(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106407790 A
(43)申请公布日 2017.02.15

(21)申请号 201610843590.3

(22)申请日 2016.09.22

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 张灿灿 郑午辰

(74)专利代理机构 北京市立方律师事务所 11330
代理人 王增鑫

(51)Int.Cl.
G06F 21/36(2013.01)
G06F 21/44(2013.01)

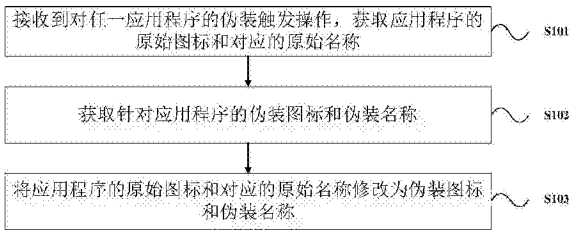
权利要求书1页 说明书9页 附图2页

(54)发明名称

应用程序的隐私保护方法和隐私保护装置

(57)摘要

本发明提供了一种应用程序的隐私保护方法和隐私保护装置，该隐私保护方法包括：接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称；获取针对应用程序的伪装图标和伪装名称；将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称。本发明的技术方案实现了在终端设备的屏幕中对应用程序的标识信息的伪装，使得终端设备的屏幕在解锁的情况下，依然可以保证应用程序对于用户的较强隐私性，防止应用程序不被除终端用户之外的第二人所使用，从而有效地保护应用程序中用户数据的隐私安全，使得用户的体验度得到提高。



CN 106407790 A

1.一种应用程序的隐私保护方法，其特征在于，包括：

接收到对任一应用程序的伪装触发操作，获取所述应用程序的原始图标和对应的原始名称；

获取针对所述应用程序的伪装图标和伪装名称；

将所述应用程序的原始图标和对应的原始名称修改为所述伪装图标和所述伪装名称。

2.根据权利要求1所述的方法，其特征在于，接收到对任一应用程序的伪装触发操作，获取所述应用程序的原始图标和对应的原始名称，包括：

基于接收到的伪装触发操作指向应用程序的包名，获取所述应用程序的原始图标和对应的原始名称。

3.根据权利要求1或2所述的方法，其特征在于，所述应用程序为基于沙箱隔离技术针对原生应用程序创建的分身应用程序。

4.根据权利要求1-3任一项所述的方法，其特征在于，获取针对所述应用程序的伪装图标和伪装名称，包括以下至少一种情形：

基于用户针对所述应用程序选择的图像信息，生成相应的应用程序的伪装图标；

将用户针对所述应用程序输入的应用名称作为该应用程序的伪装名称；

基于所述用户程序的包名，确定与所述用户程序相应的预配置的伪装图标和伪装名称。

5.根据权利要求1-4任一项所述的方法，其特征在于，还包括：

删除用户界面中所述应用程序的原始图标和对应的原始名称，并添加所述伪装图标和所述伪装名称作为所述应用程序的快捷图标标识。

6.根据权利要求1-5任一项所述的方法，其特征在于，还包括：

删除用户界面中应用程序的所述伪装图标和所述伪装名称，并添加所述原始图标和对应的原始名称作为所述应用程序的快捷图标标识。

7.根据权利要求1-6任一项所述的方法，其特征在于，还包括：

基于允许修改应用程序的原始图标和对应的原始名称的系统权限，创建应用程序的白名单；

当任一应用程序不在所述白名单内，则不能对应用程序修改其原始图标和对应的原始名称。

8.一种应用程序的隐私保护装置，其特征在于，包括：

接收模块，用于接收到对任一应用程序的伪装触发操作，获取所述应用程序的原始图标和对应的原始名称；

获取模块，用于获取针对所述应用程序的伪装图标和伪装名称；

修改模块，用于将所述应用程序的原始图标和对应的原始名称修改为所述伪装图标和所述伪装名称。

9.根据权利要求8所述的装置，其特征在于，所述接收模块，用于基于接收到的伪装触发操作指向应用程序的包名，获取所述应用程序的原始图标和对应的原始名称。

10.根据权利要求8或9所述的装置，其特征在于，所述应用程序为基于沙箱隔离技术针对原生应用程序创建的分身应用程序。

应用程序的隐私保护方法和隐私保护装置

技术领域

[0001] 本发明涉及终端设备技术领域，具体而言，本发明涉及一种应用程序的隐私保护方法和一种应用程序的隐私保护装置。

背景技术

[0002] 互联网已经进入到了成熟的时代，而网络与用户之间的交流越来越受到重视，使得智能移动终端逐渐成为绝大部分网民的必备品，相应的各种各样的应用程序也应运而生。但是由于现有的应用程序的快捷图标一般均直接显示在移动终端的主界面中，没有过多的安全防护措施，因此，存在着应用程序可能被其他人打开浏览或操作而导致的用户隐私泄露的安全性问题。

[0003] 在现有技术中，为了解决上述所存在的问题，通常采用通过对移动终端操作系统设置密码的方式来阻止恶意使用及查看移动终端的应用程序，从而保护应用程序的私密性；但如果移动终端处于解锁状态时，应用程序被一直暴露在其主界面中，若此时移动终端被其他人获取到，则依然存在无法保证移动终端的隐私安全。

发明内容

[0004] 为克服上述技术问题或者至少部分地解决上述技术问题，特提出以下技术方案：

[0005] 本发明的实施例提出了一种应用程序的隐私保护方法，包括：

[0006] 接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称；

[0007] 获取针对应用程序的伪装图标和伪装名称；

[0008] 将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称。

[0009] 优选地，接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称，包括：

[0010] 基于接收到的伪装触发操作指向应用程序的包名，获取应用程序的原始图标和对应的原始名称。

[0011] 优选地，应用程序为基于沙箱隔离技术针对原生应用程序创建的分身应用程序。

[0012] 优选地，获取针对应用程序的伪装图标和伪装名称，包括以下至少一种情形：

[0013] 基于用户针对应用程序选择的图像信息，生成相应的应用程序的伪装图标；

[0014] 将用户针对应用程序输入的应用名称作为该应用程序的伪装名称；

[0015] 基于用户程序的包名，确定与用户程序相应的预配置的伪装图标和伪装名称。

[0016] 优选地，该隐私保护方法还包括：

[0017] 删除用户界面中应用程序的原始图标和对应的原始名称，并添加伪装图标和伪装名称作为应用程序的快捷图标标识。

[0018] 优选地，该隐私保护方法还包括：

[0019] 删除用户界面中应用程序的伪装图标和伪装名称，并添加原始图标和对应的原始

名称作为应用程序的快捷图标标识。

[0020] 优选地，该隐私保护方法还包括：

[0021] 基于允许修改应用程序的原始图标和对应的原始名称的系统权限，创建应用程序的白名单；

[0022] 当任一应用程序不在白名单内，则不能对应用程序修改其原始图标和对应的原始名称。

[0023] 本发明的另一实施例提出了一种应用程序的隐私保护装置，包括：

[0024] 接收模块，用于接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称；

[0025] 获取模块，用于获取针对应用程序的伪装图标和伪装名称；

[0026] 修改模块，用于将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称。

[0027] 优选地，接收模块，用于基于接收到的伪装触发操作指向应用程序的包名，获取应用程序的原始图标和对应的原始名称。

[0028] 优选地，应用程序为基于沙箱隔离技术针对原生应用程序创建的分身应用程序。

[0029] 优选地，获取针对应用程序的伪装图标和伪装名称，包括以下至少一种情形：

[0030] 基于用户针对应用程序选择的图像信息，生成相应的应用程序的伪装图标；

[0031] 将用户针对应用程序输入的应用名称作为该应用程序的伪装名称；

[0032] 基于用户程序的包名，确定与用户程序相应的预配置的伪装图标和伪装名称。

[0033] 优选地，该隐私保护装置还包括：

[0034] 删除模块，用于删除用户界面中应用程序的原始图标和对应的原始名称，并添加伪装图标和伪装名称作为应用程序的快捷图标标识。

[0035] 优选地，该隐私保护装置还包括：

[0036] 第二删除模块，用于删除用户界面中应用程序的伪装图标和伪装名称，并添加原始图标和对应的原始名称作为应用程序的快捷图标标识。

[0037] 优选地，该隐私保护装置还包括：

[0038] 白名单创建模块，用于基于允许修改应用程序的原始图标和对应的原始名称的系统权限，创建应用程序的白名单；

[0039] 当任一应用程序不在白名单内，则不能对应用程序修改其原始图标和对应的原始名称。

[0040] 本发明的技术方案中，获取应用程序的原始图标和对应的原始名称；基于获取到的应用程序的伪装图标和伪装名称；将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称，实现了在终端设备的屏幕中对应用程序的标识信息的伪装，使得终端设备的屏幕在解锁的情况下，依然可以保证应用程序对于用户的较强隐私性，防止应用程序不被除终端用户之外的第二人所使用，从而有效地保护应用程序中用户数据的隐私安全，使得用户的体验度得到提高。

[0041] 本发明附加的方面和优点将在下面的描述中部分给出，这些将从下面的描述中变得明显，或通过本发明的实践了解到。

附图说明

[0042] 本发明上述的和/或附加的方面和优点从下面结合附图对实施例的描述中将变得明显和容易理解，其中：

[0043] 图1为本发明一个实施例的应用程序的隐私保护方法的流程示意图；

[0044] 图2为本发明的一个优选实施例的用于对应用程序的标识信息进行伪装的用户界面的示意图；

[0045] 图3为本发明的另一个优选实施例的对应用程序的标识信息进行伪装的编辑界面示意图；

[0046] 图4为本发明的后一个实施例的应用程序的隐私保护装置的结构框架示意图。

具体实施方式

[0047] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能解释为对本发明的限制。

[0048] 本技术领域技术人员可以理解，除非特意声明，这里使用的单数形式“一”、“一个”、“所述”和“该”也可包括复数形式。应该进一步理解的是，本发明的说明书中使用的措辞“包括”是指存在所述特征、整数、步骤、操作、元件和/或组件，但是并不排除存在或添加一个或多个其他特征、整数、步骤、操作、元件、组件和/或它们的组。应该理解，当我们称元件被“连接”或“耦接”到另一元件时，它可以直接连接或耦接到其他元件，或者也可以存在中间元件。此外，这里使用的“连接”或“耦接”可以包括无线连接或无线耦接。这里使用的措辞“和/或”包括一个或更多个相关联的列出项的全部或任一单元和全部组合。

[0049] 本技术领域技术人员可以理解，除非另外定义，这里使用的所有术语(包括技术术语和科学术语)，具有与本发明所属领域中的普通技术人员的一般理解相同的意义。还应该理解的是，诸如通用字典中定义的那些术语，应该被理解为具有与现有技术的上下文中的意义一致的意义，并且除非像这里一样被特定定义，否则不会用理想化或过于正式的含义来解释。

[0050] 需要说明的是，本发明实施例是基于移动终端操作系统实现的，移动终端操作系统是基于Linux操作系统自由及开放源代码的操作系统，例如，Android系统。

[0051] 图1为本发明一个实施例的应用程序的隐私保护方法的流程示意图。

[0052] 步骤S101：接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称；步骤S102：获取针对应用程序的伪装图标和伪装名称；步骤S103：将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称。

[0053] 本发明的技术方案中，获取应用程序的原始图标和对应的原始名称；基于获取到的应用程序的伪装图标和伪装名称；将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称，实现了在终端设备的屏幕中对应用程序的标识信息的伪装，使得终端设备的屏幕在解锁的情况下，依然可以保证应用程序对于用户的较强隐私性，防止应用程序不被除终端用户之外的第二人所使用，从而有效地保护应用程序中用户数据的隐私安全，使得用户的体验度得到提高。

[0054] 以下针对各个步骤的具体实现做进一步的说明：

[0055] 本领域技术人员应当可以预见，由于本发明所揭示的技术涉及到对Android系统级别资源的调用，因而，在实施本发明前需要获取系统的Root权限，即系统管理员操作权限。

[0056] 众所周知，Root权限是指Unix类操作系统(包括Linux、Android)的系统管理员权限，类似于Windows(视窗)系统中的Administrator(管理员)权限；Root权限可以访问和修改用户的移动设备中几乎所有的文件(Android系统文件及用户文件，不包括ROM)。但是，由于目前移动终端系统对于Root权限的管理是非常严格的，通常情况下多数应用或程序都不具备Root权限，因此对于某些需要具备Root权限的操作就无法执行，例如安装或卸载应用等操作；同时，此类操作调用进程每次执行相应操作时都需要向系统申请Root权限，但如果此时其他应用进程正在使用Root权限进行相关操作，则此调用进程的Root权限申请便无法成功；更甚者，如果用户在系统中设置了禁用Root权限的操作，则相关调用进程便无法进行相关操作。

[0057] 基于此，本发明提出只需要向系统发送一次Root权限获取请求，具体可通过调用系统内置的SU(Super User，超级用户)命令获取Root权限，或者通过获取具有Root权限的shell获取Root权限并在shell中启动进程，然后在获取所述系统的Root权限授权后，即可使后续其他调用进程需执行相关操作时无需重复申请Root权限；具体Root权限获取过程可参照现有技术的Root权限调用函数，本发明在此不再赘述。

[0058] 可以看出，Root权限的获取方式，从权限作用的生命周期来看，包括永久Root权限和临时Root权限，顾名思义，永久Root权限情况下，应用程序一经Root授权，以后可不必再进行Root提权操作；而临时Root权限情况下，权限作用的生命周期只是操作系统的一次从开机到关机的过程，下次开机依然需要进行Root。本发明的实现不受这种分类限制。

[0059] 当然，本领域关于Root提权的技术实施方式多种多样，因而，请注意，本发明的方法和装置的实施，虽有赖于已获Root权限，但并不受限于获取Root授权的具体实施方式。

[0060] 步骤S101：接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称。

[0061] 具体地，接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称，具体包括：基于接收到的伪装触发操作指向应用程序的包名，获取应用程序的原始图标和对应的原始名称。

[0062] 其中，应用程序为基于沙箱隔离技术针对原生应用程序创建的分身应用程序。

[0063] 原生应用程序包括但不限于：通过安装包直接安装在移动终端系统中的应用程序。

[0064] 例如，应用图标的应用程序“微信”，其是通过原生应用程序“微信”，基于沙箱隔离技术创建的分身应用程序，该分身应用程序“微信”能够实现原生应用程序“微信”的功能，方便用户在同一个移动终端系统中，进行该应用程序“微信”账号的切换。

[0065] 此处需要说明的是，通过沙箱隔离技术创建分身应用程序的过程是本领域较为成熟的现有技术，在此就不再赘述。

[0066] 还需要说明的是，任一应用程序在安装时，Android系统会通过其提供的应用程序包管理Package Manager类，来获取安装的各个应用程序的相关信息，应用程序的相关信息

包括图标、名称、版本号、包名等信息，随后将应用程序的包名与图标、名称、版本号等信息相关联地存储在应用程序信息列表中。

[0067] 例如，用户通过点击Android系统中提供的用于对应用程序的标识信息进行伪装的用户界面，图2示出了本发明的一个优选实施例的用于对应用程序的标识信息进行伪装的用户界面的示意图；用户通过点击用户界面上的“图标伪装”按钮，进入进行“图标伪装”的“编辑界面”，如图3所示，“编辑界面”中显示了多个可选的应用程序名称，供用户选择。用户在“编辑界面”中选择其希望进行伪装的应用程序；当“编辑界面”中未显示用户需要伪装的应用程序，则用户可以将其需要伪装的应用程序导入到该编辑界面中，从而对需要伪装的应用程序进行伪装。用户在“编辑界面”中选择其需要伪装的应用程序，如通过点击应用程序“微信”对应的“编辑”按钮，即执行伪装触发操作，则响应于该伪装触发操作获取“微信”的包名com.tencent.mm，并基于包名com.tencent.mm在预存的应用程序信息列表中查询以确定与com.tencent.mm对应的原始图标和对应的原始名称“微信”。

[0068] 步骤S102：获取针对应用程序的伪装图标和伪装名称。

[0069] 其中，获取针对应用程序的伪装图标和伪装名称，包括以下至少一种情形：基于用户针对应用程序选择的图像信息，生成相应的应用程序的伪装图标；将用户针对应用程序输入的应用名称作为该应用程序的伪装名称；基于用户程序的包名，确定与用户程序相应的预配置的伪装图标和伪装名称。

[0070] 具体地，基于用户针对应用程序选择的图像信息来获取应用程序的伪装图标方式包括：为用户提供上传图片或网络链接的交互接口，通过交互接口用户上传移动终端的本地图片或者网络图片链接，来获取到用户自定义的图片，并将该图片进行处理并封装为符合预定义图标标准的伪装图标。

[0071] 基于将用户针对应用程序输入的应用名称，获取应用程序的伪装名称的方式包括：为用户提供用于输入伪装名称的交互接口，通过交互接口用户输入伪装名称。

[0072] 基于应用程序的包名，确定与用户程序相应的预配置的伪装图标和伪装名称的方式包括：预存有符合应用程序图标标准的多个伪装图标，且预先配置应用程序的包名与预存的伪装图标之间的对应关系；当用户触发对任一应用程序的伪装触发操作时，可基于应用程序的包名从预存的多个伪装图标中确定与该包名对应的伪装图标。

[0073] 步骤S103：将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称。

[0074] 具体地，在已获取到系统管理员权限的情况下，即获取系统的Root权限后，根据确定的伪装图标和伪装名称，将需要伪装的应用程序的原始图标和对应的原始名称修改为确定的伪装图标和伪装名称；当需要伪装的应用程序已经伪装过，则将其当前的伪装图标和伪装名称修改为重新确定后的伪装图标和伪装名称。

[0075] 该隐私保护方法还包括：删除用户界面中应用程序的原始图标和对应的原始名称，并添加伪装图标和伪装名称作为应用程序的快捷图标标识。该隐私保护方法还包括：删除用户界面中应用程序的伪装图标和伪装名称，并添加原始图标和对应的原始名称作为应用程序的快捷图标标识。

[0076] 需要说明的是，用户界面中的桌面是通过桌面启动器launcher控制的，可以通过向launcher发送广播broadcast让launcher创建或删除快捷图标，也可以为应用程序的组

件注册某一个符号特定条件的IntentFilter，直接在launcher的桌面添加启动该组件的快捷图标。

[0077] 例如，发送删除终端设备桌面中的需要伪装的应用程序的原始图标和对应的原始名称的broadcast至Android系统的Launcher；Launcher在接受到该广播后，通过其注册的卸载接口UnInstallShortCutReceiver，将桌面中的需要伪装的应用程序的原始图标和对应的原始名称删除。随后，再发送添加桌面中需要伪装的应用程序的伪装图标和其对应的伪装名称的broadcast至Launcher；桌面应用程序Launcher在接受到broadcast后，通过其注册的添加接口InstallShortCutReceiver，将需要伪装的应用程序的伪装图标和其对应的伪装名称进行添加；从而实现将伪装图标和伪装名称作为需要伪装的应用程序的快捷图标标识。

[0078] 当用户需要将已经伪装的应用程序的伪装图标和其对应的伪装名称修改为原始图标和对应的原始名称作为应用程序的快捷图标标识，修改过程与上述过程中类似，就不在此赘述了。

[0079] 当需要伪装的应用程序已经伪装过了，则将其用户界面的当前的伪装图标和伪装名称，修改为重新确定的伪装图标和伪装名称；修改过程已经在上述过程中阐述过了，就不在此赘述了。

[0080] 具体地，接收到对任一应用程序的伪装触发操作之前，还包括：获取系统管理员操作权限。

[0081] 当Android系统需要设置通过调用Launcher添加和删除桌面中的其他应用程序的原始图标和对应的原始名称的权限时，首先需要通过引导用户在权限管理模块中去开放该权限，从而获取到该权限。获取系统管理员操作权限的方式如前所述，在此不再赘述。

[0082] 在Android系统中的AndroidManifest.xml权限配置中，需要设置上述系统级管理员权限、桌面应用程序Launcher添加快捷方式权限：

[0083] com.android.launcher.permission.INSTALL_SHORTCUT权限，和桌面应用程序Launcher卸载快捷方式权限：

[0084] com.android.launcher.permission.UNINSTALL_SHORTCUT权限，基于上述三个权限，才可以对将用户界面中的需要伪装的应用程序的原始图标和对应的原始名称进行删除，并对伪装图标和其对应的伪装名称进行添加；或是对将用户界面中已经伪装过的应用程序的当前的伪装图标和对应的伪装名称进行删除，并对重新确定的伪装图标和其对应的伪装名称进行添加。

[0085] 具体地，该隐私保护方法还包括：基于允许修改应用程序的原始图标和对应的原始名称的系统权限，创建应用程序的白名单；当任一应用程序不在白名单内，则不能对应用程序修改其原始图标和对应的原始名称；当任一应用程序在白名单内，则能对应用程序修改其原始图标和对应的原始名称。

[0086] 图4为本发明的后一个实施例的应用程序的隐私保护装置的结构框架示意图。

[0087] 接收模块201，接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称；获取模块202，获取针对应用程序的伪装图标和伪装名称；修改模块203，将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称。

[0088] 以下针对各个模块的具体实现做进一步的说明：

[0089] 接收模块201，接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称。

[0090] 具体地，接收模块201，接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称，具体包括：基于接收到的伪装触发操作指向应用程序的包名，获取应用程序的原始图标和对应的原始名称。

[0091] 其中，应用程序为基于沙箱隔离技术针对原生应用程序创建的分身应用程序。

[0092] 原生应用程序包括但不限于：通过安装包直接安装在移动终端系统中的应用程序。

[0093] 例如，应用图标的应用程序“微信”，其是通过原生应用程序“微信”，基于沙箱隔离技术创建的分身应用程序，该分身应用程序“微信”能够实现原生应用程序“微信”的功能，方便用户在同一个移动终端系统中，进行该应用程序“微信”账号的切换。

[0094] 此处需要说明的是，通过沙箱隔离技术创建分身应用程序的过程是本领域较为成熟的现有技术，在此就不再赘述。

[0095] 还需要说明的是，任一应用程序在安装时，Android系统会通过其提供的应用程序包管理Package Manager类，来获取安装的各个应用程序的相关信息，应用程序的相关信息包括图标、名称、版本号、包名等信息，随后将应用程序的包名与图标、名称、版本号等信息相关联地存储在应用程序信息列表中。

[0096] 例如，用户通过点击Android系统中提供的用于对应用程序的标识信息进行伪装的用户界面，图2示出了本发明的一个优选实施例的用于对应用程序的标识信息进行伪装的用户界面的示意图；用户通过点击用户界面上的“图标伪装”按钮，进入进行“图标伪装”的“编辑界面”，如图3所示，“编辑界面”中显示了多个可选的应用程序名称，供用户选择。用户在“编辑界面”中选择其希望进行伪装的应用程序；当“编辑界面”中未显示用户需要伪装的应用程序，则用户可以将其需要伪装的应用程序导入到该编辑界面中，从而对需要伪装的应用程序进行伪装。用户在“编辑界面”中选择其需要伪装的应用程序，如通过点击应用程序“微信”对应的“编辑”按钮，即执行伪装触发操作，则响应于该伪装触发操作获取“微信”的包名com.tencent.mm，并基于包名com.tencent.mm在预存的应用程序信息列表中查询以确定与com.tencent.mm对应的原始图标和对应的原始名称“微信”。

[0097] 获取模块202，获取针对应用程序的伪装图标和伪装名称。

[0098] 其中，获取针对应用程序的伪装图标和伪装名称，包括以下至少一种情形：基于用户针对应用程序选择的图像信息，生成相应的应用程序的伪装图标；将用户针对应用程序输入的应用名称作为该应用程序的伪装名称；基于用户程序的包名，确定与用户程序相应的预配置的伪装图标和伪装名称。

[0099] 具体地，基于用户针对应用程序选择的图像信息来获取应用程序的伪装图标方式包括：为用户提供上传图片或网络链接的交互接口，通过交互接口用户上传移动终端的本地图片或者网络图片链接，来获取到用户自定义的图片，并将该图片进行处理并封装为符合预定义图标标准的伪装图标。

[0100] 基于将用户针对应用程序输入的应用名称，获取应用程序的伪装名称的方式包括：为用户提供用于输入伪装名称的交互接口，通过交互接口用户输入伪装名称。

[0101] 基于应用程序的包名，确定与用户程序相应的预配置的伪装图标和伪装名称的方

式包括:预存有符合应用程序图标标准的多个伪装图标,且预先配置应用程序的包名与预存的伪装图标之间的对应关系;当用户触发对任一应用程序的伪装触发操作时,可基于应用程序的包名从预存的多个伪装图标中确定与该包名对应的伪装图标。

[0102] 修改模块203,将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称。

[0103] 具体地,在已获取到系统管理员权限的情况下,即获取系统的Root权限后,修改模块203根据确定的伪装图标和伪装名称,将需要伪装的应用程序的原始图标和对应的原始名称修改为确定的伪装图标和伪装名称;当需要伪装的应用程序已经伪装过,则将其当前的伪装图标和伪装名称修改为重新确定后的伪装图标和伪装名称。

[0104] 该伪装装置还包括:第一删除模块,删除用户界面中应用程序的原始图标和对应的原始名称,并添加伪装图标和伪装名称作为应用程序的快捷图标标识。

[0105] 该隐私保护装置还包括:第二删除模块,删除用户界面中应用程序的伪装图标和伪装名称,并添加原始图标和对应的原始名称作为应用程序的快捷图标标识。

[0106] 需要说明的是,桌面是通过桌面启动器launcher控制的,可以通过向launcher发送广播broadcast让launcher创建或删除快捷图标,也可以为应用程序的组件注册某一个符号特定条件的IntentFilter,直接在launcher的桌面添加启动该组件的快捷图标。

[0107] 例如,发送删除终端设备桌面中的需要伪装的应用程序的原始图标和对应的原始名称的broadcast至Android系统的Launcher;Launcher在接受到该广播后,通过其注册的卸载接口UnInstallShortCutReceiver,将桌面中的需要伪装的应用程序的原始图标和对应的原始名称删除。随后,再发送添加桌面中需要伪装的应用程序的伪装图标和其对应的伪装名称的broadcast至Launcher;桌面应用程序Launcher在接受到broadcast后,通过其注册的添加接口InstallShortCutReceiver,将需要伪装的应用程序的伪装图标和其对应的伪装名称进行添加;从而实现将伪装图标和伪装名称作为需要伪装的应用程序的快捷图标标识。

[0108] 当用户需要将已经伪装的应用程序的伪装图标和其对应的伪装名称修改为原始图标和对应的原始名称作为应用程序的快捷图标标识,修改过程与上述过程中类似,就不在此赘述了。

[0109] 当需要伪装的应用程序已经伪装过了,则将其用户界面的当前的伪装图标和伪装名称,修改为重新确定的伪装图标和伪装名称;修改过程已经在上述过程中阐述过了,就不在此赘述了。

[0110] 具体地,该隐私保护装置还包括:获取权限模块,获取系统级操作权限。

[0111] 当Android系统需要设置通过调用Launcher添加和删除桌面中的其他应用程序的原始图标和对应的原始名称的权限时,首先需要通过引导用户在权限管理模块中去开放该权限,从而获取到该权限。获取系统管理员操作权限的方式如前所述,在此不再赘述。

[0112] 在Android系统中的AndroidManifest.xml权限配置中,需要设置上述系统级管理员权限、桌面应用程序Launcher添加快捷方式权限:

[0113] com.android.launcher.permission.INSTALL_SHORTCUT权限,和桌面应用程序Launcher卸载快捷方式权限:

[0114] com.android.launcher.permission.UNINSTALL_SHORTCUT权限,基于上述三个权

限，才可以对将用户界面中的需要伪装的应用程序的原始图标和对应的原始名称进行删除，并对伪装图标和其对应的伪装名称进行添加；或是对将用户界面中已经伪装过的应用程序的当前的伪装图标和对应的伪装名称进行删除，并对重新确定的伪装图标和其对应的伪装名称进行添加。

[0115] 具体地，该隐私保护装置还包括：白名单创建模块，基于允许修改应用程序的原始图标和对应的原始名称的系统权限，创建应用程序的白名单；当任一应用程序不在白名单内，则不能对应用程序修改其原始图标和对应的原始名称；当任一应用程序在白名单内，则能对应用程序修改其原始图标和对应的原始名称。

[0116] 本技术领域技术人员可以理解，本发明包括涉及用于执行本申请中所述操作中的一项或多项的设备。这些设备可以为所需的目的而专门设计和制造，或者也可以包括通用计算机中的已知设备。这些设备具有存储在其内的计算机程序，这些计算机程序选择性地激活或重构。这样的计算机程序可以被存储在设备(例如，计算机)可读介质中或者存储在适于存储电子指令并分别耦联到总线的任何类型的介质中，所述计算机可读介质包括但不限于任何类型的盘(包括软盘、硬盘、光盘、CD-ROM、和磁光盘)、ROM(Read-Only Memory，只读存储器)、RAM(Random Access Memory，随即存储器)、EPROM(Erasable Programmable Read-Only Memory，可擦写可编程只读存储器)、EEPROM(Electrically Erasable Programmable Read-Only Memory，电可擦可编程只读存储器)、闪存、磁性卡片或光线卡片。也就是，可读介质包括由设备(例如，计算机)以能够读的形式存储或传输信息的任何介质。

[0117] 本技术领域技术人员可以理解，可以用计算机程序指令来实现这些结构图和/或框图和/或流图中的每个框以及这些结构图和/或框图和/或流图中的框的组合。本技术领域技术人员可以理解，可以将这些计算机程序指令提供给通用计算机、专业计算机或其他可编程数据处理方法的处理器来实现，从而通过计算机或其他可编程数据处理方法的处理器来执行本发明公开的结构图和/或框图和/或流图的框或多个框中指定的方案。

[0118] 本技术领域技术人员可以理解，本发明中已经讨论过的各种操作、方法、流程中的步骤、措施、方案可以被交替、更改、组合或删除。进一步地，具有本发明中已经讨论过的各种操作、方法、流程中的其他步骤、措施、方案也可以被交替、更改、重排、分解、组合或删除。进一步地，现有技术中的具有与本发明中公开的各种操作、方法、流程中的步骤、措施、方案也可以被交替、更改、重排、分解、组合或删除。

[0119] 以上所述仅是本发明的部分实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

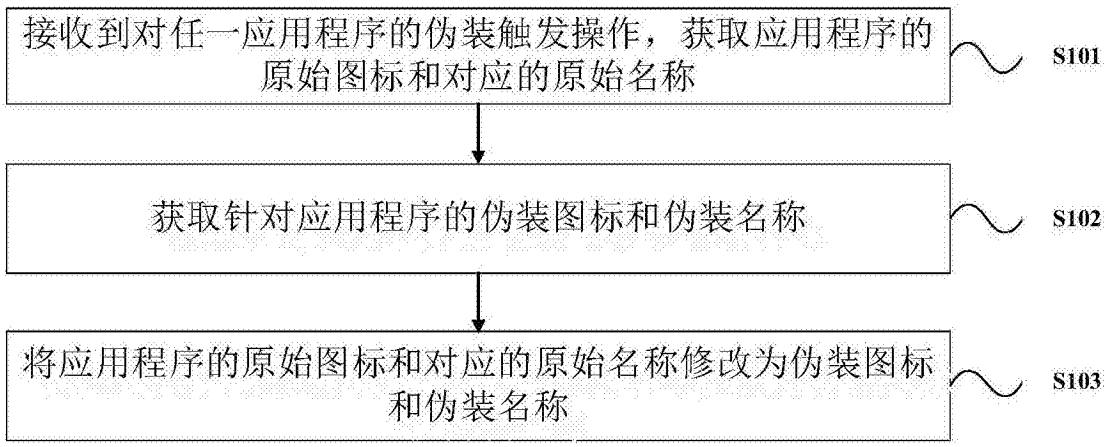
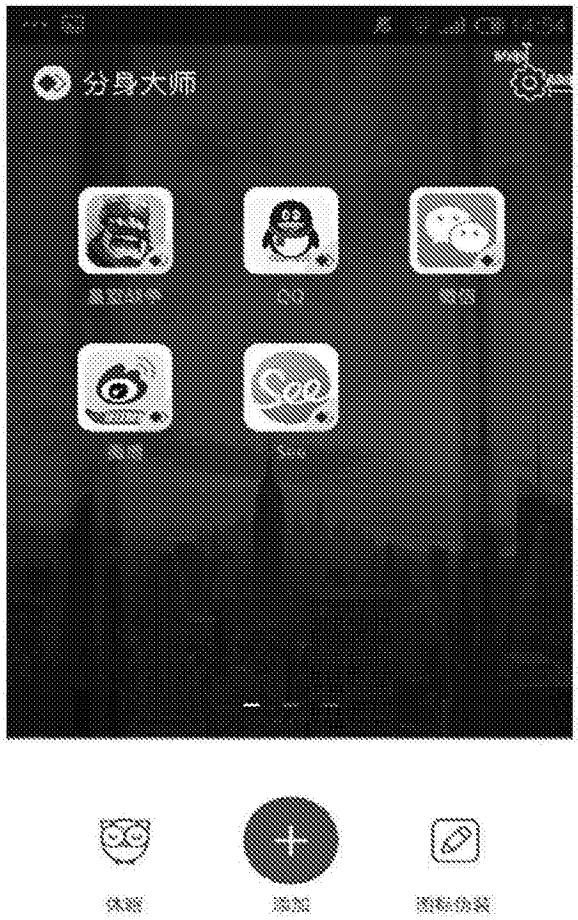

接收到对任一应用程序的伪装触发操作，获取应用程序的原始图标和对应的原始名称
S101
获取针对应用程序的伪装图标和伪装名称
S102
将应用程序的原始图标和对应的原始名称修改为伪装图标和伪装名称
S103

图1


分身大师


分身应用图标伪装
编辑
编辑
编辑
编辑

图3

图2

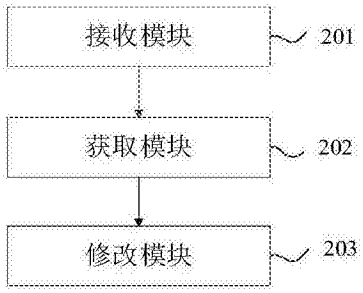


图4