[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/60

[12] 发明专利申请公开说明书

[21] 申请号 02826019.8

[43] 公开日 2005 年 4 月 27 日

[11] 公开号 CN 1610911A

[22] 申请日 2002.11.19 [21] 申请号 02826019.8

[30] 优先权

[32] 2001.11.19 [33] US [31] 60/333,035

[86] 国际申请 PCT/US2002/037048 2002.11.19

[87] 国际公布 WO2003/044721 英 2003.5.30

[85] 进入国家阶段日期 2004.6.24

[71] 申请人 小罗伯特·L·伯切特

地址 美国南卡罗来纳州

[72] 发明人 小罗伯特·L·伯切特

[74] 专利代理机构 北京市柳沈律师事务所

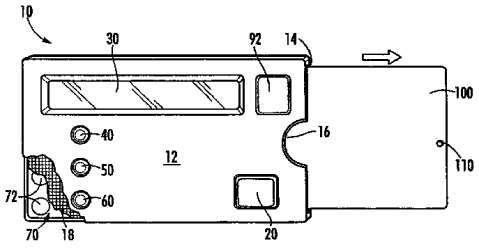
代理人 吕晓章 马 莹

权利要求书 5 页 说明书 11 页 附图 7 页

[54] 发明名称 具有防止未经授权的使用的安全性的交易卡系统

[57] 摘要

一种具有主机的系统，所述主机具有关于至少一个交易卡帐户的信息。 所述主机用于向在主机内承载的靶标卡传送卡数据。 所述主机包括生物统计传感器或用于在使用靶标卡之前验证用户的其他适当识别器件。 一旦用户被验证，则靶标卡提供与由用户选择的交易卡帐户对应的可读标识符。 主机的功能可选地可以被集成到靶标卡中。



ISSN1008-4274

1. 一种交易卡系统，所述系统包括:

存储器，被配置用来存储关于至少一个交易卡的帐户信息;

输出电路，被配置用来生成与存储在所述存储器中的交易卡对应的可读标识符;

用户输入器件，被配置用来选择存储在所述存储器中的交易卡;

处理器，其操作地连接至所述存储器、输出电路和用户输入器件，其中所述输出电路响应于从所述用户输入器件接收的输入而生成可读标识符。

2. 按照权利要求 1 的系统，还包括与所述处理器操作连接的安全输入器件，其中所述安全输入器件根据由该安全输入器件接收的输入来限制对存储在所述存储器中的帐户信息的访问。

3. 按照权利要求 2 的系统，其中所述安全输入器件是验证传感器。

4. 按照权利要求 3 的系统，其中所述验证传感器是生物统计传感器。

5. 按照权利要求 3 的系统，其中第一用户根据由所述验证传感器接收的输入来访问存储在所述存储器中的第一组帐户信息，第二用户根据由所述验证传感器接收的输入来访问存储在所述存储器中的第二组帐户信息。

6. 按照权利要求 5 的系统，其中所述验证传感器是指纹传感器。

7. 按照权利要求 1 的系统，其中由所述输出电路产生的所述可读标识符是磁信号。

8. 按照权利要求 1 的系统，其中由所述输出电路产生的所述可读标识符是条形码。

9. 按照权利要求 1 的系统，其中所述可读标识符包括保密码。

10. 按照权利要求 9 的系统，其中所述保密码对于每个交易是不同的。

11. 按照权利要求 9 的系统，其中所述保密码对于每个交易顺序地改变。

12. 按照权利要求 9 的系统，其中所述保密码是基于加密算法的。

13. 按照权利要求 1 的系统，还包括操作地连接到所述处理器的状态指示器，所述状态指示器被配置为在禁止状态和激活状态之间转换，其中当所述输出电路生成可读标识符时，所述状态指示器变为激活的。

14. 按照权利要求 13 的系统，其中所述状态指示器在被读卡器读取后变为禁止的。

15. 按照权利要求 13 的系统，其中当在所述输出电路产生可读标识符后经过预定时间时，所述状态指示器变为禁止的。

16. 按照权利要求 13 的系统，其中所述状态指示器是当该状态指示器激活时被点亮的灯。

17. 按照权利要求 13 的系统，其中所述状态指示器是这样的灯，它在所述状态指示器被激活时点亮第一种颜色，在所述状态指示器被禁止时点亮第二种颜色。

18. 按照权利要求 13 的系统，其中所述状态指示器在该状态指示器被激活时提供第一种可听的声音，在该状态指示器被禁止时提供第二种可听的声音。

19. 按照权利要求 1 的系统，还包括操作地连接到所述处理器的接口，用于下载帐户信息。

20. 按照权利要求 1 的系统，还包括操作地连接到所述处理器的显示器，所述显示器响应于所述用户输入器件而显示存储在所述存储器中的帐户信息。

21. 一种交易卡系统，所述系统包括:

靶标卡，其具有靶标存储器、靶标接口和输出电路，所述输出电路被配置为生成与存储在所述靶标存储器中的帐户信息对应的可读标识符;

主机，其具有用于接收所述靶标卡的插槽，所述主机包括:

主机存储器，被配置为存储至少一个交易卡的帐户信息，

主机接口，被配置为与所述靶标接口通信以向所述靶标卡传送帐户信息，

生物统计传感器;

处理器，操作地连接到所述主机存储器、所述主机接口和所述生物统计传感器，其中，当已经经由所述生物统计传感器验证了用户时，所述主机向所述靶标存储器传送帐户信息。

22. 按照权利要求 21 的系统，其中所述生物统计传感器是指纹传感器。

23. 按照权利要求 21 的系统，其中第一用户根据由所述生物统计传感器接收的输入来访问存储在所述主机存储器中的第一组帐户信息，第二用户根据由所述生物统计传感器接收的输入来访问第二组帐户信息。

24. 按照权利要求 21 的系统，其中由所述靶标卡的所述输出电路生成的

所述可读标识符是磁信号。

25. 按照权利要求 21 的系统，其中由所述靶标卡的所述输出电路生成的所述可读标识符是条形码。

26. 按照权利要求 21 的系统，其中由所述靶标卡生成的所述可读标识符包括保密码。

27. 按照权利要求 26 的系统，其中所述保密码对于每个交易是不同的。

28. 按照权利要求 26 的系统，其中所述保密码对于每个交易顺序地改变。

29. 按照权利要求 26 的系统，其中所述保密码是基于加密算法的。

30. 按照权利要求 21 的系统，其中所述靶标卡还包括状态指示器，该状态指示器被配置为在禁止状态和激活状态之间转换，其中当所述靶标卡的所述输出电路生成可读标识符时，所述状态指示器变为激活的。

31. 按照权利要求 30 的系统，其中当在所述输出电路生成可读标识符后经过预定时间时，所述状态指示器变为禁止的。

32. 按照权利要求 30 的系统，其中所述状态指示器是当该状态指示器激活时被点亮的灯。

33. 按照权利要求 21 的系统，其中所述靶标接口和所述主机接口使用电触点来通信。

34. 按照权利要求 21 的系统，其中所述靶标接口和所述主机接口使用无线通信来通信。

35. 按照权利要求 21 的系统，其中所述靶标接口和所述主机接口使用激光通信来通信。

36. 按照权利要求 21 的系统，其中所述靶标接口和所述主机接口使用红外线通信来通信。

37. 按照权利要求 21 的系统，其中所述靶标卡还包括显示器，所述显示器根据从所述主机的生物统计传感器接收的生物统计信息来显示用户的照片。

38. 按照权利要求 21 的系统，其中所述主机包括太阳能电池来作为电源。

39. 按照权利要求 38 的系统，还包括操作地连接到所述太阳能电池的光放大器。

40. 按照权利要求 39 的系统，其中所述光放大器是覆盖在所述太阳能电池上的至少一个棱镜。

41. 按照权利要求 21 的系统，其中所述主机包括反篡改装置，用于在所述主机被损害时擦除所述主机存储器。

42. 按照权利要求 21 的系统，其中所述靶标卡包括反篡改装置，用于在所述靶标卡被损害时擦除所述靶标存储器。

43. 按照权利要求 21 的系统，其中所述靶标卡具有与标准信用卡大致相同的厚度。

44. 按照权利要求 43 的系统，其中所述主机具有标准信用卡的厚度的大致三倍的厚度。

45. 按照权利要求 21 的系统，还包括登记器，该登记器具有用于与所述主机通信以便向所述主机存储器中存储帐户信息的接口。

46. 按照权利要求 45 的系统，其中所述登记器具有卡状部分，该卡状部分被配置为在所述主机的插槽内接收。

47. 按照权利要求 46 的系统，其中所述主机被配置为在防止使用所述主机的禁止状态和允许使用所述主机的激活状态之间进行转换，所述系统还包括具有用户输入器件的登记器，其中所述主机响应于从所述登记器的所述用户输入器件接收的输入而转换到所述激活状态。

48. 按照权利要求 21 的系统，还包括用户输入器件，它被配置为选择在所述主机存储器中存储的关于交易卡的帐户信息。

49. 一种交易卡系统，所述系统包括:

靶标卡，其具有靶标存储器、靶标接口和用于生成与存储在所述靶标存储器中的帐户信息对应的可读标识符的装置;

用于存储与至少一个交易卡对应的帐户信息的装置;

用于根据生物统计数据来限制对所述帐户信息的访问的装置;

操作地连接到所述靶标接口的装置，用于向所述靶标存储器传送由用户选择的交易卡的帐户信息。

50. 一种用于登记交易卡系统的方法，所述方法包括步骤:

(a)向用户传送靶标卡和被禁止的主机;

(b)从所述用户接收通信;

(c)要求所述用户回答至少一个安全问题;

(d)在满意地完成步骤(c)后，向所述用户提供将激活所述主机的保密码。

51. 按照权利要求 50 的方法，其中所述步骤(b)的通信是电话呼叫。

52. 按照权利要求 50 的方法，其中用帐户信息对所述主机进行了预编程。

53. 按照权利要求 50 额方法，其中在步骤(a)中还发送具有用户输入器件的登记器。

54. 按照权利要求 53 的方法，其中所述用户向所述登记器的用户输入器件输入所述保密码以激活所述主机。

55. 按照权利要求 54 的方法，其中所述登记器在激活所述主机后变为禁止。

具有防止未经授权的使用的安全性的交易卡系统

技术领域

本发明一般地涉及一种交易卡领域。具体上，本发明涉及具有用于防止未经授权的使用的安全特征的改进的交易卡系统。

背景技术

诸如信用卡、付款卡(debit card)和赊购卡(access card)等的交易卡已经获得了广泛的使用。虽然交易卡为用户提供了方便，但是欺骗性使用也盛行。欺骗性使用可以通过邮寄偷盗、伪造和通过偷窃的卡而发生。相信信用卡公司每年由于欺骗而遭受了几百万美元的损失。这些损失最终必然以更高的价格来由消费者承受。

虽然已经有防止欺骗性使用交易卡的尝试，但是存在对于新颖的交易卡系统的进一步的需要。

发明内容

本发明识别和处理现有技术结构和方法的各种缺点。因此，本发明的目的在于提供一种具有用于防止未经授权的使用的安全特征的改进的交易卡系统。

本发明提供了一种具有主机的系统，所述主机具有关于至少一个交易卡帐户的信息。所述主机用于向在主机内承载的靶标卡(drone card)传送卡数据。所述主机包括生物统计(biometric)传感器或用于在使用靶标卡之前验证用户的其他适当的识别手段。一旦用户得到了验证，则靶标卡提供对应于由用户选择的交易卡帐户的可读标识符。本领域内普通技术人员应当明白主机的功能可选地可以被集成到靶标卡中。

通过下面更详细讨论的、所公开的元件的各种组合和子组合，可以实现本发明的其他目的、特征和方面。

附图说明

参考附图，在说明书的剩余部分中，对于本领域内普通技术人员，更具体地给出了本发明的全面和允许的公开——包括其最佳方式，其中：

图 1A 是按照本发明的一个实施例的主机和被插入的靶标卡的前透视图，其中主机具有部分被切除的一部分，用于显露其中的各种内部部件；

图 1B 是图 1A 的主机和靶标卡的透视图，示出了从主机中取出靶标卡；

图 1C 是沿着图 1A 的线 1C-1C 的主机的侧视图；

图 1D 是沿着图 1A 的线 1D-1D 的主机的一部分的横断面视图；

图 2 是图 1A-C 的主机的各种功能部件的图示；

图 3A 是诸如可以用于图 1A-C 的主机的靶标卡的前视图；

图 3B 是图 3A 的靶标卡的后视图；

图 4 是图 3A 和 3B 的靶标卡的各种功能部件的图示；

图 5 是按照本发明的一个实施例的、与主机连接的登记器(enroller)的图示；

图 6 是图解验证过程的流程图；

图 7 是由当前广泛使用的类型的信用卡读取器正在扫描的靶标卡的透视图；

图 8 是示出用于靶标卡的交易尝试的表格；

图 9A 是按照一个替代实施例的编码卡的前视图；

图 9B 是图 9A 的编码卡的后视图；

图 9C 是沿着图 9A 的线 9C-9C 的卡的一部分的横截面图；

图 10 是按照一个替代实施例的登记器的透视图；

图 11 是在主机内接收的图 10 的登记器的透视图；和

图 12 是示出按照图 10 和 11 的实施例的登记过程的流程图。

在本说明书和附图中对附图标号的重复使用是用来表示本发明的相同或类似的特征或元件。

具体实施方式

详细说明本发明的当前优选实施例，在附图中对其一个或多个示例进行图解说明。通过说明本发明而不是限定本发明来提供每个示例。事实上，对本领域内的技术人员显然的是，可以在不脱离本发明的范围或精神的情况下在本发明中进行各种修改和改变。例如，可以对另一个实施例使用被图解或

描述为一个实施例的一部分的特征，以得到另一个实施例。

在一个实施例中，本发明提供了一种用于容纳关于一个或多个卡帐户的信息的主机。卡帐户包括但是不限于信用卡、付款卡、借书卡、社会保障卡、医疗保险卡、电话卡、赊购卡、折扣卡和包括与特定人或组相关联的识别信息的任何其他卡。在主机内承载的靶标卡可以被配置为对应于卡帐户。经常地，主机可以被配置为使得用户从几个卡帐户中选择特定的卡帐户。登记器进行工作，对用于个人或组的、在主机上的各种卡帐户的信息进行编程。

一旦被登记器初始化，则主机包括用于验证所需要的用户信息以及与卡帐户相关联的数据。为了使用在主机上存储的特定卡帐户，首先使用主机的验证传感器来验证用户。在选择期望的卡帐户时，主机向靶标卡上载与所选择的卡帐户相关联的数据。靶标卡可以包括输出电路，它用于生成对应于所选择的卡帐户的可读标识符(即磁信号、条形码等)。除非在某个时段内使用靶标卡，否则它最好将变得无效和需要使用另外的验证。同样，在完成交易后，靶标卡可以变得无效。

图 1A、1B 和 1C 图解了按照本发明的承载靶标卡 100 的主机 10。主机 10 具有正面 12 和用于接收靶标卡 100 的插槽 14。优选的是，主机 10 是由较为坚硬的材料形成的，并且仅仅是用于接收靶标卡 100 和容纳必要的电子元件所需要的那么厚。通常，主机 10 将具有标准信用卡厚度的大约三倍的厚度。虽然示出插槽 14 在主机 10 的短侧，但是应当明白可以沿着主机 10 的任何一侧来定位插槽 14。例如，在一些情况下可以期望沿着主机 10 的长边来定位插槽 10，以便使得用左或右手的人都能够更容易地取出靶标卡 100。接近插槽 14 的切除部分 16 使得可以通过用户的手指来拿取靶标卡 100，以便于从主机 10 中取出该靶标卡。主机 10 也可以被集成到其他的电子设备，诸如蜂窝电话或个人数字助理(PDA)。

主机 10 的内部可以包括适当的防止篡改机构，以用于防止有人试图获得存储在主机中的帐户信息。例如，主机 10 的所图解的实施例包括就在其表面之下的金属丝细网孔 18。网孔 18 的金属丝可以串行联接，以使网孔的任何损伤将删除在主机 10 中存储的所有数据。可以明白，打开主机 10 的企图将导致网孔的损伤。

主机 10 最好包括集成安装的验证传感器 20，用于验证用户的识别信息。验证传感器 20 最好是适当的生物统计传感器，诸如指纹传感器。一种已知的

可以用于此目的的指纹传感器为 FINGERLOC™，由佛罗里达的墨尔本的 AuthenTec 公司销售。应当明白，验证传感器 20 可以是用于验证用户的识别信息的任何其他适当的器件，诸如个人识别号码(PIN)键盘。

在所图解的实施例中，主机 10 包括显示器 30，它使得用户可以查看与存储在主机 10 上的各种卡帐户相关联的信息。虽然显示器 30 最好是字符液晶显示器(“LCD”)，但是也可以使用任何其他适当的显示器。用于驱动具有特定字符的 LCD 的方法是本领域内公知的。

被安装在主机 10 的正面 12 上的滚动按钮 40 使得用户可以滚动遍及用户访问的主机 10 上存储的各种卡帐户的名称。当用户滚动遍及卡帐户的名称时，每个卡帐户可以被显示在显示器 30 上。一旦用户确定要使用的具体卡帐户时，则使用输入按钮 50 来选择所期望的卡帐户。如下所详细描述的，与所选择的卡帐户对应的信息随后与保密码--起被上载到靶标卡 100。也可以通过选择显示按钮 60 在显示器 30 上查看关于特定卡帐户的信息。应当明白，显示滚动按钮 40、输入按钮 50 和显示按钮 60 可以形成为滑动开关或其他用户输入器件。

主机 10 包括接口 70，用于从登记器 200(图 5)下载用户数据并且向靶标卡 100 上载卡数据。卡数据包括对应于特定卡帐户的数据，而用户数据包括验证用户所需要的信息(诸如指纹图像)以及用于与用户相关联的每个卡帐户的卡数据。考虑到用于交换数据的多种器件和技术，可以以多种方式来实现所述接口，诸如使用电触点、红外通信或激光通信。如果仅仅想将单个卡帐户传送到靶标卡 100，则主机 10 可以在靶标卡 100 上永久地写入帐户数据。对于电触点接口，主机 10 包括内部电触点 72，它能够与在登记器 200 和靶标卡 100 上的电触点连接。登记器 200 最好包括可以被插入插槽 14 中的卡状连接器，用于向主机 10 提供必要数据。

现在参见图 2，主机 10 具有内部微处理器 80，它与机载存储器 82 进行电通信。最好是适当的 EEPROM 的存储器 82 用于存储卡数据、用户数据和保密码(下面将更全面地说明)。电源 90(最好是电池)向微处理器 80 和存储器 82 提供电源。优选的是，超薄电池将被用于这个目的，诸如由以色列的 Kibbutz Einat 的 Power Paper 有限公司销售的电池。电源 90 可以是可充电的，并且使用太阳能电池 92 来接收辅助的充电。可选的指示灯(未示出)也可以指示何时电池的电量低。

可以选则性地提供装置来扩大或放大可以用于太阳能电池92的环境光。例如，在一个实施例中，光学棱镜93可以被模压到主机10的正面12中，以便覆盖在太阳能电池92上，如图1D所示。本领域内的普通技术人员应当明白适当的光放大器的配置和选择。为了提高电池寿命，微处理器80最好保持在“休眠”模式中，直到被验证传感器20或滚动按钮40激活。术语“休眠”模式指的是由微处理器保持的、直到被输入中断的低功率状态。

验证传感器20、滚动按钮40、输入按钮50和显示按钮60向微处理器80提供输入数据。接口70也向微处理器80提供输入数据，并且接收输出数据。微处理器80响应于输入数据而工作。

微处理器80通过将输入数据与存储在存储器82中的用户数据进行比较以确定输入数据是否表示有效用户，来响应来自验证传感器20的输入数据。多个用户可以与一个主机相关联；因此用于主机的用户数据可以对应于多个人。例如，如果验证传感器20是指纹传感器，则与主机10相关联的每个人的指纹将提供对所选择的存储在主机10上的卡帐户的访问。

参见图6，在验证用户中的第一步骤是诸如通过扫描用户的指纹来从验证传感器20中读取用户输入数据。接着，主机将由验证传感器20扫描的数据和存储在主机的存储器中的数据进行比较。如果扫描的数据与存储在存储器中的用户数据不匹配，则不允许用户访问卡帐户。或者，如果扫描的数据与存储在存储器中的用户数据相匹配，则向用户提供对于用户访问的所有卡帐户的访问。

不是每个与主机相关联的用户必然可以访问存储在主机上的每个卡帐户的。主机可以提供多个安全等级以限制某些用户访问某些卡帐户。例如，考虑包括指纹传感器来作为其验证传感器的主机，它将卡数据以及用于“用户A”和“用户B”的数据存储在用于“卡A”(例如VISA)和“卡B”(例如American Express)的存储器中。因此，“用户A”和“用户B”都可以使用它们的指纹来激活主机。根据在这个示例中的用户数据，“用户A”相关联于并且可以访问“卡A”而不是“卡B”。当“用户A”滚动遍及主机上的可用卡时，仅仅显示“卡A”。但是，用户数据将“用户B”与“卡A”和“卡B”相关联。结果，“用户B”可以查看和使用“卡A”和“卡B”。

在验证时，微处理器80通过使用在与用户相关联的用户数据中的下一个卡帐户的标识来驱动显示器30从而对来自滚动按钮40的输入作出响应。通

过继续选择滚动按钮，用户可以查看用户访问的主机 10 上存储的卡帐户的全体列表。响应于来自显示按钮 60 的输入，微处理器 80 显示保密码以及所选择的卡帐户的卡数据(例如帐号)。微处理器 80 通过经由接口 70 向靶标卡 100 上载卡数据和保密码来响应于来自输入按钮 50 的输入。可选地，靶标卡 100 可以具有包含卡数据的存储器，以便仅仅向靶标卡 100 上载保密码。

保密码是与卡帐户和交易相关联的唯一代码。虽然卡帐户保持恒定，但是通常对于每个交易，保密码是不同的。如果有人试图再次使用保密码，则交易将被拒绝，作为未经授权。例如，如果所选择的卡帐户是电话卡，则电话公司将不批准记帐，除非提供了卡帐号和预期的保密码。如果第三方截取卡号码和以前的保密码以供以后使用，则电话公司将拒绝记帐。在图 8 的表格中图解说明了这个批准处理。

保密码最好是根据在主机上驻留的算法而生成的 4 数字的字母数字码。例如，保密码可以根据在主机 10 上驻留的内部时钟而随机地改变。保密码可以在诸如 20 秒的某个时间间隔期间改变，以提供提高的安全性。用于验证保密码的中央计算机将与主机同步以识别保密码。或者，多个保密码可以被存储在主机的存储器中。为了验证保密码，执行交易的读取器向发放实体的中央计算机提供当前的保密码，所述中央计算机随后查看与预期的代码的匹配。这个计算机被编程为预期在将要执行的下一个交易中的特定保密码。

可以在图 3A 和 3B 中看出，靶标卡 100 最好具有与标准信用卡类似的大小和厚度。但是，与包括对于查看信用卡的任何人可视的账号的信用卡不同，靶标卡 100 最好不包括可视信息，除了可选地包括与靶标卡相关联的用户或组的名称。可选地，在主机 12 或靶标卡 100 上提供被授权的用户的照片 102。照片 102 可以是被授权用户的永久的、静态的照片，或者可以是暂时显示被授权用户的电子照片的电子显示。如果使用电子照片，则将显示与由主机 100 授权的用户相对应的照片。因此，多个用户的多个照片可以被存储在主机 10 上，并且根据被授权的特定用户来向靶标卡 100 传送和显示适当的照片。

在处于激活状态的可读的标识符 130 处提供执行与靶标卡 100 的交易所需要的所有信息。在激活状态中，可读标识符 130 允许用户进行交易。在其他时间，可读标识符 130 将被禁止使用，从而不可进行交易。可以提供状态指示灯 110 来指示可读标识符 130 的状态。例如，状态指示灯 110 可以是在可读标识符被激活时点亮的绿色 LED。对于视觉受损的人，可以提供可听的

指示器来指示可读标识符 130 的状态的改变。

靶标卡 100 包括用于从主机 10 接收卡数据的接口 120。如上所述，因为存在多种用于交换数据的器件和技术，因此可以以多种方式来实现接口 120，诸如使用电触点、红外线或激光通信。对于电触点接口，靶标卡 100 包括能够与在主机 10 上的电触点 72 连接的电触点 122。

现在参见图 4，将说明靶标卡 100 的一个优选实施例的内部结构。在这种情况下，靶标卡具有与机载存储器 150 进行电通信的内部控制器 140，所述机载存储器 150 最好是易失性存储器。在这个实施例中，靶标卡 100 具有足够大小的存储器来存储保密码和卡数据。电源 160(最好是如上所述的超薄电池)向控制器 140 和存储器 150 提供电源。通过经由电流的连接、电感或其他适当的器件接收来自主机 10 的电力，电源 160 可以被重新充电。

如上所述，靶标卡 100 包括与控制器 140 进行电通信的接口 120，所述控制器用于传送从主机 10 接收的卡数据以存储在存储器 150 中。如前面所述，本领域包括多种用于传送数据的技术，诸如使用电触点、激光通信和红外线通信。

控制器 140 根据从主机 10 接收的卡数据来生成信号，以便激活可读标识符 130。优选的是，可读标识符 130 将呈现与诸如图 7 所示的传统的读卡器 165 的现有的读取器兼容的形式。例如，可读标识符 130 可以是在验证后被暂时激活的临时磁条或条形码显示。

为了产生临时磁条，靶标卡可以包括电矩阵以建立对应于卡帐户的磁信号。对于使用电矩阵来生成临时磁信号的讨论，参见通过引用被并入在此的、Krause 的美国专利第 6,089,451 号。

或者，可以使用位于靶标卡 100 内的磁粉或其他材料来生成可读标识符 130。主机 10 可以改变磁粉的物理位置或配置以生成各种可读标识符。例如，磁粉可以被定向以产生可以由标准读卡器读取的临时磁条。

或者，可读标识符 130 可以是 LCD 或其他适当的显示器，用于产生对应于卡数据的条形码。根据所述卡数据，主机 10 将向靶标卡 100 传送足以生成对应的条形码的数据以显示在 LCD 上。在可读标识符 130 上所示的条形码对于被传送到靶标卡 100 的每个卡帐户将是不同的。

取代以这种类型的靶标卡 100 来使用磁卡读取器，条形码读取器可以扫描靶标卡。例如，如果驻留在靶标卡的存储器中的卡帐户是信用卡，则对应

于信用卡的条形码将被显示为可读标识符。条形码读取器将读取所述可读标识符，并且与必要的信用管理机构通信以管理适当的帐户。

如上所述，状态指示灯 110 的状态指示靶标卡是否准备好使用。当卡数据被初始地传送到靶标卡 100 时，状态指示灯 110 可以变亮。在这样的实施例中，状态指示灯 110 将最好保持点亮直到可读标识符变为禁止使用。优选的是，可读标识符可以在下列情况下变为禁止使用：(1)在完成交易时或(2)在经过了某个时间段后。在许多实施例中，控制器 140 可以简单地移除至可读标识符的电力，以便禁止使用可读标识符。

靶标卡 100 可以包括交易传感器 170，用于检测何时已经尝试了与靶标卡的交易。例如，如果靶标卡被配置为通过磁读取器来进行扫描，则交易传感器 170 将检测由磁读取器对于靶标卡的扫描。一旦已经扫描了靶标卡，则可读标识符最好变得禁止使用。

在另一个实施例中，靶标卡 100 可以不包括内部电源。例如，靶标卡 100 可以被配置为具有诸如磁条的可读标识符，它不需要连续的电力来保持可读。在这样的实施例中，主机 10 将包括诸如磁头的输出电路，它向磁条写入卡帐户数据。当从主机 10 取出靶标卡 100 时，磁头可以向磁条写入卡帐户数据。也可以向靶标卡写入保密码。可以提供在主机 10 内的滚轴或生成器，以同步向靶标卡 100 上的数据写入。

现在参见图 5，登记器 200 用用户数据和卡数据(在一些情况下是保密码)来初始化主机 10。登记器 200 可以是独立的设备或通用计算机 300 的外围设备。在这个后一种情况下，登记器 200 经由接口 230 与计算机 30 通信。本领域内的技术人员将会明白，可以使用多种技术来实现接口 230，所述多种技术诸如串行线、无线通信或任何其他适当的数据传送技术。

通用计算机 300 包括用于收集用户数据的软件，包括收集验证用户所需要的信息。关于用户的一般信息，诸如姓名、地址、社会保障号等可以被键入通用计算机 300 中。登记器 200 包括用于收集验证用户所需要的信息的验证传感器 210。例如，如果主机 10 包括指纹传感器，则登记器 200 将从用户收集指纹图像。登记器 200 可以具有分离的指纹传感器来执行这个功能或使用在主机 10 上驻留的指纹传感器。登记器 200 也可以包括传感器 240，用于收集关于每个“卡”的将被存储在主机上的卡数据。传感器 240 可以是标准的交易卡读取器。

接口 220 向主机 10 传送用户数据(并且可能是保密码)。如前面所述，本领域包括多种用于传送数据的器件和技术。例如，登记器 200 可以使用在主机上的电触点来通信。

图 10-12 图解了登记器 500 的另一个实施例。在这个实施例中，登记器 500 可以具有卡状部分 502，它可以在主机 10 的插槽 14 中被接收。虽然应当明白整个登记器 500 可以具有卡状部分 502 的厚度，但是为了诸如耐用的目的，不在主机 10 内接收的部分可以较厚。登记器 500 包括用户输入器件 506，诸如键盘，用于向主机 10 输入解锁代码。登记器 500 还包括用于与主机 10 通信的接口(未示出)。登记器 500 能够以与靶标卡 100 类似的方式与主机 10 连接，诸如使用电触点、激光通信、红外线通信或其他通信手段。

在这个实施例中，可以将被禁止使用的主机 10 和靶标卡 100 与登记器 500 一起运送给用户。为了启动主机 10，用户必须从主机 10 和靶标卡 100 的发放者获得解锁代码。因此，用户将与主机 10 和靶标卡 100 的发放者通信以接收解锁代码。用户可以使用发放者的网站，或仅仅使用电话呼叫发放者来获得解锁代码。为了获得解锁代码，将要求用户回答一系列安全问题以验证用户。一旦对安全问题的答案满意，则发放者可以向用户发放解锁代码。在主机 10 中接收了登记器 500 的情况下，用户将向登记器 500 输入所述解锁代码，其将解锁主机 10。应当明白，主机 10 可以与特定登记器 500 相匹配。而且，登记器 500 可以被设计为一次使用，以防止在多个主机上使用一个登记器。

在主机 10 被启动的情况下，用户可以进行登记处理。例如，用户可以使用主机 10 的验证传感器 20 来建立帐户，并且向登记器 500 的用户输入器件 506 中键入卡帐户的信息。用于登记处理的指令可以显示在主机 10 的显示器 30 上。另外，登记器 500 可以包括数字照相机 508，用于向主机 10 传送用户的数字照片。

为了使用主机，必须使用验证传感器来验证用户。如果验证传感器是例如指纹传感器，则必须验证用户的指纹以访问存储在主机上的卡帐户。一旦被验证，则用户可以使用滚动按钮来显示用户访问的主机上存储的所有卡帐户的标识信息。一旦显示了所期望的卡帐户的标识信息，则用户可以使用显示按钮来显示用于所选择的“卡”的保密码和卡数据。为了向靶标卡上载卡数据和保密码，用户选择输入按钮。

一旦主机向靶标卡传送卡数据和保密码，则状态指示灯被点亮(如果靶标卡被加电和如此配备)。为了使用卡进行交易，用户从主机中取出卡，以使可读标识符被暴露给读取器。一旦可读标识符被暴露给读取器，则可读标识符最好变为禁止使用，并且状态指示灯关闭。如果在可读标识符被暴露给读取器之前经过了一定时间段，则可读标识符最好也变为禁止使用，并且状态指示灯关闭。用户随后向主机返回靶标卡，直到所述靶标卡需要用于另一个交易。可以明白，显示器允许看见账号和保密码，以便在必要时(诸如(很少)供应商没有适当的读卡器)可以通过电话呼叫来批准交易。

图 9A 和 9B 图解了一个替代实施例，其中前述的主机和靶标卡的功能被集成到编码卡 400 中。编码卡 400 最好与标准信用卡具有大致相同的厚度。

编码卡 400 最好包括集成安装的验证传感器 410，用于验证用户的识别信息。可以使用能够识别用户的任何适当传感器，诸如生物统计传感器。

可选地，在编码卡 400 上提供被授权用户的照片 402。照片 402 可以是被授权用户的永久的、静态照片，或可以是暂时显示被授权用户的电子照片的电子显示。如果使用电子照片，则将显示与被授权用户对应的照片。因此，用户的多个照片可以被存储在编码卡 400 上，并且根据被授权的特定用户来显示适当的照片。

编码卡 400 包括显示器 420，它使得用户可以查看与存储在编码卡 400 上的各种卡帐户相关联的信息。安装在编码卡 400 上的滚动按钮 430 使得用户可以滚动遍及用户访问的编码卡 400 上存储的各种卡帐户的名称。当用户滚动遍及卡帐户的名称时，在显示器 420 上显示出每一个。

一旦用户确定要使用的特定的卡帐户，则使用输入按钮 440 来选择期望的卡帐户。结果，可读标识符 480(图 9B)提供诸如在验证后被暂时激活的临时磁条或条形码显示的信号，它使得可以完成交易。在选择了期望的卡帐户后，指示灯 450 显示可读标识符的状态。如前面所述，指示灯指示可读标识符是被激活还是被禁止使用。交易传感器 490 可以被提供来检测何时已经尝试了与编码卡的交易。也可以通过选择显示按钮 470 在显示器 420 上查看关于特定卡帐户的信息。为了增加电池寿命，可以包括太阳能电池 460 以向编码卡 400 提供电源。可以提供棱镜 462 或其他适当的设备以增加可用于太阳能电池 460 的光，如图 9C 所示。

因此可以看出，本发明提供了一种具有新颖属性的交易卡系统。虽然已

经示出和描述了本发明的优选实施例，但是可以在不脱离本发明的精神和范围的情况下由本领域内的普通技术人员进行修改和改变。另外，应当明白，可以整体或部分地互换各个实施例的多个方面。而且，本领域内的普通技术人员可以明白，上述的说明仅仅是举例，而不是意欲限定本发明。

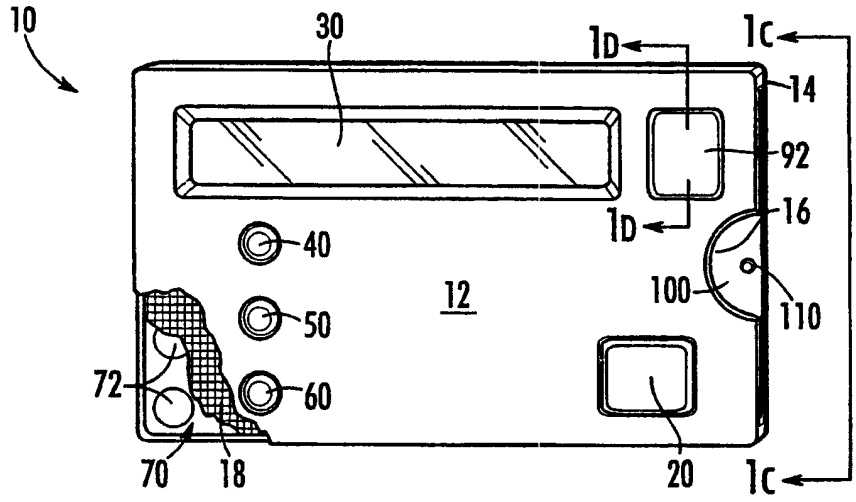


图 1A

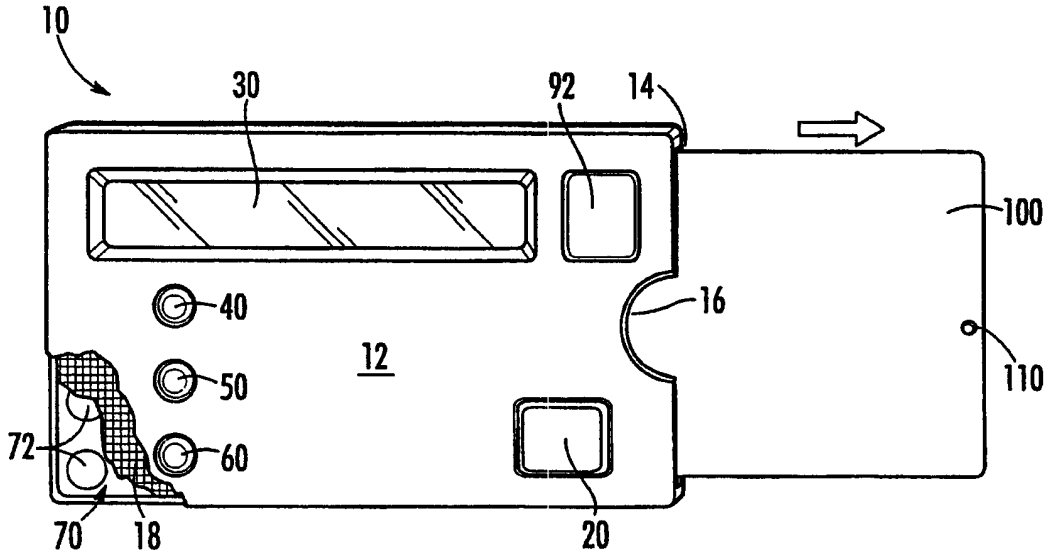


图 1B

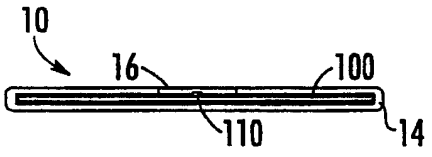


图 1C

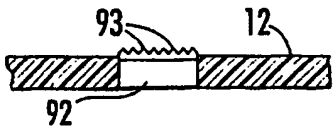


图 1D

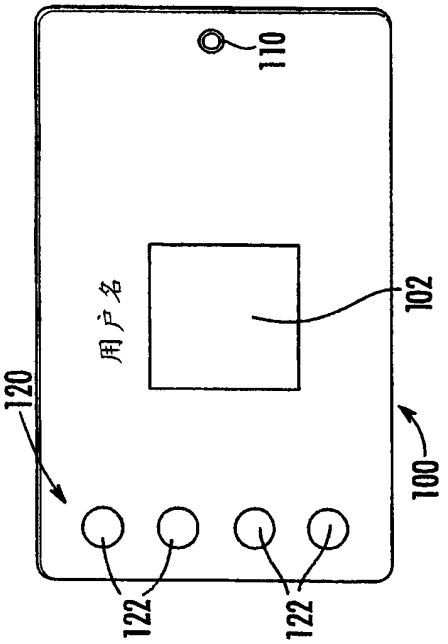

110
用户名
102
120
100
122
122

图 3A

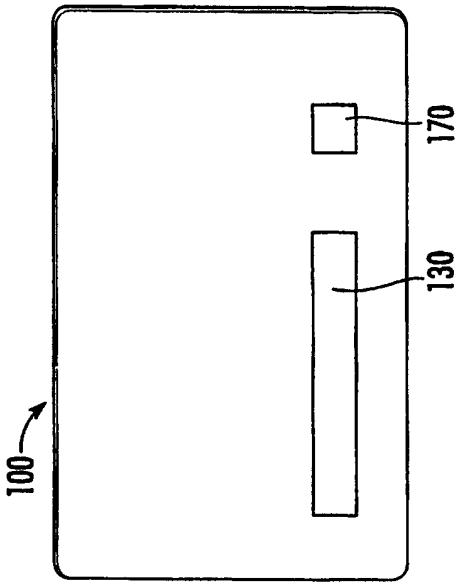

170
130
100

图 3B

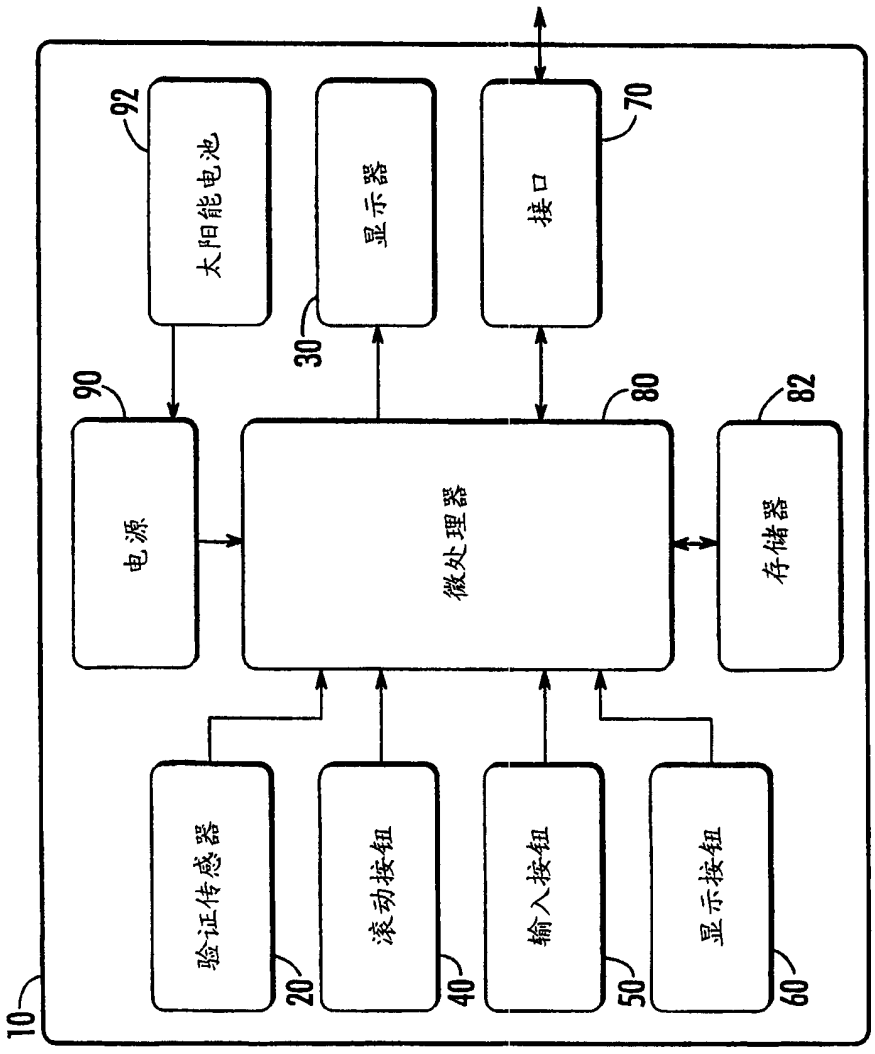

10
验证传感器
20
滚动按钮
40
输入按钮
50
显示按钮
60
电源
90
微处理器
80
存储器
82
太阳能电池
92
显示器
30
接口
70

图 2

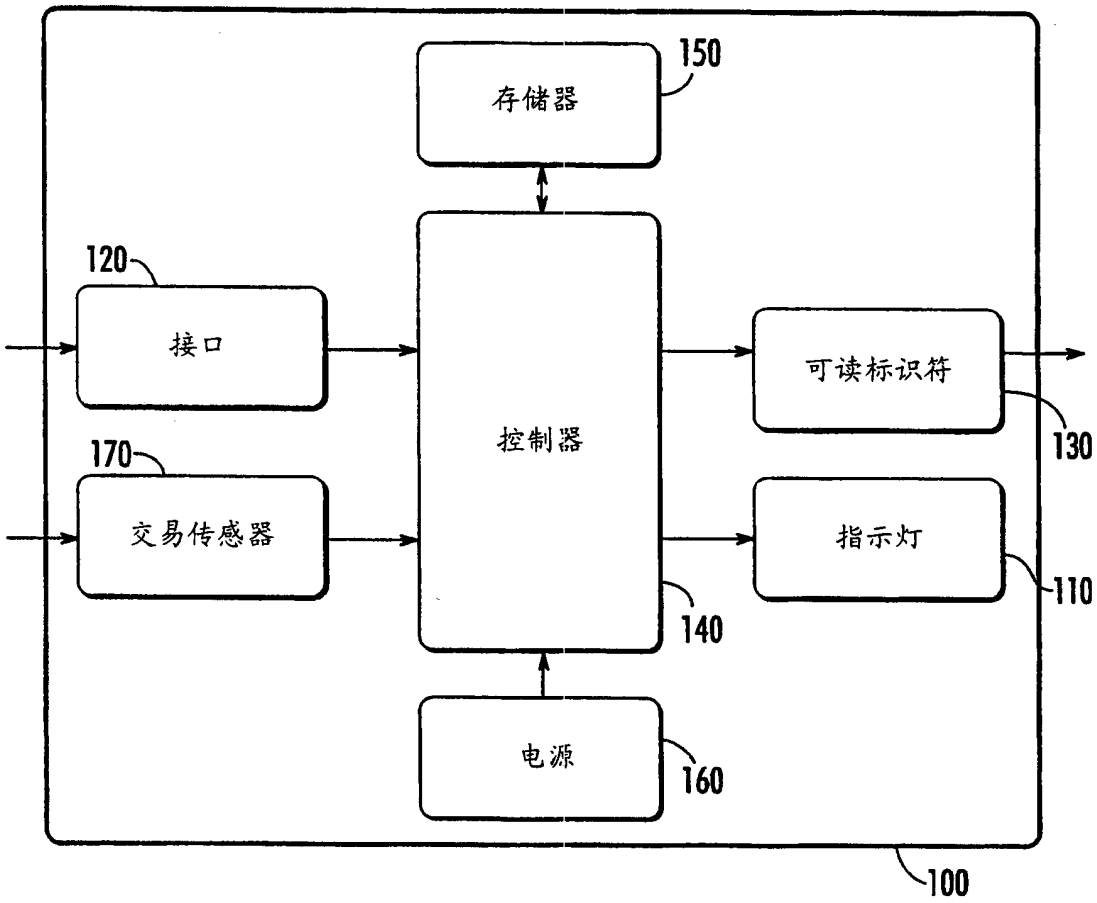

存储器
150
120
接口
控制器
可读标识符
130
170
交易传感器
指示灯
110
140
电源
160
100

图 4

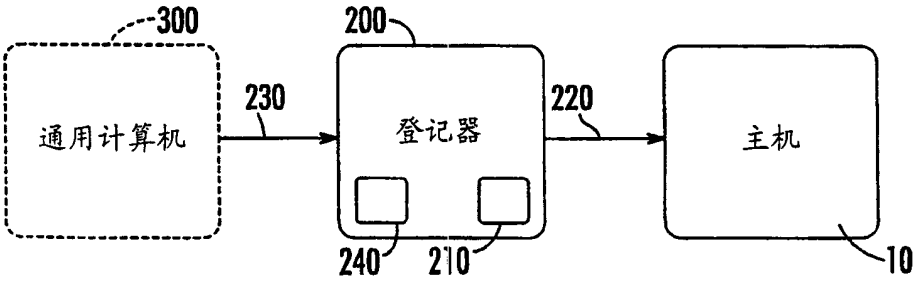

300
200
通用计算机
230
登记器
220
主机
240
210
10

图 5

图 6

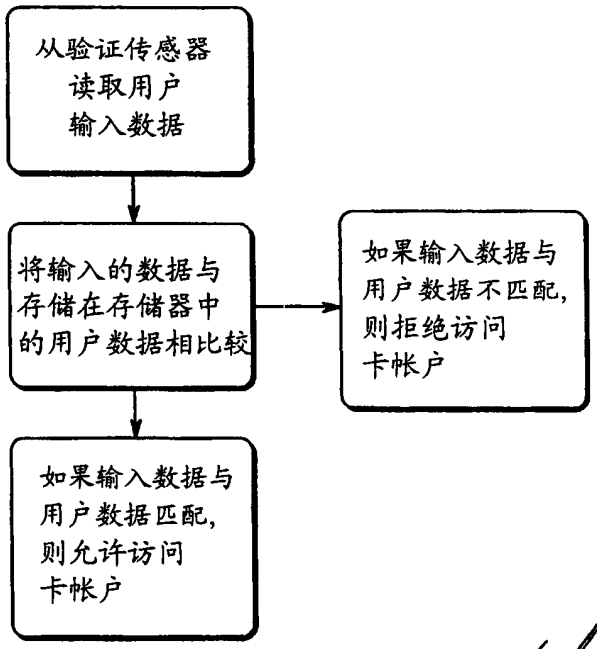
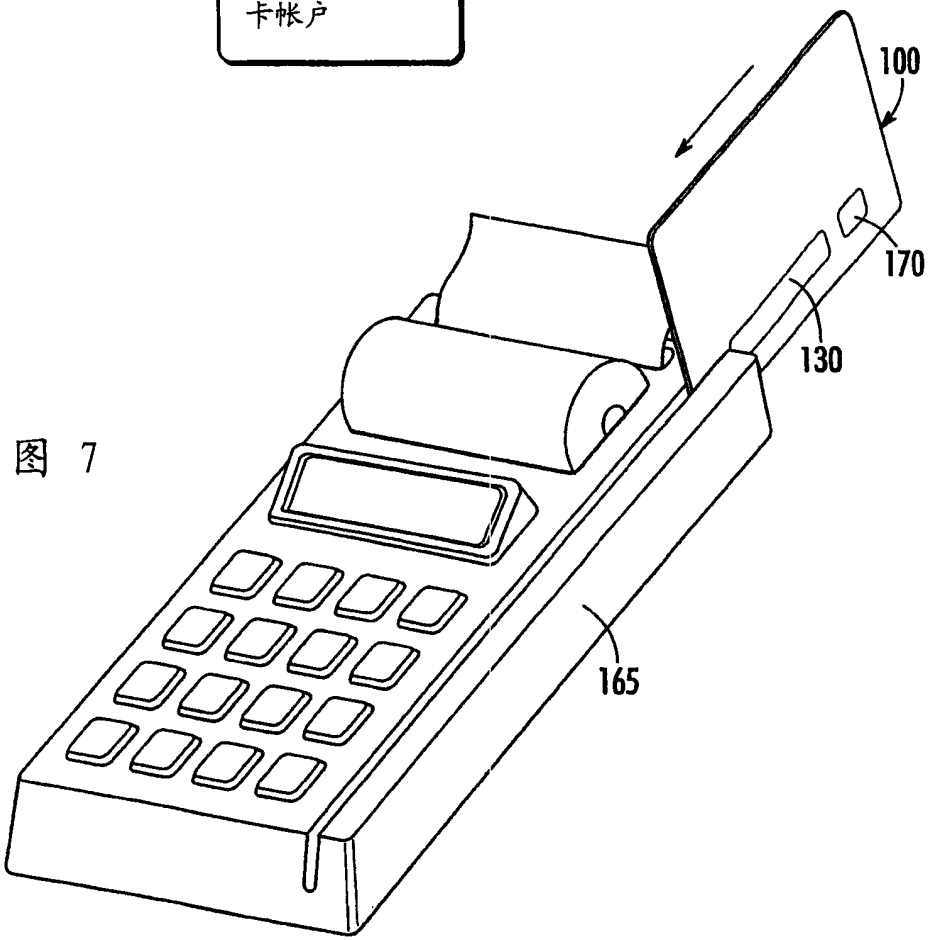

从验证传感器
读取用户
输入数据
将输入的数据与
存储在存储器中
的用户数据相比较
如果输入数据与
用户数据不匹配,
则拒绝访问
卡帐户
如果输入数据与
用户数据匹配,
则允许访问
卡帐户

图 7


100
170
130
165

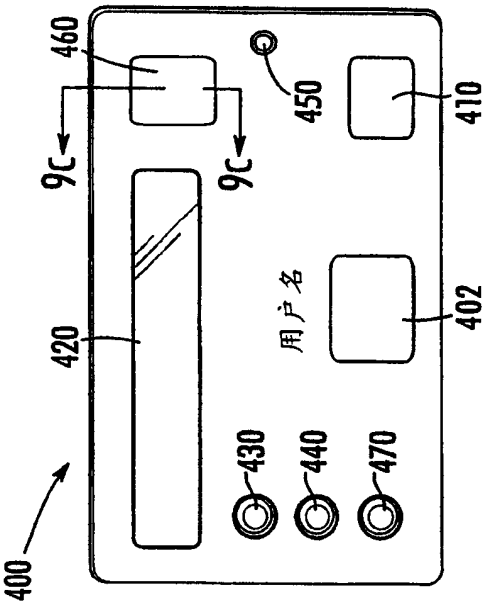


图 9A

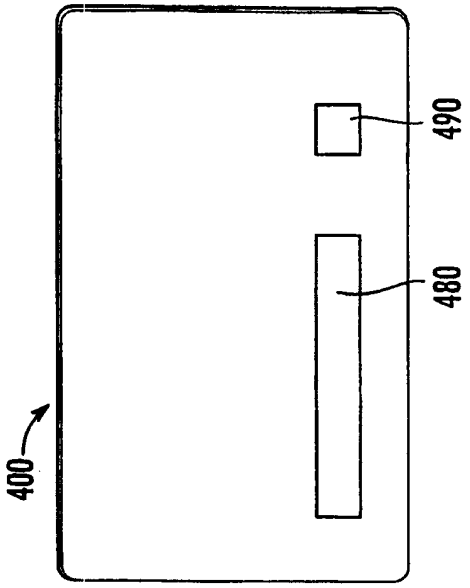


图 9B

预期的保密码	盗取的保密码	匹配 是/否
1234	1234	是
4582	4582	是
3657	3657	是
9878	9878	是
2464	4462	否
2255	2256	否
5746	7657	否
•	•	•
•	•	•
•	•	•
•	•	•

图 8

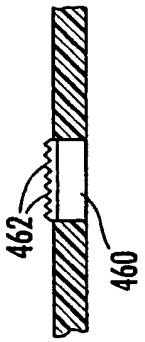


图 9C

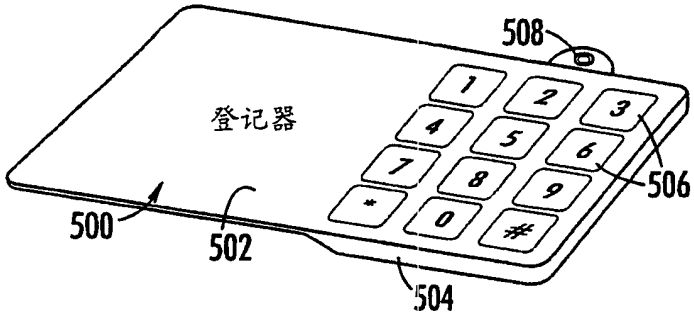

508
登记器
1
2
3
4
5
6
7
8
9
*
0
#
506
500
502
504

图 10

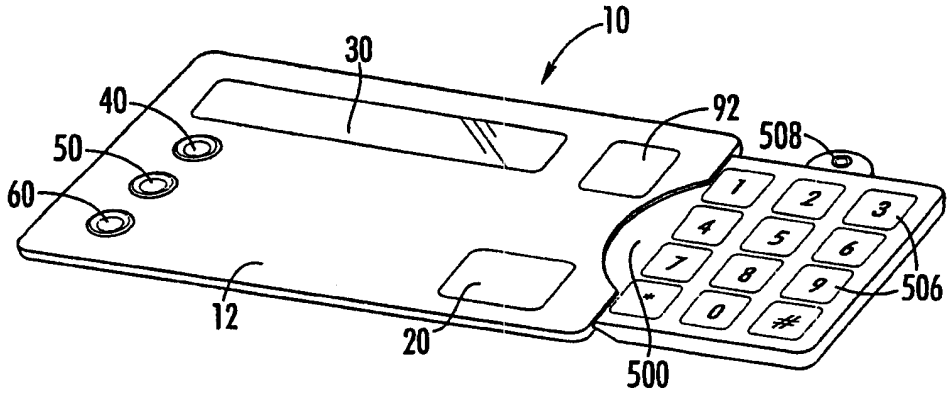

10
30
40
50
60
92
508
1
2
3
4
5
6
7
8
9
*
0
#
506
12
20
500

图 11

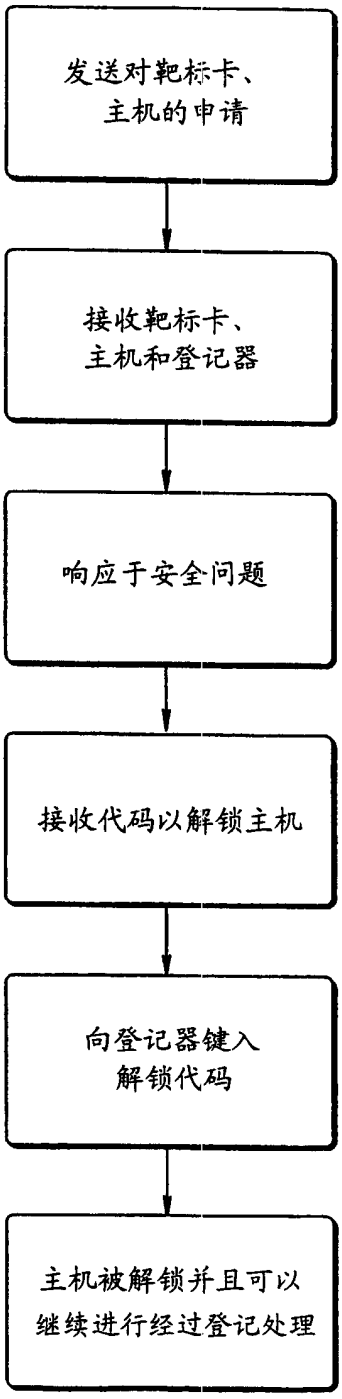

发送对靶标卡、
主机的申请
接收靶标卡、
主机和登记器
响应于安全问题
接收代码以解锁主机
向登记器键入
解锁代码
主机被解锁并且可以
继续进行经过登记处理

图 12