(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 110349311 A
(43)申请公布日 2019.10.18

(21)申请号 201910610533.4

(22)申请日 2019.07.08

(71)申请人 江苏橙贝科技有限公司
地址 213001 江苏省常州市新北区华山路18号

(72)发明人 万志伟 张其新

(74)专利代理机构 北京华际知识产权代理有限公司 11676
代理人 张文杰

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

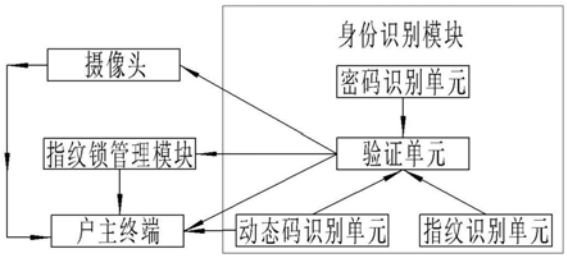
权利要求书3页 说明书9页 附图3页

(54)发明名称

一种基于区块链技术的指纹锁控制系统及方法

(57)摘要

本发明公开了一种基于区块链技术的指纹锁控制系统及方法，所述指纹锁控制系统包括身份识别模块、指纹锁管理模块和户主终端；所述身份识别模块包括密码识别单元、指纹识别单元、动态码识别单元和验证单元，所述密码识别单元、指纹识别单元、动态码识别单元分别与验证单元电连接；本发明模块设计合理，操作简单，本发明将区块链和指纹锁技术相结合，不仅有效实现了指纹锁的控制管理，保证户主的房屋安全，同时极大程度的降低了房屋威胁，技术方案中对于房屋可能出现的各种情况进行预设和相对应的模块设置，使得在发生房屋盗窃时，户主能够第一时间了解和进行有效的处理，降低财产损失的，具有较高的实用性。



CN 110349311 A

1.一种基于区块链技术的指纹锁控制系统，其特征在于：所述指纹锁控制系统包括身份识别模块、指纹锁管理模块和户主终端；所述身份识别模块包括密码识别单元、指纹识别单元、动态码识别单元和验证单元，所述密码识别单元、指纹识别单元、动态码识别单元分别与验证单元电连接；

所述密码识别单元用于录入用户的有效密码；所述指纹识别单元用于录入用户的指纹；所述户主终端可获取随机动态码，用户通过动态码识别单元录入随机动态码进行身份验证；

所述验证单元与指纹锁管理模块电连接，所述指纹锁管理模块用于控制指纹锁开启、关闭；所述验证单元、指纹锁管理模块和动态码识别单元分别与户主终端无线连接；

所述指纹锁控制系统还包括若干个摄像头，用于上传用户人脸图像，所述摄像头与验证单元电连接，所述摄像头与户主终端无线连接。

2.根据权利要求1所述的一种基于区块链技术的指纹锁控制系统，其特征在于：所述户主终端包括辅助验证模块、存储模块、查询模块和警报模块；

所述动态码识别单元、验证单元分别与辅助验证模块无线通信，用户通过辅助验证模块获取随机动态码，辅助用户进行身份验证；

所述验证单元、指纹锁管理模块分别与存储模块无线通信，所述验证单元上传身份验证结果和用户录入的身份信息，所述指纹锁管理模块上传指纹锁开启时间；

所述存储模块与查询模块电连接；所述验证单元、指纹锁管理模块分别与警报模块无线通信；所述摄像头分别与存储模块、警报模块无线通信。

3.根据权利要求2所述的一种基于区块链技术的指纹锁控制系统，其特征在于：所述存储模块包括区块链单元和索引单元，所述区块链单元与索引单元电连接；所述索引单元与查询模块电连接，所述验证单元、摄像头和指纹锁管理模块分别与区块链单元无线连接。

4.根据权利要求2所述的一种基于区块链技术的指纹锁控制系统，其特征在于：所述验证单元包括第一验证单元、第二验证单元和提示单元；

所述密码识别单元、指纹识别单元、和动态码识别单元分别与第一验证单元电连接，所述密码识别单元、指纹识别单元和动态码识别单元分别与第二验证单元电连接，所述第一验证单元、第二验证单元分别与提示单元电连接；

所述提示单元分别与存储模块、警报模块无线连接；所述提示单元分别与摄像头、指纹锁管理模块电连接。

5.根据权利要求1所述的一种基于区块链技术的指纹锁控制系统，其特征在于：所述指纹锁控制系统还包括若干个红外传感模块，用于记录用户在指纹锁前的停留时间，所述红外传感模块与摄像头电连接。

6.一种基于区块链技术的指纹锁控制方法，其特征在于：包括以下步骤：

1)用户录入身份信息，通过身份识别模块进行身份验证，若身份验证成功，则转步骤3)，若身份验证失败，则转步骤2)；

2)身份验证失败，未触发指纹锁管理模块，指纹锁处于关闭状态；

3)身份验证成功，触发指纹锁管理模块，指纹锁开启，同时指纹锁管理模块发送提示信息、指纹锁开锁时间至户主终端；触发摄像头，摄像头采集用户人脸图像，并上传至户主终端存储；身份识别模块将身份信息传输至户主终端；

4)户主终端存储身份信息和指纹锁管理模块的开锁时间,生成智能记录单,并通过存储模块存储;查询模块可发送查询信号查询智能记录单;

5)警报模块监控整个系统的工作。

7.根据权利要求6所述的一种基于区块链技术的指纹锁控制方法,其特征在于:所述步骤1)中,用户的身份验证包括以下步骤:

a)用户可选择通过密码识别单元、指纹识别单元、动态码识别单元录入身份信息,其中密码识别单元录入有效密码,指纹识别单元录入用户指纹,动态码识别单元可录入户主终端获取的随机动态码;身份信息为有效密码、有效指纹和随机动态码中的任意两种;

b)验证单元接收身份信息,记录时间t内验证单元接收身份信息的次数为N,t为5min,判断N是否满足N≤5,若满足,则转步骤c),否则转步骤e);

c)验证单元将接收到的身份信息进行验证对比,若身份信息均验证成功,则提示“YES”,转步骤d);若身份信息中出现验证失败,则提示“NO”,用户选择重新进行身份验证,则转步骤a);若用户选择放弃,则转步骤e);

d)身份验证成功,触发指纹锁管理模块,指纹锁开启,同时指纹锁管理模块发送提示信息、指纹锁开锁时间至户主终端;触发摄像头,摄像头采集用户人脸图像,并上传至户主终端存储;验证单元上传身份信息至户主终端存储;

e)身份验证失败,未触发指纹锁管理模块,指纹锁处于关闭状态。

8.根据权利要求7所述的一种基于区块链技术的指纹锁控制方法,其特征在于:所述步骤a)中,动态码识别单元工作时包括以下步骤:

I)用户选择动态码识别单元,动态码识别单元发送提示信号至户主终端,户主终端的辅助验证模块获取随机动态码A,并记录该动态码获取时间为T_1;

II)辅助验证模块将随机动态码A发送至存储模块存储,并将该随机动态码A发送至验证单元;同时用户录入所得随机动态码B,并记录该动态码录入时间为T_2;

III)计算时间差$T=T_2-T_1$,判断T是否满足T≤3min,若满足,则转步骤IV),否则转步骤V);

IV)验证单元对比随机动态码A、随机动态码B,进行身份验证;

V)随机动态码A失效,操作结束。

9.根据权利要求6所述的一种基于区块链技术的指纹锁控制方法,其特征在于:所述步骤4)中,户主终端生成智能记录单包括以下步骤:

S1:户主终端的存储模块接收指纹锁管理模块上传的指纹锁开启时间、身份识别模块上传的用户身份信息、摄像头上传的用户人脸图像;

S2:存储模块的区块链单元生成智能记录单,智能记录单包括用户身份信息、指纹锁开启时间、用户人脸图像;

S3:存储模块的索引单元提取指纹锁开启时间,对所述指纹锁开启时间进行哈希运算得到时间标识哈希值;

S4:通过索引单元将时间标识哈希值设为索引,将对应开锁时间生成的智能记录单存储在区块链节点中;

S5:户主终端的查询模块发送查询信息时,可根据时间标识哈希值索引,找到对应区块链节点中的智能记录单。

10.根据权利要求6所述的一种基于区块链技术的指纹锁控制方法，其特征在于：所述警报模块工作时包括以下几种情况：

所述验证单元在时间记录时间t内接收身份信息的次数N＞5，时间t为5min，且验证均为失败，验证单元发送提示信号至警报模块；

所述指纹锁管理模块检测到指纹锁被破坏，则指纹锁管理模块发送提示信号至警报模块；

红外传感模块记录用户停留时间t_1，当时间t_1＞20min时，验证单元未检测到用户录入的身份信息，则摄像头采集用户人脸图像，并发送提示信号至警报模块。

一种基于区块链技术的指纹锁控制系统及方法

技术领域

[0001] 本发明涉及指纹锁控制技术领域，具体是一种基于区块链技术的指纹锁控制系统及方法。

背景技术

[0002] 指纹锁是一种以人体手指部位的指纹为识别载体和手段的智能锁具，它是计算机信息技术、电子技术、机械技术和现代五金工艺的完美结晶。指纹锁一般由电子识别与控制、机械联动系统两部分组成。活体指纹的唯一性和不可复制性决定了指纹锁是目前所有锁具中较为安全的锁种。

[0003] 但在指纹锁的实际应用中，由于户主的指纹易获取，利用一些指纹模拟工具就可以打开单纯的指纹锁，因此仅仅通过指纹锁往往起不到很好的防护效果，不法分子很轻易就能够破解指纹锁，这给我们的房屋安全带来较大的隐患。

[0004] 针对上述情况，我们设计了一种基于区块链技术的指纹锁控制系统及方法，这是我们亟待解决的问题之一。

发明内容

[0005] 本发明的目的在于提供一种基于区块链技术的指纹锁控制系统及方法，以解决现有技术中的问题。

[0006] 为实现上述目的，本发明提供如下技术方案：

[0007] 一种基于区块链技术的指纹锁控制系统，所述指纹锁控制系统包括身份识别模块、指纹锁管理模块和户主终端；所述身份识别模块包括密码识别单元、指纹识别单元、动态码识别单元和验证单元，所述密码识别单元、指纹识别单元、动态码识别单元分别与验证单元电连接；

[0008] 所述密码识别单元用于录入用户的有效密码；所述指纹识别单元用于录入用户的指纹；所述户主终端可获取随机动态码，用户通过动态码识别单元录入随机动态码进行身份验证；

[0009] 所述验证单元与指纹锁管理模块电连接，所述指纹锁管理模块用于控制指纹锁开启、关闭；所述验证单元、指纹锁管理模块和动态码识别单元分别与户主终端无线连接；

[0010] 所述指纹锁控制系统还包括若干个摄像头，用于上传用户人脸图像，所述摄像头与验证单元电连接，所述摄像头与户主终端无线连接。

[0011] 本技术方案中身份识别模块包括密码识别单元、指纹识别单元、动态码识别单元，用户可通过密码识别单元录入有效密码，通过指纹识别单元录入指纹信息，并通过验证单元将这些身份信息进行验证，验证单元中预存有本地信息，本地信息包括有效密码和户主允许进入房屋的访客指纹信息库，对采集到的用户指纹信息、用户录入的有效密码进行验证；动态码识别单元在进行身份验证时，需要利用户主终端先获取随机动态码，用户再通过人工录入随机动态码来进行身份验证。

[0012] 在进行身份验证操作时，用户可在有效密码识别、指纹识别和随机动态码识别这三种验证方式中任意挑选两种进行身份验证，若两种验证方式均通过，则验证单元提示“YES”，身份验证成功，若其中有一种出现错误，或者两种均出现错误，则验证单元提示“NO”，身份验证失败；

[0013] 本技术方案中验证单元与指纹锁管理模块电连接，当用户的身份验证成功时，验证单元提示“YES”，则触发指纹锁管理模块，开启指纹锁，指纹锁管理模块会发送提示信息至户主终端，提醒户主房屋指纹锁开启，并将指纹锁开启时间记录上传；同时验证单元会将采集到的用户身份信息上传至户主终端，用于保存和后续户主的查询；当用户的身份验证失败时，验证单元提示“NO”，指纹锁管理模块不被触发，指纹锁依旧处于关闭状态。

[0014] 本技术方案中还设计了若干个摄像头，摄像头与验证单元电连接，当验证单元提示“YES”，在触发指纹锁管理模块的同时触发摄像头，摄像头会进行用户的人脸图像采集，再上传至户主终端保存，便于后续户主查询；当户主的房屋遭窃时，户主可以通过查询户主终端内保存的开锁用户人脸头像来锁定嫌疑人。

[0015] 较优化的方案，所述户主终端包括辅助验证模块、存储模块、查询模块和警报模块；

[0016] 所述动态码识别单元、验证单元分别与辅助验证模块无线通信，用户通过辅助验证模块获取随机动态码，辅助用户进行身份验证；

[0017] 所述验证单元、指纹锁管理模块分别与存储模块无线通信，所述验证单元上传身份验证结果和用户录入的身份信息，所述指纹锁管理模块上传指纹锁开启时间；

[0018] 所述存储模块与查询模块电连接；所述验证单元、指纹锁管理模块分别与警报模块无线通信；所述摄像头分别与存储模块、警报模块无线通信。

[0019] 本技术方案中户主终端包括辅助验证模块、存储模块、查询模块和警报模块；其中动态码识别单元发送提示信号至辅助验证模块，辅助验证模块可获取随机动态码，并将随机动态码发送至验证单元，用户可询问户主获得随机动态码，再通过人工录入进行身份验证，这样大大提高了户主的房屋安全；

[0020] 存储模块可以对身份验证过程中涉及到的数据进行排列，利用指纹锁的开启时间进行排列，并将指纹锁的开启时间进行哈希算法计算得到时间标识哈希值，以此为索引进行存储；这样设计后户主可根据需要查询的时间进行记录寻找，操作起来更方便快速。

[0021] 警报模块可实现对整个指纹锁控制系统的监控，极大程度的避免各种对房屋安全具有威胁的情况，保证户主的房屋安全；其中警报模块工作情况包括以下几种：

[0022] ①根据验证单元中检测数据得知，用户在5min内接收身份信息的次数N＞5，且每次身份验证均为失败，则验证单元发送提示信号至警报模块；户主可及时了解房屋情况，判断是否存在嫌疑人想要进屋盗窃的情况，必要时可直接联系物业，极大程度保障了房屋安全；

[0023] ②指纹锁管理模块检测到指纹锁被破坏，则指纹锁管理模块发送提示信号至警报模块，户主可及时判断是否有人恶意破坏门锁，并在第一时间处理，避免不必要的财产损失；

[0024] ③系统中设计了红外传感模块，当红外传感模块检测到有用户在指纹锁前停留的时间大于20min，则摄像头采集用户人脸图像，并发送提示信号至警报模块，户主可及时了

解情况，为避免有不法分子在门前观察情况，降低房屋安全威胁。

[0025] 较优化的方案，所述存储模块包括区块链单元和索引单元，所述区块链单元与索引单元电连接；所述索引单元与查询模块电连接，所述验证单元、摄像头和指纹锁管理模块分别与区块链单元无线连接。

[0026] 本技术方案中存储模块包括区块链单元和索引单元，其中区块链单元可接收验证单元发送的身份信息、摄像头上传的用户人脸图像、指纹锁管理模块上传的指纹锁开启时间，并根据这些消息生成智能记录单，便于户主后续查询时一目了然的清晰指纹锁开启情况和进入房屋的用户情况。

[0027] 在实际操作中，还可以将该系统用于公寓物业管理、酒店信息记录等多种环境中，智能记录单的记录内容也可以根据实际应用环境进行修改。

[0028] 索引单元可对指纹锁开启时间进行哈希运算，得到时间标识哈希值，数据存储更加有条理，也便于户主进行查询，实际操作更加便捷。

[0029] 较优化的方案，所述验证单元包括第一验证单元、第二验证单元和提示单元；

[0030] 所述密码识别单元、指纹识别单元、和动态码识别单元分别与第一验证单元电连接，所述密码识别单元、指纹识别单元和动态码识别单元分别与第二验证单元电连接，所述第一验证单元、第二验证单元分别与提示单元电连接；

[0031] 所述提示单元分别与存储模块、警报模块无线连接；所述提示单元分别与摄像头、指纹锁管理模块电连接。

[0032] 较优化的方案，所述指纹锁控制系统还包括若干个红外传感模块，用于记录用户在指纹锁前的停留时间，所述红外传感模块与摄像头电连接。

[0033] 一种基于区块链技术的指纹锁控制方法，包括以下步骤：

[0034] 1)用户录入身份信息，通过身份识别模块进行身份验证，若身份验证成功，则转步骤3)，若身份验证失败，则转步骤2)；

[0035] 2)身份验证失败，未触发指纹锁管理模块，指纹锁处于关闭状态；

[0036] 3)身份验证成功，触发指纹锁管理模块，指纹锁开启，同时指纹锁管理模块发送提示信息、指纹锁开锁时间至户主终端；触发摄像头，摄像头采集用户人脸图像，并上传至户主终端存储；身份识别模块将身份信息传输至户主终端；

[0037] 4)户主终端存储身份信息和指纹锁管理模块的开锁时间，生成智能记录单，并通过存储模块存储；查询模块可发送查询信号查询智能记录单；

[0038] 5)警报模块监控整个系统的工作。

[0039] 较优化的方案，所述步骤1)中，用户的身份验证包括以下步骤：

[0040] a)用户可选择通过密码识别单元、指纹识别单元、动态码识别单元录入身份信息，其中密码识别单元录入有效密码，指纹识别单元录入用户指纹，动态码识别单元可录入户主终端获取的随机动态码；身份信息为有效密码、有效指纹和随机动态码中的任意两种；

[0041] b)验证单元接收身份信息，记录时间t内验证单元接收身份信息的次数为N，t为5min，判断N是否满足N≤5，若满足，则转步骤c)，否则转步骤e)；

[0042] c)验证单元将接收到的身份信息进行验证对比，若身份信息均验证成功，则提示“YES”，转步骤d)；若身份信息中出现验证失败，则提示“NO”，用户选择重新进行身份验证，则转步骤a)；若用户选择放弃，则转步骤e)；

[0043] d)身份验证成功,触发指纹锁管理模块,指纹锁开启,同时指纹锁管理模块发送提示信息、指纹锁开锁时间至户主终端;触发摄像头,摄像头采集用户人脸图像,并上传至户主终端存储;验证单元上传身份信息至户主终端存储;

[0044] e)身份验证失败,未触发指纹锁管理模块,指纹锁处于关闭状态。

[0045] 较优化的方案,所述步骤a)中,动态码识别单元工作时包括以下步骤:

[0046] I)用户选择动态码识别单元,动态码识别单元发送提示信号至户主终端,户主终端的辅助验证模块获取随机动态码A,并记录该动态码获取时间为T_1;

[0047] II)辅助验证模块将随机动态码A发送至存储模块存储,并将该随机动态码A发送至验证单元;同时用户录入所得随机动态码B,并记录该动态码录入时间为T_2;

[0048] III)计算时间差$T=T_2-T_1$,判断T是否满足$T\leq 3min$,若满足,则转步骤IV),否则转步骤V);

[0049] IV)验证单元对比随机动态码A、随机动态码B,进行身份验证;

[0050] V)随机动态码A失效,操作结束。

[0051] 较优化的方案,所述步骤4)中,户主终端生成智能记录单包括以下步骤:

[0052] S1:户主终端的存储模块接收指纹锁管理模块上传的指纹锁开启时间、身份识别模块上传的用户身份信息、摄像头上传的用户人脸图像;

[0053] S2:存储模块的区块链单元生成智能记录单,智能记录单包括用户身份信息、指纹锁开启时间、用户人脸图像;

[0054] S3:存储模块的索引单元提取指纹锁开启时间,对所述指纹锁开启时间进行哈希运算得到时间标识哈希值;

[0055] S4:通过索引单元将时间标识哈希值设为索引,将对应开锁时间生成的智能记录单存储在区块链节点中;

[0056] S5:户主终端的查询模块发送查询信息时,可根据时间标识哈希值索引,找到对应区块链节点中的智能记录单。

[0057] 较优化的方案,所述警报模块工作时包括以下几种情况:

[0058] 所述验证单元在时间记录时间t内接收身份信息的次数$N>5$,时间t为5min,且验证均为失败,验证单元发送提示信号至警报模块;

[0059] 所述指纹锁管理模块检测到指纹锁被破坏,则指纹锁管理模块发送提示信号至警报模块;

[0060] 红外传感模块记录用户停留时间t_1,当时间$t_1>20min$时,验证单元未检测到用户录入的身份信息,则摄像头采集用户人脸图像,并发送提示信号至警报模块。

[0061] 与现有技术相比,本发明的有益效果是:

[0062] 本发明中设计了一种基于区块链技术的指纹锁控制系统及方法,其中包括身份识别模块、指纹锁管理模块和户主终端,身份识别模块用于对用户的身份进行识别,指纹锁管理模块用于控制指纹锁的开启和关闭。

[0063] 本发明设计了一种基于区块链技术的指纹锁控制系统及方法,模块设计合理,操作简单,本发明将区块链和指纹锁技术相结合,不仅有效实现了指纹锁的控制管理,保证户主的房屋安全,同时极大程度的降低了房屋威胁,技术方案中对于房屋可能出现的各种情况进行预设和相对应的模块设置,使得在发生房屋盗窃时,户主能够第一时间了解和进行

有效的处理,降低财产损失的,具有较高的实用性。

附图说明

[0064] 为了使本发明的内容更容易被清楚地理解,下面根据具体实施例并结合附图,对本发明作进一步详细的说明。

[0065] 图1为本发明一种基于区块链技术的指纹锁控制系统的整体模块连接示意图;

[0066] 图2为本发明一种基于区块链技术的指纹锁控制系统的整体模块连接示意图;

[0067] 图3为本发明一种基于区块链技术的指纹锁控制系统的户主终端连接示意图;

[0068] 图4为本发明一种基于区块链技术的指纹锁控制系统的户主终端连接示意图;

[0069] 图5为本发明一种基于区块链技术的指纹锁控制系统的户主终端、身份识别模块连接示意图。

具体实施方式

[0070] 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做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。

[0071] 如图1-图5所示,一种基于区块链技术的指纹锁控制系统,所述指纹锁控制系统包括身份识别模块、指纹锁管理模块和户主终端;所述身份识别模块包括密码识别单元、指纹识别单元、动态码识别单元和验证单元,所述密码识别单元、指纹识别单元、动态码识别单元分别与验证单元电连接;

[0072] 所述密码识别单元用于录入用户的有效密码;所述指纹识别单元用于录入用户的指纹;所述户主终端可获取随机动态码,用户通过动态码识别单元录入随机动态码进行身份验证;

[0073] 所述验证单元与指纹锁管理模块电连接,所述指纹锁管理模块用于控制指纹锁开启、关闭;所述验证单元、指纹锁管理模块和动态码识别单元分别与户主终端无线连接;

[0074] 所述指纹锁控制系统还包括若干个摄像头,用于上传用户人脸图像,所述摄像头与验证单元电连接,所述摄像头与户主终端无线连接。

[0075] 本技术方案中身份识别模块包括密码识别单元、指纹识别单元、动态码识别单元,用户可通过密码识别单元录入有效密码,通过指纹识别单元录入指纹信息,并通过验证单元将这些身份信息进行验证,验证单元中预存有本地信息,本地信息包括有效密码和户主允许进入房屋的访客指纹信息库,对采集到的用户指纹信息、用户录入的有效密码进行验证;动态码识别单元在进行身份验证时,需要利用户主终端先获取随机动态码,用户再通过人工录入随机动态码来进行身份验证。

[0076] 在进行身份验证操作时,用户可在有效密码识别、指纹识别和随机动态码识别这三种验证方式中任意挑选两种进行身份验证,若两种验证方式均通过,则验证单元提示“YES”,身份验证成功,若其中有一种出现错误,或者两种均出现错误,则验证单元提示“NO”,身份验证失败;

[0077] 本技术方案中验证单元与指纹锁管理模块电连接,当用户的身份验证成功时,验

证单元提示“YES”，则触发指纹锁管理模块，开启指纹锁，指纹锁管理模块会发送提示信息至户主终端，提醒户主房屋指纹锁开启，并将指纹锁开启时间记录上传；同时验证单元会将采集到的用户身份信息上传至户主终端，用于保存和后续户主的查询；当用户的身份验证失败时，验证单元提示“NO”，指纹锁管理模块不被触发，指纹锁依旧处于关闭状态。

[0078] 本技术方案中还设计了若干个摄像头，摄像头与验证单元电连接，当验证单元提示“YES”，在触发指纹锁管理模块的同时触发摄像头，摄像头会进行用户的人脸图像采集，再上传至户主终端保存，便于后续户主查询；当户主的房屋遭窃时，户主可以通过查询户主终端内保存的开锁用户人脸头像来锁定嫌疑人。

[0079] 所述户主终端包括辅助验证模块、存储模块、查询模块和警报模块；

[0080] 所述动态码识别单元、验证单元分别与辅助验证模块无线通信，用户通过辅助验证模块获取随机动态码，辅助用户进行身份验证；

[0081] 所述验证单元、指纹锁管理模块分别与存储模块无线通信，所述验证单元上传身份验证结果和用户录入的身份信息，所述指纹锁管理模块上传指纹锁开启时间；

[0082] 所述存储模块与查询模块电连接；所述验证单元、指纹锁管理模块分别与警报模块无线通信；所述摄像头分别与存储模块、警报模块无线通信。

[0083] 本技术方案中户主终端包括辅助验证模块、存储模块、查询模块和警报模块；其中动态码识别单元发送提示信号至辅助验证模块，辅助验证模块可获取随机动态码，并将随机动态码发送至验证单元，用户可询问户主获得随机动态码，再通过人工录入进行身份验证，这样大大提高了户主的房屋安全；

[0084] 存储模块可以对身份验证过程中涉及到的数据进行排列，利用指纹锁的开启时间进行排列，并将指纹锁的开启时间进行哈希算法计算得到时间标识哈希值，以此为索引进行存储；这样设计后户主可根据需要查询的时间进行记录寻找，操作起来更方便快速。

[0085] 警报模块可实现对整个指纹锁控制系统的监控，极大程度的避免各种对房屋安全具有威胁的情况，保证户主的房屋安全；其中警报模块工作情况包括以下几种：

[0086] ①根据验证单元中检测数据得知，用户在5min内接收身份信息的次数N＞5，且每次身份验证均为失败，则验证单元发送提示信号至警报模块；户主可及时了解房屋情况，判断是否存在嫌疑人想要进屋盗窃的情况，必要时可直接联系物业，极大程度保障了房屋安全；

[0087] ②指纹锁管理模块检测到指纹锁被破坏，则指纹锁管理模块发送提示信号至警报模块，户主可及时判断是否有人恶意破坏门锁，并在第一时间处理，避免不必要的财产损失；

[0088] ③系统中设计了红外传感模块，当红外传感模块检测到有用户在指纹锁前停留的时间大于20min，则摄像头采集用户人脸图像，并发送提示信号至警报模块，户主可及时了解情况，为避免有不法分子在门前观察情况，降低房屋安全威胁。

[0089] 所述存储模块包括区块链单元和索引单元，所述区块链单元与索引单元电连接；所述索引单元与查询模块电连接，所述验证单元、摄像头和指纹锁管理模块分别与区块链单元无线连接。

[0090] 本技术方案中存储模块包括区块链单元和索引单元，其中区块链单元可接收验证单元发送的身份信息、摄像头上传的用户人脸图像、指纹锁管理模块上传的指纹锁开启时

间，并根据这些消息生成智能记录单，便于户主后续查询时一目了然的清晰指纹锁开启情况和进入房屋的用户情况。

[0091] 在实际操作中，还可以将该系统用于公寓物业管理、酒店信息记录等多种环境中，智能记录单的记录内容也可以根据实际应用环境进行修改。

[0092] 索引单元可对指纹锁开启时间进行哈希运算，得到时间标识哈希值，数据存储更加有条理，也便于户主进行查询，实际操作更加便捷。

[0093] 所述验证单元包括第一验证单元、第二验证单元和提示单元；

[0094] 所述密码识别单元、指纹识别单元、和动态码识别单元分别与第一验证单元电连接，所述密码识别单元、指纹识别单元和动态码识别单元分别与第二验证单元电连接，所述第一验证单元、第二验证单元分别与提示单元电连接；

[0095] 所述提示单元分别与存储模块、警报模块无线连接；所述提示单元分别与摄像头、指纹锁管理模块电连接。

[0096] 所述指纹锁控制系统还包括若干个红外传感模块，用于记录用户在指纹锁前的停留时间，所述红外传感模块与摄像头电连接。

[0097] 本发明中设计了一种基于区块链技术的指纹锁控制系统及方法，其中包括身份识别模块、指纹锁管理模块和户主终端，身份识别模块用于对用户的身份进行识别，指纹锁管理模块用于控制指纹锁的开启和关闭。

[0098] 本发明设计了一种基于区块链技术的指纹锁控制系统及方法，模块设计合理，操作简单，本发明将区块链和指纹锁技术相结合，不仅有效实现了指纹锁的控制管理，保证户主的房屋安全，同时极大程度的降低了房屋威胁，技术方案中对于房屋可能出现的各种情况进行预设和相对应的模块设置，使得在发生房屋盗窃时，户主能够第一时间了解和进行有效的处理，降低财产损失的，具有较高的实用性。

[0099] 一种基于区块链技术的指纹锁控制方法，包括以下步骤：

[0100] 1)用户录入身份信息，通过身份识别模块进行身份验证，若身份验证成功，则转步骤3)，若身份验证失败，则转步骤2)；

[0101] 2)身份验证失败，未触发指纹锁管理模块，指纹锁处于关闭状态；

[0102] 3)身份验证成功，触发指纹锁管理模块，指纹锁开启，同时指纹锁管理模块发送提示信息、指纹锁开锁时间至户主终端；触发摄像头，摄像头采集用户人脸图像，并上传至户主终端存储；身份识别模块将身份信息传输至户主终端；

[0103] 4)户主终端存储身份信息和指纹锁管理模块的开锁时间，生成智能记录单，并通过存储模块存储；查询模块可发送查询信号查询智能记录单；

[0104] 5)警报模块监控整个系统的工作。

[0105] 所述步骤1)中，用户的身份验证包括以下步骤：

[0106] a)用户可选择通过密码识别单元、指纹识别单元、动态码识别单元录入身份信息，其中密码识别单元录入有效密码，指纹识别单元录入用户指纹，动态码识别单元可录入户主终端获取的随机动态码；身份信息为有效密码、有效指纹和随机动态码中的任意两种；

[0107] b)验证单元接收身份信息，记录时间t内验证单元接收身份信息的次数为N，t为5min，判断N是否满足N≤5，若满足，则转步骤c)，否则转步骤e)；

[0108] c)验证单元将接收到的身份信息进行验证对比，若身份信息均验证成功，则提示

“YES”,转步骤d);若身份信息中出现验证失败,则提示“NO”,用户选择重新进行身份验证,则转步骤a);若用户选择放弃,则转步骤e);

[0109] d)身份验证成功,触发指纹锁管理模块,指纹锁开启,同时指纹锁管理模块发送提示信息、指纹锁开锁时间至户主终端;触发摄像头,摄像头采集用户人脸图像,并上传至户主终端存储;验证单元上传身份信息至户主终端存储;

[0110] e)身份验证失败,未触发指纹锁管理模块,指纹锁处于关闭状态。

[0111] 所述步骤a)中,动态码识别单元工作时包括以下步骤:

[0112] I)用户选择动态码识别单元,动态码识别单元发送提示信号至户主终端,户主终端的辅助验证模块获取随机动态码A,并记录该动态码获取时间为T_1;

[0113] II)辅助验证模块将随机动态码A发送至存储模块存储,并将该随机动态码A发送至验证单元;同时用户录入所得随机动态码B,并记录该动态码录入时间为T_2;

[0114] III)计算时间差$T=T_2-T_1$,判断T是否满足$T\leq 3min$,若满足,则转步骤IV),否则转步骤V);

[0115] IV)验证单元对比随机动态码A、随机动态码B,进行身份验证;

[0116] V)随机动态码A失效,操作结束。

[0117] 所述步骤4)中,户主终端生成智能记录单包括以下步骤:

[0118] S1:户主终端的存储模块接收指纹锁管理模块上传的指纹锁开启时间、身份识别模块上传的用户身份信息、摄像头上传的用户人脸图像;

[0119] S2:存储模块的区块链单元生成智能记录单,智能记录单包括用户身份信息、指纹锁开启时间、用户人脸图像;

[0120] S3:存储模块的索引单元提取指纹锁开启时间,对所述指纹锁开启时间进行哈希运算得到时间标识哈希值;

[0121] S4:通过索引单元将时间标识哈希值设为索引,将对应开锁时间生成的智能记录单存储在区块链节点中;

[0122] S5:户主终端的查询模块发送查询信息时,可根据时间标识哈希值索引,找到对应区块链节点中的智能记录单。

[0123] 所述警报模块工作时包括以下几种情况:

[0124] 所述验证单元在时间记录时间t内接收身份信息的次数$N>5$,时间t为5min,且验证均为失败,验证单元发送提示信号至警报模块;

[0125] 所述指纹锁管理模块检测到指纹锁被破坏,则指纹锁管理模块发送提示信号至警报模块;

[0126] 红外传感模块记录用户停留时间t_1,当时间$t_1>20min$时,验证单元未检测到用户录入的身份信息,则摄像头采集用户人脸图像,并发送提示信号至警报模块。

[0127] 实施例1:限定条件:用户录入有效密码A、指纹信息B和随机动态码C;验证单元中预存的有效密码A_1、户主允许进入房屋的访客指纹信息库、户主终端获得的随机动态码C_1;

[0128] ①若$A=A_1$,指纹信息B与户主允许进入房屋的访客指纹信息库对比时,在信息库中找到相应指纹信息B_1,$B=B_1$;则身份验证成功,验证单元提示“YES”,指纹锁开启。

[0129] ②若$A\neq A_1$,指纹信息B与户主允许进入房屋的访客指纹信息库对比时,在信息库中未找到相应指纹信息B_1;则身份验证失败,验证单元提示“NO”,指纹锁处于关闭状态。

[0130] ③若A≠A_1,指纹信息B与户主允许进入房屋的访客指纹信息库对比时,在信息库中找到相应指纹信息B_1,B＝B_1;则身份验证失败,验证单元提示“NO”,指纹锁处于关闭状态。

[0131] ④若A＝A_1,指纹信息B与户主允许进入房屋的访客指纹信息库对比时,在信息库中未找到相应指纹信息B_1;则身份验证失败,验证单元提示“NO”,指纹锁处于关闭状态。

[0132] 实施例2:限定条件:在实施例1中的②、③、④的情况下继续操作;

[0133] 1、用户验证失败后,重新进行身份验证,第2次验证时验证成功,指纹锁开启;

[0134] 2、用户验证失败后,重新进行身份验证,用户在5min内验证次数大于5次,均验证失败,则户主得到警报。

[0135] 实施例3:限定条件:在实施例2的情况2基础上继续操作;

[0136] 1、用户验证失败后,未继续进行身份验证,在指纹锁前停留时间为15min,户主终端无明显反应;

[0137] 2、用户验证失败后,未继续进行身份验证,在指纹锁前停留时间为25min,户主终端发出警报,户主得到警报。

[0138] 3、用户验证失败后,未继续进行身份验证,暴力拆卸指纹锁,户主终端发出警报,户主得到警报。

[0139] 对于本领域技术人员而言,显然本发明不限于上述示范性实施例的细节,而且在不背离本发明的精神或基本特征的情况下,能够以其他的具体形式实现本发明。因此,无论从哪一点来看,均应将实施例看作是示范性的,而且是非限制性的,本发明的范围由所附权利要求而不是上述说明限定,因此旨在将落在权利要求的等同要件的含义和范围内的所有变化囊括在本发明内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。

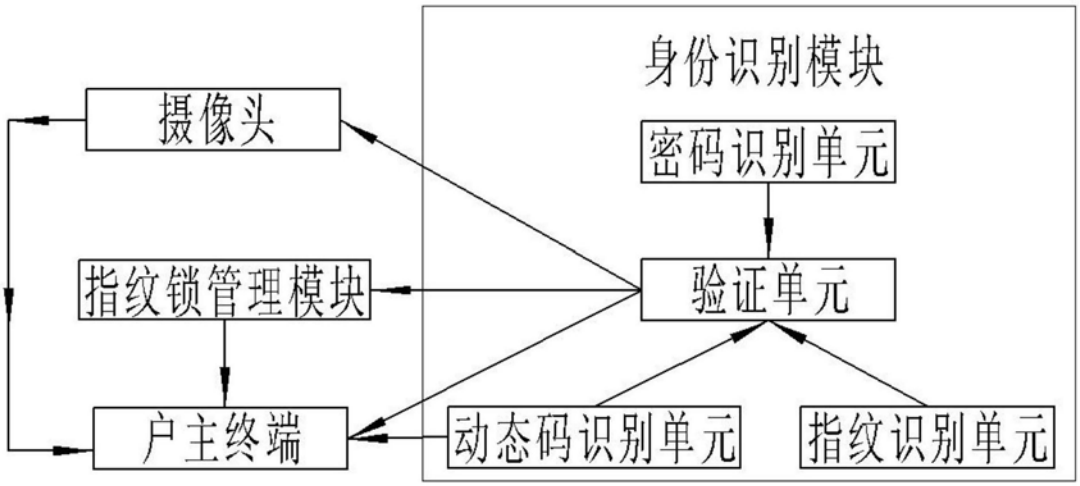

身份识别模块
摄像头
密码识别单元
指纹锁管理模块
验证单元
户主终端
动态码识别单元
指纹识别单元

图1

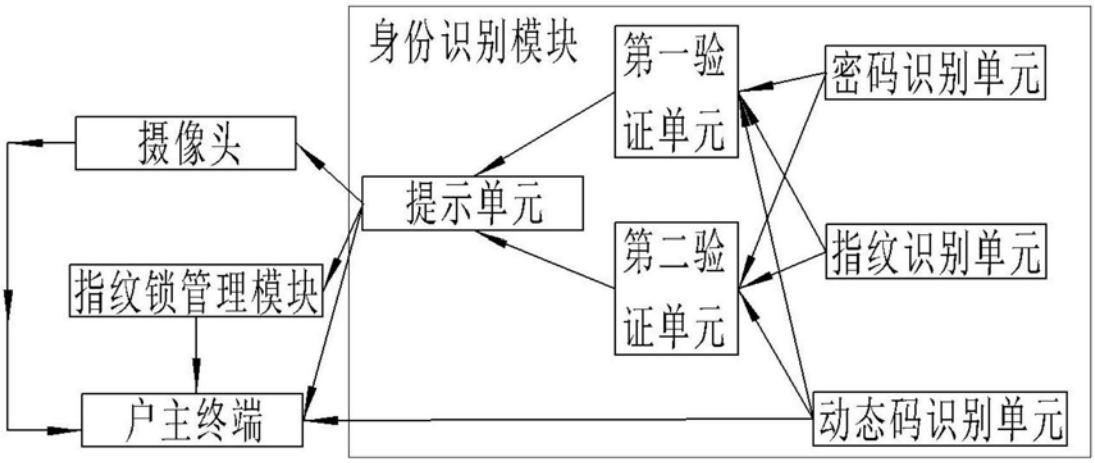

身份识别模块
第一验证单元
密码识别单元
摄像头
提示单元
第二验证单元
指纹识别单元
指纹锁管理模块
户主终端
动态码识别单元

图2

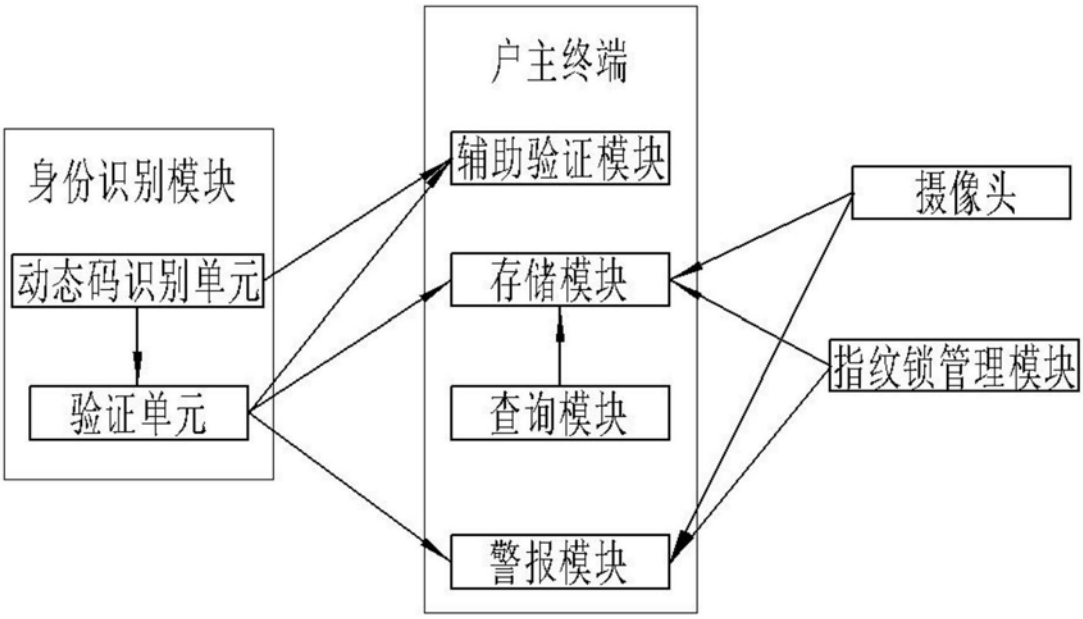

户主终端
身份识别模块
辅助验证模块
摄像头
动态码识别单元
存储模块
指纹锁管理模块
验证单元
查询模块
警报模块

图3

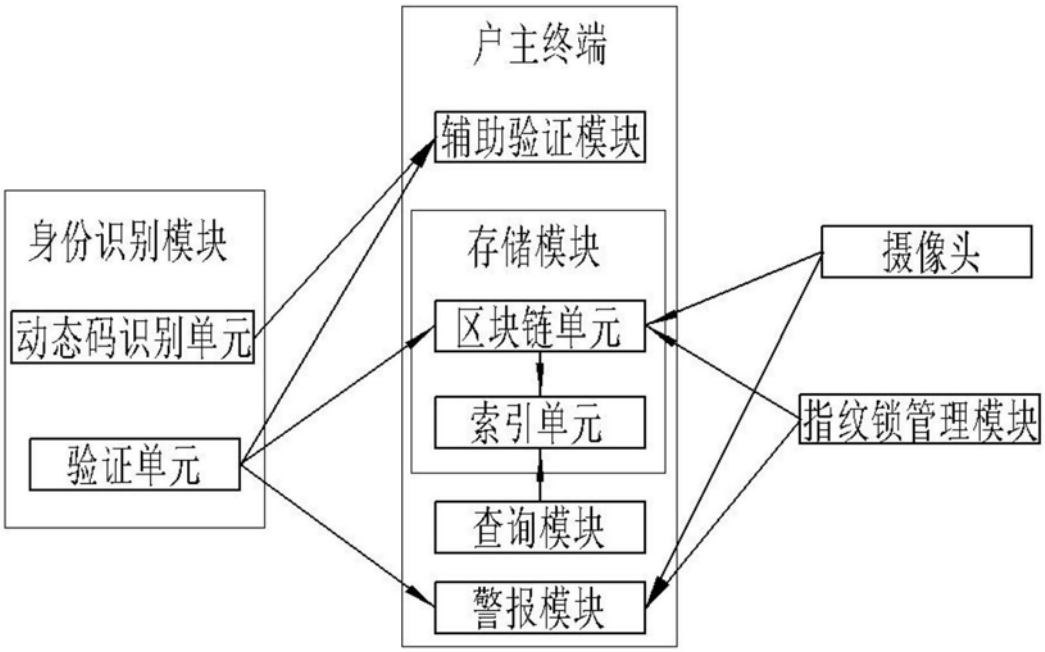

户主终端
辅助验证模块
身份识别模块
存储模块
摄像头
动态码识别单元
区块链单元
索引单元
指纹锁管理模块
验证单元
查询模块
警报模块

图4

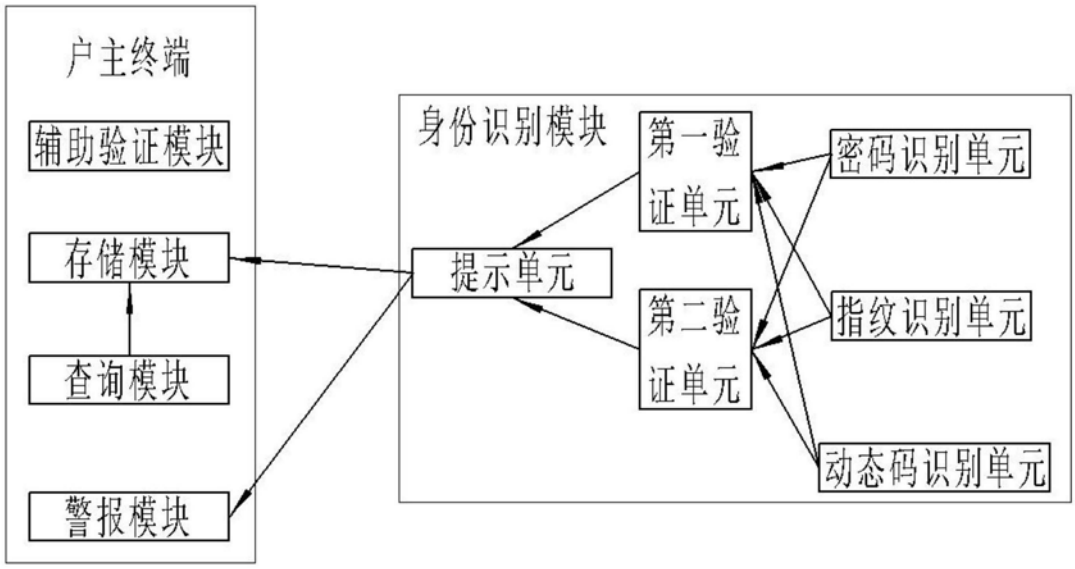

户主终端
辅助验证模块
存储模块
查询模块
警报模块
身份识别模块
第一验证单元
第二验证单元
提示单元
密码识别单元
指纹识别单元
动态码识别单元

图5