



(12) 发明专利申请

(10) 申请公布号 CN 103189873 A

(43) 申请公布日 2013.07.03

(21) 申请号 201180051690.8

(74) 专利代理机构 北京律盟知识产权代理有限公司 11287

(22) 申请日 2011.09.15

代理人 容春霞

(30) 优先权数据

61/383,693 2010.09.16 US

(51) Int. Cl.

13/080,593 2011.04.05 US

G06F 21/10 (2013.01)

13/080,598 2011.04.05 US

G06F 21/44 (2013.01)

13/080,605 2011.04.05 US

H04L 9/32 (2006.01)

(85) PCT申请进入国家阶段日

2013.04.25

H04L 29/06 (2006.01)

(86) PCT申请的申请数据

PCT/US2011/051857 2011.09.15

(87) PCT申请的公布数据

W02012/037422 EN 2012.03.22

(71) 申请人 凡瑞斯公司

地址 美国加利福尼亚州

(72) 发明人 约瑟夫·M·威诺格拉德

拉德·彼得罗维奇 健·赵

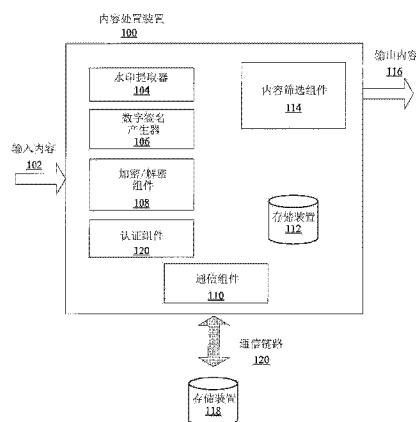
权利要求书4页 说明书26页 附图9页

(54) 发明名称

水印提取效率的改进

(57) 摘要

方法、装置和计算机程序产品促进基于嵌入在内容中的水印来应用内容使用规则。所需内容筛选操作被组织为若干单独任务，所述内容筛选操作包含水印提取和内容使用强制执行动作的施加。这些任务可由不同装置在不同时间进行。水印提取结果被存储在安全位置中且可由其它装置在不同时间存取。这些操作可由驻留在家庭网络中的一个或一个以上受信任装置进行。装置的可信任性可在装置认证过程期间被探知。另外，某些装置能力可作为所述装置认证过程的部分或通过所述装置之间的额外通信而被探知。



1. 一种方法，其包括：

响应于检测到内容处置装置中的操作而检索与内容相关联的现有水印提取记录，其中所述操作需要对内容的存取；

根据所述现有水印提取记录认证所述内容；以及

根据与所述内容相关联的内容使用政策实行内容筛选。

2. 根据权利要求 1 所述的方法，其中所述操作包括以下各者中的至少一者：

复制操作；

传送操作；

再现操作；

回放操作；以及

记录操作。

3. 根据权利要求 1 所述的方法，其中所述现有水印提取记录包括以下各者中的至少一者：

所提取的水印有效负载；

所提取的水印的数目；

与所提取的水印相关联的时戳；

内容认证信息；

与所述提取记录相关联的数字签名；

与所述内容相关联的使用规则；以及

与所述内容使用政策和所提取的水印有效负载相关联的动作。

4. 根据权利要求 1 所述的方法，其中：

所述现有水印提取记录的所述检索和内容文件的认证中的至少一者失败；

所述内容经受新水印提取操作；

所述内容使用政策根据所述新水印提取操作的结果规定动作；以及

存储所述所规定的动作以作为新水印提取记录的部分。

5. 根据权利要求 1 所述的方法，其中所述内容使用政策根据所述现有水印提取记录规定强制执行动作。

6. 根据权利要求 1 所述的方法，其中所述内容筛选包括以下各者中的至少一者：

使所述内容的至少一部分静音；

使所述内容的至少一部分消隐；

显示版权通知；

拒绝对所述内容的存取；

删除所述内容；

将内容使用信息记录在所述内容处置装置中；

将内容使用信息发送到远程服务器；

回放或显示本地存储的或从远程服务器传输的至少一广告；

回放或显示降低了分辨率的所述内容；

联系远程服务器以获得存取所述内容的许可；以及

完成与远程服务器的支付交易。

7. 根据权利要求 1 所述的方法,其中 :

所述操作需要对所述内容的实时存取;

所述现有水印提取记录包括对应于多个内容片段的分段认证信息;且根据所述分段认证信息针对所述内容的至少一片段而执行所述认证。

8. 根据权利要求 7 所述的方法,其中所述现有水印提取记录伴随有串流传输的内容。

9. 根据权利要求 1 所述的方法,其中 :

所述操作存取多个内容;

所述多个所述内容中的一者或一者以上具有在特定阈值以下的大小;以及所述内容筛选通过以下操作来实行:

串联具有在所述特定阈值以下的大小的所述多个所述内容;

对所述串联的内容进行新水印提取操作;

聚集与所述新水印提取操作相关联的所述结果和从所述现有水印提取记录获得的信息,所述信息对应于所述多个所述内容中的具有高于或等于所述特定阈值的大小的一者或一者以上;以及

根据所述所聚集结果产生动作。

10. 一种装置,其包括 :

处理器;以及

存储器,其包含处理器可执行代码,所述处理器可执行代码在由所述处理器执行时配置所述装置以:

响应于检测到内容处置装置中的操作而检索与内容相关联的现有水印提取记录,其中所述操作需要对内容的存取;

根据所述现有水印提取记录认证所述内容;以及

根据与所述内容相关联的内容使用政策实行内容筛选。

11. 根据权利要求 10 所述的装置,其中所述操作包括以下各者中的至少一者:

复制操作;

传送操作;

再现操作;

回放操作;以及

记录操作。

12. 根据权利要求 10 所述的装置,其中所述现有水印提取记录包括以下各者中的至少一者:

所提取的水印有效负载;

所提取的水印的数目;

与所提取的水印相关联的时戳;

内容认证信息;

与所述提取记录相关联的数字签名;

与所述内容相关联的使用规则;以及

与所述内容使用政策和所提取的水印有效负载相关联的动作。

13. 根据权利要求 10 所述的装置,其中所述处理器可执行代码在由所述处理器执行时

配置所述装置以：

在所述现有水印提取记录的所述检索和内容文件的认证中的至少一者失败后，即刻使所述内容经受新水印提取操作，其中所述内容使用政策根据所述新水印提取操作的结果规定动作，且其中所述所规定的动作被存储为新水印提取记录的部分。

14. 根据权利要求 10 所述的装置，其中所述内容使用政策根据所述现有水印提取记录规定强制执行动作。

15. 根据权利要求 10 所述的装置，其中所述内容筛选包括以下各者中的至少一者：

使所述内容的至少一部分静音；

使所述内容的至少一部分消隐；

显示版权通知；

拒绝对所述内容的存取；

删除所述内容；

将内容使用信息记录在所述内容处置装置中；

将内容使用信息发送到远程服务器；

回放或显示本地存储的或从远程服务器传输的至少一广告；

回放或显示降低了分辨率的所述内容；

联系远程服务器以获得存取所述内容的许可；以及

完成与远程服务器的支付交易。

16. 根据权利要求 10 所述的装置，其中

所述操作需要对所述内容的实时存取；

所述现有水印提取记录包括对应于多个内容片段的分段认证信息；且

所述处理器可执行代码在由所述处理器执行时配置所述装置以根据所述分段认证信息认证所述内容的至少一片段。

17. 根据权利要求 16 所述的装置，其中所述现有水印提取记录伴随有串流传输的内容。

18. 根据权利要求 10 所述的装置，其中

所述操作需要对多个内容的存取；

所述多个所述内容中的一者或一者以上具有在特定阈值以下的大小；以及

所述内容筛选是由在由所述处理器执行时配置所述装置以进行以下操作的所述处理器可执行代码实行：

串联具有在所述特定阈值以下的大小的所述多个所述内容；

对所述串联的内容进行新水印提取操作；

聚集与所述新水印提取操作相关联的所述结果和从所述现有水印提取记录获得的信息，所述信息对应于所述多个所述内容中的具有高于或等于所述特定阈值的大小的一者或一者以上；以及

根据所述所聚集结果产生动作。

19. 一种体现在非暂时性计算机可读媒体上的计算机程序产品，其包括：

用于响应于检测到内容处置装置中的操作而检索与内容相关联的现有水印提取记录的计算机代码，其中所述操作需要对内容的存取；

用于根据所述现有水印提取记录认证所述内容的计算机代码；以及

用于根据与所述内容相关联的内容使用政策实行内容筛选的计算机代码。

20. 一种装置，其包括：

用于响应于检测到内容处置装置中的操作而检索与内容相关联的现有水印提取记录的构件，其中所述操作需要对内容的存取；

用于根据所述现有水印提取记录认证所述内容的构件；以及

用于根据与所述内容相关联的内容使用政策实行内容筛选的构件。

水印提取效率的改进

[0001] 相关申请案

[0002] 本申请案主张第 13/080,593 号、第 13/080,605 号和第 13/080,598 号美国专利申请案的优先权，所有专利申请案都是在 2011 年 4 月 5 日申请的。上述专利申请案中的每一者主张 2010 年 9 月 16 日申请的第 61/383,693 号美国临时申请案的权益。上述专利申请案的全部内容以引用的方式并入以作为本申请案的揭示内容的部分。

技术领域

[0003] 本发明大体上涉及内容管理的领域。更明确地说，所揭示的实施例涉及从媒体内容有效且安全地提取水印以实现内容管理。

背景技术

[0004] 本章节希望提供权利要求书中所叙述的所揭示的实施例的背景或上下文。本文中的描述可包含可追求的概念，但未必为先前已设想或追求的概念。因此，除非本文中另外指示，否则本章节中描述的内容并非本申请案中的描述和权利要求书的现有技术，且不会由于包含在本章节中而被承认是现有技术。

[0005] 已提出数字水印且将其用于例如音频、视频、图像等信号的版权保护。在典型水印情形中，辅助信息信号用一种方式隐藏在宿主内容内，使得其大体上难以察觉，且同时难以在不损坏宿主内容的情况下被移除。隐藏在宿主内容内的辅助信息接着可允许在不同程度上执行内容管理。在一些实施例中，内容管理包含（但不限于）根据一个或一个以上政策的内容的使用的管理。举例来说，辅助信息可能仅传送不允许复制宿主内容（即，“不允许复制”水印）。一旦被相容的装置提取和解译，内容的复制便得以防止。相容的装置可包含（但不限于）执行筛选，或另外以符合内容使用政策的方式操作的装置。内容使用（或内容的使用）可包含（但不限于）涉及内容的操作，例如回放、复制、记录、传送、串流传输或其它操作。另外或替代地，嵌入式辅助信息可识别合法拥有者、作者和 / 或内容的作者或可提供与内容相关联的序列号或识别信息的其它内容。辅助信息还可用于其它应用，例如监视嵌入式宿主内容的使用，解决所有权争议和记录特许权等。

[0006] 为了提取和利用嵌入在各种内容中的水印，可使用实质性资源（例如，CPU 循环、数字存储器）和通信资源。这又可延迟对内容的存取，增加制造设计有最小处理负荷目标的装置的成本，增加移动装置中的电池消耗等。与提取这些水印相关联的处理负担常常因为需要执行必须在可尝试水印提取之前执行的特定额外内容变换操作（例如，解密、解压缩、多路分用等）而加重。

发明内容

[0007] 本章节希望提供某些示范性实施例的概述且无意限制本申请案中揭示的实施例的范围。

[0008] 所揭示的实施例通过减少总资源使用，在可能时利用空闲资源和及时分配资源使

用以实现低峰值要求和优化成本 - 性能权衡来改进水印提取和相关联的处理的效率。所揭示的实施例的这些和其它特征得以实行，同时维持与水印的使用相关联的适当安全等级。所揭示的实施例进一步增强经连接（例如，联网）装置的能力以通过合作努力实现水印提取、内容筛选和内容管理。可组织水印提取和内容筛选操作以使得操作中的一些或全部可在不同时间由不同装置进行，所述水印提取和内容筛选操作可包含施加内容使用强制执行动作。可通过交换网络中的各种装置之间的证书来执行安全和有效的内容水印提取和内容筛选操作。交换的证书可进一步实现装置能力的交换，进而促进操作配置的分派以进行水印提取和内容筛选操作。

[0009] 所揭示的实施例的一个方面涉及一种方法，其包含在第一装置处从第二装置接收存取内容的请求，其中所述第一装置在网络中操作。此方法进一步包括执行装置认证以探知与所述第一装置和所述第二装置中的一者或两者相关联的受信任状态，以及确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置。在一个实施例中，所述第二装置为受信任内容客户端装置，且所述第二装置经配置以执行所述水印提取和筛选操作。

[0010] 在另一实施例中，所述第二装置也为受信任内容客户端装置。但在此实施例中，受信任从属装置经配置以执行所述水印提取操作且向所述第二装置提供与提取信息相关联的信息。此外，所述第二装置经配置以执行所述筛选操作。在所述第二装置为受信任内容客户端装置的又一实施例中，受信任受委托装置经配置以执行所述水印提取和筛选操作。

[0011] 根据另一实施例，所述第一装置为受信任内容服务器，且所述第一装置经配置以执行所述水印提取和筛选操作。在另一实施例中，所述第一装置类似地为受信任内容服务器。然而，在此实施例中，受信任从属装置经配置以执行所述水印提取操作且向所述第一装置提供与提取信息相关联的信息。另外，所述第一装置经配置以执行所述筛选操作。

[0012] 在所述第一装置为受信任内容服务器的另一实施例中，受信任受委托装置经配置以执行所述水印提取和筛选操作。在又一实施例中，所述第一装置为受信任内容服务器且所述第二装置为受信任内容客户端装置。根据此实施例，所述第一装置经配置以执行所述水印提取操作，且所述第二装置经配置以执行所述筛选操作。

[0013] 在所述第一装置为受信任内容服务器且所述第二装置为受信任内容客户端装置的另一实施例中，所述第二装置经配置以执行所述水印提取操作。在此实施例中，所述第一装置经配置以执行所述筛选操作。

[0014] 根据一个实施例，上述方法中的网络为家庭网络。举例来说，此家庭网络可为数字生活网络联盟 (DLNA) 网络。而在另一实施例中，所述第二装置也在所述网络中操作，在另一实施例中，所述第二装置在所述网络外部操作。

[0015] 根据一个实施例，所述第一装置为非相容装置且所述第二装置为相容装置。在另一实施例中，所述第一装置为相容装置但所述第二装置为非相容装置。在又一实施例中，所述第一装置和所述第二装置两者都为非相容装置。

[0016] 所揭示的实施例的另一方面涉及一种包含处理器和存储器的装置，所述存储器包含处理器可执行代码。所述处理器可执行代码在由所述处理器执行时配置所述装置以在第一装置处从第二装置接收存取内容的请求，其中所述第一装置在网络中操作。所述处理器可执行代码在由所述处理器执行时还配置所述装置以执行装置认证以探知与所述第一装

置和所述第二装置中的一者或两者相关联的受信任状态。所述处理器可执行代码在由所述处理器执行时进一步配置所述装置以确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置。

[0017] 所揭示的实施例的另一方面涉及一种体现在非暂时性计算机可读媒体上的计算机程序产品。所述计算机程序产品包括用于在第一装置处从第二装置接收存取内容的请求的程序代码，所述第一装置在网络中操作。所述计算机程序产品还包含用于执行装置认证以探知与所述第一装置和所述第二装置中的一者或两者相关联的受信任状态的程序代码。所述计算机程序产品进一步包含用于确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置的程序代码。

[0018] 所揭示的实施例的另一方面涉及一种装置，其包括：用于在第一装置处从第二装置接收存取内容的请求的构件，所述第一装置在网络中操作；以及用于执行装置认证以探知与所述第一装置和所述第二装置中的一者或两者相关联的受信任状态的构件。此装置进一步包含用于确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置的构件。

[0019] 所揭示的实施例的另一方面涉及一种方法，其包括在网关装置处接收存取内容的请求，所述网关装置经配置以协调网络内的多个装置的操作。此请求是从第二装置接收以用于存取第一装置可存取的内容，其中所述第一装置经配置以在所述网络内操作。此方法进一步包含：在所述网关装置处协调装置认证以探知与所述第一装置和所述第二装置中的一者或两者相关联的受信任状态；以及在所述网关装置处确定用于使用一个或一个以上受信任装置来执行水印提取和内容筛选操作的操作配置。

[0020] 在一个实施例中，所述第二装置为经配置以在所述网络内操作的装置，而在另一实施例中，所述第二装置为经配置以在所述网络外部操作的装置。在另一实施例中，所述网关装置经配置以与所述一个或一个以上受信任装置通信以开始所述水印提取和 / 或筛选操作。在另一实例中，所述网关装置经配置以撤销所述网络内的装置的受信任状态。在又其它实例中，所述网关装置经配置以保持与所嵌入的水印相关联的使用规则。在一个变化中，所述网关装置还经配置以将所述使用规则传送到各种受信任装置。

[0021] 所揭示的实施例的另一方面涉及一种包括处理器和存储器的网关装置，所述存储器包括处理器可执行代码。所述处理器可执行代码在由所述处理器执行时配置所述网关装置以在所述网关装置处接收存取内容的请求，所述网关装置经配置以协调网络内的多个装置的操作。所述请求是从第二装置接收以用于存取第一装置可存取的内容，其中所述第一装置经配置以在所述网络内操作。所述处理器可执行代码在由所述处理器执行时进一步配置所述网关装置以协调装置认证以探知与所述第一装置和所述第二装置中的一者或两者相关联的受信任状态。所述处理器可执行代码在由所述处理器执行时还配置所述网关装置以确定用于使用一个或一个以上受信任装置来执行水印提取和内容筛选操作的操作配置。

[0022] 所揭示的实施例的另一方面涉及一种体现在非暂时性计算机可读媒体上的计算机程序产品，所述计算机程序产品包括用于在网关装置处接收存取内容的请求的程序代码，所述网关装置经配置以协调网络内的多个装置的操作。所述请求是从第二装置接收以用于存取第一装置可存取的内容，其中所述第一装置经配置以在所述网络内操作。所述计算机程序产品还包括：用于协调装置认证以探知与所述第一装置和所述第二装置中的一者

或两者相关联的受信任状态的计算机代码；以及用于确定用于使用一个或一个以上受信任装置来执行水印提取和内容筛选操作的操作配置的计算机代码。

[0023] 所揭示的实施例的另一方面涉及一种装置，所述装置包括用于将存取内容的请求从第二装置传输到第一装置的构件，所述第一装置在网络中操作。此装置还包含用于执行装置认证以探知与所述第一装置相关联的受信任状态的构件，和用于确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置的构件。

[0024] 所揭示的实施例的另一方面涉及一种方法，其包含将存取内容的请求从第二装置传输到第一装置，其中所述第一装置在网络中操作。此方法还包含执行装置认证以探知与所述第一装置相关联的受信任状态，和确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置。

[0025] 所揭示的实施例的另一方面涉及一种包括处理器和存储器的装置，所述存储器包含处理器可执行代码。所述处理器可执行代码在由所述处理器执行时配置所述装置以：将存取内容的请求从第二装置传输到第一装置，所述第一装置在网络中操作；以及执行装置认证以探知与所述第一装置相关联的受信任状态。所述处理器可执行代码在由所述处理器执行时进一步配置所述装置以确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置。

[0026] 所揭示的实施例的另一方面涉及一种体现在非暂时性计算机可读媒体上的计算机程序产品。所述计算机程序产品包含用于将存取内容的请求从第二装置传输到第一装置的程序代码，其中所述第一装置在网络中操作。所述计算机程序代码还包含用于执行装置认证以探知与所述第一装置相关联的受信任状态的程序代码，和用于确定用于使用一个或一个以上受信任装置来执行水印提取和 / 或筛选操作的操作配置的程序代码。

[0027] 所揭示的实施例的一方面涉及一种方法，其包括在第一装置处从第二装置接收装置认证证书以及验证所述证书的可靠性。此方法还包含探知所述第二装置的能力以及确定进行与内容相关联的水印提取和 / 或筛选操作的操作配置。在一个实施例中，所述证书含有指示所述第二装置的所述能力的至少一部分的信息。在一个实例中，所述证书为因特网协议上的数字传输内容保护 (DTCP-IP) 证书，且关于所述第二装置的所述能力的信息被执行为所述 DTCP-IP 证书的部分。在另一实施例中，从除了所述证书以外的来源探知所述第二装置的所述能力的至少一部分。举例来说，可通过与所述第二装置的额外通信来接收所述第二装置的所述能力的至少一部分。

[0028] 根据另一实施例，所述第二装置的所述所探知能力包含进行所述水印提取操作和 / 或内容筛选操作中的一些或全部的能力。在此情形中，所述操作配置可指定所述第二装置执行所述水印提取和内容筛选操作中的至少一者。在另一实施例中，所述第二装置的所述所探知能力包含将计算和存储器资源授予其它装置的能力。

[0029] 在一个实施例中，上述方法进一步包含在所述第二装置处从所述第一装置接收装置认证证书；验证从所述第一装置接收的所述证书的可靠性；以及探知所述第一装置的能力。在一个变化中，从所述第一装置接收的所述证书含有指示所述第一装置的所述能力的至少一部分的信息。在一个实例中，从所述第一装置接收的所述证书为因特网协议上的数字传输内容保护 (DTCP-IP) 证书，且关于所述第一装置的所述能力的信息被执行为所述 DTCP-IP 证书的部分。在另一实例中，从除了所述证书以外的来源探知所述第一装置的所述

能力的至少一部分。举例来说,可通过与所述第一装置的额外通信来接收所述第一装置的所述能力的至少一部分。在另一实施例中,所述第一装置的所述所探知能力包括进行所述水印提取和 / 或内容筛选操作中的一些或全部的能力。

[0030] 在一个实施例中,所述第一装置的所述所探知能力包括将计算和存储器资源授予其它装置的能力。在一个变化中,根据所述第一装置和所述第二装置的所述所探知能力来进行用于进行水印提取和 / 或筛选操作的操作配置的确定。在另一实施例中,所述操作配置指定所述第一装置执行所述水印提取和内容筛选操作中的至少一者。在又一实施例中,所述操作配置指定所述第一装置和所述第二装置合作地执行所述水印提取和所述内容筛选操作。

[0031] 根据另一实施例,所述操作配置根据选自由以下各者组成的群组的因素来指定所述第一装置和所述第二装置中的至少一者进行所述水印提取和内容筛选操作:计算资源的可用性;水印提取和筛选能力的可用性;装置制造商、消费者体验、处理性能和总偏好排名的集成复杂性。在一个实施例中,所述第一装置和所述第二装置中的至少一者经配置以在家庭网络中操作。举例来说,此家庭网络可为数字生活网络联盟(DLNA)网络。

[0032] 所揭示的实施例的另一方面涉及一种包含处理器和存储器的装置,所述存储器包含处理器可执行代码。所述处理器可执行代码在由所述处理器执行时配置所述装置以在第一装置处从第二装置接收装置认证证书且验证所述证书的可靠性。所述处理器可执行代码在由所述处理器执行时还配置所述装置以探知所述第二装置的能力且确定进行与内容相关联的水印提取和 / 或筛选操作的操作配置。

[0033] 所揭示的实施例的另一方面涉及一种体现在非暂时性计算机可读媒体上的计算机程序产品。所述计算机程序产品包括用于在第一装置处从第二装置接收装置认证证书的程序代码和用于验证所述证书的可靠性的程序代码。所述计算机程序产品还包含用于探知所述第二装置的能力的程序代码和用于确定进行与内容相关联的水印提取和 / 或筛选操作的操作配置的程序代码。

[0034] 所揭示的实施例的另一方面涉及一种装置,其包括用于在第一装置处从第二装置接收装置认证证书的构件和用于验证所述证书的可靠的构件。所述装置还包含用于探知所述第二装置的能力的构件和用于确定进行与内容相关联的水印提取和 / 或筛选操作的操作配置的构件。

[0035] 所揭示的实施例的另一方面涉及一种方法,其包含检测内容处置装置中的操作,其中此操作需要对内容的存取。所述方法还包含检索与所述内容相关联的现有水印提取记录和根据所述现有水印提取记录认证所述内容。此方法还包含根据与所述内容相关联的使用规则实行内容筛选。在一个实施例中,需要对所述内容的存取的所述操作可为以下各项中的至少一者:复制操作;传送操作;再现操作;回放操作和记录操作。

[0036] 在一个实施例中,所述现有水印提取记录是从所述内容处置装置外部的位置检索的。在另一实施例中,此位置为以下各项中的至少一者:云上的私人虚拟锁定器;云上的通用虚拟锁定器;家庭网络内的与DLNA(数字生活网络联盟)相容的装置上的存储装置;数字生活网络联盟(DLNA)相容网络内的存储位置;通信地连接到内容处置装置的另一装置内的存储位置和可装卸计算机可读存储媒体。

[0037] 在另一实施例中,所述现有水印提取记录包括以下各项中的至少一者:所提取的

水印有效负载；所提取的水印的数目；与所提取的水印有效负载相关联的时戳；内容认证信息；与所述提取记录相关联的数字签名；与所述内容相关联的使用规则；以及与所述使用规则和所提取的水印有效负载相关联的强制执行动作。

[0038] 在又一实施例中，所述现有水印提取记录的所述检索和内容文件的认证中的至少一者失败，且所述内容经受新水印提取操作。在此实施例中，所述方法可进一步包含产生新水印提取记录。在此实施例中，所述使用规则可根据所述新水印提取操作的结果规定强制执行动作。举例来说，所述规定的强制执行动作可被存储为所述新水印提取记录的部分。在另一实施例中，所述使用规则根据所述现有水印提取记录规定强制执行动作。

[0039] 根据另一实施例，所述内容筛选包括以下各项中的至少一者：使所述内容的至少一部分静音；使所述内容的至少一部分消隐；显示版权通知；拒绝对所述内容的存取；以及删除所述内容。在又一实施例中，所述内容处置装置为数字生活网络联盟（DLNA）相容装置。

[0040] 在一个实施例中，需要对所述内容的存取的所述操作需要对所述内容的实时存取。在此实施例中，所述现有水印提取记录包括对应于多个内容片段的分段认证信息，且所述认证是根据所述分段认证信息针对所述内容的至少一个片段而执行的。在此情形中，现有提取信息可伴随串流传输的内容。在一个实例中，所述分段认证信息包括分段散列值。在另一实例中，所述认证是针对所述内容的顺序片段执行的，而在不同实例中，所述认证是针对所述内容的非顺序片段执行的。

[0041] 在一个实例中，通过评估所述现有水印提取记录内含有的信息结合与预定时间周期相关联的内容使用信息来实行筛选。举例来说，所述内容使用信息可包括所提取的水印有效负载和紧接在需要内容存取的所述操作的检测之前的时间间隔内的相关联的时戳。

[0042] 根据另一实施例，所述内容处置装置中的需要内容存取的所述操作需要对多个内容的存取，其中所述多个所述内容中的一者或一者以上具有在特定阈值以下的大小。在此情形中，通过首先串联具有在所述特定阈值以下的大小的所述多个所述内容和对所述串联的内容进行新水印提取操作来实行内容筛选。通过聚集与所述新水印提取操作相关联的所述结果和从所述现有水印提取记录获得的信息来进一步实行内容筛选，所述信息对应于大小在所述特定阈值以上或等于所述特定阈值的所述多个所述内容中的一者或一者以上。这些操作之后为根据所述所聚集结果产生强制执行动作。

[0043] 所揭示的实施例的另一方面涉及一种包括处理器和存储器的装置，所述存储器包含处理器可执行代码。所述处理器可执行代码在由所述处理器执行时配置所述装置以检测内容处置装置中的操作，其中此操作需要对内容的存取。所述处理器可执行代码在由所述处理器执行时进一步配置所述装置以检索与所述内容相关联的现有水印提取记录。所述处理器可执行代码在由所述处理器执行时还配置所述装置以根据所述现有水印提取记录认证所述内容且根据与所述内容相关联的使用规则实行内容筛选。

[0044] 所揭示的实施例的另一方面涉及一种体现在非暂时性计算机可读媒体上的计算机程序产品。所述计算机程序代码包括用于检测内容处置装置中的操作的程序代码，其中此操作需要对内容的存取。所述计算机程序产品还包含用于检索与所述内容相关联的现有水印提取记录的程序代码、用于根据所述现有水印提取记录认证所述内容的程序代码和用于根据与所述内容相关联的使用规则实行内容筛选的程序代码。

[0045] 所揭示的实施例的另一方面涉及一种装置，其包括用于检测内容处置装置中的操作的构件，其中此操作需要对内容的存取。所述装置进一步包括用于检索与所述内容相关联的现有水印提取记录的构件。所述装置还包含用于根据所述现有水印提取记录认证所述内容的构件和用于根据与所述内容相关联的使用规则实行内容筛选的构件。

[0046] 根据结合附图进行的以下详细描述，所揭示的实施例的这些和其它优点和特征连同其组织和操作方式将变得显而易见。

附图说明

- [0047] 通过参照附图来描述所揭示的实施例，其中：
- [0048] 图 1 为根据实例实施例的内容处置装置的框图；
- [0049] 图 2 为根据实例实施例的特定水印提取和内容筛选操作的流程图；
- [0050] 图 3 为根据实例实施例的特定水印提取操作的流程图；
- [0051] 图 4 说明根据实例实施例的调用模型装置配置的框图；
- [0052] 图 5 说明根据实例实施例的委托模型装置配置的框图；
- [0053] 图 6 说明根据实例实施例的内容服务器和内容客户端装置配置的框图；
- [0054] 图 7 说明根据实例实施例的认证过程；
- [0055] 图 8 说明根据实例实施例的合作的水印提取和内容筛选操作；
- [0056] 图 9 说明根据实例实施例的内容分配架构的框图；以及
- [0057] 图 10 说明可适应所揭示的实施例的示范性装置的框图。

具体实施方式

[0058] 在以下描述中，出于解释而非限制的目的，阐述细节和描述以便提供对所揭示的实施例的透彻理解。然而，所属领域的技术人员应明白，本发明可在脱离这些细节和描述的其它实施例中实践。

[0059] 另外，在本描述中，词语“示范性”用以指充当实例、例子或说明。不必将本文中描述为“示范性”的任何实施例或设计解释为比其它实施例或设计优选或有利。而是，既定使用词语示范性来以具体方式呈现概念。

[0060] 所揭示的实施例中的一些在数字生活网络联盟 (DLNA) 相容网络的背景下进行描述。DLNA 为引导消费型电子装置、计算产业和移动装置公司的跨产业组织。DLNA 的想象为可共同操作的消费型电子装置 (CE)、个人计算机 (PC) 和移动装置在家中和路上的有线和无线网络，从而实现共享和发展新数字媒体和内容服务的无缝环境。DLNA 集中于基于开放产业标准来递送互操作性指导方针以完成跨产业数字融合。

[0061] 为了使商业数字内容可用于与 DLNA 装置一起使用，必须保护内容以防未被授权的复制和使用。数字版权管理 (DRM) 技术被广泛使用且用以保护商业内容以及管理与通过不同通道（电缆、卫星、因特网等）和模型（VOD、DVD、租用等）获取的内容相关联的使用权。然而，DRM 在当前 DLNA 之外，这将 DRM 实施的选择权留给装置制造商。此外，受认可的 DRM 技术的列表和 DRM 互操作性两者都不包含在 DLNA 的当前版本中。

[0062] 链路保护是 DLNA 中仅有的内容保护机制，其为 DLNA 相容装置的任选实施方案。链路保护的主要使用情况适用于存储在媒体服务器上且由 DRM 技术保护的商业内容。链路

保护规定此内容在发送到客户端装置（例如，电视）之前可由媒体服务器使用链路保护技术进行解密和重新加密。客户端装置接着对所接收内容进行解密且再现 / 显示所述内容。DLNA 链路保护因此实现（例如）家庭网络中的所有装置上的商业内容的仅观看共享。然而，链路保护不能防止在家庭网络中共享和消费盗版商业内容。实际上，由于内容的经解密复本可在家庭网络内使用，因此具备 DLNA 功能的内容共享可导致较容易且较广泛地共享盗版内容。

[0063] 在 DLNA 中缺乏适当的内容保护已成为使商业内容可广泛用于 DLNA 相容网络中的障碍。所揭示的实施例利用嵌入在宿主内容内的水印来识别网络（例如，DLNA 相容网络）中的未被授权或盗版的内容，且在较广范围的分配通道和装置上实现内容的使用政策的传送和颁布。在一些实施例中，筛选和 / 或内容筛选用以指包含（但不限于）由装置对内容进行检查以确定使用是否符合内容使用政策的操作。内容使用政策可（例如）包含支配内容的使用的一个或一个以上规则，包含（但不限于）特定使用导致采取指定动作的条件。还应注意，术语提取可指包含（但不限于）用以确定水印的存在的对内容的检查，以及对检测到的水印内的辅助数据的可能评定的操作。在提取期间，水印通常不从内容移除。然而，所揭示的实施例也可易于适应在提取过程期间移除所嵌入的水印的水印提取算法。根据所揭示的实施例，经由各种操作（例如，从内容提取水印），与被提取的水印相关联的使用规则的评定和适当强制执行动作的施加可分配在一个或一个以上受信任实体中。在一些实施例中，这些强制执行动作包含（但不限于）与在指定类型的使用发生时执行的操作或功能有关的内容使用政策的元素。因而，并非网络内的所有装置都需要拥有整个范围的水印提取和内容筛选能力来遵照特定内容管理方案。另外，所揭示的实施例使装置能够确定另一装置是否值得信任，且探知那个装置的水印提取和 / 或筛选能力的程度。应注意，尽管所揭示的实施例中的一些是在 DLNA 以及 DLNA 相容装置和网络的背景下描述的，但所揭示的实施例同样适用于与媒体内容（例如，电影、音频轨道、图像等）的产生、传输、发现、存储、控制和呈现相关联的其它协议、标准、联网环境和装置。

[0064] 如先前指出，水印可用以保护音频或视听内容以防未被授权的使用。举例来说，发行到电影院的电影可嵌入有携带“非家用”(NHU) 代码的水印，其指示所述电影只能被专业复制单位复制且在专业投影设备上回放。在另一实例中，在蓝光光盘、DVD 上或由授权的下载服务发行的内容可嵌入有携带“受信任来源”(TS) 代码的水印，其指示此内容意在供消费者使用，但限制条件为其必须被受信任 DRM 技术保护。在另一实例中，内容可嵌入有携带代码的水印，所述代码唯一地识别内容，例如具有产业标准识别代码，例如国际标准音视频编号 (ISAN)、国际标准音像制品编码 (ISRC)、全球发行识别符 (GRID)、国际标准书号 (ISBN)、通用产品代码 (UPC) 或从另一编号系统指派的值，且针对所述代码提供使用识别代码以（例如）在本地存储的或在线数据库中“查找”关于内容和与其使用相关联的许可（或“权利”）的更详细的描述性信息的机制。根据所揭示的实施例而提供的所嵌入的水印可嵌入有内容的音频、视频和 / 或图像部分且经设计以与内容一起保留，无论内容在什么地方出现，包含在复制、转换为不同格式、由摄像机俘获和其它有意和无意的内容操纵之后。内容处置装置（例如，蓝光光盘播放器）可检测所嵌入的水印的存在且在识别到某些未被授权的使用时限制内容的使用。举例来说，可停止内容的未被授权的复本的回放或复制或可使内容的音频部分静音，这取决于提取了哪个嵌入的代码以及内容处置装置执行了什么操作。

[0065] 在一些实施例中,通过在使用(例如,回放、复制、传输、显示等)内容之前执行水印提取来实现水印提取效率的显著改进。在此些实施例中,水印提取操作有时被称作“后台”水印提取。在使用内容之前进行的水印提取操作可产生提取记录以供安全存储,以便减少在未来使用时对同一内容进行实时提取的需要。在一些实施例中,在使用内容之时对所述内容执行实时提取。在一些例子中,水印提取也可为实时提取。作为水印提取(例如,后台水印提取)的结果,可产生提取记录,其包含(但不限于)呈适合于存储的形式表示后台提取操作的结果的信息。此外,应理解,在所揭示的实施例的上下文中的术语“后台”无意传达必须在多任务操作系统内通过后台处理来执行相关联的操作。而是,后台提取可作为前台处理、后台处理或其组合的部分而被执行。在一些实施例中,内容使用可被延迟,直到水印提取过程至少部分完成为止。在又其它实施例中,水印提取和内容使用在时间上交错,使得水印提取始终在内容使用之前。在再其它实施例中,水印提取可在内容的传送或使用期间实时地且与内容的传送或使用同步地发生。

[0066] 根据所揭示的实施例,水印提取的结果以安全方式存储,使得其可在不同时间(例如,在内容使用开始时)被检索。在此背景下,水印提取由水印提取器执行,水印提取器可经配置以提取、处理、解码和分析所嵌入的水印以辨别水印的存在和/或获得所嵌入的水印的有效负载值。在一些实施例中,水印提取可进一步包含辨别与所嵌入的水印相关联的使用规则中的一些或全部。水印的提取通常为不影响宿主内容的完整性的被动操作。可在软件、硬件和/或固件中实施的水印提取器可进一步经配置以指定必须基于所提取的水印而起始的且与相关联的使用规则一致的潜在强制执行动作。在通过对所嵌入的水印的评定而检测到内容的未被授权的使用的一个实例中,可清除(即,删除)内容。替代地,可保存内容且可在方便的时刻(例如,在回放尝试开始时)向用户告知内容状态。在其它实施例中,可向用户建议一个或一个以上推荐的校正动作,例如购买允许内容的授权回放的许可证。以上情形仅提供可在提取一个或一个以上所嵌入的水印时开始的一些示范性强制执行动作。然而,应理解,可另外或替代地实行额外强制执行动作。

[0067] 在一些实施例中,如果内容没有所嵌入的水印,那么存储指示缺乏所嵌入的水印的信息(例如,存储在相关联的媒体数据文件中)以供未来使用。举例来说,在实际内容使用时,指示缺乏水印的所存储信息可用以允许内容使用而无需进行水印提取。在一些实施例中,提取过程可产生不足以触发强制执行动作的水印。举例来说,与受信任来源(TS)水印相关联的强制执行规则需要在触发强制执行动作之前在延长的时间周期内提取水印。举例来说,针对故事片的强制执行动作逻辑可能需要在9个顺序200秒筛选间隔中的至少7个间隔中发现TS水印以便触发强制执行动作。另一方面,对于短的视听内容(例如,短于一小时,例如TV演出),强制执行逻辑可能需要在9个顺序100秒筛选间隔中的至少7个间隔中发现TS水印以便触发强制执行动作。在一些实施例中,此强制执行逻辑包含(但不限于)与将导致指定强制执行动作的内容的使用类型有关的内容使用政策的元素。为了促进内容处置装置在这些和其它类似情形中的操作,在水印提取期间提取水印后,即刻存储所提取的水印以及相关联的时戳的列表以供稍后使用。

[0068] 所存储的信息必须以安全方式保护以防操纵。在一个实例中,数字签名用以确保所存储的信息为可靠的且未篡改。还需要通过防止未被授权的第三方存取所存储的信息来确保用户隐私。这可通过利用加密技术以保护所存储的数据以防未被授权的存取来实

现。明确地说，在 DLNA 中，当装置实施链路保护时，经由因特网协议的数字传输内容保护 (DTCP-IP) 为强制技术。因而，所有 DTCP-IP 相容装置被指派了唯一装置识别代码和装置公用 / 私人密钥对。在此情形中，所存储的提取信息可由 DLNA 相容装置的私人密钥进行数字签名且使用所述装置的公用密钥进行加密。在一些实施例中，提取信息可包含（但不限于）从执行提取操作获得的信息。因此，仅所述装置可产生新数字签名且对所存储的提取信息解密，而具有相关联的公用密钥的任何人可检测对所存储的信息进行的篡改尝试。

[0069] 图 1 说明可用以适应所揭示的实施例的示范性内容处置装置 100。内容处置装置可进行一个或一个以上操作，例如输入内容 102 的再现、记录、复制、传送和 / 或回放。输入内容 102 可通过一个或一个以上通信信道（其包括有线和 / 或无线通信信道）、磁性、光学、快闪和 / 或其它计算机可读媒体或其它来源传送到内容处置装置 100。因而，内容处置装置 100 可经配置以检测输入内容 102 的存在。内容处置装置内的相同或不同组件可检测从另一实体接收的对输入内容 102 的请求。可通过内容处置装置 100 内的检测器 / 接收器组件来执行对输入内容 102 的检测或对输入内容 102 的请求的接收。此检测器 / 接收器组件可为通信组件 110 的部分或为与通信组件 110 分离的组件。在内容处置装置 100 经配置以请求来自另一实体的内容的实施例中，内容处置装置 100 内的组件（例如，正执行程序代码的处理器）可产生对所述内容的此请求且通过（例如）通信组件 100 将所述请求传输到另一装置。在一个实例中，内容处置装置 100 为 DLNA 相容装置，其可与一个或一个以上其它 DLNA 相容装置通信。内容处置装置包括筛选输入内容以查看水印是否存在的水印提取器 104。如先前所指出，水印提取器 104 可提取、处理、解码和 / 或分析所嵌入的水印且辨别与所嵌入的内容相关联的使用规则。内容处置装置还可包含数字签名产生器 106，其可经配置以根据一个或一个以上算法产生数字签名。

[0070] 另外，内容处置装置 100 内的加密 / 解密组件 108 可经配置以对输入内容 102 和 / 或由水印提取器 104 产生的提取信息的一些或全部进行加密 / 解密。加密 / 解密组件 108 可经配置以实施多种公用和 / 或私人密钥加密和 / 或解密算法。内容处置装置 100 可进一步包含认证组件 120，认证组件 120 可产生与输入内容 102 相关联的认证参数、与提取信息相关联的认证信息和 / 或装置认证信息（例如，证书）。举例来说，认证组件 120 可包含产生用于一系列输入值的散列值的散列产生组件。认证组件 120 可进一步比较新产生的认证信息与先前存储的认证信息以验证内容的完整性。认证组件 120 可经配置以实施多种散列算法，例如 MD5、SHA-1 和 SHA-2。认证组件 120 可进一步经配置以执行为实行装置认证所必要的操作。因而，认证组件 120 可产生和传送对装置认证、认证信息的请求，交换认证证书且验证另一装置的可信性。

[0071] 图 1 还说明可驻留在内容处置装置 100 内的一个或一个以上存储单元 112。这些存储单元 112 可存储输入内容 102（例如，以加密、部分加密或明文格式）、由水印提取器 104 产生的信息以及相关联的索引信息和元数据、内容认证信息、与所嵌入的内容的使用相关联的相容规则和相关联的强制执行动作以及可被检索以便实施所揭示的实施例的功能性中的任一者的计算机程序代码。因而，存储单元 112 可与内容处置装置 100 的各种组件通信，例如内容处置装置 100 内的水印提取器 104、数字签名产生器 106、加密组件 108、认证组件 120、一个或一个以上处理器等。这些组件可检索和利用存储在存储单元 112 上的信息、计算机代码和内容。图 1 还展示可驻留在内容处置装置 100 外部的存储单元 118。外部

存储单元 118 可存储上述输入内容 102、水印提取记录以及其它数据和程序代码中的一些或全部,可通过通信组件 110 经由通信链路 120 与内容处置装置 100 通信。通信组件 110 可进一步允许内容处置装置 100 或内容处置装置 100 内的特定模块或组件与外部存储单元 118 和 / 或外部实体和用户通信。

[0072] 图 1 还描绘相容强制执行器 114,其可经配置以评估与特定内容的所提取的水印相关联的强制执行逻辑,且强制执行与强制执动作作相关联的规则。举例来说,此些强制执行动作可包含中止所要操作(例如,不输出输出内容 116),使与输出内容 116 相关联的音频静音和 / 或使与输出内容 116 相关联的屏幕消隐,和 / 或呈现版权约束通知。应理解,内容处置装置 100 也可包含图 1 中未明确展示的额外组件,一个或一个以上处理器或控制器以及额外存储装置。举例来说,内容处置装置内的组件可接收与可与内容处置装置 100 通信的其它装置相关联的信息。此信息可(例如)通过通信组件 110 接收。内容处置装置 100 内的相同或单独组件可关于将筛选操作(例如,水印提取、筛选等)中的一些或全部委托给内容处置装置 100 内的组件(例如,委托给水印提取器 104、相容强制执行器 114 等)和 / 或委托给可与内容处置装置 100 通信的其它装置而作出决定。内容处置装置 100 内的组件可在硬件或软件,或其组合中实施。另外,尽管将图 1 的媒体处置装置 100 描绘为单一装置,但与内容处置装置 100 相关联的组件或模块中的一者或一者以上可实施为单独装置的部分。举例来说,水印提取器 104 可在与实施相容强制执行器 114 的第二装置分离的第一装置中实施。

[0073] 根据所揭示的实施例执行的水印提取可在每当检测到新内容(例如,在例如 DLNA 相容网络等家庭网络内)以及每当空闲资源可用于 DLNA 相容网络内的某个受信任装置时执行。这样,可通过随着时间和 / 或在家庭网络内的其它装置上分配处理负荷来减小任何给定装置上的峰值处理负荷。所揭示的实施例进一步使后台水印提取能够结合可留在家庭网络外部的其它受信任装置和 / 或作为不同网络的部分的受信任装置而执行。举例来说,后台处理操作可至少部分由驻留在 DLNA 相容网络内的受信任装置进行,所述受信任装置可直接或间接地以安全方式与可驻留在装置的非集中式网络中的装置通信。将在随后的章节中论述关于如何识别和利用受信任装置来执行内容筛选操作中的全部或部分的其它细节。在一些实例中,执行具有低优先级的后台水印提取以确保计算和存储器资源可用于其它较高优先级操作且改进用户体验。

[0074] 为了促进提取信息的存取和检索,提取记录可通过内容文件名称(其(例如)包含文件夹名称或到文件的路径),通过与水印提取记录相关联的统一资源定位符(URL)编制索引。提取记录还可含有相关联的内容的文件大小。可通过周期性地搜索装置或可驻留在家庭网络内的额外 / 附属装置上的新文件名称来检测新内容的存在。替代地或另外,可在每当水印提取的机会出现时(例如,在空闲计算和存储器资源变得可用的情形中)检测新内容的存在。

[0075] 图 2 说明与根据示范性实施例的提取信息的产生和此信息的使用相关联的操作。过程开始于 202 处,其中执行水印提取。水印提取的结果可包含所提取的水印的有效负载值和指定内容内的所提取的水印的时间位置的相关联的时戳。提取信息可进一步包含文件名称、文件大小以及与内容相关联的其它信息。在 204 处,产生内容认证信息。此信息可用以验证内容尚未被修改或篡改。举例来说,在 204 处,可产生与内容相关联的散列值。如

随后的章节中将描述,散列值产生可确保内容的可靠性和其与相关联的提取信息的恰当对应。在 206 处,计算与提取信息相关联的数字签名。在一个实例中,将数字签名附加到提取信息。在 208 处,对提取信息和相关联的数字签名的至少一部分进行加密。在一个实例中,仅对提取信息进行加密,而在另一实例中,对提取信息和相关联的数字签名两者进行加密。接着在 210 处将完全或部分加密的提取记录存储在存储媒体上。某些额外操作(例如,对内容项目编制索引、压缩内容项目等)也可在水印提取 202 之后但在存储提取信息 208 之前的某一点执行。

[0076] 参看图 2,可在时间上较晚的例子处(例如,在内容的回放时)检索所存储的提取信息。在 212 处,验证内容的可靠性。在随后的章节中将进一步详细描述内容的认证。如果内容认证不成功(214 处的“否”),那么通过(例如)返回到方框 202 来针对内容进行水印提取操作。如果内容认证成功(214 处的“是”),那么在 216 处检查与提取信息相关联的使用规则。举例来说,与非家用水印有效负载相关联的使用规则可防止在消费型装置上回放内容。使用规则可存储在内容处置装置内部或外部的存储位置处。另外或替代地,可从外部实体(例如,受信任机构)接收使用规则。在 218 处,实行可适用的强制执行动作(如果有)。举例来说,可使输出内容的音频部分静音,或可中止复制操作。应注意,在一些实施例中,在步骤 210 中存储与所提取的水印相关联的使用规则以及提取信息。在这些实施例中,在 218 处施加强制执行动作之前,必须确保所存储的使用规则为最新的。在另一实施例中,也可在 210 处存储可适用的强制执行动作以及提取信息。

[0077] 图 2 的框图中所说明的操作也可适用于其中实时地执行水印的提取的实施例(例如,在内容被再现、显示等时)。在此些实施例中,与再现内容的特定片段并行地或稍早于再现内容的特定片段在 202 处产生提取信息。可存取至少暂时存储在存储位置处的提取信息以确定是否需要与相关联的使用规则一致的强制执行动作。在实时应用中,在 206 处产生数字签名以及在 208 处对提取信息进行加密可能因为缺乏计算资源而不可行。在这些情形中,提取信息可存储在水印提取器的防篡改部分内。可根据防篡改技术和此项技术中已知的算法执行装置(即,软件和/或硬件装置)内的防篡改模块的实施。

[0078] 图 3 说明在内容处置装置处检测到新内容文件后即刻开始的操作。在一些实施例中,当装置遇到新内容且开始用于获得相关联的提取记录的后续动作时,检测到新内容。在此些情形中,“新内容”为在提取记录中不具有匹配文件和/或路径名称的任何内容。在其它实施例中,内容处置装置可监视某些操作(例如,“保存”和“导入”操作),且在满足特定条件时触发额外操作。在这些实施例中,具有匹配路径和文件名称的内容仍被视为新内容。返回参看图 3,在 302 处,检测新内容的存在。如果在 304 处检测到文件名称为新的(即,在提取记录中找不到内容文件名称匹配),那么在 318 处指定文件经受水印提取。举例来说,可将内容放置在等待列表上以进行处理来用于水印提取。在一个实施例中,如果文件的基本名称(不管文件的完整路径名称)不存在于装置或相关联的实体(例如,连接的数据库)内,那么内容文件被视为新文件。如果内容文件不是新的(即,304 处的“否”),那么在 306 处确定新内容和现有内容是否具有相同的文件大小。如果文件大小不匹配(即,306 处的“否”),那么过程移动到 318,其中内容经指定以用于水印提取。如果在 306 处文件大小匹配(即,306 处的“是”),那么在 308 处触发内容认证操作(将在随后的章节中描述内容认证程序)。如果内容认证失败(即,310 处的“否”),那么在 318 处内容经指定以用于水

印提取。否则（即，310 处的“是”），在 312 处确定内容路径名称是否为新的（即，经由比较新内容的路径名称与保存在提取记录中的现有路径名称）。如果路径名称相同（即，312 处的“否”），那么在 316 处省略水印提取。否则，如果路径名称不同（即，312 处的“是”），那么在 314 处用新文件位置更新提取记录且在 316 处省略水印提取。

[0079] 图 3 的流程图希望促进对所揭示的实施例的理解。因此，可进行额外或更少步骤以便实施各种实施例。还应注意，为了促进对新文件和 / 或重复文件的搜索，可使用多种索引编制技术和参数来对所存储的内容文件和 / 或相关联的提取记录编制索引。举例来说，文件名称可用作搜索内容文件的数据库的索引。

[0080] 在其它实施例中，装置进一步验证先前分析的文件（例如，先前已经受水印提取的文件）是否仍存在于装置上。此过程可结合搜索新文件的过程来执行，或其可在空闲资源可用时或在装置上执行删除动作时独立地执行。如果从装置移除了与提取记录相关联的内容，那么也可移除提取记录以节省存储器资源且减少搜索整个所存储的提取记录的计算工作。

[0081] 在其中提取信息在内容使用时不可用的一些实施例中，可实时地（即，在运作中）执行水印提取。如果没有足够计算和 / 或存储器资源可用于实时提取的执行和内容的使用两者，那么内容使用可被延迟，直到水印提取过程至少部分完成为止。在一些实例中，水印提取和内容使用在时间上交错（例如，在一个片段上进行水印提取，随后为使用所述片段），使得水印提取始终在内容使用之前。

[0082] 重要安全考虑为在已完成水印提取之后内容修改或替换的可能性。举例来说，可在最初导入未标记的内容，且接着外部程序可试图用新内容（其可具有所嵌入的水印）取代内容的承载水印的成分。在此过程中，攻击者可有意保留相同文件名称和文件大小以防止内容被指定用于水印提取。为了挫败此尝试，装置必须在使用所存储的提取信息之前认证内容。此操作先前结合图 2 的步骤 212 进行描述。

[0083] 可使用单向加密散列函数（例如，MD5、SHA-1 或 SHA-2）来迅速且安全地执行内容认证。在对新导入的文件进行水印提取过程期间，计算散列值且将其与提取结果一起保存，如图 2 中步骤 204 到 210 所描绘。当开始内容使用时，计算内容的散列值且将其与先前存储的散列值进行比较（例如，图 2 中的 212 处）。如果新计算出的值与所存储的散列值匹配，那么内容被视为可靠的，且因此相关联的提取信息可用以实行任何可适用的强制执行动作。否则，如果计算出的散列值与所存储的散列值不匹配，那么可完全或部分停用内容的使用（例如，中止复制、停止回放、显示版权通知等）。另外或替代地，内容可经指定以经受新水印提取操作（参看，例如，图 2 的步骤 214 处的“否”和图 3 的步骤 310 处的“否”）。

[0084] 在一些实施例中，当内容为加密格式时，产生内容认证信息（例如，散列值）（例如，在图 2 中的步骤 204 处）。这样，当进行内容认证时（例如，在图 2 中的步骤 212 处），不需要在验证内容的可靠性之前对内容进行解密。因此，在内容使用时，所揭示的实施例仅需要产生内容认证信息（例如，散列值），而不是进行完整水印提取操作。所揭示的实施例的这个方面在内容处置装置的操作的效率方面提供实质改进，特别是在水印提取之前需要内容变换（例如，解密、解压缩、多路分用等）的情况下。许多散列函数可在硬件和 / 或软件中有效地实施。在其中对水印提取记录进行加密（参看，例如，图 2 的步骤 208）的一些例子中，必须对所存储的提取信息进行解密以便检索所存储的散列值。然而，由于所存储的

水印提取记录的大小相对小,所以此解密操作不可能呈现显著处理负担。

[0085] 在选择散列函数时的至关重要的要求为抗前像,定义如下:给出散列值 h ,难以(几乎肯定任何对手都达不到)找到消息 m 使得 $h = \text{hash}(m)$ 。此要求与攻击有关,其中盗版者试图用具有相同散列值的未标记的内容替换标记的内容,以便产生自由提取的水印提取报告。在这种攻击情形中,在内容处置装置对未标记的内容进行水印提取之后,攻击者可试图用具有相同散列值的标记的内容取代未标记的内容,以避免对标记的内容的筛选。

[0086] 应注意,上述前像要求比抗碰撞要求容易满足。抗碰撞要求可如下定义:应难以找到两个不同的消息 m_1 和 m_2 使得 $\text{hash}(m_1) = \text{hash}(m_2)$ 。此要求通常使得必须使用要求更高的散列函数(例如,散列函数的 SHA-2 家族),此要求在散列函数用于索引编制方案时较普遍。然而,在较不严格的抗前像提供足够保护的情形中,可使用较简单且计算要求较小的散列函数(例如,MD5 和 SHA-1)。

[0087] 在一些实施例中,可通过从内容选择仅数据的子集以输入到散列函数计算来实现与散列函数计算相关联的处理负荷的进一步减小。在一个实例中,将选择过程维持为秘密。举例来说,可使用随机数产生器来选择随机内容片段,随机数产生器使用装置私人密钥作为种子。

[0088] 所揭示的实施例通过考虑与马赛克攻击有关的安全性问题来进一步提供内容处置装置的操作。马赛克攻击被定义为将内容分裂为多个片段,使得每一内容片段可个别地避开强制执行动作。在此攻击情形中,将内容划分为个别地经受水印提取的若干片段。在实际内容使用期间,在内容再现情况下使用(例如)播放列表特征来再次组合所述片段以用于向用户呈现。粗略的马赛克攻击通常涉及产生相对大的内容片段。举例来说,可将故事片分段为若干 10 分钟的块,以便避免个别片段上的受信任来源(TS)强制执行。此攻击可成功用于标记有 TS 的内容,因为如先前所指出,需要若干内容片段中的重复水印提取以触发强制执行动作。

[0089] 在一个实施例中,可通过安全地存储与相容装置相关联的内容使用历史且随后用每一新内容使用来检索和分析内容使用历史以防止粗略的马赛克攻击在所述装置中发生。内容使用历史提供预定义间隔(例如,装置进行的内容使用的至少最后 20 分钟)内的所有水印提取的记录以及相关联的时戳。可接着将任何新内容使用的水印提取结果附加到所检索的内容使用历史数据以便评估强制执行条件是否存在。在利用播放列表的马赛克攻击的情况下,强制执行条件的评估可基于播放列表上按列出次序的每一项目的所检索的内容使用历史和提取记录的聚集。这样,可有效地评估强制执行条件而不必在内容使用开始时进行实时水印提取操作。

[0090] 另一攻击情形与精细的马赛克攻击有关,其中内容被划分为具有精细粒度的大量片段,使得来自每一个别片段的水印提取不可行。精细的马赛克攻击意味着由于小文件处置而引起的显著开销,且因此对于许多装置来说可能不实际。举例来说,故事片可被分段为若干 1 秒剪辑且保存为一串独立文件,所述文件稍后使用某种播放列表功能而被串联。尽管如此,根据所揭示的实施例,可通过恰当地辨识精细的马赛克攻击的存在来有效地阻挠此攻击。在一个实施例中,在某一大小限制以下的内容文件的存在触发精细的马赛克防范措施。举例来说,对小于 5 秒长的视听内容文件的检测可在水印提取过程期间触发精细的马赛克防范措施的旗标。

[0091] 在一个实施例中,通过在播放列表中提供的多个串联文件上需要水印提取来阻挠精细马赛克攻击。可在内容使用之前或在内容使用期间实时地执行串联文件上的水印提取。在一个实施例中,如果串联文件含有在大小限制以下和以上的文件的混合,那么仅针对总长度在大小限制以上的邻近短文件的集合执行水印提取。此提取过程的结果可与用于在大小限制以上的文件的提取信息的结果(其应已在先前进行)组合,且用于强制执行逻辑评估和/或强制执行。

[0092] 在替代实施例中,在检测到精细的马赛克攻击后,可即刻例示高级水印提取器。高级提取器可在后台模式下执行大多数处理,且保存中间数据以供未来使用。举例来说,中间数据可由内容特征组成,所述内容特征针对水印提取为相关的且具有比原始内容小得多的大小。所揭示的实施例的此特征可导致计算和存储器资源的使用的显著减少。因此,在检测到精细马赛克攻击后,装置可即刻仅通过评估中间数据来迅速且有效地提取所嵌入的水印,这与试图从原始内容提取水印形成对比。举例来说,在使用扩展频谱水印的系统中,中间数据可包括已知扩展频谱载波与具有特定粒度的内容样本之间的相关值。在内容使用时,串联中间数据,尝试水印提取且基于从中间数据提取的任何水印来评估强制执行条件。如先前所指出,在一些实施例中,如果串联文件含有在大小限制以下和以上的文件的混合,那么仅总长度在大小限制以上的邻近短文件的集合需要中间数据串联和水印提取。此提取过程的结果可组合与在大小限制以上的文件相关联的提取信息,且用于强制执行逻辑评估和/或强制执行。

[0093] 在可建立受信任装置的网络的情形中,使用网络来共享水印提取和强制执行职责可为有利的。在一个实施例中,如果具有新内容项目的装置不能解译内容的格式,那么装置可将水印提取操作的全部或一部分托付给可解译内容格式的另一装置。执行水印提取的装置可向委托装置报告提取信息以用于进一步动作和/或安全存储。

[0094] 图4说明使用调用模型来实现合作水印提取的示范性实施例。在此实施例中,接收输入内容402的主装置404具有执行产生输出内容406的操作(例如,复制、传送、播放、记录等)的任务。如图4中所描绘,主装置404调用从属装置412来对传送到从属装置412的选定内容408执行水印提取。在从属装置412完全或部分完成水印提取后,主装置404即刻接收提取信息410且决定是否将选定内容408递送到目的地装置和/或是否批准额外强制执行动作(例如,使警告消息静音或显示警告消息)。此调用模型可应用于以下情形中:主装置404不具有水印提取的能力,或其过载(例如,在多个串流传输的例子或水印提取任务的情况下),或其不具有处置选定内容的适当编解码器。

[0095] 图5说明使用委托模型来实现合作水印提取的另一示范性实施例。在此实施例中,具有对输入内容402执行操作(例如,复制、传送、播放、记录等)的任务的委托装置504完全将水印提取委托给受委托装置510。受委托装置510从委托装置504接收选定内容508且执行水印提取操作。受委托装置510根据与提取信息514相关联的使用规则进一步决定是否将所请求的内容(即,如果作出转发内容的决定,那么为受信任内容512)转发到目的地装置514。在一个情形中,受委托装置执行水印提取和筛选操作,同时串流传输内容直到使用规则限制内容的使用为止(例如,停止串流传输或静音的音频)。在另一情形中,内容到目的地的传送可仅在部分或完全完成水印提取和筛选之后开始。另外,受委托装置510可或可不将提取信息514传回到委托装置504(此任选操作由图5中的虚线箭头描绘,其从

受委托装置 510 开始且终止于委托装置 504)。委托模型可用于以下各种情形中 : 委托装置 504 不具有水印提取的能力, 或其过载 (例如, 在多个串流传输的例子或水印提取任务的情况下), 或其不具有处置所请求内容的适当编解码器。明确地说, 此模型在以下情形中有用 : 需要存在桥接装置 (例如, 受委托装置 510) 以实现内容变换, 例如将高清晰度内容转换为 MPEG-4 移动版本等。

[0096] 在调用和委托模型两者中, 可合作地执行筛选的装置可双向地或单向地知道编解码器能力。其可在选定内容的传送开始之前或开始时查询或交换编解码器能力。举例来说, 在采用 HTTP 协议以用于内容传送的 DLNA 中, 装置使用在 DLNA 媒体格式简档中定义的 MIME-TYPE 值以作为 HTTP 请求或响应中的 Content-Type 的值来规定所请求内容的编解码器。例如 RTP (实时传输协议) 等其它内容传送协议也支持编解码器能力的交换。

[0097] 在利用调用或委托模型的一些系统中, 可能有可能选定内容的发送者 (主装置 404 或委托装置 504) 不知道接收装置 (从属装置 410 或受委托装置 510) 的编解码器能力。在一些实施例中, 在此些情形中, 如果接收装置不具有需要处理所请求内容的适当编解码器, 那么接收装置立即向发送者告知异常 (作为提取信息 514 的部分)。接收装置也可任选地请求发送者转换和重新传送呈可由接收装置处理的媒体格式的内容。

[0098] 在实时水印提取情形中, 根据所揭示的实施例的合作水印提取可在第一装置存取内容且第二装置再现 (例如, 显示) 所述内容的情形中实施。在这些情形中, 内容存取装置通常不能解译内容, 而再现装置 (其当然能够解译内容) 不受信任。在这种情况下, 内容存取装置可起始搜索以发现可解译内容的受信任装置。此受信任装置必须还能够以比内容的实时再现快或与内容的实时再现相等的速率执行水印提取。可 (例如) 通过咨询可由内容存取装置安全地存取的受信任装置的列表来识别受信任装置。此列表还可从受信任机构安全地传送到内容存取装置。在另一实施例中, 在装置发现期间基于 UPnP (通用即插即用) 联网协议而产生列表。举例来说, DLNA 使用 UPnP 以用于发现和描述装置类型和能力。在其它实施例中, 开始装置认证程序以验证装置的可信任性且探知其能力。将在随后的章节中进一步描述装置认证程序。由受信任装置产生的提取结果和 / 或强制执行事件可传回到内容存取装置以用于进一步动作和 / 或安全存储。

[0099] 上述实时水印提取情形可视为上述调用模型的实例。此实例情形允许商业内容在传统再现装置 (例如, 无水印提取器的 DLNA TV) 上递送。为了鼓励采用受信任再现装置, 内容拥有者、PayTV 公司以及越顶 (OTT) 和按需点播内容提供者可向用户提供激励, 用户将奖金内容直接再现在受信任再现装置上。替代地, 受 DRM 保护的商业内容中的旗标可由内容分配者插入以指示内容必须由受信任客户端再现。

[0100] 在一些实施例中, 如果实时水印提取操作不可行 (即使在具有额外受信任装置的合作的情况下也如此), 那么延迟的水印提取操作仍可在每当必要资源变得可用时进行。由延迟的水印提取操作产生的结果可存储为所述内容的提取记录的部分。举例来说, 水印提取记录可存储在数据库处, 其中所述记录可在未来由一个或一个以上受信任装置存取。在执行延迟的水印提取操作的情形中, 可易于使用所存储的提取记录来筛选对所述内容的任何后续实时存取。

[0101] 实时应用 (例如, 视频内容的直播) 的另一方面在于在内容再现之前仅内容的一小部分可用。在这些情况下, 可能不可能在内容使用之前使用仅本地可用资源来执行水印

提取。因此,如先前所指出,可需要实时的水印提取操作。在一些实施例中,可通过提供由受信任装置产生的提取记录以伴随串流传输的内容来消除进行实时水印提取的需要。如先前所指出,内容认证可确保内容的完整性以及其与现有提取记录的恰当对应。然而,在串流传输应用的背景下,完全认证串流传输的内容在内容的串流传输期间可能不可能,这是因为完整内容仅在串流传输会话结束时才变得可用。

[0102] 在一些实施例中,通过利用分段的散列值来启用内容的一个或一个以上部分的认证。明确地说,将内容划分为具有特定大小(例如,时间为10秒或大小为1MB)的若干片段,且针对每一内容片段产生散列值且将其与对应水印提取记录存储在一起。这样,可根据内容片段的粒度用计算出的散列值以较小单元来认证内容。在串流传输操作期间,可通过计算所接收的内容片段的对应散列值和将所述散列值与存储在提取记录中的散列值进行比较来认证所接收的内容片段(例如,驻留在缓冲器中的内容片段)。当片段在串流传输操作期间变得可用时,可按顺序并连续地选择片段以用于认证。或者,可选择内容片段的子集以用于认证。在一个实施例中,可根据确定模式(例如,选择每第三个片段)或根据随机/伪随机选择模式(例如,具有均匀分配的随机选择)来选择片段的子集。对于甚至一个片段,认证失败可用信号通知内容已被操纵,且因此触发实时提取操作。或者,检测到内容操纵可中止内容使用。

[0103] 根据所揭示的实施例,分段的散列值由一系列散列值组成,其中每一散列值是从内容的片段计算的。片段可通过内容的固定时间周期或固定字节大小定义。此外,可填补最终内容以产生具有预定义的固定大小的片段。用于产生分段散列函数的一个示范性算法描述如下。假定C为视听内容,且 c_1, c_2, \dots, c_n 为C的连续片段,或C的随机选定片段。在选择片段的情况下,可实现认证粒度与性能之间的灵活性。举例来说,为了获得较佳计算性能,可选择较少片段。片段的大小也将对性能具有影响,如由计算和资源效率所测量。明确地说,较小片段需要较少计算以用于认证所述特定片段。然而,可需要最小片段大小限制来确保散列函数的安全性。

[0104] 在一个实施例中,可通过提供在如由(例如)随机数产生器确定的特定范围内变化的片段大小来进一步增强所产生的散列值的安全性。用于产生与可变片段大小相关联的散列值的示范性算法描述如下。假定HF为散列函数,其接受种子值s和数据块 c_n 以产生散列值 h_n 。可使用以下操作集合来计算片段 c_1, c_2, \dots, c_n 的散列值:

$$[0105] h_1 = HF(s, c_1); \quad (1)$$

$$[0106] h_2 = HF(h_1, c_2);$$

[0107] ...

$$[0108] h_n = HF(h_{n-1}, c_n).$$

[0109] 可如下计算直到片段 c_i ($1 < i < n$)的内容的散列值 H_i 。

$$[0110] H_i = HF(s, h_1 + h_2 + \dots + h_i) \quad (2)$$

[0111] 使用散列值以用于内容认证的一个主要优点为散列函数将串流传输的内容视为二进制流,而不管内容格式如何、内容是否被加密以及哪些加密算法用于加密。所揭示的实施例可结合不同散列函数而使用。举例来说,在奔腾90MHz计算机上的软件中的MD5实施方案可按每秒45百万位处理输入数据。为了进一步加速散列处理,可将来自每一片段的某些选择性字节而不是每一字节视为散列函数的输入。

[0112] 在另一实时水印提取情形中,根据所揭示的实施例的合作水印提取可在内容存取装置缺乏同时执行内容存取、传输、再现和水印提取的处理能力的情形中实施。明确地说,此情形可在相同装置经配置以进行多个内容流的同时存取和传输时出现。在这些情形中,可将水印提取委托给有能力且受信任装置。提取信息和 / 或强制执行事件可传回到内容存取装置以用于进一步动作和 / 或安全存储。此实时合作水印提取为上述调用模型的另一实例。

[0113] 图 6 说明另一实例实施例,其中内容由内容服务器 602 递送到内容客户端装置 604。内容服务器 602 和 / 或内容客户端装置 604 可与存储单元 606、从属装置 608 和 / 或受委托装置 610 通信。取决于系统配置,内容服务器 602 和 / 或客户端内容装置 604 可作为主装置与如先前结合图 4 的调用模型论述的从属装置 608 通信。类似地,取决于系统配置,内容服务器 602 和 / 或客户端内容装置 604 可作为委托装置与如先前结合图 5 的委托模型论述的受委托装置 610 通信。图 6 中描绘的通信链路 612 实现图 6 中所展示的装置之间的内容、提取信息和其它信息的通信。举例来说,通信链路 612 中的一者或一者以上可允许不同装置之间的安全通信(例如,经由链路加密)。另外,内容服务器 602、内容客户端装置 604、存储单元 606、从属装置 608 和受委托装置 610 中的一者或一者以上可驻留在家庭网络(例如,DLNA)内。在其它实施例中,内容服务器 602、内容客户端装置 604、存储单元 606、从属装置 608 和受委托装置 610 中的一者或一者以上可驻留在家庭网络外部。

[0114] 参看图 6,可了解可在实时和非实时应用中使用所描绘的装置中的一者或一者以上执行水印提取和适用筛选操作和强制执行动作的实施。另外,图 6 中描绘的内容处置装置可驻留在网络(例如,DLNA 相容网络)内部,所述网络可包含可直接或间接彼此通信的多个其它服务器装置、客户端装置、存储单元等。另外,位于此网络内的装置可与驻留在网络外部的多个其它装置通信。在一些实施例中,网关装置 614 可经由通信链路 612 与图 6 中描绘的其它装置和 / 或驻留在家庭网络内部或外部的其它装置中的一者或一者以上通信。网关装置 614 可(例如)协调各种装置的操作以促进水印提取、提取记录的传送、认证操作、受信任装置列表的传送和 / 或获取等。将在随后的章节中论述关于网关装置 614 的操作的进一步细节。

[0115] 在一些情形中,大量内容处置装置(例如,图 6 中描绘的内容处置装置)可彼此通信以交换内容文件或进行其它操作。然而,可能仅些内容处置装置的子集具有进行水印提取、对照内容使用规则来评估提取记录和 / 或实行强制执行动作的能力。因此,任务仍然是关于如何恰当地识别具有这些能力中的全部或一部分的值得信任的装置。进一步有必要确定在各种装置之间分配所需工作负荷以及在装置之间进行各种通信的最有效且安全的方式。

[0116] 根据所揭示的实施例执行的装置认证使得每一装置能够验证另一装置为“受信任”装置。通过建立装置的可信任性,每一装置的能力可向彼此传送。图 7 说明根据实例实施例可在装置 A702 与装置 B704 之间执行的认证程序。在操作 706 中,装置 A702 将其证书传输到装置 B704。在操作 708 中,装置 B704 验证装置 A702 的所接收到的证书,进而确定装置 A 的可信任性,以及装置 A702 的一些或所有能力。在一个实例中,受信任装置认证使得装置 B704 能够验证由装置 A702 提供的证书是从受信任机构颁发的。类似地,在操作 710 中,装置 B704 可将其证书传输到装置 A702。在操作 712 中,装置 A702 确定装置 B704 是否

为受信任装置且进一步探知装置 B 的能力。应注意,认证过程可包含此项技术中已知的额外操作。举例来说,认证过程还可包含装置 A702 与装置 B704 之间的一个或一个以上挑战和对应响应的通信。在一些实施例中,进行这些额外操作以确保所传送的信息不仅是从缓存位置复制的。

[0117] 在一些实施例中,可使用 DTCP-IP 认证协议执行装置认证。DTCP-IP 规范包含强制完全认证和任选扩展完全认证程序。DTCP-IP 使用高级加密标准 (AES)-128 以用于内容加密。DTCP-IP 的两种认证程序都使用基于公用密钥的椭圆曲线数字签名算法 (EC-DSA) 以用于签名和验证。由数字传输许可管理员 (DTLA) (即, DTCP-IP 的许可管理员和开发者) 颁发的装置证书存储在相容装置中且在认证过程期间使用。所有相容装置还被指派了唯一装置 ID 和由 DTLA 产生的装置公用 / 私人密钥对。装置证书包括多个字段,包含关于证书格式、装置 ID、数字签名、DTCP 公用密钥等的信息。DTCP-IP 认证协议的使用允许认证装置在证明装置为相容之后证实受认证的装置拥有由 DTLA 发行的私人密钥。

[0118] 在一个示范性实施例中,与 DTCP-IP 装置证书相关联的保留位中的一些可用以用信号通知装置的内容筛选 (例如,水印提取和强制执行) 能力。因此,此装置证书可用以确定装置是否为受信任装置且获得关于装置的筛选能力的信息。在其它实施例中,例如提取记录数据库的位置等额外信息可在两个装置之间交换。装置可进一步交换关于其处理和存储能力的信息。

[0119] 在另一实施例中,装置认证可使用远程证明来获得受认证的装置为相容的增加的保证。远程证明在认证装置与受认证的装置之间使用加密协议以使得认证装置能够确定受认证的装置被证实为相容的且未被修改。协议需要受认证的装置执行其内部处理状态 (例如计算数据或代码的散列或对其计算操作执行时序测量) 的具体计算 (或“测量”),其结果向认证装置提供其在测量时的操作与在装置被证明为按相容方式表现之时执行的操作匹配的确定性。在一个示范性实施例中,可使用例如受信任平台模块 (TPM) 或其它安全处理单元等“受信任硬件根”来执行远程证明。TPM 为硬件装置,其可将密码、证书、加密密钥和其它值安全地存储在内部存储器中,且基于从较通用的计算机处理器 (例如, CPU) 接收的指令和其它数据值来将密码学原语的非常有限的集合应用于那些值。存储在 TPM 的内部存储器中的值保持为秘密且仅可通过 TPM 的有限加密函数存取。TPM 通常包含在来自 CPU 的单独计算机芯片 (例如, 附着到 PC 的母板) 中,但也可并入到含有 TPM 和一个或一个以上 CPU 以及其它硬件功能的系统级芯片中。将此数据存储在硬件芯片上而不是计算机硬盘驱动器上或可由通用 CPU 直接存取的存储器内使得能够针对装置的行为建立“受信任硬件根”且显著地增加整个平台的安全性。此硬件存储位置确保所存储的信息更安全而不会受外部软件攻击和物理偷窃。TPM 提供三种安全功能性 :1) 由仅对 TPM 可用的密钥加密的任何数据的安全存储 ;2) 包含 BIOS、启动扇区、操作系统和应用软件的平台的完整性的测量和报告 ;和 3) 使用由 TPM 保护的签名密钥经由数字签名对平台或专用数据进行的认证。

[0120] 为了在 TPM 平台中实现装置认证,受信任一方 (例如, 证书机构) 将签署由 TPM 保护的签名密钥。也由 TPM 保护的此些证书用以证明签名密钥确实属于有效 TPM。具有受 TPM 保护的证书和签名密钥的两个装置可基于 DTCP-IP 认证以与上文所论述相同的方式执行认证过程。唯一的不同之处在于 TPM 平台中的签署密钥更安全。

[0121] 具有 TPM 能力的装置可认证另一不具有 TPM 能力的装置。此认证可导致不相等的

可信任性,其接着可由服务提供者使用以提供不同服务。举例来说,高值内容(例如,高清晰度或早先发行的内容)可仅被递送到具有TPM能力的装置,而其它内容可被递送到具有TPM能力和不具有TPM能力的装置两者。

[0122] TPM含有数个160位寄存器(称作平台配置寄存器(PCR))以用受信任方式测量和报告平台环境的状态。从受信任根开始,其使得受信任实体能够获得关于平台状态的忘不了的信息。可执行程序可通过计算其散列代码来测量另一程序并组合当前测量与散列值且将组合存储在PCR中。因此,PCR表示从通电到目前的经执行程序的历史的累积测量。此受信任链提供对恶意程序的有力防御,例如脆弱程序上的病毒、间谍软件和攻击。其还可用于检测和停用未被授权的程序,例如盗版软件或非法程序。

[0123] 软件媒体播放器(尤其在PC环境中)已成为大多数内容保护系统的弱点。在TPM平台上扩展媒体播放器的受信任链通过启用检测且进一步停用未被授权的程序和/或对软件播放器的修改来加强安全性。

[0124] TPM可针对数据加密产生可迁移或不可迁移密钥。非可迁移密钥从不离开产生其的TPM,而可迁移密钥可被导出到其它平台(装置)。因此,可通过使用TPM产生的非可迁移密钥对内容加密来将内容锁定到具有TPM能力的装置中,使得内容仅可在所述装置上被解密和播放。此被理解为使用“受信任软件根”执行远程证明的唯一做法。然而,当前已知或可能在未来变成已知的其它方法和装置可用以实现装置认证的目的。

[0125] 基于各种装置的受信任状态以及其能力的评定,可在那些装置之间共享需要确保与内容相关联的恰当水印提取和筛选操作的各种操作。为了促进论述,可将与将内容从内容服务器提供到内容客户端装置(参看,例如图6的内容服务器602和内容客户端装置604)相关联的操作划分为(1)水印提取和(2)筛选。举例来说,水印提取可包含(但不限于)提取水印、计算内容认证信息、产生数字签名和将结果存储在安全位置中。另一方面,筛选可包含(但不限于)验证内容可靠性、获取和验证使用规则以及实施强制执行动作(如果需要)。也应理解,水印提取和筛选操作之间的某一重叠可能存在。举例来说,某些操作(例如,获取和验证相容规则)可作为水印提取和筛选操作中的一者或两者的部分而进行。因此,仅呈现上述操作划分以促进对基础概念的理解而无意限制所揭示的实施例的范围。

[0126] 取决于装置是否受信任(即,认证为相容的)、计算资源的可用程度、相容能力、所需操作安全性、架构和设计复杂性、用户体验考虑、内容拥有者的偏好和其它因素,水印提取和筛选操作可由可驻留在家庭网络内部和/或外部的一个或一个以上装置进行。举例来说,表1提供水印提取和筛选的职责可如何在八个示范性情形中在各种装置之间共享的列表。

[0127] 表1-操作的实例划分

[0128]

情形	负责任的装置	水印提取	筛选
1	内容客户端装置	内容客户端装置	内容客户端装置
2	内容客户端装置	从属装置	内容客户端装置

3	内容客户端装置	受委托装置	受委托装置
4	内容服务器	内容服务器	内容服务器
5	内容服务器	从属装置	内容服务器
6	内容服务器	受委托装置	受委托装置
7	内容客户端装置和内容服务器	内容服务器	内容客户端装置
8	内容客户端装置和内容服务器	内容客户端装置	内容服务器

[0129] 表 1 说明在情形 1 中, 水印提取和筛选操作两者都在内容客户端装置处执行, 而在情形 4 中, 两个操作都在内容服务器处执行。在剩余情形中, 水印提取和筛选操作通过内容客户端装置、内容服务器、受委托装置和 / 或从属装置的合作进行。明确地说, 在情形 2 中, 内容客户端装置调用进行水印提取的从属装置。举例来说, 此从属装置可为具有水印提取能力的另一受信任内容客户端装置或受信任服务器装置。在情形 3 中, 内容客户端装置 (其为受信任装置) 将水印提取和筛选操作两者都委托给受信任受委托装置。情形 4 到 6 提供情形 1 到 3 的类似情形。但在情形 4 到 6 中, 内容服务器为可独立地进行筛选操作、调用从属装置以进行筛选操作或将这些操作委托给受委托装置的负责任的装置。在情形 7 中, 内容服务器进行水印提取操作且内容客户端装置执行筛选。在情形 8 中, 内容客户端装置进行水印提取操作且内容服务器执行筛选。

[0130] 可了解, 表 1 的示范性列表不提供所有合作情形的详尽列表。举例来说, 情形 7 的变化可经建构, 其中水印提取由内容服务器通过调用从属装置来实施。如先前所指出, 选择一个或一个以上受信任装置以与一个或一个以上受信任装置合作进行特定操作可受多种因素 (例如, 用户偏好、实施的复杂性等) 影响。表 2 提供基于六个不同因素的表 1 的八个情形的示范性评估。

[0131] 表 2- 情形 1 到 8 的示范性评估

[0132]

情形	处理性能	装置制造商的集成复杂性	消费者体验	架构复杂性	呈合适格式的内容的可用性	总偏好排名
S1	非常好	中等	非常好	高	是	1
S2	一般	高	可能较差	中等到高	可能	7
S3	一般	中等到高	一般到好的	中等到高	很可能	8
S4	可能较差	中等	非常好	低	很可能不	2
S5	一般	高	可能较差	低到中等	可能	6
S6	一般到好的	中等到高	一般到好的	低到中等	很可能	4
S7	可能较差	中等	非常好	低	很可能不	5
S8	非常好	中等	非常好	高	是	3

[0133] 表 2 的示范性评估提供用于情形 1 到 8 中的装置的每一配置的优点的粗略评定。出于说明的目的,表 2 进一步包含有限数目个因素。然而,应理解,例如每一装置的计算负荷和存储能力、内容拥有者的偏好等额外因素也可在进行每一情形的评定时加以考虑。表 2 的最右栏提供每一情形的总偏好排名。可通过考虑表 2 中列出的所有评估项和 / 或表 2 中未列出的额外因素来产生此总排名。在一个实施例中,此总偏好排名用作默认设置,其在缺少特殊指令的情况下规定装置的优于其它配置的特定配置。

[0134] 表 2 的审阅揭露,即使内容服务器和内容客户端装置两者能够执行水印提取和 / 或筛选操作,将某些操作指派给所述装置中的一者或两者(或甚至第三装置,例如受委托装置或从属装置)以适应特定偏好也可为优选的。根据所揭示的实施例,如果客户端内容装置和内容服务器两者都为受信任实体,那么其可探知彼此的能力,并决定如何最有效地进行水印提取和筛选操作。如果装置中仅一者为受信任装置,那么所述装置必须确定如何独立地或与其它受信任装置合作地执行必要的水印提取和筛选操作。

[0135] 图 8 为根据示范性实施例与以合作方式进行的水印提取和筛选操作相关联的流程图。在 802 处,检测到对内容存取的请求。此请求通常由内容客户端装置起始且被引导到内容服务器。然而,在一些实例中,请求可在内容客户端装置、内容服务器和 / 或其它装置之间传送。在 804 处,执行装置认证。举例来说,可执行结合图 7 描述的装置认证以确定装置的受信任状态且获得某些装置能力。如果在 806 处确定两个装置都受信任(即,806 处的“是”),那么在 808 处某些装置能力可任选地在两个受信任装置之间交换。如先前所指出,装置能力中的一些或全部可在 804 处的装置认证步骤期间交换。然而,在一些实施例中,可在单独步骤中进行装置认证和装置能力的获取。举例来说,某些装置能力(例如,装置是否可执行水印提取或筛选)可在认证步骤(即,804 处)期间被探知,而其它装置能力(例如,装置是否具有进行额外操作的空闲计算资源)在随后的信息交换操作(即,808 处)期间被探知。

[0136] 返回参看图 8,在 810 处,两个装置合作地确定恰当的操作配置。此步骤允许基于所要准则在两个受信任装置(和 / 或额外受信任装置)之间划分工作。举例来说,可基于表 2 中列出的偏好来选择对应于情形 S1 到 S8(参看表 1) 中的一者的操作配置。或者,可选择具有最高总偏好排名的可用操作配置。在 812 处,水印提取和 / 或内容筛选操作由在 810 处选择的适当装置进行。还应注意,812 处的内容筛选操作可仅包括从受信任装置(或从对受信任装置已知的安全存储位置)接收现有水印提取记录,且根据所接收的提取记录进行筛选(例如,参看图 2 的步骤 212 到 218)。在先前存在的水印提取记录不存在(或不能被存取)的其它实施例中,在 812 处可通过一个或一个以上受信任装置执行水印提取和 / 或内容筛选操作。

[0137] 如果在图 8 中的 806 处确定为“否”,那么过程移动到 814,其中确定是否只有一个装置受信任。可在(例如)受信任内容客户端装置不能认证内容服务器时作出此确定。或者,如随后的章节中将描述,中心机构可作出此确定。如果只有一个装置受信任(即,814 处的“是”),那么在 816 处受信任装置确定用于进行水印提取和 / 或筛选操作的恰当配置。在这么做时,受信任装置可利用在家庭网络内部或外部的其它受信任装置的服务。在确定恰当配置之后,过程即刻移动到 812,其中进行水印提取和 / 或内容筛选操作。如果在 814 处确定装置中无一者受信任(即,814 处的“否”),那么在 818 处可中止过程(例如,拒绝内容

存取)。或者,可以受保护的格式(例如,以加密格式)提供内容。在一些实施例中,以降级格式递送内容。在又其它实施例中,仅递送内容的一部分。

[0138] 图8中描述的操作可在家庭网络内的每一装置试图获取内容时至少部分被重复以提供内容,或索要筛选来自家庭网络内的另一装置的服务/信息。另外,如果在网络内部与外部的装置之间存在用于认证的机构,那么上述操作也可在装置的至少一者驻留在家庭网络外部时执行。

[0139] 表3提供基于两个装置的受信任状态和两个装置处的水印提取和筛选能力的可用性而组织的装置配置可能性的示范性列表。S1到S8分别表示先前结合示范性情形1到8所论述的装置配置。

[0140] 表3-基于筛选能力的操作配置可能性

[0141]

				内容客户端装置				不受信任	
				受信任					
				水印提取可用	水印提取不可用				
				筛选可用	筛选不可用	筛选可用	筛选不可用		
内容服务器	受信任	水印提取可用	筛选可用	S1、S2、S3、 S4、S5、S6、 S7、S8	S3、S4、 S5、S6、 S8	S2、S3、 S4、S5、 S6、S7	S3、S4、 S5、S6	S4、 S5、 S6	
			筛选不可用	S1、S2、S3、 S6、S7	S3、S6	S2、S3、 S6、S7	S3、S6	S6	
	水印提取不可用	筛选可用	S1、S2、S3、 S5、S6、S8	S3、S5、 S6、S8	S2、S3、 S5、S6	S3、S5、 S6	S5、 S6		
		筛选不可用	S1、S2、S3、 S6	S3、S6	S2、S3、 S6	S3、S6	S6		
不受信任				S1、S2、S3	S3	S2、S3	S3	N/A	

[0142] 表3说明根据示范性实施例的基于每一装置的受信任状态和可用筛选能力的不同操作配置的可用性。一旦确定操作配置中的哪些可用,可选择特定配置以实行所要筛选操作。举例来说,如先前所指出,可选择提供最佳总偏好排名的配置。

[0143] 通过向各装置和在内容分配的各点处提供水印提取和筛选能力,可实现内容的安全分配。水印提取和筛选操作的分离进一步促进具有有限计算资源的“相容”装置(例如移动装置)的扩散。这些相容装置为受信任装置,其可(例如)实施水印提取和/或筛选能力的仅一部分,且依赖其它装置来提供剩余操作能力。图9为不同内容分配情形的示范性图,其涉及相容内容服务器902、非相容内容服务器904、相容内容客户端装置906、非相容内容客户端装置908以及受保护和未受保护的内容。受保护的内容可由内容保护机制保护(例如加密)。在此情形中,如910处所说明,受保护内容可由能够对内容进行解密的相容内容客户端装置906播放且因此被递送到相容内容客户端装置906。此在910处说明。然而,应注意,在920处此受保护的内容也可被递送到非相容内容客户端装置908。如果(例

如) 非相容内容客户端装置 908 已获取必要的解密能力, 那么其可能能够使用受保护的内容。可(例如)非法地(例如, 装置被黑客入侵或加密密钥被偷窃)或合法地(例如, 如果内容拥有者决定暂时将能力授予非相容客户端装置 908) 获取此能力。

[0144] 返回参看图 9, 在 912 处, 可从相容内容服务器 902 将未受保护的内容递送到执行水印提取和 / 或筛选操作的相容内容客户端装置 906。在 916 处, 也可从非相容内容服务器 904 将未受保护的内容递送到筛选内容的相容内容客户端装置 906。相容内容装置 906 可使用前述合作方法中的一者来有效地筛选未受保护的内容。图 9 还说明在 914 处可从相容内容服务器 902 将未受保护的内容递送到非相容客户端内容装置 908。在此情形中, 相容内容服务器 902 在递送内容之前执行必要的水印提取和筛选。

[0145] 图 9 中描绘的示范性内容递送架构也考虑在 918 处将未受保护的内容(例如, 盗版内容)从非相容内容服务器 904 递送到非相容内容客户端装置 908。如先前所指出, 为了减少未被授权的内容使用的可能性, 可通过向内容用户提供激励来鼓励相容内容客户端装置的扩散。另外, 在 920 处阻止受保护内容到非相容客户端装置 908 的递送(或部分内容的递送)可鼓励用户获取相容装置。根据所揭示的实施例促进此升级, 因为非相容内容客户端装置 908 可仅需要获取筛选能力中的一些或全部。获取这些筛选能力使得装置能够接收受保护内容(例如, 在 920 处)。另外, 通过使用先前描述的合作提取方法, 装置可接收并筛选来自非相容内容服务器 904 的未受保护的内容。

[0146] 如先前所指出, 相容装置(例如, 902 或 906)可能不具有执行对以特定媒体格式编码的内容的水印提取和 / 或筛选所需要的适当编解码器。以下政策中的一者可应用于此情形: 1) 停止内容的传送或使用; 2) 使用调用或委托模型中的一者以进行水印提取和 / 或筛选; 3) 允许内容的有限或无限传送或使用(限制可包含允许此传送或使用的最大次数)。

[0147] 在特别可适用于集中式架构的另一实施例中, 根据所揭示的实施例的合作水印提取可在以下情形中实施: 特殊受信任装置(例如, 图 6 中描绘的“网关”614)协调和控制其它装置来实现内容共享和消耗, 以及水印提取、筛选和数字版权管理。因而, 网关装置可协调水印提取、提取记录的传送、认证操作、受信任装置列表的传送和 / 或获取等。网关装置通常驻留在家庭网络(例如, DLNA 相容网络)内部。在一些实施例中, 网关与各种装置之间的通信被加密。

[0148] 可直接由服务提供者控制的网关装置可负责将水印提取任务指派给家庭网络中的一个或一个以上有能力且受信任装置。举例来说, 网关装置可为被授权以获取和解密受保护内容和 / 或为家庭网络中的此受保护内容服务的唯一装置。网关装置可进一步能够控制相容内容服务器以用于内容递送、暴露、服务和传输。网关装置还可控制相容内容客户端装置以用于内容再现。

[0149] 在另一实例中, 网关装置可另外或替代地负责确定进行各种筛选操作所必要的适当操作配置。网关装置还可引导受信任装置且使受信任装置同步以进行筛选操作。举例来说, 网关可使用调用和委托模型中的一者以实行必要筛选操作。在一些实施例中, 受信任装置认证操作也可由网关装置进行。另外, 网关装置可维持撤销列表且可具有撤销网络内的装置的受信任状态的权限。另外, 网关装置可保持与不同的所嵌入的水印相关联的使用规则。这些使用规则可用以规定各种强制执行动作。这些使用规则也可传送到各种受信任装置。网关装置还可控制筛选且更新政策强制执行的使用规则。

[0150] 在又其它实施例中，网关装置可与驻留在家庭网络外部的一个或一个以上外部装置（例如，另一网关装置、内容服务器装置、内容客户端装置等）通信。在这些实施例中，网关装置可控制家庭网络与外部装置之间的内容流、认证信息和其它信息。

[0151] 根据一些实施例，所有水印提取记录可存储在可由网关存取的中心位置中。水印提取记录可另外在家庭网络的其它装置上被复制。筛选效率的进一步改进可通过水印提取记录的安全和私人交换来实现。交换必须在家庭网络（例如，DLNA 相容网络）内或经由因特网来自云空间的受信任装置之间进行。提取记录的交换可在两个装置的认证期间发生，使得安全性（包含保密性和完整性）得以确保。举例来说，使用 DTCP-IP 的认证协议，任何信息（例如提取记录）可在两个装置之间安全地交换。

[0152] 如果两个装置中的一者不具有提取记录，那么可能需要所述两个装置之间的提取记录的交换。在此情形中，记录可从一个装置复制到另一装置。在另一情形中，记录的交换对于合并和同步两个装置的记录可为必要的。在这些情形中，记录的交换可按以下方式进行。如果由第一装置上的文件名称或散列代码识别的内容项目的提取记录不存在于第二装置上的记录中，那么可将遗失的记录添加到第二装置（且反之亦然）。另一方面，如果用于同一内容项目的记录存在于两个装置上，那么使用具有最后日期和时戳（例如，最后修改日期和时间）的记录以使两个装置的内容同步。

[0153] 当与用户相关联的提取记录保持在云中时，所述提取记录可视为允许或拒绝用户再现内容的中心“虚拟记录”储存库的部分。这些虚拟记录可以若干方式组织。在一个实例实施例中，每一用户在云中具有用于对应于其家庭网络中的内容文件的提取记录的私人虚拟锁具。这种配置的优点为用户可随处存取记录以接收再现其内容的许可。在另一实例实施例中，将来自所有用户（例如，地理区域中的所有用户或服务提供者的所有用户）的所有虚拟记录存储在通用锁具中。提取记录可由散列代码编制索引。因此，仅一个记录需要存储在内容项目的云中，唯一散列代码可从所述内容项目产生。此组织的一个优点为这些记录为匿名的且较不冗余。

[0154] 在一些实施例中，提取记录的仅一部分存储在云中。在一个实例中，仅对应于成功内容存取请求的提取记录存储在云中。在另一实例中，仅对应于不成功内容存取请求的提取记录存储在云中。在其它实施例中，通过使用受信任服务或通过使询问来源模糊来保护用户的隐私。在又其它实施例中，给予某些用户增强的特权以促进提取记录的存取和交换。举例来说，这些特权可被授予不具有不成功内容存取请求记录的用户，而具有不成功内容存取请求历史的用户可能必须接受与额外认证和验证操作相关联的一些延迟。

[0155] 应理解，本发明的各种实施例可个别地或共同地在包括各种硬件和 / 或软件模块和组件的装置中实施。这些装置（例如）可包括处理器、存储器单元、通信地彼此连接的接口，且范围可从桌上型计算机和 / 或膝上型计算机到例如媒体播放器、移动装置等消费型电子装置。举例来说，图 10 说明装置 1000 的框图，各种所揭示的实施例可在装置 1000 内实施。装置 1000 包括：至少一个处理器 1002 和 / 或控制器；至少一个存储器 1004 单元，其与处理器 1002 通信；以及至少一个通信单元 1006，其使得能够通过通信链路 1008 直接或间接地与其它实体、装置和网络交换数据和信息。通信单元 1006 可根据一个或一个以上通信协议提供有线和 / 或无线通信能力，且因此其可包括恰当的发射器 / 接收器天线、电路和端口以及编码 / 解码能力，其对于数据和其它信息的恰当传输和 / 或接收可为必要的。图

10 中描绘的示范性装置 1000 可作为图 1、4 和 5 中描绘的内容处置装置 100、主装置 404、从属装置 412、委托装置 504、受委托装置 510 和 / 或目的地装置 514 的部分而集成到其中。

[0156] 返回参看图 1, 水印提取器 104、数字签名产生器 106、加密组件 108、认证组件 120 等中的任一者可在软件、硬件、固件或其组合中实施。类似地, 每一模块内的各种组件或子组件可在软件、硬件或固件中实施。可使用此项技术中已知的连接方法和媒体中的任一者来提供模块和 / 或模块内的组件之间的连接性, 所述连接方法和媒体包含 (但不限于) 经由因特网、有线或无线网络使用适当协议进行的通信。

[0157] 在方法或过程的一般背景下描述本文中描述的各种实施例, 所述方法或过程可在在一个实施例中由体现在计算机可读媒体中的计算机程序产品实施, 所述计算机程序产品包含由联网环境中的计算机执行的计算机可执行指令 (例如, 程序代码)。计算机可读媒体可包含可装卸和非可装卸存储装置, 其包含 (但不限于) 只读存储器 (ROM)、随机存取存储器 (RAM)、光盘 (CD)、数字多功能光盘 (DVD) 等。因此, 在本申请案中描述的计算机可读媒体包括非暂时性存储媒体。一般来说, 程序模块可包含执行特定任务或实施特定抽象数据类型的例程、程序、对象、组件、数据结构等。计算机可执行指令、相关联的数据结构和程序模块表示本文中揭示的方法的执行步骤的程序代码的实例。这些可执行指令或相关联的数据结构的特定序列表示用于实施这些步骤或过程中描述的功能的对应动作的实例。

[0158] 已出于说明和描述的目的而呈现实施例的以上描述。以上描述无意为详尽的或将本发明的实施例限于所揭示的精确形式, 且鉴于以上教示, 修改和变化为可能的, 且可从各种实施例的实践获取。选择和描述本文中论述的实施例以便解释各种实施例以及其实际应用的原理和本质, 以使得所属领域的技术人员能够在各种实施例中且借助于适于所预期的特定使用的各种修改来利用本发明。本文中描述的实施例的特征可在方法、设备、模块、系统和计算机程序产品的所有可能组合中加以组合。

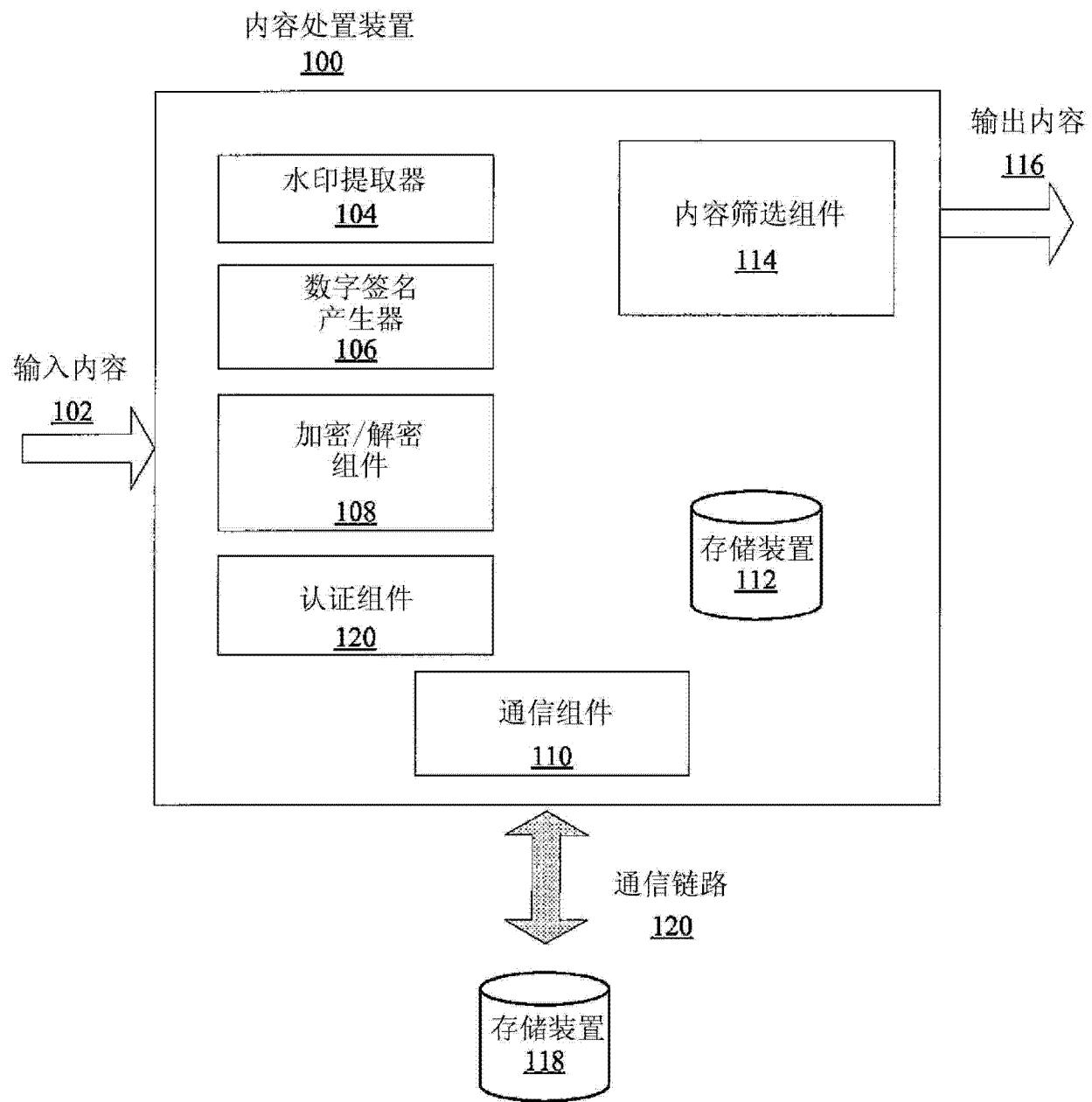


图 1

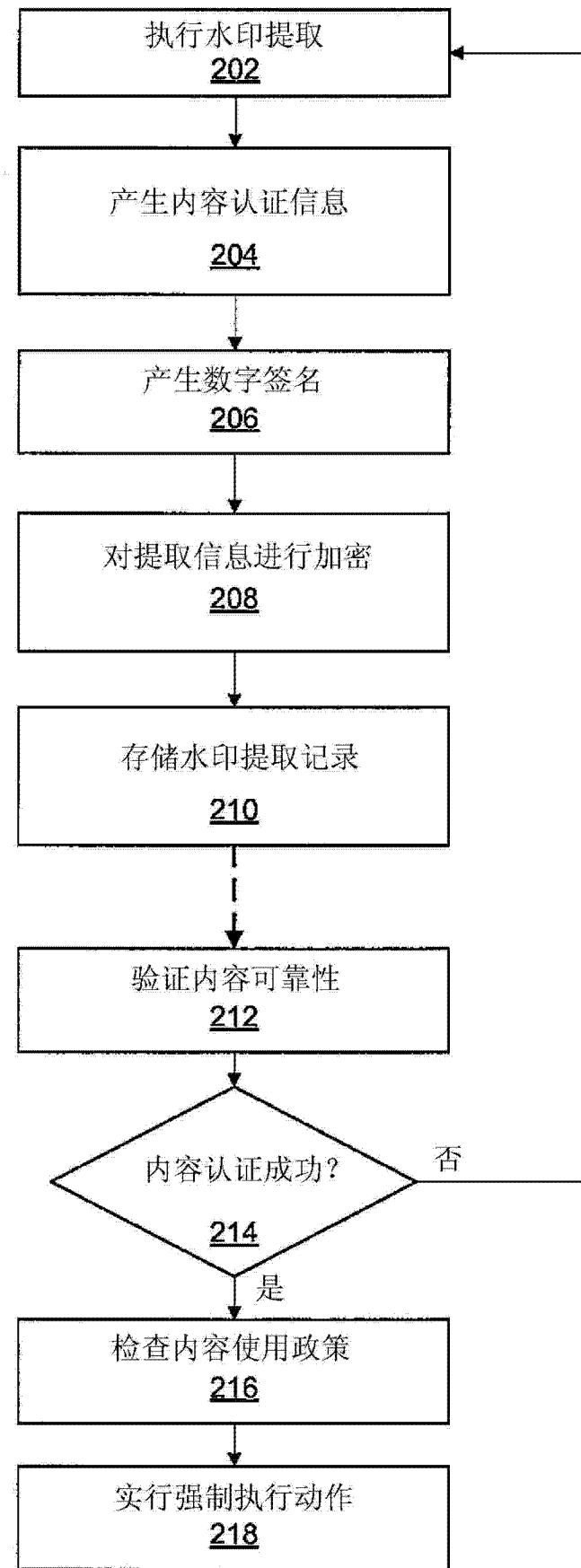


图 2

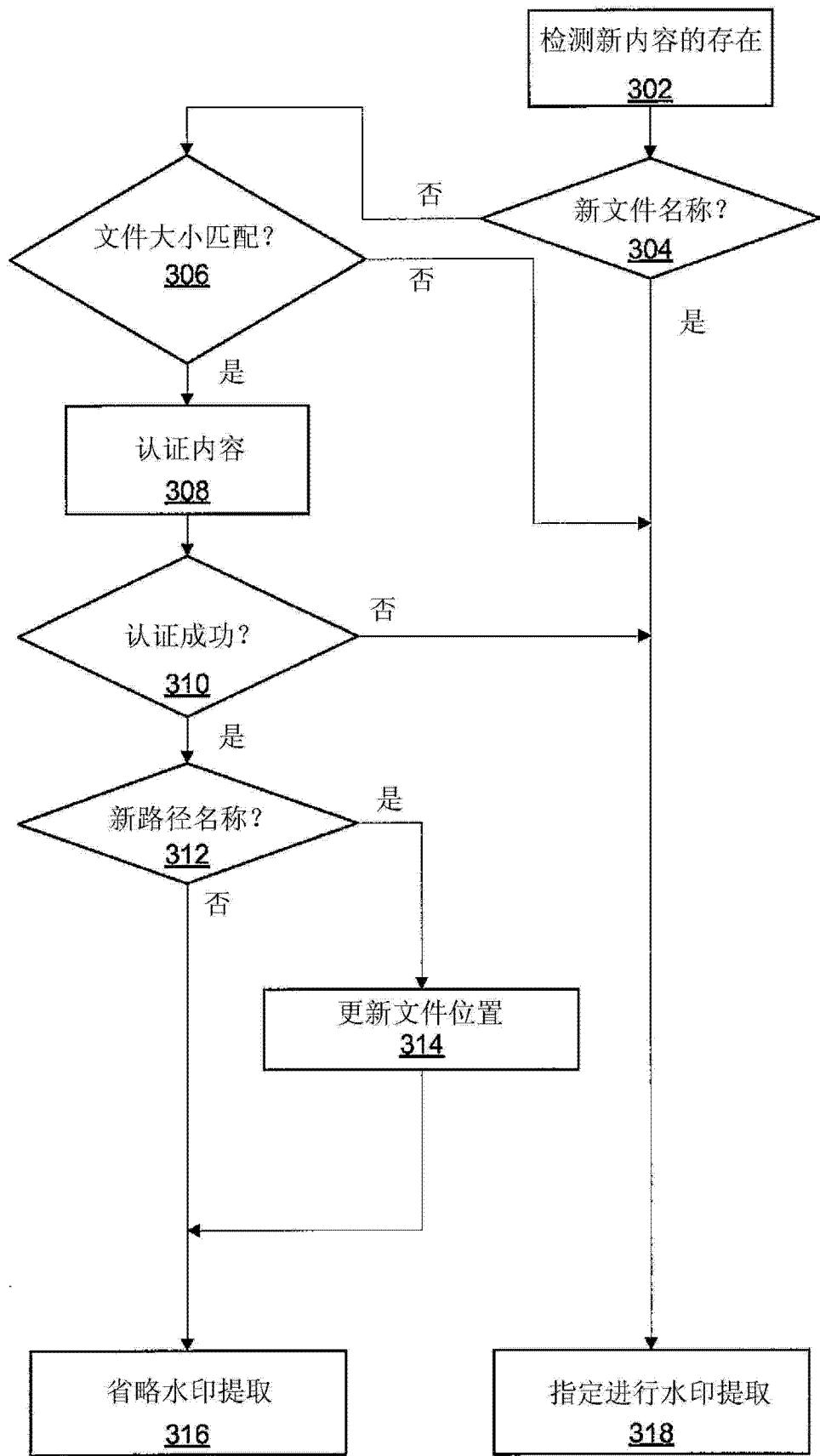


图 3

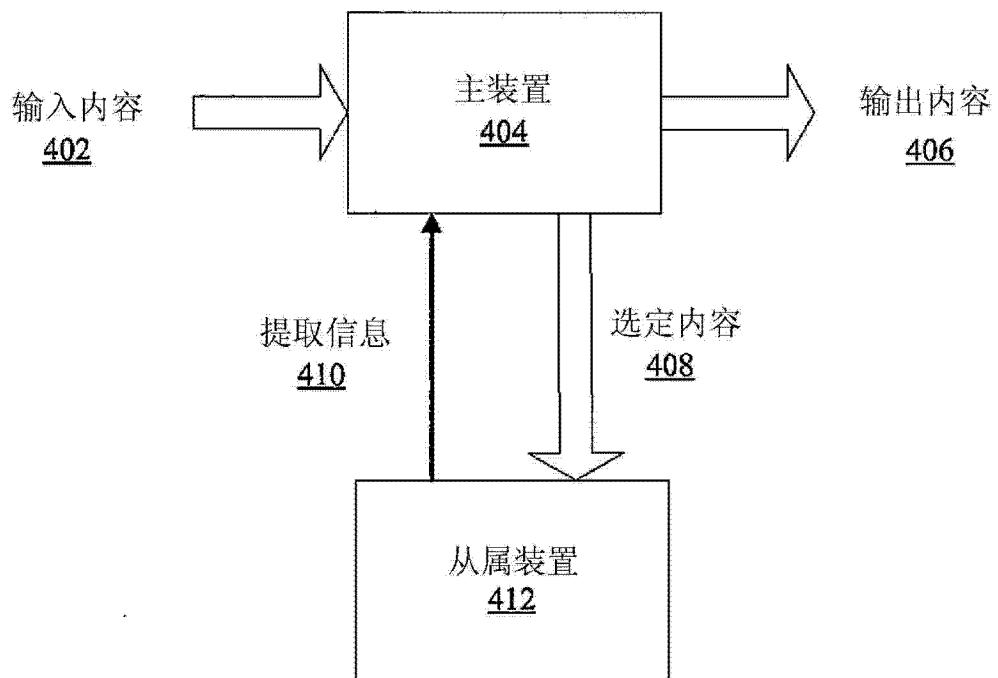


图 4

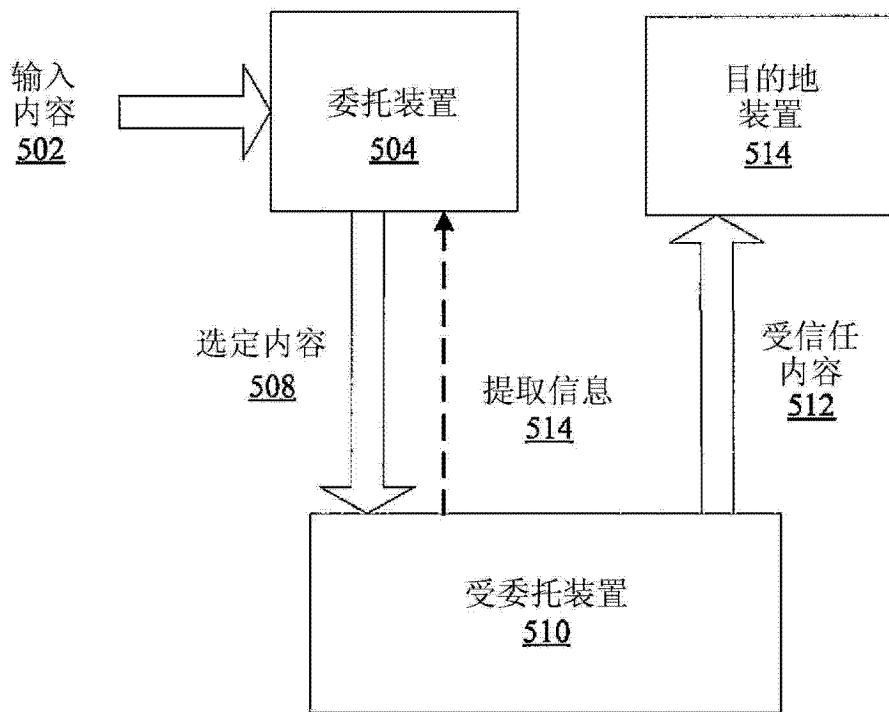


图 5

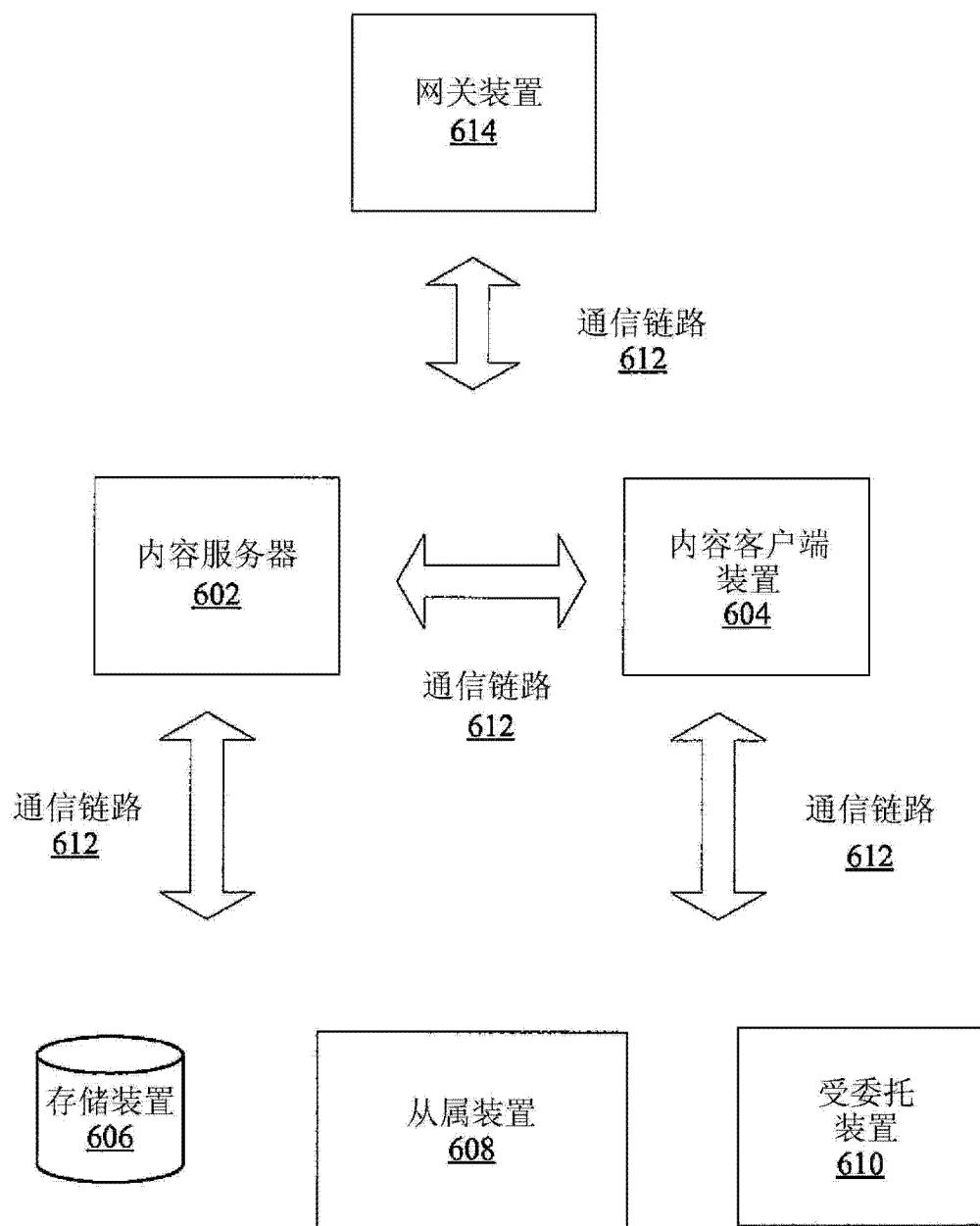


图 6

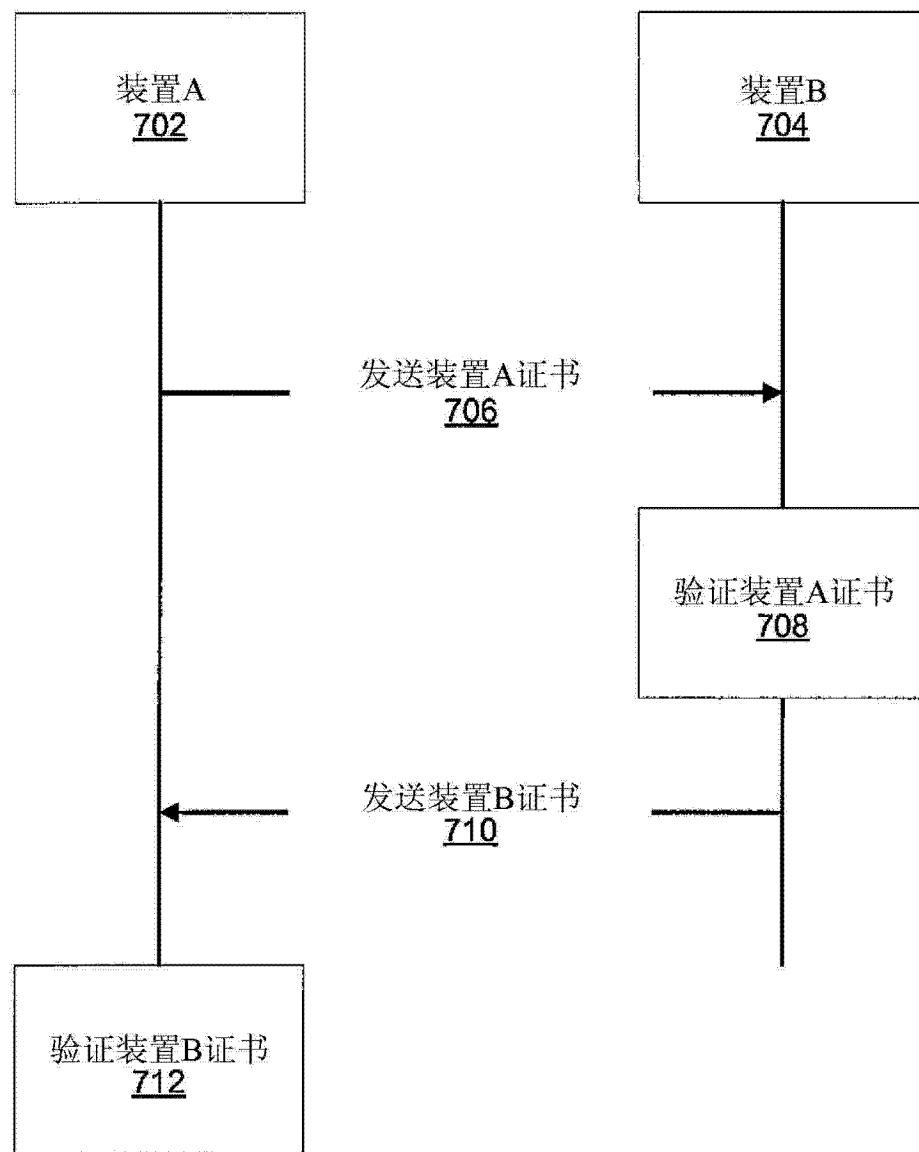


图 7

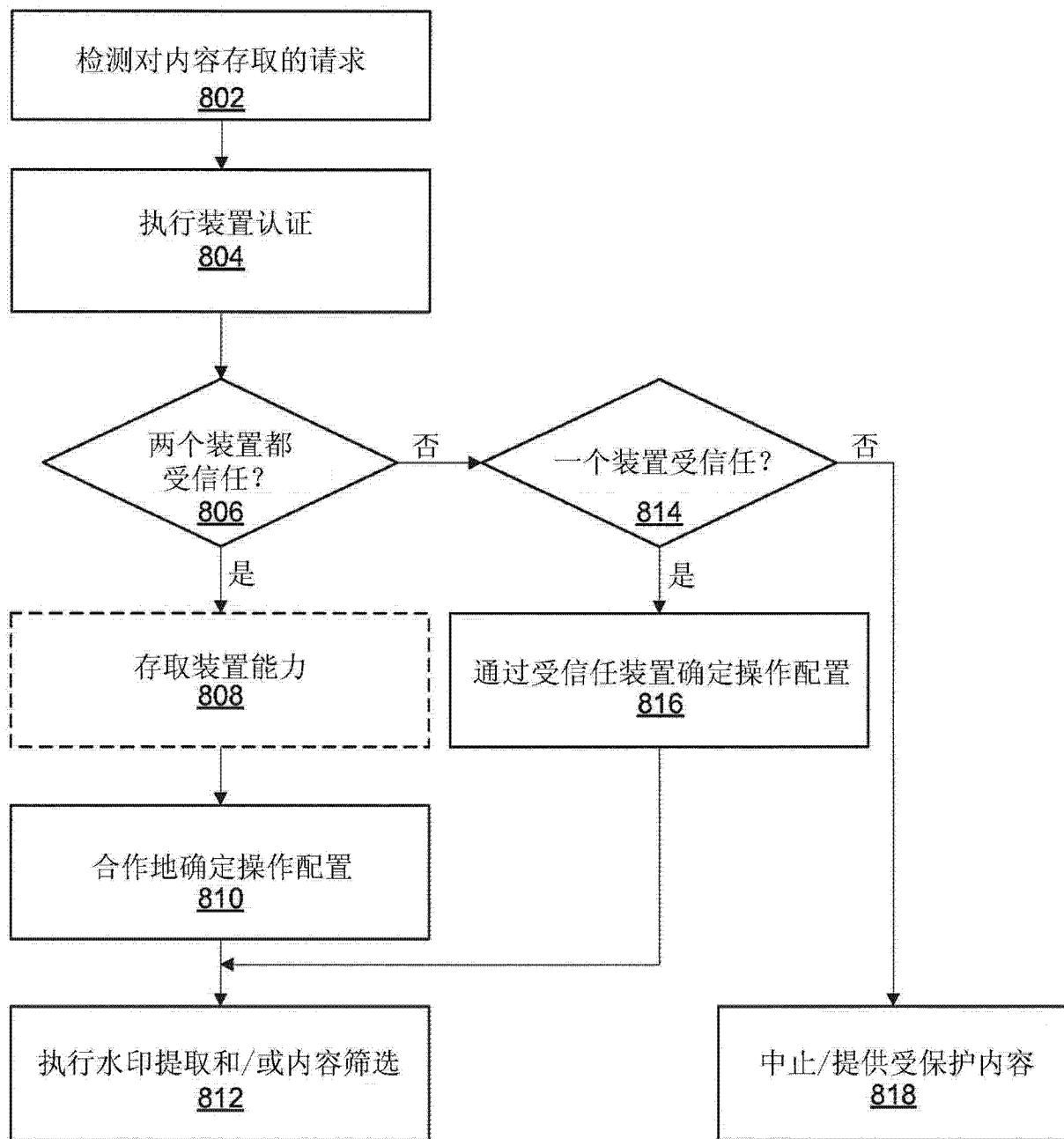


图 8

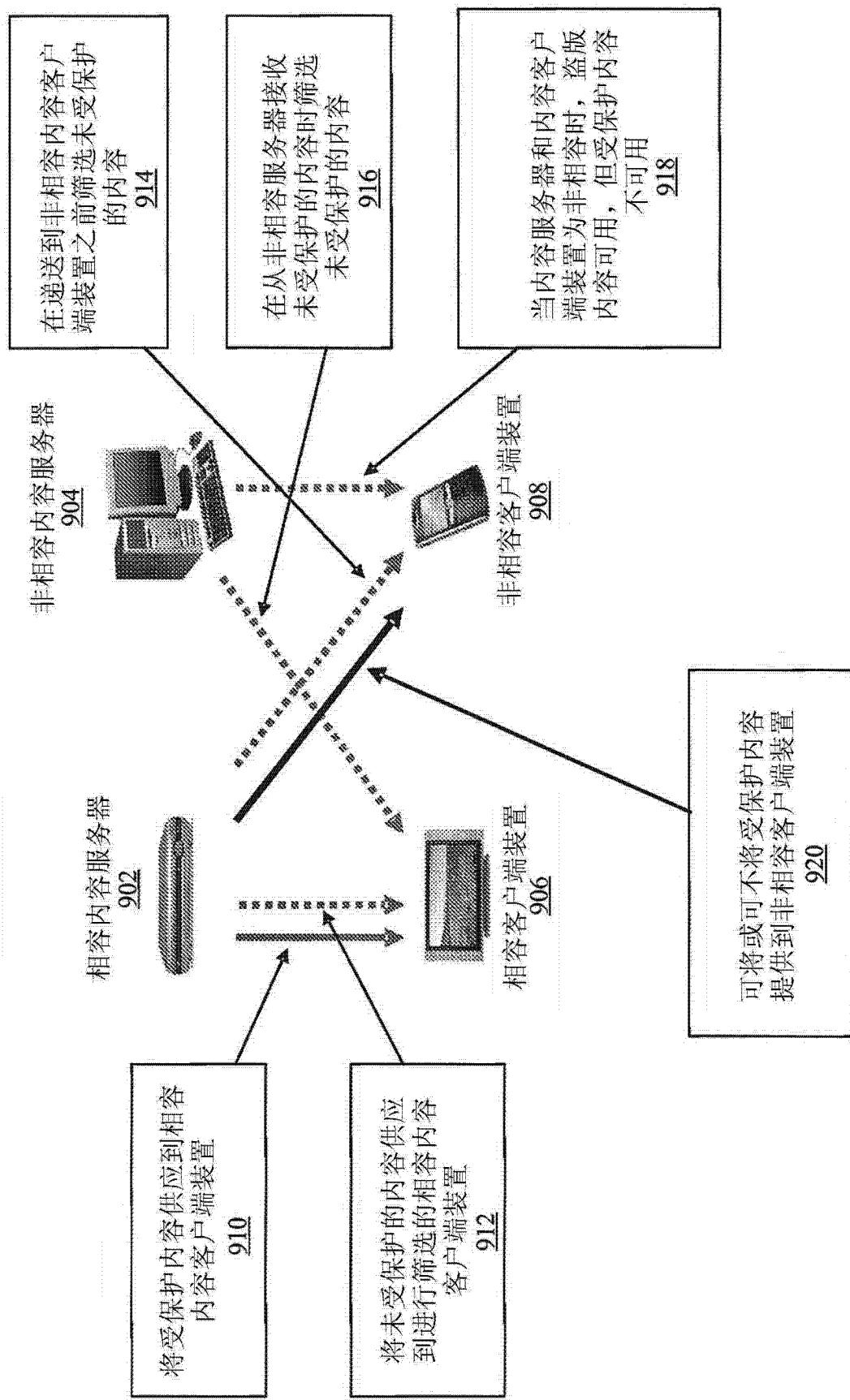


图 9

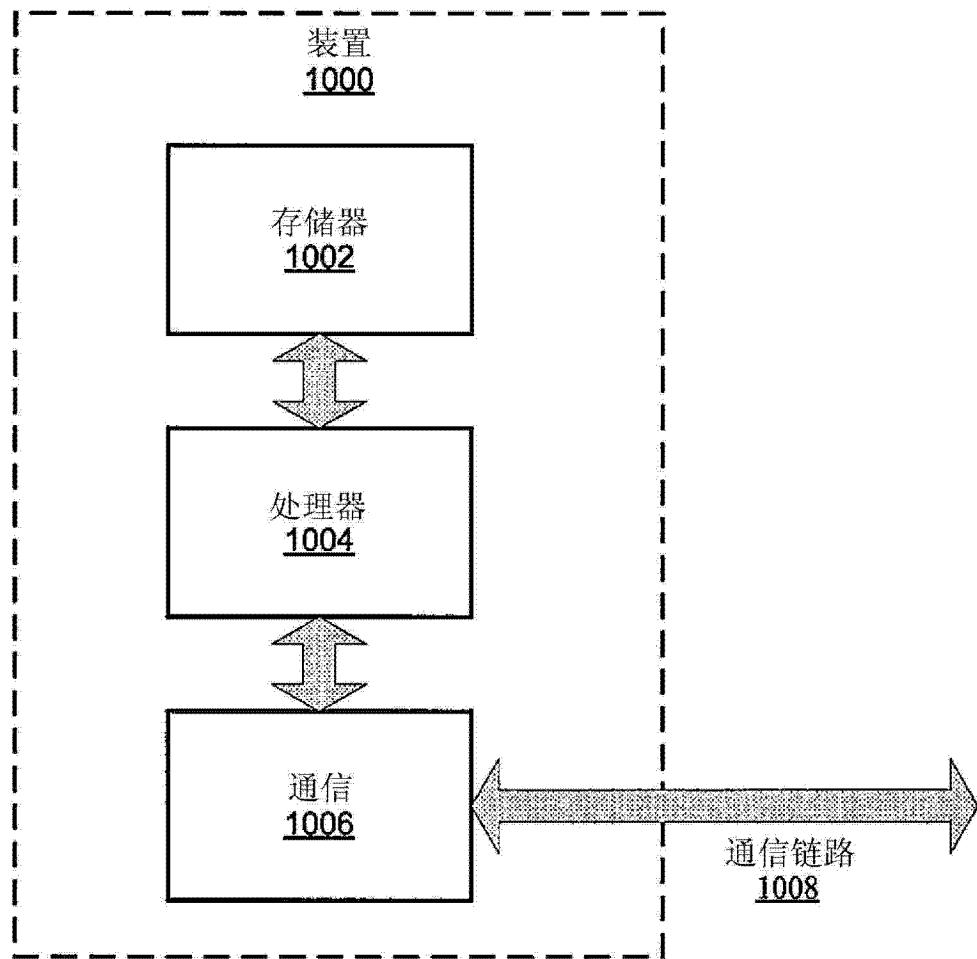


图 10