(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 112861082 A
(43)申请公布日 2021.05.28

(21)申请号 202011347540.9

(22)申请日 2020.11.26

(30)优先权数据
16/697,364 2019.11.27 US

(71)申请人 密歇根州立大学董事会
地址 美国密歇根州
申请人 福特全球技术公司

(72)发明人 阿伦·罗什 阿尼尔·K·贾恩
德巴扬·德布
夸库·O·普拉卡-阿桑特
克里希纳斯瓦米·文卡塔斯·普拉萨德

(74)专利代理机构 北京允天律师事务所 11697
代理人 高源 李建航

(51)Int.Cl.
G06F 21/31(2013.01)
G06K 9/62(2006.01)

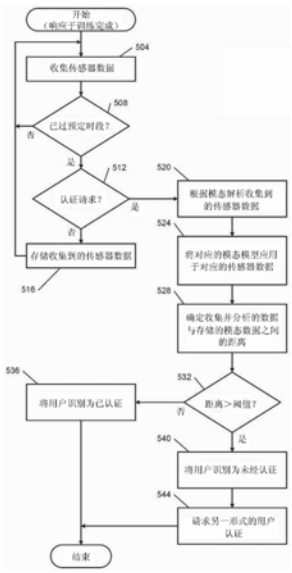
权利要求书3页 说明书11页 附图7页

(54)发明名称

用于被动认证的集成系统和方法

(57)摘要

一种被动认证方法，包括：响应于从第一用户接收到请求的动作，获得一组传感器数据和将该组传感器数据中的第一传感器数据分类成一组模态中的第一模态。该方法包括：针对该组模态中的第一模态，通过将第一模态模型应用于第一传感器数据来确定距离值和将该距离值与第一用户的针对第一模态的第一验证值进行比较。该方法包括：基于上述比较来确定该距离值的第一认证决定。该方法包括：响应于第一认证决定指示第一传感器数据对应于第一用户，来执行请求的动作。



CN 112861082 A

1.一种被动认证方法,包括:

响应于从第一用户接收到请求的动作:

获得一组传感器数据;

将所述一组传感器数据中的第一传感器数据分类成一组模态中的第一模态;

针对所述一组模态中的所述第一模态:

通过将第一模态模型应用于所述第一传感器数据来确定距离值;

将所述距离值与所述第一用户的针对所述第一模态的第一验证值进行比较;

基于所述比较,来确定所述距离值的第一认证决定;以及

响应于所述第一认证决定指示所述第一传感器数据对应于所述第一用户,来执行所述请求的动作。

2.根据权利要求1所述的被动认证方法,其中,所述第一用户的针对所述第一模态的所述第一验证值被存储在距离数据库中,其中,所述距离数据库包括所述第一用户的针对所述一组模态中的每个模态的相应验证值。

3.根据权利要求1所述的被动认证方法,还包括:

响应于所述第一认证决定指示所述第一传感器数据不对应于所述第一用户,来请求附加的认证决定。

4.根据权利要求3所述的被动认证方法,其中,所述附加的认证决定包括请求密码或生物特征数据。

5.根据权利要求1所述的被动认证方法,其中,将所述距离值与所述第一用户的针对所述第一模态的所述第一验证值进行比较包括:

确定在所述距离值与所述第一用户的所述第一验证值之间的差。

6.根据权利要求5所述的被动认证方法,还包括:

获得与所述第一模态对应的第一阈值;以及

响应于所述差小于所述第一阈值,来将所述一组传感器数据认证为所述第一用户。

7.根据权利要求1所述的被动认证方法,还包括:

针对所述一组模态中的每个模态确定一组认证决定的加权组合,所述一组认证决定包括所述第一认证决定;以及

响应于所述一组认证决定中的每个认证决定指示相应传感器数据对应于所述第一用户,来执行所述请求的动作。

8.根据权利要求1所述的被动认证方法,还包括:

在预定训练时段内,确定所述第一用户的针对所述一组模态中的每个模态的一组验证值。

9.一种用于第一用户设备的被动认证系统,包括:

至少一个处理器;以及

耦接至所述至少一个处理器的存储器,

其中,所述存储器存储:

距离数据库,其包括第一用户的针对一组模态中的每个模态的验证值;以及

用于由所述至少一个处理器执行的指令,并且

其中,所述指令包括:响应于接收到请求的动作,

获得一组传感器数据；

将所述一组传感器数据中的第一传感器数据分类成一组模态中的第一模态；

针对所述一组模态中的所述第一模态：

通过将第一模态模型应用于所述第一传感器数据来确定配对的样本数据；

将所述配对的样本数据与存储在所述距离数据库中的所述第一用户的针对所述第一模态的所述验证值进行比较；

基于所述比较，来确定所述配对的样本数据的第一认证决定；以及

响应于所述第一认证决定指示所述第一传感器数据对应于所述第一用户，来执行所述请求的动作。

10.根据权利要求9所述的被动认证系统，其中，所述指令包括：

响应于所述第一认证决定指示所述第一传感器数据不对应于所述第一用户，来请求附加的认证决定。

11.根据权利要求10所述的被动认证系统，其中，所述附加的认证决定包括请求密码或生物特征数据。

12.根据权利要求9所述的被动认证系统，其中，将所述配对的样本数据与存储在所述距离数据库中的所述第一用户的针对所述第一模态的所述验证值进行比较包括：

确定在所述配对的样本数据与存储在所述距离数据库中的所述第一用户的所述验证值之间的距离。

13.根据权利要求12所述的被动认证系统，其中，所述指令包括：

获得与所述第一模态对应的第一阈值；以及

响应于所述距离小于所述第一阈值，来将所述一组传感器数据认证为所述第一用户。

14.根据权利要求13所述的被动认证系统，其中，所述指令包括：响应于所述距离大于所述第一阈值，

锁定所述第一用户设备；以及

拒绝执行所述请求的动作，其中，所述请求的动作为访问车辆或乘车共享服务。

15.根据权利要求9所述的被动认证系统，其中，所述指令包括：

针对所述一组模态中的每个模态确定一组认证决定，所述一组认证决定包括所述第一认证决定；以及

响应于所述一组认证决定中的每个认证决定指示相应传感器数据对应于所述第一用户，来执行所述请求的动作。

16.根据权利要求9所述的被动认证系统，其中，所述第一模态模型包括两个堆叠的长短期记忆架构，其中，所述两个堆叠的长短期记忆架构是使用训练数据集预先训练的。

17.根据权利要求9所述的被动认证系统，其中，所述指令包括：

在预定训练时段内，确定所述第一用户的针对所述一组模态中的每个模态的一组验证值。

18.根据权利要求17所述的被动认证系统，其中，确定所述第一用户的针对所述一组模态中的每个模态的所述一组验证值包括：

在预定训练时段内从一组传感器获得微调数据集；

根据所述一组模态对所述微调数据集的数据进行分类；

使用相应的分类数据训练每个相应的模态模型;以及

确定所述第一用户的针对所述一组模态中的每个模态的所述一组验证值作为每个相应的模态模型的输出。

19.根据权利要求9所述的被动认证系统,还包括多个传感器,其中,所述一组传感器数据从所述多个传感器获得。

20.一种用于第一用户设备的被动认证系统,包括:

多个传感器;

至少一个处理器;以及

耦接至所述至少一个处理器的存储器,

其中,所述存储器存储:

距离数据库,其包括第一用户的针对一组模态中的每个模态的验证值;

阈值数据库,其包括用于所述一组模态的加权组合的阈值;以及

用于由所述至少一个处理器执行的指令,并且

其中,所述指令包括:响应于接收到请求的动作,

从所述多个传感器获得一组传感器数据;

将所述一组传感器数据中的第一传感器数据分类成所述一组模态中的第一模态;

针对所述一组模态中的所述第一模态:

通过将第一模态模型应用于所述第一传感器数据来确定配对的样本数据;

获得存储在所述距离数据库中的所述第一用户的针对所述第一模态的第一验证值;

确定所述配对的样本数据与所述验证值之间的距离;

获得存储在所述阈值数据库中的针对所述第一模态的第一阈值;以及

响应于所述距离小于所述第一阈值,来执行所述请求的动作。

用于被动认证的集成系统和方法

技术领域

[0001] 本公开内容涉及用户认证方法，并且更具体地涉及使用移动计算设备的被动认证方法。

背景技术

[0002] 智能手机上普遍流行的用户认证方案依赖于明确的用户交互，在该用户交互中用户键入密码或者呈现诸如面部、指纹或虹膜的生物特征提示。这种认证机制除了对用户来说麻烦和突兀之外还可能造成安全问题和隐私问题。

[0003] 此处提供的背景技术描述是出于总体上呈现本公开内容的上下文的目的。在该背景技术部分中描述的范围内，当前指定的发明人的工作以及在提交时可能未以其他方式作为现有技术的描述的各方面均未明确地或隐含地被承认为相对于本公开内容的现有技术。

发明内容

[0004] 一种被动认证方法包括：响应于从第一用户接收到请求的动作，获得一组传感器数据；以及将所述一组传感器数据中的第一传感器数据分类成一组模态中的第一模态。该方法包括：针对所述一组模态中的第一模态，通过将第一模态模型应用于第一传感器数据来确定距离值；以及将所述距离值与第一用户的针对第一模态的第一验证值进行比较。该方法包括：基于所述比较，来确定所述距离值的第一认证决定。该方法包括：响应于第一认证决定指示第一传感器数据对应于第一用户，来执行请求的动作。

[0005] 在其他方面，第一用户的针对第一模态的第一验证值被存储在距离数据库中，并且距离数据库包括第一用户的针对所述一组模态中的每个模态的相应验证值。在其他方面，该方法包括：响应于第一认证决定指示第一传感器数据不对应于第一用户，来请求附加的认证决定。在其他方面，附加的认证决定包括请求密码或生物特征数据。

[0006] 在其他方面，将距离值与第一用户的针对第一模态的第一验证值进行比较包括：确定在所述距离值与第一用户的第一验证值之间的差。在其他方面，该方法包括：获得与第一模态对应的第一阈值；以及响应于所述差小于第一阈值，来将所述一组传感器数据认证为第一用户。

[0007] 在其他方面，该方法包括：针对所述一组模态中的每个模态确定一组认证决定的加权组合，所述一组认证决定包括所述第一认证决定。在其他方面，该方法包括：响应于所述一组认证决定中的每个认证决定指示相应传感器数据对应于第一用户，来执行请求的动作。在其他方面，该方法包括：在预定训练时段内，确定第一用户的针对所述一组模态中的每个模态的一组验证值。

[0008] 一种用于第一用户设备的被动认证系统，包括：至少一个处理器，以及耦接至所述至少一个处理器的存储器。存储器存储：距离数据库，其包括第一用户的针对所述一组模态中的每个模态的验证值；以及指令，其用于由所述至少一个处理器执行。所述指令包括：响应于接收到请求的动作，获得一组传感器数据；以及将所述一组传感器数据中的第一传感

器数据分类成所述一组模态中的第一模态。所述指令包括:针对所述一组模态中的第一模态,通过将第一模态模型应用于第一传感器数据来确定配对的样本数据;以及将配对的样本数据与存储在距离数据库中的第一用户的针对第一模态的验证值进行比较。所述指令包括:基于所述比较,来确定配对的样本数据的第一认证决定。所述指令包括:响应于第一认证决定指示第一传感器数据对应于第一用户,来执行请求的动作。

[0009] 在其他方面,指令包括:响应于第一认证决定指示第一传感器数据不对应于第一用户,来请求附加的认证决定。在其他方面,附加的认证决定包括请求密码或生物特征数据。在其他方面,将配对的样本数据与存储在距离数据库中的第一用户的针对第一模态的验证值进行比较包括:确定在配对的样本数据与存储在距离数据库中的第一用户的验证值之间的距离。

[0010] 在其他方面,指令包括:获得与第一模态对应的第一阈值,以及响应于所述距离小于第一阈值,来将所述一组传感器数据认证为第一用户。在其他方面,指令包括:响应于所述距离大于第一阈值,锁定第一用户设备;以及拒绝执行请求的动作。请求的动作为访问车辆或乘车共享服务。

[0011] 在其他方面,所述指令包括:针对所述一组模态中的每个模态确定一组认证决定,所述一组认证决定包括第一认证决定;以及响应于所述一组认证决定中的每个认证决定指示相应传感器数据对应于第一用户,来执行请求的动作。

[0012] 在其他方面,第一模态模型包括两个堆叠的长短期记忆架构,其中,所述两个堆叠的长短期记忆架构是使用训练数据集预先训练的。在其他方面,所述指令包括:在预定训练时段内,确定第一用户的针对所述一组模态中的每个模态的一组验证值。

[0013] 在其他方面,确定第一用户的针对所述一组模态中的每个模态的一组验证值包括:在预定训练时段内从一组传感器获得微调数据集;根据所述一组模态对微调数据集的数据进行分类;使用相应的分类数据训练每个相应的模态模型;以及确定第一用户的针对所述一组模态中的每个模态的所述一组验证值作为每个相应模态模型的输出。在其他方面,该系统包括多个传感器。在其他方面,所述一组传感器数据从多个传感器获得。

[0014] 一种用于第一用户设备的被动认证系统,包括:多个传感器;至少一个处理器;以及耦接至所述至少一个处理器的存储器。存储器存储:距离数据库,其包括第一用户的针对一组模态中的每个模态的验证值;阈值数据库,其包括用于所述一组模态的加权组合的阈值;以及指令,其用于由所述至少一个处理器执行。所述指令包括:响应于接收到请求的动作,从多个传感器获得一组传感器数据;以及将所述一组传感器数据中的第一传感器数据分类成所述一组模态中的第一模态。所述指令包括:针对所述一组模态中的第一模态,通过将第一模态模型应用于第一传感器数据来确定配对的样本数据;获得存储在距离数据库中的第一用户的针对第一模态的第一验证值;以及确定在配对的样本数据与验证值之间的距离。所述指令包括:获得存储在阈值数据库中的针对第一模态的第一阈值;以及响应于所述距离小于第一阈值,来执行请求的动作。

[0015] 根据详细的描述、权利要求书和附图,本公开内容的其他应用领域将变得明显。详细描述和特定示例仅旨在用于说明的目的,并且不旨在限制本公开内容的范围。

附图说明

[0016] 根据详细描述和附图将更加全面地理解本公开内容。

[0017] 图1是根据本公开内容的原理的被动认证系统的高级示例实施方式。

[0018] 图2是描绘示例用户设备的功能框图。

[0019] 图3是被动认证模块的示例实施方式的功能框图。

[0020] 图4是描绘被动认证系统的模态模型的训练的功能框图。

[0021] 图5是描绘通过被动认证应用的用户的示例认证的流程图。

[0022] 图6是描绘针对被动认证应用的特定用户的示例训练的流程图。

[0023] 图7是描绘被动认证应用的模态模型的示例更新的流程图。

[0024] 在附图中,附图标记可以被重复使用以标识相似和/或相同的元件。

具体实施方式

[0025] 被动认证系统通过利用来自用户的现有设备传感器的数据验证用户身份来对用户进行认证。在各种实现方式中,被动认证系统用于例如通过按压用户设备应用的按钮或者车辆或遥控器上的解锁按钮来在用户请求乘车共享服务或解锁其车辆时对用户进行非干扰性认证。被动认证系统可以通过以下来识别正在操作用户设备的用户的行为趋势或模态:利用来自现有用户设备传感器的数据,并且使用来自用户设备上的一组传感器的针对每个模态或传感器的一组训练数据来对暹罗长短期记忆(LSTM)机器学习模型进行训练。

[0026] 被动认证系统可以作为用户设备上的应用进行操作。在下载时,该应用可以在短的训练时段内执行简要的数据收集以获得与用户设备的真正所有者有关的个人化数据。在这种方式下,一旦请求被发出,用户就可以通过应用被动地进行认证。

[0027] 被动认证系统可以在对针对特定用户的多种模态(即,多种类型的传感器数据)进行训练的短的训练时段期间自动地学习特定用户的模态。然后,被动认证系统在用户请求解锁车辆或请求乘车服务时例如可以通过使用在用户设备的用户操作期间被动地获得的一组最新的用户收集数据来在所述请求之一期间对用户进行认证。被动认证系统可以实现为用户可以在其用户设备上下载的用户设备应用。被动认证应用可以在对针对特定用户的学习模块(暹罗LSTM)进行训练的最短时段之后收集并发送在预定时段期间收集到的来自一组传感器的一组用户设备数据,每个传感器对应于特定的模态。

[0028] 在各种实现方式中,被动认证系统可以在操作被动认证应用的同时连续地对用户进行认证。在其他实现方式中,被动认证系统可以仅响应于车辆的乘坐请求或解锁请求来对用户进行认证。由于被动认证系统连续地收集传感器数据,因此一旦请求了乘坐或者接收到车辆解锁请求,被动认证系统就可以利用当前收集到的传感器数据来验证用户设备的操作者。

[0029] 移动平台上的当前认证方案要求与用户设备进行显式用户交互称为显式认证(explicit authentication)以便获得对用户设备的访问。用于用户设备访问的进入点通常是密码或诸如面部、指纹、虹膜等的生物特征提示。密码和PIN长期以来被视为保护信息和控制对移动设备的访问的顶峰。然而,这些基于知识的认证方案易于受到社会工程学的黑客攻击、猜测、过肩攻击等。

[0030] 随着技术的最新发展,智能手机通过学习用户的诸如面部、指纹或虹膜的生物特

征可以更好地对用户进行认证，所述生物特征被认为是个人独有的。这些特征由于其独特性而被认为比基于知识的认证方案更可靠。缺点是，生物特征认证提出了与收集生物特征数据有关的隐私问题。另外，生物特征传感器级别的欺骗攻击、以及存储在用户设备内的生物特征模板可能被盗均在与基于生物特征的认证有关的日益严峻的问题中。

[0031] 尽管显式认证方案的使用很普遍，但是显式认证因为用户需要在使用用户设备之前主动地关注认证步骤因此既麻烦又突兀。此外，用户可能更喜欢设置简单的密码和弱密码，增加用于锁定时间的非活动时段，或者完全地禁用认证步骤。另外，虽然PIN码、密码和生物特征扫描非常适合于单次认证，但是当解锁手机时在由真正用户成功进行认证后就无法有效地检测入侵。

[0032] 替代地，本公开内容的被动认证系统通过频繁且不干扰地对用户与用户设备的交互进行监测来提供附加的安全层，从而解决了这些挑战。被动认证系统不需要任何明确的认证步骤。

[0033] 在各种实现方式中，被动认证系统可以从用户设备的多达30个不同的传感器收集数据以对用户进行被动地认证。在整个本公开内容中，具体讨论了八种模态，所述八种模态包括来自触摸屏传感器的击键动力学(键保持时间、手指区域和手指压力)、GPS位置、加速度计、陀螺仪手势、磁力计、重力传感器、线性加速度和旋转传感器。

[0034] 然而，可以包括附加的模态，例如应用使用(正在使用的用户设备应用的名称)、电池电量(剩余电池电量的百分比)、蓝牙连接(设备周围的蓝牙连接名称)、亮度水平(屏幕亮度水平)、基站塔连接(设备周围的基站塔名称)、文件读入/写出(从用户设备的磁盘读取或写入至用户设备的磁盘的文件)、扫视手势(用户扫视其用户设备)、来自摄像装置的用户的面部图像、心率传感器(用户的每分钟心率跳动)、湿度传感器(环境空气湿度百分比)、光传感器(环境光测量)、NFC连接(设备周围的NFC连接名称)、方向传感器(用户设备在X、Y和Z平面上的方向)、拾取手势(拾取用户设备)、气压计(大气压)、屏幕触摸传感器(触摸位置)、步数计数器(步行的步数)、步幅检测器(用户正在行走)、温度传感器(环境温度)、倾斜检测器(设备倾斜)、音量级别(由用户设置的音量级别)、唤醒手势(用户设备打开)和WiFi连接(WiFi连接名称)。

[0035] 被动认证系统实现了用于从与用户设备中的多个被动传感器对应的训练数据中提取深度时间特征的暹罗LSTM架构来进行用户认证。

[0036] 大多数被动认证研究都集中在用于认证的单一感测模态上。当认证时间窗口短时，在用户的用户设备上基于单个生物特征模态对用户进行认证变得非常具有挑战性。另外，给定用户所从事的任务、数据量和不同传感器模态的可用性也会变化。如本公开内容中所呈现的，鲁棒的被动认证方案必须能够使用利用多个用户设备传感器进行被动认证的多模态方法来适应于在人类智能电话或人类-用户设备交互中观察到的高用户内可变性。

[0037] 由于一种或几种模态的认证准确性降低，因此融合来自多种模态的决定来对用户进行认证已经被证明是非常有用的。大多数的多模态生物特征识别系统基于最小、最大或总和规则在分数级别融合分类器。被动认证系统采用分数总和融合技术，已经显示了该分数总和融合技术与其他融合方案相比在多模态生物识别系统中表现良好。被动认证系统实现了暹罗LSTM网络以解决时间依赖性。

[0038] 参照图1，示出了被动认证系统100的高级示例实现方式。被动认证系统100对用户

设备104例如智能电话或其他移动计算设备的用户或所有者进行认证。用户设备104可以经由因特网112针对认证请求系统108验证用户的身份。例如，认证请求系统108可以是：响应于乘车请求而请求用户认证的乘车共享服务；响应于接收到解锁请求或其他车辆操作请求等而请求用户认证的车辆控制单元。

[0039] 被动认证系统100包括应用数据库116和用户数据存储数据库120。应用数据库116存储具有预先训练的认证模型的被动认证应用，所述预先训练的认证模型针对使用训练传感器数据或训练数据集训练的一组模态。

[0040] 用户可以在用户设备104上从应用数据库116下载具有预先训练的模型的被动认证应用。被动认证应用在下载之后可以通过各种屏幕提示指示用户根据由用户对用户设备104的唯一使用来更新或调整预先训练的模型。如图2中更详细示出的，一旦针对特定用户进行了训练，被动认证应用就从存在于用户设备104上的多个传感器收集传感器数据，并且连续地或者响应于来自认证请求系统108的特定提示来进行操作以对用户进行认证。

[0041] 用户数据存储数据库120在用户设备104上存储由被动认证模块收集的各种用户数据。被动认证模块以预定的间隔经由因特网112将收集到的数据上传至用户数据存储数据库120。在各种实现方式中，用户数据存储数据库120从被动认证系统100中排除，并且在预定时段内仅传感器数据的子集被收集并且被存储在用户设备104上。另外，在其他实现方式中，被动认证系统100可以将预先训练的模型存储在远离用户设备104的服务器上，从而引起被动认证应用在经由因特网108接收到一组认证数据之后在远程服务器上对用户进行认证，并且将认证数据转发至认证请求系统108。

[0042] 在离线阶段中，针对每种模态训练预先训练的模型。在部署期间，连续地对来自用户设备传感器模态的输入数据进行监测。如果输入数据成功地通过认证标准，则做出当前用户确实是用户设备的合法所有者的决定。如果输入数据未通过认证标准，则被动认证系统100将用户从用户设备锁定并且提供明确的认证方法例如密码或者诸如指纹扫描的生物特征。

[0043] 在示例实现方式中，用于针对每个模态预先训练认证模型的训练数据集可以包括来自对于一组用户最常用的用户设备中当前存在的多达30个传感器的测量，例如一组30个或更多个用户。可以在15天的时段中收集针对每个用户的数据。为了连续地收集数据，被动认证应用在用户设备启动时自动打开并且在后台连续运行的同时被动地记录传感器数据。为了收集击键动态，可以从应用数据库116下载自定义的软键盘。自定义的软键盘也可以被实现为目标应用例如乘车请求或乘车共享应用的一部分。

[0044] 被动认证系统100的优点在于：不需要用户与数据收集应用进行交互，从而使用户能够如同通常在他们的日常生活中那样使用他们的用户设备。也可以连续地获取针对模态的数据，即使在用户没有主动地与他们的用户设备进行交互时也是如此。

[0045] 现在参照图2，示出了描绘示例用户设备104的功能框图。用户设备104包括操作系统204和多个传感器。多个传感器包括击键传感器208、GPS位置传感器212、加速度计216、陀螺仪传感器220、磁力计224、重力传感器228、线性加速度计232和旋转传感器236。如上所述，多个传感器不限于图2所示的传感器。

[0046] 击键传感器208可以确定键保持时间、手指面积和手指压力。GPS位置传感器212可以确定用户的GPS位置，所述位置包括纬度和经度。加速度计216可以确定用户设备在X、Y和

Z平面中的加速度。陀螺仪传感器220可以确定用户设备在X、Y和Z平面中的旋转速率。磁力计224可以确定在X、Y和Z平面中的地球磁场。重力传感器228可以确定重力的方向和大小。线性加速度计232可以确定在X、Y和Z平面中的线性加速度。旋转传感器236可以确定用户设备在X、Y和Z平面中的旋转。

[0047] 如先前所提及，多个传感器目前在所有智能手机和智能手表中是可用的，从而使得被动认证应用240能够在不需要安装附加的传感器硬件的情况下收集传感器数据。被动认证应用240包括唯一的用户接口244、数据收集模块248和被动认证模块252。用户接口244为特定的数据收集提供提示，以根据由用户对用户设备104的唯一使用来更新被动认证模块252的预先训练的模型。

[0048] 在各种实现方式中，被动认证模块252从数据收集模块248直接地接收数据以用于认证。附加地或替选地，被动认证模块252经由操作系统204从本地存储装置256接收数据以用于认证，或者经由操作系统204和收发器260从用户数据存储数据库120接收数据以用于认证。

[0049] 数据收集模块248经由操作系统204从多个传感器接收传感器数据。数据收集模块248在预定时段内指导传感器数据的收集并且使用针对多个模态的一组收集到的数据经由操作系统204更新本地存储装置256。对于由数据收集模块248在预定时段内收集的每组数据，数据收集模块248可以替换本地存储装置256中包括的先前存储的数据集。在各种实现方式中，本地存储装置256可以在一组时间例如最近24小时内存储数据。在其他实现方式中，可以经由用户设备104的收发器260将针对多个用户设备的传感器数据远程地存储在用户数据存储数据库120中。

[0050] 击键传感器208通过对用户的键入节奏和习惯进行建模来进行操作，这可以用于对用户设备的用户进行认证。每当用户在他们的用户设备104上键入字符时，数据收集模块248就可以收集并且记录手指压力、手指面积和保持时间。键入的确切字符不会被记录，因此收集到的击键模态是非侵入性质的。

[0051] 对于用户设备的用户，每当用户设备104移动时，数据收集模块248就从GPS位置传感器212收集并记录纬度坐标和经度坐标的对。位置被认为是个人特征的测量，因此可以在用户的日常位置中找到可区分的模态。

[0052] 被动认证应用240还考虑了移动。数据收集模块248使用六个附加的传感器(加速度计216、陀螺仪传感器220、磁力计224、重力传感器228、线性加速度计232和旋转传感器236)收集并记录运动。对于所有的六个传感器，在三个轴X、Y和Z上记录测量。由于用户行为的高度可变性，因此可以呈现在测量上的用户内时间间隔(chronological gap)，例如，他们可能关闭他们的用户设备或者可能由于电池电量耗尽而关闭用户设备。这些间隔由使用LSTM架构生成的模型解决。

[0053] 可以实现用于被动认证的两种方法：(i)在线方法和(ii)离线方法(如先前所提及)。在线方法在部署模型之前会在一段时段内使用与用户有关的样本来训练认证模型。在线方法的主要限制涉及训练针对每个用户的单独的模型。因此，对遍及所有用户的整体认证性能进行准确地评价由于高变化而具有挑战性。另外，所需的数据量、模型部署之前的数据收集持续时间以及存储训练数据的隐私问题仍是持续存在的挑战。

[0054] 另一方面，离线方法训练了一种通用的认证模型，该模型学习了针对各个模态的

显著表现。在这种方法下，当用户安装应用时将部署相同的训练模型。此外，用户可以在安装应用后立即利用认证机制。

[0055] 被动认证应用240可以实现两种方法的组合，采用离线学习策略用于被动认证，所述被动认证在将被动认证应用240下载至用户设备104后具有微调阶段。在微调阶段期间，被动认证应用240经由用户接口244提示用户遵照一组使用说明，以根据用户使用或处理用户设备104的精确方式方法来准确地更新预先训练的模型。

[0056] 在下载之前，针对八个模态中的每个模态训练暹罗LSTM网络以学习深度时间特征。来自用户的训练样本被转换成通过暹罗网络学习的嵌入空间。因此，在部署期间，仅需要从输入数据中提取特征以用于认证，从而消除了在每个用户设备上存储隐私数据的需求。然后，可以根据下载被动认证应用的用户(例如，用户设备的所有者)来使针对每个模态的预先训练的模型个人化或定制针对每个模态的预先训练的模型。在各种实现方式中，被动认证应用可以具有用于用户设备的多个用户的多种账户，从而使得用户设备能够针对每个用户使模型个人化并且对每个用户进行认证。

[0057] 现在参照图3，示出了被动认证模块252的示例实现方式的功能框图。如先前所提及，被动认证模块252可以从用户设备的本地存储装置或用户设备上的被动认证应用接收传感器数据以进行认证。在各种实现方式中，被动认证模块252从远程存储装置位置接收传感器数据以进行认证。

[0058] 输入解析模块304接收传感器数据以用于个人化训练或认证。如前所述，一旦被动认证应用被下载至用户设备上，被动认证应用就可以根据用户的具体使用来更新被动认证模块252的预先训练的模型。被动认证应用可以通过一系列操作来指导用户，以使针对每种模态的预模型个人化。

[0059] 如果输入解析模块304确定用户数据是用于训练或微调模型的，则将传感器数据转发至模态选择模块308。如前所指示，针对每个模态(例如，击键、位置等)(使用训练数据集并且针对每个用户进行更新)生成模型。被动认证模块252仅描绘了第一模态。然而，如所描述的，被动认证模块252将实现和组合例如八个不同的模态，并且可以使用更少数目或更多数目的模态。

[0060] 模态选择模块308分离出传感器数据的每个模态并且将传感器数据转发至对应的模态模块，例如，第一模态模块312(例如，击键)。另外，用户可以根据用户在隐私方面的偏好而选择退出经由某些模态的认证。模态选择模块通过在给定用户偏好的情况下选择所有可用模态的最佳组合来帮助维持高的认证准确性。

[0061] 第一模态模块312包括实现了LSTM架构的第一模态模型316，以根据用户的传感器数据生成第一模态模型316，以便使模型个人化(微调阶段)。第一模态模型316通过一组训练数据进行预先训练，以通过分类并确定输入传感器数据的距离值来学习识别或认证用户。例如，第一模态模型316可以分析传感器数据输入并且计算每个输入的距离值，以在微调阶段期间表示经验证的用户。然后，在认证期间，可以基于当前分析的传感器数据与经验证的用户的先前距离值之间的距离(例如，差)对用户进行认证。例如，如果距离超过阈值，则不会对用户进行认证。在各种实现方式中，第一模态映射数据库(first modality map database)320可以被包括在第一模态模块312中以存储用户设备的用户的经验证的距离值。

[0062] 在已经实现了第一模态模块312以确定用户的表示之后，可以使用被动认证模块252来对用户进行认证。当接收到认证请求时，最新的一组传感器数据被转发至被动认证模块252以用于认证。输入解析模块304基于包括已接收到认证请求的指示的传感器数据输入来确定传感器数据正在被转发以进行认证。然后，传感器数据被转发至被动认证模块252的模型应用模块324。模型应用模块324获得第一模态模型316并且将第一模态模型316应用于传感器数据，以进行分类并且确定传感器数据的距离值。在各种实现方式中，传感器数据可以被直接地转发至第一模态模型316以对传感器数据进行分类。

[0063] 模型应用模块324还可以将已知存储的用户距离数据(存储在第一模态映射数据库320中)与当前接收的传感器数据进行比较。然后，真实用户的第一模态映射数据库320的已知映射距离与确定的传感器数据的距离之间的相似性或距离被转发至认证确定模块328以用于比较。认证确定模块328可以包括预定阈值或者可以访问可选的动态阈值数据库332，以将真实用户的已知距离与传感器数据的确定距离之间的当前距离与动态阈值进行比较。

[0064] 如果阈值是动态的，则将被执行的每个认证合并至第一模态模型316中并且由阈值调整模块336根据连续更新的第一模态映射数据库320调整相应的阈值。只要确定的传感器数据的距离不超过阈值，则用户已经被认证。然而，如果距离超过阈值，则无法对用户进行认证，并且可以向用户呈现其他的认证方案例如密码或者面部或指纹的生物特征扫描以用于显式认证。

[0065] 该确定被转发至被动认证应用的用户接口以及认证请求系统以执行所请求的功能(诸如解锁或请求乘车)。在各种实现方式中，每个认证请求可以根据经认证的用户的平均距离或位置来更新阈值。附加地或替选地，每个认证还可以更新第一模态模型312。将每个模态模型应用于相应的传感器数据，并且针对每个模态将传感器数据与已知用户数据之间的差异转发至认证确定模块328。在各种实现方式中，每个模态模块具有单独确定的阈值，并且对于要进行认证的用户，针对其获得传感器数据的每个模态必须被验证或超过相应的阈值。替选地，可能需要验证模态的子集，或者至少相应的差异必须在阈值的预定范围内。

[0066] 参照图4，示出了描绘模态模型的训练的功能框图。第一模态模型312在数据采样模块404处接收训练数据集。包括在该训练数据集中的是指示提交至第一模态模型312的训练数据集中的每对是否都是匹配对(同一用户)或不同的用户。

[0067] 假设我们提取针对给定传感器模态的D维数据样本(例如，加速度计具有在3个轴即X、Y和Z上的数据)。针对每个用户的样本数目可以不同。可以由数据采样模块404通过在具有T移位的预先定义的移位的连续数据上移动固定大小T(认证时间窗口)的窗口来分割训练数据集，并且构建交叠的固定大小的片段。因此，对于每个用户，D×T段集包括在训练数据集中。然后，将这些段传递至预处理模块。一对分段(两个输入)被转发至预处理模块408。

[0068] 采样模块的输出包括来自其原始域即时域中的模态的测量。频域可以处理并消除噪声，同时还可以在顺序数据内的数据中保留区分模态。预处理模块408仅针对运动传感器——即，加速度计、陀螺仪、磁力计、线性加速度计、重力和旋转——将测量从时域映射至频域。使用快速傅立叶变换(FFT)用于将在每个特征维上的时域信号转换成频域信号。FFT

向量的输出在时域中与样本连接在一起，以使用来自两个域的信息。然后，该对的第一数据样本被转发至第一LSTM 412，并且该对的第二数据样本被转发至第二LSTM 416。

[0069] 被动认证模块旨在针对每个模态获得高度区分性的特征，所述特征可以使用经指导的学习将样本从真实用户与冒名顶替者用户区分开。换言之，被动认证模块想要学习数据从模态到嵌入空间的信息丰富转换，所述嵌入空间可以保留训练样本之间的距离关系。

[0070] 假设一对输入样本$\{X_i, X_j\}$被输入至第一模态模型312中。假设y_{ij}为包括在训练数据集中的标签，所述标签被转发至距离调节模块420，使得如果X_i和X_j属于同一用户，则$y_{ij}=0$，以及如果X_i和X_j不属于同一用户，则$y_{ij}=1$。将输入样本映射至嵌入空间(例如，存储在第一模态映射数据库320中)，在该嵌入空间中，来自同一用户的两个样本距离较近，而来自不同用户的两个样本相距较远。暹罗网络架构(第一LSTM 412和第二LSTM 416)非常适合这种验证任务，所述暹罗网络架构是由两个相同的子网络组成的神经网络架构。以这种方式，可以学习两个输入样本之间的关系。在暹罗网络中，两个子网络之间的权重是共享的，并且权重基于标签y_{ij}进行更新。先前曾提出暹罗卷积神经网络(CNN)以用于被动认证，然而，CNN不太适合于捕获样本内的时间依赖性。

[0071] 相反，LSTM——递归神经网络(RNN)的变型——被设计用于对时间序列数据进行分类、处理和预测。在被动认证模块中，针对每个模态模型堆叠两个LSTM以便学习时间序列数据的分层表示。第一LSTM 412输出向量$h_1^1, \ldots, h_T^1$的序列，然后将它们作为输入馈送至第二LSTM416。第二LSTM 416的最后的隐藏状态h_T^2代表由$f_\theta(\bullet)$表示的最终非线性嵌入，其中θ表示暹罗LSTM网络的参数。隐藏层的这种层次使得能够更显著地表示时间序列数据。为了训练暹罗LSTM网络，在距离调节模块420中限定并且实现了成对的对比损失函数。

[0072] 对于给定的一对输入样本，将来自两个子网络的两个输出特征向量之间的欧几里德(Euclidean)距离馈送至距离调节模块420，该距离调节模块还接收指示两个输入是否来自同一用户或不同用户的标签，并且应用对比损失函数。该损失函数根据与该对样本相关联的标签y_{ij}来调节长距离或短距离。以这种方式，两对之间的欧几里德距离$d_\theta(Xi, Xj)$对于真正对是小的，而对于冒名顶替者对是大的，其中$d_\theta(X_i, X_j) = ||f_\theta(X_i) - f_\theta(X_j)||_2$。对比损失函数限定为：$l_\theta = \sum_{i,j=1}^{N} L_\theta(X_i, X_j, y_{ij})$，其中，$L_\theta = (1-y_{ij})\frac{1}{2}(d_\theta)^2 + (y_{ij})\frac{1}{2}\{\max(0, \alpha - d_\theta)\}^2$，其中，α＞0称为余量。如图3所述，距离调节模块420可以将已知距离存储在第一模态映射数据库320中并且进行访问以用于比较来呈现用于认证的传感器数据。

[0073] 参照图5，示出了描绘通过被动认证应用的用户的示例认证的流程图。控制响应于被动认证应用的训练完成而开始。在504处，控制收集传感器数据。控制进行至508以确定是否已过预定时段。如果未过预定时段，则控制返回至504以继续收集传感器数据。如果已过预定时段，则控制进行至512以确定是否已经请求认证。例如，可以响应于用户请求乘坐或者用户请求解锁车辆或启动车辆的发动机而请求认证。

[0074] 如果尚未请求认证，则控制继续至516以存储收集到的传感器数据。如前所述，在预定时段内收集的传感器数据可以本地存储在用户设备上或者在被动认证应用内，或者远程地存储在服务器上。一旦收集到的数据被存储，控制就返回至504以收集另一组数据。在各种实现方式中，在516处，收集到的传感器数据替换先前存储的传感器数据。

[0075] 返回至512，如果请求认证，则控制进行至520，以解析收集到的传感器数据并且根

据模态——例如，该数据是用于击键确定还是位置确定——对数据进行分类。然后，控制继续至524，以将对应的模态模型应用于传感器数据的每个对应部分，来使用训练后的模态模型识别传感器数据是否被认证为用户。

[0076] 控制继续至528，以确定收集并分析的数据与存储的模态数据之间的距离或差异。控制继续至532，以确定该距离是否大于预定阈值。如果该距离不大于预定阈值，则控制进行至536以将用户识别为已认证。然后，控制结束。如果该距离大于预定阈值，则控制进行至540以将用户识别为未经认证。然后，控制进行至544，以请求另一形式的用户认证。

[0077] 例如，认证的附加形式可以是在确认乘坐请求或车辆被解锁之后在用户设备上或在车辆处的诸如密码、PIN、生物特征数据等的显式认证。在各种实现方式中，如果用户未被认证，则控制可以在用户设备处请求显式认证，以便执行请求(例如，乘坐或解锁车辆)并且可以在乘坐或车辆处请求其他形式的认证，以提高安全性。然后，控制结束。

[0078] 参照图6，示出了描绘针对被动认证应用的特定用户的示例微调(训练)的流程图。控制响应于下载被动认证应用而开始。控制进行至604，以经由用户设备的用户接口向用户提示训练指令。例如，训练指令可以包括用于在短和/或预定时间段内移动或使用用户设备的指导。控制继续至608，以从用户设备的多个传感器收集传感器数据。然后，控制进行至612，以确定是否已过预定时段。如果未过预定时段，则控制返回至604，以继续向用户提示用于预定训练时段的训练指令。如果已过预定时段，则控制进行至616，以根据模态类型解析收集到的传感器数据。然后，控制继续至620，以将解析的传感器数据转发至相应的模态模型，所述模态模型被训练以识别当前的传感器数据是否是经验证的用户设备的所有者。在图7中更详细地描述，在624处，控制使用在训练期间收集的传感器数据训练每个模态模型。

[0079] 参照图7，示出了描绘被动认证应用的模态模型的示例训练的流程图。控制在704处开始，以对转发的传感器数据进行采样。控制继续至708，以选择第一对采样的传感器数据。然后，控制继续至712，以确定第一对采样的传感器数据是否包括运动数据，例如，加速度计传感器数据。如果第一对采样的传感器数据包括运动数据，则控制继续至716以将传感器数据从时域信号转换成频域信号。

[0080] 然后，控制继续至720，以连接时域信号和转换的频域信号，并且进行至724。返回至712，如果传感器数据不包括运动传感器数据，则控制进行至724。在724处，控制将所选对的第一输入数据和第二输入数据转发至一组两个堆叠的暹罗LSTM架构中。控制继续至728，以确定两个暹罗LSTM架构的输出之间的距离。在732处，控制获得包括在原始转发的传感器数据中的标签，如果这是训练数据，则所述标签指示该数据是来自同一用户或是来自不同用户。

[0081] 在736处，控制基于标签调节两个暹罗LSTM输出之间的距离；即，如果两个原始输入来自同一用户，则控制确保距离较小；以及如果两个原始输入来自不同用户，则控制确保距离较大。该方法也用于模型的预先训练。然后，控制进行至740，以存储经调节的距离。在744处，控制确定在采样的传感器数据中是否包括附加的数据。如果在采样的传感器数据中不包括附加的数据，则控制结束。如果在采样的传感器数据中包括附加的数据，则控制进行至748以选择下一对，并且返回至712以用于附加的处理。

[0082] 为了说明和描述的目的，已经提供了实施方式的前述描述。其并非旨在穷举或限

制本公开内容。特定实施方式的各个元件或特征通常不限于该特定实施方式，而是在适用的情况下是可互换的，并且即使未具体示出或描述也可以在所选实施方式中使用。同样也可以以许多方式变化。这样的变型不应被认为是背离本公开内容，并且所有这样的修改旨在被包括在本公开内容的范围内。

[0083] 术语“模块”或术语“控制器”可用术语“电路”替换。术语“模块”可以指代一部分或包括：专用集成电路(ASIC)；数字、模拟或模拟/数字混合离散电路；数字、模拟或模拟/数字混合集成电路；组合的逻辑电路；现场可编程的门阵列(FPGA)；执行代码的处理器电路(共享、专用或组)；存储由处理器电路执行的代码的存储电路(共享、专用或组)；提供上述功能的其他合适的硬件组件；或诸如片上系统中的上述某些或全部的组合。尽管已经公开了各种实施方式，但是可以采用其他变型。所有的组件和功能可以以各种组合互换。所附权利要求书旨在覆盖落入本发明的真正精神内的相对于所公开的实施方式的这些和任何其他变型。

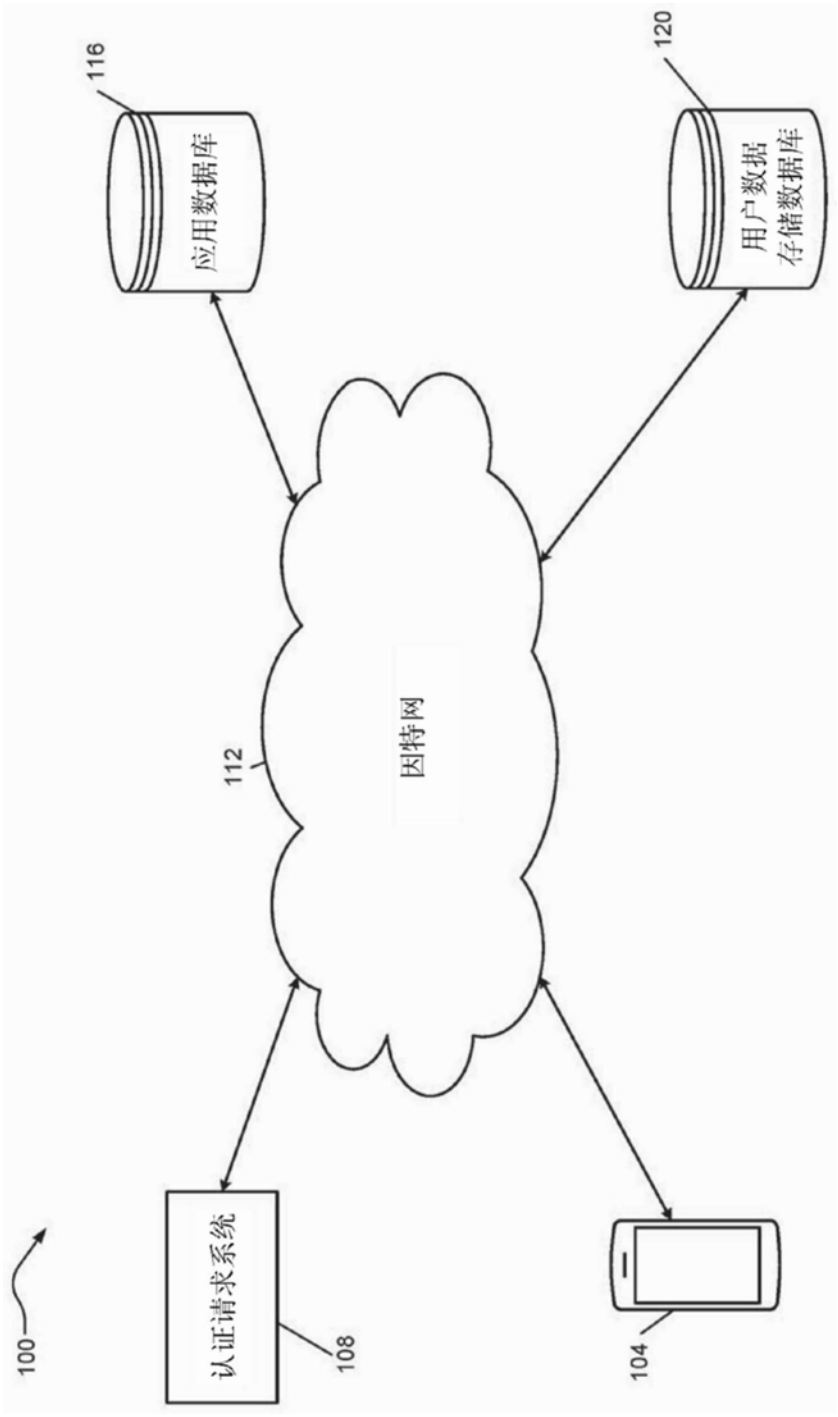


图1

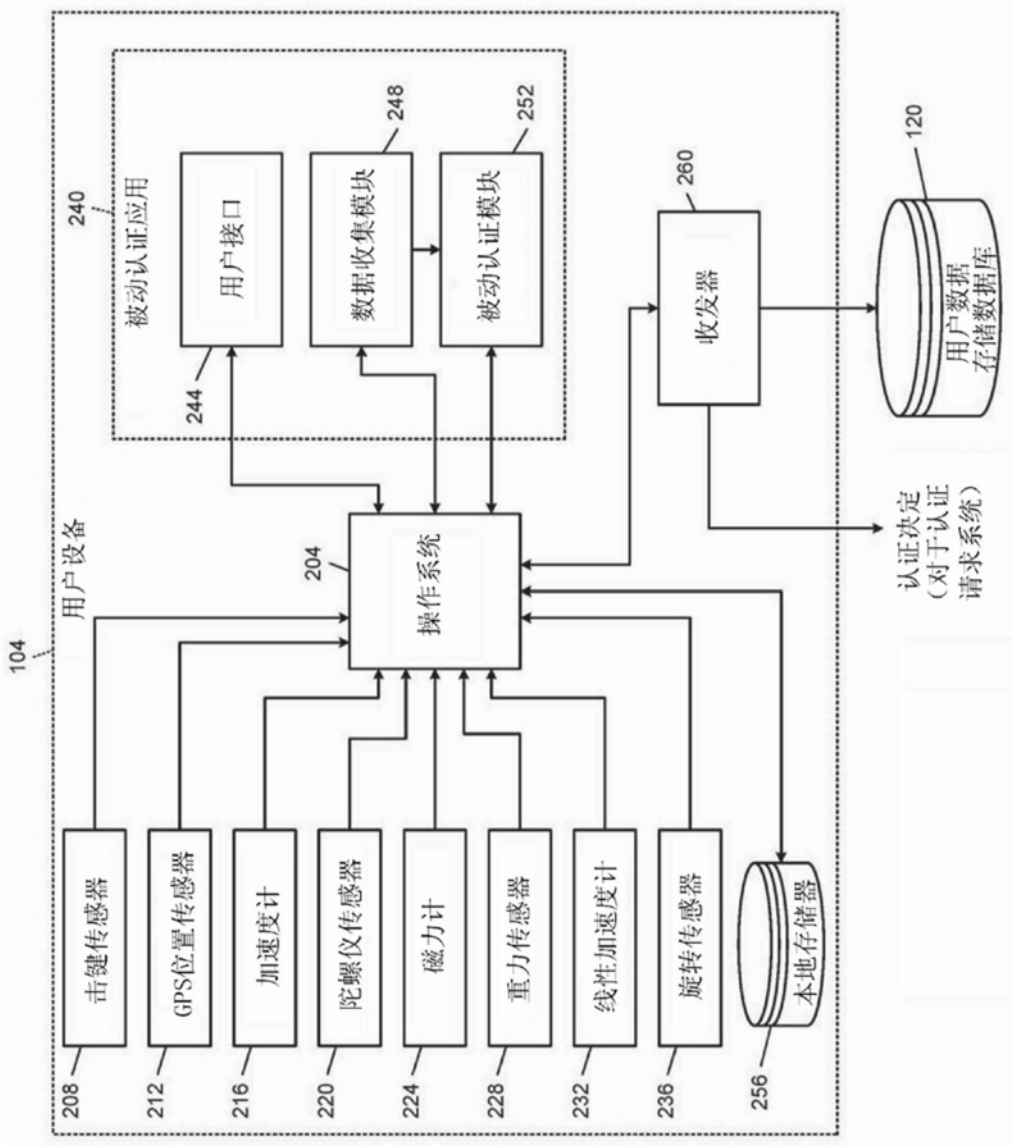

104
用户设备
240
被动认证应用
244
用户接口
248
数据收集模块
252
被动认证模块
204
操作系统
260
收发器
120
用户数据
存储数据库
认证决定
（对于认证
请求系统）
208
击键传感器
212
GPS位置传感器
216
加速度计
220
陀螺仪传感器
224
磁力计
228
重力传感器
232
线性加速度计
236
旋转传感器
256
本地存储器

图2

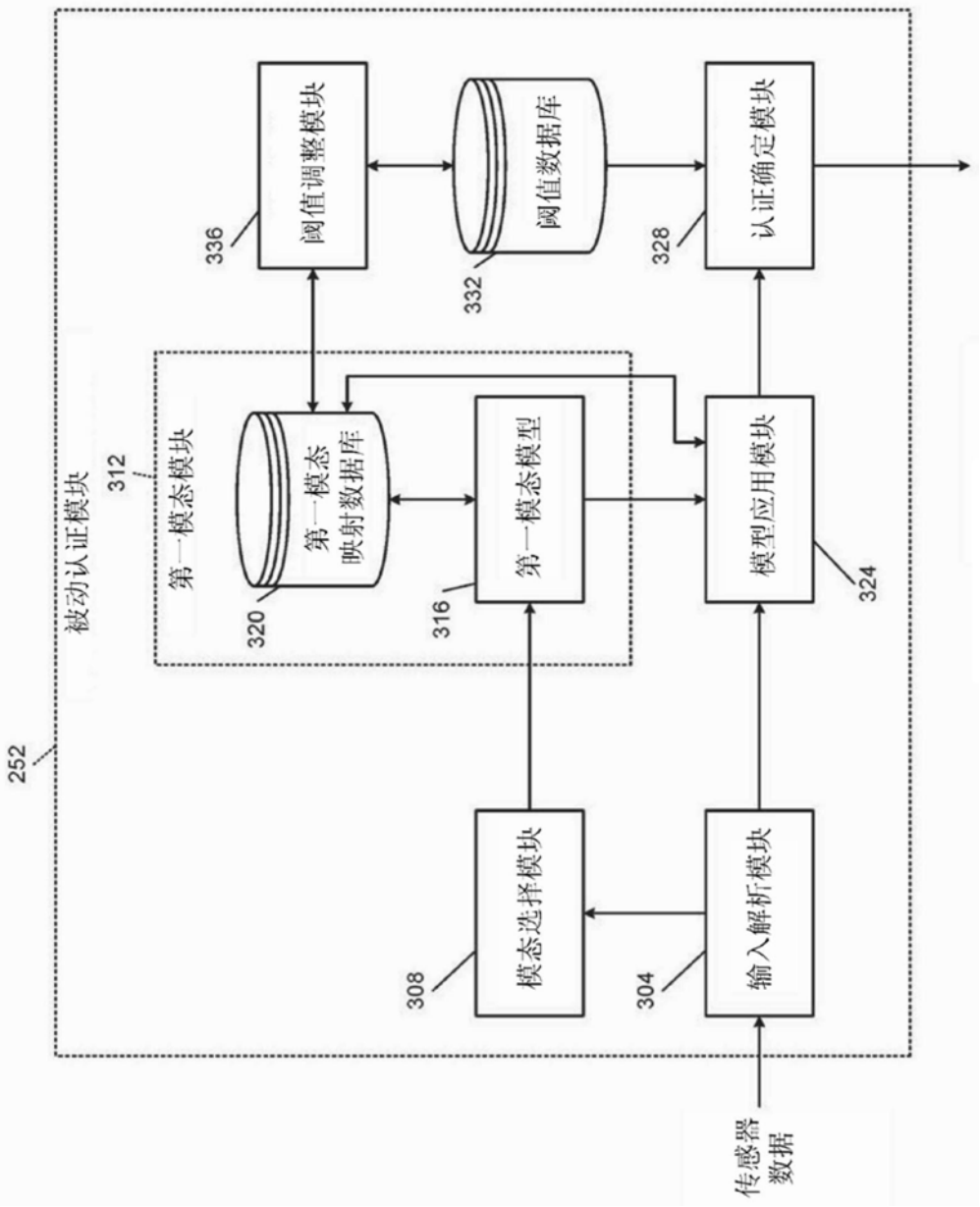

252
被动认证模块
312
第一模态模块
336
阈值调整模块
332
阈值数据库
328
认证确定模块
320
第一模态
映射数据库
316
第一模态模型
模型应用模块
324
308
模态选择模块
304
输入解析模块
传感器
数据

图3

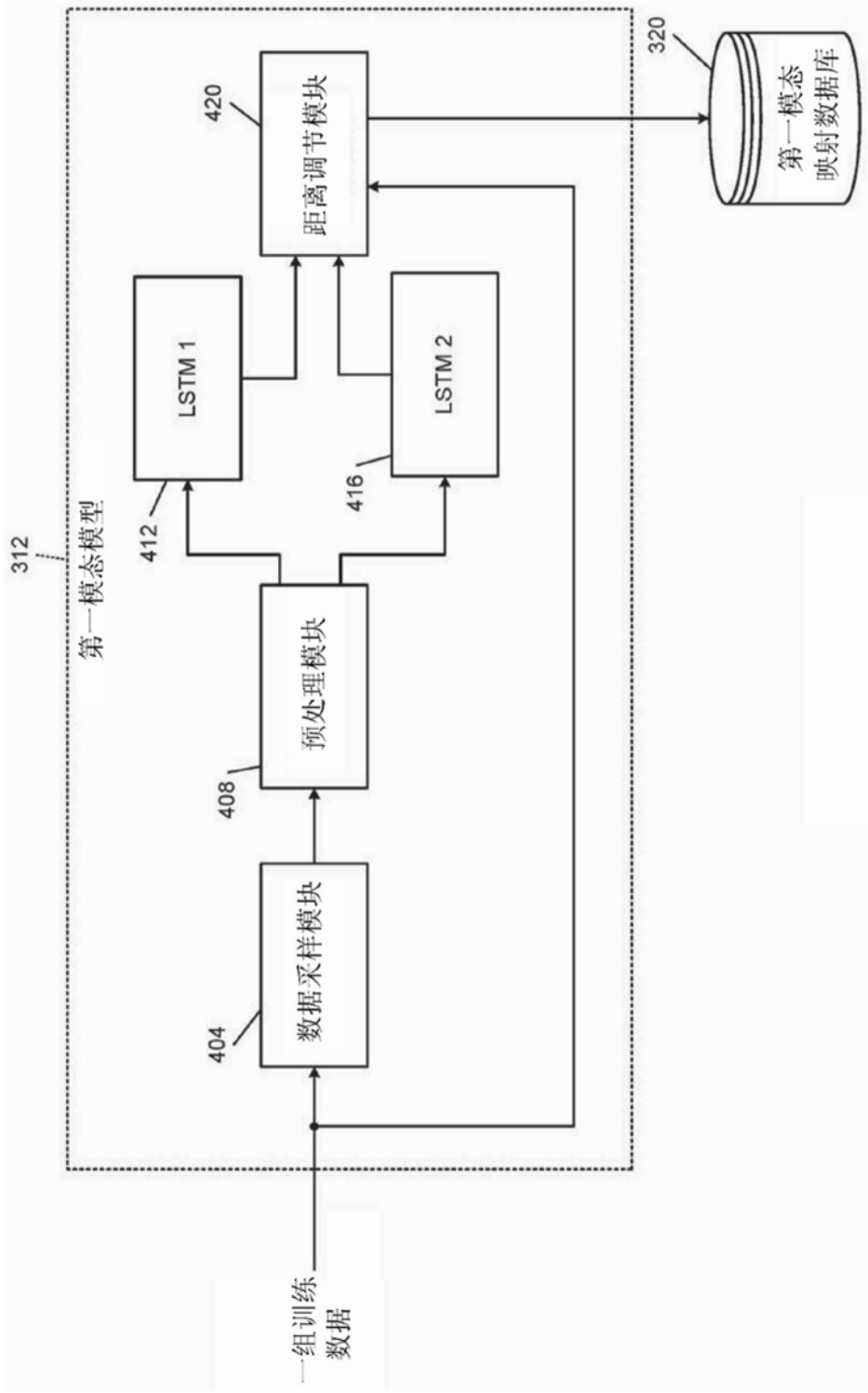

一组训练数据
404
数据采样模块
408
预处理模块
412
LSTM 1
416
LSTM 2
420
距离调节模块
312
第一模态模型
320
第一模态映射数据库

图4

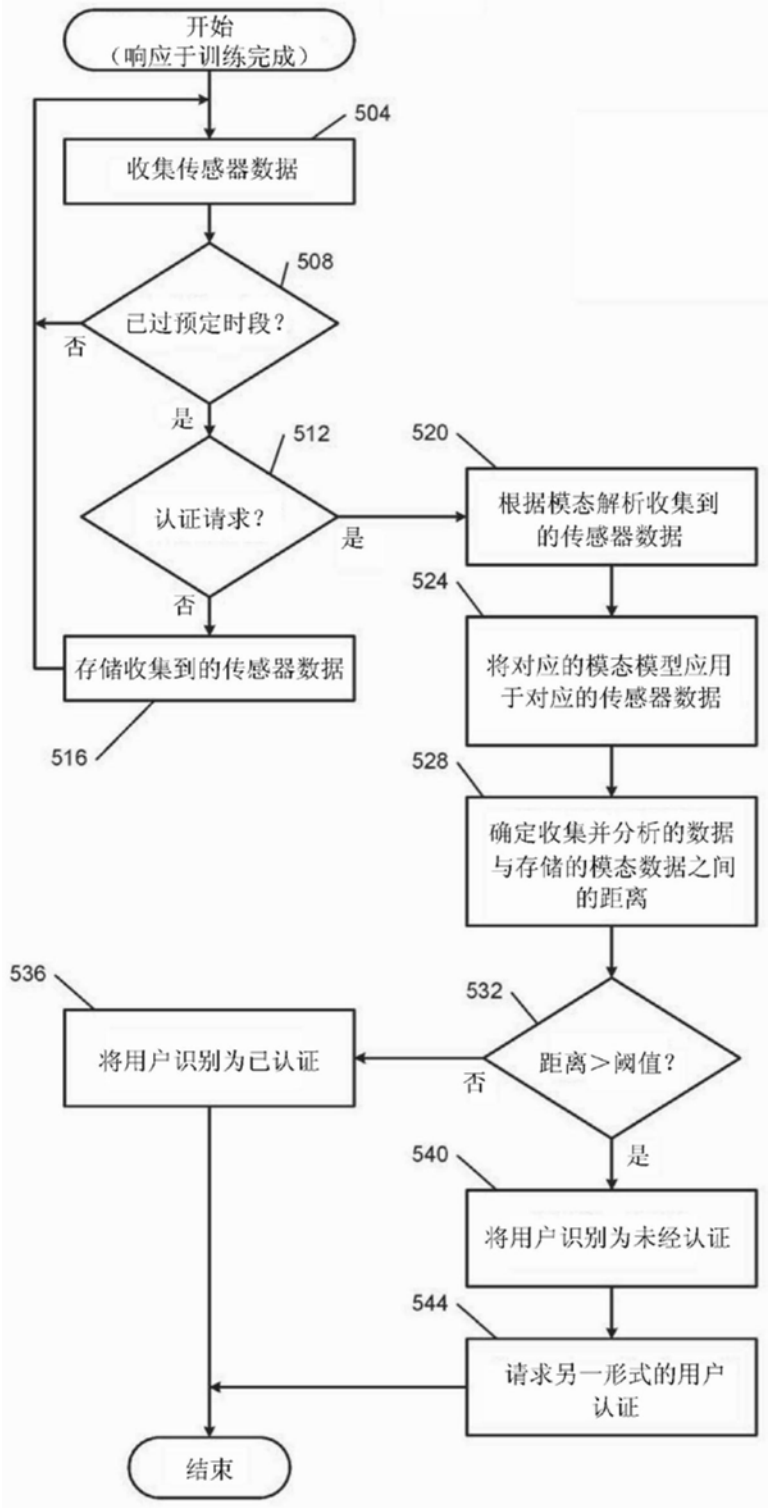

开始
（响应于训练完成）
504
收集传感器数据
508
已过预定时段？
否
是
512
认证请求？
是
否
520
根据模态解析收集到的传感器数据
524
将对应的模态模型应用于对应的传感器数据
528
确定收集并分析的数据与存储的模态数据之间的距离
532
距离＞阈值？
否
是
536
将用户识别为已认证
540
将用户识别为未经认证
544
请求另一形式的用户认证
存储收集到的传感器数据
516
结束

图5

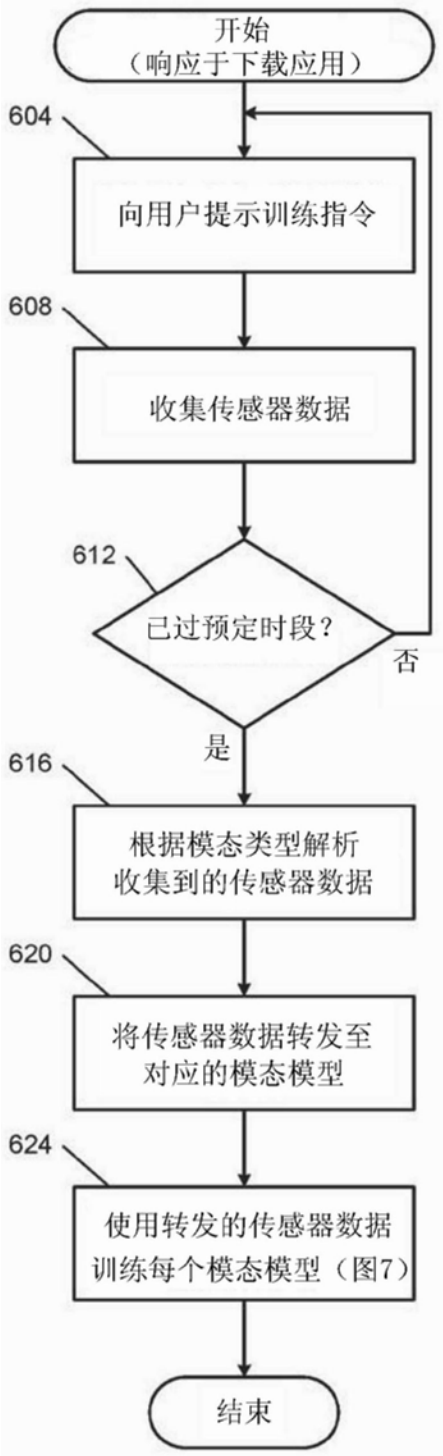

开始
（响应于下载应用）
604
向用户提示训练指令
608
收集传感器数据
612
已过预定时段？
否
是
616
根据模态类型解析
收集到的传感器数据
620
将传感器数据转发至
对应的模态模型
624
使用转发的传感器数据
训练每个模态模型（图7）
结束

图6

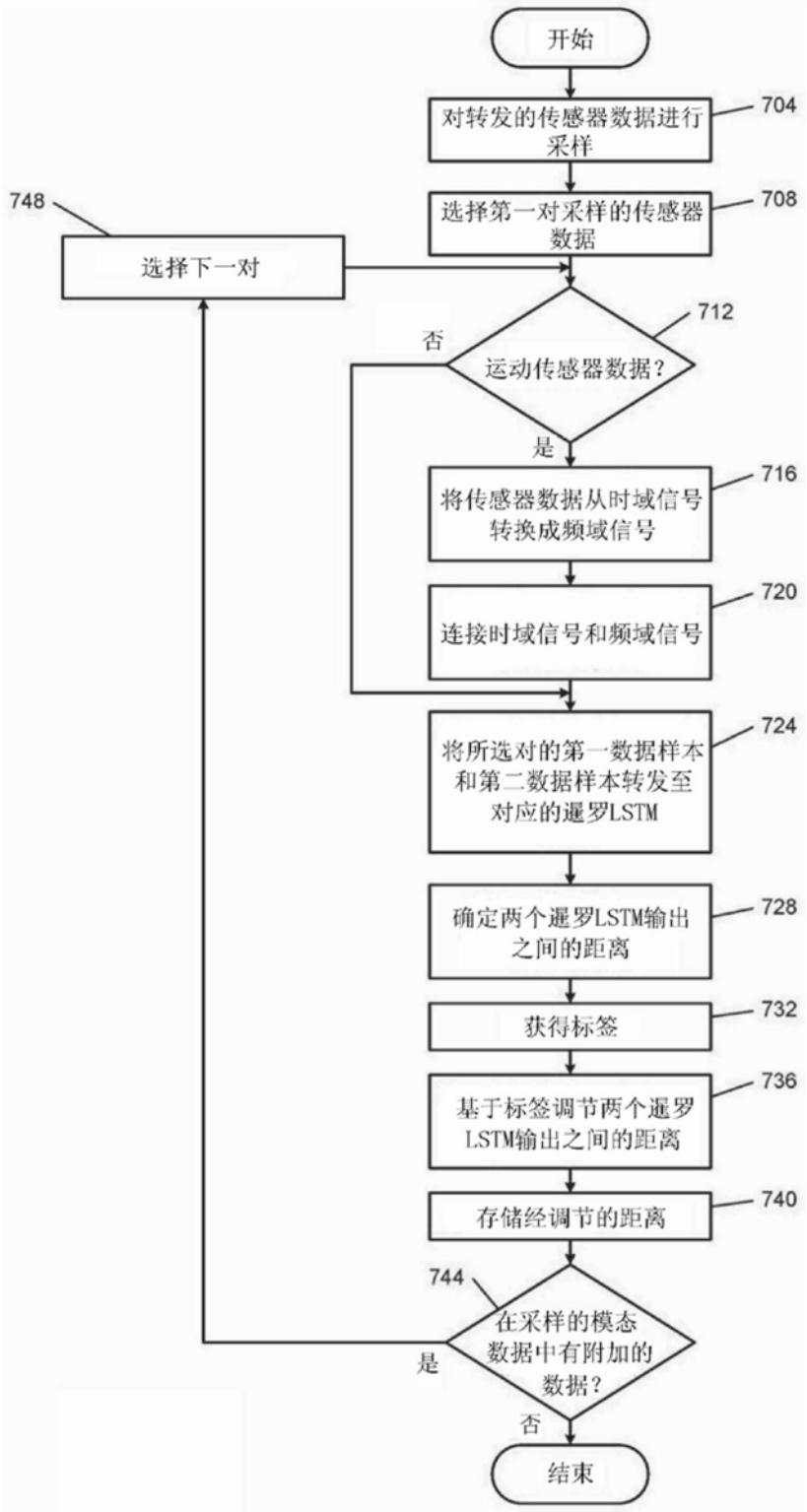

开始
对转发的传感器数据进行采样
704
选择第一对采样的传感器数据
708
748
选择下一对
712
否
运动传感器数据？
是
将传感器数据从时域信号转换成频域信号
716
连接时域信号和频域信号
720
将所选对的第一数据样本和第二数据样本转发至对应的遢罗LSTM
724
确定两个遢罗LSTM输出之间的距离
728
获得标签
732
基于标签调节两个遢罗LSTM输出之间的距离
736
存储经调节的距离
740
744
在采样的模态数据中有附加的数据？
是
否
结束

图7