(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102833423 B
(45)授权公告日 2014.06.04

(21)申请号 201210356310.8

(22)申请日 2012.09.24

(73)专利权人 武汉大学
地址 430072 湖北省武汉市武昌区珞珈山武汉大学

(72)发明人 王树良 杨德馨 池荷花

(74)专利代理机构 武汉科皓知识产权代理事务所(特殊普通合伙) 42222
代理人 严彦

(51)Int.Cl.
H04M 1/725(2006.01)
G06F 3/0488(2013.01)

审查员 刘宁宁

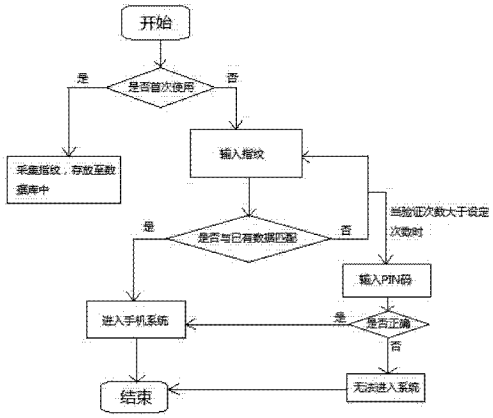
权利要求书1页 说明书5页 附图4页

(54)发明名称

一种基于指纹识别的触摸屏手机及登录解锁方法

(57)摘要

一种基于指纹识别的触摸屏手机及登录解锁方法,在触摸屏传感控制器后设置指纹采集器,登录解锁时:步骤1,判断是否要设置指纹样本,是则在触摸屏上提供指纹输入框,采集指纹输入框获取的指纹数据作为指纹样本存储,否则进入步骤2进行验证;步骤2,在触摸屏上提供指纹输入框,采集指纹输入框获取的指纹数据,对比指纹输入框获取的指纹数据和存储的指纹样本,判断是否匹配,是则进入手机的系统,否则进入步骤3;步骤3,判断验证次数是否达到预设的验证次数上限,是则进入步骤4,否则返回步骤2重新进行下一次验证;步骤4,提示用户输入手机的PIN码,判断用户输入手机的PIN码是否正确,是则进入手机的系统,否则禁止进入手机的系统。



CN 102833423 B

1. 一种基于指纹识别的触摸屏手机的登录解锁方法，所述手机的屏幕由外到里依次为触摸屏、触摸检测部件、显示器和触摸屏传感控制器，其特征在于：触摸屏传感控制器后设置指纹采集器，指纹采集器所得采集图像输入手机的中央处理部件，登陆解锁过程包括以下步骤，

步骤 1，判断是否要设置指纹样本，是则在触摸屏上提供指纹输入框，采集指纹输入框获取的指纹数据作为指纹样本，采集一个以上手指的指纹样本并将指纹样本存储至手机的数据库中，否则进入步骤 2 进行验证；

步骤 2，在触摸屏上提供相应数目的钥匙图标，当用户点击某一钥匙图标时，在触摸屏上提供指纹输入框，采集指纹输入框获取的指纹数据，对比指纹输入框获取的指纹数据和手机的数据库中存储的相应指纹样本，判断是否匹配，是则进入手机的系统，否则进入步骤 3；

步骤 3，判断验证次数是否达到预设的验证次数上限，是则进入步骤 4，否则返回步骤 2 重新进行下一次验证；

步骤 4，提示用户输入手机的PIN码，判断用户输入手机的PIN码是否正确，是则进入手机的系统，否则禁止进入手机的系统；

所述采集指纹输入框获取的指纹数据时，先根据触摸屏传感控制器采集后输入手机的中央处理部件的坐标信息，判断用户输入的坐标是否在指纹输入框内，是则对采集图像进行图像预处理并提取指纹特征信息，否则提示重新输入。

一种基于指纹识别的触摸屏手机及登录解锁方法

技术领域

[0001] 本发明涉及手机通信的安全性领域，尤其涉及一种基于指纹识别的触摸屏手机登录解锁方法。

背景技术

[0002] 苹果公司开启了触摸屏的时代，触摸屏手机已成为了人们的新宠。触摸屏确实很便捷，只要指尖轻轻一碰，便可轻松完成任务。手机发展的终端是“一机在手，走遍天下”。例如可以通过手机远程打开家里的热水器、可以通过手机进行银行转账业务、可以通过手机进行身份识别等。这小小的手机里存储了庞大的信息量，极大地方便和简化了人们的生活。但隐患问题便随之而来，那就是安全性问题。现在的手机大多采用多点触控解锁或者是简单的数字设定解锁，这种手机加密功能极易被破解，不能保证机主信息的安全性。

[0003] 因此，本领域亟待出现采用指纹加密解密手机端的技术方案。

发明内容

[0004] 本发明的目的是提供一种基于指纹识别的手机登录解锁技术方案，可通过用户输入的指纹数据是否与数据库中的数据匹配，以此判定拥有该指纹的用户时候可进入手机系统。

[0005] 本发明的技术方案提供一种基于指纹识别的触摸屏手机，手机的屏幕由外到里依次为触摸屏、触摸检测部件、显示器和触摸屏传感控制器，在触摸屏传感控制器后设置指纹采集器，指纹采集器所得采集图像输入手机的中央处理部件。

[0006] 本发明还相应提供一种基于指纹识别的触摸屏手机登录解锁方法，包括以下步骤：

[0007] 步骤 1，判断是否要设置指纹样本，是则在触摸屏上提供指纹输入框，采集指纹输入框获取的指纹数据作为指纹样本，并将指纹样本存储至手机的数据库中，否则进入步骤 2 进行验证；

[0008] 步骤 2，在触摸屏上提供指纹输入框，采集指纹输入框获取的指纹数据，对比指纹输入框获取的指纹数据和手机的数据库中存储的指纹样本，判断是否匹配， 是则进入手机的系统，否则进入步骤 3；

[0009] 步骤 3，判断验证次数是否达到预设的验证次数上限，是则进入步骤 4，否则返回步骤 2 重新进行下一次验证；

[0010] 步骤 4，提示用户输入手机的 PIN 码，判断用户输入手机的 PIN 码是否正确，是则进入手机的系统，否则禁止进入手机的系统。

[0011] 而且，采集一个以上手指的指纹样本并存储至手机的数据库中；当进入步骤 2 进行验证时，在触摸屏上提供相应数目的钥匙图标，当用户点击某一钥匙图标时，在触摸屏上提供指纹输入框，对比指纹输入框获取的指纹数据和手机的数据库中存储的相应指纹样本。

[0012] 而且，采集指纹输入框获取的指纹数据时，先判断用户输入的坐标是否在指纹输入框内，是则对采集图像进行图像预处理并提取指纹特征信息，否则提示重新输入。

[0013] 而且，根据触摸屏传感控制器采集后输入手机的中央处理部件的坐标信息，判断用户输入的坐标是否在指纹输入框内。

[0014] 本发明所提供方案是一种针对如今触摸屏手机解锁方式的安全性低而提出的安全性高、不易破解的解锁方法，可以有效避免恶意盗取机主重要信息行为，保护机主的隐私。

附图说明

[0015] 图 1 是本发明实施例中首界面示意图；

[0016] 图 2 是本发明实施例中指纹录入界面的示意图；

[0017] 图 3 是本发明实施例中成功登陆界面的示意图；

[0018] 图 4 是本发明实施例中重新输入指纹界面的示意图；

[0019] 图 5 是本发明实施例中指纹开启失败时，转用紧急通道按钮的界面示意图；

[0020] 图 6 是本发明实施例中通过 PIN 码进入手机的界面示意图；

[0021] 图 7 是本发明实施例的流程图；

[0022] 图 8 是本发明实施例中手机屏幕示意图。

[0023] 具体实施方式

[0024] 以下结合附图和实施例详细说明本发明技术方案。

[0025] 本发明实施例提供的基于动态密码的触摸屏手机解锁方法可采用软件技术实现，流程图参见图 7：

[0026] 步骤 1，判断是否要设置指纹样本，是则在触摸屏上提供指纹输入框，采集指纹输入框获取的指纹数据作为指纹样本，并将指纹样本存储至手机的数据库中，否则进入步骤 2 进行验证。

[0027] 首次使用此功能时，需采集指纹样本。这其中包括指纹识别、指纹存储等过程以及系统核对指纹次数和欢迎语等功能设置。用户可以根据个人需求向数据库添加指纹数据。手机的数据库可采用现有技术实现，后续验证使用数据库保存的已有数据。可以在手机的中央处理器（CPU）中留出存储指纹数据的空间。

[0028] 步骤 2，在触摸屏上提供指纹输入框，采集指纹输入框获取的指纹数据，对比指纹输入框获取的指纹数据和手机的数据库中存储的指纹样本，判断是否匹配， 是则进入手机的系统，否则进入步骤 3。

[0029] 步骤 3，判断验证次数是否达到预设的验证次数上限，是则进入步骤 4，否则返回步骤 2 重新进行下一次验证。

[0030] 验证次数上限可由用户或手机厂商预先根据情况设置，实施例设置为 3。

[0031] 步骤 4，提示用户输入手机的 PIN 码，判断用户输入手机的 PIN 码是否正确，是则进入手机的系统，否则禁止进入手机的系统。

[0032] 步骤 2、3、4 实现验证过程，当用户输入的指纹与数据库中已存储的指纹数据相匹配时，便可成功登录手机系统；若两者无法匹配，则弹出提示窗口，要求用户重新输入指纹并进行核对，直至用户设置的验证次数上限为止。如果在规定的验证次数上限内无法成功

解锁，则启用紧急通道——PIN 码。用户可输入手机的 PIN 码进行手机解锁。

[0033] 经过对比分析，本发明建议手机所采用最优的触摸屏是电容式触摸屏。电容式触摸屏的构造主要是在玻璃屏幕上镀一层透明的薄膜体层，再在导体层外加上一块保护玻璃，双玻璃设计能彻底保护导体层及感应器 。电容式触摸屏在触摸屏四边均镀上狭长的电极，在导电体内形成一个低电压交流电场用户触摸屏幕时，由于人体电场，手指与导体层间会形成一个耦合电容，四边电极发出的电流会流向触点，而电流强弱与手指到电极的距离成正比，位于触摸屏幕后的控制器便会计算电流的比例及强弱，准确算出触摸点的位置。电容触摸屏的双玻璃不但能保护导体及感应器，更有效地防止外在环境因素对触摸屏造成影响，就算屏幕沾有污秽尘埃或油渍，电容式触摸屏依然能准确算出触摸位置。

[0034] 用户对触摸屏的接触通过触摸传感技术采集，可采用现有技术。现有技术中触摸屏手机的屏幕由外到里依次为 :触摸屏、触摸检测部件、显示器、触摸屏传感控制器。触摸传感控制器目前提供一些通用的性能选项和形态，如滑块和邻近传感器。触摸传感器技术的进步使传感器驱动型接口更易于实现，对终端用户更为直观和简单。大多数触摸传感控制器依据所检测到的电容变化来工作。当某种物体或某个人接近或触摸传感器的导电金属片时，手指与金属片之间的电容发生变化。导电物体（如手指）在传感器附近移动将改变电容传感器的电场线并使电容发生变化。控制电路可测出电容的变化。触摸传感器接口通常通过测量与传感器垫片相连的电路的阻抗来检测电容变化。触摸控制器周期性地测量传感器输入通道的阻抗并用这些值来导出一个内部基准，即校准阻抗。控制器以这个阻抗值为基础判定是否发生了触摸事件。

[0035] 步骤 1 采集指纹样本和步骤 2 获取指纹数据需要进行指纹识别。具体指纹识别目前有两种现有技术 :A、读取指纹图像，对初步读取到的人体指纹图像进行清晰处理 ;建立指纹的数字特征数据 ;利用模糊比较法，对输入指纹和已存指纹进行对比。B、取像和取像设备，光学设备(历史久远)，利用光的全反射原理 ;优点 :体积小(3*1*1 英寸);纤维光、微型三棱镜矩阵，硅晶体传感器(最近)，例如 :电容传感器、温度感应传感器、超声波扫描(指纹取像技术中非常好的一类，建议使用)。通过对两种方式比较，前一种价格低、体积小、识别率高。

[0036] 为改进指纹识别效果，可以进行图像增强 :当手指不干净或者有伤疤、干燥、湿润时，不能获得清晰的图像。为了克服这种现象，可以设计一个适合、匹配的滤镜和恰当的阀值。可参考第三代生物射频传感器 :第三代生物射频指纹识别技术，射频传感器技术是通过传感器本身发射出微量射频信号，穿透手指的表皮层去控测里层的纹路，来获得最佳的指纹图像。因此对干手指，汉手指等困难手指通过可高达 99%，防伪指纹能力强，指纹敏感器的识别原理只对人的真皮皮肤有反应，从根本上杜绝了人造指纹的问题，宽温区 :适合特别寒冷或特别酷热的地区。因为射频传感器产生高质量的图像，因此射频技术是最可靠，最有力的解决方案。除此之外，高质量图像还允许减小传感器，无需牺牲认证的可靠性，从而降低成本并使得射频传感器思想的应用到可移动和大小不受拘束的任何领域中。

[0037] 本发明进一步提出，可以采集一个以上手指的指纹样本并存储至手机的数据库中 ;当进入步骤 2 进行验证时，在触摸屏上提供相应数目的钥匙图标，当用户点击某一钥匙图标时，在触摸屏上提供指纹输入框，对比指纹输入框获取的指纹数据和手机的数据库中存储的相应指纹样本。

[0038] 为便于实施参考，提供实施例的具体实现流程说明如下：

[0039] (1) 当用户首次使用此功能时，需进行指纹数据采集，经过信息处理后，将该数据存至数据库中。此步骤是对指纹数据的采集、图像与处理的综合应用，包括以下子步骤。

[0040] (1.1) 如图 8 所示，实施例所用手机的屏幕由外到里依次为：触摸屏 101、触摸检测部件 102、显示器 103、触摸屏传感控制器 104 和指纹采集器 105。指纹采集器可参考现有技术实现，例如晶体传感器等。所得指纹存储至手机的数据库 106 中。

[0041] 在用户的手指触摸安装在显示器前端的触摸屏之后，系统根据手指在指定位置的指纹录入进行数据分析。触摸检测部件位于显示屏幕前，主要作用是检测用户触摸位置，而触摸屏传感控制器的主要作用是从触摸检测装置上接受触摸信息，并将其转换成出点坐标，再传送给手机的 CPU；同时指纹采集器采集指纹的图像，所得采集图像输入 CPU。这时坐标数值将会与指纹采集器的坐标数值(和预设的指纹输入框位置一致)进行比较，若输入的坐标在指纹处理器的坐标之内，则 CPU 开始进行指纹图像的处理。

[0042] (1.2) 指纹图像处理主要包括图像采集、图像预处理、细节点提取及指纹匹配。其中在 (1.1) 通过指纹采集器已完成对图像采集，指纹采集器采集的图像输入 cpu，接下来需要进行图像预处理。预处理的目的是去除图像中的噪声，把它变成一幅清晰的点线图，以便提取正确的指纹特征，从而达到正确匹配。预处理过程主要包括指纹规格化、平滑滤波处理、方向增强处理、二值化、细化等，可采用现有技术，本发明不予赘述。

[0043] (1.3) 在步骤 (1.2) 的基础上提取指纹特征信息，得到指纹特征模板，即可作为指纹样本存储至指纹数据库中的有效数据。

[0044] 以上指纹图像的处理过程可采用软件编程技术由 cpu 执行实现，也可以将图像预处理过程模块化设计为采用图像转换器实现，生成输入指纹特征模板可模块化设计为采用指纹模板处理器实现。指纹采集器输出图像到图像转换器，图像转换器输出到指纹模板处理器，然后存储到数据库。

[0045] 为了提高效率，具体实施时，用户输入指纹时可以先通过触摸屏进行指纹触点的定位及判断；当采集指纹输入框获取的指纹数据时，先根据触摸屏传感控制器采集后输入手机的中央处理部件的坐标信息，判断用户输入的坐标是否在指纹输入框内，是则对采集图像进行图像预处理并提取指纹特征信息，否则提示重新输入。可以通过触摸检测部件和触摸屏传感控制器的坐标数值与指纹处理器的坐标数值进行比较，若所输入的内容的坐标在指纹处理器的坐标之内，则 CPU 开始进行指纹图像的处理。所输入的指纹在规定范围内时，采用指纹处理器处理得到指纹特征模板，并将其存入数据库中。

[0046] 步骤 2 中，先判断用户输入的坐标是否在指纹输入框内，是则对比指纹输入框获取的指纹数据和手机的数据库中存储的指纹样本，否则提示重新输入。

[0047] (2) 用户每次使用手机，验证使用过程如下：

[0048] 用户每次使用手机，点亮屏幕时，会出现一扇已有一把锁的中国式大门(大门旁边会有一把或并列摆有几把钥匙(根据数据库里的指纹个数决定。即指纹库有一个指纹，桌面上有一把钥匙)，如图 1。

[0049] 当用户点击钥匙图标时，屏幕会显示如图 2 所示的空白区域作为指纹输入区，弹出“开启指令”提示用户输入指纹。对输入指纹的采集、图像与处理与(1)实现方式一致，具体匹配可采用现有技术。

[0050] 当用户的指纹信息匹配成功时，画面中门上的锁会自动打开，并且出现欢迎语（用户可个性化设置，例如“Welcome ！”）开门后即可看到手机桌面信息，如图 3。

[0051] 若用户的指纹匹配不成功，则会弹出提示信息“请重新输入指令”要求用户在指纹区重新输入。同时，门锁会增加一把锁（门锁增加的个数由机主设定的验证次数有关，例如，机主设定验证次数为三，则门锁最大值有 3 把），如图 4 出现了两把锁。

[0052] 若三次验证权限已用完，屏幕会显示“抱歉，开启不成功，您无法进入！”，如图 5，出现了三把锁。

[0053] 为了确保因识别不清晰等因素干扰到本机机主无法正常使用手机，在如图 5 所示情况发生时，桌面的右下角会有“紧急通道”字样。当用户点击时，屏幕会弹出“请输入本机 PIN 码”的提示，如图 6。这时用户只要输入正确的 PIN 码即可进入到自己的手机系统中。

[0054] 若用户最终无法解锁手机或手机丢失时，用户可到该手机品牌的官网上进行挂失。在输入自己的身份证等有效证件后，便可通过云服务读取下载自己的重要信息。用户在使用时需将自己的信息上传到云服务器的前提下，才可下载读取信息。这样既可以保护行货手机的版权，与水货手机服务相区别，又可以为用户提供方便安全的服务。

[0055] 验证过程中的获取指纹数据具体实现与（1）中采集指纹样本的具体实现一致。

[0056] 本文中所描述的具体实施例仅仅是对本发明精神作举例说明。本发明所属技术领域的技术人员可以对所描述的具体实施例做各种各样的修改或补充或采用类似的方式替代，但并不会偏离本发明的精神或者超越所附权利要求书所定义的范围。

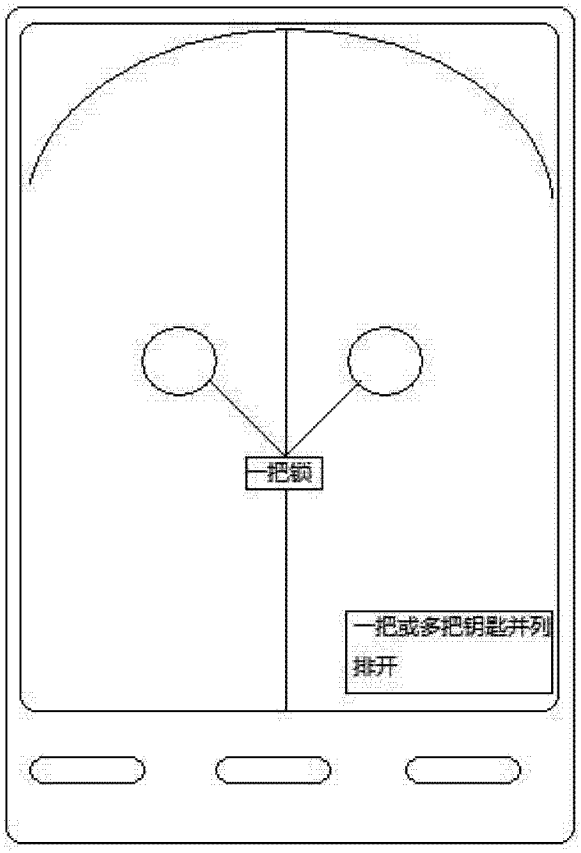


图 1

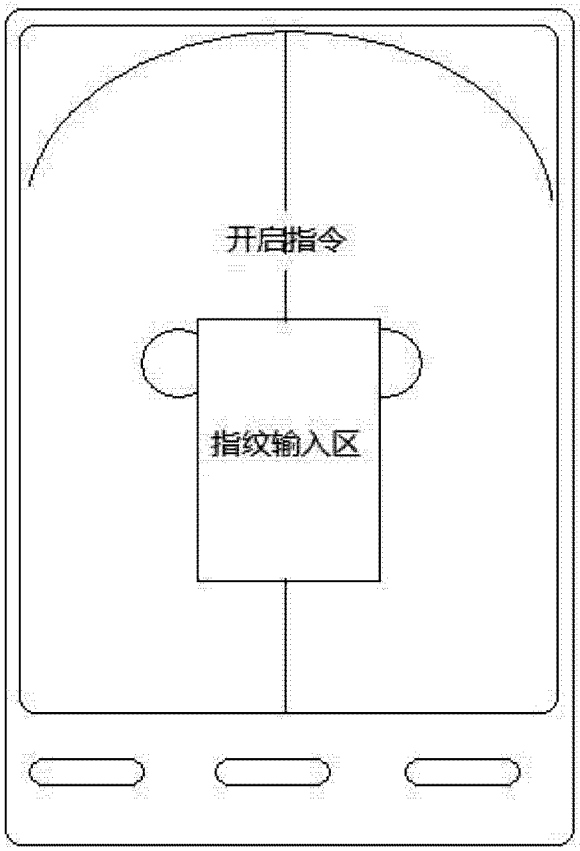


图 2

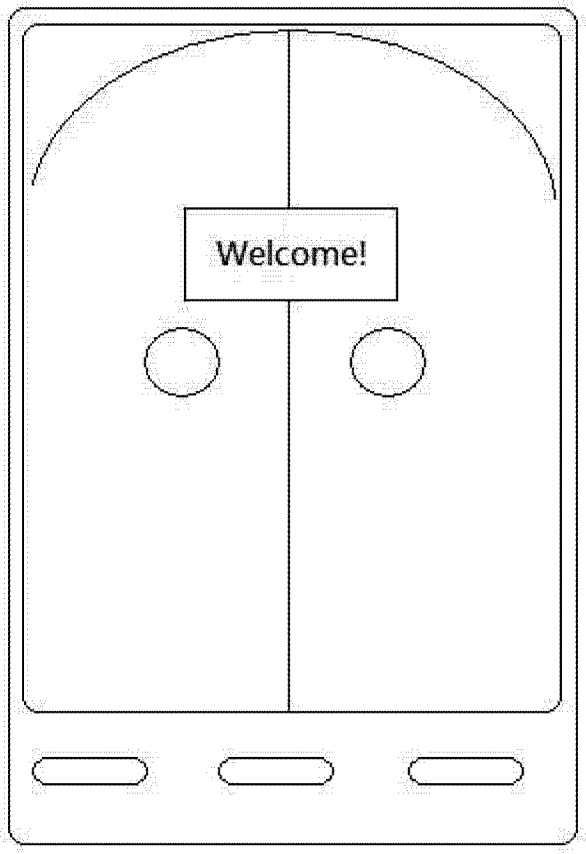


图 3

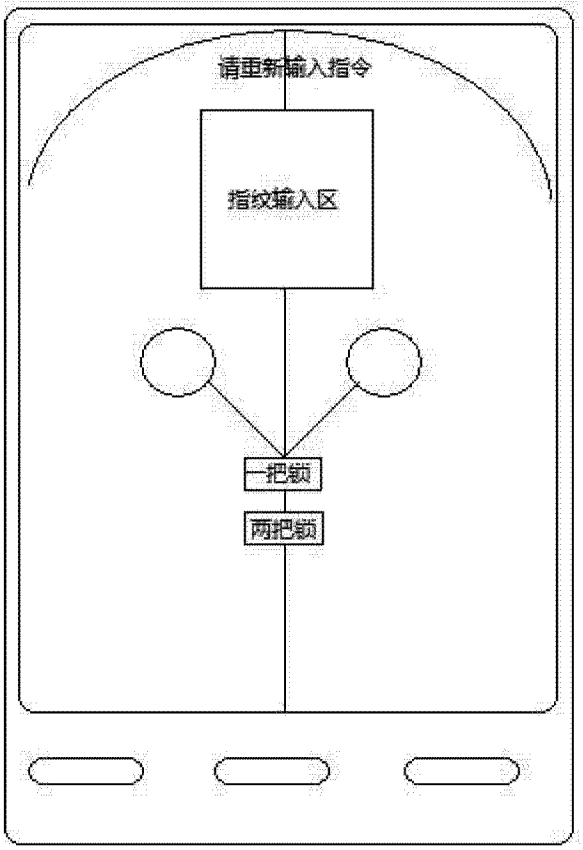


图 4

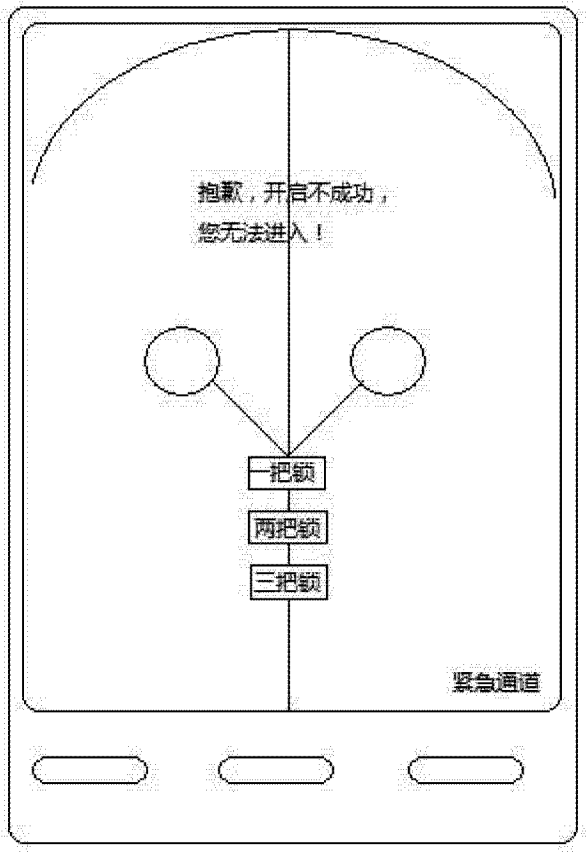


图 5

图 6

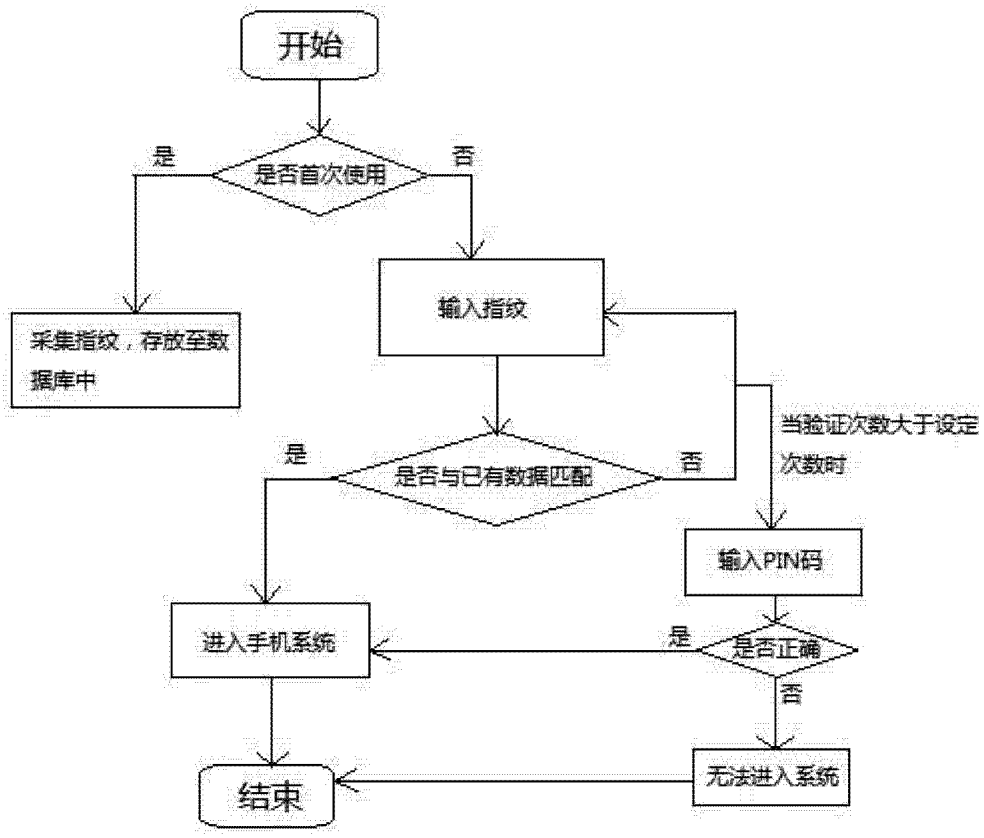

开始
是否首次使用
是
否
采集指纹，存放至数据库中
输入指纹
是否与已有数据匹配
是
否
当验证次数大于设定次数时
输入PIN码
是否正确
是
否
进入手机系统
无法进入系统
结束

图 7

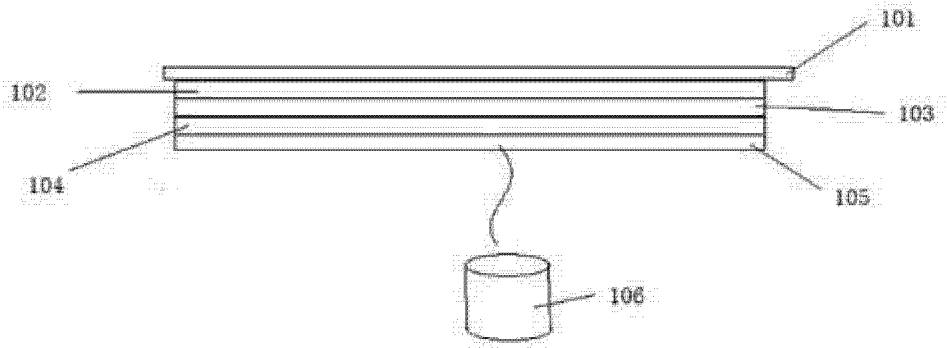

101
102
103
104
105
106

图 8