(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 105205386 A
(43)申请公布日 2015.12.30

(21)申请号 201410294478.X

(22)申请日 2014.06.25

(71)申请人 腾讯科技(深圳)有限公司
地址 518000 广东省深圳市福田区振兴路赛格科技园2栋东403室

(72)发明人 胡钊 蒋鑫 吴昊 周思维

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 何平 邓云鹏

(51)Int.Cl.
G06F 21/46(2013.01)
G06F 21/83(2013.01)

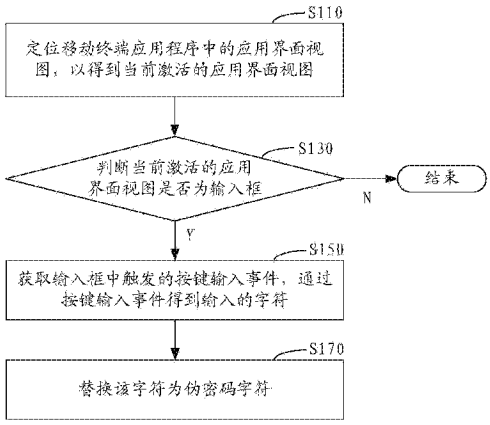
权利要求书2页 说明书7页 附图4页

(54)发明名称

移动终端应用程序密码保护方法和装置

(57)摘要

本发明提供了一种移动终端应用程序密码保护方法和装置。所述方法包括:定位移动终端应用程序中的应用界面视图,以得到当前激活的应用界面视图;判断当前激活的应用界面视图是否为输入框,若为是,则获取输入框中触发的按键输入事件,通过按键输入事件得到输入的字符;替换字符为伪密码字符。所述装置包括:定位模块,用于定位应用界面视图,以得到激活的应用界面视图;判断模块,用于判断激活的应用界面视图是否为输入框,若为是,则通知事件获取模块获取输入框中触发的按键输入事件,通过按键输入事件得到输入的字符;替换模块,用于替换字符为伪密码字符。采用本发明能提高应用中对移动终端应用程序中各种密码的处理的安全性。



CN 105205386 A

1. 一种移动终端应用程序密码保护方法，包括如下步骤：

定位移动终端应用程序中的应用界面视图，以得到当前激活的应用界面视图；

判断所述当前激活的应用界面视图是否为输入框，若为是，则

获取所述输入框中触发的按键输入事件，通过所述按键输入事件得到输入的字符；

替换所述字符为伪密码字符。

2. 根据权利要求 1 所述的方法，其特征在于，所述定位移动终端应用程序中的应用界面视图，以得到当前激活的应用界面视图的步骤包括：

对移动终端应用程序定位触摸屏幕中触点所在的应用界面视图，所述触点所在的应用界面视图即为当前激活的应用界面视图。

3. 根据权利要求 1 所述的方法，其特征在于，所述判断所述当前激活的应用界面视图是否为输入框的步骤包括：

获取当前激活的应用界面视图对应的标识；

判断所述获取的标识是否为输入框标识，若为是，则进入所述获取所述输入框中触发的按键输入事件，通过所述按键输入事件得到输入的字符的步骤。

4. 根据权利要求 1 所述的方法，其特征在于，所述获取所述输入框中触发的按键输入事件，通过所述按键输入事件得到输入的字符的步骤包括：

侦听得到输入框中触发的按键输入事件，根据所述侦听得到的按键输入事件定位输入框中光标所在位置；

获取所述光标所在位置输入的字符，并按照所述光标所在位置保存输入的字符。

5. 根据权利要求 1 所述的方法，其特征在于，所述输入框为密码输入框，所述获取所述输入框中触发的按键输入事件，通过所述按键输入事件得到输入的字符的步骤之后，所述方法还包括：

动态加密所述输入的字符得到加密字符串；

向验证服务器发送所述加密字符串，以请求所述验证服务器进行验证登录。

6. 一种移动终端应用程序密码保护装置，其特征在于，包括：

定位模块，用于定位移动终端应用程序中的应用界面视图，以得到当前激活的应用界面视图；

判断模块，用于判断所述当前激活的应用界面视图是否为输入框，若为是，则通知事件获取模块；

所述事件获取模块用于获取所述输入框中触发的按键输入事件，通过所述按键输入事件得到输入的字符；

替换模块，用于替换所述字符为伪密码字符。

7. 根据权利要求 6 所述的装置，其特征在于，所述定位模块还用于对移动终端应用程序定位触摸屏中触点所在的应用界面视图，所述触点所在的应用界面视图即为当前激活的应用界面视图。

8. 根据权利要求 6 所述的装置，其特征在于，所述判断模块包括：

标识获取单元，用于获取当前激活的应用界面视图对应的标识；

标识判断单元，用于判断所述获取的标识是否为输入框标识，若为是，则通知所述事件获取模块。

9. 根据权利要求 6 所述的装置，其特征在于，所述事件获取模块包括：

侦听单元，用于侦听得到输入框中触发的按键输入事件，根据所述侦听得到的按键输入事件定位输入框中光标所在位置；

字符获取单元，用于获取所述光标所在位置输入的字符，并按照所述光标所在位置保存输入的字符。

10. 根据权利要求 6 所述的装置，其特征在于，所述输入框为密码输入框，所述装置还包括：

动态加密模块，用于动态加密所述输入的字符得到加密字符串；

登录发起模块，用于向验证服务器发送所述加密字符串，以请求所述验证服务器进行验证登录。

移动终端应用程序密码保护方法和装置

技术领域

[0001] 本发明涉及互联网应用技术，特别是涉及一种移动终端应用程序密码保护方法和装置。

背景技术

[0002] 随着互联网的发展，用户已经可以使用各种移动设备随时随地进行各种输入，例如，为即时通信工具的登录进行密码输入，用户将通过即时通信工具中的密码输入框完成密码的输入操作，以触发密码输入框中的按键输入事件。

[0003] 然而，用户输入的各种字符所涉及的安全性问题层出不穷，系统中由按键输入事件所得到的字符的盗取方式由简单的假框等方式发展到了技术性非常高的内存截获盗取方式。

[0004] 为避免输入字符的盗取，应用可在用户触发输入操作时加载自定义键盘，接管系统中处理按键输入事件流程。但是，自定义键盘存在着兼容性问题，应用被恶意代码注入后自定义键盘将无法发挥其作用。

[0005] 此外，系统也可通过按键输入事件回调函数拦截输入的字符，以对其进行各种加密处理，但是，由于拦截点是系统的公开接口，且处于系统处理按键事件流程的末端，因此易于被破坏者轻易利用。

[0006] 因此，应用中对各种按键输入事件的处理存在着安全上的局限性，使得移动终端应用程序中的密码安全性不高。

发明内容

[0007] 基于此，有必要提供一种能提高密码安全性的移动终端应用程序密码保护方法。

[0008] 此外，还有必要提供一种能提高密码安全性的移动终端应用程序密码保护系统。

[0009] 一种移动终端应用程序密码保护方法，包括如下步骤：

[0010] 定位移动终端应用程序中的应用界面视图，以得到当前激活的应用界面视图；

[0011] 判断所述当前激活的应用界面视图是否为输入框，若为是，则

[0012] 获取所述输入框中触发的按键输入事件，通过所述按键输入事件得到输入的字符；

[0013] 替换所述字符为伪密码字符。

[0014] 一种移动终端应用程序密码保护装置，包括：

[0015] 定位模块，用于定位移动终端应用程序中的应用界面视图，以得到当前激活的应用界面视图；

[0016] 判断模块，用于判断所述当前激活的应用界面视图是否为输入框，若为是，则通知事件获取模块；

[0017] 所述事件获取模块用于获取所述输入框中触发的按键输入事件，通过所述按键输入事件得到输入的字符；

[0018] 替换模块，用于替换所述字符为伪密码字符。

[0019] 上述移动终端应用程序密码保护方法和装置，在移动终端应用程序所开启的应用界面视图中进行定位以得到当前所激活的应用界面视图，判断当前激活的应用界面视图是否为输入框，若为是，则说明该输入框即将触发按键输入事件，此时，将获取用户在输入框中触发的按键输入事件，通过按键输入事件得到输入的字符，并对该字符进行替换，以得到伪密码字符，将得到的伪密码字符交由系统处理按键事件流程，即便发生了伪密码字符的盗取也无法获知输入框中真正输入的字符，有效提高了密码的安全性。

附图说明

[0020] 图 1 为一个实施例中移动终端应用程序密码保护方法的流程图；

[0021] 图 2 为图 1 中判断当前激活的应用界面视图是否为输入框的方法流程图；

[0022] 图 3 为图 1 中获取输入框中触发的按键输入事件，通过按键输入事件得到输入的字符的方法流程图；

[0023] 图 4 为另一个实施例中移动终端应用程序密码保护方法的流程图；

[0024] 图 5 为一个实施例中移动终端应用程序密码保护的应用示意图；

[0025] 图 6 为一个实施例中移动终端应用程序密码保护装置的结构示意图；

[0026] 图 7 为图 6 中判断模块的结构示意图；

[0027] 图 8 为图 6 中事件获取模块的结构示意图；

[0028] 图 9 为另一个实施例中移动终端应用程序密码保护装置的结构示意图。

具体实施方式

[0029] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0030] 在一个实施例中，如图 1 所示，一种移动终端应用程序密码保护方法，包括如下步骤：

[0031] 步骤 110，定位移动终端应用程序中的应用界面视图，以得到当前激活的应用界面视图。

[0032] 本实施例中，应用界面视图即为当前运行的移动终端应用程序所展示于屏幕中的视图，将为用户提供相应的操作界面，其中，展示于屏幕中的应用界面视图为一个或者多个，例如，其可为供用户触发操作的按钮、输入框等。

[0033] 在当前展示于屏幕的应用界面视图中进行定位，随着用户的操作得到当前被用户所激活的应用界面视图。

[0034] 在一个实施例中，上述步骤 110 包括：对移动终端应用程序定位触摸屏中触点所在的应用界面视图，该触点所在的应用界面视图即为当前激活的应用界面视图。

[0035] 本实施例中，用于展示应用界面视图的屏幕为触摸屏。随着用户的手指在触摸屏中的移动，将感知相应触点的移动，当触点移动到任意应用界面视图时，该应用界面视图将被激活，触点所在的应用界面视图即为当前激活的应用界面视图。

[0036] 步骤 130，判断当前激活的应用界面视图是否为输入框，若为是，则进入步骤 150，

若为否，则结束。

[0037] 本实施例中，对当前激活的应用界面视图进行判断，若判断到当前激活的应用界面视图为输入框，则说明用户即将触发按键输入事件，在输入框中进行字符的输入；若判断到当前激活的应用界面视图不是输入框，则说明用户即将触发其它的一些操作，而与按键输入事件无关，因此，将结束按键输入事件的处理流程。

[0038] 具体的，将通过触摸事件（TouchEvent 事件）回调函数进行当前激活的应用界面视图是否为输入框的判断，以准确感知用户和应用之间的交互。

[0039] 步骤 150，获取输入框中触发的按键输入事件，通过按键输入事件得到输入的字符。

[0040] 本实施例中，将通过在输入框中触发的按键输入事件在输入框中进行字符的输入，此时，将直接获取由按键输入事件产生的输入的字符。

[0041] 步骤 170，替换该字符为伪密码字符。

[0042] 本实施例中，将输入的每一字符均替换为相应的伪密码字符，以达到伪装干扰的目的，扰乱恶意窃取的行为。

[0043] 通过如上所述的按键输入事件的处理，将使得 android 平台下所触发的按键输入事件更为安全，不会因其独特的开源特性而为恶意盗取者提供了便捷，极大地降低了输入字符被盗取的风险，从而使得运行于 android 平台中具备支付功能的应用在登录和支付环节都更为安全。

[0044] 在一个实施例中，如图 2 所示，上述步骤 130 包括：

[0045] 步骤 131，获取当前激活的应用界面视图对应的标识。

[0046] 本实施例中，每一应用界面视图均有唯一对应的标识，因此，若定位得到当前激活的应用界面视图之后，将获取当前激活的应用界面视图所对应的标识。

[0047] 随着用户与屏幕的接触，系统将感知捕获到触摸事件，并通过一定的接口函数进行触摸事件的处理。具体的，以即时通信工具的例，当用户在即时通信工具的启动界面上触摸了密码输入框所在的区域之后，将获取这一区域所对应的标识。

[0048] 步骤 133，判断获取的标识是否为输入框标识，若为是，则进入步骤 150，若为否，则结束。

[0049] 本实施例中，获取的标识将指示了当前被激活的应用界面视图是否是密码输入框，即密码框控件视图，具体的，调用触摸事件回调函数对获取的标识进行判断，以根据判断结果进行后续的处理过程。

[0050] 在一个实施例中，如图 3 所示，上述步骤 150 包括：

[0051] 步骤 151，侦听得到输入框中触发的按键输入事件，根据侦听得到的按键输入事件定位输入框中光标所在位置。

[0052] 本实施例中，随着输入框中进行的字符输入，光标所在位置也在不断发生变化。侦听得到输入框中触发的按键输入事件之后，将重载 onSelectionChanged 函数获取输入框中光标所在位置，实现光标所在位置的实时跟踪。

[0053] 步骤 153，获取光标所在位置输入的字符，并按照光标所在位置保存输入的字符。

[0054] 本实施例中，以光标所在位置为字符串数组内存的下标，将输入的字符保存于该字符串数组内存中，以实现字符的准确获取和保存。

[0055] 具体的，对于输入框所进行的字符输入而言，所采用的输入方式包括了硬键盘输入和软键盘输入，因此将根据输入方式进行字符的获取。

[0056] 在硬键盘输入方式下，将重载 dispatchKeyEvent 函数获取光标所在位置获取当前输入的字符，并保存到新的字符串数组内存中。

[0057] 在软键盘输入方式下，将新建 InputConnection 输入通道，将新建的 InputConnection 输入通道和当前触发的按键输入事件绑定，通过新建的 InputConnection 输入通道处理当前触发的按键输入事件，此时，将重载 commintText、sendKeyEvent、setComposingText 和 finishComposingText 等系统函数拦截当前输入的字符，并复制到新的字符串数组内存中。

[0058] 该字符串数组内存均是以光标所在位置为下标进行输入字符的保存的。

[0059] 在一个实施例中，如图 4 所示，如上所述的输入框为密码输入框，上述步骤 150 之后，如上所述的方法还包括如下步骤：

[0060] 步骤 410，动态加密输入的字符得到加密字符串。

[0061] 本实施例中，获取得到的输入的字符即为用户进行应用登录所对应的密码，因此，为进一步保证登录的安全性，将对输入的字符进行动态加密，以使得用于进行登录验证的密码不是以明文形式进行传递的。

[0062] 步骤 430，向验证服务器发送加密字符串，以请求验证服务器进行验证登录。

[0063] 本实施例中，应用将与验证服务器进行交互，以通过验证服务器完成应用所发起的验证登录。

[0064] 具体的，应用将向验证服务器发送加密字符串，验证服务器在接收到应用所发送的加密字符串之后，将对加密字符串进行解密以完成应用的验证登录，保证了登录密码的安全。

[0065] 通过如上所述的方式，将有效地防止了密码被恶意程序监听和盗取，保证了用户的密码安全，提高了应用的安全性。

[0066] 在一个实施例中，在输入框为密码输入框的场景下，上述步骤 150 之后还将包括了检测输入的字符的合法性的步骤。

[0067] 本实施例中，将检测输入的字符是否符合应用自身规定的字符形式要求，例如，即时通信工具只接受规定范围内的字符所组成的字符串，对于不在规定范围内的其它字符或者特殊字符，即时通信工具是无法正常登录的，因此，需要检测输入的字符的合法性，判断输入的字符是否合法，并在判断结果为是的前提条件下方可进行字符的替换以及动态加密，以保证应用的正常运行。

[0068] 下面结合一个具体的实施例来详细阐述上述移动终端应用程序密码保护方法。该实施例中，如图 5 所示，在移动终端所运行的应用程序中，在用户开始输入时即触发开始了整个移动终端应用程序的密码保护流程。

[0069] 将首先执行步骤 510，通过 TouchEvent 回调确认光标所在视图，并执行步骤 520 进行当前光标所在视图是否为密码框的判断，以通过步骤 510 和步骤 520 准确感知用户和移动终端中应用程序之间的交互。

[0070] 若步骤 520 判断当前光标所在视图并不是密码框，则说明当前所进行的交互与本发明所涉及的应用程序密码保护并不相关，因此，将交由系统处理。

[0071] 若步骤520判断当前光标所在视图为密码框，则由步骤530加载密码框控件类，即加载密码控件视图，并随着密码框中字符的输入执行步骤540，重载系统函数onSelectionChanged来获取密码框中光标所在位置，以对密码框中光标的移动进行实时跟踪。

[0072] 由于所采用的输入方式包括了软键盘输入和硬键盘输入，因此，将需要根据输入方式进行字符的获取。

[0073] 也就是说，在硬键盘输入的场景下，将执行步骤550重载系统函数dispatchKeyEvent进行密码框中的字符拦截，并与步骤540所得到的光标所在位置作为下标组成新密码字符串，以便于保存于字符串数组内存中。

[0074] 在软键盘输入的场景下，将执行步骤570和580建立新的InputConnection输入通道，重载系统函数commintText、sendKeyEvent、setComposingText和finishComposingText进行字符拦截，以得到密码框当前输入的字符，并与步骤540所得到的光标所在位置作为下标组成新密码字符串，以便于保存于字符串数组内存中。

[0075] 所组装得到的新密码字符串将在加密后发送至服务器中进行验证登录，即通过执行步骤590完成移动终端应用程序的验证登录，并且使得密码不以明文形式进行传递，进一步保证了登录的安全性。

[0076] 如图6所示，在一个实施例中，一种按键输入事件的处理装置包括定位模块610、判断模块630、事件获取模块650和替换模块670。

[0077] 定位模块610，用于定位应用界面视图，以得到当前激活的应用界面视图。

[0078] 本实施例中，应用界面视图即为当前运行的应用所展示于屏幕中的视图，将为用户提供相应的操作界面，其中，展示于屏幕中的应用界面视图为一个或者多个，例如，其可为供用户触发操作的按钮、输入框等。

[0079] 定位模块610在当前展示于屏幕的应用界面视图中进行定位，随着用户的操作得到当前被用户所激活的应用界面视图。

[0080] 在一个实施例中，定位模块610还用于定位触摸屏中触点所在的应用界面视图，该触点所在的应用界面视图即为当前激活的应用界面视图。

[0081] 本实施例中，用于展示应用界面视图的屏幕为触摸屏。随着用户的手指在触摸屏中的移动，定位模块610将感知相应触点的移动，当触点移动到任意应用界面视图时，该应用界面视图将被激活，触点所在的应用界面视图即为当前激活的应用界面视图。

[0082] 判断模块630，用于判断当前激活的应用界面视图是否为输入框，若为是，则通知事件获取模块650，若为否，则停止执行。

[0083] 本实施例中，判断模块630对当前激活的应用界面视图进行判断，若判断模块630判断到当前激活的应用界面视图为输入框，则说明用户即将触发按键输入事件，在输入框中进行字符的输入；若判断模块630判断到当前激活的应用界面视图不是输入框，则说明用户即将触发其它的一些操作，而与按键输入事件无关，因此，将结束按键输入事件的处理流程。

[0084] 具体的，判断模块630将通过触摸事件（回调函数进行当前激活的应用界面视图是否为输入框的判断，以准确感知用户和应用之间的交互。

[0085] 事件获取模块650，用于获取输入框中触发的按键输入事件，通过按键输入事件得

到输入的字符。

[0086] 本实施例中，将通过在输入框中触发的按键输入事件在输入框中进行字符的输入，此时，事件获取模块 650 将直接获取由按键输入事件产生的输入的字符。

[0087] 替换模块 670，用于替换字符为伪密码字符。

[0088] 本实施例中，替换模块 670 将输入的每一字符均替换为相应的伪密码字符，以达到伪装干扰的目的，扰乱恶意窃取的行为。

[0089] 通过如上所述的按键输入事件的处理，将使得 android 平台下所触发的按键输入事件更为安全，不会因其独特的开源特性而为恶意盗取者提供了便捷，极大地降低了输入字符被盗取的风险，从而使得运行于 android 平台中具备支付功能的应用在登录和支付环节都更为安全。

[0090] 如图 7 所示，在一个实施例中，上述判断模块 630 包括标识获取单元 631 和标识判断单元 633。

[0091] 标识获取单元 631，用于获取当前激活的应用界面视图对应的标识。

[0092] 本实施例中，每一应用界面视图均有唯一对应的标识，因此，若定位得到当前激活的应用界面视图之后，标识获取单元 631 将获取当前激活的应用界面视图所对应的标识。

[0093] 随着用户与屏幕的接触，系统中的标识获取单元 631 将感知捕获到触摸事件，并通过一定的接口函数进行触摸事件的处理。具体的，以即时通信工具的例，当用户在即时通信工具的启动界面上触摸了密码输入框所在的区域之后，标识获取单元 631 将获取这一区域所对应的标识。

[0094] 标识判断单元 633，用于判断获取的标识是否为输入框标识，若为是，则通知事件获取模块 650，若为否，则停止执行。

[0095] 本实施例中，获取的标识将指示了当前被激活的应用界面视图是否是密码输入框，即密码框控件视图，具体的，标识判断单元 633 调用触摸事件回调函数对获取的标识进行判断，以根据判断结果进行后续的处理过程。

[0096] 如图 8 所示，在一个实施例中，上述事件获取模块 650 包括侦听单元 651 和字符获取单元 653。

[0097] 侦听单元 651，用于侦听得到输入框中触发的按键输入事件，根据侦听得到的按键输入事件定位输入框中光标所在位置。

[0098] 本实施例中，随着输入框中进行的字符输入，光标所在位置也在不断发生变化。侦听单元 651 侦听得到输入框中触发的按键输入事件之后，将重载 onSelectionChanged 函数获取输入框中光标所在位置，实现光标所在位置的实时跟踪。

[0099] 字符获取单元 653，用于获取光标所在位置输入的字符，并按照光标所在位置保存输入的字符。

[0100] 本实施例中，字符获取单元 653 以光标所在位置为字符串数组内存的下标，将输入的字符保存于该字符串数组内存中，以实现字符的准确获取和保存。

[0101] 具体的，对于输入框所进行的字符输入而言，所采用的输入方式包括了硬键盘输入和软键盘输入，因此字符获取单元 653 将根据输入方式进行字符的获取。

[0102] 在硬键盘输入方式下，字符获取单元 653 将重载 dispatchKeyEvent 函数获取光标所在位置获取当前输入的字符，并保存到新的字符串数组内存中。

[0103] 在软键盘输入方式下，字符获取单元653将新建InputConnection输入通道，将新建的InputConnection输入通道和当前触发的按键输入事件绑定，通过新建的InputConnection输入通道处理当前触发的按键输入事件，此时，将重载commintText、sendKeyEvent、setComposingText和finishComposingText等系统函数拦截当前输入的字符，并复制到新的字符串数组内存中。

[0104] 该字符串数组内存均是以光标所在位置为下标进行输入字符的保存的。

[0105] 如图9所示，在一个实施例中，上述输入框为密码输入框，如上所述的装置还包括了动态加密模块910和登录发起模块930。

[0106] 动态加密模块910，用于动态加密输入的字符得到加密字符串。

[0107] 本实施例中，获取得到的输入的字符即为用户进行应用登录所对应的密码，因此，为进一步保证登录的安全性，动态加密模块910将对输入的字符进行动态加密，以使得用于进行登录验证的密码不是以明文形式进行传递的。

[0108] 登录发起模块930，用于向验证服务器发送加密字符串，以请求验证服务器进行验证登录。

[0109] 本实施例中，应用将与验证服务器进行交互，以通过验证服务器完成应用所发起的验证登录。

[0110] 具体的，登录发起模块930将向验证服务器发送加密字符串，验证服务器在接收到应用所发送的加密字符串之后，将对加密字符串进行解密以完成应用的验证登录，保证了登录密码的安全。

[0111] 通过如上所述的方式，将有效地防止了密码被恶意程序监听和盗取，保证了用户的密码安全，提高了应用的安全性。

[0112] 在一个实施例中，在输入框为密码输入框的场景下，上述装置还将包括了合法性检测模块，该合法性检测模块用于检测输入的字符的合法性。

[0113] 本实施例中，合法性检测模块将检测输入的字符是否符合应用自身规定的字符形式要求，例如，即时通信工具只接受规定范围内的字符所组成的字符串，对于不在规定范围内的其它字符或者特殊字符，即时通信工具是无法正常登录的，因此，需要合法性检测模块检测输入的字符的合法性，判断输入的字符是否合法，并在判断结果为是的前提条件下方可进行字符的替换以及动态加密，以保证应用的正常运行。

[0114] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述程序可存储于一计算机可读取存储介质中，如本发明实施例中，该程序可存储于计算机系统的存储介质中，并被该计算机系统中的至少一个处理器执行，以实现包括如上述各方法的实施例的流程。其中，所述存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0115] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

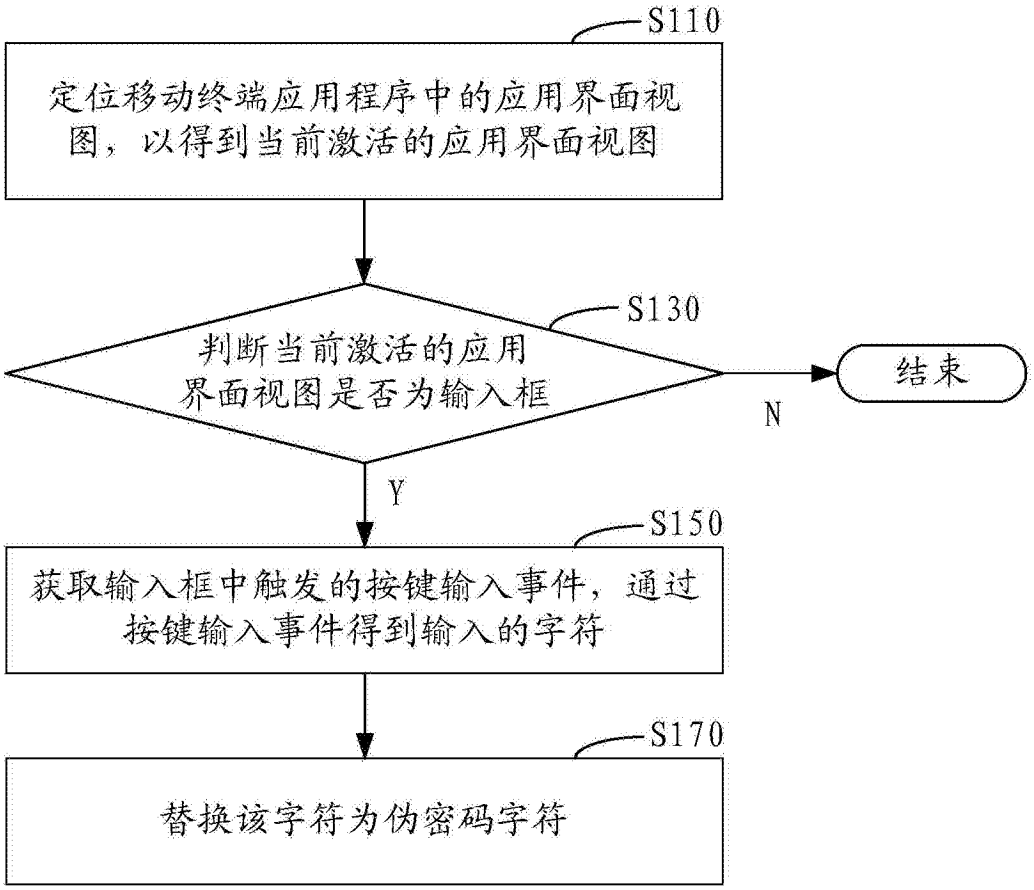

S110
定位移动终端应用程序中的应用界面视图，以得到当前激活的应用界面视图
S130
判断当前激活的应用界面视图是否为输入框
结束
N
Y
S150
获取输入框中触发的按键输入事件，通过按键输入事件得到输入的字符
S170
替换该字符为伪密码字符

图 1

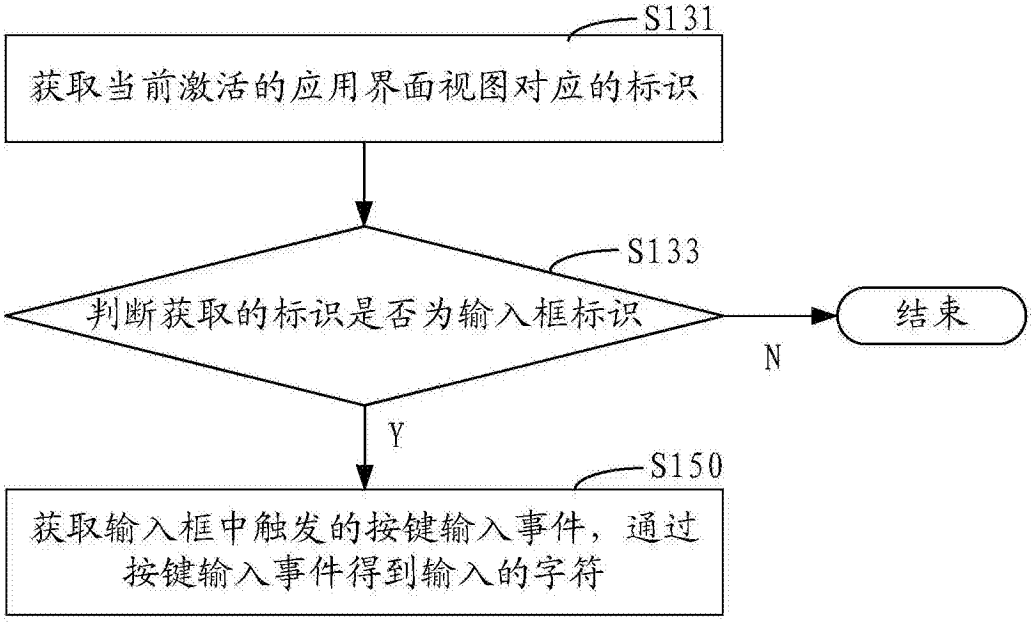

S131
获取当前激活的应用界面视图对应的标识
S133
判断获取的标识是否为输入框标识
结束
N
Y
S150
获取输入框中触发的按键输入事件，通过按键输入事件得到输入的字符

图 2

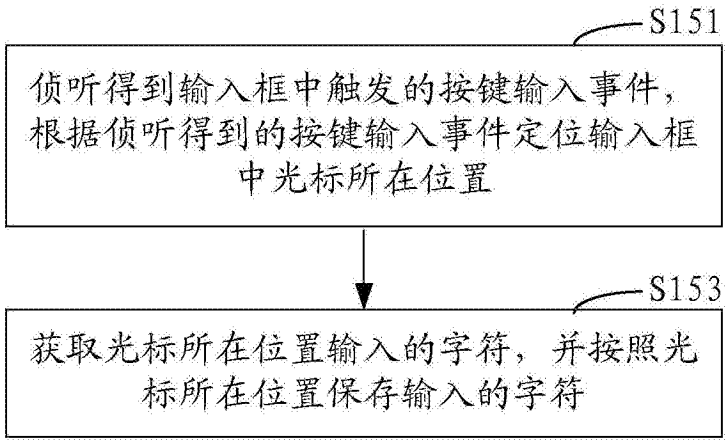

S151
侦听得到输入框中触发的按键输入事件，根据侦听得到的按键输入事件定位输入框中光标所在位置
S153
获取光标所在位置输入的字符，并按照光标所在位置保存输入的字符

图 3

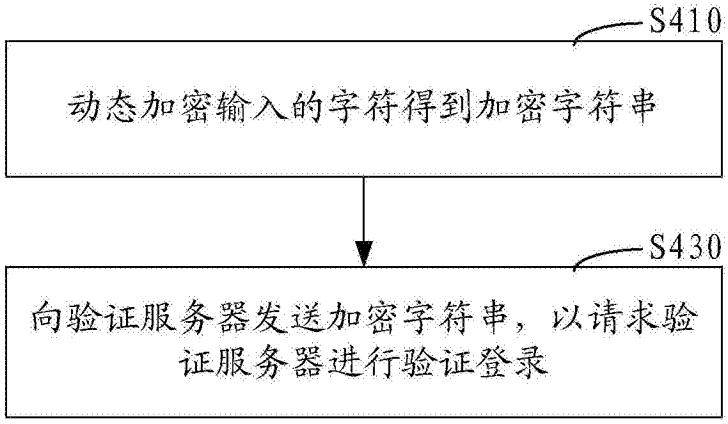

S410
动态加密输入的字符得到加密字符串
S430
向验证服务器发送加密字符串，以请求验证服务器进行验证登录

图 4

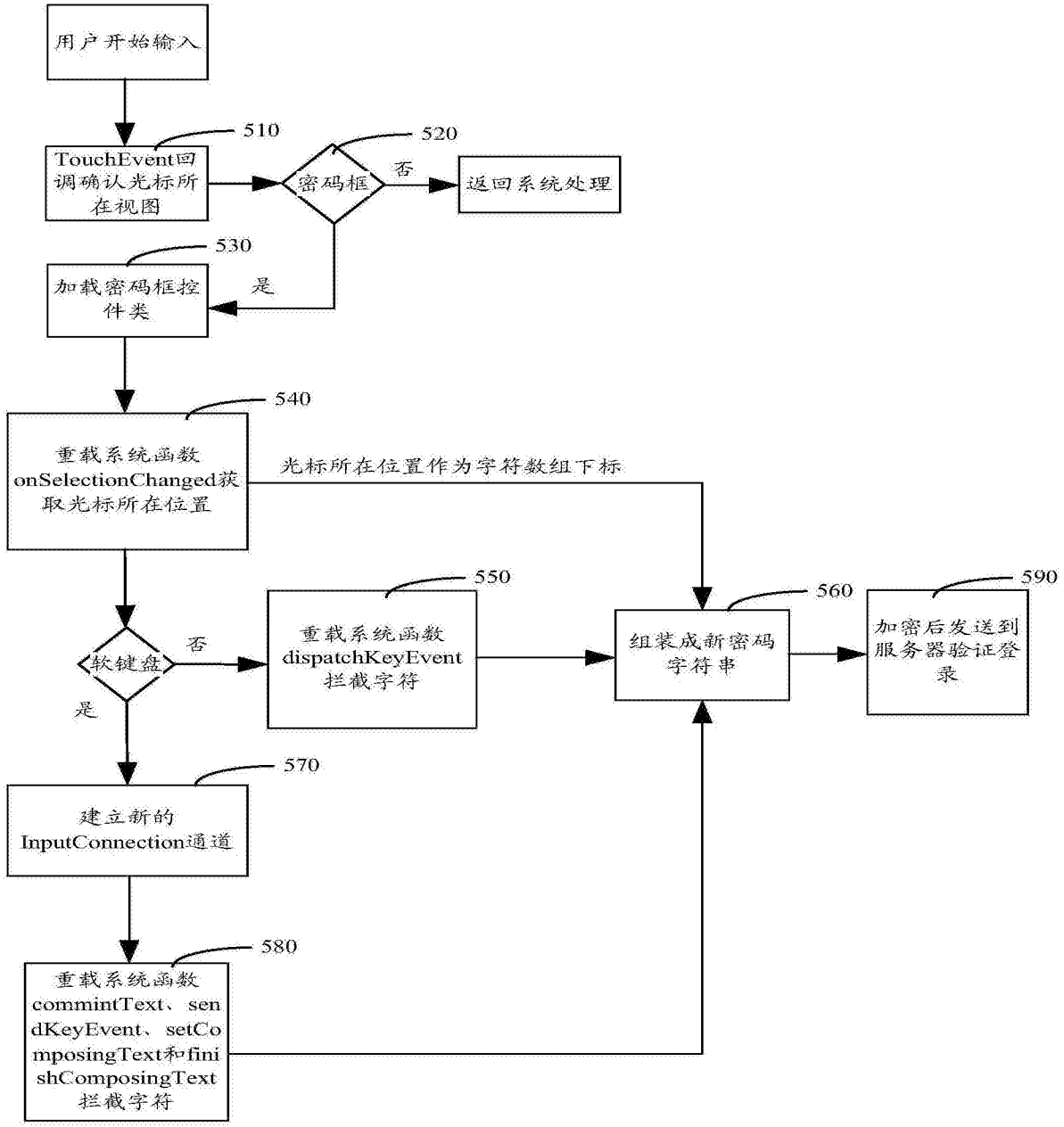

用户开始输入
510
TouchEvent回调确认光标所在视图
520
密码框
否
返回系统处理
是
530
加载密码框控件类
540
重载系统函数onSelectionChanged获取光标所在位置
光标所在位置作为字符数组下标
550
重载系统函数dispatchKeyEvent拦截字符
否
软键盘
是
560
组装成新密码字符串
590
加密后发送到服务器验证登录
570
建立新的InputConnection通道
580
重载系统函数commintText、sendKeyEvent、setComposingText和finishComposingText拦截字符

图 5

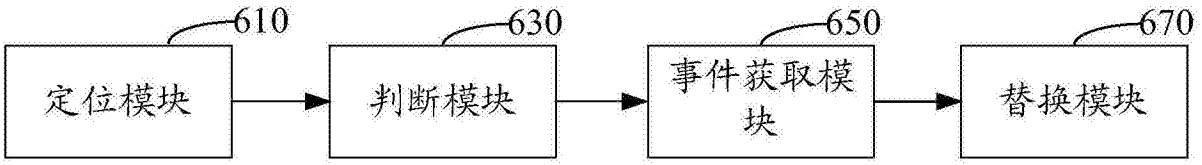

610
定位模块
630
判断模块
650
事件获取模块
670
替换模块

图 6

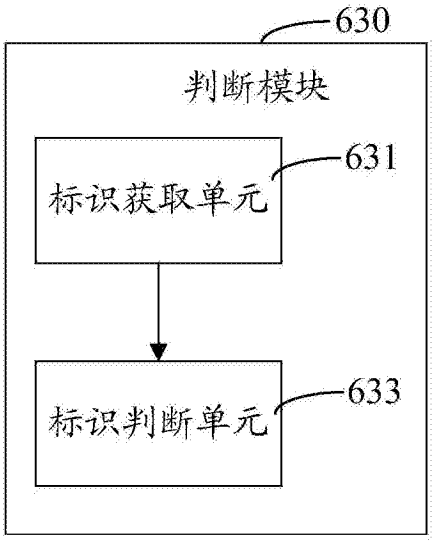

630
判断模块
631
标识获取单元
633
标识判断单元

图 7

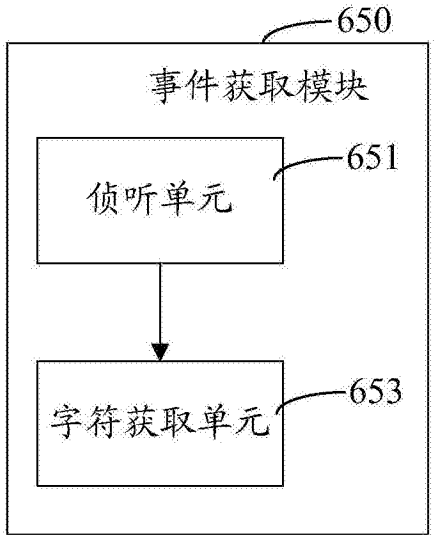

650
事件获取模块
651
侦听单元
653
字符获取单元

图 8

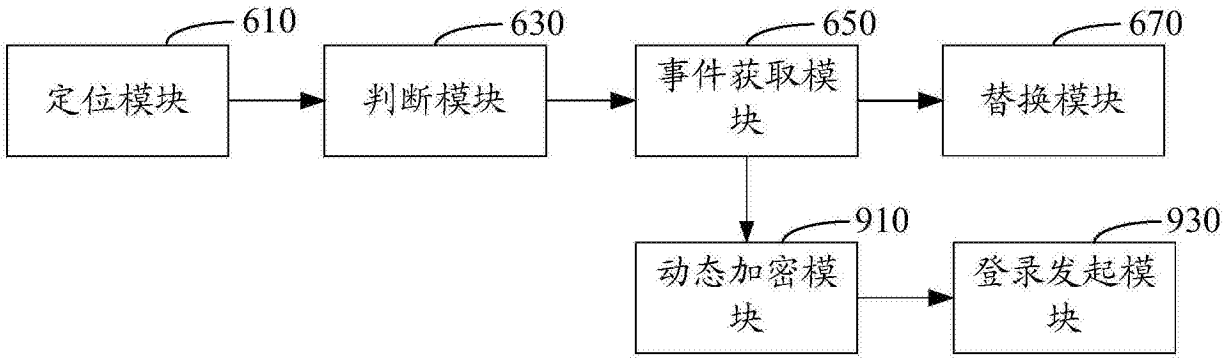

610
定位模块
630
判断模块
650
事件获取模块
670
替换模块
910
动态加密模块
930
登录发起模块

图 9