐私设置而从所述数据库中检索的。

26.根据前述权利要求中任一项所述的方法,还包括显示所识别的候选的一个或多个人脸图像以及与其相关联的个人信息。

27.根据前述权利要求中任一项所述的方法,还包括如果所识别的候选对公众构成高风险或者是罪犯,则向所述用户设备发送通知。

28.根据权利要求26所述的方法,其中,所述个人信息包括所识别的候选的姓名。

29.根据权利要求26或28所述的方法,其中,所述个人信息包括到与所识别的匹配相关联的在线档案的链接。

30.根据前述权利要求中任一项所述的方法,其中,向所述用户设备发送的个人信息是从包含所述个人信息的网页当中具有最高页面评级值的网页获得的。

31.根据前述权利要求中任一项所述的方法,还包括:

基于所识别的候选的个人信息,确定对所述主体访问场所或账户的许可;

如果所识别的候选是授权用户,则准许所述主体的访问,或者

如果所识别的候选不是授权用户或者不能识别与所述捕获的人脸图像匹配的候选,则拒绝所述主体的访问;以及

发送指示准许或拒绝访问所述场所或所述账户的消息。

32.根据权利要求31所述的方法,其中,所述账户与银行、金融机构或信贷公司相关联。

33.根据前述权利要求中任一项所述的方法,包括向多个用户提供对所述数据库的访问。

34.根据权利要求33所述的方法,其中,所述多个用户位于相同的地理区域或与相同的商业类型相关联。

35.根据前述权利要求中任一项所述的方法,其中,所述人脸图像数据包括第二主体的第二捕获的人脸图像。

36.根据权利要求35所述的方法,还包括识别在单个图像中被捕获到了人脸图像的两个或更多个主体之间的关系。

37.一种验证用户的身份的方法,包括:

提供所述用户的人脸图像数据和个人识别号，所述人脸图像数据包括捕获的人脸图像；

将所述人脸图像数据转换成人脸识别数据；

将所述人脸识别数据和所述个人识别号和与多个存储的个体人脸图像相关联的参考人脸识别数据和参考个人识别号进行比较，以识别与所述捕获的人脸图像和所述个人识别号匹配的至少一个可能的候选；以及

在识别出所述候选时，向用户设备发送确认以指示该所述用户是授权用户。

38.一种提供关于主体的信息的系统，包括：

人脸图像处理模块，其能够操作为将所述主体的捕获的人脸图像转换成人脸识别数据；以及

人脸识别模块，其能够操作为：

将所述人脸识别数据和与多个存储的个体人脸图像相关联的参考人脸识别数据进行比较，以识别与所述捕获的人脸图像匹配的至少一个可能的候选，

在识别出与所捕捉的人脸图像匹配的候选时，从数据库中检索与所述候选相关联的个人信息，以及

向用户设备发送所述个人信息，并使所述用户设备显示所述个人信息。

39.根据权利要求38所述的系统，还包括多个成像设备，其中所述多个成像设备中的每个能够操作为捕获包括所述主体的人脸的至少一个图像以生成捕获的图像。

40.根据权利要求38所述的系统，其中，所述多个成像设备无线地耦合到存储所述多个存储的图像的监控站。

41.根据权利要求38-40中任一项所述的系统，其中，所述人脸图像处理模块能够操作为由所述用户设备预处理所述主体的图像。

42.根据权利要求38-41中任一项所述的系统，其中，所述人脸图像处理模块能够操作为在所述主体的图像中检测人脸图像。

43.根据权利要求41所述的系统，其中预处理包括裁剪、调整尺寸、灰度转换、中值滤波、直方图均衡化或尺寸归一化图像处理。

44.根据权利要求38-43中任一项所述的系统，其中，所述主体是人。

45.根据权利要求38-44中任一项所述的系统，其中，所述主体是罪犯。

46.根据权利要求38-45中任一项所述的系统，其中，所述人脸图像数据包括所述主体的三维人脸图像。

47.根据权利要求38-46中任一项所述的系统，其中，所述人脸图像处理模块能够操作为：

通过网络爬虫下载个体人脸图像和与其相关联的个人信息；以及

将所下载的人脸图像和相关联的个人信息存储在所述数据库中。

48.根据权利要求47所述的系统，其中，所述参考人脸识别数据包括通过所述网络爬虫下载的人脸图像。

49.根据权利要求38-48中任一项所述的系统，其中，所述参考人脸识别数据包括从互联网、职业网站、执法部门网站或机动车辆部门获得的人脸图像。

50.根据权利要求38-49中任一项所述的系统，其中，所述数据库包括与存储在所述数

据库中的人脸图像相关联的多个犯罪记录。

51.根据权利要求38-50中任一项所述的系统，其中，所述人脸识别数据包括所述主体的所述捕获的人脸图像的向量表示。

52.根据权利要求38-51中任一项所述的系统，其中，所述参考人脸识别数据包括所述数据库中存储的人脸图像的向量表示。

53.根据权利要求38-52中任一项所述的系统，其中，所述向量表示包括512点向量或1024×1024人脸数据矩阵。

54.根据权利要求38-53中任一项所述的系统，其中，所述人脸识别模块能够操作为将所述主体的所述捕获的人脸图像的向量表示和与所述数据库中存储的人脸图像相关联的向量表示进行比较。

55.根据权利要求38-54中任一项所述的系统，其中，所述人脸识别模块包括机器学习模块，比较所述人脸识别数据是由机器学习模块来执行的。

56.根据权利要求55所述的系统，其中，所述机器学习模块包括深度卷积神经网络(DCNN)。

57.根据权利要求38-56中任一项所述的系统，其中，所述候选的识别是通过k-最近邻算法(k-NN)来执行的。

58.根据权利要求38-57中任一项所述的系统，其中，所述人脸图像处理模块能够操作为检测活体姿势。

59.根据权利要求58所述的系统，其中，所述活体姿势基于第二图像相对于第一图像的偏航角和所述第二图像相对于所述第一图像的俯仰角中的至少一个，其中所述偏航角对应于以垂直轴为中心的转变，并且其中所述俯仰角对应于以水平轴为中心的转变。

60.根据权利要求38-59中任一项所述的系统，其中，所述个人信息是基于所识别的候选的预定隐私设置而从所述数据库中检索的。

61.根据权利要求38-60中任一项所述的系统，其中，所述人脸识别模块能够操作为显示所识别的候选的一个或多个图像以及与其相关联的个人信息。

62.根据权利要求38-61中任一项所述的系统，其中，所述人脸识别模块能够操作为：如果所识别的候选对公众构成高风险或者是罪犯，则向所述用户设备发送通知。

63.根据权利要求38-62中任一项所述的系统，其中，所述个人信息包括所识别的候选的姓名。

64.根据权利要求38-63中任一项所述的系统，其中，所述个人信息包括到与所识别的匹配相关联的在线档案的链接。

65.根据权利要求38-64中任一项所述的系统，其中，向所述用户设备发送的个人信息是从包含所述个人信息的网页当中具有最高页面评级值的网页获得的。

66.根据权利要求38-65中任一项所述的系统，其中，所述人脸识别模块能够操作为：

基于所识别的候选的个人信息，确定对所述主体访问场所或账户的许可；

如果所识别的候选是授权用户，则准许所述主体的访问，或者

如果所识别的候选不是授权用户或者不能识别与所述捕获的人脸图像匹配的候选，则拒绝所述主体的访问；以及

发送指示准许或拒绝访问所述场所或所述账户的消息。

67.根据权利要求66所述的系统，其中，所述账户与银行、金融机构或信贷公司相关联。

68.根据权利要求38-67中任一项所述的系统，其中，所述人脸识别模块能够操作为向多个用户提供对所述数据库的访问。

69.根据权利要求68所述的系统，其中，所述多个用户位于相同的地理区域或与相同的商业类型相关联。

70.根据权利要求38-69中任一项所述的系统，其中，所述人脸图像数据包括第二主体的第二捕获的人脸图像。

71.根据权利要求38-70中任一项所述的系统，其中，所述人脸识别模块能够操作为提供访问以识别在单个图像中被捕获到了人脸图像的两个或更多个主体之间的关系。

72.一种验证用户的身份的系统，包括：

人脸图像处理模块，其能够操作为将主体的捕获的人脸图像转换成人脸识别数据；以及

人脸识别模块，其能够操作为：

提供所述用户的人脸图像数据和个人识别号，所述人脸图像数据包括捕获的人脸图像；

将所述人脸图像数据转换成人脸识别数据；

将所述人脸识别数据和所述个人识别号和与多个存储的个体人脸图像相关联的参考人脸识别数据和参考个人识别号进行比较，以识别与所述捕获的人脸图像和所述个人识别号匹配的至少一个可能的候选；以及

在识别出所述候选时，向用户设备发送确认以指示所述用户是授权用户。

基于人脸识别来提供关于人的信息的方法

[0001] 相关申请的交叉引用

[0002] 根据35 U.S.C.§119(e),本申请要求于2019年08月09日提交的美国临时专利申请号62/884,766的优先权。前述申请通过引用整体并入本文。

技术领域

[0003] 本发明涉及基于人脸识别来提供关于人的信息的方法和系统。

背景技术

[0004] 在许多情况下,对于个体来说可能期望更多地了解他们诸如通过商业、约会或其他关系而认识的人。有许多传统的方法来了解新的人。例如,这些方法中的一些是询问这个人的背景或历史,或者从这个人那里接收诸如名片之类的文件。然而,由这个人提供的信息以及这些信息,无论是口头还是书面的,都可能是虚假的。个体几乎没有办法确定该信息是准确的还是虚假的。替代地,可以在网站上搜索新认识的人,或者执行背景调查。然而,在许多情况下,人可以擅用新的姓名或身份以向个体呈现虚假的姓名和历史。因此,即使是最好的搜索也不会产生准确的结果。

[0005] 在一些情况下,个体需要立即了解新认识的人的信息,以确定这个人是否诚实或具有所声称的背景。现有的方法不能快速提供关于该个体的准确信息。例如,传统的背景调查可能需要三天到一个月的时间。这种延迟通常使得所获得的关于这个人的信息是不准确且无用的。

[0006] 因此,强烈需要一种改进的方法和系统来获得关于人的信息,并且基于预定的标准来选择性地提供该信息。

发明内容

[0007] 本公开在多个方面解决了以上所提及的需要。在一个方面,本公开提出了一种用于提供关于人(例如,陌生人、新认识的人、记忆有缺陷的人)的信息的方法。该方法包括:(i)接收从用户设备发送的人脸图像数据。该人脸图像数据至少包括主体(subject)的捕获的人脸图像;(ii)将人脸图像数据转换成人脸识别数据;(iii)由服务器设备将人脸识别数据和与多个存储的个体人脸图像相关联的参考人脸识别数据进行比较,以识别与捕获的人脸图像匹配的至少一个可能的候选;(iv)在识别出与捕获的人脸图像匹配的候选时,从数据库中检索与该候选相关联的个人信息(例如,履历、档案信息);以及(v)向用户设备发送个人信息,并使用户设备显示该个人信息。

[0008] 在一些实施例中,该方法包括由用户设备预处理主体的图像。预处理可以包括由用户设备在主体的图像中检测人脸图像。预处理还可以包括裁剪、调整尺寸、灰度转换、中值滤波、直方图均衡化或尺寸归一化图像处理。在一些实施例中,人脸图像由有相机功能的用户设备捕获。在一些实施例中,用户设备被提供在具有针对相机的开口的定制外壳中。在一些实施例中,图像由网络相机捕获。在一些实施例中,图像是从第二用户设备导入的。在

一些实施例中，主体是人。在一些实施例中，主体是罪犯。在一些实施例中，人脸图像数据包括主体的三维人脸图像。

[0009] 在一些实施例中，该方法还包括：(i)通过网络爬虫下载个体人脸图像以及与其相关联的个人信息；以及(2)将下载的人脸图像和相关联的个人信息存储在数据库中。在一些实施例中，参考人脸识别数据包括通过网络爬虫下载的人脸图像。参考人脸识别数据可以包括从互联网、职业网站、执法部门网站或机动车辆部门获得的人脸图像。在一些实施例中，数据库包括与存储在数据库中的人脸图像相关联的多个犯罪记录。

[0010] 在一些实施例中，人脸识别数据包括主体的捕获的人脸图像的向量表示。类似地，参考人脸识别数据也可以包括数据库中存储的人脸图像的向量表示。在一些实施例中，向量表示包括512点向量或1024×1024人脸数据矩阵。

[0011] 在一些实施例中，比较步骤还包括将主体的捕获的人脸图像的向量表示和与数据库中存储的人脸图像相关联的向量表示进行比较。比较人脸识别数据可以由机器学习模块来执行。机器学习模块包括深度卷积神经网络(CNN)。在一些实施例中，候选的识别通过k-最近邻算法(k-NN)来执行。

[0012] 在一些实施例中，该方法还可以包括检测活体(liveness)姿势(gesture)。活体姿势基于第二图像相对于第一图像的偏航角和第二图像相对于第一图像的俯仰角中的至少一个，其中偏航角对应于以垂直轴为中心的转变，并且其中俯仰角对应于以水平轴为中心的转变。

[0013] 在一些实施例中，个人信息是基于所识别的候选的预定隐私设置而从数据库中检索的。在一些实施例中，该方法还包括显示所识别的候选的一个或多个人脸图像以及与其相关联的个人信息。在一些实施例中，该方法还可以包括如果所识别的候选对公众构成高风险或者是罪犯，则向用户设备发送通知。在一些实施例中，个人信息可以包括所识别的候选的姓名。在一些实施例中，个人信息可以包括到与所识别的匹配相关联的在线档案的链接。在一些实施例中，向用户设备发送的个人信息是从包含个人信息的网页当中具有最高页面评级(PageRank)值的网页获得的。

[0014] 在一些实施例中，该方法还包括：(i)基于所识别的候选的个人信息，确定对主体访问场所或账户的许可；(ii)如果所识别的候选是授权用户，则准许该主体的访问，或者如果所识别的候选不是授权用户或者不能识别与捕获的人脸图像匹配的候选，则拒绝该主体的访问；以及(iii)发送指示准许或拒绝访问场所或账户的消息。在一些实施例中，账户与银行、金融机构或信贷公司相关联。

[0015] 在一些实施例中，该方法附加地包括向多个用户提供对数据库的访问。多个用户可以位于相同的地理区域或者与相同的商业类型相关联。

[0016] 在一些实施例中，人脸图像数据包括第二主体的第二捕获的人脸图像。在一些实施例中，该方法包括识别在单个图像中被捕获到了人脸图像的两个或更多个主体之间的关系。

[0017] 在另一方面，本公开提供了一种验证用户的身份的方法。该方法包括：(a)提供人脸图像数据和用户的个人识别号，该人脸图像数据包括捕获的人脸图像；(b)将人脸图像数据转换成人脸识别数据；(c)将人脸识别数据和个人识别号和与多个存储的个体人脸图像相关联的参考人脸识别数据和参考个人识别号进行比较，以识别与捕获的人脸图像和个人

识别号匹配的至少一个可能的候选;以及(d)在识别出候选时,向用户设备发送确认以指示该用户是授权用户。

[0018] 在另一方面,本公开还提出了一种提供关于主体的信息的系统。该系统包括:(i)人脸图像处理模块,其可操作以将主体的捕获的人脸图像转换成人脸识别数据;以及(ii)人脸识别模块,其可操作以:(a)将人脸识别数据和与多个存储的个体人脸图像相关联的参考人脸识别数据进行比较,以识别与捕获的人脸图像匹配的至少一个可能的候选,(b)在识别出与捕获的人脸图像匹配的候选时,从数据库中检索与该候选相关联的个人信息,以及(c)向用户设备发送个人信息,并使用户设备显示该个人信息。

[0019] 在一些实施例中,该系统包括多个成像设备,其中多个成像设备中的每个可操作以捕获包括主体的人脸的至少一个图像,以生成捕获的图像。多个成像设备无线地耦合到存储多个存储图像的监控站。

[0020] 在又一方面,本公开提供了一种提供安全性的方法。该方法包括(i)在个体所经过的多个区域中提供成像设备,其中成像设备可操作以获得每个个体的人脸图像;以及(ii)由如上所描述的系统执行人脸识别。

[0021] 在一些实施例中,人脸图像处理模块可操作以由用户设备预处理主体的图像。预处理可以包括由用户设备在主体的图像中检测人脸图像。预处理还可以包括裁剪、调整尺寸、灰度转换、中值滤波、直方图均衡化或尺寸归一化图像处理。在一些实施例中,人脸图像由有相机功能的用户设备捕获。在一些实施例中,用户设备被提供在具有针对相机的开口的定制外壳中。在一些实施例中,图像由网络相机捕获。在一些实施例中,图像是从第二用户设备导入的。在一些实施例中,主体是人。在一些实施例中,主体是罪犯。在一些实施例中,人脸图像数据包括主体的三维人脸图像。

[0022] 在一些实施例中,人脸图像处理模块可操作以:(i)通过网络爬虫下载个体人脸图像和与其相关联的个人信息;以及(ii)将下载的人脸图像和相关联的个人信息存储在数据库中。

[0023] 在一些实施例中,参考人脸识别数据包括通过网络爬虫下载的人脸图像。参考人脸识别数据可以包括从互联网、职业网站、执法部门网站或机动车辆部门获得的人脸图像。在一些实施例中,数据库包括与存储在数据库中的人脸图像相关联的多个犯罪记录。

[0024] 在一些实施例中,人脸识别数据包括主体的捕获的人脸图像的向量表示。类似地,参考人脸识别数据也可以包括数据库中存储的人脸图像的向量表示。在一些实施例中,向量表示包括512点向量或1024×1024人脸数据矩阵。

[0025] 在如上所描述的系统中,人脸识别模块可操作以将主体的捕获的人脸图像的向量表示与数据库中存储的人脸图像相关联的向量表示进行比较。比较人脸识别数据可以由机器学习模块来执行。机器学习模块包括深度卷积神经网络(CNN)。在一些实施例中,候选的识别通过k-最近邻算法(k-NN)来执行。

[0026] 在一些实施例中,该方法还可以包括检测活体姿势。活体姿势基于第二图像相对于第一图像的偏航角和第二图像相对于第一图像的俯仰角中的至少一个,其中偏航角对应于以垂直轴为中心的转变,并且其中俯仰角对应于以水平轴为中心的转变。

[0027] 在一些实施例中,个人信息是基于所识别的候选的预定隐私设置而从数据库中检索的。在一些实施例中,该方法还包括显示所识别的候选的一个或多个人脸图像以及与其

相关联的个人信息。在一些实施例中，该方法还可以包括如果所识别的候选对公众构成高风险或者是罪犯，则向用户设备发送通知。在一些实施例中，个人信息可以包括所识别的候选的姓名。在一些实施例中，个人信息可以包括到与所识别的匹配相关联的在线档案的链接。在一些实施例中，向用户设备发送的个人信息是从包含个人信息的网页当中具有最高页面评级值的网页获得的。

[0028] 在一些实施例中，人脸识别模块可操作以：(i)基于所识别的候选的个人信息，确定对主体访问场所或账户的许可；(ii)如果所识别的候选是授权用户，则准许该主体的访问，或者如果所识别的候选不是授权用户或者不能识别与捕获的人脸图像匹配的候选，则拒绝该主体的访问；以及(iii)发送指示准许或拒绝访问场所或账户的消息。在一些实施例中，账户可以与银行、金融机构或信贷公司相关联。

[0029] 在一些实施例中，人脸识别模块可操作以向多个用户提供对数据库的访问。多个用户可以位于相同的地理区域或者与相同的商业类型相关联。

[0030] 在一些实施例中，人脸图像数据包括第二主体的第二捕获的人脸图像。在一些实施例中，该方法包括识别在单个图像中被捕获到了人脸图像的两个或更多个主体之间的关系。

[0031] 在另一方面，本公开提供了一种验证用户的身份的系统。该系统包括：(i)人脸图像处理模块，其可操作以将主体的捕获的人脸图像转换成人脸识别数据；以及(ii)人脸识别模块，其可操作以：(a)提供人脸图像数据和用户的个人识别号，该人脸图像数据包括捕获的人脸图像；(b)将人脸图像数据转换成人脸识别数据；(c)将人脸识别数据和个人识别号和与多个存储的个体人脸图像相关联的参考人脸识别数据和参考个人识别号进行比较，以识别与捕获的人脸图像和个人识别号匹配的至少一个可能的候选；以及(d)在识别出候选时，向用户设备发送确认以指示该用户是授权用户。

[0032] 前述概述不旨在限定本公开的每个方面，并且在其他部分中描述了附加方面，诸如以下详细描述。整个文档旨在作为统一的公开内容进行关联，并且应该理解，本文所描述的特征的所有组合都是预期的，即使这些特征的组合没有一起出现在本文档的相同句子、段落或部分中。本发明的其他特征和优点根据下面的详细描述将变得明显。然而，应该理解的是，详细描述和具体示例虽然指示了本公开的具体实施例，但仅仅是以说明的方式给出的，因为根据该详细描述，在本公开的精神和范围内的各种改变和修改对于本领域技术人员来说将变得显而易见。

附图说明

[0033] 附图中的组件不一定是按比例绘制的，而是重在强调说明本发明的原理。在附图中，在不同的视图中，相同的附图标记表示相应的部分。

[0034] 图1示出了基于人脸识别来提供关于人的信息的示例方法。

[0035] 图2示出了基于输入图像来提供关于人的信息的示例过程。

[0036] 图3示出了使用网络爬虫从互联网检索人的人脸图像和其他相关信息的示例过程。

[0037] 图4示出了所公开的方法的示例服务器端实施方式。

[0038] 图5示出了移动设备上的搜索应用的示例界面，该示例界面显示数据库中与捕获

的人脸图像匹配的候选图像。

[0039] 图6示出了示出通过搜索识别的候选人脸图像的示例界面。

[0040] 图7示出了移动设备上的搜索应用的示例界面，该示例界面显示关于人的信息。

[0041] 图8示出了为执行人脸识别而实施的示例神经网络。

[0042] 图9示出了用于实施所公开的方法的示例系统。

[0043] 图10示出了用于实施所公开的方法的示例计算系统。

具体实施方式

[0044] 本公开提供了基于人脸识别来提供关于人的信息的方法以及其各种应用，包括基于人脸的登记(check-in)、基于人脸的个人识别、基于人脸的身份验证、基于人脸的背景调查、人脸数据协作网络、相关人脸搜索和基于个人人脸的识别。所公开的方法能够以实时的方式提供关于人的准确的信息。

[0045] A.基于人脸识别来获得个人信息的方法和系统

[0046] 在一个方面，本公开提出了一种提供关于主体(例如，人、陌生人、新认识的人、记忆有缺陷的人、罪犯、醉酒的人、吸毒者、无家可归的人)的信息的方法。如图1和图2所示，该方法包括(i)接收从用户设备发送的人脸图像数据。人脸图像数据至少包括主体的捕获的人脸图像；(ii)将人脸图像数据转换成人脸识别数据；(iii)由服务器设备将人脸识别数据和与多个存储的个体人脸图像相关联的参考人脸识别数据进行比较，以识别与捕获的人脸图像匹配的至少一个可能的候选；(iv)在识别出与捕获的人脸图像匹配的候选时，从数据库中检索与该候选相关联的个人信息；以及(v)向用户设备发送个人信息，并使用户设备显示该个人信息。

[0047] 还提供了一种实施以上所描述的提供关于主体的个人信息的方法的系统。再次参考图1，在101，系统可以通过网络相机或用户设备(例如，移动设备)的机载相机来捕获主体的人脸图像。在102，系统可以可选地在用户设备上预处理捕获的人脸图像。在103，系统可以向服务器设备发送人脸图像(例如，经预处理的)，用于附加处理和执行人脸识别。在104，系统可以基于神经网络算法(例如，深度卷积神经网络(CNN))来执行人脸识别。在105，系统可以将人脸图像与存储在数据库(在106提供)中的人脸图像进行匹配。可以基于最近邻搜索，例如k最近邻(k-NN)算法来执行图像匹配，以识别一个或多个候选图像。基于一个或多个预定标准，候选图像与捕获的人脸图像匹配。在107，系统可以检索一个或多个候选图像的个人信息。个人信息可以包括主体在社交网络网站、职业网络网站或雇主网站上的在线档案。在108，系统发送检索到的个人信息并使用户设备显示检索到的个人信息。替代地和/或附加地，该系统还可以基于例如主体对公众构成的潜在风险，使用户设备显示警报消息。

[0048] 所公开的系统可以经由桌面操作或经由智能手机远程地操作，使进行犯罪调查、背景调查等的用户能够经由一个或多个人脸数据库以及到社交媒体、传统媒体、职业网站等的补充链接，即时建立身份并获得关于个体的履历数据。在经由人脸数据库即时匹配人脸的过程中，该系统还找到并发布被搜索个体的姓名。该系统还即时地发布到个体的可公开访问的社交媒体、传统媒体等的实时链接。

[0049] 除非特别说明，否则从上述讨论中显而易见的是，在整个描述中，利用诸如“处理”或“计算”或“运算”或“确定”或“识别”或“显示”或“提供”等术语的讨论指的是计算机系统

或类似的电子计算设备的动作和过程，其操纵和转换在计算机系统存储器或寄存器或其他这样的信息存储、传输或显示设备中表示为物理(电子)量的数据。

[0050] 该系统可以在嵌入客户端系统920的用户设备上发送和显示关于人的信息(也参见图9)。用户设备可以是电子设备，包括硬件、软件或嵌入式逻辑组件或两个或更多个这样的组件的组合，并且能够施行由客户端系统实施或支持的适当功能。作为示例而非限制，客户端系统可以包括计算机系统，诸如台式计算机、笔记本或膝上型计算机、上网本、平板计算机、手持电子设备、蜂窝电话、智能手机、其他合适的电子设备或其任何合适的组合。客户端系统可以使得客户端系统处的网络用户能够访问网络。客户端系统可以使其得其用户能够与在其他客户端系统处的其他用户通信。

[0051] 图3示出了提供关于人的信息的服务器端实施方式的示例。例如，该系统可以包括防火墙，以保护服务器设备与客户端设备之间通过互联网通信的安全性。对于网络爬虫功能，该系统可以包括一个或多个搜索引擎工作器，其扫描各种网站并识别包含人脸图像的图像和其他信息。该系统可以将所识别的图像和其他信息存储在文档存储集群中。网络爬虫任务被组织在爬虫任务队列中。然后，通过网络爬虫检索到的信息可以被索引并存储在数据库中，以支持响应用户输入的后续搜索。对于网络搜索功能，该系统可以包括网络服务器，该网络服务器通过与用于SQL用户数据的数据库、用于SQL搜索数据的数据库、NNDB索引集群和GPU集群进行交互，来处理从用户设备接收的请求并向用户设备发送结果。

[0052] B.图像捕获和处理

[0053] 该系统可以包括用于捕获人脸图像的照相机(静态的、视频的或两者)。相机的非限制性示例包括安装在用户设备上的相机、网络或联网相机、USB相机、模拟或数字相机、互联网协议(IP)相机、模拟或数字摄像机、闭路相机(CCTV)等。在一些实施例中，系统可以采用网络相机服务器、另一种类型的网络相机。网络相机从多个包括镜头和图像传感器的相机接收图像信号，并且每个相机在外部的某个地方分开，并且该网络相机将该图像信号转换成一个统一的图像信号来通过网络发送该图像信号，并且对由该多个相机拍摄的图像信号执行网络服务器功能。上述网络相机或网络相机服务器具有其自己的唯一IP，并且具有在JPEG或M-JPEG的压缩方法、小波压缩方法或MPEG压缩方法中使用标准网络浏览器以每秒最少10帧到最多30帧的高速通过网络发送所获得的图像信号的功能，而无需额外的PC。该系统还可以包括适于连接到互联网协议网络的监控相机。在一些实施例中，人脸识别技术可以被并入联网的监控系统。

[0054] 在一些实施例中，人脸图像由有相机功能的用户设备捕获。在一些实施例中，图像由网络相机捕获。在一些实施例中，图像从第二用户设备导入。在一些实施例中，相机可以被封装在定制外壳中。定制外壳旨在完全封装和保护用户设备，诸如iPhone和Android手机，并带有一个针对手机相机的开口。外壳被设计成安装在大厅、走廊或门口的墙壁上的独立底座上。外壳由金属或塑料制成。

[0055] 图5示出了用户设备(例如，移动设备)上的用于捕获人的人脸图像的搜索应用的示例界面。界面500包括一个或多个图标，以接收用户输入来调用用户设备的某些功能。例如，该系统可以调用用户设备的相机功能，并允许用户拍摄照片或视频，或者上传在别处获得的照片或视频。用户可以选择使用移动设备的机载相机来使用前置相机504或后置相机505捕获人脸图像。该界面还可以包括标记区域501，以帮助用户在界面500的指定区域中定

位主体的人脸，从而确保捕获的人脸图像的良好质量。在一些实施例中，该系统可以允许用户上传照片或视频(502)。可以从用户设备的照片/视频图库或库中检索照片或视频。

[0056] 在一些实施例中，该系统可以通过用户设备或相机预处理该主体的图像。本文使用的术语“图像”或“多个图像”是指静态或动态图像、视频剪辑、视频流等的单帧或多帧。预处理可以包括由用户设备检测主体的图像中的人脸图像。预处理还可以包括裁剪、调整尺寸、灰度转换、中值滤波、直方图均衡化或尺寸归一化图像处理。

[0057] 在一些实施例中，该系统可以根据阈值(例如，以千字节、兆字节或吉字节为单位的最大尺寸，以每英寸点数(DPI)或每英寸像素(PPI)为单位的最大或最小分辨率)来调整照片或视频的尺寸。在一些实施例中，系统可以基于网络和链接的传输速率来调整照片或视频的尺寸。

[0058] 在一些实施例中，系统可以通过相机、用户设备或服务器设备对捕获的图像或视频执行附加处理步骤，以将数据文件数字化，并且可选地压缩成方便的压缩文件格式，并且发送到网络协议栈，用于随后在局域网或广域网上传送。典型的压缩方案包括MPEG、JPEG、H.261或H.263、小波或各种专有压缩方案。典型的网络拓扑是流行的以太网标准IEEE 802.3，并且可以以10Mb/s到100Mb/s的速度操作。网络协议通常是TCP/IP、UDP/IP，并且如系统要求所规定的可以是单播或多播。

[0059] C.人脸图像数据库

[0060] 该系统可以包括一个或多个数据库或数据库接口，以促进与数据库的通信和对数据库的搜索。例如，该系统可以包括包含一个或多个人的图像或图像数据的图像数据库。该系统还可以包括数据库接口，其可以作为身份匹配过程的一部分用于访问第三方(例如，执法部门、DMV)的图像数据。该系统的一部分还是存储一个或多个人的档案信息的个人数据数据库。档案信息可以包括以下至少一者：姓名、性别、出生日期或年龄、国籍、通信语言、城市地址、电话号码、电子邮件地址、即时消息标识符和财务信息。档案信息还可以包括到网站上包含与感兴趣的人相关的信息的网页的链接。例如，网站可以是社交网络网站、职业网络网站、个人网站或雇主网站。该系统可以包括隐私设置模块，其操作以建立个体访问数据库的隐私设置。

[0061] 图像数据库或个人数据数据库可以是关系数据库、柱状数据库、相关性数据库或其他合适的数据库。数据库可以是本地的，也可以是分布式的。例如，在一些实施例中，数据库可以由云服务提供商(例如，亚马逊AWS、谷歌云、微软Azure)托管。尽管本公开描述或示出了特定类型的数据库，但是本公开考虑了任何合适类型的数据库。

[0062] 图6示出了系统使用例如网络爬虫从互联网获取人的人脸图像和其他相关信息的示例过程。关于识别的个体的许多信息可以通过公开手段和扫描社交网站(例如，脸书和谷歌+)或职业网站(例如，LinkedIn)获得。与个人账户相关联的在线照片可能有助于创建人脸识别数据点的附加记录。在一些实施例中，该系统可以(i)通过网络爬虫下载个体人脸图像以及与其相关联的个人信息；以及(2)将下载的人脸图像和相关联的个人信息存储在数据库中。在一些实施例中，参考人脸识别数据包括通过网络爬虫下载的人脸图像。参考人脸识别数据可以包括从互联网、职业网站、执法部门网站或机动车辆部门获得的人脸图像。在一些实施例中，数据库包括与存储在数据库中的人脸图像相关联的多个犯罪记录。

[0063] 在下载和存储人脸图像之后，系统可以基于一个或多个标准对图像进行分类。因

此，数据库还可以存储图像信息，包括已经分类的图像、已经分类的图像的网络位置和包含分类的图像的文档中的至少一个。例如，图像信息包括指向未分类图像或已经分类图像的数据库条目的网络URL或指针，以及与图像相关的文档的位置。也可以搜索数据库来定位与输入查询匹配的图像。该查询可以包括指定搜索主题或类别的图像或文本，并且还可以包括语义查询。图像和文本数据的组合也可以用作查询。

[0064] 该数据库可以根本不包含任何图像，不过可以包含数字图像分类信息以及数字图像和包含该数字图像的文档的网络地址。通常，数据库包含指向外部存储的、预先分类的数字图像和相关文档的指针。数据库本身可以是本地的或远程的，并且它可以分布在多个位置。

[0065] 在一些实施例中，系统可以将图像数据转换成特性向量或多维矩阵。特性向量或多维矩阵包括人脸结构的重要特征。在一些实施例中，数据库可以仅存储经转换的人脸图像数据(或向量化的人脸图像数据)，使得在没有反转经转换的图像的操作的情况下无法访问原始人脸图像。在一些实施例中，该系统可以对原始图像数据或经转换的图像数据应用加密。

[0066] 存储在数据库中或被数据库引用的图像可以至少部分地通过互联网获得，诸如通过自动网络爬虫的活动。在一个实施例中，图像是医学图像，并且可以搜索数据库以获取满足由搜索查询建立的阈值的至少一个图像。该数据库可以位于远处，并且可以经由服务器通过互联网来访问。在一个实施例中，对数据库服务器的图像查询可以结合由服务器执行的基于文本的搜索算法进行，以从数据库或通过数据库检索多媒体对象。

[0067] 在一些实施例中，数据库可以是已知个体的数据库(例如，执法部门、监控和最近的驾照)。例如，数据库可以是图像数据库、已知罪犯数据库、执法部门数据库或图像托管网站的数据库。可以提供犯罪或欺诈模块来处理当该系统确定被识别的人是或可能是罪犯或实施欺诈时的情况。同样，如果正在进行犯罪，该模块可以被激活。在激活时，可以向用户提供优先级通知，并且可以可选地呼叫执法部门来调查和保护捕获了罪犯图像的用户。罪犯信息也可以用于加载关于潜在危险个体的重要信息，并且可以与数据库信息和人脸识别结合使用。

[0068] D.人脸检测和识别

[0069] 该系统可以包括人脸检测模块。人脸检测可以发生在相机、用户设备或服务器设备(例如，远程服务器设备)处。人脸检测模块可以包括能够从各种角度检测人脸的人脸检测算法，尽管人脸识别算法在正面照片中最准确。在一些实施例中，在具有较低质量或者处于不同于直对人脸的角度的图像之前，人脸检测模块首先处理具有较高质量的人脸图像。该处理可以发生在相机、移动设备或可以访问图像数据或人脸识别数据的大型数据库的远程服务器处。

[0070] 人脸检测过程可以由用户设备(例如，移动设备、台式计算机)上的定制搜索应用来执行。符合质量标准的人脸图像将被选择用于附加处理，例如裁剪、调整尺寸或压缩。该系统然后向服务器设备发送处理后的人脸图像数据。由于用户设备处理人脸检测和捕获的人脸图像的预处理，减少了服务器设备执行人脸识别所需的时间。此外，减少了对网络带宽的要求，并增加了网络上的传输速度。

[0071] 在一些实施例中，人脸检测可以采用诸如高阶梯度算法(HOG)的算法。HOG适用于

可以在常规CPU上运行的较小照片。替代地，系统可以采用可以用于更大照片的更新的CNN算法。

[0072] 类似地，人脸识别过程可以发生在移动设备或远程服务器上。然而，服务器设备更适合于该任务，由于它通常配备有更快的多个处理器，并且可以访问陌生人的识别所需的大型数据库。

[0073] 为了执行人脸识别过程，该系统可以在相机(例如，监控相机)、用户设备或服务器设备上实施。该系统可以包括人脸图像处理器和体现在合适介质中的人脸识别算法。人脸识别算法可由人脸处理器利用数字格式的图像数据来执行以检测人脸。人脸识别算法产生人脸图像数据。人脸处理器与人脸特征(signature)数据库通信，以获得参考数据。人脸特征算法将人脸图像数据与参考数据进行比较，以识别相关性。该系统可以包括产生压缩图像数据的压缩算法和网络栈，该网络栈被配置成向网络发送每个检测到的人脸的人脸图像数据，并且向托管图像数据库或个人信息数据库的远程服务器发送压缩图像数据。

[0074] 在一些实施例中，人脸识别数据包括主体的捕获的人脸图像的向量表示。类似地，参考人脸识别数据也可以包括数据库中存储的人脸图像的向量表示。在一些实施例中，向量表示包括512点向量或1024×1024人脸数据矩阵。在一些实施例中，该系统可以使用人脸嵌入过程(例如，使用神经网络将人脸图像转换成向量)，该过程利用基于triplet-loss的方法或不同于标准Softmax函数的不同函数。例如，附加角度裕度损失可以用于以少一个数量级的训练数据量而获得高得多的精度。向量搜索可能要求所有参考向量都存储在存储器内(RAM)数据库中。通过像优化产品量化(OPQ)、分层可导航小世界(HNSW)等的压缩算法，该系统可以在100毫秒内搜索数十亿个人脸向量。

[0075] 在一些实施例中，比较步骤还包括将主体的捕获的人脸图像的向量表示和与数据库中存储的人脸图像相关联的向量表示进行比较。比较人脸识别数据可以由机器学习模块来执行。机器学习模块包括深度卷积神经网络(CNN)。在一些实施例中，候选的识别通过k-最近邻算法(k-NN)来执行。

[0076] 深度卷积神经网络(CNN)是用于多维信号处理的主要类型的神经网络。术语深度通常指的是具有从“几个”到几十个或更多卷积层的网络，深度学习指的是使用表示感兴趣的特定问题域的数据来训练这些系统以自动学习它们的函数参数的方法。CNN目前被用于广泛的应用领域，所有这些领域共享共同的目标，即能够从(通常是大规模的)数据库中自动学习特征，并归纳它们对学习阶段期间没有遇到的情况的响应。最终，学习到的特征可以用于诸如对CNN预期要处理的信号类型进行分类的任务。

[0077] k-NN是一种用于分类和回归的非参数方法。在这两种情况下，输入由特征空间中k个最接近的训练示例组成。输出取决于k-NN是用于分类还是回归:(1)在k-NN分类中，输出是一个类成员。通过其邻里对象的多次投票对对象进行分类，将该对象分配到其k个最近邻之中最常见的类(k是正整数，通常很小)。如果k＝1，那么该对象被简单地分配到单个最近邻的类。(2)在k-NN回归中，输出是对象的属性值。该值是k个最近邻的平均值。k-NN是一种基于实例的学习，或称惰性学习，其中函数只是局部近似，并且所有计算都推迟直到分类时进行。k-NN算法是所有机器学习算法中最简单的。

[0078] 在一些实施例中，该方法还可以包括检测活体姿势。活体姿势基于第二图像相对于第一图像的偏航角和第二图像相对于第一图像的俯仰角中的至少一个，其中偏航角对应

于以垂直轴为中心的转变，并且其中俯仰角对应于以水平轴为中心的转变。

[0079] 图6示出了移动设备上的搜索应用的示例界面，该示例界面显示数据库中与捕获的人脸图像匹配的候选图像。在执行人脸识别过程之后，该系统可以识别与捕获的人脸图像匹配的一个或多个候选图像。该系统可以基于评分算法对候选图像进行评级。例如，匹配度可以被测量为“距离”值(例如，欧几里德距离)。较小的距离值指示给定候选图像与捕获的人脸图像之间的匹配度较高。该系统可以在用户设备上显示候选图像。附加地，该系统显示关于候选图像的相关信息，例如，姓名、雇主、到可以找到该候选图像的网页的链接等。用户可以选择被认为是正确匹配的候选图像。在接收到选择特定候选图像的用户响应时，该系统将显示与选定的候选图像相关的附加信息。

[0080] 如图7所示，关于候选图像的附加信息可以包括：姓名、标题、到在线档案的链接。在线档案可以是社交网络档案(例如，脸书、谷歌+)、职业网络档案(例如，LinkedIn)或雇主网站上的员工档案。附加地，该系统还可以显示距离值以指示匹配度。

[0081] E.基于神经网络的人脸识别

[0082] 在一些实施例中，该系统可以采用机器学习模块来进行人脸识别。机器学习模块可以采用以下算法中的任何一种，包括但不限于：深度卷积神经网络(CNN)、支持向量机(SVM)、神经网络、逻辑回归、朴素贝叶斯、基于记忆的学习、随机森林、袋装树、决策树、提升树、提升树桩等。机器学习模块的一些实施例使用无监督的机器学习，其提供没有标记响应的训练数据。无监督机器学习技术的示例使用聚类，例如k-均值聚类、层次聚类等等。

[0083] 神经网络技术，也称为“人工神经网络(ANN)”，是在用于模式识别的机器学习模块中使用的最发达的工具之一。神经网络是由被称为神经元的处理元素构成的。神经元相互连接并布置成多层。每个神经元可以有多个输入，但通常只有一个输出，继而该输出通常连接到下一层的许多或所有其他神经元。神经网络通过从数据和期望的输出中提取关系信息来学习。机器学习模块中的神经网络最初被训练或馈送大量数据。在一些实施例中，机器学习模块可以采用多个神经网络，这些神经网络可以以串联、并联或嵌套的方式任一者组织。例如，初级神经网络可以识别底盘组件的异常，并试图识别可能的来源。神经网络可以以树形模式或分层结构布置，每个神经网络被训练来执行特定的模式识别任务。这样的神经网络组可以耦合到其他神经网络组，以处理更复杂的任务。

[0084] 图8示出了用于人脸识别的神经网络的示例。最初，该系统可以接收和预处理例如来自用户设备的人脸图像数据，并用实施神经网络算法的机器学习模块来分析经预处理的数据。针对人脸特征的人脸图像数据被馈送到输入层中的节点N1到Ni。

[0085] 每个输入节点通常通过例如包含乘法系数(也称为权重)的数学函数连接到第二层(例如，隐藏层)中的每个节点，即H1、H2、H3、H4和Hi。在每个隐藏层节点处，可以通过对来自每个输入层节点的值(这些值已经由包含权重的函数进行了运算)进行求和来获得节点值。类似地，隐藏层节点继而依次连接到第二隐藏层中的节点，即L1、L2、L3、L4、…、和Li。第二隐藏层的节点的节点值如上所描述类似地生成。第二隐藏层的节点连接到输出层节点。在这个示例中，只有单个节点0，其表示通知驾驶员和/或远程服务中心关于不平衡轮胎的决策。来自输出层节点的输出值可以具有各种形式。例如，可以分配输出节点值1来指示应该通知驾驶员/服务中心，并且可以分配值0来指示不应该通知驾驶员/服务中心。

[0086] 一般而言，在为捕获的人脸图像识别匹配候选图像时，该系统可以：(1)首先从用

户设备获取人脸图像数据；(2)预处理获取的人脸图像数据，例如数字化该人脸图像数据和/或向量化该人脸图像数据；(3)将经预处理的人脸图像数据馈送到实施机器学习算法(例如，人脸识别算法)的人脸识别模块；(4)使用机器学习算法处理人脸图像数据，以检测人脸的特性特征；(5)识别一个或多个匹配的候选图像以及与该一个或多个候选图像相关联的信息；以及(6)可选地警告用户是感兴趣的人。感兴趣的人可以包括宣布失踪的人、被指控犯罪的人、有犯罪记录的人、性犯罪者、遭受记忆丧失的人以及可能以其他方式对公众构成高风险的人。

[0087] F.信息输出

[0088] 再次参考图6和图7，在执行以上所描述的人脸识别过程时，该系统可以在图像数据库中识别具有不同匹配度(例如，通过距离值测量)的一个或多个匹配候选图像。该系统还可以检索存储在个人数据数据库中的档案信息。该系统可以从个人数据数据库中检索档案信息包括但不限于：姓名、性别、出生日期或年龄、出生地、国籍、通信语言、城市地址、电话号码、电子邮件地址、即时消息标识符、财务信息、婚姻状况、爱好、喜爱的运动队、教育、教育程度、大学以及其他人发布的信息。档案信息还可以包括到网站上包含与感兴趣的人相关的信息的网页的链接。例如，网站可以是社交网络网站、职业网络网站、个人网站或雇主网站。该系统可以包括隐私设置模块，其操作以建立个体访问数据库的隐私设置。

[0089] 在一些实施例中，个人信息是基于所识别的候选的预定隐私设置而从数据库中检索的。在一些实施例中，该方法还包括显示所识别的候选的一个或多个人脸图像以及与其相关联的个人信息。在一些实施例中，该方法还可以包括如果所识别的候选对公众构成高风险或者是罪犯，则向用户设备发送通知。在一些实施例中，个人信息可以包括所识别的候选的姓名。在一些实施例中，个人信息可以包括到与所识别的匹配相关联的在线档案的链接。在一些实施例中，向用户设备发送的个人信息是从包含个人信息的网页中具有最高页面评级值的网页获得的。

[0090] 该系统提供的信息可用于确定个体的身份。例如，该信息可以用于识别感兴趣的人。感兴趣的人可以包括宣布失踪的人、被指控犯罪的人、有犯罪记录的人、性犯罪者、遭受记忆丧失的人以及可能以其他方式对公众构成高风险的人。在一个示例中，社会工作者可以使用该信息来识别无家可归的人或需要帮助的人。同样，执法部门可以使用人脸识别系统来识别关于人的信息。通过准确地识别人，并且动态地实时获得关于这个人的信息，可以更准确地做出决策。社会福利可以准确地分配，从而减少欺诈。执法部门可以使用关于人的信息来了解他们是否具有可能阻止他们做出反应或导致他们做出不适当行为的医疗状况或精神问题或障碍。对于没有被捕记录和健康状况的人以及人脸检测有袭警史的人，警方可以做出不同的反应。通过人脸扫描显示，有DUI被捕史的人可能会受到与有糖尿病低血糖症状史的人不同的对待。简单的人脸扫描可以提供人的身份，即使这个人躲过了警察的追捕。

[0091] G.其他应用

[0092] (i)基于人脸识别的身份验证

[0093] 在另一方面，本公开还提供了一种基于人脸识别来验证个人身份的方法。所公开的系统使得个体能够被即时识别并被批准/不被批准进入场所(例如，建筑物、银行、设施、实验室、安全场所)。该系统完全基于人脸，并且可以无缝实施。其不需要下载应用或与触摸

屏互动。个体简单地看着相机或移动设备(例如,移动电话、iPad),然后被批准或不被批准。该系统还根据人脸、姓名和日期/时间自动记录进出大楼的个体。

[0094] 该方法可用于准许或拒绝人访问设施、场所或设备。如上所描述,如果需要,该系统可以包括捕获人的图像的部件,然后利用相关联的电路和软件处理该图像,然后将该图像与存储的图像进行比较。在访问受保护的环境中,所获取的个体图像与预先存储的图像之间的肯定匹配允许访问该设施。

[0095] 在一些实施例中,该方法还包括:(i)基于所识别的候选的个人信息,确定对主体访问场所或账户的许可;(ii)如果所识别的候选是授权用户,则准许该主体的访问,或者如果所识别的候选不是授权用户或者不能识别与捕获的人脸图像匹配的候选,则拒绝该主体的访问;以及(iii)发送指示准许或拒绝访问场所或账户的消息。在一些实施例中,账户与银行、金融机构或信贷公司相关联。

[0096] 在另一方面,本公开提供了一种验证用户身份的方法。例如,个体用户可以创建他们自己的个人"人脸文件",其包括他们的头像和安全的个人识别号(PIN)。该个体可以使用该文件/账户作为其日常交易的一种高度安全、防盗的人脸/生物识别形式。

[0097] 在一些实施例中,该方法包括(a)提供该用户的包括捕获的人脸图像的人脸图像数据和个人识别号;(b)将人脸图像数据转换成人脸识别数据;(c)将该人脸识别数据和该个人识别号和与多个存储的个体人脸图像相关联的参考人脸识别数据和参考个人识别号进行比较,以识别与捕获的该人脸图像和该个人识别号匹配的至少一个可能的候选;以及(d)在识别出候选时,向用户设备发送确认以指示该用户是授权用户。

[0098] (ii)人脸数据协作网络和相关人脸搜索

[0099] 在又一方面,该方法还包括向多个用户提供对数据库的访问。多个用户可以位于相同的地理区域或者与相同的商业类型相关联。该系统使能了相同地理区域内或相同或相关部门(例如,执法部门、零售、房地产)内的客户群组的联网,以便为了所有网络参与者的利益,经由安全的共享数据系统来共享高风险个体的头像。

[0100] 该系统使能了人脸图像作为银行、金融机构、信贷公司等的生物特征客户识别和认证的使用。该过程还包括对照系统的人脸数据库来检查每个人脸,以验证个体的身份和履历数据。

[0101] 在另一方面,该系统匹配并识别照片中的次要人脸图像,即使被搜索的人脸在背景中而不是照片的主要主体。相关人脸搜索还通过单次按钮按下使能了照片内的其他次要人脸图像的即时搜索。在一些实施例中,人脸图像数据包括第二主体的第二捕获的人脸图像。在一些实施例中,该方法包括识别在单个图像中被捕获到了人脸图像的两个或更多个主体之间的关系。

[0102] H.基于网络的通信和计算架构

[0103] 图9示出了用于实施所公开的方法的系统900的示例。该系统可以包括底盘模块120、一个或多个传感器131、132、133、134和135、一个或多个基于互联网的服务器系统910,其能够经由通信网络930与底盘模块120和一个或多个客户端系统920通信。尽管图9示出了服务器系统910、客户端系统920和网络930的特定布置,但是本公开考虑了服务器系统、客户端系统和网络的任何合适的布置。作为示例而非限制,一个或多个设备服务器和一个或多个客户端系统920可以绕过网络930直接彼此连接。作为另一示例,两个或更多个客户端

系统920和一个或多个服务器系统910可以整体或部分地在物理上或逻辑上彼此共处一地。此外，尽管图9示出了特定数量的客户端系统920和服务器系统910以及网络940，但是本公开考虑了任何合适数量的客户端系统920和服务器系统910以及网络930。

[0104] 服务器系统910可以耦合到任何合适的网络930。作为示例而非限制，网络930的一个或多个部分可以包括自组织网络、内联网、外联网、虚拟专用网(VPN)、局域网(LAN)、无线LAN(WLAN)、广域网(WAN)、无线WAN(WWAN)、城域网(MAN)、互联网的部分、公共交换电话网(PSTN)的部分、蜂窝电话网或者这些中的两个或更多个的组合。网络930可以包括一个或多个网络930。

[0105] 链路940可以将客户端系统920和服务器系统910连接到通信网络930或者彼此连接。本公开考虑了任何合适的链路940。在特定实施例中，一个或多个链路940包括一个或多个有线链路(诸如，例如数字订户线(DSL)或有线数据服务接口规范(DOCSIS))、无线链路(诸如，例如Wi-Fi或微波接入全球互通(WiMAX))或光学链路(诸如，例如同步光学网络(SONET)或同步数字体系(SDH))。在特定实施例中，一个或多个链路940各自包括自组织网络、内联网、外联网、VPN、LAN、WLAN、WAN、WWAN、MAN、互联网的部分、PSTN的部分、基于蜂窝技术的网络、基于卫星通信技术的网络、另一链路940或者两个或更多个这样的链路940的组合。在整个网络环境930中，链路940不需要必须是相同的。一个或多个第一链路940可以在一个或多个方面不同于一个或多个第二链路940。

[0106] 在一些实施例中，服务器系统910可以生成、存储、接收和发送数据，诸如，例如用户档案数据、概念档案数据、社交网络数据或其他合适的数据。服务器系统910可以由系统900的其他组件直接地或经由网络930访问。在特定实施例中，服务器系统910可以包括一个或多个服务器912。每个服务器912可以是单一服务器或跨越多个计算机或多个数据中心的分布式服务器。服务器912可以是各种类型的，例如但不限于，网络服务器、新闻服务器、邮件服务器、消息服务器、广告服务器、文件服务器、应用服务器、交换服务器、数据库服务器、代理服务器、适于执行本文所描述的功能或过程的另一服务器，或者其任意组合。在特定实施例中，每个服务器912可以包括硬件、软件或嵌入式逻辑组件或者两个或更多个这样的组件的组合，用于施行由服务器912实施或支持的适当功能。在特定实施例中，服务器系统910可以包括一个或多个数据存储914。数据存储914可用于存储各种类型的信息。在特定实施例中，存储在数据存储914中的信息可以根据特定的数据结构来组织。在特定实施例中，每个数据存储914可以是关系型、柱状、相关性或其他合适的数据库。尽管本公开描述或示出了特定类型的数据库，但是本公开考虑了任何合适类型的数据库。特定实施例可以提供使得服务器系统910和客户端系统920能够管理、检索、修改、添加或删除存储在数据存储914中的信息的接口。

[0107] 在一些实施例中，客户端系统920可以是包括硬件、软件或嵌入式逻辑组件或两个或更多个这样的组件的组合并且能够施行由客户端系统920实施或支持的适当功能的电子设备。作为示例而非限制，客户端系统920可以包括计算机系统，例如台式计算机、笔记本或膝上型计算机、上网本、平板计算机、手持电子设备、蜂窝电话、智能手机、其他合适的电子设备或其任何合适的组合。本公开考虑了任何合适的客户端系统920。客户端系统920可以使得客户端系统920处的网络用户能够访问网络930。客户端系统920可以使得其用户能够与其他客户端系统920处的其他用户通信。

[0108] 在一些实施例中，客户端系统920可以包括网络浏览器，例如微软浏览器(INTERNET EXPLORER)、谷歌浏览器(CHROME)或火狐浏览器(MOZILLA FIREFOX)，并且可以具有一个或多个附加组件、插件或其他扩展，例如工具栏(TOOLBAR)或雅虎工具栏。客户端系统920处的用户可以输入统一资源定位符(URL)或其他地址，以将网络浏览器定向到特定的服务器(例如服务器912)，并且网络浏览器可以生成超文本传输协议(HTTP)请求并将HTTP请求通信传输给服务器。服务器可以接受HTTP请求，并响应于该HTTP请求向客户端系统920通信传输一个或多个超文本标记语言(HTML)文件。客户端系统920可以基于来自服务器的HTML文件来呈现网页以呈现给用户。本公开考虑了任何合适的网页文件。作为示例而非限制，根据特定需要，网页可以根据HTML文件、可扩展超文本标记语言(XHTML)文件或可扩展标记语言(XML)文件来呈现。这样的页面还可以执行脚本，例如但不限于用JAVASCRIPT、JAVA、MICROSOFT SILVERLIGHT、标记语言和诸如AJAX(异步JAVASCRIPT和XML)等脚本的组合来编写的脚本。在本文中，在适当的情况下，对网页的引用涵盖一个或多个对应的网页文件(浏览器可以使用该网页文件来呈现网页)，反之亦然。

[0109] 图10是示出根据一些实施例的编程计算机系统的功能图。将显而易见的是，其他计算机系统架构和配置可以用于执行所描述的方法。包括如下所描述的各种子系统的计算机系统1000包括至少一个微处理器子系统(也称为处理器或中央处理单元(CPU)1006)。例如，处理器1006可以由单芯片处理器或多个处理器来实施。在一些实施例中，处理器1006是控制计算机系统1000的操作的通用数字处理器。在一些实施例中，处理器1006还包括一个或多个协处理器或专用处理器(例如，图形处理器、网络处理器等)。使用从存储器1007检索的指令，处理器1006控制在输入设备(例如，图像处理设备1003、I/O设备接口1002)上接收的输入数据的接收和操纵，以及在输出设备(例如，显示器1001)上的数据的输出和显示。

[0110] 处理器1006与存储器1007双向地耦合，存储器1007可以包括例如一个或多个随机存取存储器(RAM)和/或一个或多个只读存储器(ROM)。如本领域中众所周知的，存储器1007可以用作通用存储区域、临时(例如，暂存)存储器和/或高速缓冲存储器。除了用于在处理器1006上操作的过程的其他数据和指令之外，存储器1007还可以用于以数据对象和文本对象的形式存储输入数据和经处理的数据以及存储编程指令和数据。同样如本领域中众所周知的，存储器1007通常包括处理器1006用来执行其功能的基本操作指令、程序代码、数据和对象(例如，编程指令)。例如，取决于例如数据访问需要双向还是单向，存储器1007可以包括以下所描述的任何合适的计算机可读存储介质。例如，处理器1006还可以在存储器1007中包含的高速缓冲存储器中直接地且非常快速地检索频繁需要的数据并将其存储在该缓冲存储器中。

[0111] 可移动大容量存储设备1008为计算机系统1000提供附加的数据存储容量，并且可选地双向(读/写)或单向(只读)耦合到处理器1006。固定大容量存储器1009也可以例如提供附加的数据存储容量。例如，存储设备1008和/或1009可以包括计算机可读介质，例如磁带、闪存、PC卡、便携式大容量存储设备，例如硬盘驱动器(例如，磁性、光学或固态驱动器)、全息存储设备和其他存储设备。大容量存储器1008和/或1009通常存储处理器1006通常不活跃使用的附加编程指令、数据等。应当理解，如果需要，大容量存储器1008和1009内保存的信息可以以标准方式并入为存储器1007(例如，RAM)的一部分以作为虚拟存储器。

[0112] 除了向处理器1006提供对存储子系统的访问之外，总线1010还可以用于提供对其

他子系统和设备的访问。如图所示，这些可以包括显示器1001、网络接口1004、输入/输出(I/O)设备接口1002、图像处理设备1003以及其他子系统和设备。例如，图像处理设备1003可以包括相机、扫描仪等；I/O设备接口1002可以包括用于与触摸屏(例如，支持手势解释的电容式触敏屏)、麦克风、声卡、扬声器、键盘、定点设备(例如，鼠标、触笔、人类手指)、全球定位系统(GPS)接收器、差分全球定位系统(DGPS)接收器、加速度计交互的设备接口和/或用于与系统1000交互的任何其他合适的设备接口。多个I/O设备接口可以与计算机系统1000结合使用。I/O设备接口可以包括通用和定制的接口，其允许处理器1006发送和更通常地接收来自其他设备的数据，其他设备例如键盘、定点设备、麦克风、触摸屏、换能器读卡器、磁带读取器、语音或手写识别器、生物特征读取器、相机、便携式大容量存储设备和其他计算机。

[0113] 网络接口1004允许处理器1006使用如图所示的网络连接耦合到另一计算机、计算机网络或电信网络。例如，通过网络接口1004，处理器1006可以从另一网络接收信息(例如，数据对象或程序指令)，或者在执行方法/过程步骤的过程中向另一网络输出信息。通常表示为要在处理器上执行的指令序列的信息可以从另一网络接收并输出到另一网络。接口卡或类似设备以及由处理器1006实施(例如，在处理器1006上运行/执行)的适当软件可以用于将计算机系统1000连接到外部网络，并根据标准协议传输数据。例如，本文所公开的各种过程实施例可以在处理器1006上执行，或者可以结合共享部分处理的远程处理器跨网络执行，所述网络例如互联网、内联网或局域网。附加的大容量存储设备(未示出)也可以通过网络接口1004连接到处理器1006。

[0114] 此外，本文所公开的各种实施例还涉及具有计算机可读介质的计算机存储产品，该计算机可读介质包括用于执行各种计算机实施的操作的程序代码。计算机可读介质包括可以存储数据的任何数据存储设备，该数据随后可以被计算机系统读取。计算机可读介质的示例包括但不限于：磁性介质，例如磁盘和磁带；光学介质，例如CD-ROM盘；磁光介质，例如光盘；以及专门配置的硬件设备，例如专用集成电路(ASIC)、可编程逻辑器件(PLD)以及ROM和RAM设备。程序代码的示例包括例如由编译器产生的机器代码，或者包含可以使用解释器执行的更高级代码(例如脚本)的文件。

[0115] 如图10所示的计算机系统是适用于本文所公开的各种实施例的计算机系统的示例。适用于这种用途的其他计算机系统可以包括附加的或更少的子系统。在一些计算机系统中，子系统可以共享组件(例如，对于诸如智能手机、平板电脑等的基于触摸屏的设备，I/O设备接口1002和显示器1001共享触敏屏组件，其既检测用户输入又向用户显示输出)。此外，总线1010说明了服务于链接子系统的任何互连方案。也可以利用具有不同子系统配置的其他计算机架构。

[0116] 定义

[0117] 为了帮助理解根据本公开的组合物和方法的详细描述，提供了一些明确的定义，以有助于本公开的各个方面的明确公开。除非另有定义，否则本文所使用的所有技术和科学术语具有与本公开所属领域的普通技术人员之一通常理解的相同的含义。

[0118] 这里要注意的是，如在本说明书和所附权利要求中所使用的，单数形式“一”、“一个”和“该”包括复数指代，除非上下文另有明确规定。除非另有说明，否则术语“包括”、“包含”、“含有”或“具有”及其变体意在涵盖其后列出的项目及其等同物以及附加主题。

[0119] 重复使用短语“在一个实施例中”、“在各种实施例中”、“在一些实施例中”等。这样的短语不一定指相同实施例，但是它们可以指相同实施例，除非上下文另有规定。

[0120] 术语“和/或”或“/”意指与该术语相关的任何一个项目、项目的任何组合或所有项目。

[0121] 如本文所使用的，术语“每个”在用于指项目集合时，旨在识别集合中的单个项目，但不一定指集合中的每个项目。如果明确的公开或上下文清楚地规定了其他情况，则可以出现例外。

[0122] 本文所提供的任何和所有示例或示例性语言(例如，“诸如”)的使用仅仅旨在更好地说明本发明，而不是对本发明的范围进行限制，除非另有声明。说明书中的任何语言都不应被解释为指示任何未要求保护的元素对于本发明的实践是至关重要的。

[0123] 除非本文另有指示或者与上下文明显矛盾，否则本文所描述的所有方法都以任何合适的顺序执行。关于所提供的任何方法，该方法的步骤可以同时或顺序地发生。当该方法的步骤顺序发生时，这些步骤可以以任何顺序发生，除非另有说明。

[0124] 在方法包括步骤组合的情况下，步骤的每个和每一个组合或子组合都涵盖在本公开的范围内，除非本文另有说明。

[0125] 本文所引用的每个出版物、专利申请、专利和其他参考文献，在与本公开不一致的范围内都通过引用结合其整体。本文所公开的出版物仅被提供用于其在本发明的申请日之前的公开。本文中的任何内容都不应被解释为承认本发明没有资格凭借在先发明而先于该出版物。此外，所提供的出版日期可以与实际出版日期不同，这可能需要独立地确认。

[0126] 应当理解，本文所描述的示例和实施例仅仅是出于说明目的，本领域技术人员将会想到根据这些示例和实施例的各种修改或变化，并且这些修改或变化将被包括在本申请的精神和范围以及所附权利要求的范围内。

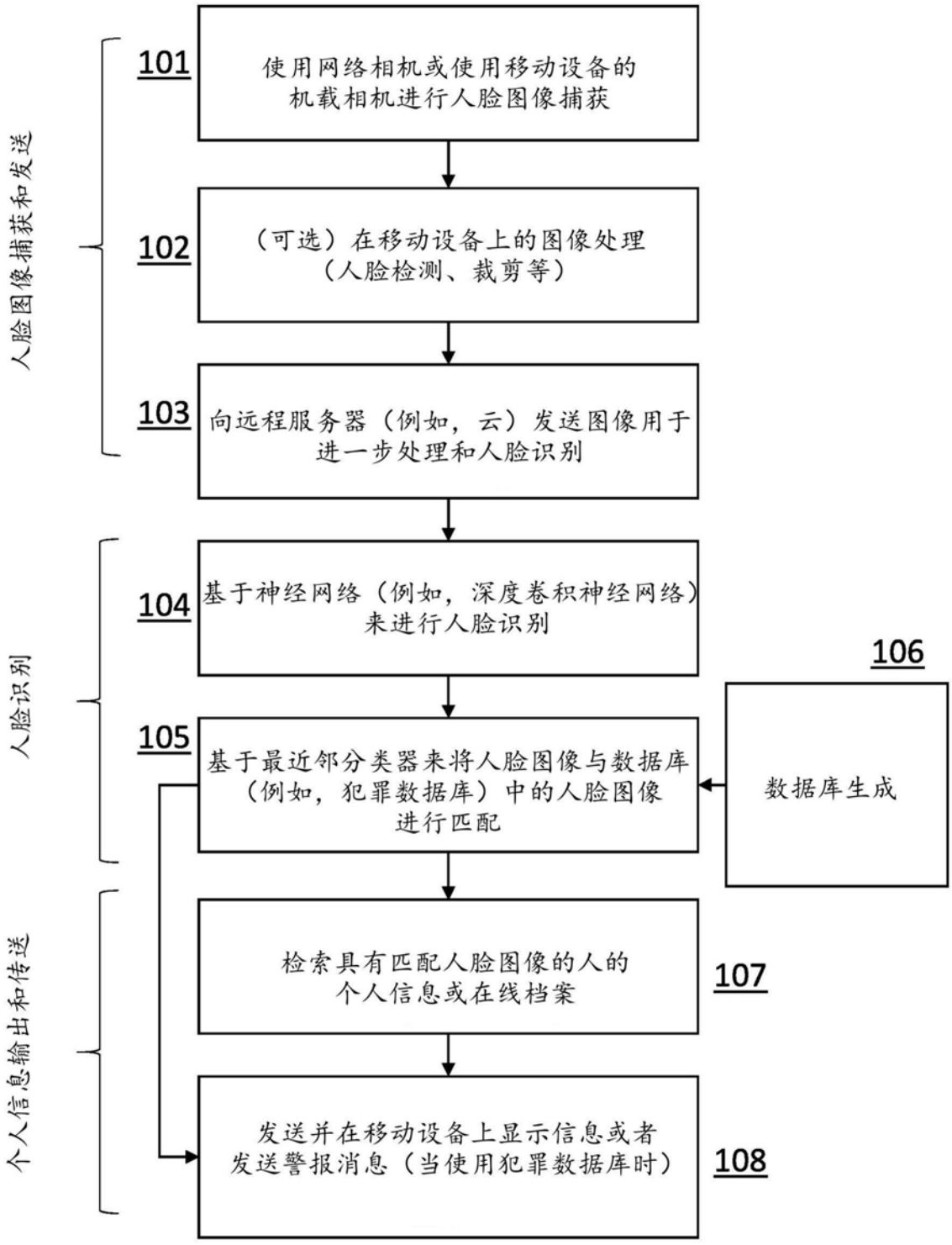

人脸图像捕获和发送
人脸识别
个人信息输出和传送
101
使用网络相机或使用移动设备的机载相机进行人脸图像捕获
102
（可选）在移动设备上的图像处理（人脸检测、裁剪等）
103
向远程服务器（例如，云）发送图像用于进一步处理和人脸识别
104
基于神经网络（例如，深度卷积神经网络）来进行人脸识别
106
105
基于最近邻分类器来将人脸图像与数据库（例如，犯罪数据库）中的人脸图像进行匹配
数据库生成
检索具有匹配人脸图像的人的个人信息或在线档案
107
发送并在移动设备上显示信息或者发送警报消息（当使用犯罪数据库时）
108

图1

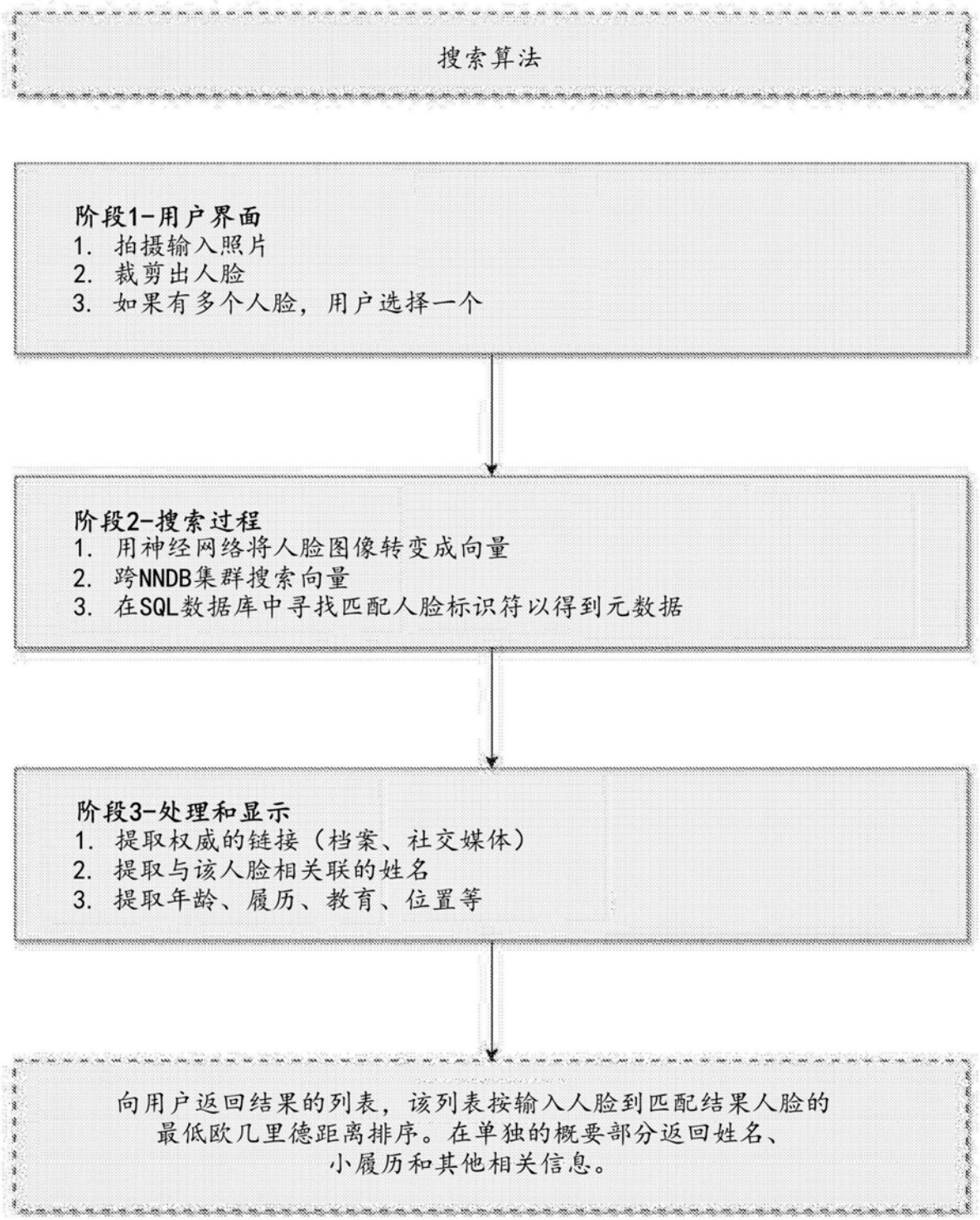

搜索算法
阶段1-用户界面
1. 拍摄输入照片
2. 裁剪出人脸
3. 如果有多个人脸，用户选择一个
阶段2-搜索过程
1. 用神经网络将人脸图像转变成向量
2. 跨NNDB集群搜索向量
3. 在SQL数据库中寻找匹配人脸标识符以得到元数据
阶段3-处理和显示
1. 提取权威的链接（档案、社交媒体）
2. 提取与该人脸相关联的姓名
3. 提取年龄、履历、教育、位置等
向用户返回结果的列表，该列表按输入人脸到匹配结果人脸的
最低欧几里德距离排序。在单独的概要部分返回姓名、
小履历和其他相关信息。

图2


爬虫算法
阶段1-网络爬虫
1. 网络爬虫植入了数千个起始URL
2. 提取每个图像，将每个图像以及图像和网页的标题和描述一起放到下载队列上
3. 跟随页面上的每个链接。跟踪重复的链接使得不会在初始循环中结束
阶段2-人脸提取
1. 下载与页面相关联的每个图像并且针对人脸进行检查
2. 将每个人脸矩形与图像id一起存储在SQL中
3. 如果图像具有人脸，则元数据（例如标题、描述）也存储在SQL中
阶段3-处理并添加到数据库
1. 向GPU集群发送人脸图像，并将其转变成向量
2. 向NNDB添加人脸向量
3. 向SQL添加元数据：标题、描述和姓名
网络爬虫是连续的过程，其连续地添加到人脸的可扩充的数据库。
其他职业的爬虫可以被集成到人脸的流水或现存数据库中，
例如大头照可以批量导入

图3

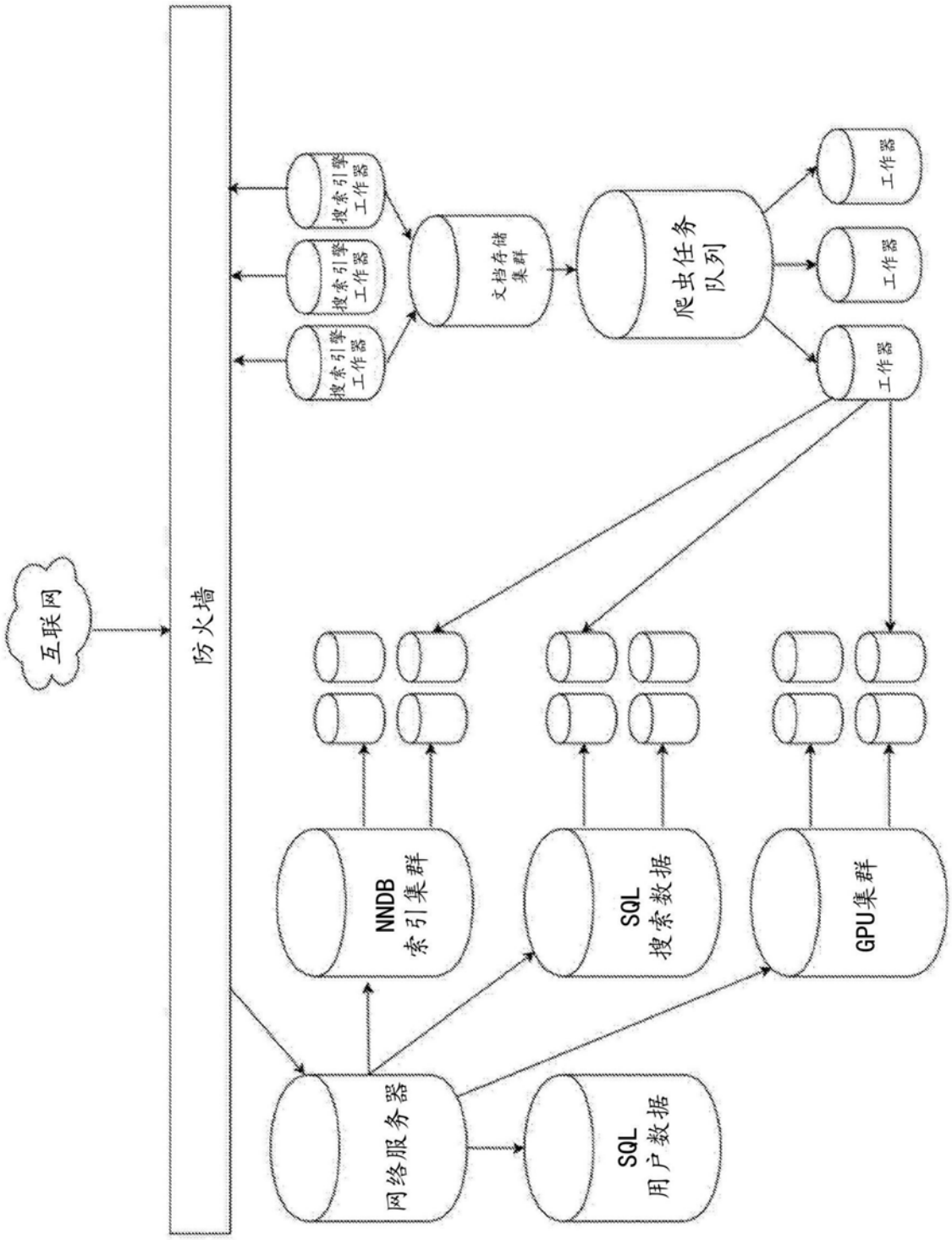

互联网
防火墙
网络服务器
SQL
用户数据
NNDB
索引集群
SQL
搜索数据
GPU集群
搜索引擎
工作器
搜索引擎
工作器
搜索引擎
工作器
文档存储
集群
爬虫任务
队列
工作器
工作器
工作器

图4

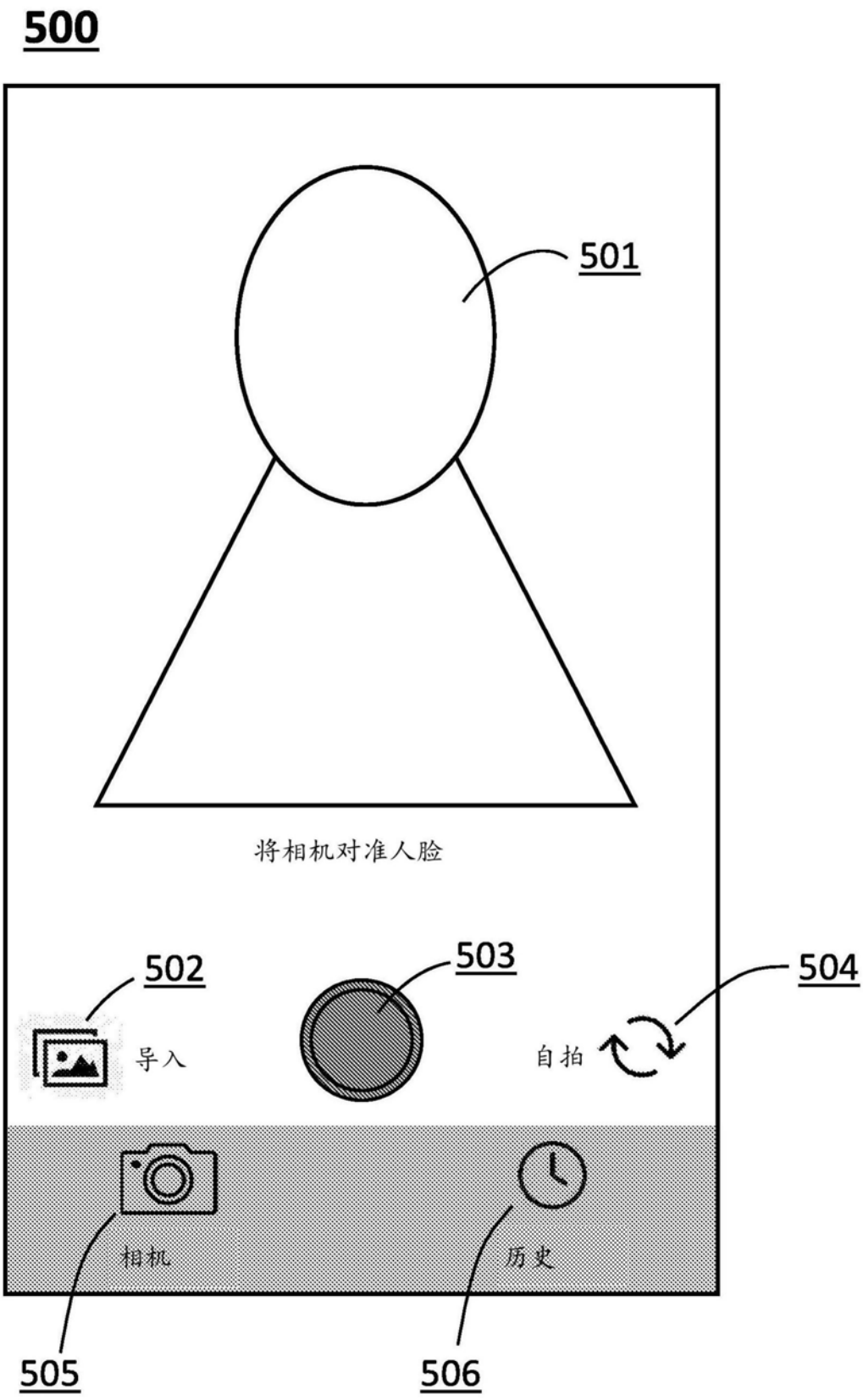


图5

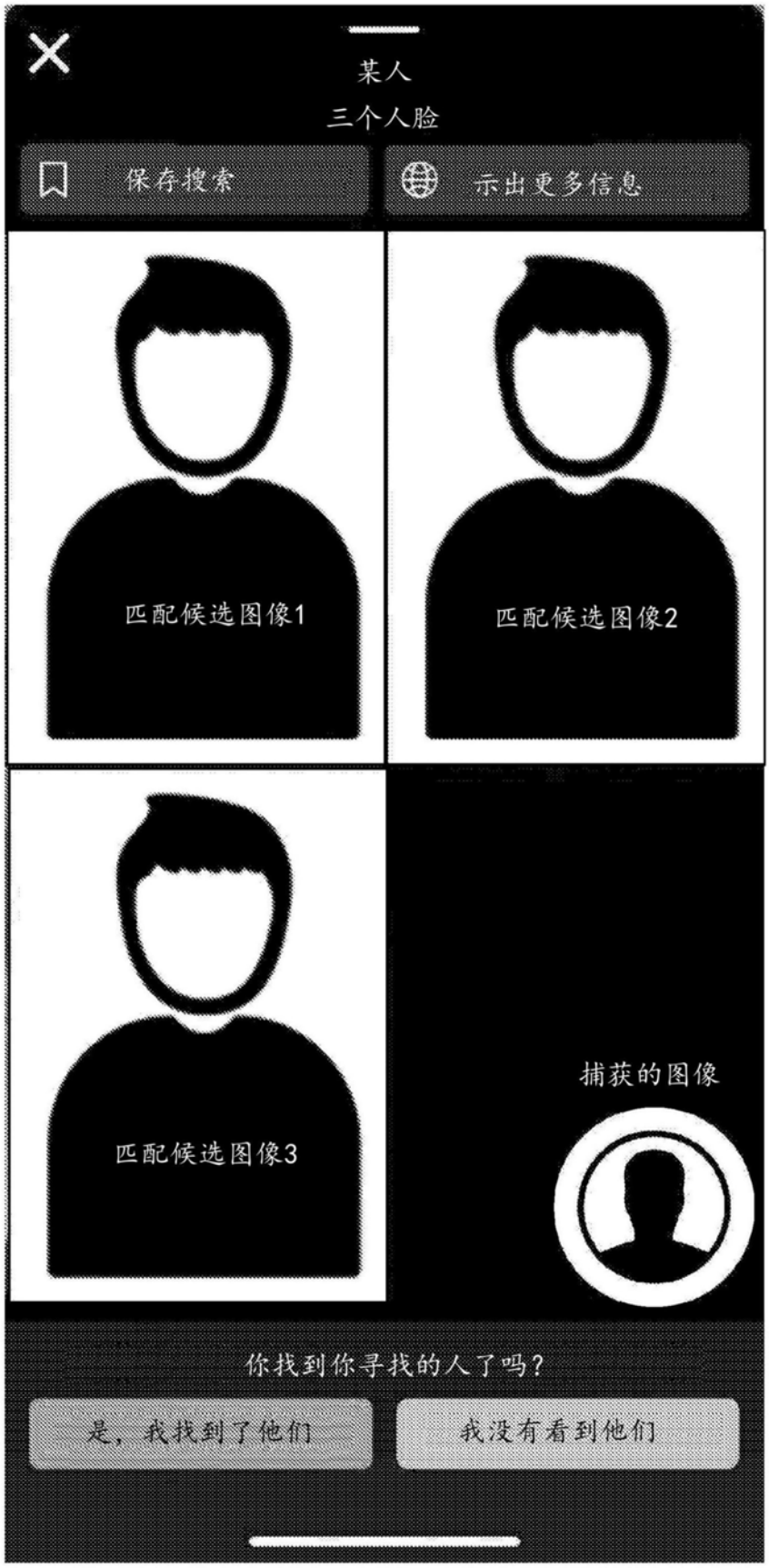

某人
三个人脸
保存搜索
示出更多信息
匹配候选图像1
匹配候选图像2
匹配候选图像3
捕获的图像
你找到你寻找的人了吗?
是，我找到了他们
我没有看到他们

图6

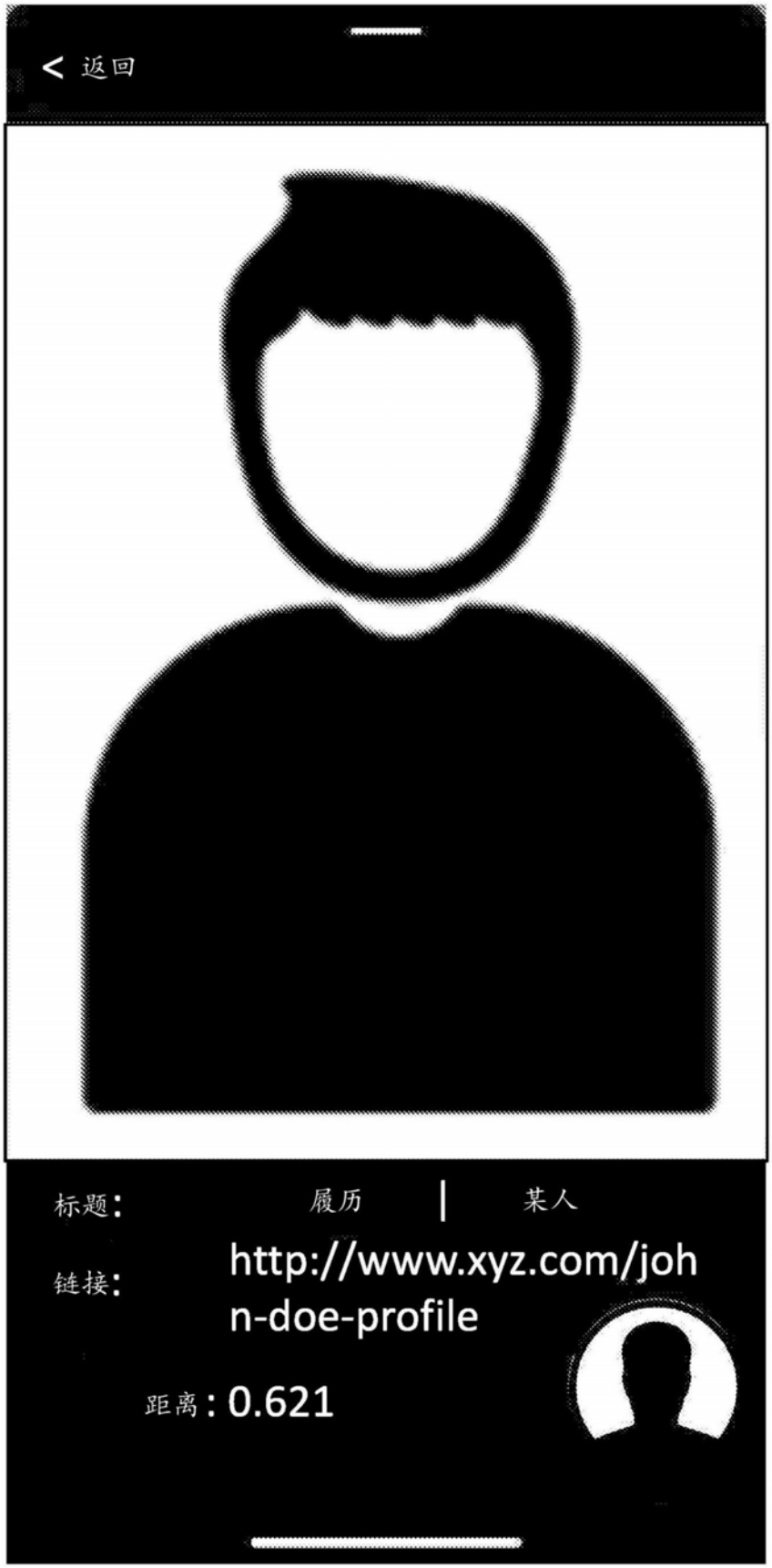


图7

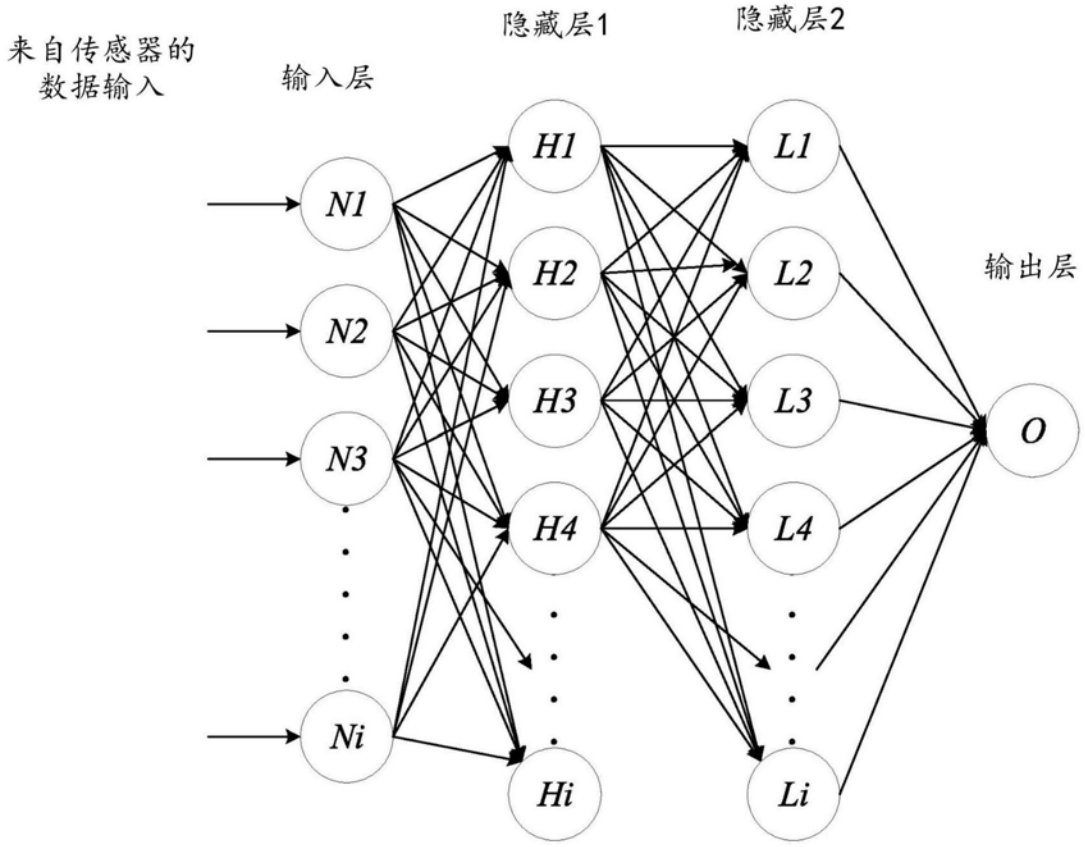

来自传感器的
数据输入
输入层
隐藏层1
隐藏层2
输出层
N1
N2
N3
Ni
H1
H2
H3
H4
Hi
L1
L2
L3
L4
Li
O

图8

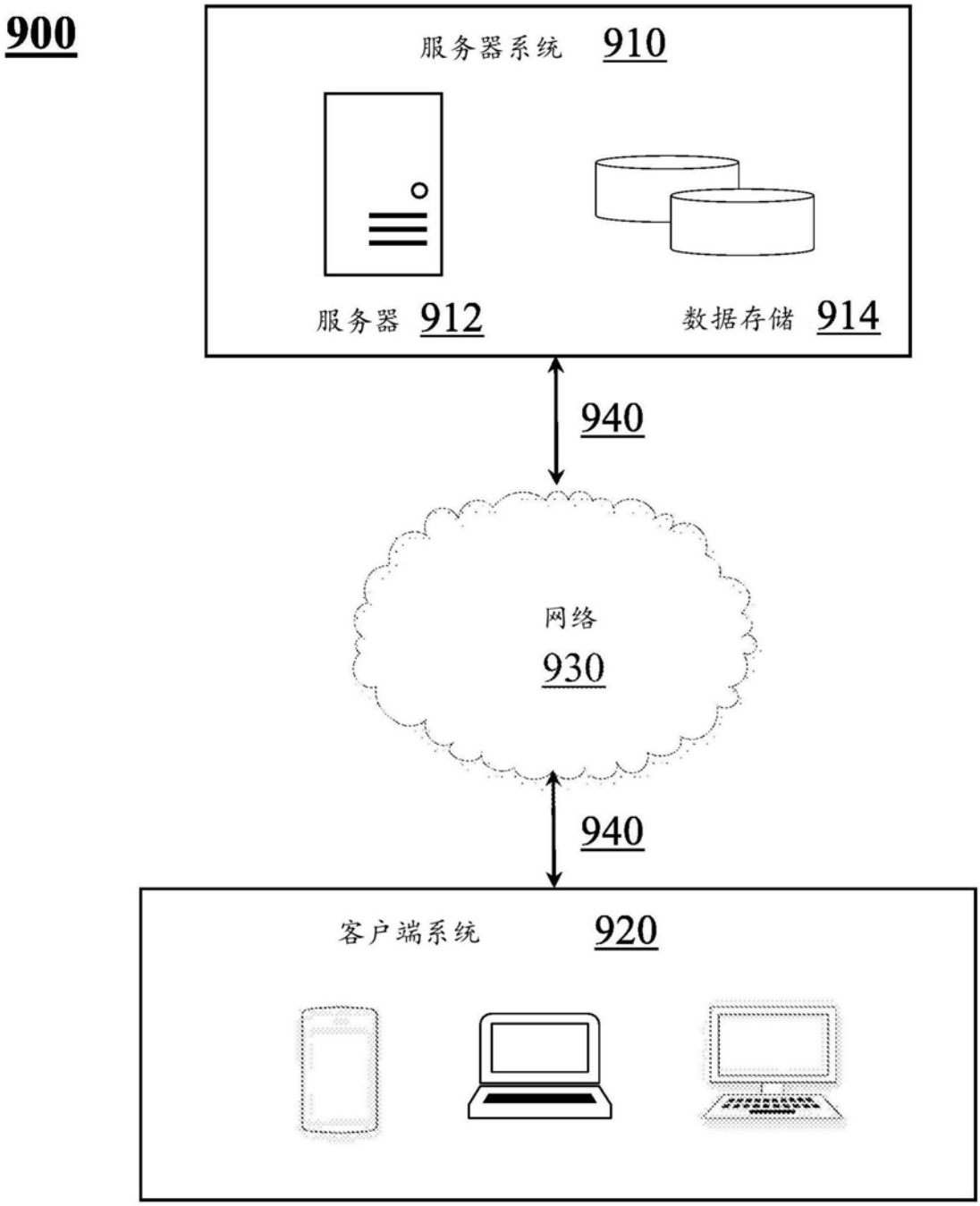


图9

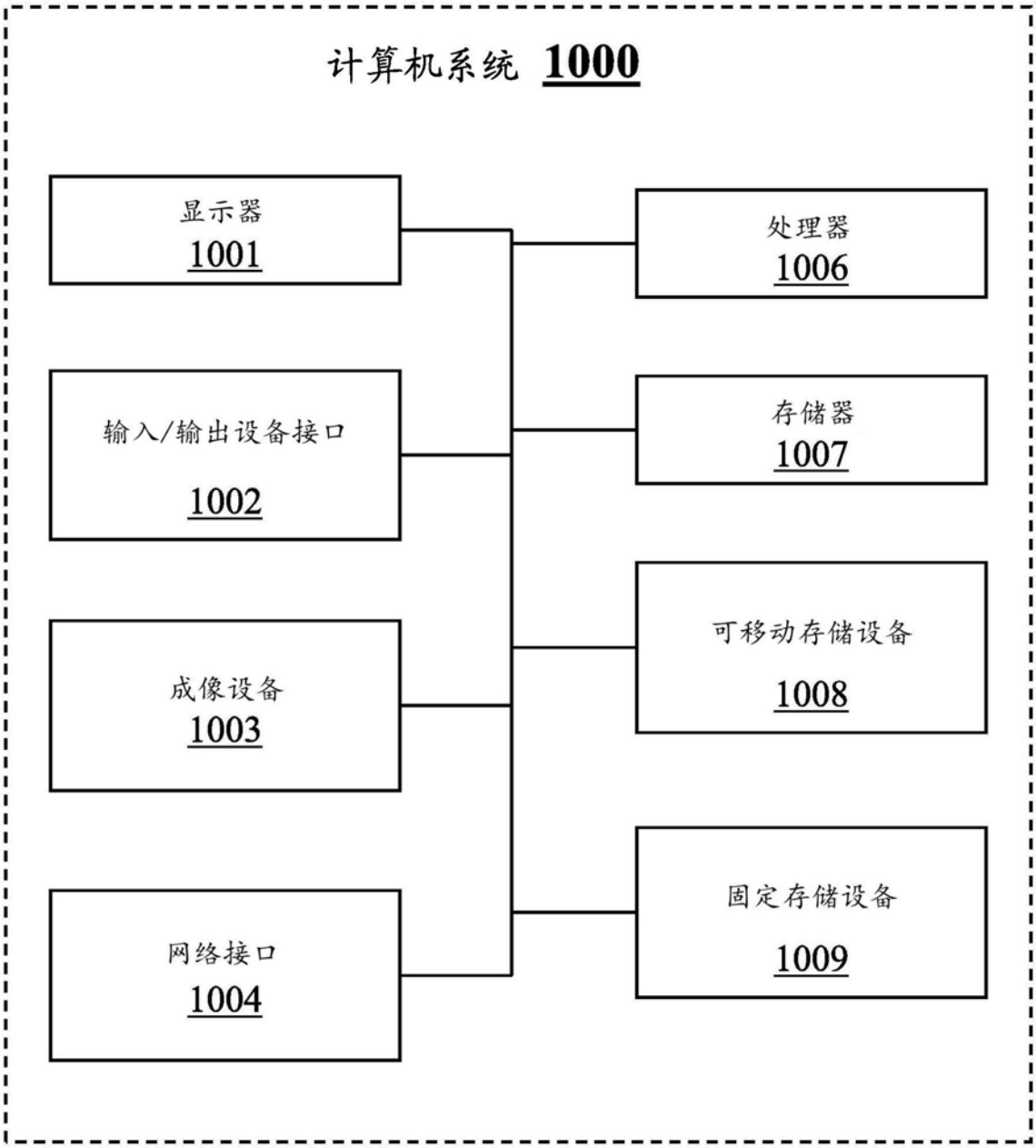

计算机系统 1000
显示器
1001
输入/输出设备接口
1002
成像设备
1003
网络接口
1004
处理器
1006
存储器
1007
可移动存储设备
1008
固定存储设备
1009

图10