

(12) 发明专利申请

(10) 申请公布号 CN 102073826 A

(43) 申请公布日 2011. 05. 25

(21) 申请号 201010263337. 3

(22) 申请日 2010. 08. 25

(30) 优先权数据

12/548, 228 2009. 08. 26 US

(71) 申请人 奥多比公司

地址 美国加利福尼亚州

(72) 发明人 V·斯瓦米纳桑 S·阿格拉瓦尔

(74) 专利代理机构 北京市金杜律师事务所

11256

代理人 王茂华

(51) Int. Cl.

G06F 21/24 (2006. 01)

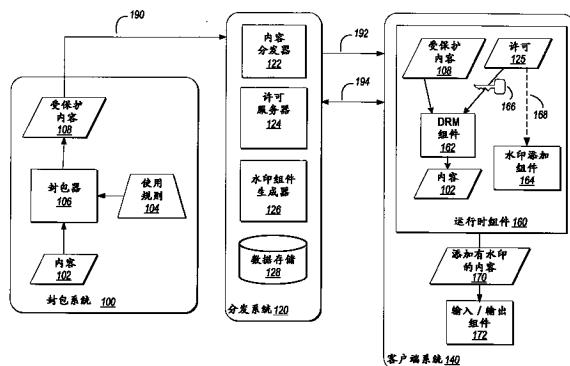
权利要求书 5 页 说明书 15 页 附图 6 页

(54) 发明名称

利用轻量级数字水印添加组件的数字版权管理的系统和方法

(57) 摘要

本发明涉及利用轻量级数字水印添加组件进行数字版权管理的系统和方法。实施方式可以包括方法以及用于执行此类方法的元件。此类方法可以包括将内容接收到计算机系统上；计算机系统可以包括配置用于使用内容的运行时组件。该方法可以包括在计算机系统上接收数字水印添加组件。数字水印添加组件可以指定用于在内容上生成数字水印的信息。该方法可以包括利用运行时组件对内容应用数字水印，以生成添加有水印的内容。数字水印可以由运行时组件根据数字水印添加组件来应用。在各种实施方式中，接收的运行时组件可以配置用于阻止在未对接收的内容应用数字水印的情况下使用接收的内容。



1. 一种计算机实现的方法，包括：

接收内容到计算机系统的存储器中，所述计算机系统包括配置用于使用所述内容的运行时组件；

接收数字水印添加组件到所述计算机系统的存储器中，其中所述数字水印添加组件与所述运行时组件独立地接收，其中所述数字水印添加组件指定用于在所述接收的内容上生成数字水印的信息；以及

使用所述运行时组件对所述接收的内容应用数字水印，以生成添加有水印的内容，其中所述数字水印由所述运行时组件根据所述数字水印添加组件来应用；

其中所述运行时组件配置用于阻止在未对所述接收的内容应用所述数字水印的情况下使用所述接收的内容。

2. 根据权利要求 1 所述的计算机实现的方法，进一步包括：

响应于确定所述数字水印添加组件已撤销，利用第二数字水印添加组件来替换所述计算机系统上的数字水印添加组件，所述第二数字水印添加组件指定用于对所述接收的内容应用数字水印的信息。

3. 根据权利要求 2 所述的计算机实现的方法，其中替换所述数字水印添加组件在无需替换所述运行时组件的情况下执行。

4. 根据权利要求 1 所述的计算机实现的方法，其中对所述接收的内容应用的所述数字水印指示以下一个或多个：

标识被授权使用受保护内容的用户的信息，标识所述计算机系统的信息，标识公布所述接收的内容的公布者的信息，以及标识所述运行时组件的信息。

5. 根据权利要求 1 所述的计算机实现的方法，其中所述接收的内容是视频内容，其中应用所述数字水印，从而在所述视频内容的一个或多个帧上叠加所述数字水印。

6. 根据权利要求 1 所述的计算机实现的方法，进一步包括：

在生成所述添加有水印的内容之前，利用来自所述数字水印添加组件的内容密钥来解密所述接收的内容的至少一部分。

7. 根据权利要求 1 所述的计算机实现的方法，其中接收所述数字水印添加组件包括接收针对所述接收的内容的许可，所述内容许可包括所述数字水印添加组件。

8. 根据权利要求 1 所述的计算机实现的方法，其中所述水印添加组件包括用于应用所述数字水印的可执行指令，其中应用所述数字水印包括执行所述水印添加组件的所述指令。

9. 根据权利要求 8 所述的计算机实现的方法，其中所述运行时组件配置用于实现虚拟机，其中至少一些所述可执行指令以字节码表示，其中应用所述数字水印包括在所述虚拟机上执行所述字节码。

10. 一种计算机实现的方法，包括：

向远程计算机系统提供数字水印添加组件，所述远程计算机系统包括配置用于使用内容部分的运行时组件，所述数字水印添加组件与所述运行时组件独立地向所述远程计算机系统提供，所述数字水印添加组件指定用于在所述内容部分上应用数字水印的信息；以及

向所述远程计算机系统提供信息，所述信息指定在未对所述接收的内容应用所述数字水印的情况下，不能在所述远程计算机系统上使用所述内容部分。

11. 根据权利要求 10 所述的计算机实现的方法,其中所述方法包括 :

在无需撤销所述运行时组件的情况下,撤销所述数字水印添加组件;

在所述撤销之后,向所述远程计算机系统提供不同于所述运行时组件的第二数字水印添加组件,所述第二数字水印添加组件指定用于在所述内容部分上应用数字水印的信息。

12. 根据权利要求 11 所述的计算机实现的方法,其中撤销所述数字水印添加组件包括 :

在已撤销水印添加组件的列表中创建与所述数字水印添加组件相对应的记录,所述列表对于特定计算机系统是可访问的。

13. 根据权利要求 10 所述的计算机实现的方法,其中所述数字水印指示以下一个或多个:

标识被授权使用受保护内容的用户的信息,标识所述计算机系统的信息,标识发布所述受保护内容的发布者的信息,以及标识所述运行时组件的信息。

14. 根据权利要求 10 所述的计算机实现的方法,其中向所述计算机系统提供数字水印添加组件包括 :

向所述远程计算机系统提供针对所述内容部分的内容许可,所述内容许可包括所述数字水印添加组件。

15. 根据权利要求 10 所述的计算机实现的方法,其中向所述远程计算机系统提供指定在未对所述接收的内容应用所述数字水印的情况下,不能在所述远程计算机系统上使用所述内容部分的信息包括 :

向所述远程计算机系统提供针对所述内容部分的内容许可,所述内容许可包括指定在未对所述接收的内容应用所述数字水印的情况下,不能在所述远程计算机系统上使用所述内容部分的信息。

16. 一种系统,包括 :

存储器;以及

耦合至所述存储器的一个或多个处理器,其中所述存储器包括可由所述一个或多个处理器执行的程序指令,用以 :

接收内容;

提供配置用于使用所述内容的运行时组件;

接收数字水印添加组件,其中所述数字水印添加组件与所述运行时组件独立地接收,其中所述数字水印添加组件指定用于在接收的内容上生成数字水印的信息;以及

其中所述运行时组件配置用于对所述接收的内容应用数字水印以生成添加有水印的内容,其中所述运行时组件配置用于根据所述数字水印添加组件来应用所述数字水印,其中所述运行时组件配置用于阻止在未对所述接收的内容应用所述数字水印的情况下使用所述接收的内容。

17. 根据权利要求 16 所述的系统,其中所述程序指令配置用于 :

响应于确定所述数字水印添加组件已经撤销,利用第二数字水印添加组件来替换所述系统的数字水印添加组件,所述第二数字水印添加组件指定用于对所述接收的内容应用数字水印的信息。

18. 根据权利要求 17 所述的系统,其中所述程序指令配置用于在无需替换所述运行时

组件的情况下,替换所述数字水印添加组件。

19. 根据权利要求 16 所述的系统,其中对所述接收的内容应用的所述数字水印指示以下一个或多个:

标识被授权使用受保护内容的用户的信息,标识所述计算机系统的信息,标识发布所述接收的内容的发布者的信息,以及标识所述运行时组件的信息。

20. 根据权利要求 16 所述的系统,其中所述接收的内容是视频内容,其中应用所述数字水印,从而在所述视频内容一个或多个帧上叠加所述数字水印。

21. 根据权利要求 16 所述的系统,其中所述程序指令配置用于在生成所述添加有水印的内容之前,利用来自所述数字水印添加组件的内容密钥来解密所述接收的内容的至少一部分。

22. 根据权利要求 16 所述的系统,其中为了接收所述数字水印添加组件,所述程序指令配置用于接收针对所述接收的内容的许可,所述内容许可包括所述数字水印添加组件。

23. 根据权利要求 16 所述的系统,其中所述水印添加组件包括用于应用所述数字水印的可执行指令,其中为了应用所述数字水印,所述运行时组件配置用于执行所述水印添加组件的所述指令。

24. 根据权利要求 23 的系统,其中所述运行时组件配置用于实现虚拟机,其中所述可执行指令的至少一些以字节码表示,其中为了应用所述数字水印,所述运行时组件配置用于在所述虚拟机上执行所述字节码。

25. 一种系统,包括:

存储器;以及

耦合至所述存储器的一个或多个处理器,其中所述存储器包括可由所述一个或多个处理器执行的程序指令,用以:

向远程计算机系统提供数字水印添加组件,所述远程计算机系统包括配置用于使用内容部分的运行时组件,所述数字水印添加组件与所述运行时组件独立地向所述远程计算机系统提供,所述数字水印添加组件指定用于在所述内容部分上应用数字水印的信息;以及

向所述远程计算机系统提供信息,所述信息指定在未对所述接收的内容应用所述数字水印的情况下,不能在所述远程计算机系统上使用所述内容部分。

26. 根据权利要求 25 所述的系统,其中所述程序指令配置用于:

在无需撤销所述运行时组件的情况下,撤销所述数字水印添加组件;

在所述撤销之后,向所述远程计算机系统提供与所述运行时组件不同的第二数字水印添加组件,所述第二数字水印添加组件指定用于在所述内容部分上应用数字水印的信息。

27. 根据权利要求 26 所述的系统,其中为了撤销所述数字水印添加组件,所述程序指令配置用于在已撤销水印添加组件的列表中创建与所述数字水印添加组件相对应的记录,所述列表对于特定计算机系统是可访问的。

28. 根据权利要求 25 所述的系统,其中所述数字水印指示以下一个或多个:

标识被授权使用受保护内容的用户的信息,标识所述计算机系统的信息,标识发布所述受保护内容的发布者的信息,以及标识所述运行时组件的信息。

29. 根据权利要求 25 所述的系统,其中为了向所述计算机系统提供数字水印添加组

件,所述程序指令配置用于向所述远程计算机系统提供针对所述内容部分的内容许可,所述内容许可包括所述数字水印添加组件。

30. 根据权利要求 25 所述的系统,其中为了向所述远程计算机系统提供指定在未对所述接收的内容应用数字水印的情况下,不能在所述远程计算机系统上使用所述内容部分的信息,所述程序指令配置用于:

向所述远程计算机系统提供针对所述内容部分的内容许可,所述内容许可包括指定在未对所述接收的内容应用所述数字水印的情况下,不能在所述远程计算机系统上使用所述内容部分的信息。

31. 一种计算机可读存储介质,在计算机系统上存储计算机可执行的程序指令,用以:
接收内容;

提供配置用于使用所述内容的运行时组件;

接收数字水印添加组件,其中所述数字水印添加组件与所述运行时组件独立地接收,其中所述数字水印添加组件指定用于在所述接收的内容上生成数字水印的信息;以及

其中所述运行时组件配置用于对所述接收的内容应用数字水印以生成添加有水印的内容,其中所述运行时组件配置用于根据所述数字水印添加组件来应用所述数字水印,其中所述运行时组件配置用于阻止在未对所述接收的内容应用所述数字水印的情况下使用所述接收的内容。

32. 根据权利要求 31 所述的介质,其中所述程序指令配置用于:

响应于确定所述数字水印添加组件已经撤销,利用第二数字水印添加组件来替换所述系统的数字水印添加组件,所述第二数字水印添加组件指定用于对所述接收的内容应用数字水印的信息。

33. 根据权利要求 32 所述的介质,其中所述程序指令配置用于在无需替换所述运行时组件的情况下,替换所述数字水印添加组件。

34. 根据权利要求 31 所述的介质,其中应用至所述接收的内容的所述数字水印指示以下一个或多个:

标识被授权使用受保护内容的用户的信息,标识所述计算机系统的信息,标识发布所述接收的内容的发布者的信息,以及标识所述运行时组件的信息。

35. 根据权利要求 31 所述的介质,其中所述接收的内容是视频内容,其中应用所述数字水印,从而在所述视频内容一个或多个帧上叠加所述数字水印。

36. 根据权利要求 31 所述的介质,其中所述程序指令配置用于在生成所述添加有水印的内容之前,利用来自所述数字水印添加组件的内容密钥来解密所述接收的内容的至少一部分。

37. 根据权利要求 31 所述的介质,其中为了接收所述数字水印添加组件,所述程序指令配置用于接收针对所述接收的内容的内容许可,所述内容许可包括所述数字水印添加组件。

38. 根据权利要求 31 所述的介质,其中所述水印添加组件包括用于应用所述数字水印的可执行指令,其中为了应用所述数字水印,所述运行时组件配置用于执行所述水印添加组件的所述指令。

39. 根据权利要求 38 所述的介质,其中所述运行时组件配置用于实现虚拟机,其中所

述可执行指令的至少一些是以字节码表示的，其中为了应用所述数字水印，所述运行时组件配置用于在所述虚拟机上执行所述字节码。

40. 一种计算机可读存储介质，在计算机系统上存储计算机可执行的程序指令，用以：向远程计算机系统提供数字水印添加组件，所述远程计算机系统包括配置用于使用内容部分的运行时组件，所述数字水印添加组件与所述运行时组件独立地向所述远程计算机系统提供，所述数字水印添加组件指定用于在所述内容部分上应用数字水印的信息；以及向所述远程计算机系统提供信息，所述信息指定在未对所述接收的内容应用所述数字水印的情况下，不能在所述远程计算机系统上使用所述内容部分。

41. 根据权利要求 40 所述的介质，其中所述程序指令配置用于：
在无需撤销所述运行时组件的情况下，撤销所述数字水印添加组件；
在所述撤销之后，向所述远程计算机系统提供与所述运行时组件不同的第二数字水印添加组件，所述第二数字水印添加组件指定用于在所述内容部分上应用数字水印的信息。

42. 根据权利要求 41 所述的介质，其中为了撤销所述数字水印添加组件，所述程序指令配置用于在已撤销水印添加组件的列表中创建与所述数字水印添加组件相对应的记录，所述列表对于特定计算机系统是可访问的。

43. 根据权利要求 40 所述的介质，其中所述数字水印指示以下一个或多个：
标识被授权使用受保护内容的用户的信息，标识所述计算机系统的标识，标识发布所述受保护内容的发布者的信息，以及标识所述运行时组件的信息。

44. 根据权利要求 40 所述的介质，其中为了向所述计算机系统提供数字水印添加组件，所述程序指令配置用于向所述远程计算机系统提供针对所述内容部分的内容许可，所述内容许可包括所述数字水印添加组件。

45. 根据权利要求 40 所述的介质，其中为了向所述远程计算机系统提供指定在未对所述接收的内容应用数字水印的情况下，不能在所述远程计算机系统上使用所述内容部分的信息，所述程序指令配置用于：
向所述远程计算机系统提供针对所述内容部分的内容许可，所述内容许可包括指定在未对所述接收的内容应用所述数字水印的情况下，不能在所述远程计算机系统上使用所述内容部分的信息。

利用轻量级数字水印添加组件的数字版权管理的系统和方法

技术领域

[0001] 本发明涉及计算机系统。更具体地，本发明涉及计算环境中的数字版权管理。

背景技术

[0002] 在几年前，个人从零售地点获得物理介质形式的内容（例如，文学作品、期刊、音乐和电影）是常见的。例如，个人可以到当地书店，并且购买书籍、报纸或者杂志形式的写作作品。在另一示例中，个人可以购买存储在光盘（CD）上的音乐或者存储在数字视频光盘（DVD）中的影片。近几年，因特网和万维网的普及为获得和使用内容的备选方法铺平了道路。例如，用户可以登录到音乐零售商的网站，并且下载音乐专辑的数字版本。在其他示例中，用户可以登录到电影订购提供商的网站，对影片进行下载或者流式传输，以便在个人计算机上观看。在书籍的情况下，用户可以登录到书商的网站，并且下载电子书（“e-book”），以便在计算机系统（诸如，台式计算机或者手持电子书阅读器）上观看。

[0003] 因特网和万维网充当很多文件共享机制的支柱。此类机制的示例包括电子邮件（“email”）和较高级的文件分发软件（诸如端对端（“P2P”）文件共享应用）。在很多情况下，此类文件共享机制常常被用来向没有授权访问电子内容的个体分发此类内容。此类分发可能部分归因于通过此类机制共享文件的相对简便性和匿名性。为了对抗未授权的内容使用，一些内容所有者采用称为数字版权管理（“DRM”）的方法来保护其内容，这种方法可以包括用于将电子内容的访问限于授权的个体和 / 或用于对此类内容的使用强制其他限制的各种技术。

发明内容

[0004] 描述了用于利用轻量级数字水印添加组件进行数字版权管理的系统和方法的各种实施方式。各种实施方式可以包括计算机实现的方法以及配置用于执行此类方法的元件。在各种实施方式中，这种方法可以包括接收内容到计算机系统上；计算机系统可以包括配置用于使用该内容的运行时组件。此类内容的一个示例包括但不限于视频内容。该方法还可以包括经由计算机系统接收数字水印添加组件（例如，与运行时组件独立接收）。数字水印添加组件可以指定用于在接收的内容上生成数字水印的信息。此类信息的示例包括但不限于：表示数字水印的图像或者图形数据、用于应用数字水印的指令和 / 或用于应用数字水印的可执行逻辑。该方法还可以包括经由运行时组件对接收的内容应用数字水印，以便生成添加有水印的内容。在各种实施方式中，可以由运行时组件根据数字水印添加组件来应用数字水印。在各种实施方式中，接收的运行时组件可以配置用于保证在未对接收的内容应用数字水印的情况下无法使用该接收的内容。

[0005] 各种实施方式可以包括用于向远程计算机系统提供上述数字水印添加组件的元件或者方法。例如，此类方法可以包括向远程计算机系统（诸如，包括上述运行时组件的计算机系统）提供此类数字水印添加组件。在各种实施方式中，提供数字水印添加组件可以

包括与运行时组件独立地提供数字水印添加组件。在各种实施方式中，数字水印添加组件可以指定用于在内容部分上应用数字水印的信息。此类方法的各种实施方式还可以包括向远程计算机系统提供指定在未对内容部分应用数字水印的情况下不能使用该内容部分的信息。

附图说明

[0006] 图 1 示出了根据各种实施方式的利用轻量级数字水印添加组件进行数字版权管理的方法和系统的各种元件的框图。

[0007] 图 2A 示出了根据各种实施方式的应用水印之前的示例图像。

[0008] 图 2B 示出了根据各种实施方式的应用水印之后的示例图像。

[0009] 图 3 示出了根据各种实施方式的应用水印之后的另一示例图像。

[0010] 图 4 示出了根据各种实施方式的利用轻量级数字水印添加组件进行数字版权管理的系统配置的一个示例。

[0011] 图 5 示出了根据各种实施方式的用于接收内容以及利用数字水印添加组件对此类内容应用水印的示例方法的流程图。

[0012] 图 6 示出了根据各种实施方式的用于提供数字水印添加组件的示例方法的流程图。

[0013] 图 7 示出了根据各种实施方式的配置用于实现利用轻量级数字水印添加组件进行数字版权管理的方法和系统的各种元件的示例计算机系统。

[0014] 虽然在此通过若干实施方式和示意性附图的方式描述了利用轻量级数字水印添加组件进行数字版权管理的系统和方法，但是本领域技术人员将认识到，利用轻量级数字水印添加组件进行数字版权管理的系统和方法不限于所描述的实施方式或者附图。应当理解，附图以及对其的详细描述并不意在将实施方式限制于所公开的特定形式。相反，本发明意在覆盖落在所附权利要求所限定的利用轻量级数字水印添加组件进行数字版权管理的系统和方法的精神和范围内的所有修改、等效项和备选方案。在此使用的任何标题仅用于组织的目的，并不意味着限制本说明书或者权利要求的范围。如在此使用的，词语“可以”按照宽松的意义来使用（即，表示具有可能性），而不是按照强制的意义来使用（即，表示必须）。类似地，词语“包括”、“包含”和“包含有”意思是包括，但不限于此。在此处提出的描述的各种部分中，术语“证实”、“验证”、“生效”、“查证”、“确认”和“核查”可以互换使用。

具体实施方式

[0015] 描述了利用轻量级数字水印添加组件进行数字版权管理的系统和方法的各种实施方式。在以下详细描述中，记载了多个特定细节以提供对所要求保护的主题的全面理解。然而，本领域技术人员将理解，所要求保护的主题可以在没有这些特定细节的情况下实施。在其他实例中，没有详细描述本领域技术人员所知的方法、装置或者系统，以避免混淆要求保护的主题。

[0016] 下文详细描述的某些部分是通过对存储在特定装置或者专用计算设备或者平台的存储器内的二进制数字信号进行操作的算法或者符号表示而给出的。在本说明书的上下文中，术语“特定装置”等包括通用计算机，只要其被编程以执行按照来自程序软件的指令

的特定功能。算法描述或者符号表示是信号处理或者相关领域内的技术人员向该领域内的其他技术人员传递其工作主旨所使用的技术的示例。此处或者通常将算法视为独立的操作序列或者产生所期待的结果的类似信号处理。在该上下文中，操作或者处理包括物理量的物理操作。通常但不是必需的，此类量可以采用能够进行存储、传送、组合、比较或者其他方式操作的电或者磁信号的形式。主要由于通用的原因，已经多次证明将此类信号称为比特、数据、值、元素、符号、字符、项、数目、数字等是方便的。然而，应当理解，所有这些或者类似的术语需要与适合的物理量相关联，并且其仅是方便的标记。除非另外特别表明，根据以下讨论变得明显的是，可以理解，贯穿本说明书全文，使用诸如“处理”、“计算”、“运算”、“确定”等术语的讨论是指特定装置（诸如专用计算机或者类似的专用电子计算设备）的动作或者过程。因此，在本发明书的上下文中，专用计算机或者类似的专用电子计算设备能够对信号进行处理或者转换，信号通常表示为专用计算机或者类似的专用电子计算设备的存储器、寄存器或者其他信息存储设备、传输设备或者显示设备内的物理电子或者磁量。

[0017] 各种实施方式可以包括配置用于向一个或多个客户端系统提供受保护内容（例如，加密内容）的分发系统。例如，分发系统可以向多个客户端系统提供基于 web 的内容，诸如视频内容（或者在此描述的任何其他类型的内容）。在各种实施方式中，分发系统还可以向客户端提供数字水印添加组件。注意，在各种实施方式中，向客户端提供水印添加组件的分发系统可以但不必一定是向客户端提供受保护内容的相同分发系统。当水印添加组件在客户端系统上执行时，其可以向内容添加数字水印。此类水印添加组件的一个示例包括但不限于 **Adobe® Pixel Bender™** 基础架构的过滤器（例如，可执行逻辑或者指令）。

[0018] 数字水印可以是可见水印或者不可见水印。可见水印可以包括叠加到视频内容的帧、单个图片或者图形内容上的图形、文本、图标或者其他图形元素。在一些情况下，可见水印可以是至少部分透明的，以便允许水印“后面的”内容的部分视图。在各种实施方式中，可见水印可以指示特定类型的信息，诸如名称和 / 或标识符。例如，可见水印可以指示被授权查看应用可见水印的内容的个体的名称。在此详述了其他类型的可见水印。可见水印可以阻止各种类型的未授权分发。例如，如果利用购买视频文件的客户的名称（或者标识客户或者可以追溯到客户的其他信息）来对视频文件进行水印添加，则客户可能不太可能与未授权的用户共享该视频文件。例如，客户可能不太可能将该视频文件上传到网站或者端对端文件共享网络，因为害怕该文件（以及由此还有对该文件的未授权共享）追溯到他。不可见水印可以包括嵌入到内容中的任何类型的信息，在没有计算机系统执行的某些附加分析的情况下，这些信息是人类不可感知的。虽然不可见水印可能是人类不可感知的，但是计算机实现的逻辑可以从添加有水印的内容中检测并且获取不可见水印。此类逻辑有时称为水印检测功能或者水印获取功能。在一些实施方式中，应用水印可以包括应用可见水印和不可见水印二者。

[0019] 在各种实施方式中，向客户端发送的水印添加组件和 / 或客户端系统上的运行时组件的逻辑可以确保：在未对内容应用数字水印添加的情况下无法访问该内容。在内容是视频内容的示例中，水印添加组件和 / 或运行时组件可以当且仅当向视频内容的至少某些帧叠加水印时，允许播放视频内容。在此详述了确保在未对内容应用数字水印的情况下无法访问该内容的其他示例。

[0020] 各种实施方式包括各种加密和 / 或解密密钥，其中任何一种都可以经由密钥导出

函数 (KDF) 来生成。密钥导出函数可以包括散列函数和 / 或其他密码操作的一个或者多个迭代或者实例, 以便生成加密或者解密密钥。密码导出函数的示例可以包括但不限于由公开密钥密码标准 (PKCS) (例如, PKCS-5) 或者 Adobe 口令安全 (AdobePassword Security) 指定的任何密钥导出函数。

[0021] 详细描述的各部分可能提到“客户端”和“服务器”或者类似的术语。例如, 各种实施方式可以包括 (除了其他元件之外) 客户端系统或者客户端设备 (或者简称“客户端”)。应当理解, 术语“客户端”和“服务器”并不对此类元件的操作、配置或者实现进行任何限制。应当理解, 这些术语仅仅是被用作方便的命名法。实际上, 各种实施方式丝毫不受传统客户端 - 服务器架构的原理的限制。例如, 在此描述的“客户端”或者“服务器”中的任何一种都可以配置用于根据多种通信协议或者系统架构 (诸如端对端 (P2P) 架构或者某些其他架构) 来进行通信, 无论这些架构是目前已知的还是将来开发的。

[0022] 在各种情况下, 该详细描述可能提到内容 (其还可以称为“内容项”、“内容数据”、“内容信息”或者简称“数据”或者“信息”)。通常, 内容可以包括向一个或者多个个体 (或者其他实体, 诸如企业或者集团) 许可的任何信息或者数据。在各种实施方式中, 内容可以包括视频、音频、文本和 / 或图形的电子表示, 其可以包括但不限于视频、电影或者其他多媒体的电子表示, 其可以包括但不限于按照 **Adobe® Flash®** 视频 (.FLV 或者 .F4V) 格式或者某些其他视频文件格式的数据文件, 不管该格式是目前已知的还是将来开发的。在某些情况下, 内容可以包括按照以下格式的数据文件 : 便携文件 格式 (.PDF)、由国际数字出版论坛 (IDPF) 创建的电子出版 (.EPUB) 格式、JPEG (.JPG) 格式、便携网络图形 (.PNG) 格式、**Adobe® Photoshop®** (.PSD) 格式或者用于电子地存储文本、图形和 / 或其他信息的某些其他格式, 不管此类格式是目前已知的还是将来开发的。在一些实施方式中, 内容可以包括上述示例的任何组合。

[0023] 在各种实例中, 该详细公开可能提到使用内容或者对内容的使用, 其可以包括访问内容、显示内容以便查看 (例如, 以便由用户查看)、播放内容 (例如, 在媒体播放器中) 或者绘制内容 (例如, 呈现 2D 或者 3D 图像) 以及其他。在某些情况下, 所使用的特定术语可能取决于其所使用的上下文。例如, 使用视频也可以称为显示或者播放视频。

[0024] 在各种实例中, 该详细描述可能提到在其上使用内容的设备。在各种实施方式中, 此类设备可以包括但不限于计算设备 (例如, 台式或者膝上型计算机或者其他类型的计算机系统)、数字音频或者多媒体播放器 (例如, MP3 播放器)、个人数字助理 (PDA)、移动电话、智能电话、电子书阅读器、数码相框、电视机、机顶盒 (其可以与电视机或者其他监视器结合使用)、手持或者移动设备, 或者配置用于访问、查看、阅读、编写和 / 或操作在此描述的任何内容数据的任何其他电子设备或者系统。任何此类设备可以经由与关于图 7 描述的类似的计算机系统来实现。

[0025] 注意, 在各种实例中, 在此给出的描述可能提到执行某些动作的给定实体。应当理解, 在某些情况下, 该语言可以表示 : 给定实体所拥有和 / 或控制的系统 (例如, 计算机系统) 在实际执行动作。

[0026] 在各种实施方式中, 可以使用各种技术来提供在此描述的 DRM 框架的任何元件之间的安全通信。例如, DRM 框架的各种元件可以与相关的公钥 - 私钥对 (诸如公钥基础架构 (PKI) 中使用的密钥对) 相关联。在各种实施方式中, 第一元件 (例如, 内容分发系统) 可

以利用第二元件的公钥来加密数据，从而安全地向第二元件传送数据（例如，内容许可）。以此方式，根据各种实施方式，只有第二元件能够解密该加密数据以访问非加密数据。例如，因为在各种实施方式中，解密数据可能需要私钥的知识，并且因为第二元件可能是具有其自身私钥知识的唯一元件，所以第二元件可以是能够利用正确的私钥来解密数据的唯一元件。注意，上述技术可以在各种实施方式中用于在此描述的DRM框架内的任何数据传送。

[0027] 封包

[0028] 图1示出了利用轻量级数字水印添加组件进行数字版权管理的方法和系统的各种组件。封包系统100可以经由一个或多个计算机系统来实现。在各种实施方式中，封包系统100可以由内容所有者或者版权持有者所有或者控制，版权持有者的一个示例包括拥有此类内容版权（例如，著作权或者其他知识产权）的实体。在一个特定的示例中，内容所有者可以向其他实体提供此类内容（例如，内容零售商或者经销商）以获得许可费。例如，这样的内容所有者可能制作内容（例如，电影），并且对向零售客户分发内容的内容零售商（例如，在线销售或者租赁内容的在线零售商）许可此类内容。

[0029] 在各种实施方式中，封包器106可以配置用于利用使用规则104对内容102进行封包，以生成受保护内容108。在一些实施方式中，保护或者封包内容102可以包括利用加密密钥来加密内容。在某些情况下，这还可以包括将使用规则104连同内容102一起加密，以生成包括此类使用规则的受保护内容。在该情况下，如果受保护内容最终被解密，则可以向内容的使用施加解密的使用规则。通常，使用规则可以包括关于内容的使用或者访问的任何限制，包括但不限于将内容的访问限制在特定时段，限制针对受保护内容所能执行的动作（例如，查看、复制、保存、分发等）。在某些情况下，与内容102一起封包的使用规则可以充当模板，其将由另一实体（例如，销售或者租赁该内容的内容分发器）来填入一个或者多个规则。例如，内容分发者可以在此类模板中指定指示内容的过期日期的规则。作为在受保护内容中存储使用规则的备选（或者除了在受保护内容中存储使用规则以外），使用规则可以存储在内容的内容许可中（下文详述）。在内容许可中存储使用规则有助于针对相同的受保护内容创建用户特定的使用规则；例如，可以针对不同的用户创建包含不同使用规则的不同许可。

[0030] 分发

[0031] 在各种实施方式中，如所示，封包系统100可以通过通信190向一个或多个分发系统120提供不同类型的受保护内容（诸如，受保护内容108）。在各种实施方式中，分发系统120可以请求此类内容。在其他情况下，封包系统100可以自动地向分发系统120递送此类内容（例如，以“推送”方式）。由分发系统120接收的受保护内容的各实例可以存储在数据存储128中，以使得内容对于分发系统的其他元件是可访问的。在各种实施方式中，数据存储128可以配置为数据库、配置用于存储数据块或者文件的一个或多个大容量存储设备（例如，物理磁盘、逻辑卷等），或者按照用于数据存储的任何其他适合配置。在各种实施方式中，数据存储128可以存储受保护内容108以及受保护内容的多个其他部分。

[0032] 内容分发器122可以配置用于向一个或多个客户端（诸如，客户端140）提供受保护内容。例如，内容分发器122可以是向各客户端提供内容的web服务器（或者其他基于网络的服务器）的组件。例如，运行时组件160可以是web浏览器的一部分，或者可以与web浏览器共同操作，以发布针对来自分发系统120的内容的请求。响应于此类请求，分发系统

120 可以向一个或多个诸如客户端 140 的客户端提供内容。在示出的实施方式中,如所示,分发系统 120 可以通过通信 192 向客户端 140 提供受保护内容 108(或者其他类型的受保护内容)。在各种实施方式中,运行时组件可以是计算机实现的运行时环境,在其上可以执行各种应用、程序、功能、脚本、字节码和 / 或其他指令。在一个特定的示例中,运行时组件 100 可以是 **Adobe® Flash®** 播放器。

[0033] 在各种实施方式中,如所示,运行时组件 160 可以通过通信 194 来发布针对受保护内容 108 的内容许可的请求。此类通信还可以包括运行时组件 160 和执行授权过程的许可服务器 124,以便使得客户端 140(和 / 或客户端 140 的用户)被授权接收内容许可。在各种实施方式中,直到生成了内容的干净 (clear) 形式,才可以使用(例如,呈现、播放、显示、绘制等)受保护内容。例如,如果加密了受保护内容 108(情况可能就是如此),则必须对受保护内容进行解密以便访问内容的非加密版本(例如,内容 102)。在各种实施方式中,上述内容许可可以包括内容密钥,其可以用于解密受保护内容 108。换言之,在各种实施方式中,在没有获得内容的适合许可的情况下,可能无法使用受保护内容 108。因此,许可服务器 124 可以仅向授权的客户端(或者操作此类客户端机器的授权的用户)提供受保护内容 108 的内容许可。

[0034] 在通信 194 期间,可以交换各种类型的信息,以执行授权过程。在一些实施方式中,运行时组件 160 可以提供与客户账号和 / 或内容购买相关联的用户名和口令。许可服务器 124 可以通过将此类信息与数据存储 120 内的信息(例如,客户记录、客户简档、购买记录等)进行比较来验证此类信息。在某些情况下,运行时组件 160 可以提供数字证书(例如,由信任的第三方发布的数字证书)作为授权过程的一部分,数字证书的一个示例包括 X.509 数字证书。在其他情况下,可以从运行时组件 160 向许可服务器 124 发送其他类型的数字证书(基于时间的代码、生物计量信息或者其他可验证信息),以建立客户端系统 140(或者控制此类系统的用户)的标识。在各种实施方式中,在通信 194 期间,可以向许可服务器 124 提供标识运行时组件 160 的信息(例如,版本或者实例标识符)、标识客户端系统 140 的信息(例如,机器地址或者网际协议地址)或者标识客户端系统 140 其他元件的信息。

[0035] 如果许可服务器 124 没有对客户端系统提供的信息做出肯定验证,则许可服务器可以向客户端系统阻止对应于受保护内容 108 的 内容许可。如果许可服务器 124 进行了肯定地验证(例如,通过将所提供的信息与记录在数据存储 128 上的信息),则许可服务器可以向运行时组件 160 发送内容许可 125(其可以包括用于解密受保护内容 108 的正确内容密钥)。在某些情况下,内容许可也可以称为内容策略。

[0036] 许可 125 可以包括用于解密受保护内容 108 的内容密钥(在很多情况但未必是所有情况下,其可以对该内容是特定的)。许可 125 还可以包括一个或多个使用规则(也可以称为策略规则)。通常,使用规则可以包括关于内容的使用或者访问的任何限制,包括但不限于:将对内容的访问限制在特定时段,限制针对受保护内容所能执行的动作(例如,查看、复制、保存、分发等)。在各种实施方式中,使用规则可以指定是否要在使用受保护内容 108 之前对该内容应用水印。在示出的实施方式中,许可 125 可以指定:受保护内容 108 仅在具有应用于该内容的水印的情况下可以被使用。在各种实施方式中,许可 125 可以指定用于应用此类水印的特定水印添加组件(下文详述)。

[0037] 在各种实施方式中，分发系统 120 还可以向运行时组件 160 提供水印添加组件 164。在各种实施方式中，在从分发系统接收该水印添加组件之前，客户端系统 140 上不存在该水印添加组件。在某些情况下（诸如在示出的实施方式中），可以将水印添加组件 164 作为内容许可 125 的一部分向运行时组件 160 递送（例如，水印添加组件 164 包括在内容许可 125 内）。在各种实施方式中，运行时组件 160 可以配置用于从内容许可 125 提取运行时组件 164，如 168 处所示。在水印添加组件 164 是内容许可 125 的一个元素的实施方式中，关于 194 描述的授权过程可以充当针对内容许可以及水印添加组件 164 的授权过程（因为水印组件包括在许可中）。在水印添加组件 164 与内容许可是不同元素的实施方式中，关于通信 194 描述的授权过程或者单独的类似授权过程可以用于控制对水印添加组件的访问。

[0038] 在各种实施方式中，由分发系统 120 向客户端系统 140 提供的 水印添加组件可以由水印组件生成器 126 生成。例如，在许可服务器将水印添加组件插入到许可 125 中的实施方式中，许可服务器可以向水印组件生成器 126 查询此类水印组件的数据表示。在各种实施方式中，此类数据可以包括配置用于对内容的一部分应用水印的可执行指令（其可以由字节码表示）。水印组件生成器 126 可以配置用于向许可服务器提供水印组件，以便将其包括在内容许可中并向客户端系统递送。在由分发系统 120 提供的水印添加组件与内容许可独立地向客户端系统提供的实施方式中，水印组件生成器 126 可以向此类客户端系统提供此类水印添加组件。

[0039] 如上所述，在一些实施方式中，在此描述的水印添加组件可以包括诸如字节码的可执行指令。在各种实施方式中，运行时组件 160 可以执行此类指令以便对内容应用水印。在一些实施方式中，运行时组件可以实现配置用于执行水印添加组件的虚拟机。例如，在水印添加组件由可执行字节码表示的实施方式中，在此描述的运行时组件可以配置用于使用上述虚拟机来执行字节码。在一个示例中，在此描述的运行时组件可以实现与 **Adobe® Pixel Bender™** 基础架构的虚拟机关联，并且水印添加组件可以与 **Adobe® Pixel Bender™** 基础架构关联的过滤器；此类过滤器可以由上述虚拟机执行以便对内容应用水印的字节码来表示。

[0040] 解密和水印添加

[0041] 在各种实施方式中，运行时组件 160 可以包括数字版权管理 (DRM) 组件 162。DRM 组件 162 的一个特定示例包括用于 **Flash®** 播放器的 **Adobe® DRM** 客户端。在各种实施方式中，DRM 组件 162 可以配置用于从许可 125 提取内容密钥 166，并且利用该密钥来解密受保护内容 108。在示出的实施方式中，此类解密的结果示出为内容 102，其可以与在封包系统 100 处原始封包的内容 102 相同。在各种实施方式中，DRM 组件 162 可以配置用于根据各种技术来执行加密 / 解密，包括但不限于对称加密 / 解密和非对称加密 / 解密。

[0042] 在各种实施方式中，内容 102 可以是受保护内容 108 的干净（例如，非加密）形式。为了保护此类内容使其免受危害，可以由运行时组件 160 提供的防篡改（或者篡改防护）环境来保护内容 102。在各种实施方式中，内容 102 可以仅对运行时组件 160 和该运行时组件的元件是可访问的或者“可见的”。以此方式，可以禁止运行时组件 160 的域之外的客户端系统 140 的其他组件访问内容 102。运行时组件的防篡改环境可以由运行时组件经由多种技术来实现，包括但不限于：在任意给定时刻仅表示存储器内的敏感数据的部分（例如，

在某些情况下是较小的包）。例如，可以逐个部分地将数据作为流来处理，从而在同一时刻只有流的一部分在存储器中是可见的。在某些情况下，防篡改环境可以对运行时组件可访问的数据或者可访问的任何元件的数据或者可执行指令（或者代码）执行模糊处理。在各种实施方式中，运行时组件 160 可以配置用于检测调试器（例如，调试应用、脚本、元件等）的存在，并且响应于此类检测来阻止对内容 102 的访问。阻止对内容 102 访问的其他安全技术可以在各种实施方式中实现，不管这些技术是目前已知的还是将来开发的。

[0043] 如上所述，可以从分发系统 120 接收水印添加组件 164（例如，在内容许可内接收或者与内容许可独立接收）。注意，在各种实例中，在从分发系统 120 接收水印添加组件 164 之前，客户端系统 140 中可能不存在该组件。在各种实施方式中，运行时组件 160 可以配置用于对内容 102 应用水印（按照水印添加组件所指定的），此后该内容 102 才变为对于运行时组件 160 的防篡改环境之外的组件是可访问的。

[0044] 在各种实施方式中，对内容应用数字水印主要被描述为由运行时组件 160 来执行。还要注意，运行组件应用水印的方式可以由水印添加组件 164 指定。例如，水印添加组件可以是指定要显示的水印或者信息的类型的数据文件，并且运行时组件可以配置用于基于此类信息对内容应用水印。在一些实施方式中，水印添加组件可以包括可执行指令，并且运行时组件可以配置用于通过执行此类指令 来应用水印。应当注意，在一些情况下，水印的应用可以由水印添加组件自身来执行。例如，在一些实施方式中，水印添加组件 160 可以是配置用于应用水印的软件模块，并且运行时组件可以发起此类模块的执行以便对内容应用水印。虽然对内容应用数字水印在此处主要描述为由运行时组件 160 执行，但是任意上述实现可以在各种实施方式中使用。

[0045] 在各种实施方式中，运行时组件 160 可以根据不同的技术应用水印。例如，应用水印可以包括将信息叠加或者以其他方式插入内容 102 中，以生成此类内容的新版本（示出为添加有水印的内容 170，下文详述）。在某些情况下，多数所生成的添加有水印的内容 170 可以与该添加有水印的内容 170 从其生成的内容 102 相同。在各种实施方式中，内容 102 与添加有水印的内容 170 之间的差别在于水印本身。例如，图 2A 的图像 200 可以是表示内容 102 的一个示例的视频帧（例如，组成视频的所有图像中的一个图像）。图 2B 的图像 210 是在对同一视频帧应用水印图形 220 之后该帧的一个示例。在各种实施方式中，对视频帧或者图像应用水印的这一过程可以由在此描述的水印添加组件 164 来实现。

[0046] 在各种实施方式中，水印的位置和 / 或方向可以随着视频内容的播放时段而改变（例如，可以对相同视频的不同帧以不同的方式应用水印）。在一个示例中，图像 210 可以是视频内容的帧，而图 3 的图像 300 可以是相同视频内容的另一帧。注意，水印 220 和水印 310 的位置和方向是不同的。在各种实施方式中，水印添加组件 164 可以改变视频内容中水印的位置和 / 或方向，以防止恶意用户裁剪掉内容的一部分（例如，图像的底部 100 像素，或者某些其他部分）以便从添加有水印的内容中移除水印。

[0047] 在各种实施方式中，运行时组件 160 可以访问关于客户端系统 140 的信息（和 / 或关于客户端系统 140 的用户的信息），并且生成添加有水印的内容 170，使得作为该内容的一部分被显示的水印指示该信息。例如，运行时组件 160 可以生成添加有水印的内容 170，使得 该水印指示包括以下一个或多个的各种标识信息：客户端系统 140 的机器标识符（例如，主机地址、网际协议地址、媒体访问控制地址或者客户端系统的某些其他标识符）、标识

客户端系统的用户和 / 或被授权使用该内容的用户的用户标识符（例如，姓名、代码、由第三方发布的标识符、用户名、客户标识符等）、标识安装在客户端系统上的一个或多个应用（例如，运行时组件）的软件标识符、标识公布所接收内容的公布者的信息，或者一些其他类型的标识符。如上所述，添加有水印的内容 170 中水印的存在可以阻止各种类型的未授权分发。例如，如果利用购买视频文件的客户的姓名对该视频文件进行了水印添加，则该客户不太可能与未授权用户共享该视频文件。

[0048] 在各种实施方式中，可以在生成水印之前，由运行时组件 160（按照水印添加组件 164 指定的）初始地获取包括在添加有水印的内容 170 的水印内的标识信息（例如，以上描述的各种标识符）。例如，运行时组件 160 可以配置用于搜索或者定位来自客户端系统 140 的标识信息（诸如以上描述的任何标识符）。例如，运行时组件 160 可以配置用于定位客户端系统 140 上的机器标识符，并且将该标识符包括在添加有水印的内容 170 的水印中。在另一示例中，运行时组件 160 可以配置用于定位客户端系统 140 上的用户标识符（例如，姓名或者用户名），并且将该标识符包括在添加有水印的内容 170 的水印中。在某些情况下，运行时组件 160 可以配置用于从分发系统 120 接收标识信息，并且将该标识符包括在添加有水印的内容 170 的水印中。在任何上述技术中，对内容应用水印以生成添加有水印的内容 170 这一过程可以在客户端系统 140 处进行。例如，在客户端系统处接收的受保护内容 108 和从受保护内容生成的内容 102（例如，经由解密）可以不包括由运行时组件 160 应用的水印。在各种实施方式中，仅当运行时组件根据水印添加组件 164 应用了水印之后，内容才包括由水印添加组件生成的特定水印。

[0049] 在一些实施方式中，包括在添加有水印的内容 170 的水印中的 信息（例如，上述各种标识符）可以由运行时组件 160 从分发系统 120 接收。例如，分发系统 120 可以在向运行时组件 160 提供的许可 125 或者某些其他数据中提供此类信息。在一个示例中，许可 125 和 / 或水印添加组件 164 可以包括表示水印图形的数据；此类图形可以由运行时组件 160 应用于内容 102，以便生成添加有水印的内容 170。在其他情况下（例如，在上述实施方式中），应用于内容 102 的实际水印图形可以根据客户端系统上的运行时组件 160 所获取的信息来生成（例如，在执行水印组件 164 之前，客户端系统上可能存在水印图形）。

[0050] 在各种实施方式中，可以将添加有水印的内容 170 向输入 / 输出 (“I/O”) 组件 172 提供。在各种实施方式中，I/O 组件 172 可以配置用于诸如在显示器（例如，以下关于图 7 描述的显示器 780）上输出添加有水印的内容 170 的图形表示。

[0051] 在各种实施方式中，被执行以便从内容 102 生成添加有水印的内容 170 的水印添加是不可逆的过程。例如，在某些情况下，仅仅给出添加有水印的内容 170，无法重新生成内容 102。

[0052] 水印强制实施

[0053] 在各种实施方式中，运行时组件 160 可以配置用于强制施加如下要求，即在确定水印添加组件 164 在客户端系统 140 上存在和 / 或执行之前，无法使用内容。在一些实施方式中，受保护内容 108 和 / 或许可 125 可以指定对该内容应用水印的特定水印添加组件。例如，许可可以指定通过包括标识特定水印组件的标识符，来指定将要使用该特定水印组件。在水印添加组件包括在内容许可中的实施方式中，要使用的特定水印添加组件可以根据此类包括来指定（例如，运行时组件可以从许可中提取水印添加组件，并且使用该水印

添加组件对内容应用水印)。

[0054] 在各种实施方式中,运行时组件 160 可以配置用于确定所指定的水印添加组件是否存在于客户端系统 140 上。如果所指定的水印 添加组件存在于客户端系统上,则运行时组件可以对内容应用特定水印,以便根据水印添加组件 164 指定的信息来生成添加有水印的内容 170。如果水印添加组件不存在于客户端系统上,则运行时组件可以禁止访问内容 102。例如,在各种实施方式中,客户端系统上可能安装有类似于水印添加组件 164 的多种其他水印添加组件(例如,来自其他分发系统的水印添加组件)。在这种情况下,运行时组件 160 可以配置用于拒绝此类水印添加组件对特定内容 102 的访问(除非此类水印添加组件被受保护内容 108 和 / 或许可 125 指定为经授权的水印添加组件)。

[0055] 在各种实施方式中,除了上述强制实施技术之外(或者作为其备选),解密受保护内容 108 的一部分以重新生成内容 102 可能需要拥有水印添加组件 164。例如,封包系统 100 和 / 或分发系统 120 可以利用第二内容密钥来加密内容 102 或者受保护内容 108 的一个或多个部分。在各种实施方式中,解密这些部分的特定密钥可以由水印添加组件 164 持有。以此方式,在未向内容(例如,受保护内容 108、内容 102)的特定部分指派适当水印添加组件的情况下,运行时组件 160 可能无法完全解密该内容。因此,即使是攻击者破解了由 DRM 组件 162 执行的解密方案,攻击者也无法解密受保护内容 108 的该部分,因为这些部分必须利用水印添加组件 164 指定的解密密钥来解密。

[0056] 水印添加组件的撤销和更新

[0057] 在某些情况下,攻击者可能试图危害水印添加组件 164 以便绕开将水印应用于输出自运行时组件的内容。例如,攻击者可能试图利用未授权组件来顶替水印添加组件 164,该未授权组件向运行时组件 160 将自身呈现为合法的运行时组件 160;此类未授权组件可以试图在未对内容应用正确水印的情况下使内容被输出。下面将详述克服上述威胁的技术。

[0058] 在各种实施方式中(如上所述),客户端系统上的内容可能要求 在运行时组件 160 提供对内容的访问(例如,对添加有水印的内容 170 的访问)之前对该内容应用水印。在某些情况下,为了克服危害水印添加组件 164 的攻击,运行时组件 160 和 / 或分发系统 120 可以配置用于撤销水印添加组件,并将其替换为新的水印添加组件(例如,已知没有受到危害的水印添加组件)。

[0059] 在各种实施方式中,分发系统 120 可以维护已撤销或者不受信水印添加组件的列表或者记录。例如,各种实施方式的每个水印添加组件可以由唯一的标识符来标识,并且分发系统 120 可以存储标识已撤销或者不受信水印组件的标识符的列表。运行时组件 160(或者其任何组件)可以配置用于访问此类列表或者记录,以确定安装在运行时组件 160 上和 / 或经由运行时组件 160 执行的特定水印添加组件是否被列为已撤销或者不受信水印添加组件。如果水印添加组件 164 被确定为不受信任或者已撤销,则运行时组件可以使该水印添加组件的使用无效。

[0060] 在水印添加组件 164 被确定为不受信或者已撤销的情况下,运行时组件 140 可以配置用于从分发系统 120 接收新的水印组件。新的水印组件可以是已知为受信或者经授权的水印添加组件。注意,上述接收新的水印添加组件的过程允许利用新的水印添加组件来更新客户端系统,而无需更新运行时组件 160。在某些情况下,水印添加组件的数据足迹可

以小于运行时组件 160 的数据足迹。通过允许利用新的水印添加组件更新客户端系统而不更新运行时组件 160, 各种实施方式可以提供更新水印添加组件的轻量级方法 (例如, 用以克服水印添加方案中的安全漏洞)。在一些实施方式中, 诸如在使用由可以由运行时组件执行的字节码表示的水印添加组件的实施方式中, 根据在此描述的技术更新水印添加可以绕过所更新的客户端系统上的某些安全要求。例如, 在某些情况下, 可以在不查询系统用户是否被允许安装或者运行水印添加组件的情况下, 对客户端系统进行更新; 此类技术可以支持系统的可用性, 并且提供更加良好的最终用户体验。

[0061] 示例系统配置

[0062] 图 4 示出了一个示例系统配置, 其可以在各种实施方式中使用。在示出的实施方式中, 多个计算机系统 (例如分发系统 120、分发系统 410-412、客户端 140 和 420-422) 可以耦合至网络 400。在示出的实施方式中, 每个系统可以配置用于经由网络 400 向任何其他系统通信。网络 400 可以是多种包括但不限于以下网络中的一个或多个: 局域网 (LAN)、广域网 (WAN)、电信网络 (例如, 移动话音和数据网络)、某些其他类型的网络或者其某些组合。在示出的实施方式中, 任何示出的分发系统可以按照上文关于分发系统 120 描述的那样进行配置。而且, 任何示出的客户端系统可以配置为上述客户端系统 140。

[0063] 在各种实施方式中, 示出的分发系统中的任何给定一个可以配置用于向任何或者全部示出的客户端系统提供水印添加组件 (如上所述)。在某些情况下, 由一个分发系统提供的水印添加组件可以与另一分发系统提供的水印添加组件不同。例如, 在各种实施方式中, 由分发系统的水印添加组件生成的水印类型可以是不同的。在另一示例中, 由分发系统的水印添加组件生成的水印可以指定不同的信息。例如, 一种可以指定用户信息, 而另一种可以指定机器信息。在各种实施方式中, 每个分发系统可以根据控制分发系统的实体的需要来提供客户水印添加组件。以此方式, 实施方式可以利用各种水印添加组件之间的差异来支持在此描述的整体 DRM 框架的安全性。例如, 即使攻击者破坏了一个水印添加组件, 上述差异也会将这种安全漏洞限制在特定的水印添加组件。

[0064] 为了进一步支持水印添加组件的安全性, 各种实施方式可以使用经过模糊的水印添加组件, 诸如利用模糊工具对表示此类组件的数据进行修改。在各种实施方式中, 此类模糊工具可以配置用于对数据、字节码和 / 或机器码 (或者其他可执行指令) 进行模糊。在一个示例中, 可以在上述实现中使用任何在此描述的水印添加组件和 / 或密码密钥之前, 对此类元件进行模糊。模糊上述项可以例如隐藏可执行代码的目的以便阻止反向工程, 从而增强各种实施方式的整体安全性。在各种实施方式中, 在此描述的安全技术可以使数据的不同部分 (例如, 加密密钥) 跨多个存储缓冲器分布 (例如, 在任何给定时间, 仅此类数据的一部分在存储器中可用), 使得存储器检验或者调试会话将不会造成对那些数据部分的安全危害。

[0065] 在各种实施方式中, 示出的任何一个给定的客户端系统都可以配置用于从任何或者全部示出的分发系统接收多个水印添加组件 (如上所述)。例如, 给定的客户端系统可以从不同的内容分发器接收内容。每个内容分发者可以具有关于向其分发的内容应用水印的不同要求。例如, 如上所述, 一个分发者可以指定用户信息作为水印的一部分, 而另一分发者可以指定机器信息作为水印的一部分。因此, 所示出任何一个给定的客户端系统可以配置用于根据类似于关于图 1 描述的技术来接收内容的多个部分, 以及针对内容的每个部

分,对内容的该部分应用正确的水印。

[0066] **示例方法**

[0067] 利用轻量级数字水印添加组件进行数字版权管理的系统和方法可以包括多种方法,以下关于图 5 和图 6 对其中的一些进行描述。在各种实施方式中,示出的方法可以由以下描述的图 7 的计算机系统来执行。

[0068] 图 5 示出了用于接收内容以及利用数字水印添加组件对该内容应用水印的流程图。在一些实施方式中,示出的方法可以经由运行时组件(诸如上述运行时组件 160)来实现。如框 500 所示,该方法可以包括在计算机系统上接收内容(例如,将内容接收到计算机系统的一个或多个存储器中);此类计算机系统可以包括配置用于使用内容的运行时组件。例如,接收内容的一个示例可以包括接收类似于上述受保护内容 108 的内容。运行时组件可以包括在此描述的运行时组件的任何示例(例如, **Adobe® Flash®** 播放器或者在此描述的 任何其他运行时组件)。另外,在该上下文中,使用内容可以包括上述使用内容的任何技术(例如,播放、查看、显示等)。示出内容接收的一个示例在上文关于通信 192 进行了描述。

[0069] 如框 502 所示,该方法还可以包括在计算机系统上接收数字水印添加组件(例如,将数字水印添加组件接收到计算机系统的一个或多个存储器中)。此类数字水印添加组件可以与上述运行时组件独立地接收。例如,在接收数字水印添加组件之前,计算机系统可以包括运行时组件。另外,数字水印添加组件可以指定用于在接收的内容上生成数字水印的信息。

[0070] 用于在接收的内容上生成数字水印的信息在各种实施方式中可以是不同的。在一个实施方式中,该信息可以包括构成将要向内容应用的实际水印的图像或者图形。在一些实施方式中,该信息可以包括关于添加有水印的内容 170 的上述任何标识信息(例如,机器标识符、用户标识符、公布者标识符等);运行时组件可以配置用于(对内容)应用包括此类标识信息的水印。在一些实施方式中,该信息可以包括可执行指令(例如,字节码或者其他指令),其可以由运行时组件实现,用以对内容应用数字水印。在一些实施方式中,该信息可以包括表示如下软件模块的数据,这些软件模块可被执行以对内容应用数字水印。

[0071] 如框 504 所示,该方法还可以包括使用运行时组件对接收的内容应用数字水印,以生成添加有水印的内容。在各种实施方式中,可以由运行时组件根据数字水印添加组件来应用数字水印。在各种实施方式中,运行时组件还可以配置用于阻止在未对接收的内容应用数字水印的情况下使用接收的内容。例如,在内容是视频内容的示例中,水印添加组件和 / 或运行时组件可以当且仅当向视频内容的至少某些帧叠加了水印时,才允许播放该视频内容。确保在未对内容应用数字水印的情况下无法访问内容的其他示例已在上文描述。

[0072] 在各种实施方式中,经由运行时组件对接收的内容应用数字水印可以包括访问信息(例如,包括但不限于机器标识符、软件标识符、公布者标识符或者用户标识符的标识信息),以及将此类信息插入接收的内容。在某些情况下,可以执行该操作以使信息是可见的(诸如上述可见水印);在其他情况下,可以执行该操作以使信息是人类不可感知的(诸如上述不可见水印)。在某些情况下,该方法可以包括向内容插入水印的可见版本和不可见版本二者。

[0073] 在数字水印添加组件包括用于应用水印的可执行指令的实施方式中,该方法可以

包括使用运行时组件来执行此类指令以对内容应用水印。在数字水印添加组件是配置用于对内容应用数字水印的软件模块的实施方式中,该方法可以包括执行数字水印添加组件以对内容应用水印。

[0074] 在各种实施方式中,用于应用水印的特定运行时组件可以配置用于确保在未对接收的内容应用数字水印的情况下无法使用接收的内容。例如,该方法使用的运行时组件可以配置用于采用上文关于水印强制实施描述的任何技术。可以根据上述方法生成的添加有水印的内容的示例包括图 2B 和图 3 的图像(当然,其他类型的水印也是可能和可以想到的)。

[0075] 图 6 示出了在各种实施方式中用于提供数字水印添加组件的流程图。在一些实施方式中,示出的方法可以经由分发系统(诸如上述分发系统 120)来实现。如框 600 所示,该方法可以包括向远程计算机系统提供数字水印添加组件;该计算机系统可以包括配置用于使用内容的部分的运行时组件。另外,可以与运行时组件独立地向计算机系统提供数字水印添加组件。例如,在某些情况下,在向该计算机系统提供水印添加组件时,运行时组件可能已经安装于远程计算机系统上。在各种实施方式中,数字水印添加组件可以指定用于在内容的部分上应用数字水印的信息(其可以类似于上文关于图 5 描述的信息)。

[0076] 如框 602 所示,该方法可以包括向远程计算机系统提供信息;此类信息可以指定:在未对接收的内容应用数字水印的情况下不能在计算机系统上使用内容的部分。在一些实施方式中,提供此类信息可以包括提供内容许可,其指定:在未对接收的内容应用数字水印的情况下不能在计算机系统上使用该内容。在某些情况下,内容许可可以将此类信息指定为内容的使用规则。在各种实施方式中,可以向客户端系统提供此类信息,客户端系统诸如上述客户端系统 140 或者配置用于实施此类使用规则(例如,对内容强制实施水印应用)的任何其他计算机系统。

[0077] 注意,在利用轻量级数字水印添加组件进行数字版权管理的系统和方法的范围内,可行和可以想到的方法不限于上述示例。在某些情况下,可以从方法中添加或者去除元素,同时保持在利用轻量级水印添加组件进行数字版权管理的系统和方法的精神和范围内。在各种实施方式中,以上关于图 1 的组件描述的任何功能性可以实现为计算机实现的方法的元素,诸如图 5 和图 6 的方法。

[0078] 示例计算机系统

[0079] 在此描述的利用轻量级数字水印添加组件进行数字版权管理的系统和方法的各种实施方式可以在一个或多个计算机系统上执行,一个或多个计算机系统可以与各种其他设备交互。一个此类计算机系统是图 7 所示的计算机系统 700,在各种实施方式中,其可以实现图 1-图 6 所示的任何元素。计算机系统 700 可以能够实现客户端系统或者分发系统的功能性(诸如以上关于图 1 描述的),其可以存储在存储器中作为处理器可执行的程序指令。在示出的实施方式中,计算机系统 700 包括经由输入/输出(I/O)接口 730 耦合至系统存储器 720 的一个或多个处理器 710。计算机系统 700 进一步包括:耦合至 I/O 接口 730 的网络接口 740 以及一个或者多个输入/输出设备 750,该输入/输出设备 750 诸如光标控制设备 760、键盘 770 以及显示器 780。在某些实施方式中,期望可以使用计算机系统 700 的单个实例来实现实施方式,然而在其他实施方式中,可以配置多个此类系统或者构成计算机系统 700 的多个节点以主管各种实施方式的不同部分或者实例。例如,在一个实施方

式中,可以经由计算机系统 700 的一个或者多个节点来实现某些元素,所述一个或者多个节点不同于实现其他元素的那些节点。虽然没有根据细节等级呈现为计算机系统 700(在一些实施方式中,其可以实现客户端系统 140 的功能性),但是分发系统 120 的功能性也可以经由诸如计算机系统 700 的计算机系统来实现。

[0080] 在各种实施方式中,计算机系统 700 可以是包括一个处理器 710 的单处理器系统,或者可以是包括多个处理器 710(例如,两个、四个、八个、或者其他适合数目)的多处理器系统。处理器 710 可以是能够执行指令的任意适合的处理器。例如,在各种实施方式中,处理器 710 可以是通用或者嵌入处理器,该处理器实现多种指令集架构 (ISA) 中的任一项,诸如 x64、PowerPC、SPARC 或者 MIPS ISA 或者任何其他合适的 ISA。在多处理器系统中,每个处理器 710 可以共同实现相同的 ISA,但这不是必须的。

[0081] 系统存储器 720 可以配置用于存储处理器 710 可访问的程序指令 722 和 / 或数据 732。在各种实施方式中,数据 732 可以包括上述任何数据,其包括但不限于:受保护内容 108、内容许可 125、内容 102 和添加有水印的内容 170。在各种实施方式中,可以使用任何适合的存储器技术来实现系统存储器 720,诸如静态随机访问存储器 (SRAM)、同步动态 RAM (SDRAM)、非易失性 / 闪存类型存储器或者任何其他类型的存储器。在示出的实施方式中,实现 DRM 框架的任何元素的程序指令和数据(如上所述)可以存储在系统存储器 720 内。例如,程序指令 722 可以是可执行的用以实现 DRM 组件 162 和水印添加组件 164。在其他实施方式中,可以接收、发送程序指令和 / 或数据,或者将其存储在不同类型的计算机可访问介质、或者独立于系统存储器 720 的类似介质、或者计算机系统 700 之上。

[0082] 在一个实施方式中,I/O 接口 730 可以配置以协调在处理器 710、系统存储器 720 以及设备中的任何外围设备之间的 I/O 流量,所述外围设备包括网络接口 740 或者诸如输入 / 输出设备 750 的其他外围接口。在某些实施方式中,I/O 接口 730 可以执行任何必要的协议、定时或者其他数据变换,以便将数据信号从适用于一个组件(例如,系统存储器 720)的格式转换至适于由另一组件(例如,处理器 710)使用的格式。在某些实施方式中,I/O 接口 730 例如可以包括用于对通过各种类型的外围总线而附接的设备的支持,所述外围总线诸如不同的外围组件互联 (PCI) 总线标准或者通用串行总线 (USB) 标准。在某些实施方式中,I/O 接口 730 的功能例如可以划分成为两个或者多个独立的部分,诸如北桥和南桥。另外,在某些实施方式中,可以将 I/O 接口 730 的某些或者全部功能性(诸如对系统存储器 720 的接口)直接结合到处理器 710 之中。

[0083] 网络接口 740 可以配置以允许在计算机系统 700 和附接至网络(例如,网络 400)的其他设备(诸如,例如分发系统 120 之类的其他计算机系统)之间交换数据,或者在计算机系统 700 的节点之间交换数据。在各种实施方式中,网络接口 740 例如可以支持经由有线或者无线通用数据网络(诸如,任意适合类型的以太网)进行通信;经由电信 / 电话网络(诸如,模拟语音网络或者数字光纤通信网络)进行通信;经由存储区域网络(诸如光纤信道 SAN)进行通信,或者经由任何其他适合类型的网络和 / 或协议进行通信。

[0084] 在某些实施方式中,输入 / 输出设备 750 包括一个或者多个显示终端、键盘小键盘、触摸板、扫描设备、语音或者光学识别设备、或者适用于由一个或者多个计算机系统 600 输入或者访问数据的任何其他设备。多个输入 / 输出设备 750 可以存在于计算机系统 700 中、或者可以分布在计算机系统 700 的各种节点上。在某些实施方式中,类似的输入 / 输

出设备可以独立于计算机系统 700，并且可以通过有线或者无线连接（诸如通过网络接口 740）来与计算机系统 700 的一个或者多个节点交互。

[0085] 在一些实施方式中，示出的计算机系统可以实现上述任何方法（诸如图 5- 图 6 示出的方法）。在其他实施方式中，可以包括不同的元素和数据。在各种实施方式中，示出的计算机系统可以配置用于生成图像和 / 或视频，诸如图 2B 和图 3 的图像（包括此类图像上的水印）。

[0086] 本领域技术人员应该理解，计算机系统 700 仅仅是示意性的，并非旨在限制实施方式的范围。尤其是，计算机系统和设备可以包括可以执行所指示功能的硬件和软件的任意组合，包括计算机、网络设备、因特网工具、PDA、无线电话、寻呼机等。计算机系统 700 还可以连接至未示出的其他设备，或者可以作为独立系统操作。另外，在某些实施方式中，由所示出组件提供的功能性可以在较少的组件中结合或者在其他组件中分布。类似地，在某些实施方式中，还可以不提供所示出某些组件的功能性和 / 或可获得其他附加的功能性。

[0087] 本领域技术人员还应该理解，在使用时，尽管各种项目示出为存储在存储器或者存储设备中，然而出于存储器管理和数据完整性的目的，这些项目或者项目的部分还可以在存储器以及其他存储设备之间传送。可替换地，在其他实施方式中，可以在存储器中或者在其他设备上执行某些或者所有软件组件，并且经由计算机内通信与示出的计算机系统进行通信。某些或者所有系统组件或者数据结构还可以（作为指令或结构化数据）存储在计算机可访问介质上，或者存储在用于由适当驱动装置读取的便携制品上，在上文中示出了各种示例。在某些实施方式中，在独立于计算机系统 700 的计算机可访问介质上存储的指令可以经由传输介质或者经由通信介质（诸如，网络和 / 或无线链接）递送的信号来传送至计算机系统 700，所述信号诸如电信号、电磁信号和 / 或数字信号。各种实施方式可以进一步包括对根据基于计算机可访问介质的上述描述实现数据的和 / 或指令进行接收、发送或者存储。由此，还可以利用其他计算机系统配置来实现此描述的实施方式。

[0088] 各种实施方式可以进一步包括对根据基于计算机可访问介质的上述描述实现数据和 / 或指令进行接收、发送或者存储。一般而言，计算机可访问的介质可以包括诸如磁性介质或者光学介质的存储介质或者存储器介质，例如，盘或者 DVD/CD-ROM、易失性介质或者非易失性介质，诸如，RAM（例如，SDRAM、DDR、RDRAM、SRAM 等）、ROM 等。在一些实施方式中，计算机可访问的介质可以包括传输介质或者经由诸如网络和 / 或无线链路的通信介质递送的信号（诸如电信号、电磁信号或者数字信号）。

[0089] 在不同的实施方式中，在此描述的方法可以在软件、硬件或其组合中实现。另外，可以改变方法的顺序，并且可以添加、重新排序、组合、省略、修改等各种元素。对于受益于本公开的本领域技术人员明显的是，可以做出各种修改和改变。在特定实施方式的上下文中描述了根据实施方式的实现。这些实施方式意在说明而不是限制。多种变化、修改、添加和改进都是可能的。因此，可以为此描述为单个实例的组件提供多个实例。各种组件、操作和数据存储之间的边界在某种程度上是任意的，并且在特定说明的配置的上下文中示出了特定的操作。可以预想功能性的其他分配，并且可以落在所附权利要求的范围内。最后，呈现为示例配置中的分离组件的结构和功能性可以实现为组合的结构或者组件。这些和其他的变化、修改、附加和改进可以落在如所附权利要求中定义的实施方式的范围内。

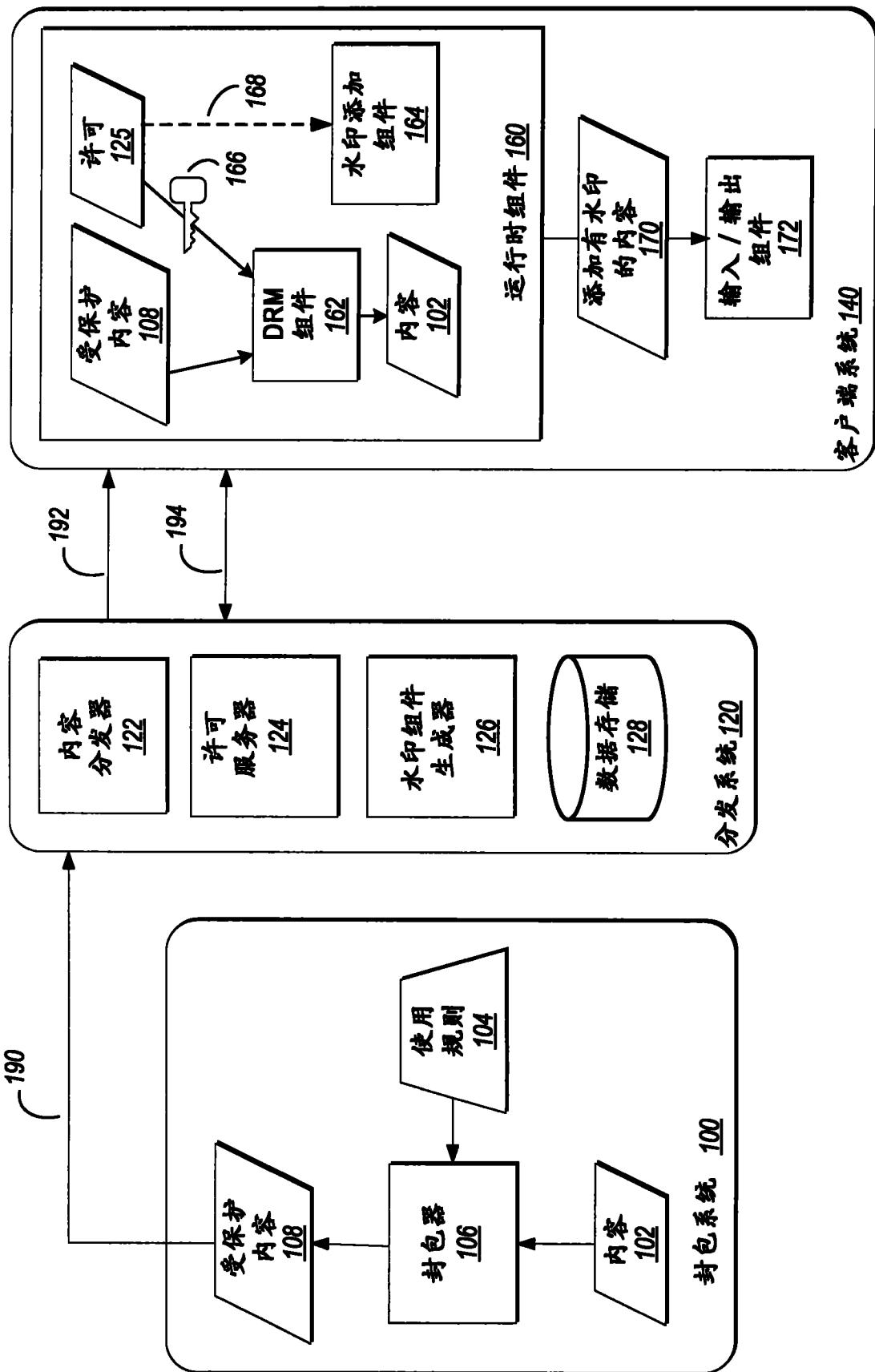
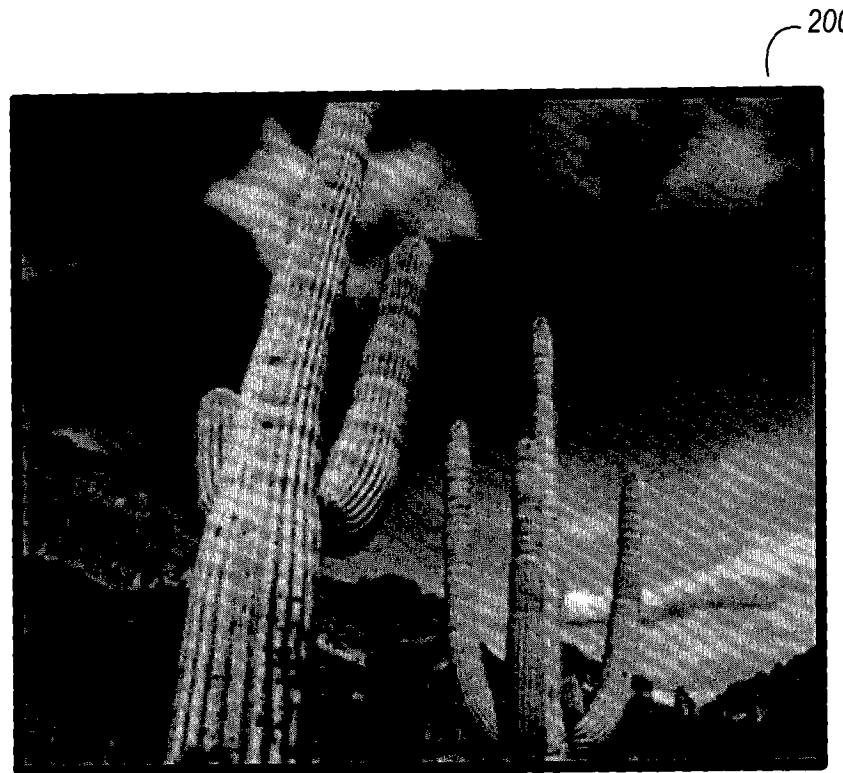
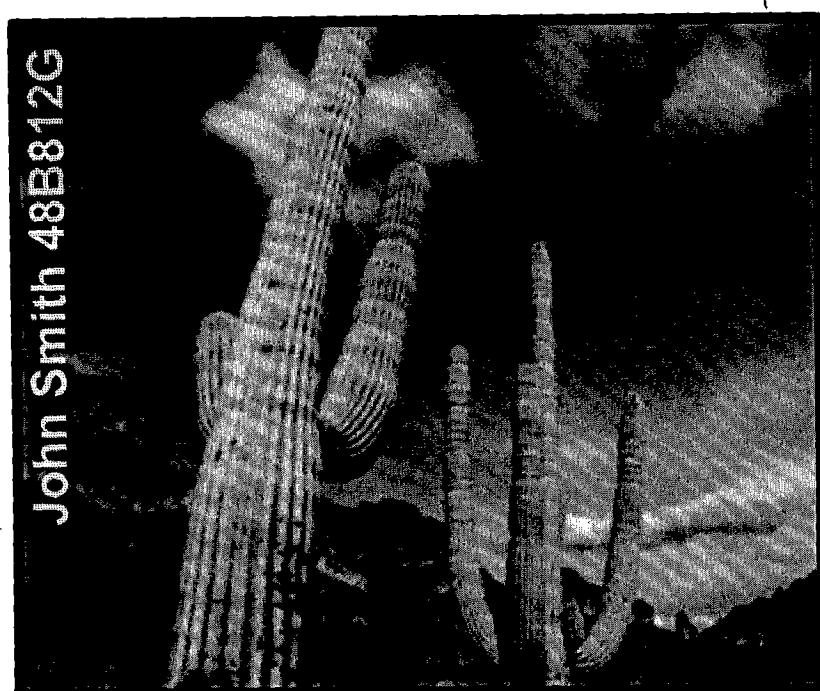


图 1



200

图 2A



210

图 2B

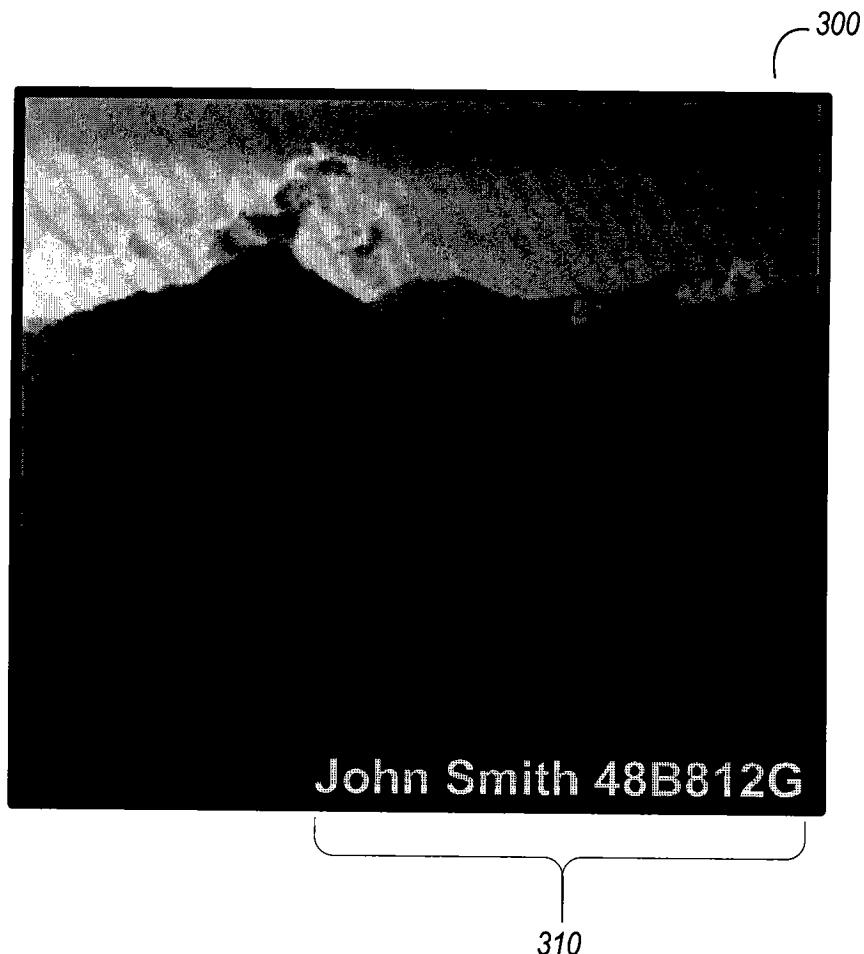


图 3

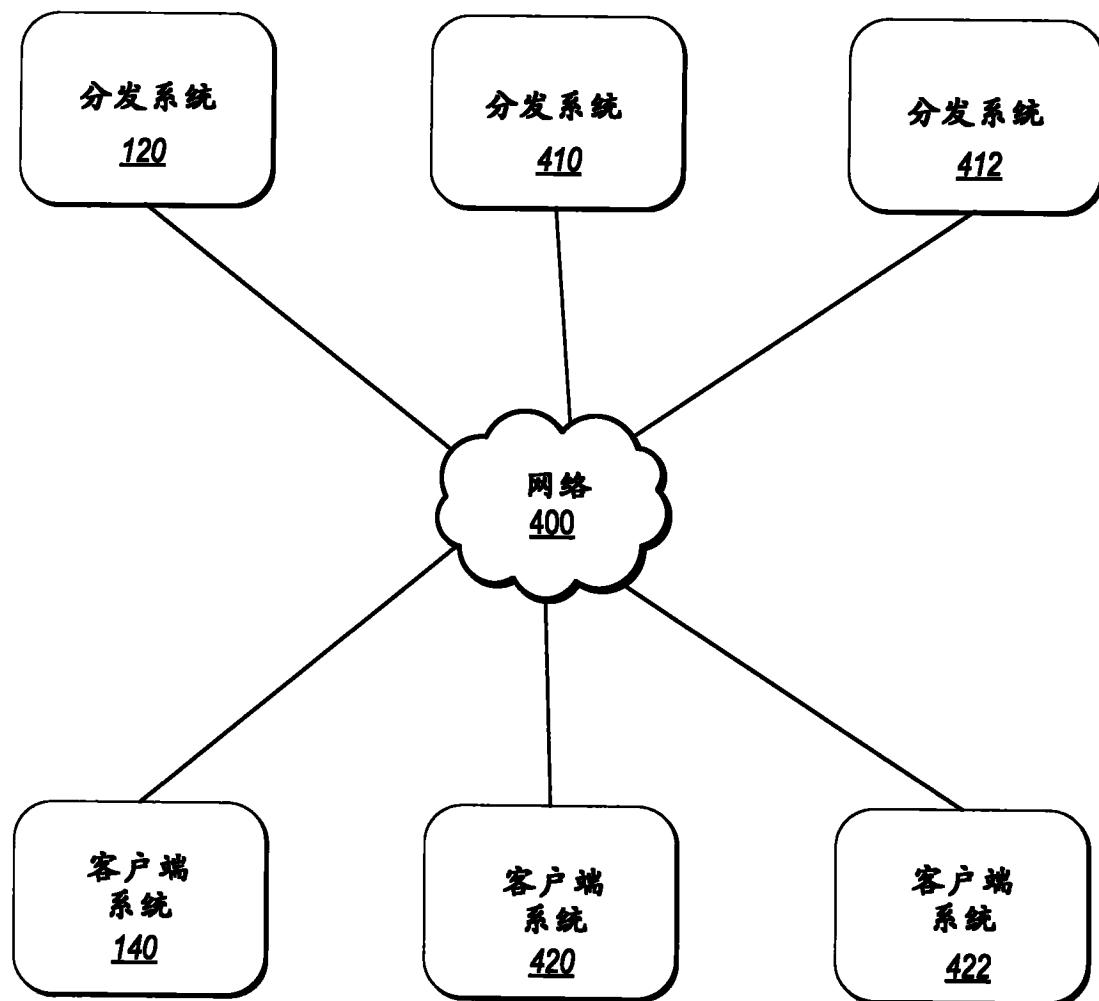


图 4

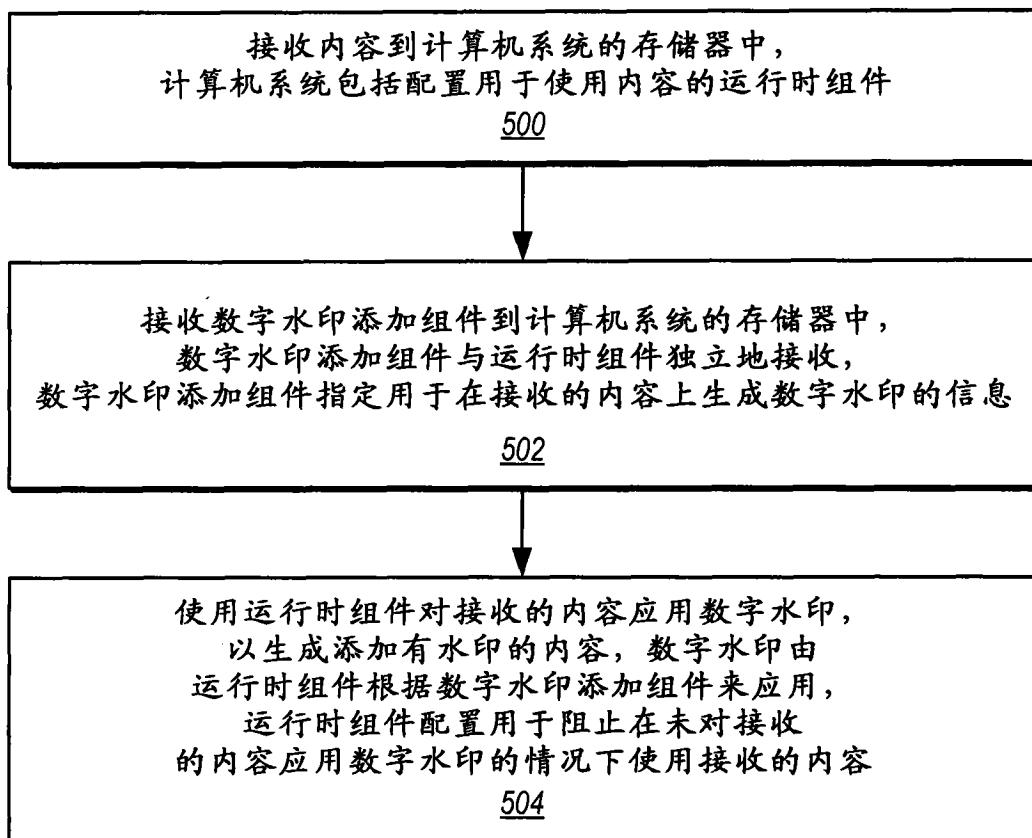


图 5

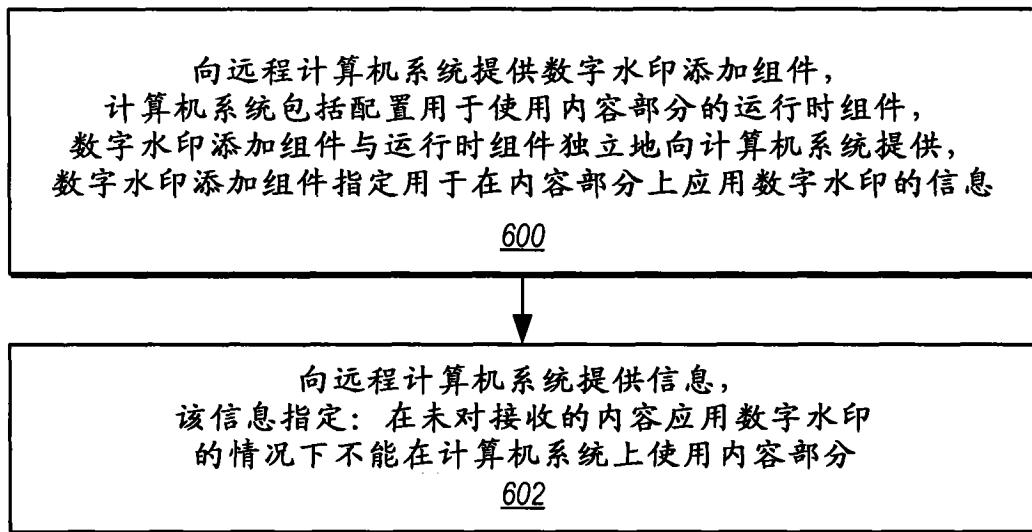


图 6

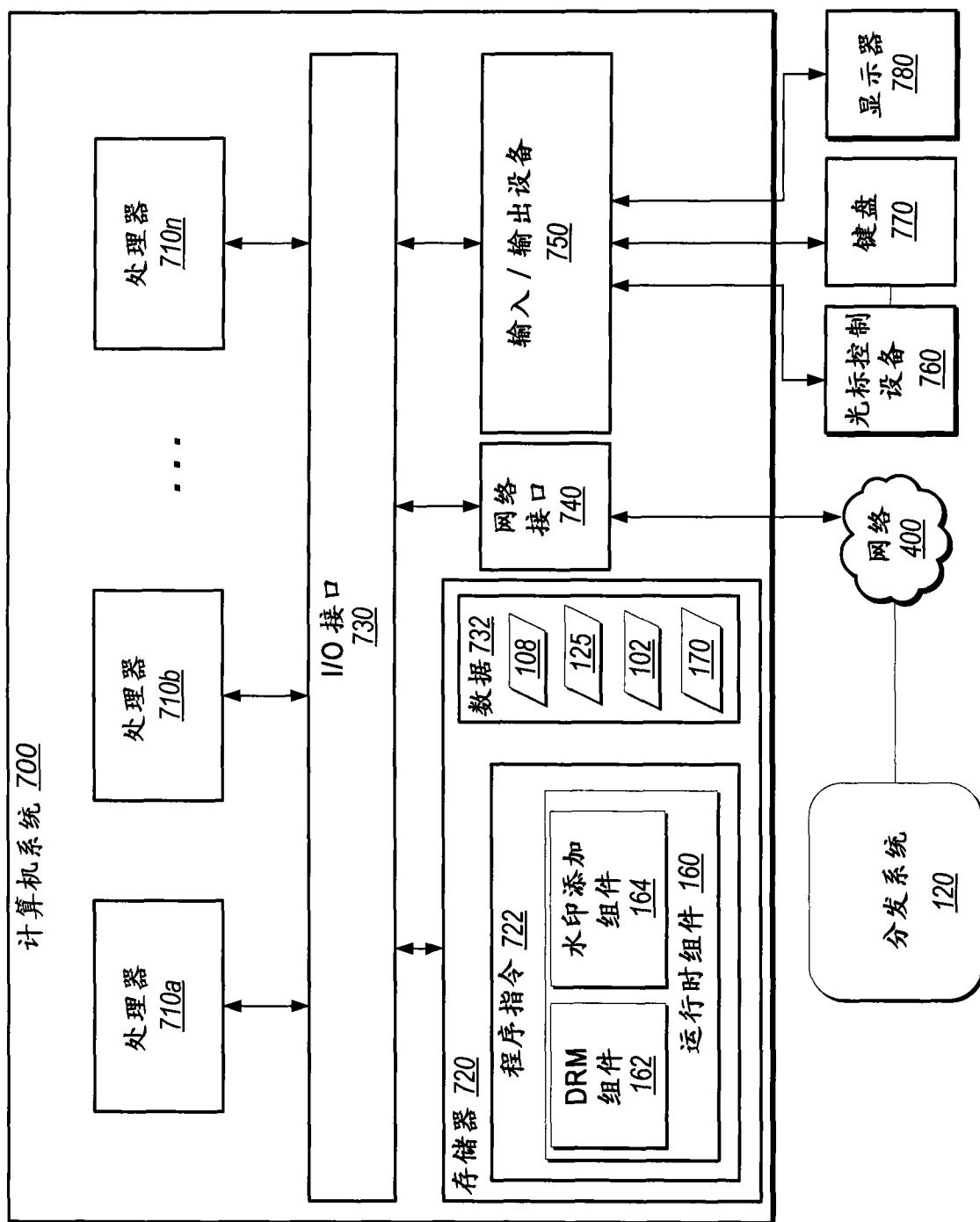


图 7