

(12) 发明专利申请

(10) 申请公布号 CN 102609633 A

(43) 申请公布日 2012. 07. 25

(21) 申请号 201110025463. X

(22) 申请日 2011. 01. 20

(71) 申请人 李学旻

地址 中国台湾台北市

(72) 发明人 李学旻

(74) 专利代理机构 永新专利商标代理有限公司

72002

代理人 刘瑜 王英

(51) Int. Cl.

G06F 21/00 (2006. 01)

G06K 19/073 (2006. 01)

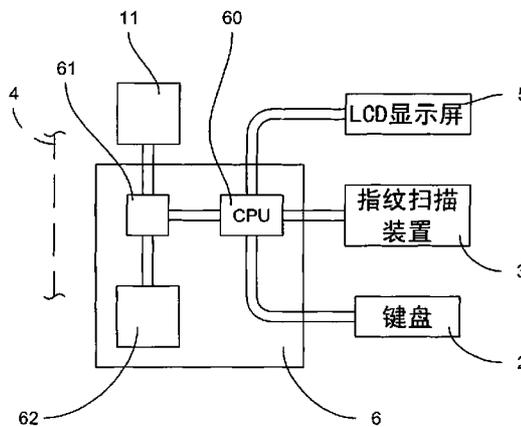
权利要求书 2 页 说明书 6 页 附图 6 页

(54) 发明名称

具有身份识别功能的 IC 卡和其安全认证系统及方法

(57) 摘要

本发明提供了一种具有身份识别功能的 IC 卡和其安全认证系统及方法。一种 IC 卡被提供，该 IC 卡包含：一个卡片本体，该卡片本体具有一个安装于一安装表面上的用于储存拥有者数据的集成电路 (IC) 芯片；一个安装于该卡片本体的安装表面上的指纹扫描装置；及一个可运作地安装于该卡片本体之内的控制电路单元，该控制电路单元包括一个电气连接至该指纹扫描装置和该 IC 芯片的中央处理单元、一个电气连接至该中央处理单元的用于与外部计算机主机通信的输出输入通信模块、及一个用于供应 IC 卡的组件所需的电力的电源模块，当该 IC 卡要与该外部计算机主机进行数据交换时，使用者是通过指纹扫描装置输入指纹数据，中央处理单元会把输入的指纹数据与储存于 IC 芯片内的拥有者指纹数据作比对，比对正确的话，该中央处理单元会发送一个允许码以允许 IC 卡与外部计算机主机进行下一步的交易。



1. 一种集成电路 (IC) 卡,其适于与一外部计算机主机进行数据交换,包含:

一个具有适当挠性的卡片本体,该卡片本体具有一个安装表面和一个安装于该安装表面上的用于储存拥有者数据的集成电路 (IC) 芯片;

一个安装于该卡片本体的安装表面上的指纹扫描装置;及

一个可运作地安装于该卡片本体之内的控制电路单元,该控制电路单元包括一个电气连接至该指纹扫描装置和该 IC 芯片的中央处理单元、一个电气连接至该中央处理单元的用于与该外部计算机主机通信的输出输入通信模块、及一个用于供应 IC 卡的组件所需的电力的电源模块,

借由如上所述的构造,当该 IC 卡要与该外部计算机主机进行数据交换时,使用者是通过指纹扫描装置输入指纹数据,中央处理单元会把输入的指纹数据与储存于 IC 芯片内的拥有者指纹数据作比对,比对正确的话,该中央处理单元会发送一个允许码以允许 IC 卡与外部计算机主机进行下一步的交易。

2. 如权利要求 1 所述的 IC 卡,还包含一个埋藏于该卡片本体内的与该通信模块连接的 RFID 天线以致于 IC 卡能够以无线方式与外部计算机主机交换数据。

3. 如权利要求 2 所述的 IC 卡,还包含一个由具有适当挠性的材料制成且可运作地安装于该卡片本体的安装表面上的 LCD 显示屏,该 LCD 显示屏与该中央处理单元电气连接使得能够显示交易数据。

4. 如权利要求 3 所述的 IC 卡,还包含一个由具有适当挠性的材料制成且可运作地安装于该卡片本体的安装表面上的键盘,该键盘可操作地输入希望的数据。

5. 如权利要求 1 所述的 IC 卡,还包含一个由具有适当挠性的材料制成且可运作地安装于该卡片本体的与该安装表面相反的背面的有机或无机显示器。

6. 如权利要求 1 所述的 IC 卡,还包含一个用于与该外部计算机主机连接的随插即用插头。

7. 一种使用如在权利要求 1 中所述的集成电路卡 (IC 卡) 来提升交易安全的方法,该方法包含如下步骤:

用指纹扫描装置输入卡片使用者的指纹数据;及

把输入的卡片使用者指纹数据与储存于 IC 芯片内的卡片拥有者指纹数据作比对,如果比对正确的话,则允许该 IC 卡与外部计算机主机进行下一步的数据交换,否则,拒绝该 IC 卡与该外部计算机主机进行下一步的数据交换。

8. 一种使用如在权利要求 1 中所述的集成电路卡 (IC 卡) 来提升交易安全的方法,该方法包含如下步骤:

用外部脸部特征提取装置提取卡片使用者的脸部特征数据或者用指纹扫描装置扫描使用者的指纹数据;及

把提取的使用者脸部特征数据或使用者的指纹数据与储存于 IC 芯片内的卡片拥有者脸部特征数据或拥有者指纹数据作比对,如果比对正确的话,则允许该 IC 卡与外部计算机主机进行下一步的数据交换,否则,拒绝该 IC 卡与该外部计算机主机进行下一步的数据交换。

9. 一种集成电路 (IC) 卡安全认证系统,其特征是在于包含:

一种如在权利要求 1 中所述的 IC 卡;

一计算机主机,该计算机主机是用于与该 IC 卡进行数据交换,该计算机主机包含:一个储存有卡片所有者指纹数据和卡片所有者脸部特征数据的存储器;一个用于提取卡片使用者脸部特征数据的脸部特征数据提取装置;及一个电气连接至该存储器和该脸部特征数据提取装置的中央处理单元;及

至少一个安装于该 IC 卡与该计算机主机中的至少一者的指纹扫描装置,

借由如上所述的构造,当该 IC 卡要与该计算机主机进行数据交换时,使用者是通过指纹扫描装置输入指纹数据,中央处理单元会把输入的指纹数据与储存于 IC 芯片内的所有者指纹数据作比对,比对正确的话,该中央处理单元会发送一个允许码以允许 IC 卡与外部计算机主机进行下一步的交易,或者,脸部特征提取装置提取卡片使用者的脸部特征数据,并且把提取的使用者脸部特征数据与储存于 IC 芯片内的卡片所有者脸部特征数据作比对,如果比对正确的话,则允许该 IC 卡与外部计算机主机进行下一步的数据交换,否则,拒绝该 IC 卡与该外部计算机主机进行下一步的数据交换。

具有身份识别功能的 IC 卡和其安全认证系统及方法

技术领域

[0001] 本发明有关于一种集成电路 (IC) 卡,更具体地,有关于一种具有身份识别功能的 IC 卡、一种 IC 卡安全认证系统、以及一种使用该 IC 卡来提升交易安全的方法。

背景技术

[0002] 随着科技的发展与进步,像是信用卡、金融卡、及其它很多能提供小额付款功能的卡片般的塑料货币越来越普及。然而,这些塑料货币虽然在使用上相当方便,但万一遗失了,拥有者必须承担遭他人盗用的风险,故若能使非拥有者使用这些卡片的机率降至最低时,将会使拥有者的风险降低。此外,由于数据在传送过程期间也会出现被拦截的现象,因此若能使数据即使在传送中被拦截也无法被他人使用的话,对拥有者而言安全性更高。

[0003] 此外,诸如健保 IC 卡、公司门禁卡、以及住户门禁卡般的卡片也很容易被冒用,因此也有改善的必要。

[0004] 鉴于此,本案发明人遂以其从事该行业的多年经验,并本着精益求精的精神,积极研究改良,遂产生了本发明“一种具有身份识别功能的 IC 卡、一种 IC 卡安全认证系统、以及一种使用该 IC 卡来提升交易安全的方法”。

发明内容

[0005] 本发明的目的是为提供一种具有身份识别功能的 IC 卡、一种 IC 卡安全认证系统、以及一种使用该 IC 卡来提升交易安全的方法。

[0006] 根据本发明中的一个特征,一种适于与一外部计算机主机进行数据交换的 IC 卡被提供,该 IC 卡的特征是在于包含:一个具有适当挠性的卡片本体,该卡片本体具有一个安装表面和一个安装于该安装表面上的用于储存拥有者数据的集成电路 (IC) 芯片;一个安装于该卡片本体的安装表面上的存拥有者数据的集成电路 (IC) 芯片;一个安装于该卡片本体的安装表面上的指纹扫描装置;及一个可运作地安装于该卡片本体之内的控制电路单元,该控制电路单元包括一个电气连接至该指纹扫描装置和该 IC 芯片的中央处理单元、一个电气连接至该中央处理单元的用于与该外部计算机主机通信的输出输入通信模块、及一个用于供应 IC 卡的组件所需的电力的电源模块,借由如上所述的构造,当该 IC 卡要与该外部计算机主机进行数据交换时,使用者是通过指纹扫描装置输入指纹数据,中央处理单元会把输入的指纹数据与储存于 IC 芯片内的拥有者指纹数据作比对,比对正确的话,该中央处理单元会发送一个允许码以允许 IC 卡与外部计算机主机进行下一步的交易。

[0007] 根据本发明中的另一特征,一种使用 IC 卡来提升交易安全的方法被提供,该 IC 卡的特征是在于包含:一个具有适当挠性的卡片本体,该卡片本体具有一个安装表面和一个安装于该安装表面上的用于储存拥有者数据的集成电路 (IC) 芯片;一个安装于该卡片本体的安装表面上的指纹扫描装置;及一个可运作地安装于该卡片本体之内的控制电路单元,该控制电路单元包括一个电气连接至该指纹扫描装置与该 IC 芯片的中央处理单元、一个电气连接至该中央处理单元的用于与外部计算机主机通信的输出输入通信模块、及一个

用于供应 IC 卡的组件所需的电力的电源模块,该方法包含如下步骤:用指纹扫描装置输入卡片使用者的指纹数据;及把输入的卡片使用者指纹数据与储存于 IC 芯片内的卡片拥有者指纹数据作比对,如果比对正确的话,则允许该 IC 卡与外部计算机主机进行下一步的数据交换,否则,拒绝该 IC 卡与该外部计算机主机进行下一步的数据交换。

[0008] 根据本发明中的另一特征,一种使用 IC 卡来提升交易安全的方法被提供,该 IC 卡的特征是在于包含:一个具有适当挠性的卡片本体,该卡片本体具有一个安装表面和一个安装于该安装表面上的用于储存拥有者数据的集成电路(IC)芯片;及一个可运作地安装于该卡片本体之内的控制电路单元,该控制电路单元包括一个电气连接到该 IC 芯片的中央处理单元、一个电气连接至该中央处理单元的用于与外部计算机主机通信的输出输入通信模块、及一个用于供应 IC 卡的组件所需的电力的电源模块,该方法包含如下步骤:用外部脸部特征提取装置提取卡片使用者的脸部特征数据或者以指纹扫描装置扫描使用者的指纹数据;及把提取的使用者脸部特征数据或使用者的指纹数据与储存于 IC 芯片内的卡片拥有者脸部特征数据或拥有者指纹数据作比对,如果比对正确的话,则允许该 IC 卡与外部计算机主机进行下一步的数据交换,否则,拒绝该 IC 卡与该外部计算机主机进行下一步的数据交换。

[0009] 根据本发明的再一特征,一种 IC 卡安全认证系统被提供,该系统的特征是在于包含:一 IC 卡,该 IC 卡包含一个具有适当挠性的卡片本体,该卡片本体具有一个安装表面和一个安装于该安装表面上的用于储存拥有者数据的集成电路(IC)芯片;及一个可运作地安装于该卡片本体之内的控制电路单元,该控制电路单元包括一个电气连接至该指纹扫描装置与该 IC 芯片的中央处理单元、一个电气连接至该中央处理单元的用于与外部计算机主机通信的输出输入通信模块、及一个用于供应 IC 卡的组件所需的电力的电源模块;一计算机主机,该计算机主机是用于与该 IC 卡进行数据交换,该计算机主机包含:一个储存有卡片拥有者指纹数据和卡片拥有者脸部特征数据的存储器;一个用于提取卡片使用者脸部特征数据的脸部特征数据提取装置;及一个电气连接至该存储器和该脸部特征数据提取装置的中央处理单元;及至少一个安装于该 IC 卡与该计算机主机中的至少一者的指纹扫描装置,借由如上所述的构造,当该 IC 卡要与该计算机主机进行数据交换时,使用者是通过指纹扫描装置输入指纹数据,中央处理单元会把输入的指纹数据与储存于 IC 芯片内的拥有者指纹数据作比对,比对正确的话,该中央处理单元会发送一个允许码以允许 IC 卡与外部计算机主机进行下一步的交易,或者,脸部特征提取装置提取卡片使用者的脸部特征数据,并且把提取的使用者脸部特征数据与储存于 IC 芯片内的卡片拥有者脸部特征数据作比对,如果比对正确的话,则允许该 IC 卡与外部计算机主机进行下一步的数据交换,否则,拒绝该 IC 卡与该外部计算机主机进行下一步的数据交换。

附图说明

[0010] 图 1 是为一个显示本发明的一实施例的 IC 卡的示意平面图;

[0011] 图 2 是为一个显示本发明的一实施例的 IC 卡的示意电路方块图;

[0012] 图 3 是为一个显示本发明的一实施例的 IC 卡的验证的示意流程图;

[0013] 图 4 是为一个显示本发明的一实施例的 IC 卡的验证的另一示意流程图;

[0014] 图 5 是为一个显示本发明的一实施例的 IC 卡安全认证系统的外部计算机主机的

示意立体图；

[0015] 图 6 是为一个显示图 5 的外部计算机的示意电路方块图；

[0016] 图 7 是为一个显示本发明的一实施例的 IC 卡安全认证系统的监视摄影机的示意立体图；

[0017] 图 8 是为一个显示本发明的另一实施例的 IC 卡的示意平面图；及

[0018] 图 9 是为一个显示适于与本发明的一实施例的 IC 卡一起使用的自动提款机的示意图。

[0019] **【主要组件符号说明】**

[0020] 1 卡片本体

[0021] 2 键盘装置

[0022] 3 指纹扫描装置

[0023] 4 RFID 天线

[0024] 5 LCD 显示屏

[0025] 6 控制电路单元

[0026] 10 安装表面

[0027] 11 IC 芯片

[0028] 60 中央处理单元

[0029] 61 通信模块

[0030] 62 电源模块

[0031] 7 外部计算机主机

[0032] 70 本体

[0033] 71 指纹扫描装置

[0034] 72 影像提取装置

[0035] 73 键盘装置

[0036] 74 LCD 显示单元

[0037] 75 主机控制电路

[0038] 8 USB 界面

[0039] MON 监视器

[0040] N1 步骤

[0041] N2 步骤

[0042] N3 步骤

[0043] N10 步骤

[0044] N20 步骤

[0045] N30 步骤

[0046] N40 步骤

[0047] R 360 度红外线扫描卡片阅读机

具体实施方式

[0048] 在后面的本发明的较佳实施例的详细说明中,相同或类似的组件是由相同的标号

标示,而且它们的详细描述将会被省略。此外,为了清楚揭示本发明的特征,在图式中的组件并非按实际比例描绘。

[0049] 图 1 为一个显示本发明的较佳实施例的一种具有身份识别功能的 IC 卡的示意平面图,而图 2 是为一个显示该 IC 卡的内部电路的示意方块图。

[0050] 请配合参阅图 1 和图 2 所示,本发明的较佳实施例的 IC 卡大致包括一个卡片本体 1、一个键盘 2、一个指纹扫描装置 3、内藏于该卡片本体 1 内的 RFID(Radio Frequency Identification) 天线 4、一个 LCD 显示屏 5、以及一个控制电路单元 6。

[0051] 在本实施例中,该卡片本体 1 是具有一定的挠性以致力于可避免因不小心的弯折而发生断裂的情况。与目前一般的信用卡、金融卡等等一样,该卡片本体 1 具有一个安装表面 10 以及一个安装在该安装表面 10 上的 IC 芯片 11。在本较佳实施例中,该 IC 芯片 11 可以储存至少一个卡片拥有者账户数据、卡片拥有者的脸部特征数据、卡片拥有者的指纹数据、卡片拥有者的身份证字号、卡片拥有者的出生日期等等的信息。

[0052] 该键盘 2 是由具有适当挠性的材料制成而且是可运作地安装于该卡片本体 1 的安装表面 10 上使得可由卡片使用者操作来输入希望的数据。应要注意的是,除了一般数字键之外,该键盘 2 还可以具有像是加减乘除般的功能键。借由操作该键盘 2,该 IC 卡本次的消费金额也可被设定再经由接触式及 / 或非接触式的卡片阅读机付款。借由操作该键盘 2,也可以启动密码与外部交易主机(图中未示)的互相认证。

[0053] 该指纹扫描装置 3 是可运作地安装于该卡片本体 1 的安装表面 10 上使得可被移动来扫描使用者的指纹数据。借由该指纹扫描装置 3 以及储存的指纹数据,IC 卡在与交易主机进行所有 B 对 B(B to B)、B 对 C(B to C)、C 对 C(C to C) 或者银行账号转账的交易时可免除输入密码来达成。

[0054] 该 RFID 天线 4 是埋藏在该卡片本体 1 之内而且是用最适当的方式绕行以致力于该 IC 卡的数据能够选择地用无线方式与外部交易主机进行交换。

[0055] 该 LCD 显示屏 5 是由具适当挠性的材料制成而且是可运作地安装于该卡片本体 1 的安装表面 10 上使得可显示诸如账号、交易金额、交易状态等等般的信息。该 LCD 显示屏 5 也可以显示单次交易金额、累积交易金额等等以达到个人理财的目的。

[0056] 该控制电路单元 6 是可运作地安装于该卡片本体 1 之内而且包括一个电气连接至该指纹扫描装置 3、该键盘 2、该 LCD 显示屏 5 的中央处理单元 60、一个电气连接至该中央处理单元 60 和该 IC 芯片 11 的通信模块 61、及一个用于供应 IC 卡的所有组件所需的电力的电源模块 62。该通信模块 61 也与该 RFID 天线 4 连接。该电源模块 62 可以是如钮扣型电池般的一般的电池,或者可以是由接触式或者非接触式感应电力的电池组或电容组件构成以致力于在与外部计算机主机以接触式或非接触式通信时能取得电力暂存于其内以提供 IC 卡的组件所需的电力。

[0057] 请配合参阅图 3 所示,以信用卡为例,当本较佳实施例的 IC 卡要与外部计算机主机(刷卡机)进行交易时,在步骤 N1 中,IC 卡使用者可以先利用键盘 2 选择想要交易的信用卡账号,然后 IC 卡的中央处理单元 60 会要求使用者利用指纹扫描装置 3 输入指纹数据。当使用者的指纹数据输入之后,在步骤 N2 中,该中央处理单元 60 会把输入的使用者指纹数据与储存在 IC 芯片 11 内的拥有者指纹数据作比对。如果比对正确的话,则该中央处理单元 60 会发送一个允许码以允许 IC 卡与外部计算机主机在步骤 N3 中进行下一步的交易,否

则,拒绝与外部计算机主机进行下一步的交易。

[0058] 应要注意的是,IC卡与外部计算机主机之间的通信可以是经由传统接触式或者是借由RFID天线经由非接触式来达成。另一方面,当该IC卡仅储存一个拥有者账号数据或者选择拥有者账号数据是可由外部计算机主机设定时,选择交易数据的步骤N1也是可以省略的。

[0059] 接着,请参阅图4并请配合参阅图9所示,以提款卡为例,当本较佳实施例的IC卡是经由IC卡接口M1来与自动提款机ATM进行交易时,除了如图3所述那样的IC卡可以先行自我认证之外(步骤N10和N20),在自我认证完成之后,可进行外部计算机交易主机的认证,即,在步骤N30中,自动提款机ATM的监视摄影机(图中未示)会提取使用者的脸部特征数据,然后与储存在IC卡内的拥有者脸部特征数据作比对。如果比对正确的话,则该中央处理单元60会发送一个允许码以允许与自动提款机在步骤N40中进行下一步的交易,否则,拒绝与自动提款机进行下一步的交易。

[0060] 应要注意的是,该允许码传送时可以经编码加密与交易时间码综合出一个仅允许使用一次的安全码使得防止在传输时被截取以供盗用。

[0061] 如图4所示的双认证方式也可以应用到信用卡交易。请再次参阅图4所示,以信用卡为例,当本较佳实施例的IC卡要与外部计算机主机(刷卡机)进行交易时,IC卡使用者可以先利用键盘2选择想要交易的信用卡账号(步骤N10),然后IC卡的中央处理单元60会要求使用者利用指纹扫描仪输入指纹数据。当使用者的数据输入之后,该中央处理单元60会把输入的使用者指纹数据与储存在IC芯片11内的拥有者指纹数据作比对(步骤N20)。如果比对正确的话,则该中央处理单元60会发送一个允许码以允许IC卡与外部计算机主机进行下一步的交易,否则,拒绝与外部计算机主机进行下一步的交易。

[0062] 如果IC卡自我认证通过之后,该IC卡是因该允许码而与外部计算机主机联机。此时,外部计算机主机会要求使用者再进行一次指纹扫描以取得使用者指纹数据或者是以摄影机提取使用者脸部特征数据。使用者指纹数据或者使用者脸部特征数据然后是与储存于外部计算机主机的拥有者指纹数据或者拥有者脸部特征数据作比对(步骤N30)。如果比对正确的话,则允许IC卡与外部计算机主机进行下一步的交易(步骤N40),否则,拒绝与外部计算机主机进行下一步的交易。

[0063] 图5是为一个描绘本发明的较佳实施例的IC卡片交易认证系统的外部计算机主机(刷卡机)7的示意图。

[0064] 如在图5中所示,该外部计算机主机7可以包括一个本体70、一个指纹扫描装置71、一个影像提取装置72、一个键盘装置73、一个LCD显示单元74以及一个安装于该本体70内部的主机控制电路75(见图6)。

[0065] 当该外部计算机主机7要与一连接上的IC卡进行交易时,使用者可以经由指纹扫描装置71输入指纹数据。该主机7随后会把输入的指纹数据与储存于IC卡内的卡片拥有者指纹数据作比对。若比对正确的话,则该主机控制电路75允许与该IC卡进行下一步的交易,否则,拒绝与该IC卡进行下一步的交易。

[0066] 本发明的IC卡可用在任何需要身份认证的领域,例如,航空公司的贵宾室、连锁店的贵宾卡或折扣卡、酒店的门锁卡、公司识别证、大楼用户卡等等。借由储存于IC卡内的拥有者的脸部特征数据以及普遍置于各场所的具有360度红外线扫描卡片阅读器R的监视

器 MON(见图 7) 提取使用者的脸部特征数据作比对,即能立即发现 IC 卡被盗用而做出警示或其它适当的处理。当然,像是健保卡般的 IC 卡也可使用本发明的 IC 卡以致力于经由指纹认证不会有被冒用的情事发生。

[0067] 应要注意的是,本 IC 卡可被设定以致力于金额低于一指定数目时,可以不必通过认证而进行交易,以达到小额付款便利性的目的。

[0068] 请参阅图 8 所示,本发明的 IC 卡也可通过 USB 接口 8 来与如笔记型计算机或者台式计算机 P 般的外部计算机主机连接。通过指纹数据比对或密码启动 IC 卡电源,经计算机的网络进行 B 对 B、B 对 C、C 对 C 等等的网上交易或与银行账号做转账或付款的功能。应要注意的是,该 USB 接口 8 可以是包括如标准的 USB、MINI USB 等等般的任何适于与外部计算机主机作连接的随插即用 USB 接口。

[0069] 综上所述,本发明的“一种具有身份识别功能的 IC 卡、一种 IC 卡安全认证系统、以及一种使用该 IC 卡来提升交易安全的方法”,确实能通过上述所公开的构造、装置,达到预期的目的与功效,且申请前未见于刊物也未公开使用,符合发明专利的新颖、进步等要素。

[0070] 尽管上文公开了附图及说明,但仅为本发明的实施例,不用于限定本发明的实施例;熟悉本领域的技术人员,根据本发明的特征范围,所作的其它等效变化或修改,都应涵盖在以下本案的权利要求范围内。

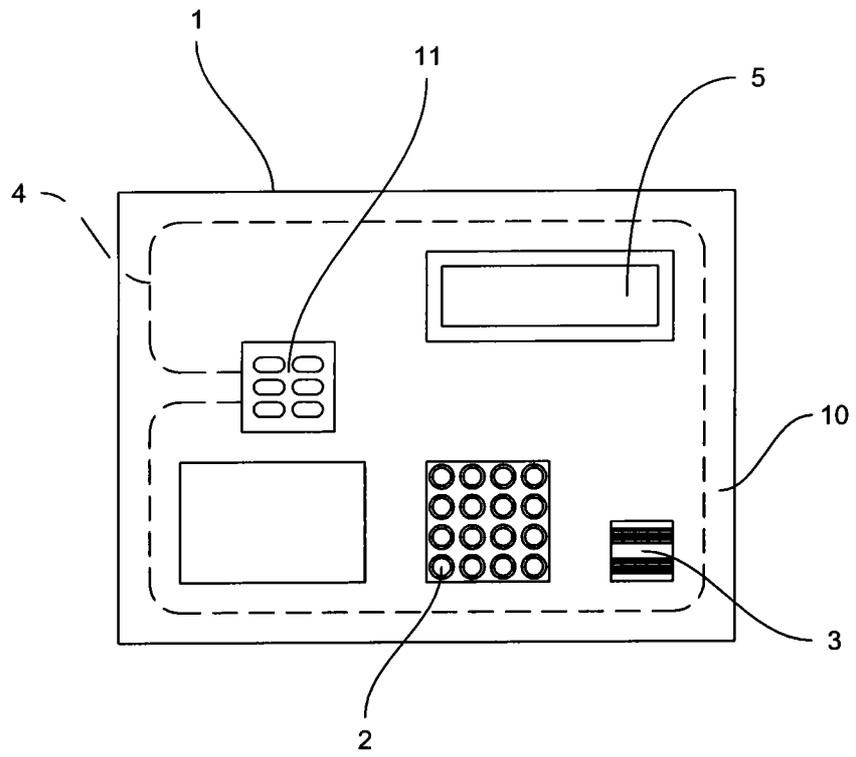


图 1

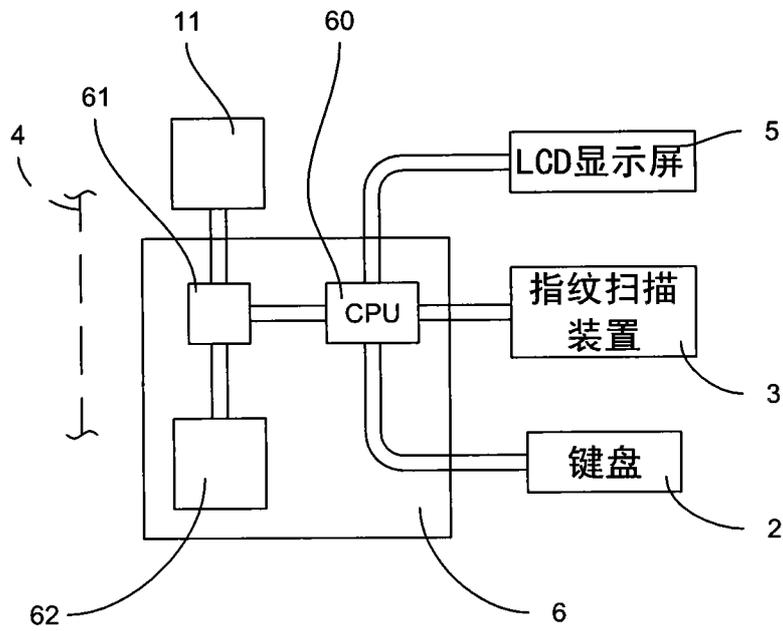


图 2

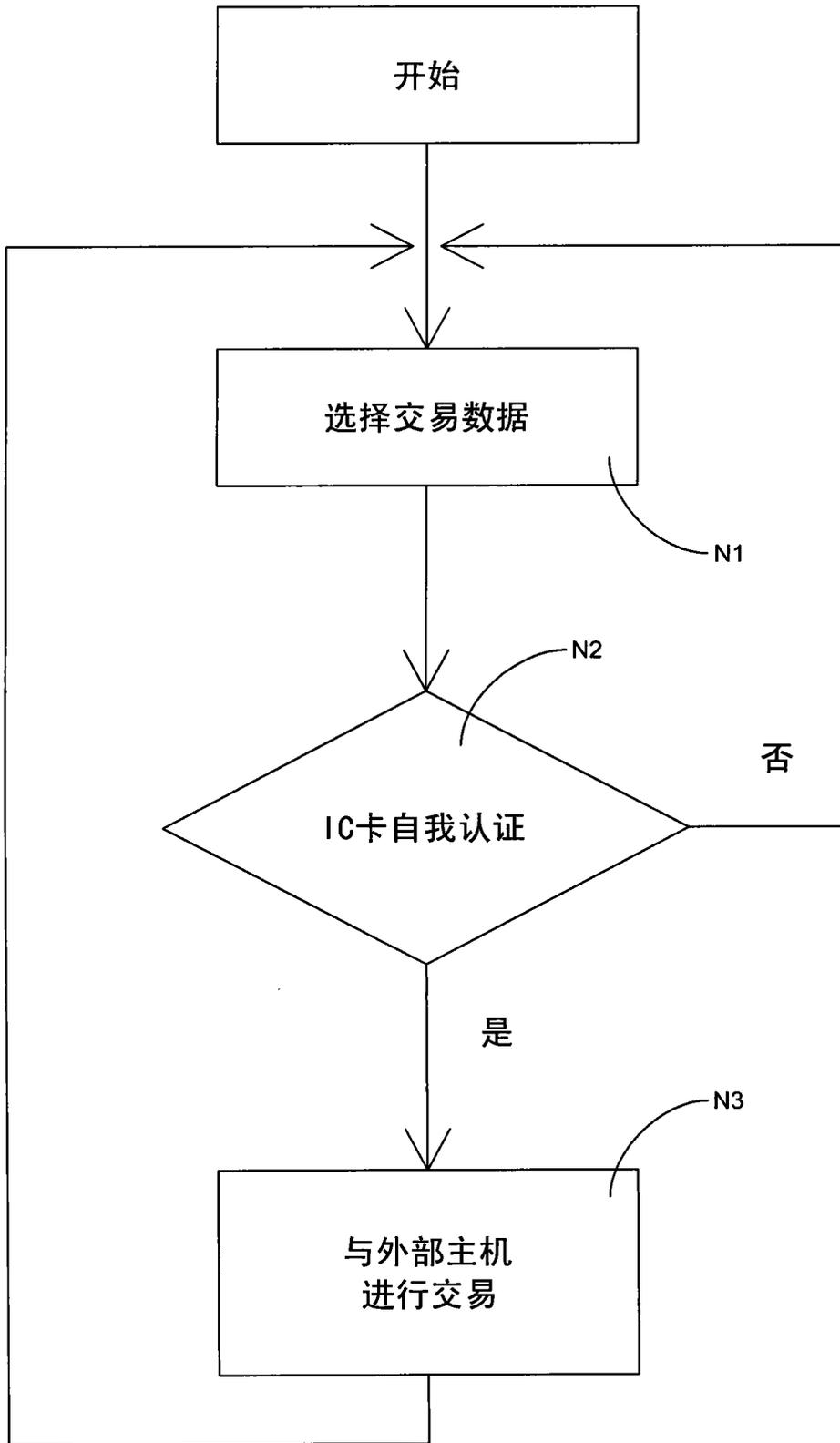


图 3

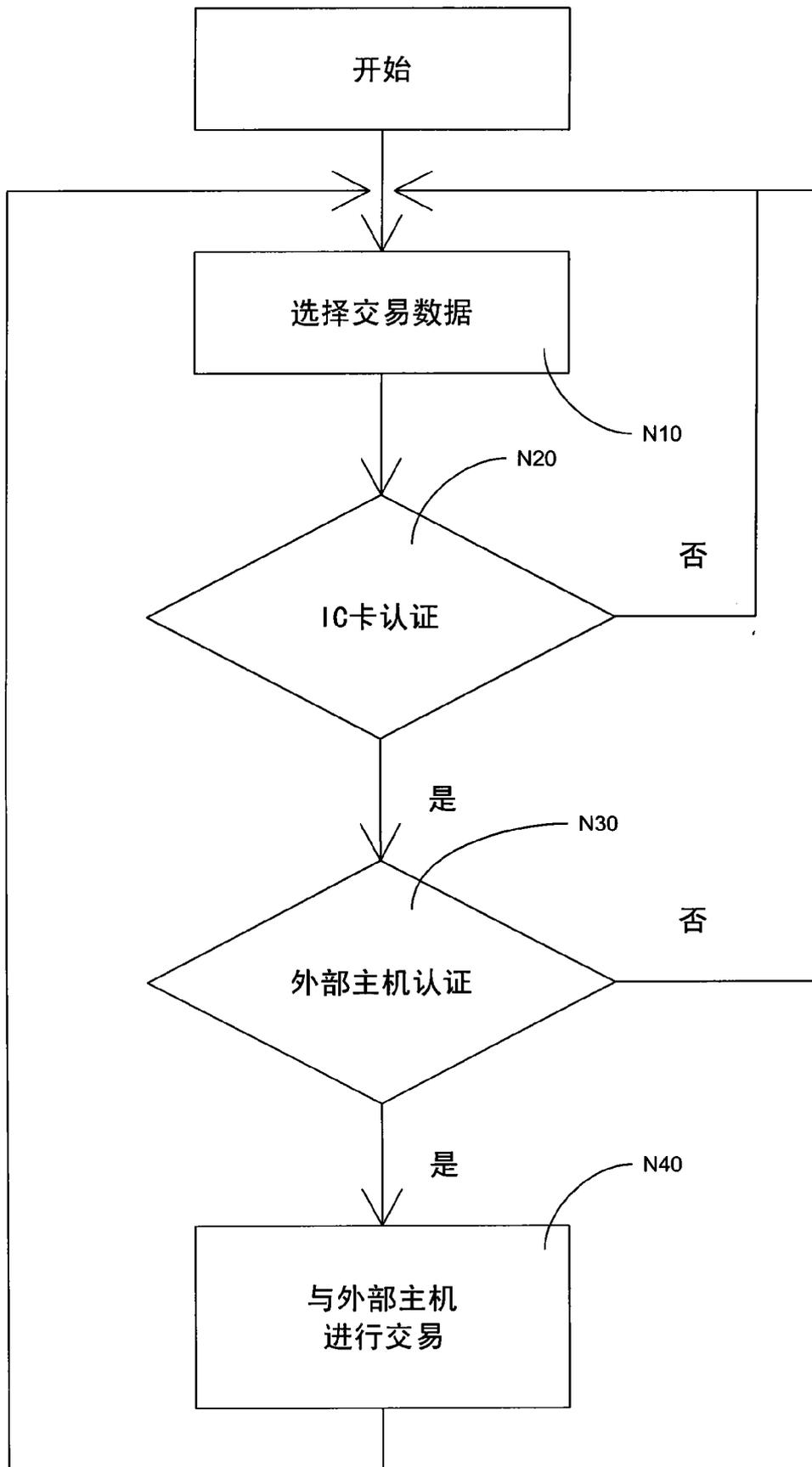


图 4

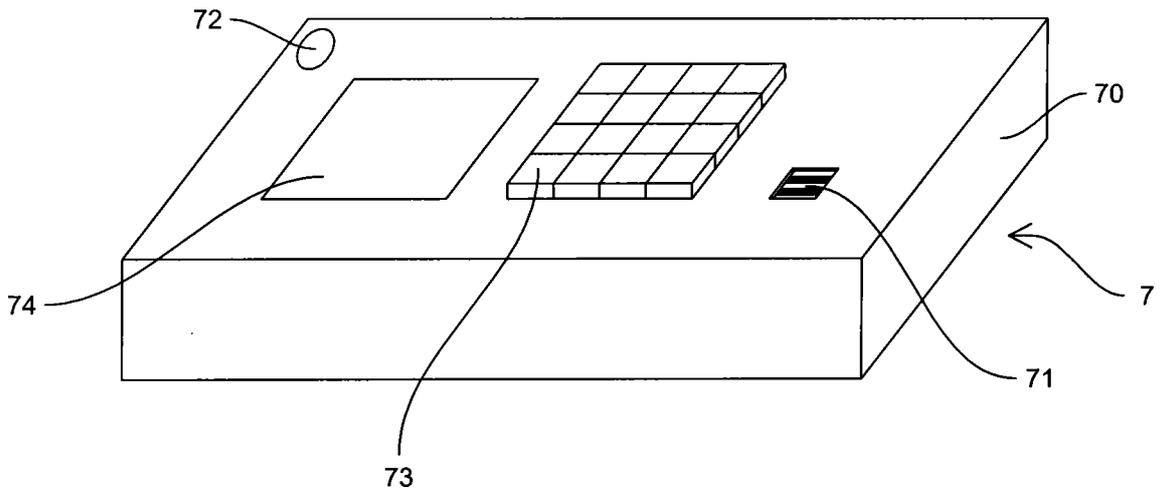


图 5

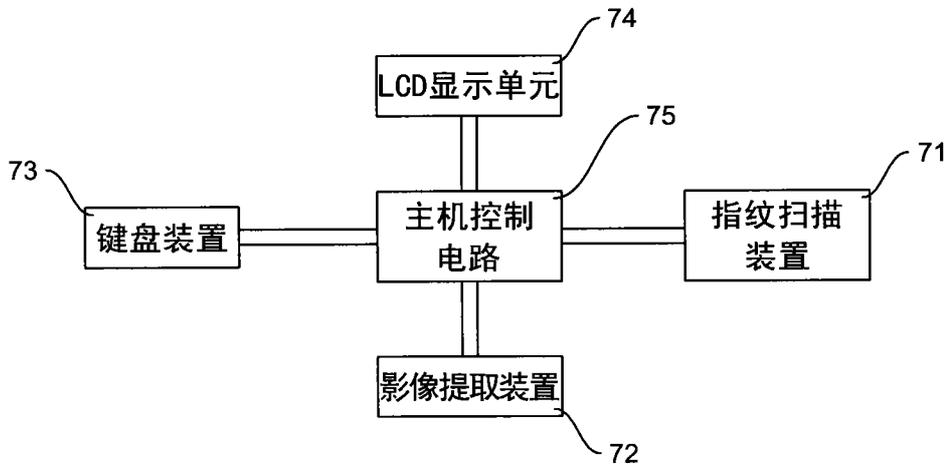


图 6

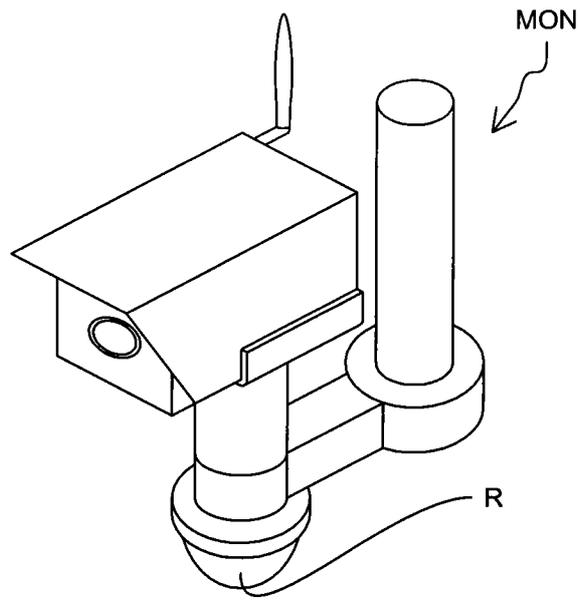


图 7

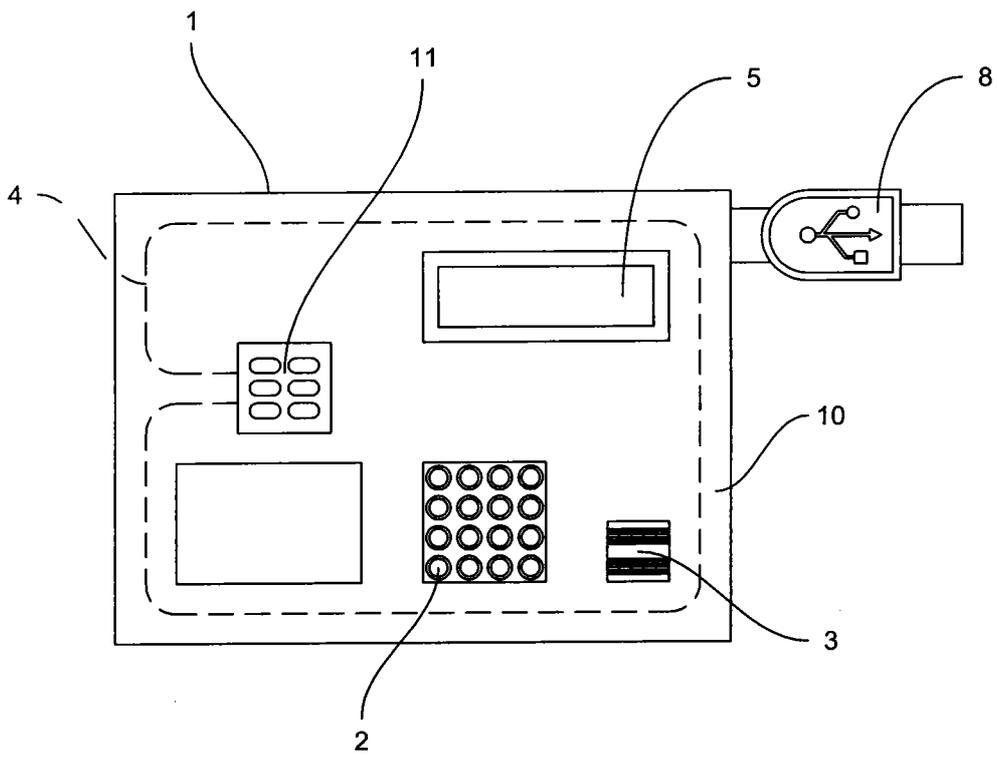


图 8

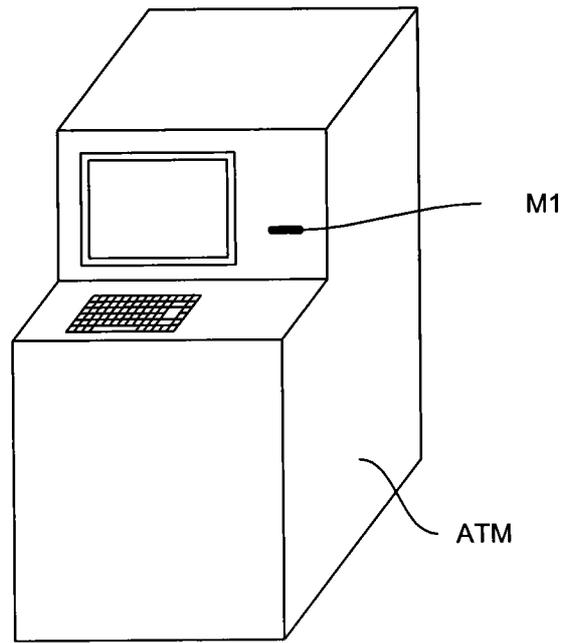


图 9