(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295774 A
(43)申请公布日 2017.01.04

(21)申请号 201610644583.0

(22)申请日 2016.08.08

(71)申请人 苏海
地址 536000 广西壮族自治区北海市海城区北海大道科技大厦5楼

(72)发明人 苏海

(74)专利代理机构 北海市佳旺专利代理事务所（普通合伙）45115
代理人 黄建中

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

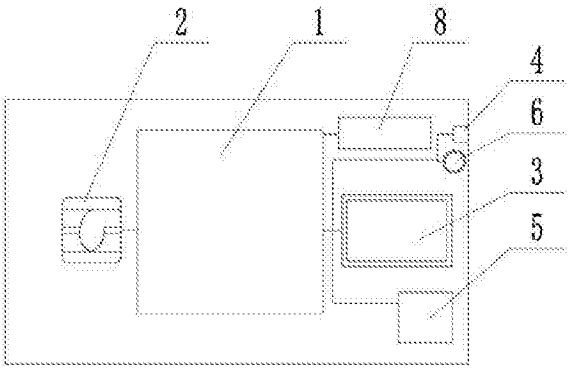
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种带指纹防伪的有源银行卡

(57)摘要

本发明涉及一种基于指纹信息识别的银行卡，包括正面标识层、芯片层、底面标识层，芯片层包括IC芯片(2)、微型控制器(1)、指纹识别器(3)、无线通信器模块(5)、发光LED(4)、蜂鸣器(6)、太阳能充电模块(8)，底面层包括信息磁条、银行卡签名标识、发卡银行警示说明，其特征在于：芯片层中IC芯片(2)有数据线与微型控制器(1)连接，微型控制器(1)分别与指纹识别器(3)、无线通信模块(5)、发光LED(4)、蜂鸣器(6)连接；正面层有持卡人二维码(7)；发光LED为红绿双色发光微型二极管或者红蓝双色发光二极管。通过指纹识别和二维码，较好地解决了银行卡被盗、信息被破解的风险，提高了银行卡的防伪功能，保护了银行卡的安全。



CN 106295774 A

1.一种带指纹防伪的有源银行卡，包括正面标识层、芯片层、底面标识层，芯片层包括IC芯片(2)、微型控制器(1)、指纹识别器(3)、无线通信器模块(5)、发光LED(4)、蜂鸣器(6)、太阳能充电模块(8)，底面层包括信息磁条、银行卡签名标识、发卡银行警示说明，其特征在于：芯片层中IC芯片(2)有数据线与微型控制器(1)连接，微型控制器(1)分别与指纹识别器(3)、无线通信模块(5)、发光LED(4)、蜂鸣器(6)连接；正面层有持卡人二维码(7)；发光LED为红绿双色发光微型二极管或者红蓝双色发光二极管。

2.如权利要求1所述一种带指纹防伪的有源银行卡，其特征在于：所述微型控制器(1)内置1枚微型纽扣电池，微型控制器(1)包含CPU模块、时钟比较模块、指纹存储和比较模块、无线通信控制模块、报警控制和驱动模块；时钟比较模块在指纹识别器有信号输入时或无线通信模块有信号时触发计时时钟，并唤醒微型控制器；在没有信号输入时，时钟比较模块触发微型控制器(1)进入睡眠状态；无线通信控制模块用于处理无线通信模块(5)接收和发送的信息；报警控制和驱动模块在核对指纹信息出错时驱动发光LED发出闪烁的红光并驱动蜂鸣器发声报警，在操作超时，驱动发光LED发出红绿或红蓝光交替闪烁。

3.如权利要求1所述一种带指纹防伪的有源银行卡，其特征在于：所述无线通信模块(5)可以是以太网通信模块，也可以是蓝牙模块，或者是以太网和蓝牙混合模块。

4.一种带指纹防伪的有源银行卡的使用方法：

(1)使用手机、计算机等无线通信设备触发银行卡，结束休眠，进入工作状态，发光二极管发出绿光；

(2)通过与微型控制器交换式通信，选择进入指纹设置模块，可以设置1-9个指纹数据选择，设置指纹的数量；设置成功后，发光LED的红、绿光交替闪烁，间隔100-200毫秒；

(3)持卡人通过指纹识别器，录入持卡人的指纹；录入成功后，发光LED发出绿光；

(4)指纹录入成功后，再设置银行卡触发后的工作时间1-5分钟，最后将手机、计算机等无线通信设备退出与银行卡的连接；发光LED在微型控制器断开无线通信设备100-500毫秒后，发光LED停止发光，银行卡进入休眠状态；

(5)持卡人需要使用银行卡时，首先用持卡人录入指纹的手指，通过指纹识别器触发微型控制器；其次微型控制器与存储的指纹数据进行指纹比较，符合则判断IC芯片是否有持卡人的指纹信息，有则比较指纹数据是否相符，指纹相符则通过数据线解除IC芯片的干扰码；接着，持卡人可以在设置的时间(1-5分钟)内正常使用银行卡，若设置时间到，需要持卡人继续通过指纹识别器延长银行卡工作时间；然后在完成银行卡操作后，IC芯片向微型控制器发出操作结束信息；最后持卡人退出银行卡，并向再次通过指纹识别器输入指纹信息，触发微型处理器进入休眠状态，等待下一次的触发；若持卡人未及时退出银行卡，或操作超时，微型处理器在时钟比较模块的触发下，通过报警控制和驱动模块，驱动蜂鸣器发声和发光LED发出交替闪烁的红绿光或红蓝光；同时向匹配的无线设备发出报警信息。

一种带指纹防伪的有源银行卡

技术领域

[0001] 本发明属于银行卡防伪识别技术领域，尤其涉及一种基于指纹信息识别的银行卡。

背景技术

[0002] 目前，银行卡犯罪常有发生，主要模式有：1、在ATM机里忘取银行卡，被别有用心的人取走现金；2、银行卡丢失，被犯罪份子破解了银行卡的数字密码；3、被犯罪份子通过POS机或其它渠道获取了银行卡信息，伪造银行卡。由于现有的银行卡缺乏交互式验证手段，现有的银行卡6位数字密码极易被破解，从而导致持卡人的损失。文献103400182A、203070421U、203930906U、205158408U、205103928U等给出一些利用指纹技术解决银行卡防伪的方法。上述文献存在的问题是不能完全解决现有银行卡犯罪的三种主要形式，任然存在使用上的缺陷。

发明内容

[0003] 本发明的目的在于克服现有技术的不足，提供一种带有指纹识别防伪功能的有源银行卡。

[0004] 一种带指纹防伪的有源银行卡，由正面标识层、芯片层、底面标识层组成。芯片层包括IC芯片、微型控制器、指纹识别器、无线通信器模块、发光LED、蜂鸣器、太阳能充电模块。正面层包括银行信息、卡号、ATM操作提示信息、持卡人二维码信息。底面层包括信息磁条、银行卡签名标识、发卡银行警示说明。

[0005] 芯片层中IC芯片有数据线与微型控制器连接。微型控制器分别与指纹识别器、无线通信模块、发光LED、蜂鸣器连接。太阳能充电模块为微型控制器提供电能补充。发光LED为红绿双色发光微型二极管或者红蓝双色发光二极管。无线通信模块可以是以太网通信模块，也可以是蓝牙模块，或者是以太网和蓝牙混合模块。微型控制器内置1枚微型纽扣电池，提供电源和储能。微型控制器包含CPU模块、时钟比较模块、指纹存储和比较模块、无线通信控制模块、报警控制和驱动模块。CPU模块负责微型控制器的运算、信息处理。时钟比较模块在指纹识别器有信号输入时或无线通信模块有信号时触发计时时钟，并唤醒微型控制器；在没有信号输入时，触发微型控制器进入睡眠状态。无线通信控制模块用于处理无线通信模块接收和发送的信息。报警控制和驱动模块在核对指纹信息出错时驱动发光LED发出闪烁的红光并驱动蜂鸣器发声报警；在操作超时，驱动发光LED发出红绿光交替闪烁。

[0006] 微型控制器电路采用微型贴片电子元件通过薄膜电路连接，然后用环氧树脂固封，最后热风整平。通过固封提高了电路运行的可靠性，同时可以防止犯罪分子对电路的破解和克隆。

[0007] 完成芯片层的电路测试、封装后，将正面标识层、芯片层、底面标识层通过压模机粘合在一起，得到带指纹防伪的有源银行卡。

[0008] IC芯片通过数据线与微型控制器连接。IC芯片可以通过发卡银行录入持卡人的指

纹信息。对于没有录入持卡人指纹信息的IC芯片，微型控制器向IC芯片发出干扰码。干扰码可以导致该IC芯片无法正常使用。

[0009] 一种带指纹防伪的有源银行卡的使用方法：

(1)使用手机、计算机等无线通信设备触发银行卡，结束休眠，进入工作状态，发光二极管发出绿光。

[0010] (2)通过与微型控制器交换式通信，选择进入指纹设置模块，可以设置1-9个指纹数据选择，设置指纹的数量；设置成功后，发光LED的红、绿光交替闪烁，间隔100-200毫秒。

[0011] (3)持卡人通过指纹识别器，录入持卡人的指纹；录入成功后，发光LED发出绿光。

[0012] (4)指纹录入成功后，再设置银行卡触发后的工作时间1-5分钟，最后将手机、计算机等无线通信设备退出与银行卡的连接；发光LED在微型控制器断开无线通信设备100-500毫秒后，发光LED停止发光，银行卡进入休眠状态。

[0013] (5)持卡人需要使用银行卡时，首先用持卡人录入指纹的手指，通过指纹识别器触发微型控制器；其次微型控制器与存储的指纹数据进行指纹比较，符合则判断IC芯片是否有持卡人的指纹信息，有则比较指纹数据是否相符，指纹相符则通过数据线解除IC芯片的干扰码；接着，持卡人可以在设置的时间(1-5分钟)内正常使用银行卡，若设置时间到，需要持卡人继续通过指纹识别器延长银行卡工作时间；然后在完成银行卡操作后，IC芯片向微型控制器发出操作结束信息；最后持卡人退出银行卡，并向再次通过指纹识别器输入指纹信息，触发微型处理器进入休眠状态，等待下一次的触发。若持卡人未及时退出银行卡，或操作超时，微型处理器在时钟比较模块的触发下，通过报警控制和驱动模块，驱动蜂鸣器发声和发光LED发出交替闪烁的红绿光或红蓝光；同时向匹配的无线设备发出报警信息。

[0014] 微型控制器还可以录入持卡人的二维码信息，或者通过发卡银行向IC芯片录入持卡人的二维码信息，通过网络验证持卡人的信息，增强银行卡的防伪功能。

[0015] 采用上述指纹防伪和二维码信息后，较好地解决了银行卡被盗、信息被破解的风险，提高了银行卡的防伪功能，保护了银行卡的安全。由于有干扰码，可以防止银行卡丢失后被克隆IC芯片。微型控制固封后，降低了破解的风险。在ATM机中遗忘银行卡，银行卡通过声光报警和无线信号报警，提醒持卡人，降低被盗刷的风险。

附图说明

[0016] 图1 本发明芯片层结构图

图2 本发明银行卡正视图

图中标号说明：1、微型控制器，2、IC芯片，3、指纹识别器，4、发光LED，5、无线通信模块，6、蜂鸣器，7、二维码，8、太阳能充电模块。

具体实施方式

[0017] 下面结合说明书附图对本发明的具体实施方式作进一步详细的说明。

[0018] 如附图1和图2所示，一种带指纹防伪的有源银行卡，由正面标识层、芯片层、底面标识层组成。芯片层包括IC芯片2、微型控制器1、指纹识别器3、无线通信器模块5、发光LED4、蜂鸣器6、太阳能充电模块8。正面层包括银行信息、卡号、ATM操作提示信息、持卡人二维码7信息。底面层包括信息磁条、银行卡签名标识、发卡银行警示说明。

[0019] 芯片层中IC芯片2有数据线与微型控制器1连接。微型控制器1分别与指纹识别器3、无线通信模块5、发光LED4、蜂鸣器6连接。太阳能充电模块8为微型控制器提供电能补充。发光LED为红绿双色发光微型二极管。无线通信模块是蓝牙模块。微型控制器1内置1枚微型纽扣电池，提供电源和储能。微型控制器1包含CPU模块、时钟比较模块、指纹存储和比较模块、无线通信控制模块、报警控制和驱动模块。CPU模块负责微型控制器的运算、信息处理。时钟比较模块在指纹识别器有信号输入时触发计时时钟，并唤醒微型控制器；在没有信号输入时，触发微型控制器1进入睡眠状态。无线通信控制模块用于处理无线通信模块5接收和发送的信息。报警控制和驱动模块在核对指纹信息出错时，驱动发光LED4发出闪烁的红光并驱动蜂鸣器发声报警；在操作超时，驱动发光LED4发出红绿光交替闪烁。

[0020] 芯片层中的微型控制器电路采用微型贴片电子元件通过薄膜电路连接，然后用环氧树脂固封，最后热风整平。通过固封提高了电路运行的可靠性，同时可以防止犯罪分子对电路的破解和克隆。其余电子元器件也通过薄膜电路相连接，并用环氧树脂固封为一个整体。

[0021] 完成芯片层的电路测试、封装后，将正面标识层、芯片层、底面标识层通过压模机粘合在一起，得到带指纹防伪的有源银行卡。

[0022] IC芯片2通过数据线与微型控制器1连接。IC芯片2可以通过发卡银行录入持卡人的指纹信息。对于没有录入持卡人指纹信息的IC芯片2，微型控制器1向IC芯片2发出干扰码。干扰码可以导致该IC芯片2无法正常使用。

[0023] 一种带指纹防伪的有源银行卡的使用方法：

(1)使用手机、计算机等无线通信设备触发银行卡，结束休眠，进入工作状态，发光二极管发出绿光。

[0024] (2)通过与微型控制器交换式通信，选择进入指纹设置模块，可以设置1-9个指纹数据选择，设置指纹的数量；设置成功后，发光LED的红、绿光交替闪烁，间隔100-200毫秒。

[0025] (3)持卡人通过指纹识别器，录入持卡人的指纹；录入成功后，发光LED发出绿光。

[0026] (4)指纹录入成功后，再设置银行卡触发后的工作时间1-5分钟，最后将手机、计算机等无线通信设备退出与银行卡的连接；发光LED在微型控制器断开无线通信设备100-500毫秒后，发光LED停止发光，银行卡进入休眠状态。

[0027] (5)持卡人需要使用银行卡时，首先用持卡人录入指纹的手指，通过指纹识别器触发微型控制器；其次微型控制器与存储的指纹数据进行指纹比较，符合则判断IC芯片是否有持卡人的指纹信息，有则比较指纹数据是否相符，指纹相符则通过数据线解除IC芯片的干扰码；接着，持卡人可以在设置的时间(1-5分钟)内正常使用银行卡，若设置时间到，需要持卡人继续通过指纹识别器延长银行卡工作时间；然后在完成银行卡操作后，IC芯片向微型控制器发出操作结束信息；最后持卡人退出银行卡，并向再次通过指纹识别器输入指纹信息，触发微型处理器进入休眠状态，等待下一次的触发。若持卡人未及时退出银行卡，或操作超时，微型处理器在时钟比较模块的触发下，通过报警控制和驱动模块，驱动蜂鸣器发声和发光LED发出交替闪烁的红绿光；同时向匹配的无线设备发出报警信息。

[0028] 微型控制器还可以录入持卡人的二维码信息，或者通过发卡银行向IC芯片录入持卡人的二维码信息，通过网络验证持卡人的信息，增强银行卡的防伪功能。

[0029] 通过指纹识别和二维码，较好地解决了银行卡被盗、信息被破解的风险，提高了银

行卡的防伪功能，保护了银行卡的安全。

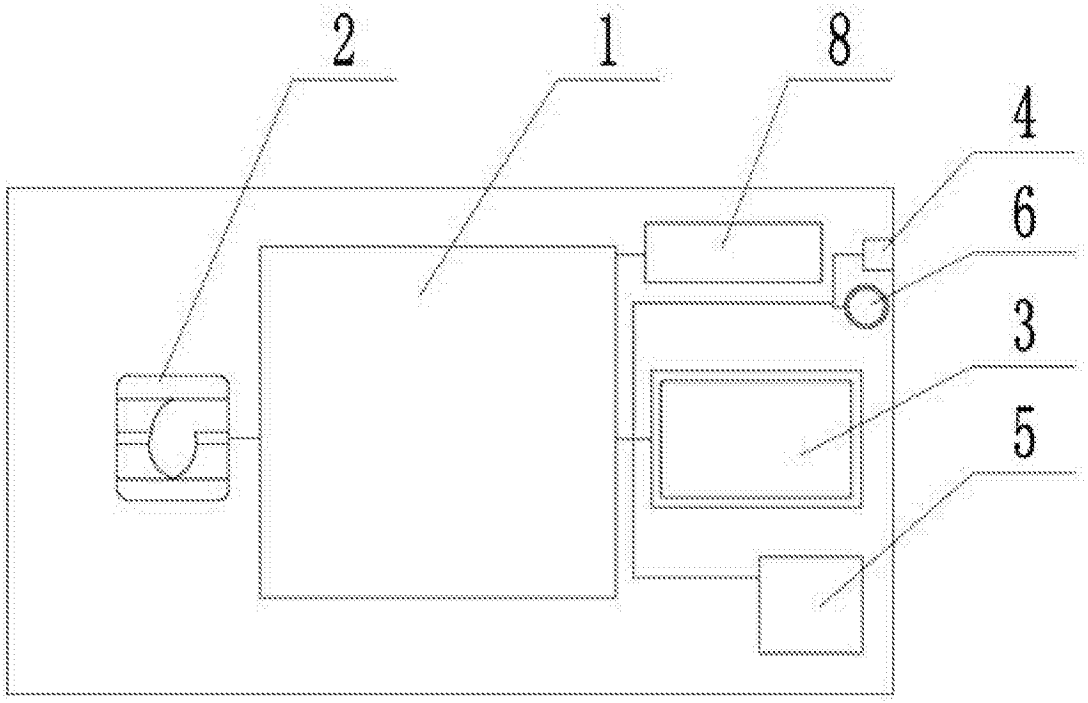


图1

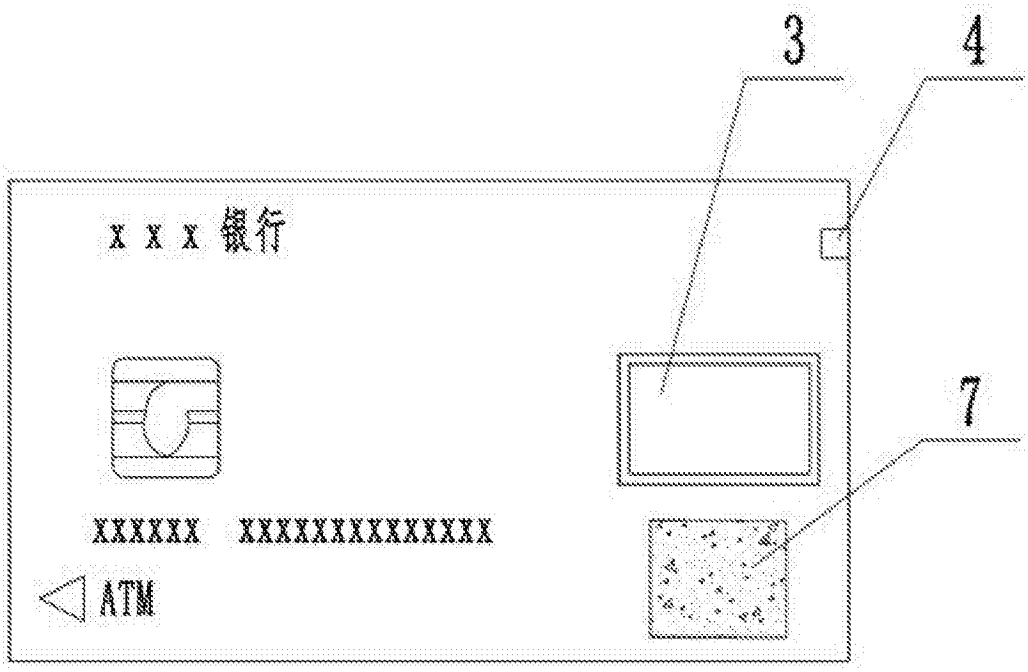


图2