(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 105653993 A
(43)申请公布日 2016.06.08

(21)申请号 201510860643.8

(22)申请日 2015.11.30

(71)申请人 东莞酷派软件技术有限公司
地址 523500 广东省东莞市松山湖高新技术产业开发区工业西一路3号一期工程1号厂房3楼

(72)发明人 白小龙

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠

(51)Int.Cl.
G06F 21/83(2013.01)
G06F 21/32(2013.01)

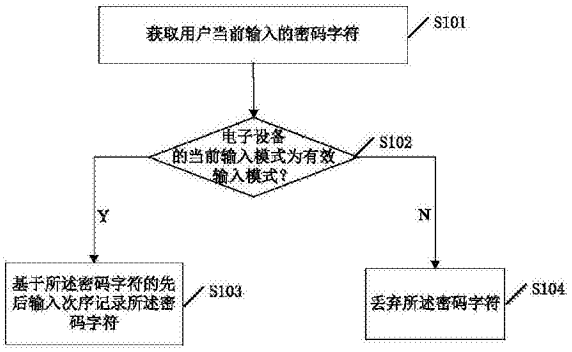
权利要求书1页 说明书6页 附图5页

(54)发明名称

一种密码输入方法、装置及电子设备

(57)摘要

本申请公开一种密码输入方法、装置和电子设备，所述方法在获取到用户当前输入的密码字符时，通过判断所述电子设备的当前输入模式是否为有效输入模式，来确定是记录还是丢弃所述当前密码字符。可见，本申请针对电子设备的密码输入场景，引入了有效及非有效/无效两种类型的输入模式，在用户输入密码过程中，电子设备可基于对输入每个字符时采用的输入模式进行判断识别，实现对用户所输入的各密码字符进行不同处理（记录或丢弃），从而，本申请中，用户可通过对两种输入模式进行结合应用，来为输入过程产生一些非真实输入的字符，以此来迷惑可能的窥窃者，防止密码在输入过程中被窥窃盗取。从而本申请解决了输入密码过程中用户密码的安全问题。



CN 105653993 A

1.一种密码输入方法，其特征在于，应用于电子设备，所述方法包括：

获取用户当前输入的密码字符；

判断所述电子设备的当前输入模式是否为有效输入模式；

如果是有效输入模式，则基于所述密码字符的先后输入次序记录所述密码字符；

如果不是有效输入模式，则丢弃所述密码字符。

2.根据权利要求1所述的方法，其特征在于，所述判断所述电子设备的当前输入模式是否为有效输入模式包括：

判断当前所述电子设备是否符合以下条件：侦测到用户手指按压在指纹识别器上，且当前用户指纹通过验证；其中，所述指纹识别器预先集成在所述电子设备中；

如果符合，则所述电子设备的当前输入模式为有效输入模式

如果不符合，则所述电子设备的当前输入模式为无效输入模式。

3.根据权利要求1或2所述的方法，其特征在于，还包括：

依据预设的输入结束条件，判断用户的密码输入过程是否结束；如果结束，则基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符，得到用户的输入密码。

4.根据权利要求3所述的方法，其特征在于，还包括：

基于预先存储的基准密码，验证所述输入密码的合法性，或向服务器提交所述输入密码。

5.一种密码输入装置，其特征在于，应用于电子设备，所述装置包括：

密码字符获取模块，用于获取用户当前输入的密码字符；

判断模块，用于判断所述电子设备的当前输入模式是否为有效输入模式；

记录模块，用于在判断结果是有效输入模式时，基于所述密码字符的先后输入次序记录所述密码字符；

丢弃模块，用于在判断结果不是有效输入模式时，丢弃所述密码字符。

6.根据权利要求5所述的装置，其特征在于，所述判断模块包括：

判断单元，用于判断当前所述电子设备是否符合以下条件：侦测到用户手指按压在指纹识别器上，且当前用户指纹通过验证；其中，所述指纹识别器预先集成在所述电子设备中；

第一输入模式确定单元，用于在判断结果为符合时，确定出所述电子设备的当前输入模式为有效输入模式

第二输入模式确定单元，用于在判断结果为不符合时，确定出所述电子设备的当前输入模式为无效输入模式。

7.根据权利要求5所述的装置，其特征在于，还包括：

输入密码获取模块，用于依据预设的输入结束条件，判断用户的密码输入过程是否结束；并在判断出结束时，基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符，得到用户的输入密码。

8.根据权利要求7所述的装置，其特征在于，还包括：

密码验证或提交模块，用于基于预先存储的基准密码，验证所述输入密码的合法性，或向服务器提交所述输入密码。

9.一种电子设备，其特征在于，包括如权利要求5-8任意一项所述的密码输入装置。

一种密码输入方法、装置及电子设备

技术领域

[0001] 本发明属于密码安全应用技术领域，尤其涉及一种密码输入方法及装置。

背景技术

[0002] 目前，数字密码已成为用户安全认证中不可或缺的一部分，在向智能手机等终端设备输入数字密码进行用户安全认证时，一般需采用相应的安全措施来防止密码被他人窥窃。

[0003] 现有密码输入方案通过隐藏输入之后的数字密码，例如采用黑点或星型符替代数字进行显示等，来解决输入密码环节用户密码的安全问题。然而此种方式的防窥窃能力有限，仅可确保用户输入密码之后的密码安全，无法解决输入执行过程中的密码安全问题，在密码输入过程中，用户密码极易被他人窥窃盗取，因此，本领域亟需提供一种安全性较高的密码输入方法，来解决输入密码过程中用户密码的安全性问题。

发明内容

[0004] 有鉴于此，本发明的目的在于提供一种一种密码输入方法、装置及电子设备，旨在解决输入密码过程中用户密码的安全性问题，从而提升用户密码的安全度。

[0005] 为此，本发明公开如下技术方案：

[0006] 一种密码输入方法，应用于电子设备，所述方法包括：

[0007] 获取用户当前输入的密码字符；

[0008] 判断所述电子设备的当前输入模式是否为有效输入模式；

[0009] 如果是有效输入模式，则基于所述密码字符的先后输入次序记录所述密码字符；

[0010] 如果不是有效输入模式，则丢弃所述密码字符。

[0011] 上述方法，优选的，所述判断所述电子设备的当前输入模式是否为有效输入模式包括：

[0012] 判断当前所述电子设备是否符合以下条件：侦测到用户手指按压在指纹识别器上，且当前用户指纹通过验证；其中，所述指纹识别器预先集成在所述电子设备中；

[0013] 如果符合，则所述电子设备的当前输入模式为有效输入模式

[0014] 如果不符合，则所述电子设备的当前输入模式为无效输入模式。

[0015] 上述方法，优选的，还包括：

[0016] 依据预设的输入结束条件，判断用户的密码输入过程是否结束；如果结束，则基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符，得到用户的输入密码。

[0017] 上述方法，优选的，还包括：

[0018] 基于预先存储的基准密码，验证所述输入密码的合法性，或向服务器提交所述输入密码。

[0019] 一种密码输入装置，应用于电子设备，所述装置包括：

[0020] 密码字符获取模块，用于获取用户当前输入的密码字符；

[0021] 判断模块，用于判断所述电子设备的当前输入模式是否为有效输入模式；

[0022] 记录模块，用于在判断结果是有效输入模式时，基于所述密码字符的先后输入次序记录所述密码字符；

[0023] 丢弃模块，用于在判断结果不是有效输入模式时，丢弃所述密码字符。

[0024] 上述装置，优选的，所述判断模块包括：

[0025] 判断单元，用于判断当前所述电子设备是否符合以下条件：侦测到用户手指按压在指纹识别器上，且当前用户指纹通过验证；其中，所述指纹识别器预先集成在所述电子设备中；

[0026] 第一输入模式确定单元，用于在判断结果为符合时，确定出所述电子设备的当前输入模式为有效输入模式

[0027] 第二输入模式确定单元，用于在判断结果为不符合时，确定出所述电子设备的当前输入模式为无效输入模式。

[0028] 上述装置，优选的，还包括：

[0029] 输入密码获取模块，用于依据预设的输入结束条件，判断用户的密码输入过程是否结束；并在判断出结束时，基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符，得到用户的输入密码。

[0030] 上述装置，优选的，还包括：

[0031] 密码验证或提交模块，用于基于预先存储的基准密码，验证所述输入密码的合法性，或向服务器提交所述输入密码。

[0032] 一种电子设备，包括如上所述的密码输入装置。

[0033] 由以上方案可知，本申请公开的密码输入方法，在获取到用户当前输入的密码字符时，通过判断所述电子设备的当前输入模式是否为有效输入模式，来确定是记录还是丢弃所述当前密码字符。可见，本申请针对电子设备的密码输入问题，引入了有效及非有效/无效两种类型的输入模式，在用户输入密码过程中，电子设备可基于对输入每个字符时采用的输入模式进行判断识别，实现对用户所输入的各密码字符进行不同处理（记录或丢弃），从而，本申请中，用户可通过对两种输入模式进行结合应用，来为输入过程产生一些非真实输入的字符，以此来迷惑可能的窥窃者，防止密码在输入过程中被窥窃盗取。从而本申请解决了输入密码过程中用户密码的安全问题。

附图说明

[0034] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

[0035] 图1是本发明实施例一提供的密码输入方法流程图；

[0036] 图2是本发明实施例一提供的两种输入模式的判断策略示意图；

[0037] 图3是本发明实施例一提供的本申请方法的一应用示例图；

[0038] 图4是本发明实施例二提供的密码输入方法流程图；

[0039] 图5是本发明实施例三提供的密码输入方法流程图；

[0040] 图6-图8是本发明实施例四提供的密码输入装置的结构示意图。

具体实施方式

[0041] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0042] 为解决输入密码过程中用户密码的安全性问题，本申请通过向电子设备引入有效及无效两种类型的输入模式，实现在用户输入密码过程中，支持用户通过对两种输入模式的结合应用，来为输入过程产生一些非真实输入的字符，以此来迷惑可能的窥窃者，防止密码在输入过程中被窥窃盗取。以下将通过多个实施例对本申请方法进行说明。

[0043] 实施例一

[0044] 本发明实施例一公开一种密码输入方法，所述方法可应用于智能手机、平板电脑等电子设备，参考图1，所述方法可以包括以下步骤：

[0045] S101：获取用户当前输入的密码字符。

[0046] 其中，所述密码字符可以是数字、字母或键盘上的各种特殊符号(如下划线、圆点符)等。

[0047] 本步骤接收用户通过设备键盘或手写等方式向电子设备输入的当前密码字符，并缓存所述当前密码字符。

[0048] S102：判断所述电子设备的当前输入模式是否为有效输入模式。

[0049] 本申请向电子设备引入两种输入模式：有效输入模式及无效输入模式，并基于指纹识别技术提供以上两种输入模式的判断策略，其中，参考图2，当用户手指按压在电子设备的指纹识别器上，且按压操作所输入的指纹通过电子设备的合法性验证(输入指纹与用户预先在电子设备注册的指纹一致，则通过验证)，则电子设备的当前模式为有效输入模式，从而，在用户合法注册的手指按压指纹识别器期间，用户向电子设备输入的密码字符可被有效录入；否则，如果用户手指未按压在指纹识别器上，或按压在指纹识别器上时所输入的指纹未通过验证，则电子设备的当前模式为无效输入模式。

[0050] 基于此，本步骤中，具体可通过判断电子设备是否符合以下条件，来获知其当前模式是否为有效输入模式：侦测到用户手指按压在指纹识别器上，且当前用户指纹通过验证。

[0051] 实际应用中，用户可依据其使用习惯预先注册一个或多个验证指纹，从而在输入密码过程中，可依据实际按压操作的便捷性需求，选择任意一个合法注册的指纹所对应的手指执行按压操作，实现将电子设备的输入模式控制为有效输入模式，而一旦用户手指脱离指纹识别器，电子设备随即进入无效输入模式，即用户可通过采用合法注册的手指在指纹识别器进行按压或撤离，控制电子设备进入有效输入模式或无效输入模式。

[0052] 本申请方法的实施需预先在电子设备中集成一指纹识别器，其中，技术人员具体可基于电子设备的ID(industrial design，工业设计)需求，并结合密码输入的安全性需求、用户操作的便捷性需求等，对指纹识别器在电子设备中的集成位置进行布局，其中，作为一优选方案，本实施例采用将指纹识别器集成在电子设备背部，此种布局方式为用户操

作指纹识别器提供了便利，同时可提升用户手指操作指纹识别器的隐秘性，从而进一步提升了输入密码过程中用户密码的安全程度

[0053] S103：如果是有效输入模式，则基于所述密码字符的先后输入次序记录所述密码字符。

[0054] 如果判断出电子设备的当前模式为有效输入模式，即用户手指当前按压在指纹识别器上，且用户指纹通过合法性验证，则用户当前录入的密码字符有效，此时，电子设备基于该密码字符的先后输入次序记录所述密码字符，确保所述密码字符的有效录入，同时确保所述密码字符在整体密码中相对位置的正确性。

[0055] S104：如果不是有效输入模式，则丢弃所述密码字符。

[0056] 如果判断出电子设备的当前模式为无效输入模式，则用户当前录入的密码字符无效，从而清除缓存，丢弃所述密码字符。

[0057] 接下来，本实施例提供本申请方法的一具体应用实例。

[0058] 参考图3，用户在输入密码过程中，先后共输入了“8112673”七位数字，其中，仅在输入第二、四、七位数字时，其合法注册的手指按压在了电子设备背部的指纹识别器上，从而最终电子设备记录下来的密码字符分别为所述第二、四、七位数字：“1”、“2”、“3”，且在记录时保持了所述第二、四、七位数字的先后输入次序，而其余数字即第一、三、五、六位数字“8”、“1”、“6”、“7”则作为无效输入被电子设备丢弃，从而即使他人窥窃到用户输入过程中输入了各个数字“8112673”，也无法得知真正的密码“123”。

[0059] 由以上方案可知，本申请公开的密码输入方法，在获取到用户当前输入的密码字符时，通过判断所述电子设备的当前输入模式是否为有效输入模式，来确定是记录还是丢弃所述当前密码字符。可见，本申请针对电子设备的密码输入问题，引入了有效及非有效/无效两种类型的输入模式，在用户输入密码过程中，电子设备可基于对输入每个字符时采用的输入模式进行判断识别，实现对用户所输入的各密码字符进行不同处理（记录或丢弃），从而，本申请中，用户可通过对两种输入模式进行结合应用，来为输入过程产生一些非真实输入的字符，以此来迷惑可能的窥窃者，防止密码在输入过程中被窥窃盗取。从而本申请解决了输入密码过程中用户密码的安全问题。

[0060] 实施例二

[0061] 本实施例二继续对实施例一的方案进行补充，参考图4，所述方法还可以包括以下步骤：

[0062] S105：依据预设的输入结束条件，判断用户的密码输入过程是否结束；并在判断出结束时，基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符，得到用户的输入密码。

[0063] 其中，所述输入结束条件具体可以是用户触发相应的结束按钮，如点击输入按钮或确定按钮，也可以是用户输入密码字符后超过一定时长未有新的字符输入等等。

[0064] 当依据所述输入结束条件判断出用户的密码输入过程结束时，电子设备可基于所记录的各密码字符的先后输入次序，拼接用户输入的各个有效密码字符，从而得到用户输入的完整密码。

[0065] 实施例三

[0066] 本实施例中，参考图5，所述密码输入方法还可以包括以下步骤：

[0067] S106:基于预先存储的基准密码,验证所述输入密码的合法性,或向服务器提交所述输入密码。

[0068] 当基于各个有效输入字符的先后输入次序,拼接各有效字符得到用户输入的完整密码后,电子设备可依据当前的实际应用场景,对用户输入的密码进行相应处理。

[0069] 如果当前场景为由终端执行的安全认证场景,如解锁屏幕进入电子设备等场景,则电子设备可通过获取用户预先注册的基准密码,并通过将用户输入的密码与所述基准密码进行匹配,来验证用户输入密码的正确性,并依据验证结果作出相应响应;如果当前场景为由服务器执行的安全认证场景,例如购物时输入银行卡密码等,则电子设备需将用户输入的密码提交至相应服务器,由服务器完成所述输入密码的合法验证工作。

[0070] 实施例四

[0071] 本实施例四公开一种密码输入装置,所述装置与以上各实施例公开的密码输入方法相对应。

[0072] 相应于实施例一,参考图6,所述装置可以包括密码字符获取模块100、判断模块200、记录模块300和丢弃模块400。

[0073] 密码字符获取模块100,用于获取用户当前输入的密码字符。

[0074] 判断模块200,用于判断所述电子设备的当前输入模式是否为有效输入模式。

[0075] 所述判断模块200包括判断单元、第一输入模式确定单元和第二输入模式确定单元。

[0076] 判断单元,用于判断当前所述电子设备是否符合以下条件:侦测到用户手指按压在指纹识别器上,且当前用户指纹通过验证;其中,所述指纹识别器预先集成在所述电子设备中;

[0077] 第一输入模式确定单元,用于在判断结果为符合时,确定出所述电子设备的当前输入模式为有效输入模式

[0078] 第二输入模式确定单元,用于在判断结果为不符合时,确定出所述电子设备的当前输入模式为无效输入模式。

[0079] 记录模块300,用于在判断结果是有效输入模式时,基于所述密码字符的先后输入次序记录所述密码字符。

[0080] 丢弃模块400,用于在判断结果不是有效输入模式时,丢弃所述密码字符。

[0081] 相应于实施例二,参考图7,所述密码输入装置还可以包括输入密码获取模块500,用于依据预设的输入结束条件,判断用户的密码输入过程是否结束;并在判断出结束时,基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符,得到用户的输入密码。

[0082] 相应于实施例三,参考图8,所述密码输入装置还可以包括密码验证或提交模块600,用于基于预先存储的基准密码,验证所述输入密码的合法性,或向服务器提交所述输入密码。

[0083] 对于本发明实施例四公开的密码输入装置而言,由于其与实施例一至实施例三公开的密码输入方法相对应,所以描述的比较简单,相关相似之处请参见实施例一至实施例三中密码输入方法部分的说明即可,此处不再详述。

[0084] 实施例五

[0085] 本实施例五公开一种电子设备，所述电子设备具体可以是智能手机、平板电脑等设备，所述电子设备包括一指纹识别器，且所述电子设备包括如实施例四所提供的密码输入装置。

[0086] 基于所述密码输入装置，所述电子设备可为用户提供两种输入模式：有效输入模式和无效输入模式，在输入密码的过程中，用户可通过对所述两种输入模式进行结合应用，来为输入过程产生一些非真实输入的字符，以此来迷惑可能的窥窃者，防止密码在输入过程中被窥窃盗取。以下将通过多个实施例对本申请方法进行说明。

[0087] 需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

[0088] 为了描述的方便，描述以上系统或装置时以功能分为各种模块或单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0089] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，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)执行本申请各个实施例或者实施例的某些部分所述的方法。

[0090] 最后，还需要说明的是，在本文中，诸如第一、第二、第三和第四等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0091] 以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

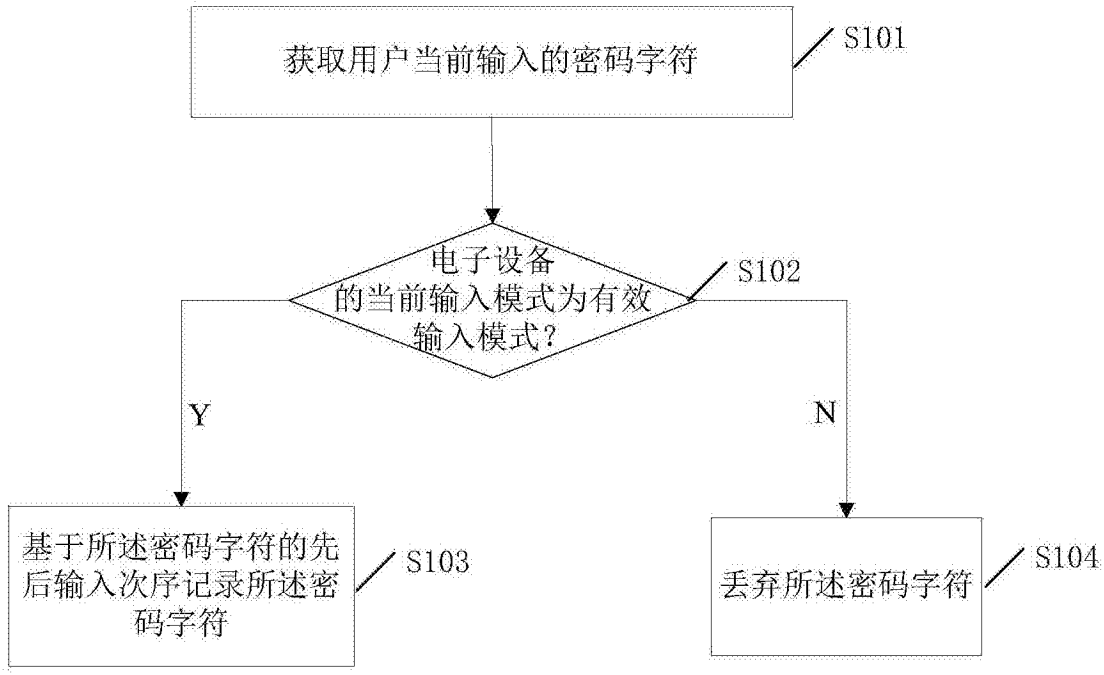

获取用户当前输入的密码字符
S101
电子设备
的当前输入模式为有效
输入模式？
S102
Y
N
基于所述密码字符的先后输入次序记录所述密码字符
S103
丢弃所述密码字符
S104

图1

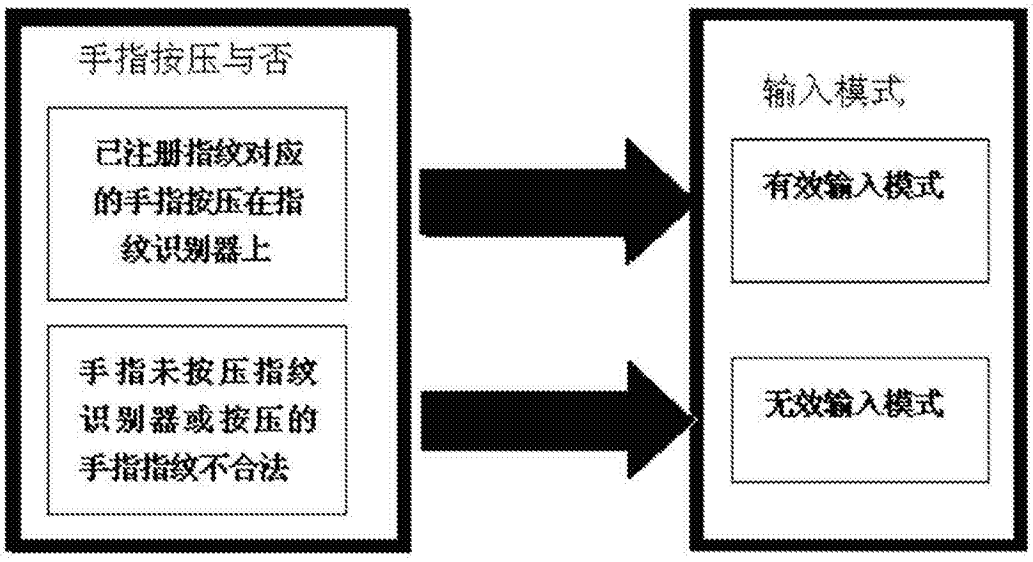

手指按压与否
已注册指纹对应的手指按压在指纹识别器上
手指未按压指纹识别器或按压的手指指纹不合法
输入模式
有效输入模式
无效输入模式

图2

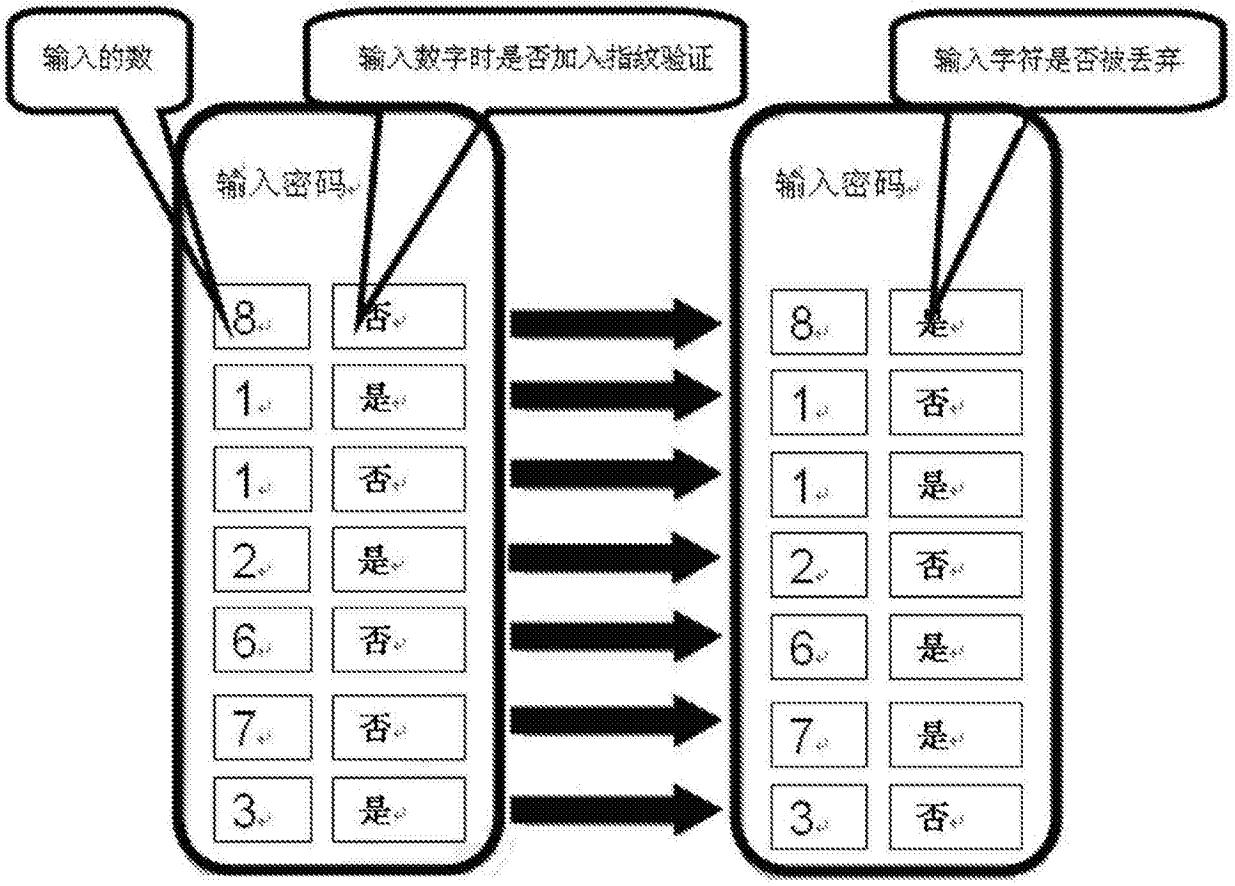

输入的数
输入数字时是否加入指纹验证
输入字符是否被丢弃
输入密码
8 否
1 是
1 否
2 是
6 否
7 否
3 是
输入密码
8 是
1 否
1 是
2 否
6 是
7 是
3 否

图3

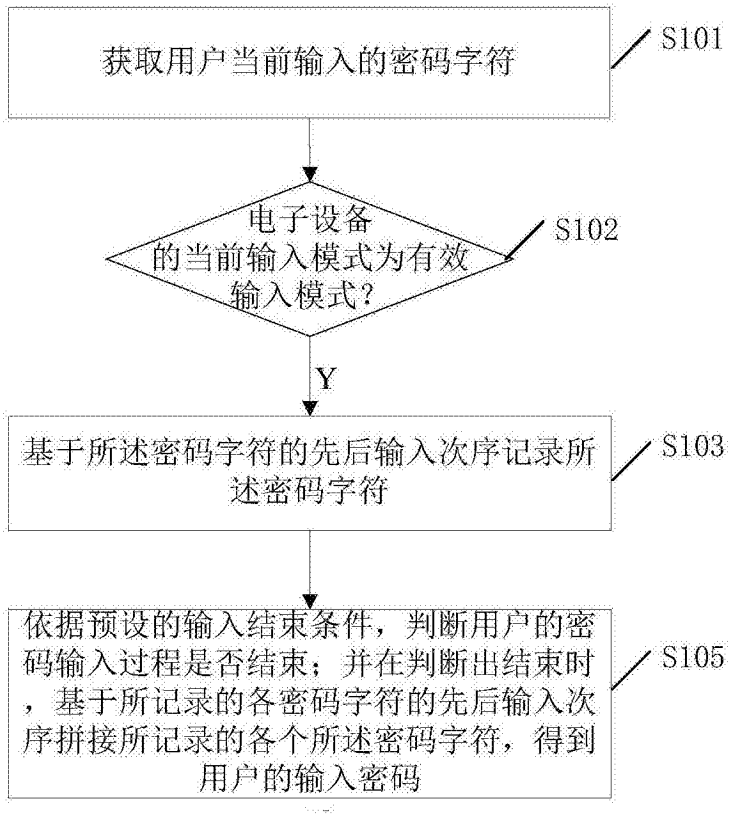

获取用户当前输入的密码字符
S101
电子设备的当前输入模式为有效输入模式？
S102
Y
基于所述密码字符的先后输入次序记录所述密码字符
S103
依据预设的输入结束条件，判断用户的密码输入过程是否结束；并在判断出结束时，基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符，得到用户的输入密码
S105

图4

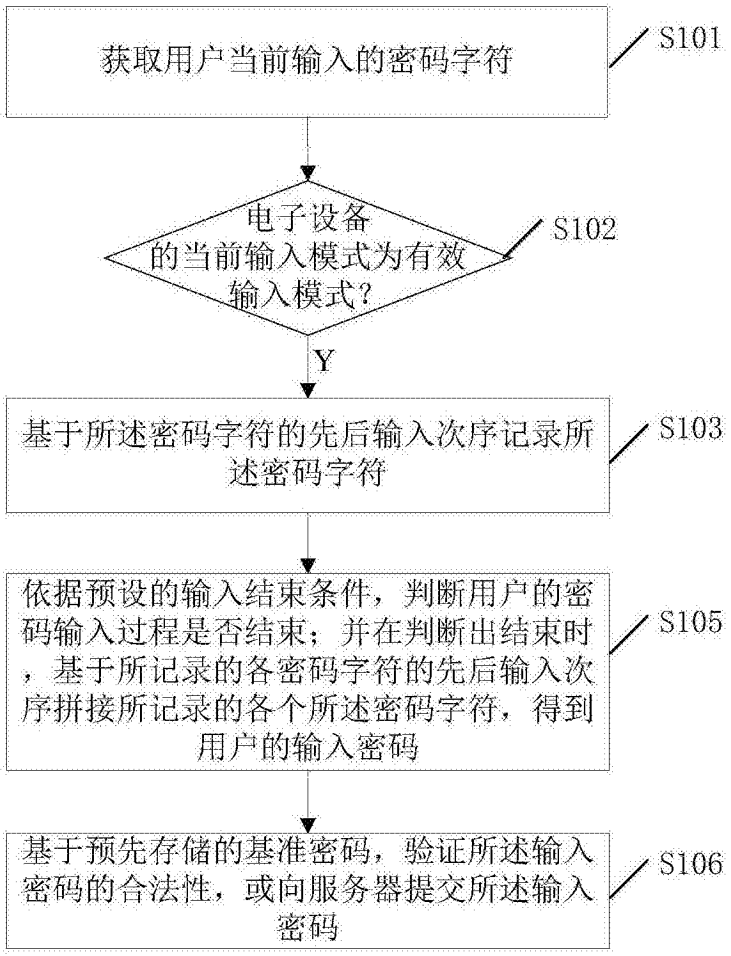

获取用户当前输入的密码字符
S101
电子设备的当前输入模式为有效输入模式？
S102
Y
基于所述密码字符的先后输入次序记录所述密码字符
S103
依据预设的输入结束条件，判断用户的密码输入过程是否结束；并在判断出结束时，基于所记录的各密码字符的先后输入次序拼接所记录的各个所述密码字符，得到用户的输入密码
S105
基于预先存储的基准密码，验证所述输入密码的合法性，或向服务器提交所述输入密码
S106

图5

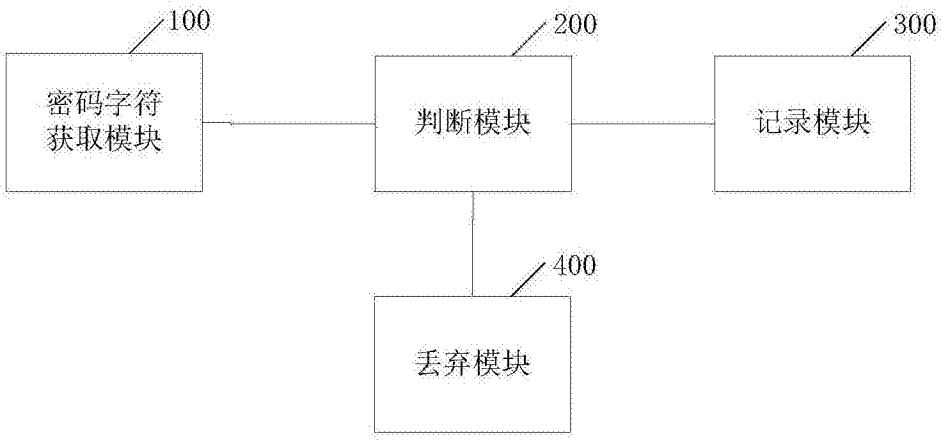

100
密码字符获取模块
200
判断模块
300
记录模块
400
丢弃模块

图6

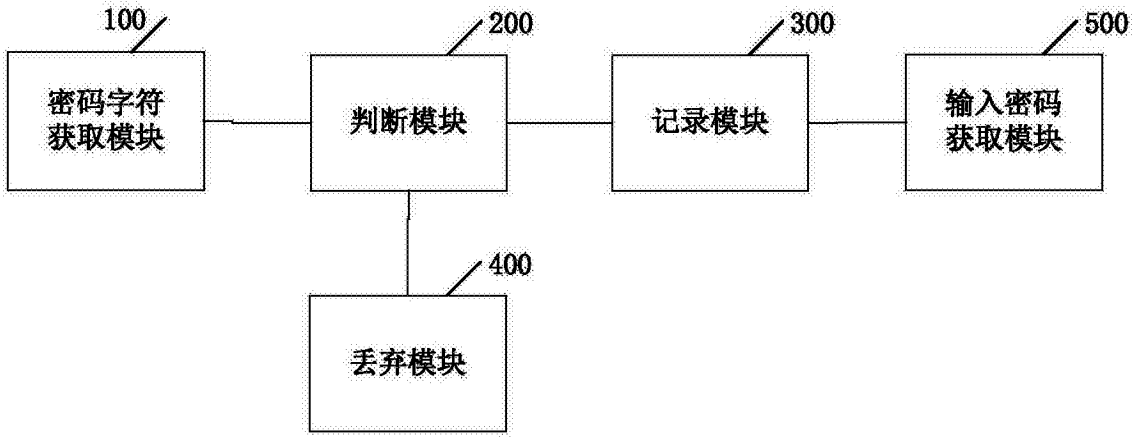

100
密码字符获取模块
200
判断模块
300
记录模块
500
输入密码获取模块
400
丢弃模块

图7

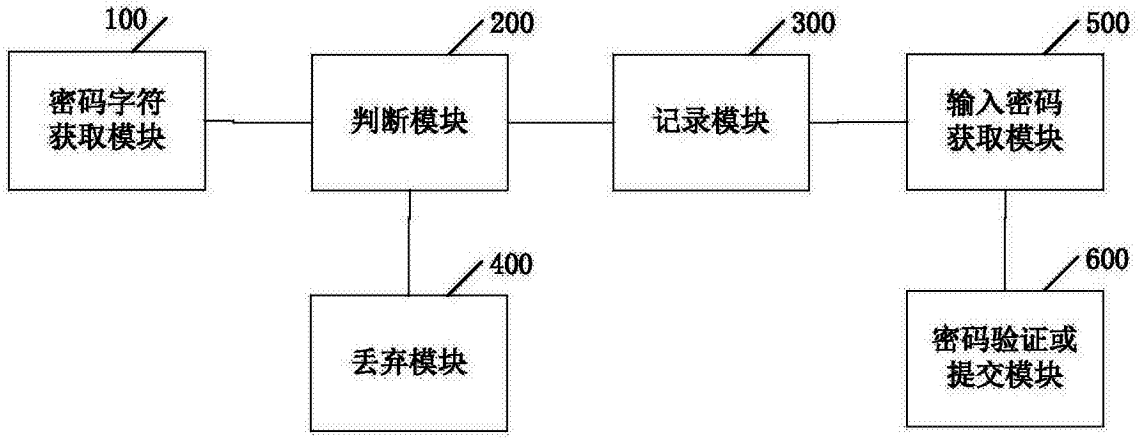

100
密码字符获取模块
200
判断模块
300
记录模块
500
输入密码获取模块
400
丢弃模块
600
密码验证或提交模块

图8