



(12)发明专利申请

(10)申请公布号 CN 110059455 A  
(43)申请公布日 2019.07.26

(21)申请号 201910283828.5

(22)申请日 2019.04.09

(71)申请人 北京迈格威科技有限公司  
地址 100190 北京市海淀区科学院南路2号  
A座316-318

(72)发明人 马福鑫 曹志敏

(74)专利代理机构 北京钲霖知识产权代理有限  
公司 11722  
代理人 李志新 李静波

(51) Int. Cl.  
G06F 21/14(2013.01)

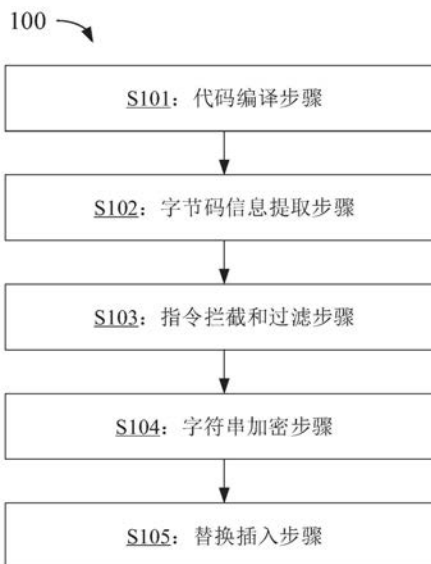
权利要求书1页 说明书5页 附图2页

(54)发明名称

代码加密方法、装置、电子设备和计算机可读存储介质

(57)摘要

本发明提供了代码加密方法、装置、电子设备和计算机可读存储介质。代码加密方法包括：对源代码进行编译，生成原始中间文件；提取原始中间文件中的字节码信息，其中，字节码信息包括一条或多条原始指令；拦截字节码信息中的一条或多条原始指令，根据预先获得的常量字符串的指令特征，对一条或多条原始指令进行过滤，获得一条或多条原始指令中包含指令特征的原始指令所对应的明文常量字符串；对明文常量字符串执行加密处理，获得加密常量字符串；利用加密常量字符串替换明文常量字符串，并且插入与加密处理相对应的解密处理的代码，获得经加密的中间文件。本发明实施例提高了应用程序的安全级别，提高了查找加密处理的效率。



CN 110059455 A

1. 一种代码加密方法,所述方法包括:
  - 代码编译步骤,对源代码进行编译,生成原始中间文件;
  - 字节码信息提取步骤,提取所述原始中间文件中的字节码信息,其中,所述字节码信息包括一条或多条原始指令;
  - 指令拦截和过滤步骤,拦截所述字节码信息中的所述一条或多条原始指令,根据预先获得的常量字符串的指令特征,对所述一条或多条原始指令进行过滤,获得所述一条或多条原始指令中包含所述指令特征的原始指令所对应的明文常量字符串;
  - 字符串加密步骤,对所述明文常量字符串执行加密处理,获得加密常量字符串;
  - 替换插入步骤,利用所述加密常量字符串替换所述明文常量字符串,并且插入与所述加密处理相对应的解密处理的代码,获得经加密的中间文件。
2. 根据权利要求1所述的方法,其中,所述指令特征包括加载常量指令特征。
3. 根据权利要求1所述的方法,其中,所述原始中间文件包括类文件。
4. 根据权利要求1所述的方法,其中,所述字节码信息提取步骤包括:
  - 利用字节码插件或者中间文件分解命令提取所述原始中间文件中的所述字节码信息。
5. 根据权利要求1所述的方法,其中,利用字节码操纵框架、字节码编辑类库和字节码工程库中的任一种执行所述字符串加密步骤和所述替换插入步骤。
6. 根据权利要求1所述的方法,其中,在中间文件初始化过程中执行所述字符串加密步骤和所述替换插入步骤。
7. 一种代码加密装置,所述装置包括:
  - 代码编译模块,配置用于对源代码进行编译,生成原始中间文件;
  - 字节码信息提取模块,配置用于提取所述原始中间文件中的字节码信息,其中,所述字节码信息包括一条或多条原始指令;
  - 指令拦截和过滤模块,配置用于拦截所述字节码信息中的所述一条或多条原始指令,根据预先获得的常量字符串的指令特征,对所述一条或多条原始指令进行过滤,获得所述一条或多条原始指令中包含所述指令特征的原始指令所对应的明文常量字符串;
  - 字符串加密模块,配置用于对所述明文常量字符串执行加密处理,获得加密常量字符串;
  - 替换插入模块,配置用于利用所述加密常量字符串代替所述明文常量字符串,并且插入与所述加密处理相对应的解密处理的代码,获得经加密的中间文件。
8. 一种电子设备,所述电子设备包括:
  - 存储器,用于存储指令;以及
  - 处理器,用于调用所述存储器存储的所述指令执行如权利要求1-6中任一项所述的方法。
9. 一种计算机可读存储介质,所述计算机可读存储介质存储有计算机可执行指令,所述计算机可执行指令在由处理器执行时,执行如权利要求1-6中任一项所述的方法。

## 代码加密方法、装置、电子设备和计算机可读存储介质

### 技术领域

[0001] 本发明一般地涉及计算机软件程序,更具体地涉及代码加密方法、装置、电子设备和计算机可读存储介质。

### 背景技术

[0002] 随着科学技术的发展和技术产业化应用水平的提升,移动终端的应用程序越来越普及。由于有巨大的利益诱惑,针对应用程序的破解和攻击也越来越猛烈。尤其是一些涉及到支付、人脸识别、私密等类型的应用程序成为首当其冲的攻击对象。

[0003] 目前,计算机程序源代码加密方案通常借助第三方的加固工具对源代码进行加固和混淆,以及做一些防拦截、防调试的策略,目的是防止被破解或者给破解增加难度。然而,很多存在于用户接口和程序逻辑中的字符串以明文的形式存在,被反编译后会暴露产品逻辑,给破解带来了极大的方便。破解者可以通过全局搜索常量字符串信息快速定位想要找的地方。

[0004] 为了解决这一问题,可以通过手动方式对程序产品中的字符串进行加密,然而这种方式效率低,容易遗漏或者出错。

### 发明内容

[0005] 为了解决现有技术中存在的上述问题,本发明实施例提供了代码加密方法、装置、电子设备和计算机可读存储介质。

[0006] 第一方面,本发明实施例提供一种代码加密方法,该方法包括:代码编译步骤,对源代码进行编译,生成原始中间文件;字节码信息提取步骤,提取原始中间文件中的字节码信息,其中,字节码信息包括一条或多条原始指令;指令拦截和过滤步骤,拦截字节码信息中的一条或多条原始指令,根据预先获得的常量字符串的指令特征,对一条或多条原始指令进行过滤,获得一条或多条原始指令中包含指令特征的原始指令所对应的明文常量字符串;字符串加密步骤,对明文常量字符串执行加密处理,获得加密常量字符串;替换插入步骤,利用加密常量字符串替换明文常量字符串,并且插入与加密处理相对应的解密处理的代码,获得经加密的中间文件。

[0007] 在一例中,指令特征包括加载常量指令特征。

[0008] 在一例中,原始中间文件包括类文件。

[0009] 在一例中,字节码信息提取步骤包括:利用字节码插件或者中间文件分解命令提取原始中间文件中的字节码信息。

[0010] 在一例中,利用字节码操纵框架、字节码编辑类库和字节码工程库中的任一种执行字符串加密步骤和替换插入步骤。

[0011] 在一例中,在中间文件初始化过程中执行字符串加密步骤和替换插入步骤。

[0012] 第二方面,本发明实施例提供一种代码加密装置,该装置包括:代码编译模块,配置用于对源代码进行编译,生成原始中间文件;字节码信息提取模块,配置用于提取原始中

间文件中的字节码信息,其中,字节码信息包括一条或多条原始指令;指令拦截和过滤模块,配置用于拦截字节码信息中的一条或多条原始指令,根据预先获得的常量字符串的指令特征,对一条或多条原始指令进行过滤,获得一条或多条原始指令中包含指令特征的原始指令所对应的明文常量字符串;字符串加密模块,配置用于对明文常量字符串执行加密处理,获得加密常量字符串;替换插入模块,配置用于利用加密常量字符串代替明文常量字符串,并且插入与加密处理相对应的解密处理的代码,获得经加密的中间文件。

[0013] 第三方面,本发明实施例提供一种电子设备,该电子设备包括:存储器,用于存储指令;以及处理器,用于调用存储器存储的指令执行上述方法。

[0014] 第四方面,本发明实施例提供一种计算机可读存储介质,计算机可读存储介质存储有计算机可执行指令,计算机可执行指令在由处理器执行时,执行上述方法。

[0015] 本发明实施例提供的代码加密方法、装置、电子设备和计算机可读存储介质通过对字节码信息中的指令进行拦截、过滤和加密,并利用加密字符串替换明文字符串,提供了一种基于自动脚本的字符串自动查找、过滤、加密和替换的方法。解决了明文字符串容易带来的安全风险问题,大大提高了应用程序的安全级别;同时解决了手动加密字符串效率低、工作量大、容易出错的问题,提高了查找加密处理的效率。

## 附图说明

[0016] 通过参考附图阅读下文的详细描述,本发明实施方式的上述以及其他目的、特征和优点将变得易于理解。在附图中,以示例性而非限制性的方式示出了本发明的若干实施方式,其中:

[0017] 图1示出了根据本发明的实施方式的代码加密方法的流程图;

[0018] 图2示出了根据本发明的实施方式的代码加密装置的框图;

[0019] 图3示出了根据本发明的实施方式的电子设备的框图。

[0020] 在附图中,相同或对应的标号表示相同或对应的部分。

## 具体实施方式

[0021] 下面将参考若干示例性实施方式来描述本发明的原理和精神。应当理解,给出这些实施方式仅仅是为了使本领域技术人员能够更好地理解进而实现本发明,而并非以任何方式限制本发明的范围。

[0022] 如图1所示,本发明的一个实施方式提供了一种代码加密方法100。方法100包括步骤S101-S105。

[0023] S101是代码编译步骤,对源代码进行编译,生成原始中间文件。

[0024] S102是字节码信息提取步骤,提取原始中间文件中的字节码信息,其中,字节码信息包括一条或多条原始指令。

[0025] S103是指令拦截和过滤步骤,拦截字节码信息中的一条或多条原始指令,根据预先获得的常量字符串的指令特征,对一条或多条原始指令进行过滤,获得一条或多条原始指令中包含指令特征的原始指令所对应的明文常量字符串。

[0026] 在一些实施方式中,可以对字节码信息中的原始指令进行遍历拦截,即,拦截其中的每一条原始指令。当然,也可以根据需求拦截其中的一部分指令。

[0027] 需要注意的是,为了行文一致性,本发明说明书中使用“常量字符串”概念,在实际应用中,常量字符串也可以称为常量字段、常量字符串信息、常量信息等。

[0028] 在一些实施方式中,通过拦截和过滤获得明文常量字符串之后,可以把常量字符串的值保存起来,准备后面的操作。例如,可以将明文常量字符串的值保存在字典中。

[0029] S104是字符串加密步骤,对明文常量字符串执行加密处理,获得加密常量字符串。

[0030] 在一些实施方式中,加密处理可以是预先设定的。另外,加密处理可以包括多种加密算法,例如,Base64、AES等常规加密算法,可根据需求随意选择,只要让常量字符串无法被直接看到和搜索到即可。

[0031] 在一些实施方式中,可以将加密后的常量字符串的值与明文常量字符串的值相对应地存储在字典中,便于后续索引和使用。

[0032] S105是替换插入步骤,利用加密常量字符串替换明文常量字符串,并且插入与加密处理相对应的解密处理的代码,获得经加密的中间文件。

[0033] 在一些实施方式中,在进行常量字符串替换时,可以通过在字典中检索明文常量字符串相对应的加密常量字符串,从而进行替换。

[0034] 在一些实施方式中,可以将加密处理相对应的解密处理插入到中间文件的初始化方法中,以保证程序逻辑的正常进行。

[0035] 本发明的实施方式提出的代码加密方法100通过提取原始中间文件中的字节码信息,有助于查找常量字符串,因为字节码信息中有常量字符串的指令具有一些共同的指令特征。通过对字节码信息中的指令进行拦截、过滤和加密,并利用加密常量字符串替换明文常量字符串,提供了一种基于自动脚本的字符串自动查找、过滤、加密和替换的方法。本发明的实施方式提出的代码加密方法100解决了明文字符串容易带来的安全风险问题,大大提高了应用程序的安全级别;同时解决了手动加密字符串效率低、工作量大、容易出错的问题,提高了查找加密处理的效率。

[0036] 作为本发明的一个实施方式,指令特征可以包括加载常量指令特征。以Java系语言为例,通常定义常量字符串的指令一般是加载常量(Load Constant,LDC)指令,将LDC指令作为常量字符串的指令特征,可以很方便、快速地查找到常量字符串。

[0037] 作为本发明的一个实施方式,以Java系语言为例,原始中间文件可以包括类文件,即,.class后缀的文件。

[0038] 作为本发明的一个实施方式,字节码信息提取步骤包括:利用字节码(Bytecode)插件或者中间文件分解命令提取原始中间文件中的字节码信息。在一些实施方式中,中间文件分解命令可以包括javap命令,其可以分解类(.class)文件,对中间文件进行反编译,查看字节码信息。

[0039] 作为本发明的一个实施方式,可以利用字节码操纵框架、字节码编辑类库和字节码工程库(Byte Code Engineering Library,BCEL)中的任一种执行字符串加密步骤S104和替换插入步骤S105。

[0040] 作为本发明的一个实施方式,可以在中间文件初始化过程中执行字符串加密步骤S104和替换插入步骤S105。

[0041] 在一些实施方式中,字节码操纵框架可以包括ASM工具和SERP工具。其中,ASM工具是一个致力于字节码操作和分析的框架,其可以用来修改一个已存在的类或者动态产生一

个新的类。ASM提供了一些通用的字节码转换和分析算法,通过这些算法可以定制更复杂的工具。与其他字节码工具相比,ASM更关注执行效率,其被设计的更小更快。SERP字节码框架可以提供一组高级的应用程序编程接口(Application Programming Interface,API)进行字节码各方面的操作。

[0042] 在一些实施方式中,字节码编辑类库可以包括javassist工具,javassist工具是一个开源的分析、编辑和创建Java字节码的类库。

[0043] 上述ASM工具、javassist工具、BCEL工具、SERP工具可以对生成的.class代码进行添加和修改之后,生成新的.class文件。需要注意的是,本发明的实施方式不限于上述列举的几种工具,在不同的编程语言环境下,可以采用不同的工具实现类似功能。

[0044] 如图2所示,本发明的一个实施方式提供了一种代码加密装置200。装置200包括模块201-205。

[0045] 代码编译模块201可以配置用于对源代码进行编译,生成原始中间文件;

[0046] 字节码信息提取模块202可以配置用于提取原始中间文件中的字节码信息,其中,字节码信息包括一条或多条原始指令。

[0047] 指令拦截和过滤模块203可以配置用于拦截字节码信息中的一条或多条原始指令,根据预先获得的常量字符串的指令特征,对一条或多条原始指令进行过滤,获得一条或多条原始指令中包含指令特征的原始指令所对应的明文常量字符串。

[0048] 字符串加密模块204可以配置用于对明文常量字符串执行加密处理,获得加密常量字符串。

[0049] 替换插入模块205可以配置用于利用加密常量字符串代替明文常量字符串,并且插入与加密处理相对应的解密处理的代码,获得经加密的中间文件。

[0050] 作为本发明的一个实施方式,指令特征可以包括加载常量指令特征。

[0051] 作为本发明的一个实施方式,原始中间文件可以包括类文件。

[0052] 作为本发明的一个实施方式,字节码信息提取模块还可以配置用于:利用字节码(Bytecode)插件或者中间文件分解命令提取原始中间文件中的字节码信息。

[0053] 作为本发明的一个实施方式,可以利用字节码操纵框架、字节码编辑类库和字节码工程库(BCEL)中的任一种执行字符串加密模块204和替换插入模块205的操作。

[0054] 作为本发明的一个实施方式,可以在中间文件初始化过程中执行字符串加密模块204和替换插入模块205的操作。

[0055] 装置中的各个模块所实现的功能与上文描述的方法中的步骤相对应,其具体实现和技术效果请参见上文对于方法步骤的描述,在此不再赘述。

[0056] 如图3所示,本发明的一个实施方式提供了一种电子设备300。其中,该电子设备300包括存储器301、处理器302、输入/输出(Input/Output,I/O)接口303。其中,存储器301,用于存储指令。处理器302,用于调用存储器301存储的指令执行本发明实施例的代码加密方法。其中,处理器302分别与存储器301、I/O接口303连接,例如可通过总线系统和/或其他形式的连接机构(未示出)进行连接。存储器301可用于存储程序和数据,包括本发明实施例中涉及的代码加密程序,处理器302通过运行存储在存储器301的程序从而执行电子设备300的各种功能应用以及数据处理。

[0057] 本发明实施例中处理器302可以采用数字信号处理器(Digital Signal

Processing,DSP)、现场可编程门阵列(Field-Programmable Gate Array,FPGA)、可编程逻辑阵列(Programmable Logic Array,PLA)中的至少一种硬件形式来实现,所述处理器302可以是中央处理单元(Central Processing Unit,CPU)或者具有数据处理能力和/或指令执行能力的其他形式的处理单元中的一种或几种的组合。

[0058] 本发明实施例中的存储器301可以包括一个或多个计算机程序产品,所述计算机程序产品可以包括各种形式的计算机可读存储介质,例如易失性存储器和/或非易失性存储器。所述易失性存储器例如可以包括随机存取存储器(Random Access Memory, RAM)和/或高速缓冲存储器(Cache)等。所述非易失性存储器例如可以包括只读存储器(Read-Only Memory,ROM)、快闪存储器(Flash Memory)、硬盘(Hard Disk Drive,HDD)或固态硬盘(Solid-State Drive,SSD)等。

[0059] 本发明实施例中,I/O接口303可用于接收输入的指令(例如数字或字符信息,以及产生与电子设备300的用户设置以及功能控制有关的键信号输入等),也可向外部输出各种信息(例如,图像或声音等)。本发明实施例中I/O接口303可包括物理键盘、功能按键(比如音量控制按键、开关按键等)、鼠标、操作杆、轨迹球、麦克风、扬声器、和触控面板等中的一个或多个。

[0060] 在一些实施方式中,本发明提供了一种计算机可读存储介质,该计算机可读存储介质存储有计算机可执行指令,计算机可执行指令在由处理器执行时,执行上文所述的任何方法。

[0061] 尽管在附图中以特定的顺序描述操作,但是不应将其理解为要求按照所示的特定顺序或是串行顺序来执行这些操作,或是要求执行全部所示的操作以得到期望的结果。在特定环境中,多任务和并行处理可能是有利的。

[0062] 本发明的方法和装置能够利用标准编程技术来完成,利用基于规则的逻辑或者其他逻辑来实现各种方法步骤。还应当注意的是,此处以及权利要求书中使用的词语“装置”和“模块”意在包括使用一行或者多行软件代码的实现和/或硬件实现和/或用于接收输入的设备。

[0063] 此处描述的任何步骤、操作或程序可以使用单独的或与其他设备组合的一个或多个硬件或软件模块来执行或实现。在一个实施方式中,软件模块使用包括包含计算机程序代码的计算机可读介质的计算机程序产品实现,其能够由计算机处理器执行用于执行任何或全部的所描述的步骤、操作或程序。

[0064] 出于示例和描述的目的,已经给出了本发明实施的前述说明。前述说明并非穷举性的也并非要将本发明限制到所公开的确切形式,根据上述教导还可能存在着各种变形和修改,或者是可能从本发明的实践中得到各种变形和修改。选择和描述这些实施例是为了说明本发明的原理及其实际应用,以使得本领域的技术人员能够以适合于构思的特定用途来以各种实施方式和各种修改而利用本发明。

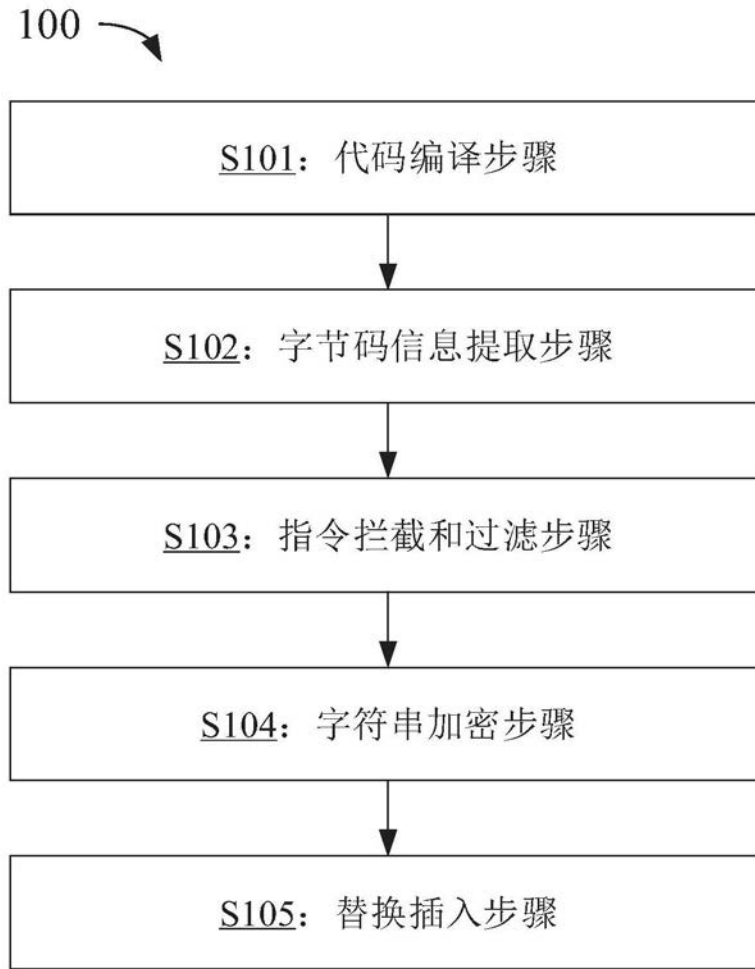


图1



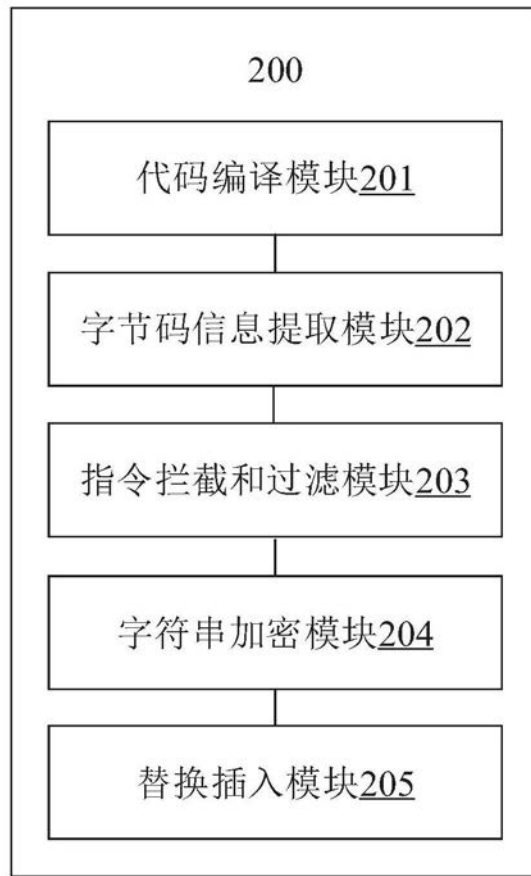


图2

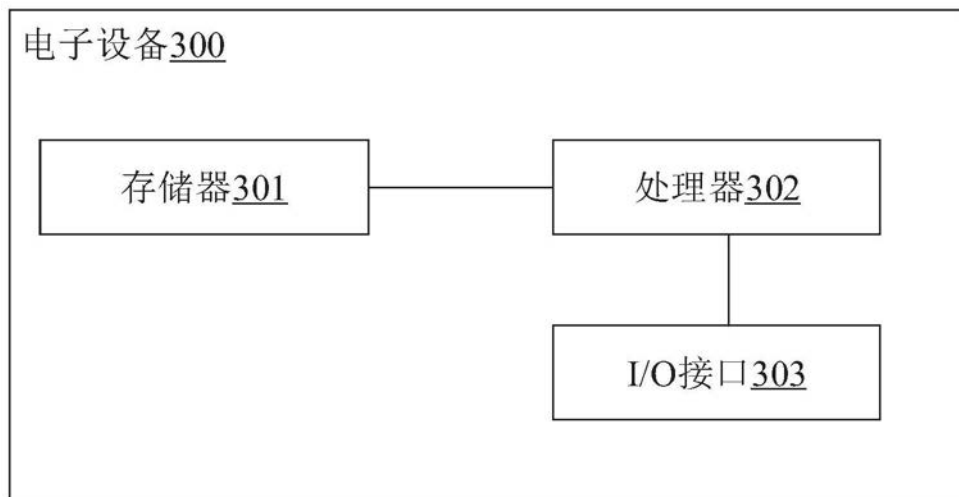


图3