(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 107707554 A
(43)申请公布日 2018.02.16

(21)申请号 201710972655.9

(22)申请日 2017.10.18

(71)申请人 维沃移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙步步高大道283号

(72)发明人 刘朝辉

(74)专利代理机构 北京润泽恒知识产权代理有限公司 11319
代理人 王洪

(51)Int.Cl.
H04L 29/06(2006.01)
H04M 1/725(2006.01)

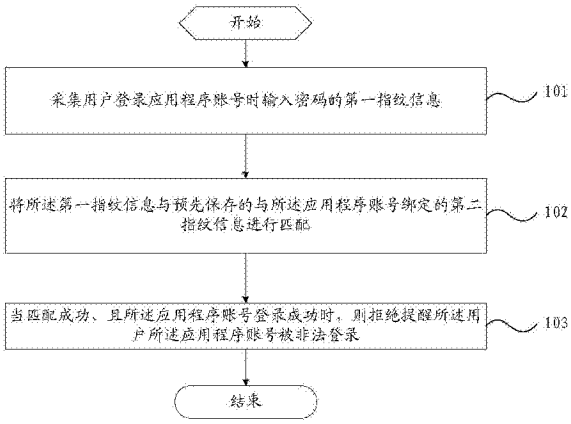
权利要求书3页 说明书10页 附图2页

(54)发明名称

一种应用程序账号的登录方法及移动终端

(57)摘要

本发明提供了一种应用程序账号的登录方法及移动终端。该方法包括：采集用户登录应用程序账号时输入密码的第一指纹信息；将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指纹信息进行匹配；当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。本发明通过预先保存与应用程序账号绑定的第二指纹信息，并将采集到的登录该应用程序账号时输入密码的第一指纹信息与该第二指纹信息相匹配，若匹配一致，则拒绝提醒用户该应用程序账号被非法登录，避免对用户造成干扰。



CN 107707554 A

1.一种应用程序账号的登录方法，应用于具有屏幕指纹识别功能指的移动终端，其特征在于，所述方法包括：

采集用户登录应用程序账号时输入密码的第一指纹信息；

将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指纹信息进行匹配；

当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。

2.根据权利要求1所述的方法，其特征在于，所述采集用户登录应用程序账号时输入密码的第一指纹信息之前，所述方法还包括：

采集所述用户首次登录所述应用程序账号时输入密码的第三指纹信息；

当所述第三指纹信息采集成功、且所述应用程序账号登录成功时，将所述第三指纹信息与所述应用程序账号绑定存储。

3.根据权利要求2所述的方法，其特征在于，所述采集所述用户首次登录所述应用程序账号时输入密码的第三指纹信息之后，所述方法还包括：

当所述第三指纹信息采集失败、且所述应用程序账号登录成功时，判断本地是否存储有所述移动终端的解锁指纹信息；

若所述本地存储有所述移动终端的解锁指纹信息，则将所述解锁指纹信息与所述应用程序账号绑定存储；

若所述本地未存储有所述移动终端的解锁指纹信息，则采集使用所述移动终端的第四指纹信息，按照预设条件对所述第四指纹信息进行筛选，将筛选得到的第四指纹信息与所述应用程序账号绑定存储。

4.根据权利要求2或3所述的方法，其特征在于，在将指纹信息与所述应用程序账号绑定存储之后，所述方法还包括：

将与所述应用程序账号绑定存储的指纹信息，标记为所述应用程序账号的主用户指纹。

5.根据权利要求4所述的方法，其特征在于，所述将与所述应用程序账号绑定存储的指纹信息，标记为所述应用程序账号的主用户指纹之后，所述方法还包括：

根据所述用户的预设指纹管理操作，展示所述移动终端中处于已登录状态的所有应用程序账号；

根据所述用户对所述所有应用程序账号中目标应用程序账号的选择操作，获取所述目标应用程序账号的主用户指纹；

根据所述用户对所述目标应用程序账号的成员指纹添加操作，采集成员指纹以及所述用户的指纹信息；

将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

若匹配成功，则将采集到的所述成员指纹与所述目标应用程序账号绑定存储。

6.根据权利要求5所述的方法，其特征在于，所述根据所述用户对所述所有应用程序账号中目标应用程序账号的选择操作，获取所述目标应用程序账号的主用户指纹之后，所述方法还包括：

根据所述用户对所述目标应用程序账号的目标成员指纹的删除操作，采集所述用户的

指纹信息；

将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

若匹配成功，则将与所述目标应用程序账号绑定存储的成员指纹中的所述目标成员指纹删除。

7.一种移动终端，其特征在于，所述移动终端具有屏幕指纹识别功能，所述移动终端包括：

第一采集模块，用于采集用户登录应用程序账号时输入密码的第一指纹信息；

第一匹配模块，用于将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指纹信息进行匹配；

拒绝提醒模块，用于当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。

8.根据权利要求7所述的移动终端，其特征在于，所述移动终端还包括：

第二采集模块，用于采集所述用户首次登录所述应用程序账号时输入密码的第三指纹信息；

第一存储模块，用于当所述第三指纹信息采集成功、且所述应用程序账号登录成功时，将所述第三指纹信息与所述应用程序账号绑定存储。

9.根据权利要求8所述的移动终端，其特征在于，所述移动终端还包括：

判断模块，用于当所述第三指纹信息采集失败、且所述应用程序账号登录成功时，判断本地是否存储有所述移动终端的解锁指纹信息；

第二存储模块，用于若所述本地存储有所述移动终端的解锁指纹信息，则将所述解锁指纹信息与所述应用程序账号绑定存储；

筛选模块，用于若所述本地未存储有所述移动终端的解锁指纹信息，则采集使用所述移动终端的第四指纹信息，按照预设条件对所述第四指纹信息进行筛选，将筛选得到的第四指纹信息与所述应用程序账号绑定存储。

10.根据权利要求8或9所述的移动终端，其特征在于，所述移动终端还包括：

标记模块，用于将与所述应用程序账号绑定存储的指纹信息，标记为所述应用程序账号的主用户指纹。

11.根据权利要求10所述的移动终端，其特征在于，所述移动终端还包括：

展示模块，用于根据所述用户的预设指纹管理操作，展示所述移动终端中处于已登录状态的所有应用程序账号；

获取模块，用于根据所述用户对所述所有应用程序账号中目标应用程序账号的选择操作，获取所述目标应用程序账号的主用户指纹；

第三采集模块，用于根据所述用户对所述目标应用程序账号的成员指纹添加操作，采集成员指纹以及所述用户的指纹信息；

第二匹配模块，用于将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

第三存储模块，用于若匹配成功，则将采集到的所述成员指纹与所述目标应用程序账号绑定存储。

12.根据权利要求11所述的移动终端，其特征在于，所述移动终端还包括：

第四采集模块，用于根据所述用户对所述目标应用程序账号的目标成员指纹的删除操作，采集所述用户的指纹信息；

第三匹配模块，用于将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

删除模块，用于若匹配成功，则将与所述目标应用程序账号绑定存储的成员指纹中的所述目标成员指纹删除。

13.一种移动终端，其特征在于，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计算机程序，所述计算机程序被所述处理器执行时实现如权利要求1至6中任一项所述的应用程序账号的登录方法的步骤。

14.一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计算机程序，所述计算机程序被处理器执行时实现如权利要求1至6中任一项所述的应用程序账号的登录方法中的步骤。

一种应用程序账号的登录方法及移动终端

技术领域

[0001] 本发明涉及账号安全技术领域，尤其涉及一种应用程序账号的登录方法及移动终端。

背景技术

[0002] 随着移动终端(例如，智能手机)的发展，移动终端给我们的生活和工作带来了很多的便利。例如，智能手机上可以安装的应用程序越来越多，每种应用程序都能为用户提供个性化服务，例如即时通讯、视频娱乐、游戏等。而不同的应用程序在使用时都需要注册账号，从而使得用户有很多的应用程序账号。

[0003] 在使用各种应用程序帐号的过程中，为了保证用户的账号安全，当用户面临更换手机登录同一帐号、或者在同一部手机上退出帐号后重新登录、或者使用同一部手机在非常住地(例如外地或外国)登录同一帐号等切换设备或切换常住地的程序登录场景时，应用程序一般会发送短信或者弹出提示框来提醒用户该账号被非法登录。例如发送诸如短信内容为“您正在XX品牌手机上登录XX应用程序，如非本人操作，请及时修改密码。”的短信；或者在应用程序界面弹出内容大致是“您的账号正在XX国家登录，如非本人操作，则密码可能已泄露，建议修改密码或冻结账号。”的提示框。

[0004] 由此可见，现有技术中的应用程序的账号登录方案，一旦面临切换终端设备或者切换地理位置登录同一账号的场景时，就会向用户提醒非法登录信息，从而给用户造成干扰。

发明内容

[0005] 本发明实施例提供一种应用程序账号的登录方法及移动终端，以解决现有技术中的应用程序的账号登录方案所存在的一旦面临切换终端设备或者切换地理位置登录同一账号的场景时，就会向用户提醒非法登录信息，从而给用户造成干扰的问题。

[0006] 为了解决上述技术问题，本发明是这样实现的：

[0007] 第一方面，本发明实施例提供了一种应用程序账号的登录方法，应用于具有屏幕指纹识别功能的移动终端，所述方法包括：

[0008] 采集用户登录应用程序账号时输入密码的第一指纹信息；

[0009] 将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指纹信息进行匹配；

[0010] 当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。

[0011] 第二方面，本发明实施例还提供了一种移动终端，所述移动终端具有屏幕指纹识别功能，所述移动终端包括：

[0012] 第一采集模块，用于采集用户登录应用程序账号时输入密码的第一指纹信息；

[0013] 第一匹配模块，用于将所述第一指纹信息与预先保存的与所述应用程序账号绑定

的第二指纹信息进行匹配；

[0014] 拒绝提醒模块，用于当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。

[0015] 第三方面，本发明实施例还提供了一种移动终端，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计算机程序，所述计算机程序被所述处理器执行时实现所述的应用程序账号的登录方法的步骤。

[0016] 第四方面，本发明实施例还提供了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计算机程序，所述计算机程序被处理器执行时实现所述的应用程序账号的登录方法的步骤。

[0017] 在本发明实施例中，通过预先保存与应用程序账号绑定的第二指纹信息，并将采集到的登录该应用程序账号时输入密码的第一指纹信息与该第二指纹信息相匹配，在匹配一致的情况下，则说明是用户自己在更换设备或者更换位置进行账号登录，此时则拒绝提醒用户该应用程序账号被非法登录，避免了对用户造成干扰的问题。

附图说明

[0018] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例的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性的前提下，还可以根据这些附图获得其他的附图。

[0019] 图1是本发明一个实施例的应用程序账号的登录方法的流程图；

[0020] 图2是本发明一个实施例的移动终端的框图；

[0021] 图3是本发明一个实施例的移动终端的硬件结构示意图。

具体实施方式

[0022] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0023] 参照图1，示出了本发明一个实施例的应用程序账号的登录方法的流程图，应用于具有屏幕指纹识别功能的移动终端，所述方法具体可以包括如下步骤：

[0024] 步骤101，采集用户登录应用程序账号时输入密码的第一指纹信息；

[0025] 其中，当用户1登录某个应用程序时，需要输入程序账号1和对应的密码，而由于本发明实施例的移动终端的屏幕具有指纹识别功能，因此，可以采集输入密码的用户指纹信息，其中，移动终端上具有指纹识别功能的屏幕可以是全屏(所谓全指纹屏则表示该移动终端的屏幕上的任意一个位置都可以采集用户触摸屏幕该位置的指纹)，也可以是部分屏幕区域(但是需要注意的是，部分屏幕区域能够覆盖账号信息的采集区域)。因此，当用户在登录某个应用程序的账号时，本发明实施例的方法可以利用移动终端的屏幕指纹识别功能来采集输入密码的用户的第一指纹信息。

[0026] 步骤102，将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指

纹信息进行匹配；

[0027] 其中，为了避免在切换终端设备或者切换地理位置登录同一应用账号的场景时，现有技术会向用户提醒非法登录信息的问题，本发明实施例的方法可以预先在上述某个应用程序(例如程序1)对应的应用服务器1上保存与程序1的用户账号绑定的用户指纹信息。举例来说，该程序1具有10个注册用户账号(例如程序账号1～程序账号10)，那么本发明实施例的方法可以在应用服务器1和/移动终端上保存10个注册用户账号的用户指纹。

[0028] 那么当面临用户切换终端设备或者切换地理位置登录同一应用账号的场景时，本发明实施例的方法就可以将步骤101采集到的程序账号1的第一指纹信息与应用服务器1上预先保存的与程序账号1绑定的第二指纹信息进行匹配。

[0029] 那么当面临用户切换地理位置登录同一应用账号的场景时，本发明实施例的方法也可以将步骤101采集到的程序账号1的第一指纹信息与移动终端上预先保存的与程序账号1绑定的第二指纹信息进行匹配。

[0030] 步骤103，当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。

[0031] 其中，当第一指纹信息和第二指纹信息匹配成功时，且该程序账号1登录成功，则说明当前登录该程序账号1的用户是经过指纹认证的用户，用户只不过是更换了终端设备或者换了一个地理位置来对自己的程序账号进行登录，此时，本发明实施例的方法可以不触发所述应用程序账号被非法登录的提醒功能，从而实现拒绝提醒所述用户所述应用程序账号被非法登录；或者，本发明实施例的方法也可以触发所述应用程序账号被非法登录的提醒功能，但是对于该提醒功能触发的提醒消息或者提醒内容进行拒绝，从而实现拒绝提醒所述用户所述应用程序账号被非法登录。这样，系统本应该发送提醒账号异常登录的信息，但是本发明实施例的方法会拒绝提醒该用户该程序账号1被非法登录，从而避免对用户造成干扰。

[0032] 在本发明实施例中，通过预先保存与应用程序账号绑定的第二指纹信息，并将采集到的登录该应用程序账号时输入密码的第一指纹信息与该第二指纹信息相匹配，在匹配一致的情况下，则说明是用户自己在更换设备或者更换位置进行账号登录，此时则拒绝提醒用户该应用程序账号被非法登录，避免了对用户造成干扰的问题。

[0033] 可选地，在一个实施例中，在执行步骤101之前，根据本发明实施例的方法还可以包括：

[0034] 采集所述用户首次登录所述应用程序账号时输入密码的第三指纹信息；

[0035] 当所述第三指纹信息采集成功、且所述应用程序账号登录成功时，将所述第三指纹信息与所述应用程序账号绑定存储。

[0036] 具体而言，当用户第一次登录该程序账号时，本发明实施例可以利用例如全指纹屏来采集用户输入密码的指纹信息，即第三指纹信息，那么只有在该第三指纹信息采集成功，且利用该输入的密码也登录该程序账号成功的情况下，本发明实施例的方法才确定该用户为该程序账号的合法用户，从而将其输入密码的第三指纹信息与该用户的程序账号绑定存储，其中，存储位置可以为该应用程序账号对应的应用程序服务器，也可以是移动终端。

[0037] 实质上，这里的第三指纹信息即构成为上述步骤102中应用程序服务器侧或移动

终端侧预先保存的第二指纹信息。

[0038] 这样，本发明实施例可以在用户首次登陆应用程序的程序账号时，采集其输入密码的指纹信息，并在用户登录程序账号成功的情况下，来将采集到的指纹信息与该用户的程序账号绑定存储，从而能够预先存储每个程序账号的用户指纹，从而构成上述第二指纹信息。

[0039] 可选地，在一个实施例中，在所述采集所述用户首次登录所述应用程序账号时输入密码的第三指纹信息的步骤之后，根据本发明实施例的方法还可以包括：

[0040] 当所述第三指纹信息采集失败、且所述应用程序账号登录成功时，判断本地是否存储有所述移动终端的解锁指纹信息；

[0041] 其中，考虑到用户指纹可能存在指纹不清晰导致第三指纹信息录入失败，即采集失败的情况，当第三指纹信息采集失败，且该程序账号登录成功的情况时(即用户输入的程序账号和账号密码都认证成功时)，本发明实施例可以判断移动终端本地是否存储有该移动终端的解锁指纹信息。所谓解锁指纹信息，目前的移动终端当处于锁屏状态时，用户可以通过录入指纹的方式来解锁该移动终端的屏幕使得其屏幕处于亮屏状态并进入主屏幕，而这里录入的能够解锁的指纹就是解锁指纹信息。

[0042] 若所述本地存储有所述移动终端的解锁指纹信息，则将所述解锁指纹信息与所述应用程序账号绑定存储；

[0043] 其中，当移动终端本地存储有该解锁指纹信息时，由于对用户输入账号密码的第三指纹信息采集失败，因此，可以直接将该解锁指纹信息与该程序账号绑定存储至应用程序服务器或移动终端，即，该解锁指纹信息同样可以构成步骤102中的第二指纹信息。其中，由于解锁指纹信息一般为机主或者与机主有亲密关系的用户，因此，该解锁指纹信息可以作为该程序账号的认证指纹(即第二指纹信息)存储至应用程序服务器或移动终端。

[0044] 若所述本地未存储有所述移动终端的解锁指纹信息，则采集使用所述移动终端的第四指纹信息，按照预设条件对所述第四指纹信息进行筛选，将筛选得到的第四指纹信息与所述应用程序账号绑定存储。

[0045] 相反，如果移动终端不支持指纹解锁屏幕或者用户预先未录入解锁指纹信息，从而导致移动终端本地未存储有该移动终端的解锁指纹信息，那么本发明实施例的方法还可以利用例如全指纹屏来采集使用该移动终端的过程中的各个指纹信息(即第四指纹信息)，然后利用预设条件对各个指纹信息进行筛选，将筛选得到的第四指纹信息与该程序账号绑定存储至应用服务器侧或移动终端侧，从而使得该筛选得到的第四指纹信息构成步骤102中的第二指纹信息。

[0046] 其中，所述预设条件可以包括以下至少之一：选择预设时间段内出现频率最高的指纹信息；选择出现时间最长的指纹信息；选择成功登陆其他应用程序的程序账号的用户指纹。

[0047] 当对各个第四指纹信息进行筛选时，当所述预设条件包括选择预设时间段内出现频率最高的指纹信息时，则可以选择预设时间段内出现频率最高的指纹信息作为与程序账号绑定存储的第四指纹信息；当所述预设条件包括选择出现时间最长的指纹信息时，则可以选择出现时间最长(所谓出现时间最长，即触摸全指纹屏的总时长最长)的指纹信息作为与程序账号绑定存储的第四指纹信息；当所述预设条件包括选择成功登陆其他应用程序的

程序账号的用户指纹时，则可以将成功登陆其他应用程序的程序账号的用户指纹作为与该程序账号绑定存储的第四指纹信息。(举例来说，当登陆的是程序1，对程序1未采集到第三指纹信息，也没有查找到解锁指纹信息，那么当用户使用指纹信息对程序2的账号登录成功时，则可以将该指纹信息作为与程序1账号绑定存储的第四指纹信息)。

[0048] 这样，本发明实施例当面临对用户首次登录应用账号时输入密码的第三指纹信息采集失败的情况时，可以将移动终端的解锁指纹信息、或经过筛选的使用移动终端的第四指纹信息来与该应用账号绑定存储，使得预先存储的第二指纹信息可以采用多种方式来获取，提升了第二指纹信息的获取灵活性。

[0049] 可选地，在一个实施例中，在将第三指纹信息或解锁指纹信息或筛选得到的第四指纹信息所述应用程序账号绑定存储之后，根据本发明实施例的方法还可以包括：

[0050] 将与所述应用程序账号绑定存储的指纹信息(即第三指纹信息或解锁指纹信息或筛选得到的第四指纹信息)，标记为所述应用程序账号的主用户指纹。

[0051] 这样，本发明实施例通过将预先保存的与应用程序账号绑定存储的指纹信息标记为该应用程序账号的主用户指纹，能够利用该主用户指纹对该应用程序账号的指纹信息进行有效管理。

[0052] 可选地，在一个实施例中，所述将与所述应用程序账号绑定存储的指纹信息，标记为所述应用程序账号的主用户指纹的步骤之后，根据本发明实施例的方法还包括：

[0053] 根据所述用户的预设指纹管理操作，展示所述移动终端中处于已登录状态的所有应用程序账号；

[0054] 其中，当检测到用户的预设指纹管理操作(其中，该预设指纹管理操作包括但不限于对预设按钮进行单击、双击，预设手势滑动等等操作)时，本发明实施例的方法可以提供一个指纹管理界面，在该指纹管理界面展示该移动终端中所有处于已登录状态的应用程序账号，例如程序1账号a、程序2账号b、程序3账号c。

[0055] 根据所述用户对所述所有应用程序账号中目标应用程序账号的选择操作，从目标应用程序服务器或者移动终端侧获取所述目标应用程序账号的主用户指纹；

[0056] 其中，用户可以在展示的所有应用程序账号中选择需要进行成员指纹管理的目标应用程序账号(例如程序1账号a)，这样，本发明实施例就可以从应用程序服务器1处或者移动终端侧获取程序1的账号a的主用户指纹。

[0057] 然后，用户就可以对该程序1账号a添加或删除成员指纹，即用户可以为每个程序账号添加或删除亲近的人的指纹信息至相应的应用程序服务器或者移动终端，其中，亲近的人的指纹作为成员指纹，该成员指纹同样作为可信任的用户指纹来对程序账号进行安全登录，在登录过程中同样不会提醒非法登录的信息。

[0058] 如下步骤介绍了本发明实施例的方法如何进行成员指纹的添加和删除操作：

[0059] 一方面，本发明实施例的方法可以进行成员指纹的添加操作，具体而言包括：

[0060] 根据所述用户对所述目标应用程序账号的成员指纹添加操作，采集成员指纹以及所述用户的指纹信息；

[0061] 其中，该成员指纹添加操作的触发方式不限，可以采用现有技术中的任意一种触发方式。例如用户1想要将其妈妈的指纹作为认证指纹进行添加，这里可以使其母亲录入指纹信息，并且用户1自己也要录入自己的认证指纹(即预先录入的第二指纹信息)；

[0062] 将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

[0063] 其中，主用户添加成员用户的指纹时，仍然需要对主用户的指纹进行认证，因此，这里将采集到的用户1的指纹信息与程序1账号1的主用户指纹进行匹配。

[0064] 若匹配成功，则将采集到的所述成员指纹与所述目标应用程序账号绑定存储至所述目标应用程序服务器或者所述移动终端；

[0065] 这样，每个程序账号的主用户都可以在自己的主用户指纹经过认证后，将其亲近的人的指纹与相应程序账号绑定存储，这样，任意一个应用程序账号都可以与主用户指纹以及成员指纹绑定存储，使得当成员指纹对应的成员用户在异地或者更换设备登录该应用程序账号时，本发明实施例的方法也不会进行账号异常登录提醒，避免对主用户和成员用户的信息干扰。

[0066] 另一方面，本发明实施例的方法还可以进行成员指纹的删除操作，具体而言包括：

[0067] 根据所述用户对所述目标应用程序账号的目标成员指纹的删除操作，采集所述用户的指纹信息；

[0068] 其中，该成员指纹删除操作的触发方式不限，可以采用现有技术中的任意一种触发方式。例如用户1想要将其已经添加至程序1账号a的妈妈的指纹进行删除，用户1自己需要录入自己的认证指纹(即预先录入的第二指纹信息)；

[0069] 将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

[0070] 其中，主用户删除成员用户的指纹时，仍然需要对主用户的指纹进行认证，因此，这里将采集到的用户1的指纹信息与程序1账号1的主用户指纹进行匹配。

[0071] 若匹配成功，则将所述目标应用程序服务器中或者所述移动终端中与所述目标应用程序账号绑定存储的成员指纹中所述目标成员指纹删除。

[0072] 这样，每个程序账号的主用户都可以在自己的主用户指纹经过认证后，将与相应程序账号绑定存储的亲近的人的指纹进行删除，使得主用户可以对与程序账号绑定的成员指纹进行有效管理，避免成员指纹冗余。

[0073] 参照图2，示出了本发明一个实施例的移动终端的框图。本发明实施例的移动终端能实现上述实施例中的应用程序账号的登录方法的细节，并达到相同的效果。图2所示的移动终端具有屏幕指纹识别功能，图2所示移动终端包括：

[0074] 第一采集模块21，用于采集用户登录应用程序账号时输入密码的第一指纹信息；

[0075] 第一匹配模块22，用于将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指纹信息进行匹配；

[0076] 拒绝提醒模块23，用于当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。

[0077] 可选地，所述移动终端还包括：

[0078] 第二采集模块，用于采集所述用户首次登录所述应用程序账号时输入密码的第三指纹信息；

[0079] 第一存储模块，用于当所述第三指纹信息采集成功、且所述应用程序账号登录成功时，将所述第三指纹信息与所述应用程序账号绑定存储。

[0080] 可选地，所述移动终端还包括：

[0081] 判断模块，用于当所述第三指纹信息采集失败、且所述应用程序账号登录成功时，判断本地是否存储有所述移动终端的解锁指纹信息；

[0082] 第二存储模块，用于若所述本地存储有所述移动终端的解锁指纹信息，则将所述解锁指纹信息与所述应用程序账号绑定存储；

[0083] 筛选模块，用于若所述本地未存储有所述移动终端的解锁指纹信息，则采集使用所述移动终端的第四指纹信息，按照预设条件对所述第四指纹信息进行筛选，将筛选得到的第四指纹信息与所述应用程序账号绑定存储。

[0084] 可选地，所述移动终端还包括：

[0085] 标记模块，用于将与所述应用程序账号绑定存储的指纹信息，标记为所述应用程序账号的主用户指纹。

[0086] 可选地，所述移动终端还包括：

[0087] 展示模块，用于根据所述用户的预设指纹管理操作，展示所述移动终端中处于已登录状态的所有应用程序账号；

[0088] 获取模块，用于根据所述用户对所述所有应用程序账号中目标应用程序账号的选择操作，获取所述目标应用程序账号的主用户指纹；

[0089] 第三采集模块，用于根据所述用户对所述目标应用程序账号的成员指纹添加操作，采集成员指纹以及所述用户的指纹信息；

[0090] 第二匹配模块，用于将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

[0091] 第三存储模块，用于若匹配成功，则将采集到的所述成员指纹与所述目标应用程序账号绑定存储。

[0092] 可选地，所述移动终端还包括：

[0093] 第四采集模块，用于根据所述用户对所述目标应用程序账号的目标成员指纹的删除操作，采集所述用户的指纹信息；

[0094] 第三匹配模块，用于将采集到的所述用户的指纹信息与所述目标应用程序账号的主用户指纹进行匹配；

[0095] 删除模块，用于若匹配成功，则将与所述目标应用程序账号绑定存储的成员指纹中的所述目标成员指纹删除。

[0096] 本发明实施例提供的移动终端能够实现上述方法实施例中移动终端实现的各个过程，为避免重复，这里不再赘述。

[0097] 图3为实现本发明各个实施例的一种移动终端的硬件结构示意图，

[0098] 该移动终端300具有屏幕指纹识别功能，该移动终端300包括但不限于：射频单元301、网络模块302、音频输出单元303、输入单元304、传感器305、显示单元306、用户输入单元307、接口单元308、存储器309、处理器310、以及电源311等部件。本领域技术人员可以理解，图3中示出的移动终端结构并不构成对移动终端的限定，移动终端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。在本发明实施例中，移动终端包括但不限于手机、平板电脑、笔记本电脑、掌上电脑、车载终端、可穿戴设备、以及计步器等。

[0099] 其中，射频单元301，用于采集用户登录应用程序账号时输入密码的第一指纹信

息；

[0100] 处理器310，用于将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指纹信息进行匹配；当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录。

[0101] 在本发明实施例中，通过预先保存与应用程序账号绑定的第二指纹信息，并将采集到的登录该应用程序账号时输入密码的第一指纹信息与该第二指纹信息相匹配，在匹配一致的情况下，则说明是用户自己在更换设备或者更换位置进行账号登录，此时则拒绝提醒用户该应用程序账号被非法登录，避免了对用户造成干扰的问题。

[0102] 应理解的是，本发明实施例中，射频单元301可用于收发信息或通话过程中，信号的接收和发送，具体的，将来自基站的下行数据接收后，给处理器310处理；另外，将上行的数据发送给基站。通常，射频单元301包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器、双工器等。此外，射频单元301还可以通过无线通信系统与网络和其他设备通信。

[0103] 移动终端通过网络模块302为用户提供了无线的宽带互联网访问，如帮助用户收发电子邮件、浏览网页和访问流式媒体等。

[0104] 音频输出单元303可以将射频单元301或网络模块302接收的或者在存储器309中存储的音频数据转换成音频信号并且输出为声音。而且，音频输出单元303还可以提供与移动终端300执行的特定功能相关的音频输出(例如，呼叫信号接收声音、消息接收声音等等)。音频输出单元303包括扬声器、蜂鸣器以及受话器等。

[0105] 输入单元304用于接收音频或视频信号。输入单元304可以包括图形处理器(Graphics Processing Unit,GPU)3041和麦克风3042，图形处理器3041对在视频捕获模式或图像捕获模式中由图像捕获装置(如摄像头)获得的静态图片或视频的图像数据进行处理。处理后的图像帧可以显示在显示单元306上。经图形处理器3041处理后的图像帧可以存储在存储器309(或其它存储介质)中或者经由射频单元301或网络模块302进行发送。麦克风3042可以接收声音，并且能够将这样的声音处理为音频数据。处理后的音频数据可以在电话通话模式的情况下转换为可经由射频单元301发送到移动通信基站的格式输出。

[0106] 移动终端300还包括至少一种传感器305，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3061的亮度，接近传感器可在移动终端300移动到耳边时，关闭显示面板3061和/或背光。作为运动传感器的一种，加速计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，可用于识别移动终端姿态(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；传感器105还可以包括指纹传感器、压力传感器、虹膜传感器、分子传感器、陀螺仪、气压计、湿度计、温度计、红外线传感器等，在此不再赘述。

[0107] 显示单元306用于显示由用户输入的信息或提供给用户的信息。显示单元306可包括显示面板3061，可以采用液晶显示器(Liquid Crystal Display,LCD)、有机发光二极管(Organic Light-Emitting Diode,OLED)等形式来配置显示面板3061。

[0108] 用户输入单元307可用于接收输入的数字或字符信息，以及产生与移动终端的用户设置以及功能控制有关的键信号输入。具体地，用户输入单元307包括触控面板3071以及

其他输入设备3072。触控面板3071，也称为触摸屏，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控面板3071上或在触控面板3071附近的操作)。触控面板3071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310，接收处理器310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控面板3071。除了触控面板3071，用户输入单元307还可以包括其他输入设备3072。具体地，其他输入设备3072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，在此不再赘述。

[0109] 进一步的，触控面板3071可覆盖在显示面板3061上，当触控面板3071检测到在其上或附近的触摸操作后，传送给处理器310以确定触摸事件的类型，随后处理器310根据触摸事件的类型在显示面板3061上提供相应的视觉输出。虽然在图3中，触控面板3071与显示面板3061是作为两个独立的部件来实现移动终端的输入和输出功能，但是在某些实施例中，可以将触控面板3071与显示面板3061集成而实现移动终端的输入和输出功能，具体此处不做限定。

[0110] 接口单元308为外部装置与移动终端300连接的接口。例如，外部装置可以包括有线或无线头戴式耳机端口、外部电源(或电池充电器)端口、有线或无线数据端口、存储卡端口、用于连接具有识别模块的装置的端口、音频输入/输出(I/O)端口、视频I/O端口、耳机端口等等。接口单元308可以用于接收来自外部装置的输入(例如，数据信息、电力等等)并且将接收到的输入传输到移动终端300内的一个或多个元件或者可以用于在移动终端300和外部装置之间传输数据。

[0111] 存储器309可用于存储软件程序以及各种数据。存储器309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手机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309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。

[0112] 处理器310是移动终端的控制中心，利用各种接口和线路连接整个移动终端的各个部分，通过运行或执行存储在存储器309内的软件程序和/或模块，以及调用存储在存储器309内的数据，执行移动终端的各种功能和处理数据，从而对移动终端进行整体监控。处理器310可包括一个或多个处理单元；优选的，处理器310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310中。

[0113] 移动终端300还可以包括给各个部件供电的电源311(比如电池)，优选的，电源311可以通过电源管理系统与处理器310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。

[0114] 另外，移动终端300包括一些未示出的功能模块，在此不再赘述。

[0115] 优选的，本发明实施例还提供一种移动终端，包括处理器310，存储器309，存储在存储器309上并可在所述处理器310上运行的计算机程序，该计算机程序被处理器310执行时实现上述应用程序账号的登录方法实施例的各个过程，且能达到相同的技术效果，为避

免重复，这里不再赘述。

[0116] 本发明实施例还提供一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序，该计算机程序被处理器执行时实现上述应用程序账号的登录方法实施例的各个过程，且能达到相同的技术效果，为避免重复，这里不再赘述。其中，所述的计算机可读存储介质，如只读存储器(Read-Only Memory，简称ROM)、随机存取存储器(Random Access Memory，简称RAM)、磁碟或者光盘等。

[0117] 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、物品或者装置不仅包括那些要素，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、物品或者装置所固有的要素。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、物品或者装置中还存在另外的相同要素。

[0118] 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(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。

[0119] 上面结合附图对本发明的实施例进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨和权利要求所保护的范围情况下，还可做出很多形式，均属于本发明的保护之内。

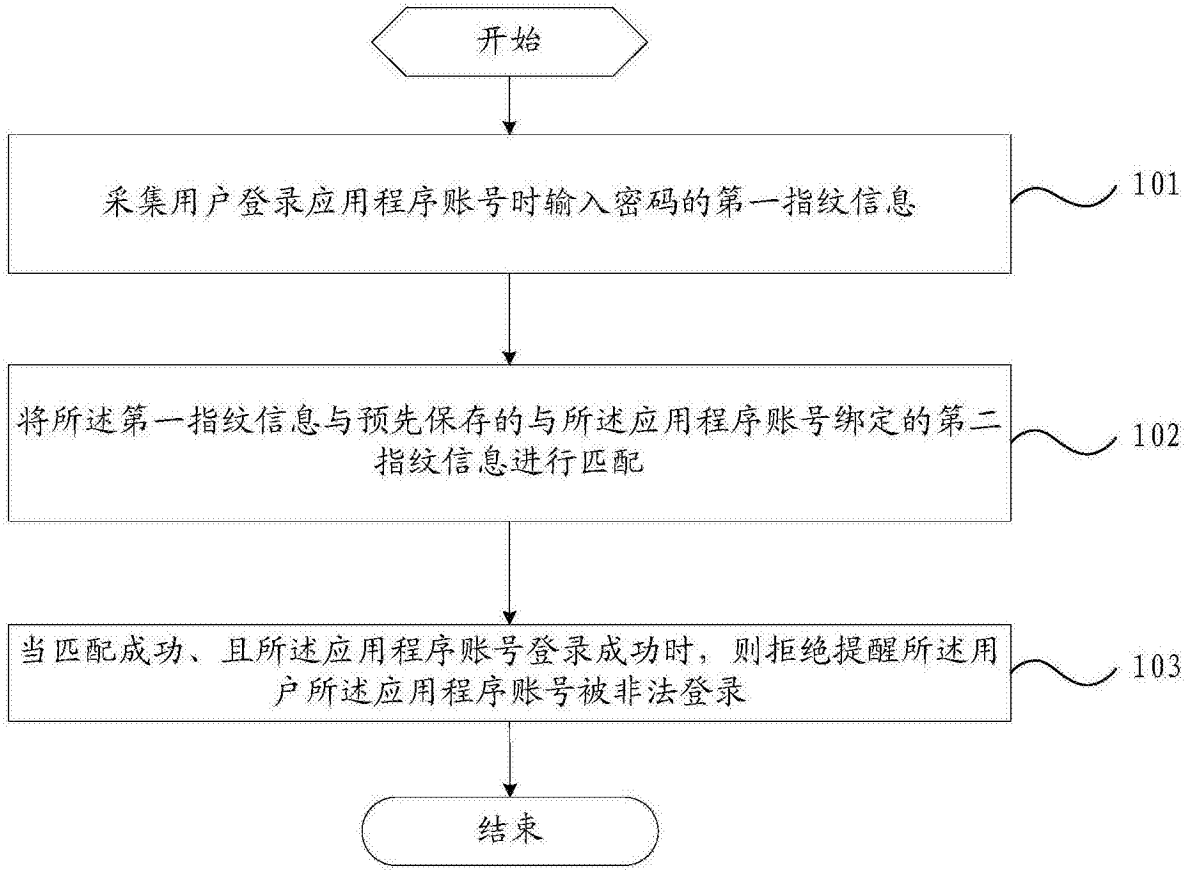

开始
采集用户登录应用程序账号时输入密码的第一指纹信息
101
将所述第一指纹信息与预先保存的与所述应用程序账号绑定的第二指纹信息进行匹配
102
当匹配成功、且所述应用程序账号登录成功时，则拒绝提醒所述用户所述应用程序账号被非法登录
103
结束

图1

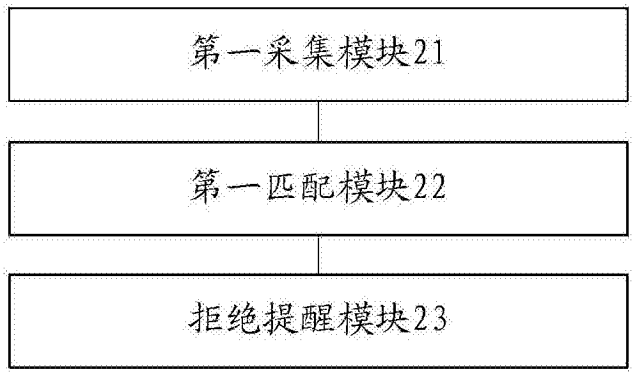

第一采集模块21
第一匹配模块22
拒绝提醒模块23

图2

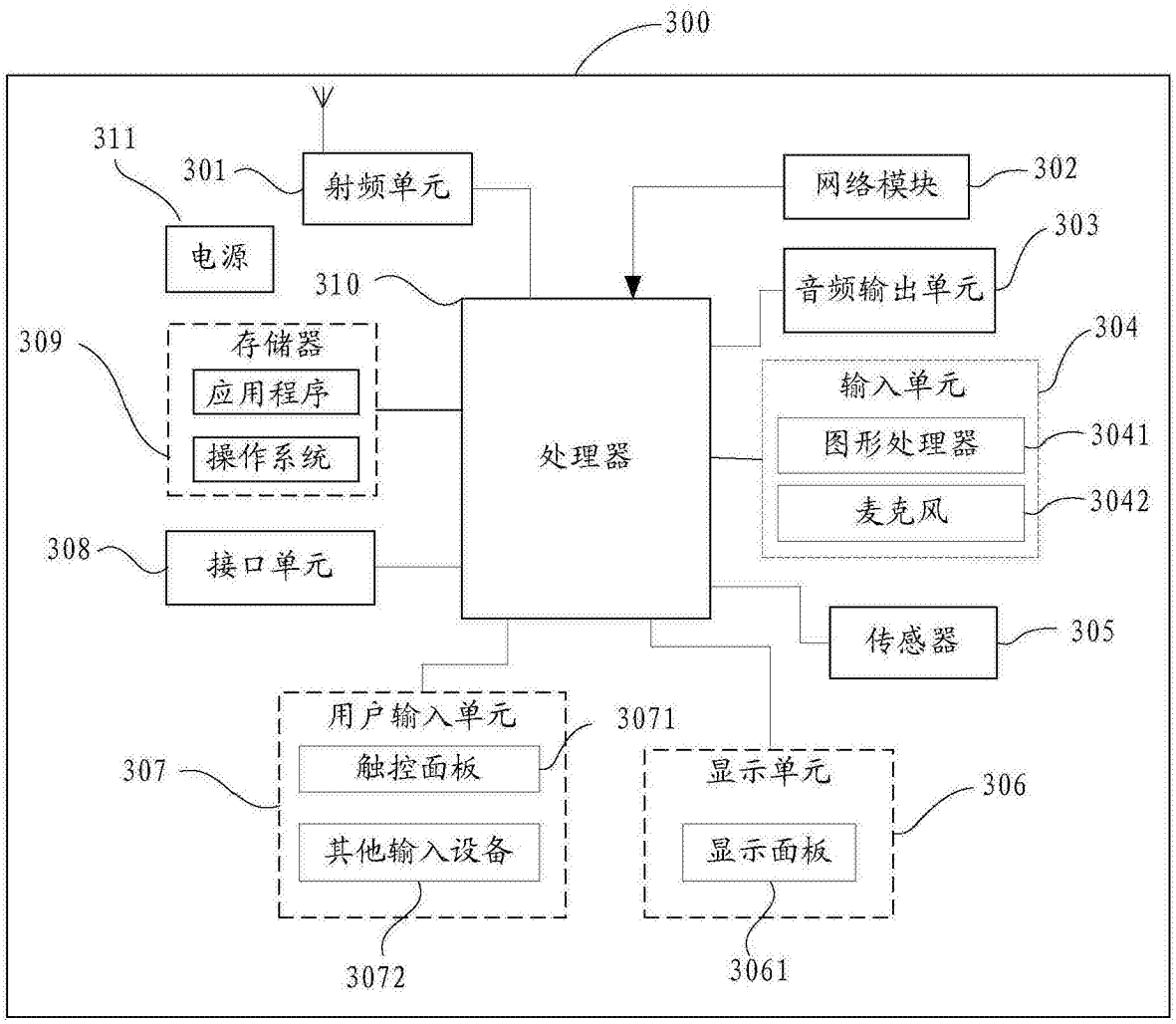

300
311
301
射频单元
网络模块
302
电源
303
音频输出单元
310
309
存储器
应用程序
操作系统
处理器
304
输入单元
图形处理器
3041
麦克风
3042
308
接口单元
传感器
305
用户输入单元
3071
307
触控面板
显示单元
306
其他输入设备
显示面板
3072
3061

图3