(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 109977639 A
(43)申请公布日 2019.07.05

(21)申请号 201811264675.1

(22)申请日 2018.10.26

(71)申请人 招商银行股份有限公司
地址 518000 广东省深圳市福田区深南大道7088招商银行大厦

(72)发明人 周天虹 陈曦 常晋云 童科浪

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国

(51)Int.Cl.
G06F 21/31(2013.01)
G06N 3/02(2006.01)

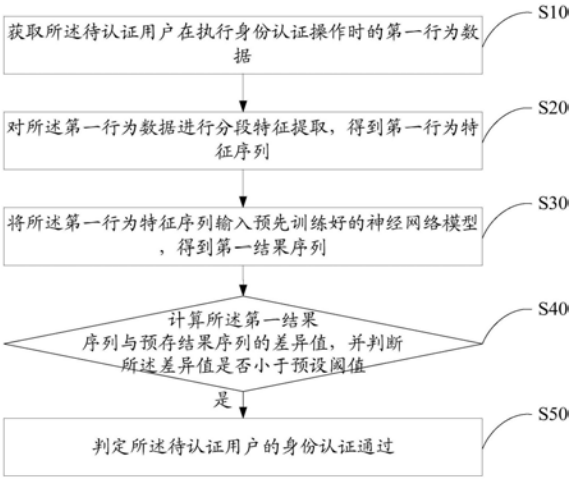
权利要求书2页 说明书11页 附图2页

(54)发明名称

身份认证方法、装置及计算机可读存储介质

(57)摘要

本发明公开了一种身份认证方法。该身份认证方法包括:获取待认证用户在执行身份认证操作时的第一行为数据;对所述第一行为数据进行分段特征提取,得到第一行为特征序列;将所述第一行为特征序列输入预先训练好的神经网络模型,得到第一结果序列;计算所述第一结果序列与预存结果序列的差异值,并判断所述差异值是否小于预设阈值;若所述差异值小于预设阈值,则判定所述待认证用户的身份认证通过。本发明还公开了一种身份认证装置及计算机可读存储介质。本发明能够解决现有的基于行为特征进行身份认证的方法,其鲁棒性较差的技术问题。



CN 109977639 A

1.一种身份认证方法,其特征在于,所述身份认证方法包括以下步骤:

获取待认证用户在执行身份认证操作时的第一行为数据;

对所述第一行为数据进行分段特征提取,得到第一行为特征序列;

将所述第一行为特征序列输入预先训练好的神经网络模型,得到第一结果序列;

计算所述第一结果序列与预存结果序列的差异值,并判断所述差异值是否小于预设阈值;

若所述差异值小于预设阈值,则判定所述待认证用户的身份认证通过。

2.如权利要求1所述的身份认证方法,其特征在于,所述获取待认证用户在执行身份认证操作时的第一行为数据的步骤之前,包括:

获取训练数据,所述训练数据包括多个用户的多个第二行为特征序列;

对所述训练数据中的第二行为特征序列按预设规则进行组合,得到多个训练样本组合;

将所述训练样本组合输入神经网络模型,得到输出结果,根据所述输出结果和预设损失函数得到损失值;

根据所述损失值通过梯度下降算法对所述神经网络模型的参数进行更新,并对所述训练样本组合进行迭代训练,得到训练好的神经网络模型。

3.如权利要求2所述的身份认证方法,其特征在于,所述对所述训练数据中的第二行为特征序列按预设规则进行组合,得到多个训练样本组合的步骤,包括:

将所述训练数据中同一用户的第二行为特征序列进行两两组合,并向各个组合中随机加入另一用户的一条第二行为特征序列,得到多个包含三条第二行为特征序列的训练样本组合;

所述将所述训练样本组合输入神经网络模型,得到输出结果,根据所述输出结果和预设损失函数得到损失值的步骤,包括:

将所述包含三条第二行为特征序列的训练样本组合输入神经网络模型,得到对应的第二结果序列,根据所述第二结果序列和预设损失函数得到损失值。

4.如权利要求3所述的身份认证方法,其特征在于,所述预设损失函数为:

$loss=\max(||R_1-R_2||^2-||R_1-R_3||^2+\delta,0)$;

其中,所述loss为损失值;

所述R_1和R_2为将所述训练样本组合中同一用户的两条第二行为特征序列输入所述神经网络模型后分别得到的两个第二结果序列;

所述R_3为将所述训练样本组合中随机加入的另一用户的一条第二行为特征序列输入所述神经网络模型后得到的第二结果序列;

所述δ为超参数,为一预设值。

5.如权利要求1所述的身份认证方法,其特征在于,所述获取待认证用户在执行身份认证操作时的第一行为数据的步骤之前,还包括:

在接收到身份认证信息录入请求时,根据所述身份认证信息录入请求获取对应的用户账号,并获取用户在执行身份信息录入操作时的第三行为数据;

对所述第三行为数据进行分段特征提取,得到第三行为特征序列;

将所述第三行为特征序列输入所述预先训练好的神经网络模型,得到所述预存结果序

列，并将所述预存结果序列与所述用户账号进行关联存储。

6.如权利要求5所述的身份认证方法，其特征在于，所述获取待认证用户在执行身份认证操作时的第一行为数据的步骤之后，还包括：

获取与所述身份认证操作对应的的用户账号，并根据所述用户账号得到所述预存结果序列。

7.如权利要求1至6中任一项所述的身份认证方法，其特征在于，所述身份认证方法还包括：

在接收到身份认证信息更改请求时，获取用户在执行身份认证信息更改操作时的第四行为数据；

对所述第四行为数据进行分段特征提取，得到第四行为特征序列；

将所述第四行为特征序列输入所述预先训练好的神经网络模型，得到第四结果序列；

更新所述预存结果序列为所述第四结果序列。

8.如权利要求1至6中任一项所述的身份认证方法，其特征在于，所述第一行为数据包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种。

9.一种身份认证装置，其特征在于，所述身份认证装置包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的身份认证程序，所述身份认证程序被所述处理器执行时实现如权利要求1至8中任一项所述的身份认证方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有身份认证程序，所述身份认证程序被处理器执行时实现如权利要求1至8中任一项所述的身份认证方法的步骤。

身份认证方法、装置及计算机可读存储介质

技术领域

[0001] 本发明涉及身份认证技术领域，尤其涉及一种身份认证方法、装置及计算机可读存储介质。

背景技术

[0002] 随着智能手机用户的不断增多，各种场景下对安全可靠的身份认证的需求也在不断增强，然而传统的基于用户口令的认证方式存在易丢失和不便于记忆等问题，基于指纹、虹膜、人脸等生理特征进行认证的机制也存在生理特征被盗取的风险。目前，已有部分研究提出可通过基于行为特征的身份认证方案来解决上述问题。

[0003] 行为特征本质上是用户在长期生活过程中形成的一种肌肉记忆，每个个体具有较强的独特性，同时也难以被他人盗取，利用行为特征作为认证手段可以增强现有认证方式的安全性。

[0004] 然而目前的各种基于行为特征进行身份认证的方法，通常利用单一的行为特征对用户进行身份认证，由于用户特征的波动性较大，导致其鲁棒性较差。因此，现有的基于行为特征进行身份认证的方法，其鲁棒性较差。

[0005] 上述内容仅用于辅助理解本发明的技术方案，并不代表承认上述内容是现有技术。

发明内容

[0006] 本发明的主要目的在于提供一种身份认证方法、装置及计算机可读存储介质，旨在解决现有的基于行为特征进行身份认证的方法，其鲁棒性较差的技术问题。

[0007] 为实现上述目的，本发明提供一种身份认证方法，所述身份认证方法包括：

[0008] 获取待认证用户在执行身份认证操作时的第一行为数据；

[0009] 对所述第一行为数据进行分段特征提取，得到第一行为特征序列；

[0010] 将所述第一行为特征序列输入预先训练好的神经网络模型，得到第一结果序列；

[0011] 计算所述第一结果序列与预存结果序列的差异值，并判断所述差异值是否小于预设阈值；

[0012] 若所述差异值小于预设阈值，则判定所述待认证用户的身份认证通过。

[0013] 可选地，所述获取待认证用户在执行身份认证操作时的第一行为数据的步骤之前，包括：

[0014] 获取训练数据，所述训练数据包括多个用户的多个第二行为特征序列；

[0015] 对所述训练数据中的第二行为特征序列按预设规则进行组合，得到多个训练样本组合；

[0016] 将所述训练样本组合输入神经网络模型，得到输出结果，根据所述输出结果和预设损失函数得到损失值；

[0017] 根据所述损失值通过梯度下降算法对所述神经网络模型的参数进行更新，并对所

述训练样本组合进行迭代训练，得到训练好的神经网络模型。

[0018] 可选地，所述对所述训练数据中的第二行为特征序列按预设规则进行组合，得到多个训练样本组合的步骤，包括：

[0019] 将所述训练数据中同一用户的第二行为特征序列进行两两组合，并向各个组合中随机加入另一用户的一条第二行为特征序列，得到多个包含三条第二行为特征序列的训练样本组合；

[0020] 所述将所述训练样本组合输入神经网络模型，得到输出结果，根据所述输出结果和预设损失函数得到损失值的步骤，包括：

[0021] 将所述包含三条第二行为特征序列的训练样本组合输入神经网络模型，得到对应的第二结果序列，根据所述第二结果序列和预设损失函数得到损失值。

[0022] 可选地，所述预设损失函数为：

[0023] $loss=\max(||R_1-R_2||^2-||R_1-R_3||^2+\delta,0)$；

[0024] 其中，所述loss为损失值；

[0025] 所述R_1和R_2为将所述训练样本组合中同一用户的两条第二行为特征序列输入所述神经网络模型后分别得到的两个第二结果序列；

[0026] 所述R_3为将所述训练样本组合中随机加入的另一用户的一条第二行为特征序列输入所述神经网络模型后得到的第二结果序列；

[0027] 所述δ为超参数，为一预设值。

[0028] 可选地，所述获取待认证用户在执行身份认证操作时的第一行为数据的步骤之前，还包括：

[0029] 在接收到身份认证信息录入请求时，根据所述身份认证信息录入请求获取对应的用户账号，并获取用户在执行身份信息录入操作时的第三行为数据；

[0030] 对所述第三行为数据进行分段特征提取，得到第三行为特征序列；

[0031] 将所述第三行为特征序列输入所述预先训练好的神经网络模型，得到所述预存结果序列，并将所述预存结果序列与所述用户账号进行关联存储。

[0032] 可选地，所述获取待认证用户在执行身份认证操作时的第一行为数据的步骤之后，还包括：

[0033] 获取与所述身份认证操作对应的用户账号，并根据所述用户账号得到所述预存结果序列。

[0034] 可选地，所述身份认证方法还包括：

[0035] 在接收到身份认证信息更改请求时，获取用户在执行身份认证信息更改操作时的第四行为数据；

[0036] 对所述第四行为数据进行分段特征提取，得到第四行为特征序列；

[0037] 将所述第四行为特征序列输入所述预先训练好的神经网络模型，得到第四结果序列；

[0038] 更新所述预存结果序列为所述第四结果序列。

[0039] 可选地，所述第一行为数据包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种。

[0040] 此外，为实现上述目的，本发明还提供一种身份认证装置，所述身份认证装置包

括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的身份认证程序,所述身份认证程序被所述处理器执行时实现如上所述的身份认证方法的步骤。

[0041] 此外,为实现上述目的,本发明还提供一种计算机可读存储介质,所述计算机可读存储介质上存储有身份认证程序,所述身份认证程序被处理器执行时实现如上所述的身份认证方法的步骤。

[0042] 本发明提供一种身份认证方法、装置及计算机可读存储介质,获取待认证用户在执行身份认证操作时的第一行为数据,其中,该第一行为数据包括多个维度的特征数据,具体包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种;对该第一行为数据进行分段特征提取,得到第一行为特征序列;将第一行为特征序列输入预先训练好的神经网络模型,得到第一结果序列;然后计算该第一结果序列与预存结果序列(即真实用户对应的结果序列)之间的差异值,并判断该差异值是否小于预设阈值;若小于,则判定该待认证用户的身份认证通过。本发明基于多维特征组合及分段特征提取用户行为特征的表征方式,可保证用户的部分特征波动性较大时,其余特征仍能保证用户身份认证过程的正常执行,使得身份认证过程具有较强鲁棒性,相比于现有技术中采用单一特征进行身份认证,本发明可提高基于行为特征进行身份认证的方法的鲁棒性。此外,本发明提出的基于神经网络的多维特征融合方式,能有效地将分散的各个特征,融合到统一的决策机制中。

附图说明

[0043] 图1为本发明实施例方案涉及的硬件运行环境的终端结构示意图;

[0044] 图2为本发明身份认证方法第一实施例的流程示意图;

[0045] 图3为本发明身份认证方法第二实施例的流程示意图。

[0046] 本发明目的的实现、功能特点及优点将结合实施例,参照附图做进一步说明。

具体实施方式

[0047] 应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0048] 由于现有的各种基于行为特征进行身份认证的方法,通常利用单一的行为特征对用户进行身份认证,由于用户特征的波动性较大,导致其鲁棒性较差。因此,现有的基于行为特征进行身份认证的方法,其鲁棒性较差。

[0049] 为了解决上述技术问题,本发明提供一种身份认证方法,获取待认证用户在执行身份认证操作时的第一行为数据,其中,该第一行为数据包括多个维度的特征数据,具体包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种;对该第一行为数据进行分段特征提取,得到第一行为特征序列;将第一行为特征序列输入预先训练好的神经网络模型,得到第一结果序列;然后计算该第一结果序列与预存结果序列(即真实用户对应的结果序列)之间的差异值,并判断该差异值是否小于预设阈值;若小于,则判定该待认证用户的身份认证通过。本发明基于多维特征组合及分段特征提取用户行为特征的表征方式,可保证用户的部分特征波动性较大时,其余特征仍能保证用户身份认证过程的正常执行,使得身份认证过程具有较强鲁棒性,相比于现有技术中采用单一特征进行身份认证,本发明可提高基于行为特征进行身份认证的方法的鲁

棒性。此外，本发明提出的基于神经网络的多维特征融合方式，能有效地将分散的各个特征，融合到统一的决策机制中。

[0050] 参照图1，图1为本发明实施例方案涉及的硬件运行环境的终端结构示意图。

[0051] 本发明实施例终端为服务端，该服务端可以是服务器，也可以是PC(Personal Computer，个人计算机)、平板电脑、便携计算机等终端设备。

[0052] 如图1所示，该终端可以包括：处理器1001，例如CPU(Central Processing Unit，中央处理器)，通信总线1002，用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信。用户接口1003可以包括显示屏(Display)、输入单元比如键盘(Keyboard)，可选用户接口1003还可以包括标准的有线接口、无线接口。网络接口1004可选的可以包括标准的有线接口、无线接口(如无线保真Wireless-Fidelity，Wi-Fi接口)。存储器1005可以是高速RAM存储器，也可以是稳定的存储器(non-volatile memory)，例如磁盘存储器。存储器1005可选的还可以是独立于前述处理器1001的存储装置。

[0053] 可选地，终端还可以包括传感器、摄像头、RF(Radio Frequency，射频)电路、音频电路、Wi-Fi模块等等。其中，传感器比如加速度传感器、方向传感器传感器、陀螺仪传感器以及其他传感器。其中，加速度传感器又叫G-sensor，获取的是x、y、z三轴的加速度数值；方向传感器简称为O-sensor，返回三轴的角度数据，方向数据的单位是角度；陀螺仪传感器叫做Gyro-sensor，返回x、y、z三轴的角加速度数据；当然，终端还可配置光传感器、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

[0054] 本领域技术人员可以理解，图1中示出的终端结构并不构成对终端的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0055] 如图1所示，作为一种计算机存储介质的存储器1005中可以包括操作系统、网络通信模块、用户接口模块以及身份认证程序。

[0056] 在图1所示的终端中，网络接口1004主要用于连接后台服务器，与后台服务器进行数据通信；用户接口1003主要用于连接客户端，与客户端进行数据通信；而处理器1001可以用于调用存储器1005中存储的身份认证程序，并执行以下操作：

[0057] 获取待认证用户在执行身份认证操作时的第一行为数据；

[0058] 对所述第一行为数据进行分段特征提取，得到第一行为特征序列；

[0059] 将所述第一行为特征序列输入预先训练好的神经网络模型，得到第一结果序列；

[0060] 计算所述第一结果序列与预存结果序列的差异值，并判断所述差异值是否小于预设阈值；

[0061] 若所述差异值小于预设阈值，则判定所述待认证用户的身份认证通过。

[0062] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0063] 获取训练数据，所述训练数据包括多个用户的多个第二行为特征序列；

[0064] 对所述训练数据中的第二行为特征序列按预设规则进行组合，得到多个训练样本组合；

[0065] 将所述训练样本组合输入神经网络模型，得到输出结果，根据所述输出结果和预设损失函数得到损失值；

[0066] 根据所述损失值通过梯度下降算法对所述神经网络模型的参数进行更新，并对所述训练样本组合进行迭代训练，得到训练好的神经网络模型。

[0067] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0068] 将所述训练数据中同一用户的第二行为特征序列进行两两组合，并向各个组合中随机加入另一用户的一条第二行为特征序列，得到多个包含三条第二行为特征序列的训练样本组合；

[0069] 将所述包含三条第二行为特征序列的训练样本组合输入神经网络模型，得到对应的第二结果序列，根据所述第二结果序列和预设损失函数得到损失值。

[0070] 进一步地，所述预设损失函数为：

[0071] $loss=\max(||R_1-R_2||^2-||R_1-R_3||^2+\delta,0)$；

[0072] 其中，所述loss为损失值；

[0073] 所述R_1和R_2为将所述训练样本组合中同一用户的两条第二行为特征序列输入所述神经网络模型后分别得到的两个第二结果序列；

[0074] 所述R_3为将所述训练样本组合中随机加入的另一用户的一条第二行为特征序列输入所述神经网络模型后得到的第二结果序列；

[0075] 所述δ为超参数，为一预设值。

[0076] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0077] 在接收到身份认证信息录入请求时，根据所述身份认证信息录入请求获取对应的用户账号，并获取用户在执行身份信息录入操作时的第三行为数据；

[0078] 对所述第三行为数据进行分段特征提取，得到第三行为特征序列；

[0079] 将所述第三行为特征序列输入所述预先训练好的神经网络模型，得到所述预存结果序列，并将所述预存结果序列与所述用户账号进行关联存储。

[0080] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0081] 获取与所述身份认证操作对应的用户账号，并根据所述用户账号得到所述预存结果序列。

[0082] 进一步地，处理器1001可以调用存储器1005中存储的身份认证程序，还执行以下操作：

[0083] 在接收到身份认证信息更改请求时，获取用户在执行身份认证信息更改操作时的第四行为数据；

[0084] 对所述第四行为数据进行分段特征提取，得到第四行为特征序列；

[0085] 将所述第四行为特征序列输入所述预先训练好的神经网络模型，得到第四结果序列；

[0086] 更新所述预存结果序列为所述第四结果序列。

[0087] 进一步地，所述第一行为数据包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种。

[0088] 基于上述硬件结构，提出本发明身份认证方法各个实施例。

[0089] 本发明提供一种身份认证方法。

[0090] 参照图2,图2为本发明身份认证方法第一实施例的流程示意图。

[0091] 在本实施例中,该身份认证方法包括:

[0092] 步骤S10,获取待认证用户在执行身份认证操作时的第一行为数据;

[0093] 在本实施例中,在上述步骤S10之前,该身份认证方法还包括:

[0094] 步骤a,在接收到身份认证信息录入请求时,根据所述身份认证信息录入请求获取对应的用户账号,并获取用户在执行身份信息录入操作时的第三行为数据;

[0095] 步骤b,对所述第三行为数据进行分段特征提取,得到第三行为特征序列;

[0096] 步骤c,将所述第三行为特征序列输入所述预先训练好的神经网络模型,得到所述预存结果序列,并将所述预存结果序列与所述用户账号进行关联存储。

[0097] 在本实施例中,执行终端为服务端,该服务端可以是服务器,也可以是PC、平板电脑、便携计算机等终端设备。

[0098] 在本实施例中,用户需先录入身份认证信息,以使得后续需进行身份认证时,可根据该已录入保存的身份认证信息与当前待认证用户的身份认证信息进行比对,以判断是否是用户本人在执行操作。具体的,服务端在接收到用户基于用户终端(如智能手机)触发的身份认证信息录入请求时,根据该身份认证信息录入请求获取对应的用户账号,并获取用户在用户终端中执行身份信息录入操作时的第三行为数据,该第三行为数据可以包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种,当然实际情况中还可以包括其他特征维度的数据。然后对第三行为数据进行分段特征提取,得到第三行为特征序列,具体的第三行为特征序列的获取方法与下述实施例中对第一行为特征序列的获取方法基本相同,此处不作赘述。需要说明的是,在具体实施例中,为减轻服务端的压力,第三行为特征序列的获取过程可在用户终端中执行,即用户终端获取用户在执行身份信息录入操作时的第三行为数据,对第三行为数据进行分段特征提取,得到第三行为特征序列,然后将该第三行为特征序列发送至服务端。服务端直接从用户终端处获取得到第三行为特征序列。

[0099] 在获得第三行为特征序列之后,将其输入至预先训练好的神经网络模型,可得到预存结果序列,即为真实用户的身份信息的一个对应预存信息,可用于与待认证用户的结果序列进行对比,以确认待认证用户是否为真实用户。在获得预存结果序列之后,将该预存结果序列与用户账号进行关联存储,用户登录该用户账号或在该用户账号对应app中执行某些需要进行身份认证的操作时可调用该预存结果序列进行对比认证。需要说明的是,为保证用户可在不同用户终端进行身份认证,将预存结果序列与用户账号可关联存储在服务端的预设数据库中,使得用户在另一用户终端进行身份认证时,该服务端可在预设数据库中获取得到预存结果序列。

[0100] 服务端首先获取该待认证用户在执行身份认证操作(如进行密码输入)时的第一行为数据,该第一行为数据可以包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种,可以理解的是,第一行为数据所包括特征维度数量越多,其身份认证结果的准确性越高。为后续具体说明如何对第一行为数据进行分段特征提取,以第一行为数据包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列为例进行说明。其中,第一行为数

据的获取，可通过移动终端的屏幕和相关传感器进行采集获得，假设用户在执行身份认证操作的过程中进行了k次触摸屏幕的行为，按压面积序列即为k次触屏行为的按压面积的序列，可记为$\{a_1,a_2,\cdots,a_k\}$，类似地，按压压力序列、按压时长序列分别为k次触屏行为的按压压力和按压时长的序列，分别记为$\{p_1,p_2,\cdots,p_k\}$、$\{t_1,t_2,\cdots,t_k\}$，按压间隔序列为各次触屏行为之间的时间间隔，记为$\{i_1,i_2,\cdots i_{k-1}\}$，加速度序列、角度序列和角加速度序列为待认证用户执行触屏行为期间，分别通过加速度传感器、方向传感器和陀螺仪传感器实时或每隔预设时间采集得到的，可分别记为$\{(x_{a1},y_{a1},z_{a1}),(x_{a2},y_{a2},z_{a2}),\cdots,(x_{an},y_{an},z_{an})\}$、$\{(x_{o1},y_{o1},z_{o1}),(x_{o2},y_{o2},z_{o2}),\cdots(x_{on},y_{on},z_{on})\}$、$\{(x_{g1},y_{g1},z_{g1}),(x_{g2},y_{g2},z_{g2}),\cdots,(x_{gn},y_{gn},z_{gn})\}$。

[0101] 此时，在“获取所述待认证用户在执行身份认证操作时的第一行为数据”步骤之后，可以包括步骤d：获取与所述身份认证操作对应的用户账号，并根据所述用户账号得到所述预存结果序列。

[0102] 服务端在监测到待认证用户执行身份认证操作时，如进行密码输入，可获取与该身份认证操作对应的用户账号，如在某app中执行某些需要进行身份认证的操作时，获取该app对应的用户账号，进而根据该用户账号从预设数据库中获得与其关联存储的预存结果序列，以便后续进行对比认证。

[0103] 步骤S20，对所述第一行为数据进行分段特征提取，得到第一行为特征序列；

[0104] 服务端在获取到第一行为数据后，对该第一行为数据进行分段特征提取，得到第一行为特征序列，分段特征提取的具体过程为：将用户执行身份认证操作的过程划分为多个时间段t_{jw}，$t_{jw}=t_j+i_j+t_{j+1}+i_{j+1}+\cdots+t_{j+w-1}+i_{j+w-1}$，表示从第j次触摸屏幕到第j+w次触摸屏幕之间的时间间隔$(w=1,2,\cdots,k;j=1,2\cdots,k-w)$；$a_{jw}=(a_j+a_{j+1}+\cdots+a_{j+w-1})/w$表示从第j次触摸屏幕到第j+w-1次触摸屏幕之间的平均按压面积；$p_{jw}=(p_j+p_{j+1}+\cdots+p_{j+w-1})/w$表示从第j次触摸屏幕到第j+w-1次触摸屏幕之间的平均按压压力；x_{ajwmin}、x_{ajwmax}、x_{ajwavg}、x_{ajwvar}分别表示t_{jw}时间段内加速度序列中x轴时间序列的最小值、最大值、均值、方差，同理，对各个通过传感器获得的序列的各个维度都进行相同的处理。最终，t_{jw}提取得到如下序列：$F_{jw}=\{t_{jw},a_{jw},p_{jw},x_{ajwmin}、x_{ajwmax}、x_{ajwavg}、x_{ajwvar},y_{ajwmin}、y_{ajwmay}、y_{ajwavg}、y_{ajwvar},z_{ajwmin}、z_{ajwmaz}、z_{ajwavg}、z_{ajwvar},x_{ojwmin}、x_{ojwmax}、x_{ojwavg}、x_{ojwvar},y_{ojwmin}、y_{ojwmay}、y_{ojwavg}、y_{ojwvar},z_{ojwmin}、z_{ojwmaz}、z_{ojwavg}、z_{ojwvar},x_{gjwmin}、x_{gjwmax}、x_{gjwavg}、x_{gjwvar},y_{gjwmin}、y_{gjwmay}、y_{gjwavg}、y_{gjwvar},z_{gjwmin}、z_{gjwmaz}、z_{gjwavg}、z_{gjwvar}\}$，进而可得到第一行为特征序列为$F=\{F_{jW};w=1,2,\cdots,k;j=1,2\cdots,k-w\}$，该第一行为特征序列从多个维度记录了用户的多个特征，因此，本实施例中，基于多维特征组合及分段特征提取用户行为特征的表征方式，可保证用户的部分特征波动性较大时，其余特征仍能保证用户身份认证过程的正常执行，使得身份认证过程具有较强鲁棒性，相比于现有技术中采用单一特征进行身份认证，本发明可提高身份认证过程的鲁棒性。

[0105] 需要说明的是，为减轻服务端的压力，该第一行为特征序列的获取过程也可在用户终端中执行，即用户终端获取用户在执行身份信息认证操作时的第一行为数据，对第一行为数据进行分段特征提取，得到第一行为特征序列，然后将该第一行为特征序列发送至服务端。服务端直接从用户终端处获取得到第一行为特征序列。

[0106] 步骤S30，将所述第一行为特征序列输入预先训练好的神经网络模型，得到第一结果序列；

[0107] 然后，服务端将第一行为特征序列输入预先训练好的神经网络模型，得到第一结

果序列，其中，该预先训练好的神经网络模型的具体训练过程可参照下述第二实施例，此处不作赘述。

[0108] 步骤S40，计算所述第一结果序列与预存结果序列的差异值，并判断所述差异值是否小于预设阈值；

[0109] 在得到第一结果序列之后，计算该第一结果序列与预存结果序列(即真实用户对应的结果序列)之间的差异值，作为差异值的其中一种计算方式，可以计算第一结果序列和预存结果序列各维度特征之间的差值后，对其差值进行平方加和后，以得到差异值，然后判断该差异值是否小于预设阈值。

[0110] 步骤S50，若所述差异值小于预设阈值，则判定所述待认证用户的身份认证通过。

[0111] 若该差异值小于预设阈值，则判定该待认证用户的身份认证通过。若该差异值大于或等于该预设阈值，则判定该待认证用户的身份认证失败，此时，可在用户终端界面显示身份认证失败信息。此外，服务端在检测到多次身份认证失败时，可控制用户终端进行锁屏等操作。

[0112] 本发明实施例提供一种身份认证方法，获取待认证用户在执行身份认证操作时的第一行为数据，其中，该第一行为数据包括多个维度的特征数据，具体包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种；对该第一行为数据进行分段特征提取，得到第一行为特征序列；将第一行为特征序列输入预先训练好的神经网络模型，得到第一结果序列；然后计算该第一结果序列与预存结果序列(即真实用户对应的结果序列)之间的差异值，并判断该差异值是否小于预设阈值；若小于，则判定该待认证用户的身份认证通过。本发明基于多维特征组合及分段特征提取用户行为特征的表征方式，可保证用户的部分特征波动性较大时，其余特征仍能保证用户身份认证过程的正常执行，使得身份认证过程具有较强鲁棒性，相比于现有技术中采用单一特征进行身份认证，本发明可提高基于行为特征进行身份认证的方法的鲁棒性。此外，本发明提出的基于神经网络的多维特征融合方式，能有效地将分散的各个特征，融合到统一的决策机制中。

[0113] 进一步的，参照图3，图3为本发明身份认证方法第二实施例的流程示意图。

[0114] 基于图2所示的第一实施例，在步骤S10之前，该身份认证方法还包括：

[0115] 步骤S60，获取训练数据，所述训练数据包括多个用户的多个第二行为特征序列；

[0116] 本实施例介绍了预先训练好的神经网络模型的具体训练方法。首先，获取训练数据，该训练数据包括多个用户的多个第二行为特征序列，第二特征行为序列的获取方式可以为：1)用户终端通过采集多个用户执行类似的身份认证操作时的第二行为数据，由于需要得到多个第二行为特征序列，因此用户需要执行多次操作，采取多个第二行为数据，然后按上述实施例中的方法对第二行为数据进行分段特征提取，进而得到第二行为特征序列；进而将多个用户的多个第二行为特征序列发送至服务端。2)服务端从用户终端处获取多个用户在执行类似的身份认证操作时的第二行为数据，然后进行分段特征提取，进而得到多个用户的多个第二行为特征序列。对应的，第二行为数据包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种，与第一行为数据和第三行为数据包括的数据维度的数量和种类相一致。

[0117] 步骤S70，对所述训练数据中的第二行为特征序列按预设规则进行组合，得到多个

训练样本组合；

[0118] 步骤S80，将所述训练样本组合输入神经网络模型，得到输出结果，根据所述输出结果和预设损失函数得到损失值；

[0119] 然后，对训练数据中的第二行为特征序列按预设规则进行组合，得到多个训练样本组合，然后将训练样本组合输入神经网络模型，得到输出结果，根据输出结果和预设损失函数得到损失值。

[0120] 具体的，步骤S70可以包括：将所述训练数据中同一用户的第二行为特征序列进行两两组合，并向各个组合中随机加入另一用户的一条第二行为特征序列，得到多个包含三条第二行为特征序列的训练样本组合；

[0121] 此时，步骤S80可以包括：将所述包含三条第二行为特征序列的训练样本组合输入神经网络模型，得到对应的第二结果序列，根据所述第二结果序列和预设损失函数得到损失值。

[0122] 具体的，将训练数据中同一用户的第二行为特征序列进行两两组合，并向各个组合中随机加入另一用户的一条第二行为特征序列，从而得到多个包含三条第二行为特征序列的训练样本组合。将该包含三条第二行为特征序列的训练样本组合输入神经网络模型，得到对应的第二结果序列。需要说明的是，包含三条第二行为特征序列的训练样本组合输入神经网络模型时，是依次进行输入的，对应得到的第二结果序列也包括三条。然后根据该第二结果序列和预设损失函数得到损失值，该预设损失函数为：

[0123] $loss=\max(||R_1-R_2||^2-||R_1-R_3||^2+\delta,0)$；

[0124] 其中，所述loss为损失值；所述R_1和R_2为将所述训练样本组合中同一用户的两条第二行为特征序列输入所述神经网络模型后分别得到的两个第二结果序列；所述R_3为将所述训练样本组合中随机加入的另一用户的一条第二行为特征序列输入所述神经网络模型后得到的第二结果序列；所述δ为超参数，为一预设值。

[0125] 步骤S90，根据所述损失值通过梯度下降算法对所述神经网络模型的参数进行更新，并对所述训练样本组合进行迭代训练，得到训练好的神经网络模型。

[0126] 最后，根据计算得到的损失值通过梯度下降算法对该神经网络模型的参数进行更新，并对每一个训练样本组合进行迭代训练，即根据损失值来更新神经网络模型中各层结点的梯度，进而更新各结点的权值参数，不断输入训练样本组合进行迭代直至网络收敛，直至该损失值稳定下降到一个较小范围(如低于一预设阈值或达到最小值)，此时，可得到训练好的神经网络模型。通过梯度下降算法可求解大规模样本数据的优化问题，具体的梯度下降算法可参照现有技术，此处不做赘述。

[0127] 在本实施例中，在训练神经网络模型时，利用单样本学习技术，可以只采集各用户的两次行为数据，即可维护一个描述特征差异性的模型，在用户无法提供多条训练样本数据的场景下，身份认证方法依旧可用，相比于现有技术中，在进行模型训练时，需要单个用户几十次甚至更多次地重复同一行为以采集行为数据，本发明可降低对用户所需提供训练样本数据数量的要求，可提高训练样本数据提供者的用户体验。

[0128] 进一步的，基于上述各实施例，提出本发明身份认证方法的第三实施例中。

[0129] 在本实施例中，该身份认证方法还可以包括：

[0130] 步骤e，在接收到身份认证信息更改请求时，获取用户在执行身份认证信息更改操

作时的第四行为数据；

[0131] 为保证身份认证信息的安全性，用户可以定期更改身份认证信息，如重新更改密码，此时行为数据也会有所变化，对应的预存结果序列也将发生变化。此时，需对预存结果序列进行更新。具体的，服务端在接收到用户基于用户终端触发的身份认证信息更改请求时，获取用户在用户终端中执行身份认证信息更改操作时的第四行为数据。对应的，该第四行为数据与第一、第二和第三行为数据包括的数据维度的数量和种类相一致，也包括按压面积序列、按压压力序列、按压时长序列、按压间隔序列、加速度序列、角度序列和角加速度序列中的多种。

[0132] 步骤f，对所述第四行为数据进行分段特征提取，得到第四行为特征序列；

[0133] 然后，对该第四行为数据进行分段特征提取，得到第四行为特征序列，具体的过程，可参照上述实施例，此处不作赘述。类似地，为减轻服务端的压力，第四行为特征序列的获取过程也可在用户终端中执行，服务端直接从用户终端处获取该第四行为特征序列。

[0134] 步骤g，将所述第四行为特征序列输入所述预先训练好的神经网络模型，得到第四结果序列；

[0135] 步骤h，更新所述预存结果序列为所述第四结果序列。

[0136] 将获得的第四行为特征序列输入该预先训练好的神经网络模型，得到第四结果序列，更新原来的预存结果序列为该第四结果序列。

[0137] 本发明还提供一种身份认证装置，该身份认证装置包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的身份认证程序，所述身份认证程序被所述处理器执行时实现如以上任一项实施例所述的身份认证方法的步骤。

[0138] 本发明身份认证装置的具体实施例与上述身份认证方法各实施例基本相同，在此不作赘述。

[0139] 本发明还提供一种计算机可读存储介质，该计算机可读存储介质上存储有身份认证程序，所述身份认证程序被处理器执行时实现如以上任一项实施例所述的身份认证方法的步骤。

[0140] 本发明计算机可读存储介质的具体实施例与上述身份认证方法各实施例基本相同，在此不作赘述。

[0141] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0142] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0143] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分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如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0144] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

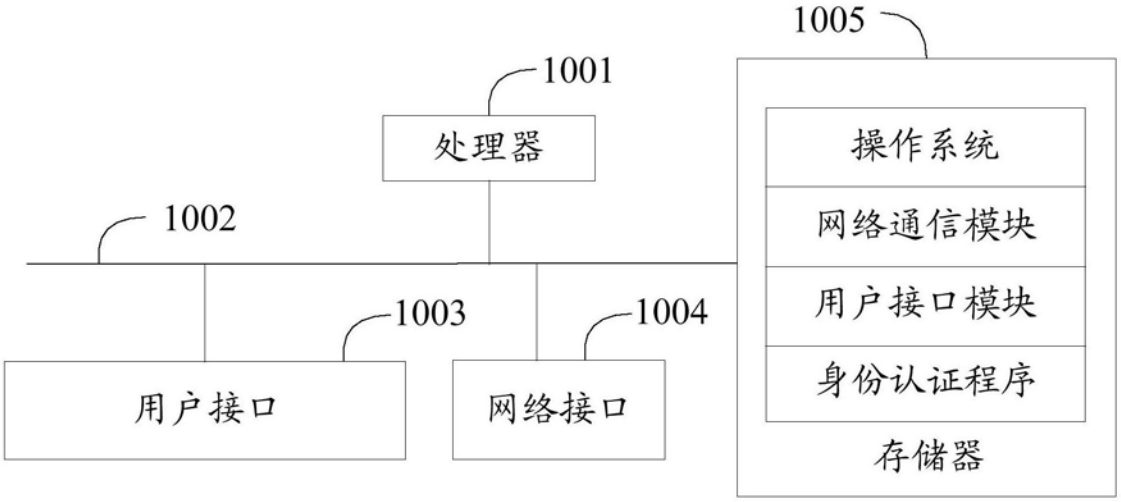

1005
1001
处理器
操作系统
网络通信模块
用户接口模块
身份认证程序
1002
1003
1004
用户接口
网络接口
存储器

图1

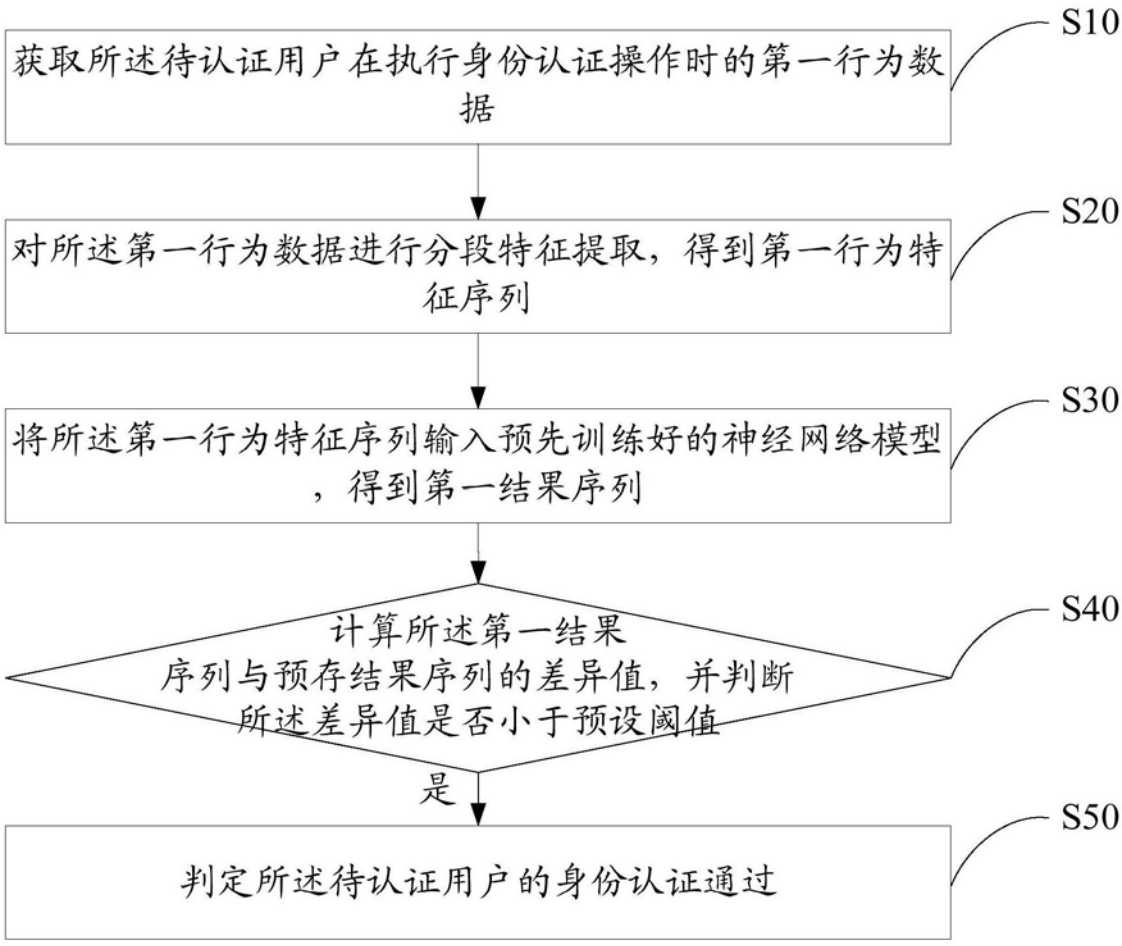

获取所述待认证用户在执行身份认证操作时的第一行为数据
S10
对所述第一行为数据进行分段特征提取，得到第一行为特征序列
S20
将所述第一行为特征序列输入预先训练好的神经网络模型，得到第一结果序列
S30
计算所述第一结果序列与预存结果序列的差异值，并判断所述差异值是否小于预设阈值
S40
是
判定所述待认证用户的身份认证通过
S50

图2

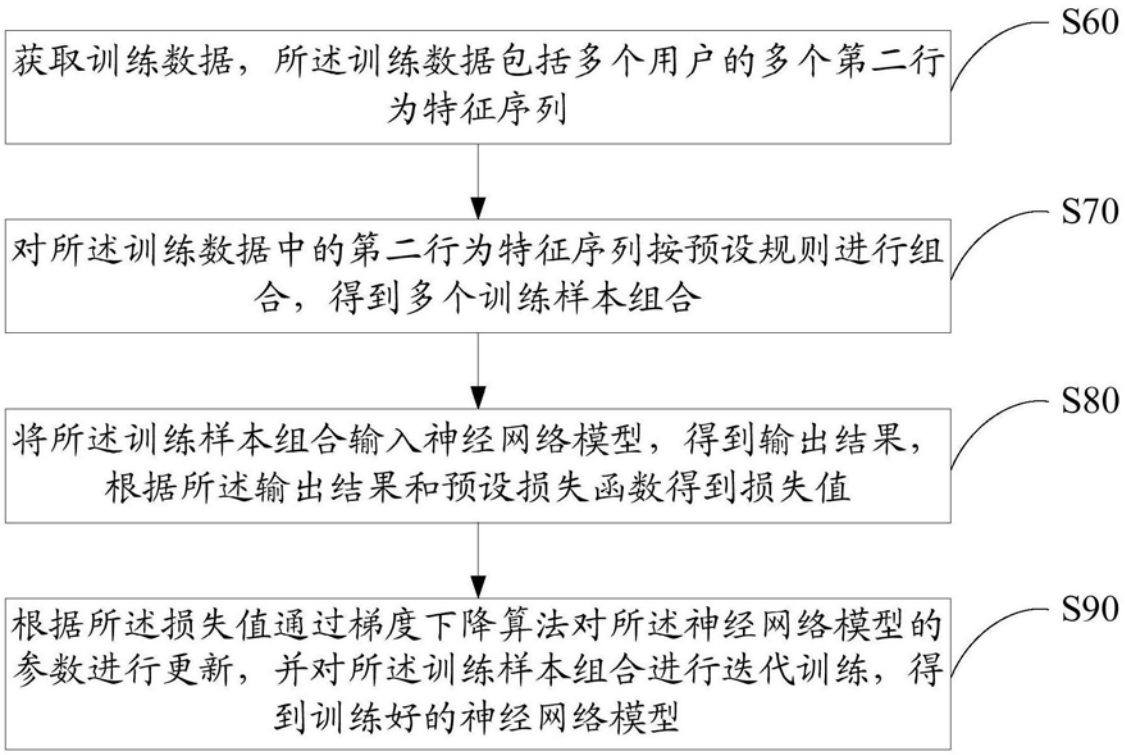

获取训练数据，所述训练数据包括多个用户的多个第二行为特征序列
S60
对所述训练数据中的第二行为特征序列按预设规则进行组合，得到多个训练样本组合
S70
将所述训练样本组合输入神经网络模型，得到输出结果，根据所述输出结果和预设损失函数得到损失值
S80
根据所述损失值通过梯度下降算法对所述神经网络模型的参数进行更新，并对所述训练样本组合进行迭代训练，得到训练好的神经网络模型
S90

图3