(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 104584086 B
(45)授权公告日 2017.11.10

(21)申请号 201380038373.1

(22)申请日 2013.07.17

(65)同一申请的已公布的文献号
申请公布号 CN 104584086 A

(43)申请公布日 2015.04.29

(30)优先权数据
1212878.1 2012.07.20 GB
1306053.8 2013.04.04 GB

(85)PCT国际申请进入国家阶段日
2015.01.19

(86)PCT国际申请的申请数据
PCT/GB2013/051913 2013.07.17

(87)PCT国际申请的公布数据
WO2014/013252 EN 2014.01.23

(73)专利权人 利森提亚集团有限公司
地址 英国南格拉摩根
专利权人 麦品帕德有限公司

(72)发明人 贾斯汀·派克

(74)专利代理机构 北京安信方达知识产权代理有限公司 11262
代理人 周靖 郑霞

(51)Int.Cl.
G07F 7/10(2006.01)
G06F 21/31(2006.01)

审查员 任爽

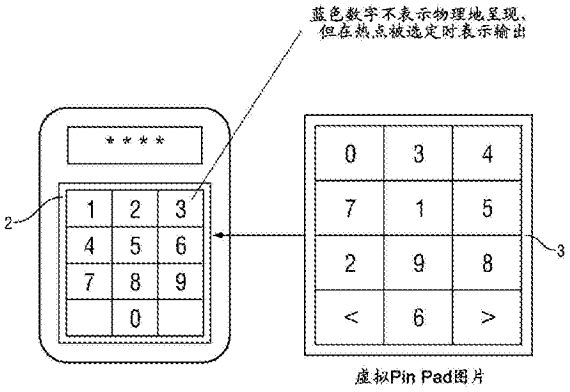
权利要求书3页 说明书20页 附图13页

(54)发明名称

PIN验证

(57)摘要

本发明提供了一种计算机实现的认证方法，包括以下步骤：使用户能够将标识符(例如PIN)输入到具有屏幕和在屏幕的小键盘区中具有可操作的小键盘的电子设备；通过经由在小键盘区至少部分显示的乱序小键盘的至少一部分的图像操作小键盘的至少一个键。用户经由图像对小键盘的键的操作生成用户意图输入的编码版本。本发明在某种意义上可理解为在底层功能小键盘上方重叠乱序小键盘的非功能图像。图像可以是任何类型的电子图像，并且可包括视频图像。本发明特别适用于，但不限于，移动电话、平板计算机、PC等。其可以在被授权访问受控资源之前必须验证用户身份的任何系统中实施。



CN 104584086 B

1.一种计算机实现的验证方法,包括以下步骤:

使用户能够将标识符的编码版本输入到电子设备中,所述电子设备具有:

i)屏幕;以及

ii)在所述屏幕的小键盘区中的由在所述电子设备上执行的过程调用产生的可操作的虚拟小键盘;

所述使用户能够将标识符的编码版本输入到电子设备中是通过经由至少部分地显示在所述小键盘区中的小键盘的至少部分的图像操作所述可操作的虚拟小键盘的至少一个键来进行的;其中,

所述图像表示或描绘了具有至少一个键的乱序小键盘,所述乱序小键盘的至少一个键相对于所述可操作的虚拟小键盘中的键的布局在位置上被重新排序或重新配置;以及

所述图像用作重叠在所述可操作的虚拟小键盘上方的遮罩或掩蔽,使得当所述用户触摸、点击或以其他方式标识所述图像中的位置时,其将操作定位在所述小键盘区中的该位置处的所述小键盘的键。

2.根据权利要求1所述的方法,其中,用户经由所述图像对所述小键盘的键的操作生成所述用户意图输入的所述编码版本。

3.根据权利要求1或2所述的方法,其中,所述图像是电子形成的,包括图形图像、光学图像、视频或某种其他形式的视觉表示。

4.根据权利要求1或2所述的方法,其中,所述小键盘区是覆盖整个屏幕或其一部分的、所述屏幕的限定的区域或部分。

5.根据权利要求1或2所述的方法,其中,所述图像在所述小键盘区中显示,使得当所述用户触摸、点击或以其他方式标识所述图像中的位置时,在该位置的小键盘的键被激活,以提供所述用户输入的编码版本。

6.根据权利要求1或2所述的方法,其中,所述图像被显示为使得其精确地、完全地或部分地占据了所述小键盘区。

7.根据权利要求1或2所述的方法,其中,所述图像被显示为使得对所述用户而言看起来,所述图像是可操作的小键盘,所述可操作的小键盘具有相对于所述电子设备的小键盘呈扰乱的顺序或配置的键。

8.根据权利要求1或2所述的方法,其中,所述小键盘区是在用户输入所述标识符之前被指定为小键盘显示区域的所述屏幕的一部分。

9.根据权利要求1或2所述的方法,其中,在所述用户的标识符的输入期间,所述小键盘区和/或所述图像保留在所述屏幕上的固定位置。

10.根据权利要求1或2所述的方法,其中,所述标识符是个人标识代码或个人标识码。

11.根据权利要求1或2所述的方法,其中,所有在所述图像中描绘的键相对于在所述小键盘中的键被重新定位或重新排序。

12.根据权利要求1或2所述的方法,其中,通过与所述屏幕交互,所述用户能够输入所述标识符。

13.根据权利要求1或2所述的方法,还包括以下步骤:将所述图像从位于远程的基于计算机的资源发送到所述电子设备。

14.根据权利要求1或2所述的方法,其中,所述小键盘区包括多个子区或“热点”,每个

子区对应于小键盘的键。

15.根据权利要求14所述的方法，其中，所述乱序小键盘的图像被呈现给用户，使得所述图像中描绘的至少一个键的位置对应于子区的位置，从而提供了所述图像中描绘的所述乱序小键盘的键和所述多个子区之间的映射。

16.根据权利要求1或2或15所述的方法，其中，在所述用户的标识符的至少一部分已经被输入之后，所述乱序小键盘中的键的配置或顺序被改变。

17.根据权利要求1或2或15所述的方法，其中，所述用户的标识符的编码版本由多个击键而被构造在所述电子设备中，所述多个击键响应于所述用户相对于所述屏幕上的所述图像所做出的点击、触摸或其他指示而在所述小键盘上被激活。

18.根据权利要求1或2或15所述的方法，其中，被输入到所述电子设备的所述标识符从所述电子设备被发送到远程的基于计算机的资源。

19.根据前述权利要求18所述的方法，其中，所述远程的基于计算机的资源接收所述用户的标识符并对其进行处理。

20.根据权利要求19所述的方法，其中，使用所述乱序小键盘的所述图像中描绘的键的配置的存储形式或版本，处理所述标识符。

21.根据权利要求20所述的方法，其中，所述键的配置的所述存储形式或版本是文件名。

22.根据权利要求21所述的方法，其中，处理涉及使用所述键的配置的所述存储形式或版本来提供所述用户输入的标识符的解码版本。

23.根据权利要求20至22中的任一项所述的方法，其中，将处理过的标识符与所述用户的标识符的存储版本进行比较，并且如果所述处理过的标识符与所述标识符的所述存储版本相匹配，则所述用户输入被认为是验证通过。

24.根据权利要求1-2、15和19-22中的任一项所述的方法，其中，所述电子设备上显示的所述图像是从乱序小键盘的多个图像中选择的。

25.根据权利要求1-2、15和19-22中的任一项所述的方法，还包括以下步骤：

生成乱序小键盘的多个图像；

从所述多个图像中选择一个图像；以及

将所选择的图像的副本发送到所述电子设备。

26.根据权利要求25所述的方法，还包括以下步骤：

在执行所述选择之前，从所述多个图像中移除至少一个图像。

27.根据权利要求26所述的方法，还包括以下步骤：

在发送所述副本到所述电子设备后，将所选择的图像从所述多个图像中移除。

28.根据权利要求26或27所述的方法，还包括以下步骤：

从所述多个图像中移除表示具有与所述小键盘的相应的键在相同位置上的至少一个键的乱序小键盘的任何图像。

29.根据权利要求1-2、15、19-22和26-27中的任一项所述的方法，其中，所述图像中描绘的所有键的位置在所述用户的标识符的输入期间相对于彼此保持不变。

30.根据权利要求1-2、15、19-22和26-27中的任一项所述的方法，其中，所述乱序小键盘的图像由所述电子设备接收自远离所述电子设备定位的基于计算机的资源。

31.根据权利要求1-2、15、19-22和26-27中的任一项所述的方法，其中，所述乱序小键盘的图像中的至少一个键的符号至少部分地被遮蔽或模糊化，但保持对所述用户可读。

32.根据权利要求1-2、15、19-22和26-27中的任一项所述的方法，其中，所述电子设备是移动电话、PC、平板计算机、笔记本电脑、PDA、读卡终端，或在外壳中的移动电话，使得其类似于读卡设备或ePOS设备、或具有通信能力的某种其他电子设备。

33.根据权利要求1-2、15、19-22和26-27中的任一项所述的方法，其中，所述图像经由web浏览器、或嵌入在浏览器中的应用、或独立的软件应用、和/或提供图形用户界面的应用来显示，使用户能够与所述屏幕交互。

34.根据权利要求1-2、15、19-22和26-27中的任一项所述的方法，还包括以下步骤：将指示符传递给用户，以确认所述乱序小键盘的图像已由合法资源提供。

35.根据权利要求34所述的方法，其中，所述指示符是听觉指示、视觉指示、文本消息、图像、视频、声音、水印、振动或其他触觉指示。

36.根据权利要求35所述的方法，其中，所述指示符已被所述用户选择。

37.根据权利要求1-2、15、19-22、26-27和35-36中的任一项所述的方法，其中，所述小键盘区在所述屏幕上的位置和/或其尺寸通过过程调用或方法调用来指定。

38.根据权利要求1-2、15、19-22、26-27和35-36中的任一项所述的方法，其中，所述图像和/或所述小键盘包括数值数字、字母字符、符号或任何其他标记，或其组合。

39.根据权利要求1-2、15、19-22、26-27和35-36中的任一项所述的方法，其中，在所述用户输入之后、或在规定的一段时间之后，所述图像从所述电子设备中擦除。

40.根据权利要求1-2、15、19-22、26-27和35-36中的任一项所述的方法，其中，所述用户输入的标识符被验证，以便控制对资源的访问。

41.根据权利要求1-2、15、19-22、26-27和35-36中的任一项所述的方法，还包括以下步骤：

将所述图像从远程的基于计算机的资源发送到所述电子设备；以及

将至少一个指令发送到所述电子设备，所述至少一个指令被配置为在被所述电子设备执行时生成所述可操作的虚拟小键盘。

42.根据权利要求12所述的方法，其中，通过触摸所述屏幕的一部分和/或使用指针设备来选择所述屏幕的区域，所述用户能够输入所述标识符。

43.根据权利要求42所述的方法，其中，所述指针设备是鼠标或轨迹球。

44.根据权利要求24所述的方法，其中，所述多个图像是在选择所述图像之前被过滤、选择或筛选出的，以确保所述多个图像中没有图像描绘与在所述小键盘中的对应的键处于相同位置的任何键。

45.根据权利要求40所述的方法，其中，所述资源包括金融资源、设备、建筑物、电子资源，医用资源、信息或数据资源、或基于计算机的资源。

PIN验证

[0001] 本发明一般涉及用户认证，更具体地涉及基于PIN的验证领域。本发明是适用于要求用户输入密码的情况，密码比如在完成操作之前需要进行证实的个人识别码(PIN)。操作可以是任何类型的操作。

[0002] 认证是用于在被允许对一些受控制的或受管理的资源(比如设备、建筑物、计算机系统、金融帐户、服务等)执行行为之前或获得访问之前需要验证个体的身份和/或认证的各种情况下使用的技术。

[0003] 一种认证的普通方法是记录一些预先选择的标识符(例如代码，或符号的组合)，标识符随后被秘密地保存在安全位置，并仅为经授权方可用。例如，标识符被存储为与特定用户或用户组相关联，且有时可结合另一预先确定标识符进行存储和/或使用。标识符通常由用户自己选择，虽然有时确定标识符者可能是资源管理者或所有者。在许多情况下，用户可以能够改变他们先前选择的标识符。通常，在用户最初加入组织时选择标识符；例如，当他开始受雇于某一公司，或关于某项服务注册提供商。在识别符已被选择并分配给授权的个体后，用户每次请求对资源或服务执行受控制的行为或获得访问的允许时被要求提供预先确定的标识符。将用户所输入的标识符与存储的版本相比较。如果用户能够提供正确的标识符，则认为他的身份已经被验证，并授权访问。而另一方面，若未提供正确的标识符，则访问被拒绝。

[0004] 在本文中，该标识符可被称为个人识别代码(PIC)。

[0005] PIC的一个常见示例是通常称作个人标识码(PIN)的4位数字代码。术语“PIC”旨在包括术语“PIN”(个人标识码)。然而，可使用其他不同长度和包含不同类型的字符或符号的代码。本发明并不旨在对所用标识符的长度，或其所包含的字符的类型进行限制。例如，它可含有数值数字、字母字符、图片、标点或任何其他种类的符号、或它们的混合体。为方便起见，在下文使用的术语“PIN”或“PIC”可以指的是用户的标识符，但不应解释为以任何方式限制标识符的长度、类型或格式。

[0006] 基于PIN验证系统通常包括小键盘，小键盘能使用户输入他们预先选择的PIN。图14a中示出了本领域已知的典型的小键盘布局。小键盘是一组设置成块或“面板”的按钮或“按键”。按键以彼此相邻的网格的形式来设置从而形成面板。按键具有印刷的、雕刻的、模压的标记(标识符)或以其他方式在它们上面展示的标记(标识符)。键上的标记通常包括例如“6”的一个符号，但是可以包括一个以上的符号，例如“AB”。键上的标记通常以规则的方式布置，比如顺序的串行。例如，数位通常以升序排序。在本文件中，术语“小键盘”可与术语“pinpad”互换使用。

[0007] 小键盘经常出现在连接到计算设备的字母数字键盘上。所公知的是其他设备，比如计算器、按钮式电话、号码锁和数字门锁也包括小键盘。便携式电信和计算设备的出现也可见被引入到诸如移动(蜂窝)电话、平板计算机、PDA等的移动设备的小键盘。

[0008] 目前，许多电子设备都包括计算机处理能力和能够显示小键盘的触摸屏界面。这些可以用于各种用途，包括允许授权用户通过输入包含预选符号的组合的密码来“解锁”设备，或输入电话号码以拨打电话。在金融交易中使用的卡读取终端也具有小键盘，以允许用

户经由小键盘来输入他的PIN。

[0009] 每个类型的智能电话(例如品牌和/或型号)可具有与其相关联的特定样式的键盘,作为其“默认”键盘。例如,键可以设置成特定格式或布局,或者可用于标记的特定字体。因此,电子设备的用户可关于该设备上的小键盘而熟悉某种“外观和感觉”。图14b中示出了众所周知的智能电话上产生和显示的典型小键盘的示例。默认小键盘的产生是通过在电话中执行过程调用。

[0010] 与具有可按压(物理可动)键的传统小键盘相比,触摸屏可用来显示具有对应于常规键盘的物理按键的数字标记或其他指示“热点”的小键盘的图像。用户触摸他所选择的与键对应的热点来代替按压可动键。置于屏幕表面之下的感测器感测用户选择了哪个区域,从而“读取”用户的输入。

[0011] 小键盘和基于PIN的技术的最常见的使用可能与金融交易相关,例如自动柜员机(称为“ATM”或“提款机”)和银行卡(即借记卡和信用卡)的销售点设备。

[0012] 引入基于PIN的认证之前,如果客户希望购买商品或服务,他将被要求提供与卡片背面上的签名进行比较的签名。然而,签名可以相对容易地伪造。

[0013] 为了解决这个问题,许多国家已经引入智能卡技术以用于信用卡、借记卡和ATM卡。这种支付系统(有时称为“芯片和PIN”系统)基于称作EMV标准的全球标准。使用这种方法,信用卡和借记卡设有嵌入式微芯片。当客户希望使用该系统为商品支付时,将卡放入访问卡上的芯片的“销售点(POS)”终端或改进的刷卡读取器。一旦卡已被验证为授权,则客户输入4位PIN,该4位PIN被提交到智能卡上的芯片;如果两者相匹配,则芯片将告知终端该PIN是正确的,否则它将通知终端该PIN是不正确的。如果输入中的每个符号在存储的版本中也被发现,并且以相同的顺序和数量,则所输入的PIN与存储的PIN匹配。

[0014] 在某些情况下,可通过以下方式来进行进入交易:刷卡上的磁条以读取卡的数据来进行金融交易,或人工输入卡资料,而不是将卡插入专用的读卡设备。

[0015] 应注意,由于PIN被发送回主机以用于验证,所以安全考虑变得值得关注,因为PIN在传输过程中可能被截取。

[0016] 自从引入了基于PIN的验证,面对面交易(卡和客户亲自出现在交易发生的零售场所)引起的欺诈已急剧减小,因为以欺诈的方式获得或猜中PIN明显比伪造签名更难。

[0017] 此外,在基于PIN的验证出现之前,如果客户的签名是伪造的,卡供应商对任何随后进行的欺诈通常负有法律责任,并被迫为顾客赔偿。然而,随着智能卡技术的引入,责任通常转移到了客户,以证明他们已经做了“合理的关注”来保护他们的PIN,而不是要求在卡提供商不得不证明在交易期间提供的签名与卡上的签名相匹配。责任的转移为卡提供商带来了非常显著的经济效益。

[0018] 基于签名的验证的另一个缺点是,其不提供其在交易进行时卡(和用户)不在零售场所出现的情形中交易——例如,通过电话或互联网进行交易。这样的交易通常认为是“无卡(CNP)”交易。现在,CNP交易在当今零售环境中很普遍,因为许多客户选择不在零售点进行金融操作。然而,尽管基于PIN的技术提供了用于“有卡”面对面交易的相对安全的认证方案,但由CNP交易引起的欺诈正在上升。

[0019] 此外,移动(蜂窝)电话技术已经为零售商和消费者等打开新的机会。包含复杂的计算能力的所谓的“智能”电话并且已经非常普及,向用户提供便利,例如在网上冲浪和查

看零售商的网站的能力。同样地，通常客户和零售商不必被绑到一个实体的地理位置，而是“在移动中”。例如，客户可能希望在公共汽车站等车的同时经由在移动电话浏览网站而进行购买；或停车服务员可能希望向在停车场的司机收取付款。在这种情况下，专用销售点终端是不可用的。

[0020] 然而，尽管移动计算技术十分普及(特别是电话)，但由于安全方面的考虑，其关于CNP交易的使用已经受到了限制，因为在从设备向卡提供商的服务器传输或从卡提供商的服务器向设备传输期间的数据(例如用户的PIN)，或同时存在于电话的内置存储器中的数据，可以被截取。

[0021] 一些与PIN相关的技术已经在设计时考虑到移动性，并且在现有技术中是已知的。

[0022] 例如，CardEase Mobile®是移动支付应用(app)，其结合移动读卡机，能够使零售商采用芯片和PIN移动卡来收取客户的支付。零售商将购买的金额输入到他的移动电话(或台式设备)下载并安装的应用。然后零售商将读卡机设备给到顾客，顾客刷其信用卡/借记卡或者将其信用卡插入到读卡机，并经由读卡机上的小键盘输入他的PIN。然后读卡机经由蓝牙连接到在零售商移动设备上的应用，然后其经由电话的因特网连接到服务提供商进行支付认证。一旦支付被批准，客户将他的卡从读卡机中移开，并且零售商将收据通过电邮或文本发送给客户。

[0023] 然而，这种已知的布置要求使用读卡机。实际上，其使用移动电话担当通常位于商店/商铺的销售点终端的角色。收取支付的商家仍需要与进行支付的客户在相同的位置，因为他必须将读卡机交给顾客以用于与客户的信用卡或借记卡一起使用。系统并不能消除对专用(即专门构造)的读卡设备的需要。

[0024] 现有技术的另一个实例公开在WO/2012/004395 A1(“iZettle”)中。iZettle装置包括用于读取智能卡的便携式读卡机设备、便携式读取机设备和支付服务器。所公开的方法的目的是消除移动电话中用于输入PIN的不安全的键盘，而代替的是使用单独的PIN输入设备，该单独的PIN输入设备实现EMV级规范。本质上，所公开的方法使用外部PIN pad，该外部PIN pad配置有所需的安全芯片和部件，并且其经由蓝牙连接与移动电话进行简单通信。因此，如上所述，iZettle的公开没有解决使用不安全的移动设备用于PIN输入的问题，它通过使用单独的PIN输入设备简单地避开了这个问题。

[0025] 实际上，iZettle文档(6-19行)声明：

[0026] “一种更实用的解决方案：如果信用卡支付可以使用已知的、轻便的和常用的设备(诸如移动电话)进行。然而，普通的移动电话没有可以用来刷您的信用卡的内置读卡机，并且即使可以克服这个特别的问题，仍然存在关于移动电话所提供的安全级别的问题。众所周知，例如，间谍程序可以入侵移动电话并截取信用卡信息和识别信息，比如当进行信用卡支付时经由电话的键盘输入到移动电话的PIN代码，而用户甚至都不知道。鉴于以上观点，标准移动电话通常不被认为是安全设备，并因此不适合用于进行信用卡支付。因此，此后，寻找一种用移动电话进行安全信用卡支付方法是备受追捧的”。

[0027] 另一个已知的装置(也来自WO/2012/004395 A1申请)包括设备(“加密狗”)和装配到智能电话的充电端口的相关软件。当进行交易时，客户的卡被插入到加密狗中。然后，请求顾客用他们的手指来在电话的触摸屏上签名，以便授权交易。使用这种方法，用户不需要输入PIN。因此，在不安全的便携式设备上进行PIN输入的问题将被避免而不是被解决。

[0028] 另一种已知方法公开于WO 2011/093998 A1中。所公开的方法也是使用插入到设备中的基于加密狗的读卡机。其不提供用于实现基于PIN授权的安全技术。

[0029] GB 2416058 A公开了一种用于验证访问服务器的请求的方法。响应于访问请求，在安全服务器中的“组合生成器”生成随机字符串。然后，其使用随机字符串来生成从服务器向用户计算机发送的“图像数据”。然后，用户计算机上的小键盘根据图像数据进行修改。然后，用户使用在计算机上显示的修改后的小键盘输入他的PIN。与用户在键的网格中选择相关的位置数据(例如第一行第一列)作为用户的PIN记录被存储，然后位置数据由用户机器转换成字符数据，例如数字串，以形成被编码的PIN。然后被编码的PIN被发送到服务器进行验证。然而，被编码的PIN可以“通过已知的图像数据解码”——第10页第22-23行。因此，随着图像数据被存储在用户计算机中，如果用户机器的安全性受到威胁(例如被攻击，或被恶意软件感染)，则可获得对图像数据的访问，从而实现第三方解码用户PIN。

[0030] 因此，需要提供一种认证方法，这种方法不会使PIN在设备之间进行传输期间或者在验证过程期间临时存储在电子设备时易受未授权访问的访问。

[0031] 理想地，基于PIN认证的解决方案，将能够实现用户以安全的方式使用PIN认证来完成CNP交易。理想地，这样的解决方案：

[0032] ●可以在诸如移动电话、平板计算设备、笔记本电脑、PDA等的便携式电子设备，或者在台式电脑或固定设备上实现；

[0033] ●将能够使基于PIN的认证在具有某些计算能力的任何适当设置的设备上执行；

[0034] ●将要求用户使用与他存储的PIN相同的数字并且以相同的顺序输入其PIN(而不是要求用户输入他的PIN的“编码”的或某种方式伪装/转换的形式)；

[0035] ●将容易和直观地使用；

[0036] ●将不要求用户的机器访问用户的“真实”PIN，或具有如何计算它的任何知识；

[0037] ●将不需要执行任何转换或编码算法(其会花费一段时间和处理开销，并且可以用来区分用户的PIN)。

[0038] 现在已经设计有这种改进的解决方案，这种解决方案至少提供以上这些优点。

[0039] 因此，根据本发明，提供了一种如本文各种实施例中所要求保护的方法和系统。

[0040] 根据本发明的第一方面，可以提供一种计算机实现的验证方法，所述方法包括以下步骤：

[0041] 经由至少部分地显示在小键盘区中的乱序小键盘的至少一部分的图像，通过操作小键盘的至少一个键，能够使用户将标识符输入到电子设备，所述电子设备具有：

[0042] i)屏幕；以及

[0043] ii)屏幕的键盘区中可操作的小键盘。

[0044] 为了便于参考，图像可称为“乱序小键盘图像”。

[0045] 小键盘在具有本领域技术人对小键盘期望的功能性方面是可操作的。本领域技术人员将明白术语“小键盘”表示电子或机械的键的网格，每个键都具有至少一个与其相关联的标记，当用户选择键时，使相关联的标记被输入到设备或系统，用于存储和/或处理。在本发明的背景下，小键盘是电子形式的小键盘。其可以被认为是“虚拟”的小键盘，因为其是机械小键盘的软件仿真。它提供所有机械键盘的功能，包括用户可以选择以提供输入到基于计算机的系统的标记的键。

[0046] 小键盘可由电子设备生成或生成在电子设备上。其可以由过程调用生成。该过程可设置在设备制造商提供的库中。

[0047] 通过对比，乱序小键盘图像是小键盘的表示。该表示可包括整个小键盘的表示或小键盘的至少一部分的表示。它可描绘(表示、说明)一个或多个“键”。图像可是电子形式的。它可以是图形图像、光学图像、视频或某种其他形式的视觉表示。它可以数字格式形成或存储在电子文件中。

[0048] 这提供了这样的优点，即表示中的“键”的布局可在传输期间或当其在电子设备上显示时可不被可能截取到表示的未授权方轻易读取。

[0049] 乱序小键盘图像本身不是小键盘，因为它不含任何功能性。它仅仅表示的键的网格。触摸、点击或以其他方式选择图像中所示的任何“键”，本身几乎不产生任何影响或生成输入。

[0050] 然而，应该注意的是，有时纯粹为了便于参考，乱序小键盘图像可称为“小键盘”、“乱序小键盘”或“覆盖键盘”，因为在使用中它表观上起到小键盘的功能。也是仅为了便于参考，图像区可称为“键”，因为这正是用户表观看到和使用的。但是，应当记住，这不是真实情况，并且图像实际上不是小键盘。

[0051] 本发明可能够使用户经由用于显示乱序小键盘图像(屏幕)的相同的设备部件输入他的标识符。换句话说，屏幕可同时作为用于乱序小键盘图像的输出(显示)设备和用作用户的标识符可经由此输入的输入设备。这与其中小键盘被显示在设备部件(例如屏幕)上而用户输入经由另一设备部件(例如键盘)被接收到的任何现有技术公开形成了鲜明对比。

[0052] 该特征的一个优点是它可实现用户的输入从图像映射到可以在用户的视图中至少部分隐藏的电子键盘，这样使得用户的输入在用户输入时被自动编码。输入的自动编码意义在于电子设备可不需要转换、编码或以任何方式处理用户的输入。小键盘可由在电子设备上执行的过程调用产生。可操作的电子小键盘可称为“参考”或者“底层(underlying)”小键盘，以便于参考。

[0053] 优选地，用户经由图像对小键盘的键的操作，生成了用户意图输入的编码版本。优选地，图像被显示在小键盘区域中，使得当用户触摸、点击或以其他方式标识图像中的位置，在该位置可操作的小键盘的键被激活以提供用户输入的编码版本。

[0054] 因此，用户的标识符经由图像被输入。用户可选择图像的一部分，以输入标识符。图像部分可比拟或者描绘小键盘键。因此，用户可通过图像操作小键盘。

[0055] 优选地，图像用作遮罩或掩蔽重叠到小键盘上方，使得当用户触摸、点击或以其他方式标识图像中的位置时，它将操作或激活位于小键盘区中的该位置处的键。

[0056] 优选地，小键盘区和/或图像在用户输入标识符期间保持在屏幕上的固定位置。这点将本发明与其中按键或整个小键盘在验证期间在屏幕上移动的已知系统相区别开。由于本发明的图像保持在固定位置，这提供了更易于使用并且要求电子设备更少的处理的解决方案。

[0057] 因此，从某种意义上说，本发明可视为能够将乱序小键盘图像“重叠”在“底层”小键盘上方，使得当用户经由覆盖的乱序小键盘图像输入他的输入时，将按照底层(优选不可见)小键盘的布局进行编码。

[0058] “底层”小键盘可视为在运行时间中在设备的易失存储器中生成和存在的对象，以

提供一种常规机械小键盘的模型。

[0059] 因此，本发明提供了这样的优点，即用户的“真实”标识符从来不会储存在设备中，并且不会为验证而被传递。因此，用户的标识符不能由任何潜在的拦截器在不知道覆盖图像和底层功能小键盘之间的映射的情况下而推导出。

[0060] 优选地，覆盖图像和底层小键盘之间的映射，不存储在电子设备中，或可由电子设备推导出。两组“键”的位置之间的映射(或相互关系)可存储在远离电子设备的服务器上。

[0061] 优选地，乱序小键盘图像可从基于远程计算机的资源发送到电子设备。资源可以是服务器。因此，乱序小键盘图像可以不在电子设备上生成。乱序小键盘图像的版本可以存储在服务器上。该版本可以是乱序小键盘图像符号(“键”)的顺序的记录。

[0062] 小键盘区可以是屏幕的限定区或部分。因此，小键盘区可占据整个屏幕区或屏幕的部分。乱序的小键盘图像可以被显示，使得它完全地、准确地或部分地覆盖小键盘区。优选地，底层小键盘被至少部分地从视野中隐藏起来，使得用户不能看到小键盘的至少一些键。

[0063] 标识符可以是个人识别代码。其可以是PIN(个人标识码)。其可包括任意数量、类型或组合的符号或标记(如上所述)。标识符可由用户在执行本发明所要求保护的方法之前预先选择。标识符可远离电子设备进行存储，例如，存储在服务器上。乱序小键盘图像和/或小键盘可包括数值数字、字母字符、标点符号、符号或其他任何标记、或它们的组合。一个或多个符号可与每个键相关联。

[0064] 优选地，用户可以能够在乱序小键盘图像中选择多个“键”，以输入包括多于一个符号的标识符。

[0065] 乱序小键盘图像可相对于参考小键盘乱序。小键盘图像可以描绘包括多个相邻键的块或网格。其可以是“乱序的”，在这个意义上，在“键”上的符号并不以顺次顺序和/或并不以预期的顺序，可能参考参考小键盘。乱序可根据随机生成过程、或近似随机过程的过程。参考小键盘可以是在小键盘区内可操作的小键盘，或与标准生产、型号、类型的电子设备相关联的默认小键盘。

[0066] 因此，相同的标记可以出现在底层小键盘和乱序的小键盘图像中，但它们被设置在不同的位置。从另一个角度来说，参考小键盘中的键的顺序与乱序图像的是不同的。乱序小键盘图像可提供与和电子设备相关联的默认小键盘相同的“外观和感觉”，但提供的“键”在不同的相对位置。

[0067] 一个、一些、或所有的“键”在乱序小键盘图像中的各个位置可与在底层小键盘中的相同的键的位置不同。

[0068] 用户可经由乱序小键盘图像，通过与显示在屏幕上的“键”进行交互来操作低层小键盘的键。例如，用户的输入可由用户通过触摸屏幕(用手指或其他设备)或者通过使用例如鼠标或轨迹球的指针设备选择所需的“键”来输入。其他选择方法可用于产生类似的作用，因此也落入本发明的范围。

[0069] 小键盘区的位置和/或尺寸可以通过过程调用或方法调用来指定。

[0070] 优选地，小键盘区包括多个子区或“热点”。在乱序小键盘图像和/或小键盘中的至少一个“键”的位置可对应于子区的位置，使得可在乱序的小键盘的“键”和小键盘和/或多个子区的键之间具有映射。期望的是映射不可由电子设备推导或得到。热点可位于乱序小

键盘图像的按键之下。

[0071] (底层)小键盘可在用户选择每个键后乱序。因此,不同的乱序底层小键盘可用于用户的输入的每次键击。

[0072] 优选地,乱序小键盘图像是由电子设备从远离电子设备放置的基于计算机的资源(例如,服务器)接收到的。其可相对于对图像的请求从服务器被发送到电子设备,请求从设备发送到服务器。乱序小键盘图像可由服务器生成。

[0073] 优选地,乱序小键盘图像是预生成的。在一个实施例中,这可意味着它是先于来自电子设备的请求生成,而不是响应于来自电子设备的请求生成。图像可在执行验证方法之前产生。

[0074] 用户的输入(标识符)的编码版本可从电子设备发送到基于计算机的远程资源。该资源可以是服务器。优选地,服务器接收用户的输入的编码版本并对其进行处理。处理可提供用户所输入的标识符的解码版本。

[0075] 因此,用户的"真实"标识符可不被发送。只有被编码的版本可被发送,这对不知道乱序小键盘图像中的"键"和底层小键盘中的键之间的映射的未授权方来说可能是无意义的。

[0076] 可以使用乱序小键盘图像的存储形式或版本来执行解码。键的配置的存储形式或版本可以是文件名。解码步骤可提供用户输入的解码版本。因此,用户的"真实"标识符可通过将编码版本中的每个符号转换成其在乱序小键盘图像中对应的符号来产生。

[0077] 可将用户的解码输入与标识符的存储版本进行比较。如果输入与存储的标识符相匹配,则用户的输入可被认为是正确的。

[0078] 优选地,方法还包括以下步骤:

[0079] 生成多个乱序小键盘图像;

[0080] 从多个乱序小键盘图像中选择一个乱序小键盘图像;以及

[0081] 将所选择的乱序小键盘图像的副本发送到电子设备。

[0082] 方法可进一步包括以下步骤:;

[0083] 在进行选择之前,从多个乱序小键盘图像中移除至少一个乱序小键盘图像。

[0084] 方法可进一步包括以下步骤:

[0085] 在发送副本到电子设备之后,从多个乱序小键盘图像中移除所选择的乱序小键盘图像。

[0086] 方法可进一步包括以下步骤:

[0087] 从多个乱序小键盘图像中移除具有与参考小键盘的相同的键在相同位置上至少一个的键的任何乱序小键盘图像。

[0088] 优选地,键在乱序小键盘图像的位置在用户的标识符的输入期间相对于彼此保持不变。这与现有技术的装置对比,在现有技术的装置中,用户选择每个键之后和/或每个验证会话之后,向用户显示的键位置和/或顺序可乱序或重新排列或在屏幕上移动。

[0089] 优选地,乱序小键盘图像中的至少一个键的符号被至少部分遮蔽或模糊化但保持用户可读。这可能对使用OCR软件读取表示困难有好处。这增强了系统和方法的安全性。

[0090] 电子设备可以是移动电话、PC、平板计算机、笔记本电脑、PDA、读卡终端或其他具有屏幕的电子设备。电子设备可以能够通过无线或固定线路支持通信协议,比如TCP/IP,但

是也可支持其他协议，比如蓝牙、RS232等。

[0091] 设备(例如移动电话)和基于计算机的资源(例如服务器)之间的通信可经由固定电信线路或经由移动电信/wifi等连接-基本上可以使用任何基于IP的设备。

[0092] 乱序小键盘图像可经由web浏览器、或嵌入在浏览器中的应用、或独立的软件应用、和/或提供图形用户界面的应用来显示，以允许用户能够与乱序小键盘图像互动。

[0093] 优选地，定位乱序小键盘图像的标记和底层小键盘之间的映射关系被远离设备进行存储，通常在远离设备的基于计算机的资源中。

[0094] 为了增强安全性，乱序小键盘图像可在被发送到电子设备之前被重命名和/或被加密。这提供了防止或至少阻止第3方(诸如恶意软件)截取和解码标识符的好处。

[0095] 方法还可包括以下步骤：将指示符输送给用户，以确认乱序小键盘图像由合法资源提供。指示符可以是“水印”。指示符可以是文本消息、图像、视频、声音、振动或其他触觉指示。指示符可已经由用户选择。

[0096] 优选地，乱序小键盘图像在用户的输入之后或一段特定时间之后将从电子设备中擦除。

[0097] 如果用户在输入标识符时发生错误，新的(即不同的)乱序小键盘图像可被发送给设备。

[0098] 根据本发明还可提供一种用于验证预先存储的个人标识代码(PIC)的计算机实现的方法，方法包括以下步骤：

[0099] -生成小键盘的表示，其中，表示中的至少一个标记的位置不同于小键盘中相应标记的位置；

[0100] -将表示发送给远程设备，用于呈现给用户使用户能够使用表示输入PIC；

[0101] -从远程设备接收所输入的PIC的编码版本；

[0102] -对被编码的版本解码，以提供所输入的PIC的解码版本；

[0103] -比较所输入的PIC的解码版本和预先存储的PIC。

[0104] 根据第二方面，提供了一种用于验证预先存储的个人标识代码(PIC)的计算机实现的方法，方法包括以下步骤：

[0105] -从基于计算机的远程定位的资源接收小键盘的表示，其中，在表示中的至少一个标记的位置不同于在小键盘中相应标记的位置；

[0106] -将表示呈现给用户，以使用户能够使用表示输入PIC；

[0107] -生成所输入的PIC的编码版本；

[0108] -发送所输入的PIC的编码版本到基于计算机的资源用于解码，使得所输入的PIC的解码版本可与预先存储的PIC比较。

[0109] 根据另一个方面，提供了一种用于验证预先存储的个人标识代码(PIC)的计算机实现的方法，方法包括以下步骤：

[0110] -使用基于计算机的资源来生成小键盘的表示，其中，在表示中的至少一个标记的位置不同于在小键盘中相应标记的位置；

[0111] -将表示发送到远程设备；

[0112] -经由远程设备将表示呈现给用户，以使用户能够使用表示输入PIC；

[0113] -从远程设备发送所输入的PIC的编码版本到基于计算机的资源；

[0114] -使用基于计算机的资源来对编码版本解码，以提供所输入PIC的解码版本，并将其与预先存储的PIC比较。

[0115] 根据本发明的另一个方面，提供了一种计算机实现的验证方法，方法包括以下步骤：

[0116] 使用户能够通过经由在与电子设备相关联的屏幕的小键盘区中呈现给用户的乱序小键盘，选择至少一个键来输入标识符。

[0117] 根据本发明的另一个方面，提供了一种设置和配置为执行上述方法的任何实施例的计算机实现的系统。

[0118] 本发明的有益效果包括：

[0119] -减少CNP交易引起的欺诈的可能性；

[0120] -显著减少与这类欺诈相关的成本；

[0121] -关于欺诈卡的使用，将责任从发卡方转移到用户；

[0122] -方便用户进行安全的CNP交易。

[0123] 参考本文描述的实施例，本发明的这些和其他方面将变得明显并得到了阐述。

[0124] 现在仅以示例的方式，并参考附图，将描述本发明的实施例，其中：

[0125] 图1至图4示出的是根据本发明可以生成的各种类型的小键盘的一些示例。

[0126] 图5示出的是根据本发明的示例性实施例的乱序小键盘表示的生成。

[0127] 图6示出的是根据本发明的注册过程。

[0128] 图7示出的是为注册设备创建的示例性自定义小键盘数据库。

[0129] 图8示出的是根据本发明的示例性交易过程；

[0130] 图9和图10示出的是根据本发明的实施例的示例性的安全交易应用过程的概观图。

[0131] 图11示出的是根据本发明实施例的示例性的“标准”小键盘。

[0132] 图12a，图12b和图12c示出的是适于重叠在图11的标准小键盘上方的乱序小键盘图像的示例。

[0133] 图13示出的是重叠在设备的标准(参考)小键盘顶部之上的乱序小键盘图像。

[0134] 图14a示出的是现有技术中所知的标准数字键面板。

[0135] 图14b示出的是现有技术中所知的移动电话上的数字小键盘。

[0136] 图15a示出的是在应用水印之前预先生成的小键盘图像。

[0137] 图15b示出的是设置在小键盘区的左下角中的具有水印的图15a的小键盘图像。

[0138] 图15c示出的是图15b的小键盘图像，但它所具有水印在不同的位置(左下)。

[0139] 图15d示出的是具有用作背景中的水印的摄影图像的图15a的小键盘图像。

[0140] 图16a至图16e示出的是根据4个不同的数值序列中生成的不同的乱序小键盘图像。

[0141] 图17示出的是具有字母和数字键组合的乱序小键盘图像。

[0142] 图18示出的是三个分图像，其当以快速连续的方式重复示出时，形成明显静态的可识别的图像。

[0143] 图19示出的是本发明如何在金融交易处理系统中实现的示例。

[0144] 转向附图，现在将描述与移动电话的使用相关的示例性实施例。然而，本发明可用

于在各种不同类型的设备上执行PIN验证，假定设备具有一定的处理能力和用于显示小键盘的屏幕。

[0145] 示例实施例还涉及金融交易相关的使用。本发明的一种应用是适合于在线银行的应用。然而，领域技术人员很容易理解的是，本发明也可采用于其他设置中以及用于非金融目的。本发明并不限于商业或商业用途。

[0146] 重要的是，本发明可用于在允许个体访问某些受控资源之前要求验证个体身份的任何情况。受控资源可以是任何类型的资源。其可以是在金融帐户上的资金设置。同样，其可以是建筑物、计算机系统、病人的病历、服务等等。例如，其可用于门锁上密码的验证，以建立允许进入建筑物之前进行的认证。

[0147] 值得注意的是，以下描述的财务导向的应用是可以实现本发明的一个用途。用于示例的目的选择该用途，是因为芯片和PIN验证可能是最广为所知的基于代码的验证的使用，并因此最容易被本文的读者认识。然而，本领域技术人员将理解，本发明并不限制本发明可最终投入使用的环境或背景方面。

[0148] 同样值得注意的是，本发明并没有构成用于执行交易本身的意义。其是一种用于对请求访问受控资源的个体的身份进行认证的验证工具。其并不主导在建立认证之后如何进行访问，也不主导在成功验证之后的任何其他操作或可能交易如何进行。

[0149] 下面描述的示例性实施例的本质上通过创建乱序形式的小键盘(可替换地称为“PIN pad”)的图像来进行操作。乱序小键盘图像被发送，用以呈现或显示于目标电子设备1上，供用户查看。在该示例中，目标设备是移动电话1，如图6所示。

[0150] 乱序小键盘图像设置成类似于用于设备的标准、默认的小键盘。每个品牌和/或型号的设备通常具有其自己风格的默认小键盘，这些小键盘自身的风格可以与其他的设备相关的默认小键盘相比，具有不同的布局、符号、尺寸、颜色等。默认的小键盘通常通过过程调用在移动电话上生成并显示，过程调用指定用于该设备的小键盘的格式和其将要在屏幕上何处显示。默认的小键盘是占用屏幕上的特定区的网格，即它在指定的位置显示。它是电话的屏幕上的预定区或部分(本文称之为“小键盘区”)。小键盘区划分子区，其中，每个子区表示默认键面板中的键。该另一种说法是，每个子区与特定符号相关联。每个键的符号显示用于用户在其相应子区位置的屏幕上查看。因此，如果用户选择(例如触摸或点击)指定到特定子区的区域，则与该键相关联的符号被记录。在这种方式中，小键盘用作由软件电子生成的机械小键盘的虚拟形式，来检测用户在限定的屏幕区中输入的位置，并使用其生成输入数据而不是使用物理上可按压的键。

[0151] 这样的虚拟小键盘，每个子区实质上是屏幕上的“热点”，并且多个热点彼此相邻组合形成小键盘。在本实施例中，电话的默认小键盘2设置成3×4栅格的按键，每个按键4具有与其相关联的符号。在这种情况下，符号包括数值数字。每个按键4是屏幕的“热点”区域，每个热点与虚拟小键盘中的符号相关联。

[0152] 与智能电话一起使用的默认小键盘2的广为所知的样式的示例如图11所示。默认小键盘2在目标设备1本身上生成——其不从位于远端的服务器发送到设备1。

[0153] 然后标准小键盘2被发送到手机上并在屏幕上小键盘区显示的乱序小键盘图像3“重叠”。该重叠通过在小键盘显示区中显示乱序小键盘图像来实现，使得乱序“键”的位置对应于默认的小键盘中热点的位置。两个小键盘上的对齐使得乱序小键盘图像仅被用户所

见，并且底层的可操作小键盘被图像至少部分地(但优选是全部地)隐藏。因此，对于用户来说，除了键具有相对彼此在不同位置之外，只有一个小键盘看起来完全像用户期望的小键盘。

[0154] 因为用于移动电话的默认小键盘是针对乱序小键盘被参考的“规范”，其可称为“参考小键盘”。

[0155] 图12a、图12b和图12c示出了适用于覆盖在图11的标准小键盘2的顶部之上的小键盘图像3的示例。

[0156] 乱序小键盘作为图像被发送到电话。可选地，其可作为视频文件被发送，这将在下文中进一步更详细地描述。图片、视频或图像3可称为“表示”，因为在某种意义上说，其表示物理(可按压)小键盘。

[0157] 乱序小键盘图像3已预先生成(即，在初始化验证过程之前)。其是从一组预先生成的乱序小键盘表示中随机选择出的，并且然后通过电信网络发送到手机(即移动电话)1。图3的乱序小键盘图像是默认的小键盘布局2的表示。默认的小键盘2和乱序小键盘图像3之间的区别是相应按键4的顺序不同。换句话说，相同的数字出现在每个小键盘中，但至少两个处于小键盘网格中的不同位置。

[0158] 该小键盘表示3被生成为具有与默认小键盘完全相同的尺寸，使得其可完全将小键盘重叠。因此，移动电话用户(客户)只看到一个无缝的小键盘。用户不知道在背景中、在他看到并使用以用于键入他的输入的小键盘表示后面已经生成的底层小键盘2的存在。图像与一个或多个指令一起被发送到用户设备以请求或调用用于生成底层小键盘所必需的程序。

[0159] 随机选择的乱序小键盘图像3被有效地覆盖到电话的默认的小键盘2上，使得在用户输入他的PIN时，设备中生成结果不同于用户意图输入或至少认为他正在输入的结果。这是由两个小键盘2,3上的不同位置的键4之间关系(映射)的结果而导致的。用户在特定位置触摸屏幕，以输入上覆的乱序小键盘图像3中所示的数字，但是这被解释为在该子区的底层小键盘2中的数字。随着用户输入顺次的输入，其对应的底层符号被连接到先前的输入，以构成完整的PIN。

[0160] 以此方式，用户的PIN的编码版本基于用户经由乱序小键盘表示3选择的隐藏键4的位置而产生。如果用户出现错误，则新的(不同的)小键盘表示3被发送到设备1。

[0161] 因此，用户认为他正在输入的PIN不是被软件记录保留在用户电话上的PIN。用户的“真实”PIN从不存储在不安全的电话1上，并且不会通过任何(不安全的)网络进行发送。只有编码版本被存储、被发送。PIN的编码版本可在发送之前加密，以进一步增强安全性。因此，任何拦截器将不能在不知道每个小键盘中的键的位置如何映射到彼此的情况下解码、猜测或转换真实PIN。

[0162] 在本实施例中，解码过程由本发明“知道”这两种小键盘的键的布局的组件来处理，并且因此能够将编码的数字转回到它们的原始副本，因此获得用户期望的输入。然后为验证的目的，将破译的PIN与用户先前存储的PIN比较。

[0163] 在示例性的实施例中，乱序小键盘图像3在其被发送给电话1之前进行加密。到达电话1后，其被加载到设备1上的存储器中安全的或受保护的部分(或至少尽可能被保护的)。换句话说，本发明将使用所有常用的安全特征，如同顾客真实PIN已经被输入(而不是

转换形式)。这提供了另一层安全和保护。

[0164] 现在将更详细讨论与本发明可以投入使用的一种方式相关的本发明的这些方面。

[0165] Pin Pad的产生

[0166] “PIN Pad的产生程序”6负责生成用于整个系统的所有的乱序小键盘图像3。图5中示出了本发明的这方面的概观图。

[0167] 如果使用简单随机的乱序小键盘,则存在一个或多个键可不被定位乱序的风险。这可借助标准和乱序PIN上相应位置上用户输入PIN的一个或多个键。这是不理想的。

[0168] 相应地,在PIN pad图像生成期间,具有一个或多个位置对应于标准小键盘的键的乱序键盘图像将被舍弃。PIN pad的产生因此优选地不是纯随机的,而是经历选择过程,以根据特定的标准选择/舍弃。

[0169] PIN pad(图像)在安全环境中进行生成,通常符合支付卡行业数据安全标准。

[0170] 在特定目标设备1上使用之前必须首先建立输出分辨率和文件类型(在该情况下,是移动电话的类型)。这确保了输出的图像是被生成用于该设备的最佳分辨率例如256×184的。

[0171] 然后选择与上述设置的分辨率相匹配的主“背景图像”7,并且选择包含用于最后的小键盘图像的所有需要的数字(键)的排列的“排列文件”5。在一个实施方式中,文件5必须是以逗号分隔的文本文件,其中每个排列在新的一行。然而,可以设计各种实现方式以获得相同的效果。例如,每个排列可以被#或*分开。

[0172] 然后,使用用户选择的字体类型、大小和颜色“排列文件“5与“背景图像”7合并以生成完整的小键盘图像3。然后对完整的小键盘图像3进行优化并减小尺寸到尽可能小,以达到最佳传输速度。

[0173] 除了如图1、图5、图9、图11、图12和图13中所示的标准单色小键盘,背景图像7都是可设置的。例如,背景的颜色和/或默认字体的类型、大小和颜色可以改变,使得可以生成小键盘的无受限制的数据库,以用于每种类型的屏幕和设备。

[0174] 在一些实施例中,广告、教育消息或其他内容可以结合在所呈现的图像中。

[0175] 这些小键盘图像可采用特殊字体或颜色,以使例如阿拉伯语的任何特定地方的字符能够被使用,并且保证图像不能被未授权光学字符识别(OCR)程序读取(从而增强安全性)。

[0176] 产生的每个小键盘图像也被给定唯一文件名并对所有已经产生的小键盘图像创建主索引。当乱序小键盘图像被发送到设备时,该图像的文件名的副本被暂时存储。该文件名包含在小键盘图像中的键的顺序。这能够使乱序小键盘图像和参考小键盘之间的映射被记录。

[0177] 出于安全目的,乱序小键盘图像3在其被加密和发送到远程设备1之前被重命名;这防止了恶意软件或其他未授权方截取和解码PIN的可能性。

[0178] 图1至图4示出的是根据本发明可提供的乱序小键盘图像3的各种外观的一些示例。

[0179] 以示例的方式,图2示出了具有秋季树叶背景的乱序小键盘图像3。这可以为零售商根据季节性变化来使用或可用于广告的目的。

[0180] 图3示出的是失真了的仅黑白的图像,使得其不能被OCR软件读取。本领域普通技

术人员将意识到此类图像要求高分辨率屏幕来正确地显示。

[0181] 图4示出的是已经改造成阿拉伯字母的单色小键盘图像。本领域普通技术人员将理解的是字符间的地方差异也可与图2和图3中所示的其他影像技术方法结合。

[0182] 在适当功率的设备上，视频覆盖可用来代替静态图像，以进一步降低可以用OCR软件来读取小键盘的潜在可能。这一特征还可用于广告的目的。

[0183] 重要的是，为了提供必要的安全级别，恶意软件以及未授权方无法读取显示给用户的乱序小键盘图像中包含的数据。如上所述，这由本发明通过提供单个图像或者图片格式的乱序小键盘来实现。虽然对于微型计算机上OCR图像是可能的，但移动电话没有能力做到这一点，并且对于隐藏的恶意软件来说几乎是不可能在不引起检测的情况下处理所要求的复杂程度。

[0184] 这个问题可以至少部分通过使用不能被OCR技术理解的随机背景和字体来解决。问题也可以通过将小键盘图像作为视频文件进行输送来解决。虽然视频文件其自身并不适于被OCR技术读取，但对第三方，从视频文件中“抓取“单个屏幕并读取它，存在技术上的可能性。

[0185] 一个可结合到本发明各种实施例的解决方案，也可将两个前述系统组合成一个系统。因此，乱序小键盘图像是以平面格式(即，使用非特殊字体并且背景为“正常“)呈现给用户，但文件本身是小视频文件，当播放时，欺骗眼睛使认为图像是固体和静态的。实际上没有任何单独的帧包含足够的信息，以使其被逆向工程返回到可理解的、可用的内容。

[0186] 系统可以实现为像3帧那样小，每个帧都被快速连续的播放，以使看上去是静态的。图18给出一个示例。当结合到视频文件中时，静态的词“Licentia”被播放，但是各个图像不可被OCR包读取。

[0187] 注册过程

[0188] 图6示出了本发明的这一方面。

[0189] 在某些实施例中，设备1在它可以与本发明的系统和下载到目标设备1的小应用8一起使用之前必须被注册。如果所使用的设备是移动电话1，则更新过程可“通过无线”自动发生；如果设备是固定终端，则可通过固定线路下载软件8，然而它也可以在制造时内置在设备中并根据要求简单地更新。

[0190] 为了在系统中注册移动电话1，用户需要进行包括以下步骤的注册过程：

[0191] 1.经由基于web的接口(例如网站)10登录到注册服务9

[0192] 2.输入他们的个人详细信息，即姓名、地址、邮编(ZIP)、电话品牌型号、电子邮件地址、移动电话号码

[0193] 所要求的数据的性质和类型可由系统运营商规定，并根据系统正在使用的应用，数据的性质和类型随地区和地区之间变化。此外，注册数据可能已经被运营商掌握，因为消费者可以是现有客户，并且因此可能只有应用程序需要被推送到设备。

[0194] 3.然后，链接将被发送到移动手持终端1，以让用户沿用，或应用8被简单地向下“推送”到手机。

[0195] 在第一次运行时，应用8在设备1上设置，并下载可能所需的任何附加数据，如加密键等。在服务器上还创建了用于注册设备的自定义小键盘图像数据库(如图7所示)。

[0196] 为了使固定设备注册到系统上，用户将完成与以下类似的过程：

[0197] 1.经由基于web的接口10登录到注册服务器9

[0198] 2.输入他们的个人详细信息,即姓名、地址、邮编(ZIP)、电话品牌型号、电子邮件地址

[0199] 上述用于移动电话,所要求的数据将由系统运营商规定。

[0200] 3.然后如果要求更新内部应用,则设备经由固定线路或无线被连接到服务器。下载需要的任何其他的数据,如加密键等。服务器上也创建用于注册设备的自定义小键盘图像数据库(见图7)。

[0201] 考虑图7。对于上述两种情况,对于注册到系统上的每个设备,小键盘图像的自定义数据库(或索引)13在主数据库11创建。主数据库包含小键盘图像,该小键盘图像已经被专门生成用于设备的用户注册模型,以确保最佳显示。然后将数据库(或索引)11随机化12,以确保不会有两个设备具有相同顺序的乱序小键盘图像,即小键盘参考“AXF015689.gif”可以是对于一个设备在位置65894而在另一个设备上在位置125948。这再一次增强了安全性。

[0202] 应当指出的是,在某些实施例中,可能不要求用户注册。这可能是软件集成到第三方应用的情况。在这样的实施例中,所需的注册方法可能已经由第三方做出了适当的操作。

[0203] 交易过程

[0204] 在图8中示出本发明的这一方面。

[0205] 用户和设备成功注册后,可以执行交易。根据系统与第三方应用集成的方式,认证(PIN请求)可由若干方法来启动。

[0206] 典型地,集成的第三方:

[0207] a.制造附接到移动设备的刷卡或芯片读取设备的,或

[0208] b.向下推送金融信息和后续支付请求到手持终端,即收费道路应用;或

[0209] c.提供网站,该网站在应用中使用时需要安全的PIN输入,以获得对信息的访问,诸如在线银行访问。

[0210] 然而,本发明不局限于这一点,并且由第三方提供的服务的性质或资源不是本发明的限制性特征。

[0211] 在上述所有示例中,具有通用触发器,以用于PIN应用程序加载并执行随后的PIN输入过程。

[0212] 一旦已经被服务器接收到对图像的请求(其可称为“基于计算机的资源”),输入设备1被识别和认证,并且如果成功,则来自设备的“索引”13的下一个小键盘图像被加密并被传送到设备1。小键盘图像按照如图7条目13(从上到下的顺序)中所示的设备“索引”2被顺序地发送,并不会被再次使用。

[0213] 一旦加密小键盘图像3由设备1接收,其将被解密并传到“安全终端申请”。

[0214] 安全终端应用

[0215] 在图9和图10中示出本发明的这一方面。

[0216] “安全终端应用”是驻留在目标设备/电话1或固定终端上的程序,并且负责安全输入和用户输入的PIN返回到服务器的传送。

[0217] 如上所述,小键盘2在设备上创建成3×4网格。每个热点被分配有数值字符。然后,应用程序用已经被预先生成并像下发送到手持终端1的随机化的小键盘表示3“覆盖”该参

考小键盘2。如上所述，这种乱序小键盘表示3已经以与下方小键盘2的尺寸完全相同的形式生成并完全覆盖它。

[0218] 因此，当用户使用乱序表示3输入他们的PIN号码14时，将生成不同的编码输出。在下面的示例中，如果用户的PIN是“6725”，则小键盘就输出“0476”。这是加密了的“0476”的小键盘输出并且该输出发送回服务器的“解密引擎”。

[0219] 一旦小键盘被按下四次，则乱序小键盘图像3将使用安全删除算法从它归属的受保护的存储器中被安全地擦除。

[0220] 解密引擎

[0221] 一旦中央服务器(“基于计算机的资源”)从手持终端1接收输入的编码的和加密的PIN，则它必须转回原始的用户PIN。

[0222] 这是由在单独的安全服务器上保持的“解密引擎”来完成，仅出于该目的。如先前所述，当设备1将自己标识给服务器并请求小键盘图像3时，发送到设备1的小键盘图像的唯一的文件名称被临时存储。该文件名包含在小键盘中的键的顺序，即图9中所示的小键盘图像的文件名将为“0347152986”。这能够使得乱序小键盘图像和参考小键盘之间的映射被记录。出于安全的目的，乱序小键盘图像3在其被加密并被发送到远程设备1之前被重命名。

[0223] 当加密PIN到达时，消息首先使用用于手机/设备的共享密钥(这可以是三重DES或公私密钥、或根据手持终端开发期间认为合适的任何内容)进行解密。

[0224] 一旦消息已被解密，由用户输入生成的编码PIN必须被解密。为了做到这一点，被发送的小键盘图像的文件名被复制到临时阵列，并且然后对于由用户输入生成的每个号码，相应阵列位置中的号码被取代，因此显示实际的PIN号码。

[0225] 因此对于用户PIN是6725的上述示例，手持终端生成并发送加密的PIN 0476。

[0226] 现在当被发送的小键盘图像的文件名被复制到阵列“0347152986”时，则会得到以下：

[0227] 阵列位置 1 2 3 4 5 6 7 8 9 0

[0228] 文件名字符 0 3 4 7 1 5 2 9 8 6

[0229] 对于生成的PIN中的每个号码，“阵列位置”被定位并且相应的“文件名字符”被取代。

[0230] PIN第一数字＝0(转到阵列位置0)；用户的PIN号码的第一数字＝6

[0231]

阵列位置	1	2	3	4	5	6	7	8	9	0
文件名字符	0	3	4	7	1	5	2	9	8	6

[0232] PIN的第二数字＝4(转到阵列位置4)，用户PIN号码的第二数字＝7

[0233]

阵列位置	1	2	3	4	5	6	7	8	9	0
文件名字符	0	3	4	7	1	5	2	9	8	6

[0234] PIN的第三数字＝7(转到阵列位置7)，用户PIN号码的第三数字＝2

[0235]

阵列位置	1	2	3	4	5	6	7	8	9	0
文件名字符	0	3	4	7	1	5	2	9	8	6

[0236] PIN的第四数字＝6(转到阵列位置6)，用户PIN号码的第四数字＝5

[0237]

阵列位置	1	2	3	4	5	6	7	8	9	0
文件名字符	0	3	4	7	1	5	2	9	8	6

[0238] 在解密过程已经完成之后，就显示用户的“真实”输入6725。然后将使用标准银行加密将PIN号6725加密并传给收单方或银行的合作伙伴进行处理。应当指出的是，在与金融交易相关的实施例中，这仅被进一步加密并传递给收单方。

[0239] 根据特定应用的性质和要求，数据可或可不被进一步加密。

[0240] 然后，阵列连同任何其他临时数据将被安全地被擦除，以确保安全。

[0241] 应当注意的是，在某些替代实施例中，可提供12个较小的键的图片(每个用于一个号码或热点)。电话或其他设备可设置为选择随机号码，并将各个图像重新排列成3×4阵列(并且因此按需求构成虚拟小键盘)。然而，这样的实施例存在潜在的安全漏洞并可为恶意软件提供多个接入点来获得用户的PIN(因为手持终端/设备将不得不将随机号码以及由此产生的PINpad的顺序传送回服务器)。因此，这样的实施例适合于在要求的安全级别相对较低的情况下的应用。

[0242] 还应当注意，尽管以上已经关于具有触摸屏的移动电话描述了本发明，但是其他实施例可包括不同类型的设备。例如，在另一个实施例中，设备可以是个人计算机、或笔记本电脑、或平板计算机。实施例将基本上如上所述起作用，除了用作例如PC的通用计算设备，通常不包括标准的过程调用以用于像移动电话那样生成小键盘，小键盘区和热点由在设备上执行的特制的软件部件指定。软件规定了构成小键盘区的那部分屏幕，以及子区(键)的位置和小键盘区中与其相关联的符号。乱序小键盘图像在该位置显示，以提供上述重叠技术。底层小键盘使用由智能电话实现的相同(或基本上相同的)的过程调用产生。

[0243] 在另一个实施例中，可提供一种与用于零售环境的已知的读卡终端类似的终端。终端可包括触摸屏幕并包括复制那些移动电话的内部部件。因此，终端可如同电话一样可以接收和发送数据，并且终端可根据上述本发明参考移动电话形式的目标设备起作用。

[0244] 因此，本发明可被配置为与各种计算相关设备一起使用，以达到相同效果。

[0245] 另外，本发明可被配置为包括进一步增强用户数据的安全性的各种特征。

[0246] 水印

[0247] 例如，所谓的“中间人攻击”是众所周知的问题。在本发明中，可使用“水印”功能来向用户(即零售商或可能的终端顾客)展示输入设备正在与合法方(例如恰当的银行)进行通信，并且因此乱序的小键盘图像已经由该合法方而不是冒名顶替者发送，来解决该问题。

[0248] 这一功能可以用不同的方式来实现。例如，当零售商注册使用该系统时，他们选择和存储只有他们和信用方知道的保密指示符(字、短语、数字、名称、图像等)。然后，交易被要求执行以下过程：

[0249] 1.读取客户的卡

[0250] 2.输入交易金额

[0251] 3.在终端上显示PIN输入屏幕

[0252] 当PIN输入屏幕被显示时，商家必须在呈递给顾客用于输入他们的PIN之前，物理地核对在屏幕上显示了他们注册的预先选择的密语等。这与ssl技术中采用的基本上是相同的原理，其中其寻找小的黄色的锁定图标作为确认网站的合法性。

[0253] 通过这么做，确保设备正在与合法方安全地对话的责任被放到了商家。如果显示了与商家期望的不同的指示符(水印)，或根本没有指示符显示，则可以假定该过程已经被破坏。

[0254] 该水印可在屏幕上停留一段持续时间，用于顾客进行PIN输入。然而，优选的是，它只显示较短的时段(例如，几秒的范围)，然后其可在被例如顾客的任何其他人看到之前消失。如果水印被其他人看到，这可允许他们执行中间人攻击。图15a示出的是预先生成的空白的pin pad图片。系统创建新的pin pad图片，以包括用户的秘语“jellybean”，然后“jellybean”被加密并被发送到设备。这在图15b中示出。

[0255] 注册后，用户还可选择在哪里显示水印，例如右、左、中心、顶部等。图15c示出了在左下角具有水印的小键盘图像。在可选版本中，文本的颜色、字体样式、或尺寸也可被选择。

[0256] 此外，水印不一定是文本形式。在一些实施例中，用户可上传照片或其他文件(例如，家庭照片或商店的照片等)，使得该图像在背景中显示。这在图15d中示出。

[0257] 水印功能适用于本发明的所有实施例，而不管本发明使用的环境或用于显示小键盘的设备的性能(例如，在线通过浏览器，经由被布置与本发明一起使用的终端，或移动电话等)。

[0258] 附加Pin pad加密

[0259] 为了进一步增强系统的安全性，本发明可使用一种或多种技术，来使未授权方更难弄清、认出或计算所显示的小键盘图像(即用户用来输入他的PIN的小键盘)和底层小键盘之间的映射。

[0260] 例如，如果用户已经选择了包含相同数字一次以上的PIN(例如1223)，则可使计算输入和“底层”小键盘之间的关系更容易。

[0261] 克服这种弊端的一种可能方法可以是创建多于一个的底层小键盘。例如，可以为每个按键生成虚拟小键盘。下面给出一个示例。

[0262] 图16a示出的是乱序小键盘图像，并且图16b示出的是“底层”小键盘。如果用户的PIN是1111，则被发送回服务器的编码PIN将是9999。这就为试图计算或猜测用户PIN的潜在黑客提供了起点。

[0263] 然而，如果使用4个不同的“底层”小键盘来代替一个小键盘，就能克服这个问题。因此，数字序列可以被发送到目标设备(例如终端、电话、PC)，并且序列被目标设备使用以形成小键盘。对于图16b中的小键盘，序列将是3156790482。利用这个方法，有可能生成用于每个被要求键按压的新的小键盘。

[0264] 因此，根据上述的说明，如图16a所示的在顶部的pin pad作为图像被发送到目标设备。然后，发送4个数字序列以用于底层小键盘的创建，例如3156790482，0746189352、0347156289、2581673904。这产生如图16b至16e中所示的小键盘。

[0265] 现在假定用户的输入是1111。代替产生9999，代码9857被生成并被发送回服务器以供解密。随着服务器“知道了”哪一个乱序小键盘图像被发送，和哪一个数字序列，产生的编码PIN似乎更加随机得多，因此更难被拦截器解读。在服务器端的解密过程保持同上。

[0266] 此外，为了进一步提高安全性，在小键盘的生成中可以使用其他字符的组合，而不仅仅是字符。例如，序列Jg6KrBjoJ6也可以被发送。这将生成如图17所示的底层小键盘。

[0267] 在这样的实施例中，在底部小键盘中随机生成的字符串的使用减少了“过滤”底层

小键盘(如上所述)以移除可能为攻击者提供用于攻击的起始点的潜在的不合适的小键盘的需要。

[0268] 然而在优选实施例中,仅使用了1.6m的乱序(“顶部”)小键盘图像而不是可能的3.6m的乱序(‘顶部’)小键盘图像,并且仍然执行检查,以确保没有重叠的和底层的小键盘之间的映射是相同的,即1=1。

[0269] 系统层次结构

[0270] 图19示出了本发明可被实施到交易系统的一种方式。

[0271] 图19包括以下系统部件、或模块。

[0272] 设备应用:在终端或移动电话上运行的app,来管理用户交互和技术工艺流程,包括启动支付交易、与读卡机交互、请求oPinPad(即乱序小键盘图像)、加密所输入的oPin以及在线发送交易用于授权。

[0273] OPinPad管理模块:在专用服务器上的中央安全数据中心运行的单机应用模块。其承载所有oPinPad TIF图像的数据库,并按需求管理oPinPad TIF图像的分配。

[0274] 认证客户端:在中央安全数据中心运行的单机应用模块,可能与oPinPad管理模块在相同的服务器上(或者,在一些实施例中在其自身的专用服务器上)。其接收来自设备的消息,并准备将信息发送到支付开关用于认证。

[0275] HPSAM应用:在专用服务器上中央安全数据中心中运行的单机应用模块。在一些实施例中,服务器可被安全硬化。

[0276] 在图19中,使用了以下术语:

[0277] ●设备:发生付款交易的支付终端或移动电话

[0278] ●oPin:“模糊PIN”-通过底层设备小键盘的键产生的编码的PIN;这不是实际的持卡人的PIN

[0279] ●真实Pin:与消费者卡相关联的真实PIN,在被发卡方验证之前其会被“交换”成oPin

[0280] ●oPinPad:模糊Pin Pad(即乱序小键盘图像)-呈现给卡持有者以输入他们的PIN并且在相对于底层设备小键盘的乱序位置具有“键”的TIF图像

[0281] ●oPinPad阵列:用于如上所述将oPin与真实Pin映射的阵列

[0282] ●HPSAM:托管支付安全访问模块

[0283] ●HSM:硬件安全模块

[0284] ●读卡机:含有或被连接到读卡机的终端/移动设备,其检索来自消费者的支付卡的详细信息

[0285] ●标签:分配给oPinPad的唯一的标识号码,以助于后续处理

[0286] ●ZMK:区域主密钥。

[0287] 参考图19中的参考数字引用,示例系统的处理流程如下:

[0288]

0	设备启动支付交易并（从用户接口）捕获金额和（从读卡机）捕获卡的详细信息。来自读卡机的敏感数据在到达应用程序之前被加密。应用程序上线并向服务器请求 oPinPad。如果可能，将在从读卡机检索卡的详细信息的同时请求 oPinPad。
1	oPinPad 管理模块从数据库检索 oPinPad（即乱序小键盘图像）并为其分配标签。oPinPad TIF 和标签（唯一 ID）被发送回设备。
2	oPinPad 阵列连同标签（唯一 ID）被发送到 HPSAM。标签/阵列组合的所有踪迹将从 oPin 管理模块（特别是存储器）中删除。
3	设备应用程序显示设备上的 oPinPad TIF（乱序小键盘）图像，并收集如上述的 oPin；oPin 立即使用场加密方法（例如 DUKPT）进行加密。然后，整个授权消息被发送到认证客户端，用于支付认证（这类信息包括金额、加密卡的

[0289]

	详细信息和加密的 oPin）。
4	认证客户端收集交易的详细信息并将其传送到支付开关。
5	支付开关在标准路径处理期间截取交易，使得 oPin 可以被替换为真实 Pin。这是通过将具有标签的 oPin 发送到 HPSAM 来完成。
6	使用标签，HPSAM 检索 oPinPad 阵列，并使用它来将 oPin 映射到真实 Pin。立即使用 3DES 和与支付开关相对应的 ZMK 将真实 Pin 加密。
7	将真实 Pin 作为 Pin 块发送回支付开关，并添加到交易，以进行行业标准的在线 Pin 支付授权消息（例如，ATM 消息）。
8	使用行业标准的 HSM 转换真实 Pin 块，使得加密 Pin 可由接收机构来处理（让受人、处理器、发行方）。

[0290] 应当注意，上述实施例是对本发明的说明的而不是限制，并且本领域的技术人员将能够设计出许多可替换的实施例而不偏离由所附权利要求书的内容所限定的本发明的范围。在权利要求中，置于括号中的任何参考标号都不应被解释为对权利要求的限制。术语“包括(comprising)”和“包含(comprises)”等不排斥任何在权利要求或整个说明书之外出现的元素或步骤。在本说明书中，“包含(comprises)”是指“包括(includes)或含有”且“包括(comprising)”是指“包含(including)或含有”。元素的单数引用并不排除这些元素的复数引用，反之亦然。事实上，在相互不同的从属权利要求中引用的某些措施并不表示这些措

施的组合不能被有利地使用。

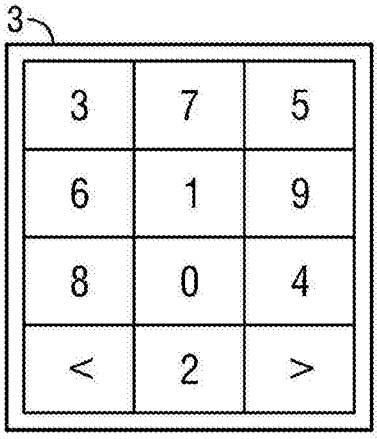


图1

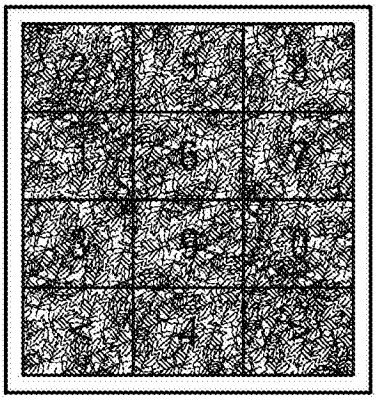


图2

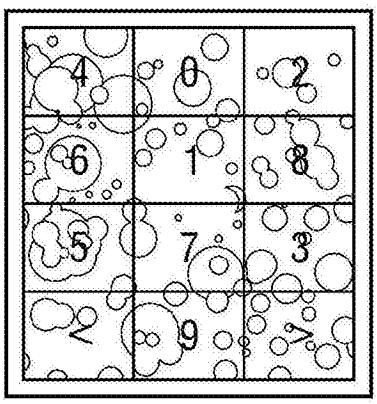


图3

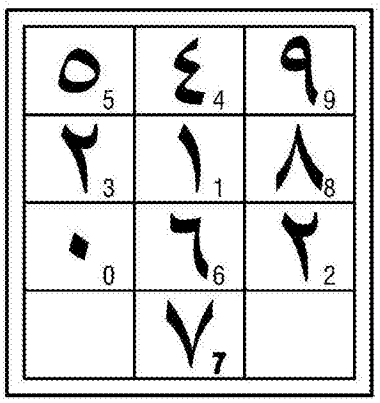

٥ 5
٤ 4
٩ 9
٢ 3
١ 1
٨ 8
٠ 0
٦ 6
٢ 2
٧ 7

图4

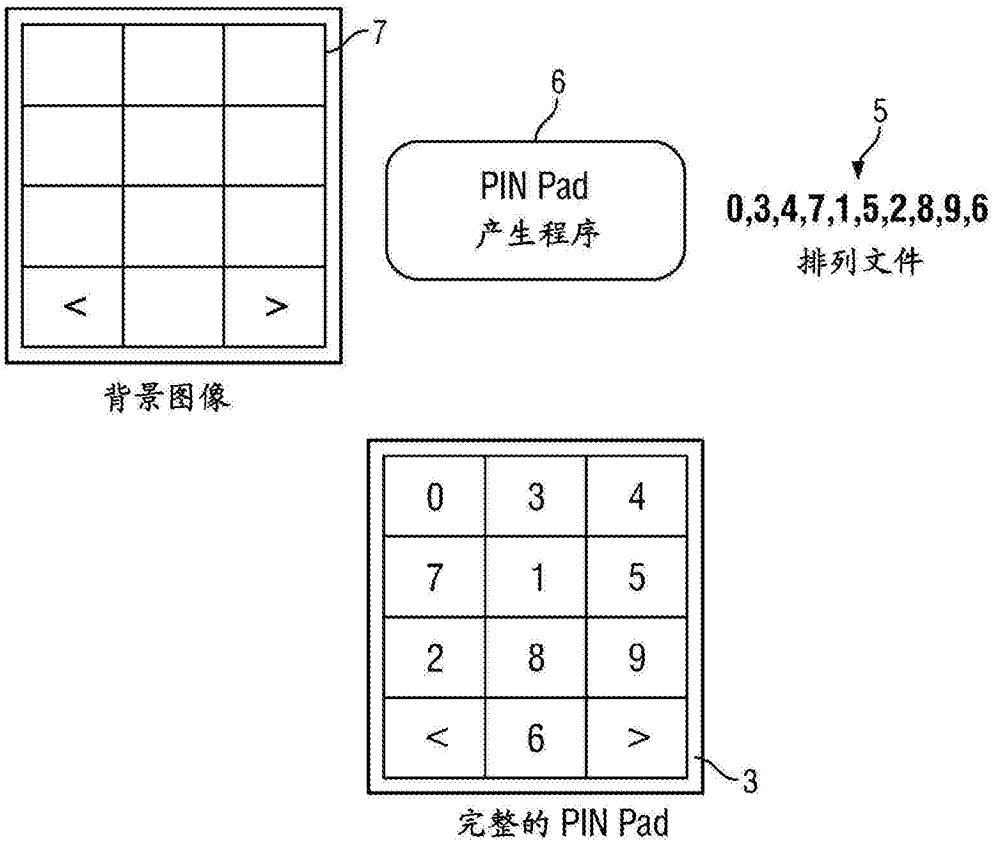

7
6
PIN Pad
产生程序
5
0,3,4,7,1,5,2,8,9,6
排列文件
<
>
背景图像
0 3 4
7 1 5
2 8 9
< 6 >
3
完整的 PIN Pad

图5

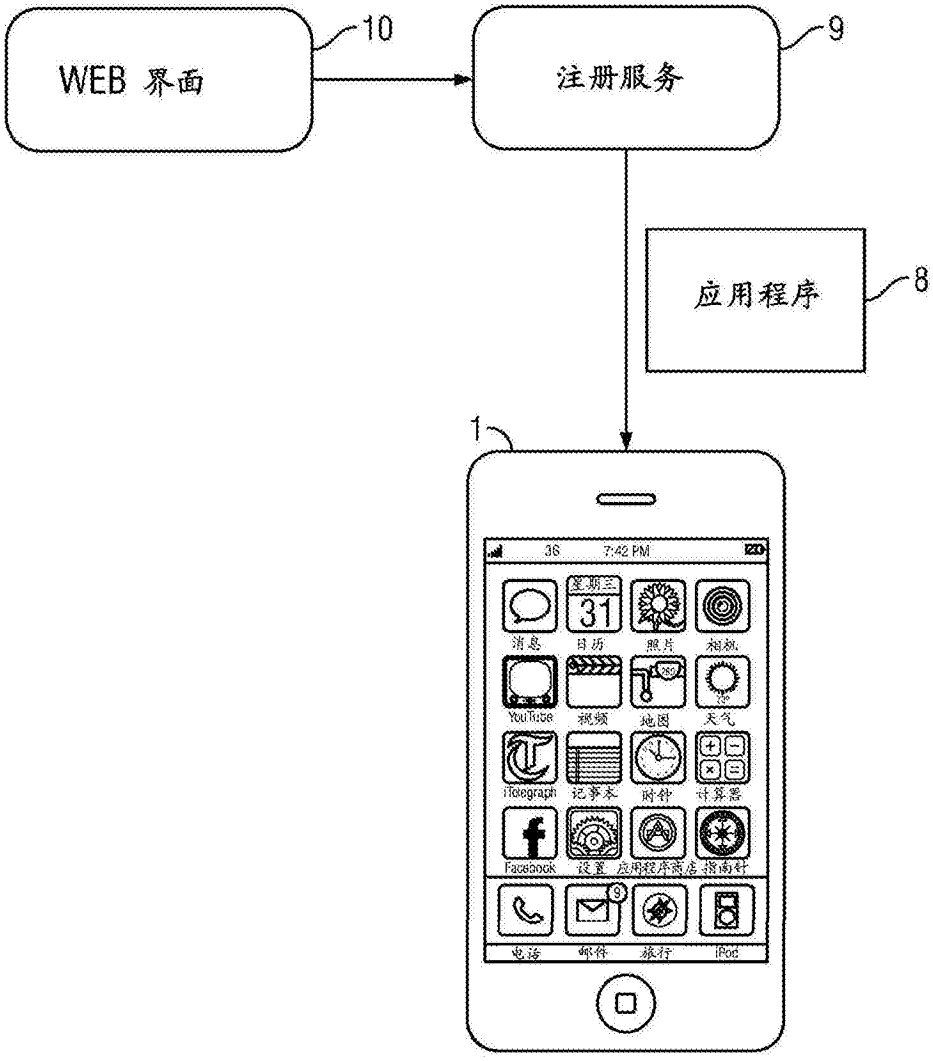

WEB 界面
10
注册服务
9
应用程序
8
1
3G
7:42 PM
星期三
31
消息
日历
照片
相机
YouTube
视频
地图
天气
iTelegraph
记事本
时钟
计算器
Facebook
设置
应用程序商店
指南针
电话
邮件
旅行
iPod

图6

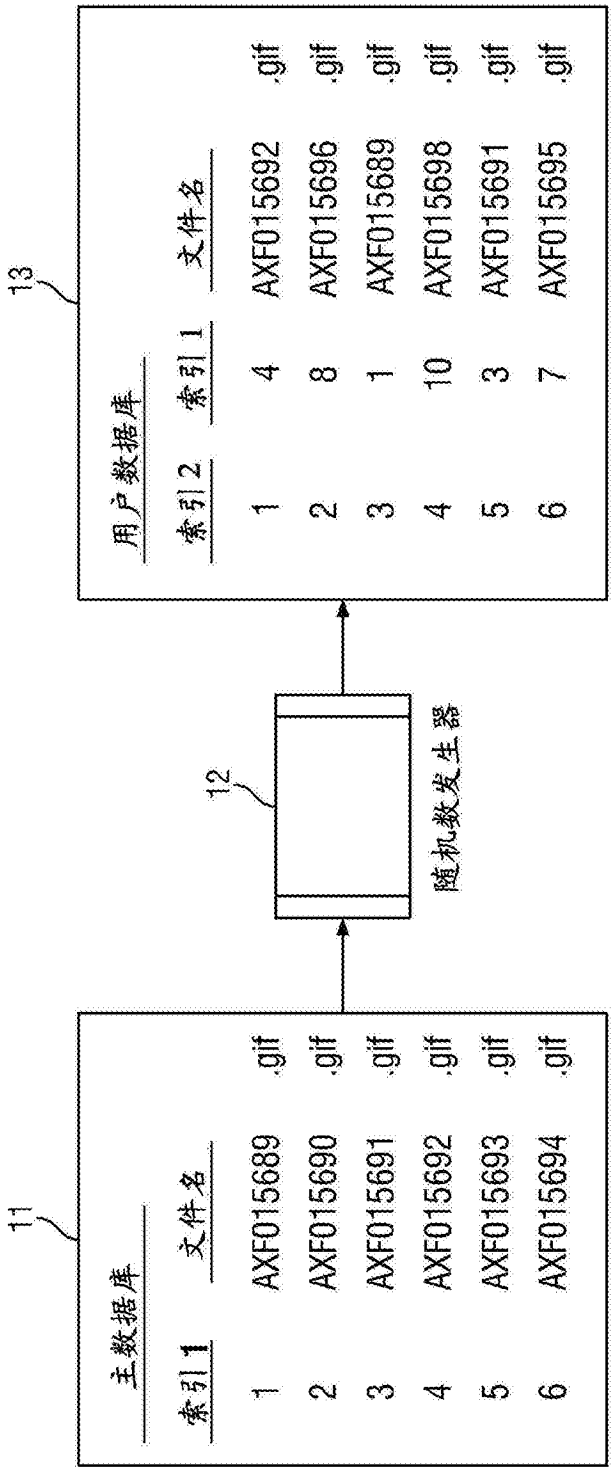

11
主数据库
索引1 文件名
1 AXF015689 .gif
2 AXF015690 .gif
3 AXF015691 .gif
4 AXF015692 .gif
5 AXF015693 .gif
6 AXF015694 .gif
12
随机数发生器
13
用户数据库
索引2 索引1 文件名
1 4 AXF015692 .gif
2 8 AXF015696 .gif
3 1 AXF015689 .gif
4 10 AXF015698 .gif
5 3 AXF015691 .gif
6 7 AXF015695 .gif

图7

图8

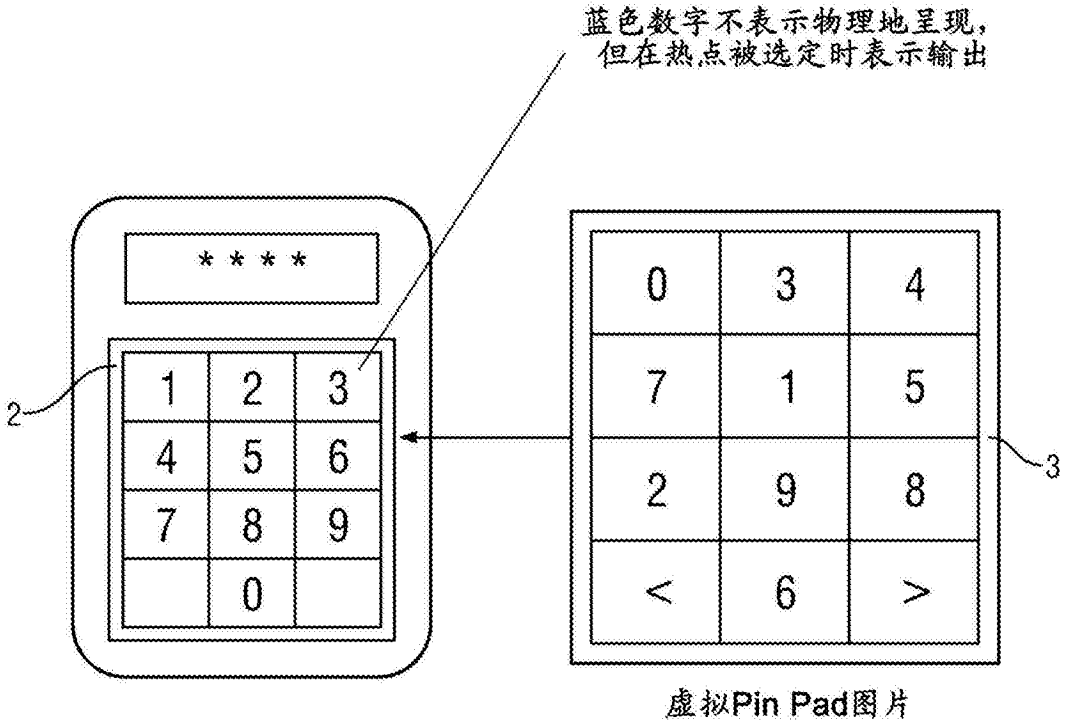

蓝色数字不表示物理地呈现，
但在热点被选定时表示输出
* * * *
1 2 3
4 5 6
7 8 9
0
2
0 3 4
7 1 5
2 9 8
< 6 >
3
虚拟Pin Pad图片

图9

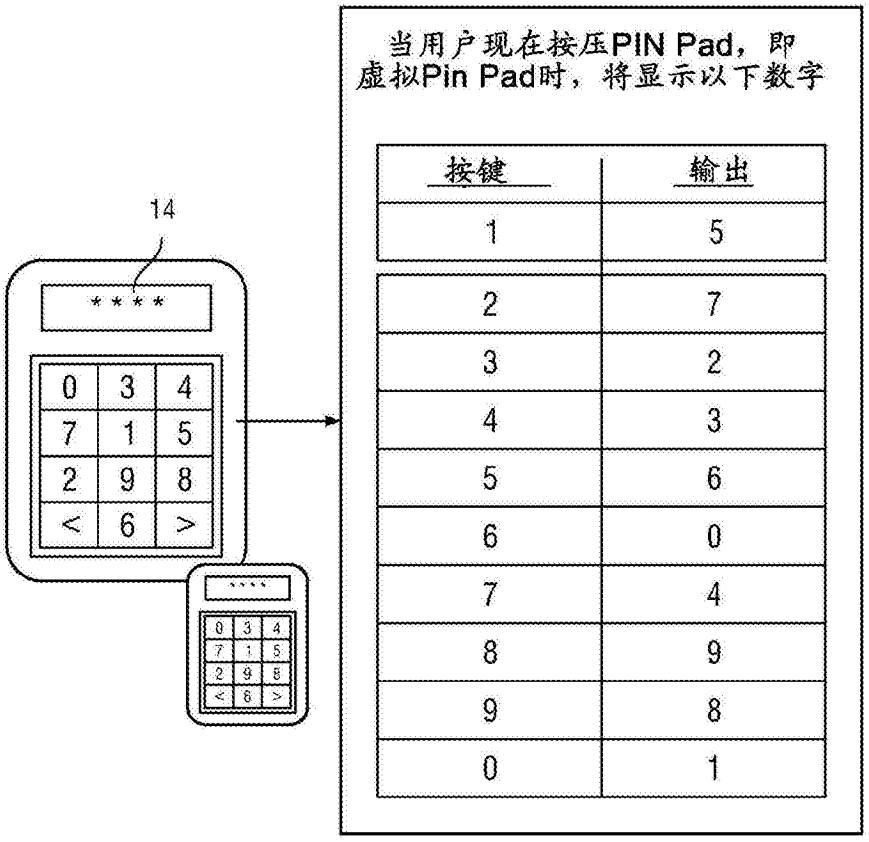

当用户现在按压PIN Pad，即
虚拟Pin Pad时，将显示以下数字
14
* * * *
0 3 4
7 1 5
2 9 8
< 6 >
按键 输出
1 5
2 7
3 2
4 3
5 6
6 0
7 4
8 9
9 8
0 1

图10

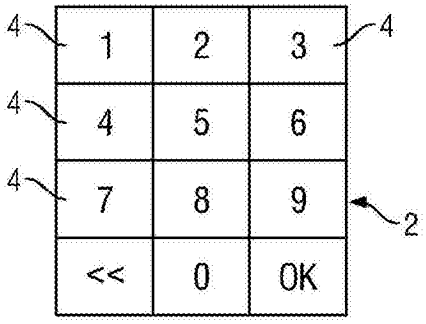


图11

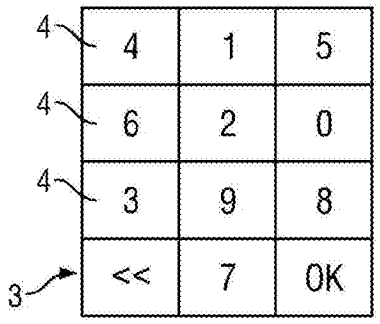


图12A

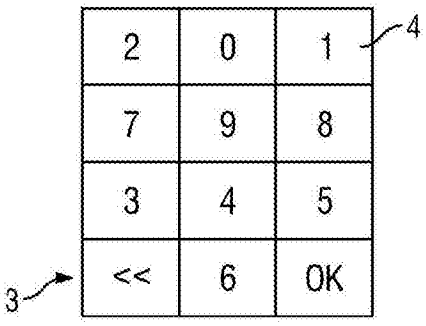


图12B

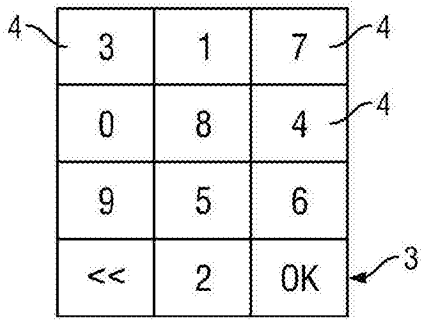


图12C

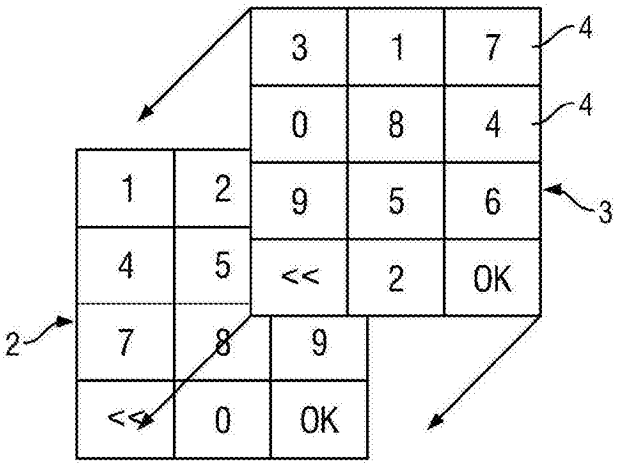


图13

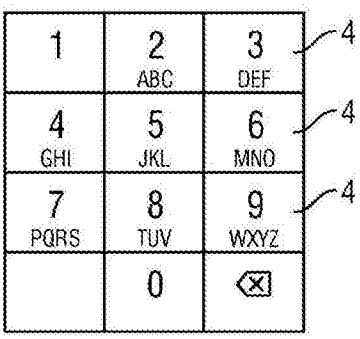


图14A(现有技术)

图14B(现有技术)

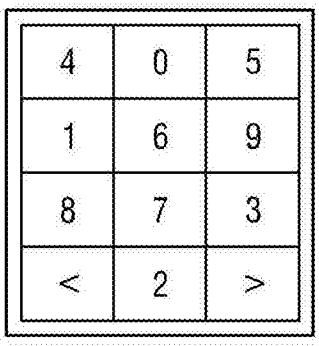


图15A

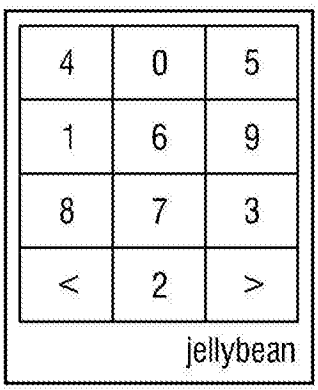


图15B

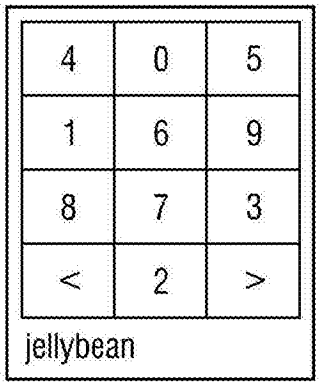


图15C

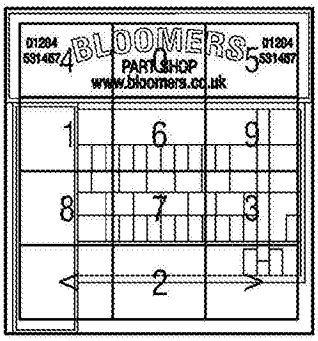


图15D

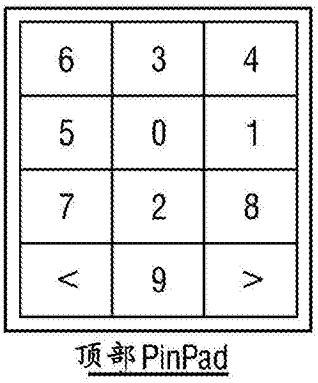


图16A

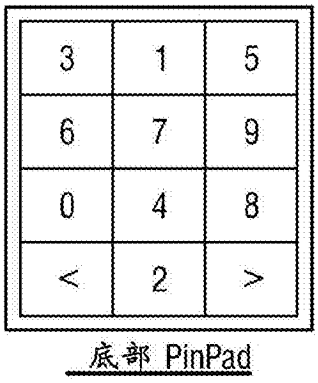


图16B

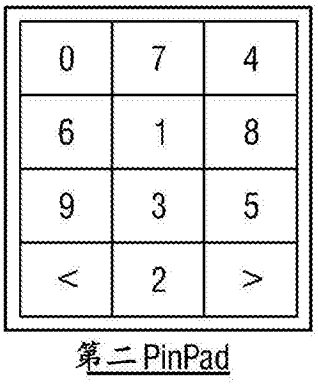


图16C

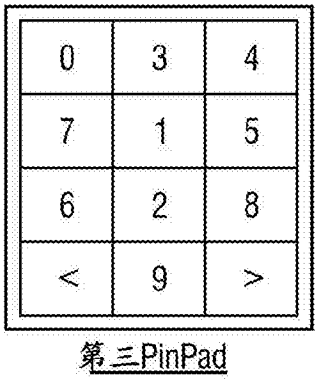


图16D

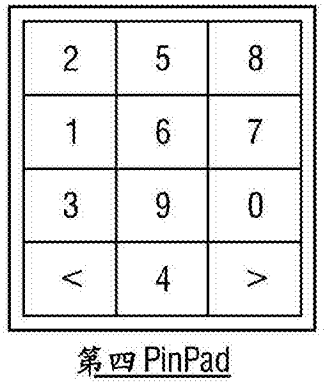

2 5 8
1 6 7
3 9 0
< 4 >
第四 PinPad

图16E

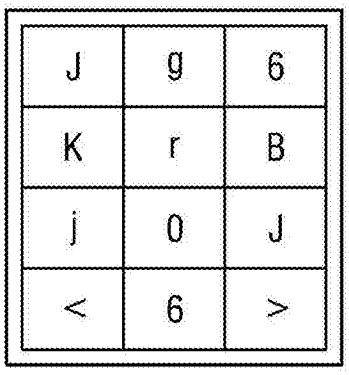

J g 6
K r B
j 0 J
< 6 >

图17

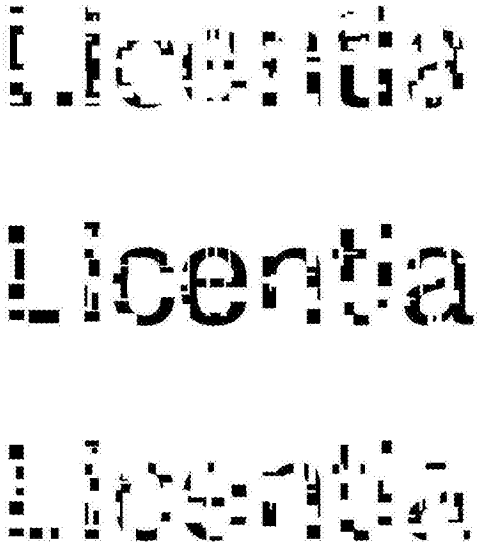

Licentia
Licentia
Licentia

图18

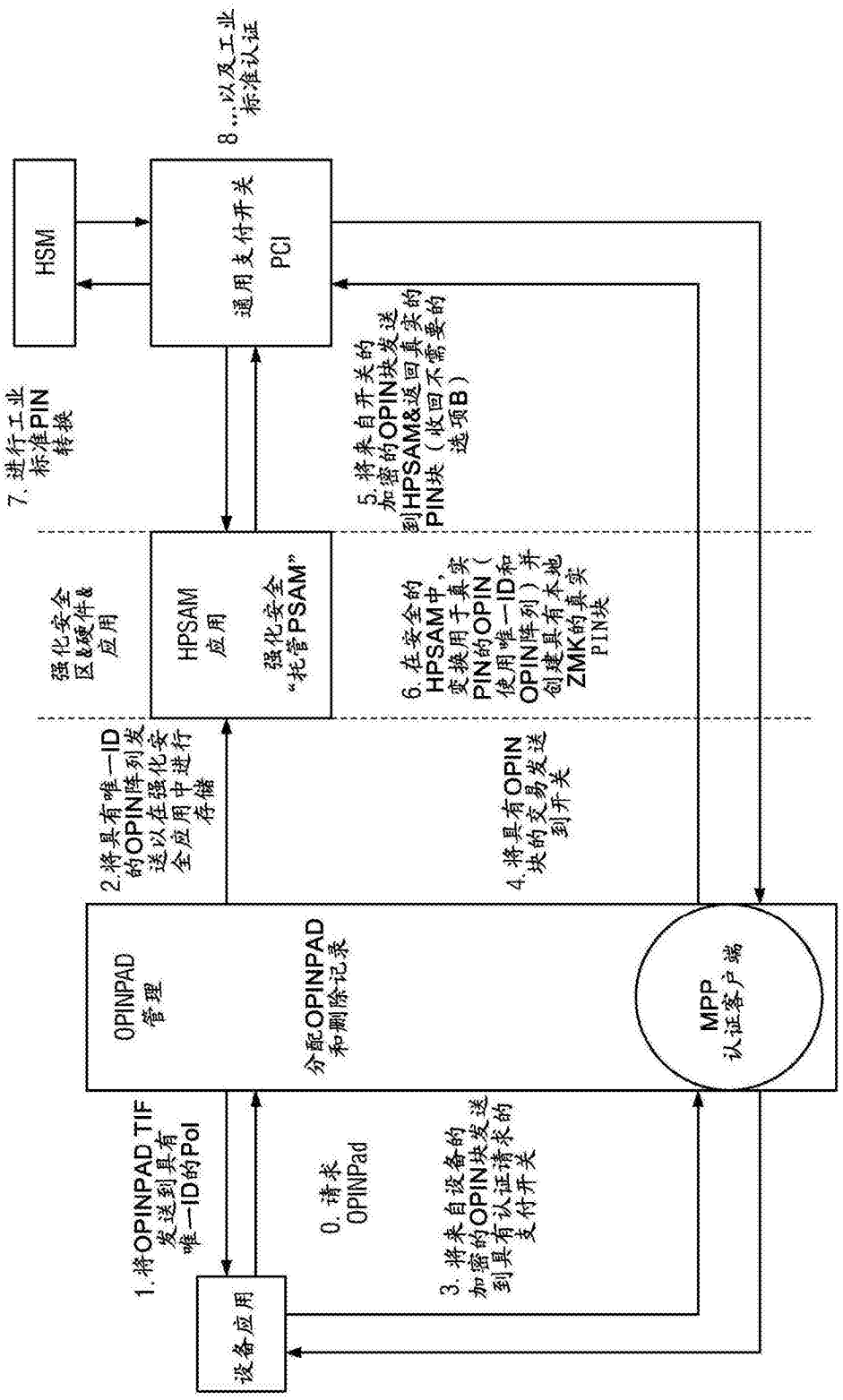

8...以及工业标准认证
HSM
通用支付开关 PCI
7. 进行工业标准PIN转换
5. 将来自开关的加密的OPIN块发送到HPSAM&返回真实的PIN块（收回不需要的选项B）
强化安全区&硬件&应用
HPSAM 应用
强化安全“托管PSAM”
6. 在安全的HPSAM中，实现用于真实PIN的OPIN（使用唯一ID和OPIN阵列）并创建具有本地ZMK的真实PIN块
2. 将具有唯一ID的OPIN阵列发送以在强化安全应用中进行存储
4. 将具有OPIN块的交易发送到开关
OPINPAD 管理
分配OPINPAD和删除记录
MPP 认证客户端
1. 将OPINPAD TIF发送到具有唯一ID的PoI
0. 请求OPINPad
3. 将来自设备的加密的OPIN块发送到具有认证请求的支付开关
设备应用

图19