

(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
2015 年 9 月 17 日 (17.09.2015)



(10) 国际公布号
WO 2015/135366 A1

- (51) 国际专利分类号:
G06F 21/51 (2013.01)
- (21) 国际申请号: PCT/CN2014/095391
- (22) 国际申请日: 2014 年 12 月 29 日 (29.12.2014)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410086128.4 2014 年 3 月 10 日 (10.03.2014) CN
- (71) 申请人: 北京奇虎科技有限公司 (BEIJING QIHOO TECHNOLOGY COMPANY LIMITED) [CN/CN]; 中国北京市西城区新街口外大街 28 号 D 座 112 室 (德胜园区), Beijing 100088 (CN)。奇智软件 (北京) 有限公司 (QIZHI SOFTWARE (BEIJING) COMPANY LIMITED) [CN/CN]; 中国北京市朝阳区酒仙桥路 6 号院 2 号楼 B 座 2 层、3 层 301-306 室, Beijing 100015 (CN)。
- (72) 发明人: 谭云宇 (TAN, Yunyu); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。范国峰 (FAN, Guofeng); 中国北京市朝阳区酒仙桥路 6

号院 2 号楼, Beijing 100015 (CN)。黄铮 (HUANG, Zheng); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。闫学松 (YAN, Xuesong); 中国北京市朝阳区酒仙桥路 6 号院 2 号楼, Beijing 100015 (CN)。

(74) 代理人: 北京智汇东方知识产权代理事务所 (普通合伙) (WISEAST INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区成府路 28 号优盛大厦 D 座-1111 室, Beijing 100083 (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,

[见续页]

(54) Title: APPLICATION ANTI-UNINSTALLATION METHOD AND DEVICE

(54) 发明名称: 应用防卸载方法及设备

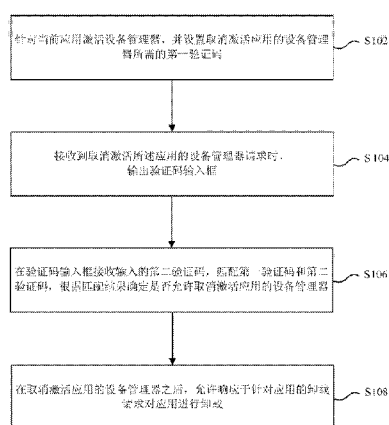


图 1 / FIG. 1

S102 FOR A CURRENT APPLICATION, ACTIVATING A DEVICE MANAGER AND SETTING A FIRST VERIFICATION CODE REQUIRED TO CANCEL THE ACTIVATING OF THE DEVICE MANAGER OF THE APPLICATION
S104 WHEN A REQUEST FOR CANCELLING THE ACTIVATING OF THE DEVICE MANAGER OF THE APPLICATION IS RECEIVED, OUTPUTTING A VERIFICATION CODE INPUT BOX
S106 RECEIVING AN INPUT SECOND VERIFICATION CODE IN THE VERIFICATION CODE INPUT BOX, MATCHING THE FIRST VERIFICATION CODE WITH THE SECOND VERIFICATION CODE, AND ACCORDING TO A MATCHING RESULT, DETERMINING WHETHER IT IS PERMITTED TO CANCEL THE ACTIVATING OF THE DEVICE MANAGER OF THE APPLICATION
S108 AFTER THE ACTIVATING OF THE DEVICE MANAGER OF THE APPLICATION IS CANCELLED, PERMITTING THE UNINSTALLING OF THE APPLICATION IN RESPONSE TO AN UNINSTALLATION REQUEST FOR THE APPLICATION

(57) Abstract: An application anti-uninstallation method and device. The application anti-uninstallation method comprises: for a current application, activating a device manager, and setting a first verification code required to cancel the activating of the device manager of the application; when a request for cancelling the activating of the device manager of the application is received, outputting a verification code input box; receiving an input second verification code in the verification code input box, matching the first verification code with the second verification code, and according to a matching result, determining whether it is permitted to cancel the activating of the device manager of the application; and after the activating of the device manager of the application is cancelled, permitting the uninstalling of the application in response to an uninstallation request for the application. The present invention can achieve the beneficial effect that the security of a user equipment is ensured by reducing the opportunity of maliciously uninstalling an application and improving the security of the application.

(57) 摘要: 一种应用防卸载方法及设备, 其中, 该应用防卸载方法包括: 针对当前应用激活设备管理器, 并设置取消激活应用的设备管理器所需的第一验证码; 接收到取消激活所述应用的设备管理器的请求时, 输出验证码输入框; 在验证码输入框接收输入的第二验证码, 匹配第一验证码和第二验证码, 根据匹配结果确定是否允许取消激活应用的设备管理器; 在取消激活应用的设备管理器之后, 允许响应于针对应用的卸载请求对应用进行卸载。能够达到减少应用被恶意卸载的机会, 提高应用安全性, 从而保证用户设备的安全的有益效果。

WO 2015/135366 A1



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)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

应用防卸载方法及设备

技术领域

本发明涉及互联网应用领域，特别是涉及一种应用防卸载方法及设备。

5

背景技术

随着信息社会的发展，移动设备在人们生活中的地位也日益重要，同时，移动设备的防盗问题也越来越受到人们的重视。由于移动设备自身防盗的局限性，很多用户选择下载安全软件保证移动设备以及移动设备内资料的安全性。例如，人们经常在手机中下载不同的手机安全应用，保证手机内存储的资料的安全或者在手机丢失之后，利用手机安全应用防止偷盗者进行刷机操作之后将手机二次出售。

现有技术中，人们下载的应用很容易被卸载。例如现有技术中有些手机中的安全软件采用监视系统日志输入的方式来达到防止被恶意卸载的目的，但这种做法很容易被破解，当手机与电脑连接之后，能够通过一些连接助手将应用卸载，另外，采用这种方式防止应用被恶意卸载的时候，很多系统日志输出不准确，容易错失拦截应用被恶意卸载的机会。同时，很多安全应用只在特定版本中提供防卸载功能。

发明内容

鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的应用防卸载方法和相应的应用防卸载设备。

依据本发明的一个方面，提供了一种应用防卸载方法，包括：针对当前应用激活设备管理器，并设置取消激活所述应用的设备管理器所需的第一验证码；接收到取消激活所述应用的设备管理器的请求时，输出验证码输入框；在所述验证码输入框接收输入的第二验证码，匹配所述第一验证码和所述第二验证码，根据匹配结果确定是否允许取消激活所述应用的设备管理器；在取消激活所述应用的设备管理器之后，允许响应于针对所述应用的卸载请求对所述应用进行卸载。

可选地，根据匹配结果确定是否允许取消激活所述应用的设备管理器，包括：当所述第一验证码和所述第二验证码匹配时，允许取消激活所述应用的设备管理器；当所述第一验证码和所述第二验证码不匹配时，拒绝取消激活所述应用的设备管理器。

可选地，当所述第一验证码与所述第二验证码匹配时，触发所述应用自行取消激活所述应用的设备管理器。

可选地，所述输出验证码输入框时，还包括：锁定当前屏幕，拒绝除验证码输入以外的其他操作。

可选地，所述除验证码输入以外的其他操作，包括：取消激活该应用的设备管理器的操作；管理软件对所述指定应用的删除操作；系统命令对所述指定应用的删除操作。

可选地，所述系统命令为安卓调试桥 adb 命令。

依据本发明实施例的另一个方面，还提供了一种应用防卸载设备，包括：验证码配置器，配置为针对当前应用激活设备管理器，并设置取消激活所述应用的设备管理器所需的第一验证码；接收器，配置为接收到取消激活所述应用的设备管理器的请求时，触发输出器；所述输出器，配置为输出验证码输入框；所述接收器，还配置为在所述验证码输入框接收输入的第二验证码；处理器，配置为匹配所述第一验证码和所述第二验证码，根据匹配结果确定是否允许取消激活所述应用的设备管理器；卸载器，配置为在取消激活所述应用的设备管理器之后，允许响应于针对所述应用的卸载请求对所述应用进行卸载。

10 可选地，所述处理器还配置为：当所述第一验证码和所述第二验证码匹配时，允许取消激活所述应用的设备管理器；当所述第一验证码和所述第二验证码不匹配时，拒绝取消激活所述应用的设备管理器。

可选地，所述处理器还配置为：当所述第一验证码与所述第二验证码匹配时，触发所述应用自行取消激活所述应用的设备管理器。

15 可选地，所述应用防卸载设备还包括：锁屏器，配置为所述输出器输出验证码输入框时，锁定当前屏幕，拒绝除验证码输入以外的其他操作。

可选地，所述除验证码输入以外的其他操作，包括：取消激活该应用的设备管理器的操作；管理软件对所述指定应用的删除操作；系统命令对所述指定应用的删除操作。

可选地，所述系统命令为安卓调试桥 adb 命令。

20 根据本发明的又一个方面，提供了一种计算机程序，其包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行上述的应用防卸载方法。

根据本发明的再一个方面，提供了一种计算机可读介质，其中存储了如上述的计算机程序。

本发明的有益效果为：

25 在本发明实施例中，针对当前应用激活设备管理器，并设置取消激活应用的设备管理器所需的第一验证码，在接收到取消激活所述应用的设备管理器的请求时，输出验证码输入框，接收输入的第二验证码，匹配第一验证码和第二验证码，进而根据匹配结果确定是否取消激活所述应用的设备管理器。当对设备管理器取消激活之后，允许响应于针对应用的卸载请求对应用进行卸载。由此可见，本发明实施例在卸载应用之前需要对取消激活应用的设备管理器进行验证，并在取消激活应用的设备管理器之后，对应用进行卸载，解决了现有技术中将应用能够通过一些设备间的连接软件被卸载以及监视系统日志输入不及时导致应用被恶意卸载的问题，达到了减少应用被恶意卸载的机会，提高应用安全性，从而保证用户设备的安全的有益效果。另外，本发明实施例增强了系统兼容性，不但适用于高版本的系统，也适用于低版本的系统，保证更多低版本的系统也能
30 35 够防止应用被恶意卸载，提高用户设备的安全性。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而

可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

附图说明

5 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 示出了根据本发明一个实施例的应用防卸载方法的处理流程图；

图 2 示出了根据本发明一个实施例的开启应用防卸载功能的界面图；

10 图 3A 示出了根据本发明一个实施例的启动设备管理器的界面图；

图 3B 示出了根据本发明一个实施例的设置图形密码的界面图；

图 4 示出了根据本发明一个实施例的如何关闭防卸载功能的界面图；

图 5 示出了根据本发明一个实施例的查看应用程序信息的界面图；

图 6 示出了根据本发明一个实施例的应用防卸载的界面图；

15 图 7 示出了根据本发明一个实施例的取消设备管理器的界面图；

图 8 示出了根据本发明一个实施例的请求输入密码的界面图；

图 9 示出了根据本发明一个优选实施例的应用防卸载方法的后台操作的处理流程图；
以及

图 10 示出了根据本发明一个实施例的应用防卸载设备的结构示意图；

20 图 11 示意性地示出了用于执行根据本发明的应用防卸载方法的计算设备的框图；以及

图 12 示意性地示出了用于保持或者携带实现根据本发明的应用防卸载方法的程序代码的存储单元。

具体实施方式

25 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

30 相关技术中提及，人们下载的应用很容易被卸载，防卸载应用通过一些设备间的连接应用软件能够被轻易卸载，采用监视系统日志输入的方式来防止应用被卸载的时候，由于系统日志输出不准确，容易导致拦截恶意卸载不及时的问题。另外，对于安卓系统或者其他操作系统而言，通常，应用的防卸载功能仅能适用于版本较高的系统，低版本系统不具备这一功能，因此也无法避免应用被轻易卸载。

35 为解决上述技术问题，本发明实施例提供了一种应用防卸载方法。图 1 示出了根据本发明一个实施例的应用防卸载方法的处理流程图。如图 1 所示，该流程至少包括步骤

S102 至步骤 S108。

步骤 S102、针对当前应用激活设备管理器，并设置取消激活应用的设备管理器所需的第一验证码。

步骤 S104、接收到取消激活所述应用的设备管理器的请求时，输出验证码输入框。

5 步骤 S106、在验证码输入框接收输入的第二验证码，匹配第一验证码和第二验证码，根据匹配结果确定是否允许取消激活应用的设备管理器。

步骤 S108、在取消激活应用的设备管理器之后，允许响应于针对应用的卸载请求对应用进行卸载。

在本发明实施例中，针对当前应用激活设备管理器，并设置取消激活应用的设备管
10 理器所需的第一验证码，在接收到取消激活所述应用的设备管理器的请求时，输出验证码输入框，接收输入的第二验证码，匹配第一验证码和第二验证码，进而根据匹配结果确定是否取消激活所述应用的设备管理器。当对设备管理器取消激活之后，允许响应于针对应用的卸载请求对应用进行卸载。由此可见，本发明实施例在卸载应用之前需要对取消激活应用的设备管理器进行验证，并在取消激活应用的设备管理器之后，对应用进
15 行卸载，解决了现有技术中将应用能够通过一些设备间的连接软件被卸载以及监视系统日志输入不及时导致应用被恶意卸载的问题，达到了减少应用被恶意卸载的机会，提高应用安全性，从而保证用户设备的安全的有益效果。另外，本发明实施例增强了系统兼容性，不但适用于高版本的系统，也适用于低版本的系统，保证更多低版本的系统也能够防止应用被恶意卸载，提高用户设备的安全性。

20 本发明实施例的应用防卸载方法起始于步骤 S102，针对当前应用激活设备管理器，并设置取消激活应用的设备管理器所需的第一验证码。本发明实施例中，从该应用向系统发送针对本应用激活设备管理器的请求，请求通过设备管理器执行相关操作，例如，请求监控屏幕解锁次数，请求锁定屏幕、请求对验证码的设置规则进行设置以及其他避免不法分子对设备执行不当操作导致应用被恶意卸载的相关操作，等等，本发明实施例
25 对此并不加以限定。例如，本发明实施例中，请求设备管理器监控屏幕解锁次数，若当前屏幕被解锁次数超过一定次数（例如 3 次），仍旧未能成功解锁，则能够锁定设备或者删除设备中的数据，避免不法分子通过其他途径将设备解锁后获取设备内的数据等信息，对用户的财产安全造成威胁。另外，本发明实施例中，能够设置验证码的规则。例如，设置验证码为数字与字母的组合并规定在验证码中数字以及字母的个数（如规定验
30 证码中包括 3 个数字以及 3 个字母，如 367xyz）。再例如，设置验证码为数字与大写字母的组合并规定数字与大写字母分别的个数，如设置验证码中数字为 2 个，大写字母为 5 个（如 23WERTY）。

上述举例中设置的验证码的个数及组合仅为示例，实际应用中设置的验证码可以为任意字符的组合，并且可以为任意个数，本发明实施例对此并不加以限定。另外，取消
35 激活该应用的设备管理器所需的验证码可以由系统来默认地设置，例如设置为用户对于该应用已设置的使用密码等，以该应用为手机卫士为例，在用户在该手机卫士中已设置

有防盗密码的情况下，此处系统默认地将该取消激活手机卫士应用的设备管理器的第一验证码设置为与该手机卫士的防盗密码一致。

上文提及，本发明实施例能够向系统发送针对本应用激活设备管理器的请求，请求通过设备管理器执行相关操作。其中，发送请求的代码中，需要在工程的

5 AndroidManifest.xml 里面先声明所需的“receiver”，代码示例如下：

```

    <receiver android:name=".app.DeviceAdminSample$DeviceAdminSampleReceiver"
        android:label="@string/sample_device_admin"
        android:description="@string/sample_device_admin_description"
        android:permission="android.permission.BIND_DEVICE_ADMIN">
10    <meta-data android:name="android.app.device_admin"
        android:resource="@xml/device_admin_sample" />
        <intent-filter>
        <action android:name="android.app.action.DEVICE_ADMIN_ENABLED" />
        </intent-filter>
15    </receiver>

```

上文提及的代码示例中的“@xml/device_admin_sample”能够指明应用申请激活设备管理器时所申请的权限明细。

具体地，一个申请全部设备管理器权限的代码示例如下：

```

    <device-admin xmlns:android="http://schemas.android.com/apk/res/android">
20    <uses-policies>
        <limit-password />
        <watch-login />
        <reset-password />
        <force-lock />
25    <wipe-data />
        <expire-password />
        <encrypted-storage />
        <disable-camera />
    </uses-policies>
30    </device-admin>

```

另外，在 Java 代码中，代码示例如下：

```

Intent intent = new Intent(DevicePolicyManager.ACTION_ADD_DEVICE_ADMIN);
intent.putExtra(DevicePolicyManager.EXTRA_DEVICE_ADMIN,mDeviceAdminSampl
e);
35    intent.putExtra(DevicePolicyManager.EXTRA_ADD_EXPLANATION,
        mActivity.getString(R.string.add_admin_extra_app_text));
        startActivityForResult(intent, REQUEST_CODE_ENABLE_ADMIN)

```

需要说明的是，上文提及的代码仅为本发明实施例发送请求的部分代码示例，为将本发明实施例阐述得清楚简洁，对于本发明实施例发送请求的全部代码在此不作赘述。

在发送激活设备管理器的请求之后，弹出让用户确认针对该应用激活设备管理器的界面。当用户手动确认之后，系统对请求进行响应，激活针对该应用的设备管理器。

上文提及，本发明实施例中，激活设备管理器之后，为避免对设备管理器的恶意取消激活，为卸载应用所使用的设备管理器配置的第一验证码。该第一验证码可以是固定不变的，还可以是定期或不定期更新的。优选地，本发明实施例中，该第一验证码为定期更新的。本发明实施例中第一验证码为非固定的，防止因为第一验证码更新不及时导致旧的第一验证码被盗用，进一步导致应用程序被恶意卸载。例如，在手机卫士中使用手机防盗功能时，若手机被盗，偷窃者利用未及时更新的验证码将手机卫士恶意卸载，导致失主无法及时标记被盗手机，造成财产损失。

当接收到取消激活应用的设备管理器请求时，本发明实施例中，被取消激活的设备管理器针对的应用本身能够收到来自系统的通知，通知该应用，当前用户正在尝试取消激活设备管理器的操作。当该应用捕获到该通知，则执行步骤 S104，输出验证码输入框。保证在用户完成取消激活设备管理器的操作之前弹出验证码输入框，阻止取消激活操作直至确定第一验证码与第二验证码匹配。为增加应用的安全性，本发明实施例还可以在输出验证码输入框时，锁定当前屏幕，并拒绝验证码输入以外的其他操作，保证若当前输入验证码者无法输入与第一验证码匹配的第二验证码，则无法使用其他任意操作对设备管理器进行取消激活，进而无法恶意删除或者卸载应用。当本发明实施例锁定当前屏幕时，其拒绝的其他操作可以是取消激活该应用的设备管理器的操作，可以是管理软件对指定应用的删除操作，也可以是系统命令，例如安卓调试桥（Android Debug Bridge，以下简称 adb 命令）对指定应用的删除操作，保证本发明实施例仅能通过输入匹配的验证码进行取消激活设备管理器的操作，进而对当前应用进行卸载，防止其他恶意操作导致的应用被卸载。本发明实施例中，可以通过多种方式对设备的屏幕进行锁定，本发明实施例对此并不加以限定。例如，直接对屏幕进行锁定，提示需要输入验证码对设备进行解锁，还可以设置当前屏幕显示无需输入验证码即可对设备进行解锁操作，但在后台对屏幕进行锁定，降低不法分子的警惕心，更加有效保证设备中应用的安全性。

验证码输入框输出之后，执行步骤 S106，在验证码输入框接收输入的第二验证码，匹配第一验证码和第二验证码，并根据匹配结果确定是否运行取消激活应用的设备管理器。具体地，当第一验证码和第二验证码不匹配时，拒绝取消激活应用的设备管理器，并显示取消激活失败，提示重新输入第二验证码。优选地，当第二验证码输入错误达到预定次数（如 5 次）时，可以启动防盗警报或者其他处理。当第一验证码和第二验证码匹配时，本发明实施例可以显示询问用户是否取消对设备管理器的激活的界面，提示用户取消激活该设备管理器可能导致应用被恶意卸载。当用户确认取消激活该设备管理器时，由该应用在后台自行取消激活设备管理器。即，本发明实施例中，当应用成功激活设备管理器之后，除应用本身之外的其他任何应用均无法取消激活设备管理器。另外，本发明实施例中，当第一验证码与第二验证码匹配之后，还可以不做进一步询问与提示，由该应用直接在后台自行取消激活设备管理器。

根据步骤 S106，若第一验证码与第二验证码匹配，能够成功取消激活应用的设备管理器。在取消激活应用的设备管理器之后，执行步骤 S108，允许响应于针对应用的卸载请求对应用进行卸载。本发明实施例通过对为设备管理器配置的第一验证码以及输入的第二验证码进行匹配，得到匹配结果确定是否取消激活应用的设备管理器，进一步确定是否响应于针对应用的卸载请求对应用进行卸载，保证应用无法通过一些如手机助手、豌豆荚等设备间的连接软件被恶意卸载。另外，采用本发明实施例提供的应用防卸载方法能够防止一些掌握安卓技术的不法分子利用 adb 命令对应用进行恶意卸载，提高应用的安全性，进而保证用户设备以及设备内资料的安全性，提高用户体验。

现以具体实施例对本发明实施例提供的应用防卸载方法进行说明。

实施例一

图 2 至图 8 示出了根据本发明一个优选实施例的应用防卸载方法的处理流程的界面图，用于支持上述任意一个应用防卸载方法，将上述应用防卸载方法阐述得更加清晰易懂。具体地，图 2 示出了根据本发明一个实施例的开启应用防卸载功能的界面图。图 3A 示出了根据本发明一个实施例的启动设备管理器的界面图。图 3B 示出了根据本发明一个实施例的设置图形密码的界面图。图 4 示出了根据本发明一个实施例的如何关闭防卸载功能的界面图。图 5 示出了根据本发明一个实施例的查看应用程序信息的界面图。图 6 示出了根据本发明一个实施例的应用防卸载的界面图。图 7 示出了根据本发明一个实施例的取消设备管理器的界面图。图 8 示出了根据本发明一个实施例的请求输入密码的界面图。需要说明的是，为将本优选实施例阐述得更加清晰易懂，本优选实施例中，选择手机卫士作为被卸载应用，选择手机为安装有手机卫士的设备。

现介绍将手机卫士从手机中卸载的过程。

如图 2 所示，当用户要求开启应用防卸载功能，手机中的手机卫士提示用户，若开启手机卫士的防卸载功能，则卸载手机卫士之前必须先解除保护，使手机的安全性提高，并询问用户是否立即开启防卸载功能。当用户确认开启保护功能之后，手机弹出如图 3A 所示的开启设备管理器的界面图，并提示用户开启防卸载功能需要激活设备管理器，并允许手机卫士执行“设置密码规则”、“监视屏幕解锁尝试次数”以及“锁定屏幕”的操作，同时，询问用户是否要激活设备管理器。

当用户选择激活设备管理器之后，可以对密码规则进行设置（即设置第一验证码）。本发明实施例中，密码可以是字符密码（如数字或者字母），例如，设置密码规则为数字与字母的组合并规定在密码中数字以及字母的个数（如规定密码中包括 3 个数字以及 3 个字母，如 367xyz）。再例如，设置密码规则为数字与大写字母的组合并规定数字与大写字母分别的个数，如设置密码中数字为 2 个，大写字母为 5 个（如 23WERTY）。上述举例中设置的密码的个数及组合仅为示例，实际应用中设置的密码可以为任意字符的组合，并且可以为任意个数，本发明实施例对此并不加以限定。

本发明实施例中，还可以设置密码规则为图形密码。如图 3B 示出的一个常用设置图形密码的界面图，在设备屏幕显示 3 乘以 3 的排列的九个可触碰点，用户可以根据个人

喜好等在九个可触碰点上设置出个性图形作为密码。例如，图 3B 示出了设置一个“L”形图案作为图形密码。本发明实施例中对于密码规则的设置还可以是其他任意密码设置方法，如指纹密码等，本发明实施例对此并不加以限定。

另外，取消激活该应用的设备管理器所需的密码规则可以由系统来默认地设置，例如设置为用户对于该应用已设置的使用密码等，以该应用为手机卫士为例，在用户在该手机卫士中已设置有防盗密码的情况下，此处系统默认地将该取消激活手机卫士应用的设备管理器的第一验证码设置为与该手机卫士的防盗密码一致。

当激活设备管理器成功之后，手机弹出如图 4 所示的界面图，提示用户防卸载功能开启成功，并提示用户当需要卸载手机卫士时，需要首先将防卸载功能关闭，或者到系统设置中查找相关选项取消对设备管理器的激活。另外，若手机开启了防盗密码，关闭防卸载功能需要验证防盗密码。

手机开启防卸载功能之后，在设备管理器中查询手机卫士的相关信息如图 5 所示。参见图 5，在手机中显示手机卫士的版本以及手机卫士的其他信息，如手机卫士的存储总量、手机卫士的存储数据以及手机卫士在手机存储内占用存储空间等等，并且如图 5 所示，手机无法直接在应用程序信息中直接对手机卫士进行强制停止以及卸载，即手机无法直接卸载手机卫士。其中，强制停止以及卸载两个操作标识为灰色（图 5 中未示出灰色显示效果），示意不可操作，即使在存储空间或容量可用的情况下，用户点击两者，也不会进入后续操作流程。另外，当手机输入安卓调试桥命令 adb 时，手机将弹出界面提示应用防卸载失败，即采用本优选实施例能够防止熟悉安卓技术的不法分子通过系统命令对手机卫士进行恶意卸载。

当手机接收到卸载例如手机卫士应用的请求时，提示手机卫士无法卸载，需要管理设备管理器。当用户点击管理设备管理器时，弹出如图 6 所示的界面图，提示用户手机卫士防卸载功能已开启，若关闭该防卸载功能需要验证防盗密码。当接收到关闭防卸载功能请求时，则手机弹出如图 7 所示的界面图，提示用户当前设备管理器已激活，并允许手机卫士执行“设置密码规则”、“监视屏幕解锁尝试次数”以及“锁定屏幕”的操作，另外，询问用户是否取消激活。当接收到取消激活请求，手机弹出如图 8 所示的验证码输入界面，并根据接收到的验证码与应用配置的第一验证码是否匹配确定是否取消激活设备管理器。当手机接收到的验证码（即第二验证码）与应用配置的第一验证码匹配，则显示询问用户是否取消对设备管理器的激活的界面，当用户确认要取消激活该设备管理器时，取消对该设备管理器的激活。当手机接收到的验证码与应用配置的第一验证码不匹配，则显示解锁失败，以使用户重新输入验证码。并且，本发明实施例中监视屏幕尝试解锁次数，在输入错误的次数达到预定次数时，执行锁定手机、清除手机数据、启动防盗警报等处理，保证用户信息安全。

上文介绍了将手机卫士从手机中卸载的过程，为将本优选实施例阐述得更加清楚明白，现对本优选实施例提供的应用防卸载方法的后台操作进行介绍。如图 9 示出了根据本发明一个优选实施例的应用防卸载方法的后台操作的处理流程图。参见图 9，该优选实

施例至少包括步骤 S902 至步骤 S912。

步骤 S902、设置广播接收器。

在本优选实施例提供的应用防卸载方法进行介绍时提及，本例中，通过激活设备管理器达到防卸载的目的，并通过取消激活设备管理器对应用进行卸载。因此，本例中，

5 在应用的 AndroidManifest.xml（安卓项目中的清单文件）中声明一个监听设备管理器变化的 BroadcastReceiver。BroadcastReceiver 是一种广播接收器。即当他人通过发广播通知多方同一消息时，BroadcastReceiver 能够接收到该广播的信息。DeviceAdminReceiver 是继承 BroadcastReceiver 特性的一种系统特殊定制的广播接收器。通过该 DeviceAdminReceiver 能够接收到通常广播接收器无法接收到的信息，如用户手机密码输入是否正确以及用户对手机密码的修改等信息。本发明实施例中，基于

10 DeviceAdminReceiver 进行扩展，得到继承 DeviceAdminReceiver 特性的 XDeviceAdminReceiver。即用户能够通过继承 DeviceAdminReceiver 生成个性化定制的子类型，进而达到期望的定制功能。

代码示例如下：

```

15 <receiver
    android:name="com.example.XDeviceAdminReceiver"
    android:description="@string/protection_uninstall_defence_description"
    android:exported="false"
    android:label="@string/protection_uninstall_defence" >
20 <meta-data
    android:name="android.app.device_admin"
    android:resource="@xml/example_device_admin" />
    <intent-filter>
        <action
25 android:name="android.app.action.DEVICE_ADMIN_ENABLED" />
    </intent-filter>
    </receiver>

```

步骤 S904、获取管理对象。

设置广播接收器成功之后，为监听（或者称之为控制）设备管理器，从系统中获取

30 一个管理对象。代码示例如下：

```

DevicePolicyManager manager = (DevicePolicyManager)
context.getSystemService(Context.DEVICE_POLICY_SERVICE)

```

步骤 S906、判断用户是否选择激活设备管理器。

设备管理器是一个系统特殊信息的接收器，本例中的设备管理器即为上文提及的

35 XDeviceAdminReceiver。当用户在安卓系统中，调用相关函数发送一个指定的 DeviceAdminReceiver 的子类（即广播特殊信息的接收器）至系统，系统接收到 DeviceAdminReceiver 的子类的相关信息，则认为存在监听系统特殊消息的接收器，即系统默认该接收器为一个设备管理器。进一步，系统将该设备管理器展示至设备管理器的

页面，并且说明该设备管理器接收何种特殊信息（如该设备管理器监听用户手机密码输入是否正确、该次解锁是否成功等信息）。当设备管理器被激活，则设备管理器从属的应用无法直接进行卸载，直至设备管理器关闭。具体地，本发明实施例中，判断用户是否选择激活指定的设备管理器的代码示例如下：

```
5      String componentName = new ComponentName(context, XDeviceAdminReceiver.class);
      boolean isAdminActive = manager.isAdminActive(componentName);
```

其中，XDeviceAdminReceiver，即为指定的设备管理器，即步骤 S902 中在 AndroidManifest.xml 中注册的那个 BroadcastReceiver。

步骤 S908、根据步骤 S906 的判断结果，若用户选择当前并不激活设备管理器，则提示用户能够激活设备管理器，并且，通过激活设备管理器，能够达到防止恶意卸载的目的。

步骤 S910、根据步骤 S906 的判断结果，若用户选择激活设备管理器，则后台执行至少如下的步骤 A 至 F 将指定的设备管理器激活：

A、声明一个激活设备管理器的 Intent：

```
15      Intent intent = new Intent(DevicePolicyManager.ACTION_ADD_DEVICE_ADMIN)
```

B、将步骤 A 中声明的 Intent 加入上文指定的广播接收器：

```
String componentName = new ComponentName(context, XDeviceAdminReceiver.class);
intent.putExtra(DevicePolicyManager.EXTRA_DEVICE_ADMIN, componentName)
```

C、在 Intent 中加入在设备管理器页面展示的、指定设备管理器的意义。其中，指定设备管理器的意义指该指定设备管理器在系统中监听何种事件。例如，当指定设备管理器的意义为监听解锁事件时，代码示例如下：

```
intent.putExtra(DevicePolicyManager.EXTRA_ADD_EXPLANATION,
                “我是一个设备管理器，我用来监听解锁事件”)
```

D、判断系统是否支持设备管理器的设置。代码示例如下：

```
25      ResolveInfo resolveInfo = context.getPackageManager().resolveActivity(intent,
                                     PackageManager.MATCH_DEFAULT_ONLY)
```

E、当系统支持设备管理器时，能够确定 resolveInfo 不会是 null，进而能够呼叫设备管理器进行激活。代码示例如下：

```
if (resolveInfo != null) {
30          context.startActivity(intent); }
```

F、当步骤 E 中确定能够呼叫设备管理器进行激活之后，系统弹出设备管理器激活的页面，提示用户对设备管理器进行激活。当用户点击激活时，设备管理器激活成功。

步骤 S912、成功激活设备管理器之后，当用户需要对应用进行卸载时，需要取消激活设备管理器。代码示例如下：

```
35      String componentName = new ComponentName(context, XDeviceAdminReceiver.class);
      manager.removeActiveAdmin(componentName)
```

其中，manager 为获取的设备管理器的管理对象。

基于上文各优选实施例提供的应用防卸载方法，基于同一发明构思，本发明实施例提供了一种应用防卸载设备。图 10 示出了根据本发明一个实施例的应用防卸载设备的结构示意图。参见图 10，本发明实施例的应用防卸载设备至少包括：验证码配置器 1010、接收器 1020、输出器 1030、处理器 1040 以及卸载器 1050。

5 现介绍本发明实施例的应用防卸载设备中的各器件或组成的功能以及各部分间的连接关系：

验证码配置器 1010，配置为针对当前应用激活设备管理器，并设置取消激活应用的设备管理器所需的第一验证码。

10 接收器 1020，配置为接收到取消激活应用的设备管理器的请求时，触发输出器 1030，以及在验证码输入框接收输入的第二验证码。

输出器 1030，与接收器 1020 相耦合，配置为输出验证码输入框。

处理器 1040，与验证码配置器 1010 以及接收器 1020 分别耦合，配置为匹配第一验证码和第二验证码，根据匹配结果确定是否允许取消激活应用的设备管理器。

15 卸载器 1050，与处理器 1040 相耦合，配置为在取消激活应用的设备管理器之后，允许响应于针对应用的卸载请求对应用进行卸载。

在本发明实施例中，针对当前应用激活设备管理器，并设置取消激活应用的设备管理器所需的第一验证码，并在接收到取消激活应用的设备管理器的请求时，输出验证码输入框，接收输入的第二验证码，匹配第一验证码和第二验证码，进而根据匹配结果确定是否取消激活应用的设备管理器。当对设备管理器取消激活之后，允许响应于针对应用的卸载请求对应用进行卸载。由此可见，本发明实施例在卸载应用之前需要对取消激活应用的设备管理器进行验证，并在取消激活应用的设备管理器之后，对应用进行卸载，解决了现有技术中将应用能够通过一些设备间的连接软件被卸载以及监视系统日志输入不及时导致应用被恶意卸载的问题，达到了减少应用被恶意卸载的机会，提高应用安全性，从而保证用户设备的安全的有益效果。另外，本发明实施例增强了系统兼容性，不但适用于高版本的系统，也适用于低版本的系统，保证更多低版本的系统也能够防止应用被恶意卸载，提高用户设备的安全性。如图 10 所示的应用防卸载设备中的验证码配置器 1010 针对当前应用激活设备管理器，并设置取消激活应用的设备管理器所需的第一验证码。本发明实施例中，从该应用向系统发送针对本应用激活设备管理器的请求，请求通过设备管理器执行相关操作，例如，请求监控屏幕解锁次数，请求锁定屏幕、请求对验证码的设置规则进行设置以及其他避免不法分子对设备执行不当操作导致应用被恶意卸载的相关操作，等等，本发明实施例对此并不加以限定。例如，本发明实施例中，请求监控屏幕被解锁的次数，若当前屏幕被解锁次数超过一定次数（例如 3 次），仍旧未能成功解锁，则能够锁定设备或者删除设备中的数据，避免不法分子通过其他途径将设备解锁后获取设备内的数据等信息，对用户的财产安全造成威胁。

35 上文提及，本发明实施例能够向系统发送针对本应用激活设备管理器的请求，请求通过设备管理器执行相关操作。其中，发送请求的代码中，需要在工程的

AndroidManifest.xml 里面先声明所需的 “receiver”，代码示例如下：

```

    <receiver android:name=".app.DeviceAdminSample$DeviceAdminSampleReceiver"
        android:label="@string/sample_device_admin"
        android:description="@string/sample_device_admin_description"
5      android:permission="android.permission.BIND_DEVICE_ADMIN">
        <meta-data android:name="android.app.device_admin"
            android:resource="@xml/device_admin_sample" />
        <intent-filter
            <action android:name="android.app.action.DEVICE_ADMIN_ENABLED" />
10      </intent-filter>
        </receiver>

```

上文提及的代码示例中的 “@xml/device_admin_sample” 能够指明应用申请激活设备管理器时所申请的权限明细。

具体地，一个申请全部设备管理器权限的代码示例如下：

```

15  <device-admin xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-policies>
        <limit-password />
        <watch-login />
        <reset-password />
20    <force-lock />
        <wipe-data />
        <expire-password />
        <encrypted-storage />
        <disable-camera />
25    </uses-policies>
    </device-admin>

```

另外，在 Java 代码中，代码示例如下：

```

Intent intent = new Intent(DevicePolicyManager.ACTION_ADD_DEVICE_ADMIN);
intent.putExtra(DevicePolicyManager.EXTRA_DEVICE_ADMIN,mDeviceAdminSampl
30 e);
intent.putExtra(DevicePolicyManager.EXTRA_ADD_EXPLANATION,
mActivity.getString(R.string.add_admin_extra_app_text));
startActivityForResult(intent, REQUEST_CODE_ENABLE_ADMIN)

```

需要说明的是，上文提及的代码仅为本发明实施例发送请求的部分代码示例，为将
35 本发明实施例阐述得清楚简洁，对于本发明实施例发送请求的全部代码在此不作赘述。

在发送激活设备管理器的请求之后，弹出让用户确认针对该应用激活设备管理器的界面。当用户手动确认之后，系统对请求进行响应，激活针对该应用的设备管理器。

上文提及，本发明实施例中，激活设备管理器之后，为避免对设备管理器的恶意取消激活，为卸载应用所使用的设备管理器配置的第一验证码。该第一验证码可以是固定

不变的，还可以是定期更新的。优选地，本发明实施例中，该第一验证码为定期更新的。本发明实施例中第一验证码为非固定的，防止因为第一验证码更新不及时导致旧的第一验证码被盗用，进一步导致应用程序被恶意卸载。例如，在手机卫士中使用手机防盗功能时，若手机被盗，偷窃者利用未及时更新的验证码将手机卫士恶意卸载，导致失主无法及时标记被盗手机，造成财产损失。

当如图 10 所示的应用防卸载设备中的接收器 1020 接收到取消激活应用的设备管理器请求时，被取消激活的设备管理器针对的应用本身能够收到来自系统的通知，并通过通知获知当前用户正在尝试取消激活设备管理器的操作。当该应用捕获到上述通知，则接收器 1020 触发输出器 1030，由输出器 1030 输出验证码输入框。保证在用户完成取消激活设备管理器的操作之前弹出验证码输入框，阻止取消激活操作直至确定第一验证码与第二验证码匹配。本发明实施例中，为增加应用的安全性，锁屏器 1060 可以在输出器 1030 输出验证码输入框时，锁屏器 1060 锁定当前屏幕，并拒绝验证码输入以外的其他操作。当锁屏器 1060 锁定当前屏幕时，其拒绝的其他操作可以是取消激活该应用的设备管理器的操作，可以是管理软件对指定应用的删除操作，也可以是系统命令，例如安卓 adb 命令对指定应用的删除操作，保证本发明实施例仅能通过输入匹配的验证码对当前应用进行卸载，防止其他恶意操作导致的应用被卸载。本发明实施例中，锁屏器 1060 可以通过多种方式对设备的屏幕进行锁定，本发明实施例对此并不加以限定。例如，锁屏器 1060 直接对屏幕进行锁定，提示需要输入验证码对设备进行解锁，锁屏器 1060 还可以设置当前屏幕显示无需输入验证码即可对设备进行解锁操作，但在后台对屏幕进行锁定，降低不法分子的警惕心，更加有效保证设备中应用的安全性。

当接收器 1020 接收到第二验证码之后，由处理器 1040 对验证码配置器 1010 配置的第一验证码与接收器 1020 接收的第二验证码进行匹配。若经处理器 1040 的匹配操作，第一验证码与第二验证码不匹配，则处理器 1040 拒绝取消激活应用的设备管理器，防止应用被恶意卸载。优选地，处理器 1040 拒绝取消激活应用的设备管理器之后，本发明实施例还可以显示取消激活失败，提示重新输入第二验证码进行匹配。另外，当第二验证码输入错误达到预定次数（如 5 次）时，本发明实施例可以启动防盗警报或者其他处理，避免应用被恶意卸载。若经处理器 1040 的匹配操作，第一验证码与第二验证码相匹配，处理器 1040 允许取消激活应用的设备管理器。例如，本发明实施例中，当第一验证码与第二验证码匹配时，可以显示询问用户是否取消对设备管理器的激活的界面，提示用户取消激活该设备管理器可能导致应用被恶意卸载。当用户确认取消激活该设备管理器时，处理器 1040 触发该应用。应用在后台自行取消激活设备管理器。即，本发明实施例中，当应用成功激活设备管理器之后，除应用本身之外的其他任何应用均无法取消激活设备管理器。另外，本发明实施例中，当第一验证码与第二验证码匹配之后，还可以不做进一步询问与提示，由该应用直接在后台自行取消激活设备管理器。

若根据处理器 1040，第一验证码与第二验证码匹配，允许取消激活应用的设备管理器。在取消激活应用的设备管理器之后，与处理器 1040 相耦合的卸载器 1050 允许相应

针对应用的卸载请求对应用进行卸载。本发明实施例通过对为设备管理器配置的第一验证码以及输入的第二验证码进行匹配，得到匹配结果确定是否拒绝取消激活应用的设备管理器，进一步确定是否响应于针对应用的卸载请求对应用进行卸载，保证应用无法通过一些如手机助手、豌豆荚等设备间的连接软件被恶意卸载，另外，采用本发明实施例提供的应用防卸载方法能够防止一些掌握安卓技术的不法分子利用 adb 命令对应用进行恶意卸载，提高应用的安全性，进而保证用户设备以及设备内资料的安全性，提高用户体验。

根据上述任意一个优选实施例或多个优选实施例的组合，本发明实施例能够达到如下有益效果：

本发明实施例中利用设备管理器防止对应用进行恶意卸载，当根据用户需求需要卸载应用时，本发明实施例需要取消对设备管理器的激活。当取消对设备管理器的激活时，本发明实施例需要进行输入验证码与应用配置的验证码的匹配，并根据匹配结果确定是否取消对设备管理器的激活，从而保证不知道验证码的不法分子无法对应用进行恶意卸载，提高应用的安全性，进一步提高用户设备的安全性。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的应用防卸载设备中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

例如，图 11 示出了可以实现根据本发明的应用防卸载方法的计算设备。该计算设备传统上包括处理器 1110 和以存储器 1120 形式的计算机程序产品或者计算机可读介质。存储器 1120 可以是诸如闪存、EEPROM（电可擦除可编程只读存储器）、EPROM、硬盘或者 ROM 之类的电子存储器。存储器 1120 具有用于执行上述方法中的任何方法步骤的程序代码 1131 的存储空间 1130。例如，用于程序代码的存储空间 1130 可以包括分别用于实现上面的方法中的各种步骤的各个程序代码 1131。这些程序代码可以从一个或者多个计算机程序产品中读出或者写入到这一个或者多个计算机程序产品中。这些计算机程序产品包括诸如硬盘，紧致盘（CD）、存储卡或者软盘之类的程序代码载体。这样的计算机程序产品通常为如参考图 12 所述的便携式或者固定存储单元。该存储单元可以具有与图 11 的计算设备中的存储器 1120 类似布置的存储段、存储空间等。程序代码可以例如以适当形式进行压缩。通常，存储单元包括计算机可读代码 1131’，即可以由例如诸如 1110 之类的处理器读取的代码，这些代码当由计算设备运行时，导致该计算设备执行上面所描述的方法中的各个步骤。

本文中所称的“一个实施例”、“实施例”或者“一个或者多个实施例”意味着，结合实施例描述的特定特征、结构或者特性包括在本发明的至少一个实施例中。此外，请注意，这里“在一个实施例中”的词语例子不一定全指同一个实施例。

应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

至此，本领域技术人员应认识到，虽然本文已详尽示出和描述了本发明的多个示例性实施例，但是，在不脱离本发明精神和范围的情况下，仍可根据本发明公开的内容直接确定或推导出符合本发明原理的许多其他变型或修改。因此，本发明的范围应被理解和认定为覆盖了所有这些其他变型或修改。

权 利 要 求

1、一种应用防卸载方法，包括：

针对当前应用激活设备管理器，并设置取消激活所述应用的设备管理器所需的

5 第一验证码；

接收到取消激活所述应用的设备管理器的请求时，输出验证码输入框；

在所述验证码输入框接收输入的第二验证码，匹配所述第一验证码和所述第二验证码，根据匹配结果确定是否允许取消激活所述应用的设备管理器；

在取消激活所述应用的设备管理器之后，允许响应于针对所述应用的卸载请求

10 对所述应用进行卸载。

2、根据权利要求 1 所述的方法，其中，根据匹配结果确定是否允许取消激活所述应用的设备管理器，包括：

当所述第一验证码和所述第二验证码匹配时，允许取消激活所述应用的设备管理器；

15 当所述第一验证码和所述第二验证码不匹配时，拒绝取消激活所述应用的设备管理器。

3、根据权利要求 2 所述的方法，其中，当所述第一验证码与所述第二验证码匹配时，触发所述应用自行取消激活所述应用的设备管理器。

4、根据权利要求 1 至 3 任一项所述的方法，其中，所述输出验证码输入框时，
20 还包括：锁定当前屏幕，拒绝除验证码输入以外的其他操作。

5、根据权利要求 4 所述的方法，其中，所述除验证码输入以外的其他操作，包括：

取消激活该应用的设备管理器的操作；

管理软件对所述指定应用的删除操作；

25 系统命令对所述指定应用的删除操作。

6、根据权利要求 5 所述的方法，其中，所述系统命令为安卓调试桥 adb 命令。

7、一种应用防卸载设备，包括：

验证码配置器，配置为针对当前应用激活设备管理器，并设置取消激活所述应用的设备管理器所需的第一验证码；

30 接收器，配置为接收到取消激活所述应用的设备管理器的请求时，触发输出器；
所述输出器，配置为输出验证码输入框；

所述接收器，还配置为在所述验证码输入框接收输入的第二验证码；

处理器，配置为匹配所述第一验证码和所述第二验证码，根据匹配结果确定是否允许取消激活所述应用的设备管理器；

卸载器，配置为在取消激活所述应用的设备管理器之后，允许响应于针对所述应用的卸载请求对所述应用进行卸载。

5 8、根据权利要求7所述的设备，其中，所述处理器还配置为：

当所述第一验证码和所述第二验证码匹配时，允许取消激活所述应用的设备管理器；

当所述第一验证码和所述第二验证码不匹配时，拒绝取消激活所述应用的设备管理器。

10 9、根据权利要求8所述的设备，其中，所述处理器还配置为：

当所述第一验证码与所述第二验证码匹配时，触发所述应用自行取消激活所述应用的设备管理器。

10、根据权利要求7至9任一项所述的设备，其中，还包括：

15 锁屏器，配置为所述输出器输出验证码输入框时，锁定当前屏幕，拒绝除验证码输入以外的其他操作。

11、根据权利要求10所述的设备，其中，所述除验证码输入以外的其他操作，包括：

取消激活该应用的设备管理器的操作；

管理软件对所述指定应用的删除操作；

20 系统命令对所述指定应用的删除操作。

12、根据权利要求11所述的设备，其中，所述系统命令为安卓调试桥adb命令。

13、一种计算机程序，包括计算机可读代码，当所述计算机可读代码在计算设备上运行时，导致所述计算设备执行根据权利要求1-6中的任一个所述的应用防卸载方法。

25 14、一种计算机可读介质，其中存储了如权利要求13所述的计算机程序。

1/8

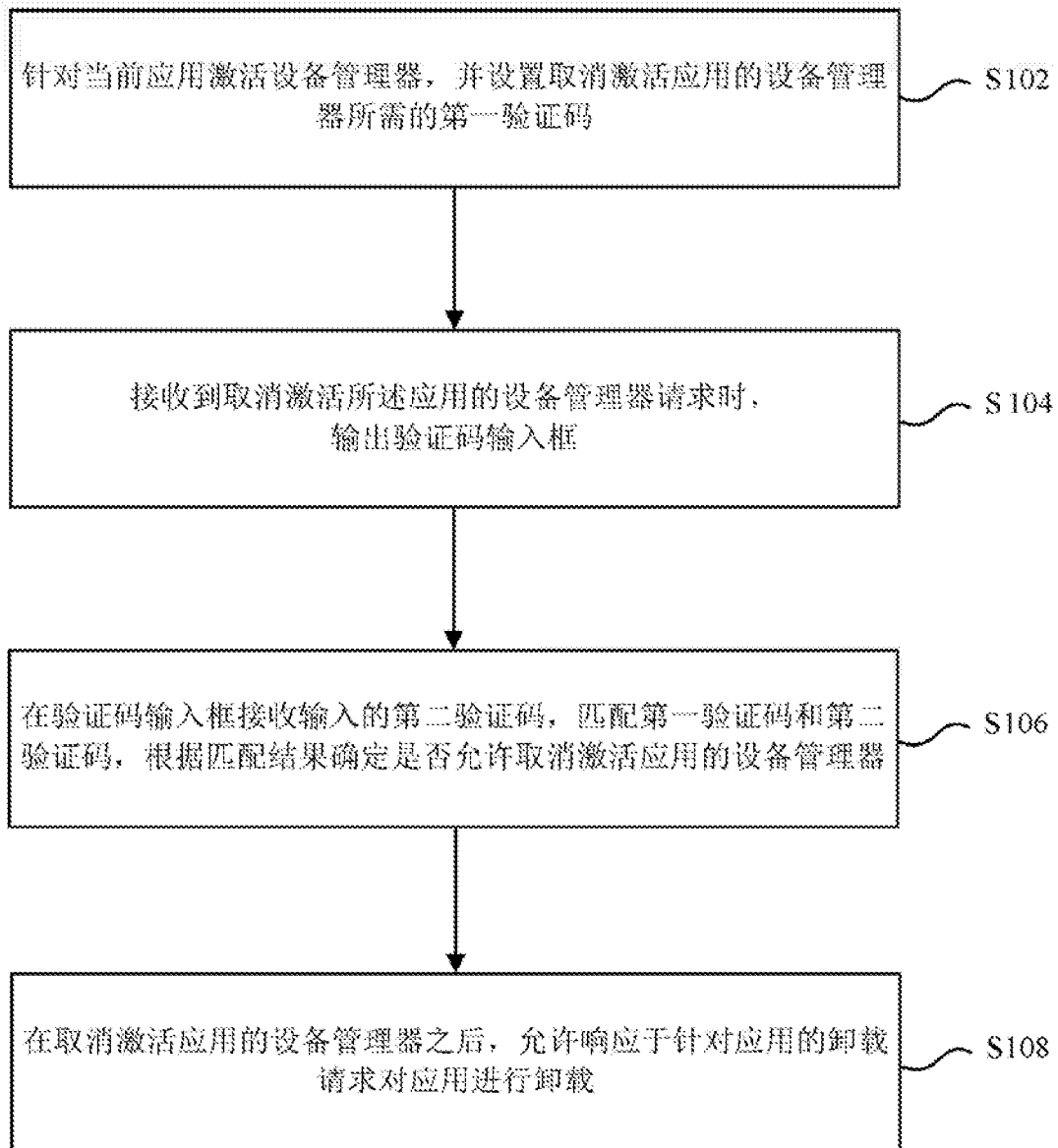


图 1

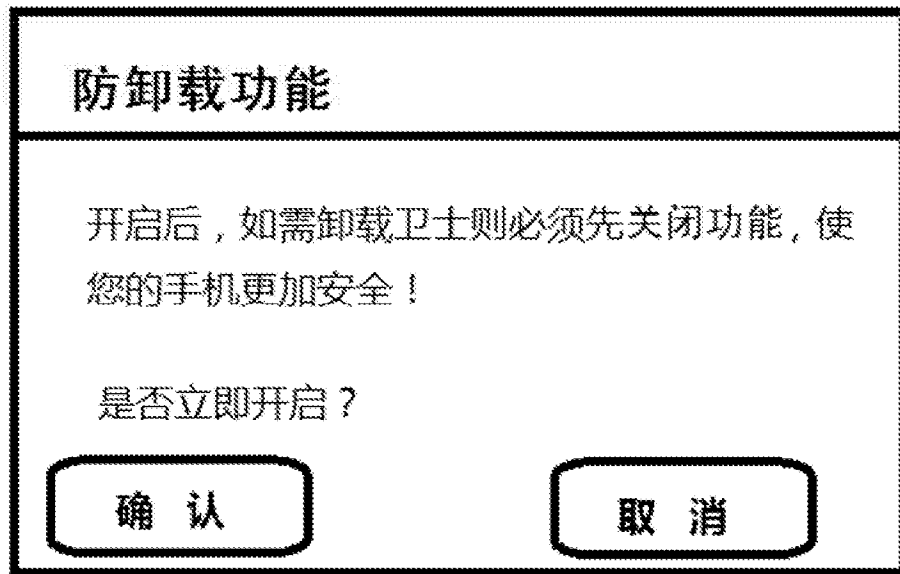


图 2

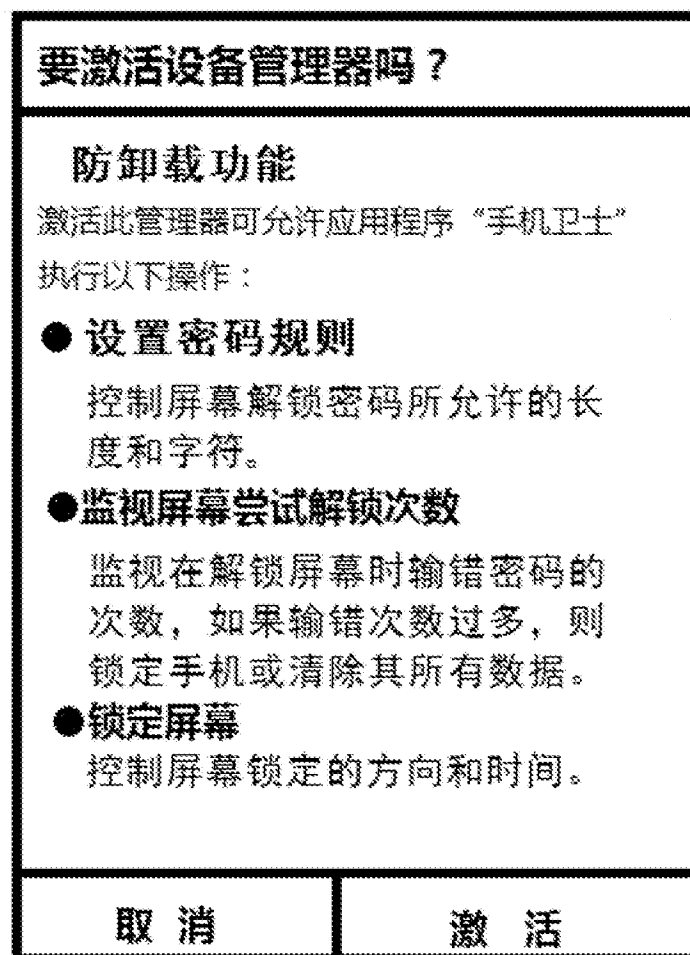


图 3A

3/8

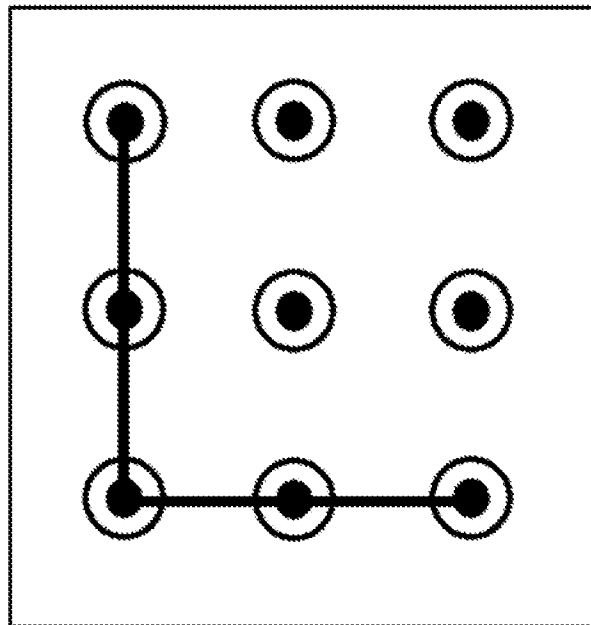


图 3B

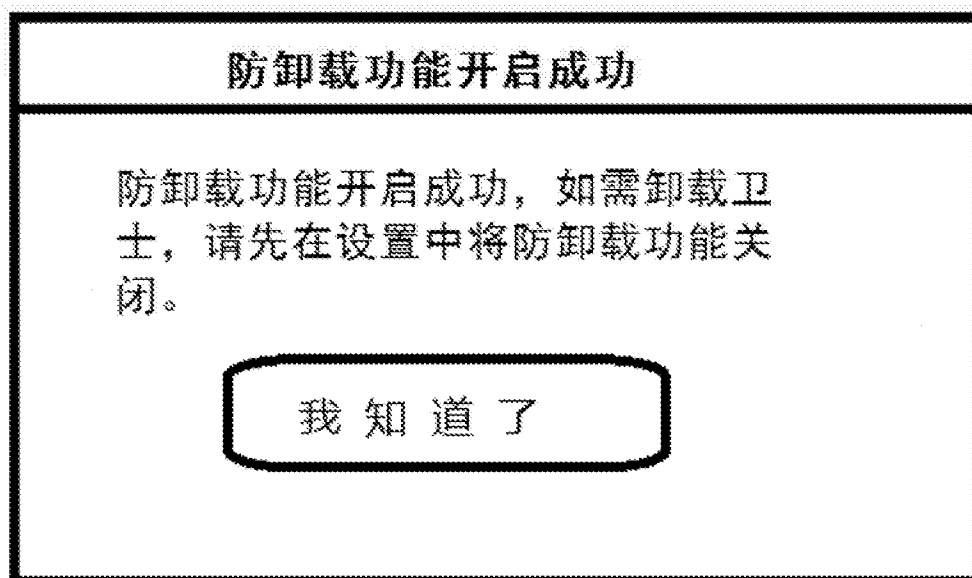


图 4



图 5

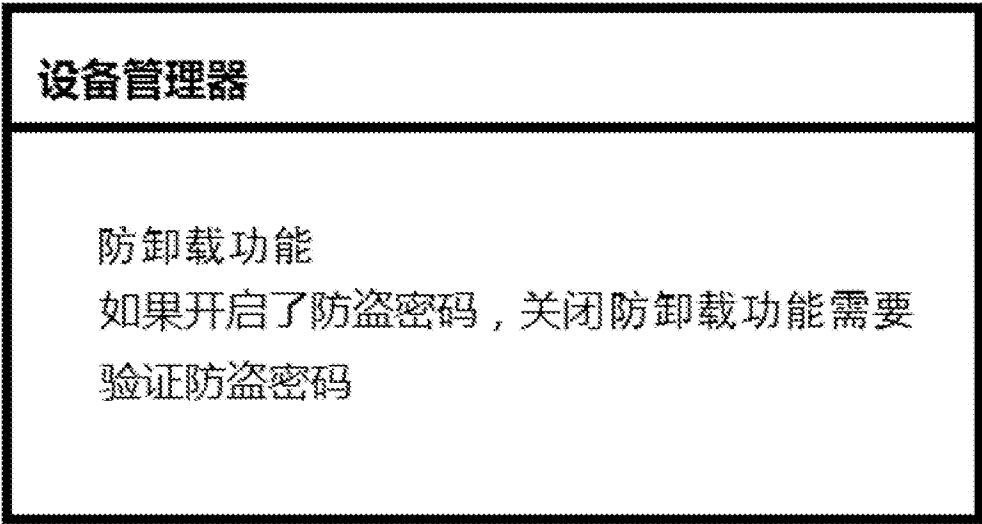


图 6

设备管理器	
防卸载功能 此管理器已激活，允许应用程序“手机卫士”执行以下操作： ● 设置密码规则 ● 监视屏幕解锁尝试次数 ● 锁定屏幕	
取 消	取消激活

图 7

防卸载功能
机主已开启防卸载功能，请输入防盗密码来取消激活：
请输入防盗密码
解 锁

图 8

6/8

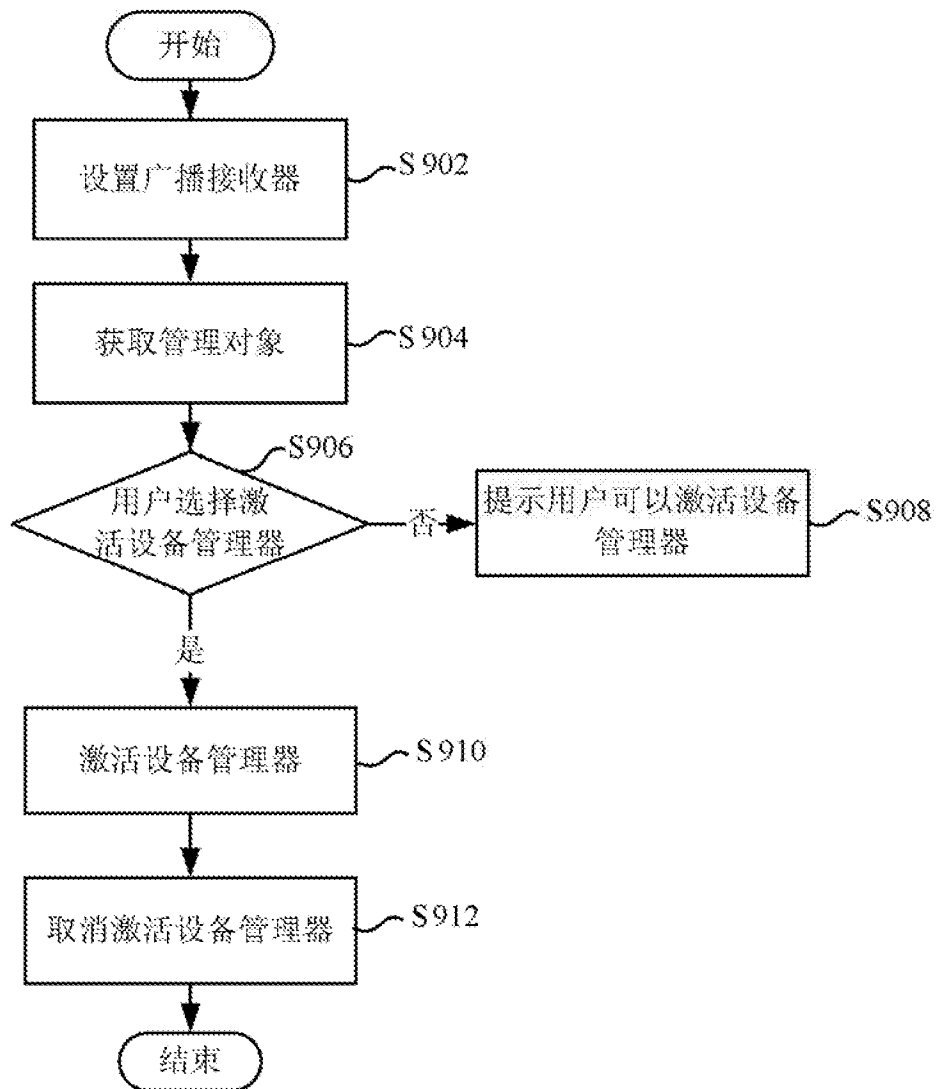


图 9

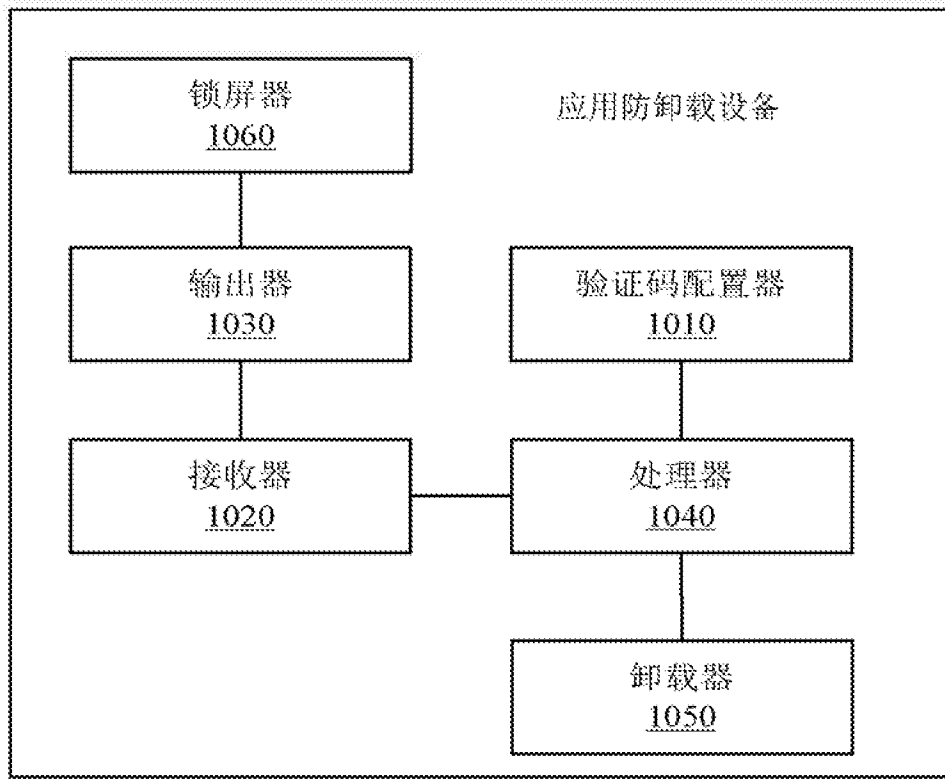


图 10

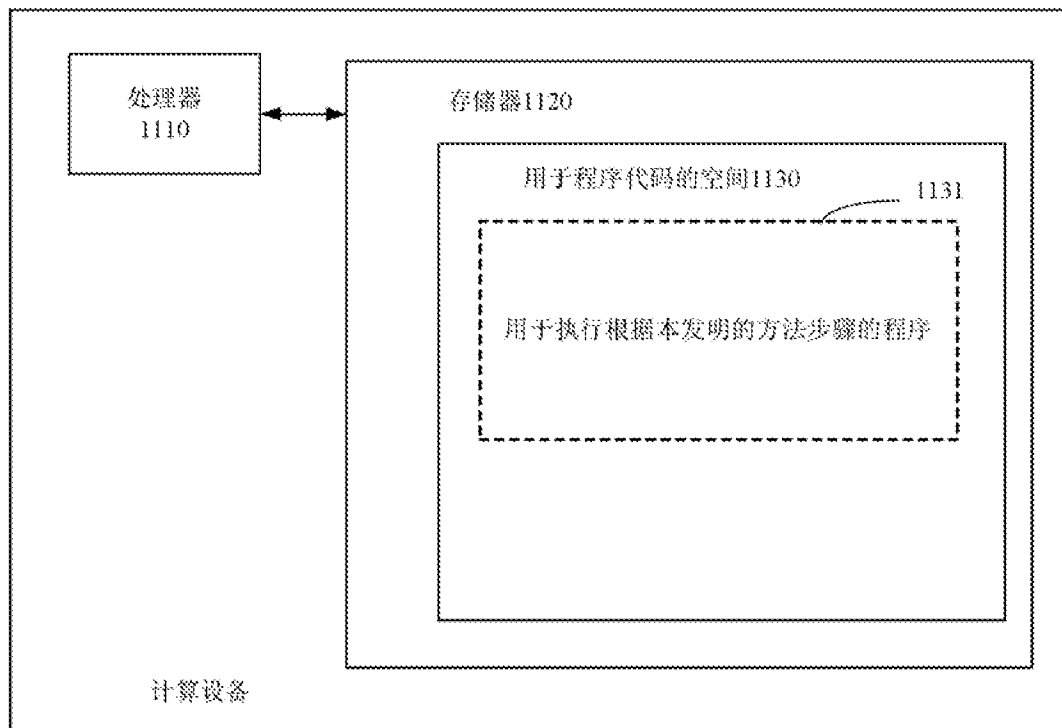


图 11

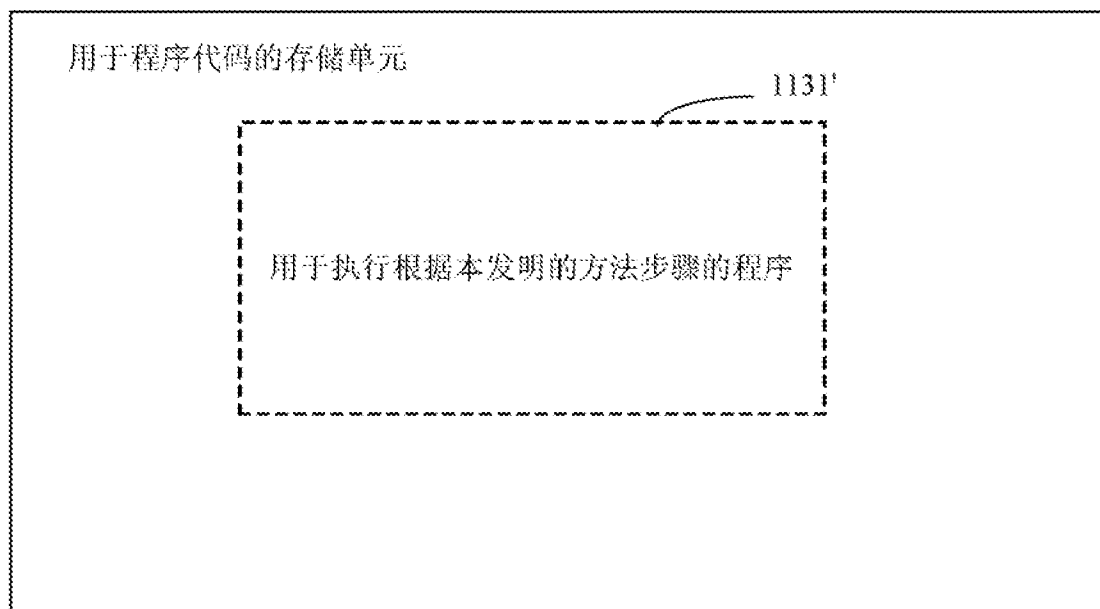


图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2014/095391

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/51 (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)

IPC: 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)

CNPAT, WPI, EPODOC, CNKI, IEEE, GOOGLE: app, application, program, remove, uninstall, unload, forbid, anti-, code, match, delete, active, manage, safety

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 103824016 A (BEIJING QIHOO TECHNOLOGY CO. et al.) 28 May 2014 (28.05.2014) claims 1-10, description, paragraph [0162]	1-14
X	CN 103383719 A (TENCENT TECH SHENZHEN CO., LTD.) 06 November 2013 (06.11.2013) claims 1-8, description, paragraphs [0038]-[0084]	1-14
PA	CN 103841192 A (TIANWEN DIGITAL MEDIA TECHNOLOGY BEIJING CO., LTD.) 04 June 2014 (04.06.2014) the whole document	1-14
PA	US 2014282971 A1 (BITIUM, INC.) 18 September 2014 (18.09.2014) the whole document	1-14

☐ 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 09 February 2015	Date of mailing of the international search report 27 February 2015
Name and mailing address of the ISA 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 QIN, Jingchan Telephone No. (86-10) 82245945

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2014/095391

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103824016 A	28 May 2014	None	
CN 103383719 A	06 November 2013	None	
CN 103841192 A	04 June 2014	None	
US 2014282971 A1	18 September 2014	WO 2014158828 A1	02 October 2014

A. 主题的分类		
G06F 21/51 (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))		
CNPAT, WPI, EPODOC, CNKI, IEEE, GOOGLE: 应用, 程序, 卸载, 防, 阻止, 验证码, 匹配, 删除, 激活, 管理, 安全, app, application, program, remove, uninstall, unload, forbid, anti-, code, match, delete, active, manage, safety		
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 103824016 A (北京奇虎科技有限公司等) 2014年 5月 28日 (2014 - 05 - 28) 权利要求 1-10, 说明书第[0162]段	1-14
X	CN 103383719 A (腾讯科技深圳有限公司) 2013年 11月 6日 (2013 - 11 - 06) 权利要求1-8, 说明书第[0038]-[0084]段	1-14
PA	CN 103841192 A (天闻数媒科技北京有限公司) 2014年 6月 4日 (2014 - 06 - 04) 全文	1-14
PA	US 2014282971 A1 (BITIUM, INC.) 2014年 9月 18日 (2014 - 09 - 18) 全文	1-14
☐ 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		国际检索报告邮寄日期
2015年 2月 9日		2015年 2月 27日
ISA/CN的名称和邮寄地址		受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国		覃婧婵
传真号 (86-10)62019451		电话号码 (86-10)82245945

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2014/095391

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	103824016	A	2014年 5月 28日	无	
CN	103383719	A	2013年 11月 6日	无	
CN	103841192	A	2014年 6月 4日	无	
US	2014282971	A1	2014年 9月 18日	WO 2014158828 A1	2014年 10月 2日