



(12) 发明专利

(10) 授权公告号 CN 101742273 B

(45) 授权公告日 2014. 08. 27

(21) 申请号 200910222852. 4

US 20080120367 A1, 2008. 05. 22,

(22) 申请日 2009. 11. 19

US 20030217264 A1, 2003. 11. 20,

(30) 优先权数据

审查员 吴永兴

08305840. 4 2008. 11. 26 EP

(73) 专利权人 汤姆森许可贸易公司

地址 法国布洛涅 - 比郎库尔

(72) 发明人 埃里克·迪尔 阿兰·迪朗

斯特凡纳·奥诺

(74) 专利代理机构 中科专利商标代理有限责任

公司 11021

代理人 王波波

(51) Int. Cl.

H04N 21/6334 (2011. 01)

H04N 21/4627 (2011. 01)

(56) 对比文件

US 20060053232 A1, 2006. 03. 09,

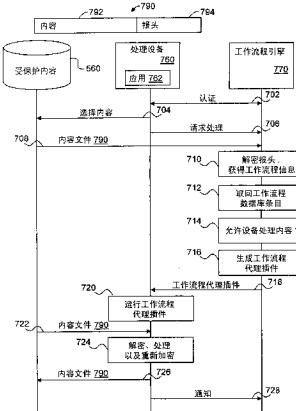
权利要求书2页 说明书7页 附图6页

(54) 发明名称

根据工作流程处理数字内容的方法和系统

(57) 摘要

本发明提供一种根据工作流程处理数字内容(532、792、832)的方法。接收数字内容(532、792、832)，并检查所述工作流程的信息，以决定是否授权处理设备来处理所述内容，所述工作流程强制所述数字内容在包括至少两个节点在内的处理链中处理，其中如果所述处理设备与所述处理链中的所述下一个处理所述数字内容的节点相对应，则授权所述处理设备处理所述内容。如果授权所述处理设备处理所述内容，则处理所述数字内容，并更新所述工作流程的信息。本发明还提供一种系统和数字支持介质。



1. 一种在至少处理设备 (510) 中根据工作流程处理数字内容 (532) 的方法, 其中所述处理设备 (510) 包括所述处理设备的标识符 (512), 所述方法包括下列步骤 :

a) 由所述处理设备 (510) 接收所述数字内容 (532) ;

b) 由所述处理设备 (510) 向第二设备 (520) 发送 (606) 内容标识符和所述处理设备的标识符 (512) ;

c) 由所述第二设备 (520) 通过获得 (610) 所述数字内容 (532) 的工作流程的信息、并将所述信息与所述处理设备的标识符 (512) 进行比较 (612) 来检查所述工作流程的信息, 以决定是否授权处理设备来处理所述内容, 所述信息包括通过利用所述内容标识符和最近处理了所述数字内容的设备的标识符所确定的可由至少一个处理设备应用于所述内容的至少一个动作; 以及

如果授权所述处理设备处理所述内容 :

d) 由所述处理设备 (510) 处理所述数字内容; 以及

e) 由所述第二设备 (520) 更新所述工作流程的信息。

2. 根据权利要求 1 所述的方法, 其中, 所述数字内容是以加密形式接收的, 以及步骤 d) 在对所述内容的进行处理之前还包括下列子步骤 :

d1) 从所述第二设备向所述处理设备 (510) 提供针对加密后的数字内容的解密密钥; 以及

d2) 由所述处理设备 (510) 对所述加密后的数字内容进行解密;

以及, 在对所述内容的进行处理之后:

d3) 由所述处理设备 (510) 对处理后的数字内容进行加密。

3. 一种在至少处理设备 (760) 中根据工作流程处理数字内容 (792) 的方法, 所述方法包括下列步骤 :

a) 由所述处理设备 (760) 向第二设备 (770) 请求 (706) 对所述数字内容 (792) 的处理,

b) 由所述第二设备 (770) 接收所述数字内容 (792) ;

c) 由所述第二设备 (770) 通过获得 (712) 所述数字内容 (792) 的工作流程的信息、并将所述信息与所述处理设备的标识符 (762) 进行比较 (714) 来检查所述工作流程的信息, 以决定是否授权处理设备来处理所述内容, 所述信息包括可由与所述内容 (792) 相对应的至少一个处理设备应用于所述内容的至少一个动作; 以及

如果授权所述处理设备处理所述内容 :

d) 由所述第二设备 (770) 向所述处理设备 (760) 发送 (718) 处理插件;

e) 由所述处理设备 (760) 运行 (720) 所述处理插件, 并接收 (722) 所述数字内容 (792);

f) 由所述处理设备 (760) 处理所述数字内容; 以及

g) 由所述第二设备 (770) 更新所述工作流程的信息。

4. 根据权利要求 3 所述的方法, 其中, 所述数字内容是以加密形式接收的, 以及步骤 f) 在对所述内容的进行处理之前还包括下列子步骤 :

f1) 从所述第二设备向所述处理设备 (760) 提供针对加密后的数字内容的解密密钥; 以及

f2) 由所述处理设备 (760) 对所述加密后的数字内容进行解密；

以及,在对所述内容的进行处理之后：

f3) 由所述处理设备 (760) 对处理后的数字内容进行加密。

5. 一种在至少处理设备 (810) 中根据工作流程处理数字内容 (832) 的方法,其中所述处理设备 (810) 包括所述处理设备的标识符 (812),所述方法包括下列步骤：

a) 由处理设备 (810) 接收所述数字内容 (832)；

b) 由所述处理设备 (810) 向第二设备 (820) 发送 (904) 所述数字内容的内容标识符以及最近处理了所述数字内容 (832) 的设备的标识符；

c) 利用所述内容标识符和最近处理了所述数字内容 (832) 的设备的标识符来确定可由至少一个处理设备应用于所述内容的至少一个动作；

d) 由所述第二设备 (820) 生成 (910) 辅助信息,所述辅助信息包括可由至少一个处理设备应用于所述内容的至少一个动作；

e) 由所述处理设备 (810) 通过将所述处理设备 (810) 的标识符与所述辅助信息进行比较来检查所述工作流程的信息,以决定是否授权处理设备来处理所述内容;以及

如果授权所述处理设备处理所述内容：

f) 由所述处理设备 (810) 处理所述数字内容;以及

g) 由所述处理设备 (810) 更新所述工作流程的信息。

6. 根据权利要求 5 所述的方法,其中,所述数字内容是以加密形式接收的,以及步骤 f) 在对所述内容的进行处理之前还包括下列子步骤：

f1) 从所述第二设备向所述处理设备 (810) 提供针对加密后的数字内容的解密密钥；以及

f2) 由所述处理设备 (810) 对所述加密后的数字内容进行解密；

以及,在对所述内容的进行处理之后：

f3) 由所述处理设备 (810) 对处理后的数字内容进行加密。

7. 一种用于根据工作流程处理数字内容 (532、792、832) 的系统 (500、800),所述系统包括：

- 接收机 (510、770、810),适于接收数字内容 (532、792、832)；

- 处理设备 (510、760、810),适于处理所述数字内容,其中所述处理设备 (510、760、810) 包括所述处理设备的标识符 (512、762、812)；

- 适于检查所述工作流程的信息以决定是否授权所述处理设备根据权利要求 1、3 和 5 中任一项所述的方法来处理所述内容的单元 (520、770、810)；

- 适于更新所述工作流程的信息的单元 (520、770、820)。

8. 根据权利要求 7 所述的用于根据工作流程处理数字内容 (532、792、832) 的系统 (500、800),其中,所述接收机 (510、770、810) 适于以加密形式接收所述数字内容,所述系统还包括：

- 第一单元,适于提供针对加密后的数字内容的解密密钥；

- 第二单元,适于对加密后的数字内容进行解密；

- 第三单元,适于对处理后的数字内容进行加密。

根据工作流程处理数字内容的方法和系统

技术领域

[0001] 本发明总体涉及数字内容处理,具体涉及针对数字内容的工作流程。

背景技术

[0002] 本节旨在向读者介绍现有技术中与下面要描述和 / 或要求的本发明的各个方面相关的各个方面。相信这有助于向读者提供背景信息,以便于更好地理解本发明的各个方面。因此,应理解,应当根据这一点来阅读这部分叙述,而不应将其接纳为现有技术。

[0003] 诸如多媒体内容(例如电影和音乐)、文档、相片等之类的内容经常需要在发布给最终用户享用之前进行处理。

[0004] 例如,电影从实际录制到发布经过许多处理步骤:剪样片、混合、数字效果添加、配音、添加字幕等等。

[0005] 容易认识到,内容提供方对处理(也称作后处理)系统有两个要求:1)严格且可跟踪的处理操作,以及2)容易传输和复制内容。本领域技术人员将理解,现有的系统满足一个或者另一个要求,但是无法同时满足这两个要求。

[0006] 模拟系统通常满足第一个要求。由于内容存储在磁带或者胶片夹上,控制处理相对比较容易:特定内容保留在特定部门中,直到将磁带发送至下一个部门。此外,万一失窃也可以跟踪磁带。另一方面,内容的传送就没那么直接了,这是由于这需要发送物理磁带,这原本就比较困难,尤其是在涉及到长距离的情况下。由于必须物理复制内容,一次向多于一个实体提供内容也较为困难。另外,在使用之后擦除和 / 或销毁内容也对用户造成了制约。

[0007] 数字系统提供了内容的简易传送和复制。然而,控制内容的处理变得更为困难:如果内容驻留在服务器上,那么很难控制谁访问了内容,并且如果一个部门错误地相信之前的部门已经完成对该内容的处理,那么可能会经常发生错误。

[0008] 图1示出了可以使用本发明的示例性处理系统。系统100包括字幕添加设备110、颜色管理设备120、配音设备140、数字特殊效果设备150、存储设备160、以及发射清除设备130,所有这些设备都是通过网络170连接的。

[0009] 在图1的系统中,例如,可以要求在内容经过发射清除130之前,将内容发送至配音140,以及可选地发送至字幕110,并且在此之前,内容通过颜色管理120和数字效果150(不按特定顺序)。由于每一个设备都能访问存储160,因而难以控制遵照工作流程来处理。

[0010] 该数字系统中的困难是数字版权管理(DRM)系统中固有的。DRM根据使用限制来控制对内容的访问。内容进行加密,并向终端用户提供单独的许可。

[0011] DRM架构包括内容提供方、内容分发方、许可发行方、以及内容用户,并且具有下列特性:1)它们在服务器周围建立,2)不允许终端用户根据获得的内容来创建新内容和许可,以及3)对内容进行解密的版权是全局的 - 用户要么拥有该权利要么不拥有。

[0012] 因此,可以认识到,大多数现有的DRM解决方案不适用于满足前文列出的两个要

求。

[0013] 国际申请 PCT/EP08/053181 提出了一种解决方案，在该解决方案中，通过让每一个处理设备存储与解密密钥和加密密钥相关联的若干规则来确保针对数字内容的工作流程。设想一下，假定数字内容要由颜色管理设备、配音设备和字幕设备按顺序来进行处理。通过使用加密密钥对内容加密来将该内容摄入系统中，只有颜色管理设备具有与该加密密钥相对应的解密密钥。颜色管理设备存储规则，该规则规定应使用加密密钥来对利用解密密码进行解密的内容进行加密，只有配音设备拥有该加密密钥相对应的解密密钥。将相同的方法应用于其他设备。这样，保证了工作流程。

[0014] 尽管这种解决方案适用于许多情况，然而在一些实例中，这种解决方案可能很难管理系统中的密钥，尤其是在由外部设备来处理内容的时候。

[0015] 因此，可以理解，需要如下的备选解决方案：能够实现其中可以容易地分发和复制数字内容的处理系统，同时还强制了严格的处理操作，该解决方案被称作数字处理管理(DPM)。

[0016] 本发明提供这样一种解决方案，以及一些变型。

发明内容

[0017] 在第一方面，本发明涉及一种根据工作流程处理数字内容的方法。接收数字内容，并检查工作流程信息，以决定是否授权处理设备来处理该内容。如果授权该处理设备来处理该内容，则处理数字内容并更新工作流程信息。

[0018] 在第一优选实施例中，以加密形式来接收该数字内容。在对内容进行处理之前，提供用于加密后的数字内容的解密密钥，并对加密后的数字内容进行解密。在对内容进行处理之后，对处理后的数字内容进行加密。

[0019] 在第二优选实施例中，该处理设备包括该处理设备的标识符。由处理设备接收该数字内容，该处理设备还将内容标识符和该处理设备的标识符发送至第二设备。第二设备通过获得与内容标识符相对应的数字内容的工作流程的信息、并将该信息与内容标识符和处理设备的标识符进行比较来执行检查。该处理设备处理内容，第二设备更新工作流程信息。

[0020] 在第三优选实施例中，该方法包括下列在先步骤：由处理设备向第二设备请求处理数字内容。该数字内容由第二设备接收，该第二设备还通过获得数字内容的工作流程的信息、并将该信息与处理设备的标识符进行比较来执行检查。第二设备向处理设备发送处理插件，该处理设备运行该处理插件，并接收该插件所处理的数字内容。第二设备执行更新。

[0021] 在第四优选实施例中，处理设备接收数字内容，并向第二设备发送该数字内容的内容标识符以及最近处理该数字内容的设备的标识符。利用该内容标识符和最近处理数字内容的设备的标识符，确定可以由至少一个处理设备应用于该内容的至少一个动作，以及第二设备生成辅助信息，该辅助信息包括所述信息。通过将处理设备的标识符与该辅助信息进行比较来执行检查，处理设备执行处理和更新。

[0022] 在第二方面中，本发明涉及一种用于根据工作流程来处理数字内容的系统。该系统包括：适于接收数字内容的接收机、适于处理数字内容的处理设备、适于检查工作流程的

信息以决定是否授权处理设备对内容进行处理的单元、以及适于更新工作流程的信息的单元。

[0023] 在第一优选实施例中,该接收机适于以加密形式接收数字内容。该系统还包括:适于提供针对加密数字内容的解密密钥的第一单元、适于对加密数字内容进行解密的第二单元、以及适于对处理后的数字内容进行加密的第三单元。

附图说明

[0024] 现在将参照附图,通过非限制性示例对本发明的优选特征进行描述,在附图中:

[0025] 图1(已经讨论过的)示出了本发明适于用其中的示例性处理系统;

[0026] 图2示出了供本发明使用的处理图;

[0027] 图3示出了根据本发明的第一优选实施例的用于数字内容处理的系统;

[0028] 图4示出了根据本发明的第一优选实施例的用于数字内容处理的方法的示例性流程图;

[0029] 图5示出了根据本发明的第一优选实施例的变型的用于数字内容处理的方法的示例性流程图;

[0030] 图6示出了根据本发明的第二优选实施例的用于数字内容处理的系统;以及

[0031] 图7示出了根据本发明的第二优选实施例的用于数字内容处理的方法的示例性流程图。

[0032] 在图中,所示框仅仅是功能实体,不必与物理分离的实体相对应。可以将这些功能实体实施为硬件、软件、或者软件和硬件的组合;此外,可以在一个或者更多集成电路上实施它们。

具体实施方式

[0033] 本发明的主要思想是一种根据工作流程处理数字内容的方法,该方法包括下列步骤:

[0034] a) 在第一设备接收数字内容

[0035] b) 向第二设备请求与数字内容相关的处理许可

[0036] c) 在第二设备中生成与该内容相关的信息

[0037] d) 检查工作流程的信息,以决定是否授权处理设备处理该内容;以及

[0038] 如果授权处理设备处理该内容:

[0039] e) 在第一设备处理数字内容;以及

[0040] f) 在第二设备中更新工作流程的信息。

[0041] 始终由中央设备(第二设备)基于上下文信息来执行处理信息的生成。例如,上下文信息可以是描述内容能够经过的所有可能处理步骤的处理图中的当前位置。

[0042] 应理解,该图仅仅是控制工作流程的示例性方式。还可以在考虑到设备和/或操作者的工作负荷的情况下控制工作流程,以使得只有具有较低工作负荷的一个或者更多设备可以在给定时间处理内容。为了让处于工作日中的位于美国的操作者处理内容,而不是让工作日已经结束的欧洲操作者来处理,还可以依赖当前时间来控制工作流程。还还可以依赖在潜在处理设备附近的人员来控制工作流程。

[0043] 可以使用任意合适的现有方法来处理密钥管理和分发（这在本发明的保护范围之外），例如由 Menezes 等人在 Handbook of Applied Cryptography, Fifth printing (August 2001), CRC Press, ISBN :0-8493-8523-7 的第 12 和 13 章中描述的方法。

[0044] 第一优选实施例

[0045] 图 3 示出了根据本发明的第一优选实施例的用于数字内容处理的系统。用于强制数字内容的工作流程的系统 500 包括：至少一个工作流程动作代理 510，适于修改数字内容 532；工作流程引擎 520；工作流程数据库 540；原始内容数据库 550；以及受保护内容数据库 560。每一个工作流程动作代理 510 存储唯一的工作流程代理标识符 (WAID) 512，优选地存储在安全位置。

[0046] 当数字内容 532 没有在被工作流程动作代理 510 处理时，对数字内容 532 进行加密（除了存储在原始内容数据库中）。将没有在被处理的数字内容 532 存储在内容文件 530 中，优选地与提供关于最近处理过数字内容 532 的工作流程动作代理 510 的 WAID 512 的信息的标识符 534 以及具有数字内容的内容标识符的报头（图中未示出）一起存储。

[0047] 工作流程引擎 520 准备在原始内容数据库 550 中存储的或者以其它任意适当的方式接收的原始内容，并且通过下列操作来准备该内容：用加扰密钥对原始数字内容进行加密以生成受保护的数字内容，以及决定将哪个工作流程用于该数字内容。将受保护的数字内容存储在受保护内容数据库 560 中，并将该数字内容的条目存储在工作流程数据库 540 中，该条目包括该数字内容的标识符、用于保护该数字内容的加扰密钥、用于该内容的工作流程、以及位置指示符。尽管如此，应当理解，为了移除已经通过的节点，每一次进行处理时还可能修改该处理图。工作流程数据库 540（和 / 或工作流程引擎）还可以存储关于 WAID512 与一个或者更多节点之间的对应关系的信息，工作流程动作代理 510 可以作为所述一个或者更多节点。

[0048] 当用户希望处理数字内容时，它从内容文件 530 中提取内容标识符，并将内容标识符与其 WAID 512 一起发送给工作流程引擎 520。工作流程动作代理 510 与工作流程引擎 520 之间的通信优选地通过安全认证信道 (SAC) 514。工作流程引擎 520 从工作流程数据库 540 取回与内容标识符相对应的条目。然后，它检查具有当前 WAID 512 的工作流程动作代理 510 是否与在最近节点（即，实例 ID 534 所指代的一个节点）之后的可能的多个节点中的一个相对应。如果允许正在请求的工作流程动作代理 510 处理数字内容 532，则工作流程引擎 520 向工作流程动作代理 510 解密所必需的内容密钥，可能将要用于保护处理后的数字内容的第二内容密钥一同发送。

[0049] 当工作流程动作代理 510 已经完成处理数字内容 532 时，它将数字内容 532 重新加密，并通知工作流程引擎 520 可以在工作流程数据库 540 中更新数字内容 532 的条目。优选地，工作流程动作代理 510 还发送内容文件 530，以存储在受保护内容数据库 560。

[0050] 图 4 示出了根据本发明的第一优选实施例的用于数字内容处理的方法的示例性流程图。

[0051] 在步骤 602，用户使用内容文件 530 的报头 536 来搜索数字内容 532。报头 536 优选地包括：工作流程 ID，标识用于内容的工作流程；能够验证数字内容 532 的完整性的字段；数字内容的标识符；能够验证报头的完整性的字段；以及包括最近节点的实例 ID 在内的元数据。优选地，对除了元数据之外的报头进行加密。然后，在步骤 604，动作代理 510 向

提供内容文件 530 的受保护内容数据库 560 请求内容文件 530。

[0052] 在步骤 606,动作代理 510 提取报头 536,并将报头 536 与其 WAID512 发送至工作流程引擎 520。在步骤 608,工作流程引擎 520 对接收的报头进行解密,并使用能够验证报头完整性的字段来验证其完整性。然后,工作流程引擎 520 取回 610 实例 ID 534,并验证 612 动作代理 510 是否被允许处理数字内容 532。如果不允许,那么工作流程引擎 520 优先地通知动作代理 510,并且中断。然而,如果允许动作代理 510 处理数字内容 532,那么工作流程引擎 520 从工作流程数据库 540 取回 614 内容密钥,并将内容密钥发送 616 至动作代理 510。

[0053] 然后,在步骤 620,工作流程动作代理 510 对数字内容 532 进行解密,并且进行处理。然后它向生成新报头的工作流程引擎 520 请求 622 新的报头,工作流程引擎 520 向动作代理 510 返回 624 新的报头,然后在步骤 626,动作代理 510 对数字内容 532 进行加密,并存储相应的内容文件。

[0054] 然后,动作引擎 520 更新 628 工作流程数据库 540 中的数字内容的条目。它通过下述操作来完成该更新:存储用于保护处理后的内容的内容密钥,以及可能地,更新位置指示符(如果使用了位置更新符的话),或者修改过程图。

[0055] 第一优选实施例的变型

[0056] 在第一优选实施例的变型中,处理设备最初不存储任何工作流程代理标识符,并且它还可以不存储用于访问数字内容的所有必需的软件。为了能够处理数字内容,该设备请求、接收并且安装工作流程代理插件。

[0057] 图 5 示出了根据本发明的第一优选实施例的变型的流程图。首先,工作流程引擎 770 认证 702 处理设备 760、适于处理数字内容的动作应用 762、以及用户(图中未示出)中的至少一个(优先地为全部)。当认证成功时,在处理设备 760 与工作流程引擎 770 之间建立安全认证信道(SAC)。

[0058] 然后,如图 5 所示,用户从受保护内容数据库 560 中选择 704 待处理的内容。然后,处理设备 760 向工作流程引擎 770 请求 706 对内容的处理。工作流程引擎 770 取回 708 与用户的选择相对应的内容文件 790,在步骤 710,对报头 794 进行解密并且提取其中的工作流程信息。工作流程引擎 770 还取回 712 与报头 794 的工作流程信息相对应的工作流程数据库条目。在步骤 714,工作流程引擎 770 决定处理设备 760 是否可以处理数字内容。优先地,通过将关于请求者(用户、处理设备 760、以及动作应用 762)的信息、内容文件 790 的报头 794 中的工作流程信息(工作流程标识符、在先节点)、来自工作流程数据库中的信息(处理图中的下一个节点)、以及可能的调度、当前时间等等进行比较来完成该决定。

[0059] 如果授权处理设备 760 来处理数字内容 792,则工作流程引擎 770 生成 716 适于强制工作流程的工作流程代理插件。该工作流程代理插件包括:用于对数字内容 792 进行解密的解密密钥,以及用于在处理之后对数字内容 792 进行重新加密的加密密钥。注意,如前所述,处理不一定意味着对数字内容 792 的修改。

[0060] 工作流程引擎 770 向处理设备 760 发送 718 工作流程代理插件,优先地在完整性验证之后,运行 720 该工作流程代理插件,并从受保护内容数据库 560 中获得 722 内容文件 790。然后,在步骤 724,处理设备 760 使用工作流程代理插件对数字内容 792 进行解密,处理该数字内容,并且使用工作流程代理插件来对其进行重新加密。

[0061] 然后,将数字内容文件 790 发送 726 至受保护内容数据库 560,以用于存储,并且处理设备 760 通知 728 工作流程引擎 770 已经对数字内容 792 进行了重新加密以及存储的内容文件。

[0062] 第二优选实施例

[0063] 在第二优选实施例中,在位于中央的工作流程数据库中包括用于内容的处理图,并且从该数据库向处理引擎发送解密密钥,但是由代理本身来判断是否允许该代理处理内容。

[0064] 图 6 示出了根据本发明的第二优选实施例的用于内容的数字内容处理的系统,图 7 示出了根据本发明的第二优选实施例的用于数字内容处理的方法的示例性流程图。

[0065] 用于强制数字内容的工作流程的系统 800 包括:至少一个工作流程动作代理 810,适于修改数字内容 832;工作流程引擎 820;以及工作流程数据库 840。每一个工作流程动作代理 810 存储唯一的工作流程代理标识符 (WAID) 812,优选地存储在安全位置。

[0066] 如同第一实施例,当数字内容 832 没有在被工作流程动作代理 810 处理时,对数字内容 832 进行加密。将没有在被处理的数字内容 832 存储在内容文件 830 中,优选地与提供关于最近处理过数字内容 832 的工作流程动作代理 810 的 WAID 812 的信息的标识符 834 以及具有数字内容的内容标识符的报头(图中未示出)一起存储。

[0067] 工作流程引擎 820 可以像第一实施例中的摄取引擎一样地准备原始内容。这样,它用加扰密钥对原始数字内容进行加密,以生成受保护的数字内容,并且决定哪个工作流程用于该数字内容。在工作流程数据库 840 中存储该数字内容的条目,该条目包括该数字内容的标识符、用于保护数字内容的加扰密钥、用于内容的工作流程、以及位置指示符。尽管如此,应当理解,为了移除已经通过的节点,每一次进行处理时可能修改该处理图。工作流程数据库 840(和 / 或工作流程引擎)还可以存储关于 WAID 812 与一个或者更多节点之间的对应关系的信息,工作流程动作代理 810 可以作为所述一个或者更多节点。

[0068] 当用户希望处理数字内容时,在步骤 902,它获得相应的内容文件 830,并且从内容文件 830 中提取内容标识符 834(即,实例 ID),并将内容标识符发送 904 至工作流程引擎 820。在第二优选实施例中,不一定要保护该消息。工作流程引擎 820 从工作流程数据库 840 中取回 906 与内容标识符相对应的工作流程信息,即由哪个动作代理对内容应用的动作。工作流程引擎 820 还提取 908 内容密钥并且生成 910 受保护许可,该受保护许可至少包括工作流程信息和内容密钥。然后,将该许可发送 912 至动作代理 810。

[0069] 可以利用任何适合的现有方式来保护该许可,例如,使用域密钥、SAC 会话密钥、广播加密、或者公钥加密。然而,因而这超出了本发明的保护范围,本文将不再详述。

[0070] 在接收到该许可,工作流程代理 820 检查 914 许可对内容进行的动作。如果能够执行许可的动作,则它从许可中取回 916 内容密钥,对内容进行解扰 918,并且处理 920 该内容。

[0071] 当工作流程动作代理 810 已经完成处理数字内容 832 时,它对数字内容 832 重新加密,并且通知工作流程引擎 820 可以在工作流程数据库 840 中更新数字内容 832 的条目。

[0072] 因而,可以认识到,本发明提供了一种用于数字处理管理的具有多个实施例的解决方案,该数字处理管理能够确保根据确定的工作流程来处理数字内容。

[0073] 可以独立地或者以适当组合的方式来提供说明书以及(在合适时)权利要求以及

附图中所公开的每一个特征。被描述为以硬件实现的特征也可以以软件实现，反之亦然。在适当的情况下，可以将连接实施为无线连接或者有线（不必是直接的或者专用的）连接。

[0074] 权利要求中出现的附图标记仅作为示意，不应对权利要求的范围起限制作用。

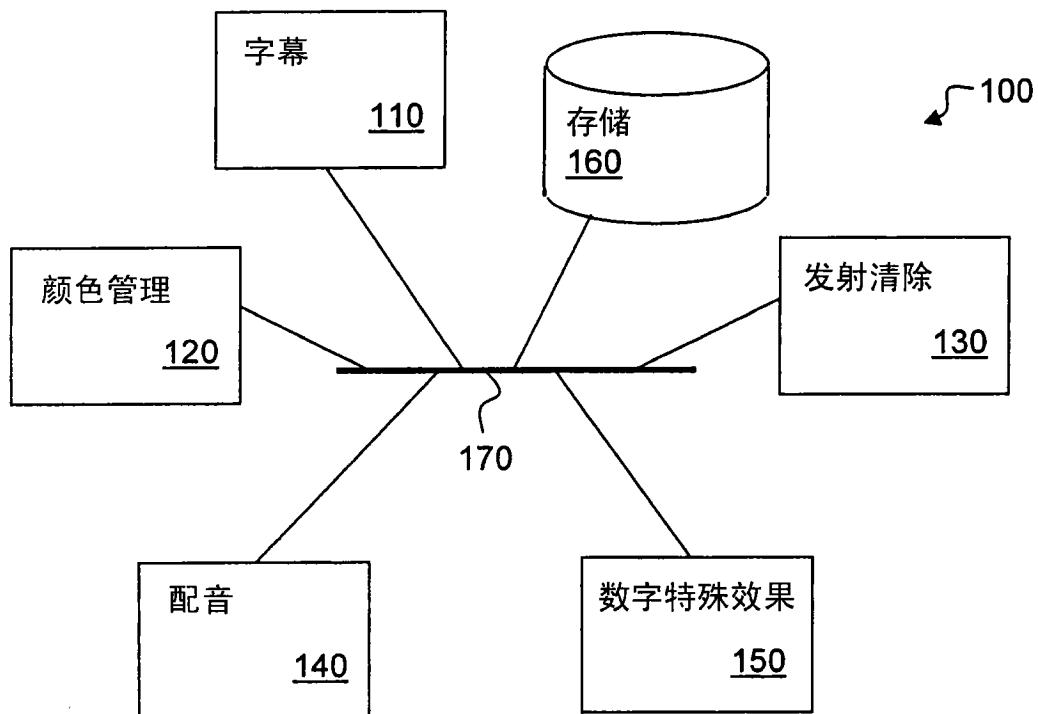


图 1

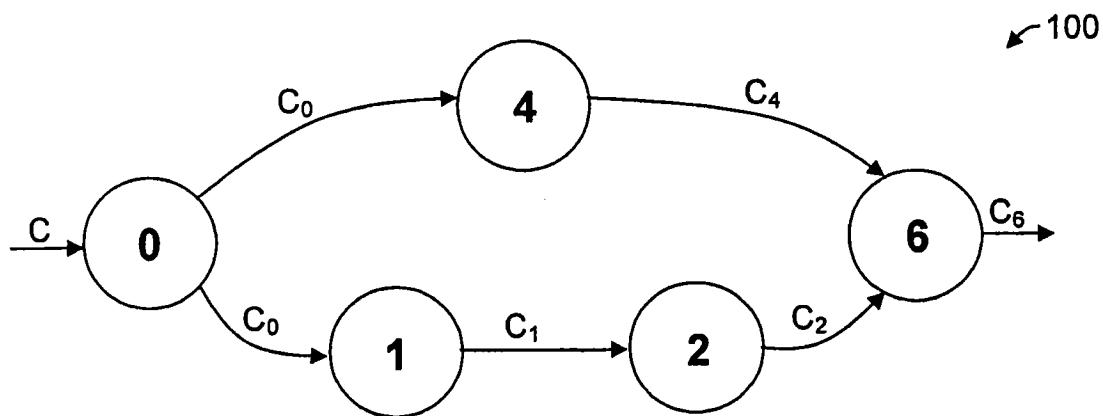


图 2

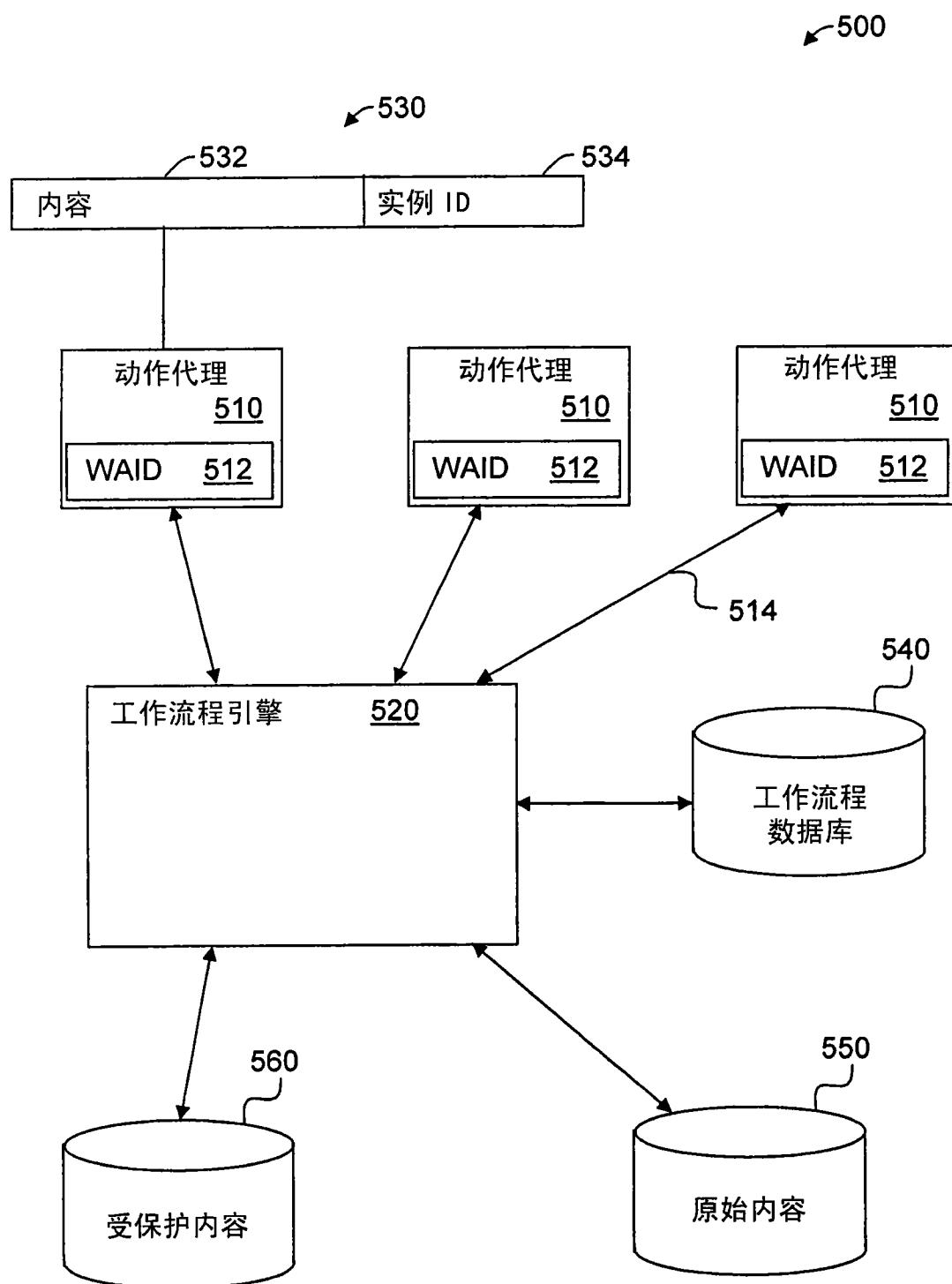


图 3

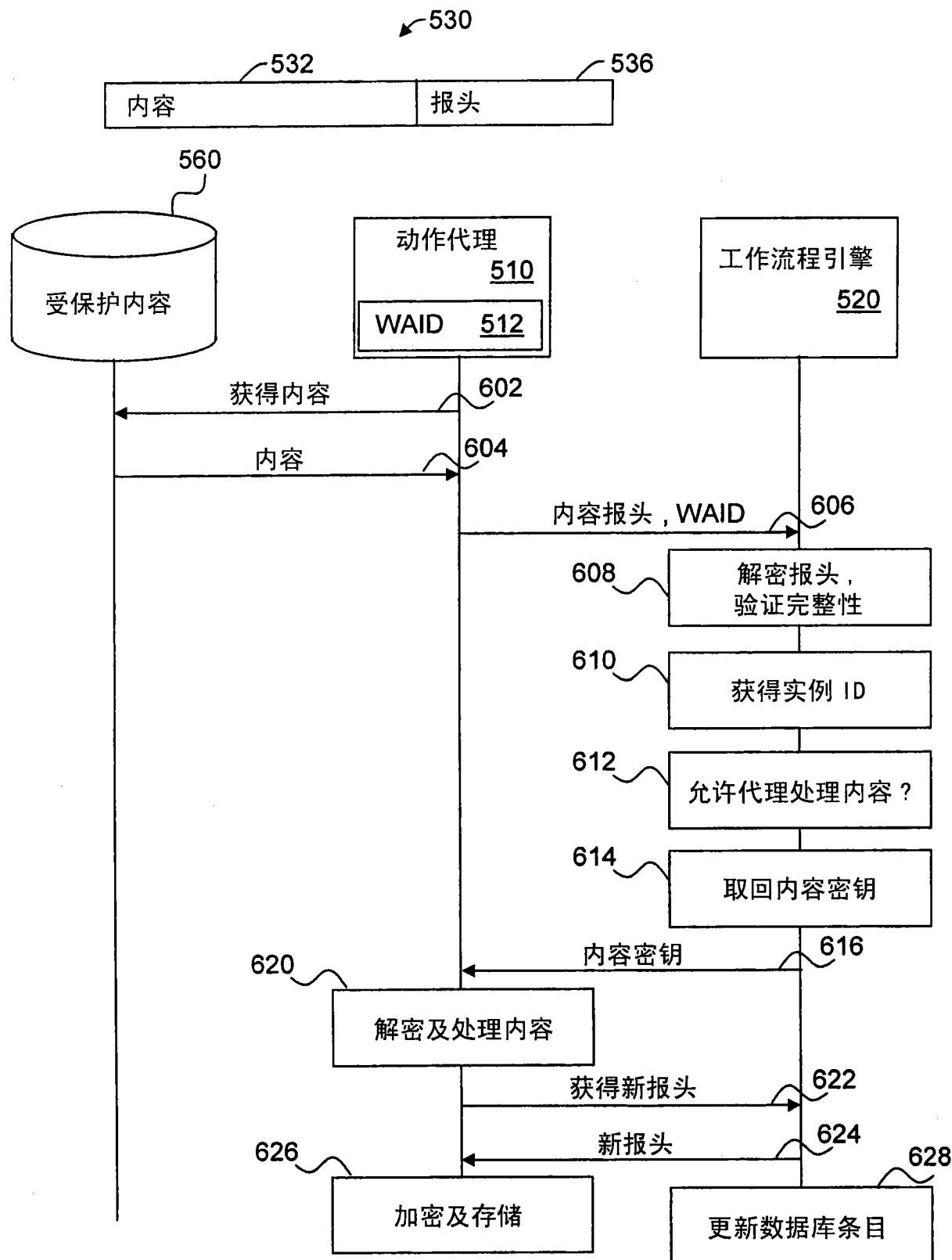


图 4

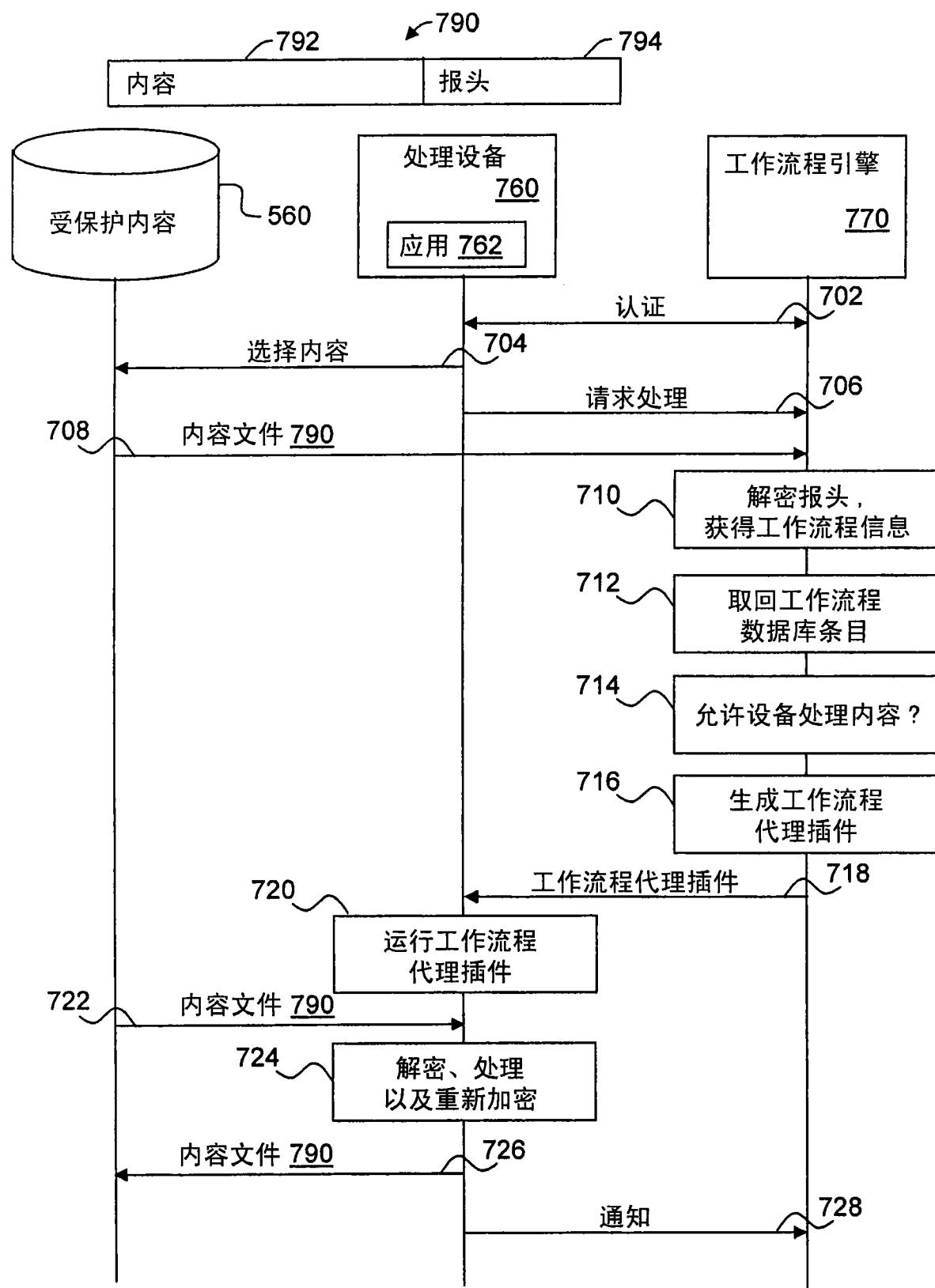


图 5

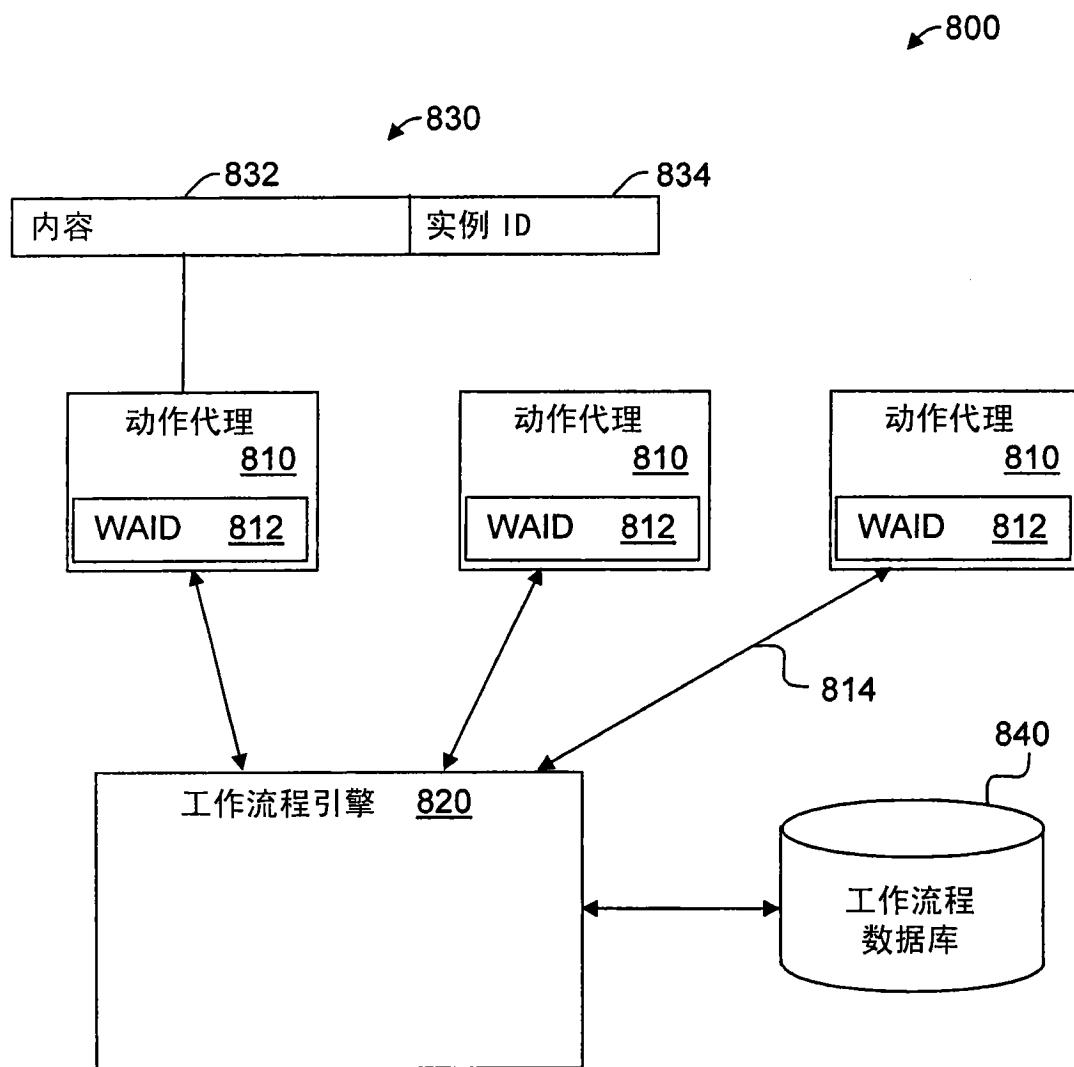


图 6

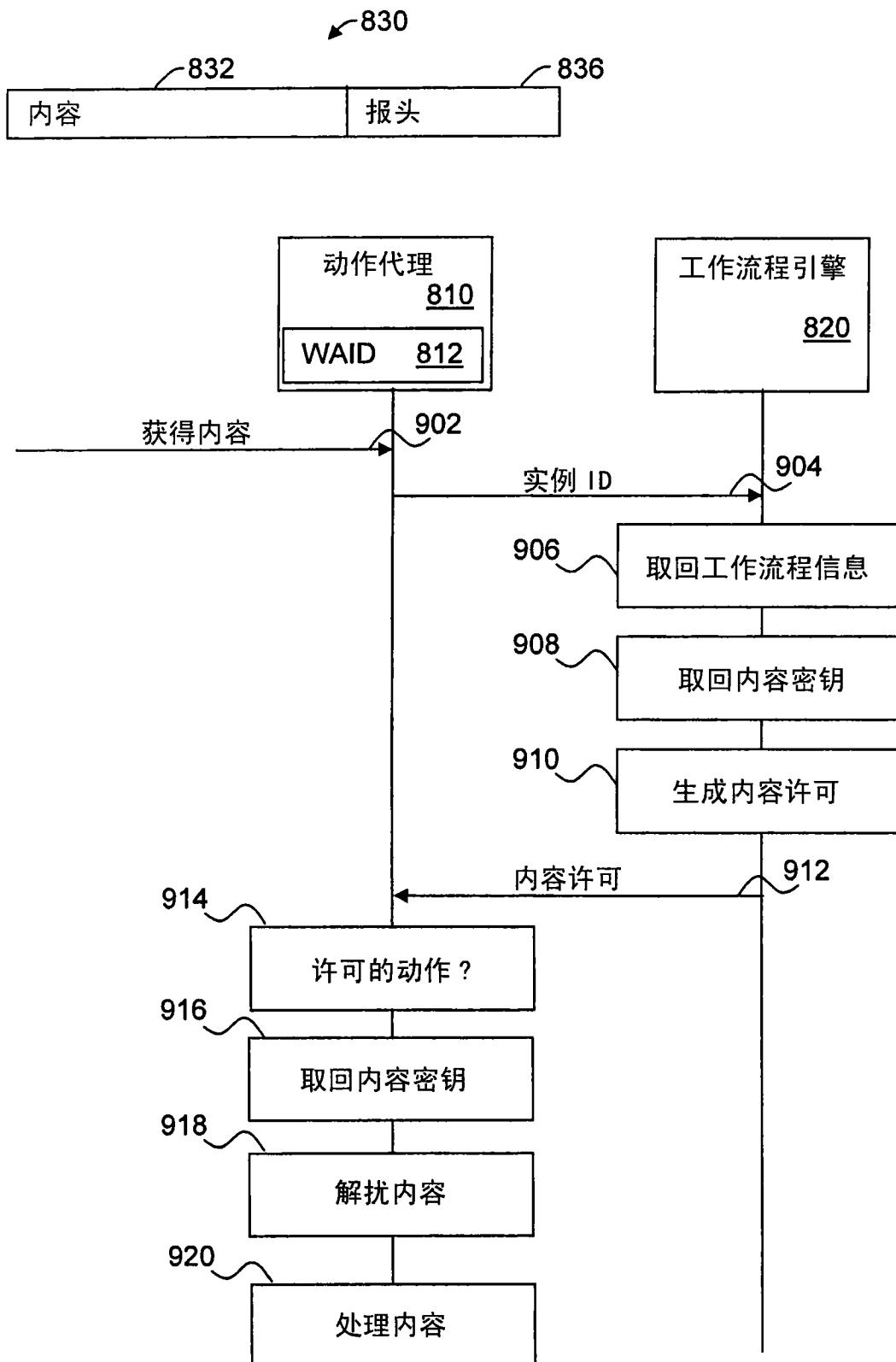


图 7