



(12)发明专利申请

(10)申请公布号 CN 110211267 A

(43)申请公布日 2019.09.06

(21)申请号 201910477912.0

(22)申请日 2019.06.03

(71)申请人 浙江大华技术股份有限公司
地址 310051 浙江省杭州市滨江区滨安路
1187号

(72)发明人 陈利刚

(74)专利代理机构 深圳市威世博知识产权代理
事务所(普通合伙) 44280
代理人 李庆波

(51) Int. Cl.
G07C 9/00(2006.01)
G08B 13/08(2006.01)
G08B 13/196(2006.01)

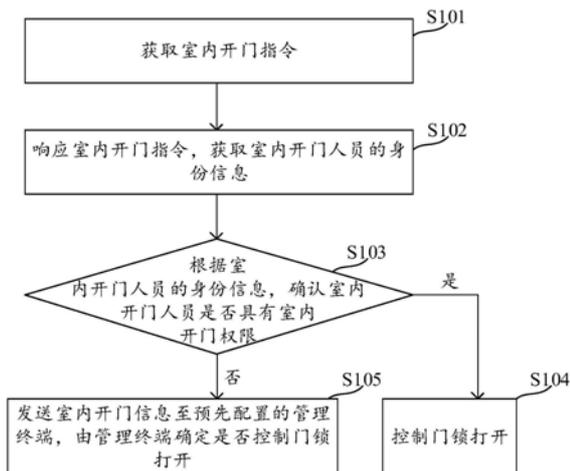
权利要求书2页 说明书7页 附图4页

(54)发明名称

室内开门控制方法、权限的配置方法、装置和存储介质

(57)摘要

本申请提供室内开门控制方法、权限的配置方法、装置和存储介质。室内开门控制方法包括：获取室内开门指令；响应室内开门指令，获取室内开门人员的身份信息；根据室内开门人员的身份信息，确认室内开门人员是否具有室内开门权限；若具有室内开门权限，则控制门锁打开；若不具有室内开门权限，则发送室内开门信息至预先配置的管理终端，由管理终端确定是否控制门锁打开。本申请的方法可以排除一些安全隐患。



1. 一种室内开门控制方法,其特征在于,所述方法包括:
获取室内开门指令;
响应所述室内开门指令,获取室内开门人员的身份信息;
根据所述室内开门人员的身份信息,确认所述室内开门人员是否具有室内开门权限;
若具有室内开门权限,则控制门锁打开;
若不具有室内开门权限,则发送室内开门信息至预先配置的管理终端,由所述管理终端确定是否控制所述门锁打开。

2. 根据权利要求1所述的室内开门控制方法,其特征在于,所述响应所述室内开门指令,获取室内开门人员的身份信息,包括:

判断所述室内开门指令是否为紧急开门指令;

若是紧急开门指令,则控制所述门锁打开,并发送室内开门信息至所述管理终端;

若不是紧急开门指令,则执行所述获取室内开门人员的身份信息的动作。

3. 根据权利要求1所述的室内开门控制方法,其特征在于,所述根据所述室内开门人员的身份信息,确认所述室内开门人员是否具有室内开门权限,包括:

根据所述身份信息,在预先配置的具有所述室内开门权限的人员名单中查找是否存在所述室内开门人员;

若在所述室内开门权限的人员名单中查找到所述室内开门人员,则确定所述室内开门人员具有所述室内开门权限;

若在所述室内开门权限的人员名单中未查找到所述室内开门人员,则确定所述室内开门人员不具有所述室内开门权限。

4. 根据权利要求3所述的室内开门控制方法,其特征在于,所述人员名单中的人员在预设环境条件下具有所述室内开门权限;根据所述室内开门人员的身份信息,确认所述室内开门人员是否具有室内开门权限,包括:

根据所述身份信息,在预先配置的具有所述室内开门权限的人员名单中查找是否存在所述室内开门人员;

若在所述室内开门权限的人员名单中查找到所述室内开门人员,则获取当前环境信息,判断所述当前环境信息是否满足所述室内开门人员的预设环境条件;

若满足,则确定所述室内开门人员具有所述室内开门权限;

若不满足,则确定所述室内开门人员不具有所述室内开门权限。

5. 根据权利要求1所述的室内开门控制方法,其特征在于,所述获取室内开门人员的身份信息包括:

获取所述室内开门人员的人脸信息或指纹信息。

6. 一种室内开门权限的配置方法,其特征在于,所述方法包括:

采集待配置人员的身份信息;

获取针对每一所述待配置人员的室内开门权限的配置指令;

根据所述配置指令,生成室内开门权限信息;

关联所述身份信息和所述室内开门权限信息;

其中,所述室内开门权限信息包括:是否具有所述室内开门权限;或者预设环境条件下是否具有所述室内开门权限。

7. 一种室内开门控制装置,其特征在于,所述室内开门控制装置包括处理器和存储器;所述存储器中存储有计算机程序,所述处理器用于执行所述计算机程序以实现如权利要求1-6中任一项所述方法的步骤。

8. 根据权利要求7所述的室内开门控制装置,其特征在于,所述室内开门控制装置包括传感器,所述传感器用于采集所述室内开门人员的身份信息。

9. 根据权利要求7所述的室内开门控制装置,其特征在于,所述室内开门控制装置包括紧急开门按钮,所述紧急开门按钮用于获取紧急开门指令。

10. 一种计算机存储介质,其特征在于,所述计算机存储介质存储有计算机程序,所述计算机程序被执行时实现如权利要求1-6中任一项所述方法的步骤。

室内开门控制方法、权限的配置方法、装置和存储介质

技术领域

[0001] 本申请涉及安防技术领域,特别是涉及室内开门控制方法、权限的配置方法、装置和存储介质。

背景技术

[0002] 近年来,随着行业的演进和变化,新型的安全问题开始暴露出来,比如经常可以看到新闻报道说,违法犯罪人员伪装成快递人员,专门挑小孩一个人在家或者老人一个人在家的时候,骗取开门,然后实施抢劫等违法行为。对于这些情况,除了安全观念宣讲外,还可以通过一些技术手段排除一些这样的安全隐患。

发明内容

[0003] 本申请提供室内开门控制方法、权限的配置方法、装置和存储介质,以解决现有技术中无法排除安全隐患的问题。

[0004] 为解决技术问题,本申请提供一种室内开门控制方法,该方法包括:获取室内开门指令;响应室内开门指令,获取室内开门人员的身份信息;根据室内开门人员的身份信息,确认室内开门人员是否具有室内开门权限;若具有室内开门权限,则控制门锁打开;若不具有室内开门权限,则发送室内开门信息至预先配置的管理终端,由管理终端确定是否控制门锁打开。

[0005] 为解决技术问题,本申请提供一种室内开门权限的配置方法,该方法包括:采集待配置人员的身份信息;获取针对每一待配置人员的室内开门权限的配置指令;根据配置指令,生成室内开门权限信息;关联身份信息和室内开门权限信息;其中,室内开门权限信息包括:是否具有室内开门权限;或者预设环境条件下是否具有室内开门权限。

[0006] 为解决技术问题,本申请提供一种室内开门控制装置,该室内开门控制装置包括处理器和存储器;存储器中存储有计算机程序,处理器用于执行计算机程序以实现如上述方法的步骤。

[0007] 为解决技术问题,本申请提供一种计算机存储介质,其中存储有计算机程序,计算机程序被执行时实现室内开门控制方法中的步骤。

[0008] 本申请的方法是:接收到室内开门指令,会先获取室内开门人员的身份信息,并确定该室内开门人员是否具有室内开门权限,具有室内开门权限的室内开门人员可以打开门,没有室内开门权限的室内开门人员需要等待管理终端确认后才能够知晓是否能够打开门,可以排除一些如室内开门人员被诱骗开门导致被室外人员抢劫的安全隐患,即增加了室内开门的权限控制,并配合管理终端控制远程开门的方式,可以实现安全又非常灵活的室内开门过程。

附图说明

[0009] 为了更清楚地说明本申请实施方式中的技术方案,下面将对实施方式描述中所需

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申请的一些实施方式,对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。

- [0010] 图1是本申请室内开门控制方法一实施方式的流程示意图;
- [0011] 图2是本申请室内开门控制方法另一实施方式的流程示意图;
- [0012] 图3是本申请室内开门权限的配置方法一实施方式的流程示意图;
- [0013] 图4是本申请室内开门控制装置一实施方式的结构示意图;
- [0014] 图5是本申请计算机存储介质一实施方式的结构示意图。

具体实施方式

[0015] 为使本领域的技术人员更好地理解本申请的技术方案,下面结合附图和具体实施方式对本申请所提供的室内开门控制方法、权限的配置方法、装置和存储介质做进一步详细描述。

[0016] 具体请参阅图1,图1是本申请室内开门控制方法一实施方式的流程示意图。本实施方式室内开门控制方法包括以下步骤。

[0017] S101:获取室内开门指令。

[0018] 室内开门指令是由室内的人员发起的开门请求。室内开门操作可以是在室内发起开门请求的人员(即室内开门人员)握住室内门把手的动作。室内门把手上的传感器(可以是压力传感器、或者可以是压力传感器和温度传感器的组合)感应到有人体部位施加作用力到门把手上,就可以相当于室内开门控制装置获取到室内开门指令。可以理解的是,室内开门操作或者可以是室内开门人员旋转室内门把手的动作。室内门把手上的传感器(可以是角度传感器、位置传感器或距离传感器等)感应到室内门把手被旋转或者室内门把手被旋转到一定角度,就可以相当于室内开门控制装置获取到室内开门指令。室内开门操作或者可以是室内开门人员按下室内的开门按钮的动作。开门按钮上的传感器(可以是压力传感器)感应到开门按钮被按下,就可以相当于室内开门控制装置获取到室内开门指令。

[0019] S102:响应室内开门指令,获取室内开门人员的身份信息。

[0020] 响应于室内开门指令,可以获取室内开门人员的身份信息。获取室内开门人员的身份信息可以是获取室内开门人员的验证信息,通过室内开门人员的验证信息与预先设置的信息是否相同来判断室内开门人员的身份。验证信息是能够证明室内开门人员是否具有室内开门权限的身份信息,具体可以通过室内开门人员的终端设备提供验证信息(即手机信息验证),也可以通过室内开门人员的身体特征来提供验证信息(即生物特征信息验证),或者验证信息是预先设置的密码或者通行证(即密码信息验证、卡片信息验证)。验证信息可以为其中的一种或是任意组合,多种验证信息的任意组合,是为了确保在室内开门人员想要从室内开门时,验证信息的安全性足够高,来增加陌生人获取验证信息的难度,提高室内的安全性。

[0021] 室内开门人员的身体特征(即用来验证的生物特征信息)可以是室内开门人员的人脸图像、静脉、指纹、声纹、掌纹和虹膜中的一种或多种。当然,室内开门人员的身体特征还可以包括其他用来识别室内开门人员身份的身体特征。获取室内开门人员身份信息的方法可以是:通过指纹收集器采集室内开门人员的指纹;通过红外成像仪采集人手局部的血

管图像;通过录音设备采集室内开门人员的声音信息。室内开门控制装置在接收到指纹收集器采集的指纹、红外成像仪采集的人手局部的血管图像或录音设备采集的室内开门人员的声音信息后,通过与其相对应的指纹数据库、血管图像数据库或声音数据库对比,确认室内开门人员的身份,更有利于对室内开门人员身份的判断,防止陌生人开锁,提高室内的安全性。

[0022] S103:根据室内开门人员的身份信息,确认室内开门人员是否具有室内开门权限。

[0023] 获取到室内开门人员的身份信息后,将获取到的室内开门人员的身份信息与预先配置的数据库对比,匹配出室内开门人员的身份。接着可以在室内开门的授权人员列表中查找是否有室内开门人员,以确认室内开门人员是否具有室内开门权限。或者可以在该室内开门人员的授权权限中查找是否有室内开门权限。室内开门人员具有室内开门权限(即若是)时,进入步骤S104;室内开门人员不具有室内开门权限(即若否)时,进入步骤S105。

[0024] S104:控制门锁打开。

[0025] S105:发送室内开门信息至预先配置的管理终端,由管理终端确定是否控制门锁打开。

[0026] 若室内开门人员不具有室内开门权限,可以将室内开门信息发送给预先配置的管理终端。室内开门信息可以包括室内开门人员的身份、开门的时间、地点等。在发送室内开门信息后可以向管理终端发送信息(可以包括语音信息、文本信息、音频信息中的至少一种)陈述开门原因和/或采集的室内外信息,让管理终端能得出更加合理的判断结果。或者可以在管理终端确定是否控制门锁打开的过程中,通过电话、聊天软件等方式向管理终端陈述开门原因和/或呈现室内外状况。

[0027] 本实施方式中接收到室内开门指令,会先获取室内开门人员的身份信息,并确定该室内开门人员是否具有室内开门权限,具有室内开门权限的室内开门人员可以打开门,没有室内开门权限的室内开门人员需要等待管理终端确认后能够知晓是否能够打开门,可以排除一些安全隐患,并且即增加了室内开门的权限控制,并配合管理终端控制远程开门的方式,可以实现安全又非常灵活的室内开门过程。

[0028] 基于图1所示的实施方式,本申请进一步提出更具体的方案,请参阅图2,图2是本申请室内开门控制方法另一实施方式的流程示意图。本实施方式室内开门控制方法包括以下步骤。

[0029] S201:获取室内开门指令。

[0030] 可如上述S101,在此不做赘述。

[0031] S202:响应室内开门指令,判断室内开门指令是否为紧急开门指令。

[0032] 获取到室内开门指令后,可以先判断室内开门指令是否是紧急开门指令。若室内开门人员通过触按紧急开门按钮发起的室内开门指令,即紧急开门按钮上的传感器感应到紧急开门按钮被触按,可以得出室内开门指令是紧急开门指令的结论。可以将火灾报警按钮等紧急情况报警按钮设置为紧急开门按钮,在按下紧急开门按钮时,既可以控制门开,又可以报警(可以近程报警、远程报警),一举两用;又可以在室内开门人员为逃避获取身份信息步骤而选择按下紧急开门按钮时,能够及时知晓门被室内开门人员开启过的情况,方便其他人员及时做出措施;也可以减少室内开门人员为逃避身份信息获取步骤而选择按下紧急开门按钮的次数。或者在室内开门人员通过非紧急开门按钮或门把手开门时,室内

或室外的紧急传感器感应到有紧急事件发生,可以得出室内开门指令是紧急开门指令的结论。

[0033] 室内或室外的紧急传感器感应到有紧急事件发生可以是:室内或室外的火灾感应器感应到室内或室外有火灾情况发生;室内的气体浓度传感器感应到室内的有毒气体浓度超过浓度阈值;室内或室外的风速感应器感应到室内或室外的风速超过风速阈值;室内或室外的地震感应器感应到室外的地震状况较严重。室内开门指令是紧急开门指令(即若是)时,进入步骤S203;室内开门指令不是紧急开门指令(即若否)时,进入步骤S204。

[0034] S203:控制门锁打开,并发送室内开门信息至管理终端。

[0035] 若判断出室内开门指令为紧急开门指令,就跳过获取室内开门人员身份信息等步骤,直接控制门锁打开,不耽误室内开门人员的时间,防止发生紧急情况时耽误室内开门人员的时间导致室内开门人员的健康或财产受到损害或发生其他不利于室内开门人员的情况。控制门锁打开时,需要将室内开门信息(可以包括时间、采集到的室内开门人员的图像信息、采集到的室内开门人员的声音信息等)上传给管理终端,方便该室的家庭成员或工作人员通过管理终端核实室内开门情况;在核实出对该室做出不利举动的人(即盗窃者、抢劫者等等)为逃避身份信息获取等步骤而选择下达紧急开门指令的情况时,可以将室内开门信息作为证据举报对该室做出不利举动的人。

[0036] S204:执行获取室内开门人员的身份信息的动作。

[0037] 若判断出室内开门指令不是紧急开门指令,就需要获取室内开门人员身份信息。可以通过获取室内开门人员的人脸信息或指纹信息、掌纹信息、静脉信息、虹膜信息、声纹信息等来采集室内开门人员的身份信息。将采集到的室内开门人员的身份信息与其相应的特征数据库对比,可以匹配出室内开门人员的身份。

[0038] 若采集到的室内开门人员的身份信息与其相应的特征数据库任一数据匹配成功,可以将室内开门人员的身份确认为匹配成功的数据代表的身份。若采集到的室内开门人员的身份信息与其相应的特征数据库所有数据均未匹配成功,可以将室内开门人员的身份规定为无身份人员(该无身份人员没有室内开门权限)。

[0039] 可以理解的是,可以在将室内开门人员的身份信息与特征数据库未匹配成功时:可以进行再次获取室内开门人员的身份信息;或者可以将室内开门人员的身份信息与特征数据库进行第二次对比。第二次获取的身份信息与第一次获取的身份信息可以是不同的类型。这样可以防止本来具有室内开门权限的室内开门人员因为失误而导致身份信息输入出错从而不能识别出室内开门人员的身份的情况发生。

[0040] 若与特征数据库未匹配成功的室内开门人员经管理终端判断为与该室有关联的人(即该室的家庭成员、工作人员以及该室的家庭成员、工作人员认识的人),就可以将采集到室内开门人员的特征加入到特征数据库,并确认与特征数据库未匹配成功的室内开门人员的权限。若与特征数据库未匹配成功的室内开门人员经管理终端判断为与该室没有关联的人(即该室的家庭成员、工作人员不认识的人),就可以将采集到室内开门人员的特征加入到黑名单数据库。黑名单数据库的人员做出室内开门举动,室内开门控制装置会向发出警报,并会给管理终端发出警告。

[0041] S205:根据身份信息,在预先配置的具有室内开门权限的人员名单中查找是否存在室内开门人员。

[0042] 其中,获取到室内开门人员的身份信息后,可以确认室内开门人员的身份,可以在预先配置的具有室内开门权限的人员名单中查找是否存在室内开门人员。在预先配置的具有室内开门权限的人员名单中未查找到室内开门人员,就可以确定室内开门人员不具有室内开门权限。在预先配置的具有室内开门权限的人员名单中查找到室内开门人员,就可以确定室内开门人员具有室内开门权限。可以在室内开门控制装置内的存储器中存储具有室内开门权限的人员名单。当然,室内开门控制装置或者可以连接到数据库服务器获取到具有室内开门权限的人员名单。

[0043] 可以理解的是,除考虑室内开门权限的人员名单,还可以综合考虑室内开门人员的预设环境条件得出结论。在预先配置的具有室内开门权限的人员名单中查找到室内开门人员(即若是)时,进入步骤S207;在预先配置的具有室内开门权限的人员名单中未查找到室内开门人员(即若否)时,进入步骤S206。

[0044] S206:确定室内开门人员不具有室内开门权限。

[0045] 确定室内开门人员不具有室内开门权限,进入步骤S210。

[0046] S207:获取当前的环境信息,判断当前环境信息是否满足室内开门人员的预设环境条件。

[0047] 室内开门人员的预设环境条件可以是室内开门人员的预设时间条件和预设场景条件(例如是外卖上门场景等)。例如,室内开门人员在第一时间段的第一场景中下达了室内开门指令,在具有室内开门权限的人员名单中查找到室内开门人员后:可以判断第一时间段是否满足预设时间条件;还可以判断第一场景是否满足预设场景条件。当前环境信息满足室内开门人员的预设环境条件(即若是)时,进入步骤S208;当前环境信息不满足室内开门人员的预设环境条件(即若否)时,进入步骤S206。

[0048] S208:确定室内开门人员具有室内开门权限。

[0049] 若当前环境信息满足室内开门人员的预设环境条件,确定室内开门人员具有室内开门权限,进入步骤S209。

[0050] 上述判断步骤可以得出室内开门人员是否具有室内开门权限的结论。对应于得出的结论,可以分情况采取以下手段。

[0051] S209:控制门锁打开;

[0052] S210:发送室内开门信息至预先配置的管理终端,由管理终端确定是否控制门锁打开。

[0053] 本实施方式中可以通过判断室内开门指令是否是紧急开门指令,判定是否是紧急开门指令还是常规开门指令,获取到紧急开门指令无需进行获取室内开门人员身份信息步骤和后续的判断步骤,会直接将门锁打开,不会耽误室内开门人员的时间,并且会在将门锁打开的同时将室内开门信息发送给管理终端,方便管理终端核实;通过设置环境条件的判断步骤,可以实现某个室内开门人员在某个场景下、某个时间下是否具有开门权限的控制,做到更加灵活地管控室内开门情况。

[0054] 请参阅图3,图3是本申请室内开门权限的配置方法一实施方式的流程示意图。本实施方式室内开门权限的配置方法包括以下步骤。

[0055] S301:采集待配置人员的身份信息。

[0056] 其中,待配置人员的身份信息可以包括人员(如家庭成员、工作人员)的生物特征

(如指纹,人脸、声纹、掌纹、静脉等)信息、手机信息、密码信息、卡片信息等。采集人员的身份信息后,可以将人员身份信息与人员的身份匹配关联上。

[0057] S302:获取针对每一待配置人员的室内开门权限的配置指令。

[0058] 其中,每一配置指令可以包括室内开门人员的身份及其室内开门权限数据。该室内开门权限数据可以包括室内开门人员的室内开门权限级别(如总能开门、条件开门、不能开门等)。室内开门权限数据还可以包括室内开门的预设环境条件。例如,配置晚上11点到次日早上6点这个时间条件,小孩、老人及其他不在名单内的人员开门需要进行管理终端审批。室内开门的预设环境条件可以包括时间条件和场景条件。

[0059] S303:根据配置指令,生成室内开门权限信息。

[0060] S304:关联身份信息和室内开门权限信息。

[0061] 在生成室内开门权限信息后,将室内开门权限信息和身份信息关联,这样在获取到室内开门人员的身份信息后,就可以很快地确认室内开门人员的室内开门权限信息,从而可以很快地确认室内开门人员是否具有室内开门权限,这样可以不耽误室内开门人员的时间。

[0062] 其中,室内开门权限信息包括:是否具有室内开门权限;或者预设环境条件下是否具有室内开门权限。

[0063] 进一步地,室内开门权限的配置方法还可以包括配置远程管理员的步骤。配置远程管理员的步骤可以是配置远程开门控制管理员的名单。名单中的远程管理员可以用于对室内开门请求进行确认以及查阅室内开门信息。

[0064] 上述室内开门控制方法和室内开门权限的配置方法一般由室内开门控制装置实现,因而本申请还提出一种室内开门控制装置。请参阅图4,图4是本申请室内开门控制装置一实施方式的结构示意图。本室内开门控制装置40包括处理器42和存储器41;存储器41中存储有计算机程序,处理器42用于执行计算机程序以实现如上述室内开门控制方法和室内开门权限的配置方法中的步骤。

[0065] 进一步地,室内开门控制装置包括传感器(图未示),传感器用于采集室内开门人员的身份信息。

[0066] 进一步地,室内开门控制装置包括紧急开门按钮(图未示),紧急开门按钮用于获取紧急开门指令。

[0067] 上述室内开门控制方法的逻辑过程以计算机程序呈现,在计算机程序方面,若其作为独立的软件产品销售或使用,其可存储在计算机存储介质中,因而本申请提出一种计算机存储介质。请参阅图5,图5是本申请计算机存储介质一实施方式的结构示意图,本实施方式计算机存储介质50中存储有计算机程序51,计算机程序被处理器执行时实现上述室内开门控制方法和室内开门权限的配置方法中的步骤。

[0068] 该计算机存储介质50具体可以为U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory,)、磁碟或者光盘等可以存储计算机程序的介质,或者也可以为存储有该计算机程序的服务器,该服务器可将存储的计算机程序发送给其他设备运行,或者也可以自运行该存储的计算机程序。该计算机存储介质50从物理实体上来看,可以为多个实体的组合,例如多个服务器、服务器加存储器、或存储器加移动硬盘等多种组合方式。

[0069] 以上仅为本申请的实施方式,并非因此限制本申请的专利范围,凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换,或直接或间接运用在其他相关的技术领域,均同理包括在本申请的专利保护范围内。

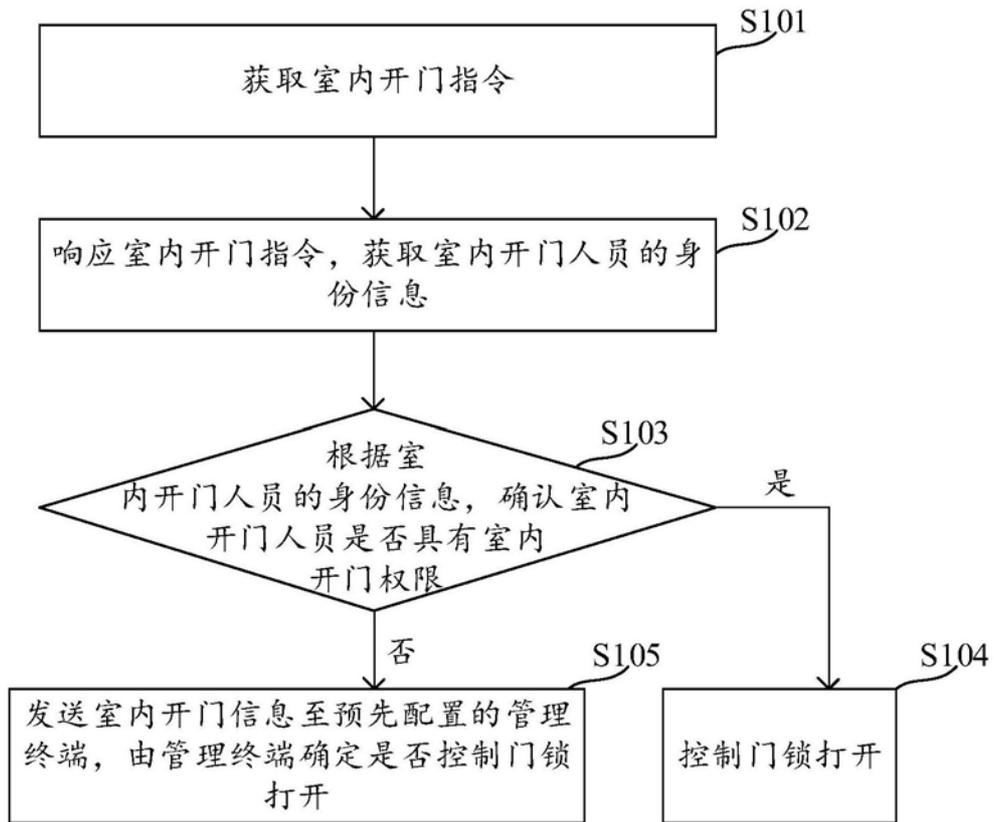


图1

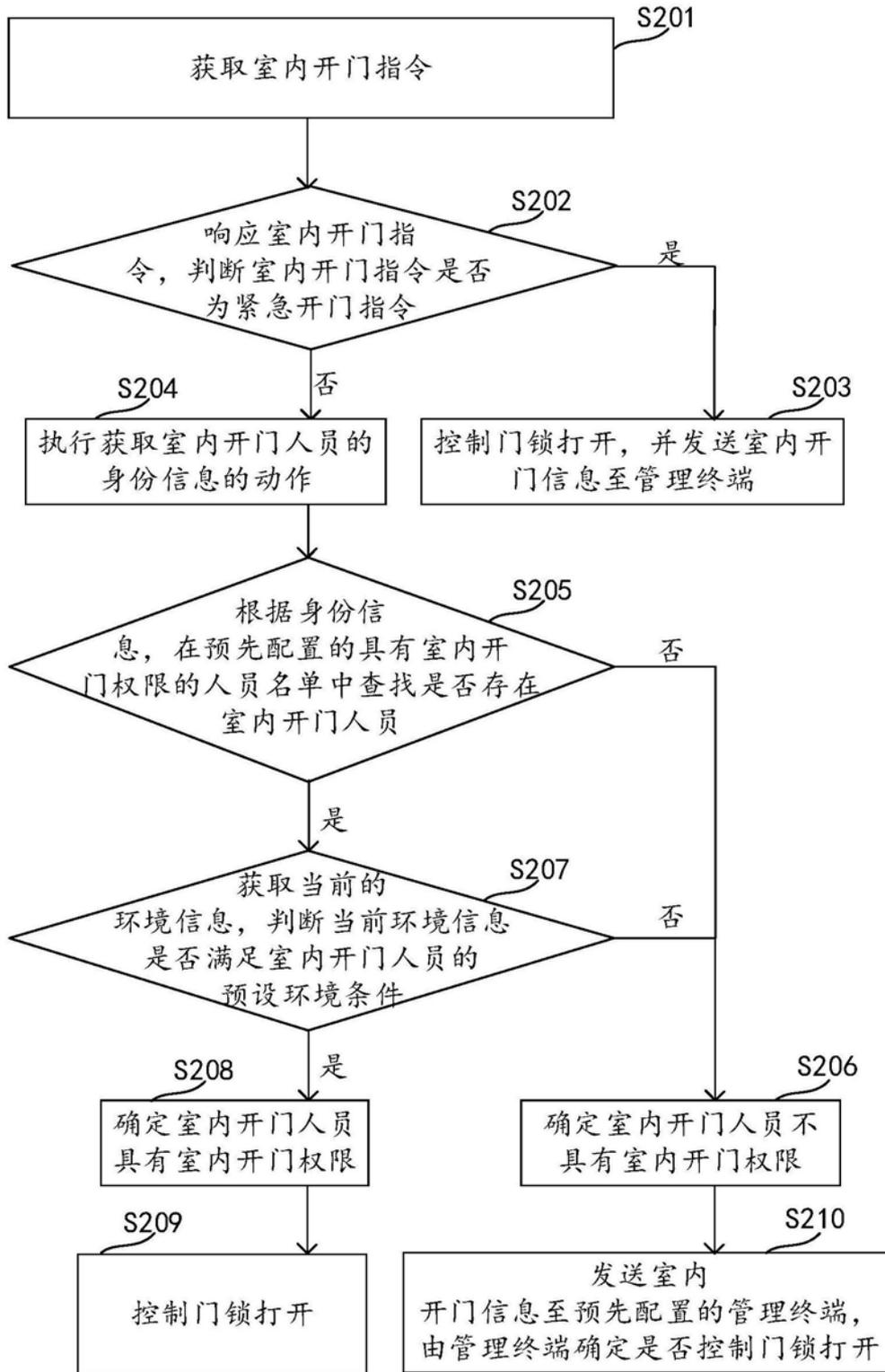


图2

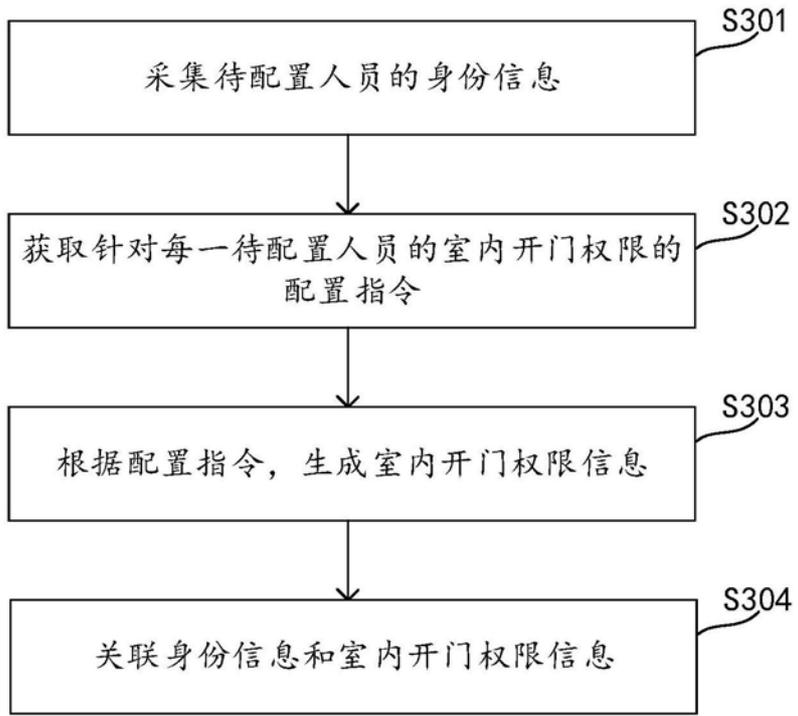


图3

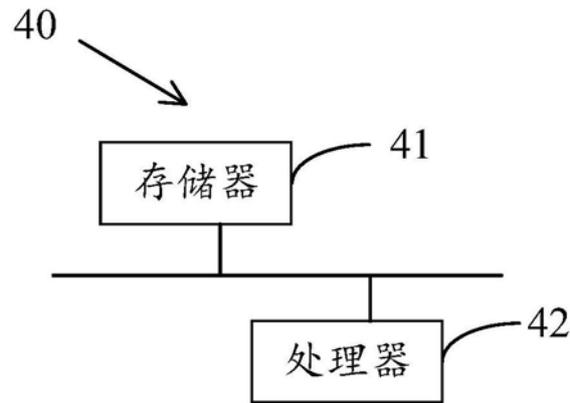


图4

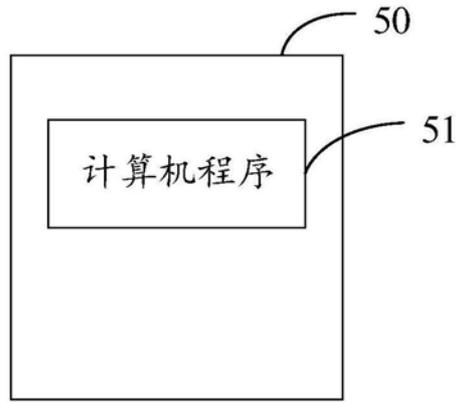


图5