

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2016 年 11 月 3 日 (03.11.2016)



(10) 国际公布号
WO 2016/173245 A1

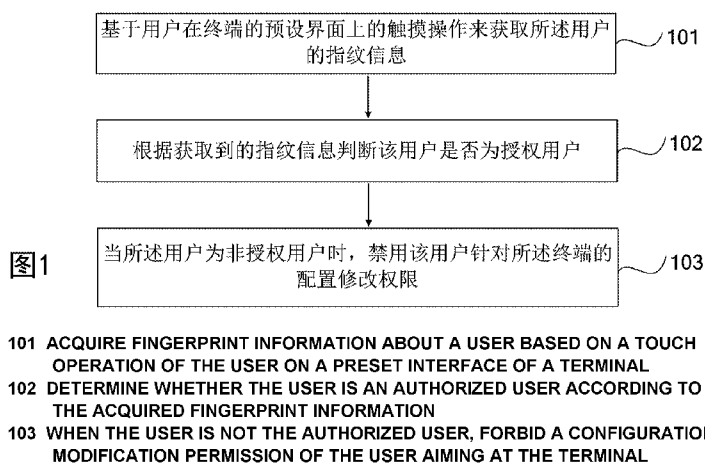
- (51) 国际专利分类号:
G06F 3/0487 (2013.01) G06F 21/32 (2013.01)
- (21) 国际申请号: PCT/CN2015/095158
- (22) 国际申请日: 2015 年 11 月 20 日 (20.11.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510209637.6 2015 年 4 月 28 日 (28.04.2015) CN
- (71) 申请人: 小米科技有限责任公司 (XIAOMI INC.)
[CN/CN]; 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层, Beijing 100085 (CN)。
- (72) 发明人: 陈巧卓 (CHEN, Qiaozhuo); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。朱印 (ZHU, Yin); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。李文昕 (LI, Wenxin); 中国北京市海淀区清河中街 68 号华润五彩城购物中心二期 13 层由小米科技有限责任公司转交, Beijing 100085 (CN)。

- (74) 代理人: 北京律智知识产权代理有限公司 (BEIJING INTELLEGAL INTELLECTUAL PROPERTY AGENT LTD.); 中国北京市朝阳区慧忠路 5 号远大中心 B 座 1802、1803、1805, Beijing 100101 (CN)。
- (81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。
- (84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: PERMISSION MANAGEMENT METHOD AND DEVICE

(54) 发明名称: 权限管理方法和装置



(57) Abstract: The present disclosure provides a permission management method. The method comprises: acquiring fingerprint information about a user based on a touch operation of the user on a preset interface of a terminal; determining whether the user is an authorized user according to the acquired fingerprint information; and when the user is not the authorized user, forbidding a configuration modification permission of the user aiming at the terminal. The present disclosure can realize the situation that a nonlocal user cannot obtain a permission for modifying configuration of a terminal when using the terminal of a user, thereby increasing the safety of using the terminal.

(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。



WO 2016/173245 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

权限管理方法和装置

本申请基于申请号为 201510209637.6、申请日为 2015 年 4 月 28 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参
5 考。

技术领域

本公开涉及通讯领域，尤其涉及权限管理方法和装置。

10 背景技术

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

- 15 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。
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：
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。
- 20 可选的，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
25 位置获取所述用户的指纹信息。
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：
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。
可选的，所述预设界面包括所述终端的屏幕的可见区域。
- 30 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：
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
35 的配置修改权限。

可选的，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。

5 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。

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：

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；

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；

10 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。

可选的，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；

15 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。

可选的，所述获取模块还包括：

20 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。

可选的，所述预设界面包括所述终端的屏幕的可见区域。

可选的，所述禁用模块包括：

25 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。

可选的，所述禁用模块还包括：

30 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。

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。

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：

处理器；

35 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：

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；

5 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：

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。

10 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

15 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。

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；

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；

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；

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；

20 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；

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；

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；

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；

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；

25 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

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
30 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。

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。
35

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”。

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。

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：

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；

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。

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；

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。

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。

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。

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。

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。

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。

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。

5 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。

10 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。

15 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。

20 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。

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。

25 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。

30 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。

35 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。

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。

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。

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。

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。

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。

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。

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：

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；

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。

5 在步骤 202 中，判断监听到的触摸事件是否为长按事件；

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；

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；

10 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；

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。

15 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。

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。

20 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。

25 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。

30 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。

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。

35 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。

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
5 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。

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。

10 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。

15 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。

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
20 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。

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
25 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。

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
30 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。

35 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。

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。

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。

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。

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。

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。

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。

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。

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：

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；

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；

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。

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。

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:

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;

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;

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。

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:

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。

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。

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。

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。

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:

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;

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。

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。

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。

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：

所述输出子模块 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，
5 通过所述预设界面向用户输出提示消息。

在以上各实施例中，所述配置修改权限包括移动应用图标权限、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。

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。

10 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。

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
15 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。

相应的，本公开还提供一种权限管理装置，所述装置包括：

处理器；

20 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：

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。

25 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：

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；

30 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。

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。

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。

35 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。

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。

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。

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。

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。

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。

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。

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。

- 5 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）
10 技术，超宽带（UWB）技术，蓝牙（BT）技术和其他技术来实现。

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。

- 15 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。

- 20 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：

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。

- 25 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。

- 30 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。

权利要求

1、一种权限管理方法，其特征在于，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；

5 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。

2、如权利要求 1 所述的方法，其特征在于，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；

10 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。

3、如权利要求 2 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；

15 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。

4、如权利要求 1~3 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。

5、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：

20 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。

6、如权利要求 5 所述的方法，其特征在于，所述方法还包括：

25 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。

7、如权利要求 1 或 5 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。

30 8、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；

35 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。

9、如权利要求 8 所述的装置，其特征在于，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；

5 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。

10、如权利要求 9 所述的装置，其特征在于，所述获取模块还包括：

10 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。

11、如权利要求 8~10 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。

12、如权利要求 8 所述的装置，其特征在于，所述禁用模块包括：

15 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。

13、如权利要求 12 所述的装置，其特征在于，所述禁用模块还包括：

20 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。

14、如权利要求 8 或 12 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。

15、一种权限管理装置，其特征在于，包括：

25 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：

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；

30 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。

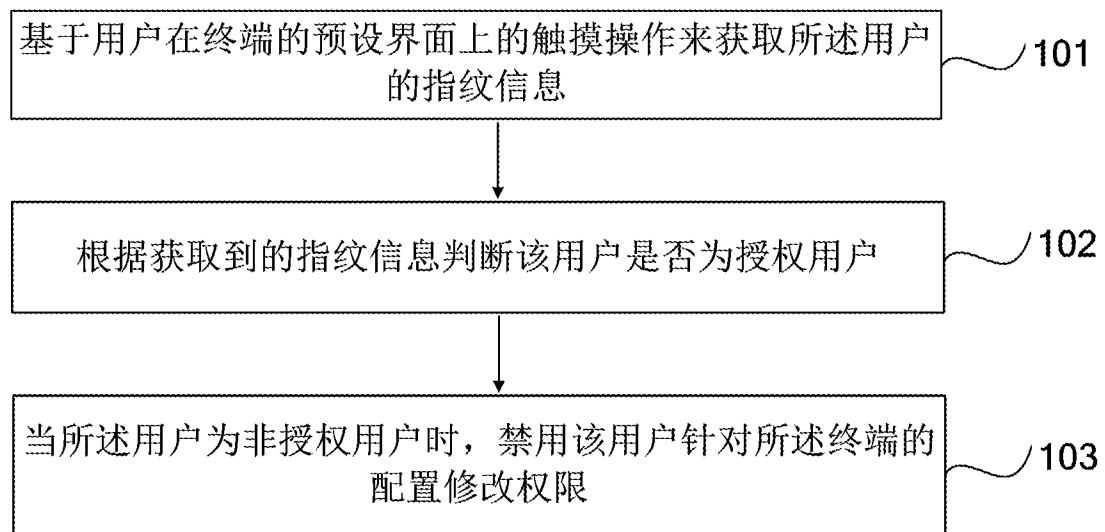


图1

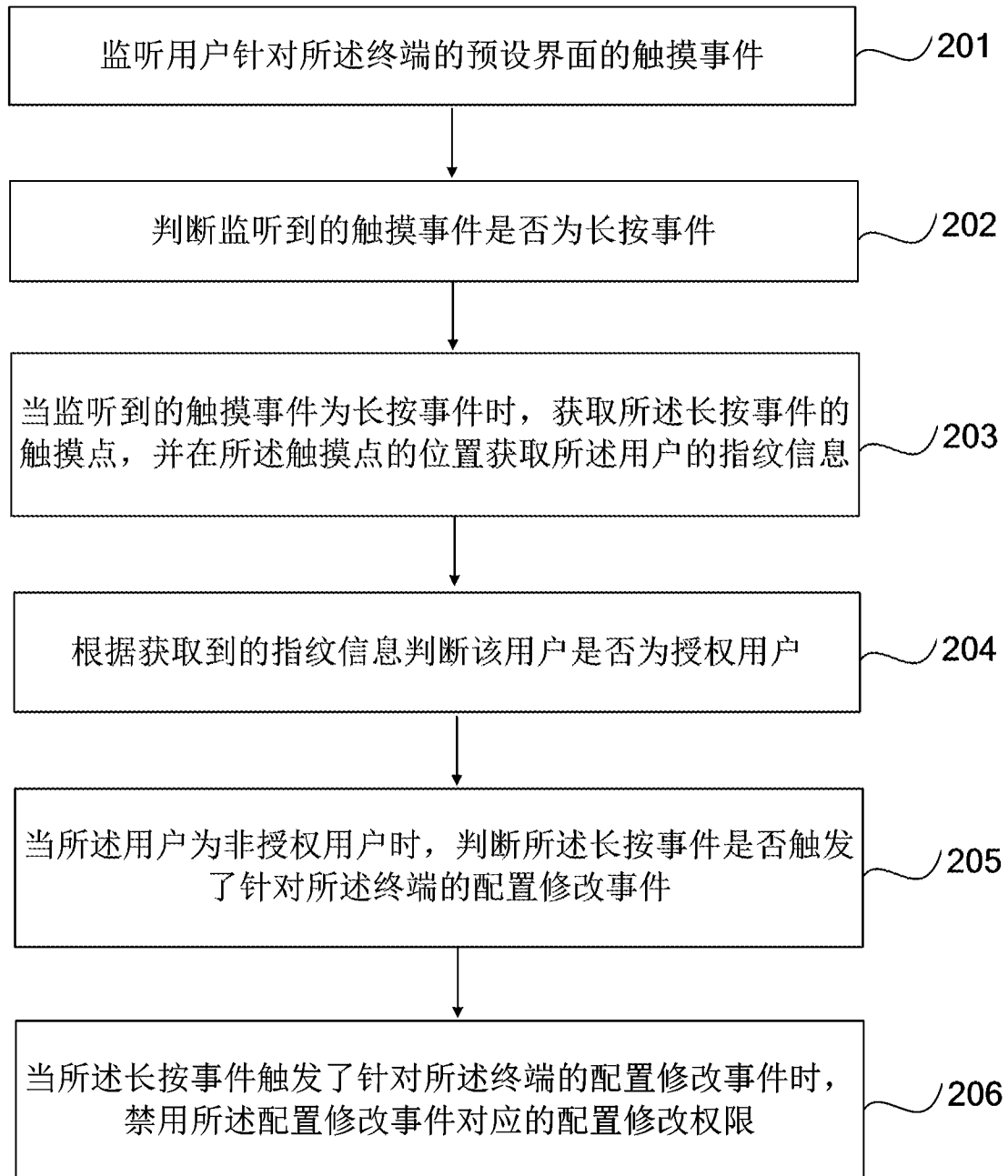


图2

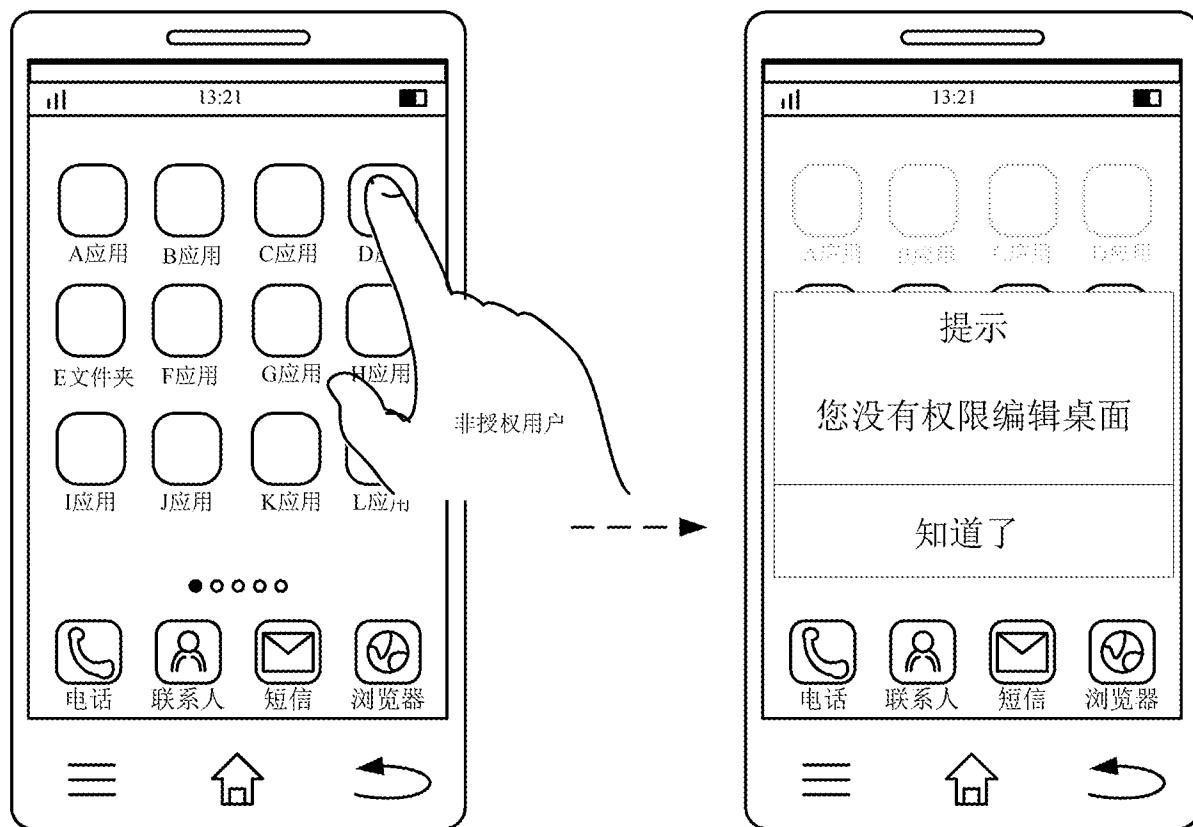


图3

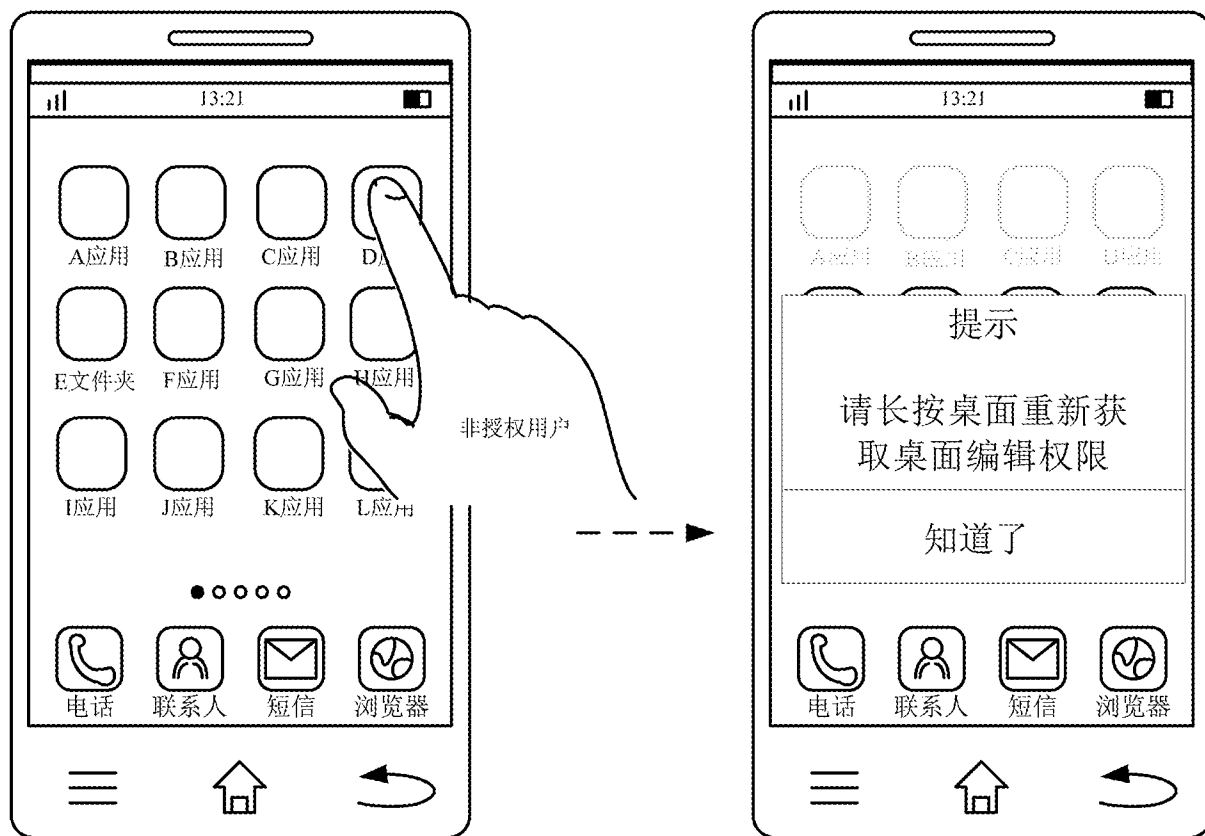


图4

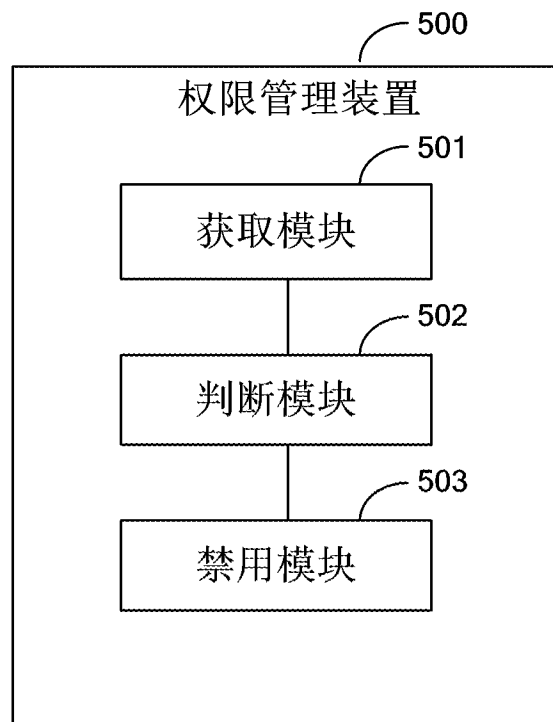


图5

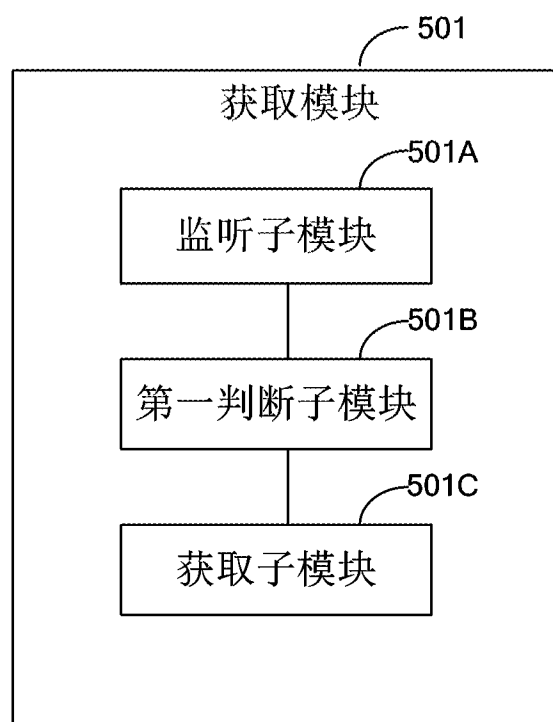


图6

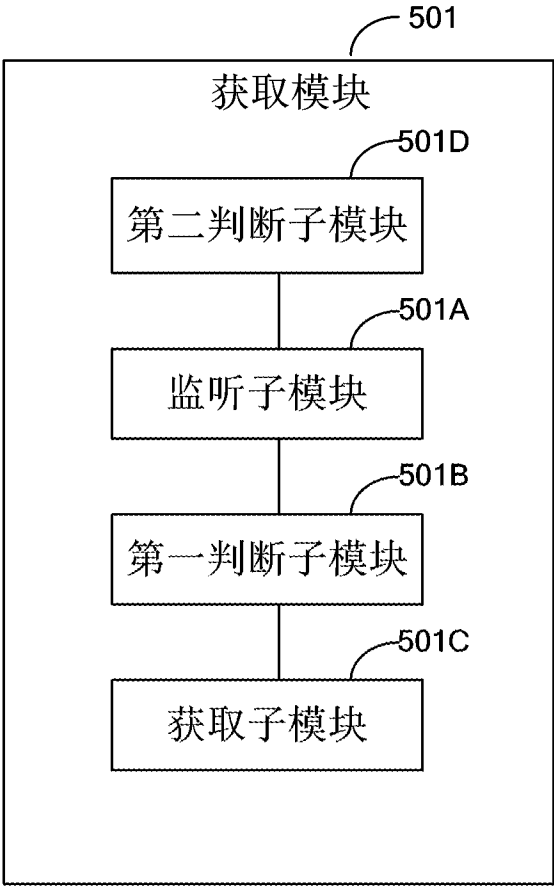


图7

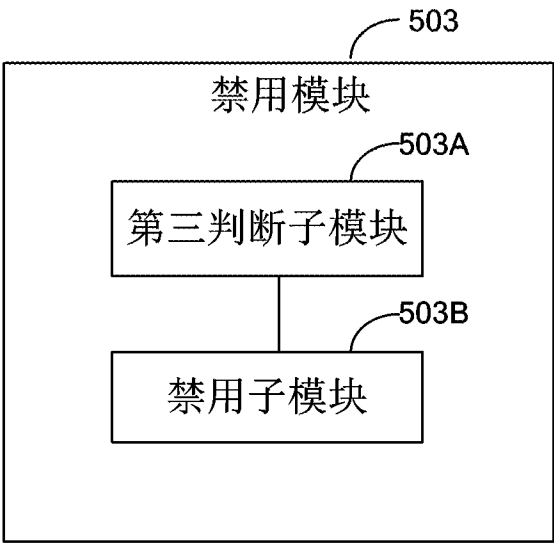


图8

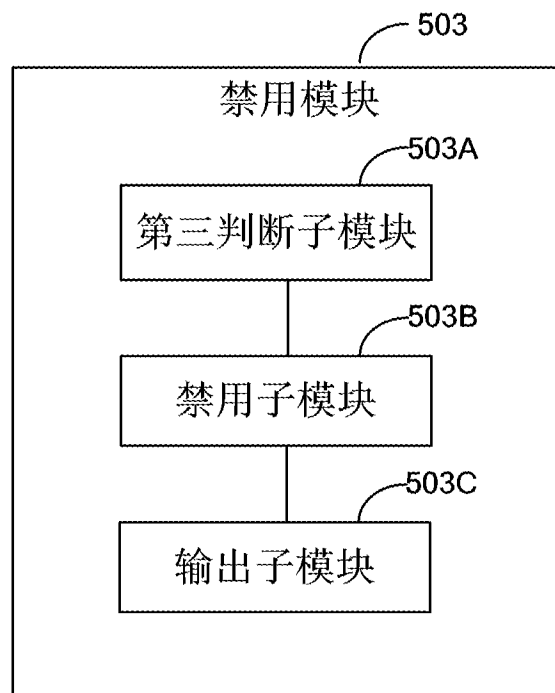


图9

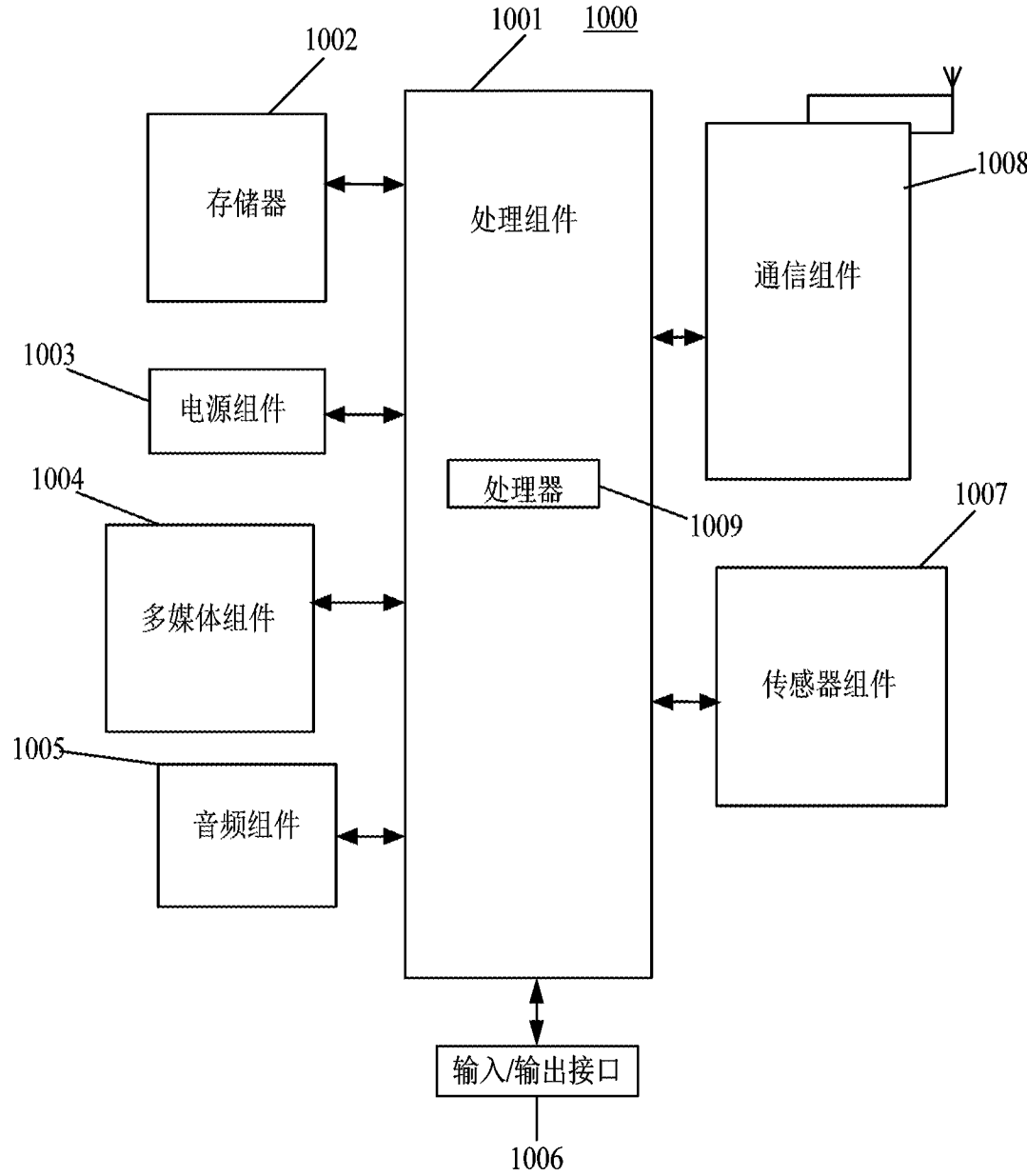


图10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/095158

A. CLASSIFICATION OF SUBJECT MATTER

G06F 3/0487 (2013.01) i; G06F 21/32 (2013.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRS, CNKI, WPI, EPODOC: authority, user, terminal, touch, fingerprint, authorize, forbid, configuration, modification, long press

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104765552 A (XIAOMI TECHNOLOGY CO., LTD.), 08 July 2015 (08.07.2015), claims 1-15	1-15
Y	CN 103577739 A (QINGDAO SHANGHUI INFORMATION TECHNOLOGY CO., LTD.), 12 February 2014 (12.02.2014), description, paragraphs 0025-0059	1-15
Y	CN 103488924 A (XIAOMI TECHNOLOGY CO., LTD.), 01 January 2014 (01.01.2014), description, paragraphs 0083-0116	1-15
Y	CN 104469717 A (GUANG DONG OPPO MOBILE TELECOMMUNICATIONS CO., LTD.), 25 March 2015 (25.03.2015), claim 1	2, 3, 4, 9, 10, 11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
07 February 2016 (07.02.2016)

Date of mailing of the international search report
23 February 2016 (23.02.2016)

Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer
DENG, Qian
Telephone No.: (86-10) **62411669**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/095158

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104765552 A	08 July 2015	None	
CN 103577739 A	12 February 2014	None	
CN 103488924 A	01 January 2014	MX 2014008738 A	28 May 2015
		EP 2854071 A2	01 April 2015
		EP 2854071 A3	01 July 2015
		KR 20150046766 A	30 April 2015
		WO 2015043193 A1	02 April 2015
		JP 2015534405 W	26 November 2015
		US 2015089631 A1	26 March 2015
CN 104469717 A	25 March 2015	None	

国际检索报告

国际申请号

PCT/CN2015/095158

A. 主题的分类 G06F 3/0487(2013.01)i; G06F 21/32(2013.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类		
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) G06F 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CPRS, CNKI, WPI, EPDOC: 权限, 用户, 终端, 触摸, 指纹, 授权, 禁用, 禁止, 配置, 修改, 长按, authority, user, terminal, touch, fingerprint, authorize, forbid, configuration, modification, long press		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 104765552 A (小米科技有限责任公司) 2015年 7月 8日 (2015 - 07 - 08) 权利要求1-15	1-15
Y	CN 103577739 A (青岛尚慧信息技术有限公司) 2014年 2月 12日 (2014 - 02 - 12) 说明书第0025-0059段	1-15
Y	CN 103488924 A (小米科技有限责任公司) 2014年 1月 1日 (2014 - 01 - 01) 说明书第0083-0116段	1-15
Y	CN 104469717 A (广东欧珀移动通信有限公司) 2015年 3月 25日 (2015 - 03 - 25) 权利要求1	2, 3, 4, 9, 10, 11
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2016年 2月 7日	国际检索报告邮寄日期 2016年 2月 23日	
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	授权官员 邓茜 电话号码 (86-10)62411669	

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/095158

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	104765552	A	2015年 7月 8日	无			
CN	103577739	A	2014年 2月 12日	无			
CN	103488924	A	2014年 1月 1日	MX	2014008738	A	2015年 5月 28日
				EP	2854071	A2	2015年 4月 1日
				EP	2854071	A3	2015年 7月 1日
				KR	20150046766	A	2015年 4月 30日
				WO	2015043193	A1	2015年 4月 2日
				JP	2015534405	W	2015年 11月 26日
				US	2015089631	A1	2015年 3月 26日
CN	104469717	A	2015年 3月 25日	无			