



(12)发明专利申请

(10)申请公布号 CN 107145602 A

(43)申请公布日 2017.09.08

(21)申请号 201710419541.1

(22)申请日 2017.06.06

(71)申请人 北京洋浦伟业科技发展有限公司
地址 100083 北京市海淀区学院路30号天
工大厦A座20层

(72)发明人 阚志刚 陈彪 方宁 卢佐华

(74)专利代理机构 北京志霖恒远知识产权代理
事务所(普通合伙) 11435
代理人 郭栋梁

(51) Int. Cl.
G06F 17/30(2006.01)
G06F 9/445(2006.01)
G06F 21/56(2013.01)

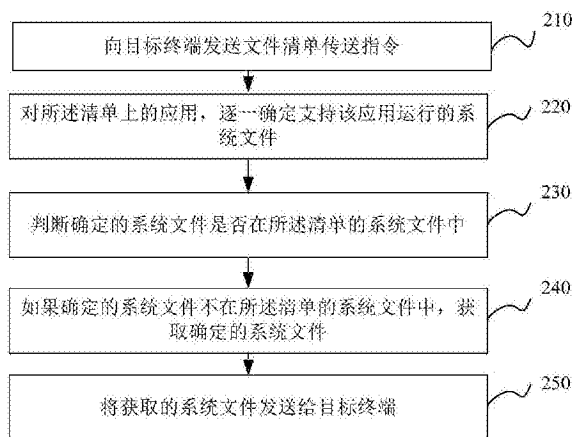
权利要求书2页 说明书8页 附图2页

(54)发明名称

外部干预式系统文件补全方法和装置

(57)摘要

本申请公开了一种外部干预式系统文件补全方法和装置。所述方法包括:向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单;对所述清单上的应用,逐一确定支持该应用运行的系统文件;判断确定的系统文件是否在所述清单的系统文件中;如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件;将获取的系统文件发送给目标终端。本申请能为终端自动下载缺失的系统文件,减轻终端操作而又确保终端安全性。



1. 一种外部干预式系统文件补全方法,其特征在于,所述方法包括:
向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单;
对所述清单上的应用,逐一确定支持该应用运行的系统文件;
判断确定的系统文件是否在所述清单的系统文件中;
如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件;
将获取的系统文件发送给目标终端。
2. 根据权利要求1所述的方法,其特征在于,获取确定的系统文件的步骤包括:
判断确定的系统文件是否在预置的系统文件存储库中;
如果确定的系统文件在预置的系统文件存储库中,从所述系统文件存储库中获取确定的系统文件;
如果确定的系统文件不在预置的系统文件存储库中,从互联网上下载确定的系统文件。
3. 根据权利要求1或2所述的方法,其特征在于,所述方法还包括:
在将获取的系统文件发送给目标终端之前,将获取的系统文件杀毒。
4. 根据权利要求3所述的方法,其特征在于,所述方法还包括:
在将获取的系统文件杀毒之后,将杀毒后的系统文件存储到系统文件存储库中。
5. 根据权利要求1所述的方法,其特征在于,所述如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件的步骤包括:
如果确定的系统文件不在所述清单的系统文件中,向目标终端发送询问请求,用于询问目标终端是否需要补全该确定的系统文件;
如果接收到来自目标终端的需要补全该确定的系统文件的响应,获取确定的系统文件。
6. 根据权利要求1所述的方法,其特征在于,向目标终端发送文件清单传送指令是响应于接收到目标终端安装应用的通知进行的。
7. 一种外部干预式系统文件补全装置,其特征在于,所述装置包括:
指令发送单元,用于向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单;
确定单元,用于对所述清单上的应用,逐一确定支持该应用运行的系统文件;
判断单元,用于判断确定的系统文件是否在所述清单的系统文件中;
获取单元,用于如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件;
系统文件发送单元,用于将获取的系统文件发送给目标终端。
8. 根据权利要求7所述的装置,其特征在于,获取单元进一步用于:
判断确定的系统文件是否在预置的系统文件存储库中;
如果确定的系统文件在预置的系统文件存储库中,从所述系统文件存储库中获取确定的系统文件;
如果确定的系统文件不在预置的系统文件存储库中,从互联网上下载确定的系统文件。

9. 根据权利要求7或8所述的装置,其特征在于,所述装置还包括:

杀毒单元,用于在将获取的系统文件发送给目标终端之前,将获取的系统文件杀毒。

10. 根据权利要求9所述的装置,其特征在于,所述装置还包括:

杀毒文件存储单元,用于在将获取的系统文件杀毒之后,将杀毒后的系统文件存储到系统文件存储库中。

外部干预式系统文件补全方法和装置

技术领域

[0001] 本公开一般涉及计算机领域,具体涉及计算机系统文件的补全,尤其涉及一种外部干预式系统文件补全方法和装置。

背景技术

[0002] 目前,许多软件应用、游戏应用在终端(包括计算机、移动电话、PDA等)上必须要求终端上有某些系统文件才能运行。然而,在终端的运行中,由于用户误删了某些包含系统文件的文件夹,或网络病毒入侵到终端删除了一些系统文件,经常出现当某些应用需要一些系统文件支持时发现这些系统文件缺失了。用户需要根据终端的提示自己到互联网下载相应缺失的系统文件。这样,带来两个问题:第一,用户操作比较繁琐;第二,用户到互联网上下载缺失的系统文件,可能又会下载到病毒,威胁终端安全。

[0003] 因此,需要一种为用户自动下载缺失的系统文件,减轻用户操作而又确保用户安全性的方案。

发明内容

[0004] 鉴于现有技术中的上述缺陷或不足,期望提供一种为用户自动下载缺失的系统文件,减轻用户操作而又确保用户安全性的技术。

[0005] 第一方面,本申请实施例提供了一种外部干预式系统文件补全方法,所述方法包括:向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单;对所述清单上的应用,逐一确定支持该应用运行的系统文件;判断确定的系统文件是否在所述清单的系统文件中;如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件;将获取的系统文件发送给目标终端。

[0006] 第二方面,本申请实施例提供了一种外部干预式系统文件补全装置,所述装置包括:指令发送单元,用于向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单;确定单元,用于对所述清单上的应用,逐一确定支持该应用运行的系统文件;判断单元,用于判断确定的系统文件是否在所述清单的系统文件中;获取单元,用于如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件;系统文件发送单元,用于将获取的系统文件发送给目标终端。

[0007] 第三方面,本申请实施例提供了一种设备,包括处理器、存储器和显示器;所述存储器包含可由所述处理器执行的指令以使得所述处理器执行:向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单;对所述清单上的应用,逐一确定支持该应用运行的系统文件;判断确定的系统文件是否在所述清单的系统文件中;如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件;将获取的系统文件发送给目标终端。

[0008] 第四方面,本申请实施例提供了一种机器可读介质,包含计算机程序,所述计算机程序包括用于执行以下的程序代码:向目标终端发送文件清单传送指令,用于指示目标终

端传送目标终端上存储的所有应用和所有系统文件的清单；对所述清单上的应用，逐一确定支持该应用运行的系统文件；判断确定的系统文件是否在所述清单的系统文件中；如果确定的系统文件不在所述清单的系统文件中，获取确定的系统文件；将获取的系统文件发送给目标终端。

[0009] 本发明实施例中，不是等到软件、游戏等应用运行时发现缺少某些系统文件再由用户从互联网上下载，而是由专门的外部干预式系统文件补全装置从外部进行干预。外部干预式系统文件补全装置命令目标终端上报其上存储的所有应用和所有系统文件的清单，对所述清单上的应用，逐一确定支持该应用运行的系统文件，如果确定的系统文件不在所述清单的系统文件中，获取确定的系统文件发送给目标终端。这样，就实现了为用户自动下载缺失的系统文件，减轻用户操作。另外，在专门的外部干预式系统文件补全装置处获取的系统文件都是有安全保障的，减少了用户自己去互联网上下载引起的不安全性。

附图说明

[0010] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0011] 图1示出了本申请一个实施例应用的系统环境示意图。

[0012] 图2示出了根据本申请一个实施例的外部干预式系统文件补全方法的示例性流程图；

[0013] 图3示出了根据本申请一个实施例的外部干预式系统文件补全装置的示例性结构框图；

[0014] 图4示出了适于用来实现本申请实施例的结构示意图。

具体实施方式

[0015] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与发明相关的部分。

[0016] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0017] 如背景技术中提到的，目前，许多软件应用、游戏应用在终端（包括计算机、移动电话、PDA等）上必须要求终端上有某些系统文件才能运行。然而，在终端的运行中，由于用户误删了某些包含系统文件的文件夹，或网络病毒入侵到终端删除了一些系统文件，经常出现当某些应用需要一些系统文件支持时发现这些系统文件缺失了。用户需要根据终端的提示自己到互联网下载相应缺失的系统文件。这样，带来两个问题：第一，用户操作比较繁琐；第二，用户到互联网上下载缺失的系统文件，可能又会下载到病毒，威胁终端安全。因此，需要一种为用户自动下载缺失的系统文件，减轻用户操作而又确保用户安全性的方案。

[0018] 本发明实施例中，不是等到软件、游戏等应用运行时发现缺少某些系统文件再由用户从互联网上下载，而是由专门的外部干预式系统文件补全装置从外部进行干预。外部干预式系统文件补全装置命令目标终端上报其上存储的所有应用和所有系统文件的清单，对所述清单上的应用，逐一确定支持该应用运行的系统文件，如果确定的系统文件不在所

述清单的系统文件中,获取确定的系统文件发送给目标终端。这样,就实现了为用户自动下载缺失的系统文件,减轻用户操作。另外,在专门的外部干预式系统文件补全装置处获取的系统文件都是有安全保障的,减少了用户自己去互联网上下载引起的不安全性。

[0019] 参考图1,其示出了本申请一个实施例应用的系统环境示意图。该环境包括多个目标终端110和外部干预式系统文件补全装置300。目标终端是要为其补全系统文件的终端。它可以是通用计算机、移动电话、PDA、车载设备等等。只要其上面需要安装系统文件以支持各种应用的运行,都可以成为目标终端110。外部干预式系统文件补全装置300是本申请外部干预式系统文件补全方法执行的主体。它可以是一个专门的设备,也可以作为服务器的一部分固化在服务器中。这里的服务器包括本地服务器、云端服务器等。外部干预式系统文件补全装置300往往与多个目标终端110进行交互,负责多个目标终端110的系统文件补全。外部干预式系统文件补全装置300与目标终端110之间可以通过局域网相连,也可以通过互联网相连,可以是有线连接,也可以是无连接。

[0020] 参考图2,其示出了根据本申请一个实施例的外部干预式系统文件补全方法。

[0021] 系统文件是指操作系统的主要文件,一般在安装操作系统过程中自动创建并将相关文件放在对应的文件夹中,这里面的文件直接影响系统的正常运行,多数都不允许随意改变。它的存在对维护计算机系统的稳定具有重要作用。在运行应用时,往往需要其中一些系统文件的支持。

[0022] 系统文件补全是当系统文件缺失时补充所缺失的系统文件。

[0023] 外部干预式是指由终端外部发起对终端的系统文件补全,而不是终端自身发起对自身的系统文件的补全。如图1所示,外部干预式系统文件补全装置300在目标终端110的外部,由外部干预式系统文件补全装置300发起的系统文件补全就是外部干预式的系统文件补全。

[0024] 如图2所示,在步骤210中,向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单。

[0025] 发送文件清单传送指令是要求目标终端传送目标终端上存储的所有应用和所有系统文件的清单的指令。

[0026] 向目标终端发送文件清单传送指令可以周期性执行。这样,如果在目标终端上还存在系统文件缺失,仅仅是缺失了上次周期性补全后又丢失的系统文件,使得对于一般情况来说,采用了本发明实施例的方法后,系统文件即使有缺失,也不会太大。例如,每天上午8:00对外部干预式系统文件补全装置300下的所有目标终端110执行一遍。这样,如果11:00某台终端上有系统文件的缺失,仅仅是在当天8:00-11:00之间新形成的缺失。

[0027] 另外,在一个实施例中,向目标终端发送文件清单传送指令是响应于接收到目标终端安装应用的通知进行的。也就是说,规定外部干预式系统文件补全装置300下的目标终端110如果安装了新应用,必须向外部干预式系统文件补全装置300发送目标终端安装应用的通知,以触发步骤210-250执行。这样做的好处是:在安装新应用后,往往该新应用需要立刻执行,而如果只是周期性对终端的系统文件进行补全,很可能在新应用安装后需要执行的时间点支持其执行的系统文件又由于病毒攻击等原因缺失了,造成用户安装新应用后体验不佳。如果在安装新应用后,终端立刻通知外部干预式系统文件补全装置300执行步骤210-250,则能够在新应用安装后立刻执行,满足应用安装后一般需要立刻执行的需求。

[0028] 在步骤220中,对所述清单上的应用,逐一确定支持该应用运行的系统文件。

[0029] 外部干预式系统文件补全装置300可以维护一个各种应用与其要求的系统文件对照表。这样,对于对所述清单上的应用,就可以逐一查找所述对照表,以确定支持其运行的系统文件。

[0030] 在步骤230中,判断确定的系统文件是否在所述清单的系统文件中。

[0031] 如果步骤220确定出的支持某一应用运行的所有系统文件都是目标终端所拥有的,说明该应用可以顺利运行,不存在系统文件缺失。

[0032] 如果步骤220确定出的支持某一应用运行的一个系统文件不在终端所拥有的系统文件中,就说明对于执行该应用来说,发生了系统文件缺失。

[0033] 在步骤240中,如果确定的系统文件不在所述清单的系统文件中,获取确定的系统文件。

[0034] 如上所述,如果步骤220确定出的支持某一应用运行的一个系统文件不在终端所拥有的系统文件中,就说明对于执行该应用来说,发生了系统文件缺失,则需要为其获取缺失的系统文件。

[0035] 在一个实施例中,步骤240包括:判断确定的系统文件是否在预置的系统文件存储库中;如果确定的系统文件在预置的系统文件存储库中,从所述系统文件存储库中获取确定的系统文件;如果确定的系统文件不在预置的系统文件存储库中,从互联网上下载确定的系统文件。

[0036] 系统文件存储库是在外部干预式系统文件补全装置300上预先设置的库,用于放置预先能想到的各种用于支持应用的系统文件。它里面存放的系统文件都是通过正式渠道获取的,具有安全性。如果确定的系统文件在预置的系统文件存储库中,就可以直接从系统文件存储库中获取确定的系统文件,这样获取的系统文件安全性高。如果确定的系统文件不在预置的系统文件存储库中,这时就要从其它渠道获取系统文件了。一个通用的做法是从互联网上下载确定的系统文件。

[0037] 由于从互联网上下载的系统文件可能有病毒,在背景技术中也提到正是因为现有技术中用户自己需要从互联网上下载缺失的系统文件的做法导致容易遭致病毒攻击、安全性较差,因此,在一个实施例中,为了提高系统文件的安全性,所述方法还包括:在将获取的系统文件发送给目标终端之前,将获取的系统文件杀毒。由于该杀毒是在外部干预式系统文件补全装置300自动进行的,用户感觉象是“透明的”,在无需用户干预的前提下自动保证了补全的系统文件的安全性。

[0038] 在一个实施例中,所述方法还包括:在将获取的系统文件杀毒之后,将杀毒后的系统文件存储到系统文件存储库中。

[0039] 这样做的好处是,不断完善外部干预式系统文件补全装置300上自带的系统文件存储库,使系统文件存储库越来越全,在下次需要获取同样的系统文件时不用去互联网上下载,提高获取效率,从而提高系统文件补全的效率。

[0040] 另外,在一个实施例中,步骤240包括:如果确定的系统文件不在所述清单的系统文件中,向目标终端发送询问请求,用于询问目标终端是否需要补全该确定的系统文件;如果接收到来自目标终端的需要补全该确定的系统文件的响应,获取确定的系统文件。

[0041] 也就是说,该实施例中,如果确定的系统文件不在所述清单的系统文件中,不是立

刻为目标终端补全系统文件,而是先发请求询问目标终端是否需要补全。如果接收到来自目标终端的需要补全该确定的系统文件的响应,则获取确定的系统文件,为目标终端补全,否则不为目标终端补全。这样做的好处是,事实上,许多用户需要安装了某应用,但可能是误安装,如在互联网上误点了某伪装成有用链接的游戏下载链接,导致安装了某一用户并不需要的游戏,此时检测到用户安装了新应用,进而为用户安装其缺失的系统文件是不必要的,导致资源的浪费。通过这种方式,减少了资源的浪费,提高了资源的合理配置。

[0042] 在步骤250中,将获取的系统文件发送给目标终端。

[0043] 将获取的系统文件发送给目标终端,以便目标终端安装该系统文件,以支持其相应的应用。

[0044] 应当注意,尽管在附图中以特定顺序描述了本发明方法的操作,但是,这并非要求或者暗示必须按照该特定顺序来执行这些操作,或是必须执行全部所示的操作才能实现期望的结果。相反,流程图中描绘的步骤可以改变执行顺序。附加地或备选地,可以省略某些步骤,将多个步骤合并为一个步骤执行,和/或将一个步骤分解为多个步骤执行。

[0045] 进一步参考图3,其示出了根据本申请一个实施例的外部干预式系统文件补全装置300的示例性结构框图。它包括指令发送单元310、确定单元320、判断单元330、获取单元340、系统文件发送单元350。

[0046] 指令发送单元310向目标终端发送文件清单传送指令,用于指示目标终端传送目标终端上存储的所有应用和所有系统文件的清单。

[0047] 发送文件清单传送指令是要求目标终端传送目标终端上存储的所有应用和所有系统文件的清单的指令。

[0048] 向目标终端发送文件清单传送指令可以周期性执行。这样,如果在目标终端上还存在系统文件缺失,仅仅是缺失了上次周期性补全后又丢失的系统文件,使得对于一般情况来说,采用了本发明实施例的方法后,系统文件即使有缺失,也不会太大。例如,每天上午8:00对外部干预式系统文件补全装置300下的所有目标终端110执行一遍。这样,如果11:00某台终端上有系统文件的缺失,仅仅是在当天8:00-11:00之间新形成的缺失。

[0049] 另外,在一个实施例中,向目标终端发送文件清单传送指令是响应于接收到目标终端安装应用的通知进行的。也就是说,规定外部干预式系统文件补全装置300下的目标终端110如果安装了新应用,必须向外部干预式系统文件补全装置300发送目标终端安装应用的通知,以触发本发明实施例的系统文件补全过程执行。这样做的好处是:在安装新应用后,往往该新应用需要立刻执行,而如果只是周期性对终端的系统文件进行补全,很可能在新应用安装后需要执行的时间点支持其执行的系统文件又由于病毒攻击等原因缺失了,造成用户安装新应用后体验不佳。如果在安装新应用后,终端立刻通知外部干预式系统文件补全装置300执行本发明实施例的系统文件补全过程,则能够在新应用安装后立刻执行,满足应用安装后一般需要立刻执行的需求。

[0050] 确定单元320对所述清单上的应用,逐一确定支持该应用运行的系统文件。

[0051] 外部干预式系统文件补全装置300可以维护一个各种应用与其要求的系统文件对照表。这样,对于对所述清单上的应用,就可以逐一查找所述对照表,以确定支持其运行的系统文件。

[0052] 判断单元330判断确定的系统文件是否在所述清单的系统文件中。

[0053] 如果确定单元320确定出的支持某一应用运行的所有系统文件都是目标终端所拥有的,说明该应用可以顺利运行,不存在系统文件缺失。

[0054] 如果确定单元320确定出的支持某一应用运行的一个系统文件不在终端所拥有的系统文件中,就说明对于执行该应用来说,发生了系统文件缺失。

[0055] 如果确定的系统文件不在所述清单的系统文件中,获取单元340获取确定的系统文件。

[0056] 如上所述,如果确定出的支持某一应用运行的一个系统文件不在终端所拥有的系统文件中,就说明对于执行该应用来说,发生了系统文件缺失,则需要为其获取缺失的系统文件。

[0057] 在一个实施例中,获取单元340进一步用于:判断确定的系统文件是否在预置的系统文件存储库中;如果确定的系统文件在预置的系统文件存储库中,从所述系统文件存储库中获取确定的系统文件;如果确定的系统文件不在预置的系统文件存储库中,从互联网上下载确定的系统文件。

[0058] 系统文件存储库是在外部干预式系统文件补全装置300上预先设置的库,用于放置预先能想到的各种用于支持应用的系统文件。它里面存放的系统文件都是通过正式渠道获取的,具有安全性。如果确定的系统文件在预置的系统文件存储库中,就可以直接从系统文件存储库中获取确定的系统文件,这样获取的系统文件安全性高。如果确定的系统文件不在预置的系统文件存储库中,这时就要从其它渠道获取系统文件了。一个通用的做法是从互联网上下载确定的系统文件。

[0059] 由于从互联网上下载的系统文件可能有病毒,在背景技术中也提到正是因为现有技术中用户自己需要从互联网上下载缺失的系统文件的做法导致容易遭致病毒攻击、安全性较差,因此,在一个实施例中,为了提高系统文件的安全性,所述装置300还包括:杀毒单元,用于在将获取的系统文件发送给目标终端之前,将获取的系统文件杀毒。由于该杀毒是在外部干预式系统文件补全装置300自动进行的,用户感觉象是“透明的”,在无需用户干预的前提下自动保证了补全的系统文件的安全性。

[0060] 在一个实施例中,所述装置300还包括:杀毒文件存储单元,用于在将获取的系统文件杀毒之后,将杀毒后的系统文件存储到系统文件存储库中。

[0061] 这样做的好处是,不断完善外部干预式系统文件补全装置300上自带的系统文件存储库,使系统文件存储库越来越全,在下次需要获取同样的系统文件时不用去互联网上下载,提高获取效率,从而提高系统文件补全的效率。

[0062] 另外,在一个实施例中,获取单元340进一步用于:如果确定的系统文件不在所述清单的系统文件中,向目标终端发送询问请求,用于询问目标终端是否需要补全该确定的系统文件;如果接收到来自目标终端的需要补全该确定的系统文件的响应,获取确定的系统文件。

[0063] 也就是说,该实施例中,如果确定的系统文件不在所述清单的系统文件中,不是立刻为目标终端补全系统文件,而是先发请求询问目标终端是否需要补全。如果接收到来自目标终端的需要补全该确定的系统文件的响应,则获取确定的系统文件,为目标终端补全,否则不为目标终端补全。这样做的好处是,事实上,许多用户需要安装了某应用,但可能是误安装,如在互联网上误点了某伪装成有用链接的游戏下载链接,导致安装了某一用户并

不需要的游戏,此时检测到用户安装了新应用,进而为用户安装其缺失的系统文件是不必要的,导致资源的浪费。通过这种方式,减少了资源的浪费,提高了资源的合理配置。

[0064] 系统文件发送单元350将获取的系统文件发送给目标终端。

[0065] 系统文件发送单元350将获取的系统文件发送给目标终端,以便目标终端安装该系统文件,以支持其相应的应用。

[0066] 下面参考图4,其示出了适于用来实现本申请实施例的计算机系统400的结构示意图。

[0067] 如图4所示,计算机系统400包括中央处理单元(CPU)401,其可以根据存储在只读存储器(ROM)402中的程序或者从存储部分408加载到随机访问存储器(RAM)403中的程序而执行各种适当的动作和处理。在RAM 403中,还存储有系统400操作所需的各种程序和数据。CPU 401、ROM 402以及RAM 403通过总线404彼此相连。输入/输出(I/O)接口405也连接至总线404。

[0068] 以下部件连接至I/O接口405:包括键盘、鼠标等的输入部分406;包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分407;包括硬盘等的存储部分408;以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分409。通信部分409经由诸如因特网的网络执行通信处理。驱动器410也根据需要连接至I/O接口405。可拆卸介质411,诸如磁盘、光盘、磁光盘、半导体存储器等等,根据需要安装在驱动器410上,以便于从其上读出的计算机程序根据需要被安装入存储部分408。

[0069] 特别地,根据本公开的实施例,上文参考图1描述的过程可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括有形地包含在机器可读介质上的计算机程序,所述计算机程序包含用于执行图1的方法的程序代码。

[0070] 在这样的实施例中,该计算机程序可以通过通信部分409从网络上被下载和安装,和/或从可拆卸介质411被安装。

[0071] 附图中的流程图和框图,图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,所述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0072] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现,也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中。这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0073] 作为另一方面,本申请还提供了一种计算机可读存储介质,该计算机可读存储介质可以是上述实施例中所述装置中所包含的计算机可读存储介质;也可以是单独存在,未装配入设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序,所述程序被一个或者一个以上的处理器用来执行描述于本申请的公式输入方法。

[0074] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解,本申请中所涉及的发明范围,并不限于上述技术特征的特定组合而成的技术方案,同时也应涵盖在不脱离所述发明构思的情况下,由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

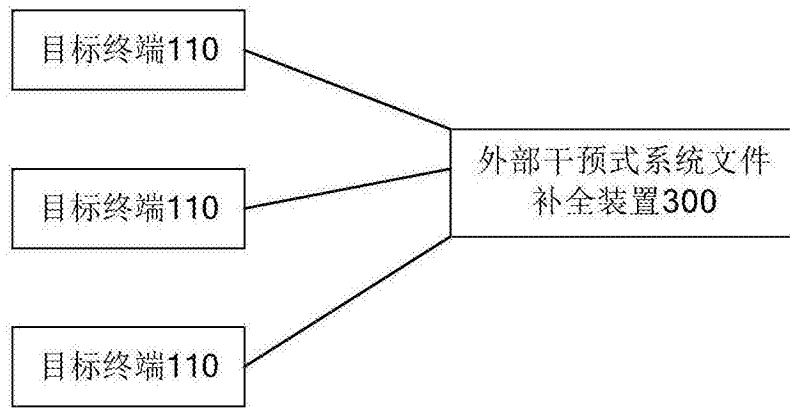


图1

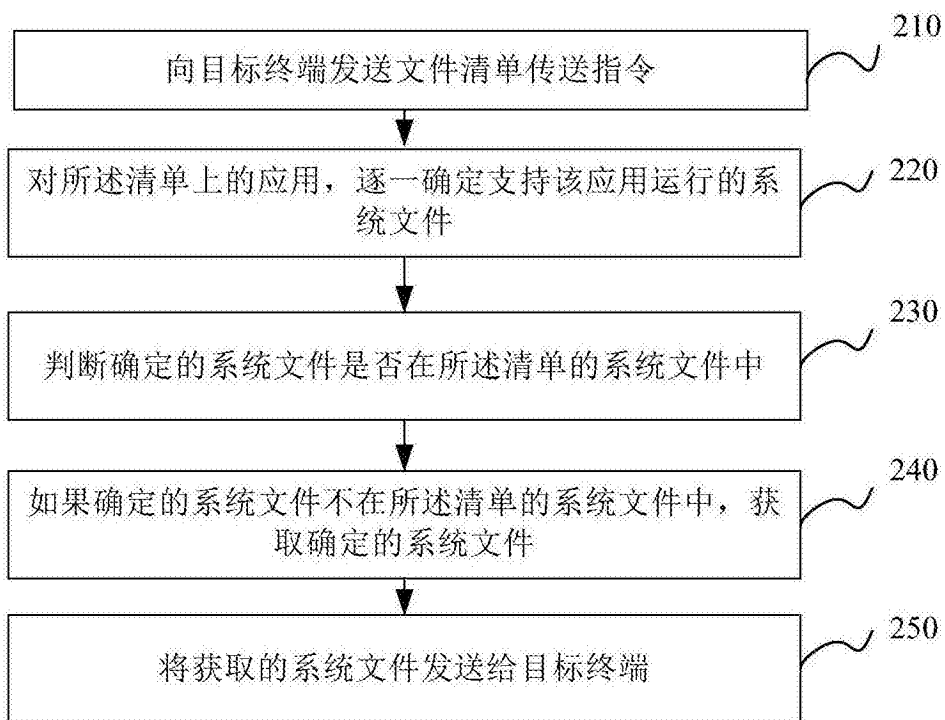


图2

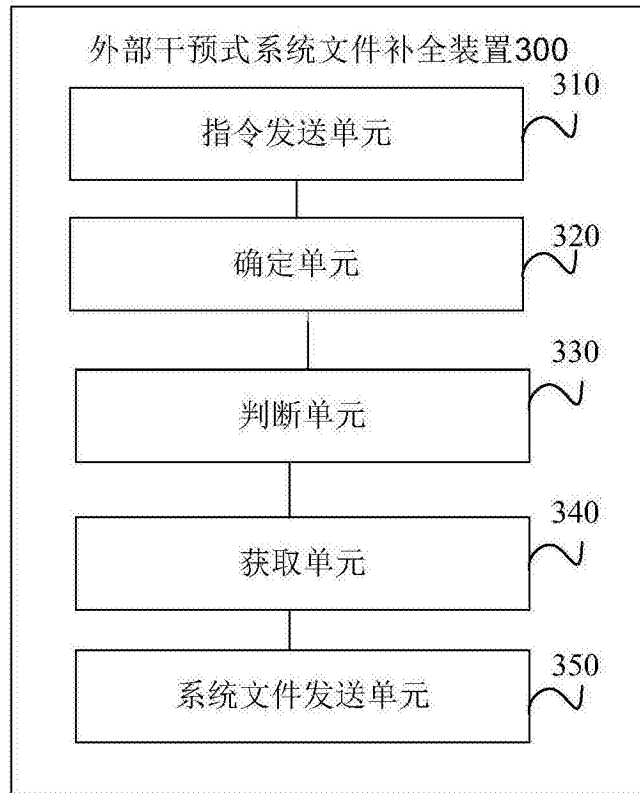


图3

400

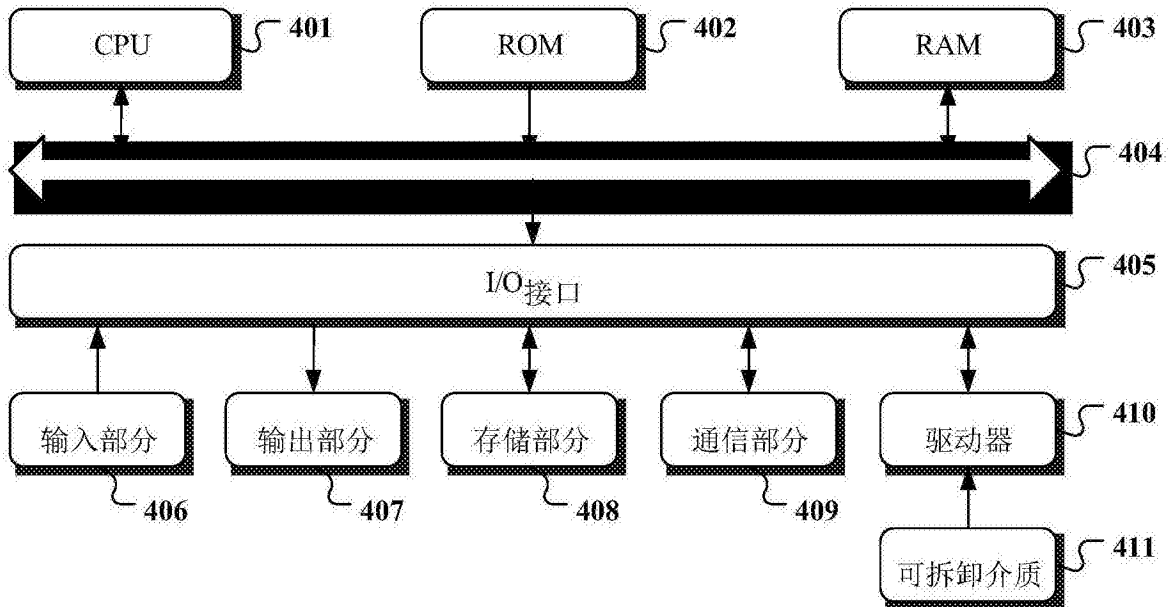


图4