(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108781234 B
(45)授权公告日 2021.07.20

(21)申请号 201780012869.X
(22)申请日 2017.06.09
(65)同一申请的已公布的文献号
申请公布号 CN 108781234 A
(43)申请公布日 2018.11.09
(85)PCT国际申请进入国家阶段日
2018.08.24
(86)PCT国际申请的申请数据
PCT/CN2017/087820 2017.06.09
(87)PCT国际申请的公布数据
WO2018/223402 ZH 2018.12.13
(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 王焕府
(74)专利代理机构 北京中博世达专利商标代理有限公司 11274
代理人 申健
(51)Int.Cl.
H04M 1/67(2006.01)
H04M 1/72463(2021.01)
(56)对比文件
CN 103745148 A,2014.04.23
CN 105787327 A,2016.07.20
审查员 熊金安

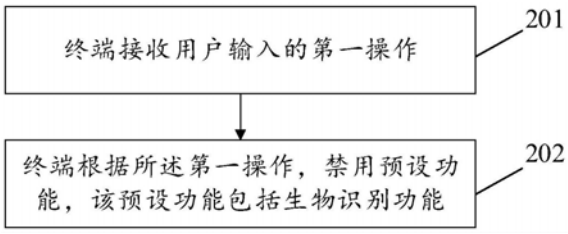
权利要求书1页 说明书15页 附图13页

(54)发明名称

功能控制方法及终端

(57)摘要

本申请公开一种功能控制方法及终端，涉及终端技术领域。为了解决现有技术中存在的由于生物识别技术的便利导致用户的隐私信息易被泄露的问题而发明。其中，该功能控制方法，包括以下步骤：终端接收用户输入的第一操作，然后终端根据该第一操作，禁用预设功能，该预设功能包括生物特征识别功能。本申请适用于用户使用终端的过程中。



CN 108781234 B

1.一种功能控制方法,其特征在于,所述方法应用于终端,所述方法包括:

处于锁屏状态的所述终端接收第一操作,所述第一操作包括按照第一规则按压特定物理按键;

所述终端根据所述第一操作,禁用预设功能,所述预设功能包括生物特征识别功能,所述生物特征识别功能用于解锁所述终端;

所述终端接收解锁密码;

所述终端根据所述解锁密码,解除所述锁屏状态。

2.根据权利要求1所述的方法,其特征在于,所述按照所述第一规则按压特定物理按键包括:同时按压第一物理按键和第二物理按键。

3.根据权利要求1所述的方法,其特征在于,所述方法还包括:

所述终端根据所述解锁密码,恢复所述预设功能。

4.根据权利要求1所述的方法,其特征在于,所述按照所述第一规则按压所述特定物理按键包括:单击或者双击所述特定物理按键。

5.根据权利要求1至4任一项所述的方法,其特征在于,在所述终端接收所述第一操作之前,所述方法还包括:

处于锁屏状态的所述终端接收生物特征识别信息;

所述终端根据所述生物特征识别信息,解除锁屏状态。

6.根据权利要求1至4任一项所述的方法,其特征在于,所述生物特征识别功能包括以下项中的任一种:虹膜识别、指纹识别或人脸识别。

7.根据权利要求1至4任一项所述的方法,其特征在于,所述禁用所述预设功能后,所述终端无法使用所述生物特征识别功能解锁。

8.根据权利要求1至4任一项所述的方法,其特征在于,所述禁用所述预设功能还包括:所述终端禁用预设应用程序。

9.根据权利要求8所述的方法,其特征在于,所述终端禁用所述预设应用程序包括:不显示所述被禁用的预设应用程序的图标;或者,所述被禁用的预设应用程序的图标显示为灰色。

10.根据权利要求7所述的方法,其特征在于,所述禁用所述预设功能后,所述终端仍处于所述锁屏状态。

11.一种终端,其特征在于,所述终端包括存储器和处理器,所述存储器被配置为存储代码,所述处理器运行所述代码使得所述终端执行上述权利要求1-10任一项所述的功能控制方法。

12.一种计算机可读存储介质,所述计算机可读存储介质中存储有指令,当其在计算机上运行时,使得计算机执行上述权利要求1至10任一项所述的方法。

功能控制方法及终端

技术领域

[0001] 本申请涉及终端技术领域，尤其涉及一种功能控制方法及终端。

背景技术

[0002] 生物识别技术是指通过计算机与光学、声学、生物传感器和生物统计学原理等高科技手段密切结合，利用人体固有的生理特性(如指纹、脸象、虹膜等)和行为特征(如笔迹、声音、步态等)来进行个人身份的鉴定。

[0003] 生物识别技术具备不易遗忘、防伪性能好、不易伪造或被盗、随身“携带”和随时随地可用等优点。因此，生物识别技术广泛应用于手机等终端。

[0004] 但是，在一些特殊场景下，正是由于生物识别技术的应用便利的特点导致用户的隐私信息更易被泄露。例如：在用户睡眠时手机被盗，盗用者可在用户尚未醒来时使用用户的指纹解锁手机获取用户的隐私信息。

发明内容

[0005] 本申请提供一种功能控制方法及终端，以解决现有技术中存在的由于生物识别技术的便利导致用户的隐私信息易被泄露的问题。

[0006] 为达到上述目的，本申请提供以下方案：

[0007] 第一方面，提供一种功能控制方法，该方法应用于终端。该方法包括以下步骤：终端接收用户输入的第一操作，然后终端根据该第一操作，禁用预设功能，该预设功能包括生物特征识别功能。

[0008] 其中，上述第一操作包括以下操作中的任意一种：用户输入预设生物特征识别信息、用户按压特定物理按键、用户输入预设密码和用户输入特定语音指令。

[0009] 本申请提供的功能控制方法，终端接收用户输入的快捷操作(第一操作)后禁用包括生物特征识别功能在内的预设功能。这样，在紧急情况下，用户能够通过快捷操作(第一操作)快速禁用生物特征识别功能，避免由于生物特征识别功能能够实现快速身份验证而带来的隐私易被泄露的问题。

[0010] 可选的，在第一方面的一种实现方式中，所述终端根据第一操作，禁用预设功能还包括：终端根据该第一操作，禁用预设应用程序。

[0011] 通过该实现方式，当终端上安装有隐私类应用时，用户可通过该快捷操作(第一操作)禁用预设应用程序，禁用后的应用程序不显示在终端的界面上，这样，其他用户在使用该终端时，无法查看或使用用户禁用的应用程序，有利于保护用户隐私。

[0012] 可选的，在第一方面的一种实现方式中，在终端接收用户输入的第一操作之前，终端处于锁屏状态。则在终端根据用户输入的第一操作，禁用预设功能之后，所述方法还包括：终端解除锁屏状态，显示第一界面，该第一界面不包括禁用的应用程序的图标。

[0013] 通过该实现方式，如果用户在终端处于锁屏状态时输入第一操作，则该第一操作除了能够触发终端禁用预设功能外，还能够触发终端解除解锁状态，显示解锁后的界面。由

于终端可能禁用了预设应用程序，则该解锁后的界面不显示被禁用的应用程序的图标。

[0014] 可选的，在第一方面的一种实现方式中，在终端接收用户输入的第一操作之前，终端处于锁屏状态。则在终端根据该第一操作，禁用预设功能之后，所述方法还包括：终端接收用户输入的第一解锁密码，该第一解锁密码用于解除终端的锁屏状态。终端根据该第一解锁密码，解除锁屏状态，显示第一界面，该第一界面不包括禁用的应用程序的图标。

[0015] 通过该实现方式，如果用户在终端处于锁屏状态时输入第一操作，则该第一操作能够触发终端禁用预设功能。被禁用的功能包括生物识别功能，因此，用户无法使用生物识别功能。则用户需要通过输入解锁密码等其他方式解锁终端。同样，解锁后的终端显示的第一界面不包括禁用的应用程序的图标。

[0016] 可选的，在第一方面的一种实现方式中，在终端根据第一操作，禁用预设功能之后，所述方法还包括：终端接收用户输入的第二操作，并根据用户输入的该第二操作，恢复预设功能。

[0017] 其中，该第二操作包括用户输入特定指纹信息、输入特定手势、特定密码、特定语音指令等。所述恢复预设功能，包括：终端使能生物特征识别功能。

[0018] 通过该实现方式，用户可通过输入第二操作解除对预设功能的禁用。

[0019] 示例性的，所述第二操作包括用户在终端解除锁屏状态并显示第一界面后输入的第二解锁密码。则终端根据用户输入的所述第二操作，恢复所述预设功能，包括：终端根据该第二解锁密码，恢复生物特征识别功能以及解除对已禁用应用程序的禁用，显示第二界面。

[0020] 其中，所述第二界面包括所有应用程序的图标，所述所有应用程序包括已解除禁用的应用程序。

[0021] 通过该实现方式，在显示解锁后的第一界面后，由于终端处于禁用了预设功能的状态，则用户可通过在解锁后输入解锁密码，进而终端根据该解锁密码解除对预设功能的禁用，并显示解除禁用后的第二界面，该第二界面恢复显示之前被禁用的应用程序的图标。

[0022] 可选的，在第一方面的一种实现方式中，在终端接收用户输入的第一操作之前，终端处于锁屏状态。则上述方法还包括：终端接收用户输入的第三操作，并根据该第三操作，解除锁屏状态，显示第二界面，该第二界面包括所有应用程序的图标。

[0023] 其中，该第三操作包括用户输入特定生物特征识别信息、输入特定手势、特定密码、特定语音指令等。

[0024] 通过该实现方式，与用户输入第一操作触发终端禁用预设功能不同，用户可输入该第三操作触发终端解锁。

[0025] 第二方面，提供一种终端，所述终端包括：接收单元，用于接收用户输入的第一操作，该第一操作包括以下操作中的任意一种：用户输入预设生物特征识别信息、用户按压特定物理按键、用户输入预设密码和用户输入特定语音指令。处理单元，用于根据所述接收单元接收的所述第一操作，禁用预设功能，所述预设功能包括生物特征识别功能。

[0026] 可选的，在第二方面的一种实现方式中，所述处理单元，还用于根据所述第一操作，禁用预设应用程序。

[0027] 可选的，在第二方面的一种实现方式中，所述终端还包括显示单元。所述处理单元，还用于当所述终端处于锁屏状态时，根据所述第一操作，禁用预设功能并解除锁屏状

态。所述显示单元，用于显示第一界面，所述第一界面不包括所述处理单元禁用的应用程序的图标。

[0028] 可选的，在第二方面的一种实现方式中，所述接收单元，还用于接收用户在所述终端处于锁屏状态时输入的第一解锁密码，所述第一解锁密码用于解除所述终端的锁屏状态。所述处理单元，还用于根据所述第一解锁密码，解除锁屏状态。所述显示单元，用于显示第一界面，所述第一界面不包括所述处理单元禁用的应用程序的图标。

[0029] 可选的，在第二方面的一种实现方式中，所述接收单元，还用于接收用户输入的第二操作。所述处理单元，还用于根据所述接收单元接收的所述第二操作，恢复所述预设功能。其中，所述恢复所述预设功能，包括：使能所述生物特征识别功能。

[0030] 可选的，在第二方面的一种实现方式中，所述接收单元，还用于接收用户输入的第二解锁密码。所述处理单元，还用于根据所述接收单元接收的所述第二解锁密码，恢复生物特征识别功能以及解除对已禁用应用程序的禁用。所述显示单元，还用于显示第二界面，所述第二界面包括所述处理单元已解除禁用的应用程序的图标。

[0031] 可选的，在第二方面的一种实现方式中，所述接收单元，还用于接收用户在终端处于锁屏状态时输入的第三操作。所述处理单元，还用于根据所述接收单元接收的所述第三操作，解除锁屏状态。所述显示单元，还用于显示第二界面，所述第二界面包括所有应用程序的图标，该所有应用程序的图标包括所述处理单元已解除禁用的应用程序的图标。

[0032] 第三方面，提供一种终端，所述终端包括：输入设备，用于接收用户输入的第一操作，所述第一操作包括以下操作中的任意一种：用户输入预设生物特征识别信息、用户按压特定物理按键、用户输入预设密码和用户输入特定语音指令。处理器，用于根据所述第一操作，禁用预设功能，所述预设功能包括生物特征识别功能。

[0033] 可选的，在第三方面的一种实现方式中，所述处理器，还用于根据所述第一操作，禁用预设应用程序。

[0034] 可选的，在第三方面的一种实现方式中，所述终端还包括显示器。所述处理器，还用于当所述终端处于锁屏状态时，根据所述第一操作，禁用预设功能并解除锁屏状态。所述显示器，用于显示第一界面，所述第一界面不包括禁用的应用程序的图标。

[0035] 可选的，在所述第三方面的一种实现方式中，所述终端还包括显示器。所述输入设备，还用于接收用户在所述终端处于锁屏状态时输入的第一解锁密码，所述第一解锁密码用于解除所述终端的锁屏状态。所述处理器，还用于根据所述第一解锁密码，解除锁屏状态。所述显示器，用于显示第一界面，所述第一界面不包括禁用的应用程序的图标。

[0036] 可选的，在第三方面的一种实现方式中，所述输入设备，还用于接收用户输入的第二操作。所述处理器，还用于根据所述所述第二操作，恢复所述预设功能。其中，所述恢复所述预设功能，包括：使能所述生物特征识别功能。

[0037] 可选的在第三方面的一种实现方式中，所述输入设备，还用于接收用户输入的第二解锁密码。所述处理器，还用于根据所述第二解锁密码，恢复生物特征识别功能以及解除对已禁用应用程序的禁用。所述显示器，还用于显示第二界面，所述第二界面包括已解除禁用的应用程序的图标。

[0038] 可选的，在第三方面的一种实现方式中，所述输入设备，还用于接收用户在终端处于锁屏状态时输入的第三操作。所述处理器，还用于根据所述第三操作，解除锁屏状态。所

述显示器，用于显示所述第二界面，所述第二界面包括所有应用程序的图标。

[0039] 第四方面，提供一种计算机可读存储介质，该计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述第一方面所述的方法。

[0040] 第五方面，提供一种计算机程序产品，该计算机程序产品包含指令，当其在计算机上运行时，使得计算机执行上述第一方面所述的方法。

附图说明

[0041] 图1为手机的一种结构示意图；

[0042] 图2为本申请实施例提供的一种功能控制方法的流程示意图；

[0043] 图3为本申请实施例提供的另一种功能控制方法的流程示意图；

[0044] 图4a为本申请实施例提供的用户在手机中录入功能禁用指纹的一种界面示意图；

[0045] 图4b为本申请实施例提供的用户在手机中录入功能禁用指纹的另一种界面示意图；

[0046] 图4c为本申请实施例提供的用户在手机中设定要禁用的生物特征识别功能的一种界面示意图；

[0047] 图4d为本申请实施例提供的用户在手机中设定要禁用的预设应用程序的一种界面示意图；

[0048] 图4e为本申请实施例提供的用户在手机中设定要禁用的预设应用程序的另一种界面示意图；

[0049] 图4f为本申请实施例提供的用户在手机中设定用于解除对已禁用功能的禁用的密码的界面示意图；

[0050] 图5为本申请实施例提供的手机响应用户在锁屏界面输入的第一操作的流程示意图；

[0051] 图5a为本申请实施例提供的手机响应用户在锁屏界面输入的指纹的界面示意图；

[0052] 图5b为本申请实施例提供的手机响应用户在锁屏界面输入的密码的界面示意图；

[0053] 图5c为本申请实施例提供的用户操作手机以解除对预设功能的禁用的界面示意图；

[0054] 图6为本申请实施例提供的一种终端的结构示意图；

[0055] 图6a为本申请实施例提供的另一种终端的结构示意图。

具体实施方式

[0056] 本申请实施例提供一种具有指纹识别功能的终端，所述终端可以为手机、平板电脑、笔记本电脑、超级移动个人计算机(Ultra-mobile Personal Computer,UMPC)、上网本、个人数字助理(Personal Digital Assistant,PDA)、车载导航、可穿戴设备等设备。

[0057] 以所述终端为手机为例，如图1所示，该手机100包括：射频(radio frequency,RF)电路110、存储器120、输入单元130、生物识别传感器140、处理器150、电源160、显示单元170、重力传感器180、音频电路190等部件。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。

[0058] 下面分别对手机100的各功能组件进行介绍：

[0059] 其中，RF电路110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，给处理器150处理；另外，将上行的数据发送给基站。通常，RF电路110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(low noise amplifier，LNA)、双工器等。此外，RF电路110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，包括但不限于全球移动通讯系统(global system of mobile communication，GSM)、通用分组无线服务(general packet radio service，GPRS)、码分多址(code division multiple access，CDMA)、宽带码分多址(wideband code division multiple access，WCDMA)、长期演进(long term evolution，LTE)、电子邮件、短消息服务(short messaging service，SMS)等。

[0060] 存储器120可用于存储软件程序以及模块，该处理器150通过运行存储在存储器120的软件程序以及模块，从而执行手机100的各种功能应用以及数据处理。存储器120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(Application，APP)等，比如声音播放功能、图像播放功能等；存储数据区可存储根据手机100的使用所创建的数据(比如音频数据、图像数据、电话本等)等。此外，存储器120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。

[0061] 输入单元130可用于接收用户输入的数字或字符信息，以及产生与手机100的用户设置以及功能控制有关的键信号输入。具体地，输入单元130可包括触摸屏131以及其他输入设备132。触摸屏131，也称为触控面板，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摸屏131上或在触摸屏131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，触摸屏131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150，并能接收处理器150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摸屏131。除了触摸屏131，输入单元130还可以包括其他输入设备132。具体地，其他输入设备132可以包括但不限于物理键盘、功能键(比如音量控制按键、电源开关按键等)、轨迹球、鼠标、操作杆等中的一种或多种。

[0062] 生物识别传感器140具体包括指纹识别传感器141、人脸识别传感器142、虹膜识别传感器143。以指纹识别传感器为例，指纹识别传感器能够采集用户的指纹信息并将采集的指纹信息上报给处理器150，处理器150根据该指纹信息对用户进行身份识别。基于生物识别传感器140，手机可在锁屏界面根据用户输入的指纹对用户进行身份验证，当身份验证成功时，手机解锁。基于生物识别传感器140，手机还可在某些支付应用对用户进行身份验证，当身份验证成功时，用户可使用支付应用进行支付。

[0063] 显示单元170可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100的各种菜单。显示单元170可包括显示面板171，可选的，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171。进一步的，触摸屏131可覆盖显示面板171，当触摸屏131检测到在其上或附近的触摸操作后，传送给处理器150以确定触摸事件的类型，随后处理器150根据触摸

事件的类型在显示面板171上提供相应的视觉输出。虽然在图1中，触摸屏131与显示面板171是作为两个独立的部件来实现手机100的输入和输入功能，但是在某些实施例中，可以将触摸屏131与显示面板171集成而实现手机100的输入和输出功能。

[0064] 重力传感器(gravity sensor)180，可以检测手机在各个方向上(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。

[0065] 手机100还可以包括其它传感器，比如光传感器。具体地，光传感器可包括环境光传感器及接近光传感器。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131的亮度；接近光传感器可以检测是否有物体靠近或接触手机，可在手机100移动到耳边时，关闭显示面板131和/或背光。手机100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。

[0066] 音频电路190、扬声器191、麦克风192可提供用户与手机100之间的音频接口。音频电路190可将接收到的音频数据转换后的电信号，传输到扬声器191，由扬声器191转换为声音信号输出；另一方面，麦克风192将收集的声音信号转换为电信号，由音频电路190接收后转换为音频数据，再将音频数据输出至RF电路110以发送给比如另一手机，或者将音频数据输出至存储器120以便进一步处理。

[0067] 处理器150是手机100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120内的软件程序和/或模块，以及调用存储在存储器120内的数据，执行手机100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150可包括一个或多个处理单元；可选的，处理器150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150中。

[0068] 手机100还包括给各个部件供电的电源160(比如电池)，可选的，电源可以通过电源管理系统与处理器150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。

[0069] 尽管未示出，手机100还可以包括天线、无线保真(Wireless-Fidelity，WiFi)模块、近距离无线通信(Near Field Communication，NFC)模块、蓝牙模块、扬声器、加速计、陀螺仪等。

[0070] 目前，由于生物识别的便利性，越来越多的终端支持生物识别。以所述生物识别为指纹识别为例，越来越多的终端支持指纹解锁，且终端上安装的支付宝、微信等支付应用也支持通过指纹进行身份验证，指纹验证成功后，用户可进行支付。具有生物特征识别功能的终端是把双刃剑。一方面，用户在使用具有生物特征识别功能的终端时，能实现快速身份验证，便于用户快速解锁终端或快速支付。另一方面，在以下场景中用户的隐私信息等也因生物特征识别功能的便利性而易被泄露。

[0071] 应用场景：用户在睡眠时手机被盗，盗用者可在用户尚未醒来时操作用户的手指使用用户的指纹解锁手机获得使用手机的权限，进而可查看手机中安装的支付应用的账户信息、相册中的照片、联系人等隐私信息。甚至，盗用者可使用用户的指纹在支付应用中进行指纹验证，并在指纹验证成功后进行转账等非法操作。

[0072] 为了解决因生物特征识别的便利性导致用户的隐私信息易被泄露甚至在紧急情

况下带来损失的问题，本申请实施例提供一种功能控制方法，该方法可应用于图1所示的终端，如图2所示，该方法包括以下步骤：

[0073] 201、终端接收用户输入的第一操作。

[0074] 其中，所述第一操作包括用户输入的指纹、虹膜等生物识别特征信息，还包括用户按压特定物理按键，具体包括单击、双击以及按照一定规则按压特定物理按键，如同时按压音量增大键和减小键等。所述第一操作还包括用户输入特定语音指令，如包含“锁定”等特定词语的语音指令。所述第一操作还包括用户输入预设手势。所述第一操作还包括用户输入特定密码，例如：用户输入第一特定密码用于解锁终端，用户输入第二特定密码用于触发终端禁用预设功能。所述第一操作还包括用户沿特定方向移动手机等。所述第一操作还可以为其他快捷操作，本申请实施例不限定该第一操作的具体实现。

[0075] 需要说明的是，所述第一操作为触发终端禁用预设功能的快捷操作。通过该快捷操作，能够实现快速禁用生物特征识别功能。用户无需在终端的“设置”功能选项中进行设置后才能禁用生物特征识别功能等预设功能带来的操作繁琐的问题。

[0076] 202、终端根据所述第一操作，禁用预设功能。

[0077] 其中，禁用的该预设功能包括生物特征识别功能，该生物特征识别功能具体包括虹膜识别、指纹识别、人脸识别等。以所述生物特征识别功能为指纹识别功能为例，禁用指纹识别功能的方式包括：方式一、终端设置指纹识别传感器以禁止指纹传感器工作。例如：终端关闭指纹传感器，或者终端给指纹识别传感器的供电电流较小，使得指纹识别传感器处于待机状态。在该方式中，即使用户输入指纹，指纹识别传感器无法工作，则无法采集用户的指纹。方式二、终端修改系统配置文件，使得系统配置文件中包含指纹识别功能已禁用的指示信息。禁用指纹识别功能后，指纹识别功能失效。具体实现为：指纹传感器采集用户输入的指纹并将该指纹上报给处理器，处理器接收指纹传感器采集的指纹后，查看系统配置文件，确定终端当前指纹识别功能被禁用，则处理器不对指纹传感器采集的指纹进行处理或者默认向上层应用返回身份验证失败的指示。例如：用户在终端上安装了“电子钱包”这一支付应用，在禁用指纹识别功能后，用户在电子钱包界面输入指纹后，处理器接收指纹传感器采集的指纹，查看系统配置文件，确定终端当前指纹识别功能被禁用，则处理器不对指纹传感器采集的指纹进行处理或向电子钱包这一应用返回身份验证失败的指示，电子钱包这一应用由于一直未收到处理器的响应或者接收到身份验证失败的指示，则用户无法使用指纹验证快速完成身份验证，进而无法打开电子钱包或使用电子钱包的支付等功能。

[0078] 在指纹识别功能失效后，对于支持指纹解锁的终端，用户无法使用指纹快速解锁终端；对于某些需要进行指纹验证才能打开或使用某些功能的应用，用户也无法使用指纹快速打开该类应用或使用该类应用的某些功能。则当应用在上述场景1时非法使用者无法使用用户的指纹在支付应用中进行指纹验证，只能通过输入密码的方式。由于密码一般由多位数字组成，非法使用者在不知晓密码的情况下，需要多次尝试输入密码。相比于非法使用者使用指纹尝试解锁，输入密码尝试解锁的错误率更高，需要尝试的时间更长。因此能够延长终端被解锁的时间，进而给用户赢得更充足的斗争时间。

[0079] 本申请实施例提供的功能控制方法，终端接收用户输入的快捷操作(第一操作)后禁用包括生物特征识别功能在内的预设功能。这样，在紧急情况下，用户能够通过快捷操作快速禁用生物特征识别功能，避免由于生物特征识别功能能够实现快速身份验证而带来的

隐私易被泄露的问题。

[0080] 目前，用户在终端上安装的应用程序的种类和数量越来越多。以手机为例，用户可能在手机上安装“支付宝”、“电子钱包”等各种支付应用。支付类的应用一般存储有用户的账户余额等信息。用户还可能在手机安装“图库”、“微信”、“QQ”等应用程序，这些应用程序存储有用户的照片以及与他人的聊天记录等信息。用户还可能根据个人的兴趣爱好安装游戏类应用等。有些应用场景下，在用户2使用用户1的终端的过程中，用户1不希望用户2查看某些应用程序，如不希望用户查看终端上安装的“图库”应用和游戏类应用。为了保护用户的隐私信息，在其他实现方式中，所述禁用预设功能还包括：终端禁用预设应用程序。

[0081] 其中，该预设应用程序包括用户预先设置的要“禁用”的一个或多个应用程序。该预设应用程序还包括用户预先设置的要“禁用”的一类或多类应用程序。或者该预设应用程序包括终端默认将手机中安装的一些应用设定为隐私类应用，则在检测到用户输入的第一操作后，终端默认禁用该隐私类应用。在终端通过输入的第一操作禁用预设应用程序后，终端在设置界面、应用管理界面或终端的主页界面均不显示该被禁用的应用程序的图标。因此，在禁用预设应用程序后，从用户角度而言，终端切断了用户操作该预设应用程序的接口，用户可能认为终端并未安装该预设应用程序。

[0082] 在其他实现方式中，终端禁用预设程序后，这些预设应用程序的图标在终端上显示为灰色，用户点击该应用图标后终端不响应。

[0083] 具体实现中，当终端接收到用户输入的第一操作时，终端获取用户设置的预设应用程序列表，修改该预设应用程序列表中应用程序的配置文件以将应用程序的状态设置为禁用。

[0084] 通过上述方法，用户可预先将终端上安装的一些应用程序设定为需要禁用的应用程序，则当终端接收到用户的快捷操作时，在禁用生物特征识别功能的同时禁用用户预先设定的这些应用程序，能够保护用户隐私。

[0085] 可选的，在终端接收用户输入的第一操作之前，如果所述终端处于锁屏状态。则在终端根据所述第一操作，禁用预设功能之后，所述方法还包括：终端解除锁屏状态，显示第一界面，该第一界面不包括禁用的应用程序的图标。

[0086] 通过该实现方式，如果用户在终端处于锁屏状态时输入第一操作，则该第一操作除了能够触发终端禁用预设功能外，还能够触发终端解除解锁状态，显示解锁后的界面。由于终端可能禁用了预设应用程序，则该解锁后的界面不显示被禁用的应用程序的图标。

[0087] 可选的的，在终端接收用户输入的第一操作之前，如果终端处于锁屏状态。则在终端根据所述第一操作，禁用预设功能之后，上述方法还包括：终端接收用户输入的第一解锁密码，该第一解锁密码用于解除所述终端的锁屏状态。终端根据该第一解锁密码，解除锁屏状态，显示第一界面，该第一界面不包括禁用的应用程序的图标。

[0088] 其中，所述第一解锁密码可以为滑动手势解锁密码，也可以为数字、字母等字符串组成的解锁密码。

[0089] 需要说明的是，所述第一界面不是指终端解锁后终端当前显示的一个界面，而是指用于显示终端中安装的应用程序的图标的所有界面的总称。当终端中安装的应用程序较多时，受限于终端屏幕，该第一界面的当前显示部分无法将所有应用程序的图标均同时呈现给用户，仅能呈现部分应用程序图标。用户需要左右或上下滑动该第一界面才能查看其

它应用程序的图标。

[0090] 通过该实现方式，如果用户在终端处于锁屏状态时输入第一操作，则该第一操作能够触发终端禁用预设功能。被禁用的功能包括生物识别功能，因此，用户无法使用生物识别功能。则由于终端仍然处于锁屏状态，则用户需要通过输入解锁密码等其他方式解锁终端。同样，解锁后的终端显示的第一界面不包括禁用的应用程序的图标。

[0091] 可选的，在步骤202“终端根据所述第一操作，禁用预设功能”之后，如图3所示，所述方法还包括以下步骤：

[0092] 301、终端接收用户输入的第二操作。

[0093] 其中，用户输入的所述第二操作包括用户按压特定物理按键、用户输入特定语音指令，如包含“解除锁定”等特定词语的语音指令、用户输入预设手势、用户输入密码、用户沿特定方向移动手机等。所述第二操作还可以为其他快捷操作，本申请实施例不限定该第二操作的具体实现。由于在用户输入第一操作后，终端的生物特征识别功能已被禁用，因此该第二操作不包括用户输入指纹等生物识别特征的操作。本申请实施例不限定所述第二操作的具体实现，所述第二操作用于触发终端恢复被禁用的功能。

[0094] 302、终端根据用户输入的所述第二操作，恢复所述预设功能。

[0095] 其中，所述恢复预设功能包括终端使能所述生物特征识别功能。

[0096] 通过图3所示的方法，在用户通过第一操作禁用预设功能后，终端接收用户的第二操作并根据该第二操作恢复已禁用的所述预设功能。

[0097] 示例性的，所述第二操作包括用户在所述终端解除锁屏状态并显示第一界面后输入的第二解锁密码。则终端根据该第二解锁密码，恢复生物特征识别功能以及解除对已禁用应用程序的禁用，显示第二界面。该第二界面包括所有应用程序的图标，所述所有应用程序包括已解除禁用的应用程序。

[0098] 其中，第二解锁密码可以与前述第一解锁密码实现方式相同。例如：该第二解锁密码可以为九宫格式的滑动手势，也可以为由数字、字母等字符组成密码。第二解锁密码和第一解锁密码可以为相同的手势或字符密码，但第一解锁密码和第二解锁密码的作用不同。具体的，在终端功能被禁用后但处于锁屏状态时，用户输入第一解锁密码，其目的是触发终端解锁。在终端功能被禁用后但处于已解锁状态后，用户输入该第二解锁密码，其目的是触发终端解除对已禁用功能的禁用。

[0099] 其中，用户可在设置菜单中输入所述第二解锁密码。

[0100] 通过该实现方式，在显示解锁后的第一界面后，由于终端处于禁用了预设功能的状态，则用户可通过在解锁后输入解锁密码，进而终端根据该解锁密码解除对预设功能的禁用，并显示解除禁用后的第二界面，该第二界面恢复显示之前被禁用的应用程序的图标。

[0101] 可选的，在终端接收用户输入的第一操作之前，如果终端处于锁屏状态。则所述方法还包括：终端接收用户输入的第三操作并根据该第三操作，解除锁屏状态，显示第二界面，所述第二界面包括所有应用程序的图标。

[0102] 其中，第三操作包括用户输入特定生物特征识别信息、输入特定手势、特定密码、特定语音指令等。其中，该第三操作和第一操作的实现形式可以相同，也可以不同。例如：第一操作为第一预设生物特征识别信息，所述第三操作为第二预设生物特征识别信息。同样，所述第一操作为第一特定密码，所述第三操作为第二特定密码。又如：所述第一操作为预设

生物特征识别信息，所述第三操作为特定密码。

[0103] 通过该实现方式，在终端处于锁屏状态时，如果用户输入的是所述第一操作，则终端禁用预设功能。如果用户输入的是该第三操作，则终端正常解锁。

[0104] 下述实施例以终端为手机，所述第一操作为用户在手机锁屏状态时输入的第一预设指纹，所述第二操作为用户在手机解锁后输入的密码，所述第三操作为用户在手机锁屏状态时输入的第二预设指纹为例进行说明。

[0105] 用户在使用指纹禁用手机的某些功能之前，需要先录入指纹以在后续过程中作为参考指纹。目前手机一般都具有指纹解锁功能，基于用户的使用习惯和使用经验，用户在使用手机时会先录入用于解锁手机的指纹。考虑到用户使用指纹禁用手机的某些功能为手机提供的新功能，在用户录入用于解锁手机的指纹后提示用户继续录入用于手机禁用某些功能的指纹(为了便于描述，下文将该指纹描述为功能禁用指纹)。参考图4a，用户打开手机的设置界面401，该界面显示有用户可对手机进行的设置操作，包括是否开启飞行模式、建立Wi-Fi连接、选取移动网络的类型以及设置要解锁和功能禁用的指纹等选项。用户在界面401中选择“解锁和功能禁用”这一选项后，手机加载界面402，该界面402显示询问用户是否录入解锁指纹的提示信息。当用户点击确认后，手机显示界面403和404以提示用户录入解锁指纹，并在成功录入解锁指纹后显示界面405以提示用户已完成解锁指纹的录入并同时在该界面405提示用户是否继续录入功能禁用指纹。当用户点击确认时，手机显示界面406和界面407提示用户接着录入功能禁用指纹，并在功能禁用指纹录入成功后显示界面408以提示用户已成功录入功能禁用指纹。

[0106] 在其他实现方式中，参考图4b，手机可在设置菜单中增加“功能禁用”这一功能选项，当用户在设置界面501打开“功能禁用”这一功能选项后，显示界面502和界面503提示用户录入功能禁用指纹，并在用户成功录入功能禁用指纹后，显示界面408提示用户已完成录入功能禁用指纹。

[0107] 参考图4c，在成功录入功能禁用指纹后，手机显示界面408提示用户已完成录入功能禁用指纹。当接收到用户在该显示界面408的确认操作后，显示界面601，提示用户设置在使用功能禁用指纹时默认要禁用的生物特征识别功能，包括“虹膜识别功能”、“人脸识别功能”和“指纹识别功能”等。当检测到用户在界面601选择将指纹识别功能设定为默认要禁用的功能时，显示界面602，提示用户已将“指纹识别功能”设定为用户使用功能禁用指纹时默认要禁用的功能。

[0108] 需要说明的是，用户可以将界面601显示的“虹膜识别功能”、“人脸识别功能”和“指纹识别功能”中的一个或多个均设定为默认要禁用的功能。例如:用户可同时将“虹膜识别”和“指纹识别”均设定为默认要禁用的功能。

[0109] 可选的，除了禁用指纹识别功能，还可根据用户需求禁用手机中已安装的应用程序。在一种示例中，参考图4d，在接收用户在界面602输入的确认操作后，显示界面701以询问用户是否设定要禁用的应用程序。当用户点击确认时，手机显示界面703，该界面703显示手机中已安装的所有应用程序，用户可选择将其中一些应用设置为要禁用的APP，界面703中以“微信”和“支付宝”为例进行说明。

[0110] 在另一种示例中，参考图4e，在接收用户在界面602输入的确认操作后，手机显示界面801，该界面801显示有手机中安装的各种类型的应用，包括“聊天类应用”、“支付类应

用”和“游戏类应用”，用户可依次设置每类应用中要禁用的应用。示例性的，用户点击“支付类应用”右侧的选项，手机加载界面802，该界面802显示手机中安装的所有支付类应用，用户可全选以将所有支付类应用都设置为预设禁用应用程序，也可仅选取其中的部分支付应用，图中以用户选取“支付宝”和“招商银行”为例，当用户点击“完成”时，该界面802则“消失”，手机返回至界面801，则用户可在其他类应用中选择要禁用的应用。当用户在界面801点击确认操作后，手机显示界面803提示用户已完成要禁用的应用的设定。

[0111] 为了便于用户解除功能禁用，在用户录入功能禁用指纹之前或之后，提示用户设定解除功能禁用的密码。参考图4f，用户在界面803点击确认操作后，手机显示界面901提示用户继续设置用于解除对已禁用功能的禁用的密码。手机接收到用户在该界面901的确认操作后，显示界面902，用户可在该界面902输入用于解除禁用的密码。在密码设定成功后，手机显示界面903，提示用户密码已设置成功。

[0112] 在用户根据图4a至4f的设置操作完成录入功能禁用指纹、解除功能禁用的密码以及设定完成要禁用的生物特征识别功能、应用程序的后，当手机检测到用户输入的指纹后，手机将用户输入的指纹与用户录入的功能禁用指纹进行比较，如果一致则身份验证成功，进而手机禁用预设的应用程序和指纹识别功能。用户可通过输入密码解除功能禁用。

[0113] 如图5所示，本申请实施例提供的方法包括以下步骤：

[0114] 1001、手机接收用户在锁屏界面输入的操作。

[0115] 其中，当该操作为用户输入密码时，执行下述步骤1010。当该操作为用户输入指纹时，执行下述步骤1002。

[0116] 1002、手机将用户在锁屏界面输入的所述指纹与第一预设指纹比较。

[0117] 考虑到手机在锁屏界面检测到用户输入的指纹可能为解锁指纹，也可能为功能禁用指纹，因此，手机在检测到用户在锁屏界面输入的指纹后，需要对该指纹进行识别并根据识别结果执行相应的操作。

[0118] 其中，该第一预设指纹为用户预先录入的功能禁用指纹。

[0119] 该步骤中，如果用户在锁屏界面输入的指纹与所述第一预设指纹一致，则表明用户输入的指纹为功能禁用指纹，手机则执行下述步骤1004。如果用户在锁屏界面输入的指纹与所述第一预设指纹不一致，手机则执行下述步骤1003以进一步将该指纹与解锁指纹进行比较，并根据比较结果执行相应的步骤。

[0120] 1003、手机将用户在锁屏界面输入的指纹与第二预设指纹比较。

[0121] 其中，该第二预设指纹为用户预先录入的解锁指纹。

[0122] 该步骤中，如果该指纹与所述第二预设指纹一致，表明用户输入的指纹为解锁指纹，则手机执行下述步骤1008。如果所述指纹与所述第二预设指纹不一致，则手机执行下述步骤1009以提示用户再次输入指纹以解锁终端。

[0123] 1004、手机禁用指纹识别功能以及预设应用程序。

[0124] 可选的，手机在禁用指纹识别功能以及预设应用程序之前，弹出提示框以提示用户是否要开启功能禁用，如果用户确认开启，则手机执行该步骤1004，否则手机不开启功能禁用。

[0125] 可选的，在该步骤1004之后，终端发出提示信息以提示用户已成功禁用预设应用程序和指纹识别功能。该提示方式包括：震动提示、指示灯闪烁等、在手机界面上显示提示

信息等。

[0126] 1005、手机接收用户输入的解锁密码。

[0127] 在手机禁用指纹识别功能后，如果用户想要解锁手机，则需要输入解锁密码，通过密码的方式解锁手机。

[0128] 需要说明的是，该步骤1005为可选步骤。在其他实现方式中，手机在执行上述步骤1004后可直接执行该步骤1006。

[0129] 1006、手机显示解锁后的第一界面，该界面不显示已禁用的所述预设应用程序的图标。

[0130] 手机解锁后，解锁后的界面只呈现部分应用程序的图标，未呈现已禁用的所述应用程序的图标。

[0131] 1007、手机接收用户输入的用于解除禁用的密码。

[0132] 在手机禁用指纹识别功能后，用户可输入用于解除禁用的密码以解除对预设功能的禁用。

[0133] 1008、手机显示解锁后的第二界面，该界面显示所述预设应用程序的图标。

[0134] 示例性的，在步骤1004中被禁用的应用程序为支付宝、招商银行等，则在本步骤中恢复显示支付宝、招商银行等支付应用的图标。

[0135] 1009、手机提示用户再次输入解锁指纹以解锁终端。

[0136] 需要说明是，上述步骤1003可以在步骤1002之后执行也可以在步骤1002之前执行；还可以与步骤1002同时执行。本申请实施例不限定步骤1002和步骤1003的执行顺序。

[0137] 1010、手机将用户在锁屏界面输入的密码与预设解锁密码比较。

[0138] 其中，所述预设解锁密码为用户预先输入的用于解除功能禁用的密码，例如图4f所示的用户输入解除功能禁用密码的过程示意图。

[0139] 如果用户输入的密码与预设解锁密码一致，表明用户输入的密码为解锁密码，则手机执行下述步骤1103。如果用户输入的密码与预设解锁密码不一致，则手机执行步骤1012提示用户再次输入解锁密码以解锁手机。

[0140] 1011、手机判断当前是否已开启指纹禁用功能。

[0141] 如果手机已开启指纹禁用功能，则执行上述步骤1006，否则执行上述步骤1008。

[0142] 1012、手机提示用户再次输入解锁密码以解锁手机。

[0143] 为了更清楚的说明图5所示的方法，参考图5a，当用户在锁屏界面输入指纹后，手机将该指纹分别与解锁指纹和功能禁用指纹比较。如果该指纹与解锁指纹一致，手机解锁并加载如1103所示的界面，该界面中显示有所有用户已安装的应用程序的图标。如果该指纹和功能禁用指纹一致，则显示界面1102，弹出提示框，提示用户是否要禁用指纹识别功能以及预设应用程序，也即开启功能禁用的功能。当用户选择确认后，手机禁用指纹识别功能以及预设应用程序。之后，由于手机处于未解锁状态，则如果用户想要解锁手机，则用户由于无法使用指纹识别功能，需要在锁屏界面输入解锁密码。

[0144] 可选的，当用户在界面1102选择确认操作且手机开启功能禁用的功能后，手机弹出提示框(图5a中未示出该界面)提示用户已禁用指纹识别功能以及预设应用程序。

[0145] 参考图5b，当用户在锁屏界面1104输入的为解锁密码时，用户输入正确的解锁密码解锁成功后，如果手机未开启功能禁用功能，则手机加载解锁后的界面1103。如果手机已

开启功能禁用功能，则手机加载解锁后的界面1105。

[0146] 以用户预设设定的要禁用的应用程序包括微信、支付宝为例，解锁后的界面1103与解锁后的界面1105相比，微信、支付宝等应用程序的图标不显示在界面1103中，仅显示在界面1105中。

[0147] 参考图5c，用户在解锁后的界面1105中点击“设置”选项，手机加载界面1106。当用户在界面1106中选择“功能禁用”这一选项后，手机显示界面1107以供用户输入密码，当用户输入的密码与预先录入的解除功能禁用的密码一致时，手机显示界面1103，也即恢复“微信”、“支付宝”的图标。

[0148] 可以理解的是，上述终端为了实现上述功能，其包含了执行各个功能相应的硬件结构和/或软件模块。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[0149] 本申请实施例可以根据上述方法示例对终端进行功能模块的划分，例如，可以对应各个功能划分各个功能模块，也可以将两个或两个以上的功能集成在一个处理模块中。上述集成的模块既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。需要说明的是，本申请实施例中对模块的划分是示意性的，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

[0150] 在采用对应各个功能划分各个功能模块的情况下，图6示出了上述实施例中所涉及的终端的一种可能的结构示意图，终端1200包括：接收单元1210，处理单元1220和显示单元1230。

[0151] 其中，所述接收单元1210，用于接收用户输入的第一操作，所述第一操作包括以下操作中的任意一种：用户输入预设生物特征识别信息、用户按压特定物理按键、用户输入预设密码和用户输入特定语音指令。所述处理单元1220，用于根据所述第一操作，禁用预设功能，所述预设功能包括生物特征识别功能。

[0152] 可选的，所述处理单元1220，还用于根据所述第一操作，禁用预设应用程序。

[0153] 可选的，所述处理单元1220，还用于当所述终端处于锁屏状态时，根据所述第一操作，禁用预设功能并解除锁屏状态。所述显示单元1230，用于显示第一界面，该第一界面不包括所述处理单元1220禁用的应用程序的图标。

[0154] 可选的，所述接收单元1210，还用于接收用户输入的第二操作。所述处理单元1220，还用于根据所述接收单元1210接收的所述第二操作，恢复所述预设功能。其中，所述恢复所述预设功能，包括：使能所述生物特征识别功能。

[0155] 可选的，所述接收单元1210，还用于接收用户输入的第二解锁密码。所述处理单元1220，还用于根据所述接收单元1210接收的所述第二解锁密码，恢复生物特征识别功能以及解除对已禁用应用程序的禁用。所述显示单元1230，还用于显示第二界面，所述第二界面包括所述处理单元已解除禁用的应用程序的图标。

[0156] 此外，结合所述方法对应的流程示意图，具体的，接收单元1210用于支持终端1200执行图2中的过程201、图3中的过程301以及图5中的过程1001、过程1005、过程1007。处理单

元1220用于支持终端1200执行图2中的过程202、图3中的过程302以及图5中的过程1002、过程1003、过程1004、过程1009、过程1010、过程1011以及过程1012。显示单元1230用于支持终端1200执行图5中的过程1006以及过程1008。

[0157] 其中，上述方法实施例涉及的各步骤的所有相关内容均可以援引到对应功能模块的功能描述，在此不再赘述。

[0158] 参阅图6a所示，本申请实施例还提供一种终端，该终端1300包括：存储器1310、处理器1320、输入设备1330和总线1340。可选的，该终端还包括显示器1350和收发器1360。其中，输入设备1330、处理器1320、存储器1310以及收发器1360通过总线1340相互连接。

[0159] 其中，所述输入设备1330，用于接收用户输入的第一操作，该第一操作包括以下操作中的任意一种：用户输入预设生物特征识别信息、用户按压特定物理按键、用户输入预设密码和用户输入特定语音指令。处理器1320，用于根据所述第一操作，禁用预设功能，所述预设功能包括生物特征识别功能。

[0160] 可选的，所述处理器1320，还用于根据所述第一操作，禁用预设应用程序。

[0161] 可选的，所述处理器1320，还用于当所述终端处于锁屏状态时，根据所述第一操作，禁用预设功能并解除锁屏状态。所述显示器1350，用于显示第一界面，所述第一界面不包括禁用的应用程序的图标。

[0162] 可选的，所述输入设备1330，还用于接收用户在所述终端处于锁屏状态时输入的第一解锁密码，所述第一解锁密码用于解除所述终端的锁屏状态。所述处理器1320，还用于根据所述第一解锁密码，解除锁屏状态。所述显示器1350，用于显示第一界面，所述第一界面不包括禁用的应用程序的图标。

[0163] 可选的，所述输入设备1330，还用于接收用户输入的第二操作。所述处理器1320，还用于根据所述所述第二操作，恢复所述预设功能。其中，所述恢复所述预设功能，包括：使能所述生物特征识别功能。

[0164] 可选的，所述输入设备1330，还用于接收用户输入的第二解锁密码。所述处理器1320，还用于根据所述第二解锁密码，恢复生物特征识别功能以及解除对已禁用应用程序的禁用。所述显示器1350，还用于显示第二界面，所述第二界面包括已解除禁用的应用程序的图标。

[0165] 可选的，所述输入设备1330，还用于接收用户在终端处于锁屏状态时输入的第三操作。所述处理器1320，还用于根据所述第三操作，解除锁屏状态。所述显示器1350，用于显示所述第二界面，所述第二界面包括所有应用程序的图标。

[0166] 本申请实施例提供的终端通过输入设备接收用户输入的快捷操作(第一操作)后，处理器禁用包括生物特征识别功能在内的预设功能。这样，在紧急情况下，用户能够通过快捷操作(第一操作)快速禁用生物特征识别功能，避免由于生物特征识别功能能够实现快速身份验证而带来的隐私易被泄露的问题。

[0167] 其中，存储器1310用于存储软件程序及模块，处理器1320通过运行存储在存储器1310的软件程序及模块，从而执行终端的各种功能应用以及实现数据处理。

[0168] 处理器1320可以是中央处理器(Central Processing Unit，CPU)，通用处理器，数字信号处理器(Digital Signal Processor，DSP)，专用集成电路(Application-Specific Integrated Circuit，ASIC)，现场可编程门阵列(Field Programmable Gate Array，FPGA)

或者其他可编程逻辑器件、晶体管逻辑器件、硬件部件或者其任意组合。其可以实现或执行结合本申请公开内容所描述的各种示例性的逻辑方框，模块和电路。所述处理器也可以是实现计算功能的组合，例如包含一个或多个微处理器组合，DSP和微处理器的组合等等。

[0169] 输入设备1330用于实现用户与终端的交互和/或信息输入到终端中。例如，输入设备可以接收用户输入的数字或字符信息，以产生与用户设置或功能控制有关的信号输入。在本申请具体实施方式中，输入可以是触控面板，也可以是其他人机交互界面，例如实体输入键、麦克风等，还可是其他外部信息撷取装置，例如摄像头等。触控面板，也称为触摸屏或触控屏，可收集用户在其上触摸或接近的操作动作。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上或接近触控面板的位置的操作动作，并根据预先设定的程式驱动相应的连接装置。在本申请的其他实施方式中，输入设备所采用的实体输入键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。麦克风形式的输入设备可以收集用户或环境输入的语音并将其转换成电信号形式的、处理器可执行的命令。

[0170] 总线1340可以是外设部件互连标准(Peripheral Component Interconnect，PCI)总线或扩展工业标准结构(Extended Industry Standard Architecture，EISA)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图6a中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

[0171] 收发器1360用于终端和其他网络实体或设备交互，例如终端通过该收发器1360与基站交互等。

[0172] 结合本申请公开内容所描述的方法或者算法的步骤可以硬件的方式来实现，也可以是由处理器执行软件指令的方式来实现。软件指令可以由相应的软件模块组成，软件模块可以被存放于随机存取存储器(Random Access Memory，RAM)、闪存、只读存储器(Read Only Memory，ROM)、可擦除可编程只读存储器(Erasable Programmable ROM，EPROM)、电可擦可编程只读存储器(Electrically EPROM，EEPROM)、寄存器、硬盘、移动硬盘、只读光盘(CD-ROM)或者本领域熟知的任何其它形式的存储介质中。一种示例性的存储介质耦合至处理器，从而使处理器能够从该存储介质读取信息，且可向该存储介质写入信息。当然，存储介质也可以是处理器的组成部分。处理器和存储介质可以位于ASIC中。

[0173] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本申请所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进行传输。计算机可读介质包括计算机存储介质和通信介质，其中通信介质包括便于从一个地方向另一个地方传送计算机程序的任何介质。存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0174] 以上所述的具体实施方式，对本申请的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本申请的具体实施方式而已，并不用于限定本申请的保护范围，凡在本申请的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本申请的保护范围之内。

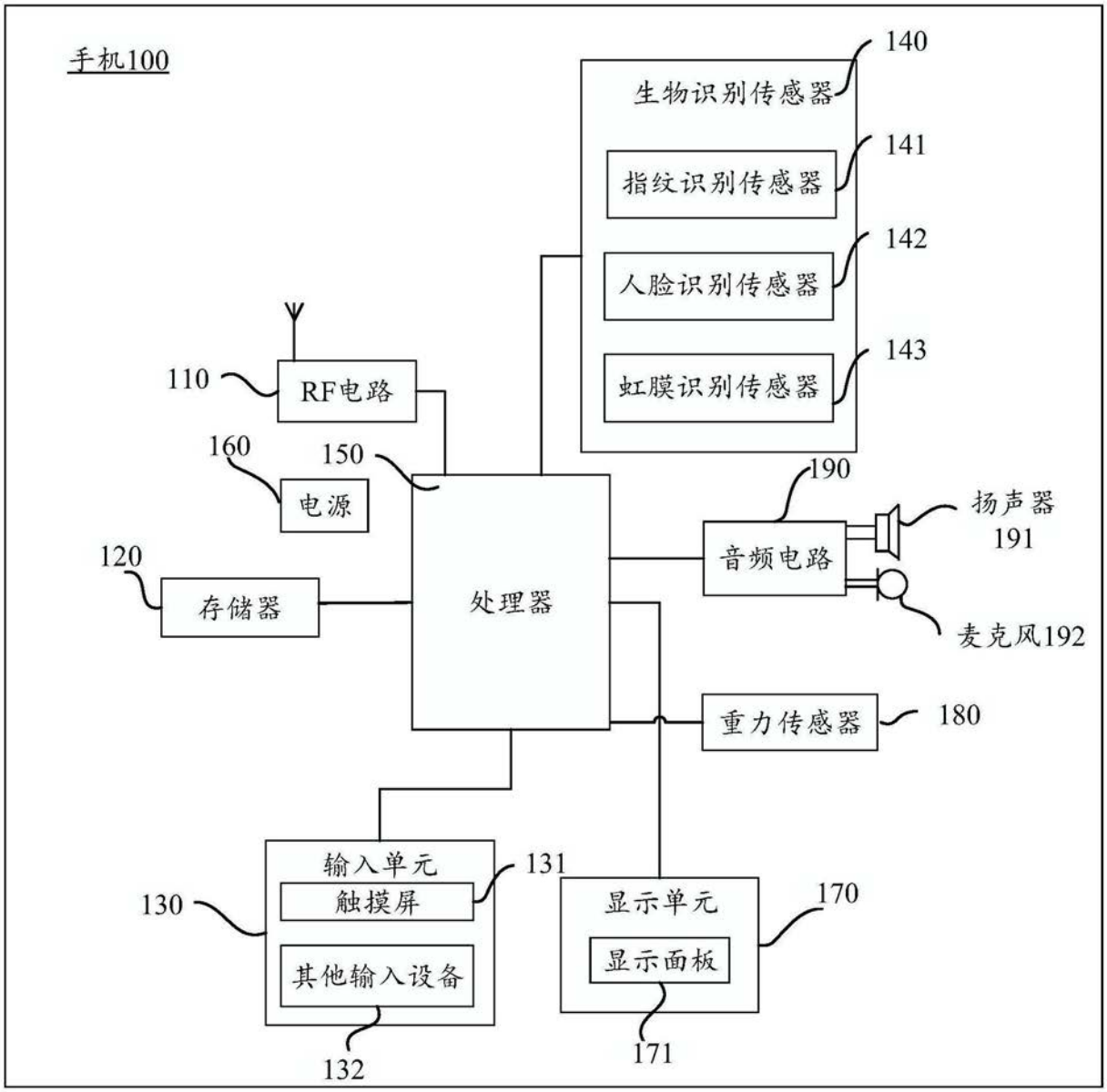

手机100
140
生物识别传感器
141
指纹识别传感器
142
人脸识别传感器
143
虹膜识别传感器
110
RF电路
160
电源
150
处理器
190
音频电路
扬声器
191
麦克风192
120
存储器
重力传感器
180
输入单元
131
130
触摸屏
其他输入设备
132
显示单元
170
显示面板
171

图1

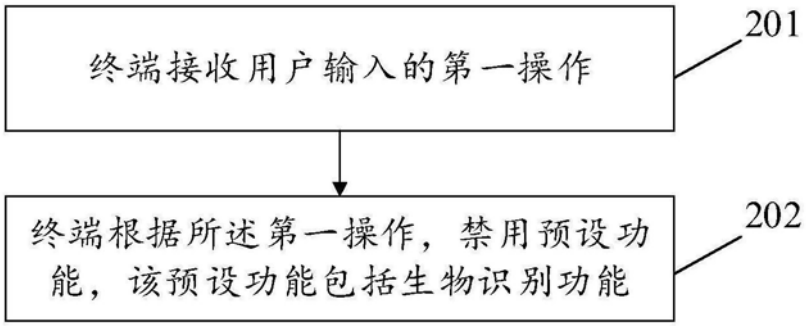

终端接收用户输入的第一操作
201
终端根据所述第一操作，禁用预设功能，该预设功能包括生物识别功能
202

图2

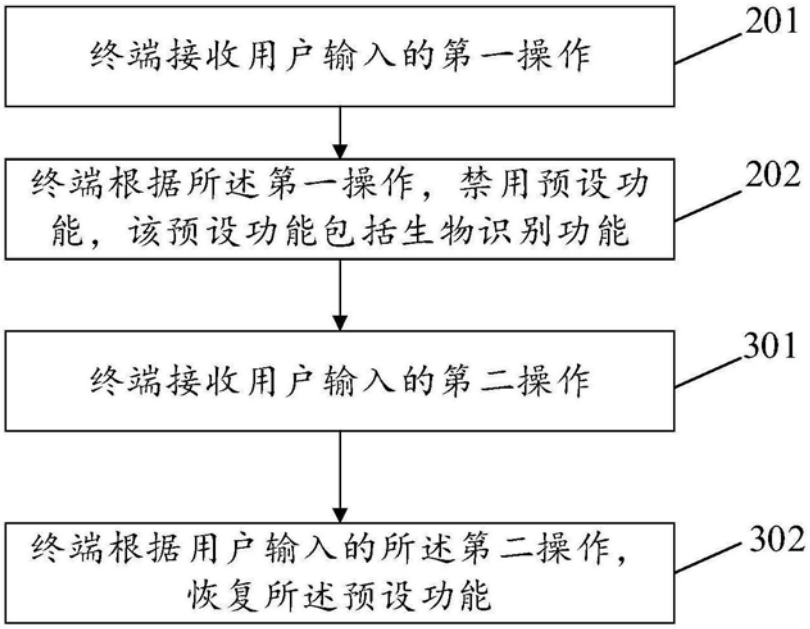

终端接收用户输入的第一操作
201
终端根据所述第一操作，禁用预设功能，该预设功能包括生物识别功能
202
终端接收用户输入的第二操作
301
终端根据用户输入的所述第二操作，恢复所述预设功能
302

图3

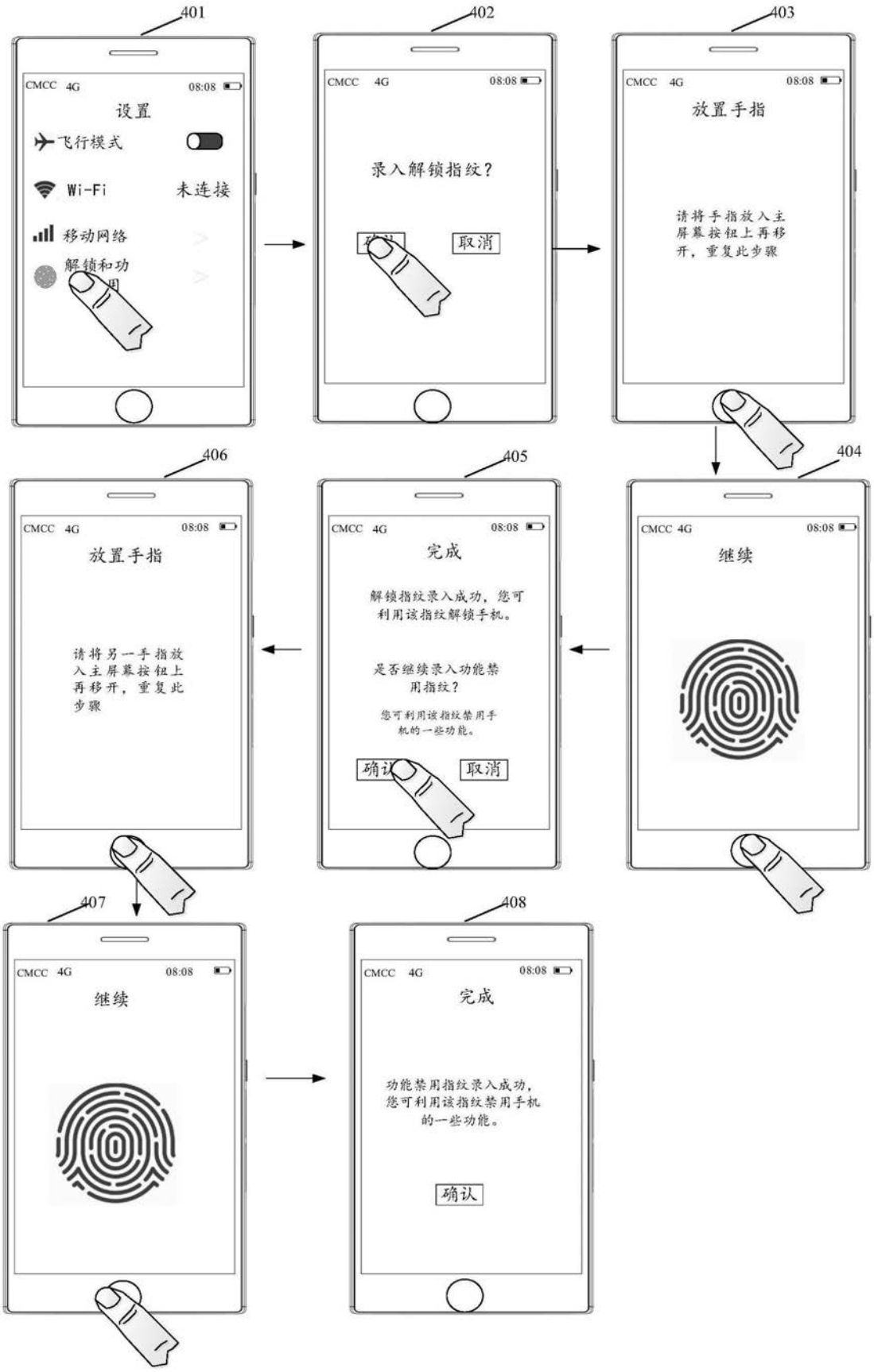

401
CMCC 4G 08:08
设置
飞行模式
Wi-Fi 未连接
移动网络
解锁和功
402
CMCC 4G 08:08
录入解锁指纹?
取消
403
CMCC 4G 08:08
放置手指
请将手指放入主屏幕按钮上再移开，重复此步骤
404
CMCC 4G 08:08
继续
405
CMCC 4G 08:08
完成
解锁指纹录入成功，您可利用该指纹解锁手机。
是否继续录入功能禁用指纹?
您可利用该指纹禁用手机的一些功能。
取消
406
CMCC 4G 08:08
放置手指
请将另一手指放入主屏幕按钮上再移开，重复此步骤
407
CMCC 4G 08:08
继续
408
CMCC 4G 08:08
完成
功能禁用指纹录入成功，您可利用该指纹禁用手机的一些功能。
确认

图4a

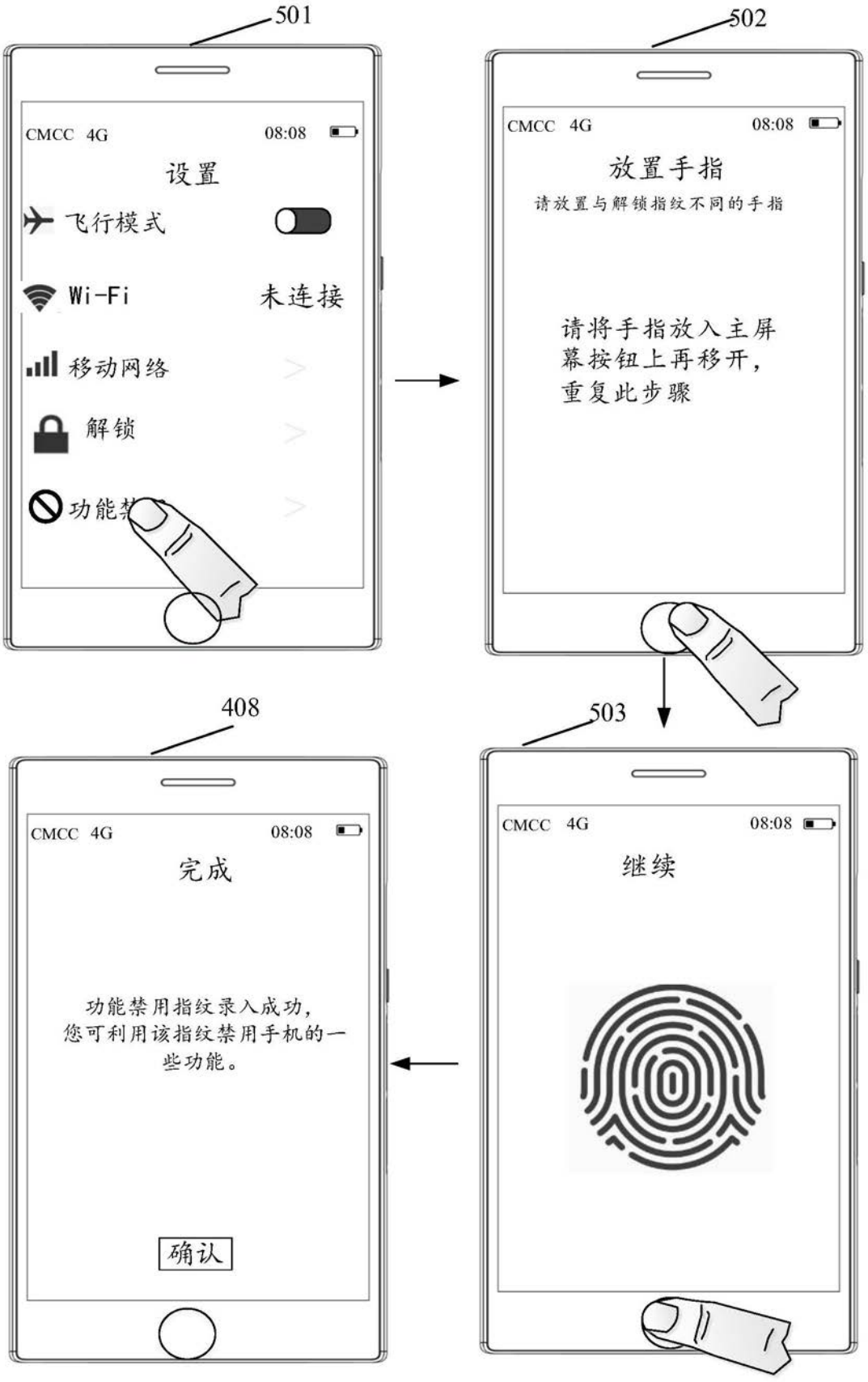

501
CMCC 4G
08:08
设置
飞行模式
Wi-Fi
未连接
移动网络
解锁
502
CMCC 4G
08:08
放置手指
请放置与解锁指纹不同的手指
请将手指放入主屏幕按钮上再移开，重复此步骤
503
CMCC 4G
08:08
继续
408
CMCC 4G
08:08
完成
功能禁用指纹录入成功，您可利用该指纹禁用手机的一些功能。
确认

图4b

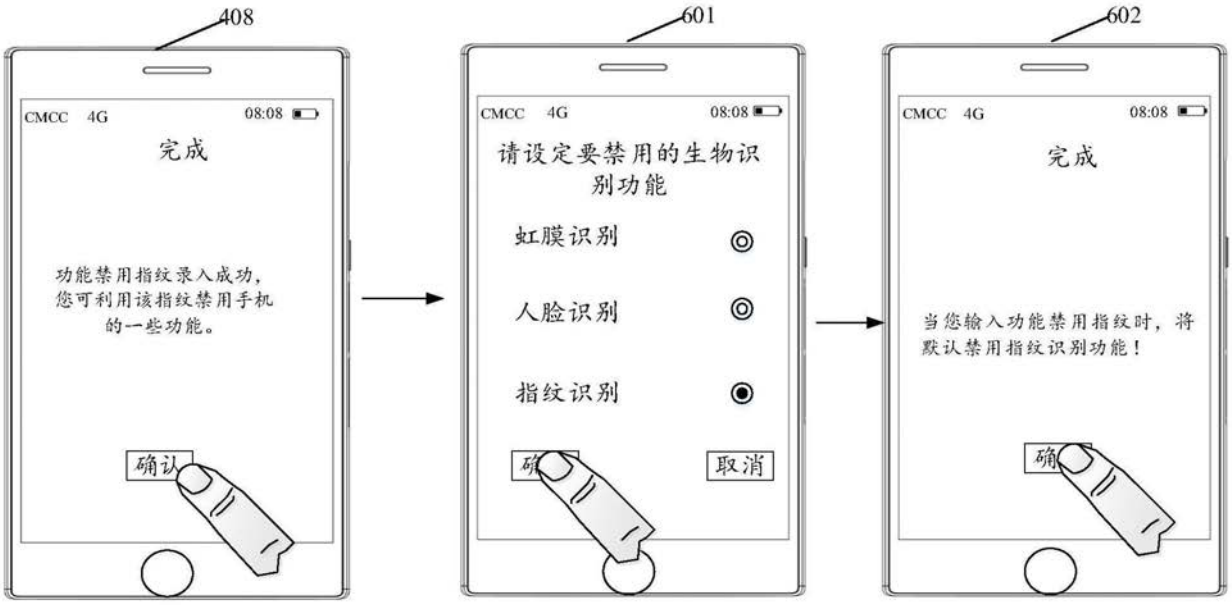

408
CMCC 4G
08:08
完成
功能禁用指纹录入成功，
您可利用该指纹禁用手机
的一些功能。
确认
601
CMCC 4G
08:08
请设定要禁用的生物识
别功能
虹膜识别
人脸识别
指纹识别
确
取消
602
CMCC 4G
08:08
完成
当您输入功能禁用指纹时，将
默认禁用指纹识别功能！
确

图4c

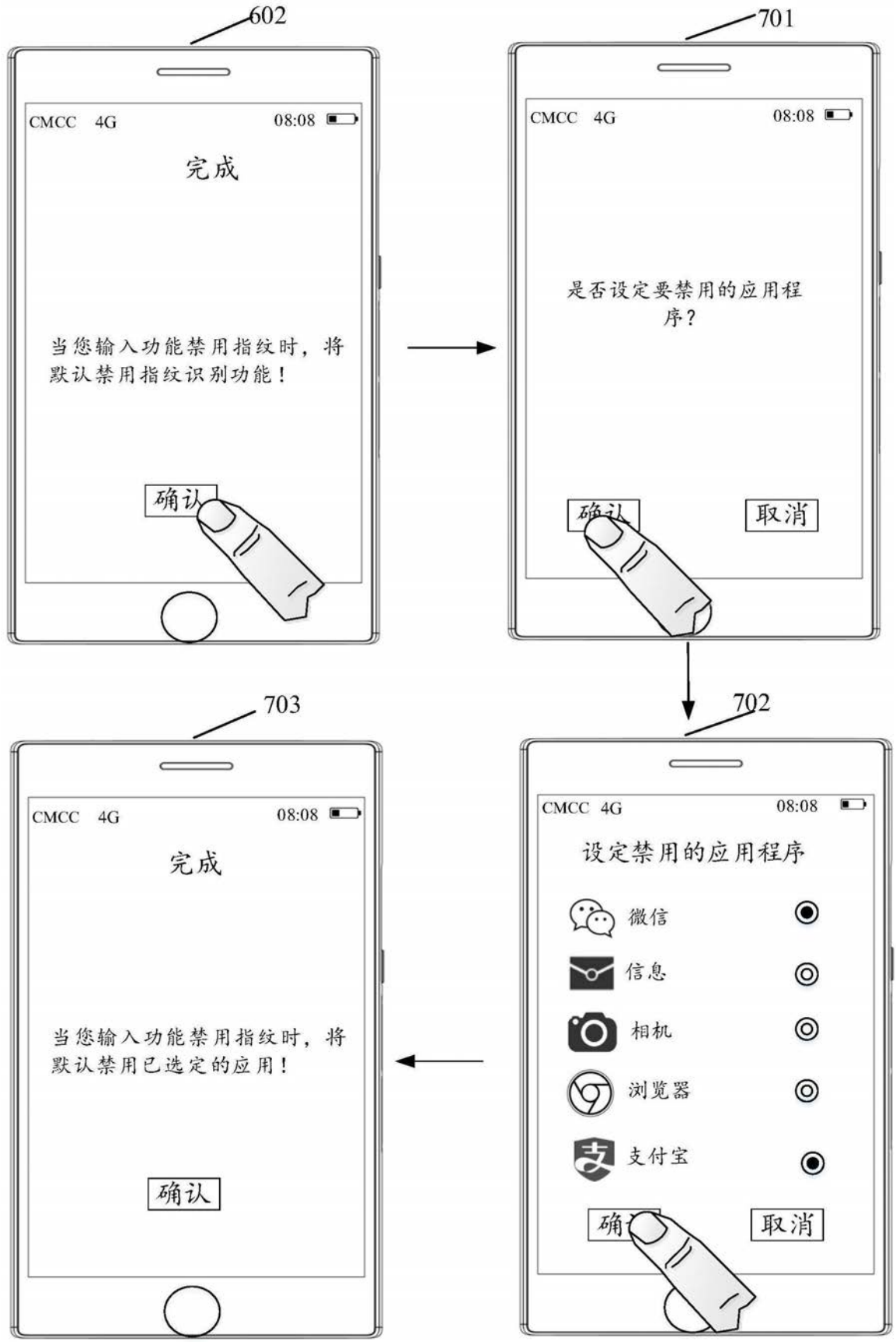

602
CMCC 4G 08:08
完成
当您输入功能禁用指纹时，将默认禁用指纹识别功能！
确认
701
CMCC 4G 08:08
是否设定要禁用的应用程序？
确认
取消
702
CMCC 4G 08:08
设定禁用的应用程序
微信
信息
相机
浏览器
支付宝
确认
取消
703
CMCC 4G 08:08
完成
当您输入功能禁用指纹时，将默认禁用已选定的应用！
确认

图4d

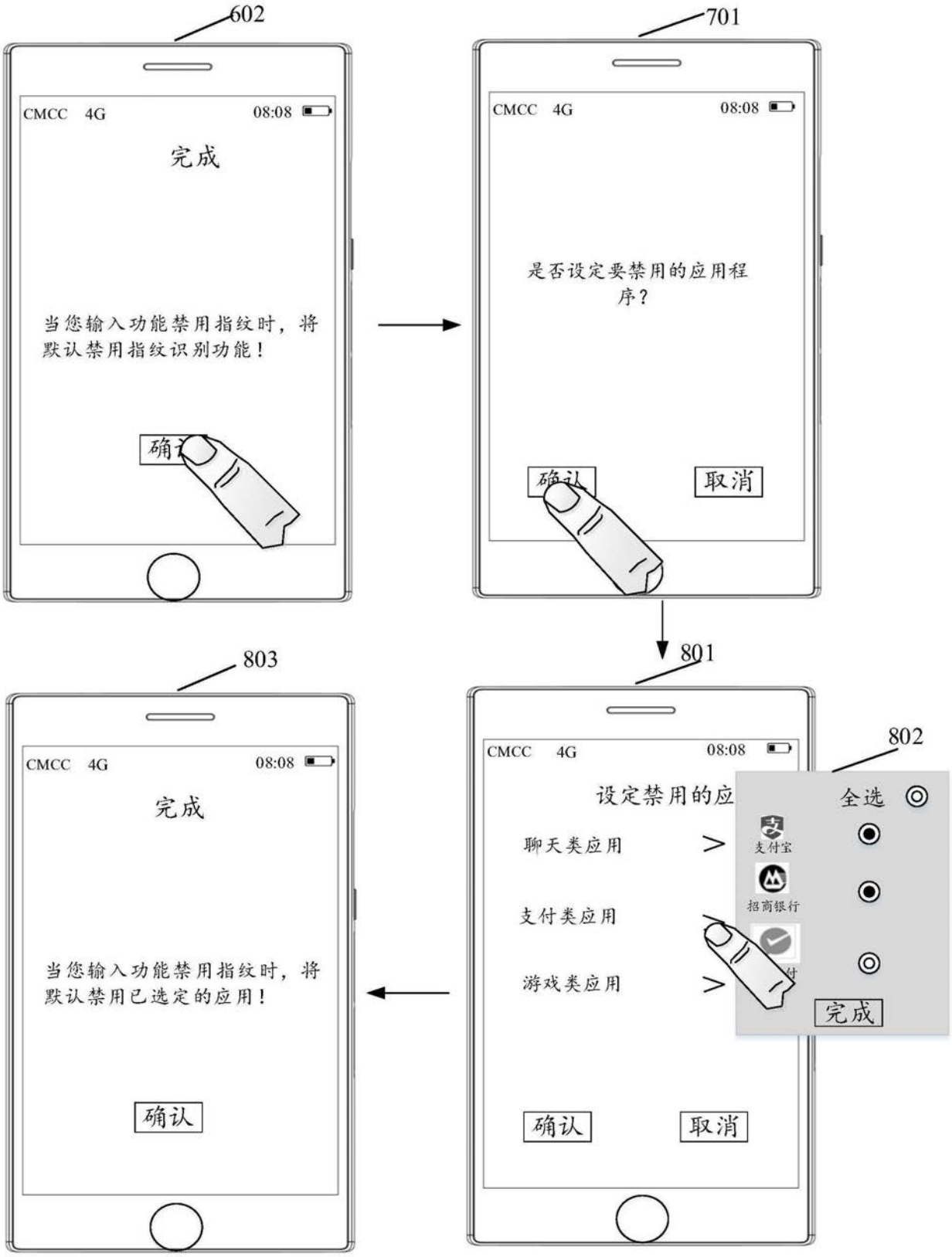

602
CMCC 4G 08:08
完成
当您输入功能禁用指纹时，将默认禁用指纹识别功能！
701
CMCC 4G 08:08
是否设定要禁用的应用程序？
确认
取消
801
CMCC 4G 08:08
设定禁用的应
全选
聊天类应用
支付宝
支付类应用
招商银行
游戏类应用
802
完成
确认
取消
803
CMCC 4G 08:08
完成
当您输入功能禁用指纹时，将默认禁用已选定的应用！
确认

图4e

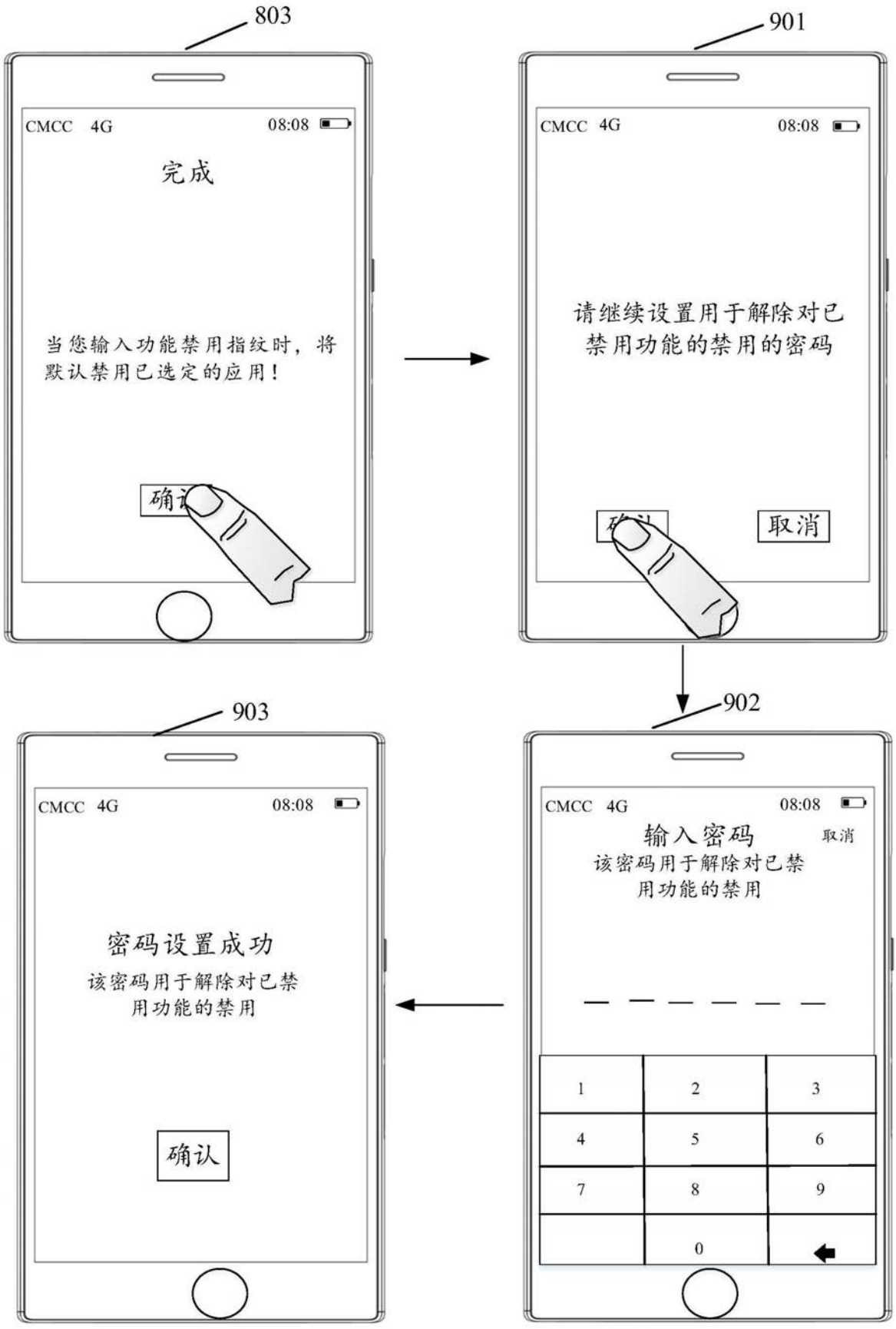

803
CMCC 4G
08:08
完成
当您输入功能禁用指纹时，将默认禁用已选定的应用！
确认
901
CMCC 4G
08:08
请继续设置用于解除对已禁用功能的禁用的密码
确认
取消
902
CMCC 4G
08:08
输入密码
取消
该密码用于解除对已禁用功能的禁用
1 2 3
4 5 6
7 8 9
0
903
CMCC 4G
08:08
密码设置成功
该密码用于解除对已禁用功能的禁用
确认

图4f

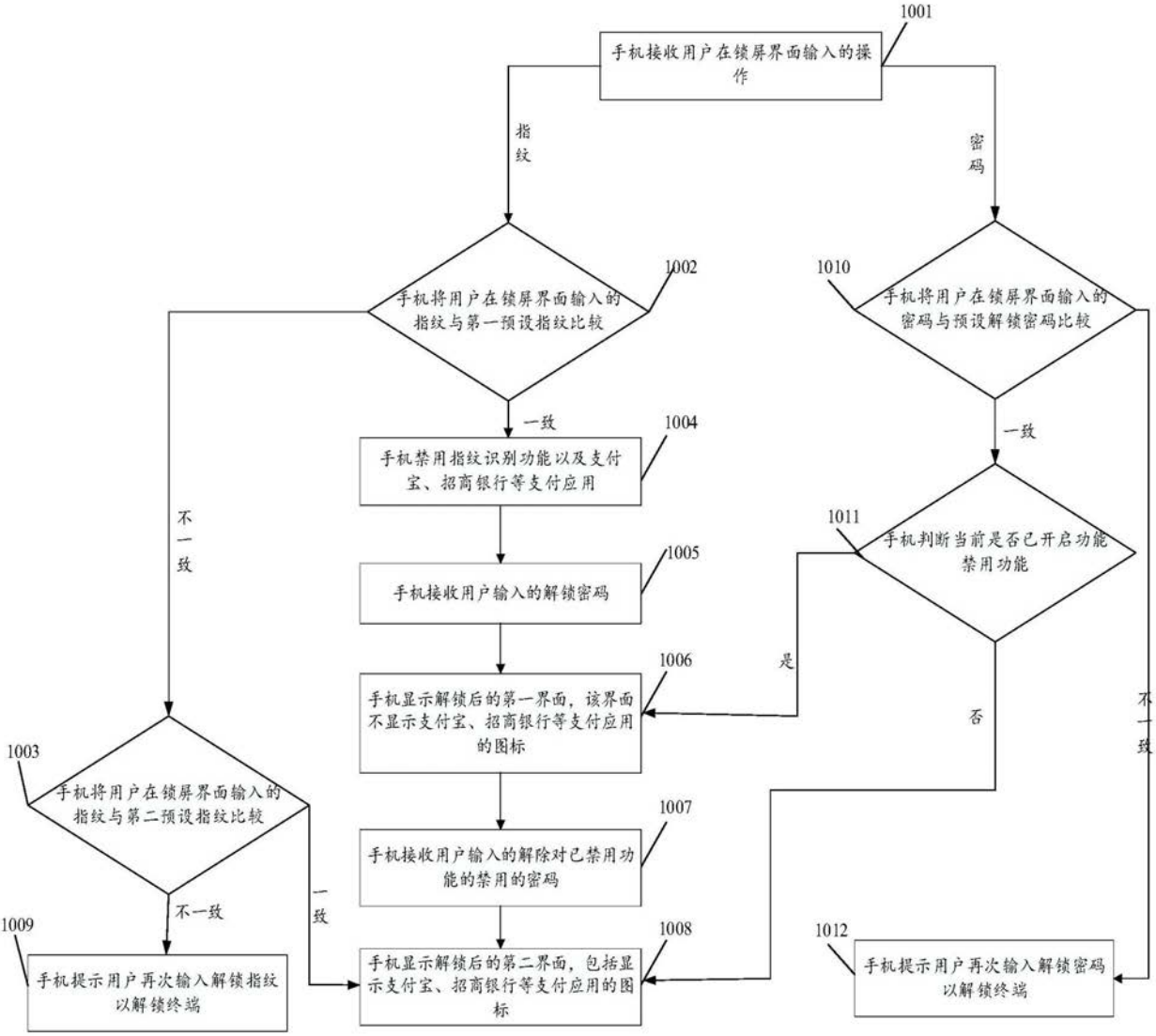

1001
手机接收用户在锁屏界面输入的操作
指纹
密码
1002
手机将用户在锁屏界面输入的指纹与第一预设指纹比较
1010
手机将用户在锁屏界面输入的密码与预设解锁密码比较
一致
1004
手机禁用指纹识别功能以及支付宝、招商银行等支付应用
一致
1011
手机判断当前是否已开启功能禁用功能
不一致
1005
手机接收用户输入的解锁密码
是
否
1006
手机显示解锁后的第一界面，该界面不显示支付宝、招商银行等支付应用的图标
不一致
1003
手机将用户在锁屏界面输入的指纹与第二预设指纹比较
1007
手机接收用户输入的解除对已禁用功能的禁用的密码
不一致
一致
1009
手机提示用户再次输入解锁指纹以解锁终端
1008
手机显示解锁后的第二界面，包括显示支付宝、招商银行等支付应用的图标
1012
手机提示用户再次输入解锁密码以解锁终端

图5

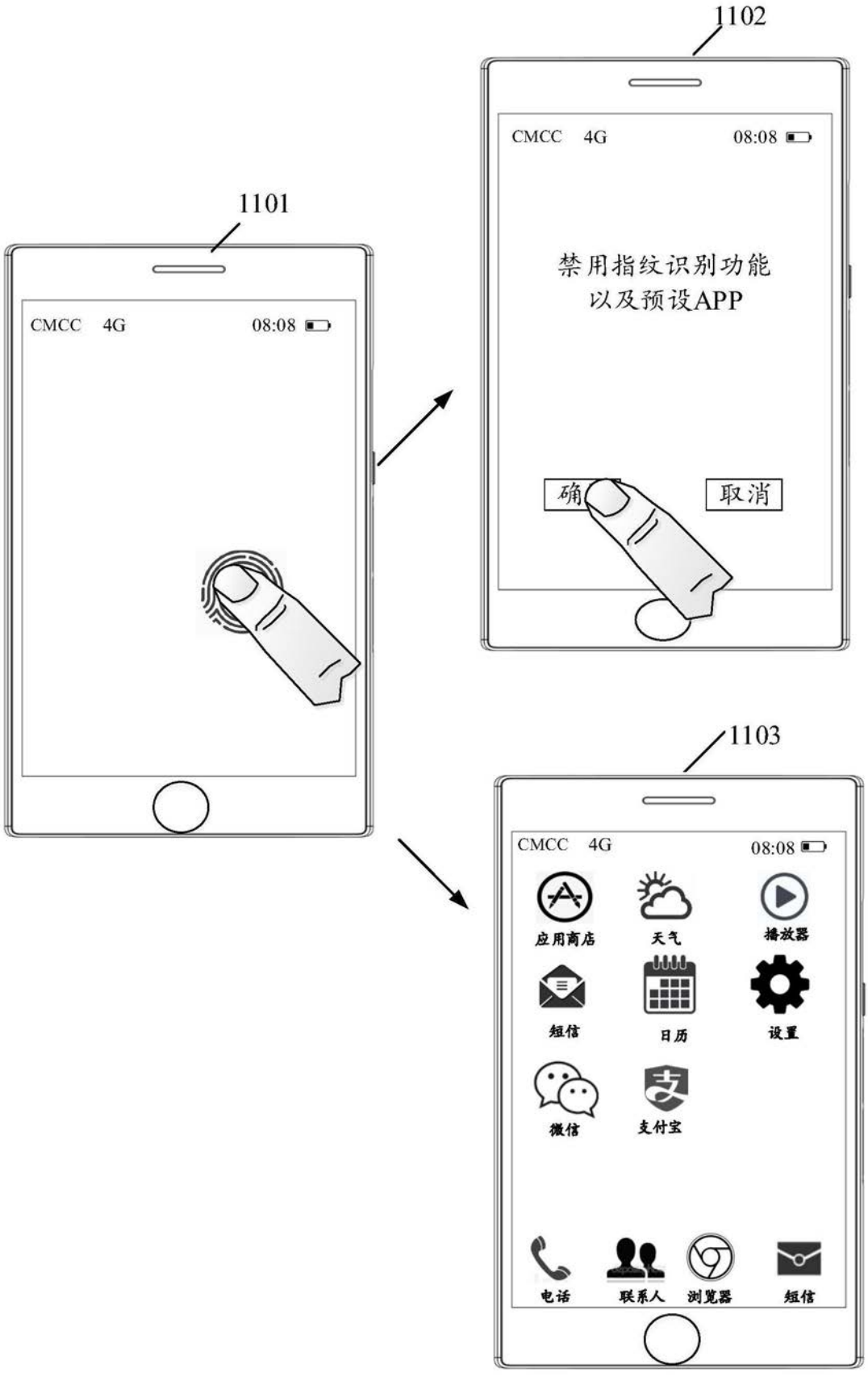

1101
CMCC 4G 08:08
1102
CMCC 4G 08:08
禁用指纹识别功能
以及预设APP
确
取消
1103
CMCC 4G 08:08
应用商店
天气
播放器
短信
日历
设置
微信
支付宝
电话
联系人
浏览器
短信

图5a

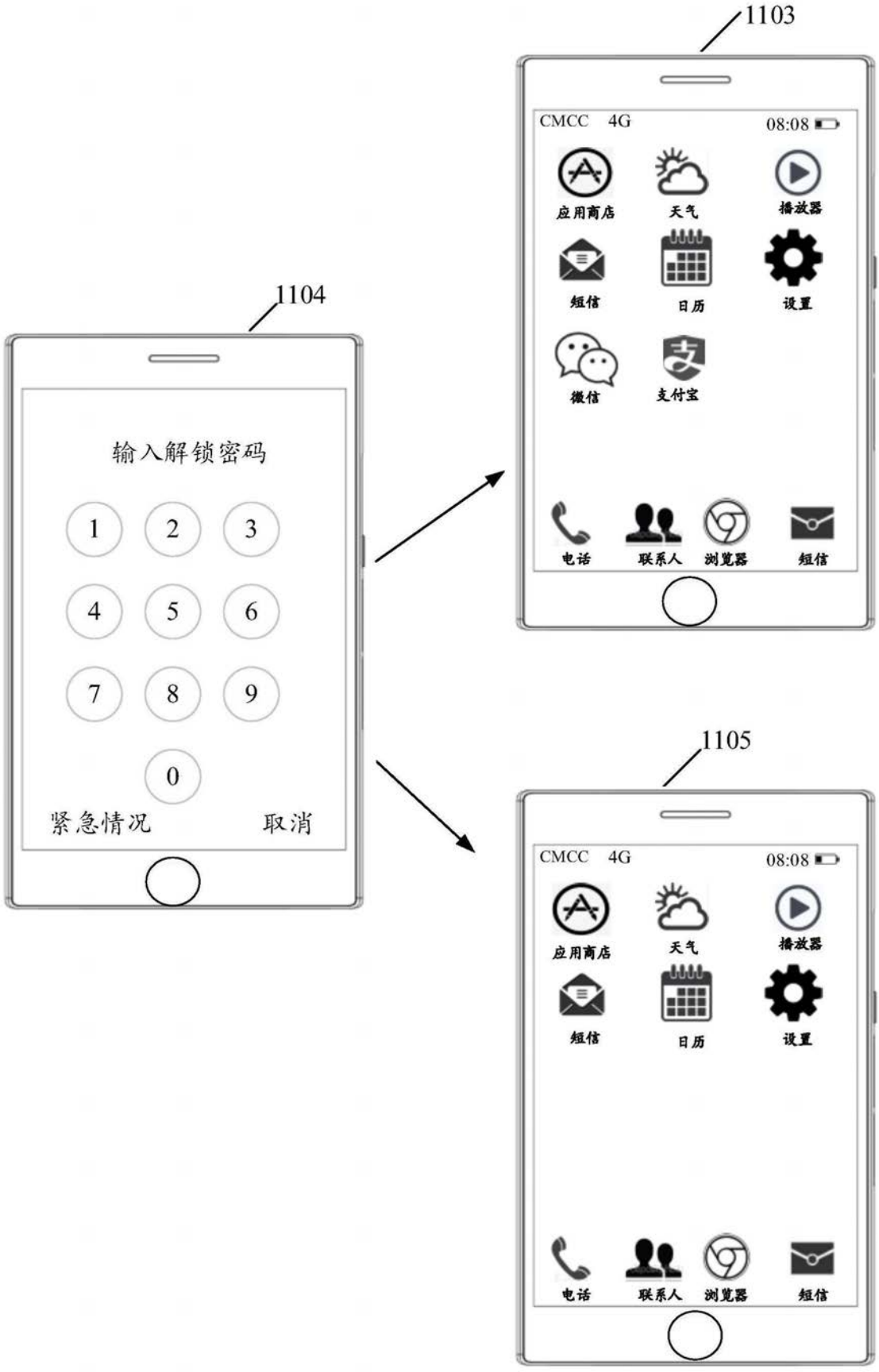

1103
CMCC 4G
08:08
应用商店
天气
播放器
短信
日历
设置
微信
支付宝
电话
联系人
浏览器
短信
1104
输入解锁密码
1 2 3
4 5 6
7 8 9
0
紧急情况
取消
1105
CMCC 4G
08:08
应用商店
天气
播放器
短信
日历
设置
电话
联系人
浏览器
短信

图5b

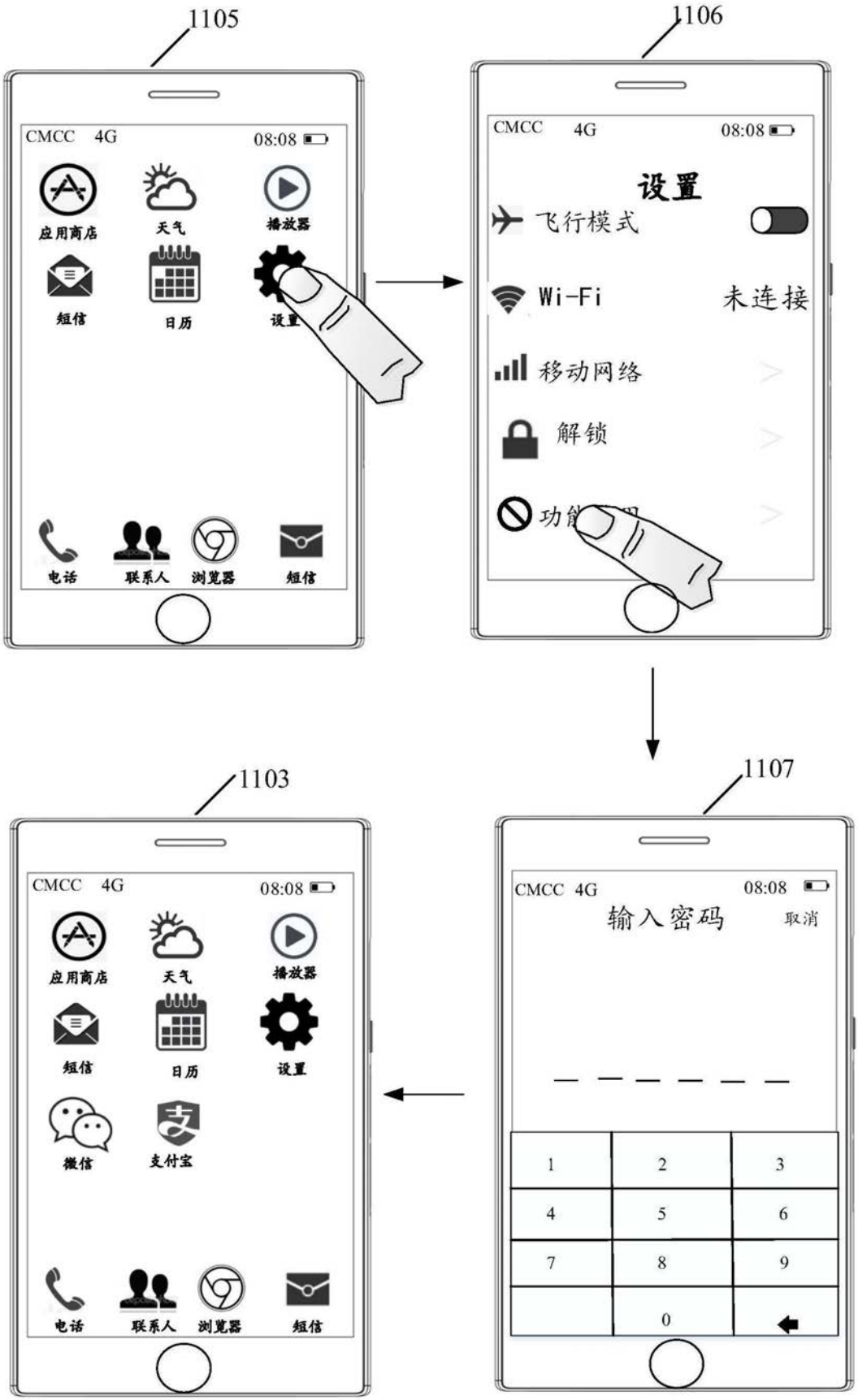

1105
CMCC 4G 08:08
应用商店
天气
播放器
短信
日历
设置
电话
联系人
浏览器
短信
1106
CMCC 4G 08:08
设置
飞行模式
Wi-Fi
未连接
移动网络
解锁
1107
CMCC 4G 08:08
输入密码
取消
1 2 3
4 5 6
7 8 9
0
1103
CMCC 4G 08:08
应用商店
天气
播放器
短信
日历
设置
微信
支付宝
电话
联系人
浏览器
短信

图5c

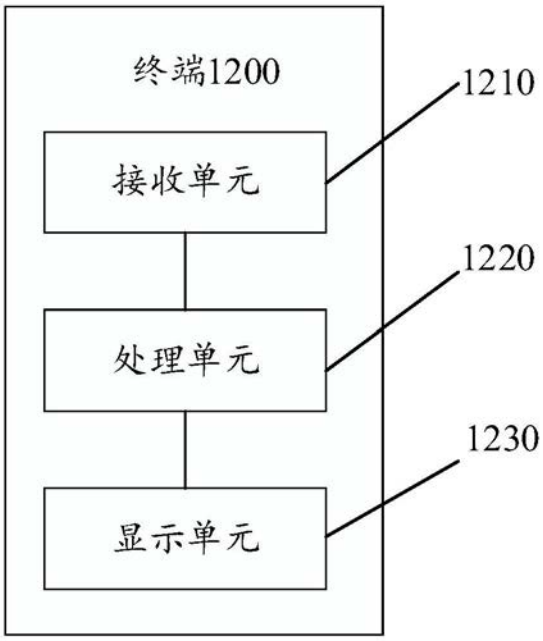

终端1200
1210
接收单元
1220
处理单元
1230
显示单元

图6

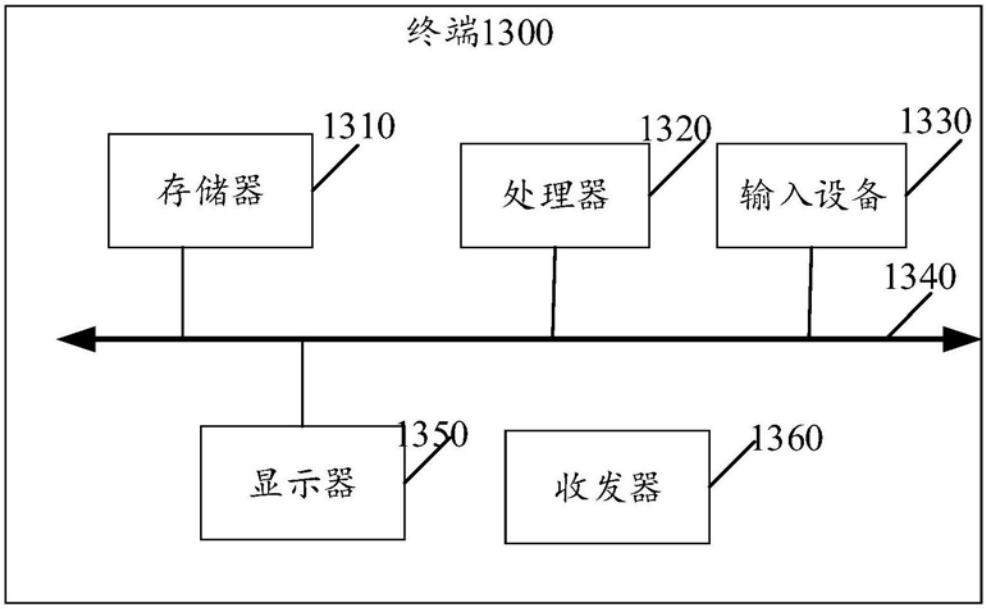

终端1300
1310
存储器
1320
处理器
1330
输入设备
1340
1350
显示器
1360
收发器

图6a