

(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 10 月 20 日 (20.10.2016)



(10) 国际公布号
WO 2016/165537 A1

- (51) 国际专利分类号:
G06F 21/32 (2013.01)
- (21) 国际申请号: PCT/CN2016/077296
- (22) 国际申请日: 2016 年 3 月 25 日 (25.03.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510173017.1 2015 年 4 月 13 日 (13.04.2015) 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乔治城资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。
- (72) 发明人: 及
- (71) 申请人 (仅对美国): 马向阳 (MA, Xiangyang) [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)。 丁保增 (DING, Baozeng) [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,

[见续页]

(54) Title: METHOD FOR CONTROLLING INTELLIGENT TERMINAL AND APPARATUS FOR CONTROLLING INTELLIGENT TERMINAL

(54) 发明名称: 一种控制智能终端的方法及控制智能终端的装置

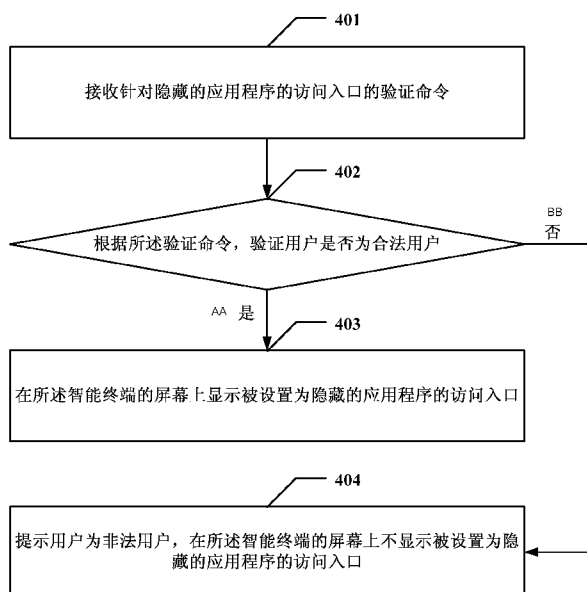


图 4

(57) Abstract: Provided are a method for controlling an intelligent terminal and an apparatus for controlling an intelligent terminal, which are used to provide an application program protecting method which is convenient to operate and high in security. The method comprises: receiving a verification command for an access entry of a hidden application program; performing user validity verification according to the verification command; and if the user validity verification succeeds, displaying the access entry of the application program, set to be hidden, on a screen of an intelligent terminal.

(57) 摘要: 本发明实施例提供了一种控制智能终端的方法及控制智能终端的装置, 用以提供一种操作方便、安全性较高的保护应用程序的方法。该方法包括接收针对隐藏的应用程序的访问入口的验证命令; 根据所述验证命令进行用户合法性验证; 若所述用户合法性验证成功, 则在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口。

- 401 Receiving a verification command for an access entry of a hidden application program
402 Verifying whether a user is a legal user according to the verification command
403 Displaying the access entry of the application program, set to be hidden, on a screen of an intelligent terminal
404 Prompting that the user is an illegal user, so as not to display the access entry of the application program, set to be hidden, on a screen of an intelligent terminal
AA Yes
BB No

WO 2016/165537 A1



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))。

一种控制智能终端的方法及控制智能终端的装置

技术领域

本发明涉及信息安全技术领域，尤其涉及一种控制智能终端的方法及控制智能终端的装置。

背景技术

随着智能终端的日益普及和功能的日益丰富，用户可以随时随地使用智能终端中的各种应用程序来实现相应的功能，这些功能包括支付、扫描、打印、邮件、拍照、录像、录音、电话、短信等等，这些应用程序在给用户带来巨大便利性的同时，也带来了安全隐患，比如伪造短信，冒充支付，邮件泄露等等。

为了保护用户隐私，防止用户信息的泄漏，目前采用的方法是对智能终端中的应用程序分别进行保护，在每一实现需要保护的的功能的应用程序上设置一把锁，或者针对同一功能提供两个应用程序，其中一个应用程序不设置锁，另一应用程序设置一把锁。在用户需要使用设置了锁的应用程序时，先点击该设置了锁的应用程序的图标，之后智能终端上出现输入密码界面，当用户输入密码的密码正确时，打开应用程序，并将打开的应用程序显示给用户，用户进行相应的操作。

例如，在需要保护的的功能为短信功能时，在智能终端上设置带锁的安全邮箱应用程序，并同时设置不带锁的短信应用程序。通常应用程序以图标的形式呈现给用户，图1中所示的是针对短信功能提供设置锁的安全邮箱图标和信息图标的示意图，图2点击安全邮箱图标后呈现给用户的输入密码界面的示意图，图3是成功完成验证后展示给用户的安全邮箱使用界面的示意图。

上述对智能终端中的应用程序分别进行保护的方法实现了对应用程序的保护。但是发明人发现，这些上锁的应用程序的图标直接为攻击者指明了目标，并且这种保护仅仅取决于该应用本身，用户需要保护N个应用程序就要设置N次密码，每打开一个被保护的应用程序就要输入一次密码，智能终端对输入的

该密码进行一次验证。然而，用户可能需要较方便且较安全地使用这些被保护的的应用程序。因此，越来越需要保护这些被保护的的应用程序并使用这些被保护的的应用程序的方法。

发明内容

本发明实施例提供一种控制智能终端的方法及控制智能终端的装置，用以提供一种操作方便、安全性较高的保护应用程序的方法。

本发明实施例提供的一种控制智能终端的方法及控制智能终端的装置具体如下：

一种控制智能终端的方法，包括：

接收针对隐藏的应用程序的访问入口的验证命令；

根据所述验证命令进行用户合法性验证；

若所述用户合法性验证成功，则在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口。

一种控制智能终端的装置，包括：

接收模块，用于接收针对隐藏的应用程序的访问入口的验证命令；

第一验证模块，用于根据所述验证命令进行用户合法性验证，若验证结果为用户合法性验证成功，则触发访问入口显示模块；

访问入口显示模块，用于在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口。

在本发明实施例的方案中，将需要保护的应用程序的访问入口设置为隐藏和合法性验证进行了有机结合，在合法性验证成功时，才将被设置为隐藏的应用程序的访问入口在智能终端的显示屏上显示，进而合法用户可通过该被设置为隐藏的应用程序的访问入口访问该应用程序。由于被设置为隐藏的应用程序的访问入口不被显示在智能终端的屏幕上，因此，非法用户无法从该智能终端的屏幕上获知通过该被设置为隐藏的应用程序的访问入口能进行访问的应用

程序是否存在，这就一定程度上保护了用户信息安全；即使非法用户通过非常规技术手段确定该智能终端中存在该被设置为隐藏的应用程序的访问入口，仍需要进行合法性验证，这一合法性验证也在一定程度上确保了用户信息安全。此外，在本发明实施例中，可以将一个或多个需要保护的应用程序的访问入口设置为隐藏，这种对应用程序的保护方法不依赖于应用本身，并且在将多个需要保护的应用程序的访问入口设置为隐藏时，用户只需输入一次验证命令，方便了用户操作，保证用户信息安全的同时提高了用户体验。

附图说明

图1为本申请背景技术中提供的针对短信功能提供设置锁的安全邮箱图标和信息图标的示意图；

图2为本申请背景技术中提供的点击安全邮箱图标后呈现给用户的输入密码界面的示意图；

图3为本申请背景技术中提供的成功完成验证后展示给用户的安全邮箱使用界面的示意图；

图4为本申请实施例提供的控制智能终端的方法的流程示意图；

图5为本申请实施例提供的利用外接硬件进行用户合法性验证的流程示意图；

图6为本申请实施例提供的利用生物特征进行用户合法性验证的流程示意图；

图7为本申请实施例提供插入与智能手机相匹配的U盾之前智能手机的触摸屏上的显示的图标的示意图；

图8为本申请实施例提供的插入与智能手机相匹配的U盾之后智能手机的触摸屏上的显示的图标的示意图；

图9为本申请实施例提供的在智能手机的触摸屏显示的应用程序的访问入口和对应的按钮的示意图；

图 10 为本申请实施例提供的用户选中的是通话记录图标和视频图标对应的按钮后智能手机的触摸屏上的显示结果示意图；

图 11 为本申请实施例提供的智能手机上显示的搜索框和信息输入组件的示意图；

图 12 为本申请实施例提供的在搜索框中输入的关键字为 shipin 时，接收用户针对所述选择按钮的选中命令后，智能手机的触摸屏上的显示结果示意图；

图 13 为本申请实施例提供的智能手机上显示的第一区域和包含智能手机中的应用程序的图标的第二区域的示意图；

图 14 为本申请实施例提供的在确定被拖拽到第一区域的应用程序的访问入口为通话记录图标和视频图标时智能手机的触摸屏上的显示结果示意图；

图 15 为本申请实施例提供的控制智能终端的装置的结构示意图之一；

图 16 为本申请实施例提供的控制智能终端的装置的结构示意图之二；

图 17 为本申请实施例提供的控制智能终端的装置的结构示意图之三。

具体实施方式

本申请实施例提供了一种控制智能终端的方法及控制智能终端的装置。该方法包括：接收针对隐藏的应用程序的访问入口的验证命令；根据所述验证命令进行用户合法性验证；若所述用户合法性验证成功，则在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口。由于在合法性验证成功时，才将被设置为隐藏的应用程序的访问入口在智能终端的显示屏上显示，这就为用户信息安全提供了双重保障，使得攻击者无法直接从智能终端的显示屏上获知通过被设置为隐藏的应用程序的访问入口能进行访问的应用程序是否存在，也即无法确定是否存在攻击目标，此外，即使是盲攻击，在使用非常规技术手段确定攻击目标存在时，仍需要进行合法性验证，较大程度上确保了包括用户个人隐私信息在内的用户信息安全。

以下结合说明书附图对本发明的优选实施例进行说明，应当理解，此处所描述的优选实施例仅用于说明和解释本发明，并不用于限定本发明。并且在冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

参见图 4，为本申请实施例提供的控制智能终端的方法的流程示意图，该方法包括：

步骤 401：接收针对隐藏的应用程序的访问入口的验证命令；

本步骤 401 中的验证命令即为用于查看及访问隐藏的应用程序的访问入口的验证命令；

所述验证命令可以为密码，也可以为生物学特征（如指纹特征、手势特征、面部特征）。

步骤 402：根据所述验证命令，验证用户是否为合法用户；若验证结果为合法用户，则执行步骤 403；若验证结果为非法用户，则执行步骤 404；

本步骤 402 也即对用户合法性进行验证，验证结果为合法用户则表明用户合法性验证成功；验证结果为非法用户则表明用户合法性验证失败；

上述步骤 401 和步骤 402 中的合法用户验证可以通过外接硬件和/或生物特征来实现，下文中将使用外接硬件和/或生物特征进行用户合法验证的具体实现过程进行详细说明。

步骤 403：在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口；

其中，应用程序的访问入口具体的表现形式可以为应用程序的图标、文字显示的应用程序名称或者应用程序标识号等。通过应用程序的访问入口可以对该应用程序进行访问。

本步骤 403 中，被设置为隐藏显示的应用程序的访问入口，除非用户通过合法性验证，否则在安装该应用程序的智能终端中的任何地方，该应用程序的访问入口均是被隐藏的，对用户来说是不可见的。

步骤 404：提示用户为非法用户，在所述智能终端的屏幕上不显示被设置

为隐藏的应用程序的访问入口。

所述智能终端的屏幕可以是具有触摸功能的显示屏，也可以是不具备触摸功能的显示屏；当然，若执行本发明实施例的方案中需要使用触摸技术，则这里的智能终端的屏幕应当理解为是具有触摸功能的显示屏。

所述隐藏的应用程序的访问入口是预先设置的，可以将一个或大于等于 2 个需要保护的应用程序的访问入口设置为隐藏，这种对应用程序的保护方法不依赖于应用本身，并且在将至少 2 个需要保护的应用程序的访问入口设置为隐藏时，用户只需进行一次验证，方便了用户操作，保证用户信息安全的同时提高了用户体验。

在本步骤 403 中，隐藏的应用程序的访问入口可以是所述智能终端制造商预设的，也可以是用户通过控制智能终端的 APP (Application, 应用软件) 设置的。当然，本发明实施例中也不限于这两种设置方式，还可以使用其它的设置方式。

下面对分别对利用外接硬件和生物特征进行用户合法性验证的过程进行说明：

一、利用外接硬件对用户合法性验证过程，如图 5 所示，包括以下步骤 501 至步骤 508：

步骤 501：对所述智能终端是否连接了外接硬件进行检测，在检测到所述智能终端连接了外接硬件之后执行步骤 502；在没有检测到时，继续进行检测。

步骤 501 中，智能终端与外接硬件的连接可以分为两种，一种是无连接，另一种是有线连接；其中无线连接可以通过 RFID (Radio Frequency Identification, 射频识别) 技术进行的连接或者 NFC (Near Field Communication, 近场通信) 技术进行的连接等；有线连接可以通过外接设备插入智能终端的插槽进行的连接；

无线连接时，智能终端开启 RFID 功能或者 NFC 功能时，外接硬件靠近智能终端，智能终端就可以感知到外接硬件并进行连接，进而控制智能终端的装

置（也即上述步骤 401 至步骤 404 的执行主体）可以对所述智能终端是否通过无线链路连接了外接硬件进行检测。

有线连接时，控制智能终端的装置通过对智能终端插槽内是否插入了外接硬件进行检测，在检测到所述插槽内插入了外接硬件时，控制智能终端的装置即确定检测到所述智能终端连接了外接硬件。

步骤 502：判断所述外接硬件是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件，若判断结果为是，则执行步骤 503；若判断结果为否，则执行步骤 504；

步骤 503：在所述智能终端的屏幕上显示验证命令输入组件，之后执行步骤 505；

所述输入组件可以是实现各种输入方式的输入组件中的一种或多种，例如：实现手写方式进行输入的组件，实现语音方式进行输入的组件（例如虚拟话筒），实现文字、字符和/表情方式进行输入的组件（例如虚拟键盘），实现轨迹方式进行输入的组件（例如图案）等等。可以根据合法的验证命令的表现形式及具体需要进行相应输入组件的显示，本申请实施例中并不对具体为何种输入组件进行限定。

步骤 504：结束用户合法性验证。

步骤 505：接收用户在显示的所述验证命令输入组件中输入的验证命令，之后执行步骤 506；

步骤 506：将所述验证命令提供给所述外接硬件，之后执行步骤 507；

步骤 507：接收所述外接硬件根据所述验证命令进行用户合法性验证后得到的验证结果；之后执行步骤 508；

本步骤 507 中，所述外接硬件可通过将所述验证命令与自身存储的合法的验证命令进行匹配，由匹配结果来确定验证结果；

步骤 508：将接收的所述验证结果作为用户合法性验证结果。

进一步地，在使用外接硬件进行用户合法性验证的情况下，为了实现为

设置为隐藏的应用程序的访问入口的隐藏,较优的,在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后,所述方法还包括:

对所述智能终端是否与所述外接硬件断开了连接进行检测;

在所述外接硬件与所述智能终端为有线连接时,智能终端是与所述外接硬件断开连接可以为外接硬件被从插槽中移出,也可以为利用所述智能终端断开外接硬件与所述智能终端的数据连接但没有从插槽中移出;

在所述外接硬件与所述智能终端为有线连接时,智能终端是与所述外接硬件断开连接可以为外接硬件与所述智能终端断开了数据连接(例如外接硬件远离智能终端和/或智能终端关闭了连接所述外接硬件的功能);

若检测到所述智能终端与所述外接硬件断开了连接,则隐藏被设置为隐藏的应用程序的访问入口。

具体的,所述外接硬件可以为智能卡、USB(Universal Serial Bus,通用串行总线)设备、NFC设备中的任一种,还可以其它的硬件设备,下面分别对外接硬件为智能卡、USB设备和NFC设备时进行用户合法性验证的过程进行说明:

1) 外接硬件为智能卡时:

智能卡类似于普通的外插SD卡(Secure Digital Memory Card,安全数码卡),但与SD卡不同的是,智能卡具有自己的操作系统和文件系统,可对自身的文件系统中的文件执行一定的操作,针对本申请实施例,控制智能终端的装置(该控制智能终端的装置是上述步骤501至步骤508的执行主体,也是上述步骤401至步骤404的执行主体)通过智能卡进行用户合法性验证的过程如下:

步骤a101:控制智能终端的装置检测到智能终端的智能卡插槽中插入了智能卡,之后执行步骤a102;

步骤a101中,控制智能终端的装置检测到智能终端的USB插槽中插入了智能卡也即为检测到所述智能终端连接了智能卡;

步骤a102:控制智能终端的装置读取智能卡中的文件系统,之后执行步骤

a103;

步骤 a103: 控制智能终端的装置判断所述文件系统中是否存在设定的识别文件, 若存在, 则执行步骤 a104, 若不存在, 则执行步骤 a105;

步骤 a104: 控制智能终端的装置确定所述智能卡是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件, 之后执行步骤 a106;

上述步骤 a103 和步骤 a104 也即为根据所述文件系统中是否存在设定的识别文件, 判断所述智能卡是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件的过程;

步骤 a105: 控制智能终端的装置结束用户合法性验证。

步骤 a106: 控制智能终端的装置在所述智能终端的屏幕上显示验证命令输入组件, 之后执行步骤 a107;

在控制智能终端的装置在所述智能终端的屏幕上显示验证命令输入组件之后, 用户可通过显示的验证命令输入组件来输入验证命令;

步骤 a107: 控制智能终端的装置接收用户在显示的所述验证命令输入组件中输入的验证命令, 之后执行步骤 a108;

步骤 a108: 控制智能终端的装置将接收的所述验证命令写入到智能卡的指定密码文件中, 之后执行步骤 a109;

这里将接收的所述验证命令写入到智能卡的指定密码文件中也即将验证命令提供给智能卡;

需要说明的是, 本步骤 a108 中, 为了确保验证命令安全性, 保证传输过程中以及传输给非法智能卡时不被非法用户窃取, 控制智能终端的装置也可以对接收的所述验证命令进行加密, 之后将加密后的验证命令按照预设的格式写入到智能卡的指定密码文件中;

由于能用于访问隐藏的应用程序接口的智能卡是与智能终端配对的智能卡, 因此, 控制该智能终端的装置和智能卡之间已经事先约定好预设的格式以及指定密码文件。

本步骤 a108 执行之后,智能卡将会从该指定密码文件中读取验证命令(或者加密后的验证命令),验证该验证命令是否正确,并将验证结果写入到验证结果文件中;

这里合法的智能卡中事先存储了正确的/合法的验证命令,还可以存储解密算法,该解密算法与所述控制智能终端的装置对验证命令进行加密时的加密算法相对应,进而可以进行验证命令的判断,若智能卡为非法智能卡,其内没有存储正确的/合法的验证命令,也可能没有存储所述解密算法,也就无法进行验证,即使进行了验证,验证结果将会为非法用户,这就进一步确保了隐藏的应用程序的访问入口的安全性。

步骤 a109: 控制智能终端的装置从验证结果文件中读取验证结果,之后执行步骤 a110;

本步骤 a109 也可以说是从智能卡中获取所述验证结果;

步骤 a110: 控制智能终端的装置将读取的所述验证结果作为用户合法性验证结果。

至此,通过智能卡进行用户合法性验证的过程结束。

2) 外接硬件为 USB 设备时:

控制智能终端的装置和所述 USB 设备进行用户合法性验证的过程如下:

步骤 a201: 控制智能终端的装置检测到智能终端的 USB 插槽中插入了 USB 设备,之后执行步骤 a202;

本步骤 a201 之后,所述 USB 设备将向控制智能终端的装置发送身份验证邀约请求,该邀约请求用于邀请所述控制智能终端的装置在该 USB 设备上身份验证;

步骤 a201 中,控制智能终端的装置检测到智能终端的 USB 插槽中插入了 USB 设备也即为检测到所述智能终端连接了 USB 设备;

步骤 a202: 控制智能终端的装置接收所述 USB 设备的发送的携带有设备信息的身份验证邀约请求,之后执行步骤 a203;

步骤 a203: 控制智能终端的装置根据所述身份验证邀约请求中携带的所述设备信息, 判断所述 USB 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件, 若是, 则执行步骤 a204, 若不是, 则执行步骤 a205;

本步骤 203 中, 控制智能终端的装置可以将所述设备信息与自身存储的设备信息进行匹配, 利用匹配结果来判断所述 USB 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件。

步骤 a204: 控制智能终端的装置将验证命令输入组件显示在所述智能终端的屏幕上, 之后执行步骤 a206;

在控制智能终端的装置在所述智能终端的屏幕上显示验证命令输入组件之后, 用户可通过显示的验证命令输入组件来输入验证命令;

步骤 a205: 控制智能终端的装置结束用户合法性验证。

步骤 a206: 控制智能终端的装置接收用户在显示的所述验证命令输入组件中输入的验证命令, 之后执行步骤 a207;

步骤 a207: 控制智能终端的装置将所述验证命令传输给所述 USB 设备, 之后执行步骤 a208;

需要说明的是, 本步骤 a207 中, 为了确保验证命令安全性, 为了确保验证命令安全性, 保证传输过程中以及传输给非法 USB 设备时不被非法用户窃取, 控制智能终端的装置也可以对接收的所述验证命令进行加密, 之后将加密后的验证命令传输给所述 USB 设备;

本步骤 a207 执行之后, USB 设备会将接收的验证命令 (或者加密后的验证命令) 与存储的合法的验证命令进行比较, 验证接收的验证命令是否正确, 并将验证结果;

本步骤 a207 执行之后, 所述 USB 设备将会接收到所述验证命令 (或加密后的验证命令), 验证接收的验证命令是否正确, 以及将验证结果传输给控制智能终端的装置;

这里合法的 USB 设备中事先存储了正确的/合法的验证命令, 还可以存储

解密算法，该解密算法与所述控制智能终端的装置对验证命令进行加密时的加密算法相对应，进而可以进行验证命令的判断，若 USB 设备为非法 USB 设备，其内没有存储正确的验证命令，也可能没有存储所述解密算法，无法对接收到的加密后的验证命令进行解密，也就无法进行验证，即使进行了验证，验证结果将会为非法用户，这就进一步确保了隐藏的应用程序的访问入口的安全性。

步骤 a208: 控制智能终端的装置接收 USB 设备发送的验证结果，之后执行步骤 a209;

步骤 a209: 控制智能终端的装置将接收的所述验证结果作为用户合法性验证结果。

具体的，上述 USB 设备和控制智能终端的设备之间进行通信时，可以采用设定的通信机制进行通信，例如采用套接字（Socket）这种通信机制进行通信，此时可以事先在控制智能终端的装置上存储第一服务程序以及在合法的 USB 设备上存储第二服务程序，该第一服务程序用来监听是否有身份验证邀请请求以及进行数据的收发，该第二服务程序用来要求控制智能终端的装置进行身份验证以及进行数据的收发。

至此，通过 USB 设备进行用户合法性验证的过程结束。

3) 外接硬件为 NFC 设备时:

NFC 技术是由 RFID 技术及互联互通技术整合演变而来，在单一芯片上结合感应式读卡器、感应式卡片和点对点的功能，能在短距离内与兼容设备进行识别和数据交换。

这里利用 NFC 设备进行用户合法性验证，需要智能终端支持并开启 NFC 功能，此时，才能与 NFC 设备进行通信，进而进行下面的验证过程;

具体的，控制智能终端的装置和所述 NFC 设备进行用户合法性验证的过程如下:

步骤 a301: 控制智能终端的装置确定智能终端连接了 NFC 设备，之后执行步骤 a302;

步骤 a302: 控制智能终端的装置读取 NFC 设备中的身份识别信息, 之后执行步骤 a303;

步骤 a303: 控制智能终端的装置根据读取的身份识别信息, 判断所述 NFC 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件, 若判断结果为是, 则执行步骤 a304, 若判断结果为否, 则执行步骤 a305;

具体的, 本步骤 303 中, 控制智能终端的装置将读取的身份识别信息与预先存储的合法的身份识别信息进行对比, 若相同, 则确定所述 NFC 设备是用于对所述隐藏的应用程序的访问入口进行访问的外接硬件; 若不相同, 则确定所述 NFC 设备不是用于对所述隐藏的应用程序的访问入口进行访问的外接硬件;

步骤 a304: 控制智能终端的装置将验证命令输入组件显示在所述智能终端的屏幕上, 之后执行步骤 a306;

在控制智能终端的装置在所述智能终端的屏幕上显示验证命令输入组件之后, 用户可通过显示的验证命令输入组件来输入验证命令;

步骤 a305: 控制智能终端的装置的结束用户合法性验证。

步骤 a306: 控制智能终端的装置接收用户在显示的所述验证命令输入组件中输入的验证命令, 之后执行步骤 a307;

步骤 a307: 控制智能终端的装置将所述验证命令传输给所述 NFC 设备, 之后执行步骤 a308;

本步骤 a307 执行之后, 所述 NFC 设备会接收到所述验证命令, 验证该验证命令是否正确, 以及将验证结果传输给控制智能终端;

这里合法的 NFC 设备中事先存储了正确的验证命令, 进而可以利用该正确的验证命令对接收的所述验证命令进行验证, 若 NFC 设备为非法 NFC 设备, 其中没有存储正确的验证命令, 也就无法进行验证, 即使进行了验证, 验证结果将会为非法用户, 这就进一步确保了隐藏的应用程序的访问入口的安全性。

步骤 a308: 控制智能终端的装置接收 NFC 设备发送的验证结果, 之后执

行步骤 a309;

步骤 a309: 控制智能终端的装置将接收的所述验证结果作为用户合法性验证结果。

至此, 通过 NFC 设备进行用户合法性验证的过程结束。

上述进行用户合法性验证的过程中, 无论是使用智能卡、USB 设备还是使用 NFC 设备均进行了两次验证, 先进行设备验证, 设备验证通过后, 再对用户输入的验证命令进行验证, 相对于现有技术仅使用用户输入的验证命令(如密码)对用户合法性进行验证, 较大程度上提高了用户合法性验证的安全性。

二、利用生物特征对用户合法性验证过程, 如图 6 所示, 包括以下步骤 601 至步骤 604:

步骤 601: 接收用户针对隐藏的应用程序的访问入口的验证开始命令;

步骤 602: 启动用于进行生物特征扫描的扫描工具;

这里的生物特征包括: 声音特征、指纹特征、虹膜特征、手势特征和面部特征中的一种或多种。

针对声音特征, 可以在所述智能终端的显示屏上显示一段文本和虚拟话筒, 然后提示用户朗读此段文本, 进而可以得到声音特征;

针对指纹特征, 此时需要智能终端支持指纹扫描, 启动指纹扫描设备后, 用户可在指纹扫描设备上进行指纹特征的录入, 进而控制智能终端的装置可以获得指纹特征;

针对虹膜特征, 此时需要智能终端支持虹膜扫描, 启动虹膜扫描设备后, 用户双眼对准虹膜设备进而进行虹膜特征的录入, 进而控制智能终端的装置可以获得虹膜特征;

针对手势特征和面部特征, 需要启动智能终端的摄像功能, 可以利用现有的手势识别技术和人脸识别技术进行识别, 进而获得手势特征和面部特征;

步骤 603: 接收扫描工具扫描到的生物特征, 将该扫描到的生物特征作为针对隐藏的应用程序的访问入口的验证命令;

步骤 604: 利用之前存储的合法用户的生物特征对本次扫描到的生物特征进行用户合法性验证。

本步骤 604 中, 可将存储的合法用户的生物特征进行对本次扫描到的生物特征进行匹配, 若相似度大于设定值, 则确定用户为合法用户; 否则, 确定用户为非法用户。

具体的生物特征匹配算法可参考现有的相关算法, 这里不再赘述。

至此, 利用生物特征对用户合法性验证的过程结束。

进一步地, 在使用生物特征对用户合法性验证时, 为了实现对为设置为隐藏的应用程序的访问入口的隐藏, 较优的, 在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后, 所述方法还包括:

接收所述扫描工具扫描的生物特征;

利用之前存储的合法用户的生物特征对扫描工具本次扫描到的生物特征进行用户合法性验证;

若用户合法性验证成功, 则隐藏所述被设置为隐藏的应用程序的访问入口。

下面通过图 7 和图 8 对使用 USB 设备进行控制智能终端的效果进行说明:

假设智能终端为智能手机, 应用程序的访问入口的具体表现形式为图标, 智能手机中全部的图标为时钟图标、视频图标、手机图标、通话记录图标、信息图标、设置图标和 S 备忘录图标, 预先设置的被隐藏的应用程序的图标为通话记录图标和视频图标, 插入该智能手机的 USB 插槽的 USB 设备通过了用户合法性验证, 则图 7 和图 8 分别给出了插入 USB 设备之前及之后智能手机的触摸屏上的显示的图标的示意图。

上述隐藏的应用程序入口是事先被设置的, 下面对隐藏的应用程序入口的设置进行说明:

在隐藏的应用程序的访问入口是用户设置时, 例如用户通过 APP 设置, 可通过以下步骤 A 至步骤 C 设置隐藏的应用程序的访问入口:

步骤 A: 向用户提供用于设置隐藏的应用程序的访问入口的界面;

步骤 B: 接收用户的选中命令, 并确定该选中命令所对应的应用程序的访问入口为隐藏的应用程序的访问入口;

步骤 C: 隐藏确定出的所述应用程序的访问入口。

优选地, 可以通过以下方式 1、方式 2 和方式 3 中的任一种方式来设置:

方式 1:

该方式 1 通俗地说即为浏览方式, 包括以下步骤 b1 至步骤 b4:

步骤 b1: 接收用户的设置隐藏的应用程序的访问入口开始命令;

步骤 b2: 将所述智能终端中各应用程序的访问入口和对应的选择按钮显示在屏幕上;

在本步骤 b2 中, 假设应用程序的访问入口的具体表现形式仍是图标, 智能手机中的应用程序的访问入口包括: 时钟图标、视频图标、手机图标、通话记录图标、信息图标、设置和 S 备忘录图标, 此时在智能手机的触摸屏显示的应用程序的图标和对应的按钮可以如图 9 所示。

步骤 b3: 接收用户针对所述选择按钮的选中命令, 并将选中命令选中的选择按钮对应的应用程序的访问入口确定为隐藏的应用程序的访问入口。

在本步骤 b3 中, 在图 9 的基础上, 假设用户选中的是通话记录图标和视频图标对应的选择按钮, 则用户选择后智能手机的触摸屏上的显示可以如图 10 所示。

步骤 b4: 隐藏确定出的所述应用程序的访问入口;

步骤 b5: 接收用户的设置隐藏的应用程序的访问入口完成命令;

本步骤 b5 中, 用户按下图 10 中的完成按钮即可, 此时, 移动终端即可获知用户已经完成了对需要隐藏的应用程序的访问入口的设置。

需要说明的是, 上述步骤 b1 和步骤 b5 是本申请实施例的可选步骤, 也可以不执行步骤 b1 和步骤 b5。

上述步骤 b4 中, 可以利用以下方式一或者方式二隐藏被设置为隐藏的应

用程序的访问入口：

方式一：将被设置为隐藏的应用程序的访问入口的可见性状态由可见状态更改为不可见状态；

方式二：将确定为隐藏的应用程序的访问入口的可见性状态由可见状态更改为不可见状态且将通过该隐藏的应用程序的访问入口被访问的应用程序的可用性状态由可用状态更改为不可用状态；

由于将应用程序的访问入口的可见性状态更改为了不可见，这就使得该应用程序的访问入口不能被移动终端显示，也就实现了通过上述方式一和方式二均实现了将被选中的每一选择按钮对应的应用程序的访问入口进行隐藏，此时，智能终端的屏幕上被选中的每一选择按钮对应的应用程序的访问入口均不存在了。此外，方式二中还将通过该隐藏的应用程序的访问入口被访问的应用程序的可用性状态可用性状态更改为了不可用状态，使得即使通过其他方式获得用户使用该被隐藏的应用程序的访问入口所能访问的应用程序的过程中保存的用户信息文件，由于该应用程序是不可用的，因此也无法打开该获得的该用户信息文件，进一步确保了用户信息的安全。

方式 2:

该方式 2 通俗地说即为搜索方式，可包括以下步骤 c1 至步骤 c7:

步骤 c1: 接收用户的设置隐藏的应用程序的访问入口开始命令；

步骤 c2: 将搜索框和用于进行信息的输入的输入组件显示在屏幕上，所述搜索框用于接收用户输入的设置隐藏的应用程序的访问入口；

若智能终端为智能手机，则本步骤 c2 中智能手机上显示的搜索框和信息输入组件可以如图 11 所示。

步骤 c3: 接收用户在搜索框中输入的关键字信息；

步骤 c4: 根据所述关键字信息查找应用程序的访问入口，并将查找到的应用程序的访问入口和对应的选择按钮显示在屏幕上；

步骤 c5: 接收用户针对所述选择按钮的选中命令，并将该选择按钮对应的

应用程序的访问入口作为该选中命令所对应的应用程序的访问入口。

若步骤 c3 中输入的关键字为 shipin，则本步骤 b5 中接收用户针对所述选择按钮的选中命令后智能手机的触摸屏上的显示可以如图 12 所示。

步骤 c6：将选择按钮对应的应用程序的访问入口隐藏。

具体可利用上述方式一或方式二实现对所述隐藏的应用程序的访问入口的隐藏；

步骤 c7：接收用户的设置隐藏的应用程序的访问入口完成命令。

在上述执行一次步骤 c3、步骤 c4 和步骤 c5，用户可能只选择一个需要设置为隐藏的应用程序的访问入口，智能终端接收本次用户针对所述选择按钮的选中命令后，可将搜索框中的关键字清空，提示用户可继续进行搜索，或者在获知用户在键盘区域触发了“下一个”按键时，搜索框中的关键字清空，提示用户可继续进行搜索，继续进行隐藏的应用程序的访问入口的设置，在用户输入关键字时，继续执行步骤 c3、步骤 c4 和步骤 c5 直至接收到用户的设置隐藏的应用程序的访问入口完成命令。

上述步骤 c1 和步骤 c7 是本申请实施例的可选步骤，也可以不执行步骤 c1 和步骤 c7。

方式 3：

该方式 3 通俗地说即为拖拽方式，包括以下步骤 d1 至步骤 d6：

步骤 d1：接收用户的设置隐藏的应用程序的访问入口开始命令；

步骤 d2：将第一区域和第二区域显示在屏幕上，其中，在第二区域显示所述智能终端中的应用程序的访问入口，在第一区域显示用户的选中命令所对应的应用程序的访问入口；

若智能终端为智能手机，则本步骤 d2 中智能手机上显示的第一区域和包含智能手机中的应用程序的图标的第二区域的示意图可以如图 13 所示。图 13 中显示的是将智能终端的屏幕竖分为两个区域，也可以横分为两个区域，还可以借助在智能终端的屏幕上显示封闭的图形（如圆形、正方形、长方形、六边

形等等)来实现两个区域的划分,将封闭的线条以内的区域作为第一区域,将封闭的线条以外的区域作为第二区域,或者将封闭的线条以内的区域作为第二区域,将封闭的线条以外的区域作为第一区域。

步骤 d3: 接收用户以将第二区域内的应用程序的访问入口拖入第一区域内的形式发出的选中命令,并确定拖入第一区域内的应用程序的访问入口作为该选中命令所对应的应用程序的访问入口为隐藏的应用程序;

在本步骤 d3 中,在图 13 的基础上,假设确定被拖入到第一区域的应用程序的访问入口为通话记录图标和视频图标,智能手机的触摸屏上的显示可以如图 14 所示。

步骤 d4: 隐藏第一区域内的应用程序的访问入口;

步骤 d5: 接收用户的设置隐藏的应用程序的访问入口完成命令;

上述步骤 d1 和步骤 d5 是本发明实施例的可选步骤,也可以不执行步骤 d1 和步骤 d5。

具体可利用上述方式一或方式二实现对所述被设置为隐藏的应用程序的访问入口的隐藏。

上述方法 1、方法 2 和方法 3 中,若使用方式一设置隐藏的应用程序的访问入口,则所述在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口,包括:

将确定为隐藏的应用程序的访问入口的可见性状态由不可见状态更改为可见状态;

若使用方式二设置隐藏的应用程序的访问入口,则所述在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口,包括:

将确定为隐藏的应用程序的访问入口的可见性状态由不可见状态更改为可见状态且将通过该隐藏的应用程序的访问入口所能访问的应用程序的可用性状态由不可用状态更改为可用状态。

进一步地,在上述步骤 401 至步骤 403 的基础上,所述方法还包括:

在接收到隐藏应用程序的访问入口的命令时，或者在检测到用户在设定时长内未对任何一个隐藏的应用程序进行操作时，或者在确定用户完成对隐藏的应用程序的访问入口的设置时，隐藏所述被设置为隐藏的应用程序的访问入口。

这里可通过上述方式一或者方式二隐藏所述被设置为隐藏的应用程序的访问入口。

优选地，在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口，包括：

将所述隐藏的应用程序的访问入口与未隐藏的应用程序的访问入口在不同的窗口中或者在同一窗口中显示；

或者，

在所述智能终端的屏幕上显示浮动窗口，所述浮动窗口中显示被设置为隐藏的应用程序的访问入口。

基于同一发明构思，本申请实施例还提供了一种控制智能终端的装置，由于该控制智能终端的装置所解决问题的原理与前述控制智能终端的方法相似，因此该控制智能终端的装置实施可以参见前述方法的实施，重复之处不再赘述。

如图 15 所示，其为本申请实施例提供的一控制智能终端的装置的结构示意图，包括：接收模块 151、第一验证模块 152 和访问入口显示模块 153；其中：

接收模块 151，用于接收针对隐藏的应用程序的访问入口的验证命令；

第一验证模块 152，用于根据所述验证命令进行用户合法性验证，若验证结果为用户合法性验证成功，则触发访问入口显示模块；

访问入口显示模块 153，用于在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口。

较优的，所述装置还包括：

设置模块 154，用于通过以下方式设置隐藏的应用程序的访问入口：向用户提供用于设置隐藏的应用程序的访问入口的界面；接收用户的选中命令，并确定该选中命令所对应的应用程序为隐藏的应用程序；隐藏确定出的所述应用程序的访问入口。

较优的，所述装置还包括：

隐藏模块 155，用于在接收到隐藏应用程序的访问入口的命令时，或者在检测到用户在设定时长内未对任何一个隐藏的应用程序进行操作时，或者在确定用户完成对隐藏的应用程序的访问入口的设置时，隐藏所述隐藏的应用程序的访问入口。

较优的，所述访问入口显示模块 153，具体用于将所述隐藏的应用程序的访问入口与未隐藏的应用程序的访问入口在不同的窗口中或者在同一窗口中显示；或者在所述智能终端的屏幕上显示浮动窗口，所述浮动窗口中显示被设置为隐藏的应用程序的访问入口。

具体的，可以仅使用密码对用户的合法性进行验证，也可以利用外接硬件对用户合法性进行验证，还可以利用生物特征对用户合法性进行验证，在利用外接硬件对用户进行合法性验证时的控制智能终端的装置的结构示意图如图 16 所示；在利用外接硬件对用户进行合法性验证时的控制智能终端的装置的结构示意图如图 17 所示；

图 16 中，控制智能终端的装置除包括接收模块 151、第一验证模块 152 和访问入口显示模块 153；还包括：

检测模块 161，用于在接收模块接收针对隐藏的应用程序的访问入口的验证命令之前，对所述智能终端是否连接了外接硬件进行检测，在检测到所述智能终端连接了外接硬件时，触发判断模块 162；

判断模块 162，用于判断所述外接硬件是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件，在判断结果为是时，触发输入组件显示模块 163；

输入组件显示模块 163，用于在所述智能终端的屏幕上显示验证命令输入组件；

所述接收模块 151，具体用于接收用户在显示的所述验证命令输入组件中输入的验证命令。

较优的，所述第一验证模块 152，具体用于将所述验证命令提供给所述外接硬件；获取所述外接硬件根据所述验证命令进行用户合法性验证后得到的验证结果；将获取的所述验证结果作为用户合法性验证结果。

较优的，所述外接硬件为智能卡、通用串行总线 USB 设备或近场通信 NFC 设备。

较优的，所述判断模块 162，具体用于在所述外接硬件为智能卡时，读取所述智能卡中的文件系统；根据所述文件系统中是否存在设定的识别文件，判断所述智能卡是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件；或者，

所述判断模块 162，具体用于在所述外接硬件为 USB 设备时，接收所述 USB 设备发送的携带有设备信息的身份验证邀约请求；根据所述身份验证邀约请求中携带的所述设备信息，判断所述 USB 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件；或者，

所述判断模块 162，具体用于在所述外接硬件为 NFC 设备时，读取所述 NFC 设备中的身份识别信息；根据所述身份识别信息，判断所述 NFC 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件。

所述装置还包括隐藏模块 164；

所述检测模块 161，还用于在访问入口显示模块在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后，对所述智能终端是否与外接硬件断开了连接进行检测，在检测到所述智能终端与所述外接硬件断开了连接时，触发所述隐藏模块 164；

所述隐藏模块 164，用于隐藏被设置为隐藏的应用程序的访问入口。

图 17 中，控制智能终端的装置除包括接收模块 151、第一验证模块 152 和访问入口显示模块 153；还包括：启动模块 171；

所述接收模块 151，还用于在接收针对隐藏的应用程序的访问入口的验证命令之前，接收用户针对隐藏的应用程序的访问入口的验证开始命令；

所述装置还包括：

启动模块 171，用于启动用于进行生物特征扫描的扫描工具；

所述接收模块 151，具体用于接收扫描工具扫描到的生物特征，将该扫描到的生物特征作为针对隐藏的应用程序的访问入口的验证命令。

较优的，所述生物特征包括：声音特征、指纹特征、虹膜特征、手势特征和面部特征中的一种或多种。

所述第一验证模块 152，具体用于利用之前存储的合法用户的生物特征对扫描工具扫描到的生物特征进行用户合法性验证。

较优的，所述装置还包括第二验证模块 172 和隐藏模块 173；

所述接收模块 151，还用于在访问入口显示模块在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后，接收所述扫描工具扫描的生物特征，将接收的生物特征输出给第二验证模块 172；

所述第二验证模块 172，用于利用之前存储的合法用户的生物特征对扫描工具本次扫描到的生物特征进行用户合法性验证，若验证结果为用户合法性验证成功，则触发隐藏模块 173；

所述隐藏模块 173，用于隐藏所述被设置为隐藏的应用程序的访问入口。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本发明实施例可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式实现。基于这样的理解，本发明实施例的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是 CD-ROM，U 盘，移动硬盘等）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）执行本发明各个实施例所述的方法。

本领域技术人员可以理解附图只是一个优选实施例的示意图，附图中的模块或流程并不一定是实施本发明所必须的。

本领域技术人员可以理解实施例中终端中的模块可以按照实施例描述进行分布于实施例的终端中，也可以进行相应变化位于不同于本实施例的一个或多个终端中。上述实施例的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权 利 要 求 书

- 1、一种控制智能终端的方法，其特征在于，包括：
接收针对隐藏的应用程序的访问入口的验证命令；
根据所述验证命令进行用户合法性验证；
若所述用户合法性验证成功，则在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口。
- 2、如权利要求 1 所述的方法，其特征在于，在接收针对隐藏的应用程序的访问入口的验证命令之前，所述方法还包括：
检测到所述智能终端连接了外接硬件；
判断所述外接硬件是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件；
若判断结果为是，则在所述智能终端的屏幕上显示验证命令输入组件；
所述接收针对隐藏的应用程序的访问入口的验证命令，包括：
接收用户在显示的所述验证命令输入组件中输入的验证命令。
- 3、如权利要求 2 所述的方法，其特征在于，所述根据所述验证命令进行用户合法性验证，包括：
将所述验证命令提供给所述外接硬件；
获取所述外接硬件根据所述验证命令进行用户合法性验证后得到的验证结果；
将获取的所述验证结果作为用户合法性验证结果。
- 4、如权利要求 2 所述的方法，其特征在于，所述外接硬件为智能卡、通用串行总线 USB 设备或近场通信 NFC 设备。
- 5、如权利要求 4 所述的方法，其特征在于，
在所述外接硬件为智能卡时，所述判断所述外接硬件是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件，包括：读取所述智能卡中的文件系统；根据所述文件系统中是否存在设定的识别文件，判断所述智能卡是否

为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件；或者，

在所述外接硬件为 USB 设备时，所述判断所述外接硬件是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件，包括：接收所述 USB 设备发送的携带有设备信息的身份验证邀约请求；根据所述身份验证邀约请求中携带的所述设备信息，判断所述 USB 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件；或者，

在所述外接硬件为 NFC 设备时，所述判断所述外接硬件是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件，包括：读取所述 NFC 设备中的身份识别信息；根据所述身份识别信息，判断所述 NFC 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件。

6、如权利要求 2 所述的方法，其特征在于，在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后，所述方法还包括：

检测到所述智能终端与所述外接硬件断开了连接；

隐藏被设置为隐藏的应用程序的访问入口。

7、如权利要求 1 所述的方法，其特征在于，在接收针对隐藏的应用程序的访问入口的验证命令之前，所述方法还包括：

接收用户针对隐藏的应用程序的访问入口的验证开始命令；

启动用于进行生物特征扫描的扫描工具；

所述接收针对隐藏的应用程序的访问入口的验证命令，包括：

接收扫描工具扫描到的生物特征，将该扫描到的生物特征作为针对隐藏的应用程序的访问入口的验证命令。

8、如权利要求 7 所述的方法，其特征在于，所述生物特征包括：声音特征、指纹特征、虹膜特征、手势特征和面部特征中的一种或多种。

9、如权利要求 7 所述的方法，其特征在于，所述根据所述验证命令进行用户合法性验证，包括：

利用之前存储的合法用户的生物特征对扫描工具扫描到的生物特征进行用户合法性验证。

10、如权利要求 7 所述的方法，其特征在于，在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后，所述方法还包括：

接收所述扫描工具扫描的生物特征；

利用之前存储的合法用户的生物特征对扫描工具本次扫描到的生物特征进行用户合法性验证；

若用户合法性验证成功，则隐藏所述被设置为隐藏的应用程序的访问入口。

11、如权利要求 1 所述的方法，其特征在于，通过以下方式设置隐藏的应用程序的访问入口：

向用户提供用于设置隐藏的应用程序的访问入口的界面；

接收用户的选中命令，并确定该选中命令所对应的应用程序的访问入口为隐藏的应用程序的访问入口；

隐藏确定出的所述应用程序的访问入口。

12、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

在接收到隐藏应用程序的访问入口的命令时，或者在检测到用户在设定时长内未对任何一个隐藏的应用程序进行操作时，或者在确定用户完成对隐藏的应用程序的访问入口的设置时，隐藏所述被设置为隐藏的应用程序的访问入口。

13、如权利要求 1 所述的方法，其特征在于，在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口，包括：

将所述隐藏的应用程序的访问入口与未隐藏的应用程序的访问入口在不同的窗口中或者在同一窗口中显示；或者，

在所述智能终端的屏幕上显示浮动窗口，所述浮动窗口中显示被设置为隐藏的应用程序的访问入口。

14、一种控制智能终端的装置，其特征在于，包括：

接收模块，用于接收针对隐藏的应用程序的访问入口的验证命令；

第一验证模块，用于根据所述验证命令进行用户合法性验证，若验证结果为用户合法性验证成功，则触发访问入口显示模块；

访问入口显示模块，用于在所述智能终端的屏幕上显示被设置为隐藏的应

用程序的访问入口。

15、如权利要求 14 所述的装置，其特征在于，所述装置还包括：

检测模块，用于在接收模块接收针对隐藏的应用程序的访问入口的验证命令之前，对所述智能终端是否连接了外接硬件进行检测，在检测到所述智能终端连接了外接硬件时，触发判断模块；

判断模块，用于判断所述外接硬件是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件，在判断结果为是时，触发输入组件显示模块；

输入组件显示模块，用于在所述智能终端的屏幕上显示验证命令输入组件；

所述接收模块，具体用于接收用户在显示的所述验证命令输入组件中输入的验证命令。

16、如权利要求 15 所述的装置，其特征在于，所述第一验证模块，具体用于将所述验证命令提供给所述外接硬件；获取所述外接硬件根据所述验证命令进行用户合法性验证后得到的验证结果；将获取的所述验证结果作为用户合法性验证结果。

17、如权利要求 15 所述的装置，其特征在于，所述外接硬件为智能卡、通用串行总线 USB 设备或近场通信 NFC 设备。

18、如权利要求 17 所述的装置，其特征在于，所述判断模块，具体用于在所述外接硬件为智能卡时，读取所述智能卡中的文件系统；根据所述文件系统中是否存在设定的识别文件，判断所述智能卡是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件；或者，

所述判断模块，具体用于在所述外接硬件为 USB 设备时，接收所述 USB 设备发送的携带有设备信息的身份验证邀约请求；根据所述身份验证邀约请求中携带的所述设备信息，判断所述 USB 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件；或者，

所述判断模块，具体用于在所述外接硬件为 NFC 设备时，读取所述 NFC 设备中的身份识别信息；根据所述身份识别信息，判断所述 NFC 设备是否为用于对所述隐藏的应用程序的访问入口进行访问的外接硬件。

19、如权利要求 15 所述的装置，其特征在于，所述装置还包括隐藏模块；

所述检测模块，还用于在访问入口显示模块在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后，对所述智能终端是否与外接硬件断开了连接进行检测，在检测到所述智能终端与所述外接硬件断开了连接时，触发所述隐藏模块；

所述隐藏模块，用于隐藏被设置为隐藏的应用程序的访问入口。

20、如权利要求 14 所述的装置，其特征在于，所述接收模块，还用于在接收针对隐藏的应用程序的访问入口的验证命令之前，接收用户针对隐藏的应用程序的访问入口的验证开始命令；

所述装置还包括：

启动模块，用于启动用于进行生物特征扫描的扫描工具；

所述接收模块，具体用于接收扫描工具扫描到的生物特征，将该扫描到的生物特征作为针对隐藏的应用程序的访问入口的验证命令。

21、如权利要求 20 所述的装置，其特征在于，所述装置还包括第二验证模块和隐藏模块；

所述接收模块，还用于在访问入口显示模块在所述智能终端的屏幕上显示被设置为隐藏的应用程序的访问入口之后，接收所述扫描工具扫描的生物特征，将接收的生物特征输出给第二验证模块；

所述第二验证模块，用于利用之前存储的合法用户的生物特征对扫描工具本次扫描到的生物特征进行用户合法性验证，若验证结果为用户合法性验证成功，则触发隐藏模块；

所述隐藏模块，用于隐藏所述被设置为隐藏的应用程序的访问入口。



图 1



图 2



图 3

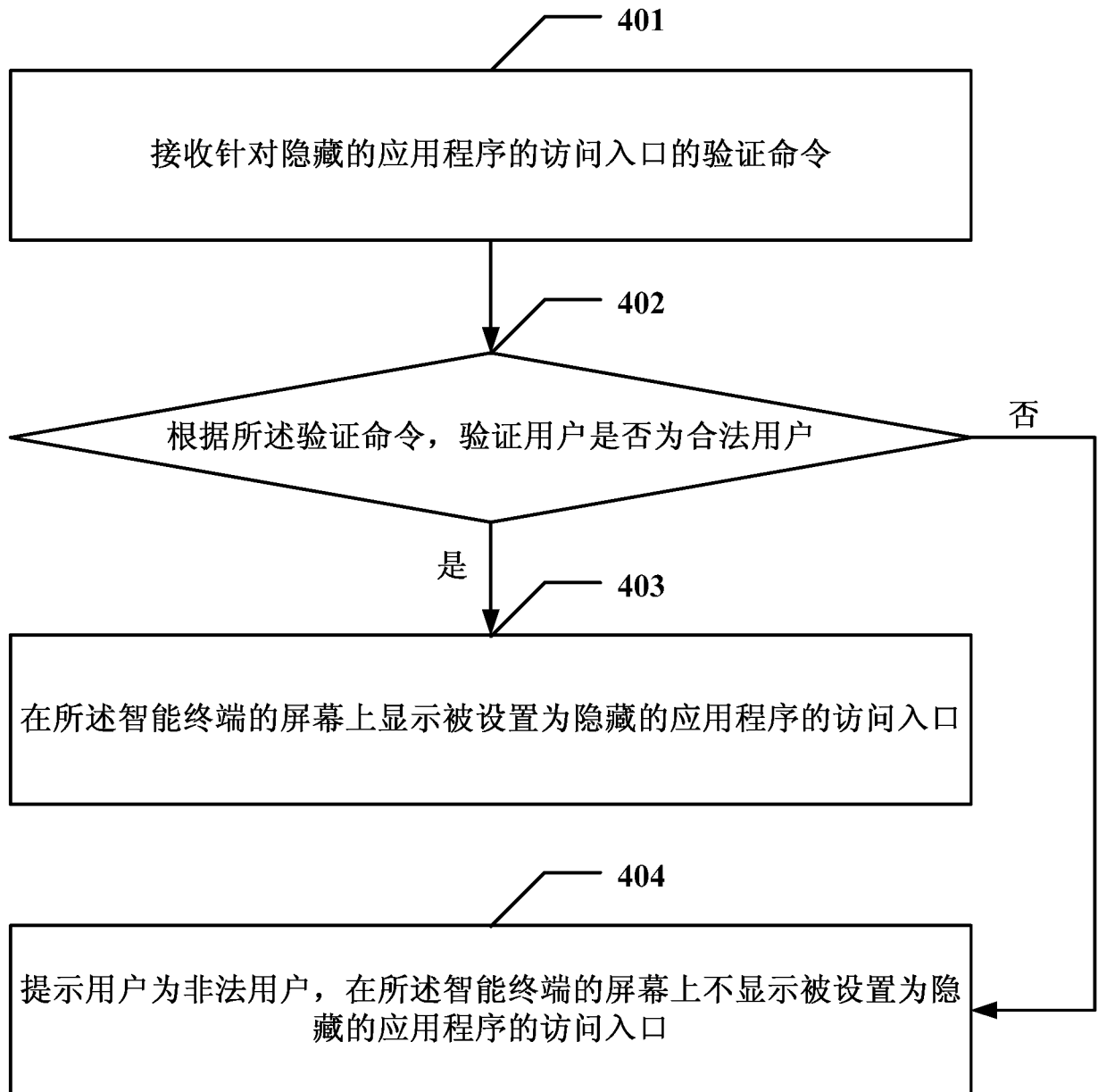


图 4

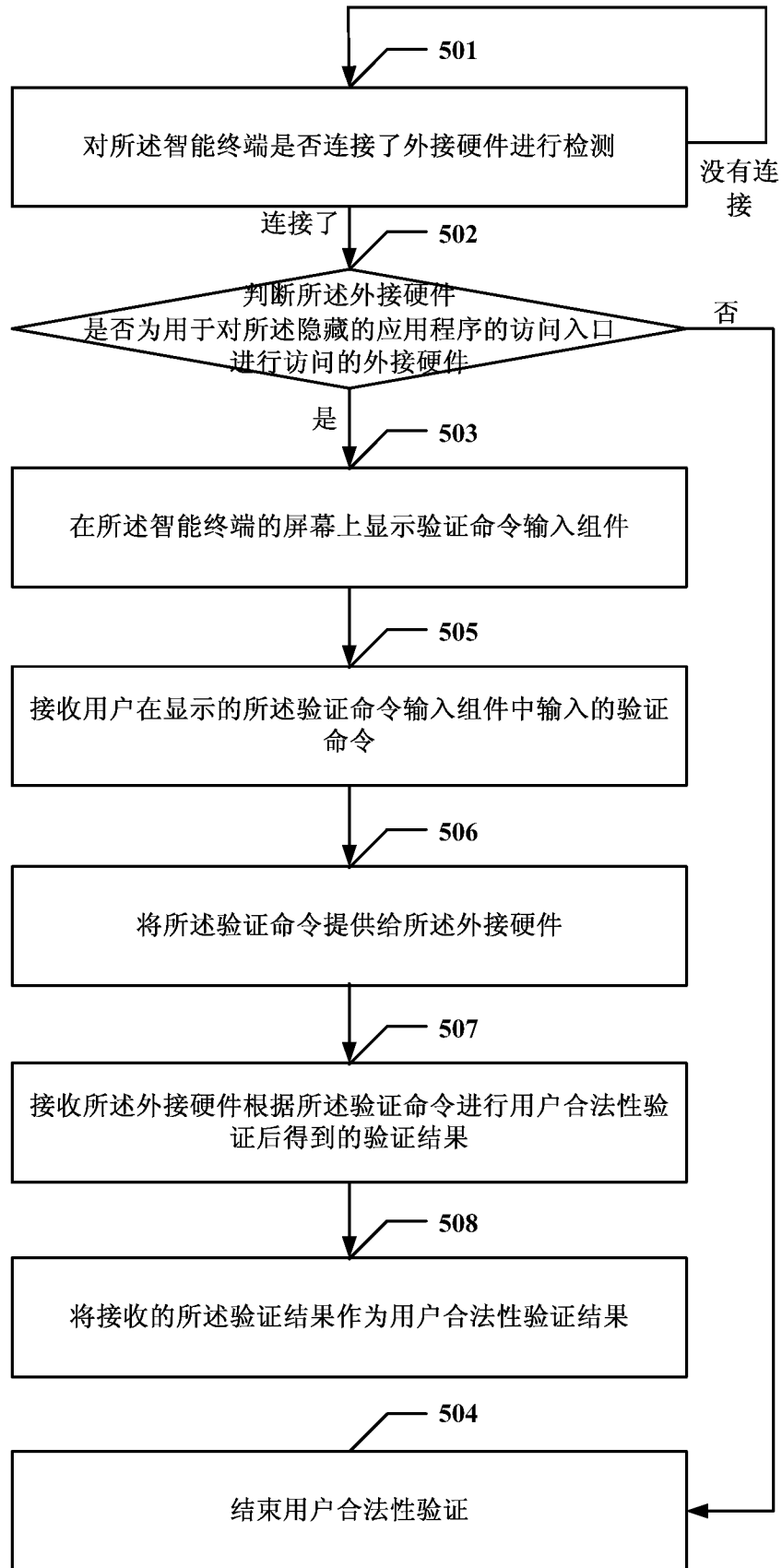


图 5

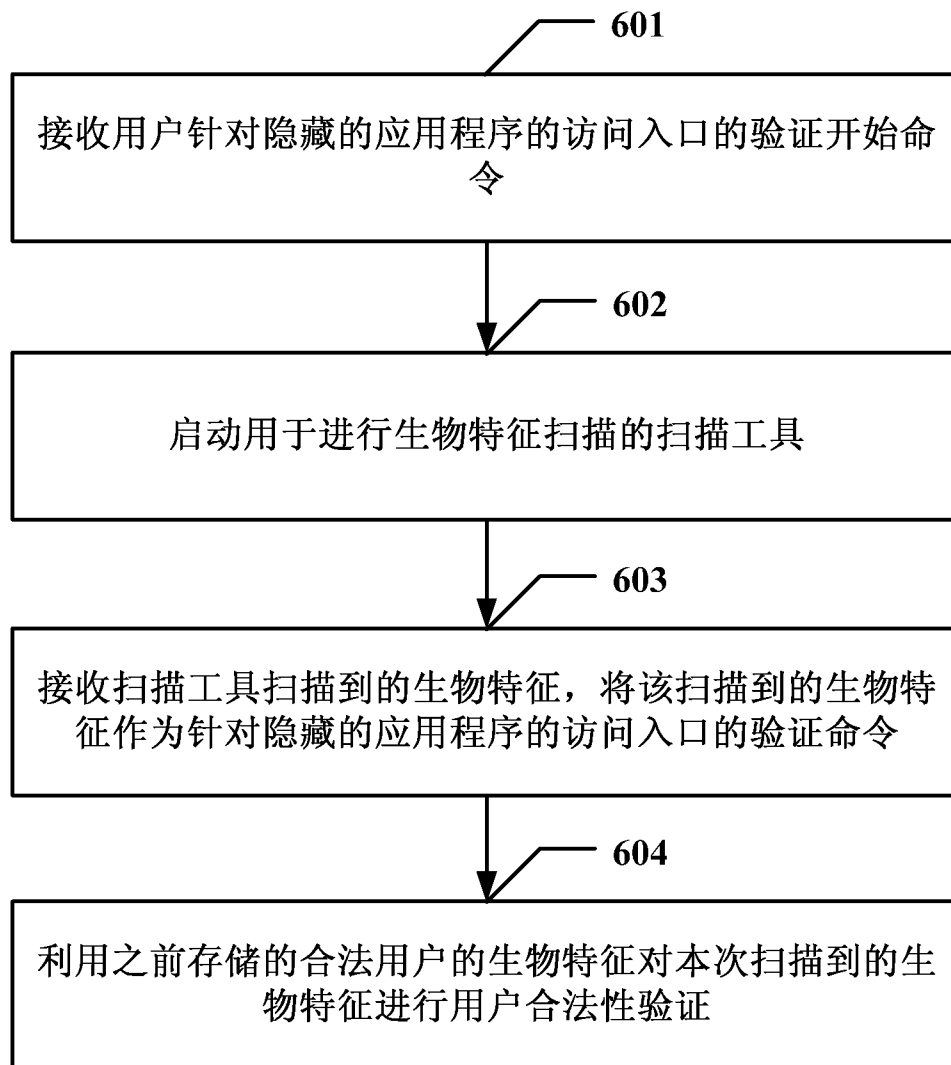


图 6

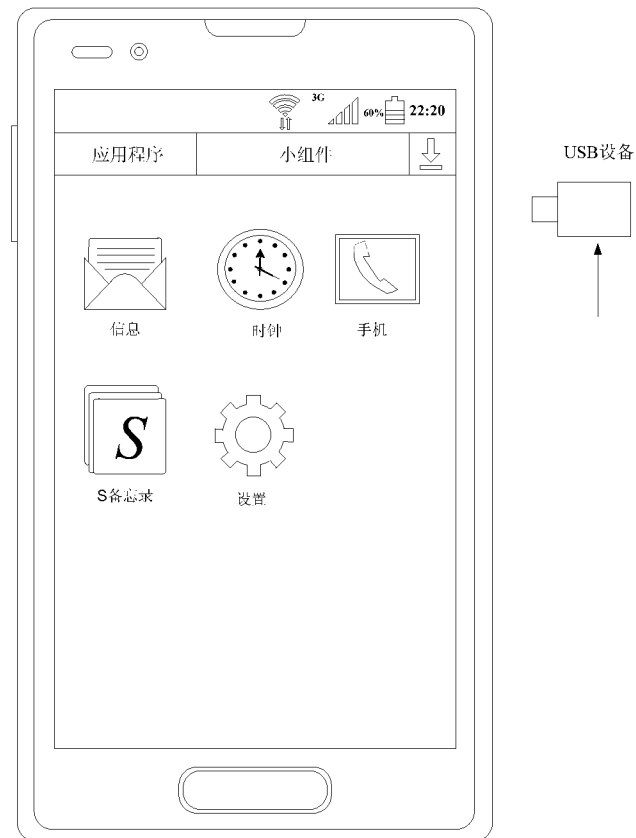


图 7



图 8

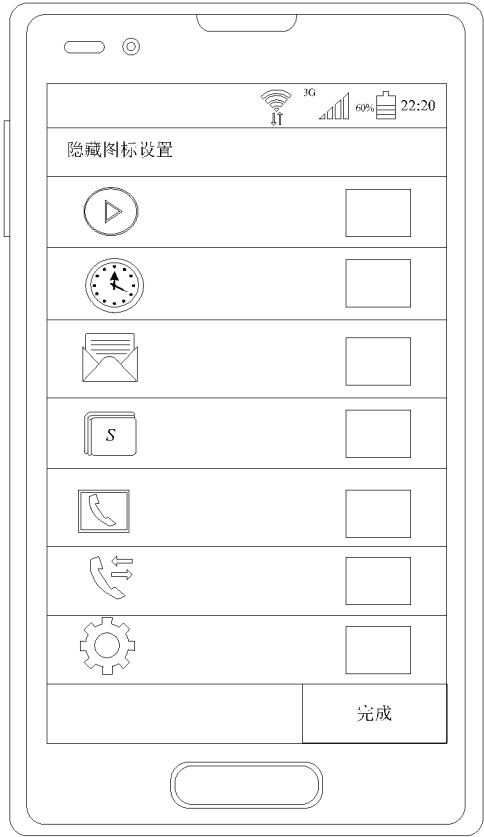


图 9

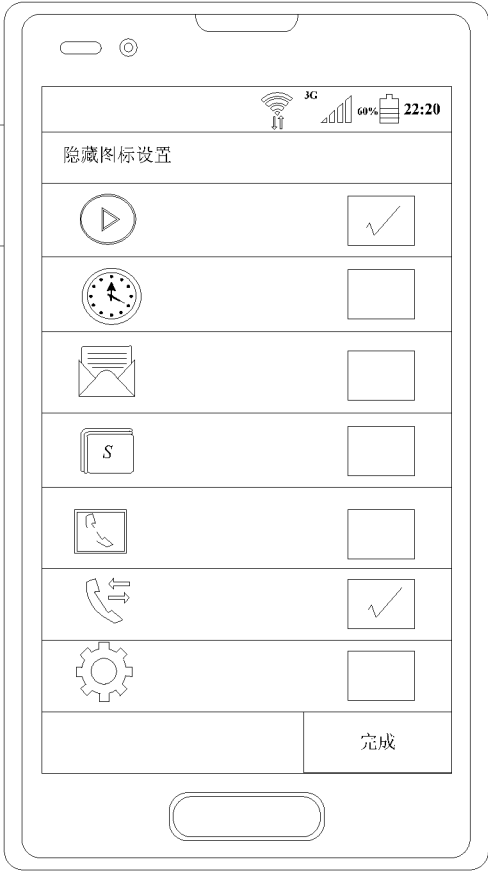


图 10

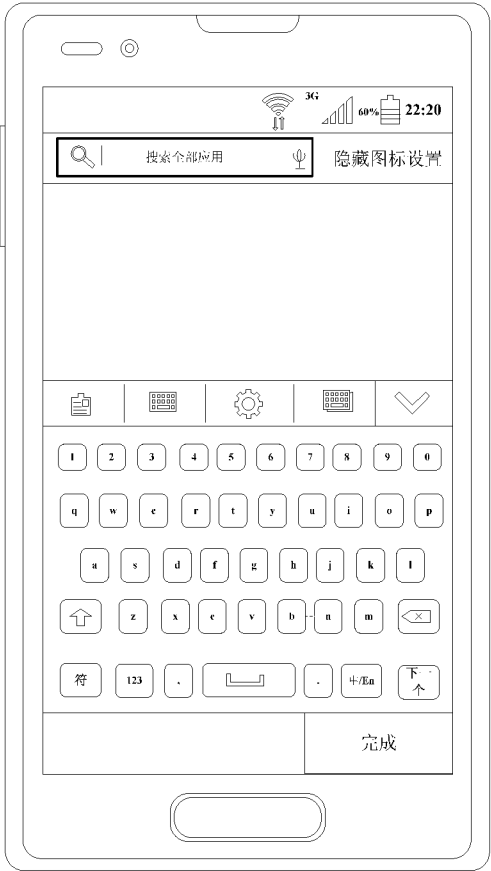


图 11



图 12

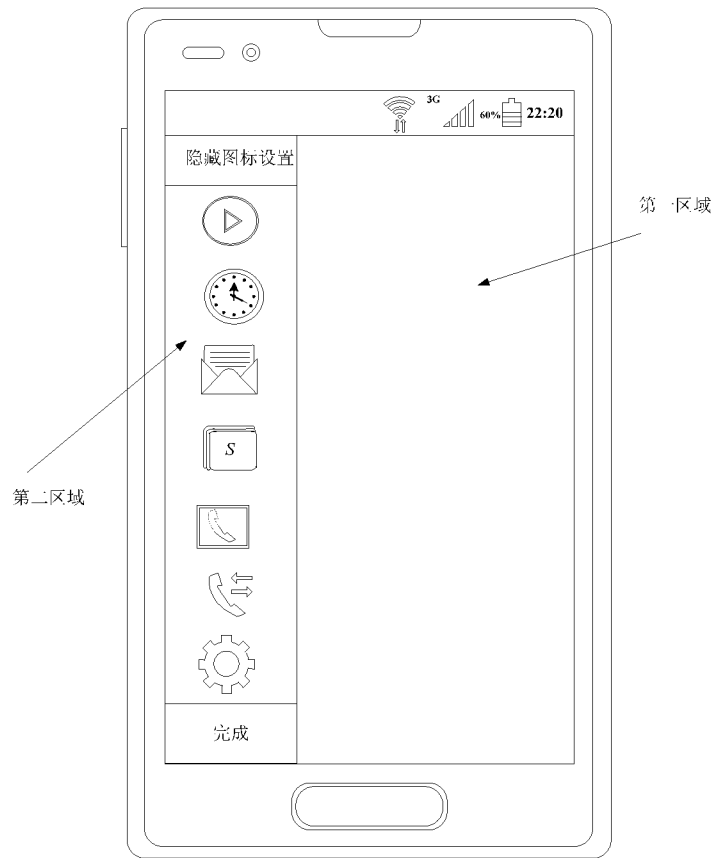


图 13

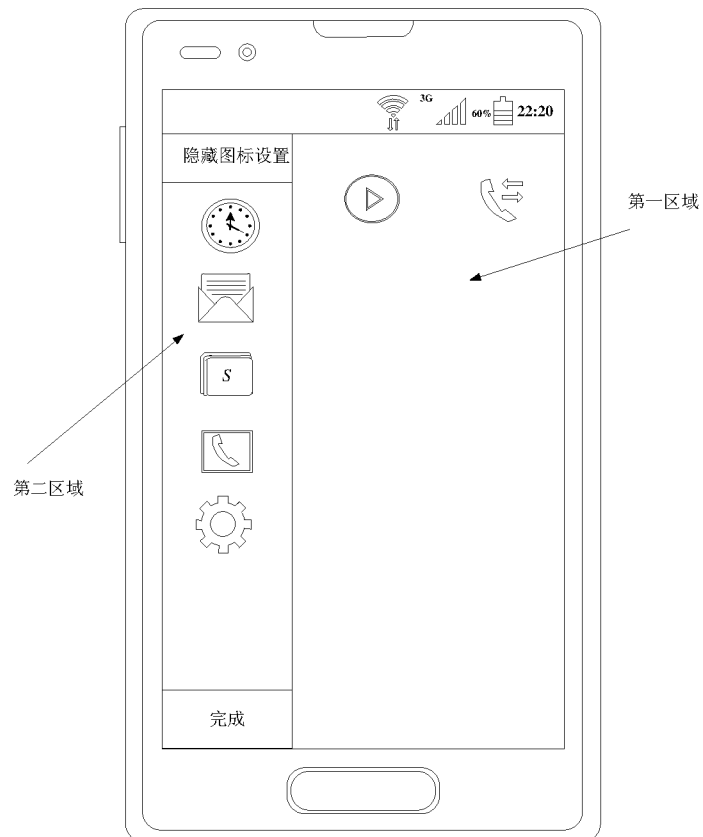


图 14

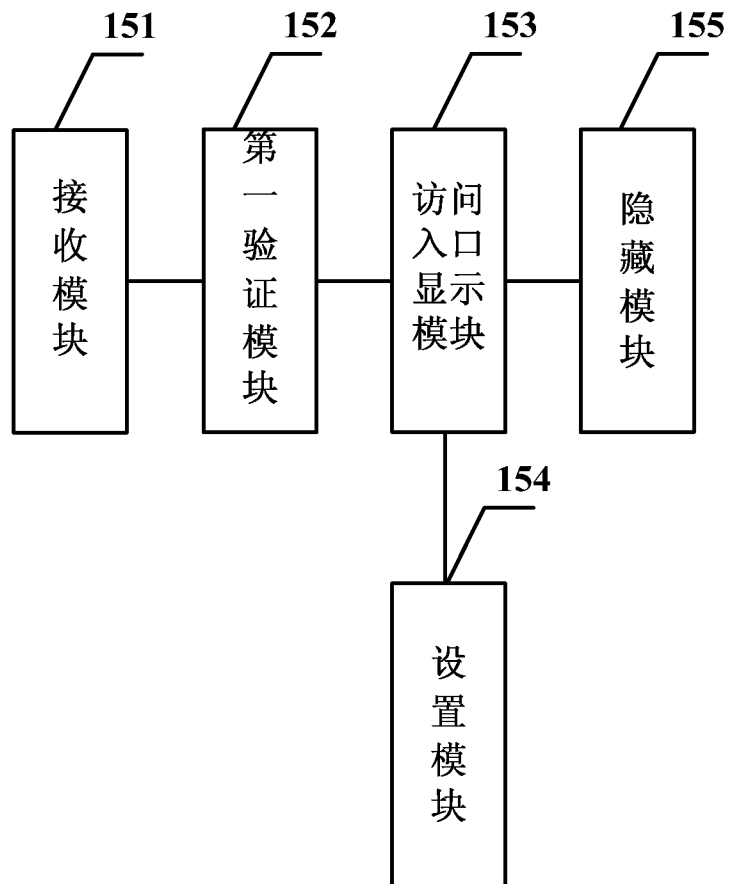


图 15

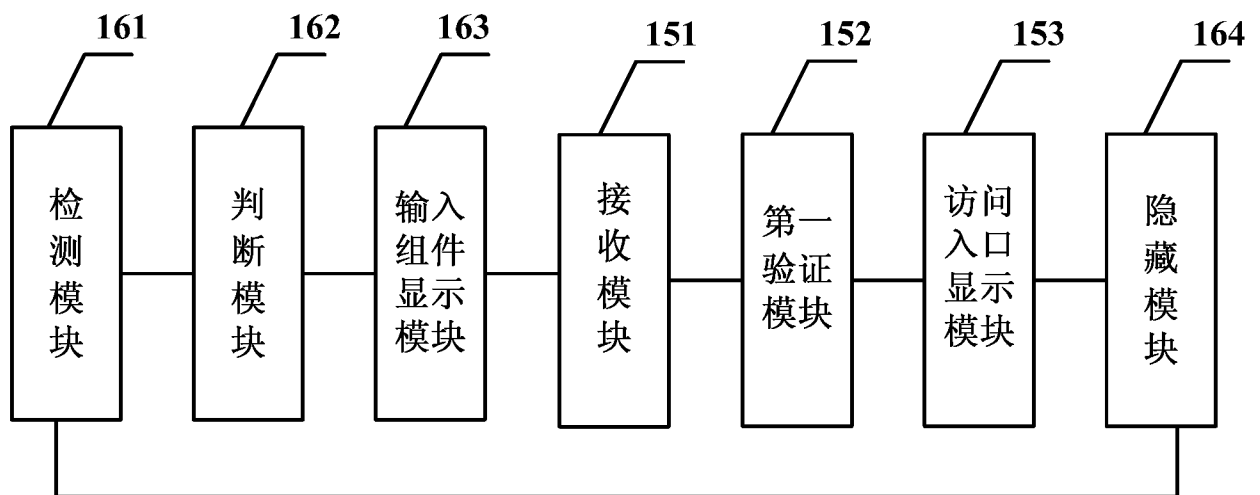


图 16

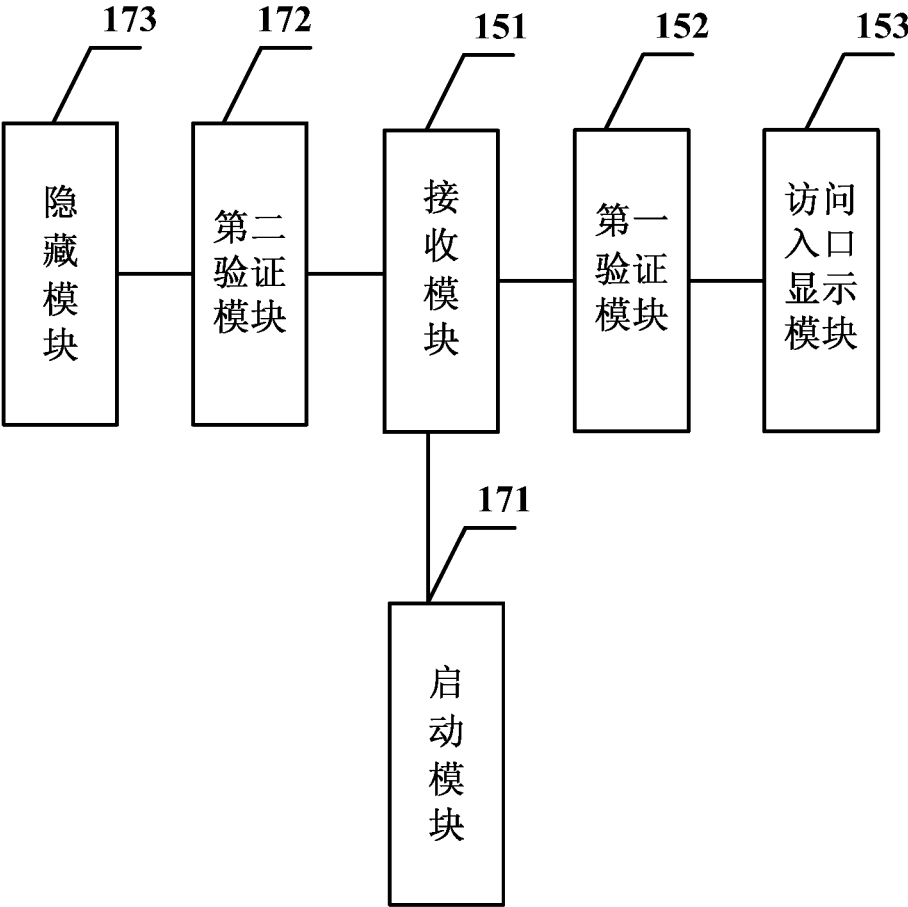


图 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/077296

A. CLASSIFICATION OF SUBJECT MATTER

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 21/-

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)

CPRSABS, CNABS, CNTXT, DWPI, USTXT, VEN: application, conceal, identification, verify, access, entrance, voice, iris, NFC, biological, scan, fingerprint, gesture, smart, card

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103377332 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 30 October 2013 (30.10.2013) claims 1 to 6	1, 11-14
Y	CN 103377332 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 30 October 2013 (30.10.2013) claims 1 to 6	2-10, 15-21
Y	CN 101616416 A (ZTE CORCP.) 30 December 2009 (30.12.2009) claims 1 to 5	2-10, 15-21
A	CN 102664903 A (LI, Ming) 12 September 2012 (12.09.2012) the whole document	1-21

☐ 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 22 June 2016	Date of mailing of the international search report 29 June 2016
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 Li, Xiaoqing Telephone No. (86-10) 62411891

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/077296

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103377332 A	30 October 2013	EP 2843569 A1	04 March 2015
		EP 2843569 A4	27 May 2015
		WO 2013159725 A1	31 October 2013
		SG 11201406765 A1	30 December 2014
		US 2015058972 A1	26. February 2015
		KR 20150006453 A	16 January 2015
		CN 103377332 B	20 April 2016
CN 101616416 A	30 December 2009	CN 101616416 B	29 August 2012
CN 102664903 A	12 September 2012	None	

A. 主题的分类 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) G06F21/- 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)) CPRSABS;CNABS;CNTXT;CNKI;DWPI;USTXT;VEN:应用程序, 隐藏, 身份, 验证, 访问, 入口, 声音, 虹膜, NFC, 生物扫描, 指纹, 手势, 智能卡 application, conceal, identificaiton, verify, access, entrance, voice, iris, NFC, biological, scan, fingerprint, gestrue, smart, card		
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
X	CN 103377332 A (腾讯科技深圳有限公司) 2013年 10月 30日 (2013 - 10 - 30) 权利要求1-6	1, 11-14
Y	CN 103377332 A (腾讯科技深圳有限公司) 2013年 10月 30日 (2013 - 10 - 30) 权利要求1-6	2-10, 15-21
Y	CN 101616416 A (中兴通讯股份有限公司) 2009年 12月 30日 (2009 - 12 - 30) 权利要求1-5	2-10, 15-21
A	CN 102664903 A (李明) 2012年 9月 12日 (2012 - 09 - 12) 全文	1-21
☐ 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 6月 22日		国际检索报告邮寄日期 2016年 6月 29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 李小青 电话号码 (86-10)62411891

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/077296

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	103377332	A	2013年 10月 30日	EP	2843569	A1	2015年 3月 4日
				EP	2843569	A4	2015年 5月 27日
				WO	2013159725	A1	2013年 10月 31日
				SG	11201406765Y	A	2014年 12月 30日
				US	2015058972	A1	2015年 2月 26日
				KR	20150006453	A	2015年 1月 16日
				CN	103377332	B	2016年 4月 20日
CN	101616416	A	2009年 12月 30日	CN	101616416	B	2012年 8月 29日
CN	102664903	A	2012年 9月 12日	无			