



(12)发明专利申请

(10)申请公布号 CN 111508110 A

(43)申请公布日 2020.08.07

(21)申请号 202010282769.2

(22)申请日 2020.04.12

(71)申请人 广州通达汽车电气股份有限公司
地址 510540 广东省广州市白云区北太路
1633号广州民营科技园科盛路8号配
套服务大楼605-3房

(72)发明人 邢映彪 张远山 林虎 高志刚

(74)专利代理机构 北京权智天下知识产权代理
事务所(普通合伙) 11638
代理人 王新爱

(51)Int.Cl.
G07C 9/00(2020.01)
H04L 29/06(2006.01)
H04L 29/08(2006.01)

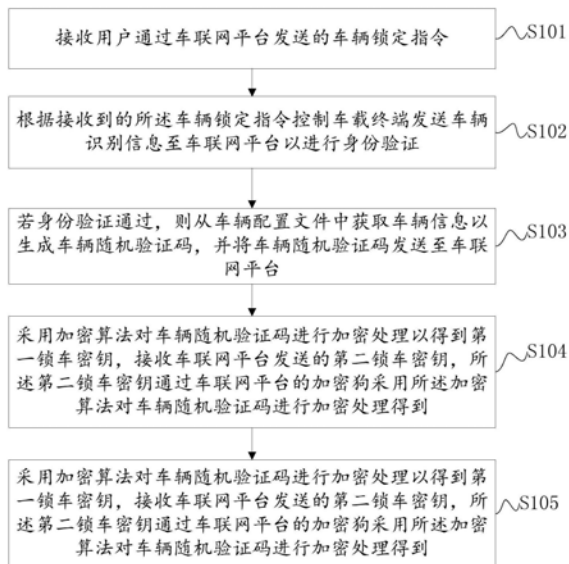
权利要求书2页 说明书8页 附图3页

(54)发明名称

一种实现车辆远程锁定的方法及装置

(57)摘要

本申请实施例公开了一种实现车辆远程锁定的方法及装置。本申请实施例提供的技术方案,通过在车载终端与车联网平台采用相同的加密方式对车辆随机验证码进行加密,进而在车载终端处对两者得到的锁车密钥进行验证,这样不仅解决了发送平台以及被锁车辆的身份信息,也解决了锁车指令在传输过程中存在的被篡改的问题,使得远程锁车更加安全可靠。采用加密狗技术并不影响锁车处理时间,通过本申请实施例的方案使得整个锁车处理时长相对于现有锁车技术锁车处理时长减少了2-3秒。



1. 一种实现车辆远程锁定的方法,其特征在于,包括:

接收用户通过车联网平台发送的车辆锁定指令;

根据接收到的所述车辆锁定指令控制车载终端发送车辆识别信息至车联网平台以进行身份验证;

若身份验证通过,则从车辆配置文件中获取车辆信息以生成车辆随机验证码,并将车辆随机验证码发送至车联网平台;

采用加密算法对车辆随机验证码进行加密处理以得到第一锁车密钥,接收车联网平台发送的第二锁车密钥,所述第二锁车密钥通过车联网平台的加密狗采用所述加密算法对车辆随机验证码进行加密处理得到;

判断所述第一锁车密钥与所述第二锁车密钥是否一致,如果验证一致,则向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作。

2. 根据权利要求1所述的实现车辆远程锁定的方法,其特征在于,在所述向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作之后,还包括:

接收发动机ECU发送的锁车成功信息,发送锁车成功信息至车联网平台以更新车联网平台中对应车辆的状态信息;

根据锁车成功信息控制车辆仪表显示车辆锁定状态。

3. 根据权利要求1所述的实现车辆远程锁定的方法,其特征在于,所述用户通过车联网平台发送的车辆锁定指令,包括:

用户通过移动终端发送车辆锁定指令至车联网平台以使得车联网平台向车载终端发送车辆锁定指令。

4. 根据权利要求1所述的实现车辆远程锁定的方法,其特征在于,所述车辆锁定操作包括:

控制关闭发送机操作、限制发动机转速操作和控制发动机熄火操作中的一种或多种。

5. 根据权利要求1-4中任意一项所述的实现车辆远程锁定的方法,其特征在于,所述加密算法包括MD5信息摘要算法,所述发动机ECU与车载终端之间通过CAN总线进行数据传输。

6. 根据权利要求1所述的实现车辆远程锁定的方法,其特征在于,所述车辆信息包括时间字串信息、终端号字串信息、车辆识别号信息和防重放攻击字串信息;

所述从车辆配置文件中获取车辆信息以生成车辆随机验证码,包括:

从车辆配置文件中获取时间字串信息、终端号字串信息、车辆识别号信息和防重放攻击字串信息,并对时间字串信息、终端号字串信息、车辆识别号信息和防重放攻击字串信息进行不可逆运算以生成车辆随机验证码。

7. 根据权利要求1所述的实现车辆远程锁定的方法,其特征在于,所述车辆识别信息包括VIN号和PIN码;

所述控制车载终端发送车辆识别信息至车联网平台以进行身份验证,包括:

控制车载终端发送VIN号和PIN码至车联网平台进行验证,当验证通过后,车联网平台获取与车载终端对应的自定义序列号,并将自定义序列号发送至车载终端;

判断接收到的自定义序列号是否正确,如果是,则执行所述从车辆配置文件中获取车

辆信息以生成车辆随机验证码。

8. 一种实现车辆远程锁定的装置,其特征在於,包括:

接收模块:用于接收用户通过车联网平台发送的车辆锁定指令;

发送模块:用于根据接收到的所述车辆锁定指令控制车载终端发送车辆识别信息至车联网平台以进行身份验证;

数据获取模块:用于若身份验证通过,则从车辆配置文件中获取车辆信息以生成车辆随机验证码,并将车辆随机验证码发送至车联网平台;

加密模块:用于采用加密算法对车辆随机验证码进行加密处理以得到第一锁车密钥,接收车联网平台发送的第二锁车密钥,所述第二锁车密钥通过车联网平台的加密狗采用所述加密算法对车辆随机验证码进行加密处理得到;

判断模块:用于判断所述第一锁车密钥与所述第二锁车密钥是否一致,如果验证一致,则向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作。

9. 一种电子设备,其特征在於,包括:

存储器以及一个或多个处理器;

所述存储器,用于存储一个或多个程序;

当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如权利要求1-7任一所述的实现车辆远程锁定的方法。

10. 一种包含计算机可执行指令的存储介质,其特征在於,所述计算机可执行指令在由计算机处理器执行时用于执行如权利要求1-7任一所述的实现车辆远程锁定的方法。

一种实现车辆远程锁定的方法及装置

技术领域

[0001] 本申请实施例涉及汽车技术领域,尤其涉及一种实现车辆远程锁定的方法和装置。

背景技术

[0002] 目前,进行车辆上锁的方式有如下两种方式:第一种是传统的直接通过钥匙进行上锁的方式;第二种是远程上锁的方式。并且虽然无线网络的发展,远程锁车的方式越来越普及,由于远程锁车有着无比的便利,高效,快速,经济等优越性而被广泛应用。但是远程锁车会存在如下问题,因为其采用无线通信的方式,所以会涉及到网络监听等黑客技术窃取方面的问题,容易使车辆产生安全性问题。因此,设计一种能够保证车辆安全的方案成为本领域技术人员亟待解决的技术问题。

发明内容

[0003] 本申请实施例提供一种实现车辆远程锁定的方法及装置,其通过在车载终端与车联网平台采用相同的加密方式对车辆随机验证码进行加密,进而在车载终端处对两者得到的锁车密钥进行验证,这样不仅解决了发送平台以及被锁车辆的身份信息,也解决了锁车指令在传输过程中存在的被篡改的问题,使得远程锁车更加安全可靠。

[0004] 在第一方面,本申请实施例提供了一种实现车辆远程锁定的方法,包括:

[0005] 接收用户通过车联网平台发送的车辆锁定指令;

[0006] 根据接收到的车辆锁定指令控制车载终端发送车辆识别信息至车联网平台以进行身份验证;

[0007] 若身份验证通过,则从车辆配置文件中获取车辆信息以生成车辆随机验证码,并将车辆随机验证码发送至车联网平台;

[0008] 采用加密算法对车辆随机验证码进行加密处理以得到第一锁车密钥,接收车联网平台发送的第二锁车密钥,第二锁车密钥通过车联网平台的加密狗采用加密算法对车辆随机验证码进行加密处理得到;

[0009] 判断第一锁车密钥与第二锁车密钥是否一致,如果验证一致,则向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作。

[0010] 更为优选的,在向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作之后,还包括:

[0011] 接收发动机ECU发送的锁车成功信息,发送锁车成功信息至车联网平台以更新车联网平台中对应车辆的状态信息;

[0012] 根据锁车成功信息控制车辆仪表显示车辆锁定状态。

[0013] 更为优选的,用户通过车联网平台发送的车辆锁定指令,包括:

[0014] 用户通过移动终端发送车辆锁定指令至车联网平台以使得车联网平台向车载终端发送车辆锁定指令。

- [0015] 更为优选的,车辆锁定操作包括:
- [0016] 控制关闭发送机操作、限制发动机转速操作和控制发动机熄火操作中的一种或多种。
- [0017] 更为优选的,加密算法包括MD5信息摘要算法,发动机ECU与车载终端之间通过CAN总线进行数据传输。
- [0018] 更为优选的,车辆信息包括时间字符串信息、终端号字符串信息、车辆识别号信息和防重放攻击字符串信息;
- [0019] 从车辆配置文件中获取车辆信息以生成车辆随机验证码,包括:
- [0020] 从车辆配置文件中获取时间字符串信息、终端号字符串信息、车辆识别号信息和防重放攻击字符串信息,并对时间字符串信息、终端号字符串信息、车辆识别号信息和防重放攻击字符串信息进行不可逆运算以生成车辆随机验证码。
- [0021] 更为优选的,车辆识别信息包括VIN号和PIN码;
- [0022] 控制车载终端发送车辆识别信息至车联网平台以进行身份验证,包括:
- [0023] 控制车载终端发送VIN号和PIN码至车联网平台进行验证,当验证通过后,车联网平台获取与车载终端对应的自定义序列号,并将自定义序列号发送至车载终端;
- [0024] 判断接收到的自定义序列号是否正确,如果是,则执行从车辆配置文件中获取车辆信息以生成车辆随机验证码。
- [0025] 在第二方面,本申请实施例提供了一种实现车辆远程锁定的装置,包括:
- [0026] 接收模块:用于接收用户通过车联网平台发送的车辆锁定指令;
- [0027] 发送模块:用于根据接收到的车辆锁定指令控制车载终端发送车辆识别信息至车联网平台以进行身份验证;
- [0028] 数据获取模块:用于若身份验证通过,则从车辆配置文件中获取车辆信息以生成车辆随机验证码,并将车辆随机验证码发送至车联网平台;
- [0029] 加密模块:用于采用加密算法对车辆随机验证码进行加密处理以得到第一锁车密钥,接收车联网平台发送的第二锁车密钥,第二锁车密钥通过车联网平台的加密狗采用加密算法对车辆随机验证码进行加密处理得到;
- [0030] 判断模块:用于判断第一锁车密钥与第二锁车密钥是否一致,如果验证一致,则向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作。
- [0031] 在第三方面,本申请实施例提供了一种电子设备,包括:
- [0032] 存储器以及一个或多个处理器;
- [0033] 存储器,用于存储一个或多个程序;
- [0034] 当一个或多个程序被一个或多个处理器执行,使得一个或多个处理器实现如第一方面的实现车辆远程锁定的方法。
- [0035] 在第四方面,本申请实施例提供了一种包含计算机可执行指令的存储介质,计算机可执行指令在由计算机处理器执行时用于执行如第一方面的实现车辆远程锁定的方法。
- [0036] 本申请实施例通过在车载终端与车联网平台采用相同的加密方式对车辆随机验证码进行加密,进而在车载终端处对两者得到的锁车密钥进行验证,这样不仅解决了发送平台以及被锁车辆的身份信息,也解决了锁车指令在传输过程中存在的被篡改的问题,使

得远程锁车更加安全可靠。采用加密狗技术并不影响锁车处理时间,通过本申请实施例的方案使得整个锁车处理时长相对于现有锁车技术锁车处理时长减少了2-3秒。

附图说明

- [0037] 图1是本申请实施例提供的一种实现车辆远程锁定的方法的流程图;
- [0038] 图2是本申请实施例提供的另一种实现车辆远程锁定的方法的流程图;
- [0039] 图3是本申请实施例提供的一种实现车辆远程锁定的装置的结构示意图;
- [0040] 图4是本申请实施例提供的一种电子设备的结构示意图。

具体实施方式

[0041] 为了使本申请的目的、技术方案和优点更加清楚,下面结合附图对本申请具体实施例作进一步的详细描述。可以理解的是,此处所描述的具体实施例仅仅用于解释本申请,而非对本申请的限定。另外还需要说明的是,为了便于描述,附图中仅示出了与本申请相关的部分而非全部内容。在更加详细地讨论示例性实施例之前应当提到的是,一些示例性实施例被描述成作为流程图描绘的处理或方法。虽然流程图将各项操作(或步骤)描述成顺序的处理,但是其中的许多操作可以被并行地、并发地或者同时实施。此外,各项操作的顺序可以被重新安排。当其操作完成时处理可以被终止,但是还可以具有未包括在附图中的附加步骤。处理可以对应于方法、函数、规程、子例程、子程序等等。

[0042] 本申请提供的实现车辆远程锁定的方法在车载终端与车联网平台采用相同的加密方式对车辆随机验证码进行加密,进而在车载终端处对两者得到的锁车密钥进行验证。相对于现有的远程解锁方案,本申请实施例的方案不仅解决了发送平台以及被锁车辆的身份信息,也解决了锁车指令在传输过程中存在的被篡改的问题,使得远程锁车更加安全可靠。

[0043] 图1给出了本申请实施例提供的一种实现车辆远程锁定的方法的流程图,本实施例中提供的实现车辆远程锁定的方法可以由实现车辆远程锁定的设备执行,该实现车辆远程锁定的设备可以通过软件和/或硬件的方式实现,该实现车辆远程锁定的设备可以是两个或多个物理实体构成,也可以是一个物理实体构成。一般而言,该实现车辆远程锁定的设备可以是电脑,手机,平板或车载终端等。

[0044] 下述以车载终端为执行实现车辆远程锁定的方法的设备为例,进行描述。参照图1,该实现车辆远程锁定的方法具体包括:

[0045] S101:接收用户通过车联网平台发送的车辆锁定指令。

[0046] 更为优选的,所述用户通过车联网平台发送的车辆锁定指令,包括:

[0047] 用户通过移动终端发送车辆锁定指令至车联网平台以使得车联网平台向车载终端发送车辆锁定指令。在本实施例中,用户的移动终端、车载终端、车联网平台均处于同一个网络系统中,其之间可以通过无线网络进行所有的信息指令的传输。当车辆使用者想对相应车辆进行锁定时,其需要通过其智能终端向车联网发送车辆锁定指令来验证其身份,当车辆使用者想要查看车辆的状态时,也可以直接在智能终端处链接到车联网平台来实现对车辆信息的查看。

[0048] S102:根据接收到的车辆锁定指令控制车载终端发送车辆识别信息至车联网平台

以进行身份验证。

[0049] 更为优选的,所述车辆识别信息包括VIN号和PIN码;

[0050] 所述控制车载终端发送车辆识别信息至车联网平台以进行身份验证,包括:

[0051] 控制车载终端发送VIN号和PIN码至车联网平台进行验证,当验证通过后,车联网平台获取与车载终端对应的自定义序列号,并将自定义序列号发送至车载终端。

[0052] 判断接收到的自定义序列号是否正确,如果是,则执行所述从车辆配置文件中获取车辆信息以生成车辆随机验证码。

[0053] 在本实施例中VIN号是车辆识别号码,是由一组由十七个英数组成,用于汽车上的一组独一无二的号码,可以识别汽车的生产商、引擎、底盘序号及其他性能等资料,通过上述号码可以识别对应的车辆。PIN号是个人识别密码,车载终端处拥有特定的PIN号能够标识其个人的身份,上述两种号码均是为了进行特定的身份识别,防止非法用户进行车辆控制。

[0054] 在车联网平台对车载终端的身份进行识别之后,车载终端也需要对车联网平台进行验证,通过这样的双向认证使得信息的传输更加的可靠。当车联网平台对车载终端的身份验证之后,会获取与车载终端相关的自定义序列号,并将获取的序列号返回给车载终端进行识别,以使得车载终端对车联网平台进行身份验证。

[0055] S103:若身份验证通过,则从车辆配置文件中获取车辆信息以生成车辆随机验证码,并将车辆随机验证码发送至车联网平台。

[0056] 更为优选的,所述车辆信息包括时间字串信息、终端号字串信息、车辆识别号信息和防重放攻击字串信息;

[0057] 所述从车辆配置文件中获取车辆信息以生成车辆随机验证码,包括:

[0058] 从车辆配置文件中获取时间字串信息、终端号字串信息、车辆识别号信息和防重放攻击字串信息,并对时间字串信息、终端号字串信息、车辆识别号信息和防重放攻击字串信息进行不可逆运算以生成车辆随机验证码。

[0059] 车载终端验证序列号正确后向车联网平台发送由时间字串、终端号信息字串、VIN号信息字串、防重放攻击字串组合在一起进行加密后得到的字串A;重放攻击又称重播攻击、回放攻击,是指攻击者发送一个目的主机已接收过的包,来达到欺骗系统的目的,主要用于身份认证过程,破坏认证的正确性。重放攻击可以由发起者,也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据,之后再把它重新发给认证服务器。为了防止黑客进行重放攻击,在进行车辆随机验证码获取时,在其中加入防重放攻击字串来提高信息识别的安全性。上述车辆随机验证码与车辆识别信息以及防重放攻击信息关联,通过这种信息关联使得验证码被攻克的可能性大大降低,进而提升控制的安全性。

[0060] S104:采用加密算法对车辆随机验证码进行加密处理以得到第一锁车密钥,接收车联网平台发送的第二锁车密钥,第二锁车密钥通过车联网平台的加密狗采用加密算法对车辆随机验证码进行加密处理得到。

[0061] 在本实施例中对车辆随机验证码进行加密时,车载终端与车联网平台的加密狗采用的加密算法一定要相同;这样是为了便于后续得到的密钥进行信息的比对。

[0062] 更为优选的,所述加密算法包括MD5信息摘要算法,所述发动机ECU与车载终端之

间通过CAN总线进行数据传输。MD5信息摘要算法是一种被广泛使用的密码散列函数,可以产生出一个128位(16字节)的散列值(hash value),用于确保信息传输完整一致。通过MD5算法可以知晓,两者的信息来源相同,因为如果在这个过程中,车辆随机验证码中间有一个字符改变了,那么最终得到的锁车密钥也会发生改变。因此,直接对计算得到的结果进行比对即可实现对车辆随机验证码进行比对验证。在本实施例中,除了采用MD5算法还可以采用其他不可逆算法来进行操作。

[0063] 具体的,在本步骤中,车联网平台的加密狗将根据车联网平台的数据证书对字串A进行不可逆运算得到字串B,并将字串B发送给车载终端。车载终端也同样的采用MD5算法对字串A进行不可逆运算。在本实施例中,字串A指的是车辆随机验证码,字串B指的是第二锁车密钥。在本实施例中,通过车联网平台以及车载终端分别采用MD5加密方法对随机验证码进行加密,并验证加密后得到的两个锁车密钥数字证书是否一致的方法来提升车辆远程控制的安全性和可靠性。

[0064] S105:判断第一锁车密钥与第二锁车密钥是否一致,如果验证一致,则向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作。

[0065] 当验证通过时,也即是加密后得到的锁车密钥是相同的,那么则可以说明发送锁车指令的是来自于车辆拥有者。

[0066] 更为优选的,所述车辆锁定操作包括:

[0067] 控制关闭发送机操作、限制发动机转速操作和控制发动机熄火操作中的一种或多种。在本实施例中,采用的是直接对发送机进行锁定的方式,使得发动机在处于锁定状态的时候不进行工作,这样无论是谁在这种情况下也无法开启车辆。

[0068] 图2是本申请实施例提供的另一种实现车辆远程锁定的方法的流程图,如图2所示,本申请实施例除了上述步骤之外,还包括:

[0069] S106:接收发动机ECU发送的锁车成功信息,发送锁车成功信息至车联网平台以更新车联网平台中对应车辆的状态信息。

[0070] 本步骤主要是为了更新车辆的状态信息,车联网平台是用于管理车辆的平台,其通过获取车辆的各种状态,然后与用户进行数据信息的交互,使得用户可以直接通过网络即可了解到自己车辆的状态,而不必到车辆现场去查看。因此,当发动机ECU完成锁车时,则发送相应的锁车成功信息至车联网平台以进行数据更新。

[0071] S107:根据锁车成功信息控制车辆仪表显示车辆锁定状态。

[0072] 除了在网络端进行车辆锁定显示之外,还需要在本地端进行车辆锁定显示。车载终端根据接收到的锁车成功信息来控制车辆仪表显示车辆的锁定状态,使得车主在车辆端时,能够直接通过读取仪表处的显示结果来进行车辆状态的读取。

[0073] 本申请实施例通过在车载终端与车联网平台采用相同的加密方式对车辆随机验证码进行加密,进而在车载终端处对两者得到的锁车密钥进行验证,这样不仅解决了发送平台以及被锁车辆的身份信息,也解决了锁车指令在传输过程中存在的被篡改的问题,使得远程锁车更加安全可靠。采用加密狗技术并不影响锁车处理时间,通过本申请实施例的方案使得整个锁车处理时长相对于现有锁车技术锁车处理时长减少了2-3秒。

[0074] 在上述实施例的基础上,图3为本申请实施例提供的一种实现车辆远程锁定的装

置的结构示意图。参考图3,本实施例提供的实现车辆远程锁定的装置具体包括:

[0075] 接收模块21:用于接收用户通过车联网平台发送的车辆锁定指令;

[0076] 发送模块22:用于根据接收到的车辆锁定指令控制车载终端发送车辆识别信息至车联网平台以进行身份验证;

[0077] 数据获取模块23:用于若身份验证通过,则从车辆配置文件中获取车辆信息以生成车辆随机验证码,并将车辆随机验证码发送至车联网平台;

[0078] 加密模块24:用于采用加密算法对车辆随机验证码进行加密处理以得到第一锁车密钥,接收车联网平台发送的第二锁车密钥,第二锁车密钥通过车联网平台的加密狗采用加密算法对车辆随机验证码进行加密处理得到;

[0079] 判断模块25:用于判断第一锁车密钥与第二锁车密钥是否一致,如果验证一致,则向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作。

[0080] 更为优选的,在判断模块25之后,还包括:

[0081] 第一锁定模块:用于接收发动机ECU发送的锁车成功信息,发送锁车成功信息至车联网平台以更新车联网平台中对应车辆的状态信息;

[0082] 第二锁定模块:根据锁车成功信息控制车辆仪表显示车辆锁定状态。

[0083] 本申请实施例通过在车载终端与车联网平台采用相同的加密方式对车辆随机验证码进行加密,进而在车载终端处对两者得到的锁车密钥进行验证,这样不仅解决了发送平台以及被锁车辆的身份信息,也解决了锁车指令在传输过程中存在的被篡改的问题,使得远程锁车更加安全可靠。

[0084] 本申请实施例提供的实现车辆远程锁定的装置可以用于执行上述实施例提供的实现车辆远程锁定的方法,具备相应的功能和有益效果。

[0085] 本申请实施例提供了一种电子设备的结构示意图,参照图4,该电子设备包括:处理器31、存储器32、通信模块33、输入装置34及输出装置35。该电子设备中处理器31的数量可以是一个或者多个,该电子设备中的存储器32的数量可以是一个或者多个。该电子设备的处理器31、存储器32、通信模块33、输入装置34及输出装置35可以通过总线或者其他方式连接。

[0086] 存储器32作为一种计算机可读存储介质,可用于存储软件程序、计算机可执行程序以及模块,如本申请任意实施例的实现车辆远程锁定的方法对应的程序指令/模块(例如,实现车辆远程锁定的装置中的接收模块21、发送模块22、数据获取模块23、加密模块24和判断模块25)。存储器32可主要包括存储程序区和存储数据区,其中,存储程序区可存储操作系统、至少一个功能所需的应用程序;存储数据区可存储根据设备的使用所创建的数据等。此外,存储器32可以包括高速随机存取存储器,还可以包括非易失性存储器,例如至少一个磁盘存储器件、闪存器件、或其他非易失性固态存储器件。在一些实例中,存储器32可进一步包括相对于处理器远程设置的存储器,这些远程存储器可以通过网络连接至设备。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

[0087] 通信模块33用于进行数据传输。

[0088] 处理器31通过运行存储在存储器32中的软件程序、指令以及模块,从而执行设备的各种功能应用以及数据处理,即实现上述的实现车辆远程锁定的方法。

[0089] 输入装置34可用于接收输入的数字或字符信息,以及产生与设备的用户设置以及功能控制有关的键信号输入。输出装置35可包括显示屏等显示设备。

[0090] 本申请实施例通过在车载终端与车联网平台采用相同的加密方式对车辆随机验证码进行加密,进而在车载终端处对两者得到的锁车密钥进行验证,这样不仅解决了发送平台以及被锁车辆的身份信息,也解决了锁车指令在传输过程中存在的被篡改的问题,使得远程锁车更加安全可靠。采用加密狗技术并不影响锁车处理时间,通过本申请实施例的方案使得整个锁车处理时长相对于现有锁车技术锁车处理时长减少了2-3秒。

[0091] 上述提供的电子设备可用于执行上述实施例提供的实现车辆远程锁定的方法,具备相应的功能和有益效果。

[0092] 本申请实施例还提供一种包含计算机可执行指令的存储介质,计算机可执行指令在由计算机处理器31执行时用于执行一种实现车辆远程锁定的方法,该实现车辆远程锁定的方法包括:

[0093] 接收用户通过车联网平台发送的车辆锁定指令;

[0094] 根据接收到的车辆锁定指令控制车载终端发送车辆识别信息至车联网平台以进行身份验证;

[0095] 若身份验证通过,则从车辆配置文件中获取车辆信息以生成车辆随机验证码,并将车辆随机验证码发送至车联网平台;

[0096] 采用加密算法对车辆随机验证码进行加密处理以得到第一锁车密钥,接收车联网平台发送的第二锁车密钥,第二锁车密钥通过车联网平台的加密狗采用加密算法对车辆随机验证码进行加密处理得到;

[0097] 判断第一锁车密钥与第二锁车密钥是否一致,如果验证一致,则向发送机ECU发出加密锁定指令以控制发送机ECU对接收到加密锁定指令进行解密进而实现车辆锁定操作。

[0098] 存储介质——任何的各种类型的存储器设备或存储设备。术语“存储介质”旨在包括:安装介质,例如CD-ROM、软盘或磁带装置;计算机系统存储器或随机存取存储器,诸如DRAM、DDR RAM、SRAM、EDO RAM,兰巴斯(Rambus)RAM等;非易失性存储器,诸如闪存、磁介质(例如硬盘或光存储);寄存器或其它相似类型的存储器元件等。存储介质可以还包括其它类型的存储器或其组合。另外,存储介质可以位于程序在其中被执行的第一计算机系统中,或者可以位于不同的第二计算机系统中,第二计算机系统通过网络(诸如因特网)连接到第一计算机系统。第二计算机系统可以提供程序指令给第一计算机用于执行。术语“存储介质”可以包括驻留在不同位置中(例如在通过网络连接的不同计算机系统中)的两个或更多存储介质。存储介质可以存储可由一个或多个处理器执行的程序指令(例如具体实现为计算机程序)。

[0099] 当然,本申请实施例所提供的一种包含计算机可执行指令的存储介质,其计算机可执行指令不限于如上的实现车辆远程锁定的方法,还可以执行本申请任意实施例所提供的实现车辆远程锁定的方法中的相关操作。

[0100] 上述实施例中提供的实现车辆远程锁定的装置、存储介质及电子设备可执行本申请任意实施例所提供的实现车辆远程锁定的方法,未在上述实施例中详尽描述的技术细节,可参见本申请任意实施例所提供的实现车辆远程锁定的方法。

[0101] 上述仅为本申请的较佳实施例及所运用的技术原理。本申请不限于这里的特定实

施例,对本领域技术人员来说能够进行的各种明显变化、重新调整及替代均不会脱离本申请的保护范围。因此,虽然通过以上实施例对本申请进行了较为详细的说明,但是本申请不仅仅限于以上实施例,在不脱离本申请构思的情况下,还可以包括更多其他等效实施例,而本申请的范围由权利要求的范围决定。

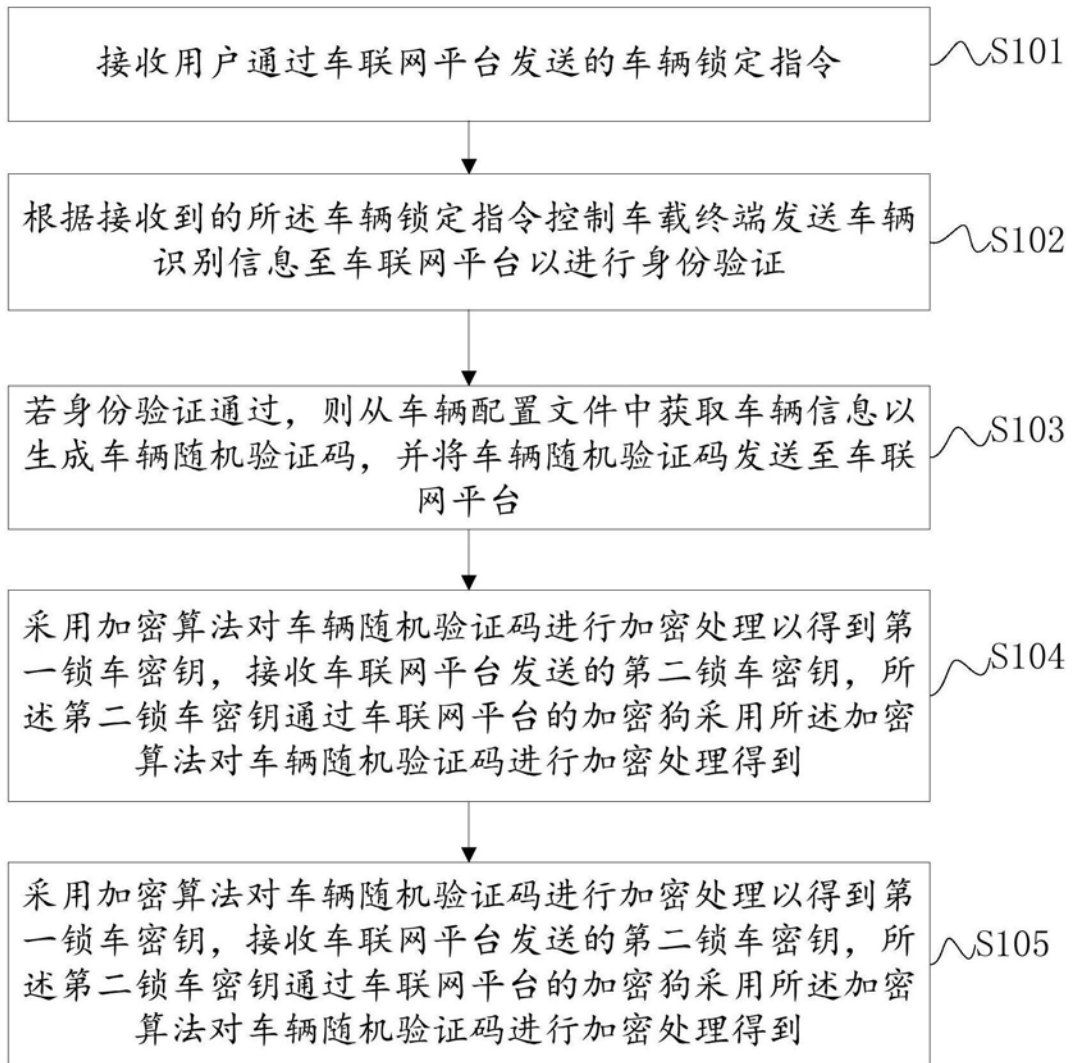


图1

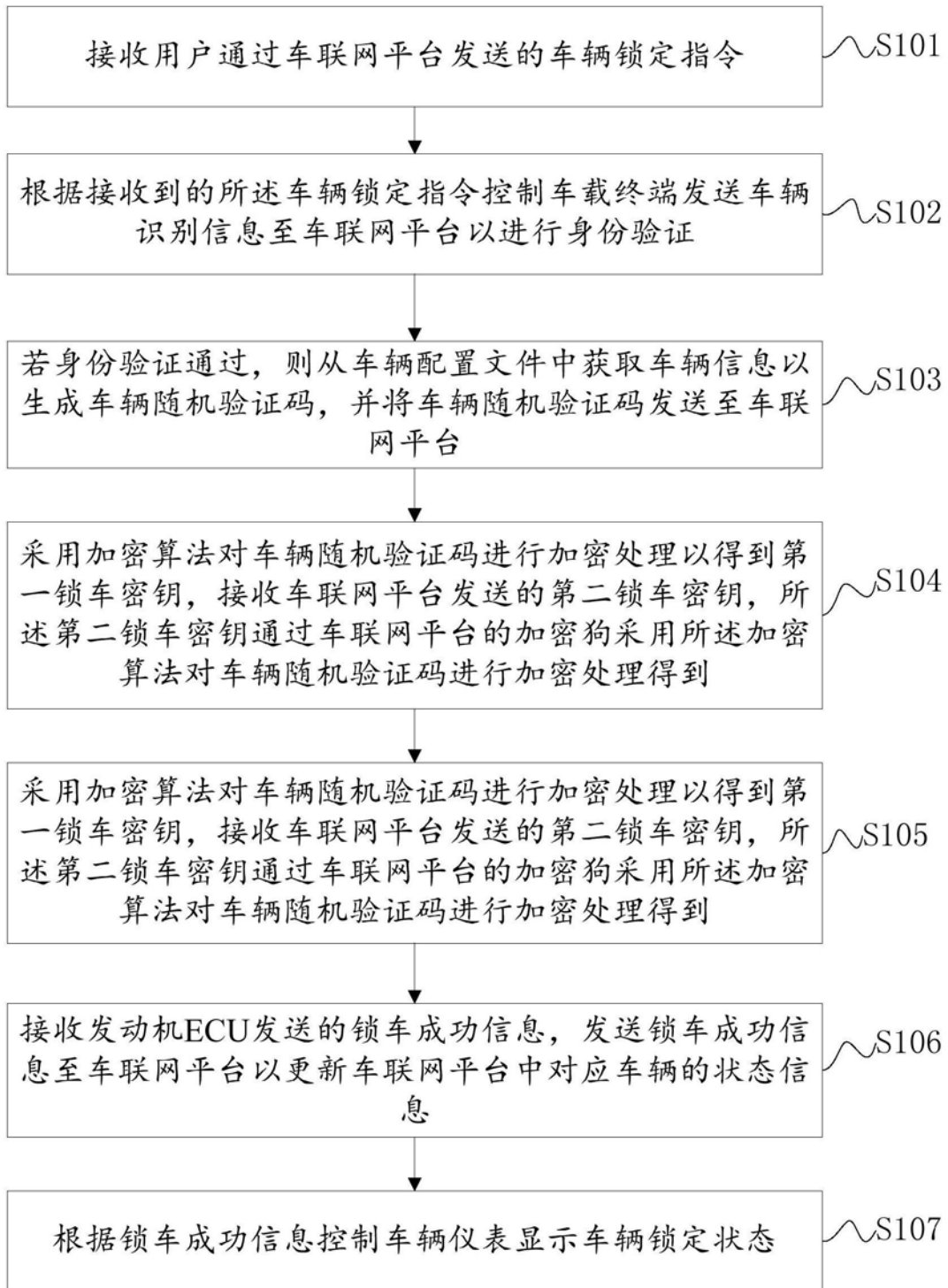


图2

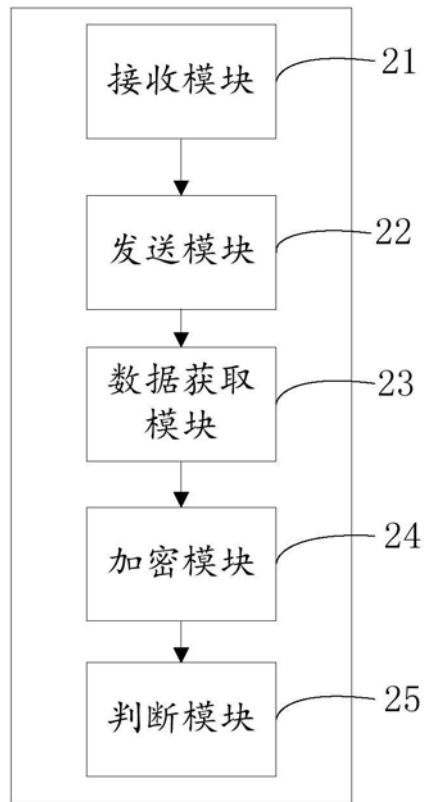


图3

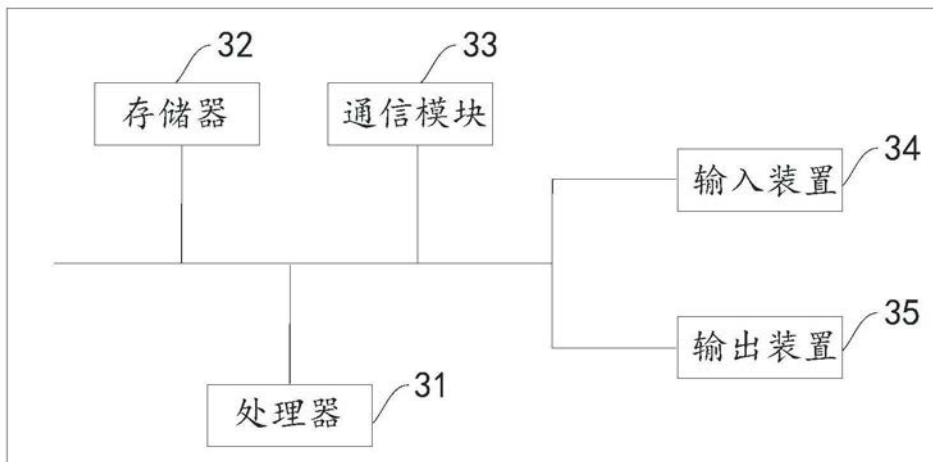


图4