(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 103902147 A
(43)申请公布日 2014.07.02

(21)申请号 201210589938.2

(22)申请日 2012.12.31

(71)申请人 腾讯科技(深圳)有限公司
地址 518031 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 温彦杰

(74)专利代理机构 深圳市深佳知识产权代理事务所(普通合伙) 44285
代理人 唐华明

(51)Int.Cl.
G06F 3/0481(2013.01)
G06F 3/0484(2013.01)
G06F 3/01(2006.01)

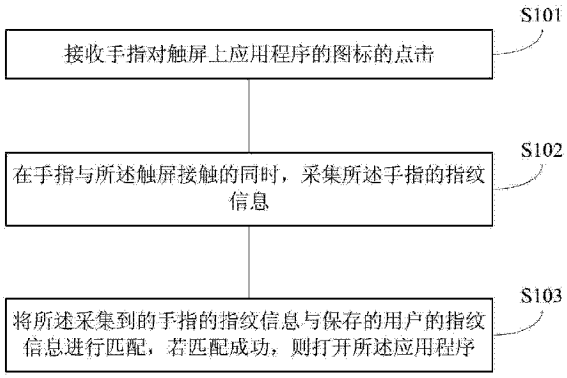
权利要求书2页 说明书6页 附图2页

(54)发明名称

一种开启应用程序的方法和装置

(57)摘要

本发明实施例提供一种开启应用程序的方法和装置，以减少用户与智能终端的交互成本。所述方法包括：接收手指对触屏上应用程序的图标的点击；在手指与所述触屏接触的同时，采集所述手指的指纹信息；将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。与现有技术在智能终端上对用户的身份进行认证时需要用户输入密码相比，本发明实施例提供的方法充分利用了智能终端触屏的“一触即可感知”的功能，在用户开启应用程序而需要对用户身份进行验证时不需要用户输入密码，在用户使用应用程序而将手指接触触屏时即可完成对用户的身份认证从而打开应用程序，减少了用户与机器交互的成本。



CN 103902147 A

1. 一种开启应用程序的方法，其特征在于，所述方法包括：

接收手指对触屏上应用程序的图标的点击；

在手指与所述触屏接触的同时，采集所述手指的指纹信息；

将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。

2. 如权利要求 1 所述的方法，其特征在于，所述将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配包括：

将所述采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配。

3. 如权利要求 2 所述的方法，其特征在于，所述将所述采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配包括：

将所述采集到的手指的指纹信息与所述应用程序的数据库保存的所述用户的指纹信息进行匹配。

4. 如权利要求 2 所述的方法，其特征在于，所述将所述采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配包括：

将所述采集到的手指的指纹信息与本地第三方应用程序保存的所述用户的指纹信息进行匹配。

5. 如权利要求 1 所述的方法，其特征在于，所述将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配包括：

将所述采集到的手指的指纹信息传送至后台服务器，以使所述后台服务器将所述采集到的手指的指纹信息与所述后台服务器保存的所述用户的指纹信息进行匹配；

接收所述后台服务器执行所述匹配后返回的匹配结果。

6. 一种开启应用程序的装置，其特征在于，所述装置包括：

输入接收模块，用于接收手指对触屏上应用程序的图标的点击；

指纹采集模块，用于在手指与所述触屏接触的同时，采集所述手指的指纹信息；

指纹匹配模块，用于将所述指纹采集模块采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。

7. 如权利要求 6 所述的装置，其特征在于，所述指纹匹配模块包括：

本地匹配子模块，用于将所述采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配。

8. 如权利要求 7 所述的装置，其特征在于，所述本地匹配子模块包括：

第一匹配单元，用于将所述采集到的手指的指纹信息与所述应用程序的数据库保存的所述用户的指纹信息进行匹配。

9. 如权利要求 7 所述的装置，其特征在于，所述本地匹配子模块包括：

第二匹配单元，用于将所述采集到的手指的指纹信息与本地第三方应用程序保存的所述用户的指纹信息进行匹配。

10. 如权利要求 6 所述的装置，其特征在于，所述指纹匹配模块包括：

传送单元，用于将所述采集到的手指的指纹信息传送至后台服务器，以使所述后台服务器将所述采集到的手指的指纹信息与所述后台服务器保存的所述用户的指纹信息进行匹配；

接收单元，用于接收所述后台服务器执行所述匹配后返回的匹配结果。

一种开启应用程序的方法和装置

技术领域

[0001] 本发明涉及互联网应用领域，尤其涉及一种开启应用程序的方法和装置。

背景技术

[0002] 随着智能技术的飞速发展，智能终端，例如，智能手机、平板电脑等已经逐渐成为人们常用的电子消费品。智能手机等智能终端相对于传统的手机，一个较大的技术改进在于：屏幕不仅是一种显示设备，重要的是，智能手机的屏幕还是一种输入设备，例如，电容触屏便是智能手机上的常用输入设备。

[0003] 无论是在功能应用方面还是在信息量存储方面，智能手机已经远远超过了传统的手机。由于海量的信息和隐私保护的需要，智能手机在用户使用其中的应用程序时提供了身份认证机制。例如，在使用 QQ、微信等即时通讯应用程序时，用户在输入这些即时通讯的账号后，需要提供密码；只有当应用程序对用户的身份认证通过后，才能打开该应用程序。

[0004] 对于智能终端上的身份认证，现有的技术方案是用户事先设置密码，在需要进行身份认证时，系统会要求用户输入事先设置的密码。在用户输入密码后，系统将其与用户事先设置的密码匹配，若匹配成功，则身份认证通过。

[0005] 上述在智能终端上对用户的身份进行认证与在传统的手机上对用户的身份进行认证没有区别，仍然需要用户输入密码方式，本质上还是有一个人机交互的过程。这种身份认证方式会增加用户的成本，例如，打开一个应用程序前，需要额外的输入密码这一操作；由于智能手机往往是触屏，这种通过输入密码的身份认证方式还容易出错，需要重新输入，这些都为用户打开应用程序带来了不便。

发明内容

[0006] 本发明实施例提供一种开启应用程序的方法和装置，以减少用户在打开应用程序时与智能终端的交互成本。

[0007] 本发明实施例提供一种开启应用程序的方法，所述方法包括：

[0008] 接收手指对触屏上应用程序的图标的点击；

[0009] 在手指与所述触屏接触的同时，采集所述手指的指纹信息；

[0010] 将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。

[0011] 本发明实施例提供一种开启应用程序的装置，所述装置包括：

[0012] 输入接收模块，用于接收手指对触屏上应用程序的图标的点击；

[0013] 指纹采集模块，用于在手指与所述触屏接触的同时，采集所述手指的指纹信息；

[0014] 指纹匹配模块，用于将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。

[0015] 从上述本发明实施例可知，由于在接收手指对触屏上应用程序的图标的点击、从而手指与触屏接触的同时，就完成对所述手指的指纹信息的采集，而将所述采集到的手指

的指纹信息与保存的用户的指纹信息进行匹配这一动作，用户不会感知到。因此，与现有技术在智能终端上对用户的身份进行认证时需要用户输入密码相比，本发明实施例提供的方法充分利用了智能终端触屏的“一触即可感知”的功能，在用户开启应用程序而需要对用户身份进行验证时不需要用户输入密码，在用户使用应用程序而将手指接触触屏时即可完成对用户的身份认证从而打开应用程序，减少了用户与机器交互的成本。

附图说明

[0016] 为了更清楚地说明本发明实施例的技术方案，下面将对现有技术或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，对于本领域技术人员来讲，还可以如这些附图获得其他的附图。

[0017] 图 1 是本发明实施例提供的开启应用程序的方法流程示意图；

[0018] 图 2 是本发明实施例提供的开启应用程序的装置结构示意图；

[0019] 图 3 是本发明另一实施例提供的开启应用程序的装置结构示意图；

[0020] 图 4 是本发明另一实施例提供的开启应用程序的装置结构示意图；

[0021] 图 5 是本发明另一实施例提供的开启应用程序的装置结构示意图；

[0022] 图 6 是本发明另一实施例提供的开启应用程序的装置结构示意图。

具体实施方式

[0023] 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，所描述的实施例仅仅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，本领域技术人员所获得的所有其他实施例，都属于本发明保护的范围。

[0024] 请参阅附图 1，是本发明实施例提供的开启应用程序的方法流程示意图，主要用于智能终端。附图 1 示例的开启应用程序的方法主要包括步骤 S101 和步骤 S102，详细说明如下：

[0025] S101，接收手指对触屏上应用程序的图标的点击。

[0026] 如前所述，现有的智能终端（例如，智能手机等）普遍采用触屏，例如电容触屏或电阻触屏。与传统手机的显示屏不同的是，智能终端的触屏不仅是一种显示装置，还是一种输入设备。因此，在本发明实施例中，当智能终端的使用者使用手指对触屏上应用程序的图标的点击，系统即接收手指对触屏上应用程序的图标的点击。

[0027] S102，在手指与触屏接触的同时，采集所述手指的指纹信息。

[0028] 用户在打开智能终端的应用程序时，必然会点击智能终端触屏上显示的应用程序图标即与智能终端触屏接触。换言之，用户在使用应用程序时不可避免地会接触智能终端的触屏。

[0029] 在本发明实施例中，在手指与触屏接触的同时，即采集所述手指的指纹信息。例如，使用即时通信应用程序 QQ 时，除了登录账号外，一般还需要密码。在本发明实施例中，在用户使用手指点击触屏上应用程序 QQ 的图标时，或者在输入了登录账号后，在触屏上显示的密码输入框处使用手指触摸一下，即可完成对手指的指纹信息的采集。

[0030] S103，将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。

[0031] 在本发明实施例中，在打开应用程序前对用户的身份认证可以是本地认证或后台服务器认证。由于在开机之前，智能终端上不能与后台服务器建立通信，因此，在开机时对用户的身份认证(即只有是该智能终端的合法用户才能予以开机)是通过本地认证进行，而在用户打开应用程序前，由于已经开机，因此，这种场景下对用户的身份认证可以是本地认证或后台服务器认证。

[0032] 作为本发明一个实施例，将采集到的手指的指纹信息与保存的用户的指纹信息进行匹配可以是：将所述采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配。显然，这种实施方式的前提或前期工作是，需要先将智能终端用户的指纹信息保存至智能终端本地。

[0033] 手指与触屏接触可以是通过手指触摸智能终端触屏上应用程序的图标实现，在这种场景下，作为将采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配的一个实施例，可以是将所述采集到的手指的指纹信息与所述应用程序的数据库保存的所述用户的指纹信息进行匹配。换言之，用户所使用的应用程序集成了数据库，该数据库保存有用户的指纹信息，因此，当手指触摸应用程序的图标时，即可将所述采集到的手指的指纹信息与所述应用程序的数据库保存的用户的指纹信息进行匹配。若所述采集到的手指的指纹信息与所述应用程序的数据库保存的用户的指纹信息匹配成功，则打开所述应用程序。

[0034] 作为将采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配的另一实施例，可以是将所述采集到的手指的指纹信息与本地第三方应用程序保存的所述用户的指纹信息进行匹配。在本实施例中，本地第三方应用程序与智能终端的指纹信息采集模块关联。当手指与触屏接触时，采集到的所述手指的指纹信息传送至第三方应用程序。由于第三方应用程序与智能终端的指纹信息采集模块关联时，已经收录了用户的指纹信息，因此，当手指与触屏接触时，即可将所述采集到的手指的指纹信息与本地第三方应用程序保存的所述用户的指纹信息进行匹配。若所述采集到的手指的指纹信息与所述本地第三方应用程序保存的所述用户的指纹信息匹配成功，则打开所述应用程序。

[0035] 如前所述，对用户的身份认证可以是后台服务器认证。作为本发明将采集到的手指的指纹信息与保存的用户的指纹信息进行匹配的另一实施例，可以是客户端将所述采集到的手指的指纹信息传送至后台服务器，以使所述后台服务器将所述采集到的手指的指纹信息与所述后台服务器保存的所述用户的指纹信息进行匹配，然后，所述客户端接收所述后台服务器执行所述匹配后返回的匹配结果。在这一实施方式中，智能终端用户可以事先通过智能终端向后台服务器注册，将自己的指纹信息注册到后台服务器进行保存。当智能终端感知到有手指与触屏接触时即采集该手指的指纹信息，然后，将所述采集到的手指的指纹信息传送至后台服务器，由后台服务器将所述采集到的手指的指纹信息与其保存的用户的指纹信息进行匹配，然后将匹配的匹配结果返回给客户端，所述客户端接收所述后台服务器执行所述匹配的匹配结果。若返回的匹配结果是后台服务器将所述采集到的手指的指纹信息与其保存的用户的指纹信息匹配成功，则对用户的身份认证通过，客户端系统打开应用程序。在本发明实施例中，后台服务器可以是传统的后台服务器，也可以是云技术使用的云服务器，本发明对此不做限定。

[0036] 从上述本发明实施例提供的开启应用程序的方法可知，由于在接收手指对触屏上应用程序的图标的点击、从而手指与触屏接触的同时，就完成对所述手指的指纹信息的采

集，而将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配这一动作，用户不会感知到。因此，与现有技术在智能终端上对用户的身份进行认证时需要用户输入密码相比，本发明实施例提供的方法充分利用了智能终端触屏的“一触即可感知”的功能，在用户开启应用程序而需要对用户身份进行验证时不需要用户输入密码，在用户使用应用程序而将手指接触触屏时即可完成对用户的身份认证，减少了用户与机器交互的成本。

[0037] 请参阅附图2，是本发明实施例提供的开启应用程序的装置结构示意图。为了便于说明，仅仅示出了与本发明实施例相关的部分。附图 2 示例的开启应用程序的装置可以是智能终端浏览器，或者是智能终端浏览器中的某个功能模块 / 单元，其包括指纹采集模块 201、指纹匹配模块 202 和输入接收模块 203，其中 ：

[0038] 输入接收模块 203，用于接收手指对触屏上应用程序的图标的点击。

[0039] 如前所述，现有的智能终端（例如，智能手机等）普遍采用触屏，例如电容触屏或电阻触屏。与传统手机的显示屏不同的是，智能终端的触屏不仅是一种显示装置，还是一种输入设备。因此，在本发明实施例中，当智能终端的使用者使用手指对触屏上应用程序的图标的点击，输入接收模块 203 即接收手指对触屏上应用程序的图标的点击。

[0040] 指纹采集模块 201，用于在手指与所述触屏接触的同时，采集所述手指的指纹信息。

[0041] 用户在打开智能终端的应用程序时，必然会点击智能终端触屏上显示的应用程序图标即与智能终端触屏接触。换言之，用户在使用应用程序时不可避免地会接触智能终端的触屏。

[0042] 在本实施例中，在手指与触屏接触的同时，指纹采集模块 201 即采集所述手指的指纹信息。例如，使用即时通信应用程序 QQ 时，除了登录账号外，一般还需要密码。在本实施例中，在用户使用手指点击触屏上应用程序 QQ 的图标时，或者在输入了登录账号后，在触屏上显示的密码输入框处使用手指触摸一下，指纹采集模块 201 即可完成对手指的指纹信息的采集。

[0043] 指纹匹配模块 202，用于将所述指纹采集模块 201 采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。

[0044] 在本实施例中，在打开应用程序前指纹匹配模块 202 对用户的身份认证可以是本地认证或后台服务器认证。由于在开机之前，智能终端上不能与后台服务器建立通信，因此，在开机时指纹匹配模块 202 对用户的身份认证（即只有是该智能终端的合法用户才能予以开机）是通过本地认证进行，而在用户打开应用程序前，由于已经开机，因此，这种场景下指纹匹配模块 202 对用户的身份认证可以是本地认证或后台服务器认证。

[0045] 需要说明的是，以上开启应用程序的装置的实施方式中，各功能模块的划分仅是举例说明，实际应用中可以根据需要，例如相应硬件的配置要求或者软件的实现的便利考虑，而将上述功能分配由不同的功能模块完成，即将所述开启应用程序的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。而且，实际应用中，本实施例中的相应的功能模块可以是由相应的硬件实现，也可以由相应的硬件执行相应的软件完成，例如，前述的指纹采集模块，可以是具有执行前述在手指与触屏接触的同时，采集所述手指的指纹信息的硬件，例如指纹采集器，也可以是能够执行相应计算机程序从而完成前述功能的一般处理器或者其他硬件设备 ；再如前述的指纹匹配模块，可以是具有执行前述

将所述指纹采集模块(或指纹采集器)采集到的手指的指纹信息与保存的用户的指纹信息进行匹配,若匹配成功,则打开所述应用程序,例如指纹匹配器,也可以是能够执行相应计算机程序从而完成前述功能的一般处理器或者其他硬件设备(本说明书提供的各个实施例都可应用上述描述原则)。

[0046] 附图2示例的指纹匹配模块202可以包括本地匹配子模块301,如附图3所示本发明另一实施例提供的开启应用程序的装置。本地匹配子模块301用于将指纹采集模块201采集到的手指的指纹信息与保存于本地的用户的指纹信息进行匹配。显然,本地匹配子模块301这种对用户身份进行认证的方式的前提或前期工作是,需要先将智能终端用户的指纹信息保存至智能终端本地。

[0047] 手指与触屏接触可以是通过手指触摸智能终端触屏上应用程序的图标实现,在这种场景下,附图3示例的本地匹配子模块301可以包括第一匹配单元401,如附图4所示本发明另一实施例提供的开启应用程序的装置。第一匹配单元401用于将指纹采集模块201采集到的手指的指纹信息与应用程序的数据库保存的所述用户的指纹信息进行匹配。换言之,用户所使用的应用程序集成了数据库,该数据库保存有用户的指纹信息,因此,当手指触摸应用程序的图标时,第一匹配单元401即可将指纹采集模块201采集到的手指的指纹信息与所述应用程序的数据库保存的用户的指纹信息进行匹配。若所述第一匹配单元401将所述采集到的手指的指纹信息与所述应用程序的数据库保存的用户的指纹信息匹配成功,则打开所述应用程序。

[0048] 附图3示例的本地匹配子模块301可以包括第二匹配单元501,如附图5所示本发明另一实施例提供的开启应用程序的装置。第二匹配单元501用于将指纹采集模块201采集到的手指的指纹信息与本地第三方应用程序保存的所述用户的指纹信息进行匹配。在本实施例中,本地第三方应用程序与智能终端的指纹采集模块201关联。当手指与触屏接触时,指纹采集模块201采集到的手指的指纹信息传送至第三方应用程序。由于第三方应用程序与智能终端的指纹采集模块201关联时,已经收录了用户的指纹信息,因此,当手指与触屏接触时,第二匹配单元501即可将指纹采集模块201采集到的手指的指纹信息与本地第三方应用程序保存的用户的指纹信息进行匹配。若所述第二匹配单元501将采集到的手指的指纹信息与所述本地第三方应用程序保存的所述用户的指纹信息匹配成功,则打开所述应用程序。

[0049] 附图2示例的指纹匹配模块202可以包括传送单元601和接收单元602,如附图6所示本发明另一实施例提供的开启应用程序的装置,其中:

[0050] 传送单元601,用于将指纹采集模块201采集到的手指的指纹信息传送至后台服务器,以使所述后台服务器将所述采集到的手指的指纹信息与所述后台服务器保存的所述用户的指纹信息进行匹配;

[0051] 接收单元602,用于接收所述后台服务器执行所述匹配后返回的匹配结果。

[0052] 在附图6示例的开启应用程序的装置中,智能终端用户可以事先通过智能终端向后台服务器注册,将自己的指纹信息注册到后台服务器进行保存。当智能终端感知到有手指与触屏接触时指纹采集模块201即采集该手指的指纹信息,然后,传送单元601将指纹采集模块201采集到的手指的指纹信息传送至后台服务器,由后台服务器将指纹采集模块201采集到的手指的指纹信息与其保存的用户的指纹信息进行匹配,然后将匹配的匹配结

果返回给客户端。客户端的接收单元 602 接收所述后台服务器执行所述匹配的匹配结果。若返回的匹配结果是后台服务器将所述采集到的手指的指纹信息与其保存的用户的指纹信息匹配成功，则对用户的身份认证通过，客户端系统打开应用程序。在本实施例中，后台服务器可以是传统的后台服务器，也可以是云技术使用的云服务器，本发明对此不做限定。

[0053] 需要说明的是，上述装置各模块 / 单元之间的信息交互、执行过程等内容，由于与本发明方法实施例基于同一构思，其带来的技术效果与本发明方法实施例相同，具体内容可参见本发明方法实施例中的叙述，此处不再赘述。

[0054] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，比如以下各种方法的一种或多种或全部：

[0055] 接收手指对触屏上应用程序的图标的点击；

[0056] 在手指与所述触屏接触的同时，采集所述手指的指纹信息；

[0057] 将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序。

[0058] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成，该程序可以存储于一计算机可读存储介质中，存储介质可以包括：只读存储器（ROM，Read Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁盘或光盘等。

[0059] 以上对本发明实施例提供的一种开启应用程序的方法和装置进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

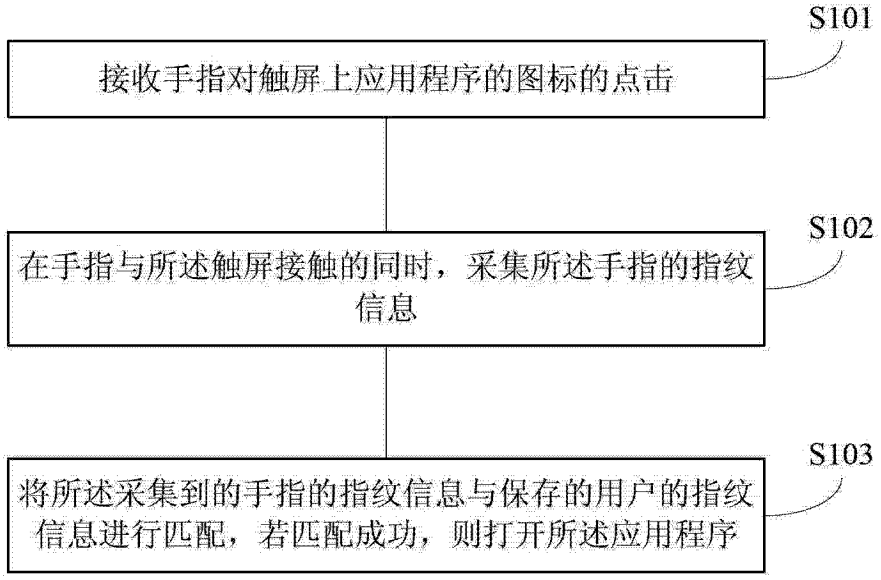

S101
接收手指对触屏上应用程序的图标的点击
S102
在手指与所述触屏接触的同时，采集所述手指的指纹信息
S103
将所述采集到的手指的指纹信息与保存的用户的指纹信息进行匹配，若匹配成功，则打开所述应用程序

图 1

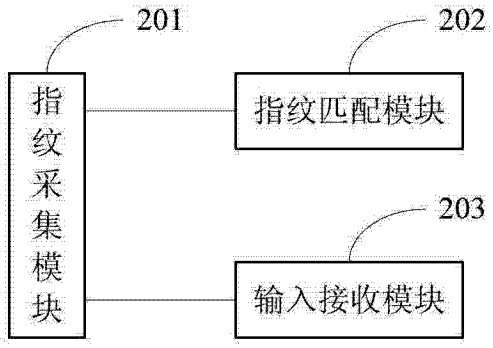

201
202
指纹采集模块
指纹匹配模块
203
输入接收模块

图 2

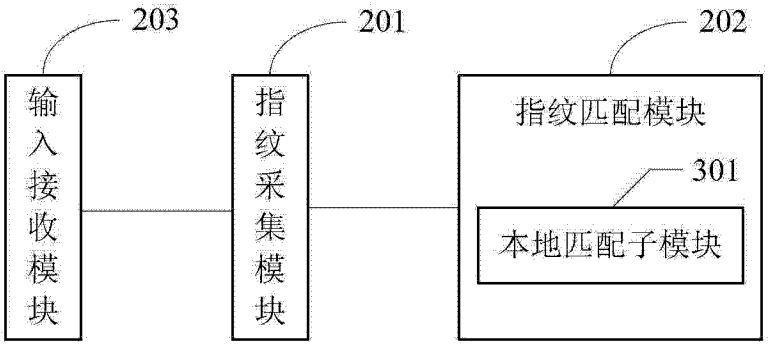

203
201
202
输入接收模块
指纹采集模块
指纹匹配模块
301
本地匹配子模块

图 3

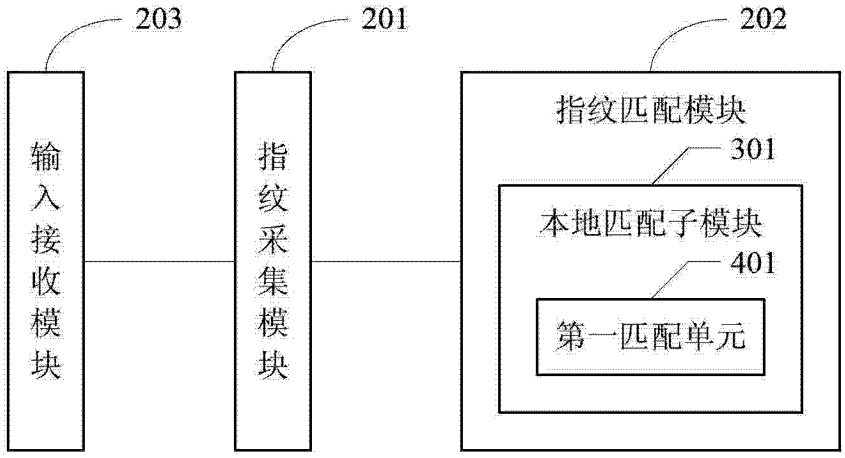

203
201
202
输入接收模块
指纹采集模块
指纹匹配模块
301
本地匹配子模块
401
第一匹配单元

图 4

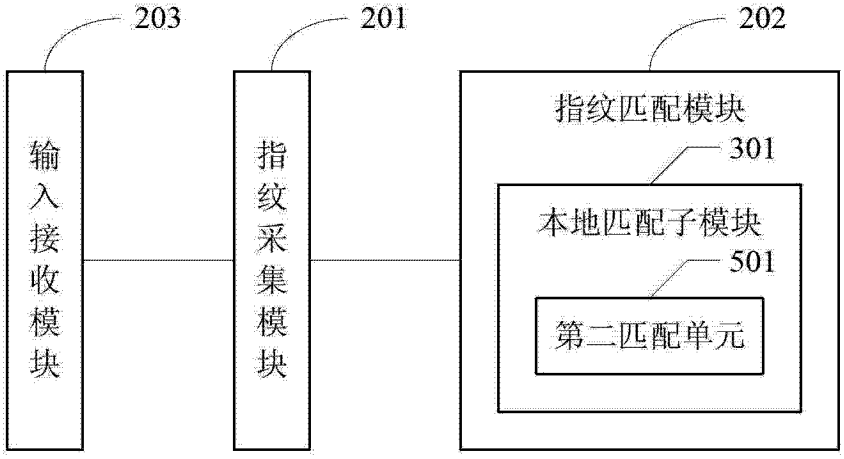

203
201
202
输入接收模块
指纹采集模块
指纹匹配模块
301
本地匹配子模块
501
第二匹配单元

图 5

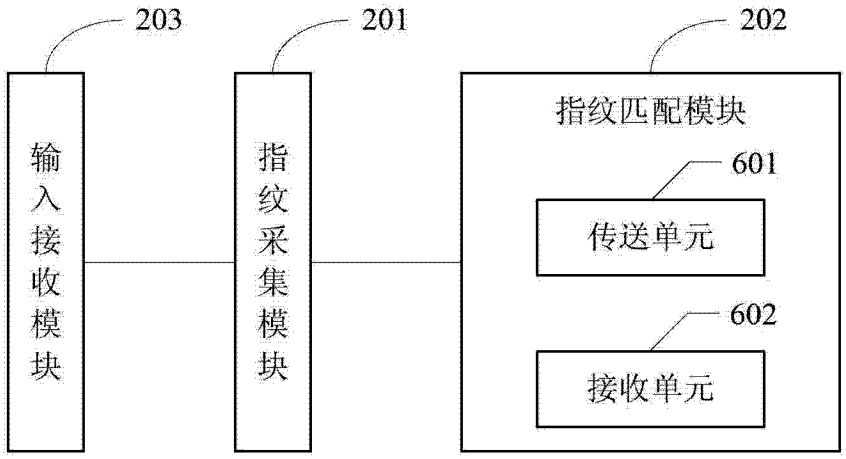

203
201
202
输入接收模块
指纹采集模块
指纹匹配模块
601
传送单元
602
接收单元

图 6