

(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
2017年3月9日 (09.03.2017)



(10) 国际公布号
WO 2017/036345 A1

- (51) 国际专利分类号:
G06F 3/023 (2006.01) G06F 21/56 (2013.01)
- (21) 国际申请号: PCT/CN2016/096787
- (22) 国际申请日: 2016年8月25日 (25.08.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510552192.1 2015年9月2日 (02.09.2015) CN
- (71) 申请人: 阿里巴巴集团控股有限公司 (ALIBABA GROUP HOLDING LIMITED) [—/CN]; 英属开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 严跃 (YAN, Yue) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。程刚 (CHENG, Gang) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。乔丽莎 (QIAO, Lisha) [CN/CN]; 中国浙江省杭州市余杭区文一西路 969

号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京国昊天诚知识产权代理有限公司 (CO-HORIZON INTELLECTUAL PROPERTY INC.); 中国北京市朝阳区小关北里甲 2 号渔阳置业大厦 B 座 605, Beijing 100029 (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,

[见续页]

(54) Title: INFORMATION INPUT METHOD AND DEVICE

(54) 发明名称: 一种信息输入方法和装置

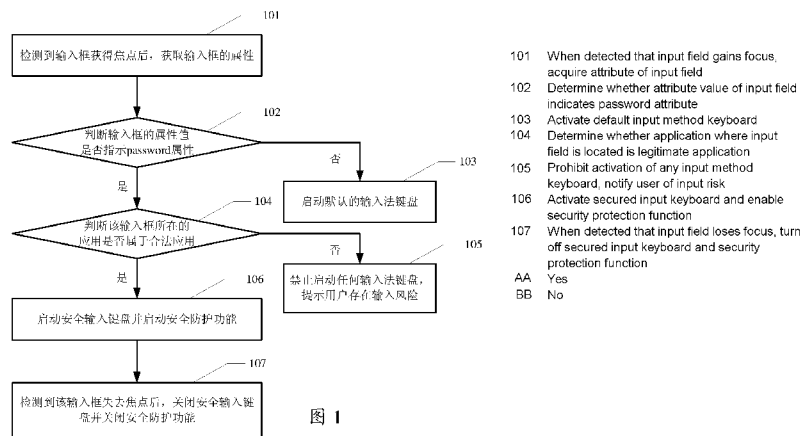


图 1

(57) Abstract: An information input method and device. The method comprises: when an input environment of confidential information is detected, activating a secured input keyboard and enabling a security protection function, wherein when the security protection function is enabled, the calling of interfaces for screen capturing and/or screen recording is prohibited. When the input environment of confidential information is detected, the method activates the secured input keyboard and a security protection module to prohibit the calling of the interfaces for screen capturing and/or screen recording, thereby preventing malware from stealing information by screen capturing or recording and improving security when inputting confidential information such as passwords.

(57) 摘要: 一种信息输入的方法和装置, 其中方法包括: 识别出保密信息的输入环境时, 启动安全输入键盘并启动安全防护功能; 其中所述安全防护功能启动后禁止调用截屏和/或录屏的接口。该方法在识别出保密信息的输入环境时, 启动安全输入键盘并启动安全防护模块, 以禁止调用截屏和/或录屏的接口, 从而避免恶意软件通过截屏或录屏的方式窃取信息, 提高了诸如密码等保密信息的输入安全性。



WO 2017/036345 A1



RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, **本国际公布:**

CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, — 包括国际检索报告(条约第 21 条(3))。
TG)。

一种信息输入方法和装置

【技术领域】

本发明涉及计算机应用技术领域，特别涉及一种信息输入方法和装置。

【背景技术】

5 目前，移动设备正在成为网络攻击的主要对象，各种钓鱼应用、免费的 wifi 等各种不良软件在移动设备中窃取着用户信息。然而用户在使用移动设备时，常常需要输入一些需要保密的信息，例如密码，那么如何保证这些信息的安全输入亟待解决。现有的解决方式主要是在进行密码输入时，调用系统自带的输入法，而不使用第三方输入法。然而这种方式只能在一定程度上
10 避免恶意软件通过监听输入键盘的方式窃取密码。

【发明内容】

有鉴于此，本发明提供了一种信息输入的方法和装置，以便于提高诸如密码等信息输入的安全性。

具体技术方案如下：

15 本发明提供了一种信息输入的方法，该方法包括：

识别出保密信息的输入环境时，启动安全输入键盘并启动安全防护功能；

其中所述安全防护功能启动后禁止调用截屏和/或录屏的接口。

根据本发明一优选实施方式，识别保密信息的输入环境包括：

20 检测到输入框获得焦点后，获取所述输入框的属性，依据所述输入框的属性识别保密信息的输入环境。

根据本发明一优选实施方式，所述依据所述输入框的属性识别保密信息的输入环境包括：

如果所述输入框的属性值指示密码 password 属性，则识别出保密信息的输入环境。

25 根据本发明一优选实施方式，所述安全输入键盘为系统自带的密码键盘。

根据本发明一优选实施方式，该方法还包括：

识别出非保密信息的输入环境时，启动默认的输入法键盘。

根据本发明一优选实施方式，在所述启动安全输入键盘并启动安全防护功能之前，还包括：

- 5 判断所述保密信息的输入环境是否属于合法应用，如果是，则继续执行所述启动安全输入键盘并启动安全防护功能的步骤。

根据本发明一优选实施方式，该方法还包括：

如果判断出所述保密信息的输入环境不属于合法应用，则禁止启动任何输入法键盘，和/或提示用户存在输入风险。

- 10 根据本发明一优选实施方式，所述禁止调用截屏和/或录屏的接口包括：

获取系统窗口，通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口。

根据本发明一优选实施方式，通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口包括：

- 15 通过 WindowManager.LayoutParams 参数设置窗口的 flag 为 flag_secure。

根据本发明一优选实施方式，该方法还包括：

识别出退出所述保密信息的输入环境后，关闭所述安全输入键盘并关闭所述安全防护功能。

根据本发明一优选实施方式，识别退出所述保密信息的输入环境包括：

- 20 检测到输入框失去焦点后，识别出退出所述保密信息的输入环境。

本发明还提供了一种信息输入的装置，该装置包括：

环境识别模块，用于识别输入环境；

功能启动模块，用于在所述环境识别模块识别出保密信息的输入环境时，启动安全输入键盘并启动安全防护模块；

- 25 所述安全防护模块，用于在启动后禁止调用截屏和/或录屏的接口。

根据本发明一优选实施方式，所述环境识别模块，具体用于检测到输入框获得焦点后，获取所述输入框的属性，依据所述输入框的属性识别保密信息的

输入环境。

根据本发明一优选实施方式,所述环境识别模块在依据所述输入框的属性识别保密信息的输入环境时,具体执行:

5 如果所述输入框的属性值指示密码 password 属性,则识别出保密信息的输入环境。

根据本发明一优选实施方式,所述安全输入键盘为系统自带的密码键盘。

根据本发明一优选实施方式,所述功能启动模块,还用于在所述环境识别模块识别出非保密信息的输入环境时,启动默认的输入法键盘。

根据本发明一优选实施方式,该装置还包括:

10 判断模块,用于在所述环境识别模块识别出保密信息的输入环境时,判断所述保密信息的输入环境是否属于合法应用;

所述功能启动模块在所述判断模块的判断结果为是时,执行所述启动安全输入键盘并启动安全防护模块的操作。

15 根据本发明一优选实施方式,所述功能启动模块还用于在所述判断模块的判断结果否时,禁止启动任何输入法键盘,和/或提示用户存在输入风险。

根据本发明一优选实施方式,所述功能启动模块在禁止调用截屏和/或录屏的接口时,具体执行:

获取系统窗口,通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口。

20 根据本发明一优选实施方式,所述功能启动模块在通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口时,具体执行:

通过 WindowManager.LayoutParams 参数设置窗口的 flag 为 flag_secure。

根据本发明一优选实施方式,该装置还包括:

25 功能关闭模块,用于在所述环境识别模块识别出退出所述保密信息的输入环境后,关闭所述安全输入键盘并关闭所述安全防护模块。

根据本发明一优选实施方式,所述环境识别模块检测到输入框失去焦点后,识别出退出所述保密信息的输入环境。

由以上技术方案可以看出，本发明在识别出保密信息的输入环境时，启动安全输入键盘并启动安全防护模块，以禁止调用截屏和/或录屏的接口。一方面，使用安全输入键盘，以避免恶意软件通过监听键盘的方式窃取信息，另一方面，启动安全防护功能，以避免恶意软件通过截屏或录屏的方式窃取信息，提高了诸如密码等保密信息的输入安全性。

【附图说明】

图 1 为本发明实施例所提供的方法流程图；

图 2a 为本发明实施例提供的一个应用界面的实例图；

图 2b 为图 2a 所示应用界面上的非保密信息输入场景的实例图；

图 2c 为图 2a 所示应用界面上的保密信息的输入场景的实例图；

图 3 为本发明实施例提供的装置结构图。

【具体实施方式】

为了使本发明的目的、技术方案和优点更加清楚，下面结合附图和具体实施例对本发明进行详细描述。

本发明的核心思想在于，在识别出保密信息的输入环境时，启动安全输入键盘并启动安全防护功能，其中安全防护功能启动后禁止调用截屏和/或录屏的接口。这一处理过程主要在系统级别执行。

对输入环境的识别主要是对输入框这种类型的组件进行判断，即依据输入框的属性识别保密信息的输入环境。对于其他类型组件，如果也存在保密需求，也可以采用类似方式进行处理。例如，对于按钮类型的组件，可以依据按钮的属性（例如按钮的 text 属性表明为“登录”或“注册”等按钮）识别保密信息的输入环境。下面的实施例均以输入框为例进行描述。

对输入环境的识别除了依据组件进行判断之外，还可以从页面进行判断，例如对于需要进行安全防护的页面，可以预先插入一个执行功能（JavaScript），当该执行功能执行时会主动发出该页面需要安全防护的信息。

一旦接收到该信息，则识别出该页面为保密信息的输入环境。

图 1 为本发明实施例所提供的方法流程图，如图 1 中所示，该流程可以包括以下步骤：

在 101 中，检测到输入框获得焦点后，获取输入框的属性。

5 当用户点击输入框准备进行输入时，会产生 onfocus 事件，因此，如果捕捉到输入框组件产生的 onfocus 事件，则确定检测到输入框获得焦点。

输入框组件具有一定的 type（属性），其中如果 type 值指示为 password（密码）属性，则说明该输入框用于进行密码输入，属于本发明中涉及的保密信息的输入环境。当然，本发明并不限于密码输入，也可以用于其他保密信息的输入，如果输入框用于其他保密信息的输入，则 type 值也可以对应指示其他属性，也可以预先定义一个 type 值指示需要进行保密信息的输入。在本发明实施例中仅以密码输入为例进行描述。

在 102 中，判断输入框的属性值是否指示 password 属性，如果否，执行 103；如果是，执行 104。

15 本步骤的判断实际上就是判断该输入环境是否为保密信息的输入环境。

在 103 中，启动默认的输入法键盘，结束当前流程。

如果当前输入框并非用于输入密码，即是非保密信息的输入环境，则无需进行额外的安全防护，采用默认的输入法进行信息输入即可，因此启动默认的输入法键盘，从而可以在没有必要进行安全保护的情况下，保留用户的使用习惯，提高用户的输入效率。在此处默认的输入法键盘可以是用户设置的第三方输入法，也可以是系统自带的输入法。

在 104 中，判断该输入框所在的应用是否属于合法应用，如果否，执行 105；如果是，执行 106。

本步骤是对保密信息的输入环境是否为合法应用进行的判断，可以预先通过白名单的方式预设一些合法应用信息，或者通过黑名单的方式预设一些非法应用信息；然后获取该输入框所在的应用信息，例如应用的包名、版本、大小等信息中的一种或任意组合，然后利用预设的白名单或黑名单来判断该

应用信息是否合法。此处，对于应用合法性判断的方式仅为举例，实际应用中，可以通过多种方式确定应用是否合法，例如，获取应用的发布商信息，根据应用发布商的黑名单或白名单，确定该应用是否合法；或者，获取该应用的评价信息，根据该应用的评价信息的好坏，确定该应用是否合法；或者，
5 由用户设置哪些应用作为合法应用；或者由系统安全中心或安装的安全防护软件，扫描应用以确定应用是否合法，若扫描发现应用存在对系统功能的非法调用等，则认为应用不合法。执行步骤 104 的主要目的在于：进一步提高信息输入的安全性，如果是非法应用，则可以进一步加强信息输入安全保护（如下述步骤 105 所述的方式），因此，本申请并不对如何判断应用是否合
10 法的方式进行具体限定，根据实际情况，可以定义各种应用合法或非法的判断方式，此处不再一一列举。

在 105 中，禁止启动任何输入法键盘，提示用户存在输入风险，结束当前流程。

如果输入框所在的应用为非法应用，那么该应用就可能有窃取用户信息的风险。禁止启动任何输入法键盘使得用户无法继续进行信息输入，从而保证保密信息不被窃取。提示用户存在输入风险也可以使得用户不再进行信息输入，从而保证保密信息不被窃取。因此可以采取禁止启动任何输入法键盘以及提示用户存在输入风险中的任一种处理，也可以如本步骤所示，同时采用两种处理。
15

20 在 106 中，启动安全输入键盘并启动安全防护功能。

本步骤中启动的安全输入键盘可以是系统自带的密码键盘，也可以是已经经过安全验证并确认安全的第三方输入法键盘。

安全防护功能是一个系统级的功能，其启动后会禁止任何应用调用截屏和/或录屏的接口，也禁止任何其他系统级的功能接收到截屏和/或录屏命令
25 后调用截屏和/或录屏的接口。

具体地，安全防护功能可以通过获取系统窗口，并设置系统窗口的 flag（标志）来禁止调用截屏和/或录屏的接口。其中获取系统窗口可以通过函数

getWindow()来实现,从而获取当前的系统窗口。设置系统窗口的 flag 可以通过函数 setFlags() 或者 addFlags() 来实现,在具体设置时,可以通过 WindowManager.LayoutParams 参数设置窗口的 flag 为 flag_secure。即:

```
getWindow().addFlags(WindowManager.LayoutParams.FLAG_SECURE)
```

5 或者

```
getWindow().setFlags(WindowManager.LayoutParams.FLAG_SECURE, 0)
```

在 107 中,检测到该输入框失去焦点后,关闭安全输入键盘并关闭安全防护功能。

检测到输入框失去焦点,说明退出保密信息的输入环境,无需继续进行安全输入的保护,因此可以关闭安全输入键盘,恢复使用默认的输入法键盘。可以关闭安全防护功能,使得截屏软件或者录屏软件可以恢复功能,这样实际上仅在保密信息输入时,屏蔽掉了截屏和录屏功能,最大程度地降低对截屏软件或者录屏软件的正常功能所造成的影响。

需要说明的是,本发明实施例提供的上述方式可以应用于移动设备,也可以应用于诸如 PC 等固定设备。以手机为例举一个实例,假设在应用 A 中出现如图 2a 中所示的页面,用户需要在各项目对应的输入框中填写内容。其中用户名、邮箱、收货地址这些信息都是不需要保密的,只有密码是需要保密的信息。例如,当用户点击用户名对应的输入框时,根据输入框的属性确定并非指示 password 属性,因此直接启动默认的输入法键盘,如图 2b 中所示。当用户点击密码对应的输入框时,根据输入框的属性确定指示 password 属性,即是保密信息的输入环境,则进一步获取应用 A 的信息,例如应用 A 的包名、版本号、大小等信息,与预置的白名单中的各项应用信息进行比较,加入确定该应用 A 为合法应用,则启动系统自带的密码键盘并启动安全防护功能,如图 2c 中所示。在用户输入密码的过程中禁止截屏和录屏功能,当用户完成密码的输入后,该密码对应的输入框失去焦点,则关闭系统自带的密码键盘并关闭安全防护功能。

图 3 为本发明实施例提供的装置结构图,如图 3 中所示,该装置可以包

括：环境识别模块 01、功能启动模块 02 和安全防护模块 03，还可以包括判断模块 04 和功能关闭模块 05。各组成单元的主要功能如下：

环境识别模块 01 负责识别输入环境，对输入环境的识别主要是对输入框这种类型的组件进行判断，即依据输入框的属性识别保密信息的输入环境。

5 对于其他类型组件，如果也存在保密需求，也可以采用类似方式进行处理。

具体地，环境识别模块 01 可以在检测到输入框获得焦点后，获取输入框的属性，依据输入框的属性识别保密信息的输入环境。如果输入框的属性值指示 password 属性，则识别出保密信息的输入环境。其中，当用户点击输入框准备进行输入时，会产生 onfocus 事件，因此，如果捕捉到输入框组件
10 产生的 onfocus 事件，则确定检测到输入框获得焦点。当然，本发明并不限于密码输入，也可以用于其他保密信息的输入，如果输入框用于其他保密信息的输入，则属性值也可以对应指示其他属性。

功能启动模块 02 负责在环境识别模块 01 识别出保密信息的输入环境时，启动安全输入键盘并启动安全防护模块。其中，安全输入键盘可以为系统自带的
15 密码键盘，也可以是已经过安全验证并确认安全的第三方输入法键盘。

如果环境识别模块 01 识别出非保密信息的输入环境，则功能启动模块 02 可以启动默认的输入法键盘。例如当前输入框并非用于输入密码，则无需进行额外的安全防护，采用默认的输入法进行信息输入即可，因此启动默认的输入法键盘。在此处默认的输入法键盘可以是用户设置的第三方输入法，
20 也可以是系统自带的输入法。

安全防护模块 03 负责在启动后禁止调用截屏和/或录屏的接口。该安全防护模块 03 是一个系统级的模块，其启动后会禁止任何应用调用截屏和/或录屏的接口，也禁止任何其他系统级的模块接收到截屏和/或录屏命令后调用截屏和/或录屏的接口。

25 另外，在环境识别模块 01 识别出保密信息的输入环境时，判断模块 04 可以首先判断保密信息的输入环境是否属于合法应用。在判断模块 04 的判断结果为是时，功能启动模块 02 执行启动安全输入键盘并启动安全防护模块 03 的操作；

在判断模块 04 的判断结果为否时，功能启动模块 02 禁止启动任何输入法键盘，和/或提示用户存在输入风险。

判断单元 04 在判断保密信息的输入环境是否属于合法应用时，可以预先通过白名单的方式预设一些合法应用信息，或者通过黑名单的方式预设一些非法应用信息；然后获取输入框所在的应用信息，例如应用的包名、版本、大小等信息中的一种或任意组合，然后利用预设的白名单或黑名单来判断该应用信息是否合法。

功能启动模块 02 在禁止调用截屏和/或录屏的接口时，可以获取系统窗口，通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口。其中获取系统窗口可以通过函数 getWindow()来实现，从而获取当前的系统窗口。设置系统窗口的 flag 可以通过函数 setFlags()或者 addFlags()来实现，在具体设置时，可以通过 WindowManager.LayoutParams 参数设置窗口的 flag 为 flag_secure。即：

getWindow().addFlags(WindowManager.LayoutParams.FLAG_SECURE)

或者

getWindow().setFlags(WindowManager.LayoutParams.FLAG_SECURE, 0)

在环境识别模块 01 识别出退出保密信息的输入环境后，例如环境识别模块 01 检测到输入框失去焦点后，识别出退出保密信息的输入环境。此时，功能关闭模块 05 可以关闭安全输入键盘，并且可以关闭安全防护模块，使得截屏软件或者录屏软件可以恢复功能，这样实际上仅在保密信息输入时，屏蔽掉了截屏和录屏功能，最大程度地降低对截屏软件或者录屏软件的正常功能所造成的影响。

在本发明所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元

中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机
5 可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本发明各个实施例所述方法的部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory, ROM）、随机存取存储器（Random Access Memory, RAM）、磁碟或者光盘等各种可
10 以存储程序代码的介质。

以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本发明保护的范围之内。

权 利 要 求 书

1、一种信息输入的方法，其特征在于，该方法包括：

识别出保密信息的输入环境时，启动安全输入键盘并启动安全防护功能；

5 其中所述安全防护模块启动后禁止调用截屏和/或录屏的接口。

2、根据权利要求 1 所述的方法，其特征在于，识别保密信息的输入环境包括：

检测到输入框获得焦点后，获取所述输入框的属性，依据所述输入框的属性识别保密信息的输入环境。

10 3、根据权利要求 2 所述的方法，其特征在于，依据所述输入框的属性识别保密信息的输入环境包括：

如果所述输入框的属性值指示密码 password 属性，则识别出保密信息的输入环境。

15 4、根据权利要求 1 所述的方法，其特征在于，所述安全输入键盘为系统自带的密码键盘。

5、根据权利要求 1 至 4 任一权项所述的方法，其特征在于，该方法还包括：识别出非保密信息的输入环境时，启动默认的输入法键盘。

6、根据权利要求 1 至 4 任一权项所述的方法，其特征在于，在所述启动安全输入键盘并启动安全防护功能之前，还包括：

20 判断所述保密信息的输入环境是否属于合法应用，如果是，则继续执行所述启动安全输入键盘并启动安全防护功能的步骤。

7、根据权利要求 6 所述的方法，其特征在于，该方法还包括：

如果判断出所述保密信息的输入环境不属于合法应用，则禁止启动任何输入法键盘，和/或提示用户存在输入风险。

25 8、根据权利要求 1 至 4 任一权项所述的方法，其特征在于，所述禁止调用截屏和/或录屏的接口包括：

获取系统窗口，通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的

接口。

9、根据权利要求 8 所述的方法，其特征在于，通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口包括：

通过 WindowManager.LayoutParams 参数设置窗口的 flag 为 flag_secure。

5 10、根据权利要求 1 至 4 任一权项所述的方法，其特征在于，该方法还包括：

识别出退出所述保密信息的输入环境后，关闭所述安全输入键盘并关闭所述安全防护功能。

11、根据权利要求 10 所述的方法，其特征在于，识别退出所述保密信息的
10 输入环境包括：

检测到输入框失去焦点后，识别出退出所述保密信息的输入环境。

12、一种信息输入的装置，其特征在于，该装置包括：

环境识别模块，用于识别输入环境；

15 功能启动模块，用于在所述环境识别模块识别出保密信息的输入环境时，
启动安全输入键盘并启动安全防护模块；

所述安全防护模块，用于在启动后禁止调用截屏和/或录屏的接口。

13、根据权利要求 12 所述的装置，其特征在于，所述环境识别模块，具体用于检测到输入框获得焦点后，获取所述输入框的属性，依据所述输入框的属性识别保密信息的输入环境。

20 14、根据权利要求 13 所述的装置，其特征在于，所述环境识别模块在依据所述输入框的属性识别保密信息的输入环境时，具体执行：

如果所述输入框的属性值指示密码 password 属性，则识别出保密信息的输入环境。

15、根据权利要求 12 所述的装置，其特征在于，所述安全输入键盘为系统
25 自带的密码键盘。

16、根据权利要求 12 至 15 任一权项所述装置，其特征在于，所述功能启动模块，还用于在所述环境识别模块识别出非保密信息的输入环境时，启动默认

的输入法键盘。

17、根据权利要求 12 至 15 任一权项所述装置，其特征在于，该装置还包括：

判断模块，用于在所述环境识别模块识别出保密信息的输入环境时，判断所述保密信息的输入环境是否属于合法应用；

5 所述功能启动模块在所述判断模块的判断结果为是时，执行所述启动安全输入键盘并启动安全防护模块的操作。

18、根据权利要求 17 所述的装置，其特征在于，所述功能启动模块还用于在所述判断模块的判断结果为否时，禁止启动任何输入法键盘，和/或提示用户存在输入风险。

10 19、根据权利要求 12 至 15 任一权项所述装置，其特征在于，所述功能启动模块在禁止调用截屏和/或录屏的接口时，具体执行：

获取系统窗口，通过设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口。

20、根据权利要求 18 所述的装置，其特征在于，所述功能启动模块在通过
15 设置系统窗口的标志 flag 来禁止调用截屏和/或录屏的接口时，具体执行：

通过 WindowManager.LayoutParams 参数设置窗口的 flag 为 flag_secure。

21、根据权利要求 12 至 15 任一权项所述装置，其特征在于，该装置还包括：

功能关闭模块，用于在所述环境识别模块识别出退出所述保密信息的输入环境后，关闭所述安全输入键盘并关闭所述安全防护模块。

20 22、根据权利要求 21 所述的装置，其特征在于，所述环境识别模块检测到输入框失去焦点后，识别出退出所述保密信息的输入环境。

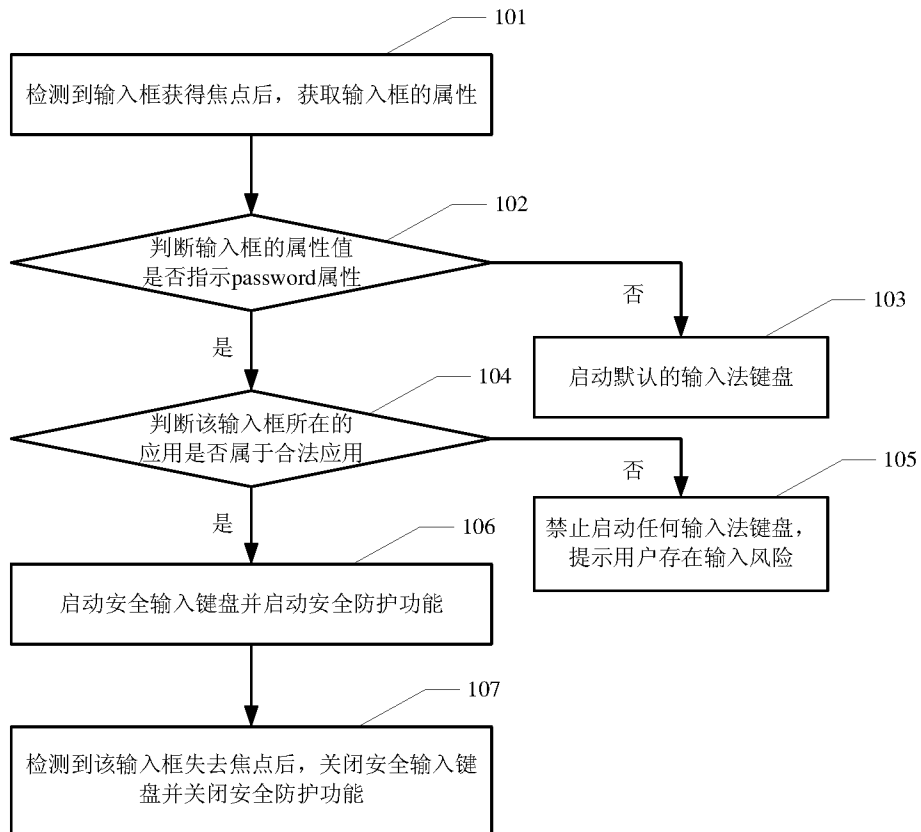


图 1

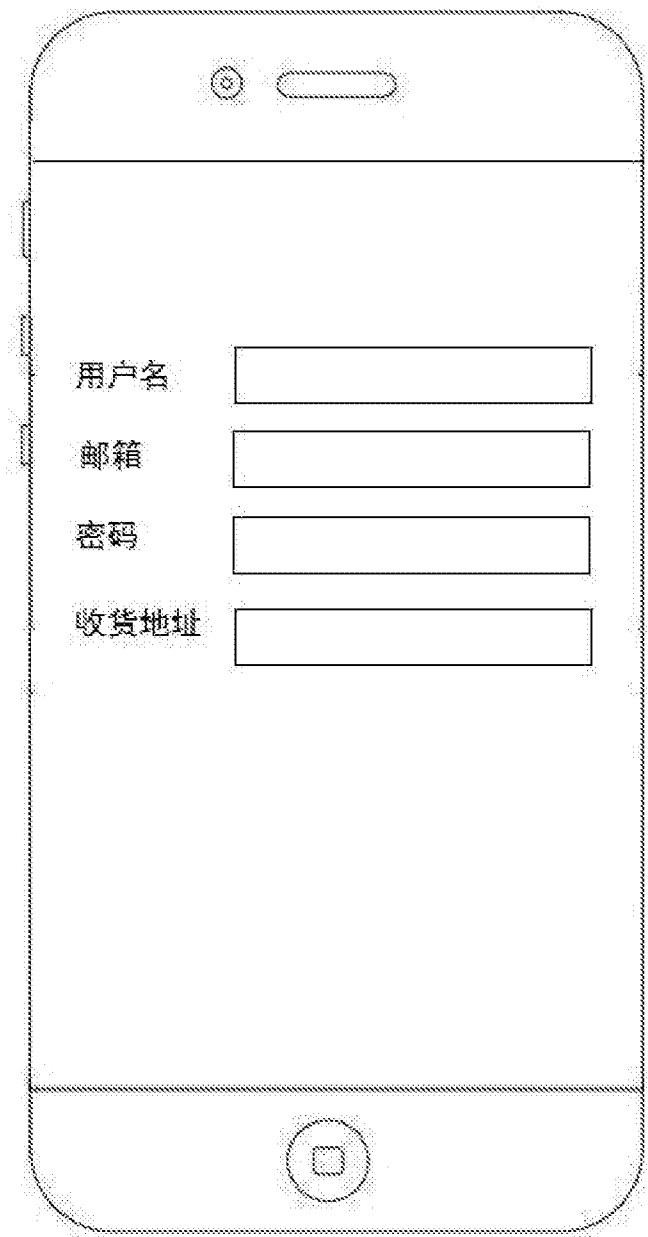


图 2a

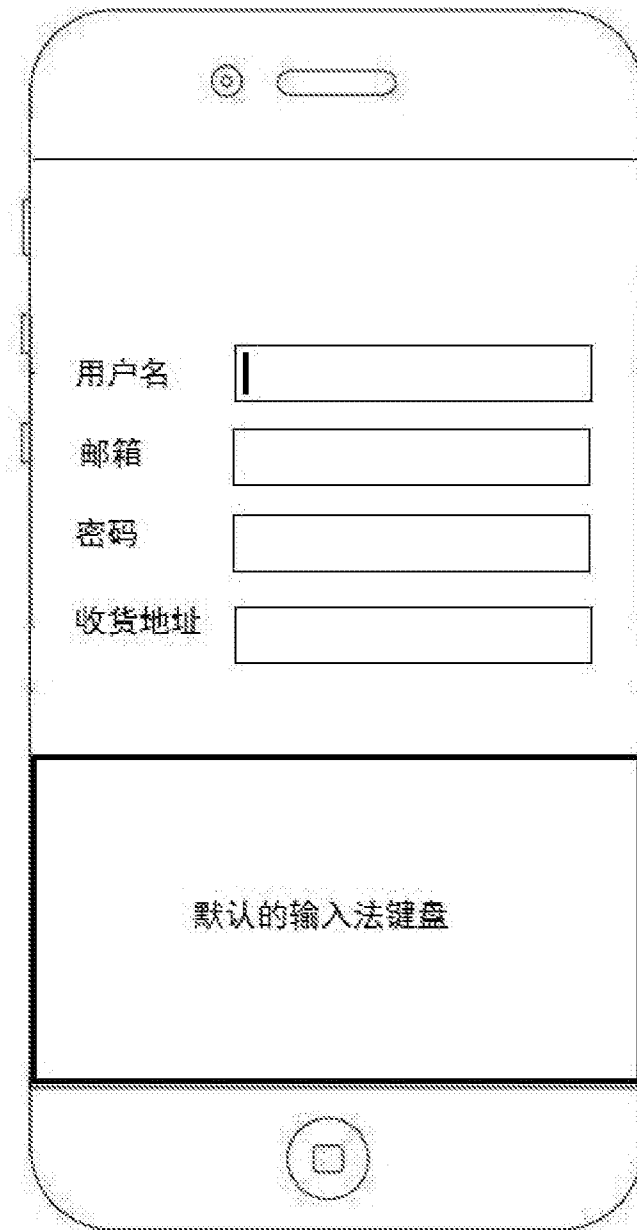


图 2b

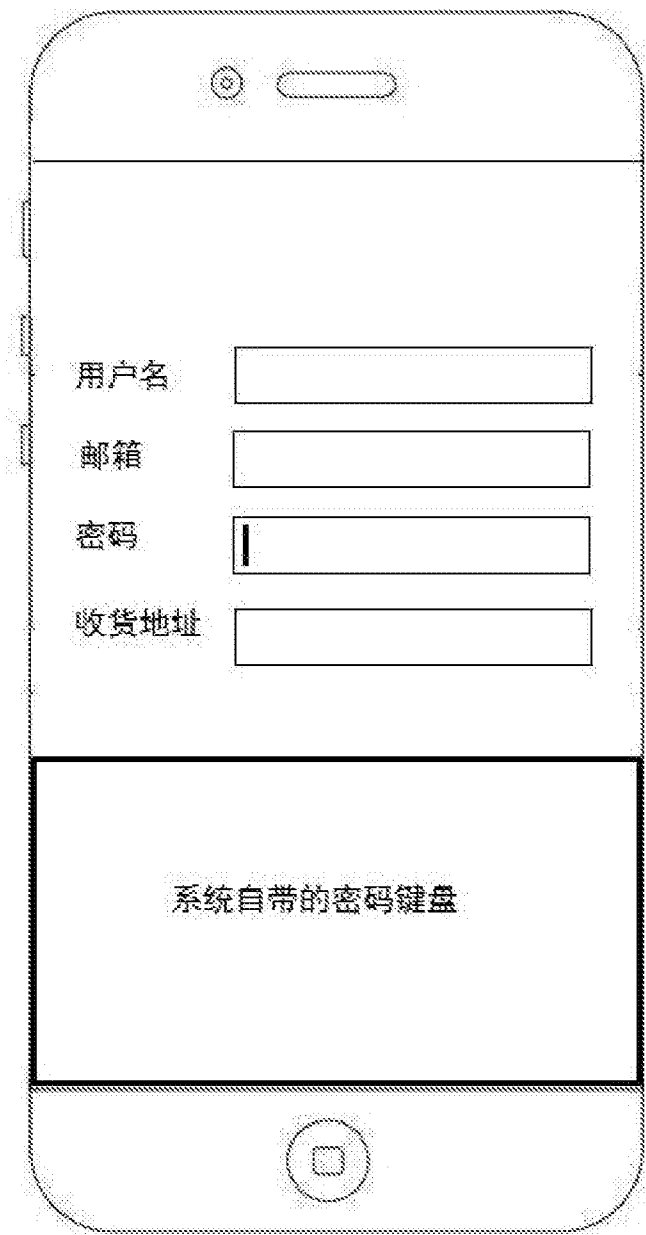


图 2c

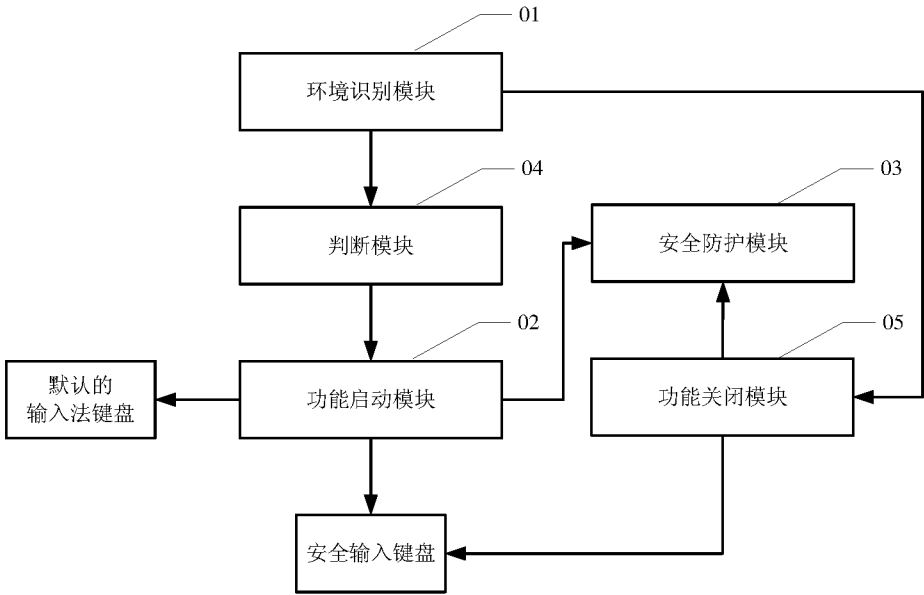


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/096787

A. CLASSIFICATION OF SUBJECT MATTER

G06F 3/023 (2006.01) i; G06F 21/56 (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)

WPI, EPODOC, CNPAT, CNKI, IEEE: input method, privacy, screenshot, screen recording, input, keyboard, password, secret, private, invoke, application, program, safe, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104281272 A (BEIJING SUMAVISION TECHNOLOGIES CO., LTD.), 14 January 2015 (14.01.2015), description, paragraphs [0026]-[0032], and figure 7	1-22
Y	CN 103853993 A (LENOVO (BEIJING) CO., LTD.), 11 June 2014 (11.06.2014), description, paragraphs [0053]-[0077]	1-22
A	CN 103076988 A (CHINA UNIONPAY MERCHANT SERVICES CO., LTD.), 01 May 2013 (01.05.2013), the whole document	1-22
A	US 2014101772 A1 (PANASONIC CORPORATION), 10 April 2014 (10.04.2014), the whole document	1-22

☐ 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 17 November 2016 (17.11.2016)	Date of mailing of the international search report 02 December 2016 (02.12.2016)
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 WU, Qiong Telephone No.: (86-10) 010-62413702

International application No.
PCT/CN2016/096787

Form PCT/ISA/210 (patent family annex) (July 2009)

A. 主题的分类 G06F 3/023 (2006.01)i; G06F 21/56 (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)) WPI, EPDOC, CNPAT, CNKI, IEEE: 输入法, 键盘, 密码, 私密, 隐私, 秘密, 调用, 截屏, 录屏, 应用, 程序, 安全, input, keyboard, password, secret, private, invoke, application, program, safe, security																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>CN 104281272 A (北京数码视讯科技股份有限公司) 2015年 1月 14日 (2015 - 01 - 14) 说明书第[0026]-[0032]段, 附图7</td> <td>1-22</td> </tr> <tr> <td>Y</td> <td>CN 103853993 A (联想北京有限公司) 2014年 6月 11日 (2014 - 06 - 11) 说明书第[0053]-[0077]段</td> <td>1-22</td> </tr> <tr> <td>A</td> <td>CN 103076988 A (银联商务有限公司) 2013年 5月 1日 (2013 - 05 - 01) 全文</td> <td>1-22</td> </tr> <tr> <td>A</td> <td>US 2014101772 A1 (PANASONIC CORPORATION) 2014年 4月 10日 (2014 - 04 - 10) 全文</td> <td>1-22</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	Y	CN 104281272 A (北京数码视讯科技股份有限公司) 2015年 1月 14日 (2015 - 01 - 14) 说明书第[0026]-[0032]段, 附图7	1-22	Y	CN 103853993 A (联想北京有限公司) 2014年 6月 11日 (2014 - 06 - 11) 说明书第[0053]-[0077]段	1-22	A	CN 103076988 A (银联商务有限公司) 2013年 5月 1日 (2013 - 05 - 01) 全文	1-22	A	US 2014101772 A1 (PANASONIC CORPORATION) 2014年 4月 10日 (2014 - 04 - 10) 全文	1-22
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
Y	CN 104281272 A (北京数码视讯科技股份有限公司) 2015年 1月 14日 (2015 - 01 - 14) 说明书第[0026]-[0032]段, 附图7	1-22															
Y	CN 103853993 A (联想北京有限公司) 2014年 6月 11日 (2014 - 06 - 11) 说明书第[0053]-[0077]段	1-22															
A	CN 103076988 A (银联商务有限公司) 2013年 5月 1日 (2013 - 05 - 01) 全文	1-22															
A	US 2014101772 A1 (PANASONIC CORPORATION) 2014年 4月 10日 (2014 - 04 - 10) 全文	1-22															
☐ 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 11月 17日		国际检索报告邮寄日期 2016年 12月 2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 吴琼 电话号码 (86-10)010-62413702															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/096787

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	104281272	A	2015年 1月 14日	无	
CN	103853993	A	2014年 6月 11日	无	
CN	103076988	A	2013年 5月 1日	无	
US	2014101772	A1	2014年 4月 10日	JP 2014075096 A	2014年 4月 24日