(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 208569672 U
(45)授权公告日 2019.03.01

(21)申请号 201820539702.0

(22)申请日 2018.04.16

(73)专利权人 东莞市芯安智能科技有限公司
地址 523710 广东省东莞市塘厦镇农霖路12号

(72)发明人 朱海林

(74)专利代理机构 深圳中一联合知识产权代理有限公司 44414
代理人 张全文

(51)Int.Cl.
G06K 19/077(2006.01)
G06K 9/00(2006.01)

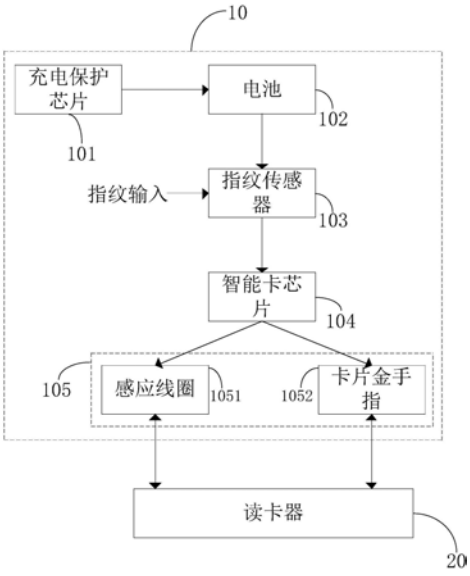
权利要求书1页 说明书6页 附图2页

(54)实用新型名称

指纹生物识别智能IC卡和指纹识别系统

(57)摘要

本实用新型属于IC卡技术领域，提供了一种指纹生物识别智能IC卡和指纹识别系统；其中，所述指纹生物识别智能IC卡包括：构造为生成充电保护信号的充电保护芯片；与充电保护芯片连接，构造为根据充电保护信号输出直流电源的电池；与电池连接，构造为根据直流电源获取用户的指纹特征数据，并在指纹特征数据与预设指纹数据匹配时生成指纹认证信号的指纹传感器；与指纹传感器连接，构造为根据指纹认证信号输出安全芯片数据的智能卡芯片；连接在读卡器和智能卡芯片之间，构造为将安全芯片数据传输至读卡器的通讯模块；通过本实用新型可解决现有技术中IC卡的数据安全等级较低以及IC卡的数据易被复制或者盗窃的问题。



CN 208569672 U

1.一种指纹生物识别智能IC卡,其特征在于,包括:

构造为生成充电保护信号的充电保护芯片;

与所述充电保护芯片连接,构造为根据所述充电保护信号输出直流电源的电池;

与所述电池连接,构造为根据所述直流电源获取用户的指纹特征数据,并在所述指纹特征数据与预设指纹数据匹配时生成指纹认证信号的指纹传感器;

与所述指纹传感器连接,构造为根据所述指纹认证信号输出安全芯片数据的智能卡芯片;

连接在读卡器和所述智能卡芯片之间,构造为将所述安全芯片数据传输至读卡器的通讯模块;

其中,所述充电保护芯片为ETA9686系列芯片;

所述通讯模块包括感应线圈,所述感应线圈与所述读卡器非接触式通讯;

所述通讯模块包括卡片金手指,所述卡片金手指与所述读卡器接触式通讯。

2.根据权利要求1所述的指纹生物识别智能IC卡,其特征在于,还包括:

与所述智能卡芯片通讯连接,构造为根据所述安全芯片数据生成主控信号的控制器;

与所述电池和所述控制器连接,构造为将所述主控信号传输至智能终端的蓝牙芯片。

3.根据权利要求2所述的指纹生物识别智能IC卡,其特征在于,还包括:

与所述电池和所述控制器连接,构造为根据所述主控信号显示用户指纹验证信息的显示屏。

4.一种指纹识别系统,其特征在于,包括:IC卡服务器、至少一个IC卡识别终端和至少一个如权利要求1-3任一项所述指纹生物识别智能IC卡;

其中,所述IC卡识别终端包括IC卡读写设备,所述IC卡识别终端通过IC卡读写设备与所述指纹生物识别智能IC卡连接,所述IC卡识别终端通过网络和所述IC卡服务器连接。

5.根据权利要求4所述的指纹识别系统,其特征在于,所述IC卡识别终端为POS机和/或ATM机。

6.根据权利要求4所述的指纹识别系统,其特征在于,所述IC卡识别终端通过银行专用网络与所述IC卡服务器连接。

指纹生物识别智能IC卡和指纹识别系统

技术领域

[0001] 本实用新型属于IC卡技术领域，尤其涉及一种指纹生物识别智能IC卡和指纹识别系统。

背景技术

[0002] 随着现代工艺的快速发展，IC(Integrated Circuit，集成电路)卡已经成为目前人们日常生活中必不可少的组成部分；由于制造成本低廉以及体积较小，IC 卡已经广泛地应用在金融、消费等电子领域；现有的IC卡通常将密码模块存储在IC卡中；当用户使用时，IC卡只能通过内部的加密方式来进行安全验证，进而实现IC卡内部所存储的数据与外部设备之间的双向传输过程。

[0003] 然而若IC卡被不法分子盗取或者被不法分子拾得，不法分子通过计算机程序能够破解IC卡内部的加密机制，进而盗取存储在IC卡中的数据信息，导致用户的数据和信息外泄；因此，现有的IC卡所采用的内部加密机制和机器验证码无法保证IC卡中数据安全，IC卡中的密码以及存储数据容易被外界不法分子窃取或者复制。

实用新型内容

[0004] 本实用新型提供一种指纹生物识别智能IC卡和指纹识别系统，旨在解决现有技术无法保证IC卡中的数据安全，以及IC卡的密码容易被外界不法分子窃取或者复制的问题。

[0005] 本实用新型第一方面提供一种指纹生物识别智能IC卡，包括：

[0006] 构造为生成充电保护信号的充电保护芯片；

[0007] 与所述充电保护芯片连接，构造为根据所述充电保护信号输出直流电源的电池；

[0008] 与所述电池连接，构造为根据所述直流电源获取用户的指纹特征数据，并在所述指纹特征数据与预设指纹数据匹配时生成指纹认证信号的指纹传感器；

[0009] 与所述指纹传感器连接，构造为根据所述指纹认证信号输出安全芯片数据的智能卡芯片；

[0010] 连接在读卡器和所述智能卡芯片之间，构造为将所述安全芯片数据传输至读卡器的通讯模块。

[0011] 在其中的一个实施例中，所述通讯模块包括感应线圈，所述感应线圈与所述读卡器非接触式通讯。

[0012] 在其中的一个实施例中，所述通讯模块包括卡片金手指，所述卡片金手指与所述读卡器接触式通讯。

[0013] 在其中的一个实施例中，还包括：

[0014] 与所述智能卡芯片通讯连接，构造为根据所述安全芯片数据生成主控信号的控制器；

[0015] 与所述电池和所述控制器连接，构造为将所述主控信号传输至智能终端的蓝牙芯片。

[0016] 在其中的一个实施例中，还包括：

[0017] 与所述电池和所述控制器连接，构造为根据所述主控信号显示用户指纹验证信息的显示屏。

[0018] 本实用新型第二方面提供一种指纹识别系统，包括：IC卡服务器、至少一个IC卡识别终端和至少一个如上所述指纹生物识别智能IC卡；

[0019] 其中，所述IC卡识别终端包括IC卡读写设备，所述IC卡识别终端通过 IC卡读写设备与所述指纹生物识别智能IC卡连接，所述IC卡识别终端通过网络和所述IC卡服务器连接。

[0020] 在其中的一个实施例中，所述IC卡识别终端为PSO机和/或ATM机。

[0021] 在其中的一个实施例中，所述IC卡识别终端通过银行专用网络与所述IC 卡服务器连接。

[0022] 本实用新型相对于现有技术所取得的有益技术效果为：在上述指纹生物识别智能IC卡中，通过电池可向该智能IC卡提供稳定的直流电源，进而保证该智能IC卡的正常使用；通过指纹传感器可实时获取用户的指纹特征数据，只要当用户的指纹特征数据与提前存储在该智能IC卡中的预设指纹数据完全匹配一致时，该指纹生物识别智能IC卡才能与外界的读卡设备进行数据交互操作，因此该智能IC卡通过指纹验证的方式极大地提高了用户所持有IC卡中的数据安全等级，防止了用户的IC卡的密码或者信息被不法分子窃取或复制，全面地维护了用户的财物与信息安全；从而有效地克服了现有技术中IC卡的数据容易被外界不法分子窃取或复制以及数据安全等级较低的不足之处。

附图说明

[0023] 为了更清楚地说明本实用新型实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本实用新型的一些实施例，对于本领域技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0024] 图1是本实用新型实施例提供的一种指纹生物识别智能IC卡的模块结构图；

[0025] 图2是本实用新型实施例提供的另一种指纹生物识别智能IC卡的模块结构图；

[0026] 图3是本实用新型实施例提供的指纹识别系统的模块结构图。

具体实施方式

[0027] 为了使本实用新型的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本实用新型进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本实用新型，并不用于限定本实用新型。

[0028] 图1示出了本实用新型实施例提供的指纹生物识别智能IC卡10的模块结构，为了便于说明，仅示出了与本实用新型实施例相关的部分，详述如下：

[0029] 如图1所示，指纹生物识别智能IC卡10包括充电保护芯片101、电池102、指纹传感器103、智能卡芯片104以及通讯模块105；其中，充电保护芯片101 生成充电保护信号，电池102与充电保护芯片101连接，充电保护芯片101将充电保护信号传输至电池102，电池102根据充电保护信号输出直流电源，该直流电源用于向指纹生物识别智能IC卡提供稳定的直流

电能;具体的,充电保护芯片101所生成的充电保护信号可作为驱动信号,只有电池102接入该充电保护信号时,电池102才会输出直流电源;因此,在本实用新型实施例所提供的指纹生物识别智能IC卡10内部设有电池102,则电池102作为内部电源向指纹生物识别智能IC卡10进行供电,从而用户可使用指纹生物识别智能IC 卡在现场进行脱机认证,并且通过增设了充电保护芯片101可防止用户出现误触发现象,即只有电池102接收充电保护信号时,指纹生物识别智能IC卡10 才会进行指纹验证操作,从而极大地提高了用户的使用便捷性。

[0030] 作为一种可选的实施方式,充电保护芯片101为ETA9686系列芯片。

[0031] 指纹传感器103与电池102连接,指纹传感器103根据直流电源获取用户的指纹特征数据,并且当指纹特征数据与预设指纹数据完全匹配一致时,指纹传感器103生成指纹认证信号;其中通过直流电源向指纹传感器103提供稳定的直流电能,以驱动指纹传感器103处于正常工作状态;预设指纹数据是提前存储在该指纹传感器103中,当指纹传感器103得电后,指纹传感器103获取用户的指纹特征数据,通过对指纹特征数据与预设指纹数据进行一一对比分析后得到指纹用户的指纹认证结果,若用户的指纹特征数据与预设指纹数据完全匹配或者相同,那么指纹传感器103生成指纹认证信号,进而用户可正常使用指纹生物识别智能IC卡10;相反,若用户的指纹特征数据与预设指纹数据并不完全匹配或者相同,那么说明此时用户属于非法入侵者,指纹验证失败,用户无法继续使用指纹生物识别智能IC卡10,因此通过指纹传感器103的指纹验证操作保障了指纹生物识别智能IC卡10中的数据安全,防止了外界分子盗窃或者复制指纹生物识别智能IC卡中的数据和密码。

[0032] 作为一种可选的实施方式,指纹传感器103采用QS808指纹系列芯片来实现指纹验证功能。

[0033] 需要进行说明的是,由于人体的指纹具有较为复杂的数据结构,那么上述指纹特征数据和预设指纹数据可以包括人体各种数据结构,如纹数、中心点位置等;作为一种可选的实施方式,所述指纹特征数据与预设指纹数据匹配是指用户指纹的各种数据结构(如纹数、中心点位置等)与预先存储在指纹生物识别智能IC卡10中的各种数据结构完全相同。

[0034] 智能卡芯片104与指纹传感器103连接,智能卡芯片104根据指纹认证信号输出安全芯片数据;其中安全芯片数据包括但不限于用户存储在指纹生物识别智能IC卡的金融数字信息、个人身份信息、密码以及个人消费记录等;若指纹传感器103将指纹认证信号输出至智能卡芯片104时,则说明用户的指纹已经验证成功,此时智能卡芯片104输出安全芯片数据以实现数据交互的功能;通讯模块105连接在读卡器20与智能卡芯片104之间,通讯模块105将安全芯片数据传输至读卡器20;其中通讯模块105与读卡器20可进行双向数据传递,因此指纹生物识别智能IC卡10不仅可将安全芯片数据发送至读卡器20 中,指纹生物识别智能IC卡10也可接收读卡器20所传输的数据,以实现读卡器20与指纹生物识别智能IC卡10之间的信息双向传输。

[0035] 作为一种优选的实施方式,智能卡芯片104为SLE4044系列芯片。

[0036] 通过本实用新型实施例,由于在指纹生物识别智能IC卡10的内部具有电池102,通过电池102所输出的直流电源可向指纹生物识别智能IC卡10提供直流电能,进而指纹生物识别智能IC卡10在使用时可以进行脱机认证,提高了用户的使用便捷性;并且通过指纹传感器103对用户的指纹进行验证,只有当用户的指纹验证成功以后,指纹生物识别智能IC卡10才会与外部的读卡器 20进行双向数据传输,考虑到人体指纹的独特性和不可替代性,因

此通过指纹验证的方式极大地提高了存储在指纹生物识别智能IC卡10的数据安全等级，防止用户的财物以及个人信息被外界不法分子窃取或者盗窃；从而有效地克服现有技术中智能IC卡中所存储的数据安全等级低，用户的个人信息和密码易遭到外界不法分子窃取或者复制的问题。

[0037] 作为一种可选的实施方式，通讯模块105包括感应线圈1051，感应线圈 1051与读卡器20非接触式通讯，从而指纹生物识别智能IC卡10与读卡器20 采用无线传输的形式进行双向数据传输。

[0038] 作为一种可选的实施方式，通讯模块105包括卡片金手指1052，卡片金手指1052与读卡器20接触式通讯，从而指纹生物识别智能IC卡10与读卡器20 采用有线传输的形式进行双向数据传输。

[0039] 需要说明的是，结合附图1，在本实用新型所提供的指纹生物识别智能IC 卡10中，通讯模块105只包括感应线圈1051也可以只包括卡片金手指1052，从而用户使用指纹生物识别智能IC卡10时只能在接触式通讯和非接触式通讯两者选择其一与读卡器20进行双向数据传递；同时通讯模块105也可以同时包括感应线圈1051和卡片金手指1052，进而用户使用指纹生物识别智能IC 卡10时可同时采用接触式通讯和非接触式通讯与读卡器20进行双向数据传递；从而用户在实际使用指纹生物识别智能IC卡10时，可以选择使用接触式通讯方式或者非接触式通讯方式与外部的读卡器20进行双向数据传递，极大地提高了指纹生物识别智能IC卡10的使用普遍性，增强了用户的使用舒适感。

[0040] 图2示出了本实用新型实施例提供的指纹生物识别智能IC卡10的另一种模块结构，与图1中所示出的指纹生物识别智能IC卡10相比，图2中所示出的指纹生物识别智能IC卡10还包括了控制器106、蓝牙芯片107以及显示屏 108，详述如下：

[0041] 控制器106与智能卡芯片104通讯连接，当用户通过指纹生物识别智能IC 卡10进行指纹验证成功以后，控制器106将安全芯片数据传输至控制器106，由于该安全芯片数据包括用户存储在指纹生物识别智能IC卡10中的各种信息和数据等，控制器106根据安全芯片数据生成主控信号，通过该主控信号可全面的了解用户的指纹验证信息和存储在指纹生物识别智能IC卡10中的多种数据；可选的，控制器106可采用单片机和CPU(Central Processing Unit、中央处理器)等来实现上述功能；蓝牙芯片107与电池102和控制器106连接，通过电池102所生成的直流电源可向蓝牙芯片107提供稳定的电能；优选的，蓝牙芯片107与智能终端30采用蓝牙通讯传输方式，控制器106将主控信号传输至智能终端30，由于在智能终端30中安装APP(Application，应用程序)，智能终端30根据该主控信号在APP上显示用户的指纹验证信息，此处的指纹验证信息包括但不限于：用户的指纹验证结果、用户的个人登录信息以及登录提示信息等；从而用户在使用指纹生物识别智能IC卡10进行指纹验证的过程中，可以通过智能终端20远程随时随地直观的获知用户的指纹验证信息，使用户能够更加直观地了解指纹生物识别智能IC卡10的使用情况。

[0042] 作为一种优选的实施方式，蓝牙芯片107为nrf51822芯片。

[0043] 作为一种可选的实施方式，智能终端20为手机、笔记本电脑或者台式电脑等。

[0044] 显示屏108与电池102和控制器106连接，显示屏108根据主控信号显示用户的指纹验证信息，其中通过显示屏108所显示的指纹验证信息与上述通过智能终端30上的APP所显示的指纹验证信息可以相同也可以不相同；由于显示屏108设于指纹生物识别智能IC卡10

的内部，因此当用户使用指纹生物识别智能IC卡10时，通过指纹生物识别智能IC卡可实时显示用户的指纹验证情况和用户的登录结果等信息。

[0045] 结合附图2中所示出的指纹生物识别智能IC卡10，当用户使用指纹生物识别智能IC卡时，用户既可以通过设于指纹生物识别智能IC卡10中的显示屏108也可以通过智能终端20上的APP直观获知用户的指纹验证信息，从而指纹生物识别智能IC卡10采用了上述两种方式向用户直观的展示指纹验证信息，即提高了用户的使用舒适感也加强了指纹生物识别智能IC卡10中的数据安全性。

[0046] 图3示出了本实用新型实施例提供的指纹识别系统40的模块结构，详述如下：

[0047] 如图3所示，指纹识别系统40包括：IC卡服务器402、至少一个IC卡识别终端401和至少一个如上所述的指纹生物识别智能IC卡10；其中，IC卡识别终端401包括IC卡读写设备4011，IC卡识别终端401通过IC卡读写设备 4011与指纹生物识别智能IC卡10连接，从而IC卡识别终端401与指纹生物识别智能IC卡10能够进行双向数据传输操作；可选的，IC卡读写设备4011 为IC卡读卡器；IC卡识别终端401通过网络和IC卡服务器402连接。

[0048] 在图3所示出的指纹识别系统40的模块结构中，指纹生物识别智能IC卡 10的内部结构以及所具有的功能可参照上文关于图1和图2实施例的论述，此处将不再赘述；若用户使用指纹生物识别智能IC卡10进行指纹验证成功后， IC卡识别终端401可以通过无线或者有线的方式与指纹生物识别智能IC卡10 进行通讯连接，IC卡识别终端401可读取指纹生物识别智能IC卡10中所存储的安全芯片数据，如上所述，该安全芯片数据包括用户存在该指纹生物识别智能IC卡10中的各种数据和信息；IC卡识别终端401将安全芯片数据通过网路传输至IC卡服务器402，此时IC卡服务器402对于安全芯片数据进行处理和分析操作后，以执行与其对应的操作；并且当IC卡服务器402根据该安全芯片数据执行对应的操作后，IC卡服务器402将更新后的功能数据通过IC卡识别终端401再次发送至指纹生物识别智能IC卡10中，以更新指纹生物识别智能IC卡10中所存储相关数据。

[0049] 需要进行说明的是，上述指纹识别系统40可包含多个IC卡识别终端401 和多个指纹生物识别智能IC卡10，而每一个IC卡识别终端401与每一个指纹生物识别智能IC卡10一一对应连接，IC卡识别终端401与IC卡服务器402 所采用的网络连接具有传输范围广、信号强度高的有点；因此，可在多个相隔距离较远的位置分别设置IC卡识别终端401，当用户使用生物识别智能IC卡 10时，处于不同地理位置的IC卡识别终端401可将安全芯片数据集中发送至 IC卡服务器402中进行统一处理和分析，因此本实用新型实施例所提供的指纹识别系统40可应用在较广的地理范围内，具有极高的便利性。

[0050] 需要说明的是，在本文中，所述多个是指2个以上。

[0051] 作为一种优选的实施方式，IC卡识别终端401为POS机和/或ATM机。

[0052] 作为一种优选的实施方式，IC卡识别终端401通过银行专用网络与IC卡服务器402连接。

[0053] 考虑到银行金融领域对于用户数据安全需求的特殊性，本实用新型所提供的指纹识别系统40优先适用于银行等金融领域，进而维护用户的信息和数据安全，防止用户的财产被不法分子窃取或者泄漏。

[0054] 本领域技术人员可以理解的是，作为一种示例性的，本文中的实施例将指纹生物识别智能IC卡10应用在银行交易等金融领域，但是若在具体的实际应用过程中，技术人员

将上述指纹生物识别智能IC卡10应用在其它的领域，如门禁卡、购物卡以及交通卡等领域，这些仅仅为本实用新型所提供的指纹生物识别智能IC卡10的应用而已，在不违背上文中关于指纹生物识别智能IC卡 10所记载技术特征和本实用新型的发明构思的前提下，这些仍然属于本实用新型所保护的范围。

[0055] 通过本实用新型实施例，若用户需要使用所述指纹生物识别智能IC卡10 时，只有在指纹生物识别智能IC卡10中通过指纹验证成功以后，指纹生物识别智能IC卡10才会与外界读卡设备进行数据通讯，因此，相比于现有的智能 IC卡采用内部加密机制和机器验证码对数据进行安全保护的方法，本实用新型实施例所提供的指纹生物识别智能IC卡10采用指纹验证的方式提高了数据的安全等级，防止存储在指纹生物识别智能IC卡10中的相关数据和密码被外界不法分子盗取或者复制，全面的维护了用户的信息和财产安全；进一步地，由于本实用新型所提供的指纹生物识别智能IC卡10具有多功能、高安全性等优点，技术人员可将指纹生物识别智能IC卡10应用在银行金融、公共交通以及商店购物等各个领域，具有极广的应用前景和使用范围；从而有效地解决了现有技术中智能IC卡的数据安全等级低、用户所存储的信息容易遭到外界不法分子窃取以及适用范围窄的问题。

[0056] 需要说明的是，在本文中，诸如第一和第二之类的关系术语仅仅用来将一个实体与另一个实体区分开来，而不一定要求或者暗示这些实体之间存在任何这种实际的关系或者顺序。而且术语“包括”、“包含”或者任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的产品或者结构所固有的要素。在没有更多限制的情况下，由语句“包括……”或者“包含……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者终端设备中还存在另外的要素。此外，在本文中，“大于”、“小于”、“超过”等理解为不包括本数；“以上”、“以下”、“以内”等理解为包括本数。

[0057] 以上所述仅为本实用新型的较佳实施例而已，并不用以限制本实用新型，凡在本实用新型的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本实用新型的保护范围之内。

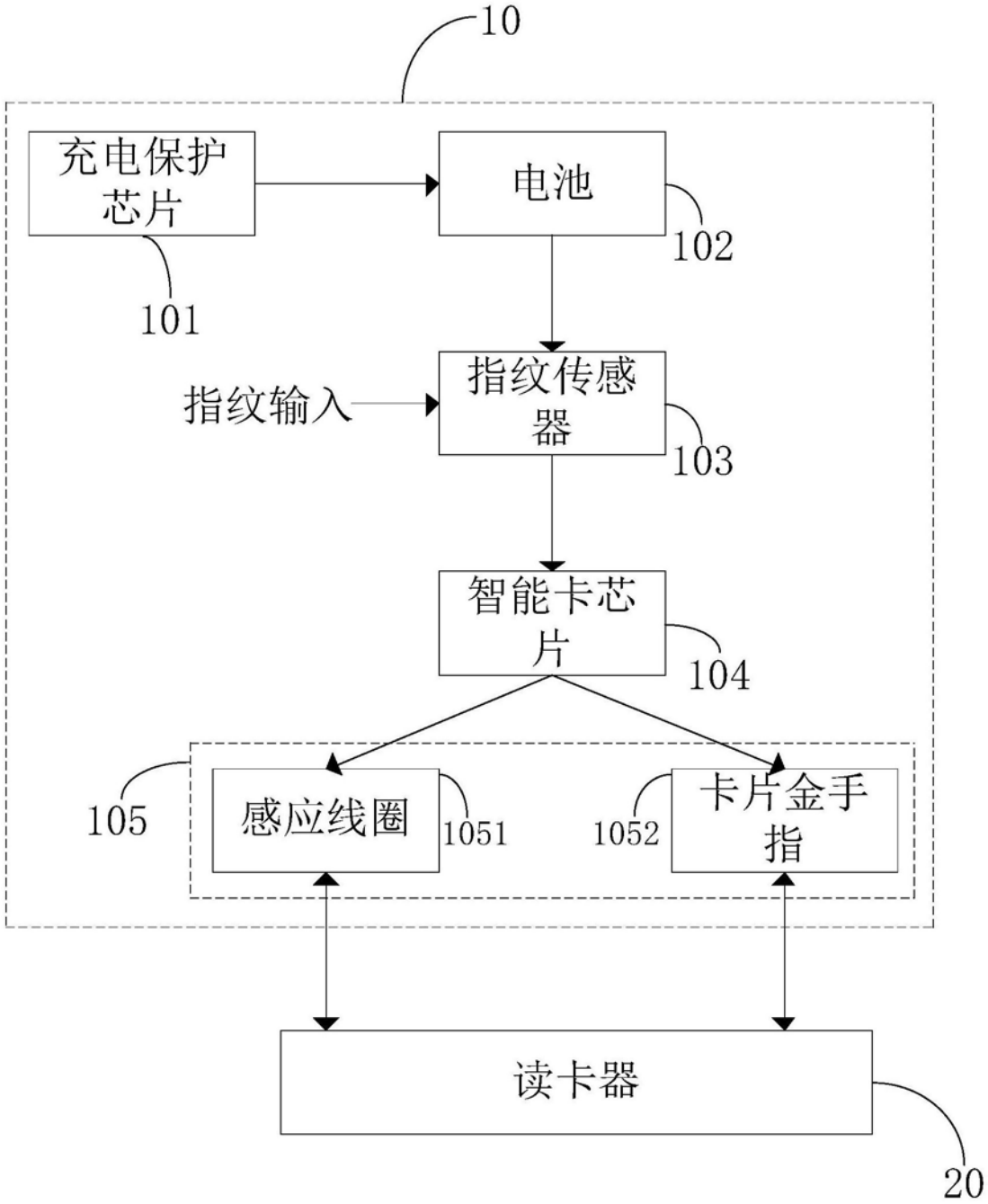

10
充电保护芯片
101
电池
102
指纹输入
指纹传感器
103
智能卡芯片
104
105
感应线圈
1051
1052
卡片金手指
读卡器
20

图1

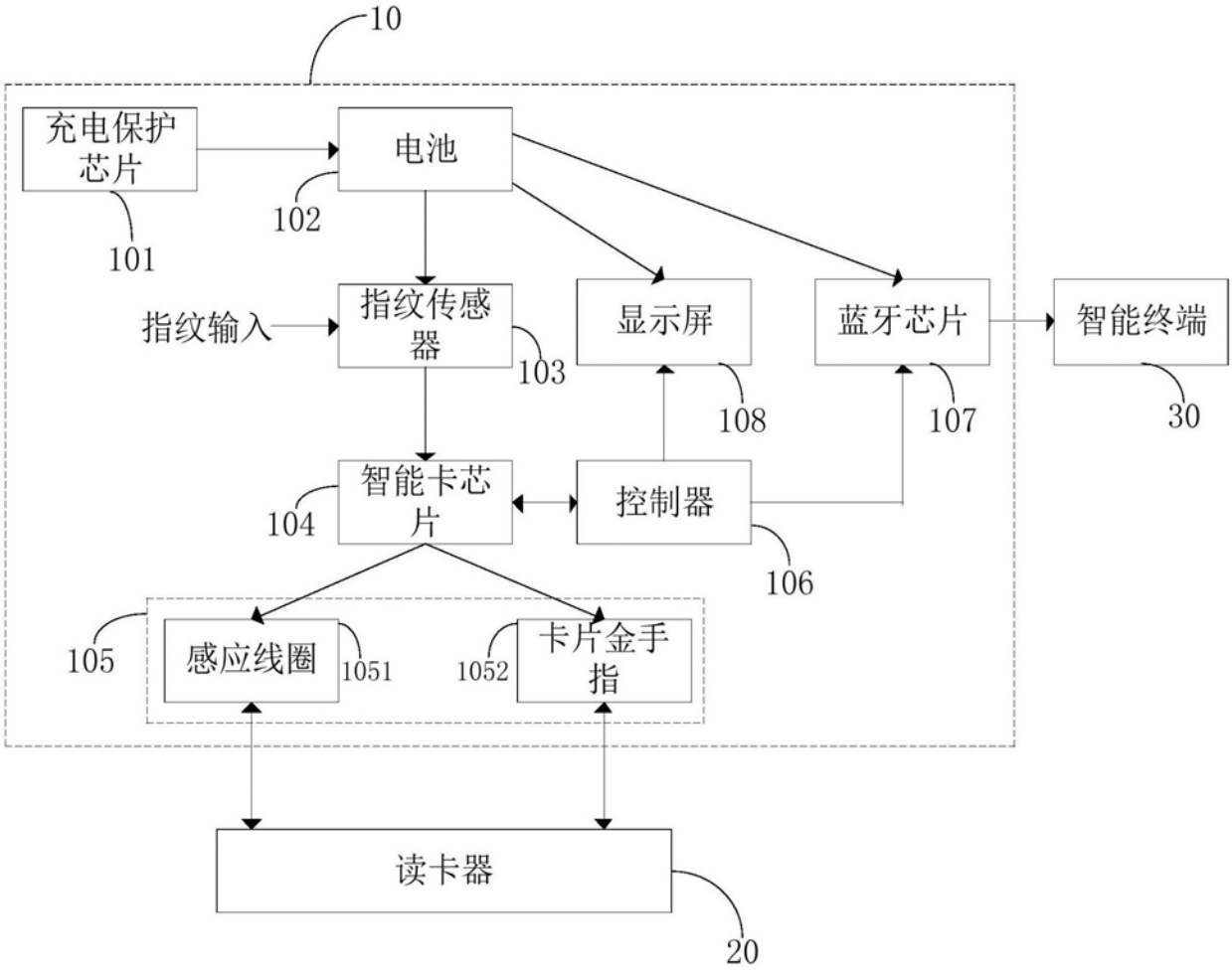

10
充电保护芯片
101
电池
102
指纹输入
指纹传感器
103
显示屏
108
蓝牙芯片
107
智能终端
30
智能卡芯片
104
控制器
106
105
感应线圈
1051
1052
卡片金手指
读卡器
20

图2

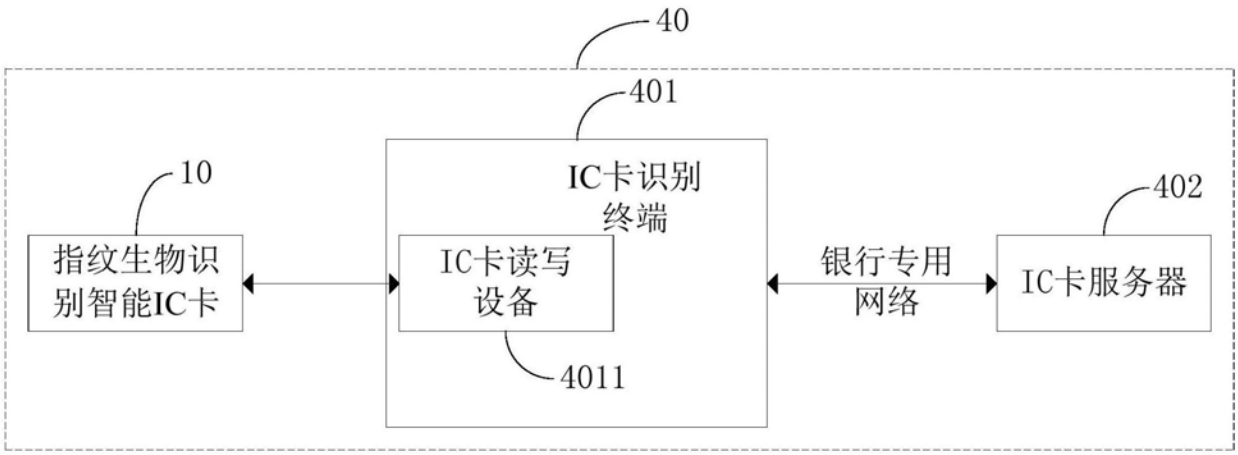

40
401
10
IC卡识别终端
402
指纹生物识别智能IC卡
IC卡读写设备
银行专用网络
IC卡服务器
4011

图3