



(45)授权公告日 2018.11.23

塞格尔·瓦格梅尔

申请公布号 CN 104756135 A

代理人 郑霞

(51) Int. Cl.

G06K 9/00(2006.01)

(56)对比文件

US 2010/0127827 A1, 2010.05.27,

US 2010/0046830 A1, 2010.02.25,

US 8160307 B2, 2012.04.17,

US 2008/0002860 A1, 2008.01.03.,

US 4371951 A, 1983.02.01,

US 2009/0297032 A1, 2009.12.03,

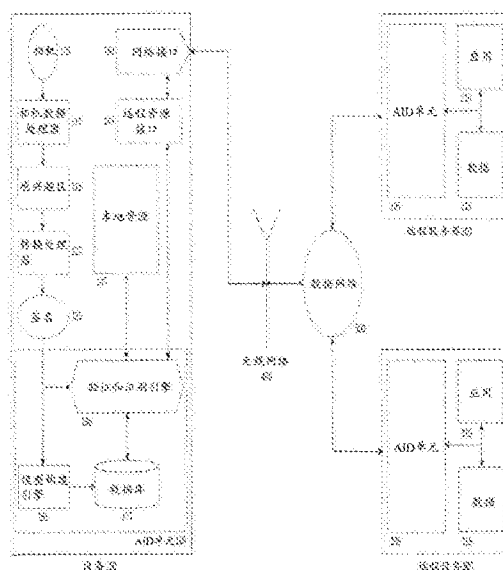
US 2011/0229045 A1, 2011.09.22,

审查员 滕冲

权利要求书2页 说明书11页 附图4页

用于与配备有相机的设备相关的生物特征验证的系统和方法

本发明总体上涉及用于验证和识别的生物特征技术的使用,并且更具体地涉及基于无接触的解决方案,该解决方案用于经由诸如移动设备之类的计算机来验证和识别用户,从而选择性地允许或拒绝对各种资源的访问。在本发明中,使用个人的手掌的一个图像或一组图像,通过涉及下列关键步骤的过程来进行验证和/或识别,所述关键步骤为:(1)使用局部分类器检测手掌区域;(2)从一个或多个感兴趣区中提取特征;以及(3)计算相对于存储在数据库中的用户模型的匹配得分,该数据库可以通过学习过程而得到动态增强。



1. 一种用于提供对资源的选择性访问的系统,该资源基于学习过程而与计算设备相关地获得,所述系统包括:

(a) 与所述计算设备相关联的至少一个相机,所述相机被配置为拍摄第一用户的人的掌纹的至少一个图像,其中在图像拍摄的过程中所述人的掌纹与所述计算设备没有物理接触;其中所述计算设备被配置为接收身份的第二要素,其中所述身份的第二要素包括用户名、用户ID、密码、唯一员工ID、社会保险号码、电子邮件地址、安全提问、指纹识别、面部识别、虹膜识别、手写签名识别、与人的掌纹相区分的生物手段或上述的组合;

其中所述计算设备执行以下操作:

(1) 使用经过训练的检测器,通过所述学习过程,从多个范例图像内的多个可辨别的局部特征中形成多个分类器,其中所述分类器将每个像素标记为手掌像素和非手掌像素;

(2) 使用所述经过训练的检测器和所述分类器来将相邻的手掌像素编组为连通分量,从而定位并分割所述人的掌纹的感兴趣区;

(3) 使用所述感兴趣区内的小抽样窗口来识别图像分块,所述图像分块包围所述人的掌纹的特性生物特征,并且

(4) 从所述图像分块的像素级数据中提取签名,其中所述签名对于所述第一用户是唯一的,并且所述签名被用于将所述第一用户与第二用户区分开,并且其中从所述图像分块的像素级数据中提取签名包括创建所述图像分块中的边缘定向的直方图;以及

(5) 基于所述签名以及包含多个用户模型的至少一个数据库来确定对所述资源中的一个或多个资源的访问,所述确定对所述资源中的一个或多个资源的访问用于验证和识别;以及

(6) 将人的掌纹的所述至少一个图像存储在所述范例图像的集合中。

2. 如权利要求1所述的系统,还包括学习处理器,其被配置为用新数据来改善所述多个用户模型,其中所述学习处理器选择性地包括所述人的掌纹的所述至少一个图像、所述图像分块的像素级数据以及所述签名,以增强所述数据库及所述验证和识别。

3. 如权利要求1所述的系统,其中所述计算设备是移动设备。

4. 如权利要求1所述的系统,其中所述计算设备是台式设备。

5. 如权利要求1所述的系统,其中所述计算设备是固定的嵌入式设备。

6. 如权利要求1所述的系统,其中所述计算设备包括闪光灯组件,该闪光灯组件在所述图像拍摄时选择性地启动,以便为所述人的掌纹的至少一个图像的感兴趣区检测、特征提取和签名处理提供最低充足光照。

7. 如权利要求1所述的系统,其中所述使用所述感兴趣区内的小抽样窗口来识别图像分块使用从所述感兴趣区上的所述图像分块中提取出的描述符。

8. 如权利要求7所述的系统,其中所述描述符被编码成高维稀疏向量,并且其中所述高维稀疏向量可以汇集成至少一个组。

9. 如权利要求8所述的系统,其中所述高维稀疏向量被汇集成至少一个组。

10. 如权利要求1所述的系统,其中所述签名是从一个特征包表示或多个特征包表示中计算出的。

11. 如权利要求1所述的系统,其中所述多个分类器是基于哈尔小波和AdaBoost算法。

12. 如权利要求1所述的系统,其中所述多个分类器是基于支持向量机。

13. 如权利要求1所述的系统,其中所述多个分类器是基于卷积神经网络。
14. 如权利要求1所述的系统,其中所述用户模型包括从所述第一用户的人的手掌图像的集合中计算出的统计模型。
15. 如权利要求1所述的系统,其中所述用户模型包括高斯密度模型。
16. 如权利要求1所述的系统,其中所述用户模型包括高斯密度模型的混合。
17. 如权利要求1所述的系统,其中所述资源中的至少一个资源远离所述计算设备。
18. 如权利要求1所述的系统,其中所述资源中的至少一个资源驻留于所述计算设备上。
19. 如权利要求1所述的系统,其中所述资源中的至少一个资源是应用。
20. 如权利要求1所述的系统,其中所述资源中的至少一个资源是数据库。
21. 如权利要求1所述的系统,其中所述第一用户的掌纹的两个图像的单个签名被一起用于该第一用户的验证或识别。
22. 如权利要求1所述的系统,其中所述基于所述签名以及包含多个用户模型的至少一个数据库来确定对所述资源中的一个或多个资源的访问选择性地允许一个或多个用户进行一个或多个事务。
23. 如权利要求1所述的系统,其中利用所述第一用户的人的掌纹的闪光和非闪光图像的序列作为反欺骗机制的一部分,以确定呈现的手是三维物体还是手的二维表示。
24. 如权利要求1所述的系统,其中利用在所述第一用户的人的掌纹的移动期间捕捉的图像数据作为反欺骗机制的一部分,以确定呈现的手是三维物体还是手的二维表示。
25. 如权利要求1所述的系统,其中利用所述第一用户的人的掌纹的闪光和非闪光图像的序列以及该序列中连续图像之间的一个或多个时间间隔作为反欺骗机制的一部分,以确定敌方是否企图利用先前记录的图像序列来进行验证或识别。
26. 如权利要求1所述的系统,其中作为反欺骗机制的一部分,储存所述第一用户的先前使用的所有图像以便与新图像进行对比,从而确定敌方是否企图利用先前记录的图像来进行验证或识别。
27. 如权利要求1所述的系统,其中作为反欺骗机制的一部分,将事务信息嵌入于所述第一用户的人的掌纹的图像或闪光模式的序列的时序内,从而确定为了验证或识别而提供的所述第一用户的人的掌纹的至少一个图像是否匹配所述事务信息。

用于与配备有相机的设备相关的生物特征验证的系统和方法

[0001] 相关申请的交叉引用

[0002] 本申请依赖于并且要求2012年9月5日提交的美国临时专利申请号61/696,820的申请日的权益,该文献的全部公开内容通过引用并入于此。

[0003] 发明背景

发明领域

[0004] 本发明总体上涉及用于验证和识别的生物特征技术的使用,并且更具体地涉及基于无接触的解决方案,该解决方案用于经由诸如移动设备之类的计算机来验证和识别用户,从而选择性地允许或拒绝对各种资源的访问。在本发明中,使用个人的手掌的一个图像或一组图像,通过涉及下列关键步骤的过程来进行验证和/或识别,所述关键步骤为:(1)使用局部分类器(local classifier)检测手掌区域;(2)从一个或多个感兴趣区提取特征;以及(3)相对于存储在数据库中的用户模型,计算匹配得分,该数据库可以通过学习过程而得到动态增强。

[0005] 相关技术讨论

[0006] 诸如智能电话、平板计算机和笔记本计算机等移动设备已被许多人每天广泛地采用和使用。这些设备已变得越来越强大,并且随着开发者创造出越来越多的运行于这些设备上的应用和服务,它们变得更加深入我们的日常生活之中。这些移动设备不仅本身提供了强大的计算平台,而且它们还提供了对在远程平台上可用的几乎无限种服务、应用和数据的连接性,这些远程平台通常经由通往蜂窝基站并继而回传到因特网骨干网的无线链路来访问。除了访问这些远程平台之外,移动设备还具有通过短距离和远距离无线连接而连接至其他移动设备的能力。

[0007] 或许最重要的是,这些设备的日益增加的普及与这些设备中的组成部件相关的成本的不断降低相结合,已经导致这些设备变得能够以更强的性能而同时对于许多用户仍然负担得起的价格获得。例如,由于组成部件成本的降低以及更强大的软件的开发,相当数目的智能电话现在包括强大的相机,所述相机可以拍摄八百万像素或更高量级的非常细致的照片。

[0008] 在移动设备及其与如此之多的功能相关的广泛使用以及它们与如此之多的不同资源进行交互的需求的背景下,出现的一个重要问题是需要控制对这些资源中的每一个的访问,以便只有那些应被授权访问适用资源的个人或设备才能够实际上进行访问。在典型情况下,通过输入文本/数字字符串(诸如用户ID和密码)来控制资源访问。例如,智能电话用户在他被允许访问该设备上的任何功能之前可能被要求输入四位数码。另外,设备上的每个本地应用或其他资源可能要求该用户在获得对该资源的访问之前输入一个或多个文本/数字字符串。在这种情况下,正确的数据(用户ID、密码等)可以储存于该设备的存储器中。或者,为了访问位于该设备的远程的资源(应用、数据、通信能力等),可能要求用户和/或设备传输一组正确的文本/数字字符串到该远程资源,而该远程资源进而在允许访问该资源之前检验所传输的数据匹配于正确数据。

[0009] 人们可以想象到,举例而言,对于典型的智能电话用户,上述用于验证和识别的技术存在若干个缺点。其中之一是,需要记住用于如此之多的不同应用、服务及其他资源的用户ID和密码,而这些不同应用、服务及其他资源各自对于必须如何构成这些ID和密码均有其自己的要求,这可能是相当让人畏缩的,并且用户对于那些他们不经常访问的资源往往会忘记它们的ID和密码。另一不利之处在于,使用文本/数字字符串来控制对资源的访问会存在安全问题。例如,存在可以用于破解这些字符串以获得对资源的未经授权访问的强大软件程序。

[0010] 而且,由用户使用他或她的手指在智能电话屏幕上输入密码和用户ID的基于接触的典型方法自身就会造成安全风险。有经验的黑客往往能够基于由手指留下的残油而从屏幕“拾取”出指纹图案,从而获得未经授权访问。在输入诸如四位数字等短数字字符串来解锁设备的背景下尤其如此。一旦设备被解锁,该设备上的许多资源可能甚至没有安全防护,从而导致严重的安全风险。

[0011] 一种以消除或减少以上讨论的缺点为目标的解决方案涉及使用生物特征技术来控制对可经由移动设备获取的资源的访问。虽然这些解决方案在一些情况下消除了以上讨论的缺点中的一些缺点,但它们仍然遭受到诸多不利。例如,一些基于接触的解决方案要求用户将他或她的手指放置在有能力捕捉该用户指纹的设备传感器上,该指纹继而与本地的或者位于远程的指纹数据相匹配,以确定是否存在足以允许该用户或该设备访问一个或多个资源的匹配。在这种情况下,如上文所提到,指纹可能会被黑客从设备传感器拾取出来,并被用于随后利用那个被盗用的指纹来获得对一个或多个资源的未经授权访问。这些解决方案通常还遭受到这样的缺点:即,在试图在典型的一天里获取对设备上的许多不同资源的访问的忙碌用户的背景下,执行确定指纹是否匹配所必需的处理所花费的时间可能是不可接受的。

[0012] 存在涉及细菌、病毒或其他生物危害传播的、与基于接触的方法相关联的额外健康问题,在多个用户之间共享设备的情况下尤为如此。如本领域中已知,个人的指尖,以及更一般而言个人的手,往往是在人与人之间传递细菌、病毒或其他生物危害的主要媒介之一。在单个设备在多人之间共享的情况下,基于接触的验证和识别方法——其中由用户用他或她的指尖输入识别字符串,或者通过基于接触的生物特征方法(诸如指纹或掌纹识别等等)来验证或识别他或她自己——产生了经由共享的接触媒介传递所述生物危害的风险。

发明内容

[0013] 因此,本发明的一个目的是提供一种基于无接触的生物特征系统和方法,该系统和方法支持对用户和设备的准确、安全和快速的验证和/或识别,从而提供对可通过配备有相机的设备访问的资源的选择性访问。

[0014] 在本发明的一个实施方式中,此类配备有相机的设备(下文为了方便起见而有时将其称为“智能电话”,但该设备应理解为包括所有的具有相机功能的设备,包括移动设备和固定设备(例如台式计算机))的用户(该用户被要求识别或验证自己,以作为获取对一个或多个资源的访问的条件)使用该智能电话的相机拍摄他们的一个手掌或全部两个手掌的一张或者一系列照片。本发明的系统继而采用计算机视觉技术来分析该掌纹图像,并且检

验掌纹签名匹配于数据库中的用户模型(用户验证),或者在数据库中的许多模型间找出匹配的用户模型(用户识别)。

[0015] 通过下面结合附图对示例性实施方式的详细描述,本发明的其他特征和方面将会变得显而易见。

附图说明

[0016] 图1是描绘本发明的优选实施方式的系统的主要组件的示意图;

[0017] 图2是用于图示本发明的优选实施方式的方法的框图;

[0018] 图3是图示根据本发明的优选实施方式的、在移动设备与一个或多个远程服务器之间的安全连接性的示意图;

[0019] 图4是图示根据本发明的优选实施方式的、在对用户或设备进行验证中的关键步骤的流程图;以及

[0020] 图5是图示根据本发明的优选实施方式的、在对用户或设备进行识别中的关键步骤的流程图。

具体实施方式

[0021] 现在详细参考本发明的各个示例性实施方式。应当理解的是,如本文所宽泛地公开,以下对示例性实施方式的讨论并不旨在限制本发明。相反,提供下面的讨论以便给予读者对本发明某些方面和特征的更详细的理解。

[0022] 在详细描述本发明的实施方式之前,应当理解的是,本文所使用的术语的目的仅仅是描述具体的实施方式,而不是旨在作出限制。除非另有定义,本文使用的所有技术术语具有与该术语所属领域的普通技术人员所通常理解的含义相同的含义。虽然在实施本发明时能够使用类似于或等同于本文所描述方法和材料的任何方法和材料,现在描述优选的方法和材料。本文提到的所有出版物均通过引用而并入与此,以公开和描述与引用该出版物有关的方法和/或材料。若本公开内容与任何并入的出版物相冲突,则以本公开内容为准。

[0023] 如在本文和随附的权利要求书中所使用的那样,除非上下文另有明确规定,单数形式“一个”、“一种”等包括复数个指代物。因此,举例而言,提到的“一个手掌”包括个人的单一手掌或者全部两个手掌,并且提到的“一个图像”包括对一个或多个图像的参考。此外,对于可使用等同术语描述的术语的使用包括对那些等同术语的使用。因此,举例而言,术语“相机”的使用应理解为包括任何能够获取物体的图像的设备。作为另一示例,并且如上文所述,术语“智能电话”包括所有具有相机功能的设备。

[0024] 下面给出本发明的优选实施方式的描述。参考图1,下面给出本发明的系统的关键组件以及在其中这些组件相互交互的背景的讨论,从而得出本发明的优点。设备100可以是包含能够拍摄高质量照片的相机的任何设备。优选地,设备100的相机还包含闪光灯元件,该闪光灯元件能够被选择性地和快速地启用和停用,以供照亮所要拍摄的区域。这样的设备100的示例包括智能电话、平板计算机、笔记本电脑和任何其他可由用户携带并提供使本发明的功能性可以操作的计算平台的设备,以及台式计算机或多种固定的嵌入式设备。此类固定的嵌入式设备的示例包括固定至提供对物理空间或其他资源的安全访问的设施入口通道或其他关键位置的相机设备,或者固定至用于诸如时间和出勤规程以及其他应用

目的的关键位置的相机设备。尽管不是必需的,设备100还可以包含各种其他特征,诸如屏幕(也可以是触摸屏)、小键盘、加速度计、GPS功能、存储容量和中央处理器(CPU)。

[0025] 设备100包括至少一个相机105,该相机105优选地能够产生例如二百万像素或更高像素(诸如四百万像素、六百万像素或八百万像素)的高质量照片。相机数据处理器110接收来自相机105的图像数据,并且如本领域已知那样对该数据进行处理,以创建代表该照片的像素数据,所述像素数据能够以各种方式得到使用,包括用于结合这里所描述的本发明而列出的目的。来自相机数据处理器110的数据被馈送到感兴趣区检测器115,该感兴趣区检测器115用于在更宽阔的图像内定位手掌的区域,并且以高精度度和一致性水平来划定所述区域,例如,通过具有不同的光照条件和手掌相对于该相机的定向的多种独立的图像,来提供该手掌上基本上相同形状和位置的手掌区域的遮罩(mask)。

[0026] 在感兴趣区检测器115的一个实施方式中,使用基于滑动窗口的局部分类器来检测感兴趣区,以便通过分类得分来标记手掌像素和非手掌像素,随后通过分割步骤来将相邻的手掌像素编组为输入图像中的连通分量。由于从大量的范例图像的集合中学习了相当数目的可判别的局部特征以捕捉手掌外观的稳定特性从而形成强大的分类器,因此可以实现高水平的准确性和对图像噪声的鲁棒性。作为结果,经过训练的检测器能够在以各种手定向和光照条件自由拍摄的输入图像上精确地定位和划定一个或多个感兴趣区。

[0027] 在感兴趣区检测器115的一个实施方式中,使用基于哈尔小波(Haar Wavelets)和AdaBoost(参考文献1)的局部分类器来检测用户的手的手掌区域中的感兴趣区。在感兴趣区检测器115的另一实施方式中,使用基于支持向量机(参考文献2)的局部分类器来检测用户的手的手掌区域中的感兴趣区。在感兴趣区检测器115的又一实施方式中,使用例如在美国专利号5,067,164和5,058,179以及在(参考文献3和4)中所述的卷积神经网络来检测用户的手的手掌区域中的感兴趣区。

[0028] 感兴趣区检测器115继而将包括手掌区域遮罩在内的图像数据馈送到转换处理器120,该转换处理器120用于从代表个人的手掌区域的特性特征的图像分块中提取可用于将该个人与其他用户相区分的签名125,其中所述分块是该手掌区域遮罩内的小抽样窗口。

[0029] 在一个实施方式中,签名125是按如下计算出的向量。首先,计算出在图像中的若干个精心挑选的区中的边缘定向的直方图。这可以使用众所周知的用于提取局部图像描述符的计算机视觉方法中之一来执行,所述计算机视觉方法诸如:尺度不变特征变换(SIFT)(例如,参见参考文献5)、定向梯度直方图(HOG)(例如,参见参考文献6)以及其他本领域已知的参考文献。其次,例如使用众所周知的K平均聚类算法,将每个定向直方图与已经从训练数据计算出的若干个原型进行对比。最后,形成签名向量以使得该向量的分量k对应于上述的第k个原型。分量k包含这样一些区的数目:这些区的直方图更接近于原型k而非所有其他原型。该操作序列在文献中被称为“特征包(Bag of Features)”表示(例如,参见参考文献7)。从当前的教导中应当显而易见的是,在本发明的其他实施方式中可以使用多个特征包来保存局部区之间的几何关系。

[0030] 签名125继而馈送到验证和识别引擎(AID引擎)130,该验证和识别引擎130用于实现下述的本发明的许多关键过程。AID引擎130与用户模型数据库135(如果存在的话)通信,以储存用户模型的本地副本。因此,在驻留于设备100本地上并且不要求与例如远程服务器或远程设备进行外部通信的应用或服务的情况下,可以将从相机105所拍摄的掌纹图

像产生的用户签名与储存于用户模型数据库135中的一个或多个已知的用户模型进行对比以供验证或识别。所述用户模型是从个人手掌图像的集合中计算出的统计模型,其中从这些图像导出的签名定义了该模型。在一个实施方式中,用户模型包括从用户的基准图像计算出的签名的所谓高斯密度模型。给定查询图像的签名S,使用该用户模型来计算匹配得分。如果匹配得分是:

$$[0031] \quad R = \sum_i \frac{(S_i - M_i)^2}{V_i + u}$$

[0032] 则认为该签名与用户模型相匹配,其中 M_i 和 V_i 是给定用户的所有基准图像的签名向量的第 i 个分量的均值和方差,并且 u 是小常数。如果匹配得分 R 大于针对该用户模型的预选阈值,则认为签名是与该用户模型相匹配。验证和识别引擎130、模型构建引擎155和用户模型数据库135形成AID单元160。

[0033] 签名125还被馈送到模型构建引擎155,以便在首次用户注册过程中初始化用户模型,或者在该模型已经存在的情况下选择性地合并所述签名的信息以完善储存于用户模型数据库135中的用户模型。在本发明的一个实施方式中,模型构建引擎155使用从用户的新图像提取出的签名来更新上述的均值 M_i 和方差 V_i 。

[0034] 设备100还优选地包含远程资源接口145,该远程资源接口145与AID引擎130通信。远程资源接口145充当实现于设备100上的验证和识别功能与那些在诸如远程服务器和远程设备等外部/远程资源上存在的相同功能之间的接口。因此,举例而言,远程资源接口145与驻留于远程服务器上的应用进行交互,以协调由远程应用所要求的验证或识别。这可以包括对外部资源对于操作设备100的用户的验证或识别或者对于设备100本身的验证或识别的请求进行管理和响应。

[0035] 远程资源接口145可以与网络接口150通信,以便与验证和识别活动相关地传输和接收数据。可以使用各种无线通信协议,包括射频以及其他通信协议——包括并且不限于蓝牙和其他近场通信技术。在本发明的优选实施方式中,如本领域已知的那样,例如借助于减少或消除与本发明的验证和识别方法相关联的用户数据和其他数据可被未经授权方所截获的可能性的加密和/或其他方法,来保护在开放式无线链路上从设备100来回通信的数据。网络接口150通常包括本领域已知的射频收发器模块,并且允许设备100经由无线链路而与无线网络400通信。无线网络400通常进而再次如本领域已知的那样,将设备100所传输的或者要由设备100所接收的数据回传到数据网络500。

[0036] 仅仅举例来说,本发明允许设备100的用户或设备100本身由远程服务器以及驻留于远程服务器上的应用和其他资源来验证或识别。如图1中所示,远程服务器200可以经由上文讨论的通信路径而与设备100通信。以这种方式,并且通过驻留于设备100上的远程资源接口145的控制,驻留于远程服务器200上的AID单元205可以请求和接收来自设备100的验证和识别数据,以供与驻留于远程服务器200上或者可由远程服务器200访问的已知和确认的用户模型进行对比,这在下文会更全面地描述。该验证和识别能力提供了对驻留于远程服务器200上的一个或多个应用210、数据215及其他资源的选择性访问。相同的能力还可以提供对包括驻留于设备100上的应用、数据和/或其他资源在内的本地资源140的选择性访问,以及在此类本地资源寻求访问远离设备100的数据或其他资源的情况下的选择性访问。

[0037] 在本发明的另一实施方式中,上文所讨论的通信可在设备100与一个或多个远程设备300之间发生。远程设备300可以是与设备100相同或不同的设备类型,并且根据本发明的教导的验证/识别功能性可以双向发生。也就是说,设备100可以响应于来自远程设备300的验证/识别请求,以便例如经由远程设备300上的AID单元305来访问驻留于远程设备300上的一个或多个应用310和/或数据315。而远程设备300也可以接收和响应于由设备100发起的验证和识别请求,以便让远程设备300(或者对其进行操作的用户)访问驻留于设备100上的资源。在一些情况下,设备100和远程设备300两者在共享资源之前都会要求对彼此进行验证和/或识别。例如,这可能会发生在设备100和远程设备300的用户之间的期望的保密通信的背景下。

[0038] 转向图2,现在描述根据本发明的优选实施方式的用户/设备验证和/或识别方法。通过初步讨论,首先描述在本发明的教导的上下文中在验证与识别之间的差异。

[0039] 在验证的情况下,用户以用户ID或用户名的形式呈现身份,而本发明的系统检验该用户确实是他或她所声称的用户。该系统继而将从用户手掌的一个图像或多个图像中导出的签名与用户模型数据库中的对应模型进行对比。如果它们匹配,则该用户得到验证。如果它们不匹配,则该用户被拒绝。

[0040] 图4中示出了优选实施方式中的、根据本发明的教导的用于用户验证的流程图。作为第一步骤,位于设备100处的用户可以向设备100中输入他或她的姓名或其他识别信息,或者该用户的身份可能已经被预先装载于设备100中。单独地,用户使用设备100的相机105来拍摄他或她的一只手或两只手的手掌的一个图片或一组图片。接下来,相机数据处理器110将原始像素数据发送至感兴趣区检测器115,感兴趣区检测器115确定图像内的手掌区域。来自感兴趣区检测器115的被遮罩手掌区域被馈送到转换处理器120,转换处理器120导出用户的唯一签名。这样的转换功能可以替代地在远程资源上处理,或者部分地在远程资源上并部分地在设备100上处理。在被成像的手掌区域与设备100之间无直接接触的情况下,通过使用无需超出常用的数码相机之外的任何特殊硬件而由最终用户自由拍摄并且处于任何定向的手的高分辨率图像,本发明的系统使用多步骤软件解决方案来识别个人,所述多步骤软件解决方案涉及特征提取、将特征处理成用户签名、以及用户签名与已储存的用户签名或用户模型的匹配,其中:(i)从输入图像检测和分割出单一感兴趣区或多个感兴趣区,以便移除无关的像素数据并分离出手掌区域;(ii)从图像提取出若干个高维稀疏特征向量(例如,参见参考文献8);(iii)在将邻近的特征向量汇集成更紧凑和稳健的图像表示的过程中,针对每个图像创建单一签名;以及(iv)将多个图像签名组合成针对每一单个用户的身份模型。

[0041] 验证和识别引擎130继而在用户模型数据库135中(基于先前呈现的用户识别数据)查找用户的模型。此时,如果导出的用户签名与储存的用户模型相匹配,则该用户被验证并且被允许访问期望的资源或一组资源。或者,如果用户签名与模型不匹配,则该用户被拒绝访问期望的资源或一组资源。关于查找和匹配的上述功能性可以替代地远离设备100地执行。

[0042] 在识别的情况下,用户仅呈现一个掌纹图像或一组图像,而验证和识别引擎130将来源于所述一个或多个掌纹图像的签名与用户模型数据库135中的所有模型或模型子集进行对比。如果发现匹配,则用户得到识别。如果没有发现匹配,则该用户是未知的。

[0043] 图5中示出了用于用户识别的流程图。在这种情况下,如同在验证的情况下那样,用户拍摄他或她的手的手掌的一个图片或一组图片。该数据再次由相机数据处理器110处理成像素形式,并且被发送至感兴趣区检测器115以确定图像内的手掌区域。来自感兴趣区检测器115的被遮罩手掌区域被馈送到转换处理器120,转换处理器120导出该用户的唯一签名,并且继而AID引擎130将导出的签名与储存于用户模型数据库135中的所有模型或模型子集进行对比。上述提及的转换功能和对比功能可以替代地在远程资源上处理,或者部分地在远程资源上并部分地在设备100上处理。在任何情况下,如果发现匹配,则该用户被识别,并且可被授权访问一个资源或一组资源。如果没有发现匹配,则该用户不被识别,并且不会授权访问期望的资源或一组资源。

[0044] 使用哪个模式(验证或识别)取决于应用。一般而言,验证提供较高的准确度,但提供较低的用户体验度,这是因为用户需要采取额外的步骤来输入他或她的身份的附加要素。身份的第二要素可以采取任何常见的形式,诸如用户名、用户ID、密码、唯一员工ID、社会保险号码、电子邮件地址、多种其他生物特征形式等等。在本发明的一个实施方式中,身份的第二要素是从个人的第二只手的一个或多个掌纹图像导出的签名,其中该个人的两个掌纹图像或多组图像中的每一个的单个签名一起用于验证或识别。

[0045] 需要注意的是,在上述每一种情况下(验证或识别),可以将通过在设备100处拍摄的用户手掌的一个图像或一组图像生成的签名与位于远程服务器200或者一个或多个远程设备300中之一或全部两者处的数据库中所包含的一个模型或多个模型进行匹配,而不是将用户签名与位于设备100本地内的用户模型数据库135内的模型进行匹配。在这种情况下,设备100的用户通常会寻求访问驻留于这些远程平台处的一个或多个资源,而不是位于设备100本地内的资源。举例而言,例如在解锁智能电话的情况下,处理可以在智能电话/设备100处本地进行,而如果例如是与基于远程的应用相关地进行验证,则该处理的一些部分可以在远程服务器200处进行,其中进行匹配所针对的用户模型有可能储存于远程服务器200处而不是储存于智能电话本地上。另外,从本教导应当显而易见的是,用户模型、签名和/或其他生物特征数据可以在AID单元160、205、305中的任何单元之间同步,以允许在设备100、远程服务器200、远程设备300中的任何一个处进行本地验证或识别,而无需所述设备100、远程服务器200或远程设备300在本地生成该用户模型、签名和/或其他生物特征数据。

[0046] 现在返回图2,可以看到在本发明的优选实施方式中,在步骤(1),使用设备100来利用相机105(步骤(3))拍摄所要识别(步骤(2))的用户的手掌的一个图片或一系列图片。可以在设备100中嵌入闪光灯组件(步骤(4))以提供对图像的必要的预处理,特别是因为其涉及为个人手掌图像的感兴趣区检测、特征提取和签名处理提供最低充足光照。接下来,由感兴趣区检测器115对图像的手掌区进行遮罩(步骤(5)),并将其馈送到转换处理器120(步骤(6))以将原始像素转换成唯一识别用户签名,即,签名125。该用户签名是紧致码,其包含与用户的掌纹图像相关联的相关识别信息,并且可以快速而精确地与用户模型的大型数据库进行匹配,所述数据库例如是用户模型数据库135或者位于远程平台处的数据库(步骤(7))。所导出的用户签名的一个益处在于,它使得基本上不可能从用户模型的数据库重建用户的手掌图像。在步骤(8)中,AID引擎130将来自所述手掌图像或所述一组手掌图像的用户签名与用户模型数据库中的用户签名进行对比,以在适用的时候识别或验证该用户。上

述转换功能和对比功能可以替代地在远程资源上处理,或者部分地在远程资源上并部分地在设备100上处理。

[0047] 现在转向图3,可以看到在关于远程资源完成验证或识别的情况下,设备100与该远程资源之间的通信优选地通过本领域已知的安全连接而发生。这可能涉及本领域已知的一个或多个技术,例如包括强加密、公钥加密或私钥加密、数字证书和/或数字签名等等。

[0048] 现在已经描述了本发明的系统和主要方法,下面将会论述附加的新颖特征,例如用于防止与验证/识别相关的欺骗的各种方法,以及用于编码和与远程资源交换事务信息的新颖方法。

[0049] 欺骗防护是本发明的一个重要方面。它防止敌方例如使用手掌的打印照片而不是真手进行验证。本发明的涉及欺骗防护的一个新颖方面包括检测和使用人手的三维特性以提供针对欺骗的安全性。

[0050] 在欺骗检测的一个示例中,为了在照片与真手之间进行区分,本发明的系统在间歇地并且以变化的时长使用相机闪光灯的情况下以快速序列拍摄一系列图片。用闪光灯拍摄的三维物体(真手)的图片将会具有由该闪光灯所创造出的高亮区和阴影,而在手的二维表示(例如,在另一移动设备的显示屏上所显示的手掌或者手掌图像的打印照片)中手的位置将不会显示出这样的高亮区和阴影。这使得本发明的系统能够利用在闪光照片与非闪光照片之间创造出的手上的高亮区和阴影的对比来区分打印照片和真手。这样,碰巧获取了授权用户的手掌的图片的未经授权方不能使用该图片来获得对本地或远程资源的未经授权访问。

[0051] 用于检测真手的进一步方法包括手的三维建模。在这种情况下,本发明的系统可提示用户在拍摄一系列多个图片时转动他或她的手。真实的三维物体将会以每个连续的图像显出手的不同部分,而二维物体将总是仅仅伴有不同程度的失真地显示出手的完全相同部分。这让本发明的系统得以区分打印照片和真手。类似地,可以提示用户在拍摄一系列图片的同时将手攥成拳头或者从拳头打开,而不是旋转手。其他区分真手和手的照片的方法也是有可能的。

[0052] 本发明的另一新颖方面在于可以检测和防止重放攻击(replay attacks)的方法。在这种情况下,敌方改造移动设备,以使得它向网络发送来自合法用户的真手的一个或一系列先前记录的图片用于验证或识别,而不是发送由相机拍摄的图像。这里假定敌方可能在授权用户不知情或不能够阻止的情况下拍摄授权用户的手的图片。如果这在事实上是个风险(例如,在授权用户正在睡觉或者无意识的情况下),则优选的是以这样的方式使用所述系统:要求一个或多个附加的身份要素,诸如独立于掌纹图像的用户ID或其他形式的数据),来验证用户。

[0053] 为了检测和防御重放攻击,本发明的系统发出一系列图片并以多种间隔闪光,即,其记录一系列图片,其中一些图片是闪光灯关闭时记录的,而另一些是闪光灯开启时记录的。特定图片以及闪光开/关序列可以是随机地或者根据预定序列选择的,并且可以针对每个验证或识别请求而改变。本发明的系统可以容易地检测出敌方是否使用了先前记录的一系列图片,这是因为图片和闪光的开/关模式将不会匹配于实际发送至移动设备的模式。

[0054] 用以检测重放攻击的另一方法涉及储存所有先前使用过的图像并且将新图像与该数据库进行对比。由于两个不同的手掌的图像背后的像素数据基本上绝不可能完全相同

或者基本上相同达某一容限水平,因此该系统可以检测先前拍摄的图像在何时被再次使用。还可以想象到其他检测重放攻击的方法。

[0055] 本发明的又一新颖方面在于将事务信息或其他数据嵌入于一系列照片和/或闪光模式的时序内的能力。该时序模式还可以用于对关于该事务本身的信息进行编码。继而可以对该信息施加加密哈希码。哈希码使得所产生的代码紧凑(短),并且还防止观察该闪光模式的任何人推导出关于该代码的原始内容的任何信息。在本发明的一个实施方式中,将图像和/或闪光模式的序列的时序用作反欺骗机制的一部分,以便确定为了验证或识别而提供的图像序列是否与来自事务本身的信息相匹配。一种特定实现方案可以包括:

[0056] 1. 具有闪光模式的手掌区域的低分辨率视频。

[0057] 2. 手掌区域的一个或若干个高分辨率静止图像。

[0058] 3. 计算机视觉技术,以确保该一个或多个高分辨率图像是来自于与该视频中的图像相同的物体。

[0059] 基于本发明的系统和方法的以上描述可以理解到,各种应用都是有可能的。示例包括但不限于访问一个或多个设备、访问驻留于那些设备上或者远程地位于服务器上或其他远程设备上的一个或多个应用、多种事务型应用(诸如选举投票、国家福利分配、财务支付)以及任何其他类型的要求确认用户身份的事务。

[0060] 总之,在示例性实施方式中,本发明提供了用于验证或识别个人的计算机系统(包括在合适的硬件上运行的软件的组合)、计算机实现方法以及设备,所述验证或识别包括通过涉及以下步骤的过程来使用个人的手掌的一个图像或一组图像,所述步骤有:(1)使用局部分类器检测手掌区域;(2)从一个或多个感兴趣区提取特征;以及(3)计算相对于储存在数据库中的用户模型的匹配得分,该数据库可以通过学习过程而得到动态增强。因此,本发明包括一种用于提供对资源的选择性访问的系统,该资源可与包含执行于合适的计算机硬件上的软件的设备相关地获得,其中所述系统包括:(a)至少一个与所述设备相关联的相机,所述相机能够拍摄人的掌纹的至少一个照片;(b)检测器模块,其使用局部分类器以在无需物理接触的情况下定位和分割手掌的感兴趣区;(c)转换处理器,其将与人的掌纹的所述感兴趣区相关联的原始像素数据转换成与所述掌纹相关联的唯一签名;以及(d)验证和识别引擎,所述验证和识别引擎基于所述唯一签名以及包含多个用户模型的至少一个数据库来确定是否应当授权访问所述资源中的一个或多个资源。该系统还可包括学习处理器,该学习处理器用新数据来改善用户模型,其中所述学习处理器选择性地包括所述掌纹图像,以增强所述数据库及所述验证和识别引擎。在一些实施方式中,所述设备是移动设备,而在其他实施方式中,所述设备是台式设备或固定的嵌入式设备。所述系统可以包括闪光灯组件,该闪光灯组件在图像捕捉时选择性地启动,以便为人的手掌图像的感兴趣区检测、特征提取和签名处理提供最低充足光照。在各个实施方式中,所述系统的转换处理器使用从所述感兴趣区上的分块提取出的描述符。所述描述符可以被编码成高维稀疏向量,所述高维稀疏向量可以汇集成至少一个组。

[0061] 作为在本发明的系统内实现的方法的一部分,该系统可以具有从一个特征包表示或多个特征包表示计算出签名的特征。另外,所述系统的检测器模块可以使用哈尔小波和AdaBoost算法。在各个实施方式中,所述系统包括使用支持向量机或卷积神经网络的检测器模块。所述系统的用户模块可以是人的手掌图像的集合计算出的统计模型。同样地,所

述用户模型可以是高斯密度模型或者是高斯密度模型的混合。

[0062] 本发明的系统可以配置成使得所述资源中的至少一个资源远离所述设备。或者,所述资源中的至少一个资源可以驻留于所述设备上。在一些实施方式中,所述资源中的至少一个资源是应用或数据库。

[0063] 在本发明的系统的各个实施方式中,人的两个掌纹图像中的每一个的单个签名(如果可用)被一起用于对该人的验证或识别。

[0064] 在本发明的系统的一些实施方式中,掌纹验证或识别与其他手段(modality)相结合,所述其他手段诸如下列各项中的一项或多项:密码、安全提问、指纹识别、面部识别、虹膜识别、手写签名识别以及其他生物特征和非生物特征手段。

[0065] 本发明的系统能够以这样的方式实现:使得应用选择性地允许一个或多个用户进行一个或多个事务。

[0066] 本发明的系统还可以包括使用人的手掌的闪光和非闪光图像的序列,除其他事项外,这可以用作反欺骗机制的一部分,以确定所呈现的手是三维物体还是手的二维表示。此外,本发明的系统能够以这样的方式实现:利用在人的手掌的移动期间捕捉的图像数据作为反欺骗机制的一部分,以确定所呈现的手是三维物体还是手的二维表示。在一些实施方式中,利用人的手掌的闪光和非闪光图像的序列以及连续图像之间的一个或多个时间间隔作为反欺骗机制的一部分,以确定敌方是否企图利用先前记录的图像序列来进行验证或识别。

[0067] 在本发明的一些实施方式中,作为反欺骗机制的一部分,储存人的先前使用过的所有图像,例如储存在驻留于计算设备上的数据库中,以供与新图像进行对比,从而确定敌方是否企图利用先前记录的图像来进行验证或识别。进一步地,在某些实施方式中,这样实现本发明的系统:使得事务信息或其他数据被嵌入于一系列图像和/或闪光模式的时序内作为反欺骗机制的一部分,从而确定为了验证或识别而提供的图像序列是否匹配于来自事务本身的信息。

[0068] 虽然已经示出和描述了本发明的具体实施方式,但对于本领域技术人员显而易见的是,基于本文的教导,可以在不脱离本发明及其更宽泛的方面的前提下作出改变和修改。

[0069] 引用参考文献

[0070] (1)Paul Viola and Michael Jones,Rapid Object Detection using a Boosted Cascade of Simple Features,Proceedings of IEEE Computer Vision and Pattern Recognition,2001,pages 1:511-518.

[0071] (2)Corinna Cortes and Vladimir N.Vapnik,Support-Vector Networks,Machine Learning,20,1995.

[0072] (3)Yann LeCun,Léon Bottou,Yoshua Bengio,Patrick Haffner:Gradient-Based Learning Applied to Document Recognition,Proceedings of the IEEE,86(11):2278-2324,November 1998.

[0073] (4)Pierre Sermanet,Koray Kavukcuoglu,Soumith Chintala and Yann LeCun:Pedestrian Detection with Unsupervised Multi-Stage Feature Learning,Proc.International Conference on Computer Vision and Pattern Recognition (CVPR'13),IEEE,June 2013.

- [0074] (5) David G.Lowe, "Distinctive image features from scale-invariant keypoints," International Journal of Computer Vision, 60, 2 (2004), pp. 91-110.
- [0075] (6) N.Dalal and B.Triggs. Histograms of oriented gradients for human detection. In Proceedings of Computer Vision and Pattern Recognition, 2005.
- [0076] (7) Y-Lan Boureau, Jean Ponce and Yann LeCun: A theoretical analysis of feature pooling in vision algorithms, Proc. International Conference on Machine learning (ICML'10), 2010.
- [0077] (8) Yann LeCun, Koray Kavukcuoglu and Clément Farabet: Convolutional Networks and Applications in Vision, Proc. International Symposium on Circuits and Systems (ISCAS'10), IEEE, 2010.

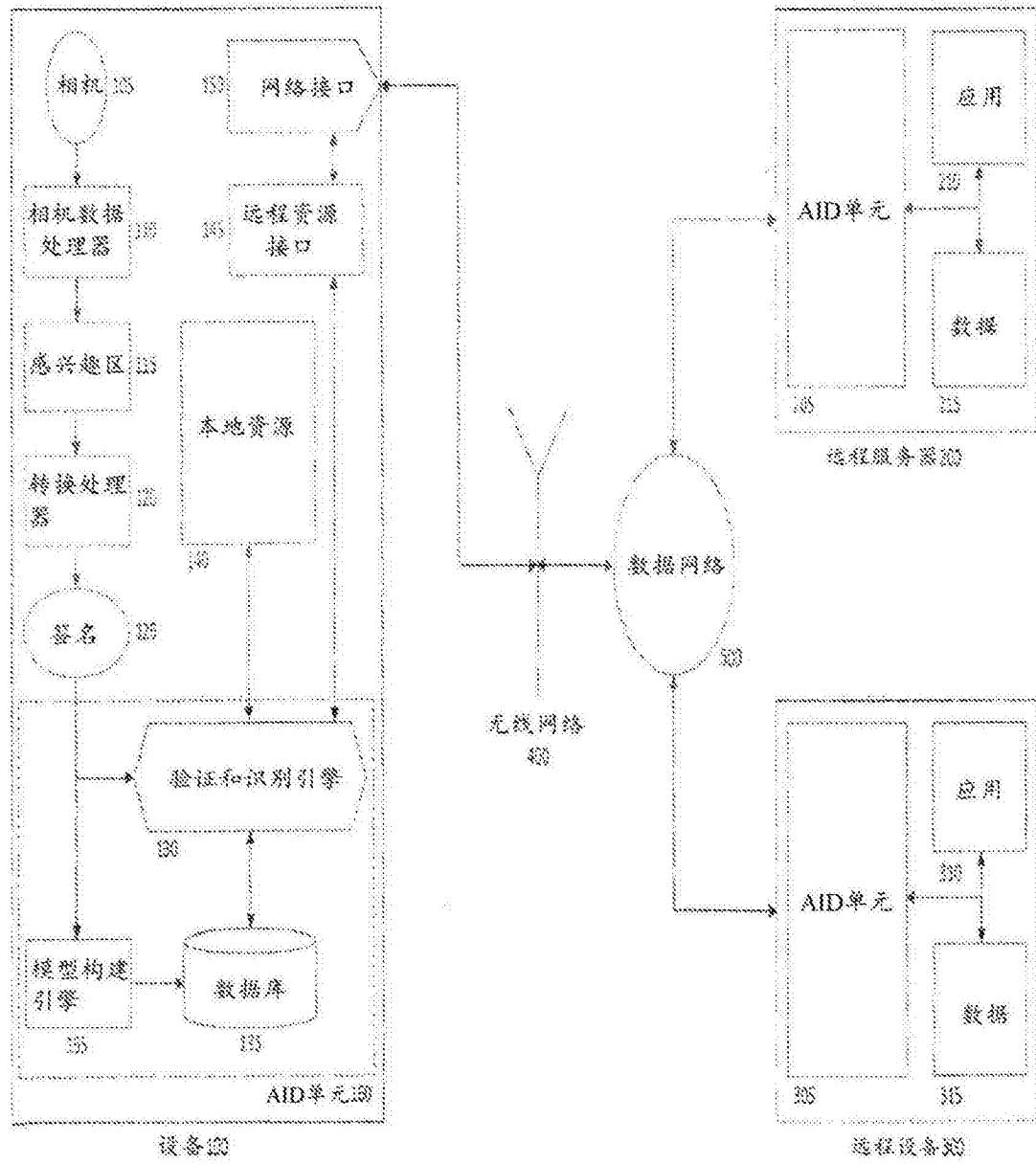


图1

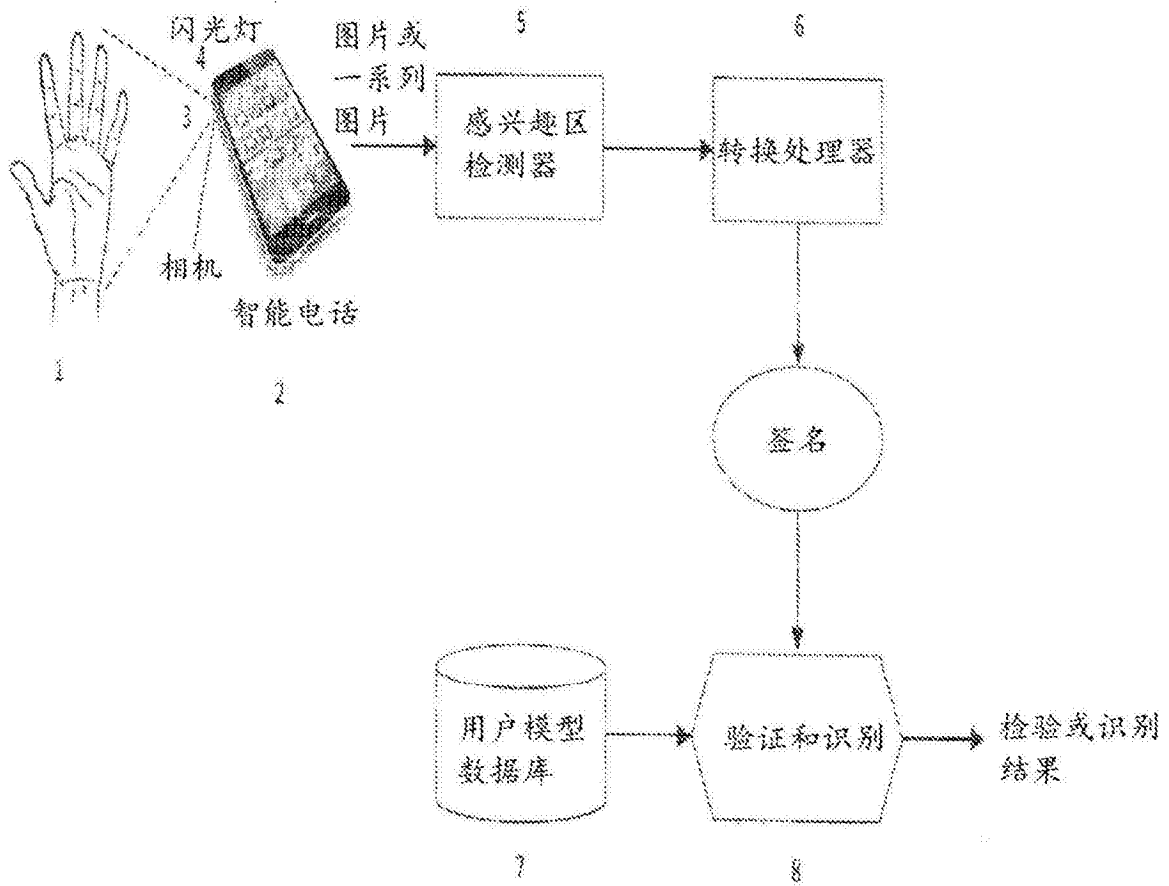


图2

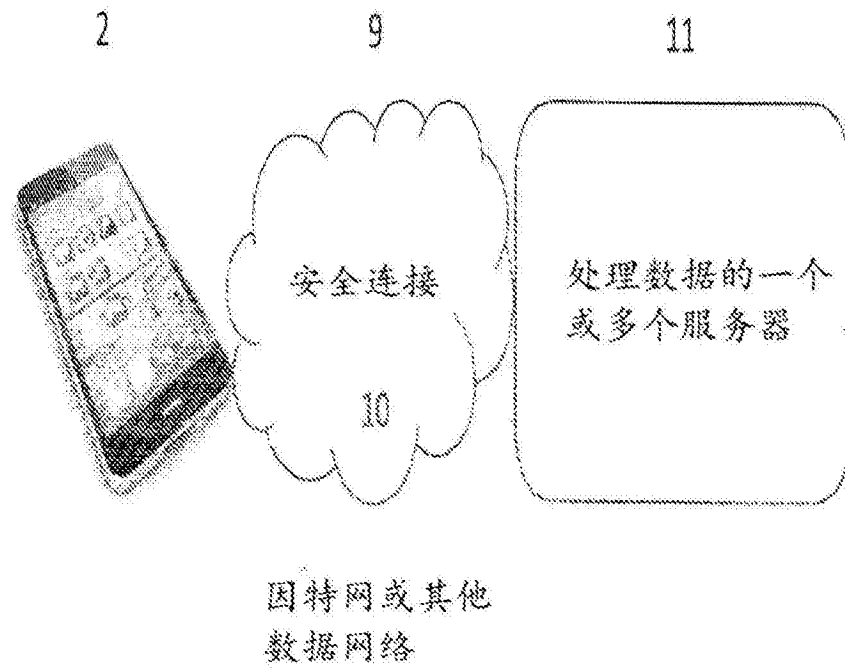


图3

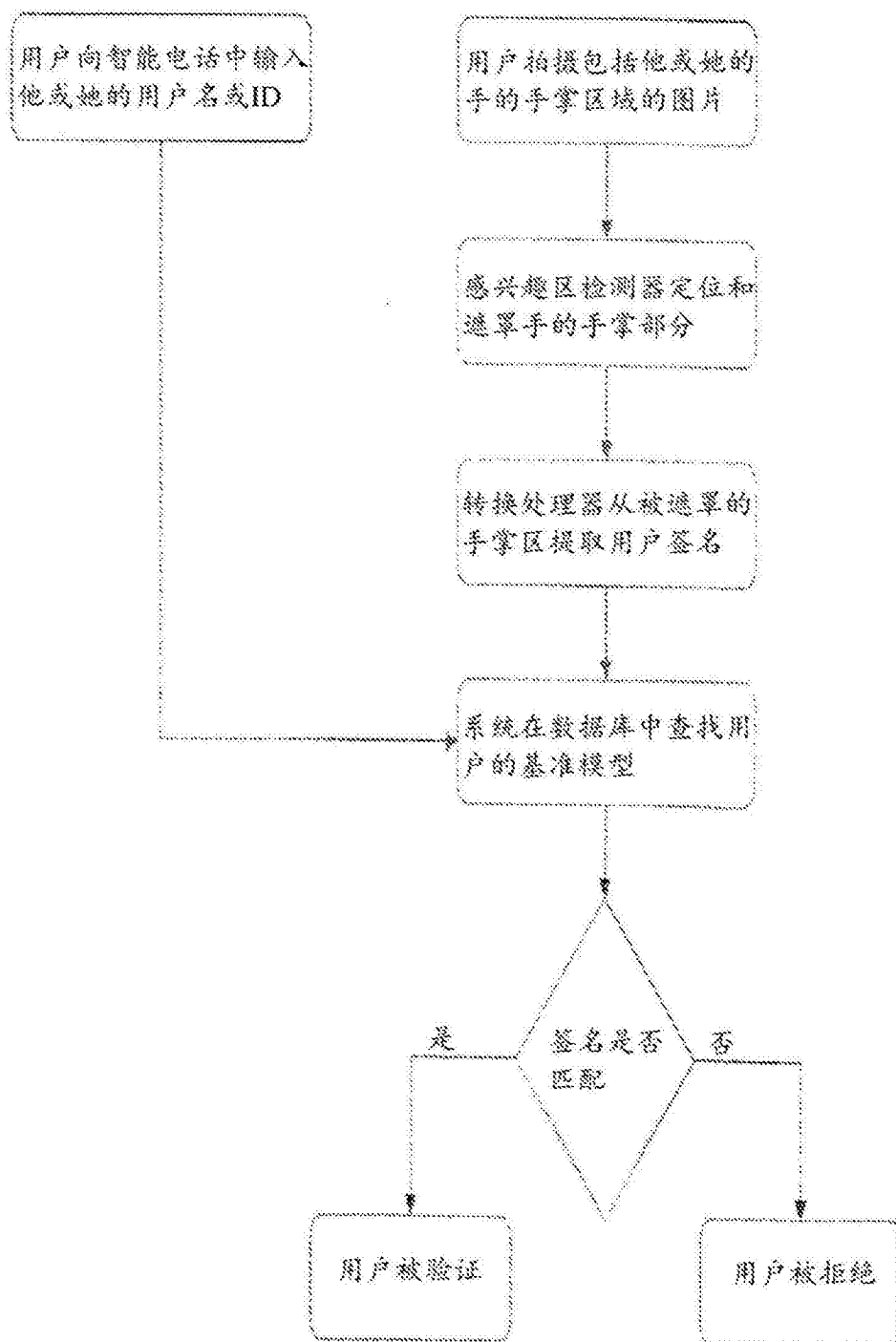


图4

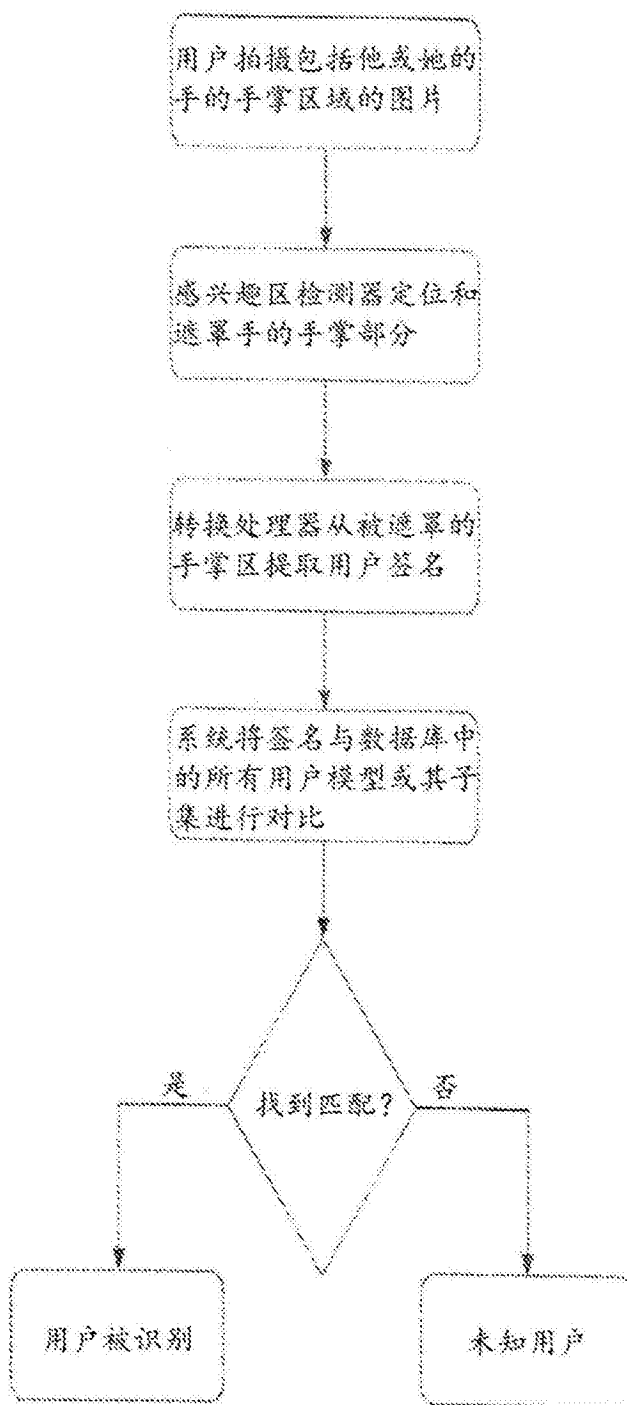


图5