(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 105913513 A
(43)申请公布日 2016.08.31

(21)申请号 201610206865.2

(22)申请日 2016.04.05

(71)申请人 深圳市汇海威视科技有限公司
地址 518000 广东省深圳市南山区西丽官龙第一工业区A栋

(72)发明人 韩飞虎 韩亚林 朱福兴

(74)专利代理机构 深圳市博锐专利事务所 44275
代理人 张明

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

权利要求书2页 说明书8页 附图6页

(54)发明名称

门锁系统的控制方法及其系统

(57)摘要

本发明公开了一种门锁系统的控制方法及其系统，方法包括：客户端将通信主机的ID号和智能锁的ID号进行关联；客户端发送申请入网指令至通信主机；智能锁发送请求入网指令至通信主机；通信主机接收指令后，通知客户端和服务器所述智能锁入网成功；客户端获取智能锁的控制权限；智能锁向通信主机发送开门请求指令；通信主机通过云端服务器向客户端发送所述开门请求指令；客户端进行开锁密码验证；开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；通信主机发送开锁指令至智能锁；智能锁对开锁密码进行验证；验证正确后，智能锁进行开锁操作。通过为智能锁申请入网，可提高智能锁的安全，还可实现安全远程开锁。

CN 105913513 A

1.一种门锁系统的控制方法，其特征在于，包括：

客户端获取通信主机的ID号和智能锁的ID号；

将所述通信主机的ID号和智能锁的ID号进行关联；

客户端通过无线网络发送申请入网指令至通信主机；

智能锁通过通信接口发送请求入网指令至通信主机；

通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功；

客户端获取智能锁的控制权限；

智能锁向通信主机发送开门请求指令；

通信主机通过云端服务器向客户端发送所述开门请求指令；

客户端接收所述开门请求指令后，进行开锁密码验证；

所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；

通信主机发送所述开锁指令至智能锁；

智能锁接收所述开锁指令后，对开锁密码进行验证；

所述开锁密码验证正确后，智能锁进行开锁操作。

2.根据权利要求1所述的门锁系统的控制方法，其特征在于，所述“客户端获取智能锁的控制权限”之后，进一步包括：

通信主机接收布防指令；

当通信主机检测到有人进入预设的警戒区或检测到预设次数的开锁失败时，通信主机通过云端服务器推送消息至客户端；

同时，通信主机发出警报，并将对所述检测过程拍摄获取的图像信息上传至云端服务器。

3.根据权利要求1所述的门锁系统的控制方法，其特征在于，所述“客户端获取智能锁的控制权限”之后，进一步包括：

智能锁录入包括指纹、IC卡和开锁密码的开锁信息；

客户端对对应各个成员的指纹和IC卡进行编号。

4.根据权利要求3所述的门锁系统的控制方法，其特征在于，所述“客户端对对应各个成员的指纹和IC卡进行编号”之后，进一步包括：

智能锁接收一指纹、一IC卡或开锁密码的开锁信息，并对所述开锁信息进行验证；

验证正确后，发送已开锁指令、开锁类型和对应所述开锁信息的编号至通信主机；

通信主机依据所述已开锁指令获取开锁时间；

通信主机上传包括开锁类型、所述编号和开锁时间的开锁记录至云端服务器；

服务器保存所述开锁记录，同时发送所述开锁记录至客户端。

5.一种门锁系统的控制系统，其特征在于，包括：

第一获取模块，用于客户端获取通信主机的ID号和智能锁的ID号；

关联模块，用于将所述通信主机的ID号和智能锁的ID号进行关联；

第一发送模块，用于客户端通过无线网络发送申请入网指令至通信主机；

第二发送模块，用于智能锁通过通信接口发送请求入网指令至通信主机；

通知模块，用于通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服

务器所述智能锁入网成功；

第二获取模块，用于客户端获取智能锁的控制权限；

第三发送模块，用于智能锁向通信主机发送开门请求指令；

第四发送模块，用于通信主机通过云端服务器向客户端发送所述开门请求指令；

第一验证模块，用于客户端接收所述开门请求指令后，进行开锁密码验证；

第五发送模块，用于所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；

第六发送模块，用于通信主机发送所述开锁指令至智能锁；

第二验证模块，用于智能锁接收所述开锁指令后，对开锁密码进行验证；

开锁模块，用于所述开锁密码验证正确后，智能锁进行开锁操作。

6.根据权利要求5所述的门锁系统的控制系统，其特征在于，还包括：

第一接收模块，用于通信主机接收布防指令；

第一推送模块，用于当通信主机检测到有人进入预设的警戒区或检测到预设次数的开锁失败时，通信主机通过云端服务器推送消息至客户端；

警报模块，用于同时，通信主机发出警报，并将对所述检测过程拍摄获取的图像信息上传至云端服务器。

7.根据权利要求5所述的门锁系统的控制系统，其特征在于，还包括：

录入模块，用于智能锁录入包括指纹、IC卡和开锁密码的开锁信息；

编号模块，用于客户端对对应各个成员的指纹和IC卡进行编号。

8.根据权利要求7所述的门锁系统的控制系统，其特征在于，还包括：

第三验证模块，用于智能锁接收一指纹、一IC卡或开锁密码的开锁信息，并对所述开锁信息进行验证；

第七发送模块，用于验证正确后，发送已开锁指令、开锁类型和对应所述开锁信息的编号至通信主机；

第三获取模块，用于通信主机依据所述已开锁指令获取开锁时间；

上传模块，用于通信主机上传包括开锁类型、所述编号和开锁时间的开锁记录至云端服务器；

保存模块，用于服务器保存所述开锁记录，同时发送所述开锁记录至客户端。

门锁系统的控制方法及其系统

技术领域

[0001] 本发明涉及安全领域，尤其涉及一种门锁系统的控制方法及其系统。

背景技术

[0002] 现有智能锁的技术主要有：钥匙开锁、密码开锁，IC卡开锁，指纹开锁，或是钥匙、密码、IC卡、指纹混合开锁功能。

[0003] 但上述的各种开锁方式在单独实现时还存在以下缺点：

[0004] 1、还存在被破解的可能，安全性不高，防盗效果不好；

[0005] 2、无法预防被非法开锁；

[0006] 3、被非法开锁后无法取证；

[0007] 4、无法查看历史开锁记录；

[0008] 5、无法解决安全远程开锁，让自己的亲朋好友可以进门；

[0009] 6、锁被开后无法实时知道。

[0010] 在公开号为CN103903321A的中国专利公开文件中，提出了一种智能锁，包括主控芯片，分别与智能锁体、数据存储芯片、电源、图像/视频模块、通讯模块、对讲模块、功能选择装置电连接；智能锁包含图像/视频录入模块、图像/视频传输模块和对讲模块，一方面可以将来访者来访时的图像或者视频通过通讯模块传递给持有手机、IPAD等移动终端设备的用户，让用户能够清楚、直观地知道谁人造访，另一方面，来访者可以通过对讲模块和持有手机、IPAD等移动终端设备的用户进行更直接的通话，让用户确定造访者的身份再决定是否开锁，提高了智能锁的安全性，操作简单、方便快捷。但该方法仍无法有效地预防被非法开锁，且在每次开锁时没有进行通知和记录，无法查看历史开锁记录，锁被开后也无法实时知道。

发明内容

[0011] 本发明所要解决的技术问题是：提供一种门锁系统的控制方法及其系统，可有效预防被非法开锁，提高防盗效果，安全性高。

[0012] 为了解决上述技术问题，本发明采用的技术方案为：一种门锁系统的控制方法，包括：

[0013] 客户端获取通信主机的ID号和智能锁的ID号；

[0014] 将所述通信主机的ID号和智能锁的ID号进行关联；

[0015] 客户端通过无线网络发送申请入网指令至通信主机；

[0016] 智能锁通过通信接口发送请求入网指令至通信主机；

[0017] 通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功；

[0018] 客户端获取智能锁的控制权限；

[0019] 智能锁向通信主机发送开门请求指令；

[0020] 通信主机通过云端服务器向客户端发送所述开门请求指令；

[0021] 客户端接收所述开门请求指令后，进行开锁密码验证；

[0022] 所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；

[0023] 通信主机发送所述开锁指令至智能锁；

[0024] 智能锁接收所述开锁指令后，对开锁密码进行验证；

[0025] 所述开锁密码验证正确后，智能锁进行开锁操作。

[0026] 本发明还涉及一种门锁系统的控制系统，包括：

[0027] 第一获取模块，用于客户端获取通信主机的ID号和智能锁的ID号；

[0028] 关联模块，用于将所述通信主机的ID号和智能锁的ID号进行关联；

[0029] 第一发送模块，用于客户端通过无线网络发送申请入网指令至通信主机；

[0030] 第二发送模块，用于智能锁通过通信接口发送请求入网指令至通信主机；

[0031] 通知模块，用于通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功；

[0032] 第二获取模块，用于客户端获取智能锁的控制权限；

[0033] 第三发送模块，用于智能锁向通信主机发送开门请求指令；

[0034] 第四发送模块，用于通信主机通过云端服务器向客户端发送所述开门请求指令；

[0035] 第一验证模块，用于客户端接收所述开门请求指令后，进行开锁密码验证；

[0036] 第五发送模块，用于所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；

[0037] 第六发送模块，用于通信主机发送所述开锁指令至智能锁；

[0038] 第二验证模块，用于智能锁接收所述开锁指令后，对开锁密码进行验证；

[0039] 开锁模块，用于所述开锁密码验证正确后，智能锁进行开锁操作。

[0040] 本发明的有益效果在于：通过为智能锁申请入网，将客户端、通信主机和智能锁进行关联，避免智能锁被别人非法控制，提高智能锁的安全；同时，客户端获取智能锁的控制权限，当有亲友拜访时，可直接通过客户端进行安全远程开锁，方便快捷，提高用户体验；通过对开锁密码进行两次验证，防止开锁密码在发送过程中被获取、篡改，进一步提高了安全性。

附图说明

[0041] 图1为本发明一种门锁系统的控制方法的流程图；

[0042] 图2为本发明实施例一门锁系统的结构示意图；

[0043] 图3为本发明实施例一的方法流程图一；

[0044] 图4为本发明实施例一的方法流程图二；

[0045] 图5为本发明实施例一的方法流程图三；

[0046] 图6为本发明实施例一的方法流程图四；

[0047] 图7为本发明实施例一的方法流程图五；

[0048] 图8为本发明一种门锁系统的控制系统的结构示意图；

[0049] 图9为本发明实施例二的系统结构图。

[0050] 标号说明：

[0051] 1、智能锁；2、通信主机；3、客户端；4、服务器；

[0052] 11、第一主控模块；12、警报提示模块；13、锁体机构；14、指纹模块；15、按键模块；16、IC卡模块；

[0053] 21、第二主控模块；22、红外探测模块；23、摄像模块；24、存储模块；25、网络模块；26、语音输入模块；27、语音输出模块；28、光感应探测模块；29、夜视补光模块；

[0054] 101、第一获取模块；102、关联模块；103、第一发送模块；104、第二发送模块；105、通知模块；106、第二获取模块；107、第三发送模块；108、第四发送模块；109、第一验证模块；110、第五发送模块；111、第六发送模块；112、第二验证模块；113、开锁模块；114、第一接收模块；115、第一推送模块；116、警报模块；117、录入模块；118、编号模块；119、第三验证模块；120、第七发送模块；121、第三获取模块；122、上传模块；123、保存模块。

具体实施方式

[0055] 为详细说明本发明的技术内容、所实现目的及效果，以下结合实施方式并配合附图详予说明。

[0056] 本发明最关键的构思在于：将智能锁、通信主机和客户端进行关联，提高智能锁的安全，并实现安全远程控制开锁。

[0057] 请参阅图1，一种门锁系统的控制方法，包括：

[0058] 客户端获取通信主机的ID号和智能锁的ID号；

[0059] 将所述通信主机的ID号和智能锁的ID号进行关联；

[0060] 客户端通过无线网络发送申请入网指令至通信主机；

[0061] 智能锁通过通信接口发送请求入网指令至通信主机；

[0062] 通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功；

[0063] 客户端获取智能锁的控制权限；

[0064] 智能锁向通信主机发送开门请求指令；

[0065] 通信主机通过云端服务器向客户端发送所述开门请求指令；

[0066] 客户端接收所述开门请求指令后，进行开锁密码验证；

[0067] 所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；

[0068] 通信主机发送所述开锁指令至智能锁；

[0069] 智能锁接收所述开锁指令后，对开锁密码进行验证；

[0070] 所述开锁密码验证正确后，智能锁进行开锁操作。

[0071] 从上述描述可知，本发明的有益效果在于：可提高智能锁的安全，还可进行安全远程开锁。

[0072] 进一步地，所述“客户端获取智能锁的控制权限”之后，进一步包括：

[0073] 通信主机接收布防指令；

[0074] 当通信主机检测到有人进入预设的警戒区或检测到预设次数的开锁失败时，通信主机通过云端服务器推送消息至客户端；

[0075] 同时，通信主机发出警报，并将对所述检测过程拍摄获取的图像信息上传至云端服务器。

[0076] 由上述描述可知，通信主机接收布防指令进入布防状态，对警戒区域进行检测，若感应到警戒区域内有人体移动，则发出警报阻吓非法者，同时拍摄图像并通知用户，当通信主机检测有多次开锁失败，即使不处于布防状态也执行上述操作，可有效预防非法开锁，进一步提高安全性。

[0077] 进一步地，所述“客户端获取智能锁的控制权限”之后，进一步包括：

[0078] 智能锁录入包括指纹、IC卡和开锁密码的开锁信息；

[0079] 客户端对对应各个成员的指纹和IC卡进行编号。

[0080] 由上述描述可知，对指纹和IC卡进行编号，方便用户对开锁信息的管理。

[0081] 进一步地，所述“客户端对对应各个成员的指纹和IC卡进行编号”之后，进一步包括：

[0082] 智能锁接收一指纹、一IC卡或开锁密码的开锁信息，并对所述开锁信息进行验证；

[0083] 验证正确后，发送已开锁指令、开锁类型和对应所述开锁信息的编号至通信主机；

[0084] 通信主机依据所述已开锁指令获取开锁时间；

[0085] 通信主机上传包括开锁类型、所述编号和开锁时间的开锁记录至云端服务器；

[0086] 服务器保存所述开锁记录，同时发送所述开锁记录至客户端。

[0087] 由上述描述可知，可有效保存开锁记录，方便之后查看历史开锁记录，同时，用户可以实时知道门锁状态并查看实时图像信息，进一步提高了安全性。

[0088] 请参照图8，本发明还提出了一种门锁系统的控制系统，包括：

[0089] 第一获取模块，用于客户端获取通信主机的ID号和智能锁的ID号；

[0090] 关联模块，用于将所述通信主机的ID号和智能锁的ID号进行关联；

[0091] 第一发送模块，用于客户端通过无线网络发送申请入网指令至通信主机；

[0092] 第二发送模块，用于智能锁通过通信接口发送请求入网指令至通信主机；

[0093] 通知模块，用于通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功；

[0094] 第二获取模块，用于客户端获取智能锁的控制权限；

[0095] 第三发送模块，用于智能锁向通信主机发送开门请求指令；

[0096] 第四发送模块，用于通信主机通过云端服务器向客户端发送所述开门请求指令；

[0097] 第一验证模块，用于客户端接收所述开门请求指令后，进行开锁密码验证；

[0098] 第五发送模块，用于所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；

[0099] 第六发送模块，用于通信主机发送所述开锁指令至智能锁；

[0100] 第二验证模块，用于智能锁接收所述开锁指令后，对开锁密码进行验证；

[0101] 开锁模块，用于所述开锁密码验证正确后，智能锁进行开锁操作。

[0102] 进一步地，还包括：

[0103] 第一接收模块，用于通信主机接收布防指令；

[0104] 第一推送模块，用于当通信主机检测到有人进入预设的警戒区或检测到预设次数的开锁失败时，通信主机通过云端服务器推送消息至客户端；

[0105] 警报模块，用于同时，通信主机发出警报，并将对所述检测过程拍摄获取的图像信息上传至云端服务器。

[0106] 进一步地，还包括：

[0107] 录入模块，用于智能锁录入包括指纹、IC卡和开锁密码的开锁信息；

[0108] 编号模块，用于客户端对对应各个成员的指纹和IC卡进行编号。

[0109] 进一步地，还包括：

[0110] 第三验证模块，用于智能锁接收一指纹、一IC卡或开锁密码的开锁信息，并对所述开锁信息进行验证；

[0111] 第七发送模块，用于验证正确后，发送已开锁指令、开锁类型和对应所述开锁信息的编号至通信主机；

[0112] 第三获取模块，用于通信主机依据所述已开锁指令获取开锁时间；

[0113] 上传模块，用于通信主机上传包括开锁类型、所述编号和开锁时间的开锁记录至云端服务器；

[0114] 保存模块，用于服务器保存所述开锁记录，同时发送所述开锁记录至客户端。

[0115] 实施例一

[0116] 本发明的实施例一为：一种门锁系统的控制方法，如图2所示，所述门锁系统包括智能锁1、通信主机2、客户端3和服务器4，所述智能锁1通过通信接口与通信主机2连接，所述通信主机2、客户端3和服务器4通过无线网络相互连接；所述智能锁1包括第一主控模块11、警报提示模块12、锁体机构13、指纹模块14、按键模块15和IC卡模块16，所述第一主控模块11分别与所述警报提示模块12、锁体机构13、指纹模块14、按键模块15和IC卡模块16连接；所述通信主机2包括第二主控模块21、红外探测模块22、摄像模块23、存储模块24、网络模块25、语音输入模块26、语音输出模块27、光感应探测模块28和夜视补光模块29，所述第二主控模块21分别与所述红外探测模块22、摄像模块23、存储模块24、网络模块25、语音输入模块26、语音输出模块27、光感应探测模块28和夜视补光模块29连接。

[0117] 优选地，所述红外探测模块22为被动红外探测模块。

[0118] 所述客户端3可以为PC电脑，优选地，所述客户端3为移动终端，如手机和平板电脑等。

[0119] 优选地，所述服务器4为云端服务器。

[0120] 当需要对门锁系统进行控制时，先将客户端、通信主机和智能锁进行关联，为智能锁申请入网；如图3所示，包括如下步骤：

[0121] S101：客户端获取通信主机的ID号和智能锁的ID号；在客户端上安装相关软件，用户通过账号和密码登录所述软件，通过扫描二维码或手动输入ID，将通信主机和智能锁添加到用户账号中。

[0122] S102：将所述通信主机的ID号和智能锁的ID号进行关联；关联的目的是便于通信以ID号为识别。优选地，可为所述智能锁命名，当用户有多个智能锁时容易识别。

[0123] S103：客户端通过无线网络发送申请入网指令至通信主机；用户在客户端上操作，为所述智能锁申请入网。

[0124] S104：智能锁通过通信接口发送请求入网指令至通信主机；用户在智能锁按键上按申请入网按键，智能锁则会发送请求入网指令。

[0125] S105：通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功；入网成功后，用户就可以通过客户端操作智能锁。

[0126] S106:客户端获取智能锁的控制权限。

[0127] 智能锁入网成功后,可在智能锁上录入开锁信息;如图4所示,包括如下步骤:

[0128] S201:智能锁录入包括指纹、IC卡和开锁密码的开锁信息;录入开锁信息后,即可通过指纹、IC卡或密码进行开锁。

[0129] S202:客户端对录入的指纹和IC卡进行编号或命名;可对应各个成员进行编号命名,方便对各开锁用户的信息进行管理。

[0130] 录入完开锁信息后,用户可现场开锁;如图5所示,包括如下步骤:

[0131] S301:智能锁接收一指纹、一IC卡或开锁密码的开锁信息,并对所述开锁信息进行验证。

[0132] S302:验证正确后,发送包括已开锁指令和开锁类型至通信主机;若为指纹开锁或IC卡开锁,则还需发送对应的编号;可选地,开锁成功后可语音提示“已开锁”。

[0133] S303:通信主机依据所述已开锁指令获取开锁时间。

[0134] S304:通信主机上传包括开锁类型、所述编号和开锁时间的开锁记录至云端服务器。

[0135] S305:服务器保存所述开锁记录,同时发送所述开锁记录至客户端;用户接收到推送消息后可以从客户端软件上查看实时视频,也可查看历史开锁记录。

[0136] 用户也可以远程控制开锁;如图6所示,包括如下步骤:

[0137] S401:智能锁向通信主机发送开门请求指令;当亲友到访时,可按下智能锁上的开门请求按钮,智能锁则会发送开门请求指令。

[0138] S402:通信主机通过云端服务器向客户端发送所述开门请求指令;通信主机通过无线网络向云端服务器发送开门请求指令,云端服务器接收到所述指令后向用户客户端发送推送消息。

[0139] S403:客户端接收所述开门请求指令后,进行开锁密码验证;用户点开客户端软件的推送消息,查看实时视频,确认到访者是亲友后,点击开锁命令,并在客户端软件上输入开锁密码。

[0140] S404:所述开锁密码验证正确后,发送包括所述开锁密码的开锁指令至通信主机;客户端软件对输入的开锁密码进行验证,验证正确后则向通信主机发送开锁指令。

[0141] S405:通信主机发送所述开锁指令至智能锁。

[0142] S406:智能锁接收所述开锁指令后,对开锁密码进行验证;到访亲友可按下智能锁上的验证按钮,智能锁则会开始对开锁密码进行二次验证,防止开锁密码在传输过程中被窃取篡改,进一步提高了安全性。

[0143] S407:所述开锁密码验证正确后,智能锁进行开锁操作。

[0144] 可选地,在步骤S404之前,到访亲友可直接打电话向用户请求开锁,用户点开客户端软件的推送消息,查看实时视频,确认到访者是亲友后,直接点击开锁命令,并在客户端软件上输入开锁密码。

[0145] 用户还可以预先设置开启锁的警戒区域和开锁失败次数阈值,并控制通信主机的布防状态和撤防状态,当有人非法开锁时可阻吓非法者并进行取证;如图7所示,包括如下步骤:

[0146] S501:通信主机接收布防指令,进入布防状态;可选地,用户可在客户端软件上选

择要布防的通信主机，客户端通过无线网络向通信主机发布布防指令；也可通过手持遥控器向通信主机发送布防指令。

[0147] S502：当通信主机检测到有人进入预设的警戒区时或检测到预设次数的开锁失败，通信主机通过云端服务器推送消息至客户端；用户可以通过客户端软件查看实时视频，并进行语音对讲、喊话。

[0148] S503：通信主机发出警报，并拍摄图像；通信主机发出警号声阻吓进入警戒区域的非法人员，并进行录像或拍摄照片，方便后续进行取证。

[0149] S504：通信主机将警报记录和拍摄获取的图像信息上传至云端服务器；用户可以通过客户端软件查看或下载云端服务器上的历史警报记录和图像信息。

[0150] 优选地，检测到预设次数的开锁失败在撤防状态下也可自动进行警报和取证。

[0151] 所述步骤S502、S503和S504可同时进行。

[0152] 本实施例通过为智能锁申请入网，可避免智能锁被别人非法控制，提高智能锁的安全；对开锁信息进行编号，可方便用户管理；用户可现场开锁，也可远程开锁，方便用户使用，提高用户体验；还可检测开锁失败次数以及在布防状态感应警戒区域的人体移动，可有效防止被非法开锁，进一步提高了安全性。

[0153] 实施例二

[0154] 请参照图9，本实施例为对应上述实施例的一种门锁系统的控制系统，包括：

[0155] 第一获取模块101，用于客户端获取通信主机的ID号和智能锁的ID号；

[0156] 关联模块102，用于将所述通信主机的ID号和智能锁的ID号进行关联；

[0157] 第一发送模块103，用于客户端通过无线网络发送申请入网指令至通信主机；

[0158] 第二发送模块104，用于智能锁通过通信接口发送请求入网指令至通信主机；

[0159] 通知模块105，用于通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功；

[0160] 第二获取模块106，用于客户端获取智能锁的控制权限；

[0161] 第三发送模块107，用于智能锁向通信主机发送开门请求指令；

[0162] 第四发送模块108，用于通信主机通过云端服务器向客户端发送所述开门请求指令；

[0163] 第一验证模块109，用于客户端接收所述开门请求指令后，进行开锁密码验证；

[0164] 第五发送模块110，用于所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机；

[0165] 第六发送模块111，用于通信主机发送所述开锁指令至智能锁；

[0166] 第二验证模块112，用于智能锁接收所述开锁指令后，对开锁密码进行验证；

[0167] 开锁模块113，用于所述开锁密码验证正确后，智能锁进行开锁操作。

[0168] 还包括：

[0169] 第一接收模块114，用于通信主机接收布防指令；

[0170] 第一推送模块115，用于当通信主机检测到有人进入预设的警戒区或检测到预设次数的开锁失败时，通信主机通过云端服务器推送消息至客户端；

[0171] 警报模块116，用于同时，通信主机发出警报，并将对所述检测过程拍摄获取的图像信息上传至云端服务器。

[0172] 还包括：

[0173] 录入模块117，用于智能锁录入包括指纹、IC卡和开锁密码的开锁信息；

[0174] 编号模块118，用于客户端对对应各个成员的指纹和IC卡进行编号。

[0175] 还包括：

[0176] 第三验证模块119，用于智能锁接收一指纹、一IC卡或开锁密码的开锁信息，并对所述开锁信息进行验证；

[0177] 第七发送模块120，用于验证正确后，发送已开锁指令、开锁类型和对应所述开锁信息的编号至通信主机；

[0178] 第三获取模块121，用于通信主机依据所述已开锁指令获取开锁时间；

[0179] 上传模块122，用于通信主机上传包括开锁类型、所述编号和开锁时间的开锁记录至云端服务器；

[0180] 保存模块123，用于服务器保存所述开锁记录，同时发送所述开锁记录至客户端。

[0181] 综上所述，本发明提供的一种门锁系统的控制方法及其系统，通过为智能锁申请入网，将客户端、通信主机和智能锁进行关联，避免智能锁被别人非法控制，提高智能锁的安全；同时，客户端获取智能锁的控制权限，当有亲友拜访时，可直接通过客户端进行安全远程开锁，方便快捷，提高用户体验；通过对开锁密码进行两次验证，防止开锁密码在发送过程中被获取、篡改，进一步提高了安全性；通信主机感应到警戒区域内有人体移动或检测到预设次数的开锁失败，则发出警报阻吓非法者，同时拍摄图像并通知锁用户，可有效预防非法开锁，进一步提高安全性；对指纹和IC卡进行编号，方便用户对开锁信息的管理；可有效保存开锁记录，方便之后查看历史开锁记录，同时，用户可以实时获取门锁状态并查看实时图像信息，进一步提高了安全性。

[0182] 以上所述仅为本发明的实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等同变换，或直接或间接运用在相关的技术领域，均同理包括在本发明的专利保护范围内。

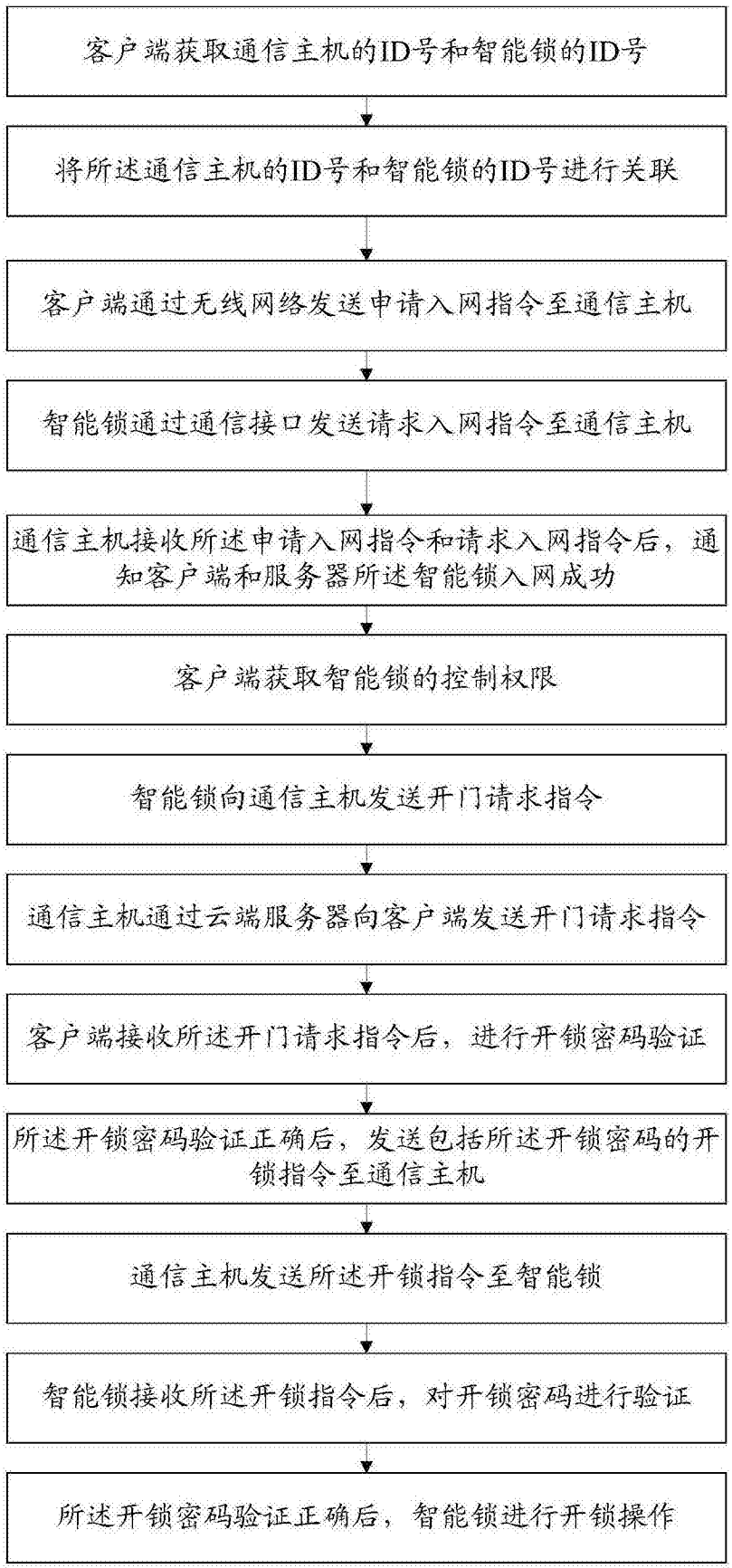
客户端获取通信主机的ID号和智能锁的ID号
将所述通信主机的ID号和智能锁的ID号进行关联
客户端通过无线网络发送申请入网指令至通信主机
智能锁通过通信接口发送请求入网指令至通信主机
通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功
客户端获取智能锁的控制权限
智能锁向通信主机发送开门请求指令
通信主机通过云端服务器向客户端发送开门请求指令
客户端接收所述开门请求指令后，进行开锁密码验证
所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机
通信主机发送所述开锁指令至智能锁
智能锁接收所述开锁指令后，对开锁密码进行验证
所述开锁密码验证正确后，智能锁进行开锁操作

图1

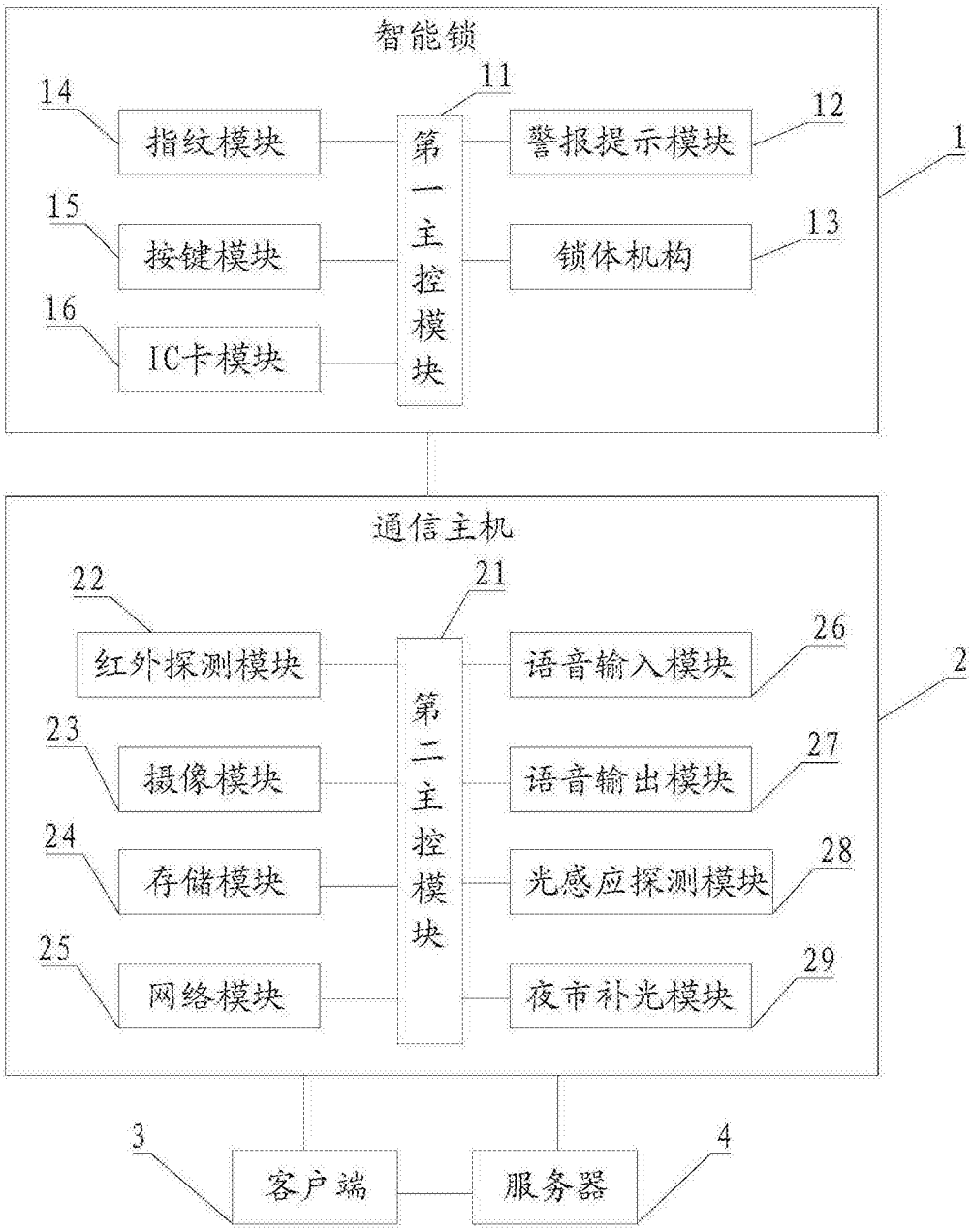
智能锁
11
14
指纹模块
第一主控模块
警报提示模块
12
1
15
按键模块
锁体机构
13
16
IC卡模块
通信主机
22
21
红外探测模块
语音输入模块
26
2
23
摄像模块
语音输出模块
27
24
存储模块
光感应探测模块
28
25
网络模块
夜市补光模块
29
第二主控模块
3
客户端
服务器
4

图2

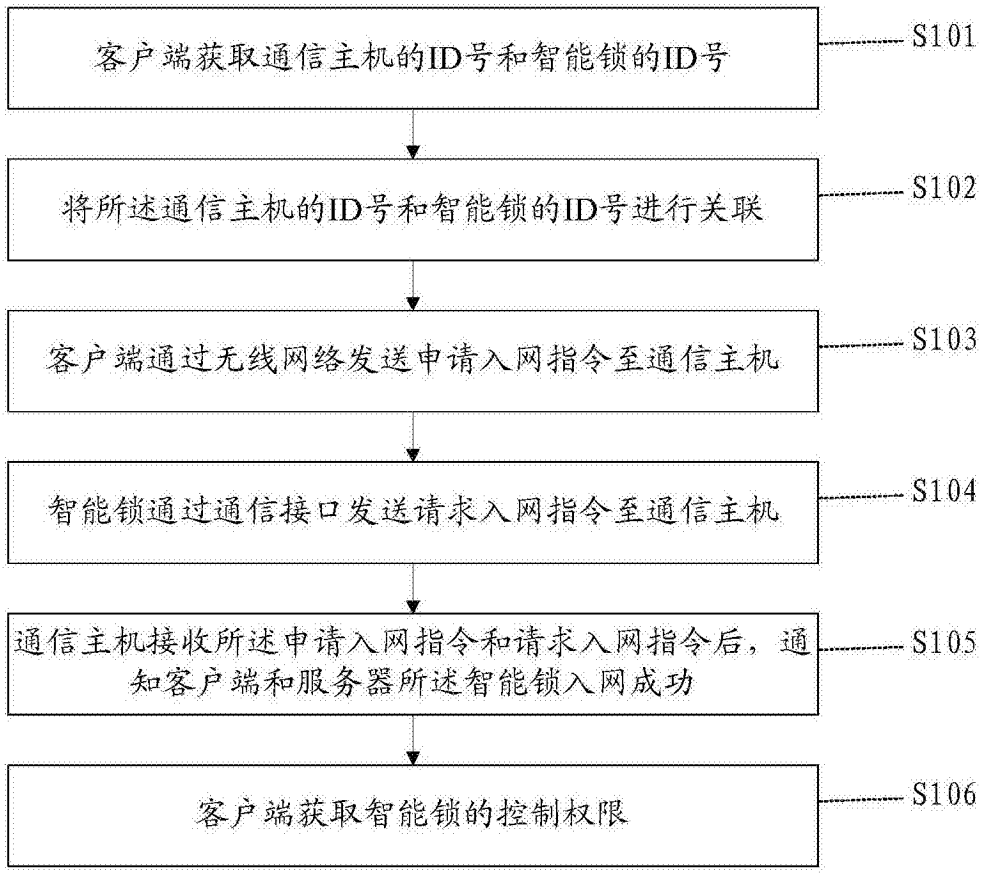
客户端获取通信主机的ID号和智能锁的ID号
S101
将所述通信主机的ID号和智能锁的ID号进行关联
S102
客户端通过无线网络发送申请入网指令至通信主机
S103
智能锁通过通信接口发送请求入网指令至通信主机
S104
通信主机接收所述申请入网指令和请求入网指令后，通知客户端和服务器所述智能锁入网成功
S105
客户端获取智能锁的控制权限
S106

图3

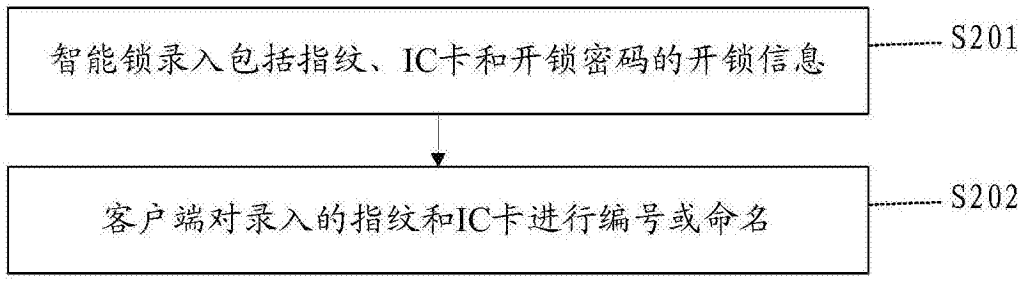
智能锁录入包括指纹、IC卡和开锁密码的开锁信息
S201
客户端对录入的指纹和IC卡进行编号或命名
S202

图4

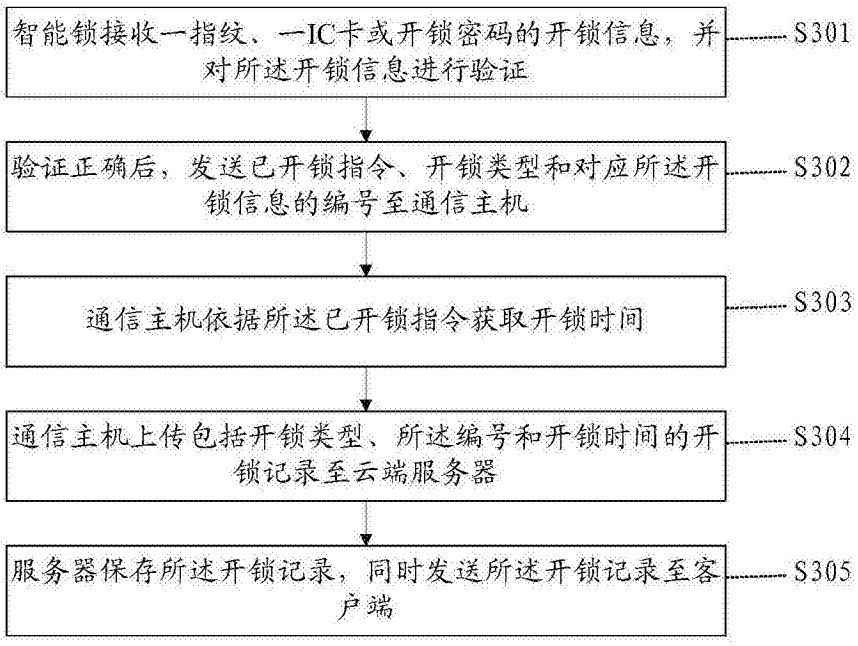
智能锁接收一指纹、一IC卡或开锁密码的开锁信息，并对所述开锁信息进行验证
S301
验证正确后，发送已开锁指令、开锁类型和对应所述开锁信息的编号至通信主机
S302
通信主机依据所述已开锁指令获取开锁时间
S303
通信主机上传包括开锁类型、所述编号和开锁时间的开锁记录至云端服务器
S304
服务器保存所述开锁记录，同时发送所述开锁记录至客户端
S305

图5

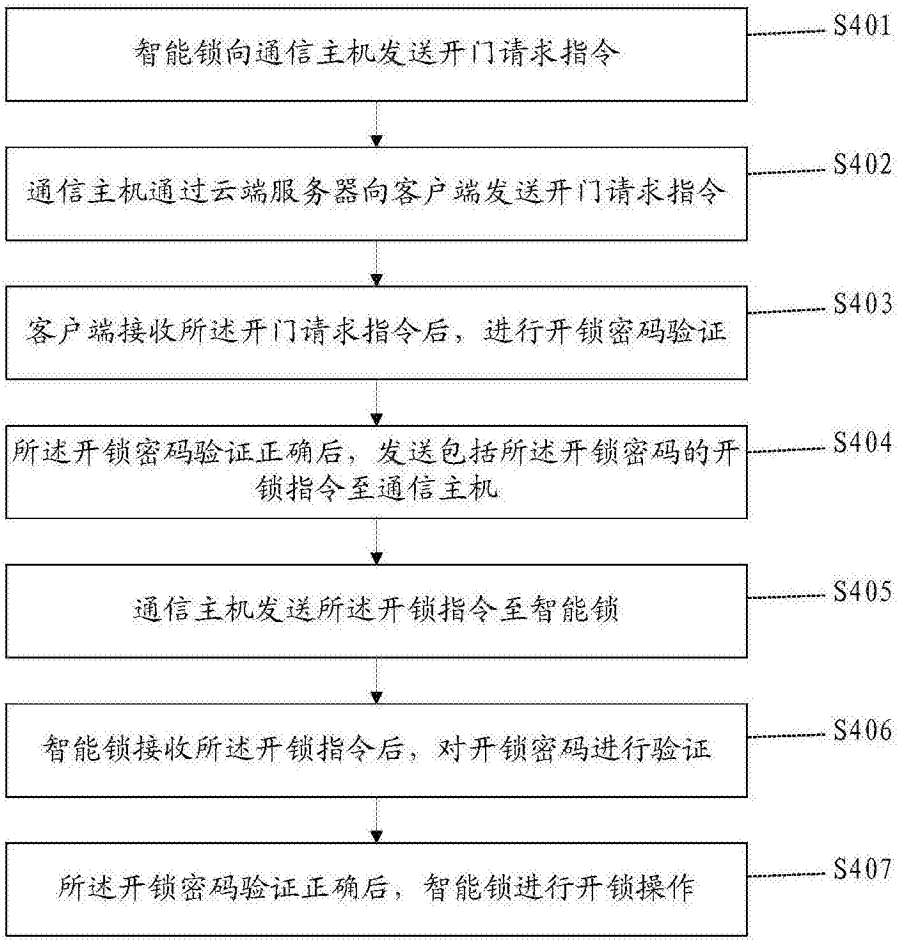
智能锁向通信主机发送开门请求指令
S401
通信主机通过云端服务器向客户端发送开门请求指令
S402
客户端接收所述开门请求指令后，进行开锁密码验证
S403
所述开锁密码验证正确后，发送包括所述开锁密码的开锁指令至通信主机
S404
通信主机发送所述开锁指令至智能锁
S405
智能锁接收所述开锁指令后，对开锁密码进行验证
S406
所述开锁密码验证正确后，智能锁进行开锁操作
S407

图6

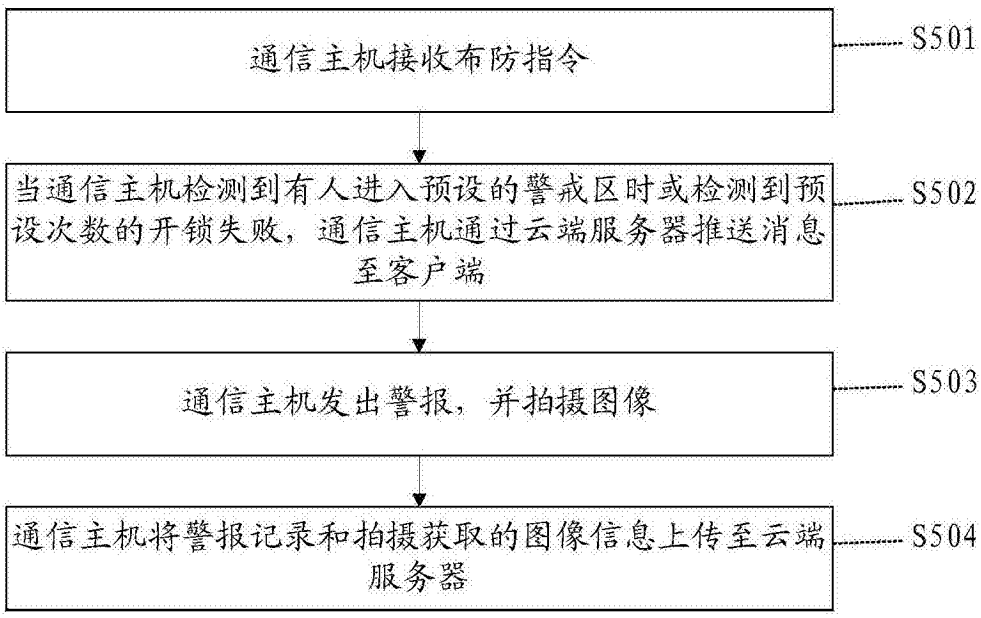
通信主机接收布防指令
S501
当通信主机检测到有人进入预设的警戒区时或检测到预设次数的开锁失败，通信主机通过云端服务器推送消息至客户端
S502
通信主机发出警报，并拍摄图像
S503
通信主机将警报记录和拍摄获取的图像信息上传至云端服务器
S504

图7

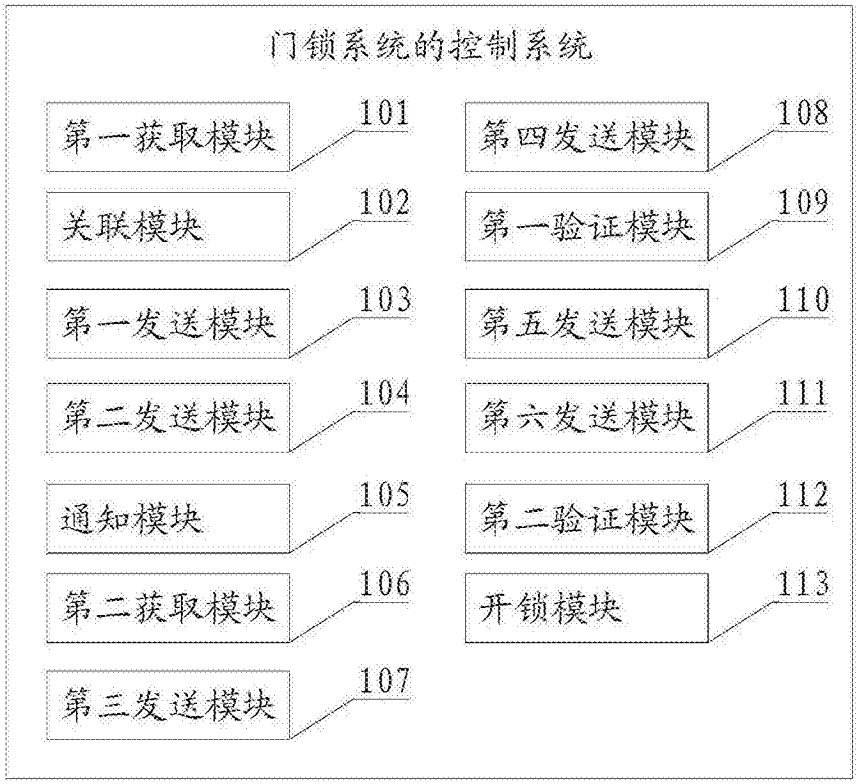
门锁系统的控制系统
第一获取模块
101
关联模块
102
第一发送模块
103
第二发送模块
104
通知模块
105
第二获取模块
106
第三发送模块
107
第四发送模块
108
第一验证模块
109
第五发送模块
110
第六发送模块
111
第二验证模块
112
开锁模块
113

图8

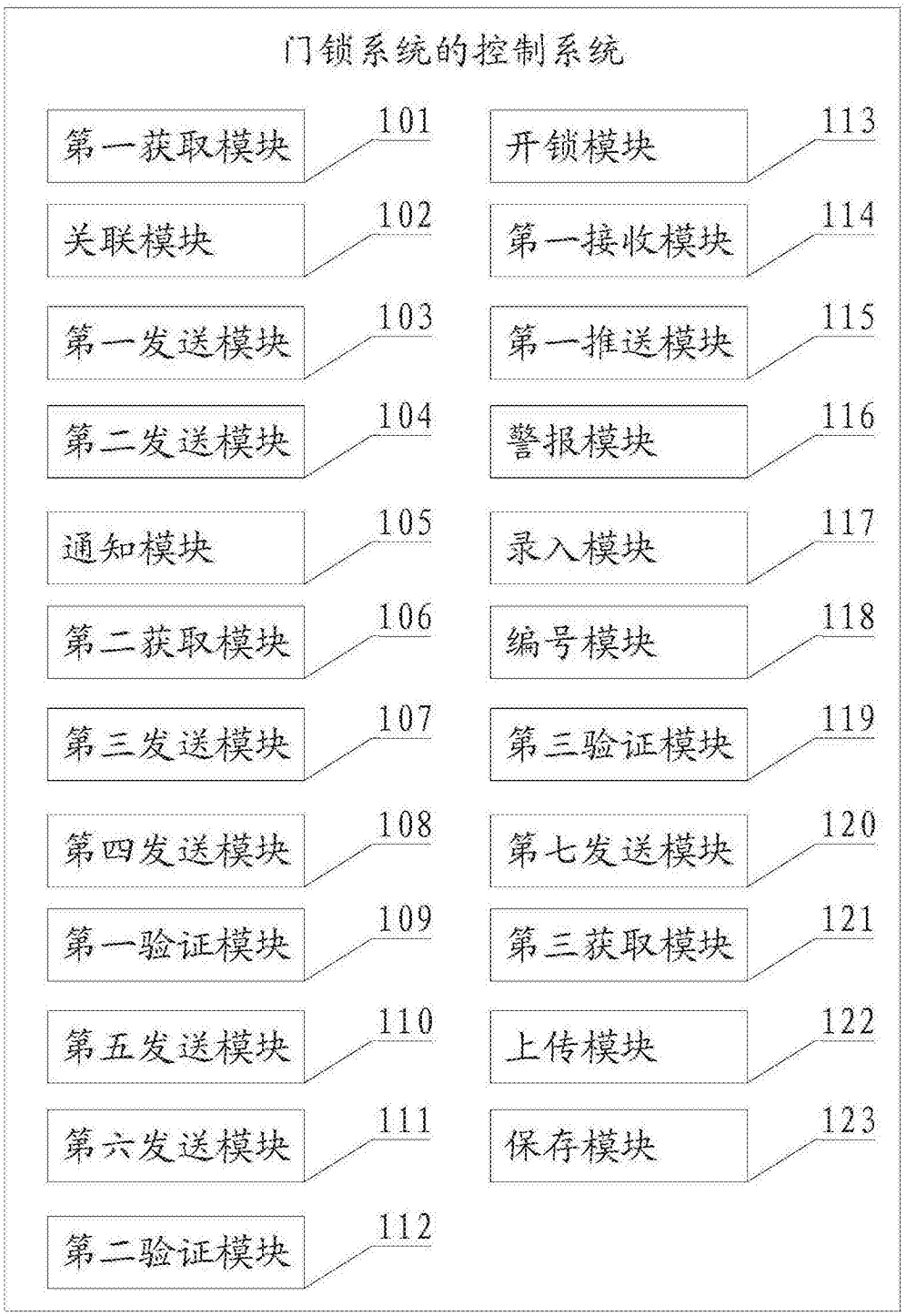
门锁系统的控制系统
第一获取模块
101
关联模块
102
第一发送模块
103
第二发送模块
104
通知模块
105
第二获取模块
106
第三发送模块
107
第四发送模块
108
第一验证模块
109
第五发送模块
110
第六发送模块
111
第二验证模块
112
开锁模块
113
第一接收模块
114
第一推送模块
115
警报模块
116
录入模块
117
编号模块
118
第三验证模块
119
第七发送模块
120
第三获取模块
121
上传模块
122
保存模块
123

图9