[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200880009600.7

[43] 公开日 2010 年 2 月 3 日

[11] 公开号 CN 101641701A

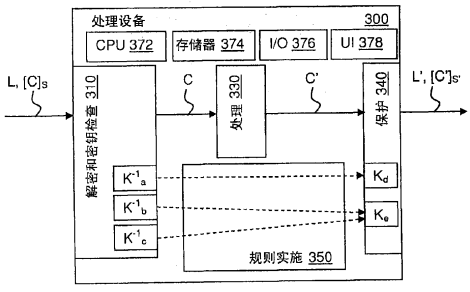
[22] 申请日 2008.3.17
[21] 申请号 200880009600.7
[30] 优先权
[32] 2007. 3.27 [33] EP [31] 07300899.7
[86] 国际申请 PCT/EP2008/053181 2008.3.17
[87] 国际公布 WO2008/116779 英 2008.10.2
[85] 进入国家阶段日期 2009.9.23
[71] 申请人 汤姆森许可贸易公司
地址 法国布洛涅 - 比郎库尔
[72] 发明人 斯特凡纳·奥诺 奥利维耶·赫恩
[74] 专利代理机构 中科专利商标代理有限责任公司
代理人 王波波
权利要求书 3 页 说明书 10 页 附图 4 页

[54] 发明名称

用于对内容进行数字处理管理以实现所施加的工作流的设备和方法

[57] 摘要

本发明提供了一种设备(200、300、600)，接收(402)受保护内容($[C]_S$)和所述内容(C)的许可(L)；使用输入密钥(K_i^{-1})来对所述内容解保护(408、410)；以及检索(404)与所述输入密钥相关联的规则。 然后，所述设备处理(412)所述内容，以创建新内容(C')；检索在检索到的规则中与所述输入密钥相关联的至少一个输出密钥(K_j)；使用所述输出密钥来保护(414、416)内容；以及发送新保护的内容($[C']_{S'}$)和对应的许可(L')。 因此，由于设备存储特定密钥以访问内容所需，并且由于所述规则根据所述输入密钥来施加特定输出密钥，因而可以施加工作流。 在优选实施例中，使用对称密钥(S)来对内容进行加扰，所述对称密钥(S)是由所述许可中的非对称密钥来加密的。 备选实施例使用水印技术来代替加密。 本发明在视频处理中尤其适用。



1. 一种处理内容（C）的方法，包括以下步骤：

- 接收（402、702）受保护的内容（$[C]_S$；L）；

- 使用所存储的解密密钥的集合中的解密密钥（K^{-1}_i）来对所述内容解保护（408、410；714）；

- 对所述内容进行处理（412、716），以获得处理后的内容（C'）；以及

- 使用所存储的加密密钥的集合中的至少一个加密密钥来对所述处理后的内容进行保护（414、416；718、720）；

其特征在于，每个解密密钥与所存储的加密密钥的集合中的至少一个加密密钥相关联；以及

所述方法还包括选择（404）所述至少一个加密密钥的步骤，其中，选择与用于解密的解密密钥相关联的至少一个加密密钥；

其中，如果使用对称加密，则所选的至少一个加密密钥与用于解密的解密密钥不同，而如果使用非对称加密，则所选的至少一个加密密钥不属于相同的密钥对。

2. 如权利要求 1 所述的方法，其中，通过加扰密钥（S）来对接收到的受保护内容进行加扰，所述加扰密钥是使用非对称加密算法来加密的，其中，对所述内容解保护的步骤（408、410）包括以下步骤：

- 使用解密密钥来对加密的加扰密钥（$\{S\}_{Kr}$）进行解密（408）以获得所述加扰密钥；以及

- 使用所述加扰密钥（S）来对加扰的内容（$[C]_S$）进行解扰（410）。

3. 如权利要求 2 所述的方法，其中，对所述处理后的内容（C'）进行保护（414、416）的步骤包括以下步骤：

- 产生（414）新的加扰密钥（S'）；

- 使用所述新的加扰密钥来对所述处理后的内容进行加扰（414）；以及

- 使用具有所述至少一个加密密钥的非对称加密算法来对所述新的加扰密钥进行加密（416）。

4. 如权利要求 3 所述的方法，其中，将加密的加扰密钥结合在与所述受保护的内容相关联的许可（L）中。

5. 如权利要求 4 所述的方法，其中，许可（L）还包括注释。

6. 如权利要求 2 所述的方法，其中，对加密的加扰密钥进行解密的步骤包括：迭代地利用多个解密密钥，直到对加密的加扰密钥进行成功解密为止。

7. 如权利要求 1 所述的方法，其中，通过鲁棒水印来保护接收到的受保护内容，并通过脆弱水印来对加有鲁棒水印的内容加水印，其中，对所述受保护内容解保护（714）的步骤包括以下步骤：

- 去除所述脆弱水印；以及

- 去除（714）所述鲁棒水印。

8. 如之前任一权利要求所述的方法，其中，所述内容是多媒体内容。

9. 一种用于处理受保护内容的设备，包括：

使用所存储的解密密钥的集合中的解密密钥（K^{-1}_i）来对所述受保护内容解保护的装置（220、310）；

用于处理所述内容的装置（230、330）；

使用所存储的加密密钥的集合中的至少一个加密密钥来保护所述内容的装置（240、340）；

用于存储多个输入密钥和输出密钥的装置（374）；

其特征在于，

每个解密密钥与所存储的加密密钥的集合中的至少一个加密密钥相关联；

所述设备包括：通过选择与用于解密的解密密钥相关联的至少一个加密密钥来选择至少一个加密密钥的装置（350）；

其中，如果使用对称加密，则所选的至少一个加密密钥与用于解密的解密密钥不同，而如果使用非对称加密，则所选的至少一个加密密钥不属于相同的密钥对。

10. 如权利要求 9 所述的设备，其中，通过加扰密钥来对接收到的内容进行加扰，所述加扰密钥是使用非对称加密算法来加密的，并

且，用于对所述受保护内容解保护的装置（220、310）适于：

- 使用解密密钥来对加密的加扰密钥进行解密以获得所述加扰密钥；以及

- 使用所述加扰密钥来对加扰的内容进行解扰。

11. 如权利要求 10 所述的设备，还包括用于产生新的加扰密钥的装置（340），并且其中，用于保护所述处理后的内容的装置（240、340）适于：

- 使用所述新的加扰密钥来对所述处理后的内容进行加扰；以及

- 使用具有所述至少一个加密密钥的非对称加密算法来对所述新的加扰密钥进行加密。

12. 如权利要求 10 所述的设备，其中，用于对加密的加扰密钥解保护的装置（220、310）适于：迭代地利用多个解密密钥，直到对加密的加扰密钥进行成功解密为止。

13. 如权利要求 9 所述的设备，其中，通过鲁棒水印来保护接收到的内容，并通过脆弱水印来对加有鲁棒水印的内容加水印，用于对所述受保护内容解保护的装置（220）适于：

- 去除所述脆弱水印，以及

- 去除所述鲁棒水印。

用于对内容进行数字处理管理以实现所施加的工作流的设备和方法

技术领域

本发明总体涉及数字内容保护，更具体地，涉及在处理链中对这种内容的保护。

背景技术

本节意在向读者介绍可能与以下描述和/或要求保护的本发明的各方面相关的领域的各个方面。相信这种讨论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。相应地，应注意，应根据这一点来阅读这些陈述，而不应将其接纳为现有技术。

内容，如多媒体内容——例如影片和音乐——文档、照片等等，通常需要在被发行以供终端用户享用之前进行处理。

例如，从实际录制到发行，影片要经过许多处理步骤：剪样片（de-rushing）、混录、添加数字效果、配音、添加字幕等等。

容易认识到，内容提供者对处理（也称为后处理）系统有两个要求：1）严格和可跟踪的处理操作；以及2）容易传送和复制内容。本领域技术人员可以认识到，现有技术的系统满足一个或另一个要求，但不能同时满足这两个要求。

一般而言，模拟系统满足第一个要求。由于将内容存储在磁带或胶片夹上，因此对处理进行控制相对容易：特定内容保持在特定部门内，直到磁带被发送给下一部门。此外，万一失窃也可以跟踪磁带。另一方面，内容的传送则不那么直接，这是由于这需要发送物理磁带，这原本就较为困难，尤其是在涉及长距离的情况下。也难以将内容一次提供给多于一个实体，这是由于必须对内容进行物理复制。此外，在使用之后擦除和/或销毁内容也可以对用户提供约束。

数字系统提供了内容的简易传送和复制。然而，对内容的处理进行控制则难得多：如果内容驻留于服务器上，则非常难于控制谁可以

访问它，并且，如果一个部门错误地认为先前部门已经完成了内容的处理，则可能经常出现错误。

图 1 示出了可使用本发明的示例处理系统。系统 100 包括字幕添加设备 110、颜色管理设备 120、配音设备 140、数字特效设备 150、存储设备 160 和发射清除设备 130，这些设备均由网络 170 连接。

在图 1 的系统中，例如，可以要求内容在发送至配音 140 以及可选地还发送至字幕添加 110 之前，在经过发射清除 130 之前，经过颜色管理 120 和数字效果 150（不按特定顺序）。由于每个设备都可以访问存储 160，因此难以控制遵照工作流来处理。

在数字版权管理（DRM）系统中，数字系统中的这种困难是固有的。DRM 根据使用限制来控制对内容的访问。对内容进行加密并向终端用户提供单独的许可。

DRM 架构包括内容提供者、内容分发者、许可发布者和内容用户，并具有以下特性：1）他们是都围绕服务器而建立的；2）不允许终端用户根据所获得的内容创建新的内容和许可；以及 3）对内容进行解密的版权是全局的——用户要么拥有该版权，要么没有该版权。

因此，可以认识到，现有技术的 DRM 方案不适于满足以上列出的两个要求。

因此，可以认识到，需要一种实现处理系统的方案，在该处理系统中，可以容易地分发和复制数字内容，同时该处理系统还施加严格的处理操作，该方案被称为数字处理管理（DPM）。

本发明提供了这种方案。

发明内容

在第一方面，本发明涉及一种处理内容的方法。接收受保护的内容，并使用所存储的解密密钥的集合中的解密密钥来对所述受保护的内容解保护。对所述内容进行处理，以获得处理后的内容，使用所存储的加密密钥的集合中的至少一个加密密钥来对所述处理后的内容进行保护。每个解密密钥与所存储的加密密钥的集合中的至少一个加密密钥相关联，所述至少一个加密密钥是通过选择与用于解密的解密密

钥相关联的至少一个加密密钥来选择的。如果使用对称加密，则所选的至少一个加密密钥与用于解密的解密密钥不同，而如果使用非对称加密，则所选的至少一个加密密钥不属于相同的密钥对。

在优选实施例中，使用加扰密钥来对接收到的受保护内容进行加扰，继而使用非对称加密算法来对所述加扰密钥进行加密。通过以下方式对内容解保护：使用所述解密密钥来对加密的加扰密钥进行解密以获得所述加扰密钥，并使用所述加扰密钥来对加扰的内容进行解扰。

优选地，对所述处理后的内容进行保护的步骤包括：产生新的加扰密钥；使用所述新的加扰密钥来对所述处理后的内容进行加扰；以及使用具有所述至少一个加密密钥的非对称加密算法来对所述新的加扰密钥进行加密。有利地，将加密的加扰密钥结合在与所述受保护的内容相关联的许可中，此外，许可还包括注释。

此外，优选地，对加密的加扰密钥进行解密包括：迭代地利用多个解密密钥，直到对加密的加扰密钥进行成功解密为止。

在另一优选实施例中，通过鲁棒水印来保护接收到的受保护内容，并且，通过脆弱水印来对压制了鲁棒水印的内容压制水印。通过去除所述脆弱水印并去除所述鲁棒水印来对所述受保护内容解保护。

所述方法尤其适于多媒体内容。

在第二方面，本发明涉及一种用于处理受保护内容的设备。所述设备包括：使用所存储的解密密钥的集合中的解密密钥来对所述受保护内容解保护的装置；用于处理所述内容的装置；使用所存储的加密密钥的集合中的至少一个加密密钥来保护所述内容的装置；以及用于存储多个输入密钥和输出密钥的装置。每个解密密钥与所存储的加密密钥的集合中的至少一个加密密钥相关联。所述设备还包括：通过选择与用于解密的解密密钥相关联的至少一个加密密钥来选择至少一个加密密钥的装置。如果使用对称加密，则所选的至少一个加密密钥与用于解密的解密密钥不同，而如果使用非对称加密，则所选的至少一个加密密钥不属于相同的密钥对。

在优选实施例中，通过加扰密钥来对接收到的内容进行加扰，所述加扰密钥是使用非对称加密算法来进行加密的，并且，用于对所述

受保护内容解保护的装置适于：使用所述解密密钥来对加密的加扰密钥进行解密以获得所述加扰密钥；以及使用所述加扰密钥对加扰的内容进行解扰。

有利地，所述设备还包括用于产生新的加扰密钥的装置，并且，用于保护所述处理后的内容的装置适于：使用所述新的加扰密钥来对所述处理后的内容进行加扰；以及使用具有所述至少一个加密密钥的非对称加密算法来对所述新的加扰密钥进行加密。

此外，有利地，用于对加密的加扰密钥解保护的装置适于：迭代地利用多个解密密钥，直到对加密的加扰密钥进行成功解密为止。

在另一优选实施例中，通过鲁棒水印来保护接收到的内容，并且，通过脆弱水印来对压制了鲁棒水印的内容压制水印，用于对所述受保护内容解保护的装置适于去除所述脆弱水印以及去除所述鲁棒水印。

附图说明

现在将参照附图，以示例方式描述本发明的优选特征，附图中：

图 1（已描述）示意了可使用本发明的示例处理系统；

图 2 示意了本发明的总体发明思想；

图 3 示意了根据本发明优选实施例的设备；

图 4 示意了根据本发明优选实施例的方法的流程图；

图 5 示意了本发明在示例处理系统中的使用；

图 6 示意了总体发明思想的备选使用；以及

图 7 示意了本发明的备选实施例的流程图。

具体实施方式

图2示意了本发明的总体发明思想。受保护内容205到达处理设备200，处理设备200检查210谁发布了该内容，并且根据发布者或发布者组（在多于一个发布者可能准备了同种内容的情况下）的标识来提取规则（以下进一步讨论）。然后，处理设备200对该内容解保护220，并使用解保护后的内容225来进行处理230，处理230通常产生修改的、无保护的内容235。然后，基于所提取的、对新内容235施加250特定保护

的规则来保护240新内容235，输出新的受保护内容245。然而应注意，该处理不必须修改内容；例如在发射清除期间，该内容可以保持不变。

优选实施例

优选实施例使用密码术来控制过程。每个设备存储用于对输入内容进行解密的多个输入密钥以及用于对输出内容进行重新加密的多个输出密钥。通常，所存储的密钥是系统中使用的所有密钥的子集。

图3示意了实现本发明优选实施例的设备，而图4示意了根据本发明优选实施例的方法。

处理设备300包括至少一个处理器372、至少一个存储器374、可包括单独的输入和输出单元的通信装置376、以及用户接口378。优选地，至少一个处理器372执行以下描述的功能单元所执行的功能。本领域技术人员可以认识到，处理设备300还包括其他硬件和软件单元（例如至少一条数据总线），尽管这些超出了本发明的范围并且为了示意清楚而未在图中示出。

系统中的每个内容与许可相关联，优选地，该许可处于与内容相同的文件中，但是，也可以将内容和关联的许可存储在互相关联的两个不同文件中。许可L可以被写为$\{S, 注释\}_{Ki}$，其中优选地，S是用于对内容进行加扰的对称密钥，“注释”是数字信息，例如时间戳和由一个或多个用户输入的名称，$\{\}_{Ki}$表示括号内的数据是使用非对称密钥K_i、通过非对称加密算法（如RSA）来加密的。注释也可以包括DRM版权，例如以版权表述语言（RSL）表述的DRM版权。可以认识到，本发明实现了这种数据沿着处理工作流的完整性。

此外，与加密密钥K_i相对应的解密密钥表示为$K^{-1}{}_i$。

优选地，规则包括一种处理设备、输入解密密钥$K^{-1}{}_i$和对应的输出加密密钥K_i，其中该规则是针对该处理设备而计划的。针对该处理设备，规则声明了使用输入密钥解密后的内容应当使用由规则给定的输出加密密钥来加密。应注意，可以使用具有一个输入解密密钥的规则，该解密密钥与多于一个输出加密密钥相关联。例如，如果来自特定源的内容应当以多于一个拷贝输出，或者如果要向处理设备的操作

者给出输出加密密钥的选择，则可能出现这种情况。尤其是如果在系统中同时使用后面的这些情况，则将操作者包括在规则中以通知设备是否要使用多个输出和/或操作者选择是有利的。

处理设备300接收402数据$L[C]_S$，该数据包括：使用加扰密钥S加扰后（由方括号表示）的内容$L[C]_S$，加扰密钥S优选是对称的；以及许可L，包括加扰密钥S和可能的一个或多个注释，该许可是使用具有密钥K_i的非对称加密算法来加密的。应注意，可以将数据发送至处理设备300以及由处理设备300请求数据。

在接收到数据$L[C]_S$后，解密和密钥检查模块310在存储器372中存储的多个规则当中选择404规则。

如图所示，处理设备300包括3个规则，针对这3个规则，在解密和处理模块310中指示了输入解密密钥$K^{-1}{}_a$、$K^{-1}{}_b$和$K^{-1}{}_c$，在保护模块340中指示了输出加密密钥K_d和K_e，并且，规则实施模块350验证实施了规则。在该示例中，第一规则R1具有$K^{-1}{}_a$作为输入解密密钥，具有K_d作为输出加密密钥，规则R2具有密钥$K^{-1}{}_b$和K_e，规则R3具有密钥$K^{-1}{}_c$和K_e。应注意，R2和R3具有不同的输入解密密钥和相同的输出加密密钥。优选地，策略服务器（未示出）在系统中分发规则，以确保创建一个或多个处理链。

如果没有这种规则可用，或者如果已经尝试了所存储的所有规则（“不正确”），则该方法止于步骤406“结束”。然而，如果解密和密钥检查模块310成功选择了规则（“正确”），则方法在步骤408继续，在步骤408中，用该规则的解密密钥$K^{-1}{}_i$来解密L。

解密和密钥检查模块310可以验证解密是否成功，例如通过在许可中的预定地方包括标准公开值（如“deadbeef”）；如果找到该值，则该许可被成功解密。在解密不成功的情况下（“不正确”），方法回到步骤404，在步骤404中，选择另一个（优选地是下一个）规则。

另一方面，如果解密成功（“正确”），则解密和密钥检查模块310在其中提取加扰密钥S和任何注释，并使用加扰密钥S来对加扰后的内容$[C]_S$进行解扰410。

一旦解扰了内容C，就将其转发至处理模块330，以进行处理412

并可能添加和/或删除注释。然后，处理模块330将正常修改的内容C'转发至保护模块340，保护模块340首先用新的加扰密钥S'来对修改的内容C'进行加扰414，然后通过使用由规则实施模块根据对许可进行成功解密的所选规则而施加的密钥对新的加扰密钥S'和任何注释进行加密，来创建416新许可L'。然后，例如，将新数据（包括许可L'和内容$[C']_{S'}$）直接发送至另一设备以进一步处理，或发送至外部存储单元。

尽管以上实施例描述了使用非对称密钥来保护许可，但是本领域技术人员可以认识到，也可以使用对称密钥来达到该目的，尽管这种使用某种程度上减低了系统的安全性。

图5示意了本发明在示例网络500中的使用，示例网络500包括由局域网550连接的导入设备510、数字特效设备520、颜色管理设备530和导出设备540。

导入设备510导入内容，在本示例中，该内容是无保护的（由"无密钥"示意），导入设备510对该内容进行加扰并使用密钥K_0来创建许可。然后，数字特效设备520和颜色管理设备530可以使用该内容，但是导出设备540不可以，这是由于后者不具有必需的输入解密密钥。

数字特效设备520可以使用密钥K^{-1}_0来访问来自导入设备510的内容，在这种情况下，使用密钥K_1来加密并输出该内容以由颜色管理设备530使用，但是不由导出设备540使用。数字特效设备520也可以使用密钥K^{-1}_2来访问来自颜色管理设备530的内容，在这种情况下，使用密钥K_3来加密并输出该内容以由导出设备540使用，但是不由颜色管理设备530使用。

类似地，颜色管理设备530可以使用密钥K^{-1}_0来访问来自导入设备510的内容，在这种情况下，使用密钥K_2来加密并输出该内容以由数字特效设备520使用，但是不由导出设备540使用。颜色管理设备530也可以使用密钥K^{-1}_1来访问来自数字特效设备520的内容，在这种情况下，使用密钥K_3来加密并输出该内容以由导出设备540使用，但是不由颜色管理设备530使用。

导出设备540可以使用密钥K^{-1}_3来使用来自数字特效设备520或颜色管理设备530的内容，假定该内容是使用密钥K_3来加密的。然后，

导出设备540导出该内容，在该示例中该内容未加密，如图中“无密钥”所示。

因此，可以认识到，本发明在示例系统中实施工作流。由导入设备510引入系统的内容在可以由导出设备540导出之前，必须经过数字特效设备520和颜色管理设备530（尽管在本例中顺序是无关的）。

尽管优选实施例描述了视频处理，但是可以认识到，本发明也可以应用至其他环境，在这些环境中施加严格的工作流是重要的或合乎需要的，如编程中（其中可以对不同文件进行保护）、针对印刷媒体（其中例如可以对不同文章和图片进行保护）、或针对文档（应当以特定顺序对其进行修改和/或附上数字签名）。

图6示意了本发明的备选使用。邮件处理设备600包括至少一个处理器672、至少一个存储器674、可包括单独的输入和输出单元的通信装置676，以及优选地包括用户接口678。

邮件处理设备600适于执行一种“离开办公室（Out of Office）”功能，即，自动传送输入的邮件。尽管用加密的输入邮件示出了示例实施例，但是应理解，该示例实施例也可以与非加密的输入邮件一起使用（在这种情况下，输入解密密钥可以被认为是0，即，解密输出等于输入）。

在邮件处理器中，规则R规定，来自特定发送方的邮件要使用特定输入解密密钥来解密、要使用特定输出加密密钥来加密、并要发送至由规则提供的目的地。应注意，可以使一个输入消息产生多个加密输出消息，每个输出消息以特定目的地为目的地（在图中通过使输入密钥K^{-1}_C与输出密钥K_e和K_f相关联来示意）。

因此，可以认识到，本发明也可以用于电子邮件的安全自动传送。

备选实施例

优选实施例采用了密码术，而备选实施例采用水印。

该实施例使用鲁棒水印来实现可跟踪性和机密性，并将确保完整性的脆弱水印与鲁棒水印一起使用。应注意，本发明可以采用任何处于技术发展水平的鲁棒和脆弱水印算法。

在备选实施例中，在处理系统中给出恒定消息。例如，鲁棒水印可以使用“dead”而脆弱水印可以使用“beef”。因此，使用密钥K的内容C的鲁棒水印可以表示为$\{C, dead\}_K$。脆弱水印表示为{C, beef}。许可内容L可以表示为$\{\{C, dead\}_K, beef\}$，即，根据公知的良好习惯做法，将脆弱水印插入已用鲁棒水印压制上水印的内容中。

图7示意了根据备选实施例的内容处理的流程图。

在步骤702，处理设备接收许可内容L。在步骤704，通过验证等式{L}=beef来搜索脆弱水印。在步骤706，迭代地使用设备中存储的规则来搜索鲁棒水印，每个规则包括输入密钥K_i和输出密钥K_j。这是通过验证等式$\{\{C, dead\}K_a\}K_i=dead$来完成的，其中$K_a$是用于插入鲁棒水印的密钥，$K_i$是当前规则的输入密钥。

在步骤708，检查找到了何种水印（如果有水印）。如果未找到水印，则方法在步骤710结束。如果找到了两种水印之一，但是找不到另一种水印，则在步骤712报告错误。最后，如果鲁棒水印和脆弱水印均被找到，则方法继续在步骤714去除鲁棒水印以产生无保护的内容C。

由于脆弱水印被设计为一旦内容被修改该脆弱水印即被销毁，因此不需要具体去除该水印。

一旦获得了无保护内容C，则可以在步骤716对其进行修改以获得新内容C’。在处理之后，使用根据规则与正确输入密钥相对应的输出密钥，将新的鲁棒水印添加至新内容C’。然后，在步骤720，将脆弱水印添加至压制了鲁棒水印的内容，以创建新的许可内容L’，在步骤722发送新许可内容L’。

本领域技术人员可以认识到，可以例如通过在数字环境中使用优选实施例的密码术方案，当内容“变为模拟”时使用备选实施例的水印方案，然后当内容重新进入该数字环境或另一数字环境时再回到密码术方案，来对本发明的实施例进行组合。

本领域技术人员也可以认识到，可以同时且针对相同内容既使用密码术方案又使用水印方案。这需要对保护进行成功的双重验证以能够访问该内容。

因此可以认识到，该方法提供了对内容进行保护并施加严格工作

流的一种备选方式。

可以认识到，本发明实现了严格工作流的实施，例如用于处理视频内容，还实现了这种内容的保护。

应理解，完全通过示例描述了本发明。可以独立地或以任何合适组合来提供说明书以及（在合适时）权利要求和附图中公开的每个特征。被描述为以硬件实现的特征也可以以软件实现，反之亦然。在适用时，连接可以被实现为无线连接或有线（不必是直接的或专用的）连接。

权利要求中出现的参考标记仅作为示意，不应对权利要求的范围起限制作用。

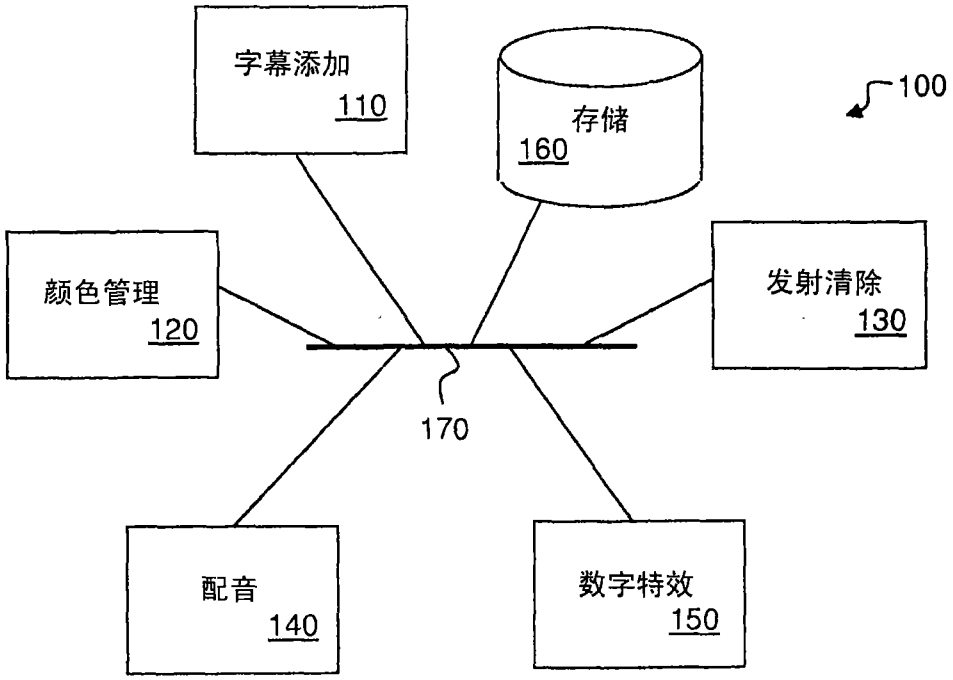

字幕添加
110
存储
160
100
颜色管理
120
发射清除
130
170
配音
140
数字特效
150

图 1

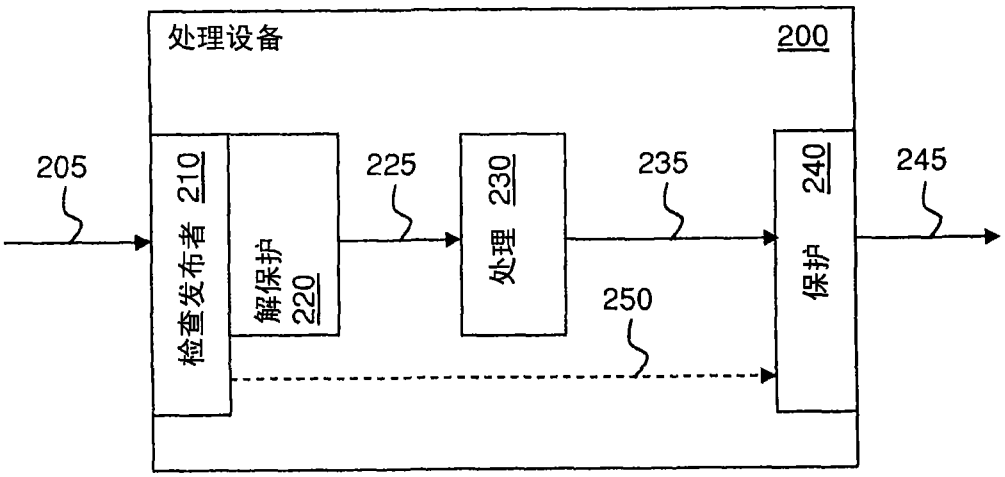

处理设备
200
205
检查发布者 210
解保护 220
225
处理 230
235
保护 240
245
250

图 2

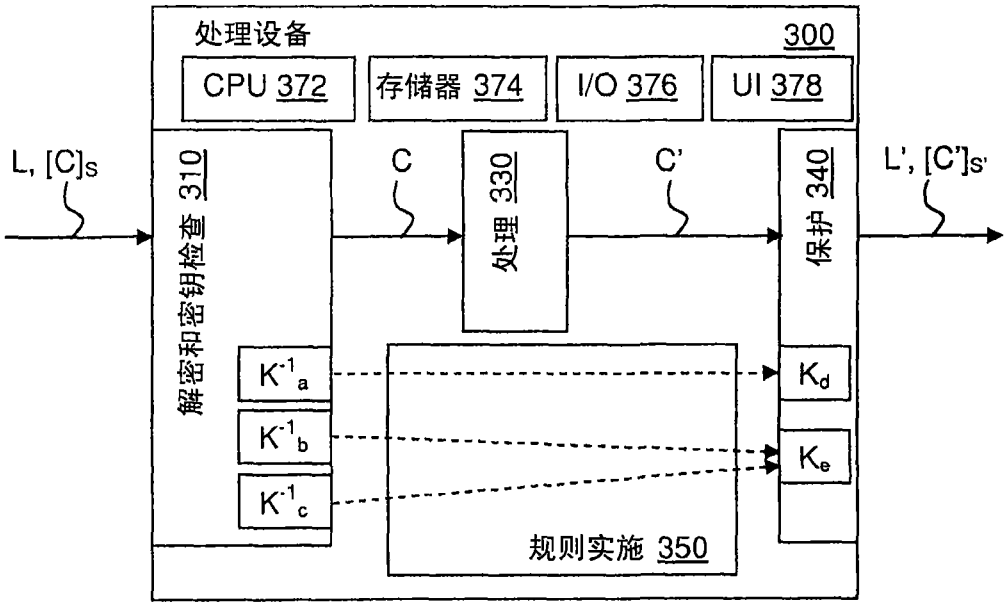

处理设备
300
CPU 372
存储器 374
I/O 376
UI 378
L, [C]S
解密和密钥检查 310
C
处理 330
C'
保护 340
L', [C']S'
K-1a
K-1b
K-1c
Kd
Ke
规则实施 350

图 3

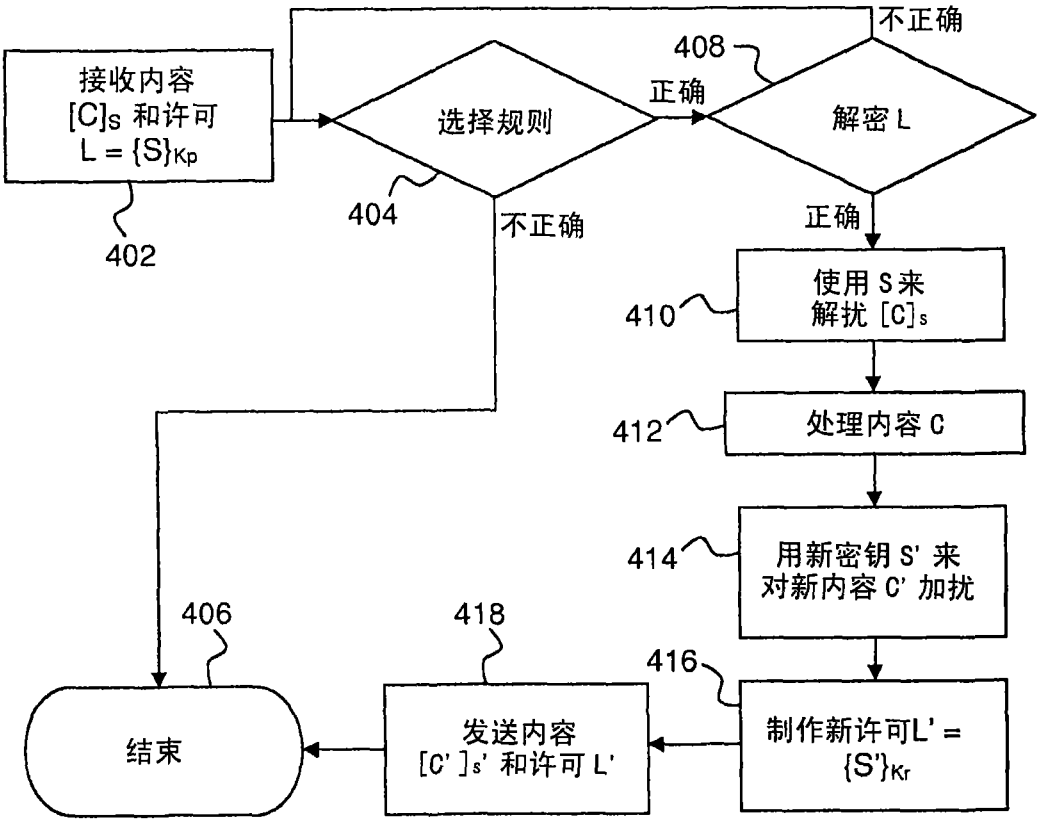

接收内容
[C]S 和许可
L = {S}Kp
402
选择规则
404
不正确
正确
解密 L
408
不正确
正确
使用 S 来
解扰 [C]S
410
处理内容 C
412
用新密钥 S' 来
对新内容 C' 加扰
414
制作新许可L' =
{S'}Kr
416
发送内容
[C']S' 和许可 L'
418
结束
406

图 4

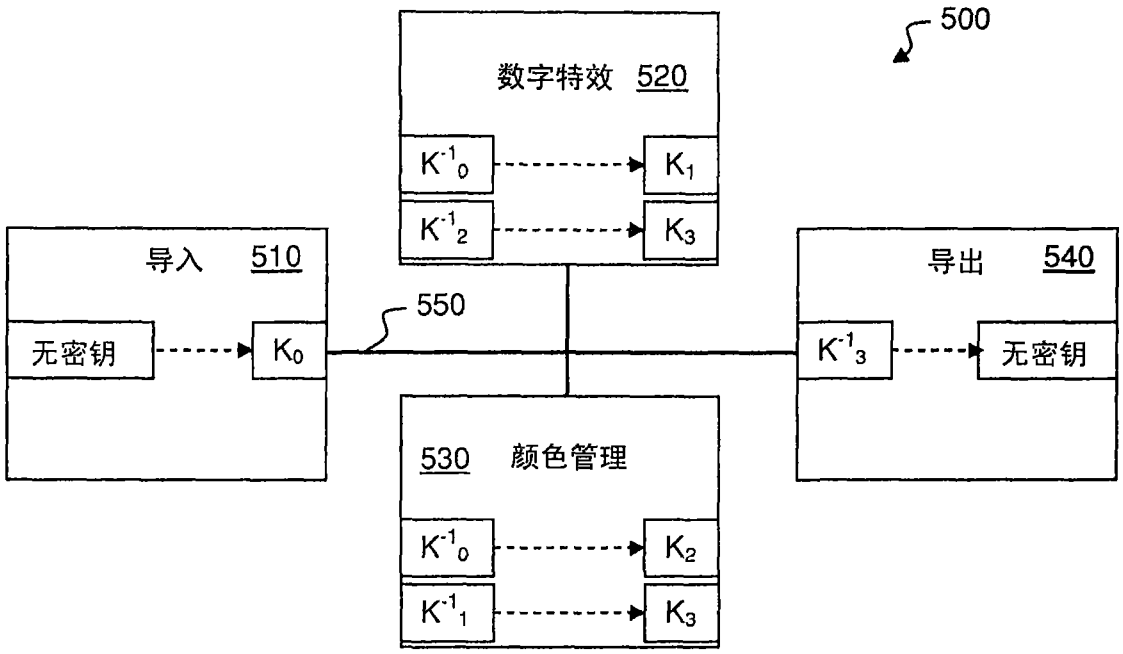

500
数字特效 520
K^{-1}_0
K_1
K^{-1}_2
K_3
导入 510
无密钥
K_0
550
导出 540
K^{-1}_3
无密钥
530 颜色管理
K^{-1}_0
K_2
K^{-1}_1
K_3

图 5

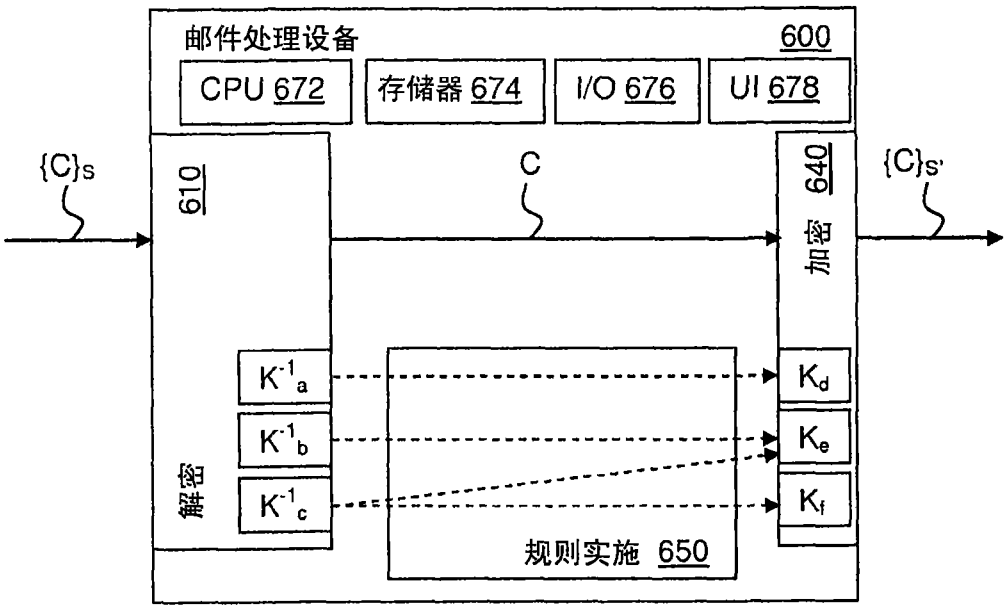

邮件处理设备
600
CPU 672
存储器 674
I/O 676
UI 678
{C}s
610
C
640
加密
{C}s'
K^{-1}_a
K^{-1}_b
K^{-1}_c
解密
K_d
K_e
K_f
规则实施 650

图 6

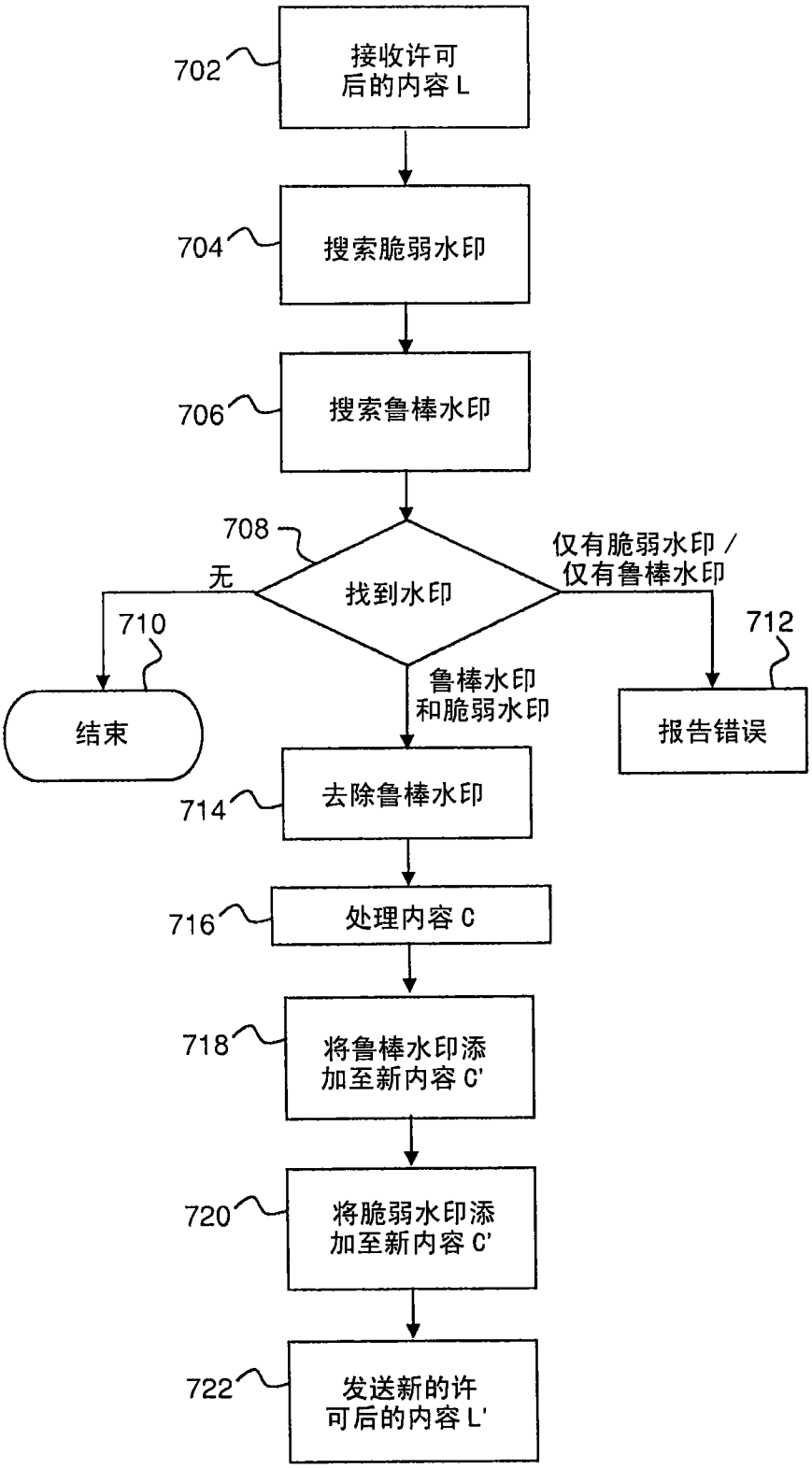

702
接收许可后的内容 L
704
搜索脆弱水印
706
搜索鲁棒水印
708
找到水印
无
仅有脆弱水印 / 仅有鲁棒水印
710
结束
712
报告错误
鲁棒水印和脆弱水印
714
去除鲁棒水印
716
处理内容 C
718
将鲁棒水印添加至新内容 C'
720
将脆弱水印添加至新内容 C'
722
发送新的许可后的内容 L'

图 7