[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06K 17/00 (2006.01)
G06K 9/00 (2006.01)
G07F 19/00 (2006.01)
G07F 7/08 (2006.01)
G07F 7/00 (2006.01)

[12] 实用新型专利说明书

专利号 ZL 200520104273.7

[45] 授权公告日 2007 年 5 月 23 日

[11] 授权公告号 CN 2904122Y

[22] 申请日 2005.8.23
[21] 申请号 200520104273.7
[73] 专利权人 北京中天一维科技有限公司
地址 100098 北京市海淀区知春路甲 48 号盈都大厦 C 座 1－11D
[72] 设计人 王 珽 韩晓舟

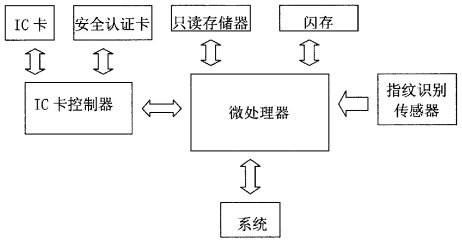
[74] 专利代理机构 北京中博世达专利商标代理有限公司
代理人 王黎延
权利要求书 2 页 说明书 5 页 附图 1 页

[54] 实用新型名称

基于 IC 卡技术的密码辅助记忆系统

[57] 摘要

本实用新型公开了一种基于 IC 卡技术的密码辅助记忆系统，包括有用于存储应用固件的电可擦写只读存储器，用于存储用户银行帐户相关信息的缓存，用于存储用户银行帐户及对应设定密码的 IC 卡、用于 IC 卡读取的 IC 卡控制器和用于 IC 卡识别的微处理器，所述电可擦写只读存储器、缓存及 IC 卡控制器均电连接于所述微处理器，所述 IC 卡可插入 IC 卡控制器并由该 IC 卡控制器读取 IC 卡内存储的信息。 本实用新型使用存储有储户密码和相应帐户信息的 IC 卡而替代传统的磁条卡，并采用 IC 卡预先存储待识别用户的指纹信息，作身份验证的基础指纹信息，能很好地增强银行系统的安全性。



1、一种基于 IC 卡技术的密码辅助记忆系统，其特征在于，该系统包括有用于存储应用固件的电可擦写只读存储器，用于存储用户银行帐户相关信息的缓存，用于存储用户银行帐户及对应设定密码的 IC 卡、用于 IC 卡读取的 IC 卡控制器和用于 IC 卡识别的微处理器，所述电可擦写只读存储器、缓存及 IC 卡控制器均电连接于所述微处理器，所述 IC 卡可插入 IC 卡控制器并由该 IC 卡控制器读取 IC 卡内存储的信息。

2、根据权利要求 1 所述的基于 IC 卡技术的密码辅助记忆系统，其特征在于，该系统还包括用于指纹信息提取的压电 / 热电真皮层指纹传感器，所述指纹传感器通过 A/D 转换器连接于所述微处理器；对应地，所述 IC 卡内存储有用户的指纹信息。

3、根据权利要求 1 所述的基于 IC 卡技术的密码辅助记忆系统，其特征在于，该系统还包括用于识别所述 IC 卡身份的安全认证卡，该安全认证卡电连接于所述 IC 卡控制器。

4、根据权利要求 1 至 3 中任一权利要求所述的基于 IC 卡技术的密码辅助记忆系统，其特征在于，所述 IC 卡可为带卡操作系统的 CPU 卡，具体包括 CPU、随机存储器、只读存储器和电可擦写只读存储器，所述随机存储器、只读存储器和电可擦写只读存储器通过数据及控制线连接于所述 CPU。

5、根据权利要求 3 所述的基于 IC 卡技术的密码辅助记忆系统，其特征在于，所述安全认证卡包括微处理器、内存、程序区、数据区及通讯端口，所述内存、程序区、数据区及通讯端口通过数据及控制线连接于所述微处理器。

6、根据权利要求 1 至 3 中任一权利要求所述的基于 IC 卡技术的密码辅助记忆系统，其特征在于，所述缓存及电可擦写只读存储器与所述

微处理器的电连接具体是通过 DMA 总线而连接的；所述 IC 卡及安全认证卡与 IC 卡控制器的电连接具体是通过 7816 接口连接的；所述系统及 IC 卡控制器与所述微处理器的电连接具体是通过串行通信接口而连接的。

7、根据权利要求 6 所述的基于 IC 卡技术的密码辅助记忆系统，其特征在于，所述串行通信接口可为 RS232、RS485、USB 接口或 1394 接口。

基于IC卡技术的密码辅助记忆系统

技术领域

本实用新型涉及一种基于IC卡技术的密码辅助记忆系统，尤其涉及一种可使用指纹识别技术进行密码辅助记忆的系统。

背景技术

目前的储户银行卡主要采用磁条卡，因为磁条卡没有完整的加密体系，很容易被不法分子复制，所以近年来利用银行卡犯罪的案例越来越多。据公安部统计：2003年，全国公安机关共立金融票证犯罪案件3800余起，涉案金额约34亿元，这不仅使储户和银行蒙受了巨大的经济损失，而且给银行业造成了很大的负面影响，给中国的银行卡的普及蒙上了一层阴影。

不法分子利用银行卡盗取储户资金主要有以下几种方法：

不法分子通过“窃号＋烧卡”的方法盗取储户资金。不法分子在ATM自动取款机上安装摄像探头，储户取完钱后随手扔掉交易流水单，他们利用这张单子盗取银行卡信息并制作伪卡，然后使用偷拍到的用户密码，盗取储户的资金。

不法分子制造 “吞卡”假象获取用户卡和密码。不法分子在ATM机上装摄像探头，在插卡口处安装外接吞卡装置。当储户提款的时候，卡被吞卡装置吞入，无法取出。在客户取款失败离开后，不法分子取出银行卡，利用探头获得的密码取款。

从以上几种犯罪方式可以看出，储户银行卡上的资金被窃取主要是因为不法分子利用了储户使用键盘输入密码时隐蔽性不好，易被窥视的问题，获取储户密码。这给了不法分子以可乘之机。一旦出现储户账户上的资金被窃取，不但对储户造成经济上的损失，同时储户通常会认为是银行的工作失误所致，这样就造成权责不明，给银行的声誉造成恶劣的影响。

与此同时，由于在日常生活中有越来越多的使用密码的地方，而且为了安全考虑，设置的各个密码又不相同。以至于经常会忘记自己设置的密码是什么。尤其是对于一些老年人，经常忘记了自己的银行卡的密码，这样既影响了储户取款，又降低了银行的工作效率。

可见，目前利用密码进行身份认证的方式存在较大的安全缺陷，有较大的安全风险。

实用新型内容

针对上述现有银行磁条卡认证系统中所存在的问题和不足，本实用新型的目的是提供一种安全可靠的基于 IC 卡技术的密码辅助记忆系统。

本实用新型是这样实现的：一种基于 IC 卡技术的密码辅助记忆系统，包括有用于存储应用固件的电可擦写只读存储器，用于存储用户银行帐户相关信息的缓存，用于存储用户银行帐户及对应设定密码的 IC 卡、用于 IC 卡读取的 IC 卡控制器和用于 IC 卡识别的微处理器（Micro Controller Unit，MCU），所述电可擦写只读存储器、缓存及 IC 卡控制器均电连接于所述微处理器，所述 IC 卡可插入 IC 卡控制器并由该 IC 卡控制器读取 IC 卡内存储的信息。

优选地，该系统还包括用于指纹信息提取的压电/热电真皮层指纹传感器，所述指纹传感器通过 A/D 转换器连接于所述微处理器；对应地，所述 IC 卡内存储有用户的指纹信息。

优选地，该系统还包括用于识别所述 IC 卡身份的安全认证（PSAM）卡，该安全认证卡电连接于所述 IC 卡控制器。

本实用新型使用存储有储户密码和相应帐户信息的 IC 卡作为密码卡，并采用 IC 卡预先存储待识别用户的指纹信息，作身份验证的基础指纹信息；本实用新型将先进的指纹识别技术、计算机控制处理技术、安全认证卡技术、通信技术相结合，并使用 IC 卡作为储户密码卡，进行指纹信息的存储，实现了身份认证的唯一性、准确性、不可丢失性、不可仿制和不可授予性以及不可抵赖性。

真正实现了系统对“人”的识别。另外，本实用新型可实现身份认证整个过程实现脱机比对，增加了整个系统的安全性。本实用新型能很好地增强银行系统的安全性。

附图说明

图 1 是本实用新型的结构示意图；

图 2 是本实用新型带 COS 的 IC 卡结构示意图。

具体实施方式

以下配合附图对本实用新型进行详细说明。

如图 1 所示，本实用新型包括闪存（Flash）、电可擦写只读存储器（EEPROM）、微处理器（MCU）、IC 卡（IC Card）和 IC 卡控制器（IC Card Contoller），如图中虚框中所示的。IC 卡及安全认证卡通过 7816 接口与 IC 卡控制器连接；IC 卡控制器通过 RS232 或 RS485 串行通信接口连接于微处理器。这里，串行通信接口也可以是多通道缓冲串口（McBSP）、连接口（Linkport）、内部集成电路总线（I2C）接口、串行外设接口（SPI）等。闪存及电可擦写只读存储器与微处理器通过 DMA（直接存储器存取）总线连接。本实用新型的 IC 卡可使用任何可以进行信息存储的 IC 卡。IC 卡中预先存有储用户的帐号及其对应的密码信息。可以在 IC 卡中存储多组帐号和密码，每组密码对应一个简捷的数字编码。如果 IC 卡中只有一个帐户和密码则不用编码，缺省为此帐户和密码。对于控制读出 IC 卡的密码用户可以设置开卡密码，也可以不进行设置。

首先将储户原来使用的密码小键盘换成带 IC 卡读卡器的密码小键盘（IC 卡密码键盘，也可不用设置，直接通过识别 IC 卡 ID 也可）。当储户要进行提款交易时，同原来一样是先刷卡/存折，然后储户可以选择使用原来的在密码小键盘上输入密码的方式或者使用密码 IC 卡的方式。如果储户选择使用密码 IC 卡验证的方式，此时用户需要在 IC 卡密码键盘上插入密码 IC 卡。如果之前用户设

置了开卡密码，用户输入开卡密码(如果没有设置不用输入)。认证通过后，用户输入帐号编码(如果只有一个帐号，则不用输入)，IC 卡键盘将 IC 卡中对应的密码取出，发送给系统，如果认证通过就可以提交给后台进行提款交易。

本实用新型还可以和指纹识别技术相结合，用指纹识别作为 IC 卡的开卡认证方式。指纹识别技术是生物识别技术的一种。它使用指纹特征作为对个人身份认证的方法。该算法首先通过指纹识别传感器(FringerprintSensor)读取储户的指纹图象。在获取指纹图象之后，识别芯片对图象进行初步处理，使之更加清晰可辨。指纹由多种“脊”状图形构成，类似于山脊，由于纹路不连续，脊状图形多种多样，诸如分岔、弧形、交叉、三角等，称为指纹特征值。接下来，指纹辨识软件建立指纹的“数字表示特征”数据，将指纹特征值转换成特征数据。识别软件将这些脊状图形进行坐标定位，进而从坐标位置上标示出特征点。用户的指纹信息经过以上算法转换后存储在个人的密码 IC 卡中。具体认证过程为：储户原来使用的密码小键盘换成带指纹识别和 IC 卡读卡器的密码小键盘。当储户要进行提款交易时，仍然是先刷卡 / 存折，然后储户可以选择使用原有的在密码小键盘上输入密码的方式或者使用指纹认证的方式。如果选择使用指纹验证的方式，此时用户需要在指纹 IC 卡键盘上插入密码 IC 卡，同时进行即时采集储户的指纹信息，在小键盘内进行指纹验证，认证通过后，用户输入帐号编码(如果只有一个帐号，则不用输入)，指纹 IC 卡键盘将密码 IC 卡中对应的密码取出，发送给系统，认证通过后就可以提交给后台进行提款交易。

如图 2 所示，为了加强系统的安全性，IC 卡可采用带 COS(Card Operation System)的 CPU 卡，该卡的组成部分及功能如下：CPU 及加密逻辑：保证 EEPROM 中数据安全，使外界不能用任何非法手段获取 EEPROM 中的数据。RAM：COS 工作时存放命令参数、返回结果、安全状态及临时工作密钥的区域。ROM：存放 COS 程序的区域。EEPROM：存放储户应用数据区域，COS 将储户数据以文件形式保存在 EEPROM 中。储户指纹信息即存储在这个区域。本实用新型的密码 IC 卡将其中存储的指纹模板与微处理芯片送进的指纹模板进行比对，如果比

对成功，则可以进行读出密码卡内的密码，如果比对失败则无法进行密码卡的读取。这种方法指纹比对在卡内完成，即整个比对过程都在卡内加密的环境中完成，因此具有更高的安全性。

为了保证IC卡的合法性，避免被仿制和伪造，本实用新型设置了PSAM卡，对IC卡的合法性进行验证。PSAM卡由以下部分组成：微处理器（CPU）及加密逻辑、内存（RAM）、程序区（ROM）、数据区（EEPROM）及通讯端口（I/O）。用户数据存放在被加密逻辑保护的EEPROM中，COS掩膜在ROM中，以保证代码安全。在操作卡片过程中，过程密钥被生成后放在RAM空间中，并且一些临时数据也将保存在RAM中，掉电后自动丢失，保证其安全性。PSAM卡和身份IC卡在发卡的过程中存储有一对密钥，当IC卡插入本实用新型的时候，PSAM卡会自动验证密码IC卡密钥的合法性，如果验证通过，则可以读取密码IC卡中信息，否则验证中断。利用PSAM卡，大大提高了本实用新型身份验证的安全性和可靠性。

如图1所示， MCU与系统之间通过RS232、RS485或USB、1394等连接方式连接。本实用新型的MCU可为DSP芯片或ARM处理器。DSP芯片是一种具有特殊结构的微处理器。它可以用来快速地实现各种数字信号处理算法，尤其广泛应用在二维和三维图形处理、图像压缩与传输、图像增强、动画、机器人视觉等方面。ARM是一种32位处理器，是一款高性能、低功耗、低成本的嵌入式微处理器。作为32位嵌入式RISC微处理器它提供嵌入式ICE-RT逻辑和嵌入式跟踪宏核(ETMS))两个前沿特性。智能卡和SIM卡的安全应用是ARM处理器主要的应用领域之一。当在指纹传感器上完成指纹采集过程后MCU芯片调用指纹比对算法，通过模糊比较的方法，把IC卡中的指纹模板和实时采集到的指纹的模板进行比较，计算出它们的相似程度，最终得到两个指纹的匹配结果，并将比对结果发送回给系统。本实用新型的MCU可采用TI公司的C5000、C6000DSP芯片或ARM公司的ARM7或ARM9。本领域技术人员应当理解，使用其它类型的MCU也可实现本实用新型的技术方案。

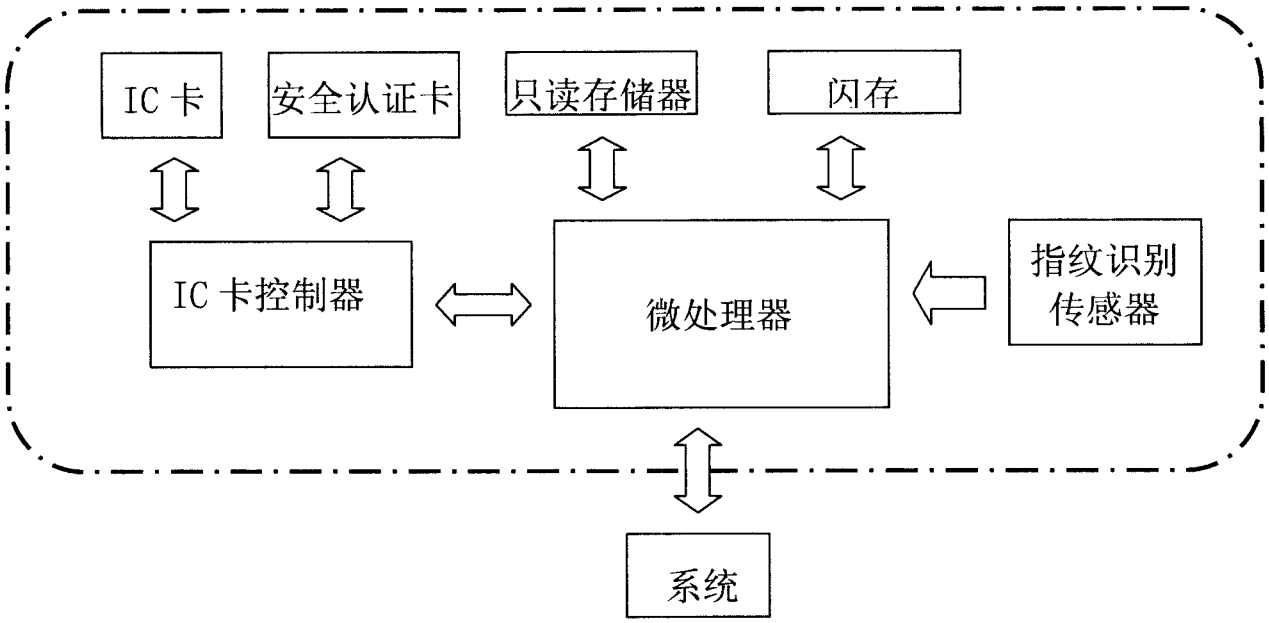

IC 卡
安全认证卡
只读存储器
闪存
IC 卡控制器
微处理器
指纹识别
传感器
系统

图 1

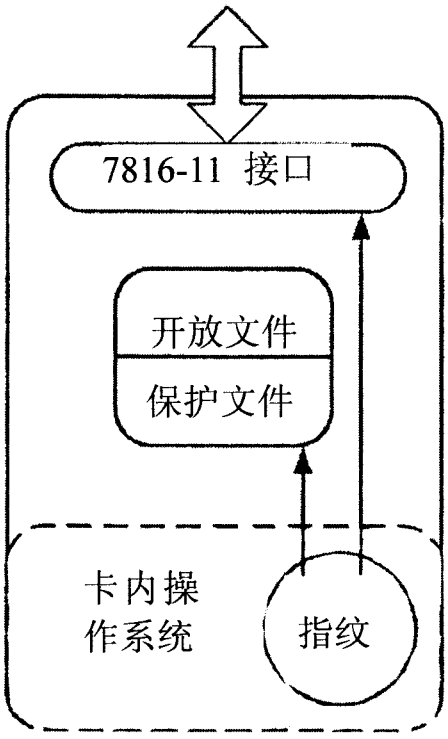

7816-11 接口
开放文件
保护文件
卡内操
作系统
指纹

图 2