(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 104765552 B
(45)授权公告日 2019.04.19

(21)申请号 201510209637.6

(22)申请日 2015.04.28

(65)同一申请的已公布的文献号
申请公布号 CN 104765552 A

(43)申请公布日 2015.07.08

(73)专利权人 小米科技有限责任公司
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13层

(72)发明人 陈巧卓 朱印 李文昕

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
G06F 3/0487(2013.01)
G06F 21/32(2013.01)

(56)对比文件
US 2014/0292666 A1,2014.10.02,说明书第[0016],第[0027]-[0028]段,第[0047]段,第[0051]段及附图1.
EP 1857954 A1,2007.11.21,全文.
WO 2015/016524 A1,2015.02.05,全文.
JP 特表2012-527657 A,2012.11.08,全文.
CN 104469717 A,2015.03.25,全文.
CN 103488924 A,2014.01.01,全文.
CN 103577739 A,2014.02.12,全文.

审查员 吉利

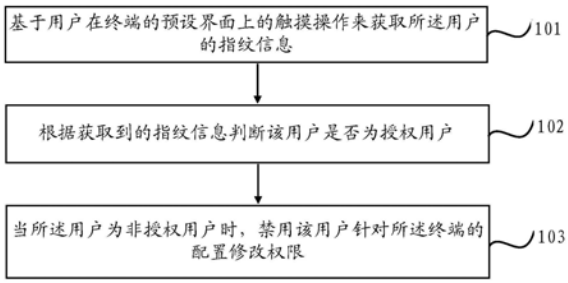
权利要求书2页 说明书12页 附图8页

(54)发明名称

权限管理方法和装置

(57)摘要

本公开提出一种权限管理方法,所述方法包括:基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息;根据获取到的指纹信息判断该用户是否为授权用户;当所述用户为非授权用户时,禁用该用户针对所述终端的配置修改权限。本公开可以实现在非本机用户使用用户的终端时无法获得修改终端配置的权限,从而增加了终端使用的安全性。



CN 104765552 B

1.一种权限管理方法,其特征在于,所述方法包括:

在解锁状态下,基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息;

根据获取到的指纹信息判断该用户是否为授权用户;

当所述用户为非授权用户时,通过修改预先建立的触摸事件与对应的配置修改事件之间的触发关系,禁用该用户的触摸操作所触发的配置修改事件所对应的配置修改权限;

所述触摸操作包括长按操作,所述基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息包括:

监听用户针对所述终端的预设界面的触摸事件;

判断监听到的触摸事件是否为长按事件;

当监听到的触摸事件为长按事件时,获取所述长按事件的触摸点,并在所述触摸点的位置获取所述用户的指纹信息。

2.如权利要求1所述的方法,其特征在于,所述监听用户针对所述终端的预设界面的触摸事件之前,所述方法还包括:

判断所述终端是否已被解锁;

当所述终端已被解锁时,开始监听用户针对所述终端的预设界面的触摸事件。

3.如权利要求1～2任一所述的方法,其特征在于,所述预设界面包括所述终端的屏幕的可见区域。

4.如权利要求1所述的方法,其特征在于,所述当所述用户为非授权用户时,禁用该用户针对所述终端的配置修改权限包括:

当所述用户为非授权用户时,判断所述触摸操作是否触发了针对所述终端的配置修改事件;

当所述触摸操作触发了针对所述终端的配置修改事件时,禁用所述配置修改事件对应的配置修改权限。

5.如权利要求4所述的方法,其特征在于,所述方法还包括:

当禁用了所述配置修改事件对应的配置修改权限后,通过所述预设界面向用户输出提示消息。

6.如权利要求1或4所述的方法,其特征在于,所述配置修改权限包括移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限。

7.一种权限管理装置,其特征在于,所述装置包括:

获取模块,用于在解锁状态下,基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息;

判断模块,用于根据获取到的指纹信息判断该用户是否为授权用户;

禁用模块,用于在所述用户为非授权用户时,通过修改预先建立的触摸事件与对应的配置修改事件之间的触发关系,禁用该用户的触摸操作所触发的配置修改事件所对应的配置修改权限;

所述触摸操作包括长按操作,所述获取模块包括:

监听子模块,用于监听用户针对所述终端的预设界面的触摸事件;

第一判断子模块，用于判断监听到的触摸事件是否为长按事件；

获取子模块，用于在监听到的触摸事件为长按事件时，获取所述长按事件的触摸点，并在所述触摸点的位置获取所述用户的指纹信息。

8.如权利要求7所述的装置，其特征在于，所述获取模块还包括：

第二判断子模块，用于在所述监听子模块监听用户针对所述终端的预设界面的触摸事件之前，判断所述终端是否已被解锁；当所述终端已被解锁时，开始由所述监听子模块监听用户针对所述终端的预设界面的触摸事件。

9.如权利要求7～8任一所述的装置，其特征在于，所述预设界面包括所述终端的屏幕的可见区域。

10.如权利要求7所述的装置，其特征在于，所述禁用模块包括：

第三判断子模块，用于在所述用户为非授权用户时，判断所述触摸操作是否触发了针对所述终端的配置修改事件；

禁用子模块，用于在所述触摸操作触发了针对所述终端的配置修改事件时，禁用所述配置修改事件对应的配置修改权限。

11.如权利要求10所述的装置，其特征在于，所述禁用模块还包括：

输出子模块，用于在禁用了所述配置修改事件对应的配置修改权限后，通过所述预设界面向用户输出提示消息。

12.如权利要求7或10所述的装置，其特征在于，所述配置修改权限包括移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限。

13.一种权限管理装置，其特征在于，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：

在解锁状态下，基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

根据获取到的指纹信息判断该用户是否为授权用户；

当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限；

所述触摸操作包括长按操作，所述基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息包括：

监听用户针对所述终端的预设界面的触摸事件；

判断监听到的触摸事件是否为长按事件；

当监听到的触摸事件为长按事件时，获取所述长按事件的触摸点，并在所述触摸点的位置获取所述用户的指纹信息。

权限管理方法和装置

技术领域

[0001] 本公开涉及通讯领域，尤其涉及权限管理方法和装置。

背景技术

[0002] 用户在使用手机时，通常可以通过一些特定的操作，例如长按操作，来对桌面上的应用进行修改。然而在这种情况下，也增加了智能手持终端被非本机用户误操作的发生几率。

发明内容

[0003] 为克服相关技术中存在的问题，本公开提供一种权限管理方法和装置。

[0004] 根据本公开实施例的第一方面，提供一种权限管理方法，所述方法包括：

[0005] 基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

[0006] 根据获取到的指纹信息判断该用户是否为授权用户；

[0007] 当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限。

[0008] 可选的，所述触摸操作包括长按操作；

[0009] 所述基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息包括：

[0010] 监听用户针对所述终端的预设界面的触摸事件；

[0011] 判断监听到的触摸事件是否为长按事件；

[0012] 当监听到的触摸事件为长按事件时，获取所述长按事件的触摸点，并在所述触摸点的位置获取所述用户的指纹信息。

[0013] 可选的，所述监听用户针对所述终端的预设界面的触摸事件之前，所述方法还包括：

[0014] 判断所述终端是否已被解锁；

[0015] 当所述终端已被解锁时，开始监听用户针对所述终端的预设界面的触摸事件。

[0016] 可选的，所述预设界面包括所述终端的屏幕的可见区域。

[0017] 可选的，所述当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限包括：

[0018] 当所述用户为非授权用户时，判断所述触摸操作是否触发了针对所述终端的配置修改事件；

[0019] 当所述触摸操作触发了针对所述终端的配置修改事件时，禁用所述配置修改事件对应的配置修改权限。

[0020] 可选的，所述方法还包括：

[0021] 当禁用了所述配置修改事件对应的配置修改权限后，通过所述预设界面向用户输出提示消息。

[0022] 可选的，所述配置修改权限包括移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限。

[0023] 根据本公开实施例的第二方面，提供一种权限管理装置，所述装置包括：

[0024] 获取模块，用于基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

[0025] 判断模块，用于根据获取到的指纹信息判断该用户是否为授权用户；

[0026] 禁用模块，用于在所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限。

[0027] 可选的，所述触摸操作包括长按操作；

[0028] 所述获取模块包括：

[0029] 监听子模块，用于监听用户针对所述终端的预设界面的触摸事件；

[0030] 第一判断子模块，用于判断监听到的触摸事件是否为长按事件；

[0031] 获取子模块，用于在监听到的触摸事件为长按事件时，获取所述长按事件的触摸点，并在所述触摸点的位置获取所述用户的指纹信息。

[0032] 可选的，所述获取模块还包括：

[0033] 第二判断子模块，用于在所述监听子模块监听用户针对所述终端的预设界面的触摸事件之前，判断所述终端是否已被解锁；当所述终端已被解锁时，开始由所述监听子模块监听用户针对所述终端的预设界面的触摸事件。

[0034] 可选的，所述预设界面包括所述终端的屏幕的可见区域。

[0035] 可选的，所述禁用模块包括：

[0036] 第三判断子模块，用于在所述用户为非授权用户时，判断所述触摸操作是否触发了针对所述终端的配置修改事件；

[0037] 禁用子模块，用于在所述触摸操作触发了针对所述终端的配置修改事件时，禁用所述配置修改事件对应的配置修改权限。

[0038] 可选的，所述禁用模块还包括：

[0039] 输出子模块，用于在禁用了所述配置修改事件对应的配置修改权限后，通过所述预设界面向用户输出提示消息。

[0040] 可选的，所述配置修改权限包括移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限。

[0041] 根据本公开实施例的第三方面，提供一种权限管理装置，包括：

[0042] 处理器；

[0043] 用于存储处理器可执行指令的存储器；

[0044] 其中，所述处理器被配置为：

[0045] 基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

[0046] 根据获取到的指纹信息判断该用户是否为授权用户；

[0047] 当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限。本公开的实施例提供的技术方案可以包括以下有益效果：

[0048] 本公开的以上实施例中，通过基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息，并根据获取到的指纹信息判断该用户是否为授权用户；当所述用户为非授权用户时，则禁用该用户针对所述终端的配置修改权限，使得非本机用户在使用用户的终端时将无法获得修改终端配置的权限，从而增加了终端使用的安全性。

[0049] 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

[0050] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

[0051] 图1是根据一示例性实施例示出的一种权限管理方法的流程示意图；

[0052] 图2是根据一示例性实施例示出的另一种权限管理方法的流程示意图；

[0053] 图3是根据一示例性实施例示出的一种系统桌面的交互示意图；

[0054] 图4是根据一示例性实施例示出的另一种系统桌面上的交互示意图；

[0055] 图5是根据一示例性实施例示出的一种权限管理装置的示意框图；

[0056] 图6是根据一示例性实施例示出的另一种权限管理装置的示意框图；

[0057] 图7是根据一示例性实施例示出的另一种权限管理装置的示意框图；

[0058] 图8是根据一示例性实施例示出的另一种权限管理装置的示意框图；

[0059] 图9是根据一示例性实施例示出的另一种权限管理装置的示意框图；

[0060] 图10是根据一示例性实施例示出的一种用于所述权限管理装置的一结构示意图。

具体实施方式

[0061] 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公开相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本公开的一些方面相一致的装置和方法的例子。

[0062] 在本公开使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本公开。在本公开和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0063] 应当理解，尽管在本公开可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本公开范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0064] 本公开提出一种权限管理方法，通过基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息，并根据获取到的指纹信息判断该用户是否为授权用户；当所述用户为非授权用户时，则禁用该用户针对所述终端的配置修改权限，使得非本机用户在使用用户的终端时将无法获得修改终端配置的权限，从而增加了终端使用的安全性。

[0065] 如图1所示，图1是根据一示例性实施例示出的一种权限管理方法，应用于终端中，包括以下步骤：

[0066] 在步骤101中，基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

[0067] 所述终端可以包括触摸式的移动终端;例如,所述移动终端可以是用户的智能手机或者平板电脑。

[0068] 在步骤102中,根据获取到的指纹信息判断该用户是否为授权用户;

[0069] 在步骤103中,当所述用户为非授权用户时,禁用该用户针对所述终端的配置修改权限。

[0070] 用户在使用终端的过程中,通常可以通过一些特定的触摸操作来对终端系统桌面上的应用进行修改;例如,以小米公司的MIUI系统为例,用户可以通过长按系统桌面上的应用图标来触发对该应用进行删除、拖动等操作。

[0071] 然而,由于常规设计中,在对用户的配置修改权限进行管理时,缺乏用户身份的认证机制,非本机用户通过长按系统桌面上的应用图标仍然能够正常的取得对该应用进行修改的权限,因此这在某种程度上增加了误操作的几率,而且在对安全性和私密性提出更高要求的大环境下,已无法满足用户的需求。

[0072] 在本实施例中,为了解决以上问题,可以在现有的配置修改权限的管理中引入身份认证机制,通过从用户日常使用终端时针对所述终端的预设界面的触摸操作中来获取用户的指纹信息,然后通过获取到的指纹信息来对用户的身份进行认证,对于认证为非授权用户的用户可以禁用该用户针对所述终端的配置修改权限。

[0073] 在本实施例中,由于是基于用户在日常使用所述终端的触摸操作来获取用户的指纹信息,而用户在日常使用所述终端的过程中,所触摸的区域通常不固定,因此所述预设界面可以包括所述终端的屏幕的可见区域。

[0074] 在从技术层面上实现时,可以预先在所述终端的屏幕的可见区域中植入指纹传感芯片,一旦在屏幕的可见区域中植入指纹传感芯片后,此时所述终端的整个屏幕均可作为指纹识别区来采集用户的指纹信息,从而用户在日常使用所述终端时,所述用户针对所述终端屏幕中的任何一个区域的触摸操作均可用来获取该用户的指纹信息。

[0075] 其中,由于获取用户指纹信息时,通常要求用户的手指完全按压在终端的屏幕上,因此在从用户日常使用终端的触摸操作中来获取用户的指纹信息时,可以通过在解锁状态下监听用户针对所述终端的屏幕的可见区域中的长按事件来获取用户的指纹信息。

[0076] 例如,终端可以首先判断当前是否处于解锁状态,如果当前处于解锁状态时,可以开始实时的监听用户针对预设界面的触摸事件,并判断监听到的触摸事件是否为长按事件,如果监听到的触摸事件为长按事件,此时可以获取该长按事件的触摸点,然后可以通过与所述触摸点位置对应的指纹传感芯片来获取该用户的指纹信息。

[0077] 当获取到所述用户的指纹信息时,此时可以通过将获取到的指纹信息与终端系统内预先录入的授权用户的指纹信息进行匹配,如果获取到的指纹信息与终端系统内预先录入的授权用户的指纹信息匹配,那么表明当前正在使用所述终端的用户为授权用户,对于授权用户,可以不对该用户的配置修改权限进行任何限制。

[0078] 当然,如果获取到的指纹信息与终端系统内预先录入的授权用户的指纹信息不匹配,那么表明当前正在使用所述终端的用户为非授权用户,对于非授权用户,可以对该用户的配置修改权限进行限制。

[0079] 在本实施例中,用户在对终端进行配置修改时,通常是由用户的一些特定的触摸事件来触发的;例如,如前所述,用户可以通过在终端的系统桌面上的应用图标进行长按操

作，来触发对该应用进行删除、拖动等操作。因此，在对非授权用户的配置修改权限进行限制时，则可以通过禁用该用户的触摸操作所触发的配置修改事件所对应的配置修改权限来实现。

[0080] 其中，所述配置修改权限可以包括移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限等。

[0081] 例如，当基于所述用户的触摸操作成功获取到该用户的指纹信息，并且通过指纹信息匹配后确定出该用户为非授权用户时，终端首先可以判断该用户的触摸操作是否触发了配置修改事件，如果该用户的触摸操作触发了配置修改事件，则可以禁用与该配置修改事件对应的配置修改权限。举例而言，假设用户试图通过对终端系统桌面上的应用图标进行长按操作来删除该应用，当终端在后台监听到这一长按事件时，可以在后台禁用该长按事件所触发的应用删除事件所对应的应用删除权限，当禁用了所述应用删除权限后，用户通过对终端系统桌面上的应用图标进行长按操作将无法完成针对该应用的删除操作。

[0082] 当然，在对非授权用户的配置修改权限进行禁用时，所禁用的权限类型可以并不限于以上描述的移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限，也可以是以上描述的各种权限中的一种或者多种的组合，本领域技术人员可以根据实际的需求结合实际的应用场景进行灵活使用。

[0083] 例如，在家庭环境中使用终端时，为了防止小孩玩耍终端时误将系统桌面上的应用图标删除，或者将桌面上的应用图标拖动放乱位置，在对非授权用户的配置修改权限进行禁用时，可以只对移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限进行禁用。而在学校或者工作环境中使用终端时，为了保证用户终端的私密性和安全性，在对非授权用户的配置修改权限进行禁用时，除了对移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限进行禁用以外，还可以对针对系统设置进行修改的权限进行禁用。

[0084] 其中，值得说明的而是，在禁用所述用户的触摸操作所触发的配置修改事件所对应的配置修改权限时，可以通过修改所述终端的系统中预先建立的触摸事件与对应的配置修改事件之间的触发关系来实现。

[0085] 例如，在常规设计中，终端的系统中通常预先建立了长按事件与对系统桌面上的图标进行删除、拖动等事件之间的触发关系，当终端在后台监听到该用户针对系统桌面上的应用图标的长按事件时，可以立即触发针对该应用图标的删除、拖动等事件。因此，在禁用该用户的长按操作所触发的对系统桌面上的图标进行删除、拖动的权限时，可以通过对终端的系统中预先建立的所述触发关系进行修改或者删除，将所述触发关系变得无效来实现。

[0086] 在本实施例中，当成功禁用了用户的配置修改权限后，此时可以通过所述预设界面向用户输出提示消息以提示该用户。其中所述提示消息可以是一个提示用户没有修改权限的提示框，也可以是一个提示用户重新进行指纹验证的提示框。

[0087] 例如，以用户通过长按操作对终端系统桌面上的应用图标进行删除或拖拽操作为例，假设终端通过监听用户的长按事件获取到该用户的指纹信息后，通过指纹信息匹配认证出该用户为非授权用户，在一种实现方式中，可以在终端系统桌面上输出一个“您没有权限编辑桌面”的文本框，以提示该用户没有编辑桌面的权限。在另一中实现方式中，可以在

终端系统桌面上输出一个“请长按桌面重新获取桌面编辑权限”的文本框，以提示该用户当前没有编辑桌面的权限，可以通过再次长按所述终端的屏幕的可见区域来进行指纹认证以获取桌面编辑的权限。

[0088] 在本实施例中，当所述终端禁用了非授权用户的配置修改权限后，当授权用户再次使用所述终端时，仍然可以通过监听该用户针对所述终端的屏幕的可见区域的长按事件来获取该用户的指纹信息，并通过将获取到的指纹信息与系统中预先录入的授权用户的指纹信息进行匹配来对该用户的身份进行认证，如果认证通过，此时终端将不会对该用户的配置修改权限进行任何的限制，该用户可以正常的对该终端的配置进行修改。

[0089] 在以上实施例中，在配置修改权限的管理中引入了身份认证机制，通过基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息，并根据获取到的指纹信息判断该用户是否为授权用户；当所述用户为非授权用户时，则禁用该用户针对所述终端的配置修改权限，使得非本机用户在使用用户的终端时将无法获得修改终端配置的权限，从而增加了终端使用的安全性。

[0090] 如图2所示，图2是根据一示例性实施例示出的一种权限管理方法，应用于终端中，包括以下步骤：

[0091] 在步骤201中，监听用户针对所述终端的预设界面的触摸事件；

[0092] 所述终端可以包括触摸式的移动终端；例如，所述移动终端可以是用户的智能手机或者平板电脑。

[0093] 在步骤202中，判断监听到的触摸事件是否为长按事件；

[0094] 在步骤203中，当监听到的触摸事件为长按事件时，获取所述长按事件的触摸点，并在所述触摸点的位置获取所述用户的指纹信息；

[0095] 在步骤204中，根据获取到的指纹信息判断该用户是否为授权用户；

[0096] 在步骤205中，当所述用户为非授权用户时，判断所述长按事件是否触发了针对所述终端的配置修改事件；

[0097] 在步骤206中，当所述长按事件触发了针对所述终端的配置修改事件时，禁用所述配置修改事件对应的配置修改权限。

[0098] 用户在使用终端的过程中，通常可以通过一些特定的触摸操作来对终端系统桌面上的应用进行修改；例如，以小米公司的MIUI系统为例，用户可以通过长按系统桌面上的应用图标来触发对该应用进行删除、拖动等操作。

[0099] 然而，由于常规设计中，在对用户的配置修改权限进行管理时，缺乏用户身份的认证机制，非本机用户通过长按系统桌面上的应用图标仍然能够正常的取得对该应用进行修改的权限，因此这在某种程度上增加了误操作的几率，而且在对安全性和私密性提出更高要求的大环境下，已无法满足用户的需求。

[0100] 在本实施例中，为了解决以上问题，可以在现有的配置修改权限的管理中引入身份认证机制，通过从用户日常使用终端时针对所述终端的预设界面的触摸操作中来获取用户的指纹信息，然后通过获取到的指纹信息来对用户的身份进行认证，对于认证为非授权用户的用户可以禁用该用户针对所述终端的配置修改权限。

[0101] 在本实施例中，由于是基于用户在日常使用所述终端的触摸操作来获取用户的指纹信息，而用户在日常使用所述终端的过程中，所触摸的区域通常不固定，因此所述预设界

面可以包括所述终端的屏幕的可见区域。

[0102] 在从技术层面上实现时，可以预先在所述终端的屏幕的可见区域中植入指纹传感芯片，一旦在屏幕的可见区域中植入指纹传感芯片后，此时所述终端的整个屏幕均可作为指纹识别区来采集用户的指纹信息，从而用户在日常使用所述终端时，所述用户针对所述终端屏幕中的任何一个区域的触摸操作均可用来获取该用户的指纹信息。

[0103] 其中，由于获取用户指纹信息时，通常要求用户的手指完全按压在终端的屏幕上，因此在从用户日常使用终端的触摸操作中来获取用户的指纹信息时，，可以通过在解锁状态下监听用户针对所述终端的屏幕的可见区域中的长按事件来获取用户的指纹信息。

[0104] 例如，终端可以首先判断当前是否处于解锁状态，如果当前处于解锁状态时，可以开始实时的监听用户针对预设界面的触摸事件，并判断监听到的触摸事件是否为长按事件，如果监听到的触摸事件为长按事件，此时可以获取该长按事件的触摸点，然后可以通过与所述触摸点位置对应的指纹传感芯片来获取该用户的指纹信息。

[0105] 当获取到所述用户的指纹信息时，此时可以通过将获取到的指纹信息与终端系统内预先录入的授权用户的指纹信息进行匹配，如果获取到的指纹信息与终端系统内预先录入的授权用户的指纹信息匹配，那么表明当前正在使用所述终端的用户为授权用户，对于授权用户，可以不对该用户的配置修改权限进行任何限制。

[0106] 当然，如果获取到的指纹信息与终端系统内预先录入的授权用户的指纹信息不匹配，那么表明当前正在使用所述终端的用户为非授权用户，对于非授权用户，可以对该用户的配置修改权限进行限制。

[0107] 在本实施例中，用户在对终端进行配置修改时，通常是由用户的一些特定的触摸事件来触发的；例如，如前所述，用户可以通过在终端的系统桌面上的应用图标进行长按操作，来触发对该应用进行删除、拖动等操作。因此，在对非授权用户的配置修改权限进行限制时，则可以通过禁用该用户的触摸操作所触发的配置修改事件所对应的配置修改权限来实现。

[0108] 其中，所述配置修改权限可以包括移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限等。

[0109] 例如，当基于所述用户的触摸操作成功获取到该用户的指纹信息，并且通过指纹信息匹配后确定出该用户为非授权用户时，终端首先可以判断该用户的触摸操作是否触发了配置修改事件，如果该用户的触摸操作触发了配置修改事件，则可以禁用与该配置修改事件对应的配置修改权限。举例而言，假设用户试图通过对终端系统桌面上的应用图标进行长按操作来删除该应用，当终端在后台监听到这一长按事件时，可以在后台禁用该长按事件所触发的应用删除事件所对应的应用删除权限，当禁用了所述应用删除权限后，用户通过对终端系统桌面上的应用图标进行长按操作将无法完成针对该应用的删除操作。

[0110] 当然，在对非授权用户的配置修改权限进行禁用时，所禁用的权限类型可以并不限于以上描述的移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限，也可以是以上描述的各种权限中的一种或者多种的组合，本领域技术人员可以根据实际的需求结合实际的应用场景进行灵活使用。

[0111] 例如，在家庭环境中使用终端时，为了防止小孩玩耍终端时误将系统桌面上的应用图标删除，或者将桌面上的应用图标拖动放乱位置，在对非授权用户的配置修改权限进

行禁用时，可以只对移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限进行禁用。而在学校或者工作环境中使用终端时，为了保证用户终端的私密性和安全性，在对非授权用户的配置修改权限进行禁用时，除了对移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限进行禁用以外，还可以对针对系统设置进行修改的权限进行禁用。

[0112] 其中，值得说明的而是，在禁用所述用户的触摸操作所触发的配置修改事件所对应的配置修改权限时，可以通过修改所述终端的系统中预先建立的触摸事件与对应的配置修改事件之间的触发关系来实现。

[0113] 例如，在常规设计中，终端的系统中通常预先建立了长按事件与对系统桌面上的图标进行删除、拖动等事件之间的触发关系，当终端在后台监听到该用户针对系统桌面上的应用图标的长按事件时，可以立即触发针对该应用图标的删除、拖动等事件。因此，在禁用该用户的长按操作所触发的对系统桌面上的图标进行删除、拖动的权限时，可以通过对终端的系统中预先建立的所述触发关系进行修改或者删除，将所述触发关系变得无效来实现。

[0114] 在本实施例中，当成功禁用了用户的配置修改权限后，此时可以通过所述预设界面向用户输出提示消息以提示该用户。其中所述提示消息可以是一个提示用户没有修改权限的提示框，也可以是一个提示用户重新进行指纹验证的提示框。

[0115] 例如，请参见图3和图4，以用户通过长按操作对终端系统桌面上的应用图标进行删除或拖拽操作为例，假设终端通过监听用户的长按事件获取到该用户的指纹信息后，通过指纹信息匹配认证出该用户为非授权用户，在一种实现方式中，可以在终端系统桌面上输出一个如图3所示出的“您没有权限编辑桌面”的文本框，以提示该用户没有编辑桌面的权限。在另一中实现方式中，可以在终端系统桌面上输出一个如图4所示出的“请长按桌面重新获取桌面编辑权限”的文本框，以提示该用户当前没有编辑桌面的权限，可以通过再次长按所述终端的屏幕的可见区域来进行指纹认证以获取桌面编辑的权限。

[0116] 在本实施例中，当所述终端禁用了非授权用户的配置修改权限后，当授权用户再次使用所述终端时，仍然可以通过监听该用户针对所述终端的屏幕的可见区域的长按事件来获取该用户的指纹信息，并通过将获取到的指纹信息与系统中预先录入的授权用户的指纹信息进行匹配来对该用户的身份进行认证，如果认证通过，此时终端将不会对该用户的配置修改权限进行任何的限制，该用户可以正常的对该终端的配置进行修改。

[0117] 在以上实施例中，在配置修改权限的管理中引入了身份认证机制，通过基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息，并根据获取到的指纹信息判断该用户是否为授权用户；当所述用户为非授权用户时，则禁用该用户针对所述终端的配置修改权限，使得非本机用户在使用用户的终端时将无法获得修改终端配置的权限，从而增加了终端使用的安全性。

[0118] 与前述权限管理方法实施例相对应，本公开还提供了一种装置的实施例。

[0119] 图5是根据一示例性实施例示出的一种权限管理装置的示意框图。

[0120] 如图5所示，根据一示例性实施例示出的一种权限管理装置500，包括：获取模块501、判断模块502和禁用模块503；其中：

[0121] 所述获取模块501被配置为，基于用户在终端的预设界面上的触摸操作来获取所

述用户的指纹信息；

[0122] 所述判断模块502被配置为，根据获取到的指纹信息判断该用户是否为授权用户；

[0123] 所述禁用模块503被配置为，在所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限。

[0124] 在以上实施例中，在配置修改权限的管理中引入了身份认证机制，通过基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息，并根据获取到的指纹信息判断该用户是否为授权用户；当所述用户为非授权用户时，则禁用该用户针对所述终端的配置修改权限，使得非本机用户在使用用户的终端时将无法获得修改终端配置的权限，从而增加了终端使用的安全性。

[0125] 请参见图6，图6是本公开根据一示例性实施例示出的另一种装置的框图，该实施例在前述图5所示实施例的基础上，所述触摸操作包括长按操作；所述获取模块501可以包括监听子模块501A、第一判断子模块501B和获取子模块501C；其中：

[0126] 所述监听子模块501A被配置为，监听用户针对所述终端的预设界面的触摸事件；

[0127] 所述第一判断子模块501B被配置为，判断监听到的触摸事件是否为长按事件；

[0128] 所述获取子模块501C被配置为，在监听到的触摸事件为长按事件时，获取所述长按事件的触摸点，并在所述触摸点的位置获取所述用户的指纹信息。

[0129] 请参见图7，图7是本公开根据一示例性实施例示出的另一种装置的框图，该实施例在前述图6所示实施例的基础上，所述获取模块501还可以包括第二判断子模块501D；其中：

[0130] 所述第二判断子模块501D被配置为，在所述监听子模块501A监听用户针对所述终端的预设界面的触摸事件之前，判断所述终端是否已被解锁；当所述终端已被解锁时，开始由所述监听子模块501A监听用户针对所述终端的预设界面的触摸事件。

[0131] 在以上各实施例中，所述预设界面包括所述终端的屏幕的可见区域。

[0132] 需要说明的是，上述图7所示的装置实施例中示出的第二判断子模块501D的结构也可以包含在前述图5的装置实施例中，对此本公开不进行限制。

[0133] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0134] 请参见图8，图8是本公开根据一示例性实施例示出的另一种装置的框图，该实施例在前述图5所示实施例的基础上，所述禁用模块503可以包括第三判断子模块503A和禁用子模块503B；其中：

[0135] 所述第三判断子模块503A被配置为，在所述用户为非授权用户时，判断所述触摸操作是否触发了针对所述终端的配置修改事件；

[0136] 所述禁用子模块503B被配置为，在所述触摸操作触发了针对所述终端的配置修改事件时，禁用所述配置修改事件对应的配置修改权限。

[0137] 需要说明的是，上述图8所示的装置实施例中示出的第三判断子模块503A和禁用子模块503B的结构也可以包含在前述图6-7的装置实施例中，对此本公开不进行限制。

[0138] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0139] 请参见图9，图9是本公开根据一示例性实施例示出的另一种装置的框图，该实施

例在前述图8所示实施例的基础上，所述禁用模块503还可以包括输出子模块503C；其中：

[0140] 所述出子模块503C被配置为，在禁用了所述配置修改事件对应的配置修改权限后，通过所述预设界面向用户输出提示消息。

[0141] 在以上各实施例中，所述配置修改权限包括移动应用图标的权限、新建文件夹的权限、将应用移出文件夹的权限、删除应用的权限以及对系统设置进行修改的权限。

[0142] 需要说明的是，上述图9所示的装置实施例中示出的输出子模块503C的结构也可以包含在前述图5-7的装置实施例中，对此本公开不进行限制。

[0143] 上述装置中各个模块的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程，在此不再赘述。

[0144] 对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理模块，即可以位于一个地方，或者也可以分布到多个网络模块上。可以根据实际的需要选择其中的部分或者全部模块来实现本公开方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0145] 相应的，本公开还提供一种权限管理装置，所述装置包括：

[0146] 处理器；

[0147] 用于存储处理器可执行指令的存储器；

[0148] 其中，所述处理器被配置为：

[0149] 基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

[0150] 根据获取到的指纹信息判断该用户是否为授权用户；

[0151] 当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限。

[0152] 相应的，本公开还提供一种终端，所述终端包括有存储器，以及一个或者一个以上的程序，其中一个或者一个以上程序存储于存储器中，且经配置以由一个或者一个以上处理器执行所述一个或者一个以上程序包含用于进行以下操作的指令：

[0153] 基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

[0154] 根据获取到的指纹信息判断该用户是否为授权用户；

[0155] 当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限。

[0156] 图10是根据一示例性实施例示出的一种权限管理装置的结构示意图。

[0157] 如图10所示，根据一示例性实施例示出的一种权限管理装置1000，该装置1000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。

[0158] 参照图10，装置1000可以包括以下一个或多个组件：处理组件1001，存储器1002，电源组件1003，多媒体组件1004，音频组件1005，输入/输出(I/O)的接口1006，传感器组件1007，以及通信组件1008。

[0159] 处理组件1001通常控制装置1000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1001可以包括一个或多个处理器1009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1001可以包括一个或多个模块，便于处理组件1001和其他组件之间的交互。例如，处理部件1001可以包括多媒体模块，

以方便多媒体组件1004和处理组件1001之间的交互。

[0160] 存储器1002被配置为存储各种类型的数据以支持在装置1000的操作。这些数据的示例包括用于在装置1000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1002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。

[0161] 电源组件1003为装置1000的各种组件提供电力。电源组件1003可以包括电源管理系统，一个或多个电源，及其他与为装置1000生成、管理和分配电力相关联的组件。

[0162] 多媒体组件1004包括在所述装置1000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1004包括一个前置摄像头和/或后置摄像头。当装置1000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。

[0163] 音频组件1005被配置为输出和/或输入音频信号。例如，音频组件1005包括一个麦克风(MIC)，当装置1000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1002或经由通信组件1008发送。在一些实施例中，音频组件1005还包括一个扬声器，用于输出音频信号。

[0164] I/O接口1002为处理组件1001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。

[0165] 传感器组件1007包括一个或多个传感器，用于为装置1000提供各个方面的状态评估。例如，传感器组件1007可以检测到装置1000的打开/关闭状态，组件的相对定位，例如所述组件为装置1000的显示器和小键盘，传感器组件1007还可以检测装置1000或装置1000一个组件的位置改变，用户与装置1000接触的存在或不存在，装置1000方位或加速/减速和装置1000的温度变化。传感器组件1007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1007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1007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。

[0166] 通信组件1008被配置为便于装置1000和其他设备之间有线或无线方式的通信。装置1000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1008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1008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。

[0167] 在示例性实施例中，装置1000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，用于执行上述方法。

[0168] 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1002，上述指令可由装置1000的处理器1009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。

[0169] 其中，当所述存储介质中的指令由移动终端的处理器执行时，使得移动终端能够执行一种权限管理方法，包括：

[0170] 基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息；

[0171] 根据获取到的指纹信息判断该用户是否为授权用户；

[0172] 当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限。

[0173] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、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公开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。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由下面的权利要求指出。

[0174] 应当理解的是，本公开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。本公开的范围仅由所附的权利要求来限制。

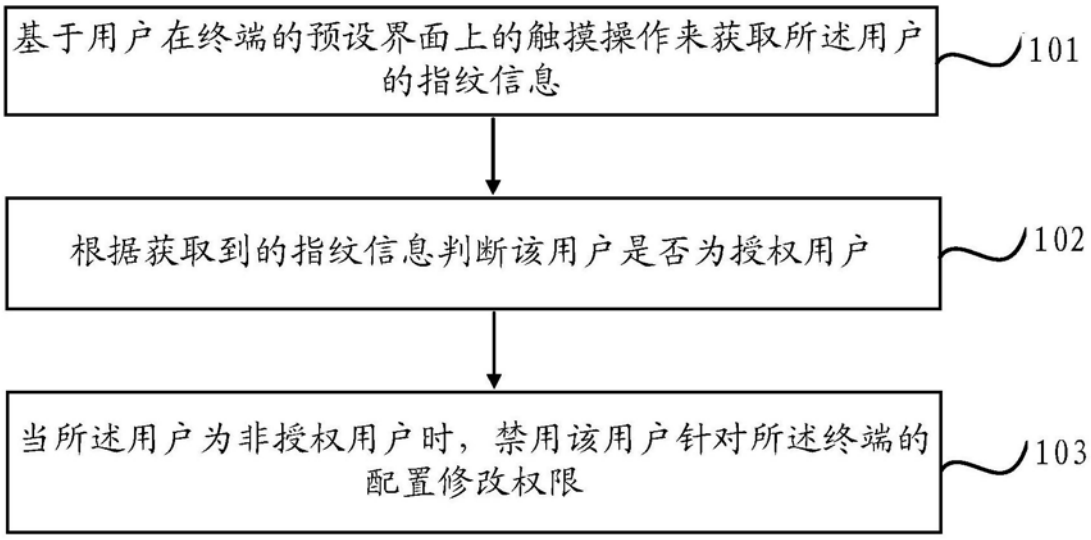

基于用户在终端的预设界面上的触摸操作来获取所述用户的指纹信息
101
根据获取到的指纹信息判断该用户是否为授权用户
102
当所述用户为非授权用户时，禁用该用户针对所述终端的配置修改权限
103

图1

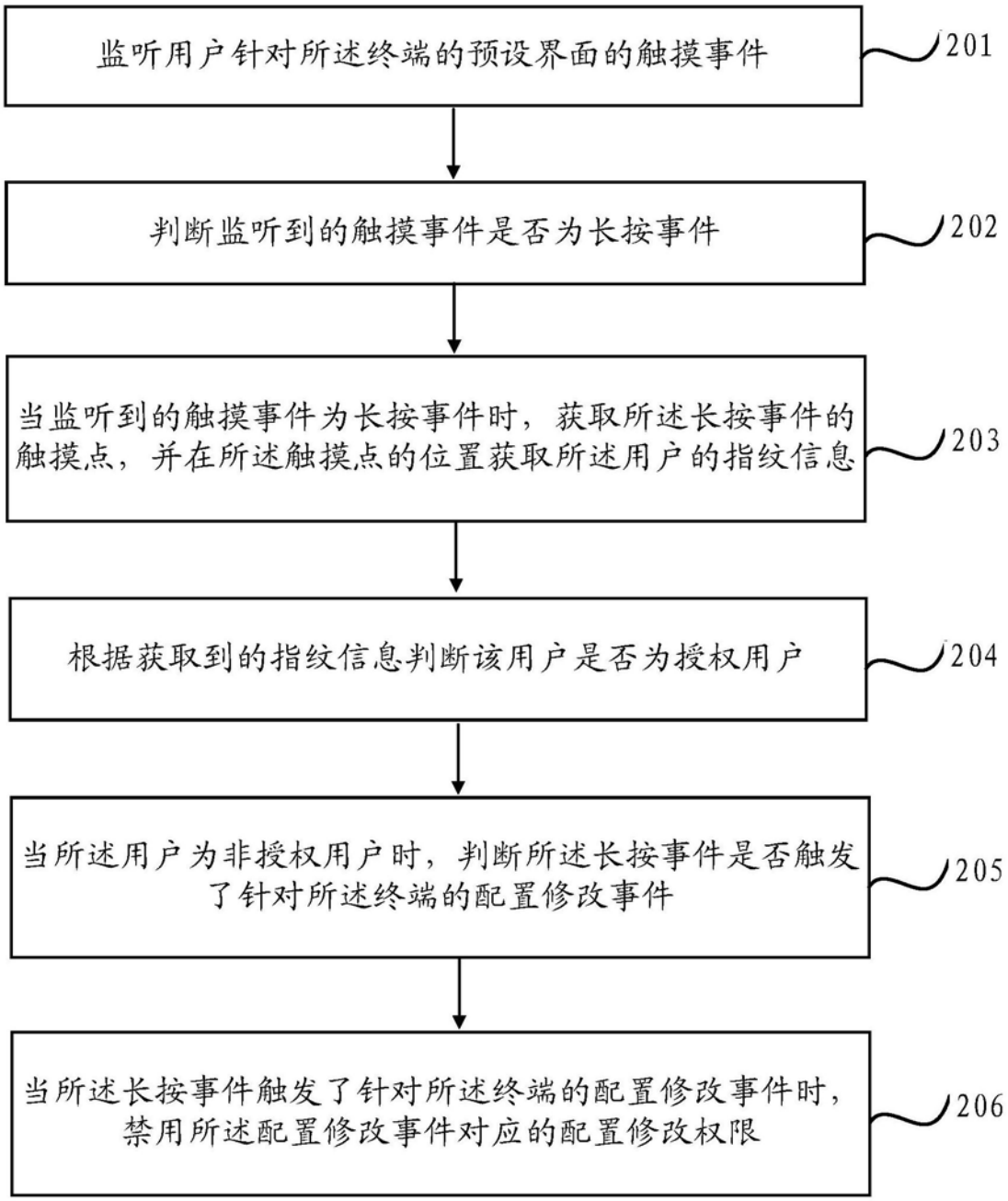

监听用户针对所述终端的预设界面的触摸事件
201
判断监听到的触摸事件是否为长按事件
202
当监听到的触摸事件为长按事件时，获取所述长按事件的触摸点，并在所述触摸点的位置获取所述用户的指纹信息
203
根据获取到的指纹信息判断该用户是否为授权用户
204
当所述用户为非授权用户时，判断所述长按事件是否触发了针对所述终端的配置修改事件
205
当所述长按事件触发了针对所述终端的配置修改事件时，禁用所述配置修改事件对应的配置修改权限
206

图2

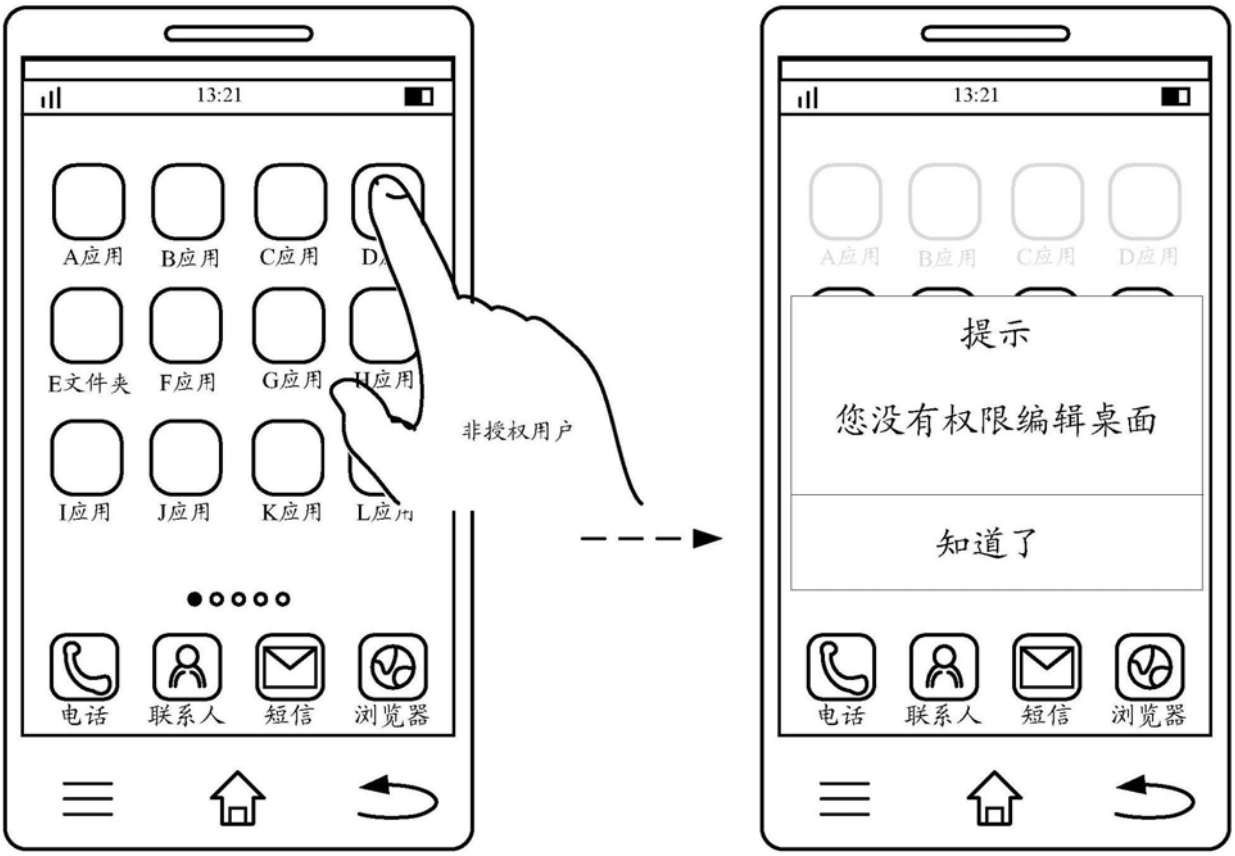

13:21
A应用
B应用
C应用
E文件夹
F应用
G应用
I应用
J应用
K应用
电话
联系人
短信
浏览器
非授权用户
13:21
提示
您没有权限编辑桌面
知道了
电话
联系人
短信
浏览器

图3

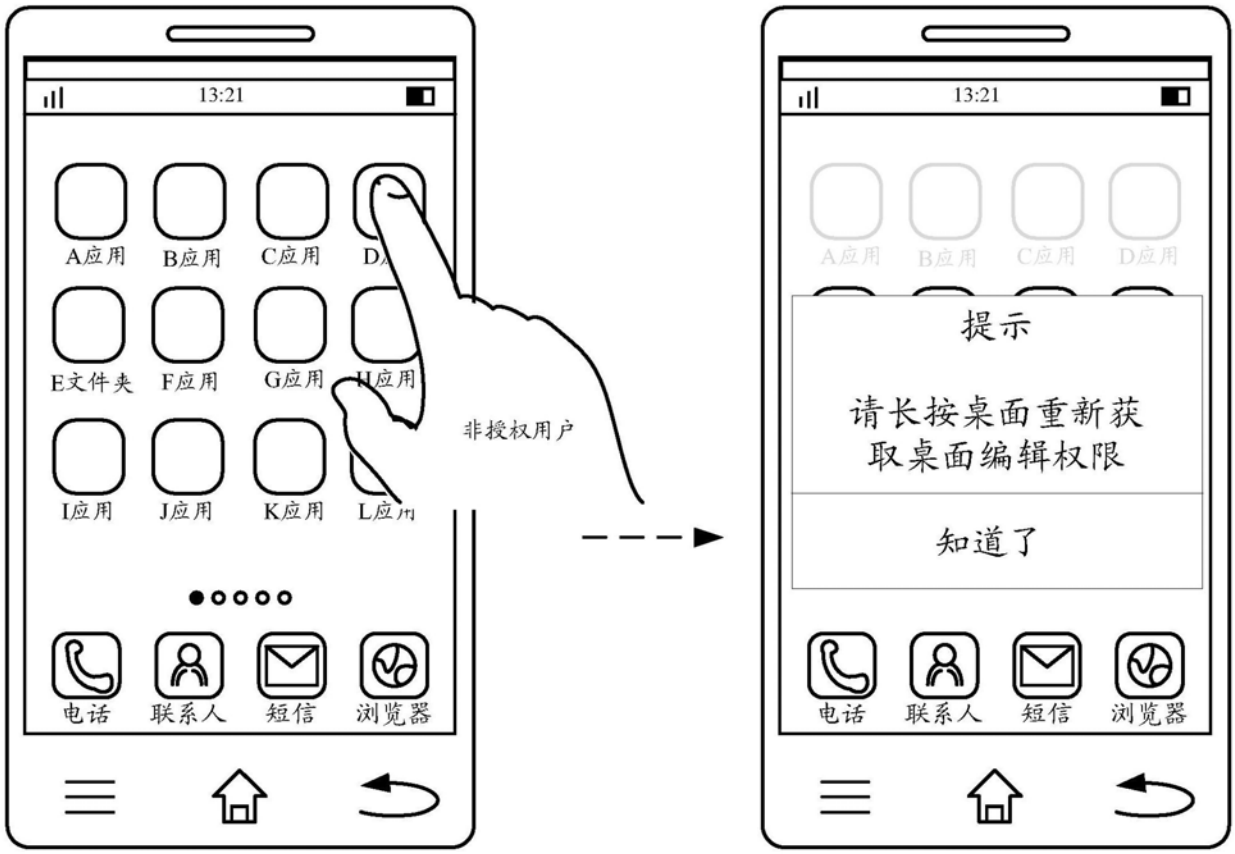

13:21
A应用
B应用
C应用
E文件夹
F应用
G应用
I应用
J应用
K应用
电话
联系人
短信
浏览器
非授权用户
13:21
提示
请长按桌面重新获取桌面编辑权限
知道了
电话
联系人
短信
浏览器

图4

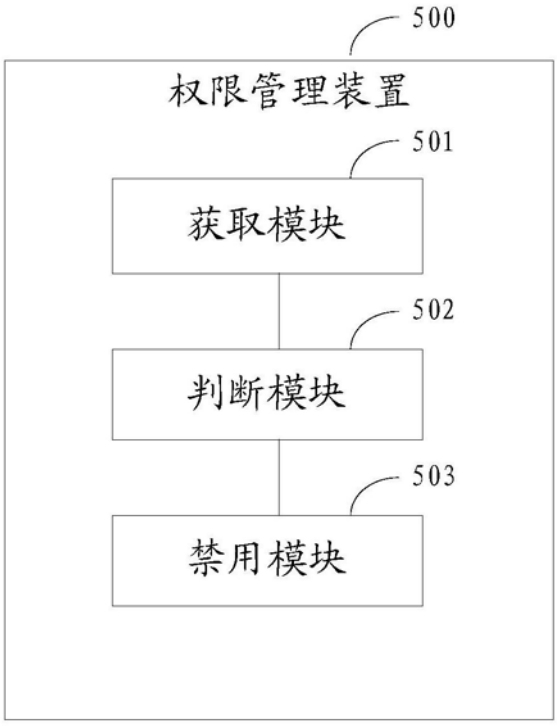

500
权限管理装置
501
获取模块
502
判断模块
503
禁用模块

图5

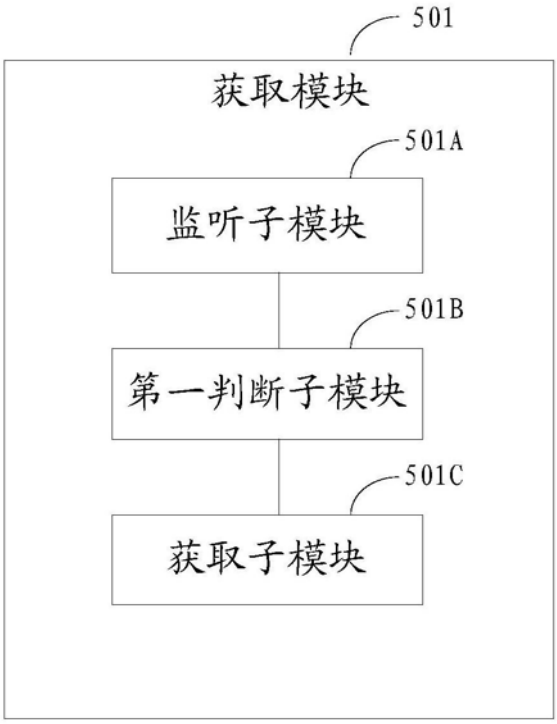


图6

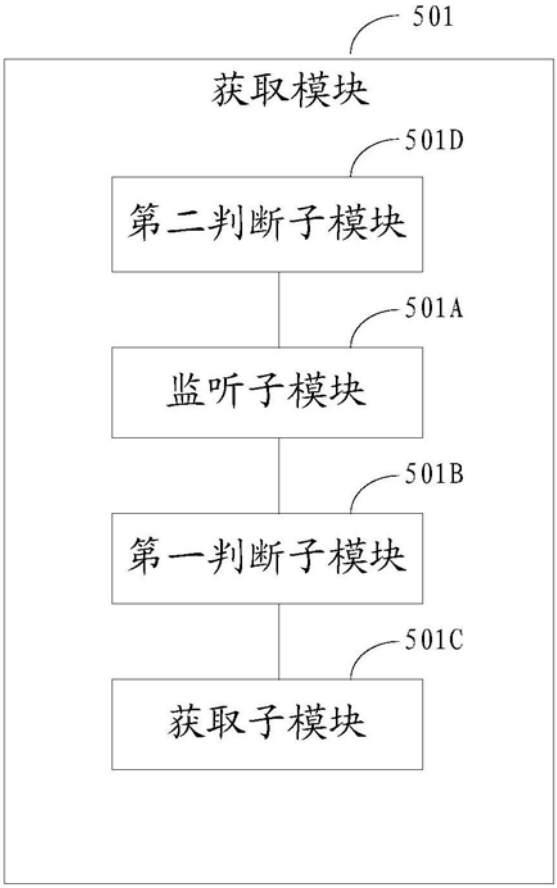

501
获取模块
501D
第二判断子模块
501A
监听子模块
501B
第一判断子模块
501C
获取子模块

图7

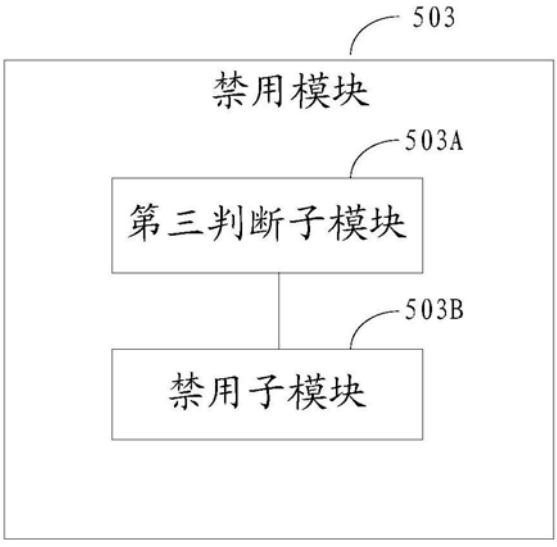

503
禁用模块
503A
第三判断子模块
503B
禁用子模块

图8

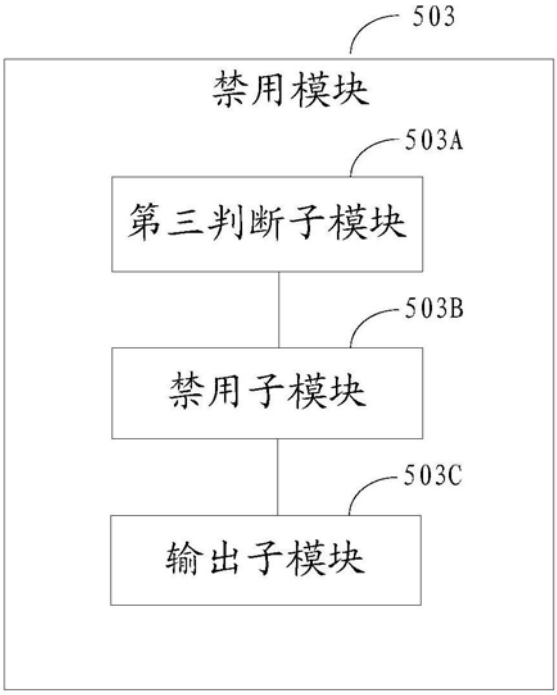


图9

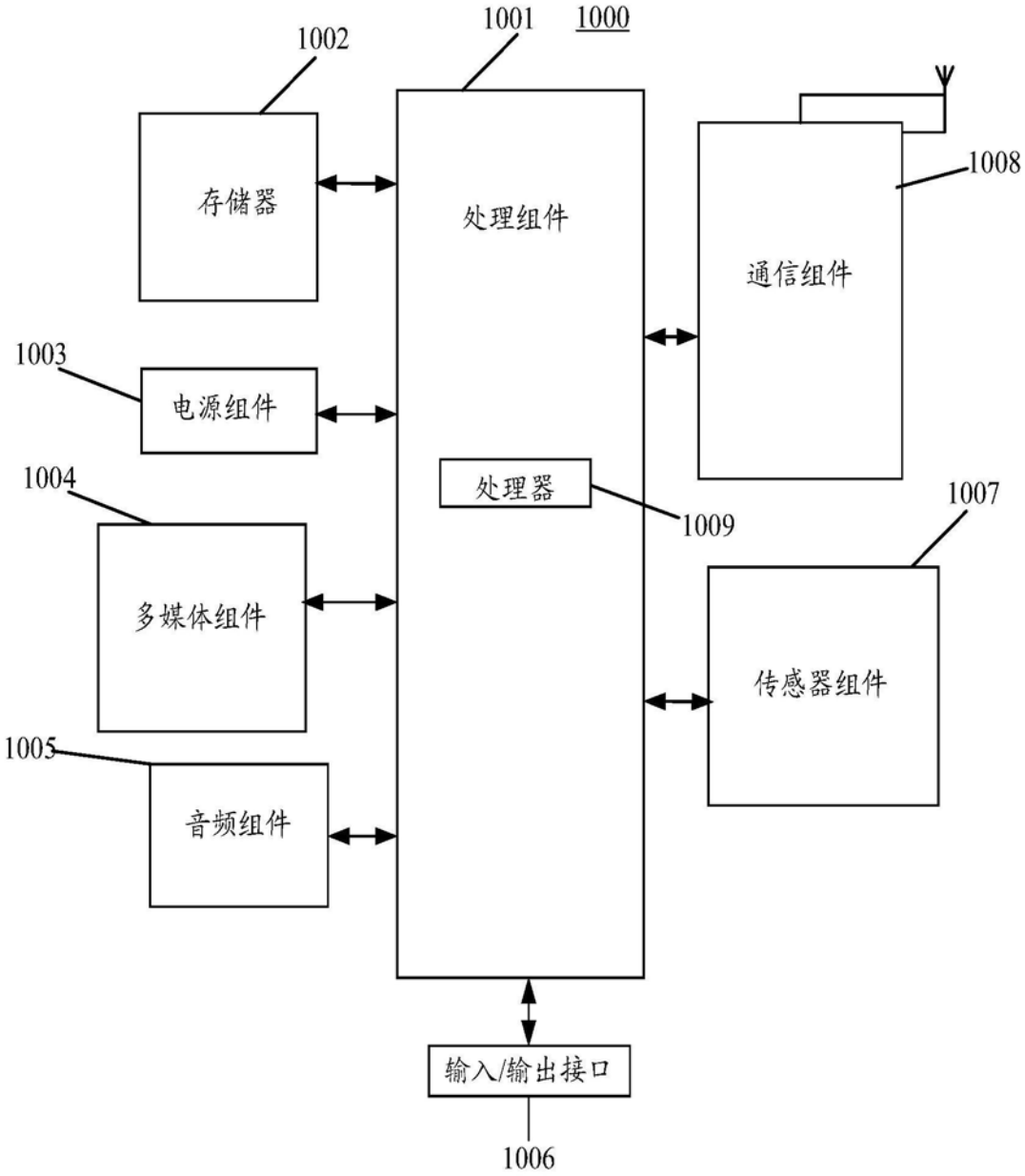

1001
1000
1002
存储器
处理组件
1008
通信组件
1003
电源组件
处理器
1009
1004
1007
多媒体组件
传感器组件
1005
音频组件
输入/输出接口
1006

图10