(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 106951757 A
(43)申请公布日 2017.07.14

(21)申请号 201710112398.1

(22)申请日 2017.02.28

(71)申请人 宇龙计算机通信科技(深圳)有限公司
地址 518057 广东省深圳市南山区科技园北区梦溪道2号

(72)发明人 高志峰

(74)专利代理机构 北京三聚阳光知识产权代理有限公司 11250
代理人 马永芬

(51)Int.Cl.
G06F 21/32(2013.01)
H04M 1/725(2006.01)

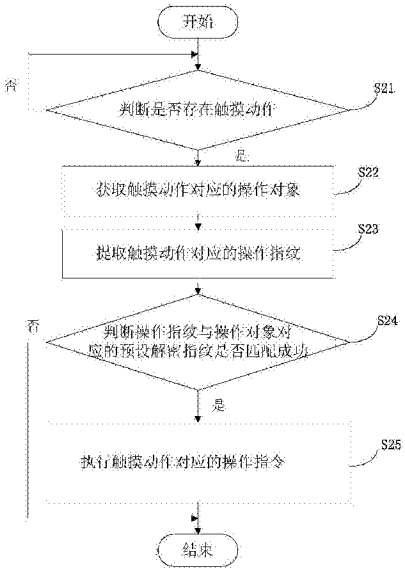
权利要求书2页 说明书9页 附图6页

(54)发明名称

一种操作应用程序的方法和装置

(57)摘要

本发明公开了一种操作应用程序的方法和装置，所述方法包括：判断是否存在触摸动作；若存在触摸动作，则获取所述触摸动作对应的操作对象；提取所述触摸动作对应的操作指纹；判断所述操作指纹与所述操作对象对应的预设解密指纹是否匹配成功；当所述操作指纹与所述预设解密指纹匹配成功时，执行所述触摸动作对应的操作指令。该方案通过将用户对操作对象的操作指纹与该操作对象对应的预设解密指纹进行匹配，如果匹配成功则执行相应的操作指令，否则说明操作指纹不对，则无法执行相关操作，从而保护用户的隐私，避免陌生人恶意操作，并且可以有效避免屏幕解锁瞬间的触摸动作引起误操作，提高了终端中用户信息的安全性和隐私性。



CN 106951757 A

1.一种操作应用程序的方法，用于终端中，所述终端具有能够全屏识别指纹的触摸屏，其特征在于，包括：

判断是否存在触摸动作；

若存在触摸动作，则获取所述触摸动作对应的操作对象；

提取所述触摸动作对应的操作指纹；

判断所述操作指纹与所述操作对象对应的预设解密指纹是否匹配成功；

当所述操作指纹与所述预设解密指纹匹配成功时，执行所述触摸动作对应的操作指令。

2.根据权利要求1所述的操作应用程序的方法，其特征在于，所述提取所述触摸动作对应的操作指纹包括：

判断所述触摸动作对应的操作指令是否为预设操作指令；

当所述操作指令为所述预设操作指令时，提取所述操作指纹。

3.根据权利要求2所述的操作应用程序的方法，其特征在于，所述预设操作指令为打开所述操作对象。

4.根据权利要求1至3中任一项所述的操作应用程序的方法，其特征在于，所述操作对象包括：应用程序、文件夹、私密空间以及聊天记录。

5.根据权利要求1所述的操作应用程序的方法，其特征在于，在所述判断是否存在触摸动作之前还包括：

获取所述终端中的至少一个所述操作对象；

为每个所述操作对象设置对应的所述预设解密指纹。

6.一种操作应用程序的装置，用于终端中，所述终端具有能够全屏识别指纹的触摸屏，其特征在于，包括：

第一判断模块，用于判断是否存在触摸动作；

第一获取模块，用于若存在触摸动作，则获取所述触摸动作对应的操作对象；

提取模块，用于提取所述触摸动作对应的操作指纹；

第二判断模块，用于判断所述操作指纹与所述操作对象对应的预设解密指纹是否匹配成功；

执行模块，用于当所述操作指纹与所述预设解密指纹匹配成功时，执行所述触摸动作对应的操作指令。

7.根据权利要求6所述的操作应用程序的装置，其特征在于，所述提取模块包括：

判断单元，用于判断所述触摸动作对应的操作指令是否为预设操作指令；

提取单元，用于当所述操作指令为所述预设操作指令时，提取所述操作指纹。

8.根据权利要求7所述的操作应用程序的装置，其特征在于，所述预设操作指令为打开所述操作对象。

9.根据权利要求6至8中任一项所述的操作应用程序的装置，其特征在于，所述操作对象包括：应用程序、文件夹、私密空间以及聊天记录。

10.根据权利要求6所述的操作应用程序的装置，其特征在于，还包括：

第二获取模块，用于在所述判断是否存在触摸动作之前，获取所述终端中的至少一个所述操作对象；

设置模块，用于为每个所述操作对象设置对应的所述预设解密指纹。

一种操作应用程序的方法和装置

技术领域

[0001] 本发明涉及控制技术领域，具体涉及一种操作应用程序的方法和装置。

背景技术

[0002] 目前，随着通信技术的飞速发展，手机、平板电脑等移动终端成为了人们生活中不可缺少的一部分。由于移动终端涉及到用户生活的各个方面，因此对于移动终端的隐私安全性越来越受到人们的关注，移动终端的安全认证技术应运而生。

[0003] 现有的移动终端的安全认证方案大都是基于指纹识别，即在移动终端内部增加一个安全系统，通过指纹识别进入，在这个独立的系统空间内部可以放置私密的文件、照片和一些应用程序。指纹识别即是指通过比较不同指纹的细节特征点来进行鉴别。指纹识别技术涉及图像处理、模式识别、计算机视觉、数学形态学、小波分析等众多学科。由于每个人的指纹不同，就是同一人的十指之间，指纹也有明显区别，因此指纹可用于身份安全鉴定。

[0004] 现有的安全认证方案功能比较单一，只能用一个指纹对一个私密空间进行安全防护。而且私密空间和正常空间的切换很不方便。假如想对单个应用程序进行加密，一般必须要同时输入手势密码、数字密码以及指纹信息等，操作比较复杂。而且，一旦某个移动终端或者应用程序通过安全认证解密后，其他用户就可以对该移动终端或者应用程序进行相关查看和操作，这就给用户的隐私信息带来了安全隐患。现有的移动终端已经可以实现全屏指纹识别，并可以将显示屏划分为数个指纹识别区域，但是只能实现在特定指纹识别区域中自定义一些加密操作。

[0005] 因此，如何提高终端中用户的隐私安全，成为一个亟待解决的技术问题。

发明内容

[0006] 有鉴于此，本发明实施例提供了一种操作应用程序的方法和装置，以解决现有技术中移动终端中用户的隐私信息安全性较低的问题。

[0007] 本发明第一方面提供了一种操作应用程序的方法，所述终端具有能够全屏识别指纹的触摸屏，包括：判断是否存在触摸动作；若存在触摸动作，则获取所述触摸动作对应的操作对象；提取所述触摸动作对应的操作指纹；判断所述操作指纹与所述操作对象对应的预设解密指纹是否匹配成功；当所述操作指纹与所述预设解密指纹匹配成功时，执行所述触摸动作对应的操作指令。

[0008] 通过实施第一方面描述的方法，可以实时检测用户在触摸屏上的触摸动作，通过将用户对操作对象的操作指纹与该操作对象对应的预设解密指纹进行匹配，如果匹配成功则执行相应的操作指令，否则说明操作指纹不对，有可能是陌生人的恶意操作，则无法执行相关操作，从而保护用户的隐私，如此，即使已经解锁屏幕的终端，陌生人拿到之后也是无法对相应的操作对象(比如应用程序或者应用程序的某一项功能)进行操作的，并且可以有效避免屏幕解锁瞬间的触摸动作引起误操作，提高了终端中用户信息的安全性和隐私性。

[0009] 结合本发明第一方面，本发明第一方面第一实施方式中，所述提取所述触摸动作

对应的操作指纹包括：判断所述触摸动作对应的操作指令是否为预设操作指令；当所述操作指令为所述预设操作指令时，提取所述操作指纹。

[0010] 通过执行上述步骤，可以为操作对象的某一预设操作指令设置解密指纹，只有用户的触摸动作对应的操作指令为预设操作指令时，才会提取该触摸动作对应的操作指纹，如此，有目的的进行操作指纹的提取，不仅降低了终端的功耗，提高了终端的处理速度，而且避免出现无用的指纹信息对数据处理结果的影响。

[0011] 结合本发明第一方面，本发明第一方面第二实施方式中，所述预设操作指令为打开所述操作对象。

[0012] 通过执行上述步骤，可以保证只有匹配成功的操作指纹才能打开该操作对象，此处预设操作指令包含但不限于打开所述操作对象，也可以是对操作对象的信息更改、数据读写和删除等操作指令，即对于操作对象的一切可执行的操作指令均可以作为预设操作指令的待选目标，用户可以根据实际需要添加或删除相应的预设操作指令，扩大了指纹识别的适用范围，进一步提高了用户信息的安全性。

[0013] 结合本发明第一方面或第一方面第一实施方式或第一方面第二实施方式，本发明第一方面第三实施方式中，所述操作对象包括：应用程序、文件夹、私密空间以及聊天记录。

[0014] 通过执行上述步骤，此处的操作对象包含但不限于：应用程序、文件夹、私密空间以及聊天记录，自然地，操作对象也可以是某一个应用程序的某一项功能，比如地图定位、短信查看等，用户可以根据实际需要来选取操作对象，如此大大丰富了用户信息的加密方式，使用户的隐私更加精细化、个性化，从而提高了用户体验。

[0015] 结合本发明第一方面，本发明第一方面的第四实施方式中，在所述判断是否存在触摸动作之前还包括：获取所述终端中的至少一个所述操作对象；为每个所述操作对象设置对应的所述预设解密指纹。

[0016] 通过执行上述步骤，可以预先为终端中被选中的操作对象设置对应的预设解密指纹，被选中的操作对象可以是多个，每个操作对象对应的预设解密指纹可以相同也可以不同，具体根据用户实际需要进行设置，如此，实现了对用户信息的多重保护，进一步提高了用户信息的安全性。

[0017] 此外，本发明第二方面提供一种操作应用程序的装置，所述操作应用程序的装置包括用于执行上述第一方面或第一方面任意一种操作应用程序的方法的模块或单元。

[0018] 例如，所述操作应用程序的装置包括：第一判断模块，用于判断是否存在触摸动作；第一获取模块，用于若存在触摸动作，则获取所述触摸动作对应的操作对象；提取模块，用于提取所述触摸动作对应的操作指纹；第二判断模块，用于判断所述操作指纹与所述操作对象对应的预设解密指纹是否匹配成功；执行模块，用于当所述操作指纹与所述预设解密指纹匹配成功时，执行所述触摸动作对应的操作指令。

[0019] 通过实施第二方面的操作应用程序的装置，可以实时检测用户在触摸屏上的触摸动作，通过将用户对操作对象的操作指纹与该操作对象对应的预设解密指纹进行匹配，如果匹配成功则执行相应的操作指令，否则说明操作指纹不对，有可能是陌生人的恶意操作，则无法执行相关操作，从而保护用户的隐私，如此，即使已经解锁屏幕的终端，陌生人拿到之后也是无法对相应的操作对象(比如应用程序或者应用程序的某一项功能)进行操作的，并且可以有效避免屏幕解锁瞬间的触摸动作引起误操作，提高了终端中用户信息的安全性

和隐私性。

[0020] 结合本发明第二方面，本发明第二方面第一实施方式中，所述提取模块包括：判断单元，用于判断所述触摸动作对应的操作指令是否为预设操作指令；提取单元，用于当所述操作指令为所述预设操作指令时，提取所述操作指纹。

[0021] 通过实施上述操作应用程序的装置，可以为操作对象的某一预设操作指令设置解密指纹，只有用户的触摸动作对应的操作指令为预设操作指令时，才会提取该触摸动作对应的操作指纹，如此，有目的的进行操作指纹的提取，不仅降低了终端的功耗，提高了终端的处理速度，而且避免出现无用的指纹信息对数据处理结果的影响。

[0022] 结合本发明第二方面，本发明第二方面第二实施方式中，所述预设操作指令为打开所述操作对象。

[0023] 通过实施上述操作应用程序的装置，可以保证只有匹配成功的操作指纹才能打开该操作对象，此处预设操作指令包含但不限于打开所述操作对象，也可以是对操作对象的信息更改、数据读写和删除等操作指令，即对于操作对象的一切可执行的操作指令均可以作为预设操作指令的待选目标，用户可以根据实际需要添加或删除相应的预设操作指令，扩大了指纹识别的适用范围，进一步提高了用户信息的安全性。

[0024] 结合本发明第二方面或第二方面第一实施方式或第二方面第二实施方式，本发明第二方面第三实施方式中，所述操作对象包括：应用程序、文件夹、私密空间以及聊天记录。

[0025] 通过实施上述操作应用程序的装置，此处的操作对象包含但不限于：应用程序、文件夹、私密空间以及聊天记录，自然地，操作对象也可以是某一个应用程序的某一项功能，比如地图定位、短信查看等，用户可以根据实际需要来选取操作对象，如此大大丰富了用户信息的加密方式，使用户的隐私更加精细化、个性化，从而提高了用户体验。

[0026] 结合本发明第二方面，本发明第二方面的第四实施方式中，还包括：第二获取模块，用于在所述判断是否存在触摸动作之前，获取所述终端中的至少一个所述操作对象；设置模块，用于为每个所述操作对象设置对应的所述预设解密指纹。

[0027] 通过实施上述操作应用程序的装置，可以预先为终端中被选中的操作对象设置对应的预设解密指纹，被选中的操作对象可以是多个，每个操作对象对应的预设解密指纹可以相同也可以不同，具体根据用户实际需要进行设置，如此，实现了对用户信息的多重保护，进一步提高了用户信息的安全性。

[0028] 所述操作应用程序的装置所包括的模块或单元不限于上述命名方式。

[0029] 本申请的这些方面在以下实施例的描述中会更加简明易懂。

[0030] 本发明第三方面提供了一种终端，包括能够全屏识别指纹的触摸屏、以及本发明第二方面或第二方面的任一实施方式所述的操作应用程序的装置。

[0031] 本发明第四方面提供了另一种终端，包括：包括：至少一个处理器；以及与所述至少一个处理器通信连接的存储器；其中，所述存储器存储有可被所述至少一个处理器执行的指令，所述指令被所述至少一个处理器执行，以使所述至少一个处理器执行如下方法：判断是否存在触摸动作；若存在触摸动作，则获取所述触摸动作对应的操作对象；提取所述触摸动作对应的操作指纹；判断所述操作指纹与所述操作对象对应的预设解密指纹是否匹配成功；当所述操作指纹与所述预设解密指纹匹配成功时，执行所述触摸动作对应的操作指令。

[0032] 上述终端可以实时检测用户在触摸屏上的触摸动作，通过将用户对操作对象的操作指纹与该操作对象对应的预设解密指纹进行匹配，如果匹配成功则执行相应的操作指令，否则说明操作指纹不对，有可能是陌生人的恶意操作，则无法执行相关操作，从而保护用户的隐私，如此，即使已经解锁屏幕的终端，陌生人拿到之后也是无法对相应的操作对象(比如应用程序或者应用程序的某一项功能)进行操作的，并且可以有效避免屏幕解锁瞬间的触摸动作引起误操作，提高了终端中用户信息的安全性和隐私性。

附图说明

[0033] 通过参考附图会更加清楚的理解本发明的特征和优点，附图是示意性的而不应理解为对本发明进行任何限制，在附图中：

[0034] 图1示出了本发明实施例中手机的结构图；

[0035] 图2示出了根据本发明实施例的操作应用程序的方法的流程图；

[0036] 图3示出了根据本发明实施例的启动操作对象的操作流程示意图；

[0037] 图4示出了根据本发明实施例的改变操作对象在触摸屏上的位置后的操作示意图；

[0038] 图5示出了根据本发明实施例的为操作对象添加指纹加密的操作示意图；

[0039] 图6示出了根据本发明实施例的操作应用程序的装置的结构示意图；

[0040] 图7示出了根据本发明实施例的操作应用程序的装置的另一个结构示意图；

[0041] 图8示出了根据本发明实施例的终端的结构示意图。

具体实施方式

[0042] 为使本发明实施例的目的、技术方案和优点更加清楚，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。

[0043] 如图1所示，是本发明的实施例的应用场景示意图。移动终端为手机或平板电脑等移动设备，移动终端以手机为例，手机的部分结构框图如图1所示，手机包括射频电路210、存储器220、输入单元230、显示单元240、传感器250、音频电路260、无线模块270、处理器280以及电源290等部分。本领域技术人员可以理解，图1中示出的手机结构并不构成对手机的限定，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。

[0044] 其中RF电路210用于收发信息或通话过程中，信号的接收和发送。存储器220用于存储软件程序以及模块，处理器280通过运行存储在存储器220的软件程序以及模块，从而执行手机的各种功能应用以及数据处理。输入单元230用于接收输入的数字或字符信息，以及产生与手机的用户设置以及功能控制有关的键信号输入。输入单元230可包括触控面板231以及其他输入设备232。其他输入设备232可以包括但不限于物理键盘、功能键、鼠标、操作杆中的一种或几种。显示单元240用于显示由用户输入的信息或提供给用户的信息以及手机的各种菜单。显示单元240可以包括显示面板241。触控面板231可覆盖显示面板241，当触控面板231检测到在其上或附近的触摸操作后，传送给处理器280以确定触摸事件的类型，随后处理器280根据触摸事件的类型在显示面板241上提供相应的视觉输出。

[0045] 手机还可包括至少一种传感器250，如光传感器、运动传感器以及其他传感器。光传感器可包括环境光传感器及接近传感器，环境传感器可根据环境光线的明暗来调节显示面板241的亮度，接近传感器可在手机移动到耳边时，关闭显示面板241和/或背光。本实施例中光传感器可以设置在手机的正面和背面的壳体上，用于检测用户持握手机时的遮挡区域。此处还可以包括压力传感器，设置在手机的正面或背面壳体上，用于通过检测压力的方式获得用户持握手机时的遮挡区域。此外，手机还可以配置陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，不再赘述。

[0046] 音频电路260、扬声器261、传声器262可提供用户与手机之间的音频接口。无线模块270可以是WIFI模块，为用户提供无线的互联网访问服务。

[0047] 处理器280是手机的控制中心，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220内的软件程序和/或模块，以及调用存储在存储器220内的数据，执行手机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280可以包括一个或多个处理单元。此外，手机还包括各部件供电的电源290，通过电源管理系统与处理器280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。

[0048] 尽管未示出，手机还可以包括摄像头、蓝牙模块等，在此不再赘述。

[0049] 请参阅图2，本发明实施例提供的一种操作应用程序的方法，应用于具有能够全屏识别指纹的触摸屏的终端中，包括：

[0050] S21：判断是否存在触摸动作。本实施例中的终端的触摸屏具有全屏指纹识别功能，可以实时检测用户在触摸屏上的触摸动作，进而确定是否存在指纹操作，如果判断结果为是进入步骤S22，否则仅需检测是否存在触摸动作。

[0051] S22：若存在触摸动作，则获取触摸动作对应的操作对象。如果触摸动作存在，则可以根据该触摸动作在触摸屏上的触摸位置、以及该触摸位置处的图标来获取该图标对应的操作对象，此处操作对象包含但不限于：应用程序、文件夹、私密空间以及聊天记录。比如用户想要对手机中的音乐应用进行操作时，如图3所示，用户触摸触摸屏上音乐应用的图标(如图3中小方框内所示)，则音乐应用即为本次操作的操作对象，根据用户的触摸位置和音乐应用的图标可以获取到音乐应用及其相关信息。自然地，操作对象也可以是某一个应用程序的某一项功能，比如地图定位、短信查看等，用户可以根据实际需要来选取操作对象，如此大大丰富了用户信息的加密方式，使用户的隐私更加精细化、个性化，从而提高了用户体验。

[0052] S23：提取触摸动作对应的操作指纹。本实施例中的终端具有能够全屏识别指纹的触摸屏，可以在触摸屏的任意位置对触摸动作的操作指纹进行提取，如图3和4所示，如果用户对桌面图标重新排序，比如音乐应用的图标位置发生改变，但是对该应用的指纹识别过程不受影响。

[0053] 作为一种优选方案，步骤S23可以包括：判断触摸动作对应的操作指令是否为预设操作指令，当操作指令为预设操作指令时，提取操作指纹。即可以为操作对象的某一预设操作指令设置解密指纹，只有用户的触摸动作对应的操作指令为预设操作指令时，才会提取该触摸动作对应的操作指纹；在本实施例中，可以是特定区域位置的指纹提取与识别，识别区域的大小是和操作对象图标在屏幕上显示的相对大小相适应的，也即与触摸屏可操作的区域大小是相适应的，如此，有目的的进行操作指纹的提取并识别，不仅降低了终端的功

耗，提高了终端的处理速度，而且避免出现无用的指纹信息对数据处理结果的影响。此处预设操作指令包含但不限于打开操作对象，比如预设操作指令为打开音乐应用，也可以是对操作对象的信息更改、数据读写和删除等操作指令，即对于操作对象的一切可执行的操作指令均可以作为预设操作指令的待选目标，用户可以根据实际需要添加或删除相应的预设操作指令，扩大了指纹识别的适用范围，进一步提高了用户信息的安全性。

[0054] S24：判断操作指纹与操作对象对应的预设解密指纹是否匹配成功；通过将用户对操作对象的操作指纹与该操作对象对应的预设解密指纹进行匹配，如果匹配成功说明是用户的正常操作，则进入步骤S25，否则说明操作指纹不对，有可能是陌生人的恶意操作，如图3所示，可以弹出提示框，提示用户重新确认指纹信息，或者在多次重试之后发出报警，以便用户及时发现异常，从而保护用户的隐私，如此，即使已经解锁屏幕的终端，陌生人拿到之后也是无法对相应的操作对象(比如应用程序或者应用程序的某一项功能)进行操作的，并且可以有效避免屏幕解锁瞬间的触摸动作引起误操作，提高了终端中用户信息的安全性和隐私性。

[0055] S25：当操作指纹与预设解密指纹匹配成功时，执行触摸动作对应的操作指令。匹配成功时，说明是用户的正常操作，则执行本次用户触摸动作对应的操作指令，比如操作指令为打开音乐应用，则在指纹匹配成功后即可打开音乐应用，以便于用户的下一步操作。

[0056] 需要说明的是，在常规的操作过程中，由于指纹识别的速度非常快，在正确匹配的情况下，用户感知不到识别流程，只有在指纹匹配不成功时才给予提示响应，因此提高了用户体验。。

[0057] 作为一种优选方案，在步骤S21之前还可以包括：获取终端中的至少一个操作对象；为每个操作对象设置对应的预设解密指纹。即可以预先为终端中被选中的操作对象设置对应的预设解密指纹，被选中的操作对象可以是多个，每个操作对象对应的预设解密指纹可以相同也可以不同，具体根据用户实际需要进行设置。自然地，此处被选中的操作对象可以是终端中一切可操作的对象，即用户可以在不同的操作层面上添加指纹加密，可以在启动某个私密空间时、也可以在启动某个安全财务应用时、在打开某个文件夹时或者也可以是打开和某人的聊天记录时添加。比如用户可以将手机屏幕解锁设置为一种指纹，打开应用的时候再使用另外一种指纹，特定位置的应用只能通过特定指纹打开，使得手机多了一层防护，增加了手机的安全性。

[0058] 具体地，可以通过在被选中的操作对象的图标处长按屏幕，以调出添加指纹加密选项。此处的长按屏幕可以是对时间的定义也可以是对压力的定义。如图5所示，比如要对手机中的微信的通讯录进行加密，长按通讯录图标即可调出【添加和取消指纹加密选项】，添加指纹加密后，每当用户打开微信，全屏指纹识别模块就开始检测通讯录位置的触摸动作进而进行指纹识别。如此，实现了对用户信息的多重保护，进一步提高了用户信息的安全性。为了便于管理指纹加密信息、包括加密的操作对象、加密的图标相对位置等，可以在终端的设置选项里增加【加密信息管理】选项，从而实现一键关闭或者清除指纹加密信息。

[0059] 本实施例中提供的操作应用程序的方法，用于终端(比如手机、平板电脑等)中，可以实时检测用户在触摸屏上的触摸动作，通过将用户对操作对象的操作指纹与该操作对象对应的预设解密指纹进行匹配，如果匹配成功则执行相应的操作指令，否则说明操作指纹不对，有可能是陌生人的恶意操作，则无法执行相关操作，从而保护用户的隐私，如此，即使

已经解锁屏幕的终端，陌生人拿到之后也是无法对相应的操作对象(比如应用程序或者应用程序的某一项功能)进行操作的，并且可以有效避免屏幕解锁瞬间的触摸动作引起误操作，提高了终端中用户信息的安全性和隐私性。

[0060] 参见图6，是本发明实施例提供的一种操作应用程序的装置的结构示意图，用于终端(比如手机、平板电脑等)中，其包括：

[0061] 第一判断模块61，用于判断是否存在触摸动作；详细内容参见上述实施例中的步骤S21。

[0062] 第一获取模块62，用于若存在触摸动作，则获取触摸动作对应的操作对象；详细内容参见上述实施例中的步骤S22。

[0063] 提取模块63，用于提取触摸动作对应的操作指纹；详细内容参见上述实施例中的步骤S23。

[0064] 第二判断模块64，用于判断操作指纹与操作对象对应的预设解密指纹是否匹配成功；详细内容参见上述实施例中的步骤S24。

[0065] 执行模块65，用于当操作指纹与预设解密指纹匹配成功时，执行触摸动作对应的操作指令。详细内容参见上述实施例中的步骤S26。

[0066] 本实施例中提供的操作应用程序的装置，可以保证只有匹配成功的操作指纹才能打开该操作对象，此处预设操作指令包含但不限于打开操作对象，也可以是对操作对象的信息更改、数据读写和删除等操作指令，即对于操作对象的一切可执行的操作指令均可以作为预设操作指令的待选目标，用户可以根据实际需要添加或删除相应的预设操作指令，扩大了指纹识别的适用范围，进一步提高了用户信息的安全性。

[0067] 可选地，本发明一些实施例中，如图7所示，提取模块63包括：判断单元631，用于判断触摸动作对应的操作指令是否为预设操作指令；提取单元632，用于当操作指令为预设操作指令时，提取操作指纹。详细内容参见上述实施例中的步骤S23的优选方案。

[0068] 上述操作应用程序的装置，可以为操作对象的某一预设操作指令设置解密指纹，只有用户的触摸动作对应的操作指令为预设操作指令时，才会提取该触摸动作对应的操作指纹，如此，有目的的进行操作指纹的提取，不仅降低了终端的功耗，提高了终端的处理速度，而且避免出现无用的指纹信息对数据处理结果的影响。

[0069] 可选地，预设操作指令为打开操作对象。

[0070] 上述操作应用程序的装置，可以保证只有匹配成功的操作指纹才能打开该操作对象，此处预设操作指令包含但不限于打开操作对象，也可以是对操作对象的信息更改、数据读写和删除等操作指令，即对于操作对象的一切可执行的操作指令均可以作为预设操作指令的待选目标，用户可以根据实际需要添加或删除相应的预设操作指令，扩大了指纹识别的适用范围，进一步提高了用户信息的安全性。

[0071] 可选地，操作对象包括：应用程序、文件夹、私密空间以及聊天记录。

[0072] 上述操作应用程序的装置，此处的操作对象包含但不限于：应用程序、文件夹、私密空间以及聊天记录，自然地，操作对象也可以是某一个应用程序的某一项功能，比如地图定位、短信查看等，用户可以根据实际需要来选取操作对象，如此大大丰富了用户信息的加密方式，使用户的隐私更加精细化、个性化，从而提高了用户体验。

[0073] 可选地，该操作应用程序的装置还包括：第二获取模块66，用于在判断是否存在触

摸动作之前，获取终端中的至少一个操作对象；设置模块67，用于为每个操作对象设置对应的预设解密指纹。

[0074] 上述操作应用程序的装置，可以预先为终端中被选中的操作对象设置对应的预设解密指纹，被选中的操作对象可以是多个，每个操作对象对应的预设解密指纹可以相同也可以不同，具体根据用户实际需要进行设置，如此，实现了对用户信息的多重保护，进一步提高了用户信息的安全性。

[0075] 本发明实施例还提供了一种终端，包括能够全屏识别指纹的触摸屏和上述任一种操作应用程序的装置。

[0076] 下面以一种手机为例说明本发明的一种终端。

[0077] 如图8所示，相应地，本发明实施例中还提供一种终端，包括：至少一个处理器81、存储器82、触摸屏83和全屏指纹识别模块84，图8中以一个处理器为例，处理器81，存储器82、触摸屏83以及全屏指纹识别模块84通过总线80连接，存储器82存储有可被至少一个处理器81执行的指令，指令被至少一个处理器81执行，以使至少一个处理器执行如下方法：

[0078] 判断是否存在触摸动作；

[0079] 若存在触摸动作，则获取所述触摸动作对应的操作对象；

[0080] 提取所述触摸动作对应的操作指纹；

[0081] 判断所述操作指纹与所述操作对象对应的预设解密指纹是否匹配成功；

[0082] 当所述操作指纹与所述预设解密指纹匹配成功时，执行所述触摸动作对应的操作指令。

[0083] 可选的，所述提取所述触摸动作对应的操作指纹包括：判断所述触摸动作对应的操作指令是否为预设操作指令；当所述操作指令为所述预设操作指令时，提取所述操作指纹。

[0084] 可选的，所述预设操作指令为打开所述操作对象。

[0085] 可选的，所述操作对象包括：应用程序、文件夹、私密空间以及聊天记录。

[0086] 可选的，在本发明的一些实施例中，处理器81通过执行计算机指令，在所述判断是否存在触摸动作之前还可以实现：

[0087] 获取所述终端中的至少一个所述操作对象；

[0088] 为每个所述操作对象设置对应的所述预设解密指纹。

[0089] 相关说明可以对应参见图2至5的步骤所对应的相关描述和效果进行理解，此处不做过多赘述。

[0090] 上述实施例提供的终端，可以实时检测用户在触摸屏上的触摸动作，通过将用户对操作对象的操作指纹与该操作对象对应的预设解密指纹进行匹配，如果匹配成功则执行相应的操作指令，否则说明操作指纹不对，有可能是陌生人的恶意操作，则无法执行相关操作，从而保护用户的隐私，如此，即使已经解锁屏幕的终端，陌生人拿到之后也是无法对相应的操作对象(比如应用程序或者应用程序的某一项功能)进行操作的，并且可以有效避免屏幕解锁瞬间的触摸动作引起误操作，提高了终端中用户信息的安全性和隐私性。

[0091] 本领域技术人员可以理解，实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁

碟、光盘、只读存储记忆体(ROM)或随机存储记忆体(RAM)等。

[0092] 虽然结合附图描述了本发明的实施例，但是本领域技术人员可以在不脱离本发明的精神和范围的情况下作出各种修改和变型，这样的修改和变型均落入由所附权利要求所限定的范围之内。

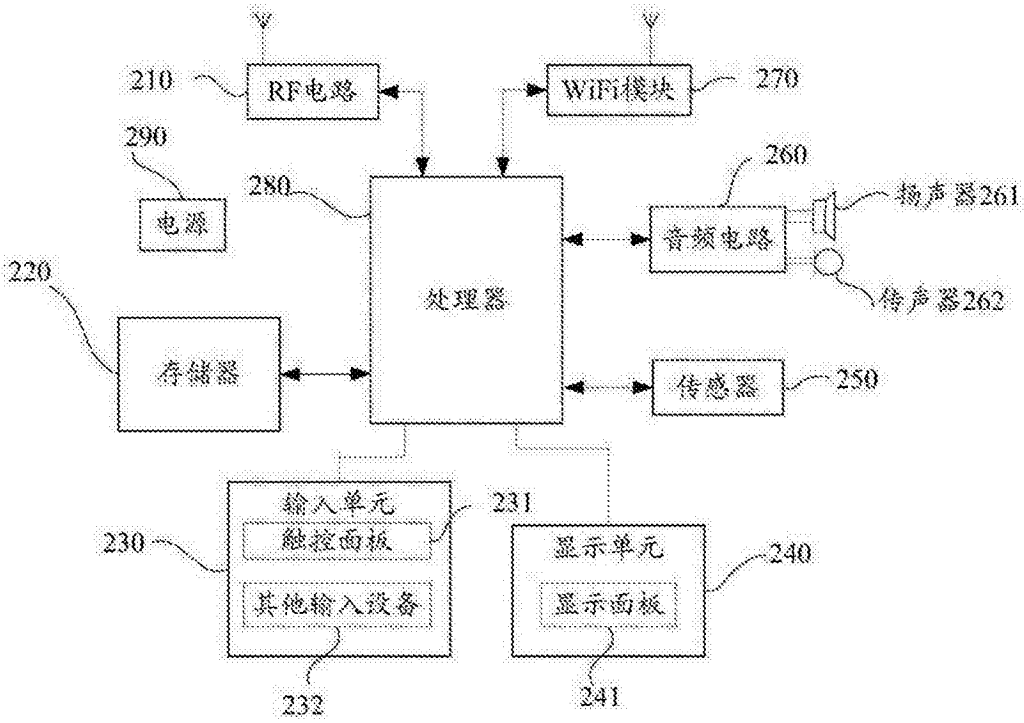

210
RF电路
WiFi模块
270
290
电源
280
处理器
260
音频电路
扬声器261
传声器262
220
存储器
传感器
250
输入单元
触控面板
231
230
其他输入设备
显示单元
240
显示面板
232
241

图1

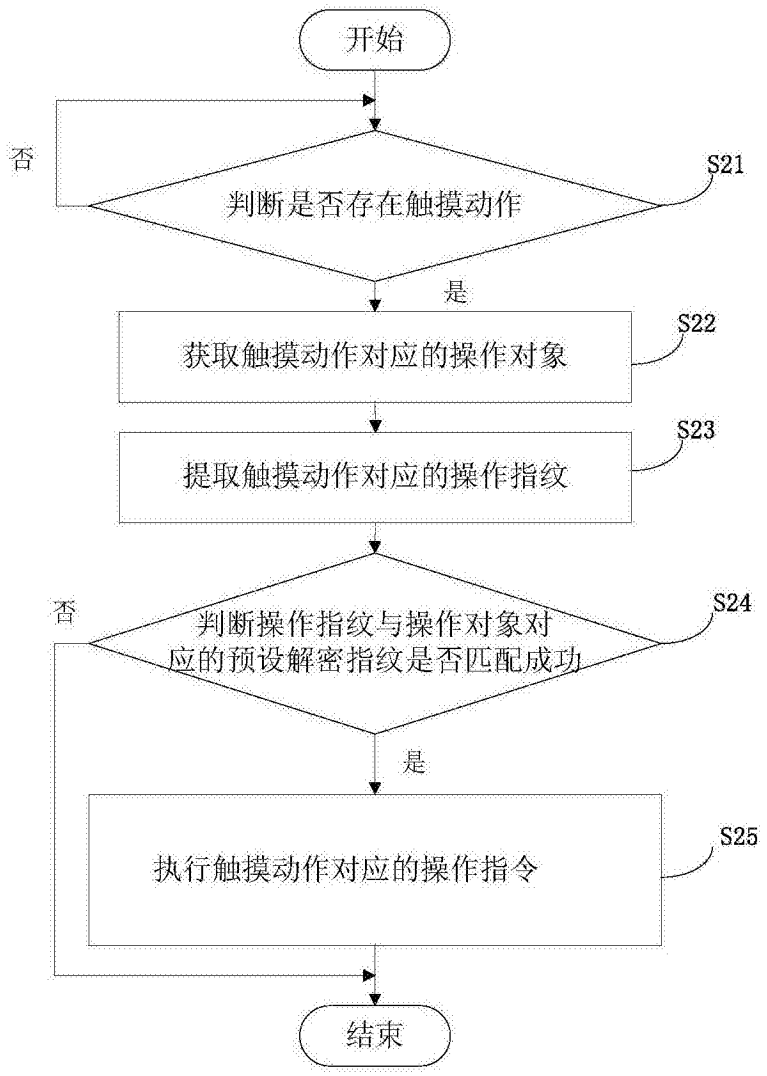

开始
否
判断是否存在触摸动作
S21
是
获取触摸动作对应的操作对象
S22
提取触摸动作对应的操作指纹
S23
否
判断操作指纹与操作对象对应的预设解密指纹是否匹配成功
S24
是
执行触摸动作对应的操作指令
S25
结束

图2

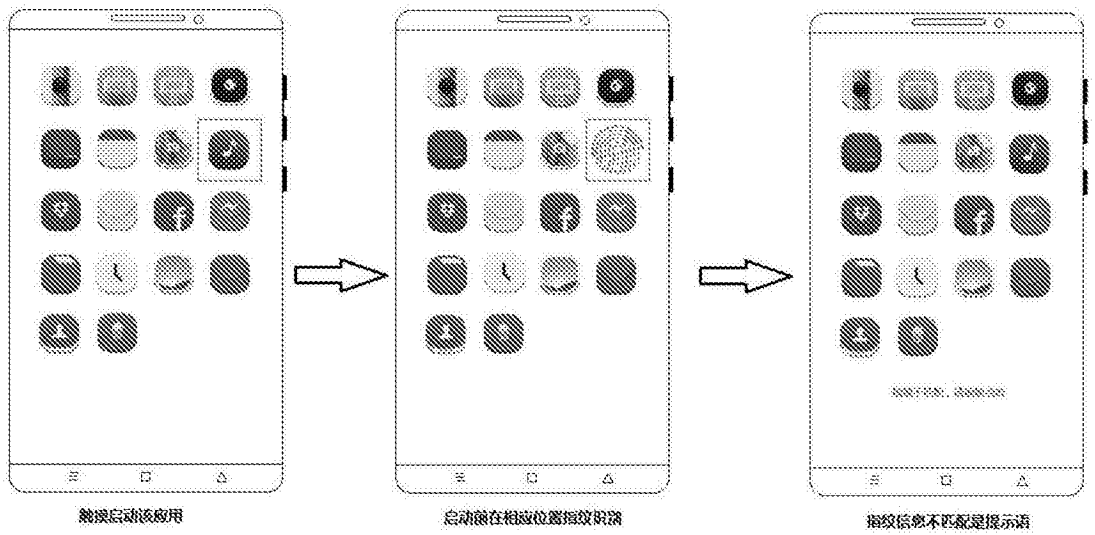


图3

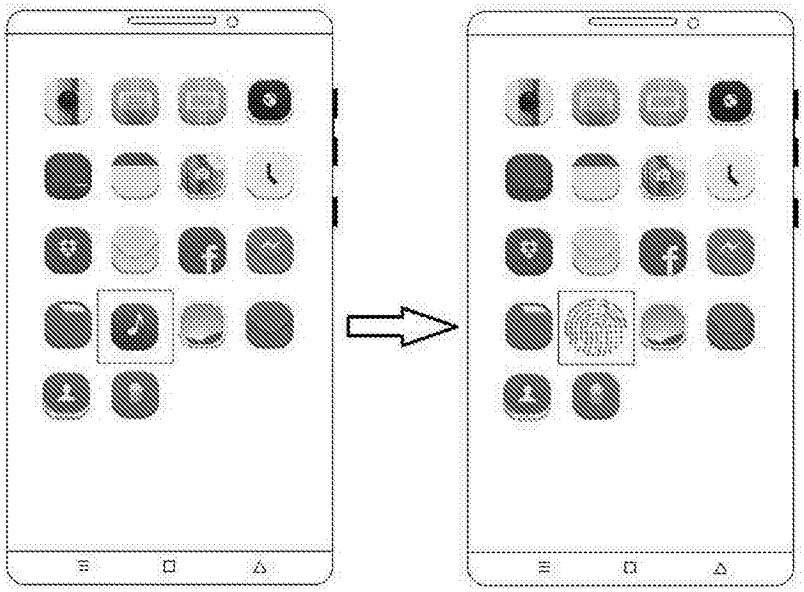


图4

图5

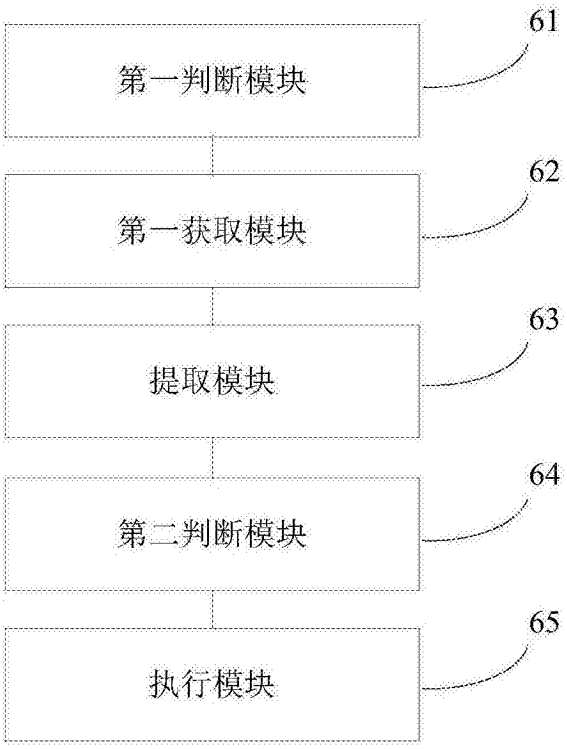


图6

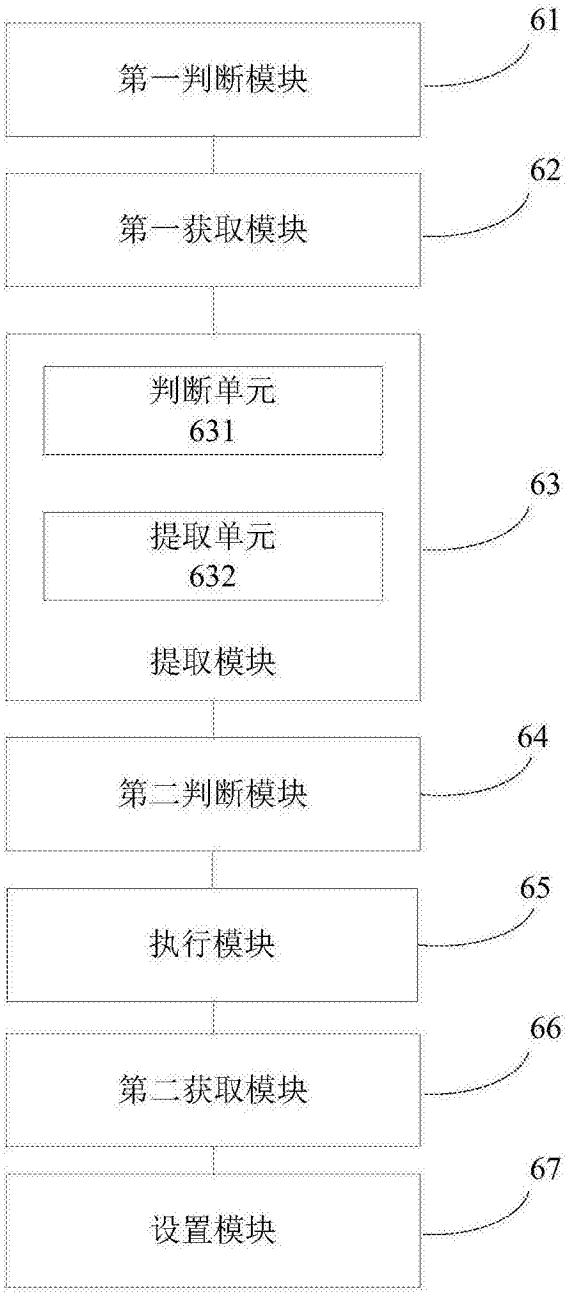

61
第一判断模块
62
第一获取模块
判断单元
631
63
提取单元
632
提取模块
64
第二判断模块
65
执行模块
66
第二获取模块
67
设置模块

图7

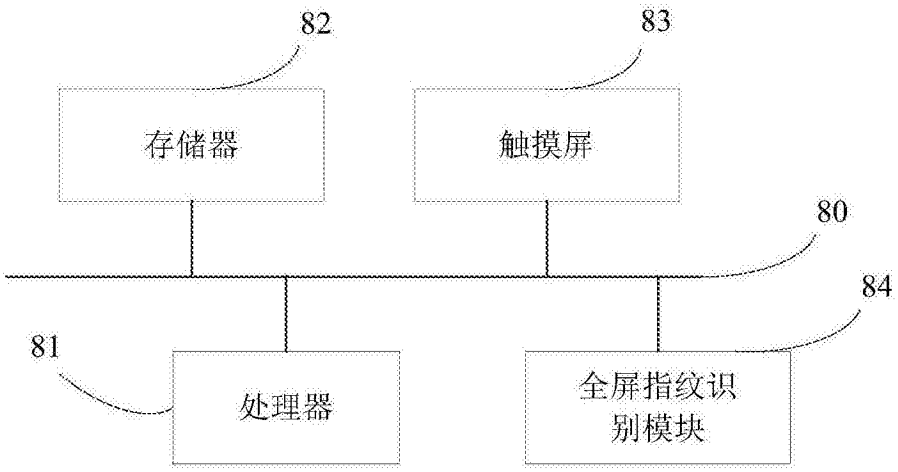


图8