(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 109800548 A
(43)申请公布日 2019.05.24

(21)申请号 201711141994.9

(22)申请日 2017.11.17

(71)申请人 深圳市鹰硕技术有限公司
地址 518100 广东省深圳市宝安区新安三路建达工业区1栋二楼202室

(72)发明人 卢启伟 杨宁 刘佳

(74)专利代理机构 深圳余梅专利代理事务所（特殊普通合伙）44519
代理人 井杰 高真辉

(51)Int.Cl.
G06F 21/31(2013.01)
G06F 21/84(2013.01)

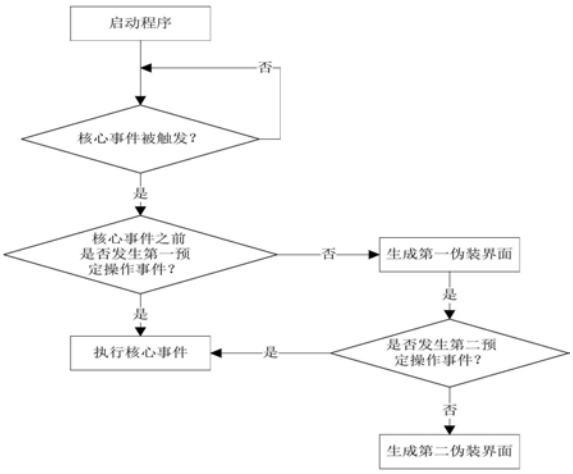
权利要求书2页 说明书11页 附图5页

(54)发明名称

一种防止个人信息泄露的方法和装置

(57)摘要

本发明提供一种防止个人信息泄露的方法，特别是一种用于互联网教学领域的防止个人信息泄露的方法和装置，本发明的方法和装置没有在启动程序时进行身份验证，而是选择在核心事件被触发后才进行判断是否执行核心事件，取消了每次启动程序都对身份进行验证提高了用户的体验，另一方面，程序的身份验证成功不代表在共享设备、使用过程中的借出设备时就不发生个人信息的泄露，因此，在触发核心事件时的一系列判断才能有效的对个人信息泄露进行监控和拦截。



CN 109800548 A

1.一种防止个人信息泄露的方法,其特征在于,包括:

S1:开始;

S2:启动程序;

S3:判断是否有核心事件被触发,若是,进入S4;

S4:判断触发核心事件之前发生的操作与行为库中预先存储的第一预定操作事件是否匹配,如果是,进入S5,如果否进入S6;

S5:执行核心事件;

S6:生成伪装界面,提供伪装信息;

S7:结束。

2.根据权利要求1的所述方法,其特征在于,所述步骤S6具体包括:

S601:根据核心事件的界面来生成第一伪装界面,并提供伪装信息;

S602:判断在第一伪装界面上是否发生第二预定操作事件,如果是,执行S5;如果否,执行S603;

S603:生成第二伪装界面;

所述的第二预定操作事件对应于核心事件的功能操作。

3.根据权利要求1的所述方法,其特征在于,所述步骤S6具体包括:

S601':根据核心事件的界面来生成第一伪装界面,并提供伪装信息;

S602':判断在第一伪装界面上是否发生第二预定操作事件,如果是,执行604';如果否,执行S603':

S603':生成第二伪装界面;

S604':退出第一伪装界面,执行S3;

所述的第二预定操作事件对应于核心事件的功能操作。

4.根据权利要求1的所述方法,其特征在于,执行所述核心事件能够获得需要保护的信息,所述的预先存储的第一预定操作事件是该程序所具有的实际功能的操作。

5.根据权利要求1的所述方法,其特征在于,执行所述核心事件能够获得需要保护的信息,所述的预先存储的第一预定操作事件是该程序所具有的实际功能的操作的组合。

6.一种防止个人信息泄露的设备,其特征在于,包括:

第一接收模块,用于接收用户启动程序指令;

第二接收模块,用于接收用户触发核心事件指令,第一判断模块,用于判断核心事件是否被触发,第二判断模块,用于判断触发核心事件之前发生的操作与行为库中预先存储的第一预定操作事件是否匹配;

存储介质,用于存储行为库。

7.根据权利要求6的所述设备,其特征在于,还包括:

第三判断模块,用于判断在第一伪装界面上是否发生第二预定操作事件。

8.根据权利要求6的所述设备,其特征在于,还包括:显示模块,用于在第二判断模块的身份验证为否时,向操作者反馈第一虚假界面。

9.根据权利要求8的所述设备,其特征在于,还包括:显示模块根据核心事件的界面来生成第一虚假界面。

10.根据权利要求9的所述设备,其特征在于,还包括:显示模块,还用于在第三判断模

块身份验证为否时,向操作者反馈第二虚假界面。

一种防止个人信息泄露的方法和装置

技术领域

[0001] 本发明涉及在线教育技术领域，特别是涉及一种用于互联网在线教育过程中防止个人信息泄露的方法和装置。

背景技术

[0002] 随着当前通讯技术的发展和智能化设备的普及，智能计算设备如智能电话、平板电脑、膝上型电脑等制造成本普遍降低，已经成为了大多数普通民众日常生活中不可或缺的一个重要组成部分。使用移动设备中进行在线学习、深造越来越普遍，其具有学习地点灵活化，学习内容个性化，学习模式私人化等特点，而且随着学习程序的社交功能越来越多，在线学习程序也同样具有即时在线通话、交流等功能，而社交本身具有私密性，应被列为个人敏感信息。因此，在线学习程序的功能分为两部分，一种是课程类的，这部分功能不具有私密性，另一种为个人信息类的，比如学习成绩、社交学习的好友、虚拟货币信息等。一种典型的在城市上班通勤过程中的在线学习模式为学员通过移动设备进行在线学习，在学习过程中可能将移动设备借给同行的有共同学习爱好的同伴共享，在借出过程中，课程类的功能是可以让同伴观看的，但个人信息是不希望泄露的。我们将对设备拥有者的个人敏感信息进行未经允许的访问或获取的行为称为个人信息泄露，如何防止在线学习中，移动设备在借出时或分享时对个人信息的保护，是各种智能计算设备客观面临的一个技术问题。

[0003] 还有一种需要对个人信息的保护情况是应对恶意程序(也被称为“恶意程序”)的威胁，恶意程序是指当被计算机执行时不利地影响计算机的性能和/或危害存储在计算机上的数据的完整性的未经授权的指令。作为示例，恶意程序可以获得对应用的访问；扰乱计算机操作；擦除存储在计算机上的文件；收集敏感信息(例如密码或其它个人信息)；追踪计算机的用户的行为；使用计算机以用于非预期操作等等。

[0004] 一种现有技术是提供了具有多种访问模式的移动计算设备，所述移动设备在设备的触摸屏显示器上显示用于在一级访问模式下或二级访问模式下访问所述设备的锁屏页面。所述一级访问模式提供对设备的若干应用程序的访问，并且二级访问模式提供对有限的一组应用程序的访问。移动设备接收锁屏页面上的触摸输入以在二级访问模式下访问设备。移动设备通过允许对该组应用程序的访问以及限制对多个应用程序中的剩余应用程序的访问来将设备解锁至所述二级访问模式。但这种设备依赖于设备拥有人对设备的提前设定，主动的将设备在一级访问模式和二级访问模式之间切换，但在现实生活中很多的信息泄露发生在设备拥有人没有准备或没有防备的情况下，若没有将一级访问模式切换到二级访问模式，导致设备共享或外借发生了敏感的人个信息外泄。另外，这种技术只能将程序按不同涉及隐私的级别分级，但不能对程序内部的多种不同功能进行涉及隐私等级的区分。也就是说，这种设备的对个人信息的保护功能还是具有缺陷。

[0005] 还有一种现有技术，是一种恶意行为的监控方法及装置，属于监控领域。所述方法包括：检测是否有事件被触发；若检测到事件被触发，将检测到的事件与行为列表中的各行为进行比对，并判断检测到的事件是否符合行为列表中的行为；若检测到该事件符合行为

列表中的行为，将行为与行为库中预先存储的恶意行为进行匹配；若行为与行为库中预先存储的恶意行为相匹配，则判定行为为恶意行为，被检测到的事件为恶意事件；对恶意行为中的恶意事件进行拦截。本发明通过采用自动对恶意行为中的恶意事件进行拦截的方式，从而使得在恶意行为监控过程中，能够自动对恶意行为进行有效、快速识别并实时拦截。但这种匹配的行为很难适应快速的恶意行为变化，一种监控装置是无法包括所有种类的恶意行为的，该技术中只是理论上可行。

[0006] 还有一种现有技术提供了一种应用程序的保护方法和装置，为提高应用程序的安全性且提高用户体验。该应用程序的保护方法包括接收用户输入的第一信息，所述第一信息用于启动第一应用程序；判断所述第一应用程序是否属于预先设定的要伪装的应用程序；在所述第一应用程序属于预先设定的要伪装的应用程序时，向用户显示预先设定的伪装界面，所述伪装界面用于表明所述应用程序出现异常。该方法提高应用程序的安全性且提高用户体验。当然，根据不同应用程序设定的启动方式，第一信息也不限于点击信息，例如也可以是双击、选择等信息。这种保护方法最大的问题是对待任何程序访问人都无差别的生成伪装界面，给设备拥有者也造成很大的困扰，每次打开该选定程序，都会生成伪装界面，需要输入解密信息才能进行下一步的操作，非常的不方便，而且正如前文分析，很多程序的大部分的功能都不涉及个人信息，对学习程序本身来说，大部分的功能都不具有隐私性，比如具体的课程内容和课程安排等，只有涉及个人信息的部分才具有隐私性。如果对程序本身设定过于严格的保密级别，既没有必要，也不方便操作。

[0007] 还有一种现有技术提供了一种基于自然交互的隐式身份认证方法，其步骤包括：1)隐式触发并开启隐式身份认证过程；2)开启多个采集设备，隐式采集用户的多个生物特征信息；3)判断是否采集到可利用的生物特征信息，如果没有采集到可利用的生物特征信息，则在预设采集次数内提示隐式引导性信息并开启与引导性信息相关的采集设备采集用户的生物特征信息，并继续判断是否采集到可利用的生物特征信息；如果采集到可利用的生物特征信息，则将采集到的可利用的生物特征信息作为用户的待认证生物特征信息与对应的预存生物特征信息进行验证匹配；4)如果匹配一致，则允许用户进行特定操作；如果匹配不一致，则提示用户未通过身份认证并进行显示身份认证。这种方法通过自然交互过程中的隐式身份认证方式可以对用户身份进行自然、高安全性认证，相较于现有动态身份认证的方式，认证过程自然不死板，在不干扰用户的情况下，隐式提取待认证生物特征信息进行身份认证，或者通过简单隐式引导性提示信息，促使用户产生特定自然反应后，再隐式提取待认证生物特征信息进行身份认证。这种技术相对于现有的验证方式有了很大的改善，但仍存在重大的缺陷，即隐式的身份认证方式还不够“隐式”，因为当一系列的生物信息被搜集后，如果不能通过验证，就开始了显性的验证，显性的验证实质上是对操作人员的一种提醒，这是设备拥有者不希望看到了，其更希望整个过程在隐性的前提下完成。

[0008] 现有技术中还有一种用户身份识别系统的识别方法，包括以下步骤：系统采集用户历史操作信息及操作信息上传至云平台，云平台对用户历史操作信息进行分析学习，找出用户操作习惯集合作为标志信息进行存储；所述历史操作习惯集合随着用户的使用次数增加而迭代更新；使用时，系统对用户的身份信息进行验证，若验证失败则拒绝用户访问，若验证通过则将用户操作信息与存储的标志信息进行比对，比对成功则运行用户访问，否则拒绝用户访问。适用于身份识别。但根据其记载的用户A使用手机的在线支付功能，打开

某付款APP，用户每次在支付操作前，在手机的触摸屏上画一个圆圈，再进行支付操作。系统把这种操作习惯记录下来作为以后的对比操作，但这种手势的精度是非常低的，而且非常容易被人观察及模仿，另外，这种手势本身也没有任何的实际意义，其只是现有技术中的手势验证而已。对于激活验证的时机，其也是在程序启动前的一种隐性身份验证，也是无差别的，每次都会进行验证，对会对用户的正常使用带来不便。

[0009] 综上，可以得知，现有技术中，对于设行备中的敏感个人信息的保护方法，一种是人为的在正常使用的第一状态和限制性使用的第二状态下切换，限制性使用包括可供使用的程序数量减少，去除了包括敏感信息的程序，还有一种限制性使用是伪装界面，干脆就无法使用，或需要解密后再使用，或者，与人为切换相对应的是提前预设特定程序，一旦触发这类程序，自动开启伪装界面，只有通过人为的解密才能进一步使用，这使得隐式的身份验证变得显性，是设备拥有者不希望看到的。

发明内容

[0010] 提出本发明的目的是给出一种保护个人信息，对个人信息泄露具有足够防护的方法和设备，并且该方法或设备不会明显增加使用人或者设备拥有者的操负担，而且在整个验证过程中，都是隐性的验证。

[0011] 本发明的目的在于提供一种防止个人信息泄露的方法，所述方法包括：

[0012] 一种防止个人信息泄露的方法，包括：

[0013] S1：开始；

[0014] S2：启动程序；

[0015] S3：判断是否有核心事件被触发，若是，进入S4；

[0016] S4：判断触发核心事件之前发生的操作与行为库中预先存储的第一预定操作事件是否匹配，如果是，进入S5，如果否进入S6；

[0017] S5：执行核心事件；

[0018] S6：生成伪装界面，提供伪装信息；

[0019] S7：结束。

[0020] 优选的是，所述步骤S6包括：

[0021] S601：根据核心事件来生成第一伪装界面，并提供伪装信息；

[0022] S602：判断在第一伪装界面上是否发生第二预定操作事件，如果是，执行S5；如果否，执行S603：

[0023] S603：生成第二伪装界面。

[0024] 优选的是，所述步骤S6包括：

[0025] S601’：根据核心事件来生成第一伪装界面，并提供伪装信息；

[0026] S602’：判断在第一伪装界面上是否发生第二预定操作事件，如果是，执行604’；如果否，执行S603’：

[0027] S603’：生成第二伪装界面；

[0028] S604’：退出第一伪装界面，执行S3。

[0029] 优选的是，执行所述核心事件能够获得需要保护的信息，所述的预先存储的第一预定操作事件是该程序所具有的实际功能的操作。

[0030] 优选的是，执行所述核心事件能够获得需要保护的信息，所述的预先存储的第一预定操作事件是该程序所具有的实际功能的操作的组合。

[0031] 一种防止个人信息泄露的设备，包括：

[0032] 第一接收模块，用于接收用户启动程序指令；

[0033] 第二接收模块，用于接收用户触发核心事件指令，第一判断模块，用于判断核心事件是否被触发，第二判断模块，用于判断触发核心事件之前发生的操作与行为库中预先存储的第一预定操作事件是否匹配；

[0034] 存储介质，用于存储行为库。

[0035] 优选的是，还包括：第三判断模块，用于判断在第一伪装界面上是否发生第二预定操作事件。

[0036] 有益效果：

[0037] 1、本申请的防止个人信息泄露的方法并没有在启动程序时进行身份验证，而是选择在核心事件被触发后才进行判断是否执行核心事件，取消了每次启动程序都对身份进行验证提高了用户的体验，另一方面，程序的身份验证成功不代表在共享设备、使用过程中的借出设备时就不发生个人信息的泄露，因此，在触发核心事件时的一系列判断才能有效的对个人信息泄露进行监控和拦截。

[0038] 2、本申请中“预定操作”实质就是设备的拥有者在触发核心事件之前习惯性的对其他功能的操作被记录和保存，当设备的拥有者在希望执行核心事件时，由于操作的习惯会先执行预定操作。如果设备经过判断在触发核心事件之前有这样的预定操作，则会认为是设备的拥有者在执行相应的操作从而正常执行核心事件，否则认为是个人信息泄露。“预定操作”为有实质功能的操作，并不是简单的手势操作，手势操作容易被人模仿，但实质功能的操作特别是连续的实质功能操作的组合是不容易被他人发现的，因为他人无法在看似平常的程序使用中看出操作之间的人为设定的联系。

[0039] 3、本申请还提出了科学的伪装界面生成的手段，由于隐性的身份验证与第一伪装界面相结合，使得设备拥有者在正常使用时由于误操作引起的生成第一伪装界面时其本人无法有效的识别出，因此，出于避免对设备拥有者的正常使用造成误导，这里在第一伪装界面的环境下，也预先设定第二预定操作事件，该第二预定操作事件与设备拥有者在操作核心事件的部分操作完全一致，仍然是利用设备拥有者的操作习惯来进行身份验证，并不向其进行显性的认证，将整个的验证过程都作为隐性的验证来体现。将第一伪装界面置于两次的预定操作事件判之间，大大避免了设备拥有者的误操作的概率，有效的保护了设备拥有者个人隐私。

附图说明

[0040] 图1为现在技术常规的执行核心操作的流程图；

[0041] 图2为本发明中防止个人信息泄露的第一实施例流程图；

[0042] 图3为本发明中防止个人信息泄露的第二实施例流程图；

[0043] 图4为本发明中防止个人信息泄露的第三实施例流程图；

[0044] 图5为本发明中示例在线学习程序的第1标签菜单界面；

[0045] 图6为本发明中示例在线学习程序的第2标签菜单界面；

[0046] 图7为本发明中示例在线学习程序的第3标签菜单界面。

[0047] 附图标记:1、第1标签菜单;2、第2标签菜单;3、第3标签菜单。

具体实施方式

[0048] 下面将结合附图对本发明的具体实施方式进行详细说明。应当理解,此处所描述的实施例仅仅是用于解释本发明,并不是用于限制本发明。有关领域的普通技术人员在不背离本发明精神的情况下所做的各种变化和变形,都在本发明的独立权利要求和从属权利要求的范围内。

[0049] 在本文中,程序代表包括个人敏感信息的应用程序,该应用程序包括多种功能,对这些功能的执行称为事件,核心事件代表了执行应用程序中的一个功能从而获取了个人敏感信息。在现有技术中,用户一般都需要在设备启动时或解除屏幕保护时对设备进行解锁,解锁的操作一般包括对身份的验证。图1是现有技术的典型的一种操作流程,启动设备后就进行一系列的启动程序,执行核心事件。而在共享设备、使用过程中的借出设备时,个人敏感信息的泄露发生在身份验证之后,本实施例中,并没有在启动程序中进行身份验证,而是选择在核心事件被触发后才进行判断是否执行核心事件,这是因为每次启动程序都对身份进行验证是一件非常繁锁的操作,容易引起用户的不满,另一方面,程序的身份验证成功不代表在共享设备、使用过程中的借出设备时就不发生个人信息的泄露。只有在触发核心事件时的一系列判断才能有效的对个人信息泄露进行监控和拦截。

[0050] 本实施例中对于核心事件被触发后的判断提出一种正向验证的逻辑,一般的验证都是看这个行为是否与个人信息泄露行为库中数据相匹配,如果是,就被认定为个人信息泄露行为,因此设备只能根据现有数据库的数据来进行判断,对于既不能判断是合法的,也不能判断是恶意的的,就只能将其放行。但这种判断是非常低效的,设备通常需要经常更新数据库来应对日益增多种类的恶意行为。

[0051] 这种设定在实践中有重要意义,不但可以排除他人的触发核心事件的行为,更重要的是,对恶意程序后台触发核心事件进行了有效的管控,目前恶意的病毒更新很频繁,新病毒层出不穷,因此很多恶意病毒并未被及时收集到数据库中,如果仅是因为某种触发行为没有被记录在数据库里,设备就将其放行。这样,就带来了个人敏感信息会被恶意程序获取的可能。而本发明中,对于是否执行核心事件的判断仅限于判断其是否满足预设的事件的发生。这大大减轻了设备判断操作的负担。

[0052] 参见图2,一种防止个人信息泄露的方法,所述方法包括:

[0053] S1:开始;一般在设备启动时或设备拥有者解除锁屏时就会启动该防止个人信息泄露的方法。因为在设备中,会有很多个涉及个人敏感信息的程序,比如各类在线学习程序,只要是对这些程序进行启动就需要防止个人信息泄露。

[0054] S2:启动程序;只要多个涉及个人敏感信息的程序中的任意一个被启动,就需要进入后面的判断。

[0055] S3:判断是否有核心事件被触发,若是,进入S4;对于上述程序中,很多功能不会涉及到个人信息,而这些信息可能是操作者平时大量的、反复使用的功能,比如图5-7是一种典型的在线学习程序中第1-3标签菜单界面,其中,第3标签菜单界面涉及个人信息,是核心事件。这里的第1标签菜单界面中的“通用功能1”、“通用功能2”、“通用功能3”就不涉及个人

敏感信息，通用功能可以是在线查词、课程查找、推送新闻等不涉及个人信息的功能，如果每次用户在使用第1标签菜单界面时，系统都执行判断或者身份验证，那么将非常影响用户的体验。但对于第3标签菜单界，这里包括了用户的大量的个人信息，比如学习兴趣好友、好友留言、虚拟财产及触发在线支付程序等，这些就属于个人的敏感信息。如果想触发第3标签菜单界面，系统应该去判断是否是设备拥有者在使用这个功能。所以在S3中，如果发现涉及个人敏感信息的事件被触发才会进入后面的判断，如果没有，系统不会打断用户的操作，保持设程序运行的流畅性。

[0056] S4：判断触发核心事件之前发生的操作与行为库中预先存储的第一预定操作事件是否匹配，如果是，进入S5，如果否进入S6；需要申明的是，这里的预先存诸的预定操作有别于输入密码或者输入指纹进行匹配也不是简单手预定手势，在某现有技术中，对于操作习惯可以包括但不限于用户使用的应用程序、用户的屏幕解锁手势/密码、用户的习惯性手势、用户的习惯性连续操作手势。但这些现有技术中对操作习惯的采集都不能很好的解决个人信息泄露的问题。首先如果将其他的应用程序做为触发核心事件的前提，那么核心事件也是并列的应用程序，但正如前文所说，每次启运程序都进行验证是复杂的，另外，信息泄露发生在某程序的具体功能上而不是整个程序都涉及泄露个人信息，提高安全级别或扩大对信息的保护会引起用户体验度下降。输入密码是显式验证；而手势易于被模仿；指纹验证并不是操作习惯，仍是生物信息的一部分。

[0057] 步骤S4希望用不打断用户操作的方式进行判断。预定操作事件指的是对打开的程序中其他功能的执行或者一系列这类功能执行的集合，比如通用功能，比如课程信息。只要在触发核心事件之前，操作者执行了一系列预定的程序的功能，设备即可判断操作人员是设备的拥有者，从而可以进入后面的S5中，否者，认为这种触发核心事件的行为是个人信息泄露。需要进一步解释的，本申请中的预见定操作对应着实际的应用程序的功能，用户在执行这操作时会有实际的功能由程序完成，这不同于将其他程序作为预先操作或者用手势指纹等无实际意义的操作。

[0058] 在现有技术中，很少有技术关注到操作人员对应用程序的功能性的习惯性操作或者一贯性操作与操作者身份的认证之间的联系，很多的程序针对操作者的习惯提供了更人性化的设置，一方面，这些程序被设计为允许操作者调整UI界面，比如操作者可以将平时不用的按钮删除，再增加新的、常用的按钮，这体现了按个人风格定制UI界面的思维，经过调整，UI界面上的按钮更加适应于操作者的需要；另一方面，很多程序主动的对用户进行信息的推送，比如百度会根据操作者的阅读习惯推送新闻，天猫会根据操作者的查找习惯推送特定种类的商品，这种推送的行为也提高的用户的阅读效率，可见，智能化的根据操作者的习惯对程序本身的设定或修改可以提高操作者的用户体验。同样，本实施例中，“预定操作”实质就是设备的拥有者在触发核心事件之前习惯性的对其他功能的操作被记录和保存，这些功能本身有自己的实质意义，但相互之间并没有任何的逻辑联系，因此，将这些功能或者功能的组合作为预定操作既能使操作人员进行实质性的操作，又能很好的进行隐式的身份验证，当设备的拥有者在希望执行核心事件时，由于操作的习惯会先执行预定操作。如果设备经过判断在触发核心事件之前有这样的预定操作，则会认为是设备的拥有者在执行相应的操作从而进入S5，否则认为是个人信息泄露。对于习惯性的预先操作来说，这不会增加用户的负担，因为其不作为判定条件，用户也用这样去操作程序的功能。作为一种举例，对于

图5，一个用户习惯在第1标签菜单界面先触发通用功能2比如了解最新课程介绍，然后再触发通用功能1了解相应科目的考试时间，然后再进入第3标签菜单界面触发个人信息2，比如查看账户余额决定是否要充值。那么先执行通用功能2再执行执行通用功能1就是进入第3标签菜单界面这个核心事件的“预定操作”。对于“预定操作”的设置，其可以是灵活的和多变的，其与设备拥有者的习惯密切相关。

[0059] 当然，如果有必要，设备的拥有者完全可以基于信息安全的需要，人为的培养一种独特的操作习惯，然后为作一种全新身份验证来对核心事件触发限定条件。这种全新身份验证有别于现有的密码或指纹验证，后者只是单纯的身份验证，但使用预定操作来验证身份，其本身是可以为操作者提供程序的功能的服务的，另外，其没有明显的程序的间断性。

[0060] S5：执行核心事件；经过一系列的判断，程序将执行核心事件，比如展示第3标签菜单界面下面的各种信息。

[0061] S6：生成伪装界面，提供伪装信息。生成伪装界面的意义在于，将整个操作都按隐式的操作来执行，不会向正在使用的人提供任何关于身份验证通过或不通过的提示或者信息。伪装界面或者伪装信息的提供是现有技术，这点在前文的背景技术里已经提到，但现有技术中，对于伪装界面的启动或者触发非常不科学，一是不分前提，只要是启动了某程序就直接生成伪装界面需要解密后再使用，这会给使用者带来非常大的不便；第二种，人为的触发伪装界面，但这种设计也无法有效的保护个人信息。可见，S6中生成伪装界面是有前提的，并不是盲目的启动程序就生成伪装界面，也不是手动切换，而是在程序的使用过程中，不着痕迹的提出身份的验证，然后再生成伪装界面，一般他人很难在正常使用程序时发现自己被设备识别出不是设备的拥有者，而且在隐式身份验证时，验证之后随之也生成了伪装界面，从而被伪装界面迷惑。

[0062] 可选的是，执行所述核心事件能够获得需要保护的信息，预定操作事件为该程序中除核心事件外的任意执行其他功能。可选的是，执行所述核心事件能够获得需要保护的信息，预定操作事件为该程序中除核心事件外的任意执行其他功能的组合。

[0063] S7：结束

[0064] 如图3所示，所述步骤S6包括：

[0065] S601：根据核心事件来生成第一伪装界面，并提供伪装信息；

[0066] S602：判断在第一伪装界面上是否发生第二预定操作事件，如果是，执行S5；如果否，执行S603；

[0067] S603：生成第二伪装界面；

[0068] 所述的第二预定操作事件对应于核心事件的功能操作。

[0069] 可选的是，可以根据操作人员在第一伪装界面上的操作进一步进行隐式的身份验证。现有技术中并没有将隐式身份验证和伪装界面连用的技术，发明人在实际的操作中发现，这种隐式的的身份验证太具有迷惑性，有时连真正的设备拥有人在误操作的情况下，也会被生成的第一伪装界面所迷惑。总结起来，还是因为隐式的身份验证与用户之间没有互动，是一种单向的信息传送的过程。为了消除这种因为误操作而引起的误激活第一伪装界面，该方法进一步包括对比在第一伪装界面的环境下，其操作是否与第二预定操作事件相匹配，如果是的话，可以被认为在核心操作之前的操作虽然不能与第一预定操作事件相符合，但仅是一种误操作。因此，可以执行S5，执行核心事件。但如果在第二次的隐式身份验证

中再次失败，系统会生成第二伪装界面，来提供虚假的信息。

[0070] 比如在在线学习程序找开的情况下，如果把手机借给朋友，让他看一眼图6中的“课程信息2”，但朋友不小心碰了一下“第3标签菜单界面”，结果看到了他的个人信息2，这种情况时有发生但没有办法保护个人信息。但根据S601-603来判断，首先设备的拥有者将“第3标签菜单界面”设为核心事件，那么在手机借给朋友时，朋友触发“第2标签菜单界面”是完全可以正常使用的，但一旦朋友点击了“第3标签菜单界面”，由于没有事先执行预定操作，所以点击“第3标签菜单界面”就会生成虚假的第一伪装界面，这时他的朋友并不能知晓这个是伪装的页面，所有的验证都是在隐式的验证方式下进行的。

[0071] 但正如前文所述，如果是投备的拥有人自己误操作导致成了第一伪装界面，其本人也难于发现，但这并不影响正常的使用，其本人只需要按照在核心事件的界面上的习惯在第一伪装界面操作相应功能，还是能够在S5中切换回真实的核心事件。这就消除了隐式身份验证的易出现误操作的问题。因此，只需要按核心操作的界面来设计第一伪装界面，并核对使用者在第一伪装界面上的操作即可。

[0072] 如图4所示，可选的是，所述步骤S6包括：

[0073] S601’：根据核心事件来生成第一伪装界面，并提供伪装信息；

[0074] S602’：判断在第一伪装界面上是否发生第二预定操作事件，如果是，执行604’；如果否，执行S603’：

[0075] S603’：生成第二伪装界面；

[0076] S604’：退出第一伪装界面，执行S3。

[0077] 这种情况下，如果在第二预定操作事件的隐式验证中获得通过，进而返回至S3，重新的对第一预定操作事件进行操作。这进一步的加强了验证的效果，但不足是，这种不符合常理的转跳实质是一种提醒，提醒设备的使用人员，程序并没有按照一贯的流程运行。不过，本申请的发明构思主要体现在第一预定操作事件——第一伪装界面——第二预定操作事件的联用，这种完全隐式的身份验证使得所有的验证行为都在使用者不知情的情况下进行。

[0078] 一种防止个人信息泄露的设备，包括：

[0079] 第一接收模块，用于接收用户启动程序指令；

[0080] 第二接收模块，用于接收用户触发核心事件指令，第一判断模块，用于判断核心事件是否被触发，第二判断模块，用于判断触发核心事件之前发生的操作与行为库中预先存储的第一预定操作事件是否匹配；

[0081] 存储介质，用于存储行为库。

[0082] 优选的是，还包括：第三判断模块，用于判断在第一伪装界面上是否发生第二预定操作事件。

[0083] 可选的是，还包括显示模块，用于在第二判断模块身份验证为否时，向操作者反馈第一虚假界面。

[0084] 可选的是，根据核心事件界面来生成第一虚假界面。

[0085] 也可以将方法应用于金融软件领域，某用户使用支付宝时，将“我的”列为核心事件，其将先点击查看“余额宝”再点击“记账本”作为预定事件，这样每次他想了解“我的”内的余额信息、银行卡信息等时，先习惯性的看“余额宝”和记账本”，随后点击“我的”，可以顺

利打开“我的”;如果是其他人使用这个设备,其可以使用“余额宝”、“记账本”及其他功能,但点击“我的”时,因为没有第一预定事件的前提,系统会依据“我的”的界面来生成第一伪装界面。

[0086] 但如果是该用户误操作生成了第一伪装界面,只需要在第一伪装界面上按预定的操作来执行“我的”相应的功能,即第二预定事件,就可以重新切换到核心事件或者重新进行第一预定事件的验证。

[0087] 硬件设备及实适环境

[0088] 在上述各实例中,设备的用户执行触摸手势来选择确定。用户可通过触摸手势或基于动作的手势指引设备来触发核心事件。例如,用户轻按并按下应用程序图标的功能按钮,本领域技术人员将会理解这些只是示例性手势,可使用其他手势执行相同功能。不同触摸手势(例如,单次轻按、两次轻按、单次轻按、轻按并按下(即,按压)、拖拽、捏合、拉伸按压、旋转等)可相互交换来提供类似功能。不同于旋转计算设备,设备可在一表面上面朝下或面朝上放置,设备可被翻转,或者任何其他基于动作的手势可通过计算设备的一个或多个方位/运动检测部件,诸如陀螺仪和加速度计检测到。

[0089] 在许多上述实例中,不仅局限于触摸屏式的智能计算设备。本领域的普通技术人员也将认识到,对于在具有光标和光标控制器或其他输入机制的设备上执行的其他实施例,可使用光标控制器或其他输入设备来与在这些实例中所示出的控件进行交互。不同于按压应用程序图标的操作方式,这类设备可允许用户结合光标控制器来使用键盘。这些均为成熟的现有技术。

[0090] 上文所述应用程序被实施为指定在计算机可读存储介质(又称为计算机可读介质)上记录的一组指令的程序。在这些指令由一个或多个计算或处理单元(例如,一个或多个处理器、处理器的内核或者其他处理单元)执行时,这些指令使得一个或多个处理单元能够执行指令中所指示的动作。计算机可读介质的实例包括但不限于CD-ROM、闪存驱动器、随机存取存储器(RAM)芯片、硬盘驱动器、可擦可编程只读存储器(EPROM)、电可擦可编程只读存储器(EEPROM)等。计算机可读介质不包括无线地传送或通过有线连接的载波和电信号。

[0091] 在本说明书中,术语“程序”意在包括驻留在只读存储器中的固件或者存储在磁性存储设备中的应用程序,所述固件或应用程序可被读取到存储器中以用于由处理器进行处理。此外,在一些实施例中,可在保留不同的程序发明的同时将多个程序发明实现为更大程序的子部分。在一些实施例中,还可将多个程序发明实施为独立程序。

[0092] 本说明书中的设备作为实例包括智能电话、平板电脑、膝上型电脑等。移动计算设备包括一个或多个处理单元、存储器接口和外围设备接口。

[0093] 外围设备接口耦接到各种传感器和子系统,所述子系统包括摄像机子系统、一个或多个无线通信子系统、音频子系统、输入/输出(I/O)子系统等。外围设备接口能够实现处理单元与各种外围设备之间的通信。例如,取向传感器(例如,陀螺仪)和加速度传感器(例如,加速度计)耦接到外围设备接口,以便促进取向和加速功能。

[0094] 相机子系统耦接到一个或多个光学传感器(例如,电荷耦合设备(CCD)光学传感器、互补金属氧化物半导体(CMOS)光学传感器等)。与光学传感器耦接的相机子系统促进相机功能,诸如图像和/或视频数据捕获。无线通信子系统用于有利于通信功能。在一些实施例中,无线通信子系统包括射频接收器和发射器,以及光学接收器和发射器。一些实施例的

这些接收器和发射器被实现为工作于一个或多个通信网络上，所述通信网络诸如是GSM网络、Wi-Fi网络、蓝牙网络等。音频子系统耦接到扬声器以输出音频。另外，音频子系统耦接到麦克风以促进支持语音-的功能诸如语音识别、数字记录等。

[0095] I/O子系统涉及输入/输出外围设备(诸如显示器、触摸屏等)和处理单元的数据总线之间通过外围设备接口的传输。输入/输出子系统包括触摸屏控制器和其他输入控制器以有利于输入/输出外围设备和处理单元的数据总线之间的传输。如图所示，触摸屏控制器耦接至触摸屏。触摸-屏控制器使用任何多点触感技术来检测触摸屏上的接触和移动。其他输入控制器耦接至其他输入/控制设备，诸如一个或多个按钮。一些实施例包括旁近触感屏和对应控制器，该对应控制器可检测替代触摸交互或除触摸交互之外的接近触摸交互。

[0096] 存储器接口耦接至存储器。在一些实施例中，存储器包括易失性存储器(例如，高-速随机存取存储器)、非易失性存储器(例如，闪存存储器)、易失性存储器和非易失性存储器的组合和/或任何其他类型的存储器。存储器存储操作系统(OS)。OS包括用于处理基础系统服务和用于执行硬件相关任务的指令。

[0097] 存储器还包括：促进与一个或多个附加设备通信的通信指令；促进图形用户界面处理的图形用户界面指令；促进图像相关的处理和功能的图像处理指令；促进输入相关(例如，触摸输入)的过程和功能的输入处理指令；促进音频-相关的过程和功能的音频处理指令；以及促进相机相关的过程和功能的相机指令。上述指令仅是示例性的，并且在一些实施例中，存储器包括附加的和/或其他指令。例如，用于智能电话的存储器可包括促进电话相关的过程和功能的电话指令。以上所识别的指令不需要作为独立的程序程序或模块来实施。可在硬件和/或程序中，包括在一个或多个信号处理和/或专用集成电路中来实现移动计算设备的各种功能。

[0098] 虽然例示的组件被示出为独立的组件，但是本领域的普通技术人员将认识到，可将两个或更多个组件集成到一个或多个集成电路中。另外，两个或更多个组件可由一条或多条通信总线或信号线来耦接在一起。另外，虽然已将许多功能描述为由一个组件执行，但是本领域的技术人员将认识到，可将相对于上述的功能拆分到两个或更多个集成电路中。

[0099] 实现本发明的一些实施例是利用了电子系统，电子系统可为计算机(例如，台式计算机、个人计算机、平板电脑等)、电话、PDA或任何其他种类的电子或计算设备。此类电子系统包括各种类型的计算机可读介质以及用于各种其他类型的计算机可读介质的接口。电子系统包括总线、处理单元、图形处理单元(GPU)、系统存储器、网络、只读存储器、永久性存储设备、输入设备以及输出设备。

[0100] 总线总体表示在通信上连接电子系统6800的许多内部设备的所有系统、外围设备、以及芯片组总线。例如，总线可通信地将一个或多个处理单元与只读存储器、GPU、系统存储器以及永久性存储设备连接。

[0101] 处理单元从这些各种存储器单元检索要执行的指令和要处理的数据，以便执行本发明的过程。在不同实施例中，一个或多个处理单元可为单个处理器或者多核处理器。一些指令被传送至GPU并且由该GPU执行。GPU可卸载各种计算指令，或补充由处理单元提供的图像处理。

[0102] 只读存储器(ROM)存储一个或多个处理单元以及电子系统的其他模块所需的静态数据和指令。另一方面，永久性存储设备是读写存储器设备。该设备是即使在电子系统

[0103] 关闭时也存储指令和数据的非易失性存储器单元。本发明的一些实施例将海量存储设备(诸如磁盘或光盘及其对应的硬盘驱动器)用作永久性存储设备。

[0104] 如本说明书以及本专利申请的任何权利要求所用,术语“计算机”、“服务器”、“处理器”及“存储器”均是指电子或其他技术设备。这些术语排除人或者人的群组。出于本说明书的目的,术语显示或正在显示意指在电子设备上显示。如在本专利申请的本说明书以及任何权利要求中所使用的,术语“计算机可读介质”以及“机器可读介质”完全限于以可由计算机读取的形式存储信息的可触摸的物理对象。这些术语不包括任何无线信号、有线下载信号以及任何其他短暂信号。

[0105] 以上介绍了本发明的较佳实施方式,旨在使得本发明的精神更加清楚和便于理解,并不是为了限制本发明,凡在本发明的精神和原则之内,所做的更新、替换、改进,均应包含在本发明所附的权利要求概况的保护范围之内。

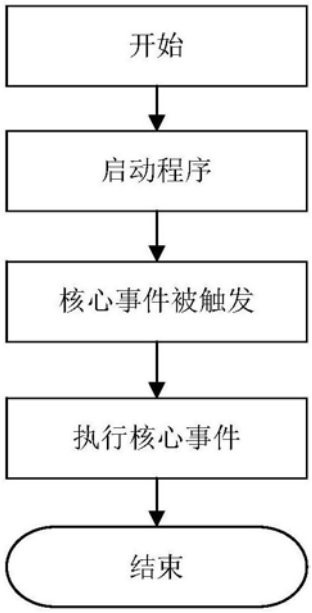

开始
启动程序
核心事件被触发
执行核心事件
结束

图1

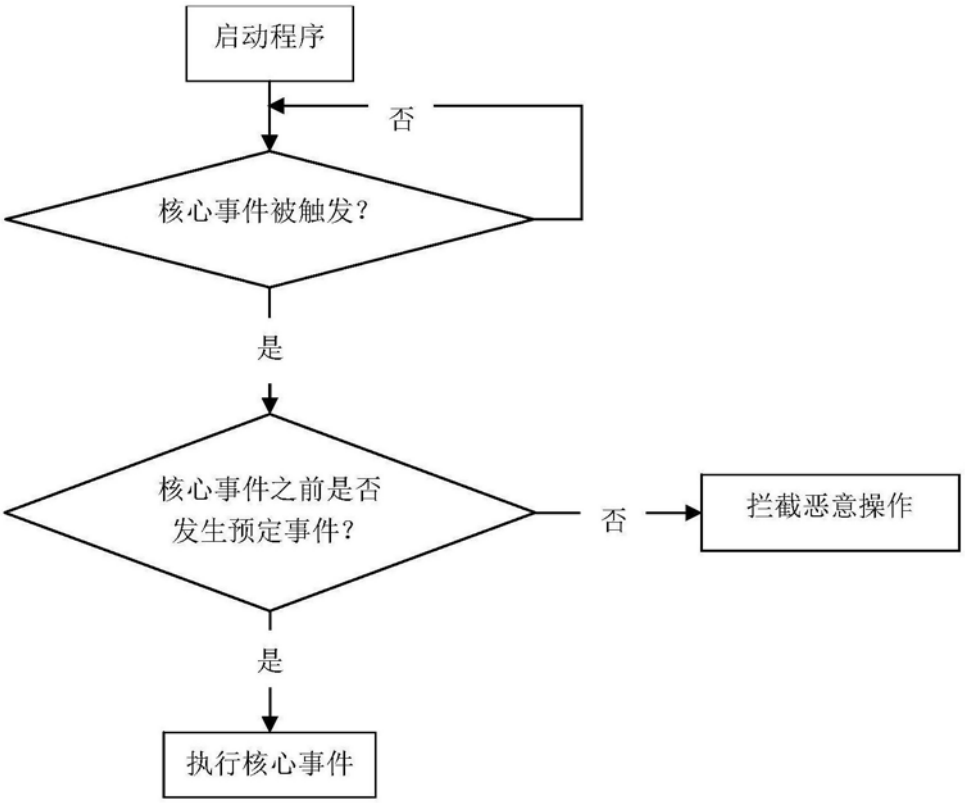

启动程序
否
核心事件被触发?
是
核心事件之前是否
发生预定事件?
否
拦截恶意操作
是
执行核心事件

图2

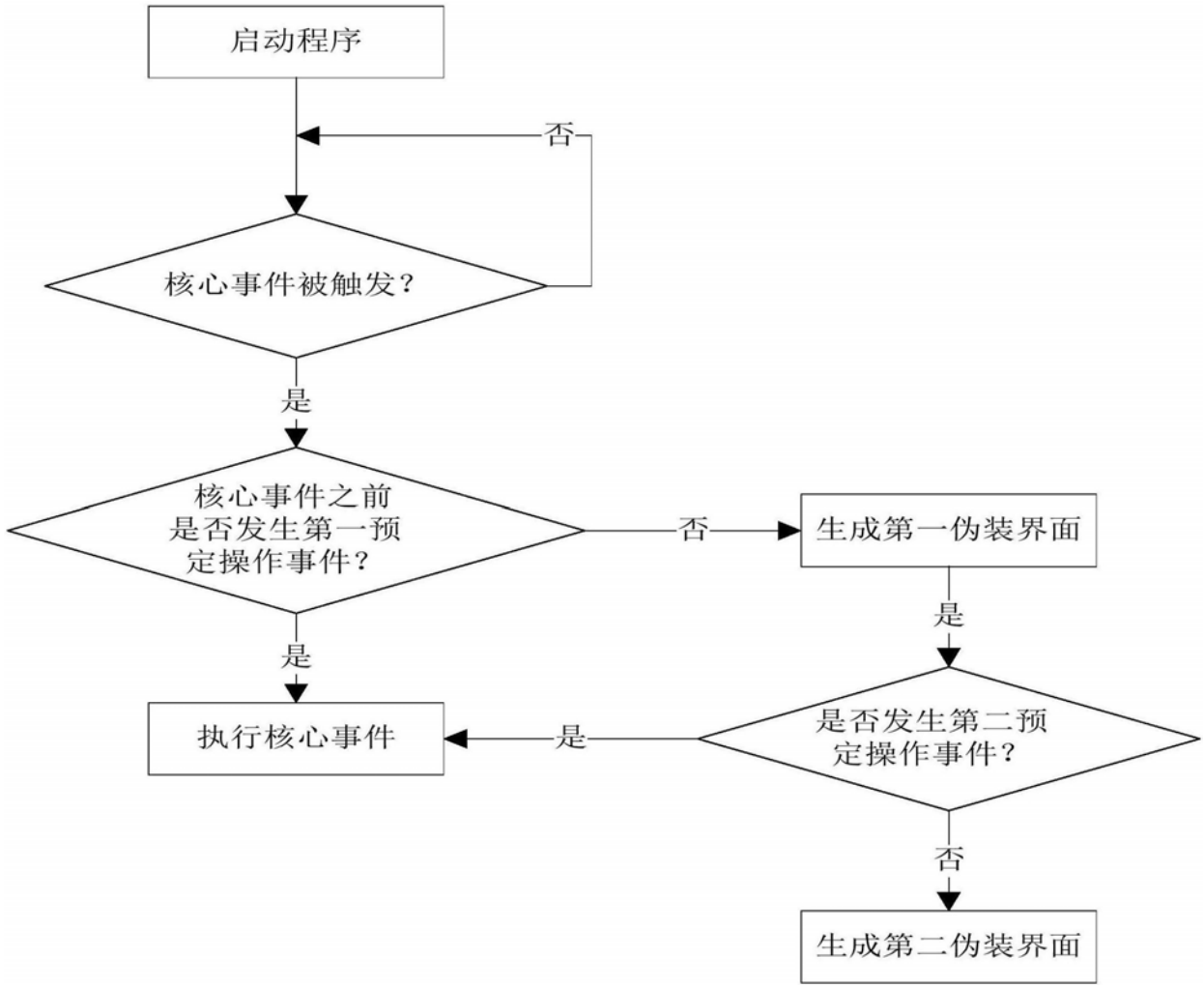

启动程序
否
核心事件被触发？
是
核心事件之前
是否发生第一预
定操作事件？
否
生成第一伪装界面
是
是
是否发生第二预
定操作事件？
是
执行核心事件
否
生成第二伪装界面

图3

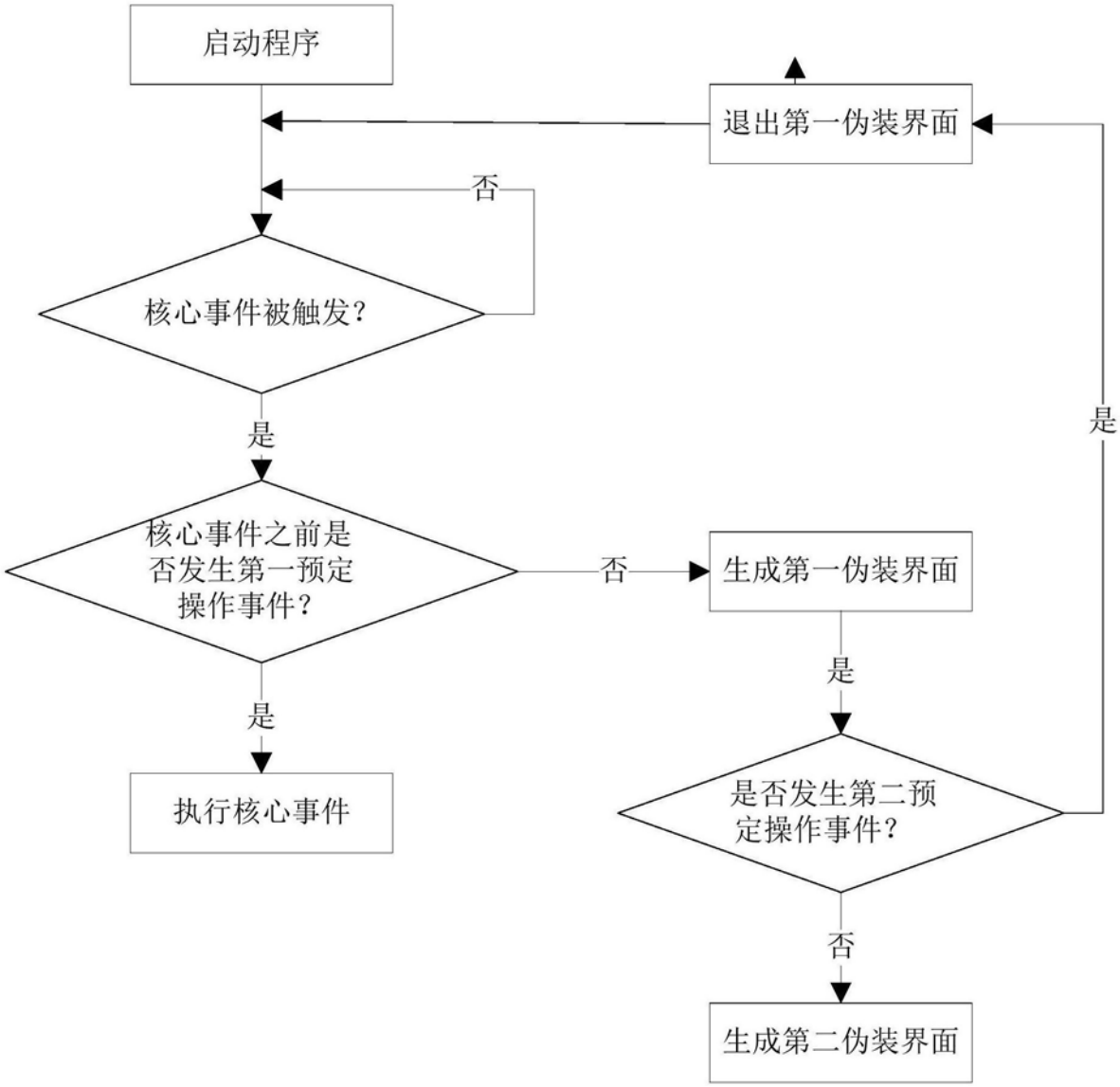

启动程序
退出第一伪装界面
否
核心事件被触发?
是
核心事件之前是否发生第一预定操作事件?
否
生成第一伪装界面
是
是
执行核心事件
是否发生第二预定操作事件?
是
否
生成第二伪装界面

图4

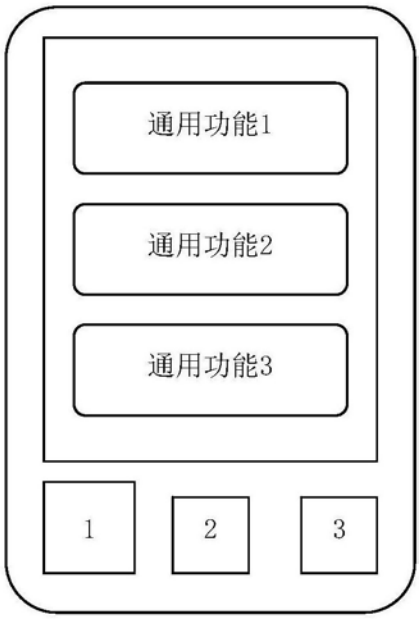


图5

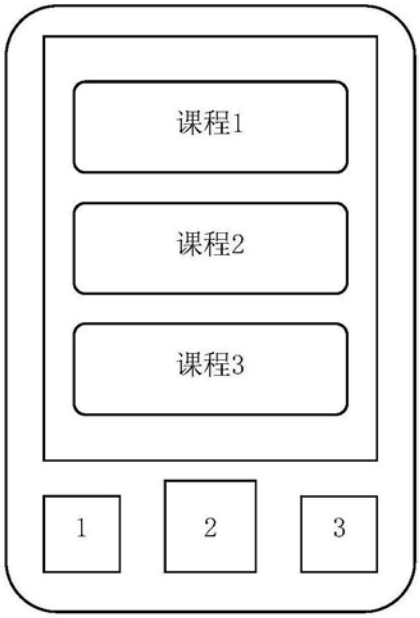


图6

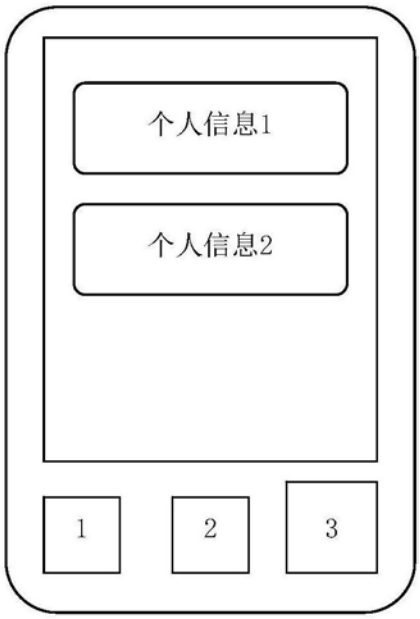


图7