(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 103996011 A
(43)申请公布日 2014.08.20

(21)申请号 201410246522.X

(22)申请日 2014.06.05

(71)申请人 福建天晴数码有限公司
地址 350000 福建省福州市马尾区星发路8号

(72)发明人 薛雄 刘德建 陈宏展 李永均 叶金龙 张明辉 高举全 钟良德

(74)专利代理机构 福州市仓山区景弘专利代理事务所(普通合伙) 35219
代理人 林祥翔 吕元辉

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

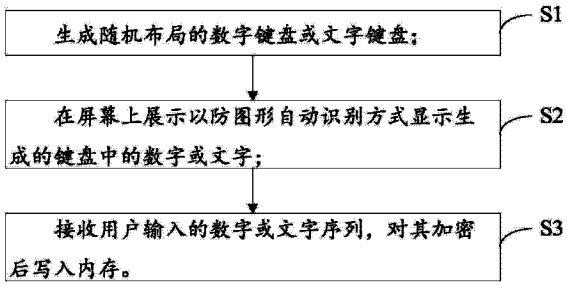
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种保护密码输入安全的方法和装置

(57)摘要

本发明披露了一种保护密码输入安全的方法。所述方法包括如下步骤:生成随机布局的数字键盘或文字键盘;在屏幕上展示以防图形自动识别方式显示生成的键盘中的数字或文字;接收用户输入的数字或文字序列,对其加密后写入内存。本发明还披露了一种保护密码输入安全的装置。本发明的技术方案能够避免从旁窥视的他人通过记忆用户输入时的手指位置与手指移动的方向从而达到盗取用户密码的目的,同时在不干扰人眼对数字或文字的鉴别的前提下成功完成对图像识别软件鉴别数字功能的阻断,防止木马或病毒程序通过识别图案中数字破解用户实际输入的密码。



CN 103996011 A

1. 一种保护密码输入安全的方法，其特征在于，包括步骤：

生成不规则布局的数字键盘或文字键盘；

在屏幕上展示以防图形自动识别方式显示生成的键盘中的数字或文字。

2. 如权利要求 1 所述的保护密码输入安全的方法，其特征在于，在步骤“在屏幕上以防图形自动识别方式显示生成的键盘中的数字或文字”后还包括步骤：

接收用户输入的数字或文字序列，对其加密后写入内存。

3. 如权利要求 2 所述的保护密码输入安全的方法，其特征在于，所述“接收用户输入的数字或文字序列”具体包括：

接收用户以手指输入的数字或文字序列同时接收与数字或文字序列对应的指纹，识别并判断接收的指纹信息是否符合预设的指纹信息。

4. 如权利要求 3 所述的保护密码输入安全的方法，其特征在于，所述预设的指纹信息包括单一指纹信息或组合指纹信息。

5. 如权利要求 1 或 2 所述的保护密码输入安全的方法，其特征在于，所述“以防图形自动识别方式显示生成的键盘中的数字或文字”具体包括：

在数字或文字上布设干扰信息；或

将数字显示为数字对应的小写或大写汉字；或

将数字键盘中各数字随机显示为阿拉伯数字、数字对应的小写汉字或数字对应的大写汉字；或

按预设方案对数字或文字进行变形。

6. 一种保护密码输入安全的装置，其特征在于，包括键盘生成单元、验证码生成单元和显示单元；

键盘生成单元用于生成不规则布局的数字键盘或文字键盘；

验证码生成单元用于将生成的不规则布局的数字键盘或文字键盘中的数字或文字以防图形自动识别方式显示；

显示单元用于在屏幕上展示以防图形自动识别方式显示的不规则布局的数字键盘或文字键盘。

7. 如权利要求 6 所述的保护密码输入安全的装置，其特征在于，还包括输入单元和加密单元；

输入单元用于接收用户输入的数字或文字序列；

加密单元用于对用户输入的数字或文字序列加密并将加密结果写入内存。

8. 如权利要求 7 所述的保护密码输入安全的装置，其特征在于，还包括判断单元；所述输入单元用于接收用户以手指输入的数字或文字序列同时接收与数字或文字序列对应的指纹；判断单元用于识别并判断输入单元接收的指纹信息是否符合预设的指纹信息。

9. 如权利要求 7 或 8 所述的保护密码输入安全的装置，其特征在于，所述预设的指纹信息包括单一指纹信息或组合指纹信息。

10. 如权利要求 6 或 7 所述的保护密码输入安全的装置，其特征在于，验证码生成单元以防图形自动识别方式显示生成的键盘中的数字或文字具体包括：

在数字或文字上布设干扰信息；或

将数字显示为数字对应的小写或大写汉字；或

将数字键盘中各数字随机显示为阿拉伯数字、数字对应的小写汉字或数字对应的大写汉字；或

按预设方案对数字或文字进行变形。

一种保护密码输入安全的方法和装置

技术领域

[0001] 本发明涉及电子技术领域，特别涉及一种保护密码输入安全的方法和装置。

背景技术

[0002] 随着电子通讯与互联网技术的飞速发展，人们面临着越来越多需要使用电子设备输入密码以实现特定目的的场合，例如网上支付、账户登录等，在因此而获取便捷服务的同时，也面临着密码安全的隐患，一旦密码被木马或病毒窃取，用户将很可能在经济等方面遭到重大损失。所以提供一种适用于手机、平板电脑、PDA、笔记本电脑以及台式电脑等电子设备的安全输入密码方案是很有必要的。

发明内容

[0003] 本发明的发明目的是提供一种能够有效保护密码输入安全的方法和装置。为达到上述发明目的，本发明所采取的技术方案如下：

[0004] 一种保护密码输入安全的方法，包括步骤：

[0005] 生成不规则布局的数字键盘或文字键盘；

[0006] 在屏幕上展示以防图形自动识别方式显示生成的键盘中的数字或文字。

[0007] 进一步地，所述的保护密码输入安全的方法中，在步骤“在屏幕上以防图形自动识别方式显示生成的键盘中的数字或文字”后还包括步骤：

[0008] 接收用户输入的数字或文字序列，对其加密后写入内存。

[0009] 进一步地，所述的保护密码输入安全的方法中，所述“接收用户输入的数字或文字序列”具体包括：

[0010] 接收用户以手指输入的数字或文字序列同时接收与数字或文字序列对应的指纹，识别并判断接收的指纹信息是否符合预设的指纹信息。

[0011] 进一步地，所述的保护密码输入安全的方法中，所述预设的指纹信息包括单一指纹信息或组合指纹信息。

[0012] 进一步地，所述的保护密码输入安全的方法中，所述“以防图形自动识别方式显示生成的键盘中的数字或文字”具体包括：

[0013] 在数字或文字上布设干扰信息；或

[0014] 将数字显示为数字对应的小写或大写汉字；或

[0015] 将数字键盘中各数字随机显示为阿拉伯数字、数字对应的小写汉字或数字对应的大写汉字；或

[0016] 按预设方案对数字或文字进行变形。

[0017] 一种保护密码输入安全的装置，包括键盘生成单元、验证码生成单元和显示单元；

[0018] 键盘生成单元用于生成不规则布局的数字键盘或文字键盘；

[0019] 验证码生成单元用于将生成的不规则布局的数字键盘或文字键盘中的数字或文

字以防图形自动识别方式显示；

[0020] 显示单元用于在屏幕上展示以防图形自动识别方式显示的不规则布局的数字键盘或文字键盘。

[0021] 进一步地，所述的保护密码输入安全的装置还包括输入单元和加密单元；

[0022] 输入单元用于接收用户输入的数字或文字序列；

[0023] 加密单元用于对用户输入的数字或文字序列加密并将加密结果写入内存。

[0024] 进一步地，所述的保护密码输入安全的装置还包括判断单元；所述输入单元用于接收用户以手指输入的数字或文字序列同时接收与数字或文字序列对应的指纹；判断单元用于识别并判断输入单元接收的指纹信息是否符合预设的指纹信息。

[0025] 进一步地，所述的保护密码输入安全的装置中，所述预设的指纹信息包括单一指纹信息或组合指纹信息。

[0026] 进一步地，所述的保护密码输入安全的装置验证码生成单元以防图形自动识别方式显示生成的键盘中的数字或文字具体包括：

[0027] 在数字或文字上布设干扰信息；或

[0028] 将数字显示为数字对应的小写或大写汉字；或

[0029] 将数字键盘中各数字随机显示为阿拉伯数字、数字对应的小写汉字或数字对应的大写汉字；或

[0030] 按预设方案对数字或文字进行变形。

[0031] 采取上述技术方案后本发明的有益效果为：能够避免从旁窥视的他人通过记忆用户输入时的手指位置与手指移动的方向从而达到盗取用户密码的目的，同时在不干扰人眼对数字或文字的鉴别的前提下成功完成对图像识别软件鉴别数字功能的阻断，防止木马或病毒程序通过识别图案中数字破解用户实际输入的密码；并且进一步能够保证输入的密码不被逆向工程查看内存的方式窃取。

附图说明

[0032] 图 1 为本发明一实施方式中一种保护密码输入安全的方法的流程图；

[0033] 图 2 为本发明另一实施方式中一种保护密码输入安全的装置的功能模块示意图。

[0034] 附图标记说明：

[0035] 1- 键盘生成单元

[0036] 2- 验证码生成单元

[0037] 3- 显示单元

[0038] 4- 输入单元

[0039] 5- 加密单元

[0040] 6- 判断单元

具体实施方式

[0041] 为详细说明本发明的技术内容、构造特征、所实现目的及效果，以下结合实施方式并配合附图详予说明。

[0042] 请参阅图 1，为本发明一实施方式中一种保护密码输入安全的方法的流程图。所述

方法包括如下步骤：

[0043] S1、生成随机布局的数字键盘或文字键盘；

[0044] S2、在屏幕上展示以防图形自动识别方式显示生成的键盘中的数字或文字；

[0045] S3、接收用户输入的数字或文字序列，对其加密后写入内存。

[0046] 进一步地，步骤 S2 中“以防图形自动识别方式显示生成的键盘中的数字或文字”具体包括：在数字或文字上布设干扰信息；或将数字显示为数字对应的简体汉字或大写汉字；或将数字键盘中各数字随机显示为阿拉伯数字、数字对应的简体汉字或数字对应的大写汉字。

[0047] 进一步地，步骤 S3 还包括：接收用户以手指输入的数字或文字序列同时接收与数字或文字序列对应的指纹，识别并判断接收的指纹信息是否符合预设的指纹信息。所述预设的指纹信息包括单一指纹信息或组合指纹信息。

[0048] 以下以一个具体案例说明本方法实现保护密码输入安全的过程：

[0049] 首先，生成随机布局的数字键盘或文字键盘。大部分情况下，储蓄卡密码、信用卡密码、网络银行账户密码等密码均是由纯数字组成的，其他部分密码可能是由字母或数字和字母的组合构成。本实施方式中以纯数字密码为例进行说明。现有技术中，一般在触摸式显示屏或无触摸输入功能的显示屏上显示出规则排列的虚拟键盘以引导用户输入密码，该虚拟键盘上数字的排列是规则的，如“0123456789”或“1234567890”排列在一行上，或以 3*3 的矩阵形式排列，如第一、二、三行分别为“123”、“456”“789”或“789”“456”“123”，此时数字 0 一般与星号或井号一起被布设在 3*3 矩阵的一侧。本实施方式中，虚拟键盘上数字的排列是不规则的，是随机打乱布局的，例如原来的“0123456789”被打乱为“2473689105”。在另外一些实施方式中，还可以是按照一定的预设加密算法生成不规则排列的数字键盘或文字键盘；或者对数字键盘或文字键盘采用随机打乱的不规则布局，例如将各数字以随机散乱布局的方式显示而非以规则矩阵形式显示；同样能够达到防止他人通过窥视得知密码构成的技术效果。

[0050] 然后，在屏幕上以防图形自动识别方式显示“2473689105”这 10 个数字序列，例如在这 10 个阿拉伯数字上布设干扰线条或其他干扰信息，或随机选择部分阿拉伯数字显示为对应该数字的简体汉字，其中对应 0123456789 的简体汉字分别为零一二三四五六七八九，如将“2473689105”显示为“24 七 368 九 105”，或随机选择部分阿拉伯数字显示为对应该数字的大写汉字，其中对应 0123456789 的大写汉字分别为零壹贰叁肆伍陆柒捌玖，如将“2473689105”显示为“贰肆 73 陆 89 壹 05”，或随机选择部分阿拉伯数字显示为对应该数字的简体汉字或大写汉字，如将“2473689105”显示为“二 4 柒 36 八 91 零五”，或将 10 个阿拉伯数字全部使用简体汉字或大写汉字或简体汉字与大写汉字的随机组合表示，如将“2473689105”显示为“二四七三六八九一零五”或“贰肆柒叁陆捌玖壹零伍”或“贰肆七三陆八九壹零伍”。

[0051] 在其他一些实施方式中，防图形自动识别方式还可以是按预设方案对数字或文字进行变形，以达到人工阅读时能够识别和判断经变形的数字或文字所代表的原始数字或文字，而图形自动识别软件无法识别该原始数字或文字的目的；所述预设方案可以是按照一定的角度、方向，以一定的幅度，对数字或文字的部分或整体进行变形。

[0052] 上述方案能够避免从旁窥视的他人通过记忆用户输入时的手指位置与手指移动

的方向从而达到盗取用户密码的目的，同时在不干扰人眼对数字或文字的鉴别的前提下成功完成对图像识别软件鉴别数字功能的阻断，防止木马或病毒程序通过识别图案中数字破解用户实际输入的密码。

[0053] 在通过机械键盘或触摸显示屏接收用户输入的密码序列之后，判断接收到的指纹是否符合预设的指纹信息。用户可以在此之前预设自己输入密码所用的指纹或指纹序列。当用户设定指纹信息为单一指纹信息时，输入所有密码所用的是同一手指；当用户设定指纹信息为组合指纹信息时，输入密码各数字或字母所用的是不同手指，对所用手指及其组合序列的选择由用户自行设定。例如：用户设定密码为5704，同时可以预设输入5，0所用的是右手食指，输入数字7，4时所用的是右手拇指，则预设指纹信息为对应于数字5，7，0，4的指纹为右手食指指纹、右手拇指指纹、右手食指指纹、右手拇指指纹，在接收用户输入密码序列后，判断所接收到的指纹序列是否与此相吻合，如不吻合则判定为密码输入有误，提示用户重新输入密码。本方案可以进一步提升密码输入的安全性，即使有人得知密码，在非用户本人操作的情况下也无法成功完成密码验证过程。

[0054] 在通过机械键盘或触摸显示屏接收用户输入的密码序列之后，按一预设算法将所输入的密码值进行加密，并将加密后的结果存储于内存空间。例如用户输入的密码为5704，加密后存入内存的对应值为RPWS。在需要读取正确密码时按照预设算法的逆向运算进行解密，提供正确的密码数值，如与第三方服务器建立加密解密协议接口以解密和读取正确密码值，以此达到保证输入的密码不被逆向工程查看内存的方式窃取的目的。

[0055] 本发明另一实施方式披露了一种保护密码输入安全的装置，包括键盘生成单元1、验证码生成单元2以及显示单元3；键盘生成单元1用于生成不规则布局的数字键盘或文字键盘；验证码生成单元2用于将生成的不规则布局的数字键盘或文字键盘中的数字或文字以防图形自动识别方式显示；显示单元3用于在屏幕上展示以防图形自动识别方式显示的随机布局的数字键盘或文字键盘。

[0056] 进一步地，验证码生成单元2以防图形自动识别方式显示生成的键盘中的数字或文字具体包括：在数字或文字上布设干扰信息；或将数字显示为数字对应的简体汉字或大写汉字；或将数字键盘中各数字随机显示为阿拉伯数字、数字对应的简体汉字或数字对应的大写汉字；或按预设方案对数字或文字进行变形。

[0057] 进一步地，所述装置还包括输入单元4和加密单元5；所述输入单元4用于接收用户输入的数字或文字序列；所述加密单元6用于对用户输入的数字或文字序列加密并将加密结果写入内存。进一步地，输入单元还用于接收用户以手指输入的数字或文字序列同时接收与数字或文字序列对应的指纹；并且所述装置还包括判断单元6，用于识别并判断通过输入单元4接收的指纹信息是否符合预设的指纹信息，所述预设指纹信息包括单一指纹信息或组合指纹信息。

[0058] 以下以一个具体案例说明本装置实现保护密码输入安全的过程：

[0059] 首先，键盘生成单元1生成随机布局的数字键盘或文字键盘。大部分情况下，储蓄卡密码、信用卡密码、网络银行账户密码等密码均是由纯数字组成的，其他部分密码可能是由字母或数字和字母的组合构成。本实施方式中以纯数字密码为例进行说明。现有技术中，一般在触摸式显示屏或无触摸输入功能的显示屏上显示出规则排列的虚拟键盘以引导用户输入密码，该虚拟键盘上数字的排列是规则的，如“0123456789”或“1234567890”

排列在一行上，或以 3*3 的矩阵形式排列，如第一、二、三行分别为“123”、“456”“789”或“789”“456”“123”，此时数字 0 一般与星号或井号一起被布设在 3*3 矩阵的一侧。本实施方式中，键盘生成单元 1 生成的虚拟键盘上数字的排列是不规则的，可以是随机打乱布局的，例如原来的“0123456789”被打乱为“2473689105”。在另外一些实施方式中，还可以是按照一定的预设加密算法生成不规则排列的数字键盘或文字键盘；或者对数字键盘或文字键盘采用随机打乱的不规则布局，例如将各数字以随机散乱布局的方式显示而非以规则矩阵形式显示；同样能够达到防止他人通过窥视得知密码构成的技术效果。

[0060] 然后，验证码生成单元 2 以防图形自动识别方式生成“2473689105”这 10 个数字序列并由显示单元 3 在屏幕上展示该键盘。例如在这 10 个阿拉伯数字上布设干扰线条或其他干扰信息，或随机选择部分阿拉伯数字显示为对应该数字的简体汉字，其中对应 0123456789 的简体汉字分别为零一二三四五六七八九，如将“2473689105”显示为“24 七 368 九 105”，或随机选择部分阿拉伯数字显示为对应该数字的大写汉字，其中对应 0123456789 的大写汉字分别为零壹贰叁肆伍陆柒捌玖，如将“2473689105”显示为“贰肆 73 陆 89 壹 05”，或随机选择部分阿拉伯数字显示为对应该数字的简体汉字或大写汉字，如将“2473689105”显示为“二 4 柒 36 八 91 零五”，或将 10 个阿拉伯数字全部使用简体汉字或大写汉字或简体汉字与大写汉字的随机组合表示，如将“2473689105”显示为“二四七三六八九一零五”或“贰肆柒叁陆捌玖壹零伍”或“贰肆七三陆八九壹零伍”。

[0061] 在其他一些实施方式中，防图形自动识别方式还可以是按预设方案对数字或文字进行变形，以达到人工阅读时能够识别和判断经变形的数字或文字所代表的原始数字或文字，而图形自动识别软件无法识别该原始数字或文字的目的；所述预设方案可以是按照一定的角度、方向，以一定的幅度，对数字或文字的部分或整体进行变形。

[0062] 上述方案能够避免从旁窥视的他人通过记忆用户输入时的手指位置与手指移动的方向从而达到盗取用户密码的目的，同时在不干扰人眼对数字或文字的鉴别的前提下成功完成对图像识别软件鉴别数字功能的阻断，防止木马或病毒程序通过识别图案中数字破解用户实际输入的密码。

[0063] 输入单元 4 可以是机械键盘或有接收信息功能的触摸显示屏；输入单元 4 接收用户输入的密码序列之后，判断单元 6 识别并判断接收到的指纹是否符合预设的指纹信息。用户可以在此之前预设自己输入密码所用的指纹或指纹序列。当用户设定指纹信息为单一指纹信息时，输入所有密码所用的是同一手指；当用户设定指纹信息为组合指纹信息时，输入密码各数字或字母所用的是不同手指，对所用手指及其组合序列的选择由用户自行设定。例如：用户设定密码为 5704，同时可以预设输入 5，0 所用的是右手食指，输入数字 7，4 时所用的是右手拇指，则预设指纹信息为对应于数字 5，7，0，4 的指纹为右手食指指纹、右手拇指指纹、右手食指指纹、右手拇指指纹，在接收用户输入密码序列后，判断单元 6 判断所接收到的指纹序列是否与此相吻合，如不吻合则判定为密码输入有误，提示用户重新输入密码。本方案可以进一步提升密码输入的安全性，即使有人得知密码，在非用户本人操作的情况下也无法成功完成密码验证过程。

[0064] 在通过输入单元 4 接收用户输入的密码序列之后，加密单元 5 按一预设算法将所输入的密码值进行加密，并将加密后的结果存储于内存空间。例如用户输入的密码为 5704，加密后存入内存的对应值为 RPWS。在需要读取正确密码时按照预设算法的逆向运算进行解

密，提供正确的密码数值，如与第三方服务器建立加密解密协议接口以解密和读取正确密码值，以此达到保证输入的密码不被逆向工程查看内存的方式窃取的目的。

[0065] 以上所述仅为本发明的实施例，并非因此限制本发明的专利保护范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

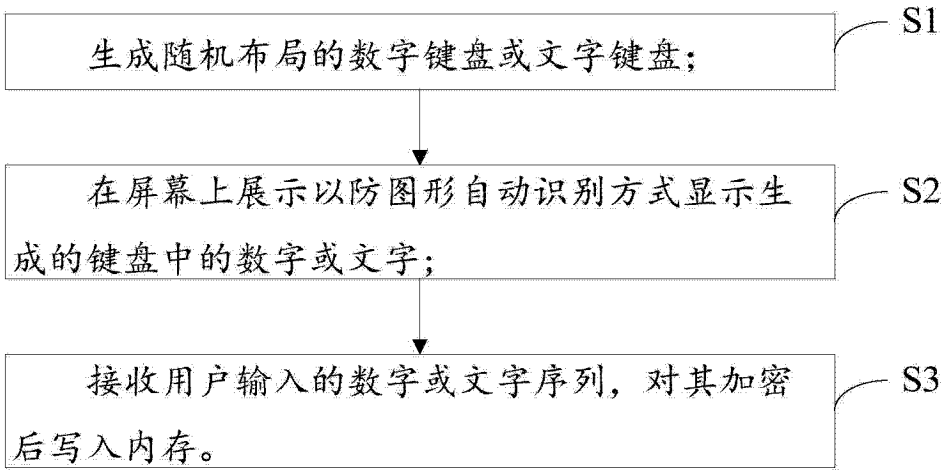

生成随机布局的数字键盘或文字键盘；
S1
在屏幕上展示以防图形自动识别方式显示生成的键盘中的数字或文字；
S2
接收用户输入的数字或文字序列，对其加密后写入内存。
S3

图 1

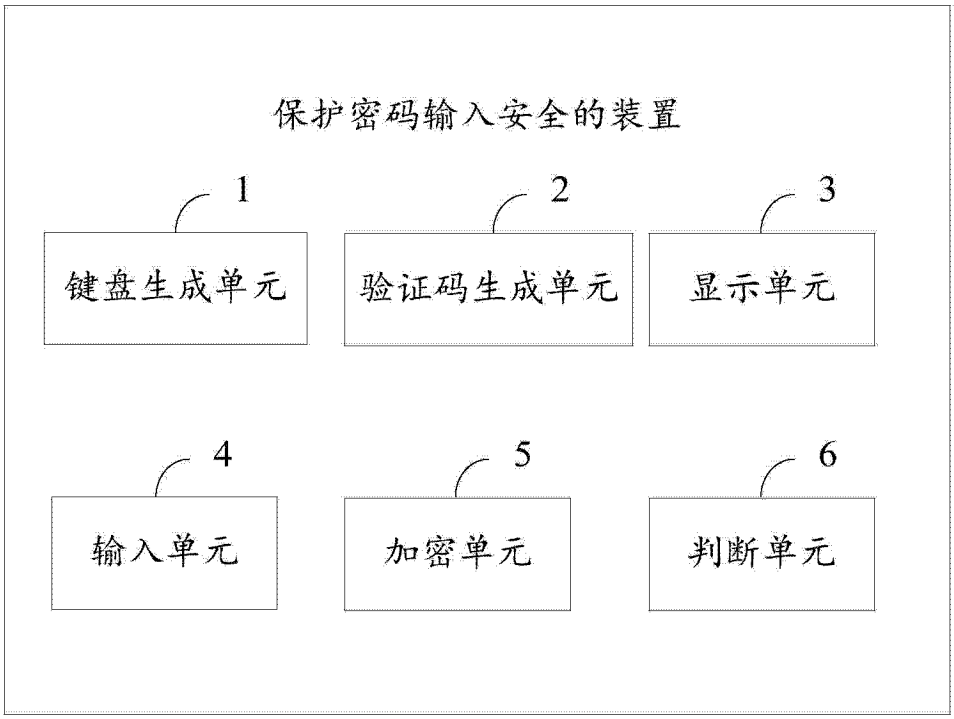

保护密码输入安全的装置
1
键盘生成单元
2
验证码生成单元
3
显示单元
4
输入单元
5
加密单元
6
判断单元

图 2