(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 106327652 B
(45)授权公告日 2019.02.15

(21)申请号 201610825883.9

(22)申请日 2016.09.14

(65)同一申请的已公布的文献号
申请公布号 CN 106327652 A

(43)申请公布日 2017.01.11

(73)专利权人 深圳市欧瑞博电子有限公司
地址 518055 广东省深圳市南山区学苑大道1001号南山智园A7栋7楼

(72)发明人 陈德华 王雄辉

(74)专利代理机构 深圳市智圈知识产权代理事务所(普通合伙) 44351
代理人 韩绍君

(51)Int.Cl.
G07C 9/00(2006.01)

(56)对比文件
CN 204731852 U,2015.10.28,
US 2016260271 A1,2016.09.08,
CN 105155940 A,2015.12.16,
CN 105261103 A,2016.01.20,
CN 204515884 U,2015.07.29,
CN 203224923 U,2013.10.02,
CN 204759544 U,2015.11.11,
CN 105785878 A,2016.07.20,

审查员 喻婷

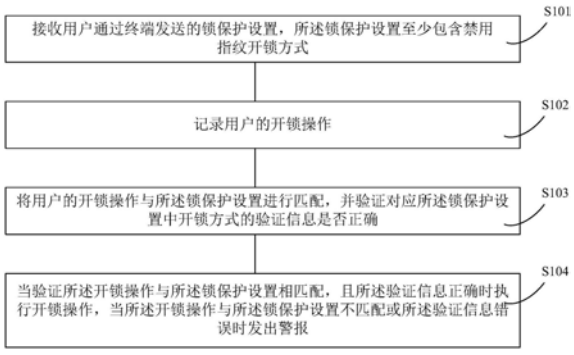
权利要求书2页 说明书7页 附图7页

(54)发明名称

电子智能门锁指纹锁保护系统及方法

(57)摘要

本发明涉及一种电子智能门锁指纹锁保护系统及方法。所述保护系统及方法通过设置通讯模块来接收用户终端发送的锁保护设置,并通过主控模块进行验证,达成了对门锁进行保护的目的,使得通过用户终端可随时随地切换门锁的保护模式,其中,通过终端可以禁用指纹开锁操作,由此使得不法分子难以通过预设的方式来破解门锁的保护方式,从而极大地增强门锁的安全性。



CN 106327652 B

1.一种电子智能门锁指纹锁保护系统，其特征在于，所述电子智能门锁指纹锁保护系统包括：

一个锁体及与其相耦合的电机驱动模块，所述电机驱动模块用于驱动锁体移动以使得门锁处于关闭或开启状态；

一个通讯模块，其通过无线通讯方式与用户终端相连接，并接收用户通过终端发送的锁保护设置，所述锁保护设置至少包含禁用指纹开锁方式；

一个指纹采集模块，用于采集用户的指纹信息，以作为指纹开锁的验证信息；

一个存储模块，用于存储对应多种开锁方式的验证信息，所述多种开锁方式分别与用户录入的多个验证信息相对应；

一个报警模块，用于在当前开锁方式与存储模块所存储的锁保护设置或当前的验证信息与存储模块的验证信息不符时发出警报；

一个主控模块，所述主控模块分别与所述电机驱动模块、通讯模块、指纹采集模块、存储模块、验证模块、报警模块相连接，用于验证当前的开锁方式与存储模块的锁保护设置，及验证当前的验证信息与存储模块的验证信息是否相符；

所述锁保护设置中进一步包括解除被禁用的开锁方式的时间限制信息。

2.一种如权利要求1所述的电子智能门锁指纹锁保护系统，其特征在于，进一步包括一个供电模块，其用于对所述主控模块、电机驱动模块、通讯模块、指纹采集模块、存储模块、验证模块、报警模块进行供电。

3.一种采用如权利要求1所述的电子智能门锁指纹锁保护系统的电子智能门锁指纹锁保护方法，其特征在于，所述方法包括：

接收用户通过终端发送的锁保护设置，所述锁保护设置至少包含禁用指纹开锁方式；

记录用户的开锁操作；

将用户的开锁操作与所述锁保护设置进行匹配，并验证对应所述锁保护设置中开锁方式的验证信息是否正确；

当验证所述开锁操作与所述锁保护设置相匹配，且所述验证信息正确时执行开锁操作，当所述开锁操作与所述锁保护设置不匹配或所述验证信息错误时发出警报。

4.一种如权利要求3所述的电子智能门锁保护方法，其特征在于，所述电子智能门锁指纹锁保护系统进一步包括一个供电模块，其用于对所述主控模块、电机驱动模块、通讯模块、指纹采集模块、存储模块、验证模块、报警模块进行供电，所述禁用指纹开锁方式包括：

主控模块通过通讯模块接收终端发送的锁保护设置；

主控模块输出控制指令至所述供电模块；

所述供电模块停止对所述指纹采集模块供电。

5.一种如权利要求3所述的电子智能门锁保护方法，其特征在于，所述锁保护设置为指纹锁保护模式，所述禁用指纹开锁方式包括：

主控模块通过通讯模块接收终端发送的锁保护设置；

所述指纹采集模块采集当前指纹信息；

所述主控模块接收当前指纹信息后不对当前指纹信息进行验证。

6.一种如权利要求3所述的电子智能门锁保护方法，其特征在于，所述锁保护设置为指纹锁保护模式，所述禁用指纹开锁方式包括：

主控模块通过通讯模块接收终端发送的锁保护设置；

所述指纹采集模块采集当前指纹信息；

所述主控模块接收当前指纹信息并进行验证；

如当前指纹信息与指纹开锁的验证信息相符时，所述主控模块不控制电机驱动模块工作。

7.一种如权利要求3所述的电子智能门锁保护方法，其特征在于，在记录用户的开锁操作前，所述方法进一步包括：

接收用户设置的指纹验证等级设置，所述指纹验证等级与指纹验证精确度相对应。

8.一种如权利要求3所述的电子智能门锁保护方法，其特征在于，所述锁保护设置中进一步包括解除被禁用的开锁方式的时间限制信息。

9.一种如权利要求3所述的电子智能门锁指纹锁保护方法，所述锁保护设置存储在服务器或存储模块中。

10.一种如权利要求3所述的电子智能门锁指纹锁保护方法，所述多种开锁方式包含指纹、按键、射频开锁方式。

电子智能门锁指纹锁保护系统及方法

技术领域

[0001] 本发明涉及安全领域，尤其涉及一种电子智能门锁指纹锁保护系统及方法。

背景技术

[0002] 随着社会城市化道路的快速发展，我国的大中型城市越来越多，因此，楼宇的安全管理系统变得是越来越重要。

[0003] 对于楼宇的安全而言，目前最重要的设备之一就是锁具。

[0004] 传统的机械锁由于构造简单，安全性能低，而且钥匙易被复制，被盗事件屡见不鲜，难以对人们的日常生活形成有效的保护。

[0005] 另一方面，随着科技的不断发展，具有防盗报警功能的电子密码锁逐渐取代传统的机械锁进入人们的生活，其可克服机械锁密码量少、安全性能差等缺点。

[0006] 然而目前大多数电子密码锁采用键盘输入方式，防窥探性和保密性较差；其它很多电子智能锁，如IC射频卡智能锁和指纹识别智能锁已经在国内外陆续出现并进入人们的视野中。

[0007] 指纹识别技术作为生物识别技术中应用最广泛、价格最低廉的识别技术之一，将其运用在电子智能门锁上时，具有成本低、安全性高、使用便捷的优点。

[0008] 然而，随着指纹识别技术的广泛运用，不法之徒也逐渐掌握了一些破解的方法，例如不法之徒可以通过非法的，不授权的方式获取门锁主人的指纹，再通过在电商平台轻松购买复制/拷贝指纹的指纹模具硅胶进行非法指纹复制，利用复制的指纹硅胶(假指纹)进行非法验证开门，此导致了本已安全的、便捷的、应用广泛、成本最低的生物特征识别技术安全性遭到了质疑，使用指纹识别技术的电子智能门锁的用户人身，财产受到极大的伤害，或者不安全风险急剧上升。

发明内容

[0009] 本发明实施例的目的在于提供一种电子智能门锁指纹锁保护系统及方法，以解决上述存在的技术问题。

[0010] 一种电子智能门锁指纹锁保护系统，所述电子智能门锁指纹锁保护系统包括：一个锁体及与其相耦合的电机驱动模块，所述电机驱动模块用于驱动锁体移动以使得门锁处于关闭或开启状态；一个通讯模块，其通过无线通讯方式与用户终端相连接，并接收用户通过终端发送的锁保护设置，所述锁保护设置至少包含禁用指纹开锁方式；一个指纹采集模块，用于采集用户的指纹信息，以作为指纹开锁的验证信息；一个存储模块，用于存储对应多种开锁方式的验证信息，所述多种开锁方式分别与用户录入的多个验证信息相对应；一个验证模块，用于验证当前的开锁方式与存储模块的锁保护设置，及验证当前的验证信息与存储模块的验证信息是否相符；一个报警模块，用于在当前开锁方式与存储模块所存储的锁保护设置或当前的验证信息与存储模块的验证信息不符时发出警报；一个主控模块，所述主控模块分别与所述电机驱动模块、通讯模块、指纹采集模块、存储模块、验证模块、报

警模块相连接;以及一个供电模块,其用于对所述主控模块、电机驱动模块、通讯模块、指纹采集模块、存储模块、验证模块、报警模块进行供电。

[0011] 一种采用上述电子智能门锁指纹锁保护系统的电子智能门锁指纹锁保护方法,所述方法包括:接收用户通过终端发送的锁保护设置,所述锁保护设置至少包含禁用指纹开锁方式;记录用户的开锁操作;将用户的开锁操作与所述锁保护设置进行匹配,并验证对应所述锁保护设置中开锁方式的验证信息是否正确;当验证所述开锁操作与所述锁保护设置相匹配,且所述验证信息正确时执行开锁操作,当所述开锁操作与所述锁保护设置不匹配或所述验证信息错误时发出警报。

[0012] 相对于现有技术,本发明实施例提供的电子智能门锁指纹锁保护系统及方法通过设置通讯模块来接收用户终端发送的锁保护设置,并通过主控模块进行验证,达成了对门锁进行保护的目的,使得通过用户终端可随时随地切换门锁的保护模式,其中,在本实施例中,通过终端可以禁用指纹开锁操作,由此使得不法分子难以通过预设的方式来破解门锁的保护方式,从而极大地增强门锁的安全性。

附图说明

[0013] 为了更清楚地说明本发明的技术方案,下面将对实施方式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发明的一些实施方式,对于本领域普通技术人员来讲,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。

[0014] 图1是本发明第一实施例提供的电子智能门锁指纹锁保护系统的结构示意图;

[0015] 图2是图1所示的系统与用户终端的交互示意图;

[0016] 图3是本发明第二实施例提供的电子智能门锁指纹锁保护方法的流程示意图;

[0017] 图4是在用户终端的界面中设置开锁方式以生成验证信息的示意图;

[0018] 图5是在用户终端的界面中设置指纹识别信息以生成验证信息的示意图;

[0019] 图6-8是本发明第二实施例提供的电子智能门锁指纹锁保护方法中实施指纹锁保护的流程示意图;

[0020] 图9是在用户终端的界面中设置指纹精度信息以生成验证信息的示意图。

具体实施方式

[0021] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0022] 请一起参阅图1及图2,本发明第一实施例提供一种电子智能门锁指纹锁保护系统100,所述电子智能门锁指纹锁保护系统100包括一个锁体(图未示)、一个电机驱动模块20、一个通讯模块30、一个指纹采集模块40、一个存储模块50、一个报警模块70、一个供电模块80、以及一个主控模块90。

[0023] 如图1所示,所述主控模块90分别与所述电机驱动模块20、通讯模块30、指纹采集模块40、存储模块50、报警模块70相连接,其为整个系统100的控制中心,负责将此各个功能模块收集的信息进行处理、运算、并控制其输出等。

[0024] 在本实施例中，所述锁体与电机驱动模块20相耦合，所述电机驱动模块20用于驱动锁体移动以使得门锁处于关闭或开启状态。

[0025] 通讯模块30通过无线通讯方式与用户终端200(详见图2)相连接，用户终端200可以是手机、平板等便携式可移动设备。本实施例中，用户终端200为智能手机，其安装对应于该保护系统100的专属应用程序(Application，图2中示出应用程序对应的手机界面30A)，在其它变更实施方式中，所述应用程序也可以是即时通讯工具等，并不局限于具体实施例。另外，在本实施例中，所述通讯模块30采用的通讯方式包括wifi、蓝牙、zigbee、RF433、红外、声波等。

[0026] 使用时，通讯模块30接收用户通过终端200发送的锁保护设置，所述锁保护设置至少包含禁用(一切)指纹开锁的指纹锁保护模式，以及同时禁用指纹与其它开锁方式至少一者的结合(例如禁用指纹开锁与所述按键开锁、射频开锁中一种或两种操作的结合操作)，所述其它开锁方式包含了按键开锁、射频开锁等。在其它变更实施方式中，所述开锁方式也可以为其它方式，如语音开锁等，并不局限于具体实施例。上述多种开锁方式分别与用户录入的多个验证信息相对应。

[0027] 具体地，指纹开锁指通过识别指纹来启动开锁动作，对应于指纹开锁的验证信息为用户手指的指纹信息；按键开锁指通过识别按键来启动开锁动作，对应于按键开锁的验证信息为用户设置的按键顺序；射频开锁指通过识别射频信号来启动开锁动作，对应于射频开锁的验证信息为用户所使用的IC(Integrated Circuit Card，集成电路卡)卡中的射频信号。

[0028] 本实施例中，禁用包括指纹识别开锁方式及其他所有开锁方式的开锁行为为完全指纹锁保护模式，只有指纹锁保护模式失效后上述开锁行为才被允许。

[0029] 所述指纹采集模块40用于采集用户的指纹信息，以作为指纹开锁的验证信息。具体地，所述指纹采集模块40包括指纹传感器及DSP(Digital Signal Process，数字信号处理)芯片等，使用时，指纹传感器将采集到的图像特征点信息送到指纹采集算法DSP芯片进行计算比对，并储存至所述存储模块50。所述存储模块50例如可以为FLASH储存芯片，其也可以为随机存取存储器(random access memory，RAM)等，并不局限于具体实施例。

[0030] DSP芯片通过高速、高效的算法技术，将图像特征点信息进行滤波，特征提取及比对后进行存储。

[0031] 可以理解的是，除指纹采集模块40外，电子智能门锁指纹锁保护系统100可以进一步包括按键采集模块41，用于采集用户设置的按键信息。或者也可以进一步包括射频信号读写卡模块42，使用时，用户可以通过该读写卡模块读取对应的IC卡的射频信号信息并写入存储模块50中。在下次使用该IC卡开锁的时候IC卡的射频信号信息可以被该读写卡模块42读出，并与存储模块50中的存储信息(如锁保护设置)进行匹配后执行开锁操作，如信息不匹配则不执行开锁操作。

[0032] 所述主控模块90用于验证当前的开锁方式与存储模块50的锁保护设置，及验证当前的验证信息与存储模块50的验证信息是否相符。可以理解的是，在其它变更实施方式中，所述存储模块50也可不存储所述锁保护设置，此时验证信息可存储在服务器(图未示)中，在执行开锁的过程中，主控模块90将验证结果发送与服务器的验证信息进行比对，以验证是否满足用户设置要求，并相应执行或不执行开锁操作。在其它变更实施方式中，所述存储

模块50除了存储验证信息及锁保护设置(即开锁验证方式),也存储有门锁其他系统设计信息(声音,操作语言),还存储开门记录信息等,用户的操作,如开门记录信息也可通过通讯模块30远程推送到用户终端200,使用户实时了解到门锁的状态。

[0033] 所述报警模块70用于在当前开锁方式与存储模块50所存储的锁保护设置,或当前的验证信息与存储模块的验证信息不符时发出警报。例如,当前的用户为非法分子,其采用伪冒的指纹信息执行开锁操作,此时被主控模块90识别出来,此时报警模块70即发出警报;又或者,用户发送的锁保护设置要求先验证按键密码,再验证射频(即禁用指纹开锁),但不法分子在操作时采用了先验证指纹,再验证按键密码的方式,这时报警模块70发出警报;又或者,用户发送的锁保护设置要求禁用指纹识别开锁方式及其他开锁方式的开锁行为(完全指纹锁保护模式),此时,即使在系统100上输出的指纹为匹配的指纹,仍不执行开锁操作,且通过报警模块70发出警报进行提醒。

[0034] 所述报警模块70包括喇叭(或蜂鸣器),即通过声音来发出警报。可以理解的是,所述报警模块70也可通过震动、发出光束等其它方式来发出警报,或者不局限于这些方式或手段等。另外,在实际应用中,所述报警模块70也可以进一步包括功效放大器对报警信号进行放大,或者发送至相关部门的报警系统进行报警,或者反馈至用户终端200提醒用户,从而让用户时刻掌握家里门锁的状态信息。

[0035] 在其它变更实施方式中,当验证当前的验证信息与存储模块50的验证信息不符时,也可通过通讯模块30发送报警信号至相关部门的报警系统进行报警,或者反馈报警信号至用户终端200提醒用户。

[0036] 所述供电模块80用于对所述主控模块90、电机驱动模块20、通讯模块30、指纹采集模块40、存储模块50、、报警模块70进行供电。具体而言,供电模块80负责整锁的电源输入、管理、监控,其将输入的DC6V或DC9V降压成DC6V和DC3.3V给各个模块供电,并且实时监控系统的电压。如果电源电压低于设定的电压,则供电模块80主动输出监控信号给主控模块90告知系统供电电池组能量已耗尽,需及时更换电池。另一方面,该供电模块80也可对系统过载、短路进行实时监控与保护。

[0037] 在本实施例中,所述保护系统100进一步包括一个显示模块95,所述显示模块95例如可以为有机电激光显示屏(OLED),其用于显示用户执行开锁或录入信息中的各类信息,可以理解的是,所述显示模块95也可以为液晶显屏等,并不局限于具体实施例。

[0038] 当禁用指纹开锁方式时,用户终端200发送锁保护设置,对指纹进行锁保护,即不允许通过指纹开锁,所述锁保护设置被所述通讯模块30接收,并传送给主控模块90,其处理的流程包括:

[0039] (1)、主控模块90输出控制指令,使供电模块80关闭对指纹采集模块40的供电,使得指纹采集模块40无法正常进行指纹采集,指纹开锁方式无法正常使用,从而达到“指纹锁保护”的目的;

[0040] (2)、虽然所述指纹采集模块40采集当前指纹信息,且所述主控模块90接收当前指纹信息(即使其与指纹开锁的验证信息相符),但不对当前指纹信息进行验证;

[0041] (3)、虽然指纹采集模块40采集当前指纹信息,且主控模块90接收当前指纹信息并进行验证,且即使当前指纹信息与指纹开锁的验证信息相符,但所述主控模块90不控制电机驱动模块20工作。

[0042] 可以理解的是，上述锁保护设置也可以在锁本体进行设置，而不是通过用户终端200进行设置，并不局限于具体实施例。

[0043] 综上所述，本发明第一实施例提供的电子智能门锁指纹锁保护系统100通过设置通讯模块30来接收用户终端200发送的锁保护设置，并通过进行验证，达到对门锁进行保护的目的，使得通过用户终端200可随时随地切换门锁的保护模式，其中，在本实施例中，通过终端可以禁用指纹开锁操作，由此使得不法分子难以通过预设的方式来破解门锁的保护方式，从而极大地增强门锁的安全性。

[0044] 请参阅图3，本发明第二实施例提供一种电子智能门锁指纹锁保护方法，其采用第一实施例所述的电子智能门锁指纹锁保护系统100。所述电子智能门锁指纹锁保护系统100包括一个锁体、电机驱动模块20、通讯模块30、指纹采集模块40、存储模块50、报警模块70、供电模块80、以及主控模块90。

[0045] 在本实施例中，所述用户终端200为智能手机，其安装对应于该保护系统100的专属应用程序。

[0046] 所述电子智能门锁保护方法包括步骤S101-S104。

[0047] 步骤S101、接收用户通过终端发送的锁保护设置，所述锁保护设置至少包含禁用指纹开锁方式；

[0048] 步骤S102、记录用户的开锁操作；

[0049] 步骤S103、将用户的开锁操作与所述锁保护设置进行匹配，并验证对应所述锁保护设置中开锁方式的验证信息是否正确；

[0050] 步骤S104、当验证所述开锁操作与所述锁保护设置相匹配，且所述验证信息正确时执行开锁操作，当所述开锁操作与所述锁保护设置不匹配或所述验证信息错误时发出警报。

[0051] 请一起参阅图4，在步骤S101中，可以通过用户终端200的用户界面30A来完成所述锁保护设置。所述锁保护设置包括禁用指纹或其与按键、射频中任意一种开锁方式，例如禁用指纹开锁，允许先验证按键，再验证射频信号(或者相反的次序)；或者同时禁用验证指纹，按键，射频信号(即锁保护模式)，取决于用户的喜好与安全使用需要。

[0052] 在其它变更实施方式中，所述锁保护设置也可以包括同类验证方式中的不同对象，如图5所示，例如保护系统100录入了多个成员(例如为家庭成员A、B、C、D、E)的指纹信息，包括指纹1-5，这时在用户终端200的用户界面30A中可以设置仅允许其中一个指纹信息(例如指纹1)进行验证，对其它指纹信息不开放验证。可以理解的是，所述指纹1-5可以为对应于同一用户五个手指的指纹，也可以为对应于五个用户同一手指的指纹，不局限于具体实施例。

[0053] 如图6所示，在再一变更实施方式中，所述锁保护设置也可以包括指纹识别的精度，即将保护功能与指纹比对等级设置相关联，即只允许其中一种指纹识别等级，如一级(较高)、二级(中等)或三级(较低)。

[0054] 通讯模块30接收到所述锁保护设置后，通过存储模块50对所述锁保护设置进行存储。

[0055] 在步骤S102及S103中，用户的开锁操作被记录到，例如通过指纹采集模块40采集到用户的指纹，或通过按键采集模块41采集到用户输入的数字(或字母)，或通过射频信号

读写卡模块42读取到IC卡的射频信号。当用户开锁操作被记录到后，其由所述主控模块90进行验证，具体验证当前的开锁方式与存储模块50的锁保护设置，及验证当前的验证信息与存储模块50的验证信息是否相符。

[0056] 例如，在其中一种实施方式中，当用户的锁保护设置为仅允许指纹1进行开锁操作时，采用其它指纹2-5中任意一者进行开锁操作将被阻止并被识别为非法操作，从而触发警报。

[0057] 在再一种实施方式中，当用户的锁保护设置为仅允许按键加射频的开锁方式(禁用指纹开锁)时，通过指纹加射频的方式也将被识别为非法操作，从而触发警报。

[0058] 请一起参阅图6至图8，在本实施例，禁用指纹开锁方式使用时，用户终端200发送锁保护设置，对指纹进行锁保护，即不允许通过指纹开锁，其具体实施方法包括以下三种，如图6所示，第一种方法包含了步骤10A、步骤10B、步骤10C：

[0059] 步骤10A、主控模块通过通讯模块接收终端发送的锁保护设置；

[0060] 步骤10B、主控模块输出控制指令至所述供电模块；

[0061] 步骤10C、所述供电模块停止对所述指纹采集模块供电。

[0062] 具体地，主控模块90输出控制指令，使供电模块80关闭对指纹采集模块40的供电，使得指纹采集模块40无法正常进行指纹采集，指纹开锁方式无法正常使用，从而达到“禁用指纹开锁”的目的。

[0063] 如图7所示，第二种方法包含了步骤20A、步骤20B、步骤20C：

[0064] 步骤20A、主控模块通过通讯模块接收终端发送的锁保护设置；

[0065] 步骤20B、所述指纹采集模块采集当前指纹信息；

[0066] 步骤20C、所述主控模块接收当前指纹信息但不对当前指纹信息进行验证。

[0067] 具体地，虽然所述指纹采集模块40采集当前指纹信息，且所述主控模块90接收当前指纹信息(即使其与指纹开锁的验证信息相符)，但不对当前指纹信息进行验证，从而达到“禁用指纹开锁”的目的。

[0068] 如图8所示，第三种方法包含了步骤30A、步骤30B、步骤30C、步骤30D：

[0069] 步骤30A、主控模块通过通讯模块接收终端发送的锁保护设置；

[0070] 步骤30B、所述指纹采集模块采集当前指纹信息；

[0071] 步骤30C、所述主控模块接收当前指纹信息并进行验证；

[0072] 步骤30D、如当前指纹信息与指纹开锁的验证信息相符时，所述主控模块不控制电机驱动模块工作。

[0073] 具体地，虽然指纹采集模块40采集当前指纹信息，且主控模块90接收当前指纹信息并进行验证，且即使当前指纹信息与指纹开锁的验证信息相符，但所述主控模块90不控制电机驱动模块20工作，从而达到“禁用止指纹开锁”的目的。

[0074] 请一起参阅图9，在本实施例中，在记录用户的开锁操作前，所述方法还进一步包括：接收用户设置的指纹验证等级设置，所述指纹验证等级与指纹验证精确度相对应。

[0075] 在此种情形下，所述验证除了包括对指纹进行验证外，还进一步包括对指纹精度进行识别，具体地，指纹采集模块40采集到用户的指纹后，所述主控模块90进行验证，且验证包括了对指纹比对精度的验证，即不满足指纹精度的识别结果，将被识别为非法操作，从而触发警报。在此种实施方式中，接收用户设置的指纹验证等级设置，所述指纹验证等级与

指纹验证精确度相对应。

[0076] 例如，如图9所示，假设系统预设的指纹识别精度包含了1-4级，其中1级精度要求最高，4级精度要求最低。

[0077] 使用时，当用户的锁保护设置为仅允许指纹1级精度要求时，仅满足指纹精度要求2-4中任意一者进行开锁操作将被阻止并被识别为非法操作，从而触发警报。

[0078] 所述报警信号可以发送至相关部门的报警系统进行报警，或者反馈至用户终端200提醒用户，从而让用户时刻掌握家里门锁的状态信息。

[0079] 可以理解的是，在本实施例中，所述锁保护设置中可进一步包括解除被禁用的开锁方式的时间限制信息，由此，在通过用户终端200进行锁保护设置时，也可同时设置解除验证的条件，例如锁保护设置中携带解除时间信息，当时间到达后上述解锁方式将自动解除。

[0080] 另外，在本实施例中，当执行完当前开锁操作后，在接收下一锁保护设置前，接受所述任意开锁方式包括指纹开锁、按键开锁、射频开锁。也即，对于任意一种开锁方式及其组合方式，当当前解锁方式满足预设条件并已完成解锁操作时，在下一次使用所述方法设置锁保护设置前，所述任意开锁方式(指纹、射频、按键)都可以用来进行解锁操作。

[0081] 另外，需要指明的是，在本实施例中，所述主控模块90用于验证当前的开锁方式与存储模块50的锁保护设置，及验证当前的验证信息与存储模块50的验证信息是否相符。可以理解的是，在其它变更实施方式中，所述存储模块50也可不存储所述锁保护设置，此时验证信息可存储在服务器(图未示)中，在执行开锁的过程中，主控模块90将验证结果发送与服务器的验证信息进行比对，以验证是否满足用户设置要求，并相应执行或不执行开锁操作。

[0082] 综上所述，本发明实施例提供的电子智能门锁指纹锁保护系统100及方法通过设置通讯模块30来接收用户终端200发送的锁保护设置，并通过主控模块90进行验证，达到对门锁进行保护的目的，使得通过用户终端200可随时随地切换门锁的保护模式，本实施例中，通过终端可以禁用指纹开锁操作，由此使得不法分子难以通过预设的方式来破解门锁的保护方式，从而极大地增强门锁的安全性。

[0083] 最后应说明的是：以上实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述实施例对本发明进行了详细的说明，本领域的普通技术人员当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

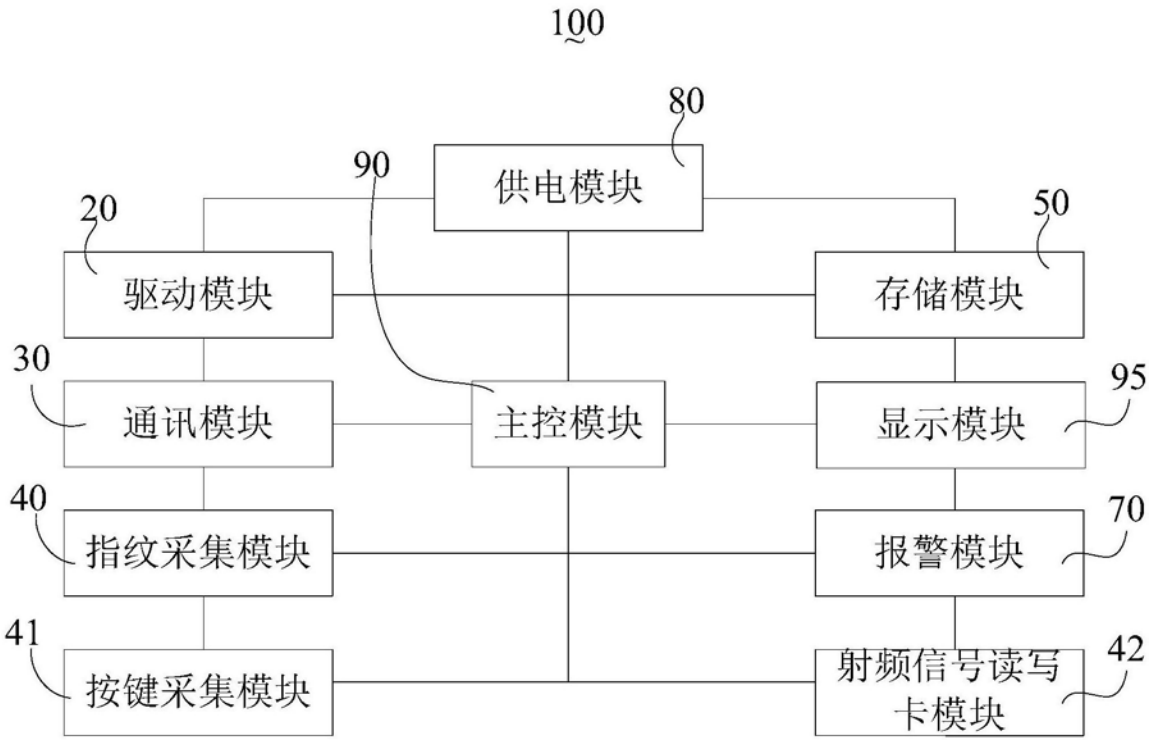

100
80
90
供电模块
20
驱动模块
50
存储模块
30
通讯模块
主控模块
95
显示模块
40
指纹采集模块
70
报警模块
41
按键采集模块
射频信号读写卡模块
42

图1

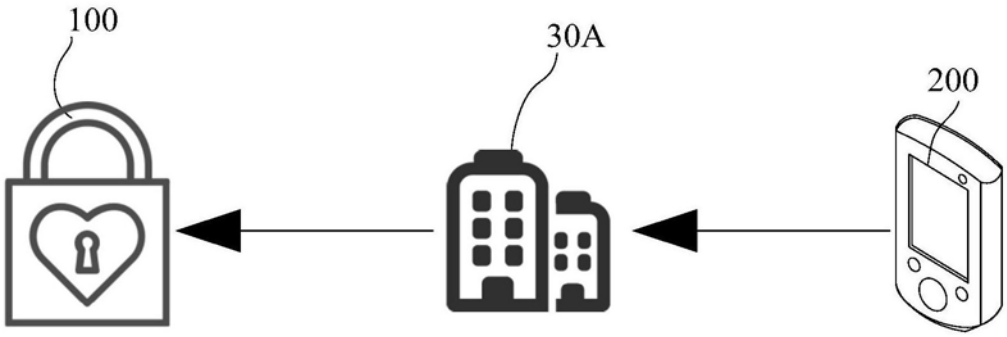

100
30A
200

图2

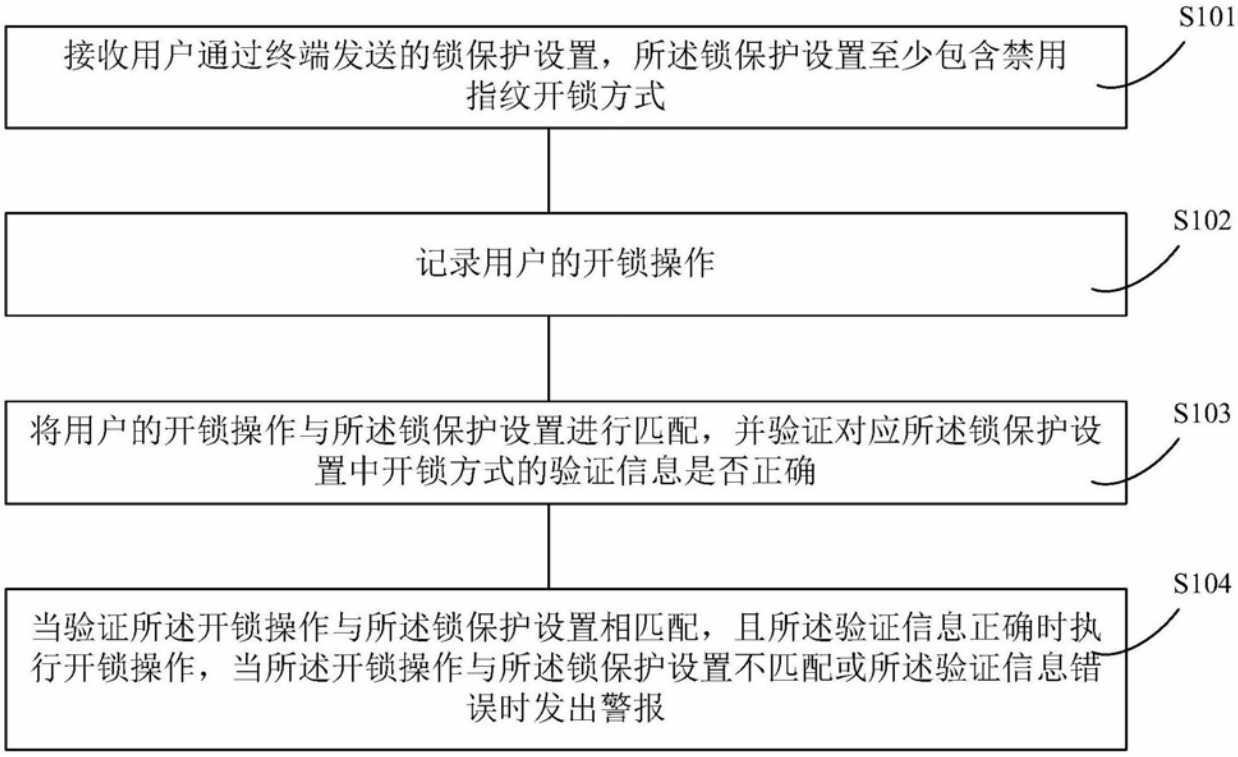

S101
接收用户通过终端发送的锁保护设置，所述锁保护设置至少包含禁用指纹开锁方式
S102
记录用户的开锁操作
S103
将用户的开锁操作与所述锁保护设置进行匹配，并验证对应所述锁保护设置中开锁方式的验证信息是否正确
S104
当验证所述开锁操作与所述锁保护设置相匹配，且所述验证信息正确时执行开锁操作，当所述开锁操作与所述锁保护设置不匹配或所述验证信息错误时发出警报

图3

图4


30A
请进行锁保护设置
（禁用开锁的方式）
用户A的指纹1
用户B的指纹2
用户C的指纹3
用户D的指纹4
用户E的指纹5
保存

图5

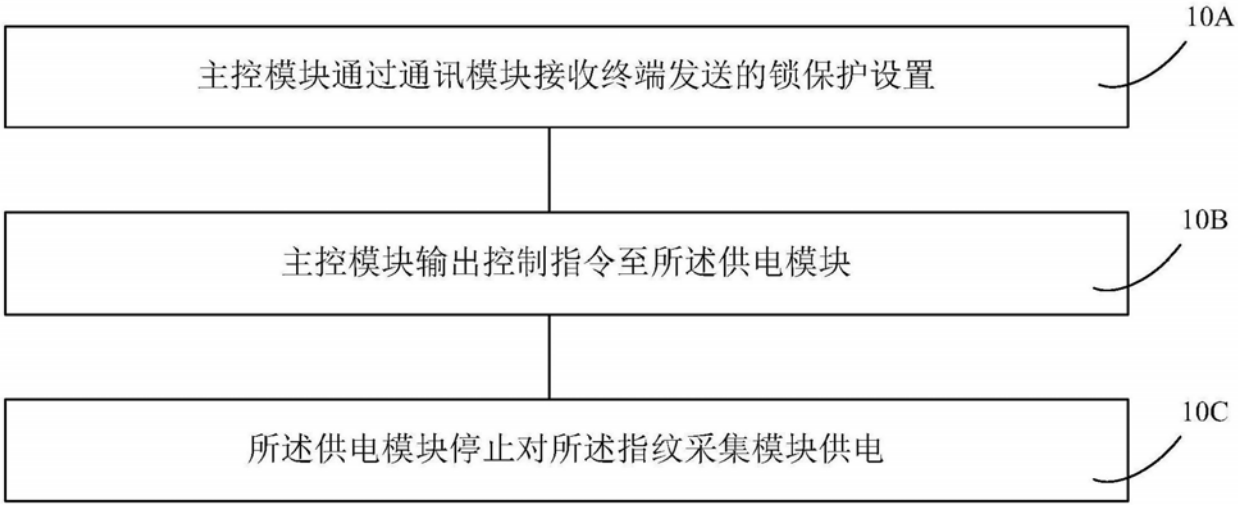

10A
主控模块通过通讯模块接收终端发送的锁保护设置
10B
主控模块输出控制指令至所述供电模块
10C
所述供电模块停止对所述指纹采集模块供电

图6

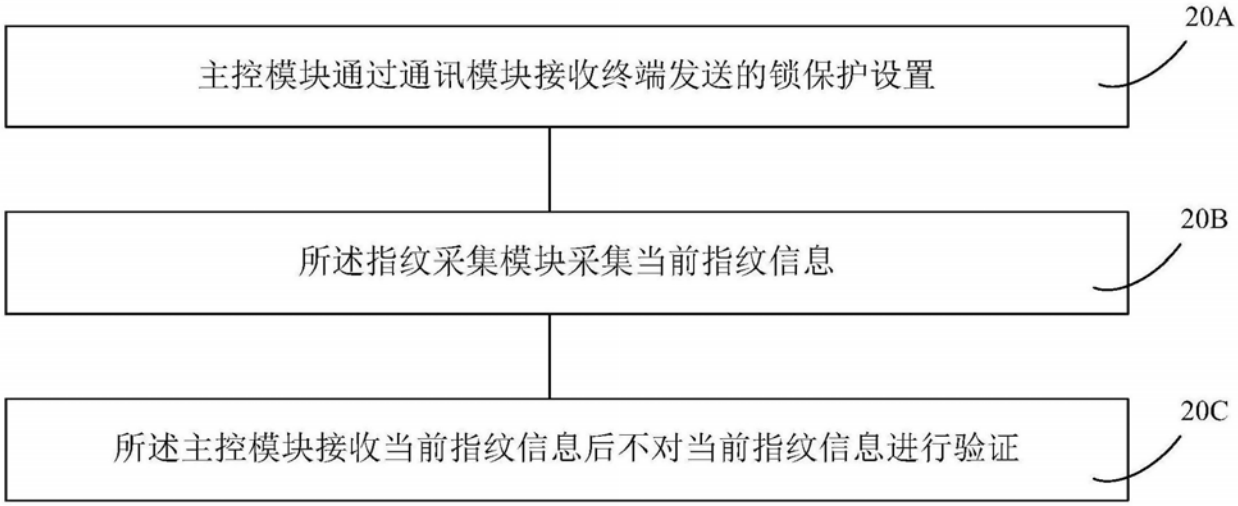

20A
主控模块通过通讯模块接收终端发送的锁保护设置
20B
所述指纹采集模块采集当前指纹信息
20C
所述主控模块接收当前指纹信息后不对当前指纹信息进行验证

图7

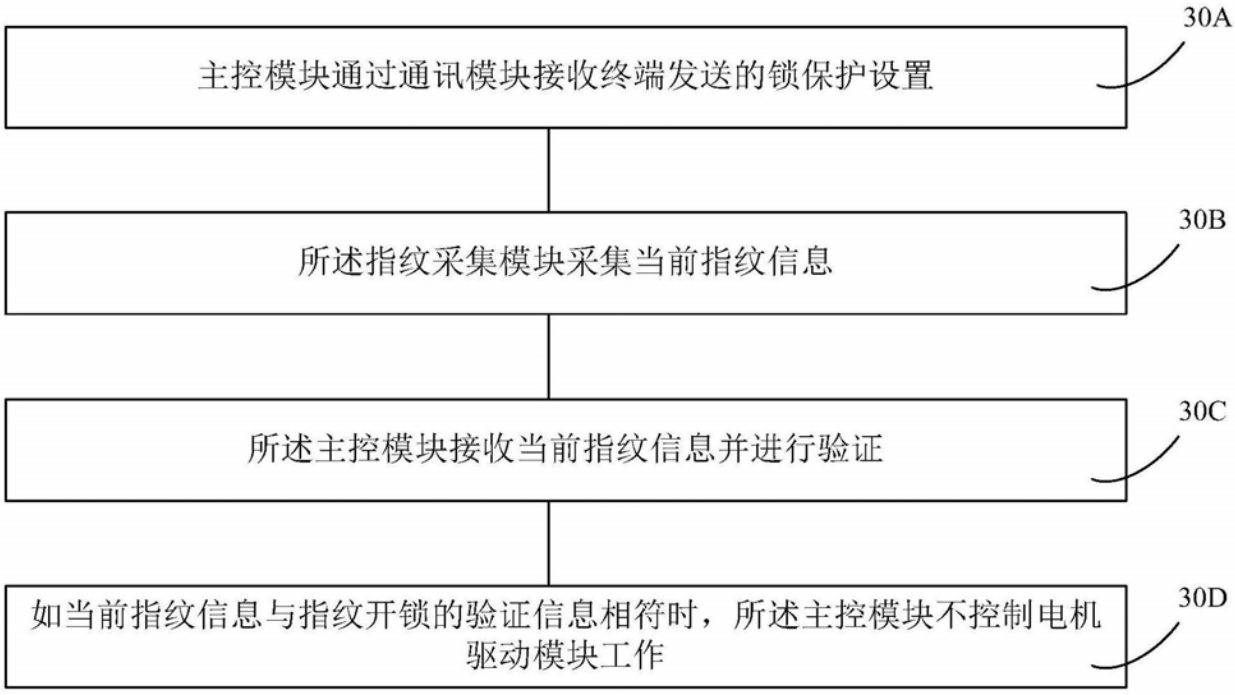

30A
主控模块通过通讯模块接收终端发送的锁保护设置
30B
所述指纹采集模块采集当前指纹信息
30C
所述主控模块接收当前指纹信息并进行验证
30D
如当前指纹信息与指纹开锁的验证信息相符时，所述主控模块不控制电机驱动模块工作

图8

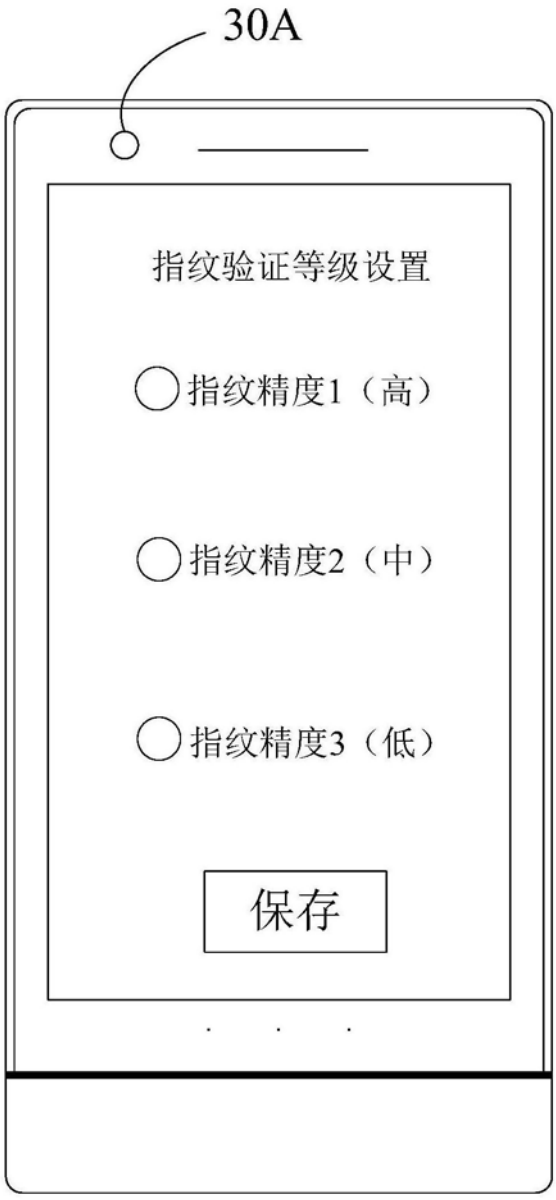


图9