



(12) 发明专利

(10) 授权公告号 CN 114120487 B

(45) 授权公告日 2024. 02. 23

(21) 申请号 202111255753.3

CN 106314368 A, 2017. 01. 11

(22) 申请日 2021. 10. 27

CN 106394486 A, 2017. 02. 15

(65) 同一申请的已公布的文献号

CN 109435893 A, 2019. 03. 08

申请公布号 CN 114120487 A

CN 109532759 A, 2019. 03. 29

(43) 申请公布日 2022. 03. 01

CN 110371080 A, 2019. 10. 25

(73) 专利权人 广州奇兵电子科技有限公司

CN 111080857 A, 2020. 04. 28

地址 510000 广东省广州市黄埔区云埔工

CN 111312237 A, 2020. 06. 19

业区耀南路27号厂房二楼

CN 111645631 A, 2020. 09. 11

(72) 发明人 魏源仁

CN 111762126 A, 2020. 10. 13

(74) 专利代理机构 广州三环专利商标代理有限

CN 111918243 A, 2020. 11. 10

公司 44202

CN 111959438 A, 2020. 11. 20

专利代理师 许羽冬 郭浩辉

CN 113147674 A, 2021. 07. 23

(51) Int. Cl.

CN 113487770 A, 2021. 10. 08

G07C 9/00 (2020. 01)

CN 210666917 U, 2020. 06. 02

KR 101835991 B1, 2018. 04. 19

审查员 代云飞

(56) 对比文件

CN 105976466 A, 2016. 09. 28

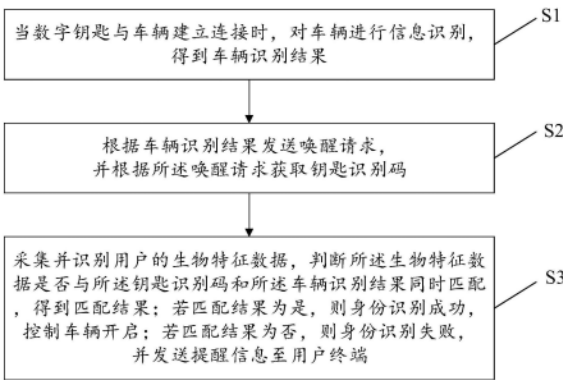
权利要求书2页 说明书6页 附图2页

(54) 发明名称

一种汽车数字钥匙管理方法、系统、设备及存储介质

(57) 摘要

本发明涉及汽车钥匙管理技术领域,尤其涉及一种汽车数字钥匙管理方法、系统、设备及存储介质,包括:当数字钥匙与车辆建立连接时,对车辆进行信息识别,得到车辆识别结果;根据车辆识别结果发送唤醒请求,并根据所述唤醒请求获取钥匙识别码;采集并识别用户的生物特征数据,判断所述生物特征数据是否与所述钥匙识别码和所述车辆识别结果同时匹配,得到匹配结果;若匹配结果为是,则身份识别成功;若匹配结果为否,则身份识别失败,解决了现有技术中的汽车数字钥匙的安全性能差,导致用户体验差、推广应用困难的问题,本发明通过身份安全认证以及用户终端授权,极大地提高了汽车数字钥匙的安全性,提高了用户体验。



1. 一种汽车数字钥匙管理方法,其特征在于,包括以下步骤:
当数字钥匙与车辆建立连接时,对车辆进行信息识别,得到车辆识别结果;
根据车辆识别结果发送唤醒请求,并根据所述唤醒请求获取钥匙识别码;
采集并识别用户的生物特征数据,判断所述生物特征数据是否与所述钥匙识别码和所述车辆识别结果同时匹配,得到匹配结果;
若匹配结果为是,则身份识别成功,控制汽车解锁;
若匹配结果为否,则身份识别失败,并发送提醒信息至用户终端;
其中,所述根据车辆识别结果发送唤醒请求的步骤,具体包括:
根据车辆识别结果获取车辆标识数据,并将所述车辆标识数据输入预先训练好的车辆识别模型,得到车辆置信度;其中,所述车辆识别模型为长短期记忆循环神经网络;
在所述车辆置信度大于预设的第一置信度且小于预设的第二置信度时,识别该车辆为匹配车辆,并发送唤醒请求;
在所述车辆置信度小于第一置信度或大于第二置信度时,识别为非匹配车辆,并发送提醒信息至用户终端。
2. 如权利要求1所述的一种汽车数字钥匙管理方法,其特征在于,所述判断所述生物特征数据是否与所述钥匙识别码和所述车辆识别结果同时匹配,得到匹配结果的步骤包括:
根据所述钥匙识别码获取对应的第一特征向量;
根据所述车辆识别结果获取车辆识别码,并根据所述车辆识别码获取对应的第二特征向量;
根据所述生物特征数据获取对应的第三特征向量;
将第一特征向量、第二特征向量分别与第三特征向量进行匹配,对用户的身份进行验证,得到匹配结果。
3. 如权利要求1所述的一种汽车数字钥匙管理方法,其特征在于,所述方法还包括:
当身份识别失败时,检测用户的生物特征数据是否为新用户;
在检测到用户的生物特征数据为新用户时,发送授权请求至用户终端;
所述用户终端根据所述授权请求获取授权管理信息,同时验证所述授权管理信息中的数字签名,若验证通过,则根据所述授权管理信息确定授权范围信息和授权使用信息;
根据所述授权范围信息和授权使用信息生成用户授权码;
根据所述用户授权码控制汽车解锁。
4. 如权利要求1所述的一种汽车数字钥匙管理方法,其特征在于:所述生物特征数据为以下一种或多种的组合:面部特征数据、指纹特征数据、虹膜特征数据和音色特征数据。
5. 如权利要求1所述的一种汽车数字钥匙管理方法,其特征在于:所述数字钥匙包括智能手机、带有NFC功能的可穿戴设备。
6. 一种汽车数字钥匙管理系统,其特征在于:包括数字钥匙系统和用户终端,所述数字钥匙系统包括车辆识别模块、钥匙识别模块以及身份匹配模块;
所述车辆识别模块,用于当数字钥匙与车辆建立连接时,进行车辆信息识别,得到车辆识别结果;
所述钥匙识别模块,用于根据车辆识别结果发送唤醒请求,并根据所述唤醒请求获取钥匙识别码;

所述身份匹配模块,用于采集并识别得到用户的生物特征数据,并判断所述生物特征数据是否与所述钥匙识别码和预先存储的原始生物特征同时匹配,得到身份匹配结果,若身份匹配结果为同时匹配,则身份识别成功,控制汽车解锁;若身份匹配结果为不同时匹配,则身份识别失败,并发送提醒信息至用户终端;

其中,所述根据车辆识别结果发送唤醒请求,具体包括:

根据车辆识别结果获取车辆标识数据,并将所述车辆标识数据输入预先训练好的车辆识别模型,得到车辆置信度;其中,所述车辆识别模型为长短期记忆循环神经网络;

在所述车辆置信度大于预设的第一置信度且小于预设的第二置信度时,识别该车辆为匹配车辆,并发送唤醒请求;

在所述车辆置信度小于第一置信度或大于第二置信度时,识别为非匹配车辆,并发送提醒信息至用户终端。

7.如权利要求6所述的一种汽车数字钥匙管理系统,其特征在于,所述系统还包括:

身份检测模块,用于当身份识别失败时,检测用户的生物特征数据是否为新用户;

授权请求模块,用于在检测到用户的生物特征数据为新用户时,发送授权请求至用户终端,所述用户终端根据所述授权请求获取授权管理信息,同时验证所述授权管理信息中的数字签名,若验证通过,则根据所述授权管理信息确定授权范围信息和授权使用信息;还用于根据所述授权范围信息和授权使用信息生成用户授权码,根据所述用户授权码控制汽车解锁。

8.一种计算机设备,其特征在于:包括处理器和存储器,所述处理器与所述存储器相连,所述存储器用于存储计算机程序,所述处理器用于执行所述存储器中存储的计算机程序,以使得所述计算机设备执行如权利要求1至5中任一项所述的方法。

9.一种计算机可读存储介质,其特征在于:所述计算机可读存储介质中存储有计算机程序,当所述计算机程序被运行时,实现如权利要求1至5任一项所述的方法。

一种汽车数字钥匙管理方法、系统、设备及存储介质

技术领域

[0001] 本发明涉及汽车钥匙管理技术领域,尤其涉及一种汽车数字钥匙管理方法、系统、设备及存储介质。

背景技术

[0002] 目前,随着技术的日益进步,人们对汽车控能化、便利化制智程度需求越来越高,数字钥匙作为汽车新型钥匙系统,已经被国内各大汽车主机厂应用。

[0003] 但是,在当下使用数字钥匙的场景下,由于缺乏对用户或设备的进行有效身份认证的步骤,导致用户和车辆处于不安全状态下,比如:可能会引起用户信息的泄露,严重的情况下会危及用户的生命安全,使得用户体验差、推广应用困难,因此,数字钥匙的使用和发展,亟需一种更安全认证方式。

发明内容

[0004] 本发明提供一种汽车数字钥匙管理方法、系统、设备及存储介质,解决的技术问题是,现有技术中的汽车数字钥匙的安全性能差,导致用户体验差、推广应用困难。

[0005] 为解决以上技术问题,本发明提供了一种汽车数字钥匙管理方法、系统、设备及存储介质。

[0006] 第一方面,本发明提供了一种汽车数字钥匙管理方法,所述方法包括以下步骤:

[0007] 当数字钥匙与车辆建立连接时,对车辆进行信息识别,得到车辆识别结果;

[0008] 根据车辆识别结果发送唤醒请求,并根据所述唤醒请求获取钥匙识别码;

[0009] 采集并识别用户的生物特征数据,判断所述生物特征数据是否与所述钥匙识别码和所述车辆识别结果同时匹配,得到匹配结果;

[0010] 若匹配结果为是,则身份识别成功,控制汽车解锁;

[0011] 若匹配结果为否,则身份识别失败,并发送提醒信息至用户终端。

[0012] 在进一步的实施方案中,所述根据车辆识别结果发送唤醒请求的步骤,具体包括:

[0013] 根据车辆识别结果获取车辆标识数据,并将所述车辆标识数据输入预先训练好的车辆识别模型,得到车辆置信度;

[0014] 在所述车辆置信度大于预设的第一置信度且小于预设的第二置信度时,识别该车辆为匹配车辆,并发送唤醒请求至所述钥匙识别模块;

[0015] 在所述车辆置信度小于第一置信度或大于第二置信度时,识别为非匹配车辆,并发送提醒信息至用户终端;

[0016] 其中,所述车辆识别模型为长短期记忆循环神经网络。

[0017] 在进一步的实施方案中,所述判断所述生物特征数据是否与所述钥匙识别码和所述车辆识别结果同时匹配,得到匹配结果的步骤包括:

[0018] 根据所述钥匙识别码获取对应的第一特征向量;

[0019] 根据所述车辆识别结果获取车辆识别码,并根据所述车辆识别码获取对应的第二

特征向量；

[0020] 根据所述生物特征数据获取对应的第三特征向量；

[0021] 将第一特征向量、第二特征向量分别与第三特征向量进行匹配,对用户的身份进行验证,得到匹配结果。

[0022] 在进一步的实施方案中,所述方法还包括:

[0023] 当身份识别失败时,检测用户的生物特征数据是否为新用户;

[0024] 在检测到用户的生物特征数据为新用户时,发送授权请求至用户终端;

[0025] 所述用户终端根据所述授权请求获取授权管理信息,同时验证所述授权管理信息中的数字签名,若验证通过,则根据所述授权管理信息确定授权范围信息和授权使用信息;

[0026] 根据所述授权范围信息和授权使用信息生成用户授权码;

[0027] 根据所述用户授权码控制汽车解锁。

[0028] 在进一步的实施方案中,所述生物特征数据为以下一种或多种的组合:面部特征数据、指纹特征数据、虹膜特征数据和音色特征数据。

[0029] 在进一步的实施方案中,所述数字钥匙包括智能手机、带有NFC功能的可穿戴设备。

[0030] 第二方面,本发明提供了一种汽车数字钥匙管理系统,所述系统包括数字钥匙系统和用户终端,所述数字钥匙系统包括车辆识别模块、钥匙识别模块以及身份匹配模块;

[0031] 所述车辆识别模块,用于当数字钥匙与车辆建立连接时,进行车辆信息识别,得到车辆识别结果;

[0032] 所述钥匙识别模块,用于根据车辆识别结果发送唤醒请求,并根据所述唤醒请求获取钥匙识别码;

[0033] 所述身份匹配模块,用于采集并识别得到用户的生物特征数据,并判断所述生物特征数据是否与所述钥匙识别码和预先存储的原始生物特征同时匹配,得到身份匹配结果,若身份匹配结果为同时匹配,则身份识别成功,控制汽车解锁;若身份匹配结果为不同时匹配,则身份识别失败,并发送提醒信息至用户终端。

[0034] 在进一步的实施方案中,所述系统还包括:

[0035] 身份检测模块,用于当身份识别失败时,检测用户的生物特征数据是否为新用户;

[0036] 授权请求模块,用于在检测到用户的生物特征数据为新用户时,发送授权请求至用户终端,所述用户终端根据所述授权请求获取授权管理信息,同时验证所述授权管理信息中的数字签名,若验证通过,则根据所述授权管理信息确定授权范围信息和授权使用信息;还用于根据所述授权范围信息和授权使用信息生成用户授权码,根据所述用户授权码控制汽车解锁。

[0037] 第三方面,本发明还提供了一种计算机设备,包括处理器和存储器,所述处理器与所述存储器相连,所述存储器用于存储计算机程序,所述处理器用于执行所述存储器中存储的计算机程序,以使得所述计算机设备执行实现上述方法的步骤。

[0038] 第四方面,本发明还提供了一种计算机可读存储介质,所述计算机可读存储介质中存储有计算机程序,所述计算机程序被处理器执行时实现上述方法的步骤。

[0039] 本发明提供了一种汽车数字钥匙管理方法、系统、设备及存储介质,通过所述方法,通过将用户的生物特征数据与车辆识别结果和钥匙识别码进行匹配,可以确保数字钥

匙解锁请求被经过身份验证的用户批准,进一步保证了数字钥匙的安全性。与现有技术相比,该方法能够实现非接触式解锁汽车,车主无需触碰车门即可解锁或者锁定车辆,更加方便用户的便利性;另外,本申请可通过在用户终端进行授权,使得车主与家人或者朋友共享车辆变得更加容易;同时,本发明实现了数字钥匙与汽车的互联协作,取代了传统意义上的物理钥匙,提高了用户体验。

附图说明

[0040] 图1是本发明实施例提供的一种汽车数字钥匙管理方法流程示意图;

[0041] 图2是本发明实施例提供的一种汽车数字钥匙管理系统框图;

[0042] 图3是本发明实施例提供的计算机设备的结构示意图。

具体实施方式

[0043] 下面结合附图具体阐明本发明的实施方式,实施例的给出仅仅是为了说明目的,并不能理解为对本发明的限定,包括附图仅供参考和说明使用,不构成对本发明专利保护范围的限制,因为在不脱离本发明精神和范围基础上,可以对本发明进行许多改变。

[0044] 针对现有技术中的汽车数字钥匙的安全性能差,导致用户体验差、推广应用困难的问题,本发明实施例提供了一种汽车数字钥匙管理方法、系统、设备及存储介质,如图1所示,本实施例提供的一种汽车数字钥匙管理方法,包括以下步骤:

[0045] S1. 当数字钥匙与车辆建立连接时,对车辆进行信息识别,得到车辆识别结果。

[0046] 在一个实施例中,所述数字钥匙包括智能手机以及带有蓝牙或NFC功能的可穿戴设备,其中,所述带有NFC功能的可穿戴设备包括智能卡、智能手表、以及智能手环。

[0047] 在本实施例中,当数字钥匙与车辆建立连接时,车辆将预先存储的车辆信息通过有线或无线连接方式发送至数字钥匙,以通过数字钥匙对车辆进行识别,从而判断数字钥匙与该车辆是否配对,其中,所述无线连接方式包括蓝牙通信、UWB通讯和NFC通讯。

[0048] S2. 根据车辆识别结果发送唤醒请求,并根据所述唤醒请求获取钥匙识别码。

[0049] 在一个实施例中,所述根据车辆识别结果发送唤醒请求的步骤,具体包括:

[0050] 根据车辆识别结果获取车辆标识数据,并将所述车辆标识数据输入预先训练好的车辆识别模型,得到车辆置信度;

[0051] 在所述车辆置信度大于预设的第一置信度且小于预设的第二置信度时,识别该车辆为匹配车辆,并发送唤醒请求至所述钥匙识别模块;

[0052] 在所述车辆置信度小于第一置信度或大于第二置信度时,识别为非匹配车辆,并发送提醒信息至用户终端;

[0053] 在本实施例中,所述车辆识别模型为长短期记忆循环神经网络,本实施例利用长短期记忆循环神经网络对所述车辆标识数据进行处理,获取预设数量的隐藏向量,将所述预设数量的隐藏向量代入至sigmoid函数中,得到车辆置信度,所述车辆置信度在0至1之间。

[0054] S3. 采集并识别用户的生物特征数据,判断所述生物特征数据是否与所述钥匙识别码和所述车辆识别结果同时匹配,得到匹配结果;若匹配结果为是,则身份识别成功,控制汽车解锁;若匹配结果为否,则身份识别失败,并发送提醒信息至用户终端。

[0055] 在一个实施例中,所述判断所述生物特征数据是否与所述钥匙识别码和所述车辆识别结果同时匹配,得到匹配结果的步骤包括:

[0056] 根据所述钥匙识别码获取对应的第一特征向量;

[0057] 根据所述车辆识别结果获取车辆识别码,并根据所述车辆识别码获取对应的第二特征向量;

[0058] 根据所述生物特征数据获取对应的第三特征向量;

[0059] 将第一特征向量、第二特征向量分别与第三特征向量进行匹配,对用户的身份进行验证,得到匹配结果。

[0060] 在一个实施例中,所述生物特征数据为以下一种或多种的组合:面部特征数据、指纹特征数据、虹膜特征数据和音色特征数据。

[0061] 在一个实施例中,本实施例提供的一种汽车数字钥匙管理方法,还包括:

[0062] 当身份识别失败时,检测用户的生物特征数据是否为新用户;

[0063] 在检测到用户的生物特征数据为新用户时,发送授权请求至用户终端;

[0064] 所述用户终端根据所述授权请求获取授权管理信息,同时验证所述授权管理信息中的数字签名,若验证通过,则根据所述授权管理信息确定授权范围信息和授权使用信息;

[0065] 根据所述授权范围信息和授权使用信息生成用户授权码;

[0066] 根据所述用户授权码控制汽车解锁。

[0067] 在发送授权请求至用户终端之前,本实施例还需对所述授权请求进行数字签名,所述数字签名可通过RSA数字签名算法和DSA数字签名算法实现,其中,所述DSA (Digital Signature Algorithm,数字签名算法,用作数字签名标准的一部分),它是另一种公开密钥算法,它不能用作加密,只用作数字签名。DSA使用公开密钥,为接受者验证数据的完整性和数据发送者的身份,需要说明的是,本领域技术人员可根据具体实施情况调整数字签名算法。

[0068] 在本实施例中,所述授权范围信息包括授权地址,所述授权使用信息包括授权权限、授权期限和权限使用方法;其中,所述授权权限包括车窗控制权限、车门控制权限、后备箱控制权限、多媒体控制权限、车辆驾驶权限中的一种或多种组合。

[0069] 本实施例提供的一种汽车数字钥匙管理方法,通过将用户的生物特征数据与车辆识别结果和钥匙识别码进行匹配,进一步保障了数字钥匙的安全性,降低车辆被盗的风险;本实施例提供的方法能够使车主通过智能手机或者可穿戴设备实现解锁汽车,无须实时携带物理钥匙,且本实施例能够远程进行钥匙授权,使得与他人共享车辆变得更加容易,大大提高了用车的便利性和安全性,即使数字钥匙丢失,也无需担心车辆被盗。

[0070] 需要说明的是,上述各过程的序号的大小并不意味着执行顺序的先后,各过程的执行顺序应以其功能和内在逻辑确定,而不对本申请实施例的实施过程构成任何限定。

[0071] 在一个实施例中,如图2所示,本实施例提供了一种汽车数字钥匙管理系统,所述系统包括:数字钥匙系统和用户终端,所述数字钥匙系统包括车辆识别模块11、钥匙识别模块12以及身份匹配模块13。

[0072] 在本实施例中,所述车辆识别模块11,用于当数字钥匙与车辆建立连接时,进行车辆信息识别,得到车辆识别结果。

[0073] 所述钥匙识别模块12,用于根据车辆识别结果发送唤醒请求,并根据所述唤醒请

求获取钥匙识别码。

[0074] 所述身份匹配模块13,用于采集并识别得到用户的生物特征数据,并判断所述生物特征数据是否与所述钥匙识别码和预先存储的原始生物特征同时匹配,得到身份匹配结果,若身份匹配结果为同时匹配,则身份识别成功,控制汽车解锁;若身份匹配结果为不同时匹配,则身份识别失败,并发送提醒信息至用户终端。

[0075] 在一个实施例中,所述系统还包括身份检测模块14和授权请求模块15。

[0076] 所述身份检测模块14,用于当身份识别失败时,检测用户的生物特征数据是否为新用户。

[0077] 所述授权请求模块15,用于在检测到用户的生物特征数据为新用户时,发送授权请求至用户终端,所述用户终端根据所述授权请求获取授权管理信息,同时验证所述授权管理信息中的数字签名,若验证通过,则根据所述授权管理信息确定授权范围信息和授权使用信息;还用于根据所述授权范围信息和授权使用信息生成用户授权码,根据所述用户授权码控制汽车解锁。

[0078] 关于一种汽车数字钥匙管理系统的具体限定可以参见上述对于一种汽车数字钥匙管理方法的限定,此处不再赘述。本领域普通技术人员可以意识到,结合本申请所公开的实施例描述的各个模块和步骤,能够以硬件、软件或者两者结合来实现。这些功能究竟以硬件还是软件方式来执行,取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用使用不同方法来实现所描述的功能,但是这种实现不应认为超出本申请的范围。

[0079] 与现有技术相比,本申请提供的一种汽车数字钥匙管理系统,通过车辆识别模块、钥匙识别模块、身份匹配模块、身份检测模块以及授权请求模块,解决了现有技术中的汽车数字钥匙的安全性能差,导致用户体验差、推广应用困难的问题,实现了通过数字钥匙即可解锁或启动汽车,同时能够有效进行权限管理,保护数据安全的技术效果,本实施例提供的系统通过通信连接实现了对车辆的控制,无需实时携带实体车钥匙;在本实施例中,数字钥匙作为虚拟钥匙,不仅方便用户使用,也能更好地实现智能终端与汽车的互联协作。

[0080] 图3是本发明实施例提供的一种计算机设备,包括存储器、处理器和收发器,它们之间通过总线连接;存储器用于存储一组计算机程序指令和数据,并可以将存储的数据传输给处理器,处理器可以执行存储器存储的程序指令,以执行上述方法的步骤。

[0081] 其中,存储器可以包括易失性存储器或非易失性存储器,或可包括易失性和非易失性存储器两者;处理器可以是中央处理器、微处理器、特定应用集成电路、可编程逻辑器件或其组合。通过示例性但不是限制性说明,上述可编程逻辑器件可以是复杂可编程逻辑器件、现场可编程逻辑门阵列、通用阵列逻辑或其任意组合。

[0082] 另外,存储器可以是物理上独立的单元,也可以与处理器集成在一起。

[0083] 本领域普通技术人员可以理解,图3中示出的结构,仅仅是与本申请方案相关的部分结构的框图,并不构成对本申请方案所应用于其上的计算机设备的限定,具体的计算机设备可以包括比图中所示更多或更少的部件,或者组合某些部件,或者具有相同的部件布置。

[0084] 在一个实施例中,提供了一种计算机可读存储介质,其上存储有计算机程序,计算机程序被处理器执行时实现上述方法的步骤。

[0085] 本发明实施例提供一种汽车数字钥匙管理方法、系统、计算机设备及存储介质，其一种汽车数字钥匙管理方法通过将车辆信息、钥匙标识码以及用户生物特征数据结合判断是否启动车辆，同时通过对车辆进行远程授权控制，可实现与多人共享车辆，适用范围广，且能够提高汽车无钥匙启动的可靠性，从而改善了用户的使用体验，更有利于提高推广效果；本实施例提供的汽车启动方法，可以使汽车的启动更便捷，降低汽车被盗的可能性。

[0086] 在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如SSD）等。

[0087] 本领域技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于计算机可读取存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。

[0088] 以上所述实施例仅表达了本申请的几种优选实施方式，其描述较为具体和详细，但并不能因此而理解为对发明专利范围的限制。应当指出的是，对于本技术领域的普通技术人员来说，在不脱离本发明技术原理的前提下，还可以做出若干改进和替换，这些改进和替换也应视为本申请的保护范围。因此，本申请专利的保护范围应以所述权利要求的保护范围为准。

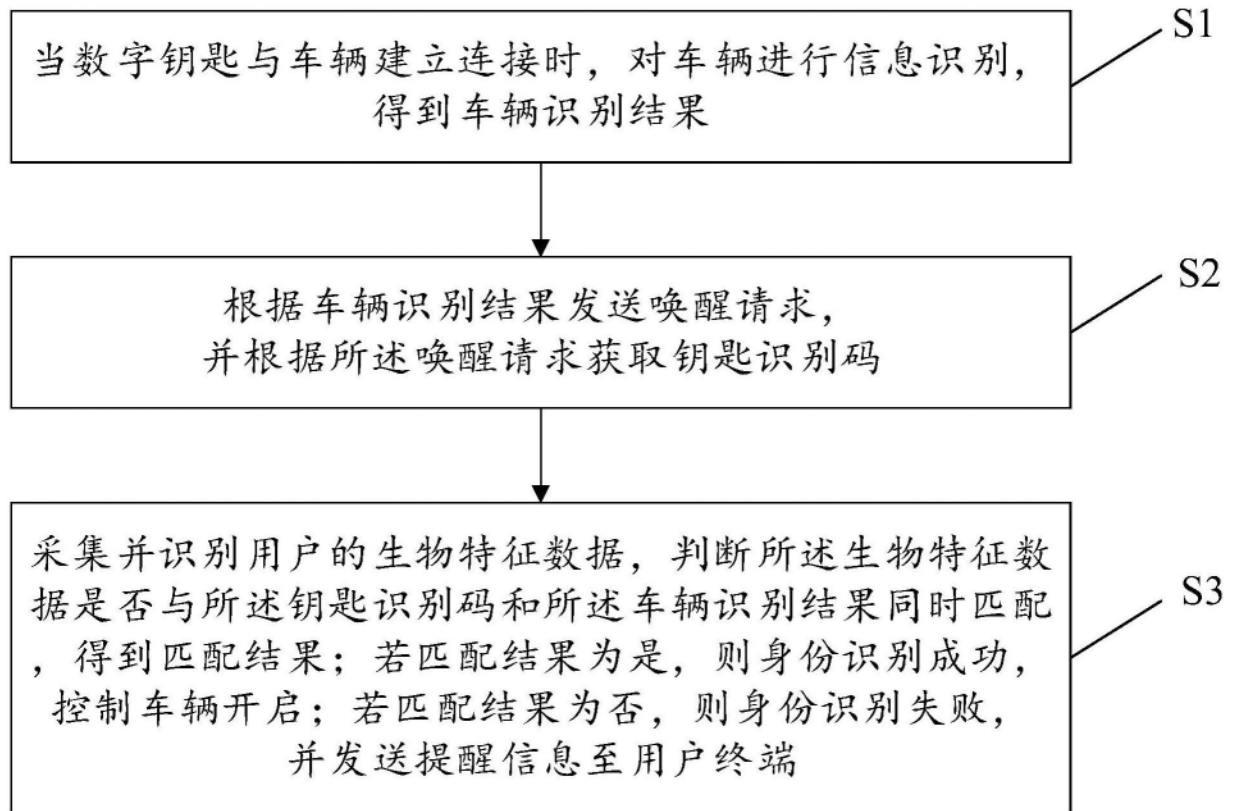


图1

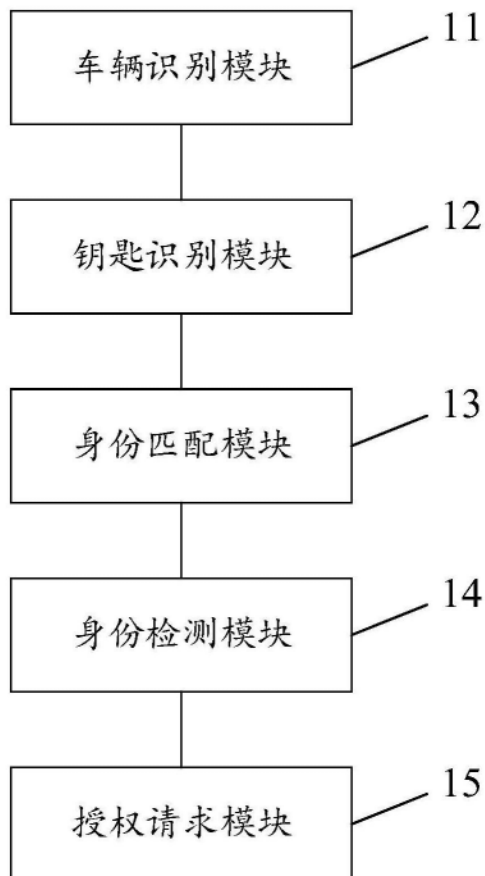


图2

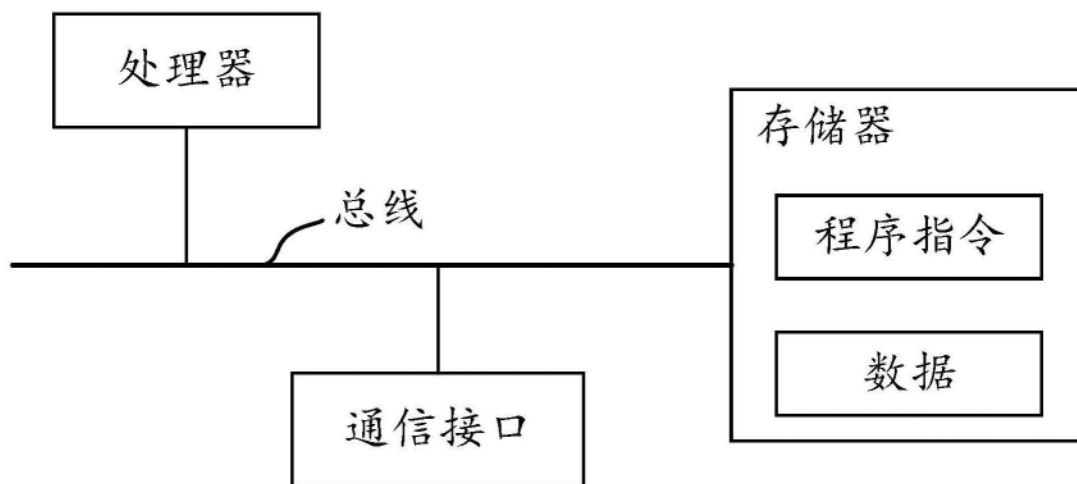


图3