(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 105468952 A
(43)申请公布日 2016.04.06

(21)申请号 201510797063.9

(22)申请日 2015.11.17

(71)申请人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 杨霞 郝允允 张少愚 王亮 郭计伟

(74)专利代理机构 北京三高永信知识产权代理有限责任公司 11138
代理人 祝亚男

(51)Int.Cl.
G06F 21/32(2013.01)

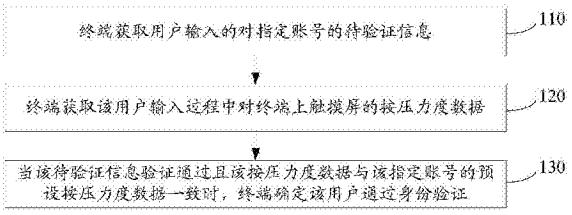
权利要求书2页 说明书10页 附图3页

(54)发明名称

身份验证方法及装置

(57)摘要

本发明公开了一种身份验证方法及装置，属于身份验证领域。该方法包括：获取用户输入的对指定账号的待验证信息；获取该用户输入过程中对终端上触摸屏的按压力度数据；当该待验证信息验证通过且该按压力度数据与该指定账号的预设按压力度数据一致时，确定该用户通过身份验证。本发明通过终端在获取用户输入的待验证信息的同时，获取用户输入待验证信息时对触摸屏的按压力度数据，并且利用待验证信息和按压力度数据同时对用户的身份进行验证，由于不法分子无法窥视窃取按压力度数据，使得即使用户账号的验证信息泄露，不法分子也无法利用泄露的验证信息通过身份验证，从而可以保障用户的账号安全。



CN 105468952 A

1.一种身份验证方法，其特征在于，所述方法包括：

获取用户输入的对指定账号的待验证信息；

获取所述用户输入过程中对终端上触摸屏的按压力度数据；

当所述待验证信息验证通过且所述按压力度数据与所述指定账号的预设按压力度数据一致时，确定所述用户通过身份验证。

2.根据权利要求1所述的方法，其特征在于，所述待验证信息为密码信息、验证码信息或指纹信息。

3.根据权利要求1所述的方法，其特征在于，获取用户输入的待验证信息之前，所述方法还包括：

在身份验证信息设置过程中，存储用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据。

4.根据权利要求3所述的方法，其特征在于，所述方法还包括：

在身份验证信息设置过程中，获取所述用户在至少两次输入身份验证信息过程中对所述终端上触摸屏的按压力度数据；

当所述至少两次输入身份验证信息过程中所获取到的按压力度数据一致时，执行存储用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据的步骤。

5.根据权利要求3所述的方法，其特征在于，所述存储用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据包括：

在所述终端中存储用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据；

或者，

将用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据发送至指定服务器，以使所述指定服务器进行存储。

6.根据权利要求1所述的方法，其特征在于，所述获取所述用户输入过程中对终端上触摸屏的按压力度数据包括：

每检测到一个字符输入行为，获取所述字符输入行为的对终端上触摸屏的按压力度数据。

7.一种身份验证装置，其特征在于，所述装置包括：

第一获取模块，用于获取用户输入的对指定账号的待验证信息；

第二获取模块，用于获取所述用户输入过程中对终端上触摸屏的按压力度数据；

验证模块，用于当所述第一获取模块获取的所述待验证信息验证通过且所述第二获取模块获取的所述按压力度数据与所述指定账号的预设按压力度数据一致时，确定所述用户通过身份验证。

8.根据权利要求7所述的装置，其特征在于，所述待验证信息为密码信息、验证码信息或指纹信息。

9.根据权利要求7所述的装置，其特征在于，所述装置还包括：

存储模块，用于在身份验证信息设置过程中，存储用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据。

10.根据权利要求9所述的装置，其特征在于，所述装置还包括设置模块：

所述设置模块，用于在身份验证信息设置过程中，获取所述用户在至少两次输入身份验证信息过程中对所述终端上触摸屏的按压力度数据；

所述设置模块，还用于当所述至少两次输入身份验证信息过程中所获取到的按压力度数据一致时，将用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据存入所述存储模块。

11.根据权利要求9所述的装置，其特征在于，所述存储模块用于：

在所述终端中存储用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据；

所述存储模块，还用于将用户输入的身份验证信息以及所述用户在输入身份验证信息过程中对所述终端上触摸屏的按压力度数据发送至指定服务器，以使所述指定服务器进行存储。

12.根据权利要求7所述的装置，其特征在于，所述第二获取模块用于：

每检测到一个字符输入行为，获取所述字符输入行为的对终端上触摸屏的按压力度数据。

身份验证方法及装置

技术领域

[0001] 本发明涉及身份认证领域，特别涉及一种身份验证方法及装置。

背景技术

[0002] 身份验证指的是通过检验用户输入的与指定账户对应的密码、验证码、指纹和预先设置的是否一致，从而判断当前用户是否为合法用户。目前，身份验证的使用十分广泛，例如移动设备开机验证、应用账号验证、移动金融服务验证等。

[0003] 现有技术中，用户预先设置一串字符作为密码，在需要进行认证时再输入一串字符，若两次输入的字符串或指纹一致，则判定当前用户为合法用户。

[0004] 在实现本发明的过程中，发明人发现现有技术至少存在以下问题：

[0005] 用户在输入字符串密码时，很容易被不法分子窥视窃取，不法分子只要使用窥视得来的字符串密码即可通过身份验证，因此安全性不高。

发明内容

[0006] 为了解决现有技术的问题，本发明实施例提供了一种身份验证方法及装置。所述技术方案如下：

[0007] 一方面，提供了一种身份验证方法，所述方法包括：

[0008] 获取用户输入的对指定账号的待验证信息；

[0009] 获取所述用户输入过程中对终端上触摸屏的按压力度数据；

[0010] 当所述待验证信息验证通过且所述按压力度数据与所述指定账号的预设按压力度数据一致时，确定所述用户通过身份验证。

[0011] 另一方面，提供了一种身份验证装置，所述装置包括：

[0012] 第一获取模块，用于获取用户输入的对指定账号的待验证信息；

[0013] 第二获取模块，用于获取所述用户输入过程中对终端上触摸屏的按压力度数据；

[0014] 验证模块，用于当所述第一获取模块获取的所述待验证信息验证通过且所述第二获取模块获取的所述按压力度数据与所述指定账号的预设按压力度数据一致时，确定所述用户通过身份验证。

[0015] 本发明实施例提供的技术方案带来的有益效果是：

[0016] 通过终端在获取用户输入的待验证信息的同时，获取用户输入待验证信息时对触摸屏的按压力度数据，并且利用待验证信息和按压力度数据同时对用户的身份进行验证，由于不法分子无法窥视窃取按压力度数据，使得即使用户账号的验证信息泄露，不法分子也无法利用泄露的验证信息通过身份验证，从而可以保障用户的账号安全。

附图说明

[0017] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于

本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0018] 图1是本发明实施例提供的一种身份验证方法流程图。

[0019] 图2是本发明实施例提供的一种身份验证方法流程图。

[0020] 图3是本发明实施例提供的一种身份验证信息设置交互图。

[0021] 图4是本发明实施例提供的一种身份验证交互图。

[0022] 图5是本发明实施例提供的一种身份验证装置结构示意图。

[0023] 图6是本发明实施例提供的一种身份验证装置结构示意图。

[0024] 图7是本发明实施例提供的一种终端的框图。

具体实施方式

[0025] 为使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明实施方式作进一步地详细描述。

[0026] 本发明提供了一种身份验证方法，适用于终端中，尤其适用于配置有Force touch(压力感应触控)触摸传感技术触摸屏的终端中。该身份验证方法可以应用于移动设备认证解锁、移动金融服务支付、应用账号认证等领域。Force Touch技术是一项全新的触摸传感技术，通过Force Touch技术，终端可以获取用户按压触摸屏的按压力度数据，例如触摸力度、轻压力度、重压力度等，终端可以记录该按压力度数据或者根据该按压力度数据执行相应的操作。

[0027] 在Force Touch技术中，用户按压的触摸屏的四个角上各自配置一个压力传感器，该压力传感器可以检测用户的按压力度，终端按照不同的按压力度反馈不同的触觉震动，因此，在使用Force Touch技术时，只有用户本人能感觉到按压的力度效果，而其他人则无法获知用户按压的力度。将Force Touch技术应用于身份验证中，获取用户输入待验证信息时对触摸屏的按压力度数据，可以给验证信息赋予额外的按压力度信息，从而增加了验证信息的维度，使其难以泄露和被不法分子破解。

[0028] 图1是根据一示例性实施例示出的一种身份验证方法的流程图，如图1所示，该身份验证方法用于终端中，包括以下步骤。

[0029] 110、终端获取用户输入的对指定账号的待验证信息。

[0030] 120、终端获取该用户输入过程中对终端上触摸屏的按压力度数据。

[0031] 130、当该待验证信息验证通过且该按压力度数据与该指定账号的预设按压力度数据一致时，终端确定该用户通过身份验证。

[0032] 综上所述，本实施例提供的身份验证方法，通过终端在获取用户输入的待验证信息的同时，获取用户输入待验证信息时对触摸屏的按压力度数据，并且利用待验证信息和按压力度数据同时对用户的身份进行验证，由于不法分子无法窥视窃取按压力度数据，使得即使用户账号的验证信息泄露，不法分子也无法利用泄露的验证信息通过身份验证，从而可以保障用户的账号安全。

[0033] 在第一种可能的实施方式中，该待验证信息为密码信息、验证码信息或指纹信息。

[0034] 在第二种可能的实施方式中，获取用户输入的待验证信息之前，上述身份验证方法还包括：

[0035] 在身份验证信息设置过程中，存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据。

[0036] 在第三种可能的实施方式中，上述身份验证方法还包括：

[0037] 在身份验证信息设置过程中，获取该用户在至少两次输入身份验证信息过程中对该终端上触摸屏的按压力度数据；

[0038] 当该至少两次输入身份验证信息过程中所获取到的按压力度数据一致时，执行存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据的步骤。

[0039] 在第四种可能的实施方式中，该存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据包括：

[0040] 在该终端中存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据；

[0041] 或者，

[0042] 将用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据发送至指定服务器，以使该指定服务器进行存储。

[0043] 在第五种可能的实施方式中，该获取该用户输入过程中对终端上触摸屏的按压力度数据包括：

[0044] 每检测到一个字符输入行为，获取该字符输入行为的对终端上触摸屏的按压力度数据。

[0045] 上述所有可选技术方案，可以采用任意结合形成本公开的可选实施例，在此不再一一赘述。

[0046] 图2是根据一示例性实施例示出的一种身份验证方法的流程图，如图2所示，该身份验证方法用于终端中，包括以下步骤。

[0047] 210、在身份验证信息设置过程中，终端获取用户在至少两次输入身份验证信息过程中对终端上触摸屏的按压力度数据。当该至少两次输入身份验证信息过程中所获取到的按压力度数据一致时，执行步骤220。

[0048] 在身份验证信息设置的过程中，用户实际输入的按压力度数据和想要输入的按压力度数据可能并不一致，也即是用户可能出现误输入的情况，一旦用户在身份验证信息设置过程中出现了误输入的情况，就会导致后续身份验证失败，因此，本发明在身份验证信息设置过程中，获取用户在至少两次输入身份验证信息过程中对终端上触摸屏的按压力度数据，以最大限度地避免用户误输入。

[0049] 其中，上述身份验证信息可以是密码、验证码(如短信验证码或通过用户的选中操作确定的图形验证码或其他形式的验证码等)或指纹等，本发明对此不做具体限定；根据用户手指在触摸屏上按压力度的程度不同，上述对终端上触摸屏的按压力度数据可以分为触摸力度、轻压力度、重压力度等，不同的按压力度数据可以对应不同的按压压强分段，例如：按压压强为10Pa-20Pa为触摸力度、20Pa-30Pa为轻压力度、30Pa-40Pa为重压力度，当然，按压力度数据并不仅限于上述的触摸力度、轻压力度和重压力度，其分割的等级越细致，身份验证的安全性越好，本公开对此也不做具体限定。

[0050] 输入身份验证信息过程中对终端上触摸屏的按压力度数据具体指的是用户在输

入每一个字符时对触摸屏的按压力度数据，例如：以身份验证信息为密码为例，若用户输入的密码为“1234”，则其对应的按压力度数据可以为“轻压力度、重压力度、轻压力度、重压力度”。

[0051] 下面，本发明以移动金融服务中密码的设置过程为例，对步骤210的技术过程进行详细说明，如图3所示。

[0052] 终端检测到移动金融服务密码设置选项的触发操作后，或终端检测到用户首次登陆移动金融客户端时，显示密码设置界面，该密码设置界面包括压控密码设置选项，终端检测到对该压控密码设置选项的触发操作后，显示密码输入界面，该密码输入界面包括密码输入框，终端检测到对该密码输入框的触发后，获取用户输入的密码以及用户在输入密码过程中对终端触摸屏的按压力度数据，而后终端再次显示密码输入界面，该界面仍然包括密码输入框，当终端检测到对该密码输入框的触发后，再次获取用户输入的密码以及用户在输入密码过程中对终端触摸屏的按压力度数据，若两次获取的密码一致且按压力度数据一致，上述按压力度数据一致指的是终端两次获取的按压力度数据误差在预设阈值范围内，上述预设阈值范围可以根据Force Touch触摸屏的灵敏度、用户的使用习惯等由技术人员或用户自己设定，本发明对此不做具体限定，则密码设置完成，终端在本地或指定服务器中对密码进行存储，若两次获取的密码不一致或按压力度数据不一致，则终端显示密码设置失败界面，并提示用户重新进行密码设置。

[0053] 在本发明的一个实施例中，在密码设置完成后，该方法还可以包括，终端显示密码设置成功界面，在该密码设置成功界面上显示用户输入的密码和按压力度数据，例如，该密码设置成功界面可显示“1234”和“轻压力度、重压力度、轻压力度、重压力度”，这样可以加深用户对密码和按压力度数据的记忆，防止用户误操作。

[0054] 当然，用户也可以针对指定账号设置个性化的按压力度模型，该按压力度模型是指用户设置的身份验证信息及每一个身份验证信息字符对应的按压力度数据，终端获取该按压力度模型后，将该按压力度模型发送至指定服务器进行存储，当用户需要在其他Force Touch设备上针对上述指定账号进行身份验证时，即可将用户输入的身份验证信息和按压力度数据发送至该指定服务器，由该指定服务器比较用户输入的身份验证信息和按压力度数据与按压力度模型是否一致，若一致，则服务器确定当前用户身份验证通过。

[0055] 需要说明的是，身份验证信息为验证码、指纹等的设置过程与上述密码的设置过程类似，在此本发明将不再一一赘述。

[0056] 在本发明中，用户在身份验证信息设置过程中，可以如步骤210所述终端获取用户在至少两次输入身份验证信息过程中对终端上触摸屏的按压力度数据，终端也可以仅仅获取用户在一次输入身份验证信息过程中对终端上触摸屏的按压力度数据，对此本发明不做具体限定。

[0057] 220、在身份验证信息设置过程中，终端存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据。

[0058] 在设置完成时，终端将用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据进行存储。在本发明的一个实施例中，为了保证存储安全，终端首先将上述身份验证信息和按压力度数据进行加密，而后再存储加密后的身份验证信息和按压力度数据。上述加密过程可以采用DES(Data Encryption Standard，

数据加密标准)、DSA(Digital Signature Algorithm,数字签名算法)等加密算法,对此本发明不做具体限定。

[0059] 需要说明的是,对于不同应用来说,由于其身份验证信息可以不同,所获取到的按压力度数据也可以不同,相应地,不同应用的身份验证信息以及按压力度数据的存储位置可以不同。当然,对于一个终端上多个应用,还可以具有相同的按压力度数据,以使得在其验证过程中,可以应用相同的按压力度数据对其进行验证。

[0060] 在本发明的一个实施例中,步骤220还可以包括步骤220A或步骤220B的内容。

[0061] 步骤220A、在该终端中存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据。

[0062] 终端可以设置有指定文件夹、指定存储路径等,以供上述身份验证信息以及按压力度数据的存储。

[0063] 当然,上述身份验证信息以及按压力度数据,或者上述按压力度模型,还可以存储于指定服务器中,这样用户在不同的终端进行身份验证时,相应的终端就可以通过访问该指定服务器获取用户的身份验证信息以及按压力度数据,从而方便用户随时随地利用不同的终端进行身份验证,因此,上述步骤220A也可以被步骤220B替代。

[0064] 步骤220B、终端将用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据发送至指定服务器,以使该指定服务器进行存储。

[0065] 下面本发明将对步骤220B的具体技术过程进行说明。

[0066] 终端向指定服务器发送身份验证信息存储请求,该身份验证信息存储请求携带用户账号、身份验证信息以及按压力度数据,指定服务器接收该身份验证信息存储请求,并从该身份验证信息存储请求中提取出用户账号、身份验证信息以及按压力度数据,而后指定服务器将上述提取出的各项数据存储入验证信息数据库中,并以用户账号作为身份验证信息以及按压力度数据的索引信息。当然,上述身份验证信息存储请求中也可以携带用户账号和按压力度模型,以使该指定服务器对上述用户账号和按压力度模型进行存储。

[0067] 在本发明的一个实施例中,在将用户账号、身份验证信息以及按压力度数据存储入验证信息数据库之前,指定服务器还可以对该身份验证信息以及按压力度数据进行加密,或者,终端在向指定服务器发送身份验证信息存储请求之前,对身份验证信息以及按压力度数据进行加密,该身份验证信息存储请求携带用户账号及加密后的身份验证信息以及按压力度数据。

[0068] 230、终端获取用户输入的对指定账号的待验证信息。

[0069] 当用户需要对移动设备进行解锁、登录应用账号或者进行移动金融支付等需要身份验证的时候,终端需要获取用户输入的指定账号的待验证信息以供终端进行身份验证。在本发明的一个实施例中,该待验证信息可以为密码信息、验证码信息或指纹信息。

[0070] 240、终端获取该用户输入过程中对终端上触摸屏的按压力度数据。

[0071] 同时,在身份验证过程中,终端也需要获取用户输入上述待验证信息的过程中对终端上触摸屏的按压力度数据。

[0072] 下面本发明将对步骤230和步骤240的技术过程进行说明,以移动金融服务中根据密码进行身份验证的情形为例。

[0073] 在移动金融客户端中,用户在进行转账、付款等交易前,终端需要对当前用户的身

份进行验证，以保护用户的财产安全，例如，当终端检测到移动金融客户端的转账操作时，即显示身份验证界面，在该身份验证界面中包含压控密码身份验证选项，当终端检测到对该压控密码身份验证选项的触发操作后，显示压控密码身份验证界面，所述压控密码身份验证界面包含密码输入框，当终端检测到对该密码输入框的触发后，获取用户输入的密码及用户输入密码时对触摸屏的按压力度数据。

[0074] 在本发明的一个实施例中，步骤240可以包括：每检测到一个字符输入行为，终端获取该字符输入行为的对终端上触摸屏的按压力度数据。

[0075] 也即是，若待验证信息包含六个字符，则终端获取用户输入每一个字符时的按压力度数据，例如，用户输入的待验证信息为“123456”，则终端获取的按压力度数据可以为“轻压力度、轻压力度、轻压力度、重压力度、轻压力度、轻压力度”。

[0076] 250、当该待验证信息验证通过且该按压力度数据与该指定账号的预设按压力度数据一致时，终端确定该用户通过身份验证。

[0077] 上述预设按压力度数据即为身份验证信息设置过程中，存储在终端或指定服务器上的，在输入验证信息时用户对终端触摸屏的按压力度数据。上述该按压力度数据与该指定账号的预设按压力度数据一致具体指的是，该按压力度数据与预设按压力度数据的误差在预设阈值范围内，上述预设阈值范围可以根据Force Touch触摸屏的灵敏度、用户的使用习惯等由技术人员或用户自己设定，本发明对此不做具体限定。

[0078] 在本发明的一个实施例中，若该待验证信息验证不通过或该按压力度数据与该指定账号的预设按压力度数据不一致，则终端可以再次获取用户重新输入的待验证信息和按压力度数据，若用户在预设次数内输入的验证信息和按压力度数据仍然不能通过身份验证，则终端将锁定该指定账号，也即是不允许用户在预设时间范围内针对该指定账号再次进行身份验证。在本发明的一个实施例中，终端在锁定该指定账号之后，可以从存储有指定账号与联系方式的账号数据库中，获取与该指定账号绑定的联系方式，如手机号码、即时通信账号等，进而通过短信、即时通信或者电话的方式向用户发送账号异常通知，以使用户可以及时发现指定账号存在安全风险，从而及时修改身份验证信息和按压力度数据。

[0079] 下面本发明将对步骤250的技术过程进行说明，如图4所示，仍然以移动金融服务中根据密码进行身份验证的情形为例。

[0080] 终端在获取用户输入的对指定账号的待验证信息和按压力度数据之后，以该指定账号为索引，向终端或指定服务器查询并获取该指定账号对应的验证信息和按压力度数据，而后终端将用户输入的待验证信息和从终端或指定服务器中获取的验证信息进行对比，若对比结果为二者一致，则对用户输入的按压力度数据和从终端或指定服务器中获取的按压力度数据进行对比，若对比结果为二者的误差在预设阈值范围内，则终端确定当前用户为合法用户。

[0081] 需要说明的是，若上述验证信息以及与其对应的按压力度数据存储于指定服务器中，则确定用户是否通过身份验证的执行主体可以为该指定服务器，具体技术过程与终端为执行主体的技术过程类似，在此本发明不再一一赘述。

[0082] 综上所述，本实施例提供的身份验证方法，通过终端在获取用户输入的待验证信息的同时，获取用户输入待验证信息时对触摸屏的按压力度数据，并且利用待验证信息和按压力度数据同时对用户的身份进行验证，由于不法分子无法窥视窃取按压力度数据，使

得即使用户账号的验证信息泄露，不法分子也无法利用泄露的验证信息通过身份验证，从而可以保障用户的账号安全。

[0083] 图5是根据一示例性实施例示出的一种身份验证装置500框图。参照图5，该装置包括第一获取模块510、第二获取模块520、验证模块530。

[0084] 该第一获取模块510，用于获取用户输入的对指定账号的待验证信息。

[0085] 在本发明的一个实施例中，该待验证信息为密码信息、验证码信息或指纹信息。

[0086] 该第二获取模块520，用于获取该用户输入过程中对终端上触摸屏的按压力度数据。

[0087] 在本发明的一个实施例中，第二获取模块520还用于每检测到一个字符输入行为，获取该字符输入行为的对终端上触摸屏的按压力度数据。

[0088] 该验证模块530，用于当该第一获取模块510获取的该待验证信息验证通过且该第二获取模块520获取的该按压力度数据与该指定账号的预设按压力度数据一致时，确定该用户通过身份验证。

[0089] 参见图6，在本发明的另一个实施例中，还提供了另一种身份验证装置600，该装置基于上述图5的实施例结构，还包括存储模块540和设置模块550。

[0090] 该存储模块540，用于在身份验证信息设置过程中，存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据。

[0091] 在本发明的一个实施例中，该存储模块540用于，在该终端中存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据。

[0092] 该存储模块540还用于，将用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据发送至指定服务器，以使该指定服务器进行存储。

[0093] 该设置模块550，用于在身份验证信息设置过程中，获取该用户在至少两次输入身份验证信息过程中对该终端上触摸屏的按压力度数据。

[0094] 该设置模块550，还用于当该至少两次输入身份验证信息过程中所获取到的按压力度数据一致时，将用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据存入该存储模块540。

[0095] 综上所述，本实施例提供的身份验证装置，通过第一获取模块获取用户输入的待验证信息，第二获取模块获取用户输入待验证信息时对触摸屏的按压力度数据，并且验证模块利用待验证信息和按压力度数据同时对用户的身份进行验证，由于不法分子无法窥视窃取按压力度数据，使得即使用户账号的验证信息泄露，不法分子也无法利用泄露的验证信息通过身份验证，从而可以保障用户的账号安全。

[0096] 需要说明的是：上述实施例提供的身份验证装置在验证用户身份时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的身份验证装置与身份验证方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0097] 本实施例提供了一种终端，该终端可以用于执行上述各个实施例中提供的身份验证方法。参见图7，该终端700包括：

[0098] 终端700可以包括RF(Radio Frequency,射频)电路710、包括有一个或一个以上计算机可读存储介质的存储器720、输入单元730、显示单元740、传感器750、音频电路760、WiFi(Wireless Fidelity,无线保真)模块750、包括有一个或者一个以上处理核心的处理器780、以及电源790等部件。本领域技术人员可以理解,图7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。其中:

[0099] RF电路710可用于收发信息或通话过程中,信号的接收和发送,特别地,将基站的下行信息接收后,交由一个或者一个以上处理器780处理;另外,将涉及上行的数据发送给基站。通常,RF电路710包括但不限于天线、至少一个放大器、调谐器、一个或多个振荡器、用户身份模块(SIM)卡、收发信机、耦合器、LNA(Low Noise Amplifier,低噪声放大器)、双工器等。此外,RF电路710还可以通过无线通信与网络和其他设备通信。所述无线通信可以使用任一通信标准或协议,包括但不限于GSM(Global System of Mobile communication,全球移动通讯系统)、GPRS(General Packet Radio Service,通用分组无线服务)、CDMA(Code Division Multiple Access,码分多址)、WCDMA(Wideband Code Division Multiple Access,宽带码分多址)、LTE(Long Term Evolution,长期演进)、电子邮件、SMS(Short Messaging Service,短消息服务)等。

[0100] 存储器720可用于存储软件程序以及模块,处理器780通过运行存储在存储器720的软件程序以及模块,从而执行各种功能应用以及数据处理。存储器720可主要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(比如声音播放功能、图像播放功能等)等;存储数据区可存储根据终端700的使用所创建的数据(比如音频数据、电话本等)等。此外,存储器720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,例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地,存储器720还可以包括存储器控制器,以提供处理器780和输入单元730对存储器720的访问。

[0101] 输入单元730可用于接收输入的数字或字符信息,以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。具体地,输入单元730可包括触敏表面731以及其他输入设备732。触敏表面731,也称为触摸显示屏或者触控板,可收集用户在其上或附近的触摸操作(比如用户使用手指、触笔等任何适合的物体或附件在触敏表面731上或在触敏表面731附近的操作),并根据预先设定的程式驱动相应的连接装置。可选的,触敏表面731可包括触摸检测装置和触摸控制器两个部分。其中,触摸检测装置检测用户的触摸方位,并检测触摸操作带来的信号,将信号传送给触摸控制器;触摸控制器从触摸检测装置上接收触摸信息,并将它转换成触点坐标,再送给处理器780,并能接收处理器780发来的命令并加以执行。此外,可以采用电阻式、电容式、红外线以及表面声波等多种类型实现触敏表面731。除了触敏表面731,输入单元730还可以包括其他输入设备732。具体地,其他输入设备732可以包括但不限于物理键盘、功能键(比如音量控制按键、开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0102] 显示单元740可用于显示由用户输入的信息或提供给用户的信息以及终端700的各种图形用户接口,这些图形用户接口可以由图形、文本、图标、视频和其任意组合来构成。显示单元740可包括显示面板741,可选的,可以采用LCD(Liquid Crystal Display,液晶显

示器)、OLED(Organic Light-Emitting Diode,有机发光二极管)等形式来配置显示面板741。进一步的,触敏表面731可覆盖显示面板741,当触敏表面731检测到在其上或附近的触摸操作后,传送给处理器780以确定触摸事件的类型,随后处理器780根据触摸事件的类型在显示面板741上提供相应的视觉输出。虽然在图7中,触敏表面731与显示面板741是作为两个独立的部件来实现输入和输入功能,但是在某些实施例中,可以将触敏表面731与显示面板741集成而实现输入和输出功能。

[0103] 终端700还可包括至少一种传感器750,比如光传感器、运动传感器以及其他传感器。具体地,光传感器可包括环境光传感器及接近传感器,其中,环境光传感器可根据环境光线的明暗来调节显示面板741的亮度,接近传感器可在终端700移动到耳边时,关闭显示面板741和/或背光。作为运动传感器的一种,重力加速度传感器可检测各个方向上(一般为三轴)加速度的大小,静止时可检测出重力的大小及方向,可用于识别手机姿态的应用(比如横竖屏切换、相关游戏、磁力计姿态校准)、振动识别相关功能(比如计步器、敲击)等;至于终端700还可配置的陀螺仪、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。

[0104] 音频电路760、扬声器761,传声器762可提供用户与终端700之间的音频接口。音频电路760可将接收到的音频数据转换后的电信号,传输到扬声器761,由扬声器761转换为声音信号输出;另一方面,传声器762将收集的声音信号转换为电信号,由音频电路760接收后转换为音频数据,再将音频数据输出处理器780处理后,经RF电路710以发送给比如另一终端,或者将音频数据输出至存储器720以便进一步处理。音频电路760还可能包括耳塞插孔,以提供外设耳机与终端700的通信。

[0105] WiFi属于短距离无线传输技术,终端700通过WiFi模块750可以帮助用户收发电子邮件、浏览网页和访问流式媒体等,它为用户提供了无线的宽带互联网访问。虽然图7示出了WiFi模块750,但是可以理解的是,其并不属于终端700的必须构成,完全可以根据需要在不改变发明的本质的范围内而省略。

[0106] 处理器780是终端700的控制中心,利用各种接口和线路连接整个手机的各个部分,通过运行或执行存储在存储器720内的软件程序和/或模块,以及调用存储在存储器720内的数据,执行终端700的各种功能和处理数据,从而对手机进行整体监控。可选的,处理器780可包括一个或多个处理核心;优选的,处理器780可集成应用处理器和调制解调处理器,其中,应用处理器主要处理操作系统、用户界面和应用程序等,调制解调处理器主要处理无线通信。可以理解的是,上述调制解调处理器也可以不集成到处理器780中。

[0107] 终端700还包括给各个部件供电的电源790(比如电池),优选的,电源可以通过电源管理系统与处理器780逻辑相连,从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源790还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

[0108] 尽管未示出,终端700还可以包括摄像头、蓝牙模块等,在此不再赘述。具体在本实施例中,终端的显示单元是触摸屏显示器,终端还包括有存储器,以及一个或者一个以上的程序,其中一个或者一个以上程序存储于存储器中,且经配置以由一个或者一个以上处理器执行。所述一个或者一个以上程序包含用于执行以下操作的指令:获取用户输入的对指定账号的待验证信息;获取该用户输入过程中对终端上触摸屏的按压力度数据;当该待验

证信息验证通过且该按压力度数据与该指定账号的预设按压力度数据一致时，确定该用户通过身份验证。

[0109] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0110] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

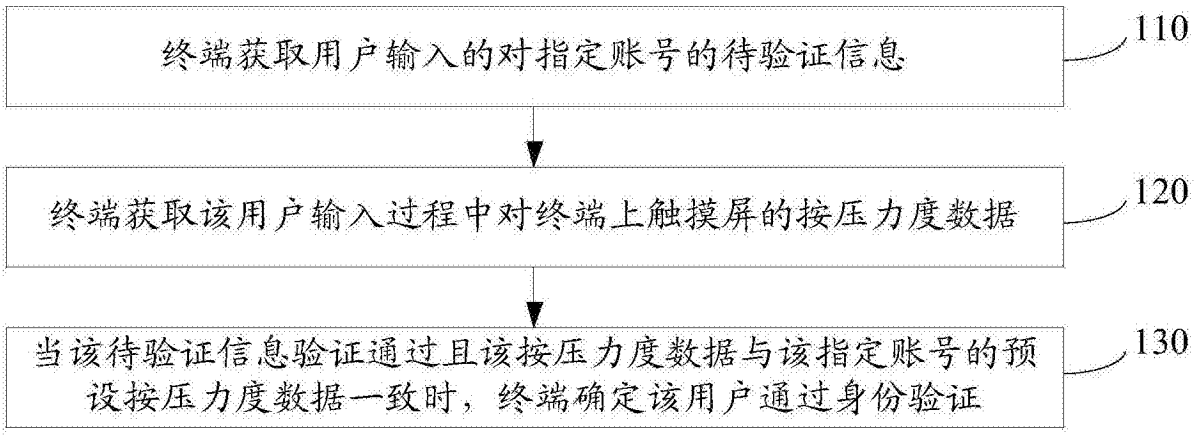

终端获取用户输入的对指定账号的待验证信息
110
终端获取该用户输入过程中对终端上触摸屏的按压力度数据
120
当该待验证信息验证通过且该按压力度数据与该指定账号的预设按压力度数据一致时，终端确定该用户通过身份验证
130

图1

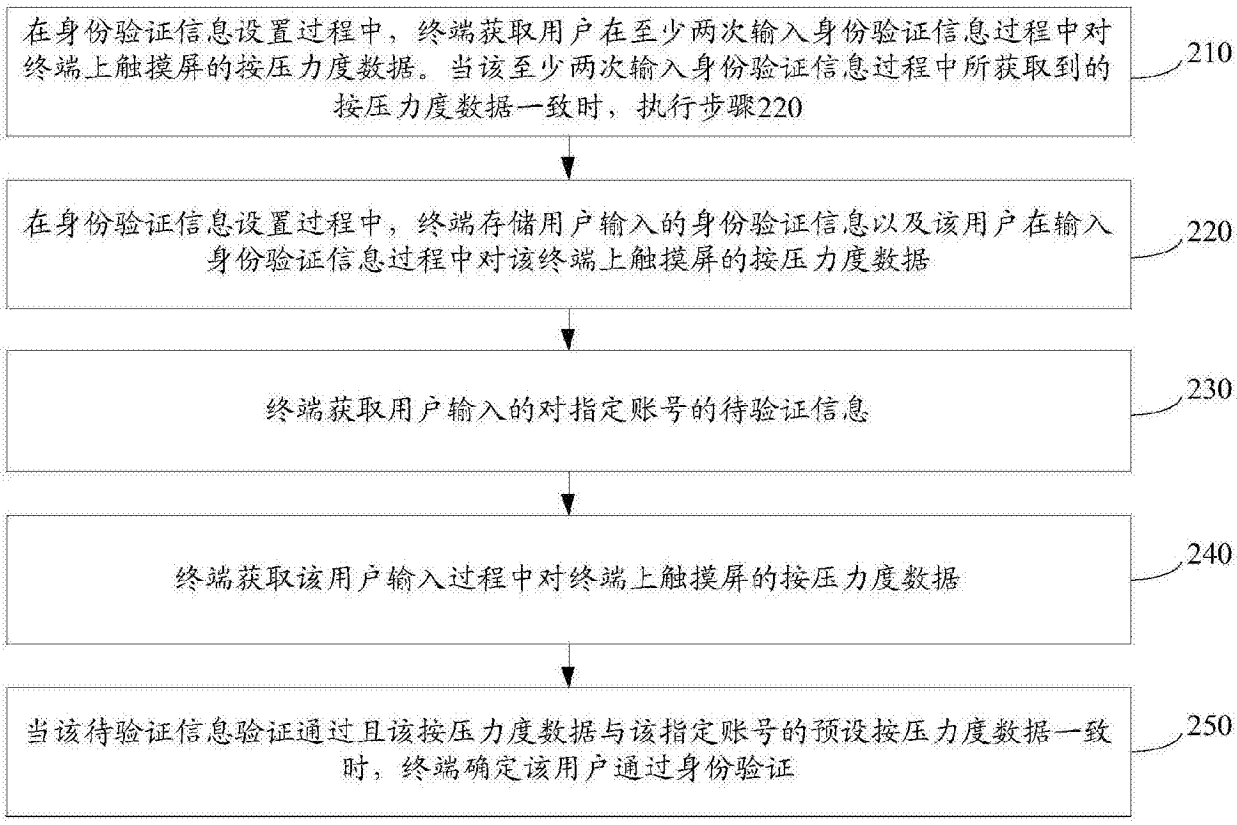

在身份验证信息设置过程中，终端获取用户在至少两次输入身份验证信息过程中对终端上触摸屏的按压力度数据。当该至少两次输入身份验证信息过程中所获取到的按压力度数据一致时，执行步骤220
210
在身份验证信息设置过程中，终端存储用户输入的身份验证信息以及该用户在输入身份验证信息过程中对该终端上触摸屏的按压力度数据
220
终端获取用户输入的对指定账号的待验证信息
230
终端获取该用户输入过程中对终端上触摸屏的按压力度数据
240
当该待验证信息验证通过且该按压力度数据与该指定账号的预设按压力度数据一致时，终端确定该用户通过身份验证
250

图2


用户
输入
触摸屏
存储
终端或指定服务器

图3


用户
输入
触摸屏
对比
结果
终端或指定服务器

图4

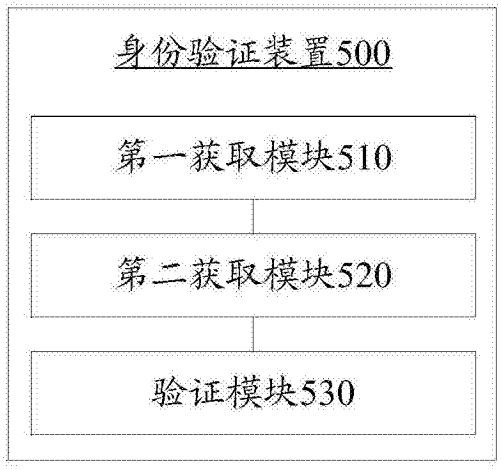

身份验证装置500
第一获取模块510
第二获取模块520
验证模块530

图5


身份验证装置600
设置模块550
存储模块540
第一获取模块510
第二获取模块520
验证模块530

图6

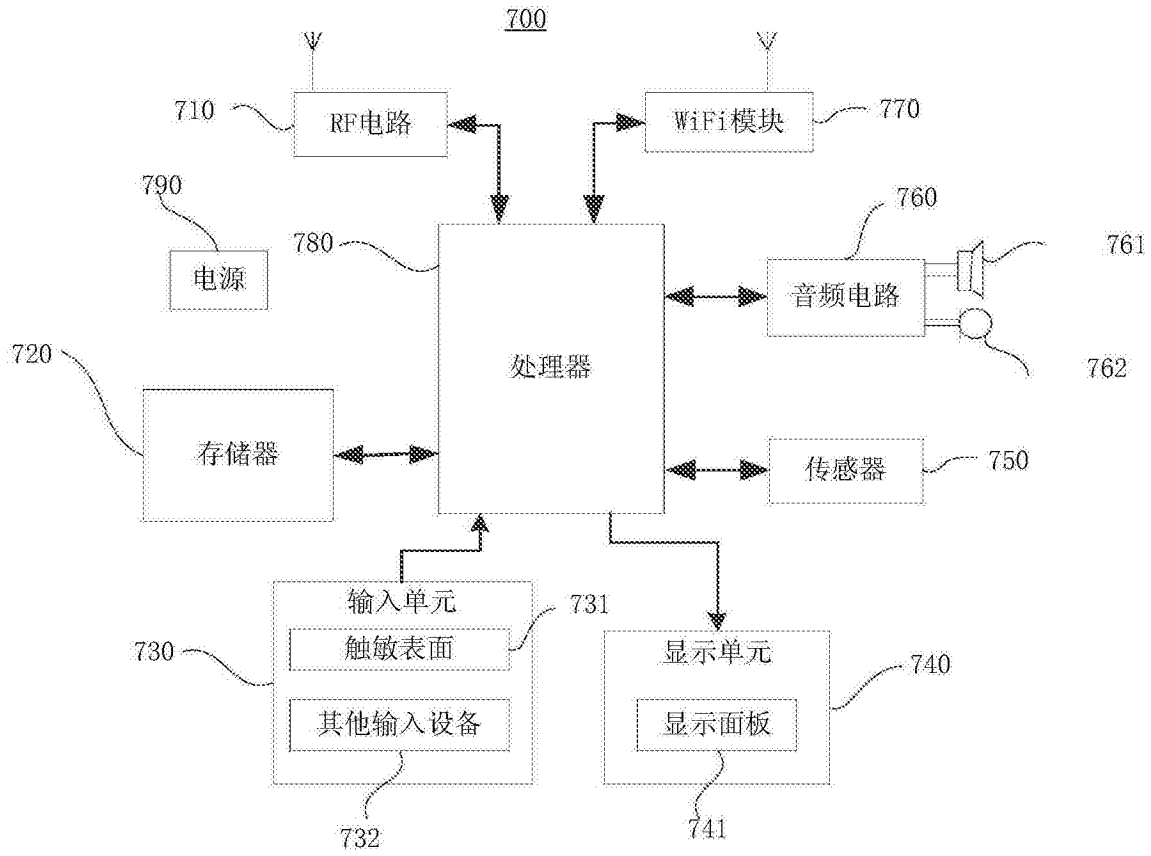

700
710
RF电路
WiFi模块
770
790
电源
780
760
761
音频电路
处理器
762
720
存储器
传感器
750
输入单元
731
730
触敏表面
显示单元
740
其他输入设备
显示面板
732
741

图7