[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 17/30 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200910140639.9

[43] 公开日 2010 年 1 月 6 日

[11] 公开号 CN 101620627A

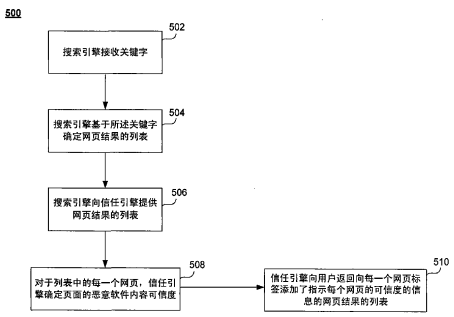
[22] 申请日 2009.6.10
[21] 申请号 200910140639.9
[30] 优先权
[32] 2008. 6.10 [33] US [31] 12/136,227
[71] 申请人 英特尔公司
地址 美国加利福尼亚
[72] 发明人 H·C·李 D·迈耶斯
[74] 专利代理机构 永新专利商标代理有限公司
代理人 王 英 刘炳胜
权利要求书 3 页 说明书 9 页 附图 7 页

[54] 发明名称

防止来自网络搜索或超链接的恶意软件重定向的技术

[57] 摘要

描述了用于建立网页的可信性以防止来自网络搜索或超链接的恶意软件重定向的各种技术。一种装置可以包括信任引擎来确定一个或多个网页中的每一个的可信度指示。信任引擎基于为网页确定的可信度指示，将信息附加到所述一个或多个网页的每一个标签中。可以描述和声明了其它实施例。



1、一种装置，包括：

信任引擎，用于确定一个或多个网页中的每一个网页的可信度指示，其中，所述信任引擎基于为网页确定的可信度指示，将信息附加到所述一个或多个网页的每一个标签中。

2、根据权利要求 1 所述的装置，其中，

所述可信度是网页是否包含恶意软件内容的指示。

3、根据权利要求 2 所述的装置，其中，

向用户显示具有所述附加的信息的所述一个或多个网页。

4、根据权利要求 2 所述的装置，其中，

声誉记录器使用存储在历史数据库中的信息来确定要附加到所述一个或多个网页的每一个标签上的信息。

5、根据权利要求 4 所述的装置，其中，

所述历史数据库用于存储记录，其中，每一个记录基于标准来表示网页的信息，其中，所述标准包括以下各项中的一项或多项：首次发现所述网页的日期、最后发现所述网页的日期、所述网页被识别为包含恶意软件内容的日期以及指示所述网页被发现的总次数的计数值。

6、根据权利要求 5 所述的装置，其中，

所述记录被动态更新。

7、一种系统，包括：

通信接口；以及

搜索引擎，用于基于来自用户的一个或多个关键字来进行网络搜索，以产生网页的列表，其中，所述搜索引擎确定所述网页中的每一个网页的

可信度指示，其中，所述搜索引擎基于为网页确定的可信度指示，将信息附加到所述一个或多个网页的每一个标签中。

8、根据权利要求 7 所述的系统，其中，

所述可信度是网页是否包含恶意软件内容的指示。

9、根据权利要求 8 所述的系统，其中，

向用户显示具有所述附加的信息的所述一个或多个网页。

10、根据权利要求 8 所述的系统，其中，

声誉记录器使用存储在历史数据库中的信息来确定要附加到所述一个或多个网页的每一个标签上的信息。

11、根据权利要求 10 所述的系统，其中，

所述历史数据库用于存储记录，其中，每一个记录基于标准来表示网页的信息，其中，所述标准包括以下各项中的一项或多项：首次发现所述网页的日期、最后发现所述网页的日期、所述网页被识别为包含恶意软件内容的日期以及指示所述网页被发现的总次数的计数值。

12、根据权利要求 11 所述的系统，其中，

所述记录被动态地更新。

13、一种方法，包括：

确定一个或多个网页中的每一个网页的可信度指示；以及

基于为网页确定的可信度指示，将信息附加到所述一个或多个网页的每一个标签中。

14、根据权利要求 13 所述的方法，其中，

所述可信度是网页是否包含恶意软件内容的指示。

15、根据权利要求 14 所述的方法，还包括：

使得向用户显示具有所述附加的信息的所述一个或多个网页。

16、根据权利要求 14 所述的方法，还包括：

使用存储在历史数据库中的信息来确定要附加到所述一个或多个网页的每一个标签上的信息。

17、根据权利要求 16 所述的方法，其中，

所述历史数据库用于存储记录，其中，每一个记录基于标准来表示网页的信息，其中，所述标准包括以下各项中的一项或多项：首次发现所述网页的日期、最后发现所述网页的日期、所述网页被识别为包含恶意软件内容的日期以及指示所述网页被发现的总次数的计数值。

18、根据权利要求 17 所述的方法，其中，

所述记录被动态地更新。

防止来自网络搜索或超链接的恶意软件重定向的技术

背景技术

近来，已经报导了大量与互联网搜索相关的恶意软件重定向。据报导，已经揭露了为了获得高的搜索引擎排名而仔细创建的数万个人网页。这些恶意软件站点使用普通的、合法的术语来将用户引导到它们的网站。恶意软件站点的一个目的是用恶意软件感染人们的计算机。

目前的搜索引擎用元数据提供的摘要信息向用户返回包含关键字的所有网页。因此，用户从搜索结果列表中无法得知所返回的网页或站点是否包含或可能包含恶意软件。

附图说明

图 1 说明了系统的一个实施例。

图 2 说明了信任引擎的一个实施例。

图 3 说明了在网页历史数据库中的记录的一个实施例。

图 4 说明了由搜索引擎跟踪的记录的级别的一个实施例。

图 5 说明了逻辑框图的一个实施例。

图 6 说明了逻辑框图的一个实施例。

图 7 说明了系统的一个实施例。

具体实施方式

各个实施例可以一般针对用于建立网页的可信性以防止来自 web 搜索或超链接的恶意软件重定向的技术。可以通过建立由通过搜索引擎进行的 web 搜索而得到的每个网页或超链接的可信度来达到这个目的。然后向用户提供每一个网页的可信度的指示，以帮助防止用户访问可能包含恶意软件内容的网页。可以描述和声明其它实施例。

各个实施例可以包括一个或多个元件。元件可以包括用于执行某些操作的任何结构。可以根据给定的一组设计参数或性能约束的需要，将每一

个元件实现为硬件、软件或它们的任意组合。尽管可以以示例的方式，用某个拓扑结构中的有限数目的元件来描述实施例，然而，根据给定实现的需要，实施例可以包括替代拓扑结构中的更多或更少的元件。值得注意的是，任何对“一个实施例”或“实施例”的提及意味着结合该实施例描述的特定的特征、结构或特性包括在至少一个实施例中。在说明书中各个地方出现的短语“在一个实施例中”并不必然全指相同的实施例。

图 1 说明了系统 100 的一个实施例。如图 1 所示，系统 100 可以包括多个元件，例如用户输入设备 102、网络连接 104、搜索引擎 106、信任引擎 108 和恶意软件过滤器 110。然而，实施例并不限于该图中所示的元件。

在高层次上，在实施例中，用户可以经由用户输入设备 102 和网络连接 104 向搜索引擎 106 提供关键字来执行 web 搜索。搜索引擎 106 基于所提供的关键字来确定网页或超链接结果的列表。然后搜索引擎 106 将网页结果的列表提供给信任引擎 108。对于在列表中的每一个网页，信任引擎 108 确定该网页的可信度。在一些实施例中，网页的可信度反映该网页是否可能包含恶意软件内容。信任引擎 108 向用户返回在每一个网页标签上添加了指示各个网页的可信级别的信息的网页结果的列表。用户能够查看添加的可信级别信息，以帮助防止用户访问可能包含恶意软件内容的网页。在实施例中，可以使用可选的恶意软件过滤器 110，以便在将搜索结果返回给用户之前滤除潜在地恶意站点或网页。

在各个实施例中，搜索引擎 106 和信任引擎 108 可以包括用于执行网页搜索并用于向用户提供包括恶意软件内容可信度的指示的网页或超链接结果的列表的实体。信任引擎 108 可以集成到搜索引擎 106 中或者是与搜索引擎 106 分离的实体。根据给定的一组设计参数和性能约束，可以用硬件元件、软件元件或上述两者的组合来实现引擎 106 和 108。另外，引擎 106 和 108 可以实现为任意数目的不同网络、系统、设备或部件的一部分，例如基于处理器的系统、计算机系统、计算机子系统、计算机、设备、工作站、终端、服务器、个人计算机（PC）、膝上型计算机、超膝上型计算机、手持计算机、个人数字助理（PDA）、机顶盒（STB）、电话、移动电话、蜂窝电话、手机、智能电话、平板计算机、无线接入点、基站（BS）、用户站（SS）、移动用户中心（MSC）、无线电网络控制器（RNC）、微处理器、诸

如专用集成电路（ASIC）的集成电路、可编程逻辑器件（PLD）、诸如通用处理器、数字信号处理器（DSP）和/或网络处理器这样的处理器、接口、路由器、集线器、网关、网桥、交换机、电路、逻辑门、寄存器、半导体器件、芯片、晶体管、或任何其它设备、机器、工具、装置、部件、或它们的组合。实施例并不限于此。

在各个实施例中，可以在不同的设备中分别实现引擎 106 和 108，所述设备用于在各种类型的有线或无线通信介质上通信。另外，可以意识到，也可以将引擎 106 和 108 实现为单个设备中的不同的部件或进程。实施例并不限于此。

对于给定实现，可以基于任意数目的信任标准来定义和更改网页或超链接的可信度。信任标准的例子可以包括：网页是否具有完全合格的域地址、包含该网页的设备的网络地址（例如，网际协议地址）、任何前述标准的存在时间、外部影响者、第三方反馈（例如，发布恶意软件站点列表的服务）、网页的验证结果（例如，恶意软件内容被识别的日期（如果可用））、首次被搜索引擎发现的日期、被搜索引擎发现的最后日期、被搜索引擎发现的总次数等。在实施例中，可以随着时间的变化来调整信任值，以反映给予给定网页的可信级别上的任何变化。

如图 2 所示，在各个实施例中，信任引擎 108 可以包括网页验证器 202、网页历史数据库 204 和网页声誉记录器 206。在高层次上，在实施例中，在搜索引擎 106 基于用户关键字向用户返回所有网页结果之前，信任引擎 108 添加关于每一个网页的历史的信息，并将历史信息作为搜索结果的一部分提供给用户作为参考。在数据库 204 中存储关于网页的历史的信息。如果在历史数据库 204 中没有特定网页的信息，则使用验证器 202 来验证该网页或确定是否由恶意软件站点（可能包含恶意软件内容）包含该网页。验证器 202 可以实时工作或离线工作。验证器 202 的结果随后被记录在数据库 204 中。网页声誉记录器 206 随后使用历史数据库 204 中的信息来将信息附加到网页结果的每一个网页标签上。附加的信息向用户指示每个网页结果的恶意软件内容可信度。例如，附加的信息可以具有诸如“搜索引擎已经发现这个网页或站点 1234 天”、或“这个网页或站点可能包含恶意软件”、或“这个网站不是已知的并且具有低可信级别”、或“这个网站是公

知的并且具有高可信级别”等的信息。这里，当搜索引擎 106 向用户返回具有添加的可信度信息的所有网页结果时，用户不太可能访问可能包含恶意软件内容的网页。

存储在历史数据库 204 中的信息被用于确定网页或超链接的可信度。如上所述，对于给定实现，可以基于任意数目的信任标准来定义或更改这个信息。上面提供了信任标准的一些可能的例子，但其实际上是无限的。图 3 说明了可以由历史数据库 204 保存的记录的示例性列表。图 3 示出的例子包括用于每个记录 302 到 308 的信任标准：“网页地址”、“首次发现日期”、“最后发现日期”、“恶意软件识别日期”和“总发现次数计数”。在实施例中，可以随着时间的变化来调整信任标准的值，以反映任何变化。

例如，记录 302 具有网页地址 www.intel.com/press；由搜索引擎 106 在 1994 年 1 月 1 日首次发现；由搜索引擎 106 在 2007 年 11 月 30 日最后一次发现；从未被验证器 202 识别为包含恶意软件内容；并且已经被搜索引擎 106 发现了总计多于 10^9 次。这里，基于记录 302 的信息，可以由声誉记录器 206 将诸如“这个网站是公知的并且具有高可信级别”的信息附加到网页 www.intel.com/press 的网页标签上。

图 3 中说明的另一个示例性记录是记录 304。记录 304 具有网页地址 www.bad.guy.county；由搜索引擎 106 在 2007 年 10 月 1 日首次发现；由搜索引擎 106 在 2007 年 11 月 30 日最后一次发现；被验证器 202 在 2007 年 11 月 27 日识别为包含恶意软件内容；以及已经被搜索引擎 106 发现了总计 10000 次。这里，基于记录 304 的信息，可以由声誉记录器 206 将诸如“这个网页或站点可能包含恶意软件”的信息附加到网页 www.bad.guy.county 的网页标签上。

在一些实施例中，如果无限地保存每一个结果网页的记录，那么数据库 204 将无限地增长，因此需要关注历史数据库 204 的可扩展性。各个实施例提供的数据库 204 中的记录列表是动态的，因此，通过清除满足某些标准的记录来保留更少的无用记录。尽管这种标准实际上可以是无限的，但它们可以包括如下标准，例如：比测量单位更久的记录（例如，距搜索引擎最后发现的时间超过 1 年的记录）、包括不再存在的网页的记录、其网页被搜索引擎发现的次数低于特定次数的记录等。在实施例中，如果网页

仍然存在并且被确定为包含恶意软件内容，则可以拒绝将其清除出数据库204。重新参考图3，可以认为记录308是能够从数据库中清除的记录。这里，可以基于搜索引擎106发现它的最后时间来清除网页www.someoldsite.com/news/1995。提供图3仅仅用于说明的目的，并不意味着限制本发明的实施例。

在实施例中，搜索引擎106和/或信任引擎108还可以为历史数据库204中记录追踪的层级设置标准。图4说明了一个这样的例子。如图4所示，这样的标准可以限制域名的粒度（左指示箭头，其中最小值是1，最大值是3）、页面层级的粒度（右指示箭头，其中最小值是2，最大值是10）、不同域名的数目（垂直地位于左侧，其中最大值是100）、不同页面层级的数目（垂直地位于右侧，其中最大值是10K）以及水平层级的数目乘以垂直层级的数目（其中它必须小于1百万）。提供图4仅仅用于说明的目的，并不意味着限制本发明的实施例。

参照下面的附图和相应例子，可以进一步描述上述实施例的操作。附图中的一些可以包括逻辑流程。尽管本文给出的这样的附图可以包括特定的逻辑流程，但是可以意识到，所述逻辑流程仅仅提供了如何可以实现本文所描述的一般功能的例子。另外，如果没有另外指明，那么并非必须按照图示的顺序来执行给定的逻辑流程。另外，可以由硬件元件、由处理器执行的软件元件或它们的任意组合来实现给出的逻辑流程。实施例并不限于此。

图5说明了逻辑流程的一个实施例。图5说明了逻辑流程500。逻辑流程500可以是由本文描述的一个或多个实施例（例如图1的搜索引擎106和/或信任引擎108）执行的操作的代表。如逻辑流程500所示，搜索引擎从用户接收关键字来执行网络搜索（框502）。搜索引擎基于所提供的关键字来确定网页或超链接结果的列表（框504）。搜索引擎向信任引擎提供网页结果列表（框506）。对于列表中的每一个网页，信任引擎确定页面的恶意软件内容可信度（框508）。后面参考图6更详细地描述了框508。信任引擎向用户返回向每一个网页标签添加了指示网页的可信度的信息的网页结果列表（框510）。使用这些附加信息，用户将有希望能够避免访问可能包含恶意软件内容的网页。

图 6 说明了逻辑流程 600 以及信任引擎如何确定页面的恶意软件内容可信度的实施例（图 5 中的框 508）。参考逻辑流程 600，对于每一个网页，信任引擎检查在历史数据库（例如图 2 的历史数据库 204）中记录的历史（框 602）。在菱形框 604，如果网页是新的，那么在历史数据库中为该网页创建新记录（框 610）。验证器（例如图 2 的网页验证器 202）确定是否由恶意软件站点来保存该网页（框 612）。相应地更新历史数据库（框 606）。在菱形框 604，如果在历史数据库中已经包括了该网页，那么也相应地更新数据库（框 606）。网页记录器（例如图 2 的记录器 206）使用历史数据库中的信息来将关于恶意软件内容可信度的信息添加到每一个网页标签（框 608）。

图 7 说明了系统的一个实施例。图 7 说明了系统 700。系统 700 可以是适于本文描述的一个或多个实施例（例如搜索引擎 106 和/或信任引擎 108）使用的系统或结构的代表。如图 7 所示，系统 700 可以包括基于处理器的系统，该基于处理器的系统包括处理器 702，其通过总线 712 耦合到存储器 704，网络接口 708，以及输入/输出（I/O）接口 710。存储器 704 还可以耦合到信任引擎 706。对于给定的实现，可以为系统 700 实现更多或更少的元件。

在各个实施例中，处理器 702 可以代表任何合适的处理器或逻辑器件，例如复杂指令集计算机（CISC）微处理器、精简指令集计算机（RISC）微处理器、超长指令字（VLIW）微处理器、实现指令集组合的处理器或其它处理器设备。在一个实施例中，例如，处理器 702 可以被实现为通用处理器，例如由位于加利福尼亚州圣塔克拉拉的 Intel®公司制造的处理器。处理器 702 还可以被实现为专用处理器，例如控制器、微控制器、嵌入式处理器、数字信号处理器（DSP）、网络处理器、媒体处理器、输入/输出（I/O）处理器、媒体访问控制（MAC）处理器、无线基带处理器、现场可编程门阵列（FPGA）、可编程逻辑器件（PLD）等。然而，实施例并不限于此。

在一个实施例中，存储器 704 可以代表能够存储数据的任何机器可读或计算机可读介质，包括易失性存储器和非易失性存储器。例如，存储器 704 可以包括：只读存储器（ROM）、随机存取存储器（RAM）、动态 RAM（DRAM）、双倍数据速率 DRAM（DDRAM）、同步 DRAM（SDRAM）、静态 RAM（SRAM）、可编程 ROM（PROM）、可擦除可编程 ROM（EPROM）、

电可擦除可编程 ROM（EEPROM）、闪速存储器、诸如铁电聚合物存储器的聚合物存储器、奥氏存储器、相变或铁电存储器、硅氧化氮氧化硅（SONOS）存储器、磁或光存储卡，或任何其它类型的适于存储信息的介质。值得注意的是，存储器 704 的一些部分或整体可以包括在与处理器 702 相同的集成电路上。或者，存储器 704 的一些部分或整体可以布置在处理器 702 的集成电路之外的集成电路或其它介质上，例如硬盘驱动器，并且处理器 702 可以经由总线 712 访问存储器 704。实施例并不限于此。

在各个实施例中，系统 700 可以包括网络接口 708。系统 700 可以被实现为无线设备、有线设备或两者的组合。当实现为无线设备时，网络接口 708 可以包括适合于在无线共享媒介上通信的部件和接口，例如一个或多个天线、发射机、接收机、收发器、放大器、滤波器、控制逻辑等。无线共享媒介的例子可以包括无线频谱的一部分，例如 RF 频谱等。当实现为有线设备时，网络接口 708 可以包括适合于在有线通信媒介上通信的部件和接口，例如输入/输出（I/O）适配器、将 I/O 适配器与相应的有线通信媒介连接的物理连接器、网络接口卡（NIC）、磁盘控制器、视频控制器、音频控制器等。有线通信媒介的例子可以包括电线、电缆、金属导线、印刷电路板（PCB）、背板、交换结构、半导体材料、双绞线、同轴电缆、光纤等。实施例并不限于此。

在各个实施例中，I/O 710 可以包括可由系统 700 的元件访问或共享的任何期望的输入和输出元件，例如键盘、鼠标、导航按键、专用硬件按键或开关、照相机、扩音器、扬声器、话音编解码器、视频编解码器、音频编解码器、显示器、触摸屏等。实施例并不限于此。

在各个实施例中，信任引擎 706 可以是适合于由通用处理器或专用处理器执行的软件，上述处理器例如处理器 702。根据给定实现的需要，还可以由硬件或硬件与软件的组合来实现信任引擎 706。实施例并不限于此。

本文已经阐明了许多具体细节来提供对实施例的透彻理解。然而，本领域的技术人员可以理解，可以在没有这些具体细节的情况下实施这些实施例。在其它情形中，未详细描述公知的操作、部件和电路，以便不模糊实施例。可以意识到，本文公开的具体结构和功能细节可以是代表性的，并非必然地限制实施例的范围。

可以使用硬件元件、软件元件或两者的组合来实现各个实施例。硬件元件的例子可以包括处理器、微处理器、电路、电路元件（例如，晶体管、电阻器、电容器、电感等）、集成电路、专用集成电路（ASIC）、可编程逻辑器件（PLD）、数字信号处理器(DSP)、现场可编程门阵列(FPGA)、逻辑门、寄存器、半导体器件、芯片、微芯片、芯片组等。软件的例子可以包括软件部件、程序、应用程序、计算机程序、应用程序、系统程序、机器程序、操作系统软件、中间件、固件、软件模块、例程、子例程、函数、方法、过程、软件接口、应用程序接口（API）、指令集、计算代码、计算机代码、代码段、计算机代码段、字、值、符号或它们的任意组合。可以根据任意数目的因素来确定是否用硬件元件和/或软件元件来实现实施例，上述因素例如：期望的计算速率、功率水平、耐热性、处理周期预算、输入数据速率、输出数据速率、存储器资源、数据总线速度和其它设计或性能约束。

可以使用措辞“耦合”和“连接”以及它们的派生词来描述一些实施例。这些术语并非旨在互相作为同义词。例如，可以使用术语“连接”和/或“耦合”来描述一些实施例，以表明两个或更多元件相互之间是直接物理连接或电连接的。然而，术语“耦合”还可以意味着两个或更多元件相互之间不是直接连接的，但是仍然相互协作或交互。

例如，可以使用可以存储指令或一组指令的机器可读介质或制品来实现一些实施例，如果由机器执行该指令，可以使得机器执行根据实施例的方法和/或操作。这样的机器可以包括，例如，任何合适的处理平台、计算平台、计算设备、处理设备、计算系统、处理系统、计算机、处理器等，并可以使用硬件和/或软件的任意合适组合来实现该机器。机器可读介质或制品可以包括，例如，任何合适类型的存储器单元、存储器设备、存储器制品、存储介质、储存设备、储存制品、储存介质和/或储存单元，例如，存储器、可移除或不可移除介质、可擦除或不可擦除介质、可写或可重写介质、数字或模拟介质、硬盘、软盘、光盘只读存储器（CD-ROM）、可录光盘（CD-R）、可重写光盘（CD-RW）、光盘、磁性介质、磁光介质、可移除存储卡或盘、各种类型的数字多用途光盘（DVD）、磁带、盒式磁带等。指令可以包括使用任何合适的高级、低级、面向对象、可视化、编译的和/

或解释的编程语言而实现的任何合适类型的代码，例如源代码、编译代码、解释代码、可执行代码、静态代码、动态代码、加密代码等。

如果没有特别声明，可以意识到，诸如“处理”、“计算”、“运算”、“确定”等的术语是指计算机或计算系统或类似的电子计算设备的动作和/或处理，其将表示为计算系统的寄存器和/或存储器中的物理量（例如，电子的）的数据操作和/或转换为其它数据，这些其它数据同样地被表示为计算系统的存储器、寄存器或其它这样的信息存储、传输或显示设备中的物理量。实施例并不限于此。

虽然本文描述了实施例的某些特征，但对于本领域的技术人员来说，可以实现许多更改、替代、改变和等价物。因此应该理解，所附的权利要求旨在覆盖落入实施例的实质精神内的所有这样的更改和改变。

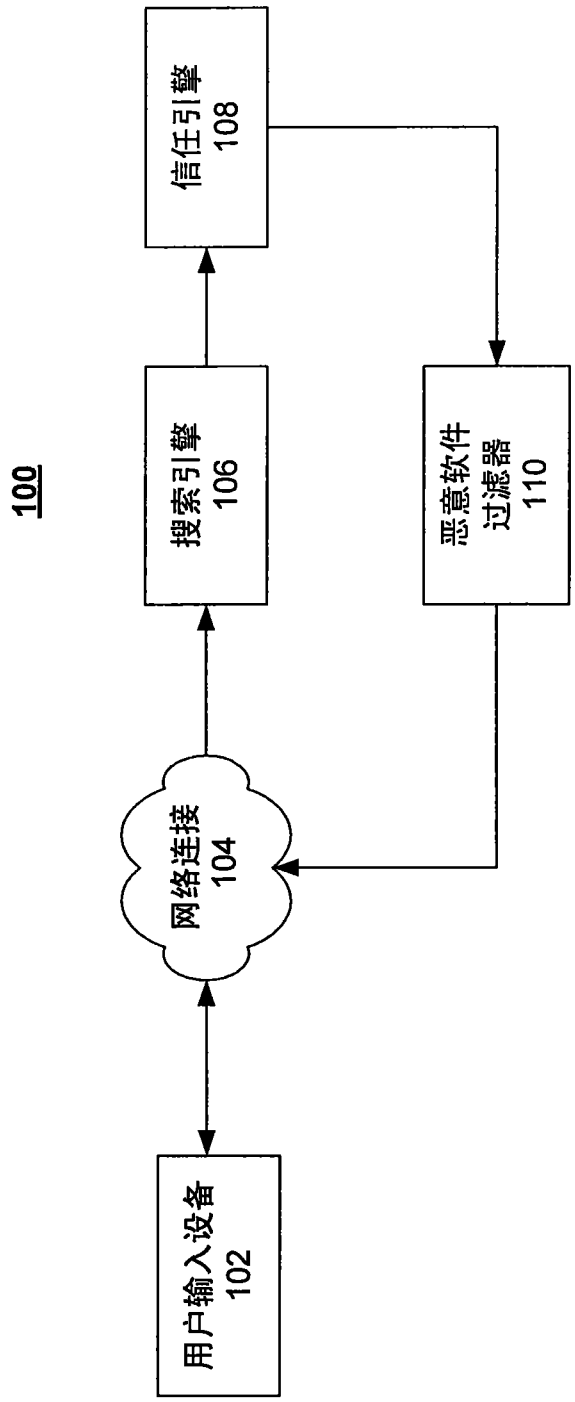


图1

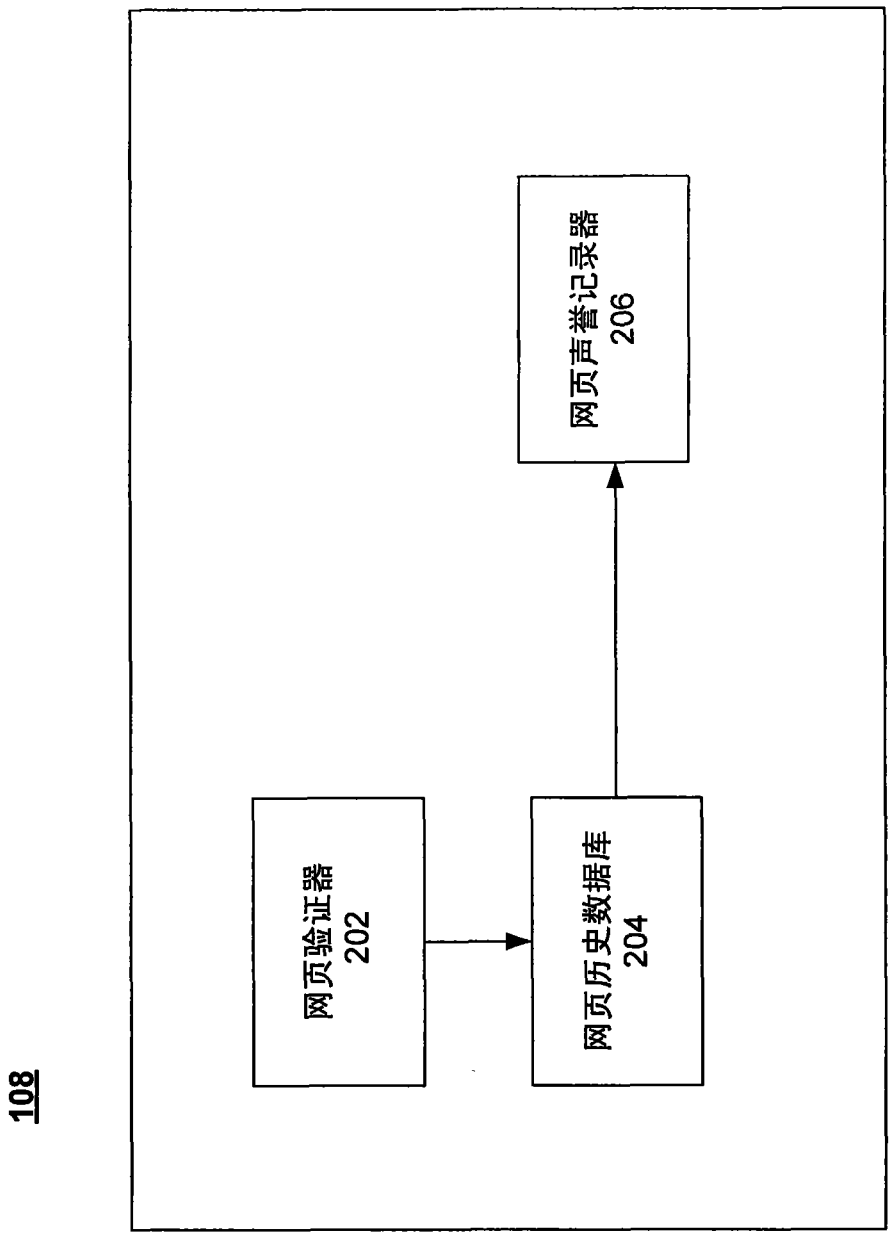
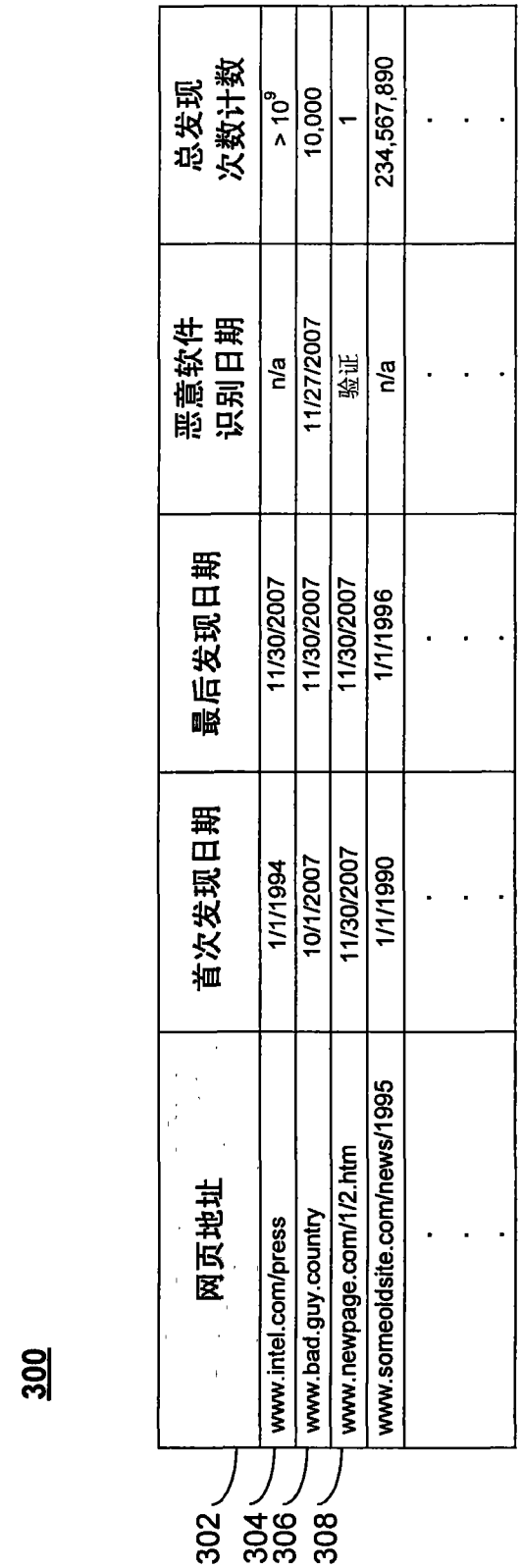


图2



网页地址	首次发现日期	最后发现日期	恶意软件识别日期	总发现次数计数
www.intel.com/press	1/1/1994	11/30/2007	n/a	$> 10^9$
www.bad.guy.country	10/1/2007	11/30/2007	11/27/2007	10,000
www.newpage.com/1/2.htm	11/30/2007	11/30/2007	验证	1
www.someoldsite.com/news/1995	1/1/1990	1/1/1996	n/a	234,567,890
. . .	. . .	. . .	. . .	. . .

图3

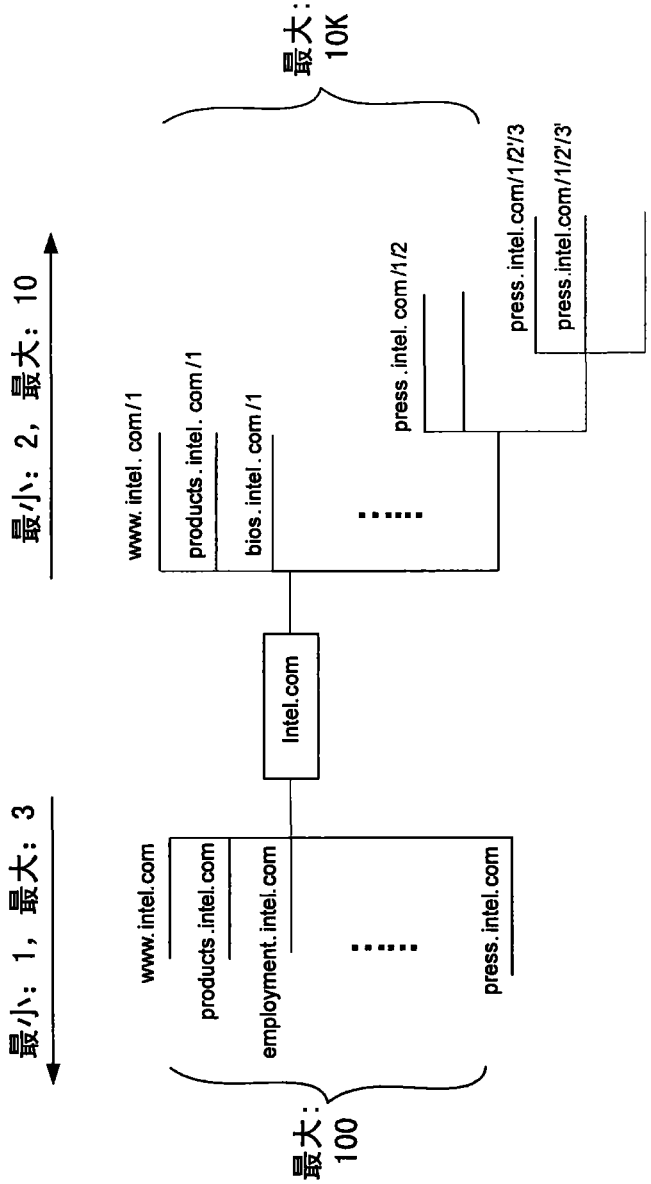

最小：1，最大：3
最小：2，最大：10
最大：100
最大：10K
Intel.com
www.intel.com
products.intel.com
employment.intel.com
press.intel.com
www.intel.com/1
products.intel.com/1
bios.intel.com/1
press.intel.com/1/2
press.intel.com/1/2/3
press.intel.com/1/2/3'

图4

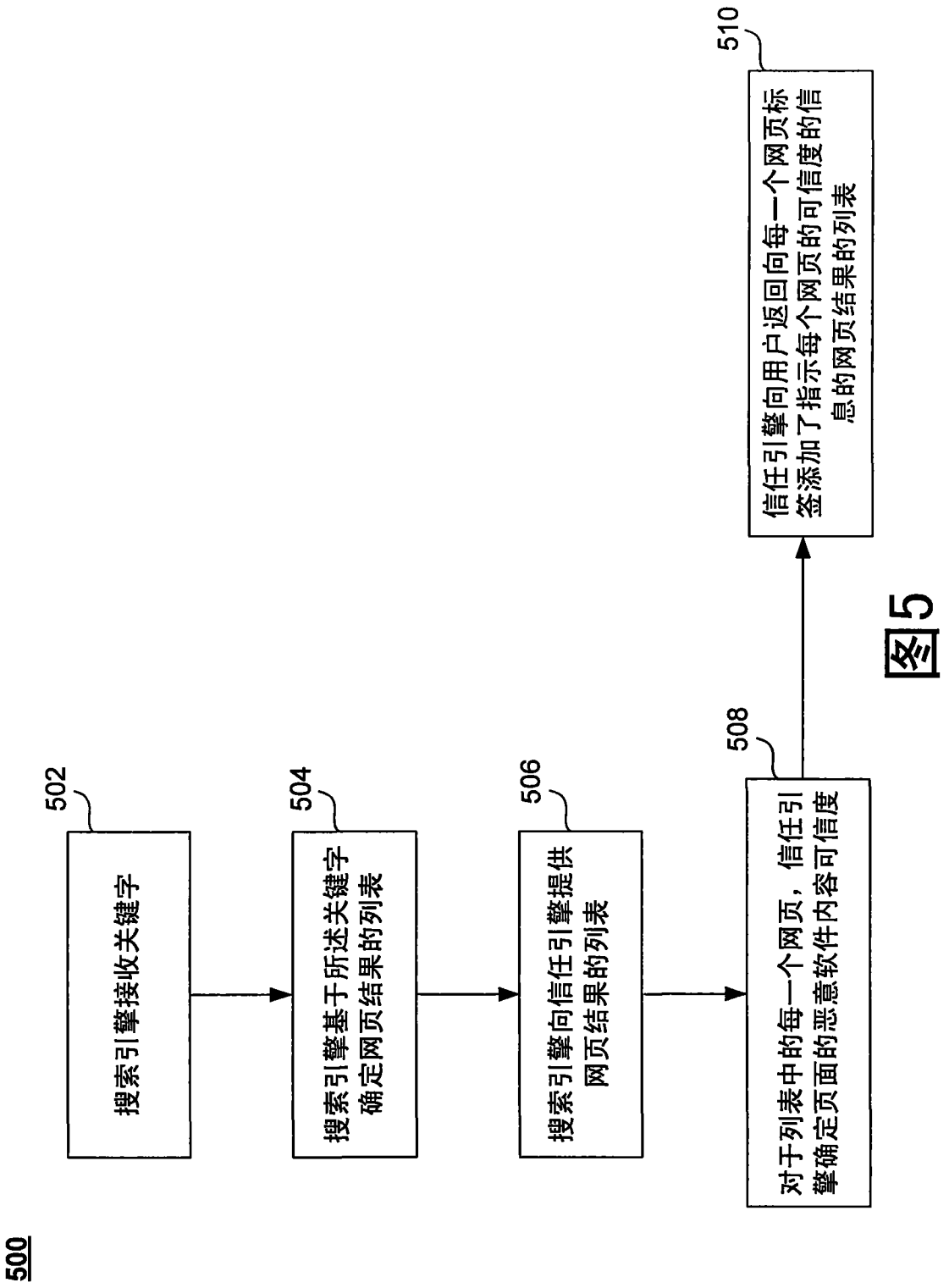

500
502
搜索引擎接收关键字
504
搜索引擎基于所述关键字确定网页结果的列表
506
搜索引擎向信任引擎提供网页结果的列表
508
对于列表中的每一个网页，信任引擎确定页面的恶意软件内容可信度
510
信任引擎向用户返回向每一个网页标签添加了指示每个网页的可信度的信息的网页结果的列表

图5

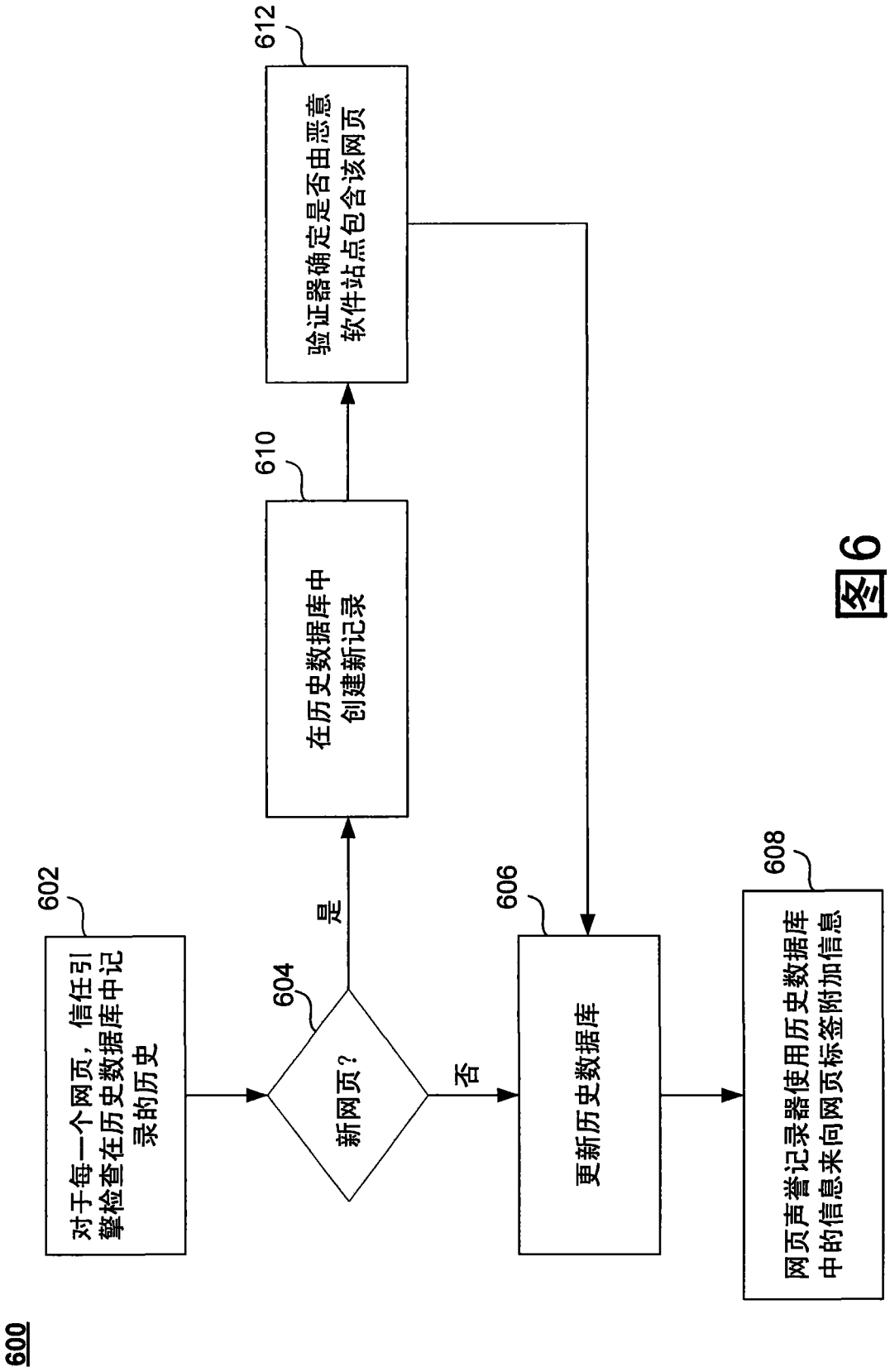

600
602
对于每一个网页，信任引擎检查在历史数据库中记录的历史
604
新网页？
是
否
610
在历史数据库中创建新记录
612
验证器确定是否由恶意软件站点包含该网页
606
更新历史数据库
608
网页声誉记录器使用历史数据库中的信息来向网页标签附加信息

图6

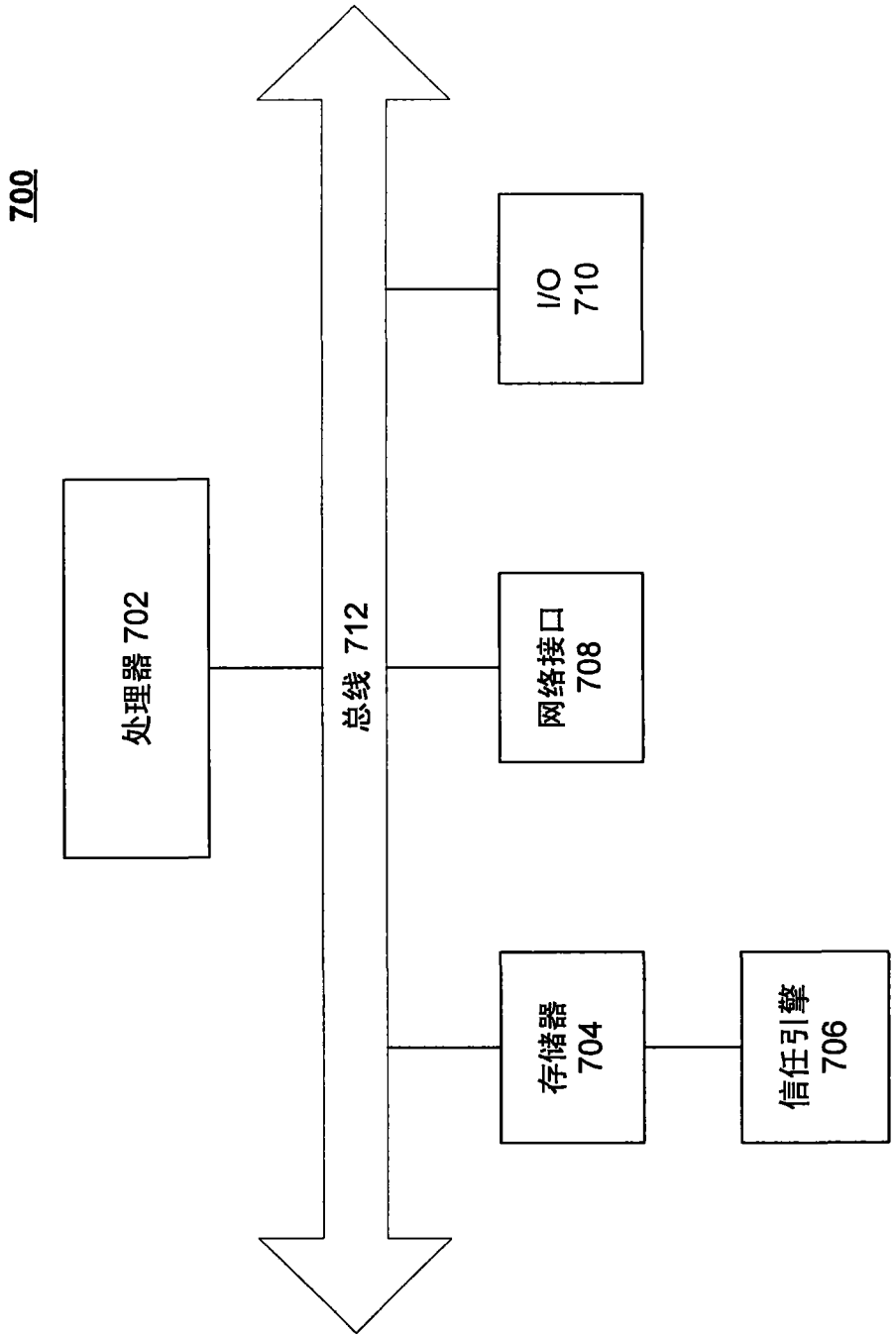


图7