(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 109109814 A
(43)申请公布日 2019.01.01

(21)申请号 201810827148.0

(22)申请日 2018.07.25

(71)申请人 特治(深圳)智能科技实业有限公司
地址 518000 广东省深圳市龙岗区龙城街道黄阁路441号龙岗天安数码城四号楼B1003

(72)发明人 郭清龙

(74)专利代理机构 深圳市中智立信知识产权代理有限公司 44427
代理人 刘蕊

(51)Int.Cl.
B60R 25/01(2013.01)
B60R 25/25(2013.01)

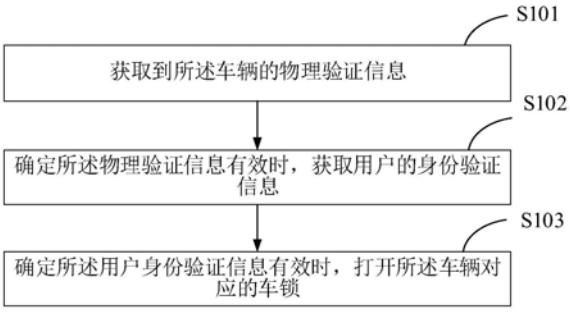
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种基于NFC识别的车辆开启方法、装置以及计算机存储介质

(57)摘要

本申请提供了一种基于NFC识别的车辆开启方法、装置以及计算机存储介质，所述车辆开启方法包括获取到所述车辆的物理验证信息；确定所述物理验证信息有效时，获取用户的身份验证信息；确定所述用户身份验证信息有效时，打开所述车辆对应的车锁。能够有效避免盗用用户身份信息开启车辆的情况，能够保证车辆正常运行的前提下，保护用户身份信息，避免给用户带来不必要的麻烦和纠纷。并且在该车辆为私家车时，能够有效保护用户私家车不被盗走，保护用户财产。



CN 109109814 A

1.一种车辆开启方法,其特征在于,所述车辆控制方法包括:

获取到所述车辆的物理验证信息;

确定所述物理验证信息有效时,获取用户的身份验证信息;

确定所述用户身份验证信息有效时,打开所述车辆对应的车锁。

2.根据权利要求1所述的车辆开启方法,其特征在于,所述获取到所述车辆的物理验证信息的步骤具体包括:

接收到所述车辆设定位置的车锁开启指令后,打开物理验证界面;

接收用户通过所述物理验证界面输入的所述物理验证信息;

所述确定所述物理验证信息有效时,获取用户的身份验证信息的步骤具体包括:

判断所述物理验证信息与预先存储的设置验证信息是否相同;

如果所述物理验证信息与所述设置验证信息相同,获取用户的身份验证信息。

3.根据权利要求2所述的车辆开启方法,其特征在于,所述物理验证信息包括密码验证信息;所述车辆设定位置的车锁包括车门锁、天窗锁以及后备箱锁中的至少一个。

4.根据权利要求2所述的车辆开启方法,其特征在于,所述接收到所述车辆设定位置的车锁开启指令后,打开物理验证界面的步骤具体包括:

接收用户通过近场通信NFC的方式向车辆设定位置的车锁发起的开启指令后,打开物理验证界面。

5.根据权利要求4所述车辆开启方法,其特征在于,所述接收用户通过近场通信NFC的方式向车辆设定位置的车锁发起的开启指令后,打开物理验证界面的步骤具体包括:

扫描所述车辆的条码信息,获取到所述车辆设定位置的车锁信息;

通过近场通信NFC的方式向车辆设定位置的车锁发起的开启指令;

开启所述物理验证界面,并接收开启所述车辆设定位置的车锁的物理验证验证信息。

6.根据权利要求1～5任一项所述的车辆开启方法,其特征在于,所述确定所述物理验证信息有效时,获取用户的身份验证信息的步骤具体包括:

在确定所述物理验证信息有效时,采集用户的身份验证信息;

所述确定所述用户的身份验证信息有效时,打开所述车辆对应的车锁的步骤具体包括:

将所述用户身份验证信息与预先存储的设置身份信息相比对,确定所述用户验证信息是否与所述设置身份信息相匹配;

所述相匹配,打开所述车辆对应的车锁。

7.根据权利要求6所述的车辆开启方法,其特征在于,所述身份验证信息包括指纹、声音、人脸识别中的至少一种。

8.根据权利要求1所述的车辆开启方法,其特征在于,所述获取到所述车辆的物理验证信息的步骤具体包括:

接收并存储用户输入的设置身份信息。

9.一种车辆开启装置,其特征在于,所述车辆开启装置包括相互耦接的处理器和人机交互控制电路,所述处理器在工作时配合所述人机交互控制电路实现如权利要求1-8任一项所述的车辆开启方法。

10.一种计算机存储介质,其特征在于,所述计算机存储介质上存储有程序数据,所述

程序数据被处理器执行时实现如权利要求1-8任一项所述的车辆开启方法。

一种基于NFC识别的车辆开启方法、装置以及计算机存储介质

技术领域

[0001] 本申请涉及汽车控制技术领域，特别是涉及一种汽车开启方法、装置以及计算机存储介质。

背景技术

[0002] 随着人们生活水平的不断提高，汽车已经成为人们生活中的必需品。

[0003] 现有的汽车开锁系统，如共享汽车，都是通过一定的验证后进行开启。目前车辆进项开启验证的方式主要有两种，一种是物理验证，一种是通过逻辑验证，但是无论哪一种验证方式，都不能避免出现身份的盗用问题。

发明内容

[0004] 本申请主要解决的技术问题是提供一种基于NFC识别的车辆开启方法、装置以及计算机存储介质，能够有效避免盗用用户身份信息开启车辆的情况，能够保证车辆正常运行的前提下，保护用户身份信息，避免给用户带来不必要的麻烦和纠纷。

[0005] 为解决上述技术问题，本申请采用的一个技术方案是：提供一种车辆开启方法，包括：获取到所述车辆的物理验证信息；

[0006] 确定所述物理验证信息有效时，获取用户的身份验证信息；

[0007] 确定所述用户身份验证信息有效时，打开所述车辆对应的车锁。

[0008] 其中，所述获取到所述车辆的物理验证信息的步骤具体包括：

[0009] 接收到所述车辆设定位置的车锁开启指令后，打开物理验证界面；

[0010] 接收用户通过所述物理验证界面输入的所述物理验证信息；

[0011] 所述确定所述物理验证信息有效时，获取用户的身份验证信息的步骤具体包括：

[0012] 判断所述物理验证信息与预先存储的设置验证信息是否相同；

[0013] 如果所述物理验证信息与所述设置验证信息相同，获取用户的身份验证信息。

[0014] 其中，所述物理验证信息包括密码验证信息；所述车辆设定位置的车锁包括车门锁、天窗锁以及后备箱锁中的至少一个。

[0015] 其中，所述接收到所述车辆设定位置的车锁开启指令后，打开物理验证界面的步骤具体包括：

[0016] 接收用户通过近场通信NFC的方式向车辆设定位置的车锁发起的开启指令后，打开物理验证界面。

[0017] 其中，所述接收用户通过近场通信NFC的方式向车辆设定位置的车锁发起的开启指令后，打开物理验证界面的步骤具体包括：

[0018] 扫描所述车辆的条码信息，获取到所述车辆设定位置的车锁信息；

[0019] 通过近场通信NFC的方式向车辆设定位置的车锁发起的开启指令；

[0020] 开启所述物理验证界面，并接收开启所述车辆设定位置的车锁的物理验证验证信息。

[0021] 其中，所述确定所述物理验证信息有效时，获取用户的身份验证信息的步骤具体包括：

[0022] 在确定所述物理验证信息有效时，采集用户的身份验证信息；

[0023] 所述确定所述用户的身份验证信息有效时，打开所述车辆对应的车锁的步骤具体包括：

[0024] 将所述用户身份验证信息与预先存储的设置身份信息相比对，确定所述用户验证信息是否与所述设置身份信息相匹配；

[0025] 其中，所述身份验证信息包括指纹、声音、人脸识别中的至少一种。

[0026] 其中，所述获取到所述车辆的物理验证信息的步骤具体包括：

[0027] 接收并存储用户输入的设置身份信息。

[0028] 为解决上述技术问题，本申请采用的另一个技术方案是：提供一种车辆开启装置，所述车辆开启装置包括相互耦接的处理器和人机交互控制电路，所述处理器在工作时配合所述人机交互控制电路实现上述任一实施方式所述的车辆开启方法。

[0029] 为解决上述技术问题，本申请采用的再一个技术方案是：提供一种计算机存储介质，所述计算机存储介质上存储有程序数据，所述程序数据被处理器执行时实现上述任一实施方式所述的车辆开启方法。

[0030] 本申请的有益效果是：区别于现有技术的情况，本申请获取到所述车辆的物理验证信息后，确定所述物理验证信息有效时，获取用户的身份验证信息，并对用户的身份验证信息进行判断，确定所述用户身份验证信息有效时，打开所述车辆对应的车锁。能够有效避免盗用用户身份信息开启车辆的情况，能够保证车辆正常运行的前提下，保护用户身份信息，避免给用户带来不必要的麻烦和纠纷。并且在该车辆为私家车时，能够有效保护用户私家车不被盗走，保护用户财产。

附图说明

[0031] 图1是本申请车辆开启方法一实施方式的流程示意图；

[0032] 图2是本申请车辆开启装置一实施方式的结构示意图；

[0033] 图3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

[0034] 下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，均属于本申请保护的范围。

[0035] 汽车，作为人们日常生活的必需品，各个部分也越来越独立化，如后备箱、天窗、车门都可以单独控制，本申请通过独立的验证实现不同位置的车锁的开启和关闭。

[0036] 具体地，请参阅图1，图1是本申请车辆开启方法一实施方式的流程示意图。本实施方式的车辆开启方法包括如下步骤：

[0037] S101：获取到所述车辆的物理验证信息。

[0038] 其中所述车辆包括私家车以及共享汽车。

[0039] 具体地，用户在需要打开该车辆设定位置的车锁时，可先通过车辆开启装置如车钥匙或者智能设备向该车辆发送指令，如通过按下车钥匙对应的按键或通过智能设备扫描共享车辆的条形码如二维码信息或将智能设备靠近车门感应位置。

[0040] 其中，该智能设备包括智能手机。

[0041] 其中，车辆设定位置的车锁包括车门锁、天窗锁以及后备箱锁中的至少一个。

[0042] 所述物理验证信息包括密码验证信息，还可以为逻辑验证，在此不做限定。

[0043] 在接收到用户的上述质量后，车钥匙或智能设备开启对应的物理验证界面，用户通过该物理验证界面输入物理验证信息。

[0044] 其中，如果该车辆为私家车，用户可自行输入物理验证信息。如果是共享汽车，在通过智能设备向该车辆设定位置的车锁发起开启指令后，只能设备接收服务器发送的物理验证信息，用户将该物理验证信息通过上述物理验证界面进行输入。

[0045] 在一个优选的实施方式中，为了避免出现现有技术中通过RFID数据传输出现的安全隐患问题，车钥匙或智能设备采用近场通信NFC的方式向车辆设定位置的车锁发起开启指令，能够有效保护数据的安全性。

[0046] 在通过场通信NFC的方式向车辆设定位置的车锁发起开启指令时，需要车辆开锁终端以及对应的车锁都具备NFC功能，一般是分别在车辆对应的车锁位置增加NFC模块来实现。

[0047] S102：确定所述物理验证信息有效时，获取用户的身份验证信息。

[0048] 在用户通过物理验证界面输入物理验证信息后，车钥匙或智能设备将该物理验证信息与预先存储的设置物理信息进行比对，确定该物理验证信息与设置物理信息是否相同。

[0049] 如判断输入的密码信息与预先存储的密码是否相同，如果相同，则证实该本次物理验证信息为有效信息，如果不同，则本次输入的物理验证信息为无效信息。

[0050] 在确定物理验证信息有效时，只能说明当前的车钥匙或智能终端与车辆的验证信息相匹配，但是对于用户是否为车主或智能终端是否为当前注册用户本人等并不确定，为了避免后续给用户带来麻烦或盗车，本实施方式在确定车钥匙或智能终端的物理验证信息有效时，进一步地对用户身份信息进行验证。

[0051] 具体地，车钥匙或智能设备在确定物理验证信息有效时，弹出用户身份验证界面，其中身份验证信息包括指纹、声音、人眼识别或人眼识别中的至少一种。

[0052] 在用户输入上述身份验证信息后，对应的车钥匙或智能设备接收该身份验证信息，并将该身份验证信息与预先存储的设置身份信息相比较，判断该身份验证信息与预先存储的设置身份信息是否相匹配。

[0053] 在一个具体的实施方式中，车辆开启装置位车钥匙即上述车辆为私家车时，接收用户通过采集用户指纹信息的方式获取用户的身份验证信息，并将该身份验证信息与预先采集存储的指纹信息相比较，判断该指纹信息与设置的指纹信息是否相匹配。

[0054] 在另一个具体的实施方式中，车辆开启装置为智能设备时即该车辆为共享汽车时，该智能设备对用户的人脸进项拍照或识别，并将识别到的人脸信息与预先存储的人脸信息进行对比，判断二者是否相同。

[0055] 在其他实施方式中，为了实现多重保险，也可以同时采用多种验证方式，如声音和

人脸同时识别,或指纹和声音同时识别等,在此不做限定。

[0056] 通过上述方式,能够有效避免盗用用户身份信息开启车辆的情况,能够保证车辆正常运行的前提下,保护用户身份信息,避免给用户带来不必要的麻烦和纠纷。并且在该车辆为私家车时,能够有效保护用户私家车不被盗走,保护用户财产。

[0057] S103:确定所述用户身份验证信息有效时,打开所述车辆对应的车锁。

[0058] 在确定物理验证信息正确且用户身份信息有效时,车辆对应位置的车锁就可以正常打开了。在此不再赘述。

[0059] 区别于现有技术,本实施方式中,获取到所述车辆的物理验证信息后,确定所述物理验证信息有效时,获取用户的身份验证信息,并对用户的身份验证信息进行判断,确定所述用户身份验证信息有效时,打开所述车辆对应的车锁。能够有效避免盗用用户身份信息开启车辆的情况,能够保证车辆正常运行的前提下,保护用户身份信息,避免给用户带来不必要的麻烦和纠纷。并且在该车辆为私家车时,能够有效保护用户私家车不被盗走,保护用户财产。

[0060] 并且,车钥匙或智能设备采用近场通信NFC的方式向车辆设定位置的车锁发起开启指令,避免了出现现有技术中通过RFID数据传输出现的安全隐患问题,能够有效保护数据的安全性。

[0061] 参与图2,图2是本申请车辆开启装置一实施方式的结构示意图。本实施方式的车辆开启装置包括相互耦接的处理器201和人机交互控制电路202。该人机交互控制电路202用于接收用户指令或显示对应的界面,如物理验证界面或身份验证界面等。

[0062] 处理器202用于获取到所述车辆的物理验证信息。

[0063] 其中所述车辆包括私家车以及共享汽车。

[0064] 车辆开启装置包括车钥匙或者智能设备。

[0065] 具体地,用户在需要打开该车辆设定位置的车锁时,可先通过车辆开启装置如车钥匙或者智能设备向该车辆发送指令,如通过按下车钥匙对应的按键或通过智能设备扫描共享车辆的条形码如二维码信息。

[0066] 其中,该智能设备包括智能手机。

[0067] 其中,车辆设定位置的车锁包括车门锁、天窗锁以及后备箱锁中的至少一个。

[0068] 所述物理验证信息包括密码验证信息,还可以为逻辑验证,在此不做限定。

[0069] 处理器201在接收到用户的上述质量后,通过人机交互控制电路202显示物理验证界面,用户通过该物理验证界面输入物理验证信息。

[0070] 其中,如果该车辆为私家车,用户可自行输入物理验证信息。如果是共享汽车,在通过智能设备向该车辆设定位置的车锁发起开启指令后,只能设备接收服务器发送的物理验证信息,用户将该物理验证信息通过上述物理验证界面进行输入。

[0071] 在一个优选的实施方式中,为了避免出现现有技术中通过RFID数据传输出现的安全隐患问题,车钥匙或智能设备采用近场通信NFC的方式向车辆设定位置的车锁发起开启指令,能够有效保护数据的安全性。

[0072] 在通过场通信NFC的方式向车辆设定位置的车锁发起开启指令时,需要车辆开锁终端以及对应的车锁都具备NFC功能,一般是分别在车辆对应的车锁位置增加NFC模块来实现。

[0073] 处理器201还用于确定所述物理验证信息有效时，获取用户的身份验证信息。

[0074] 在用户通过物理验证界面输入物理验证信息后，处理器201将该物理验证信息与预先存储的设置物理信息进行比对，确定该物理验证信息与设置物理信息是否相同。

[0075] 如判断输入的密码信息与预先存储的密码是否相同，如果相同，则证实该本次物理验证信息为有效信息，如果不同，则本次输入的物理验证信息为无效信息。

[0076] 在确定物理验证信息有效时，只能说明当前的车钥匙或智能终端与车辆的验证信息相匹配，但是对于用户是否为车主或智能终端是否为当前注册用户本人等并不确定，为了避免后续给用户带来麻烦或盗车，本实施方式在确定车钥匙或智能终端的物理验证信息有效时，进一步地对用户身份信息进行验证。

[0077] 具体地，处理器201在确定物理验证信息有效时，通过人机交互控制电路202弹出用户身份验证界面，其中身份验证信息包括指纹、声音、人眼识别或人眼识别中的至少一种。

[0078] 在用户输入上述身份验证信息后，处理器201接收该身份验证信息，并将该身份验证信息与预先存储的设置身份信息相比较，判断该身份验证信息与预先存储的设置身份信息是否相匹配。

[0079] 在一个具体的实施方式中，车辆开启装置位车钥匙即上述车辆为私家车时，处理器201接收用户通过采集用户指纹信息的方式获取用户的身份验证信息，并将该身份验证信息与预先采集存储的指纹信息相比较，判断该指纹信息与设置的指纹信息是否相匹配。

[0080] 在另一个具体的实施方式中，车辆开启装置为智能设备时即该车辆为共享汽车时，处理器201对用户的人脸进项拍照或识别，并将识别到的人脸信息与预先存储的人脸信息进行对比，判断二者是否相同。

[0081] 在其他实施方式中，为了实现多重保险，处理器201也可以同时采用多种验证方式，如声音和人脸同时识别，或指纹和声音同时识别等，在此不做限定。

[0082] 处理器201还用于确定所述用户身份验证信息有效时，打开所述车辆对应的车锁。处理器201在确定物理验证信息正确且用户身份信息有效时，车辆对应位置的车锁就可以正常打开了。在此不再赘述。

[0083] 区别于现有技术，本实施方式中，处理器获取到所述车辆的物理验证信息后，确定所述物理验证信息有效时，获取用户的身份验证信息，并对用户的身份验证信息进行判断，确定所述用户身份验证信息有效时，打开所述车辆对应的车锁。能够有效避免盗用用户身份信息开启车辆的情况，能够保证车辆正常运行的前提下，保护用户身份信息，避免给用户带来不必要的麻烦和纠纷。并且在该车辆为私家车时，能够有效保护用户私家车不被盗走，保护用户财产。

[0084] 并且，车钥匙或智能设备采用近场通信NFC的方式向车辆设定位置的车锁发起开启指令，避免了出现现有技术中通过RFID数据传输出现的安全隐患问题，能够有效保护数据的安全性。

[0085] 请参阅图3，本申请还提供一种存储装置的实施例的结构示意图。本实施例中，该存储装置30存储有处理器可运行的计算机指令31，该计算机指令31用于执行上述实施例中的方法。

[0086] 该存储装置30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指令的介质,或者也可以为存储有该计算机指令的服务器,该服务器可将存储的计算机指令发送给其他设备运行,或者也可以自运行该存储的计算机指令。

[0087] 在本申请所提供的几个实施例中,应该理解到,所揭露的方法和装置,可以通过其它的方式实现。例如,以上所描述的装置实施方式仅仅是示意性的,例如,模块或单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0088] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施方式方案的目的。

[0089] 另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0090] 集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)或处理器(processor)执行本申请各个实施方式方法的全部或部分步骤。而前述的存储介质包括: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)、磁碟或者光盘等各种可以存储程序代码的介质。

[0091] 以上所述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。

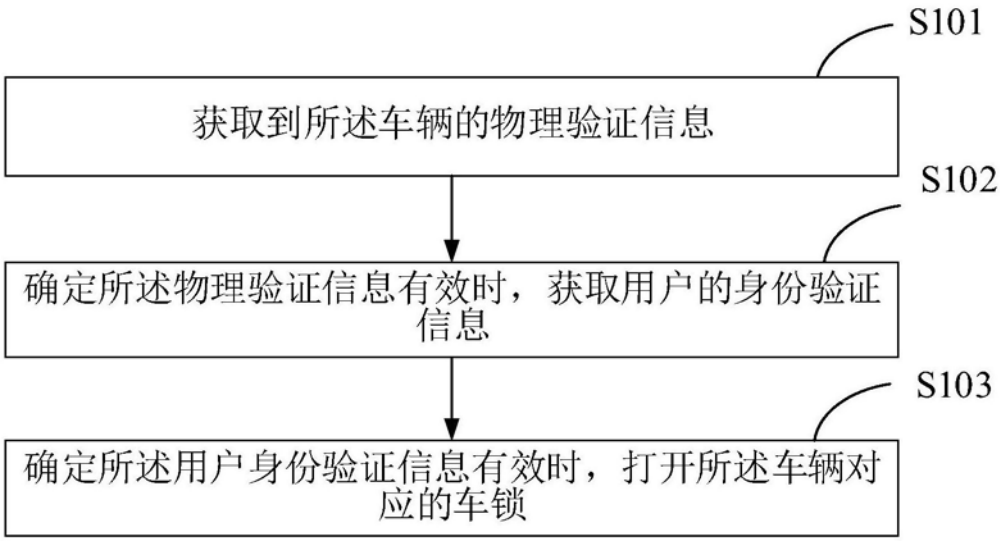

S101
获取到所述车辆的物理验证信息
S102
确定所述物理验证信息有效时，获取用户的身份验证信息
S103
确定所述用户身份验证信息有效时，打开所述车辆对应的车锁

图1

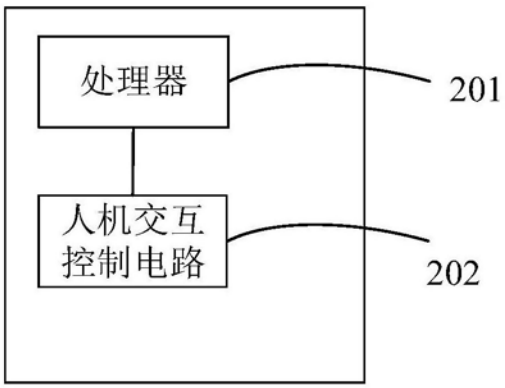

处理器
201
人机交互控制电路
202

图2

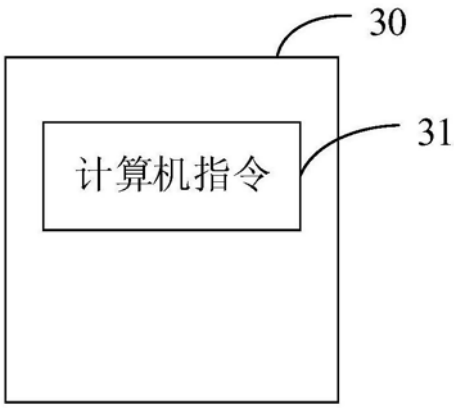

30
计算机指令
31

图3