

(12) 发明专利

(10) 授权公告号 CN 101512479 B

(45) 授权公告日 2012.04.11

(21) 申请号 200780033602.5

G06F 15/173(2006.01)

(22) 申请日 2007.09.11

H04L 9/00(2006.01)

(30) 优先权数据

11/520,273 2006.09.12 US

(56) 对比文件

US 2002112035 A1, 2002.08.15, 全文.

CN 1777851 A, 2006.05.24, 全文.

(85) PCT申请进入国家阶段日

2009.03.11

CN 1538658 A, 2004.10.20, 全文.

CN 1790218 A, 2006.06.21, 全文.

(86) PCT申请的申请数据

PCT/US2007/019897 2007.09.11

审查员 陈安安

(87) PCT申请的公布数据

W02008/033445 EN 2008.03.20

(73) 专利权人 奥多比公司

地址 美国加利福尼亚州

(72) 发明人 J·莱斯特 S·C·戈特瓦尔斯

J·D·普拉维特兹

(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 7/04(2006.01)

G06F 17/30(2006.01)

G06F 7/00(2006.01)

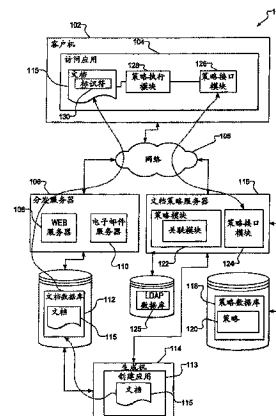
权利要求书 3 页 说明书 9 页 附图 7 页

(54) 发明名称

对数字内容的部分的选择性访问

(57) 摘要

一种方法,包括:接收访问数字内容项目的请求,所述数字内容项目包括多个部分。响应于所述请求,标识分别与所述数字内容项目的所述多个部分相关的多个策略。基于所述多个策略,选择性地允许对所述数字内容项目的所述多个部分的访问。



1. 一种用于选择性地允许对数字内容进行访问的方法,包括:

接收访问数字内容项目的请求,所述数字内容项目包括多个部分,所述请求包括与  
所述数字内容项目相关联的内容标识符,用于标识与所述数字内容项目的多个部分中的每个  
部分相关联的访问控制列表;

响应于所述请求,标识分别与所述数字内容项目的所述多个部分相关的多个策略;以  
及

基于所述多个策略,选择性地允许对所述数字内容项目的所述多个部分的访问。

2. 如权利要求 1 的方法,其中所述访问数字内容项目的请求是从访问应用接收的,所  
述访问应用被配置用于提供对所述数字内容项目的访问。

3. 如权利要求 1 的方法,其中对所述多个策略的标识是使用所述内容标识符执行的。

4. 如权利要求 1 的方法,其中所述请求包括与请求访问所述数字内容项目的实体相关  
的实体标识符,并且其中选择性地允许对所述多个部分的访问是使用所述实体标识符进  
行的。

5. 如权利要求 4 的方法,其中所述实体标识符是包括至少一个以下标识符:标识用户  
的用户标识符,标识机器的机器标识符,以及标识应用的应用标识符。

6. 如权利要求 1 的方法,其中选择性地允许访问包括选择性地提供密钥,以允许对所  
述数字内容项目的所述多个部分的访问。

7. 如权利要求 1 的方法,其中选择性地允许访问包括:针对所述多个部分的至少一个  
部分选择性地提供至少一个权限,所述至少一个权限选自:查看、编辑、打印、注释和表格填  
写权限。

8. 如权利要求 7 的方法,其中选择性地允许访问包括:在将所述多个部分的至少一个  
限定部分呈现给用户时,选择性地视觉上对其进行编校。

9. 一种用于选择性地允许对数字内容进行访问的系统,包括:

接口模块,用于接收访问数字内容的请求,所述数字内容包括多个部分,所述请求包括  
与所述数字内容相关联的内容标识符,用于标识与所述数字内容的多个部分中的每个部分  
相关联的访问控制列表;以及

策略模块,用于响应于所述请求来标识分别与所述数字内容的所述多个部分相关的多  
个策略,以及基于所述多个策略来选择性地允许对所述数字内容的所述多个部分的访问。

10. 如权利要求 9 的系统,其中所述接口模块用于通过网络从访问应用接收访问所述  
数字内容的请求,其中所述访问应用被配置用于提供对所述数字内容的访问。

11. 如权利要求 9 的系统,其中所述策略模块用于使用所述内容标识符来标识所述多  
个策略。

12. 如权利要求 9 的系统,其中所述请求包括与请求访问所述数字内容的实体相关  
的访问标识符,并且其中所述策略模块用于使用所述访问标识符来选择性地允许对所述数  
字内容的所述多个部分的访问。

13. 如权利要求 9 的系统,其中所述策略模块用于选择性地提供密钥,以允许对所述数  
字内容的所述多个部分的访问。

14. 如权利要求 9 的系统,其中所述策略模块用于针对所述数字内容的所述多个部分  
的至少一个部分选择性地提供至少一个权限,所述至少一个权限选自:查看、编辑、打印、注

释和表格填写权限。

15. 如权利要求 14 的系统,其中所述策略模块选择性地允许对数字内容项目的多个部分的至少一个限定部分进行编校。

16. 一种用于将访问说明与数字内容项目的部分相关联的方法,包括:

呈现数字内容项目的多个部分以供选择;

接收对所述数字内容项目的所述多个部分的第一部分的选择;

至少接收关于所述第一部分的第一访问说明;

接收对所述数字内容项目的所述多个部分的第二部分的选择;

至少接收关于所述第二部分的第二访问说明;以及

将所述第一访问说明和第二访问说明分别与所述数字内容项目的所述第一部分和第二部分进行关联。

17. 如权利要求 16 的方法,其中呈现所述多个部分包括:解析所述数字内容项目以标识所述多个部分,以及在呈现所述多个部分时从视觉上区分所述多个部分的至少一个。

18. 如权利要求 16 的方法,其中呈现所述多个部分包括:接收标识所述数字内容项目的所述多个部分的用户输入。

19. 如权利要求 16 的方法,其中所述第一访问说明包括至少一个以下权限:查看、编辑、打印、注释和表格填写权限。

20. 如权利要求 16 的方法,其中所述第一访问说明标识将应用所述第一访问说明的至少一个实体。

21. 如权利要求 20 的方法,其中所述至少一个实体来自包括用户、机器和应用的实体群组。

22. 如权利要求 16 的方法,其中所述第一访问说明标识所述第一访问说明有效的至少一个时间段。

23. 如权利要求 22 的方法,其中所述至少一个时间段包括相对时间段和绝对时间段的至少一个。

24. 如权利要求 16 的方法,其中所述关联包括:生成数字内容项目标识符,并至少将所述第一访问说明与所述数字内容项目标识符相关联地存储。

25. 如权利要求 16 的方法,其中所述关联包括:针对所述数字内容项目的所述多个部分的每一部分生成部分标识符,以及将所述第一部分标识符与所述第一访问说明相关联地存储,并将所述第二部分标识符与所述第二访问说明相关联地存储。

26. 如权利要求 16 的方法,其中所述第一访问说明和第二访问说明中的每一个都是策略。

27. 如权利要求 16 的方法,其中所述第一访问说明和第二访问说明中的每一个都包括密钥,选择性地使所述密钥可用,以允许对所述第一部分和第二部分的访问。

28. 一种用于将访问说明与数字内容的部分相关联的系统,包括:

接口模块,用于:

呈现数字内容的多个部分以供选择;

接收对所述数字内容的所述多个部分的第一部分的选择;

至少接收关于所述数字内容的所述多个部分的所述第一部分的第一访问策略;

接收对所述数字内容的所述多个部分的第二部分的选择 ;以及至少接收关于所述数字内容的所述多个部分的所述第二部分的第二访问策略 ;以及关联模块,用于将所述第一访问策略和第二访问策略分别与所述数字内容的所述第一部分和第二部分进行关联。

29. 如权利要求 28 的系统,其中所述接口模块用于 :解析所述数字内容以标识所述多个部分,以及关于所述数字内容的其他部分在视觉上区分所述多个部分的至少一个。

30. 如权利要求 28 的系统,其中所述接口模块用于 :接收标识所述数字内容的所述多个部分的至少一个的用户输入。

31. 如权利要求 28 的系统,其中所述第一访问策略包括至少一个以下权限 :查看、编辑、打印、注释和表格填写权限。

32. 如权利要求 28 的系统,其中所述第一访问策略标识将应用所述第一访问策略的至少一个实体。

33. 如权利要求 32 的系统,其中所述至少一个实体来自包括用户、机器和应用的实体群组。

34. 如权利要求 28 的系统,其中所述第一访问策略标识将要应用所述第一访问策略的至少一个时间段。

35. 如权利要求 28 的系统,其中所述关联模块用于生成数字内容标识符,并至少将所述第一访问策略和第二访问策略与所述数字内容标识符相关联地存储。

36. 如权利要求 28 的系统,其中所述关联模块用于 :针对所述数字内容的所述多个部分的每一部分生成部分标识符,以及将第一部分标识符与所述第一访问策略相关联地存储,并将第二部分标识符与所述第二访问策略相关联地存储。

## 对数字内容的部分的选择性访问

### [0001] 优先权要求

[0002] 本PCT申请要求2006年9月12日提交的、题目为“SELECTIVEACCESS TO PORTIONS OF DIGITAL CONTENT”的美国专利申请序列号11/520,273的权益,根据35U.S.C. § 120或365(c),要求其优先权,并且其全部内容通过参考而在此并入。

### 技术领域

[0003] 本申请涉及用于选择性地允许对数字内容进行访问的方法和系统,在一个示例性实施方式中,涉及用于实现对数字内容项目的部分进行基于策略的访问的系统。

### 背景技术

[0004] 由于数字内容(例如,电子相片、音乐、视频和文档)的容量以指数级速率激增,对这种内容的有效管理和控制变得日益重要。数字版权管理(DRM)通常是指用于执行对数字数据或内容的访问进行控制的预定义策略的多种技术。通常,DRM对数字内容特定实例(或称项目)可能伴生的使用限制的描述、分层、分析、评价、交易、监控和执行进行处理。

[0005] 当前,大量DRM技术可用于保护多种不同类型的数字内容。例如,便携式文档格式(PDF)是由加利福尼亚州圣何塞市的Adobe系统公司开发的开放标准文件格式,其提供了限制文档打印的能力。Adobe系统公司还开发了**Adobe® LiveCycle Policy Server™**软件,其支持对业务关键电子文档进行管理和监控,以及应用策略来控制对这种文档的访问和使用。类似地,Macrovision公司开发了大量的电子复制保护机制,这些机制可以用来保护视频和DVD数字内容。从很多在线商店(例如,Apple计算机公司的iTunes音乐商店)购买的音频文件受控于各种DRM机制,这些机制限制可以播放特定音频文件的设备的数量。类似地,电子图书的制造者利用DRM来限制可以观看电子图书的计算机的数量,甚至是电子图书的可观看次数。

### 附图说明

[0006] 通过示例而非限制的方式,在附图中说明了某些实施方式,在附图中:

[0007] 图1是示出了根据示例性实施方式的访问管理系统框图。

[0008] 图2是示出了根据示例性实施方式的可以部署在访问管理系统内的策略的数据结构。

[0009] 图3示出了根据示例性实施方式的用于将访问说明与数字内容项目的部分进行关联的方法流程图。

[0010] 图4是示出了可以用以将访问说明与数字内容项目的至少部分进行关联的示例性用户接口的用户接口示意图。

[0011] 图5是示出了根据示例性实施方式的用于基于各个策略来选择性地允许对数字内容项目的多个部分的每一部分进行访问的方法流程图。

[0012] 图6是示出了示例性数字内容项目(包括利用在此描述的任一方法对其访问进行

限制的部分)的用户接口示意图。

[0013] 图 7 是以计算机系统的示例性形式示出一种机器的框图,在该机器中,可以执行指令以使该机器执行在此描述的任何方法,或者在该机器中,可以存储在此描述的任一示例性数据结构。

### 具体实施方式

[0014] 在以下描述中,出于说明的目的而给出了众多特定细节,以便提供对某些示例性实施方式的全面理解。然而,对于本领域技术人员而言,本发明可以脱离这些特定细节而实现是显然的。

[0015] 例如,实施方式可以实现为单机应用(例如,不具有任何网络能力)、客户端-服务器应用或者端到端(或者分布式)应用。例如,除了通过传统渠道销售或许可以外,可以通过服务化软件(SaaS)、应用服务提供者(ASP)或者公用计算提供者来部署实施方式。

[0016] 术语“内容”应当包括可以呈现(例如,可视呈现或者可听呈现)给消费者的任何数字数据,并且可以包括文档、图像、视频和音频内容,这些仅是示例。内容的“部分”应当包括被定义为或者可辨别为部分或者份额的、内容的任何部分或份额。例如,部分可以根据内容自身的特征(例如,电子文档的段落)而自动地辨别,或者可以由用户手动地定义(例如,用户在文档中选择词的集合,或者用户选择数字图像的部分)。

[0017] 在一个示例性实施方式中,访问管理系统包括用于将数字内容项目(例如,数字文档、照片、视频或音频文件)的多个部分呈给用户以供选择的接口模块。此外,该接口模块接收对数字内容项目的多个部分之一的选择,还接收关于数字内容项目的多个部分的选定部分的访问说明。访问管理系统还包括用于将访问说明与数字内容项目的多个部分的选定部分进行关联的关联模块。

[0018] 根据另一示例性实施方式,系统包括接口模块,用于接收对包括多个部分的数字内容项目进行访问的请求。响应于该请求,访问管理系统的策略模块识别分别与数字内容项目的多个部分有关的多个策略。基于该多个策略,策略模块进一步选择性地允许对数字内容项目的多个部分的每一部分进行访问。

[0019] 图 1 是示出了根据示例性实施方式的访问管理系统 100 的框图。尽管在访问管理数字内容项目(电子文档示例性形式的)上下文中描述了示例性访问管理系统 100,但是应当理解,其他实施方式可以进行操作以管理多种不同类型的数字内容项目(例如,数字照片、视频文件或音频文件)中的任意一个。访问管理系统 100 包括客户机 102,其容纳有文档访问应用 104。客户机 102 通过网络 105 可通信地耦合至文档分发服务器 106,其示例性形式为 web 服务器 108 和电子邮件服务器 110。文档分发服务器 106 继而可通信地耦合至文档数据库 112,并可进行操作以使存储在文档数据库 112 中的数字文档(作为数字内容项目的示例)经由网络 105 可供文档访问应用 104 使用。例如,基于文档发送者的指令或者基于客户机 102 用户的请求,可以通过电子邮件服务器 110 用电子邮件将文档从文档数据库 112 发送至文档访问应用 104。还可以利用许多公知的基于 web 的递送协议(例如,超文本传输协议(HTTP)或者文件传输协议(FTP))之一来将文档通过 web 服务器 108 从文档数据库 112 递送至文档访问应用 104。

[0020] 文档数据库 112 继而可以填入由文档生成机 114 生成的文档 115。为此,文档生成

机 114 可以容纳许多创建（例如，文档创作）应用 113 的任意一个（例如，Microsoft Word 或者 Adobe **Acrobat®**），这些应用使用户能够生成或者编辑内容项目，和 / 或使用户能够将访问说明（例如，策略）与内容项目的部分进行关联。

[0021] 尽管在图 1 所示的示例性实施方式中，示出的是通过网络 105、经由电子传输将文档递送至文档访问应用 104，但是应当理解，文档可以以任何方式（诸如，通过将文档置于压缩盘 (CD) 上邮寄给客户机 102 的操作者）递送至文档访问应用 104。

[0022] 文档访问应用 104 还可以访问文档策略服务器 116，该服务器 116 进行操作以管理并监控对文档数据库 112 中文档的访问。具体地，文档策略服务器 116 可以访问存储有文档策略 120 集合的文档策略数据库 118。文档策略服务器 116 使用文档策略 120 以例如在线和离线两种方式来控制对电子文档的访问及其使用。除了通过利用文档策略 120 对电子文档的控制进行维护之外，文档策略服务器 116 还支持对文档策略 120 的创作。为此，文档生成机 114 被示为可以对文档策略服务器 116 进行访问，并且可以相应地允许文档作者指派权限，该权限规定了对特定文档的访问级别（例如，对相关文档进行打印、复制、添加页面或者移除页面、转发或者保存等的限制或允许）。文档策略服务器 116 还促进对与特定文档相关联的文档策略进行管理，从而允许作者在分发文档（例如，经由文档发布服务器 106）之后改变针对文档的策略。

[0023] 更具体地研究文档策略服务器 116，策略模块 122 促进对文档策略 120 的创建和更新，以及将特定文档策略 120 与特定文档 115 进行关联。文档策略服务器 116 还包括一个或多个策略接口模块 124，用于促进文档策略服务器 116 与文档策略数据库 118、文档生成机 114 和文档访问应用的对接。

[0024] 在一个示例性实施方式中，文档策略服务器 116 可以访问轻量目录访问协议 (LDAP) 数据库 125，以便使策略模块 122 能够确定用户是否属于有权访问数字内容项目相关部分的群组（例如，单位层级中的群组或级别）。

[0025] 返回文档访问应用 104，策略接口模块 126 使策略执行模块 128 能够针对特定文档 115 来向文档策略服务器 116 发出对与文档 115 相关联的一个或多个策略 120 的请求。这种请求例如可以包括与特定文档 115 相关联的标识符 130，以便使文档策略服务器 116 能够获取与相关文档 115 相关联的适当文档策略 120。

[0026] 在提供对特定文档 115 的任何访问之前，文档访问应用 104 还可以请求用户标识（例如，用户名 / 密码的配对、生物学标识或者一次性密码、令牌或者智能卡）。用户标识可以在本地由策略执行模块 128 使用，以选择性地提供对文档 115 的部分的访问；或者在另一实施方式中，用户标识可以传送至文档策略服务器 116，该服务器 116 能够获取并传送如下信息（例如，密钥），该信息允许策略执行模块 128 有选择性地提供对文档 115 的部分的访问。因此，在一个实施方式中，以用户标识符为示例性形式的实体标识符可以在服务器侧使用，以便确定针对特定电子文档 115 的权限；或者在另一实施方式中，实体标识符可以在客户端侧使用，以基于传送至文档访问应用 104 的完整策略来确定权限。这样，可以实现策略的在线和离线执行。在各种实施方式中，还可以使用标识机器的机器标识符和 / 或标识应用的应用标识符来确定针对数字内容项目的权限。然而，出于说明的目的，以下讨论用户标识符。

[0027] 图 2 是示出了具有与其相关的一个或多个内容策略 208 的示例性数字内容项目

200(例如,数字文档、照片、视频或音频文件)的框图。可以通过将内容策略 208 与用于相关数字内容项目 200 的内容标识符 210 相关联地存储在数据库中,来实现数字内容项目 200 与内容策略 208 之间的关联。

[0028] 数字内容项目 200 被示出为包括多个部分 202、204、206,这些部分可以互斥或者可以重叠(例如,共享公共数字内容)。在本说明书中的其他部分,将更全面地描述数字内容项目部分的定义和/或标识的示例。

[0029] 内容策略 208 例如可以包括访问策略 212、期满策略 228 和许多其他策略 230 中的任何一个(例如,分发策略等)。以访问策略 212 为例,唯一标识特定数字内容项目 200 的特定内容标识符 210 可以与多个访问控制列表 214 相关联,每个访问控制列表 (ACL) 214 与数字内容项目的相应部分相关联。因而,每个访问控制列表 214 包括标识与其关联的相应部分的部分标识符。

[0030] 每个访问控制列表 214 继而针对数字内容项目 200 相应部分的访问规定了多个控制。例如,访问控制列表 214 可以与数字内容项目 200 的部分 202 相关联,并且针对此部分规定访问控制。在访问控制列表 214 中规定的访问控制可以是特定于实体的(例如,由特定用户标识符 220 标识),并且可以定义查看权限、编辑权限、打印权限、注释权限和表格填写权限,这些仅是示例。每个权限 224 继而可以与相应密钥(例如,对称或不对称密钥)226 相关联,其中相关密钥 226 可由访问应用使用以解密数字内容项目的相应部分,并且根据相关联的权限来允许访问相应部分。在一个实施方式中,与权限相关联的每个密钥可以是不对称密钥,从而使同一密钥可以用来对相关部分进行加密和解密。

[0031] 另外,与每个部分相关联的访问控制列表 214 包括时间(与时间有关的)属性 222,其例如规定了相关部分有效的时段,或者一个或多个权限有效的时段。反映在时间属性 222 中的时段可以是绝对的(例如,参照固定日期进行表示)或者相对的(例如,参照事件进行表示)。

[0032] 图 3 是示出了根据本发明示例性实施方式的将访问说明(例如,策略 120 或者提供关于内容项目访问的限制或权限的某些其他说明)与具有多个部分的数字内容项目的至少一个部分进行关联的方法 300 的流程图。

[0033] 方法 300 开始于 302,并进行到操作 304,在 304 处,创建应用 113 接收数字内容项目 200。例如,在数字内容项目是 PDF 文档的情况下,PDF 文档可以加载到 PDF 阅读器应用(例如,Adobe®Acrobat®)的应用存储器中。作为作者使用创建应用 113 进行创作的结果、从与生成机 114(创建应用 113 在其上执行)相关联的本地存储器获取的结果或者由创建应用 113 通过网络从远程存储位置(例如,数据库 112)获取的结果,可以将内容项目 200 获取到应用存储器中。

[0034] 在操作 306,标识数字内容项目 200 的多个部分。在各种实施方式中,对多个部分的标识可以自动地或手动地执行。例如,当数字内容项目 200 是电子文档的情况下,可以自动地将段落标识为电子文档的各个部分。类似地,在电子内容项目 200 是数字照片的情况下,可以使用色彩或其他图像特征的转变来自动地标识数字图像的部分。在另一示例中,在数字内容项目 200 是视频的情况下,可以使用场景渐变技术来标识视频的不同部分,每个部分都包括一个视频帧序列。在又一实施方式中,在数字内容项目 200 是音频文件的情况下,可以使用音频特征的增量来自动定义音频文件的部分。

[0035] 进一步地,在数字内容项目 200 的多个部分被手动定义的情况下,创建应用 113 可以提供用户可借以选择、指示或者定义数字内容项目 200 的部分的多种方法中的任何一种。例如,这可以通过将数字文本的部分高亮显示、利用图像创建应用 113(例如,Adobe® Photoshop®)提供的各种手动蒙板定义工具、使用多种视频编辑应用(例如,包括在 Adobe®产品组中的那些应用)提供的剪接工具或者数字音频编辑器计算机程序(例如,Adobe® Audition®程序)提供的音频选择工具来实现。例如,对于音频数字数据,音频数据的部分的标识可以包括标识一起构成合成音频文件的多个音轨。

[0036] 在操作 308,创建应用 113 可以按照视觉上(或者其他的)区分数字内容项目 200 的一个或多个部分的方式来呈现这些部分。例如,可以利用注释(例如,高亮显示或者任何其他视觉上的区分特征)来区分数字内容项目的部分,使得用户能够轻易地分辨出数字内容项目 200 的部分,以实现选择的目的。

[0037] 在操作 310,创建应用 113 接收对数字内容项目 200 的部分的选择。此选择可以通过创建应用 113 的接口(例如,图形或音频用户接口)接收。

[0038] 在操作 312,创建应用 113 接收关于选定部分的访问说明(例如,策略)。对访问说明的接收可以包括:对访问说明进行定义、创建或创作(例如,如参照图 2 所描述的,创作访问策略 212),或者对预先存在的访问说明进行手动或自动选择。为此,访问说明可以包括访问控制列表(ACL),该 ACL 标识了按照访问说明而被授予不同程度访问权或权限的实体(例如,用户或者用户组)。在一个示例性实施方式中,创建应用 113 可以经由策略服务器 116 访问 LDAP 数据库 125,以获取用户列表和组织信息,可以将该用户列表和组织信息呈现给用户,从而使用户能够便利地识别和选择访问权和权限所属的用户(或者,用户群组)。

[0039] 除了定义各种权利、权限或限制以外,访问说明还具有与其相关联的一个或多个密钥,和生存时间(TTL)或者定义访问说明时间特征的其他探究(exploration)策略。

[0040] 在操作 314,创建应用 113 将在操作 312 处接收的访问说明与在操作 310 处选择的数字内容项目的部分进行关联。此关联可以通过与策略服务器 116 的合作实现,例如,通过指示策略服务器 116 将访问说明(例如,访问策略 212)与内容标识符 210 相关联地存储于策略数据库(例如,文档策略数据库 118)中。具体地,在示例性实施方式中,策略模块 122 可以部署所包括的关联模块,以将内容标识符 210 与一个或多个访问说明相关联地存储于策略数据库 118 中。应当理解,可以以任意多种方式来实现访问说明与数字内容项目的选定部分的关联。

[0041] 在判定操作 316,确定是否还要或将要接收对数字内容项目 200 部分的任何其他用户选择。例如,可以提示创建应用 113 的用户:确定是否还有其他访问说明要与数字内容的任何其他部分进行关联。如果判定操作 316 处的确定是肯定的,则方法 300 循环回操作 310,接收对数字内容项目其他部分的选择;随后,方法 300 循环回操作 312、314 和 316。

[0042] 另一方面,如果在操作 316 处的确定是否定的,则继而在操作 318,将数字内容项目 200 分发给消费者或使其可用于分发给消费者。例如,参照图 1,文档 115 可以被上传至文档数据库 112,以经由 web 服务器 108 或者电子邮件服务器 110 分发给消费用户的访问应用 104。更具体地,在文档生成机 114 上生成文档 115 的作者用户可以规定:相关文档 115 将经由电子邮件服务器 110、通过电子邮件分发给选择的用户群组。方法 300 随后终止于 320。

[0043] 图 4 是示出了根据示例性实施方式的可以例如由创建应用 113 在方法 300 的执行中呈现给作者用户的访问说明接口 400 的用户接口示意图。访问说明接口 400 可以提供数字内容项目 402 (例如, 电子文档) 的可视呈现, 其中各部分 404、406、408 在视觉上有所区别。接口 400 还支持用户对一个或多个部分 (例如, 图 4 中所示将被选择的部分 404) 的选择。

[0044] 接口 400 进一步包括权限对话框 410, 其包含可以针对数字内容项目 200 的选定部分而应用的权限列表。列表中的每个权限条目伴有复选框, 例如, 其允许用户从列表选择一个或多个权限。

[0045] 用户限制对话框 412 包括组输入域 414, 作者用户可以在其中输入可对其应用权限对话框 410 中标识的权限的用户群组 (例如, 单位内的某个组、等级或级别)。进一步地, 个体输入域 416 使作者用户可以单独地标识可对其应用权限的用户。在一个示例中, 可以基于策略服务器 116 从 LDAP 数据库 125 获取并传送给创建应用 113 的信息, 使用呈现群组 / 或用户的列表的下拉菜单来填写输入域 414 和 416。

[0046] 时间限制对话框 418 使作者用户可以通过输入域 420 提供针对下述内容的时间限制: 权限对话框 410 中标识的权限, 用户限制对话框 412 中标识的用户, 或者内容项目的选定部分。在示例性实施方式中, 对话框 410、412 和 418 的输入可以共同定义将关于数字内容项目 402 的部分而定义的访问说明 (例如, 策略)。

[0047] 接口 400 进一步包括“定义”按钮 422, 用户可以选择其来将定义的访问说明与数字内容项目 402 的选定部分相关联地存储。例如, 响应于用户选择了“定义”按钮 422, 针对内容项目 402 的一个或多个部分的访问控制列表 (ACL) 可以与数字内容项目 402 唯一的内容标识符相关联地存储。

[0048] 图 5 是示出了根据示例性实施方式的用于根据与多个部分的至少一个部分相关联的访问说明 (例如, 策略) 来选择性地允许对数字内容项目 200 的多个部分的每一部分进行访问的方法流程图。

[0049] 方法 500 开始于 502, 并且进行至操作 504, 在此将包括多个部分的数字内容项目接收 (例如, 加载) 到访问应用 104 中, 并且获取与数字内容项目 200 相关联的内容标识符 210。应当理解, 可以用各种方式实现对内容标识符 210 的获取。例如, 内容标识符 210 可以简单地是数字或字母数字标识符, 其可以作为与数字内容项目 200 相关联的元数据的一部分。备选地, 内容标识符 210 可以例如利用哈希函数、基于包括在数字内容项目 200 中的数据而生成。这样, 内容标识符 210 可以用来确认: 在内容标识符 210 生成以后, 数字内容项目未被修改过。

[0050] 在操作 506, 访问应用 104 可以将用户标识符提示给用户。为此, 可以向用户显示对话框, 以便提示用户输入用户名和密码, 用于验证针对数字内容项目 200 而被赋予用户的访问权或权限。当然, 在操作 506, 可以获得很多其他用户标识符, 诸如以指纹为示例性形式的生物学标识符, 或者存储在属于用户的令牌上的数字标识符。

[0051] 在操作 508, 访问应用 104 向策略服务器 (诸如, 文档策略服务器 116) 传送请求, 该请求包括在操作 504 和 506 处获取的内容项目标识符和用户标识符。

[0052] 在操作 512, 在策略服务器 116 接收访问请求, 而后, 在操作 514, 利用内容标识符 210, 策略模块 122 标识多个策略 120, 每个策略分别与数字内容项目 200 的多个部分之一相

关。例如,内容标识符 210 可以用来识别与数字内容项目 200 的多个部分的每个部分相关联的访问控制列表 (ACL) 214。

[0053] 在操作 516,针对特定部分,策略模块 122 随后可以确定:按照用户限制,是否允许与用户标识符相关联的用户访问相关部分。为此,策略模块 122 可以利用包括在用户标识符中的认证信息(例如,用户名和密码,或者生物学标识符)来认证相关用户,并确定是否允许该用户访问(例如,查看、编辑、打印、注释或者否则访问)数字内容项目 200 的相关部分。用户认证可以包括:访问 LDAP 数据库 125 以确定用户的属性(例如,单位内的身份)。

[0054] 如果在判定操作 516 处的确定是肯定的,则方法 500 进行至判定操作 518,在此确定按照时间限制(例如,由时间属性 222 规定)是否允许访问。例如,时间属性 222 可以规定:文档的相关部分仅在特定日期之前存在,而后相关部分不再有效,并且因此禁止对其进行访问。

[0055] 如果在判定操作 518 处的确定是否定的,则在操作 520,策略模块 122 可以按照访问控制列表(或者其他策略或访问说明)来识别用户允许的访问类型,并将适当的密钥包括在将要传送给访问应用的密钥组(bundle)中。为此,如上述参照图 2 所述,每个权限可以与唯一的密钥相关联,以便针对数字内容项目的相关部分来“解锁”某些功能或访问能力。

[0056] 在判定操作 522,确定相关数字内容项目 200 是否包括其他部分,这例如是通过确定是否存在其他访问控制列表 (ACL) 与相关内容标识符 210 相关联。如果是,则方法 500 循环回判定操作 516。应当注意,如果在判定操作 516 或 518 处的确定是否定的,则方法 500 进行至判定操作 522。

[0057] 在操作 524 处,策略服务器 116 随后例如分别利用策略服务器 116 和访问应用 104 的接口模块 124 和 126,将在操作 522 处生成的密钥组传送给访问应用 104。

[0058] 在操作 526,访问应用 104 通过接口模块 126 接收密钥组,并通过策略执行模块 128 来传送这些密钥。接着,策略执行模块 128 利用这些密钥对数字内容项目 200 的部分进行解密,从而选择地允许对数字内容项目 200 的多个部分的不同程度或类型的访问。方法 500 随后终止于 528。

[0059] 尽管在上述示例性实施方式中将策略服务器 116 上的策略模块 122 描述为执行操作 516-522,但是应当理解,在另一实施方式中,驻留在访问应用 104 本地的策略执行模块 128 可以执行这些操作的一些或全部。在此示例性实施方式中,策略服务器 116 可以简单地操作以识别适用于特定数字内容项目的策略集合,并将这些策略传送给本地策略执行模块 128。本地策略执行模块 128 随后可以执行与上文关于操作 516-522 描述的那些操作相类似的操作,以便生成用于解密的密钥集合,并提供对数字内容项目部分的各种程度的访问。

[0060] 图 6 是示出了根据示例性实施方式的呈现接口 600,可以借由该接口选择性地允许或禁用对数字内容部分的访问。具体地,接口 600 以电子文档 602 的形式示出了数字内容项目 200 的表示,在该文档内,第一段 604 被示为正在编校、第二段 606 被示为可查看但不可编辑,以及第 3 段被示为既可查看又可编辑。因此,通过展示呈现接口 600,访问应用 104 选择性地允许或禁用对数字内容项目的多个部分的访问。

[0061] 图 7 是以计算机系统 700 为示例性形式的机器的示意图,在计算机系统 700 中可以执行指令集,该指令集例如会使机器执行在此描述的任何一个或多个方法。在备选实施方式中,机器作为单机设备进行操作,或者可以与其他机器连接(例如,连网)。在网络化部

署中,机器可以按照服务器-客户端网络环境中的服务器或客户机的能力操作,或者作为端到端(或分布式)网络环境中的对等机器进行操作。机器可以是个人计算机(PC)、平板PC、机顶盒(STB)、个人数字助理(PDA)、蜂窝电话、web设备、网络路由器、交换机或桥,或者可以执行(顺序地或其他)指令集的任何机器,其中该指令集规定了机器所要采取的动作。进一步地,尽管示出了单个机器,但是术语“机器”应当包括单独或者联合执行指令集(或者多个集合)来执行在此描述方法的任何一个或多个的机器集合。

[0062] 示例性计算机系统700包括处理器702(例如,中央处理单元(CPU))、图形处理单元(GPU)或者二者)、主存储器704和静态存储器706,它们通过总线708彼此通信。计算机系统700可以进一步包括视频显示单元(例如,液晶显示器(LCD)或者阴极射线管(CRT))。计算机系统700还包括数字字母输入设备712(例如,键盘)、用户接口(UI)导航设备714(例如,鼠标)、盘驱动单元716、信号生成设备718(例如,扬声器)和网络接口设备720。

[0063] 盘驱动单元716包括机器可读介质722,在其上存储有一个或多个指令集和数据结构(例如,软件724),其实现在此描述的任何一个或多个方法或功能或者被其使用。在由计算机系统700执行期间,软件724还可以完全或至少部分驻留在主存储器704中和/或处理器702中,其中主存储器704和处理器702还构成了机器可读介质。

[0064] 还可以、利用多种公知传输协议之一(例如,HTTP)经由网络接口设备720通过网络726传输或接收软件724。

[0065] 尽管在示例性实施方式中将机器可读介质722示为单个介质,但是术语“机器可读介质”应当包括存储一个或多个指令集的单个介质或者多个介质(例如,集中或分布式数据库,和/或相关联的缓存和服务)。术语“机器可读介质”还可以用来包括能够存储、编码或携带指令集的任何介质,这些指令由机器执行,并且使机器执行本发明的任何一个或多个方法,或者能够存储、编码或携带由这种指令集利用或相关联的数据结构。因此,术语“机器可读介质”可以用来包括,但不限于,固态存储器、光和磁介质以及载波信号。

[0066] 尽管参照特定示例性实施方式描述了实施方式,但是显而易见的是:可以在不脱离本发明最广泛精神和范围的前提下对这些实施方式做出各种修改和改变。因此,本说明书和附图应视为说明性的而不是限制性的。仅作为说明而非限制的方式,示出了形成本发明实施方式(本发明的主题可以在其中实现)部分的附图。对所示实施方式进行了足够详细的描述,以使得本领域技术人员能够实施在此公开的教导。可以从此利用并衍生其他实施方式,使得在不脱离本公开范围的情况下,做出结构上和逻辑上的替换和改变。因此,此具体实施方式并不用来限制,各种实施方式的范围仅由所附权利要求及这种权利要求被授予的等同物的全部范围来定义。

[0067] 本发明主题的这种实施方式在此可以单独和/或统一由术语“发明”来参考,这是为了方便而不是意在自愿地将此申请的范围限制到任何单个发明或发明原理,如果实际上公开了多于一个发明或发明原理的话。这样,尽管在此示出并描述了特定实施方式,但是应当理解,被计算用来实现同样目的的任何布置都可以用来替代所示特定实施方式。本公开意在覆盖各种实施方式的任何和全部调整或变体。上述实施方式的组合和其他未在此具体公开的实施方式对于阅读了上述描述的本领域技术人员而言是显然的。

[0068] 提供本公开的摘要以符合37C.F.R. § 1.72(b),其要求允许读者快速分辨本技术

公开实质的摘要。递交的摘要并不用来解释或者限制权利要求的范围和含义。另外,在前述具体实施方式中,可见:出于简化本公开的目的,将各种特征归组为单个实施方式。这种公开方法并不应解释为反映这样的意图:所要求的权利要求需要比每个权利要求中明确记载的特征更多的特征。而是,如下述权利要求书所反映的,发明主题依赖于比单个公开实施方式的所有特征少的特征。这样,将下述权利要求书并入此具体说明,每个权利要求作为其自己的实施方式。

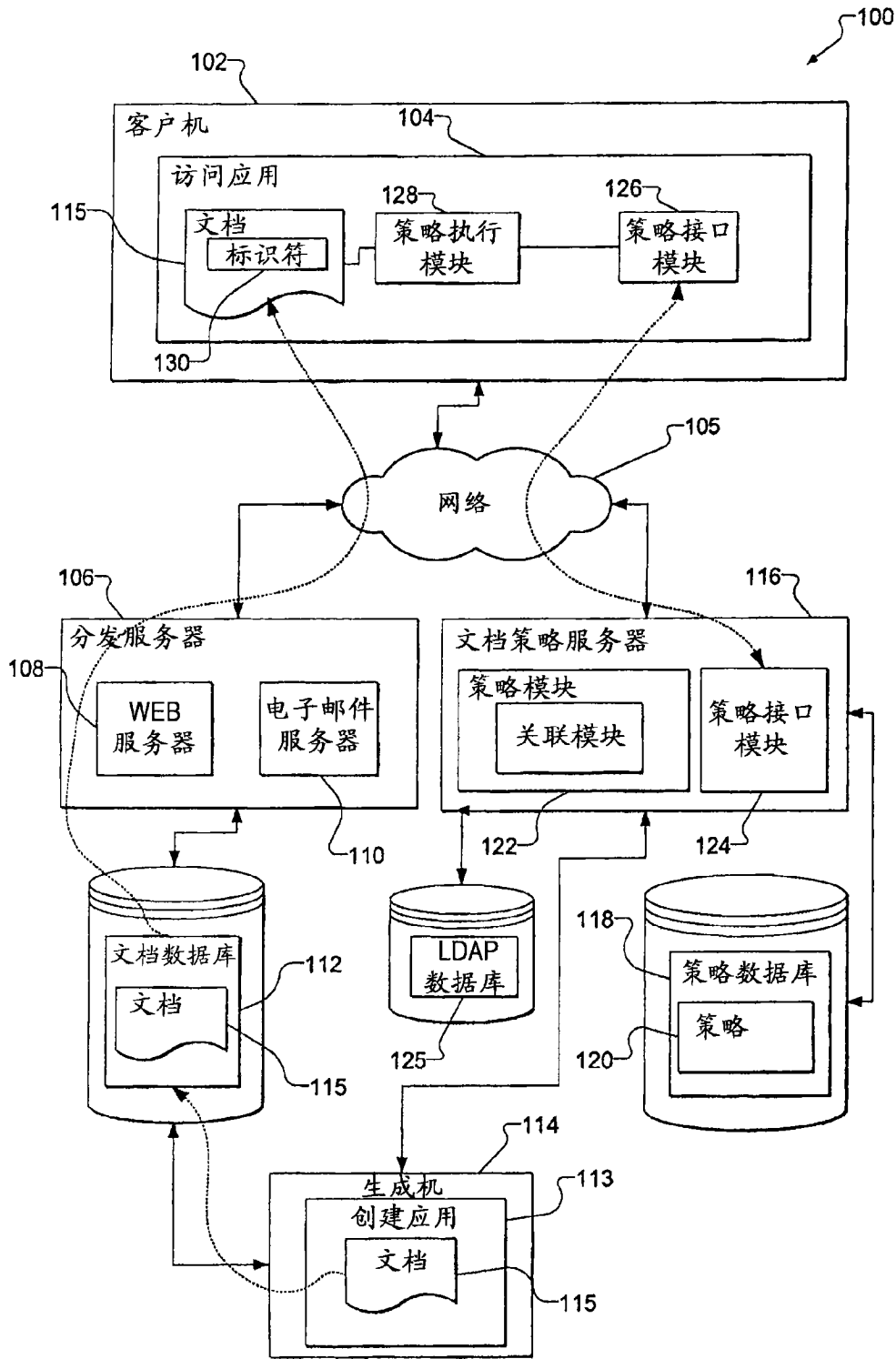


图 1

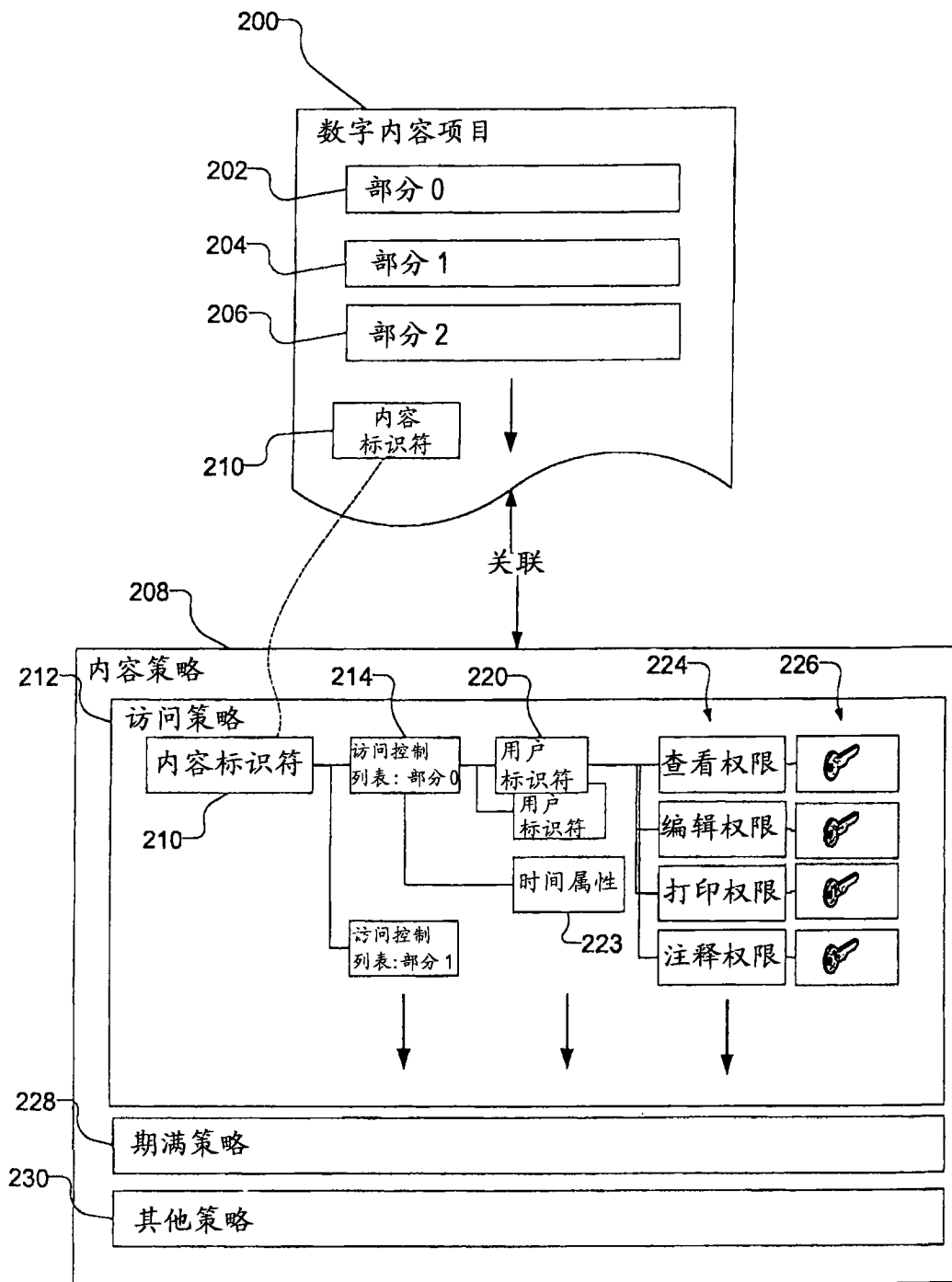


图 2

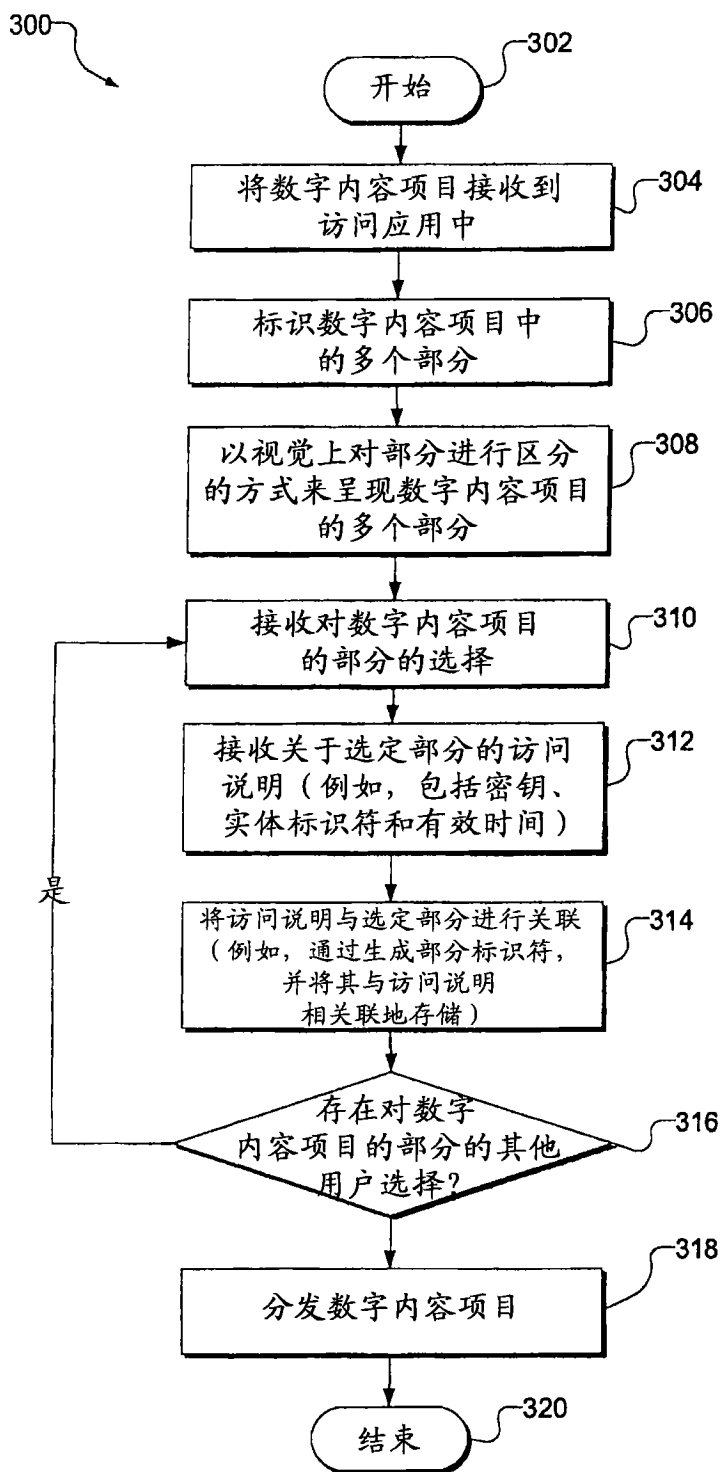


图 3

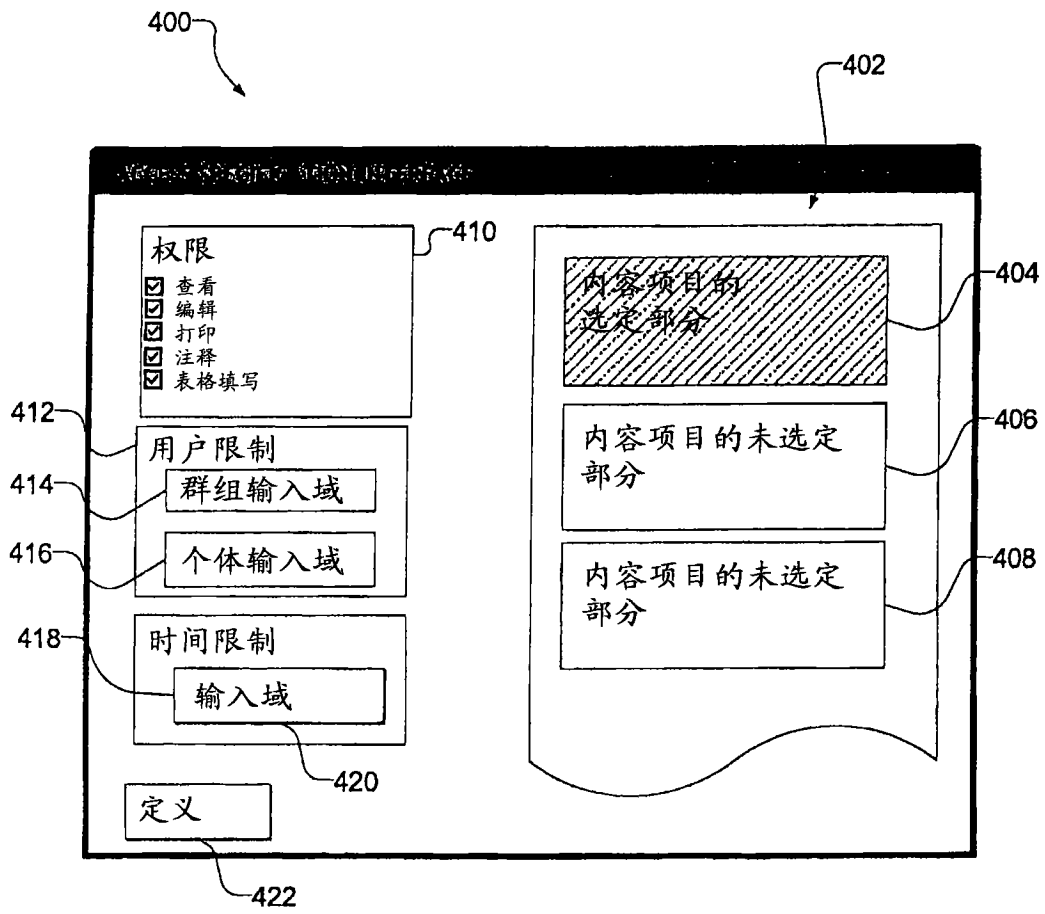


图 4

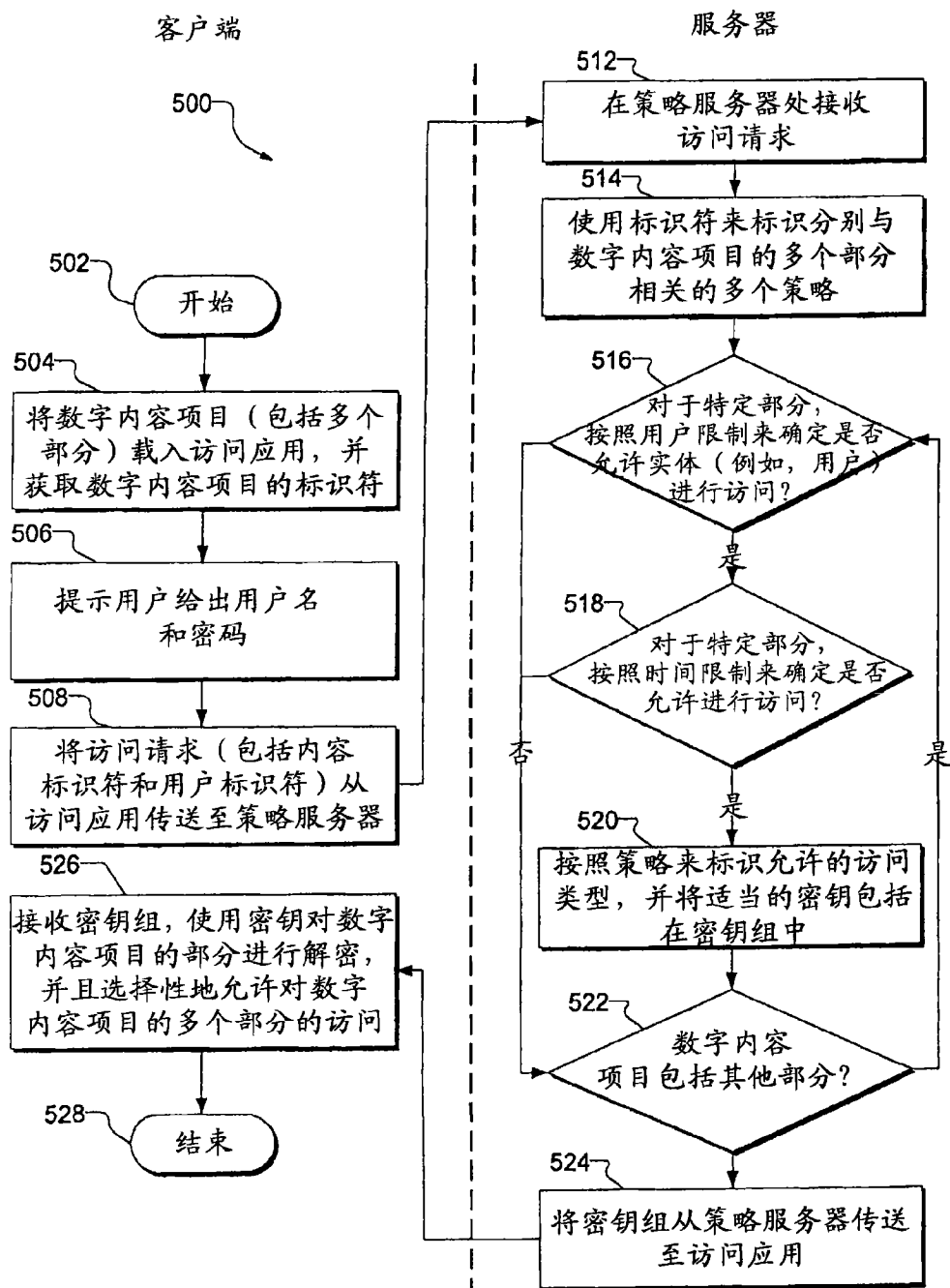


图 5

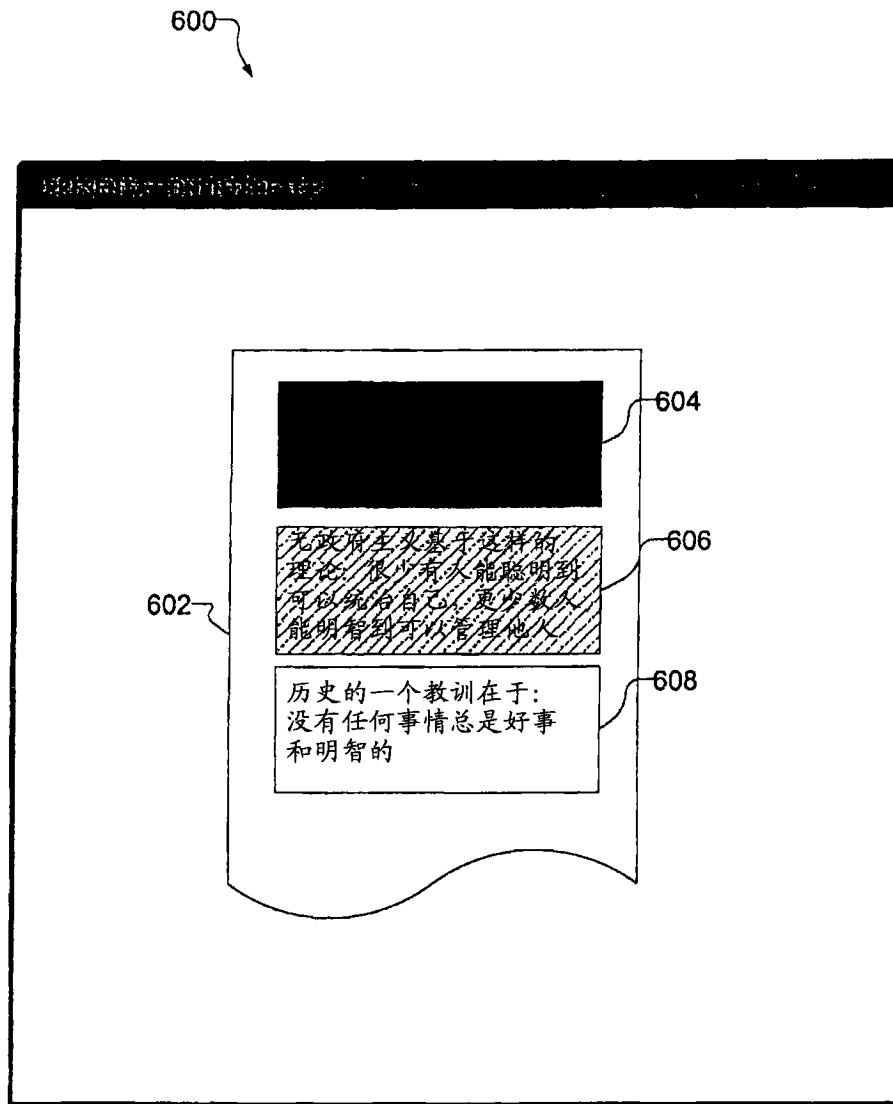


图 6

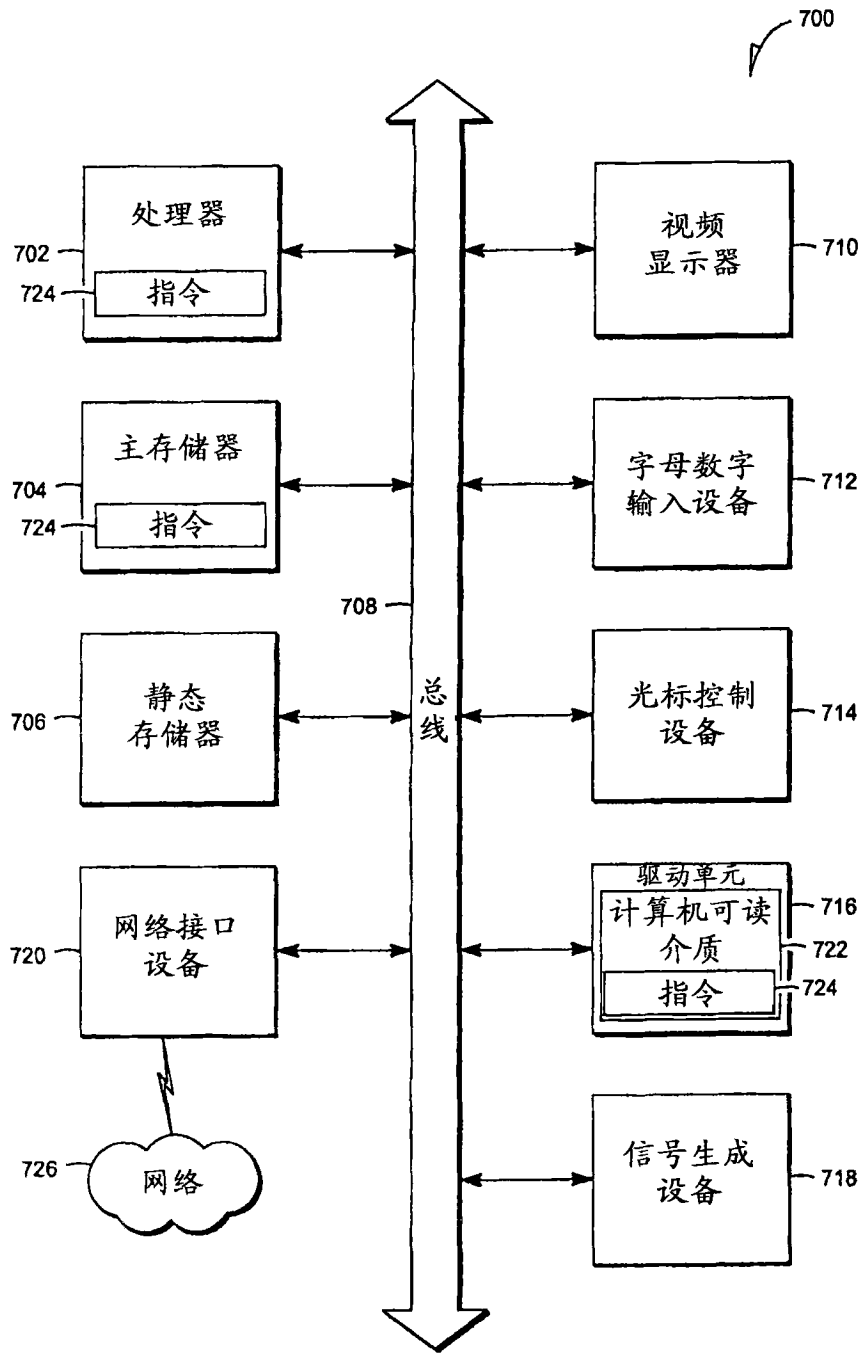


图 7