

(12) 发明专利申请

(10) 申请公布号 CN 102932557 A

(43) 申请公布日 2013. 02. 13

(21) 申请号 201210512549. X

(22) 申请日 2012. 11. 30

(71) 申请人 魏红霞

地址 212000 江苏省镇江市京口区谏壁镇于山街 32-91 号

(72) 发明人 魏红霞

(51) Int. Cl.

H04M 1/725 (2006. 01)

H04W 12/06 (2009. 01)

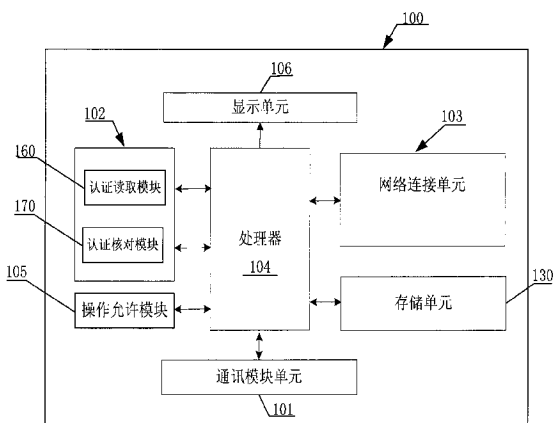
权利要求书 1 页 说明书 4 页 附图 1 页

(54) 发明名称

带安全认证装置的智能手机

(57) 摘要

本发明提供一种带有安全认证装置的智能手机,具有安全认证功能,能够识别不同的认证信息,并依据该认证信息执行对应的功能操作。该智能手机包括处理器、通讯模块单元、存储单元、用户认证模块和操作允许模块;本发明提高了智能手机操作的安全性能,能防止因未经授权而执行操作产生的安全风险。



1. 一种带安全认证装置的智能手机,其特征在于包括:
处理器,控制智能手机的各单元和模块的执行;
通讯模块单元,连接处理器,完成通讯功能;
存储单元,连接处理器,用于存储相关文件;
用户认证模块,连接处理器,用于获取并验证一外部提供的认证信息;以及
操作允许模块,连接处理器,基于前述验证结果允许或拒绝一控制指令。
2. 根据权利要求1所述的智能手机,其特征在于,所述用户认证模块包括用于获取所述认证信息的认证读取模块和用于验证所述认证信息的认证核对模块。
3. 根据权利要求2所述的智能手机,其特征在于,所述认证信息预设在一智能卡中。
4. 根据权利要求3所述的智能手机,其特征在于,所述认证信息包括用户身份认证等信息。
5. 根据权利要求4所述的智能手机,其特征在于,所述认证信息以加密的形式存储,所述用户认证模块具有解密单元。
6. 根据权利要求4所述的智能手机,其特征在于,所述存储单元包括一查询信息模块,记录所述认证信息的至少一项内容和操作记录,以供查询。
7. 根据权利要求1所述的智能手机,,其特征在于,所述存储单元中预设一验证信息,所述用户认证模块比较该验证信息与所述认证信息而产生所述验证结果。
8. 根据权利要求1所述的智能手机,其特征在于,该智能手机还包括一个显示单元,显示所述外部提供的认证信息和改写后的认证信息。

带安全认证装置的智能手机

技术领域

[0001] 本发明涉及手机领域,具体而言是关于一种带有安全认证装置的智能手机。

背景技术

[0002] 智能手机 (Smartphone) 是一种安装了相应开放式操作系统的手机。通常使用不同的操作系统,他们之间的应用软件互不兼容。因为可以安装第三方软件,所以智能手机有丰富的功能。

[0003] 智能手机的诞生,是掌上电脑 (PocketPC) 演变而来的。最早的掌上电脑是不具备手机的通话功能,但是随着用户对于掌上电脑的个人信息服务方面功能的依赖的提升,由不习惯于随时都携带手机和 PPC 两个设备,所以厂商将掌上电脑的系统移植到了手机中,于是才出现了智能手机这个概念。智能手机比传统的手机具有更多的综合性处理能力功能,比如 Symbian 操作系统的 S60 系列、Windows Mobile 操作系统的 Windows Mobile Smartphone 系列;也可以是传统 PDA 加上手机通信功能,比如 Windows Mobile 操作系统的 Windows Mobile Pocket PC Phone 系列、Palm 操作系统的 Treo 系列;也可以是其它独立类型,比如 Symbian 操作系统的 S60、Symbian3,以及一些 Linux 操作系统的智能手机。然而,就新近的发展来看,这些智能手机的类型有相融合的趋势;智能手机具有五大特点:

[0004] 1. 具备无线接入互联网的能力,即需要支持 GSM 网络下的 GPRS 或者 CDMA 网络的 CDMA 1X 或 3G (wcdma、cdma-evdo、TD-scdma) 网络,甚至 4G (HSPA+、FDD-LTE、TDD-LTE)。

[0005] 2. 具有 PDA 的功能,包括 PIM (个人信息管理),日程记事,任务安排,多媒体应用,浏览网页。

[0006] 3. 具有开放性的操作系统,拥有独立的核心处理器 (CPU) 和内存,可以安装更多的应用程序,使智能手机的功能可以得到无限扩展。

[0007] 4. 可以根据个人需要扩展机器功能。根据个人需要,实时扩展机器内置功能,以及软件升级,智能识别软件兼容性,实现了软件市场同步的人性化功能。

[0008] 5. 扩展性能强,第三方软件支持多。

[0009] 从广义上说,智能手机除了具备手机的通话功能外,还具备了 PDA 的大部分功能,特别是个人信息管理以及基于无线数据通信的浏览器, GPS 和电子邮件功能。智能手机为用户提供了足够的屏幕尺寸和带宽,既方便随身携带,又为软件运行和内容服务提供了广阔的舞台,很多增值业务可以就此展开,如:股票、新闻、天气、交通、商品、应用程序下载、音乐图片下载等等。结合 3G 通信网络的支持,智能手机的发展趋势,势必将成为一个功能强大,集通话、短信、网络接入、影视娱乐为一体的综合性个人手持终端设备,一般来说,智能手机具有以下系统、装置和功能:

[0010] 1. 作业系统:一般来说,智能手机将基于一个操作系统,可以运行程序。

[0011] 软件:几乎所有的手机包括某种形式的软件(最基本的模型是包括包括一个地址簿或某种形式的联系助理,例如),智能手机将有能力做更多的工作。它可让您创建和编辑微软 Office 文档 - 或至少查看档案。它可能允许您下载的应用,如个人和企业财务助理。

或者,它可让您编辑照片,通过全球定位系统规划行车路线,并创建一个播放数字音乐。

[0012] 2. Web 访问:更多智能手机可以用更快的速度进入该网站,该手机能连接 3G 数据网络,并增加了 Wi-Fi 的支持。不过,并不是所有的智能手机提供高速上网,但是他们都提供某种形式的访问。您可以使用手机浏览您最喜爱的网站。

[0013] 3. QWERTY 键盘:根据我们的定义,智能手机包括一个 QWERTY 键盘。他们将在您的电脑键盘 - 而不是按字母顺序排列顶部的数字键盘,在那里你必须利用 1 号进入一个有 A, B, 或 C 该键盘可硬件(物理键盘)或软件(和触摸屏一样,如 iPhone)。

[0014] 4. 消息:所有的手机可以发送和接收文字信息,而一个智能手机除了是处理电子邮件,智能手机可以同步您的个人 -, 有时你的专业 - 电子邮件帐户。一些手机可以支持多个电子邮件帐户。其他包括:访问流行的即时通讯服务,如 QQ、MSN、以及 AOL 的 AIM 和 Yahoo。

[0015] 5. 另外,智能手机功能还包括:邮件:通常智能手机是为商务人士而设计,而目前全球商务最主要的联络方式不是电话、短信而是邮件,尤其是在贸易公司或全球性公司中邮件是一个商务人士一天主要处理的工作内容,而智能手机第一需要支持的就是邮件。

[0016] 6. 联系人:除了邮件,在通话的过程中都需要调用联系人电话簿,一般人都是将电话簿只保存在手机上手机丢失或更换手机,庞大的地址簿相当的不方便,聪明一点的人是使用数据线与电脑同步,但真正正确的使用方法是无线同步,无论在电脑上或手机上进行了联系人的更改都可以得到有效的同步。

[0017] 7. 日历:商务手机日程安排是一个很好的功能。但受限于手机的操作性问题很少有人会在手机上安排所有的事情,此时又需要与电脑同步。支持文档查看和编写:除了以上,商务手机还能够处理日常工作文档,以保证手机成为一个移动的工作平台。

[0018] 由于智能手机设计的小型化、便携性的特点,使得手机可方便地在任一地点使用,就智能手机具备的具体一项功能而言,目前市场上销售的智能手机,尚不具备完善的安全和保密的功能,手机一旦丢失,可能造成手机内的资料泄密,造成无法挽回的损失;因此如何解决智能手机的保密及安全认证问题,是手机领域内要解决的重要技术问题之一。

发明内容

[0019] 本发明的目的是,针对现有技术中,智能手机安全保密功能的不足,提出一种具有安全认证装置的智能手机,在其内设置安全认证装置,仅其合法使用者或在使用者授权之后才可正常使用该智能手机。

[0020] 本发明提供一种带有安全认证装置的智能手机,包括以下单元和装置:

[0021] 处理器,控制智能手机的各单元和模块的执行;

[0022] 通讯模块单元,连接处理器,完成通讯功能;

[0023] 存储单元,连接处理器,用于存储相关文件;

[0024] 用户认证模块,连接处理器,用于获取并验证一外部提供的认证信息;以及

[0025] 操作允许模块,连接处理器,基于前述验证结果允许或拒绝一控制指令。

[0026] 优选地,所述用户认证模块包括用于获取所述认证信息的认证读取模块和用于验证所述认证信息的认证核对模块,进一步的,认证信息预设在一智能卡中;认证信息包括用户身份认证等信息;认证信息以加密的形式存储,用户认证模块具有解密单元。

[0027] 优选地,所述存储单元包括一查询信息模块,记录所述认证信息的至少一项内容和操作记录,以供查询。

[0028] 优选地,所述存储单元中预设一验证信息,所述用户认证模块比较该验证信息与所述认证信息而产生所述验证结果。

[0029] 优选地,该智能手机还包括一个显示单元,显示所述外部提供的认证信息和改写后的认证信息。

[0030] 本发明的有益效果在于:

[0031] 因为该手机具有了安全认证装置,使得该智能手机具有极佳的安全性能,仅允许其合法使用者正常使用,一旦丢失,其他持有者无法使用,对手机内的信息进行保密,保证了该智能手机内的信息安全。

附图说明

[0032] 图 1 为本发明实施例的原理框图。

具体实施方式

[0033] 为了解本发明的技术内容,特举具体实施例并配合所附图式说明如下:

[0034] 如图 1 所示,本发明的智能手机 100 用于与一智能卡配合使用,智能卡中存储了特定的认证信息,智能手机识别并根据认证信息进行相应的功能性操作。该智能手机包括通讯模块单元 101、用户认证模块 102、网络连接单元 103、处理器 104、操作允许模块 105、显示单元 106 和存储单元 130。

[0035] 通讯模块单元 101 完成智能手机的通讯任务。

[0036] 存储单元 130 除存储其他文件外,还具有一查询信息模块(未示出),该模块用于记录用户对手机 100 的操作信息,包括但不限于将用户身份信息,记录在存储单元 130,以便于进行查询和管理,从而可以实现对本实施例手机 100 的操作信息进行追溯。

[0037] 处理器 104,用于控制手机 100 的文件取得、存储和发送操作,以及对用户认证模块 102 的控制处理。

[0038] 显示单元 106 可显示手机 100 的工作模式和可设置的参数,从而便于用户操作。显示单元 106 可以是 LCD 或 LED 显示屏,也可以采用触控屏幕实现,以便实现指令输入的控制功能。

[0039] 本实施例中,该用户认证模块 102 用于对智能卡中存储的信息进行核对,操作允许模块 105 基于核对结果,允许手机 100 执行该用户输入的操作指令。用户认证模块 102 具体包括一认证读取模块 160 和一认证核对单元 170。

[0040] 认证读取模块 160 是一个侦测输入设备,用于读取一智能卡中的特定信息。智能卡中的特定信息是指能够识别持卡人身份、和/或记录了手机所预设的待执行操作的信息,该信息包括但不限于用户身份信息,这些信息可通过光学、电学、磁场或无线电波等媒介形式被认证读取模块 160 侦测到。

[0041] 为了进一步提高使用的安全性,智能卡中的信息是经过加密处理的,并且在认证读取模块 160 可被解密处理。当然,在保密性要求不高的情况下,这些信息也可以不经过加密处理。

[0042] 认证核对模块 170 用于核对认证读取模块 160 所获得的智能卡信息。当认证读取模块 160 获取到智能卡信息后,认证核对模块 170 则将该信息与预存在存储单元 130 中的用户认证信息、即验证信息进行核对认证,判断智能卡内的用户身份信息是否与存储单元 130 内的用户认证信息匹配。如果认证匹配,操作允许模块 105 则允许手机执行该用户所输入的操作指令,如果核对不匹配,操作允许模块 105 禁止手机执行该用户的操作指令。

[0043] 当然,前述验证信息可以预先存储在存储单元 130 内,也可以是存储在接入手机的身份验证服务器设备中,包括但不限于闪存式 U 盘、移动硬盘、网络存储空间等。

[0044] 在另外的一些实施例中,认证核对模块 170 核对智能卡信息与用户认证信息时,如果认证读取模块 160 侦测获得智能卡内的被手机允许的可操作次数信息时,则判断次数信息是否大于 0,如果判断为是,则操作允许模块 105 允许用户通过手机输入的操作指令,并同时对上述可操作次数信息执行减修改操作并更新在存储单元 130 和智能卡内。如果判断次数信息为 0,则操作允许模块 105 禁止用户对手机的操作指令。优选地,此时手机还发出提醒信息以提供用户进行充值操作。此处的充值是指用户在手机的提供者、拥有者、经营者等管理方进行补充可操作次数的操作,例如提供一定金额购买可操作次数等;该提醒信息可以是声信号或光信号,例如通过蜂鸣器或 LED 发出提醒声或者闪烁光,从而提示持卡的用户进行充值操作。

[0045] 显示单元 106 显示上述由认证读取模块 160 侦测获得的可操作次数信息和改写后的可操作次数信息。

[0046] 在另外的一些实施例中,认证核对装置 170 核对智能卡信息与用户认证信息时,如果认证读取装置 160 侦测获得智能卡内的被手机允许的操作时间信息时,核对被手机允许的操作时间信息与当前的操作时间,如果核对匹配,则允许用户通过手机输入操作指令。若核对不匹配,即在非允许时间则禁止用户对手机操作,优选地,此时手机还实时的发出警告信息给其的管理者。

[0047] 在另外的一些实施例中,智能手机对于异常使用状况,可实时发出讯息通知管理者,使管理者可及时监控管理。

[0048] 在其他一些实施例中,上述智能卡内集成的用户身份信息、被手机允许的可操作次数信息、可使用金额信息、操作时间信息中的至少一种,以上信息可以配以密码认证功能,也即当手机认证通过上述用户身份信息、被允许的可操作次数信息、被允许的可使用金额信息后,还需要用户提供密码认证,匹配后方可允许操作。当然,这些密码验证信息是由用户预先设定并存储的。

[0049] 综上所述,以上说明书文字与附图仅为对本发明的解释和说明,不以任何形式对本发明构成限制和限定,其范围以权利要求书为准,一切不超出其宗旨的显而易见的修改、变换和替代方案均在本发明范围内。

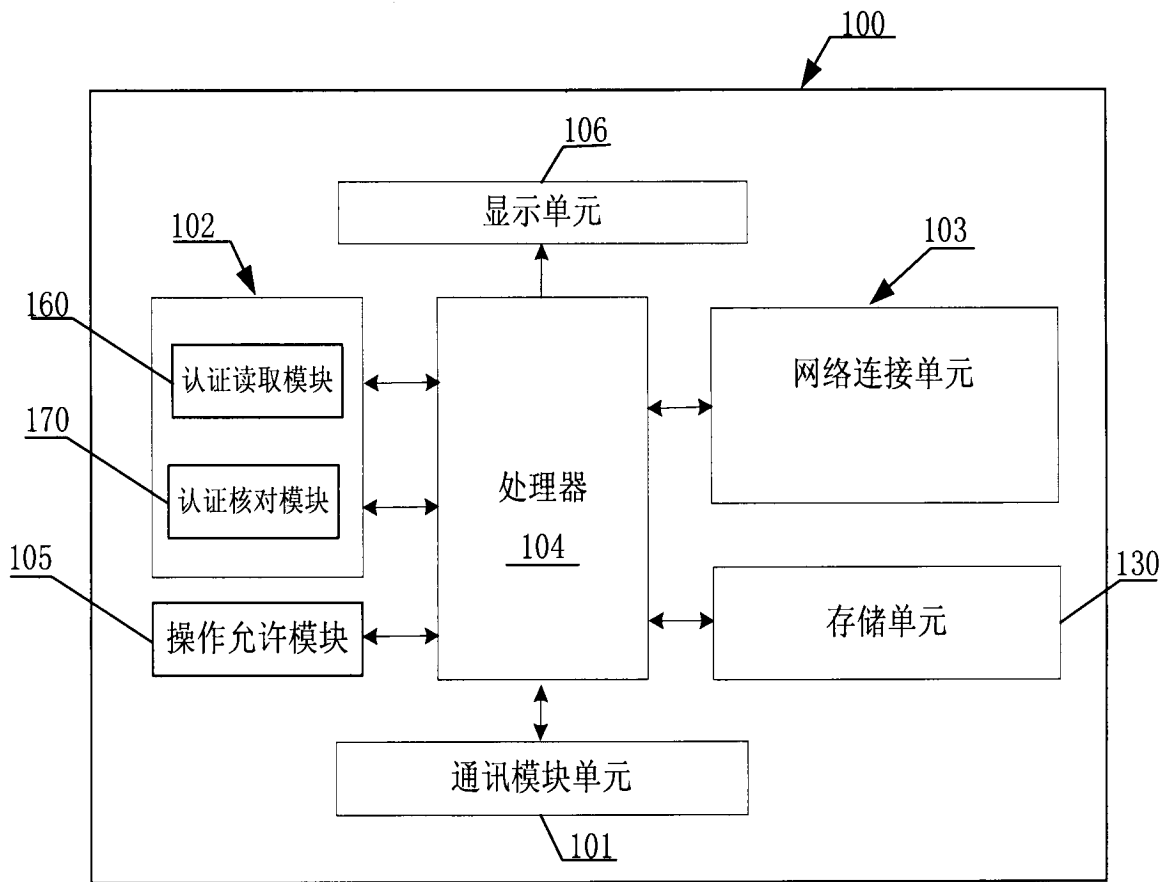


图 1