(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1952855 B
(45)授权公告日 2011.07.27

(21)申请号 200510114303.7
(22)申请日 2005.10.20
(73)专利权人 联想(北京)有限公司
地址 100085 北京市海淀区上地信息产业基地创业路6号
(72)发明人 李众庆
(74)专利代理机构 北京银龙知识产权代理有限公司 11243
代理人 郝庆芬
(51)Int.Cl.
G06F 3/02(2006.01)
(56)对比文件
CN 1558377 A,2004.12.29, 全文.
CN 1333495 A,2002.01.30, 全文.
US 2005139658 A1,2005.06.30, 全文.
JP 2004213117 A,2004.07.29, 全文.
审查员 周述虹

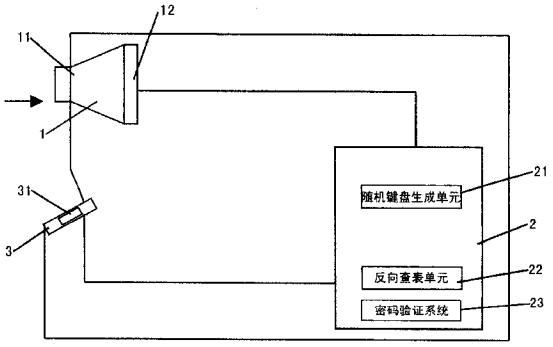
权利要求书 2 页 说明书 7 页 附图 2 页

(54)发明名称

一种防止被偷窥的密码输入方法和系统

(57)摘要

一种防止被偷窥的密码输入方法和系统，在用户需要输入密码时，触发输入密码启动单元(31)，通知系统启动生成随机密码对照表；系统接到通知后，调用随机键盘生成单元(21)，生成随机密码对照表；用户根据本次生成的随机密码对照表，输入转化后的密码；主机(2)收到用户输入的密码后，根据随机密码对照表，调用反向查表单元(22)进行反向查表，还原出原始密码，输出给密码验证系统(23)验证密码是否正确。其把用户欲输入的密码和实际输入的密码在物理空间上分开处理，保证其不被同时偷窥，使用户在输入时密码被窃取的几率降到最低。



CN 1952855 B

1. 一种密码输入方法，其特征在于，包括下列步骤：

步骤一：在用户需要输入密码时，触发输入密码启动单元 (31)，通知系统启动生成随机密码对照表；

步骤二：系统接到通知后，调用随机键盘生成单元 (21)，生成随机密码对照表；

步骤三：用户根据本次生成的随机密码对照表，输入转化后的密码；

步骤四：主机 (2) 收到用户输入的密码后，根据随机密码对照表，调用反向查表单元 (22) 反向查表，还原出原始密码，输出给密码验证系统 (23) 验证密码是否正确。

2. 根据权利要求 1 所述的密码输入方法，其特征在于，还包括下列步骤：

步骤五：然后把该次的随机密码对照表删除。

3. 根据权利要求 1 或 2 所述的密码输入方法，其特征在于，所述的步骤二还包括下列步骤：

步骤 A：当随机密码对照表生成后，通过文字图像输出系统输出给用户。

4. 一种密码输入系统，包括输入系统 (3)、显示系统 (1) 和控制输入系统 (3) 和显示系统 (1) 的主机 (2)，主机 (2) 包括密码验证系统 (23)，其特征在于，所述输入系统 (3) 包括一个输入密码启动单元 (31)；

所述主机还包括：

随机键盘生成单元 (21)，用于当用户需要输入密码而触发输入密码启动单元 (31) 时，随机键盘生成单元 (21) 生成随机密码对照表；

反向查表单元 (22)，用于根据随机密码对照表，当接到输入的密码数据时，反向查表，还原出原始密码，并输出给密码验证系统 (23) 验证密码的真伪。

5. 根据权利要求 4 所述的密码输入系统，其特征在于，所述主机 (2) 为 ATM 提款机、或者计算机、或者 POS 机、或者门禁系统、或者电话机。

6. 根据权利要求 4 所述的密码输入系统，其特征在于，所述显示系统 (1) 包括一个形状如照相机取景框的窗口 (11)，以及一个显示屏幕 (12)，用户把眼睛靠近窗口 (11)，才能看到显示屏幕 (12) 上的图像。

7. 根据权利要求 6 所述的密码输入系统，其特征在于，所述窗口 (11) 只够使用者的眼睛观察，离开窗口 (11) 一定距离或角度，其他位置和角度都无法观察到显示系统的显示屏幕 (12) 上的内容。

8. 根据权利要求 6 或 7 所述的密码输入系统，其特征在于，所述输入系统 (3) 为键盘，所述显示系统 (1) 的屏幕分为左右两部分，左边一半显示随机按键键盘；右边一半显示实际的键盘图像，显示键盘的排列，其和外接的实际键盘排列方式一致。

9. 根据权利要求 6 或 7 所述的密码输入系统，其特征在于，所述输入系统为语音识别输入系统，在显示系统 (1) 上显示当次生成的随机密码对照表，然后根据所述对照表依次用语音方式读出转换后的密码，系统通过所述语音识别输入系统接受该密码。

10. 根据权利要求 4 所述的密码输入系统，其特征在于，所述的显示系统 (1) 还包括具有与主机进行数据通讯的文字图像输出系统，当随机密码对照表生成后，通过文字图像输出系统输出给用户。

11. 根据权利要求 10 所述的密码输入系统，其特征在于，所述文字图像输出系统为带小屏幕的手机、或者 PDA、或者打印机、或者电子词典。

12. 根据权利要求 10 或 11 所述的密码输入系统，其特征在于，所述文字图像输出系统与主机进行数据通讯的通讯口为并口、串口、红外口、蓝牙、无线 WIFI、GSM、PHS、CDMA、3G、USB、1394、数字调频、或者国际互联网。

13. 根据权利要求 4 所述的密码输入系统，其特征在于，所述密码输入系统中的所有设备的连线都在系统的整体框架中，不对外暴露，使得他人不能从连线中截取到信息数据。

一种防止被偷窥的密码输入方法和系统

技术领域

[0001] 本发明涉及密码输入领域，特别是涉及一种防止被偷窥的密码输入方法和系统。

背景技术

[0002] 目前生活中输入密码的机会非常多，ATM 机、计算机键盘、电话机、POS 机、门禁等输入各种和密码有关的号码字符，银行帐号密码，证券帐号密码，电子邮件密码，手机密码，信用卡密码，进入系统的密码，进入门禁的密码等等，但是这些键盘和键盘上的字符以及连带的屏幕都是暴露在外面的，很容易被别人偷窥，导致帐号密码失窃的案件很多，犯罪分子利用各种手段进行偷窥，进而窃取帐号密码，比如站在旁边偷看，利用望远镜远距离窥视，利用微型针孔摄像头进行窥视、录像，即使用户用手挡住键盘，也很容易被专业小偷根据手型的变化来猜出密码。现有技术一般只能采用遮挡，或者隔离的办法，但是效果不佳，因此为了安全起见，需要经常更换密码，这又容易导致密码遗失，很不方便。

[0003] 另外还有不法人员在用户通过 PC 键盘刚输入密码后，在键盘上喷洒一种无色药剂，可以显示出手指在键盘上的残留痕迹，根据留有残留痕迹的按键，进行组合，就能够试探出密码，采用这样的方法是很难防范的。中国专利申请 03264135.4 涉及一种防窃密码键盘，其在键盘上装有按键，键盘安装在支座上，二者之间形成可以相对转动的活动连接，支座的周缘向上延伸形成环形挡板，挡板壁上开有通孔，转动键盘，使按键的位置时刻发生变化，加之有环形挡板的阻档，旁人就不容易偷看或者根据手指的位置猜出所输入的密码，来阻止密码外泄。中国专利申请 00213520.5，200320114061.8 也是采用了对键盘和屏幕进行物理遮档或者滚盘随机放置的方式来防止被偷窥。但上述这些方案只能防止近旁的偷窥，但是不能防止他人采用摄像头偷窥。

[0004] 中国专利申请 200420045735.8 提供了一种防偷窥的新结构键盘，包括显示器键盘、存储器、随机多路选择开关、锁存器、编码器和译码器，所述随机多路选择开关控制至少两组或两组以上编码器，所述编码器通过锁存器及译码器与设定的显示器按键连接。所述每个显示器按键都为一个独立的发光二极管数字显示器，显示器按键表面设置可视角度限制块。然而，此方案需要对键盘按键进行改造，按键上需要增加显示单元，成本很高，而且仍然无法防止摄像头偷窥。

发明内容

[0005] 本发明的目的在于克服上述缺陷，提供了一种防止被偷窥的密码输入方法和系统，其把用户欲输入的密码和实际输入的密码两部分在物理空间上分开处理，保证其不被同时偷窥，使用户在输入密码时密码被窃取的几率降到最低。

[0006] 本发明为实现上述目的而提供的一种密码输入方法，包括下列步骤：

[0007] 步骤一：在用户需要输入密码时，触发输入密码启动单元，通知系统启动生成随机密码对照表；

[0008] 步骤二：系统接到通知后，调用随机键盘生成单元，生成随机密码对照表；

[0009] 步骤二还可以包括下列步骤：

[0010] 步骤 A：当随机密码对照表生成后，通过文字图像输出系统输出给用户。

[0011] 步骤三：用户根据本次生成的随机密码对照表，输入转化后的密码；

[0012] 步骤四：主机收到用户输入的密码后，根据随机密码对照表，调用反向查表单元进行反向查表，还原出原始密码，输出给密码验证系统验证密码是否正确。

[0013] 步骤五：然后把该次的随机密码对照表删除。

[0014] 本发明还提供一种密码输入系统，包括输入系统、显示系统和控制输入系统和显示系统的主机。

[0015] 输入系统包括一个输入密码启动单元；

[0016] 输入系统可以是键盘，所述显示系统的屏幕分为左右两部分，左边一半显示随机按键键盘；右边一半显示实际的键盘图像，显示键盘的排列，其和外接的实际键盘排列方式一致；

[0017] 输入系统也可以是语音识别输入系统，在显示系统上显示当次生成的随机密码对照表，然后根据所述对照表依次用语音方式读出转换后的密码，系统通过所述语音识别输入系统接受该密码。

[0018] 显示系统可以包括一个形状如照相机取景框的窗口，以及一个显示屏幕，用户把眼睛靠近取景框，才能看到里面的图像。

[0019] 所述窗口只够使用者的眼睛观察，离开窗口一定距离或角度，其他位置和角度都无法观察到显示系统的显示屏幕上的内容；

[0020] 显示系统还包括具有与主机进行数据通讯的文字图像输出系统，当随机密码对照表生成后，通过文字图像输出系统输出给用户。

[0021] 文字图像输出系统为带小屏幕的手机、或者 PDA、或者打印机、或者电子词典。

[0022] 文字图像输出系统与主机进行数据通讯的通讯口为并口、串口、红外口、蓝牙、无线 WIFI、GSM、PHS、CDMA、3G、USB、1394、数字调频、或者国际互联网。

[0023] 主机包括密码验证系统；以及

[0024] 随机键盘生成单元，用于当用户需要输入密码而触发输入密码启动单元时，随机键盘生成单元生成随机密码对照表；

[0025] 反向查表单元，用于根据随机密码对照表，当接到用户输入的密码数据时，反向查表，还原出原始密码，并输出给验证密码系统验证密码的真伪。

[0026] 主机可以是 ATM 提款机、或者计算机、或者 POS 机、或者门禁系统、或者电话机。

[0027] 密码输入系统中的所有设备的连线都在系统的整体框架中，不对外暴露，使得他人不能从连线中截取到信息数据。

[0028] 本发明的有益效果是：本发明用户欲输入的密码和和实际输入的密码在空间上隔离处理，达到隐秘的效果，只要保证随机对照表的安全，无论对手指的动作，键盘的操作，以及在键盘上的遗留信息的偷窥都不能完成窃取密码。既可以预防他人通过摄像头或者其他方法偷窥，又不需要对输入系统大的改造，因此其成本低，符合用户使用的习惯。

[0029] 附图说明

[0030] 图 1 是本发明防止被偷窥的密码输入系统结构示意图；

[0031] 图 2 是本发明在显示系统上的键盘随机排列显示示意图；

[0032] 图 3 是本发明实际的物理键盘排列示意图；

[0033] 图 4 是本发明密码按键转化还原流程图。

具体实施方式

[0034] 下面结合附图 1-4 进一步详细说明一种防止被偷窥的密码输入方法和系统。

[0035] 实施例一：

[0036] 如图 3 所示，本发明的防止被偷窥密码输入系统是 ATM 提款机的密码输入系统。

[0037] 本实施例的 ATM 提款机密码输入系统包括显示系统 1 和键盘 3 以及控制这些设备的主机 2。

[0038] 显示系统 1 包括一个形状如照相机取景框的窗口 11，用户把眼睛靠近取景框的位置时，才能看到里面的图像，较佳地，窗口 11 只供使用者的眼睛观察，眼球离开取景框一定距离后或偏离一定角度后，其他位置和角度都无法观察到屏幕上的内容。在显示系统 1 的屏幕上，左边一半显示随机按键键盘，如图 2 所示；右边一半显示实际的键盘图像，如图 3 所示，显示键盘的排列，其和外接的实际键盘排列方式一致，该键盘图像可以由摄像头实际拍摄，或者用其它方式存入主机中，通过主机控制而在显示系统 1 上显示。

[0039] 键盘 3 采用通常的 XY 阵列扫描键盘，键盘上的字符如图 3 所示，具有键盘控制器，可以将原始密码传送到主机 2 去处理，还包括一个输入密码启动按钮 31，密码启动单元也可以采用银行卡读写器来触发。

[0040] 主机 2 还包括随机键盘生成单元 21、反向查表单元 22、验证密码系统 23。

[0041] 随机键盘生成单元 21，用于当用户需要输入密码而按下输入密码启动按钮 31 时，随机键盘生成单元 21 生成随机密码对照表，并将随机密码对照表所对应的随机按键键盘显示在显示系统 1 的左半部分，随机密码对照表中的按键的字符的排列在每次输入的时候都不相同，且每次都是随机排列出现。

[0042] 随机键盘生成算法如下：

[0043] KEY(n) ＝ RAND(1,2,3,...9,0,清除,OK)

[0044] 其中 n ＝ 1,2,3,...9,0,清除,OK，且 KEY(n) 不重复。

[0045] 反向查表单元 22，用于根据随机密码对照表，当接到用户从键盘上输入的按键数据时，反向查表，还原出原始密码，并输出给密码验证系统 23 验证密码的真伪。

[0046] 较佳地，本实施例中的 ATM 提款机中的所有设备的连线都在系统的整体框架中，不对外暴露，使得他人不能从连线中截取到信息数据。

[0047] 下面结合图 4 进一步说明本实施例中 ATM 提款机密码输入系统工作过程：

[0048] （一）在用户需要输入密码时，按下一个输入密码启动按钮 31，通知系统启动生成随机密码对照表。

[0049] （二）系统接到通知后，调用随机键盘生成单元 21，生成如表 1 所示随机密码对照表。

[0050] 表 1 随机密码对照表

[0051]

位置	键盘按键	实际按键
X1,Y1	1	4
X2,Y1	2	7

X3,Y1	3	3
X1,Y2	4	清除
X2,Y2	5	8
X3,Y2	6	9
X1,Y3	7	5
X2,Y3	8	6
X3,Y3	9	OK
X1,Y4	清除	2
X2,Y4	0	1
X3,Y4	OK	0

[0052] （三）用户根据本次生成的随机密码对照表，进行密码输入。

[0053] 用户根据生成的随机密码对照表，在键盘上输入密码。

[0054] （四）主机 2 收到用户输入的密码后，根据随机密码对照表，调用反向 查表单元 22 进行反向查表，还原出原始密码，输出给密码验证系统 23 验证密码是否正确。

[0055] （五）然后可以把该次的随机密码对照表删除。

[0056] 下面举例说明用户密码还原过程：

[0057] 如果用户输入的原始 6 位密码为：490523，然后按 OK

[0058] 根据表 1 的随机密码对照表，用户在使用键盘输入密码时：

[0059] 第二栏 4，其在键盘上对应第三栏为清除；

[0060] 第二栏 9，其在键盘上对应第三栏为 OK；

[0061] 第二栏 0，其在键盘上对应第三栏为 1；

[0062] 第二栏 5，其在键盘上对应第三栏为 8；

[0063] 第二栏 2，其在键盘上对应第三栏为 7；

[0064] 第二栏 3，其在键盘上对应第三栏为 3；

[0065] 第二栏 OK，其在键盘上对应第三栏为 0。

[0066] 因此用户在实际的键盘上按键顺序为：清除，OK，1，8，7，3，0

[0067] 系统通过键盘控制器扫描按键，根据扫描码接收到用户在键盘上的输入，变成相应的扫描码，转化为 ASCII 码，然后根据随机密码对照表在进行反向查找：

[0068] 根据表 2：在第三栏找到清除，对应第二栏为 4；

[0069] 在第三栏找到 OK，对应第二栏为 9；

[0070] 在第三栏找到 1，对应第二栏为 0；

[0071] 在第三栏找到 8，对应第二栏为 5；

[0072] 在第三栏找到 7，对应第二栏为 2；

[0073] 在第三栏找到 3，对应第二栏为 3；

[0074] 在第三栏找到 0；对应第二栏为 OK。

[0075] 根据表 2 完成还原后，向验证系统发送的密码顺序为 490523，然后按 OK。

[0076] 本实施例的由 ATM 提款机具有眼球贴近观察的窗口 11，该窗口 11 大小和眼睛差不多大小，一个普通键盘 3，主机 2 组成，键盘 3 上可以有字符，但是真正的要输入的字符，在窗口 11 内的显示屏显示对应的键盘 3，键盘上 的字符不是固定的，而是随机变化的，每次都不一样，这样只有在靠近观察的窗口屏幕内才能看到真正的键盘布局，只有用户才能看到，屏幕上能够看到手部的动作或影象，键盘 3 是公开的，他人即使看到手部的动作，也无法知

道真正输入的字符，所以无论旁边，望远镜，还是摄像头等都无法偷窥，从而彻底保护密码输入不被偷窥。

[0077] 另外，ATM 机上可以没有实际的键盘，而是采用语音识别的方式代替键盘输入密码，用户在取景框中看到密码对照表后，根据对照表，对机器念出转化后的密码，机器自动识别后，自动输入到验证系统。

[0078] ATM 机采用语音识别输入系统的方式输入密码，如 IBM 语音识别系统 ViaVoice，在取景框内显示当次生成的随机密码对照表，然后用户根据对照表依次念出转换后的密码，转换后的密码暴露在大众中，系统通过语音识别输入系统接受该密码，然后根据当次的随机密码对照表，还原成原始密码，传送到验证系统中，这样能够提供用户给用户更方便的输入密码系统，尤其对视力不好的老年人，因为屏幕上的按键可以显示得很大，而实际上的键盘无法做到，因此更加方便。

[0079] 实施例二：

[0080] 如图 3 所示，本发明的防止被偷窥密码输入系统是个人计算机 (PC) 的防偷窥密码输入系统，由一台个人计算机 (PC)2 和一个文字图像输出系统组成。

[0081] 文字图像输出系统可以是一个带小屏幕的手机，或者 PDA，或者打印机，或者电子词典，但并不限于这些，其具有和个人计算机数据通讯的能力，比如并口，串口，红外口，蓝牙，无线 WIFI，GSM，PHS，CDMA，3G，USB，1394，数字调频，或者国际互联网 (Internet) 等。

[0082] 个人计算机由显示系统 1、键盘 3 和控制这些外围设备的主机 2 组成。

[0083] 个人计算机主机 2 还包括随机键盘生成单元 21、反向查表单元 22、密码验证系统 23。

[0084] 在用户需要输入密码时，按下一个输入密码启动按钮 31，主机生成一个随机密码对照表，如表 2 所示；然后系统把随机密码对照表输出给外设，如打印机，手机，PDA，小屏幕等；用户根据随机密码对照表在键盘上输入转 换后的密码；系统在收到输入的密码后，根据随机密码对照表，反向查表，还原出原始密码，输出给验证系统密码验证密码是否正确；然后可以把该次的随机密码对照表删除。

[0085] 本实施例的随机键盘生成算法如下：

[0086] KEY(n) ＝ RAND(A，B，C，……，Z，回车键)

[0087] 其中 n ＝ A，B，C，……，Z，回车键，且 KEY(n) 不重复。

[0088] 表 2 个人计算机随机键盘对照表

[0089]

位置	键盘按键	实际按键
1	A	R
2	B	N
3	C	S
4	D	H
5	E	V
6	F	L
……	……	……
25	Y	T
26	Z	C
27	ENTER	ENTER

[0090] 下面以一台笔记本和一个手机为例具体说明以上的过程：

[0091] 笔记本电脑采用带红外接口，键盘为普通键盘，手机为带红外接口的普通带屏幕的手机，比如索爱的 T618，笔记本电脑和手机连接采用红外连接，在使用之前需要把手机上的红外口打开。

[0092] 在笔记本电脑需要用户输入密码时，先触发随机生成随机密码对照表，经过红外口，发送给手机，用户打开手机上发送过来的笔记本电脑随机密码对照表，在键盘上输入随机密码对照表中用户要输入的密码被转换后的密码字符，然后在系统中，再根据随机密码对照表反向查表，还原成原始密码，提供给系统验证。

[0093] 实施例三：

[0094] 本发明的防止被偷窥密码输入系统是 POS 机的密码输入系统。

[0095] POS 机密码输入系统，该系统包括 POS 机和手机关联，其中 POS 机银 行卡与手机卡关联，比如浦东发展银行已经开通东方银行卡和手机关联业务，在个人用户申请东方卡的时候，同时注册一个用户的手机号码，在银行卡进行每一笔交易的时候，都会用短信的方式发送到该注册的手机上。见现有技术专利 CN02151927.7，CN02128721.X，CN200410026515.5，CN02247309.2。

[0096] 与实施例一相同，POS 机包括显示系统 1、键盘 3 和控制这些外围设备的主机 2。本发明的实施例中，不需要对现有 POS 系统的硬件做任何的改动，而只需软件部分升级改动就可以。

[0097] POS 主机还包括随机键盘生成单元 21、反向查表单元 22、密码验证系统 23。

[0098] 当用户银行卡在 POS 机上刷卡后，然后输入金额，在用户需要输入密码时，POS 机或者后台系统生成一张随机密码对照表，如表 1 所示，然后以短消息的方式发送给手机，短消息的内容就是本次交易的随机密码对照表。

[0099] 本实施例的随机键盘生成算法与实施例一相同。

[0100] 然后用户根据对照表，在 POS 机的小键盘上输入经过转化后的密码，POS 机收到输入的密码后，根据本次发送的随机密码对照表，还原成原始密码，传送到 POS 机中进行验证。为了安全，在 POS 机还原密码后，删除本次产生的随机密码对照表，用户也可以把手机中对照表及时删除，较佳地，在手机中设置阅读完该种短信之后，自动删除的功能，防止他人先偷窥输入键盘的动作，然后再抢手机，看到手机上的短信内容，而能翻译出原始密码来。

[0101] POS 机也可以采用语音识别输入系统的方式输入密码，当银行帐户在进行交易要等待输入密码时，银行的短信平台给该帐户关联的手机号码发送该次交易的随机键盘密码对照表，用户根据该密码对照表，念出转化后的密码给输入系统输入密码。

[0102] 实施例四：

[0103] 本实施例的防止被偷窥密码输入系统是门禁系统的密码输入系统。

[0104] 本实施例的门禁系统密码输入系统包括显示系统 1 和键盘 3 以及控制这些设备的门禁系统主机 2。

[0105] 显示系统 1 同实施例一一样，包括一个形状如照相机取景框的窗口 11，用户把眼睛靠近取景框，才能看到里面的图像，较佳地，窗口 11 只够使用者 的眼睛观察，离开窗口 11 位置和角度，其他位置角度都无法观察到屏幕上的内容。

[0106] 本实施例的随机键盘生成算法与实施例一相同。

[0107] 同实施例一样，用户根据随机密码对照表，在键盘上输入转换后的密码，然后系统根据当次的随机密码对照表，还原成原始密码，传送到验证系统，随机密码对照表被删除。

[0108] 本发明由于每次的随机密码对照表都是随机产生的，因此即使偷窥者看到了用户的手部动作的密码输入顺序，由于和原始密码没有任何联系，因此偷窥是没有用的。本发明把用户欲输入的密码和实际输入的密码在空间、时间上分开处理，达到隐秘的效果，只要保证随机密码对照表的安全，无论对手指的动作，键盘的操作，以及遗留信息的偷窥都不能完成窃取密码，其既可以预防他人通过摄像头或者其他方法偷窥，又不需要对输入系统大的改造，因此其成本低，符合用户使用的习惯。

[0109] 本发明的实施例是为了更好地理解本发明进行的详细的描述，而并不是对本发明所保护的范围的限定，因此，本领域普通技术人员不脱离本发明的主旨情况下，未经创造性劳动而对本明所做的改变，是在本发明的保护范围内的。

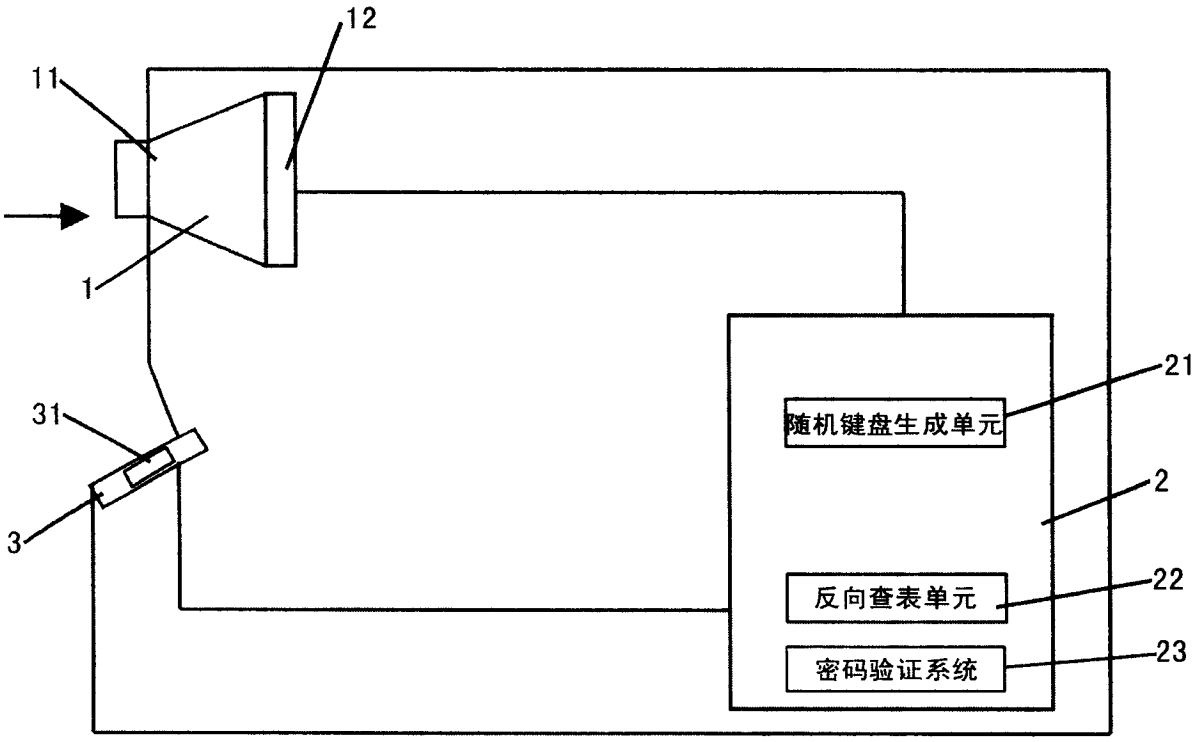

12
11
1
31
3
21
随机键盘生成单元
2
22
反向查表单元
23
密码验证系统

图 1

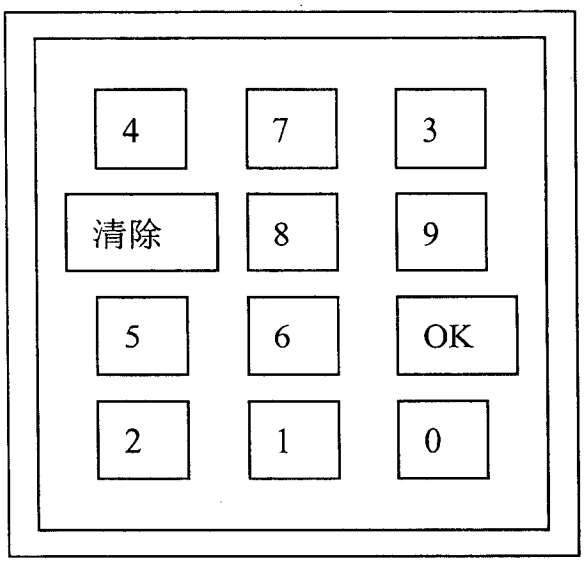

4
7
3
清除
8
9
5
6
OK
2
1
0

图 2

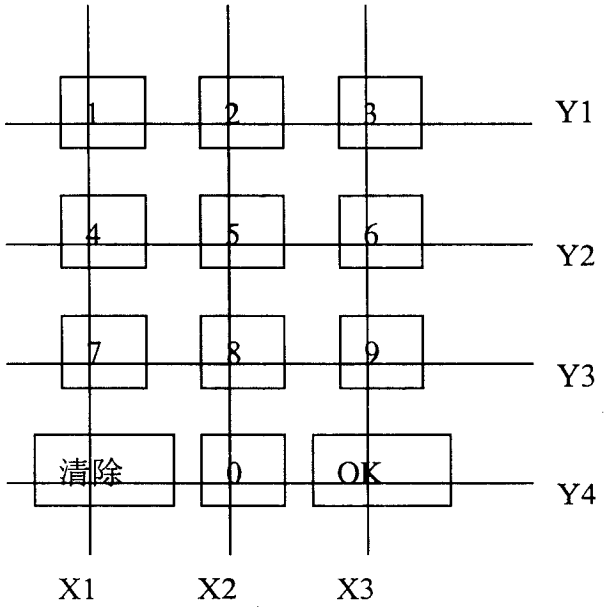

1
2
3
Y1
4
5
6
Y2
7
8
9
Y3
清除
0
OK
Y4
X1
X2
X3

图 3

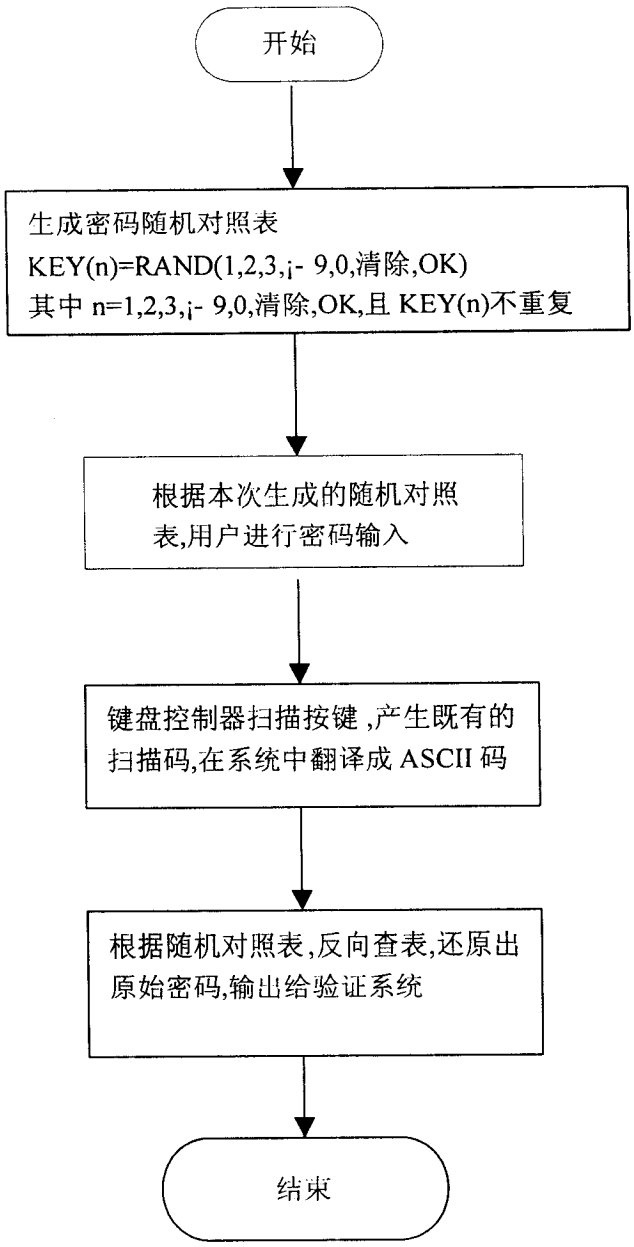

开始
生成密码随机对照表
KEY(n)=RAND(1,2,3,¡- 9,0,清除,OK)
其中 n=1,2,3,¡- 9,0,清除,OK,且 KEY(n)不重复
根据本次生成的随机对照表,用户进行密码输入
键盘控制器扫描按键,产生既有的扫描码,在系统中翻译成 ASCII 码
根据随机对照表,反向查表,还原出原始密码,输出给验证系统
结束

图 4