



(12) 发明专利

(10) 授权公告号 CN 109324863 B

(45) 授权公告日 2022. 05. 03

(21) 申请号 201811240802.4

G06F 3/0484 (2022.01)

(22) 申请日 2018.10.23

G06V 40/12 (2022.01)

(65) 同一申请的已公布的文献号
申请公布号 CN 109324863 A

(56) 对比文件

CN 106716431 A, 2017.05.24

CN 106845199 A, 2017.06.13

(43) 申请公布日 2019.02.12

US 2017213019 A1, 2017.07.27

(73) 专利权人 北京小米移动软件有限公司
地址 100085 北京市海淀区清河中街68号
华润五彩城购物中心二期9层01房间

审查员 张楚湖

(72) 发明人 黄学斌

(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 胡业勤

(51) Int. Cl.

G06F 9/451 (2018.01)

G06F 3/0481 (2022.01)

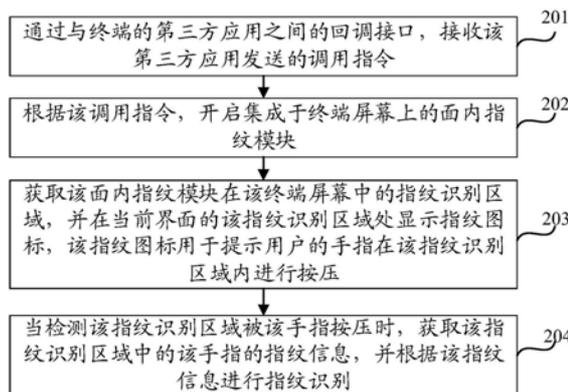
权利要求书2页 说明书14页 附图3页

(54) 发明名称

指纹识别的方法、装置及计算机可读存储介质

(57) 摘要

本公开是关于一种指纹识别的方法、装置及计算机可读存储介质,涉及终端技术领域。该方法包括:通过与终端的第三方应用之间的回调接口接收第三方应用发送的调用指令,并根据该调用指令开启面内指纹模块。由于获取了指纹识别区域,并在当前界面的该指纹识别区域处显示指纹图标,也即该指纹图标可以准确地向用户提示指纹识别区域的位置,因此,当检测该指纹识别区域被手指按压时,可以获取该指纹识别区域中的手指的指纹信息,并根据该指纹信息进行指纹识别。如此,即使第三方应用没有对面内指纹模块做兼容,用户也可以通过在真实的指纹识别区域处显示的指纹图标直观辨认出终端屏幕中的指纹识别区域,进而实现指纹识别。



1. 一种指纹识别的方法,其特征在于,所述方法应用于锁屏程序中,所述方法包括:

通过与终端的第三方应用之间的第一回调接口,接收所述第三方应用发送的调用指令,所述第一回调接口设置在所述锁屏程序中,所述第一回调接口为所述锁屏程序与所述第三方应用之间的接口;

根据所述调用指令,通过第二回调接口控制开启集成于终端屏幕上的面内指纹模块,所述第二回调接口设置在所述锁屏程序中,所述第二回调接口为所述锁屏程序与所述面内指纹模块之间的接口;

获取所述面内指纹模块在所述终端屏幕中的指纹识别区域;

在当前界面上叠加一层锁屏界面,所述锁屏界面经过透明化处理;

在所述锁屏界面的所述指纹识别区域处显示指纹图标,所述指纹图标用于提示用户的手指在所述指纹识别区域内进行按压;

当检测所述指纹识别区域被所述手指按压时,获取所述指纹识别区域中的所述手指的指纹信息,并根据所述指纹信息进行指纹识别。

2. 如权利要求1所述的方法,其特征在于,所述在当前界面的所述指纹识别区域处显示指纹图标之前,所述方法还包括:

当接收到所述面内指纹模块发送的特定信息时,确定已成功开启所述面内指纹模块,执行所述在当前界面的所述指纹识别区域处显示指纹图标的步骤,所述特定信息用于指示成功开启所述面内指纹模块。

3. 如权利要求1所述的方法,其特征在于,所述获取所述面内指纹模块在所述终端屏幕中的指纹识别区域之前,所述方法还包括:

确定所述调用指令是否用于解锁所述终端屏幕;

当所述调用指令不是用于解锁所述终端屏幕时,执行所述获取所述面内指纹模块在所述终端屏幕中的指纹识别区域的步骤。

4. 如权利要求1所述的方法,其特征在于,透明处理后的锁屏界面用于透过所述锁屏界面显示所述第三方应用的提示信息。

5. 如权利要求1所述的方法,其特征在于,所述方法还包括:

对所述指纹识别区域进行检测;

当检测到所述指纹识别区域被按压的按压事件时,获取所述按压事件的事件类型和压力值;

当所述事件类型为指定类型,且所述压力值超过预设阈值时,确定所述指纹识别区域被手指按压。

6. 如权利要求1或5所述的方法,其特征在于,所述获取所述指纹识别区域中的所述手指的指纹信息,包括:

将所述终端屏幕的背光设置为高亮模式;

在所述高亮模式下,采集所述手指的图像,并将所述手指的图像作为所述手指的指纹信息。

7. 一种指纹识别的装置,其特征在于,所述装置包括:

接收模块,用于通过与终端的第三方应用之间的第一回调接口,接收所述第三方应用发送的调用指令,所述第一回调接口设置在锁屏程序中,所述第一回调接口为所述锁屏程

序与所述第三方应用之间的接口；

开启模块,用于根据所述调用指令,通过第二回调接口控制开启集成于终端屏幕上的面内指纹模块,所述第二回调接口设置在所述锁屏程序中,所述第二回调接口为所述锁屏程序与所述面内指纹模块之间的接口；

显示模块,用于获取所述面内指纹模块在所述终端屏幕中的指纹识别区域；

叠加子模块,用于在当前界面上叠加一层锁屏界面,所述锁屏界面经过透明化处理；

显示子模块,用于在所述锁屏界面的所述指纹识别区域处显示指纹图标,所述指纹图标用于提示用户的手指在所述指纹识别区域内进行按压；

识别模块,用于当检测所述指纹识别区域被所述手指按压时,获取所述指纹识别区域中的所述手指的指纹信息,并根据所述指纹信息进行指纹识别。

8.如权利要求7所述的装置,其特征在于,所述装置还包括:

第一确定模块,用于当接收到所述面内指纹模块发送的特定信息时,确定已成功开启所述面内指纹模块,触发所述显示模块在所述当前界面的所述指纹识别区域处显示指纹图标,所述特定信息用于指示成功开启所述面内指纹模块。

9.如权利要求7所述的装置,其特征在于,所述装置还包括:

第二确定模块,用于确定所述调用指令是否用于解锁所述终端屏幕；

触发模块,用于当所述调用指令不是用于解锁所述终端屏幕时,触发所述显示模块获取所述面内指纹模块在所述终端屏幕中的指纹识别区域。

10.如权利要求7所述的装置,其特征在于,透明处理后的锁屏界面用于透过所述锁屏界面显示所述第三方应用的提示信息。

11.如权利要求7所述的装置,其特征在于,所述装置 还包括:

检测模块,用于对所述指纹识别区域进行检测；

获取模块,用于当检测到所述指纹识别区域被按压的按压事件时,获取所述按压事件的事件类型和压力值；

第三确定模块,用于当所述事件类型为指定类型,且所述压力值超过预设阈值时,确定所述指纹识别区域被手指按压。

12.如权利要求7或11所述的装置,其特征在于,所述识别模块包括:

高亮子模块,用于将所述终端屏幕的背光设置为高亮模式；

采集模块,用于在所述高亮模式下,采集所述手指的图像,并将所述手指的图像作为所述手指的指纹信息。

13.一种指纹识别的装置,其特征在于,所述装置包括:

处理器；

用于存储处理器可执行指令的存储器；

其中,所述处理器被配置为执行权利要求1-6所述的任一项方法的步骤。

14.一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指令,其特征在于,所述指令被处理器执行时实现权利要求1-6所述的任一项方法的步骤。

指纹识别的方法、装置及计算机可读存储介质

技术领域

[0001] 本公开涉及终端技术领域,尤其涉及一种指纹识别的方法、装置及计算机可读存储介质。

背景技术

[0002] 面内指纹模块的出现进一步增加了终端的屏占比,面内指纹模块是指设置于终端中,且为用户提供在终端屏幕中进行指纹识别的模块。终端中的面内指纹模块可以通过显示在屏幕中的指纹图标来获取用户的指纹信息进而实现指纹识别功能。目前,不仅终端的锁屏程序需要调用面内指纹模块进行指纹识别,终端的第三方应用也需要调用面内指纹模块进行指纹识别,从而对用户进行身份验证。

[0003] 由于面内指纹模块设置在终端屏幕中,用户无法直观辨认出终端屏幕的哪个区域是面内指纹模块的指纹识别区域。因此,第三方应用在调用面内指纹模块时,通常会在当前界面上显示一个指纹图标,提示用户在该指纹图标上按压。然而由于第三方应用没有对面内指纹模块做兼容,也即第三方应用无法获取该指纹识别区域。因此,第三方应用通常是在当前界面中任一位置处显示指纹图标,例如在当前界面的中间位置处显示一个指纹图标,进而通过该指纹图标实现指纹识别功能。

发明内容

[0004] 为克服相关技术中存在的问题,本公开提供一种指纹识别的方法、装置及计算机可读存储介质。

[0005] 第一方面,提供一种指纹识别的方法,所述方法包括:

[0006] 通过与终端的第三方应用之间的回调接口,接收所述第三方应用发送的调用指令;

[0007] 根据所述调用指令,开启集成于终端屏幕上的面内指纹模块;

[0008] 获取所述面内指纹模块在所述终端屏幕中的指纹识别区域,并在当前界面的所述指纹识别区域处显示指纹图标,所述指纹图标用于提示用户的手指在所述指纹识别区域内进行按压;

[0009] 当检测所述指纹识别区域被所述手指按压时,获取所述指纹识别区域中的所述手指的指纹信息,并根据所述指纹信息进行指纹识别。

[0010] 在本公开实施例中,通过与终端的第三方应用之间的回调接口接收第三方应用发送的调用指令,然后根据该调用指令开启集成于终端屏幕上的面内指纹模块。由于获取了面内指纹模块在终端屏幕中的指纹识别区域,并在当前界面的该指纹识别区域处显示指纹图标,也即该指纹图标可以准确地向用户提示指纹识别区域的位置,因此,用户的手指可以在该指纹识别区域内进行按压。进而当检测该指纹识别区域被手指按压时,获取该指纹识别区域中的手指的指纹信息,并根据该指纹信息进行指纹识别。也即是,通过与终端的第三方应用之间的回调接口开启面内指纹模块,并在真实的指纹识别区域处显示指纹图标。如

此,即使第三方应用没有对面内指纹模块做兼容,用户通过该在真实的指纹识别区域处显示的指纹图标也可以直观辨认出终端屏幕中面内指纹模块的指纹识别区域,进而实现指纹识别。

[0011] 可选地,所述在当前界面的所述指纹识别区域处显示指纹图标之前,所述方法还包括:

[0012] 当接收到所述面内指纹模块发送的特定信息时,确定已成功开启所述面内指纹模块,执行所述在当前界面的所述指纹识别区域处显示指纹图标的步骤,所述特定信息用于指示成功开启所述面内指纹模块。

[0013] 在本公开实施例中,由于根据调用指令开启集成于终端屏幕上的面内指纹模块可能成功也可能失败,因此,通过特定信息即可确定已成功开启了面内指纹模块,进而执行后续在指纹识别区域处显示指纹图标的步骤。

[0014] 可选地,所述获取所述面内指纹模块在所述终端屏幕中的指纹识别区域之前,所述方法还包括:

[0015] 确定所述调用指令是否用于解锁所述终端屏幕;

[0016] 当所述调用指令不是用于解锁所述终端屏幕时,执行所述获取所述面内指纹模块在所述终端屏幕中的指纹识别区域的步骤。

[0017] 在本公开实施例中,由于解锁终端屏幕的功能一般是终端自带的系统功能,也即解锁终端屏幕时通常可以准确获取指纹识别区域。因此,在获取指纹识别区域之前,先确定该调用指令是否用于解锁终端屏幕,当不是时,说明该调用指令是在第三方应用中进行指纹识别时所需的指令,进而执行后续获取指纹识别区域的步骤。如此,通过确定调用指令是否用于解锁终端屏幕来进行指纹识别,提高了指纹识别的效率。

[0018] 可选地,所述在当前界面的所述指纹识别区域处显示指纹图标,包括:

[0019] 在所述当前界面上叠加一层锁屏界面;

[0020] 在所述锁屏界面的所述指纹识别区域处显示所述指纹图标。

[0021] 可选地,所述在所述锁屏界面的所述指纹识别区域处显示所述指纹图标之前,所述方法还包括:

[0022] 对所述锁屏界面进行透明处理,透明处理后的锁屏界面用于透过所述锁屏界面显示所述第三方应用的提示信息。

[0023] 在本公开实施例中,将在当前界面上叠加的一层锁屏界面进行透明处理,也即除了该锁屏界面的指纹识别区域处显示的指纹图标之外的区域均为透明区域,如此,不仅可以通过指纹图标准确提示用户的手指在指纹识别区域内进行按压,还不影响用户观看第三方应用的提示信息。

[0024] 可选地,所述方法还包括:

[0025] 对所述指纹识别区域进行检测;

[0026] 当检测到所述指纹识别区域被按压的按压事件时,获取所述按压事件的事件类型和压力值;

[0027] 当所述事件类型为指定类型,且所述压力值超过预设阈值时,确定所述指纹识别区域被手指按压。

[0028] 在本公开实施例中,通过检测并判断指纹识别区域被按压的按压事件的事件类型

和压力值,可以确定指纹识别区域是否被手指按压,降低了指纹识别区域被误触的概率。

[0029] 可选地,所述获取所述指纹识别区域中的所述手指的指纹信息,包括:

[0030] 将所述终端屏幕的背光设置为高亮模式;

[0031] 在所述高亮模式下,采集所述手指的图像,并将所述手指的图像作为所述手指的指纹信息。

[0032] 在本公开实施例中,通过在高亮模式下采集手指的图像,提高了手指图像采集的准确率,进而提高了通过指纹信息进行指纹识别的准确率。

[0033] 第二方面,提供一种指纹识别的装置,所述装置包括:

[0034] 接收模块,用于通过与终端的第三方应用之间的回调接口,接收所述第三方应用发送的调用指令;

[0035] 开启模块,用于根据所述调用指令,开启集成于终端屏幕上的面内指纹模块;

[0036] 显示模块,用于获取所述面内指纹模块在所述终端屏幕中的指纹识别区域,并在当前界面的所述指纹识别区域处显示指纹图标,所述指纹图标用于提示用户的手指在所述指纹识别区域内进行按压;

[0037] 识别模块,用于当检测所述指纹识别区域被所述手指按压时,获取所述指纹识别区域中的所述手指的指纹信息,并根据所述指纹信息进行指纹识别。

[0038] 在本公开实施例中,通过与终端的第三方应用之间的回调接口接收第三方应用发送的调用指令,然后根据该调用指令开启集成于终端屏幕上的面内指纹模块。由于获取了面内指纹模块在终端屏幕中的指纹识别区域,并在当前界面的该指纹识别区域处显示指纹图标,也即该指纹图标可以准确地向用户提示指纹识别区域的位置,因此,用户的手指可以在该指纹识别区域内进行按压。进而当检测该指纹识别区域被手指按压时,获取该指纹识别区域中的手指的指纹信息,并根据该指纹信息进行指纹识别。也即是,通过与终端的第三方应用之间的回调接口开启面内指纹模块,并在真实的指纹识别区域处显示指纹图标。如此,即使第三方应用没有对面内指纹模块做兼容,用户通过该在真实的指纹识别区域处显示的指纹图标也可以直观辨认出终端屏幕中面内指纹模块的指纹识别区域,进而实现指纹识别。

[0039] 可选地,所述装置还包括:

[0040] 第一确定模块,用于当接收到所述面内指纹模块发送的特定信息时,确定已成功开启所述面内指纹模块,触发所述显示模块在所述当前界面的所述指纹识别区域处显示指纹图标,所述特定信息用于指示成功开启所述面内指纹模块。

[0041] 可选地,所述装置还包括:

[0042] 第二确定模块,用于确定所述调用指令是否用于解锁所述终端屏幕;

[0043] 触发模块,用于当所述调用指令不是用于解锁所述终端屏幕时,触发所述显示模块获取所述面内指纹模块在所述终端屏幕中的指纹识别区域。

[0044] 可选地,所述显示模块包括:

[0045] 叠加子模块,用于在所述当前界面上叠加一层锁屏界面;

[0046] 显示子模块,用于在所述锁屏界面的所述指纹识别区域处显示所述指纹图标。

[0047] 可选地,所述显示模块还包括:

[0048] 处理子模块,用于对所述锁屏界面进行透明处理,透明处理后的锁屏界面用于透

过所述锁屏界面显示所述第三方应用的提示信息。

[0049] 可选地,所述方法还包括:

[0050] 检测模块,用于对所述指纹识别区域进行检测;

[0051] 获取模块,用于当检测到所述指纹识别区域被按压的按压事件时,获取所述按压事件的事件类型和压力值;

[0052] 第三确定模块,用于当所述事件类型为指定类型,且所述压力值超过预设阈值时,确定所述指纹识别区域被手指按压。

[0053] 可选地,所述识别模块包括:

[0054] 高亮子模块,用于将所述终端屏幕的背光设置为高亮模式;

[0055] 采集模块,用于在所述高亮模式下,采集所述手指的图像,并将所述手指的图像作为所述手指的指纹信息。

[0056] 第三方面,提供一种指纹识别的装置,所述装置包括:

[0057] 处理器;

[0058] 用于存储处理器可执行指令的存储器;

[0059] 其中,所述处理器被配置为执行上述第一方面所述的任一项方法的步骤。

[0060] 第四方面,提供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指令,其特征在于,所述指令被处理器执行时实现上述第一方面所述的任一项方法的步骤

[0061] 第五方面,提供了一种包含指令的计算机程序产品,当其在计算机上运行时,使得计算机执行上述第一方面任一项所述方法的步骤。

[0062] 应当理解的是,以上的一般描述和后文的细节描述仅是示例性和解释性的,并不能限制本公开。

附图说明

[0063] 此处的附图被并入说明书中并构成本说明书的一部分,示出了符合本发明的实施例,并与说明书一起用于解释本发明的原理。

[0064] 图1是本公开实施例中提供的指纹识别方法所涉及的实施环境的示意图。

[0065] 图2是根据一示例性实施例示出的一种指纹识别的方法流程图。

[0066] 图3是根据一示例性实施例示出的一种指纹识别的方法流程图。

[0067] 图4是根据一示例性实施例示出的一种指纹识别的装置框图。

[0068] 图5是根据一示例性实施例示出的一种指纹识别的装置框图。

具体实施方式

[0069] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本发明相一致的所有实施方式。相反,它们仅是与本发明的一些方面相一致的装置和方法的例子。

[0070] 首先,在对本公开实施例进行详细的解释说明之前,先对本公开实施例的应用场景进行介绍:

[0071] 终端中传统的指纹模块设置在终端屏幕的下方,或者终端的背面。但设置在终端

屏幕下方的指纹模块会影响终端的屏占比,设置在终端背面的指纹模块需要对终端开凿处理,增加了终端损坏的风险。因此,为了满足用户对终端越来越高的要求,目前出现了面内指纹模块,即设置于终端中且为用户提供在终端屏幕中进行指纹识别的模块,该面内指纹模块不仅增加了终端的屏占比还避免了对终端进行开凿处理,受到了广大用户的欢迎。目前,不仅终端的锁屏程序需要调用面内指纹模块进行指纹识别,终端的第三方应用也需要调用面内指纹模块进行指纹识别,从而对用户进行身份验证。

[0072] 然而,第三方应用并没有对面内指纹模块做兼容,也即第三方应用无法获取该指纹识别区域,因此,第三方应用在调用面内指纹模块时,是在当前界面中任一位置处显示指纹图标,进而实现指纹识别功能。但由于第三方应用无法获取该指纹识别区域,因此,在当前界面显示的指纹图标往往与真实的指纹识别区域不重合,即指纹图标不能准确地反映指纹识别区域的位置,导致指纹识别的效果较差。因此,本公开实施例提供了一种指纹识别的方法,通过该方法第三方应用在当前界面显示的指纹图标可以准确地反映指纹识别区域的位置,进而提高了指纹识别的准确率。

[0073] 其次,对本公开实施例的实施环境进行介绍:

[0074] 请参见图1,其示出了本公开实施例中提供的指纹识别方法所涉及的实施环境的示意图。该实施环境可以包括:终端100。终端100可以为智能手机、电脑或者多媒体播放器等,图1以终端100为智能手机为例进行说明。

[0075] 如图1所示,终端100的屏幕1001中可以安装有面内指纹模块1002。通过该面内指纹模块1002可以完成终端屏幕解锁和指纹支付等功能。该面内指纹模块可以为光学面内指纹模块。

[0076] 其中,终端中可以设置有触摸感应模块和压力传感器。当用户用手指按压指纹识别区域时,触摸感应模块可以将手指的位置信息发送至压力传感器。压力传感器接收该位置信息,对指纹识别区域进行检测,根据手指的位置信息确定该手指是否位于指纹识别区域;当确定该手指位于指纹识别区域时,确定检测到了该指纹识别区域被按压的按压事件,并确定该按压事件的事件类型和压力值,且向锁屏程序上报事件类型和压力值。锁屏程序接收压力传感器上报的事件类型与压力值,并在检测到该事件类型为指定类型且该压力值超过预设阈值时,确定该指纹识别区域被手指按压。其中,指定类型为指纹识别对应的事件类型。然后锁屏程序指示显示模块将终端屏幕的背光设置为高亮模式。在该高亮模式下,锁屏程序可以通过与面内指纹模块之间的回调接口控制面内指纹模块来采集手指的图像,并将该手指的图像作为手指的指纹信息。此时,面内指纹模块可以将该指纹信息发送至终端的算法程序。算法程序在接收到该指纹信息时,可以确定该指纹信息与指纹模板库中的指纹信息之间的匹配度,并将匹配结果发送至锁屏程序,由锁屏程序将该匹配结果转发至第三方应用,从而完成指纹识别。

[0077] 图2是根据一示例性实施例示出的一种指纹识别的方法的流程图,该方法应用于锁屏程序中,如图2所示,包括以下步骤。

[0078] 在步骤201中,通过与终端的第三方应用之间的回调接口,接收该第三方应用发送的调用指令。

[0079] 在步骤202中,根据该调用指令,开启集成于终端屏幕上的面内指纹模块。

[0080] 在步骤203中,获取该面内指纹模块在该终端屏幕中的指纹识别区域,并在当前界

面的该指纹识别区域处显示指纹图标,该指纹图标用于提示用户的手指在该指纹识别区域内进行按压。

[0081] 在步骤204中,当检测该指纹识别区域被该手指按压时,获取该指纹识别区域中的该手指的指纹信息,并根据该指纹信息进行指纹识别。

[0082] 可选地,在当前界面的该指纹识别区域处显示指纹图标之前,该方法还包括:

[0083] 当接收到该面内指纹模块发送的特定信息时,确定已成功开启该面内指纹模块,执行该在当前界面的该指纹识别区域处显示指纹图标的步骤,该特定信息用于指示成功开启该面内指纹模块。

[0084] 可选地,获取该面内指纹模块在该终端屏幕中的指纹识别区域之前,该方法还包括:

[0085] 确定该调用指令是否用于解锁该终端屏幕;

[0086] 当该调用指令不是用于解锁该终端屏幕时,执行该获取该面内指纹模块在该终端屏幕中的指纹识别区域的步骤。

[0087] 可选地,在当前界面的该指纹识别区域处显示指纹图标,包括:

[0088] 在该当前界面上叠加一层锁屏界面;

[0089] 在该锁屏界面的该指纹识别区域处显示该指纹图标。

[0090] 可选地,在该锁屏界面的该指纹识别区域处显示该指纹图标之前,该方法还包括:

[0091] 对该锁屏界面进行透明处理,透明处理后的锁屏界面用于透过该锁屏界面显示该第三方应用的提示信息。

[0092] 可选地,该方法还包括:

[0093] 对该指纹识别区域进行检测;

[0094] 当检测到该指纹识别区域被按压的按压事件时,获取该按压事件的事件类型和压力值;

[0095] 当该事件类型为指定类型,且该压力值超过预设阈值时,确定该指纹识别区域被手指按压。

[0096] 可选地,获取该指纹识别区域中的该手指的指纹信息,包括:

[0097] 将该终端屏幕的背光设置为高亮模式;

[0098] 在该高亮模式下,采集该手指的图像,并将该手指的图像作为该手指的指纹信息。

[0099] 在本公开实施例中,通过与终端的第三方应用之间的回调接口接收第三方应用发送的调用指令,然后根据该调用指令开启集成于终端屏幕上的面内指纹模块。由于获取了面内指纹模块在终端屏幕中的指纹识别区域,并在当前界面的该指纹识别区域处显示指纹图标,也即该指纹图标可以准确地向用户提示指纹识别区域的位置,因此,用户的手指可以在该指纹识别区域内进行按压。进而当检测该指纹识别区域被手指按压时,获取该指纹识别区域中的手指的指纹信息,并根据该指纹信息进行指纹识别。也即是,通过与终端的第三方应用之间的回调接口开启面内指纹模块,并在真实的指纹识别区域处显示指纹图标。如此,即使第三方应用没有对面内指纹模块做兼容,用户通过该在真实的指纹识别区域处显示的指纹图标也可以直观辨认出终端屏幕中面内指纹模块的指纹识别区域,进而实现指纹识别。

[0100] 上述所有可选技术方案,均可按照任意结合形成本公开的可选实施例,本公开实

施例对此不再一一赘述。

[0101] 图3是根据一示例性实施例示出的一种指纹识别的方法流程图,该方法应用于锁屏程序中,如图3所示,本实施例将对图2所示的实施例进行展开说明。该方法包括以下步骤。

[0102] 在步骤301中,终端的第三方应用通过与锁屏程序之间回调接口,向锁屏程序发送调用指令。

[0103] 由于指纹识别的方便、快捷且安全的特点,越来越多的第三方应用都集成了指纹识别这一功能,进而通过指纹识别来完成用户的身份验证。当第三方应用进行指纹识别时,需要获取面内指纹模块的指纹识别区域,而解锁终端屏幕的功能往往是系统自带的功能,即解锁终端屏幕时通常能够获取到指纹识别区域。因此,本公开实施例在锁屏程序中设置了一个回调接口,通过该回调接口可以实现第三方应用与锁屏程序之间的交互,也即第三方应用可以基于该回调接口通过锁屏程序来获取面内指纹模块的指纹识别区域,进而实现指纹识别。

[0104] 需要说明的是,第三方应用可能包含多个界面,例如首页界面和其他指定功能对应的界面,因此,第三方应用可以检测是否切换到到指纹识别功能对应的界面。当第三方应用检测到切换到了指纹识别功能对应的界面时,说明第三方应用可能需要进行指纹识别,此时第三方应用可以通过与锁屏程序之间的回调接口向锁屏程序发送调用指令。当然,用户可能对第三方应用中的指纹识别功能使用的较为频繁,因此,第三方应用也可以在检测到用户打开第三方应用,即第三方应用处于首页界面时,便通过与锁屏程序之间的回调接口向锁屏程序发送调用指令。本公开实施例对第三方应用向锁屏程序发送调用指令的执行时机不作限定。

[0105] 其中,第三方应用可以是需要使用指纹识别功能对用户身份进行验证的应用,例如,支付应用。当第三方应用为支付应用时,第三方应用可以在检测到需要通过指纹识别进行支付时,向锁屏程序发送调用指令,进而进行用户身份的验证。另外,第三方应用与锁屏程序之间的回调接口可以是callback接口。

[0106] 在步骤302中,锁屏程序在接收到第三方应用发送的调用指令时,根据该调用指令,开启集成于终端屏幕上的面内指纹模块。

[0107] 锁屏程序在通过回调接口接收到第三方应用发送的调用指令之后,可以确定此时需要开启集成于终端上的面内指纹模块,因此,锁屏程序可以通过锁屏程序与面内指纹模块之间的交互开启该面内指纹模块。为了便与描述,本公开实施例将锁屏程序与第三方应用之间的接口称为第一回调接口,将锁屏程序与面内指纹模块之间的接口称为第二回调接口。因此,锁屏程序在接收到第三方应用发送的调用指令并确定需要开启面内指纹模块时,可以通过第二回调接口控制开启面内指纹模块。

[0108] 需要说明的是,锁屏程序在通过第二回调接口控制开启面内指纹模块时,可以根据接收到的调用指令生成开启指令,该开启指令用于开启面内指纹模块,然后将该开启指令发送至面内指纹模块,面内指纹模块在接收到该开启指令时,便可以开启面内指纹模块。

[0109] 进一步,当面内指纹模块成功开启后,可以通过第二回调接口向锁屏程序发送特定信息,该特定信息用于确定已成功开启面内指纹模块。锁屏程序在接收到该特定信息时,可以确定已成功开启了面内指纹模块,

[0110] 其中,第二回调接口与第一回调接口可以是同一个接口,也可以是不同的接口,本公开实施例对此不做限定。当第二回调接口与第一回调接口是同一个接口时,第三方应用与面内指纹模块均通过该一个接口与锁屏程序之间进行交互,节省了接口资源,进而节省了指纹识别所耗的资源。当第二回调接口与第一回调接口是不同的接口时,第三方应用和锁屏程序之间进行交互与面内指纹模块和锁屏程序之间进行交互可以同时进行,提高了交互的效率,进而提高指纹识别的效率。

[0111] 在步骤303中,锁屏程序确定该调用指令是否用于解锁终端屏幕,当该调用指令不是用于解锁终端屏幕时,获取面内指纹模块在终端屏幕中的指纹识别区域。

[0112] 由于锁屏程序和第三方应用都可以调用面内指纹模块;因此,该调用指令可能是锁屏程序自己触发的,也可能是第三方应用触发的。并且,锁屏程序自己触发的调用指令用于解锁终端屏幕,而第三方应用触发的调用指令用于对用户身份进行验证。因此,锁屏程序根据自己触发的调用指令和第三方应用触发的调用指令的处理机制不同。因此,锁屏程序在接收到调用指令时,可以对该调用指令进行解析,确定该调用指令是否为自己触发的调用指令;当该调用指令是自己触发的调用指令时,确定该调用指令用于解锁终端屏幕;当该调用指令不是自己触发的调用指令,也即该调用指令是第三方应用触发的调用指令时,确定该调用指令不是用于解锁终端屏幕。

[0113] 在一种可能的实施例中,锁屏程序触发的调用指令会携带锁屏程序的标识;而第三方应用触发的调用指令会携带第三方应用的标识。也即该调用指令中可以携带锁屏程序的标识或者第三方应用的标识。锁屏程序可以根据该调用指令携带的标识确定该调用指令是不是自己触发的调用指令,该过程可以为:锁屏程序对调用指令进行解析,然后根据解析得到的标识判断该调用指令是由锁屏程序自己触发的调用指令,还是第三方应用触发的调用指令。当解析得到的标识是锁屏程序的标识时,确定该调用指令是由锁屏程序自己触发的调用指令;当解析得到的指令是第三方应用的标识时,确定该调用指令是由第三方应用触发的调用指令。例如,当第三方应用是支付应用时,第三方应用触发的调用指令中可以携带支付的标识。

[0114] 需要说明的是,当锁屏程序确定该调用指令不是自己触发的调用指令,即确定该调用指令不是用于解锁终端屏幕时,则可以确定该调用指令是第三方应用触发的调用指令,说明第三方应用此时需要借助锁屏程序来获取指纹识别区域,进而实现指纹识别。因此,锁屏程序在确定该调用指令不是用于解锁终端屏幕时,可以获取面内指纹模块在终端屏幕中的指纹识别区域。

[0115] 其中,锁屏程序可以在接收到调用指令时就确定该调用指令是否用于解锁终端屏幕,也可以在接收到调用指令并根据该调用指令开启集成于终端屏幕上的面内指纹模块之后,再确定该调用指令是否用于解锁终端屏幕,还可以在接收到调用指令,并开启集成于终端屏幕上的面内指纹模块的同时又确定该调用指令是否用于解锁终端屏幕,本公开实施例对此不做限定。其中,锁屏程序如果在接收到调用指令,并在开启集成于终端屏幕上的面内指纹模块的同时又确定该调用指令是否用于解锁终端屏幕,可以节省指纹识别过程所花费的时间,提高指纹识别的效率。

[0116] 另外,锁屏程序在根据调用指令开启面内指纹模块之后,可以先接收面内指纹模块发送的特定信息并确定已成功开启面内指纹模块,再确定该调用指令是否用于解锁终端

屏幕,也可以先确定该调用指令是否用于解锁终端屏幕,再接收面内指纹模块发送的特定信息并确定已成功开启面内指纹模块,还可以在接收面内指纹模块发送的特定信息并确定已成功开启面内指纹模块的同时确定该调用指令是否用于解锁终端屏幕,本公开实施例对此不做限定。其中,锁屏程序如果在接收面内指纹模块发送的特定信息并确定已成功开启面内指纹模块的同时确定该调用指令是否用于解锁终端屏幕时,可以节省指纹识别过程所花费的时间,提高指纹识别的效率。

[0117] 在步骤304中,锁屏程序在当前界面的指纹识别区域处显示指纹图标,该指纹图标用于提示用户的手指在指纹识别区域内进行按压。

[0118] 由于面内指纹模块设置在终端屏幕中,用户无法直观辨认出终端屏幕的哪个区域是面内指纹模块的指纹识别区域,因此,可以通过指纹图标的形式向用户提示指纹识别区域的位置,进而完成指纹识别。

[0119] 在一种可能的实施例中,锁屏程序在获取面内指纹模块在终端屏幕中的指纹识别区域后,可以在当前界面上叠加一层锁屏界面,并在该锁屏界面的指纹识别区域处显示指纹图标。由于是在指纹识别区域处显示指纹图标,也即指纹图标可以准确地反映指纹识别区域的所在位置,因此,用户的手指触碰该指纹图标相当于用户的手指在指纹识别区域处进行按压,此时即可实现指纹识别功能,避免了指纹图标带给用户的误导性,因此指纹识别的效果较好。

[0120] 需要说明的是,锁屏程序还可以对锁屏界面进行透明处理,透明处理后的锁屏界面用于透过该锁屏界面显示第三方应用的提示信息。可选地,锁屏程序在当前界面上叠加一层锁屏界面后,可以先对该锁屏界面进行透明处理,然后在透明处理后的锁屏界面的指纹识别区域处显示指纹图标;还可以先在锁屏界面的指纹识别区域处显示指纹图标,然后对显示指纹图标后的锁屏界面进行透明处理,本公开实施例对此不做限定。其中,在对显示指纹图标后的锁屏界面进行透明处理时,可以将显示指纹图标后的锁屏界面中除了指纹图标之外的区域进行透明处理。

[0121] 由于第三方应用的当前界面通常会显示一些提示信息,例如当第三方应用为支付应用时,在当前界面显示“请输入指纹,并通过指纹进行身份验证以完成支付”的提示信息。因此,当在当前界面叠加一层包含指纹图标的锁屏界面时,为了防止第三方应用中的提示信息被叠加的锁屏界面遮挡,本公开实施例对该锁屏界面作了透明处理。如此,用户不仅可以准确无误的进行指纹识别,还可以清晰地查看第三方应用的当前界面中显示的所有内容,其中包括提示信息。

[0122] 其中,除了可以在指纹识别区域处显示指纹图标之外,还可以在指纹识别区域处显示指纹图标和指纹识别信息;该指纹识别信息用于提示用户在该指纹图标处按压用户的手指。例如,在指纹识别区域处显示指纹图标和“请在指纹图标处按压手指”的指纹识别信息。在这种情况下,用户可以透过该锁屏界面中除了指纹图标和指纹识别信息之外的区域查看第三方应用的所有内容,其中包括提示信息。

[0123] 在步骤305中,当锁屏程序检测指纹识别区域被手指按压时,获取该指纹识别区域中的该手指的指纹信息,并根据该指纹信息进行指纹识别。

[0124] 由于已在指纹识别区域处显示了指纹图标,且用户可以根据该指纹图标的提示将手指在该指纹识别区域处进行按压,因此,锁屏程序可以检测到指纹是被区域被手指按压,

并获取手该指纹识别区域处手指的指纹信息,进而根据该指纹信息进行指纹识别。以下将通过步骤(1)、(2)和(3)对步骤305进行详细说明:

[0125] (1) 锁屏程序对指纹识别区域进行检测。

[0126] 锁屏程序可以对指纹识别区域进行检测,并当检测到该指纹识别区域被按压的按压事件时,获取该按压事件的事件类型和压力值,当该事件类型为指定类型,且该压力值超过预设阈值时,确定该指纹识别区域被手指按压。其中,指定类型为指纹识别对应的事件类型。

[0127] 在一种可能的实施例中,锁屏程序还可以通过压力传感器对指纹识别区域进行检测。也即是,锁屏程序可以向压力传感器发送采集指令,压力传感器在接收到该采集指令后,即可对指纹识别区域进行检测。当压力传感器检测到该指纹识别区域被按压的按压事件时,确定该按压事件的事件类型和压力值,并向锁屏程序上报该事件类型和该压力值。锁屏程序在接收到该按压事件的事件类型和压力值,并当该事件类型为指定类型,且该压力值超过预设阈值时,确定该指纹识别区域被手指按压。

[0128] 其中,压力传感器在接收到该采集指令后对指纹识别区域进行检测的过程中,可以先检测是否接收到触摸感应模块发送的手指的位置信息,当接收到手指的位置信息时,对指纹识别区域进行检测,并根据手指的位置信息确定该手指是否位于指纹识别区域。当压力传感器确定该手指位于指纹识别区域时,确定检测到了该指纹识别区域被按压的按压事件。

[0129] 由于用户可能会误触指纹识别区域,而一般误触的压力值通常都较小,因此,为了避免将用户误触指纹识别区域的事件当作用户需要指纹识别时按压指纹识别区域的按压事件,本公开实施例可以设置指定类型和预设阈值,只有当按压事件的事件类型为指定类型且压力值超过预设阈值时,才确定该指纹识别区域被手指按压,提高了指纹识别的效率。

[0130] (2) 锁屏程序获取该指纹识别区域中的该手指的指纹信息。

[0131] 当锁屏程序对指纹识别区域进行检测并确定该指纹识别区域被手指按压时,可以获取该指纹识别区域中该手指的指纹信息。锁屏程序在获取指纹识别区域中的手指的指纹信息时,可以将终端屏幕的背光设置为高亮模式,在高亮模式下采集该手指的图像,并将该手指的图像作为手指的指纹信息。

[0132] 需要说明的是,锁屏程序在高亮模式下采集该手指的图像的过程中,可以控制面内指纹模块来采集手指的图像。也即是,锁屏程序可以通过与面内指纹模块之间的第二回调接口将高亮模式调整完成的信息发送给面内指纹识别模块,面内指纹识别模块在接收到该信息时,便可以在该高亮模式下采集该手指的图像,并将该手指的图像作为手指的指纹信息。

[0133] 还需要说明的是,为了进一步确保指纹识别的安全性,在锁屏程序对指纹识别区域进行检测的同时,面内指纹模块也可以对指纹识别区域进行检测,并当面内指纹模块检测到该指纹识别区域被按压的按压事件时,获取该按压事件的事件类型和压力值,当该事件类型为指定类型,且该压力值超过预设阈值时,确定该指纹识别区域被手指按压。因此,面内指纹模块在通过第二回调接口接收到锁屏程序发送的高亮模式调整完成的信息,并同时根据对指纹识别区域的检测确定该指纹识别区域被手指按压时,才开始工作,即开始在高亮模式下采集手指的图像,并将该手指的图像作为手指的指纹信息。

[0134] 可选地,锁屏程序还可以在获取指纹识别区域中的手指的指纹信息时,只将指纹识别区域处的背光设置为高亮模式,并采集该手指的图像,且将该手指的图像作为手指的指纹信息。

[0135] 为了获取更清晰的手指的图像,本公开实施例在获取手指的指纹信息时可以将终端屏幕的背光设置为高亮模式,也可以将指纹识别区域处的背光设置为高亮模式,并采集手指的图像。当将终端屏幕的背光设置为高亮模式时,不仅可以清晰地采集手指的图像,终端屏幕背光的均匀性还可以带给用户一定的舒适性。当将指纹识别区域处的背光设置为高亮模式时,不仅可以清晰地采集手指的图像,还可以节省电量,进而节省指纹识别的资源。

[0136] (3) 锁屏程序根据该指纹信息进行指纹识别。

[0137] 锁屏程序在获取指纹识别区域中的手指的指纹信息后,即可根据该指纹信息进行指纹识别。

[0138] 需要说明的是,由于锁屏程序可以控制面内指纹模块来采集的手指的图像,并将该手指的图像作为手指的指纹信息,因此,面内指纹模块可以将该指纹信息发送至算法程序。算法程序在接收到该指纹信息时,可以确定该指纹信息与指纹模板库中的指纹信息之间的匹配度,当该匹配度大于预设匹配度时,确定匹配结果为验证通过;当该匹配度不大于预设匹配度时,确定该匹配结果为验证不通过。算法程序确定出匹配结果后,将该匹配结果发送至锁屏程序,由锁屏程序将该匹配结果转发至第三方应用。

[0139] 其中,指纹模板库中存储合法用户的至少一个指纹信息,合法用户为授权使用该终端的用户,且合法用户的至少一个指纹信息在注册阶段录入并存入该指纹模板库中。另外,算法程序可以通过任一匹配度算法确定两个指纹信息之间的匹配度。并且,算法程序还可以通过两个指纹信息的特征值信息,确定两个指纹信息之间的匹配度。相应的,对于该指纹模板库中的每个指纹信息,算法程序确定该接收到的指纹信息与指纹模板库中的指纹信息之间的匹配度的步骤可以为:算法程序提取该接收到的指纹信息的第一特征值信息,以及确定该指纹模板库中的指纹信息的第二特征值信息,确定第一特征值信息和第二特征值信息之间的匹配度,将该匹配度确定为该接收到的指纹信息与指纹模板库中的指纹信息之间的匹配度。

[0140] 当算法程序通过两个指纹信息的特征值信息,确定两个指纹信息之间的匹配度时,该指纹模板库中可以不存储合法用户的至少一个指纹信息,而存储该至少一个指纹信息的特征值信息。当然,该指纹模板库中也可以同时存储至少一个指纹信息和至少一个指纹信息的特征值信息。相应的,算法程序确定该指纹模板库中的指纹信息的第二特征值信息的步骤可以为:算法程序从该指纹模板库中获取该指纹信息的第二特征值信息,或者从该指纹模板库的指纹信息中提取第二特征值信息。

[0141] 在本公开实施例中,通过与终端的第三方应用之间的回调接口接收第三方应用发送的调用指令,然后根据该调用指令开启集成于终端屏幕上的面内指纹模块。由于获取了面内指纹模块在终端屏幕中的指纹识别区域,并在当前界面的该指纹识别区域处显示指纹图标,也即该指纹图标可以准确地向用户提示指纹识别区域的位置,因此,用户的手指可以在该指纹识别区域内进行按压。进而当检测该指纹识别区域被手指按压时,获取该指纹识别区域中的手指的指纹信息,并根据该指纹信息进行指纹识别。也即是,通过与终端的第三方应用之间的回调接口开启面内指纹模块,并在真实的指纹识别区域处显示指纹图标。如

此,即使第三方应用没有对面内指纹模块做兼容,用户通过该在真实的指纹识别区域处显示的指纹图标也可以直观辨认出终端屏幕中面内指纹模块的指纹识别区域,进而实现指纹识别。

[0142] 图4是根据一示例性实施例示出的一种指纹识别的装置400的框图。如图4所示,该装置400包括接收模块401,开启模块402、显示模块403和识别模块404。

[0143] 接收模块401,用于通过与终端的第三方应用之间的回调接口,接收该第三方应用发送的调用指令;

[0144] 开启模块402,用于根据该调用指令,开启集成于终端屏幕上的面内指纹模块;

[0145] 显示模块403,用于获取该面内指纹模块在该终端屏幕中的指纹识别区域,并在当前界面的该指纹识别区域处显示指纹图标,该指纹图标用于提示用户的手指在该指纹识别区域内进行按压;

[0146] 识别模块404,用于当检测该指纹识别区域被该手指按压时,获取该指纹识别区域中的该手指的指纹信息,并根据该指纹信息进行指纹识别。

[0147] 可选地,该装置还包括:

[0148] 第一确定模块,用于当接收到该面内指纹模块发送的特定信息时,确定已成功开启该面内指纹模块,触发该显示模块在该当前界面的该指纹识别区域处显示指纹图标,该特定信息用于指示成功开启该面内指纹模块。

[0149] 可选地,该装置还包括:

[0150] 第二确定模块,用于确定该调用指令是否用于解锁该终端屏幕;

[0151] 触发模块,用于当该调用指令不是用于解锁该终端屏幕时,触发该显示模块获取该面内指纹模块在该终端屏幕中的指纹识别区域。

[0152] 可选地,该显示模块包括:

[0153] 叠加子模块,用于在该当前界面上叠加一层锁屏界面;

[0154] 显示子模块,用于在该锁屏界面的该指纹识别区域处显示该指纹图标。

[0155] 可选地,该显示模块还包括:

[0156] 处理子模块,用于对该锁屏界面进行透明处理,透明处理后的锁屏界面用于透过该锁屏界面显示该第三方应用的提示信息。

[0157] 可选地,该方法还包括:

[0158] 检测模块,用于对该指纹识别区域进行检测;

[0159] 获取模块,用于当检测到该指纹识别区域被按压的按压事件时,获取该按压事件的事件类型和压力值;

[0160] 第三确定模块,用于当该事件类型为指定类型,且该压力值超过预设阈值时,确定该指纹识别区域被手指按压。

[0161] 可选地,该识别模块包括:

[0162] 高亮子模块,用于将该终端屏幕的背光设置为高亮模式;

[0163] 采集模块,用于在该高亮模式下,采集该手指的图像,并将该手指的图像作为该手指的指纹信息。

[0164] 在本公开实施例中,通过与终端的第三方应用之间的回调接口接收第三方应用发送的调用指令,然后根据该调用指令开启集成于终端屏幕上的面内指纹模块。由于获取了

面内指纹模块在终端屏幕中的指纹识别区域,并在当前界面的该指纹识别区域处显示指纹图标,也即该指纹图标可以准确地向用户提示指纹识别区域的位置,因此,用户的手指可以在该指纹识别区域内进行按压。进而当检测该指纹识别区域被手指按压时,获取该指纹识别区域中的手指的指纹信息,并根据该指纹信息进行指纹识别。也即是,通过与终端的第三方应用之间的回调接口开启面内指纹模块,并在真实的指纹识别区域处显示指纹图标。如此,即使第三方应用没有对面内指纹模块做兼容,用户通过该在真实的指纹识别区域处显示的指纹图标也可以直观辨认出终端屏幕中面内指纹模块的指纹识别区域,进而实现指纹识别。

[0165] 关于上述实施例中的装置,其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述,此处将不做详细阐述说明。

[0166] 图5是根据一示例性实施例示出的一种用于拍摄的装置500的框图。例如,装置500可以是移动电话,计算机,数字广播终端,消息收发设备,游戏控制台,平板设备,医疗设备,健身设备,个人数字助理等。

[0167] 参照图5,装置500可以包括以下一个或多个组件:处理组件502,存储器504,电源组件506,多媒体组件508,音频组件510,输入/输出(I/O)的接口512,传感器组件514,以及通信组件516。

[0168] 处理组件502通常控制装置500的整体操作,诸如与显示,电话呼叫,数据通信,相机操作和记录操作相关联的操作。处理组件502可以包括一个或多个处理器520来执行指令,以完成上述的方法的全部或部分步骤。此外,处理组件502可以包括一个或多个模块,便于处理组件502和其他组件之间的交互。例如,处理组件502可以包括多媒体模块,以方便多媒体组件508和处理组件502之间的交互。

[0169] 存储器504被配置为存储各种类型的数据以支持在装置500的操作。这些数据的示例包括用于在装置500上操作的任何应用程序或方法的指令,联系人数据,电话簿数据,消息,图片,视频等。存储器504可以由任何类型的易失性或非易失性存储设备或者它们的组合实现,如静态随机存取存储器(SRAM),电可擦除可编程只读存储器(EEPROM),可擦除可编程只读存储器(EPROM),可编程只读存储器(PROM),只读存储器(ROM),磁存储器,快闪存储器,磁盘或光盘。

[0170] 电源组件506为装置500的各种组件提供电源。电源组件506可以包括电源管理系统,一个或多个电源,及其他与为装置500生成、管理和分配电源相关联的组件。

[0171] 多媒体组件508包括在所述装置500和用户之间的提供一个输出接口的屏幕。在一些实施例中,屏幕可以包括液晶显示器(LCD)和触摸面板(TP)。如果屏幕包括触摸面板,屏幕可以被实现为触摸屏,以接收来自用户的输入信号。触摸面板包括一个或多个触摸传感器以感测触摸、滑动和触摸面板上的手势。所述触摸传感器可以不仅感测触摸或滑动动作的边界,而且还检测与所述触摸或滑动操作相关的持续时间和压力。在一些实施例中,多媒体组件508包括一个前置摄像头和/或后置摄像头。当装置500处于操作模式,如拍摄模式或视频模式时,前置摄像头和/或后置摄像头可以接收外部的多媒体数据。每个前置摄像头和后置摄像头可以是一个固定的光学透镜系统或具有焦距和光学变焦能力。

[0172] 音频组件510被配置为输出和/或输入音频信号。例如,音频组件510包括一个麦克风(MIC),当装置500处于操作模式,如呼叫模式、记录模式和语音识别模式时,麦克风被配

置为接收外部音频信号。所接收的音频信号可以被进一步存储在存储器504或经由通信组件516发送。在一些实施例中,音频组件510还包括一个扬声器,用于输出音频信号。

[0173] I/O接口512为处理组件502和外围接口模块之间提供接口,上述外围接口模块可以是键盘,点击轮,按钮等。这些按钮可包括但不限于:主页按钮、音量按钮、启动按钮和锁定按钮。

[0174] 传感器组件514包括一个或多个传感器,用于为装置500提供各个方面的状态评估。例如,传感器组件514可以检测到装置500的打开/关闭状态,组件的相对定位,例如所述组件为装置500的显示器和小键盘,传感器组件514还可以检测装置500或装置500一个组件的位置改变,用户与装置500接触的存在或不存在,装置500方位或加速/减速和装置500的温度变化。传感器组件514可以包括接近传感器,被配置用来在没有任何的物理接触时检测附近物体的存在。传感器组件514还可以包括光传感器,如CMOS或CCD图像传感器,用于在成像应用中使用。在一些实施例中,该传感器组件514还可以包括加速度传感器,陀螺仪传感器,磁传感器,压力传感器或温度传感器。

[0175] 通信组件516被配置为便于装置500和其他设备之间有线或无线方式的通信。装置500可以接入基于通信标准的无线网络,如WiFi,2G或3G,或它们的组合。在一个示例性实施例中,通信组件516经由广播信道接收来自外部广播管理系统的广播信号或广播相关信息。在一个示例性实施例中,所述通信组件516还包括近场通信(NFC)模块,以促进短程通信。例如,在NFC模块可基于射频识别(RFID)技术,红外数据协会(IrDA)技术,超宽带(UWB)技术,蓝牙(BT)技术和其他技术来实现。

[0176] 在示例性实施例中,装置500可以被一个或多个应用专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子元件实现,用于执行上述图4或图5所示实施例提供的方法。

[0177] 在示例性实施例中,还提供了一种包括指令的非临时性计算机可读存储介质,例如包括指令的存储器504,上述指令可由装置500的处理器520执行以完成上述方法。例如,所述非临时性计算机可读存储介质可以是ROM、随机存取存储器(RAM)、CD-ROM、磁带、软盘和光数据存储设备等。

[0178] 一种非临时性计算机可读存储介质,当所述存储介质中的指令由终端的处理器执行时,使得终端能够执行一种指纹识别的方法。

[0179] 一种包含指令的计算机程序产品,当该计算机程序产品中的指令由终端的处理器执行时,使得终端能够执行上述图2和图3中指纹识别的方法。

[0180] 本领域技术人员在考虑说明书及实践这里公开的发明后,将容易想到本发明的其它实施方案。本申请旨在涵盖本发明的任何变型、用途或者适应性变化,这些变型、用途或者适应性变化遵循本发明的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。

[0181] 应当理解的是,本发明并不局限于上面已经描述并在附图中示出的精确结构,并且可以在不脱离其范围进行各种修改和改变。

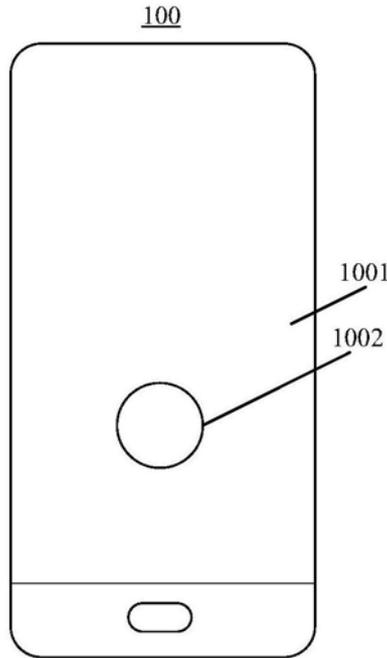


图1

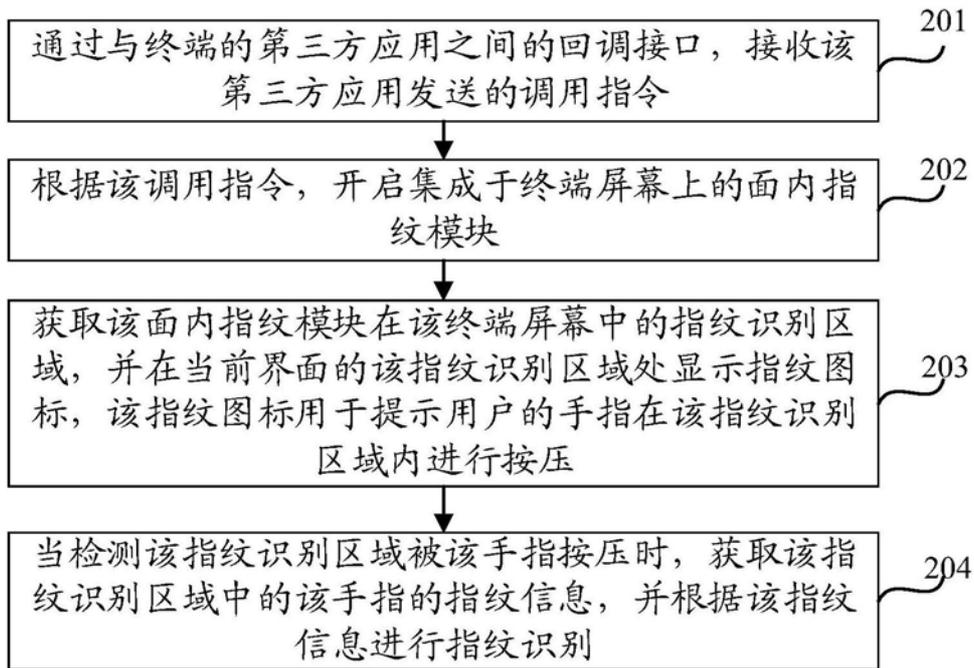


图2

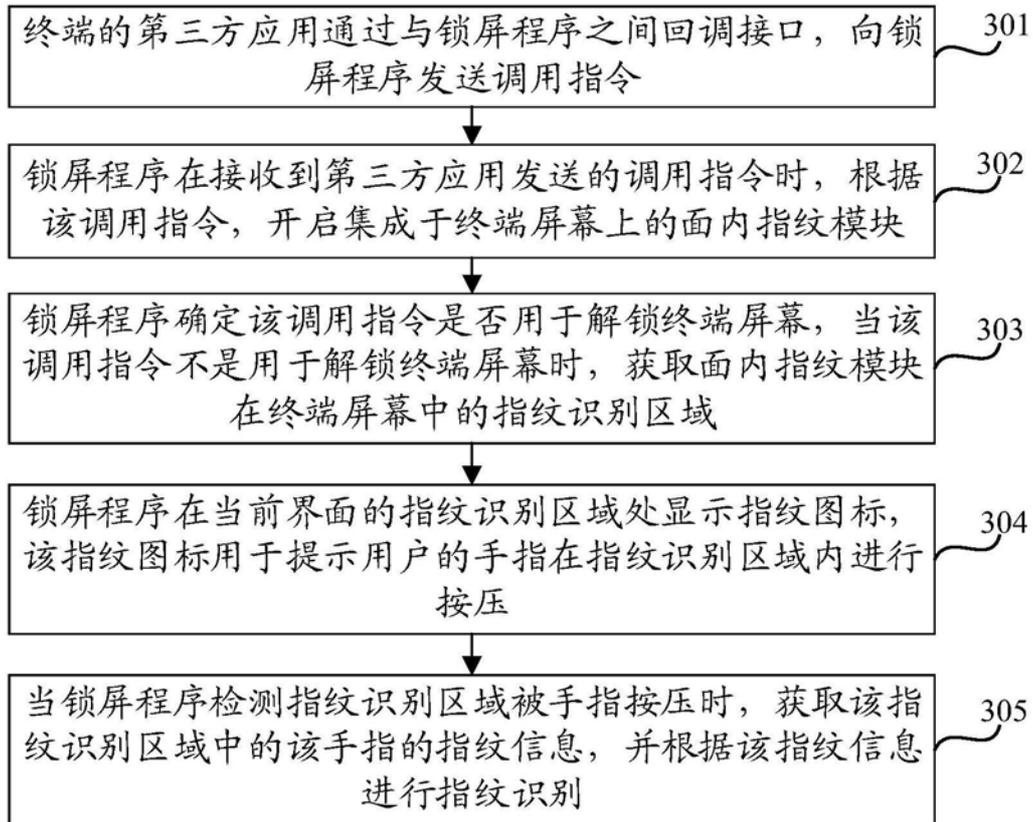


图3

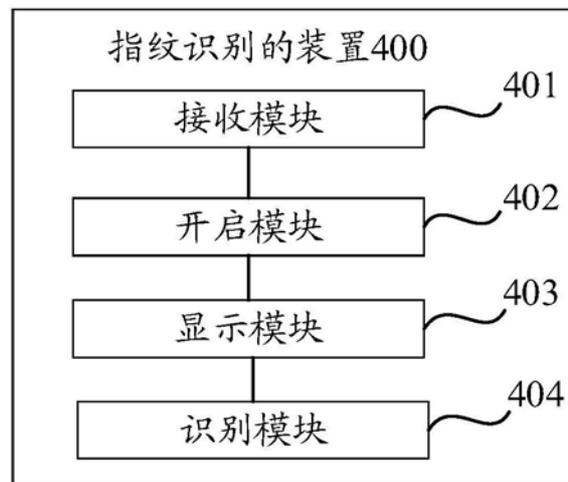


图4

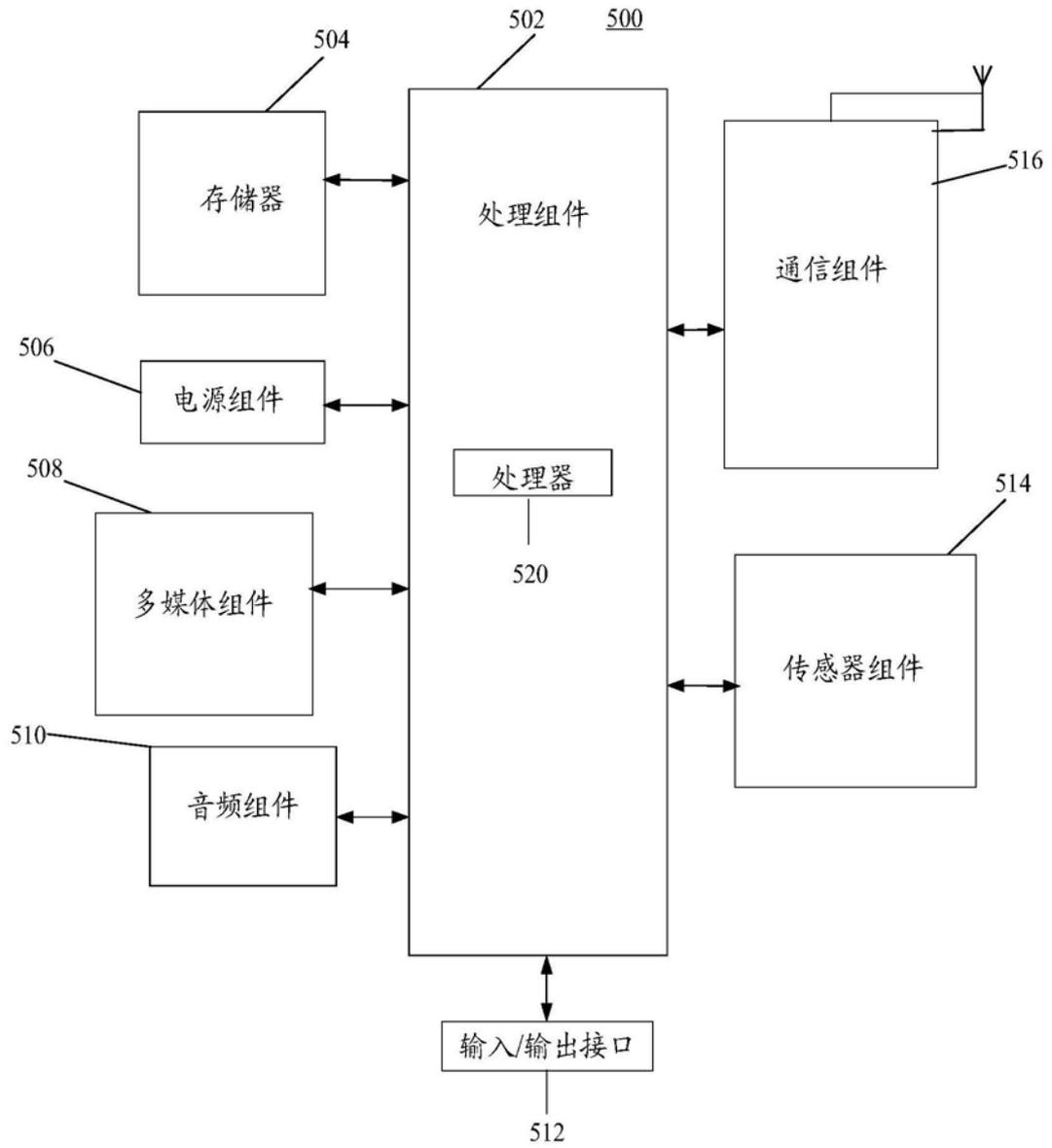


图5