



(12) 发明专利

(10) 授权公告号 CN 103139143 B

(45) 授权公告日 2016. 03. 30

(21) 申请号 201110376756. 2

CN 101740082 A, 2010. 06. 16,

(22) 申请日 2011. 11. 23

CN 101923608 A, 2010. 12. 22,

(73) 专利权人 北大方正集团有限公司

CN 1851607 A, 2006. 10. 25,

地址 100871 北京市海淀区成府路 298 号方正大厦 9 层

US 2011235801 A1, 2011. 09. 29,

专利权人 方正信息产业控股有限公司
北京方正阿帕比技术有限公司

审查员 王莉

(72) 发明人 王海涛 黄科 左凤蕊

(74) 专利代理机构 北京同达信恒知识产权代理有限公司 11291

代理人 黄志华

(51) Int. Cl.

H04L 29/06(2006. 01)

(56) 对比文件

CN 101923616 A, 2010. 12. 22,

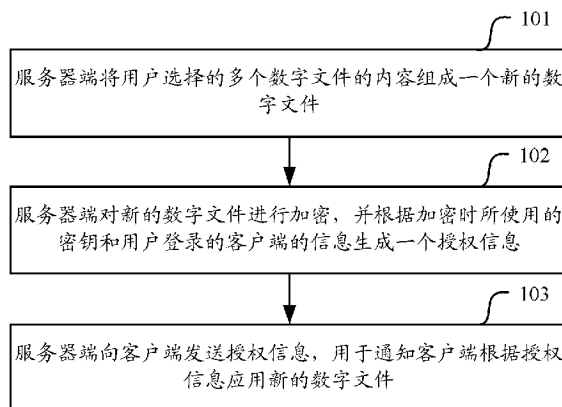
权利要求书3页 说明书8页 附图3页

(54) 发明名称

数字版权管理的方法、系统和服务器

(57) 摘要

本发明实施例涉及数字版权保护领域, 特别涉及一种数字版权管理的方法、系统和服务器, 用以解决现有技术中存在的数字版权管理无法对多个来源作品进行授权的问题。本发明实施例的方法包括: 服务器端将用户选择的多个数字文件的内容组成一个新的数字文件; 所述服务器端对所述新的数字文件进行加密, 并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息; 所述服务器端向所述客户端发送所述授权信息, 用于通知所述客户端根据所述授权信息应用所述新的数字文件。由于本发明实施例将用户选择的多个数字文件的内容组成一个新的数字文件, 向所述客户端发送针对新的数字文件的授权信息, 从而实现了了对多个来源作品进行授权。



1. 一种数字版权管理的方法,其特征在于,该方法包括:

服务器端将用户选择的多个数字文件的内容组成一个新的数字文件;

所述服务器端对所述新的数字文件进行加密,并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息;所述授权信息中包括使用权限、所述新的数字文件的标识、所述新的数字文件进行加密的密钥、客户端的信息;所述使用权限包括阅读权限、打印权限、文字拷贝权限;

所述服务器端向所述客户端发送所述授权信息,用于通知所述客户端根据所述授权信息应用所述新的数字文件;

其中,所述服务器端组成一个新的数字文件之前还包括:

服务器端从用户选择的每个数字文件中确定用户选择的内容,并将确定的内容进行缓存;

所述服务器端根据用户选择的每个数字文件对应的密钥,对缓存的内容进行脱密。

2. 如权利要求1所述的方法,其特征在于,所述服务器端将用户选择的多个数字文件的内容组成一个新的数字文件之前还包括:

所述服务器端根据收到的重组消息中包含的数字文件标识确定对应的数字文件;

所述服务器端根据重组消息中与数字文件标识绑定的内容信息确定用户选择的数字文件中的内容。

3. 如权利要求1所述的方法,其特征在于,所述服务器端组成一个新的数字文件包括:

所述服务器端按照用户选择的顺序,将多个数字文件的内容组成一个新的数字文件。

4. 如权利要求1~3任一所述的方法,其特征在于,所述服务器端生成一个授权信息之前还包括:

所述服务器端向所述客户端发送所述新的数字文件的标识;

所述服务器端生成一个授权信息包括:

所述服务器端根据收到的来自所述客户端的授权申请中包含的所述新的数字文件的标识,确定对应的所述新的数字文件;

所述服务器端根据确定的所述新的数字文件对应的密钥和所述授权申请中包含的所述客户端的信息生成一个授权信息。

5. 一种数字版权管理的方法,其特征在于,该方法包括:

重组服务器将用户选择的多个数字文件的内容组成一个新的数字文件;

所述重组服务器将从许可服务器获得的所述新的数字文件对应的密钥发送给加密服务器,通知加密服务器根据获得的密钥对所述新的数字文件进行加密;

所述重组服务器通知用户登录的客户端在需要应用所述新的数字文件后,通过所述许可服务器获取所述新的数字文件对应的授权信息;所述授权信息中包括使用权限、所述新的数字文件的标识、所述新的数字文件进行加密的密钥、客户端的信息;所述使用权限包括阅读权限、打印权限、文字拷贝权限;

其中,所述授权信息是所述许可服务器根据所述新的数字文件对应的密钥和用户登录的客户端的信息生成的;

所述重组服务器组成一个新的数字文件之前还包括:

所述重组服务器从用户选择的每个数字文件中确定用户选择的内容,并将确定的内容

进行缓存；

所述重组服务器向所述许可服务器申请针对用户选择的多个数字文件的授权；

所述重组服务器根据收到的多个数字文件对应的密钥，对缓存的内容进行脱密。

6. 如权利要求5所述的方法，其特征在于，所述重组服务器将用户选择的多个数字文件的内容组成一个新的数字文件之前还包括：

所述重组服务器根据收到的重组消息中包含的数字文件标识确定对应的数字文件；

所述重组服务器根据重组消息中与数字文件标识绑定的内容信息确定用户选择的数字文件中的内容。

7. 如权利要求5~6任一所述的方法，其特征在于，所述重组服务器组成一个新的数字文件包括：

所述重组服务器按照用户选择的顺序，将多个数字文件的内容组成一个新的数字文件。

8. 一种数字版权管理的服务器，其特征在于，该服务器包括：

组合模块，用于从用户选择的每个数字文件中确定用户选择的内容，并将确定的内容进行缓存，根据用户选择的每个数字文件对应的密钥，对缓存的内容进行脱密，将用户选择的多个数字文件的内容组成一个新的数字文件；

生成模块，用于对所述新的数字文件进行加密，并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息；所述授权信息中包括使用权限、所述新的数字文件的标识、所述新的数字文件进行加密的密钥、客户端的信息；所述使用权限包括阅读权限、打印权限、文字拷贝权限；

处理模块，用于向所述客户端发送所述授权信息，用于通知所述客户端根据所述授权信息应用所述新的数字文件。

9. 一种数字版权管理的服务器，其特征在于，该服务器包括：

重组模块，用于从用户选择的每个数字文件中确定用户选择的内容，并将确定的内容进行缓存，根据用户选择的每个数字文件对应的密钥，对缓存的内容进行脱密，将用户选择的多个数字文件的内容组成一个新的数字文件；

发送模块，用于将从许可服务器获得的所述新的数字文件对应的密钥发送给加密服务器，通知加密服务器根据获得的密钥对所述新的数字文件进行加密；

通知模块，通知用户登录的客户端在需要应用所述新的数字文件后，通过所述许可服务器获取所述新的数字文件对应的授权信息；所述授权信息中包括使用权限、所述新的数字文件的标识、所述新的数字文件进行加密的密钥、客户端的信息；所述使用权限包括阅读权限、打印权限、文字拷贝权限；

其中，所述授权信息是所述许可服务器根据所述新的数字文件对应的密钥和用户登录的客户端的信息生成的。

10. 一种数字版权管理的系统，其特征在于，该系统包括：

服务器端，用于从用户选择的每个数字文件中确定用户选择的内容，并将确定的内容进行缓存，根据用户选择的每个数字文件对应的密钥，对缓存的内容进行脱密，将用户选择的多个数字文件的内容组成一个新的数字文件，对所述新的数字文件进行加密，并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息，向所述客户端发送所述

授权信息;所述授权信息中包括使用权限、所述新的数字文件的标识、所述新的数字文件进行加密的密钥、客户端的信息;所述使用权限包括阅读权限、打印权限、文字拷贝权限;
客户端,用于根据所述授权信息应用所述新的数字文件。

数字版权管理的方法、系统和服务器

技术领域

[0001] 本发明涉及数字版权保护领域,特别涉及一种数字版权管理的方法、系统和服务器。

背景技术

[0002] 随着网络技术与数字出版技术的发展以及多种终端服务器的普及,用户对提供更丰富的数字内容作品的需求日益明显。

[0003] 一般对数字内容作品的应用是针对同一来源数字内容作品进行授权,缺乏对用户个性化使用数字内容作品的支持。这种对同一来源数字内容作品授权模式无法对数字内容作品进行更细致的权限管理和使用控制,不能满足用户对多来源数字内容作品的应用要求。为满足用户个性化需求,需要对多来源数字内容作品进行细粒度的版权保护。

[0004] 目前,行业中也提出了一些细粒度的版权保护方案,主要可分为两类:一类是使用专用的文件格式,利用格式本身的特征,将不同权限的内容进行分页的加密策略;另一类是对文档采用整体加密存储,仅从逻辑上进行分页,使用时,从软件层进行范围控制。这两类方案都只能针对单一来源作品进行分页的授权,不能对多个来源作品进行授权。

[0005] 综上所述,目前数字版权管理无法对多个来源作品进行授权。

发明内容

[0006] 本发明实施例提供一种数字版权管理的方法、系统和服务器,用以解决现有技术中存在的数字版权管理无法对多个来源作品进行授权的问题。

[0007] 本发明实施例提供的一种数字版权管理的方法,包括:

[0008] 服务器端将用户选择的多个数字文件的内容组成一个新的数字文件;

[0009] 所述服务器端对所述新的数字文件进行加密,并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息;

[0010] 所述服务器端向所述客户端发送所述授权信息,用于通知所述客户端根据所述授权信息应用所述新的数字文件。

[0011] 本发明实施例提供的另一种数字版权管理的方法,包括:

[0012] 重组服务器将用户选择的多个数字文件的内容组成一个新的数字文件;

[0013] 所述重组服务器将从许可服务器获得的所述新的数字文件对应的密钥发送给加密服务器,通知加密服务器根据获得的密钥对所述新的数字文件进行加密;

[0014] 所述重组服务器通知用户登录的客户端在需要应用所述新的数字文件后,通过所述许可服务器获取所述新的数字文件对应的授权信息;

[0015] 其中,所述授权信息是所述许可服务器根据所述新的数字文件对应的密钥和用户登录的客户端的信息生成的。

[0016] 本发明实施例提供的一种数字版权管理的服务器,包括:

[0017] 组合模块,用于将用户选择的多个数字文件的内容组成一个新的数字文件;

[0018] 生成模块,用于对所述新的数字文件进行加密,并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息;

[0019] 处理模块,用于向所述客户端发送所述授权信息,用于通知所述客户端根据所述授权信息应用所述新的数字文件。

[0020] 本发明实施例提供的另一种数字版权管理的服务器,包括:

[0021] 重组模块,用于将用户选择的多个数字文件的内容组成一个新的数字文件;

[0022] 发送模块,用于将从许可服务器获得的所述新的数字文件对应的密钥发送给加密服务器,通知加密服务器根据获得的密钥对所述新的数字文件进行加密;

[0023] 通知模块,通知用户登录的客户端在需要应用所述新的数字文件后,通过所述许可服务器获取所述新的数字文件对应的授权信息;

[0024] 其中,所述授权信息是所述许可服务器根据所述新的数字文件对应的密钥和用户登录的客户端的信息生成的。

[0025] 本发明实施例提供的一种数字版权管理的系统,包括:

[0026] 服务器端,用于将用户选择的多个数字文件的内容组成一个新的数字文件,对所述新的数字文件进行加密,并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息,向所述客户端发送所述授权信息;

[0027] 客户端,用于根据所述授权信息应用所述新的数字文件。

[0028] 由于本发明实施例将用户选择的多个数字文件的内容组成一个新的数字文件,向所述客户端发送针对新的数字文件的授权信息,从而实现了对多个来源作品进行授权;进一步的,不需要专用DRM客户端,提高了易用性。

附图说明

[0029] 图1为本发明实施例第一种数字版权管理的方法流程图;

[0030] 图2为本发明实施例第一种数字版权管理的系统流程示意图;

[0031] 图3为本发明实施例第一种数字版权管理的服务器结构示意图;

[0032] 图4为本发明实施例第二种数字版权管理的方法流程图;

[0033] 图5为本发明实施例第二种数字版权管理的系统流程示意图;

[0034] 图6为本发明实施例第二种数字版权管理的服务器结构示意图。

具体实施方式

[0035] 针对现有技术中存在的数字版权管理无法对多个来源作品进行授权的问题,本发明实施例将用户选择的多个数字文件的内容组成一个新的数字文件,向客户端发送针对新的数字文件的授权信息,从而实现了对多个来源作品进行授权。

[0036] 下面结合说明书附图对本发明实施例作进一步详细描述。

[0037] 如图1所示,本发明实施例第一种数字版权管理的方法包括下列步骤:

[0038] 步骤101、服务器端将用户选择的多个数字文件的内容组成一个新的数字文件;

[0039] 步骤102、服务器端对新的数字文件进行加密,并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息;

[0040] 步骤103、服务器端向客户端发送授权信息,用于通知客户端根据授权信息应用新

的数字文件。

[0041] 在实施中,用户可以通过网页、客户端等方式登录到服务器端。用户选择的数字文件的内容可以是数字文件的部分内容,也可以是数字文件的全部内容。

[0042] 具体的,服务器端根据收到的重组消息中包含的数字文件标识确定对应的数字文件;

[0043] 服务器端根据重组消息中与数字文件标识绑定的内容信息确定用户选择的数字文件中的内容。

[0044] 较佳地,客户端提交用户选择的数字内容文件标识和重组消息(即所选择的页码范围),服务器端根据数字内容文件标识查找到文件(数字内容文件中每一页都标识了相应的页码),再根据用户选择的页码范围从文件中进行页码的检索,将对应的页码抽取出来。

[0045] 在实施中,内容信息可以是可重组数字内容页码范围。

[0046] 如果用户选择的多个数字文件是经过加密的,步骤101之前还可以进一步包括:

[0047] 服务器端根据用户选择的每个数字文件对应的密钥,分别对用户选择的每个数字文件的内容进行脱密。

[0048] 脱密过程实际就是加密的反过程。文件在加密的时候使用某一个密钥对文件进行加密,在文件的特殊位置增加相应的加密信息,当进行脱密时使用该密钥将文件打开,并把相应的加密信息从文件中删除,从而实现了文件的脱密过程。

[0049] 在实施中,脱密的时候分两种情况:

[0050] 情况一、脱密整个文件。具体的:

[0051] 1、根据文件的标识从服务器上获取文件密钥和数字文件的加密方法;

[0052] 2、打开加密文件,通过获取的密钥和加密方法解密整个加密文件;

[0053] 3、使用解密后的信息替换加密信息,并删除原加密文件中的安全描述信息。

[0054] 情况二、只脱密用户选择的部分。具体的:

[0055] 1、根据文件的标识从服务器上获取文件密钥和数字文件的加密方法;

[0056] 2、打开加密文件,对页码进行定位,找到页码范围;

[0057] 3、通过获取的密钥和加密方法解密指定页码范围内的加密部分;

[0058] 4、使用解密后的信息替换加密文件的加密信息中信息对应的部分信息,并重新生成加密文件的安全描述信息。

[0059] 其中,在进行页码定位时可以先脱密后再读取索引和页码信息;如果文档索引和页码信息都保存在外部,还可以不脱密,直接读取文档索引和页码信息进行页码定位。

[0060] 较佳地,服务器端首先从用户选择的每个数字文件中确定用户选择的内容,然后将这部分内容进行缓存,并根据数字文件对应的密钥,对缓存的内容进行脱密。

[0061] 比如用户选择数字文件A中的1~20页和数字文件B中的4~28页,然后服务器端将数字文件A中的1~20页和数字文件B中的4~28页进行缓存(这里的缓存是复制并存储,数字文件A中的1~20页和数字文件B中的4~28页还再分别在数字文件A和B中,并不会因为缓存而删除);然后服务器端用数字文件A对应的密钥(即加密数字文件A时采用的密钥)对缓存的数字文件A中的1~20页进行脱密,用数字文件B对应的密钥(即加密数字文件B时采用的密钥)对缓存的数字文件B中的4~28页进行脱密。

[0062] 较佳地,用户在选择多个数字文件的内容时,还可以设置组合的顺序;相应的,步

骤101中,服务器端按照用户选择的顺序,将多个数字文件的内容组成一个新的数字文件。

[0063] 为了提高新的数字文件的安全性,较佳地,步骤102中,服务器端先生成一个针对新的数字文件的密钥,然后根据生成的密钥对新的数字文件进行加密。

[0064] 具体的,根据当前服务器的时间生成一个随机数,并把该随机数做为偏移量,随机生成一个固定位数的字符串做为密钥。

[0065] 较佳地,步骤102中,服务器端在对新的数字文件进行加密之后,可以通知客户端在需要应用新的数字文件时可以获取授权信息,其中包括新的数字文件对应的文件标识;

[0066] 若用户需要获取授权信息可以通过客户端向服务器端发送授权申请,其中该授权申请中包含文件标识和客户端的信息(比如客户端所在本地的硬件信息等能够标识客户端的信息);

[0067] 相应的,服务器端根据收到的文件标识,确定对应的新的数字文件,进而确定新的数字文件对应的密钥(即对新的数字文件进行加密时使用的密钥);然后服务器端根据确定密钥和客户端的信息生成一个授权信息,并将授权信息发送个客户端;

[0068] 客户端通过授权信息就可以应用新的数字文件。

[0069] 较佳地,该授权信息中还可以包括使用权限、(比如阅读权限、打印权限、文字拷贝权限等)文件的唯一标识、文件加密密钥、授权文件校验信息等。

[0070] 基于图1的发明构思,本发明实施例中还提供了一种数字版权管理的系统,由于这些服务器解决问题的原理与图1的数字版权管理的方法相似,因此这些服务器的实施可以参见方法的实施,重复之处不再赘述。

[0071] 如图2所示,本发明实施例第一种数字版权管理的系统包括:服务器端200和客户端210。

[0072] 服务器端200,用于将用户选择的多个数字文件的内容组成一个新的数字文件,对新的数字文件进行加密,并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息,向客户端发送授权信息;

[0073] 客户端210,用于根据授权信息应用新的数字文件。

[0074] 如图3所示,本发明实施例第一种数字版权管理的服务器包括:组合模块300、生成模块310和处理模块320。

[0075] 组合模块300,用于将用户选择的多个数字文件的内容组成一个新的数字文件;

[0076] 生成模块310,用于对新的数字文件进行加密,并根据加密时所使用的密钥和用户登录的客户端的信息生成一个授权信息;

[0077] 处理模块320,用于向客户端发送授权信息,用于通知客户端根据授权信息应用新的数字文件。

[0078] 较佳地,组合模块300根据收到的重组消息中包含的数字文件标识确定对应的数字文件;根据重组消息中与数字文件标识绑定的内容信息确定用户选择的数字文件中的内容。

[0079] 较佳地,组合模块300根据用户选择的每个数字文件对应的密钥,分别对用户选择的每个数字文件的内容进行脱密。

[0080] 具体的,组合模块300从用户选择的每个数字文件中确定用户选择的内容,并将确定的内容进行缓存;根据用户选择的每个数字文件对应的密钥,对缓存的内容进行脱密。

[0081] 较佳地,组合模块300按照用户选择的顺序,将多个数字文件的内容组成一个新的数字文件。

[0082] 较佳地,生成模块310向客户端发送所述新的数字文件的标识;根据收到的来自客户端的授权申请中包含的新的数字文件的标识,确定对应的新的数字文件;根据确定的新的数字文件对应的密钥和授权申请中包含的客户端的信息生成一个授权信息。

[0083] 本发明图1中服务器端可以是一个服务器,即上述服务器端的功能都可以由一个服务器实现。

[0084] 在实施中,图1的服务器端也可以有多个服务器实现,具体有几个服务器实现可以根据需要确定。下面列举一个由三个服务器实现的实施例,即服务器端包括重组服务器、许可服务器和加密服务器。

[0085] 如图4所示,本发明实施例第二种数字版权管理的方法包括下列步骤:

[0086] 步骤401、重组服务器将用户选择的多个数字文件的内容组成一个新的数字文件;

[0087] 步骤402、重组服务器将从许可服务器获得的新的数字文件对应的密钥发送给加密服务器,通知加密服务器根据获得的密钥对新的数字文件进行加密;

[0088] 步骤403、重组服务器通知用户登录的客户端在需要应用新的数字文件后,通过许可服务器获取新的数字文件对应的授权信息;

[0089] 其中,授权信息是许可服务器根据新的数字文件对应的密钥和用户登录的客户端的信息生成的。

[0090] 在实施中,用户可以通过网页、客户端等方式登录到重组服务器。用户选择的数字文件的内容可以是数字文件的部分内容,也可以是数字文件的全部内容。

[0091] 较佳的,重组服务器根据收到的重组消息中包含的数字文件标识确定对应的数字文件,根据重组消息中与数字文件标识绑定的内容信息确定用户选择的数字文件中的内容。

[0092] 在实施中,内容信息可以是可重组数字内容页码范围。

[0093] 许可服务器和加密服务器确定新的数字文件的标识的方式有很多,比如与与背景技术中新加入一个数字文件后确定数字文件的标识的方式相同;还可以重组服务器组成一个新的数字文件后可以生成一个新的数字文件的标识,将新的数字文件的标识分别发送给许可服务器和加密服务器,重组服务器还可以将新的数字文件的标识置于数字文件标识列表中,这样许可服务器和加密服务器可以根据数字文件标识列表确定新的数字文件的标识,数字文件标识列表可以存储到任何一个服务器中。

[0094] 如果用户选择的多个数字文件是经过加密的,步骤401之前还可以进一步包括:

[0095] 重组服务器向许可服务器申请针对用户选择的多个数字文件的授权;

[0096] 许可服务器将多个数字文件对应的密钥发送给重组服务器;

[0097] 重组服务器根据收到的多个数字文件对应的密钥,分别对用户选择的每个数字文件的内容进行脱密。

[0098] 脱密过程实际就是加密的反过程。

[0099] 具体的,重组服务器首先从用户选择的每个数字文件中确定用户选择的内容,然后将这部分内容进行缓存(在实施中数字文件可以存储到指定的服务器中(比如存储服务器,许可服务器,加密服务器等),则重组服务器会从其他服务器获取这部分内容),并根据

数字文件对应的密钥,对缓存的内容进行脱密。

[0100] 比如用户选择数字文件A中的1~20页和数字文件B中的4~28页,然后重组服务器将数字文件A中的1~20页和数字文件B中的4~28页进行缓存(这里的缓存是复制并存储,数字文件A中的1~20页和数字文件B中的4~28页还再分别在数字文件A和B中,并不会因为缓存而删除);然后重组服务器用数字文件A对应的密钥(即加密数字文件A时采用的密钥)对缓存的数字文件A中的1~20页进行脱密,用数字文件B对应的密钥(即加密数字文件B时采用的密钥)对缓存的数字文件B中的4~28页进行脱密。

[0101] 较佳地,用户在选择多个数字文件的内容时,还可以设置组合的顺序;相应的,步骤401中,重组服务器按照用户选择的顺序,将多个数字文件的内容组成一个新的数字文件。

[0102] 为了提高新的数字文件的安全性,较佳地,步骤402中,许可服务器先生成一个针对新的数字文件的密钥;然后重组服务器将该密钥和新的数字文件发送加密服务器;加密服务器根据收到的密钥对收到的新的数字文件进行加密。

[0103] 较佳地,步骤403中,重组服务器通知用户登录的客户端在需要应用新的数字文件后,通过许可服务器获取新的数字文件对应的授权信息。

[0104] 若用户需要获取授权信息可以通过客户端向服务器端发送授权申请,其中该授权申请中包含文件标识和客户端的信息(比如客户端所在本地的硬件信息等能够标识客户端的信息);

[0105] 相应的,许可服务器根据收到的文件标识,确定对应的新的数字文件,进而确定新的数字文件对应的密钥(即对新的数字文件进行加密时使用的密钥);然后服务器端根据确定密钥和客户端的信息生成一个授权信息,并将授权信息发送个客户端;

[0106] 客户端通过授权信息就可以应用新的数字文件。

[0107] 需要说明的是,图4只是举例说明,根据需要还可以重组服务器的功能还可以由许可服务器和/或加密服务器完成,这样服务器端只需要两个服务器即可,具体实施方式与图4类似,在此不再赘述。

[0108] 基于图4的发明构思,本发明实施例中还提供了一种数字版权管理的系统,由于这些服务器解决问题的原理与图4的数字版权管理的方法相似,因此这些服务器的实施可以参见方法的实施,重复之处不再赘述。

[0109] 如图5所示,本发明实施例第二种数字版权管理的系统包括:

[0110] 重组服务器500、许可服务器510、加密服务器520。

[0111] 其中,本发明实施例第二种数字版权管理的系统还可以进一步包括客户端530。

[0112] 下面以一个具体事例对图5的系统进行详细说明。

[0113] 事例:实现对多个CEBX格式文档的重组和版权管理。

[0114] 现有西游记.ceb,三国演义.ceb,红楼梦.ceb三个文件。

[0115] 用户从重组服务器500上选择感兴趣的数字内容作品,确定好其中感兴趣的页码范围,同时将这些范围进行组合排序:西游记.ceb中20到30页,记为A,三国演义.ceb 60到70页,记为B,红楼梦.ceb 90到95页,记为C,排列顺序为ABC。

[0116] 重组服务器500根据用户的选择向许可服务器510申请只包含所选页码范围的授权;

- [0117] 许可服务器510生成一个拥有三个文档中只包含A、B、C文档页导出权限的授权；
- [0118] 重组服务器500根据授权分别将这些文件中的指定页码范围的文档页进行脱密；
- [0119] 重组服务器500将脱密后的文档页抽取出来，按照ABC的顺序重新进行组合，形成新的文件“名著小说.ceb”。
- [0120] 重组服务器500向许可服务器510申请新密钥；
- [0121] 许可服务器510生成一个新文件密钥“KRYCY5VRXP1UXZ=”给重组服务器500；
- [0122] 重组服务器500将该密钥和名著小说.ceb传输给加密服务器520；
- [0123] 加密服务器520使用该密钥将名著小说.ceb进行加密；
- [0124] 加密服务器520将名著小说.ceb和新的密钥给存储服务器进行保存；
- [0125] 重组服务器500通知客户端530可以进行授权的获取，并将名著小说.ceb的标识信息发送给客户端530；
- [0126] 客户端530向许可服务器510发送包含客户端530信息和名著小说.ceb的标识的申请；
- [0127] 许可服务器510根据客户端530信息和名著小说.ceb对应的密钥生成授权信息，并发送给客户端530；
- [0128] 其中，许可服务器510通过名著小说.ceb的标识向存储名著小说.ceb的服务器请求获取对应的密钥。
- [0129] 客户端530下载名著小说.ceb；
- [0130] 客户端530根据授权信息应用名著小说.ceb的文件内容。
- [0131] 如图6所示，本发明实施例第二种数字版权管理的服务器包括：重组模块600、发送模块610和通知模块620。
- [0132] 重组模块600，用于将用户选择的多个数字文件的内容组成一个新的数字文件；
- [0133] 发送模块610，用于将从许可服务器获得的新的数字文件对应的密钥发送给加密服务器，通知加密服务器根据获得的密钥对新的数字文件进行加密；
- [0134] 通知模块620，用于通知用户登录的客户端在需要应用新的数字文件后，通过许可服务器获取新的数字文件对应的授权信息；
- [0135] 其中，授权信息是许可服务器根据新的数字文件对应的密钥和用户登录的客户端的信息生成的。
- [0136] 较佳地，重组模块600根据收到的重组消息中包含的数字文件标识确定对应的数字文件；根据重组消息中与数字文件标识绑定的内容信息确定用户选择的数字文件中的内容。
- [0137] 较佳地，重组模块600向许可服务器申请针对用户选择的多个数字文件的授权；根据收到的多个数字文件对应的密钥，分别对用户选择的每个数字文件的内容进行脱密。
- [0138] 具体的，重组模块600从用户选择的每个数字文件中确定用户选择的内容，并将确定的内容进行缓存，向所述许可服务器申请针对用户选择的多个数字文件的授权，根据收到的多个数字文件对应的密钥，对缓存的内容进行脱密。
- [0139] 较佳地，重组模块600按照用户选择的顺序，将多个数字文件的内容组成一个新的数字文件。
- [0140] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序

产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0141] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0142] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备服务器以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0143] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0144] 尽管已描述了本发明的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例作出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0145] 由于本发明实施例将用户选择的多个数字文件的内容组成一个新的数字文件,向客户端发送针对新的数字文件的授权信息,从而实现了对多个来源作品进行授权;进一步的,不需要专用DRM客户端,提高了易用性。

[0146] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

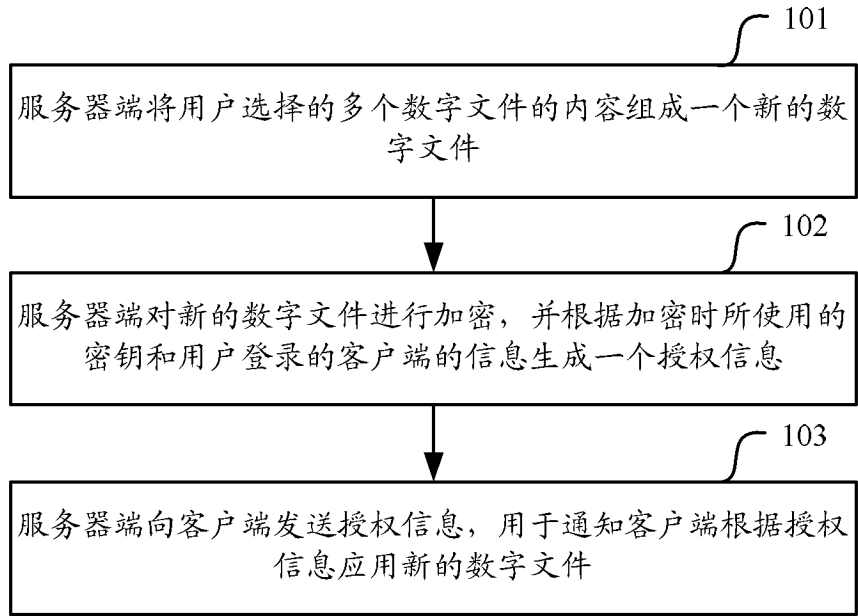


图1



图2

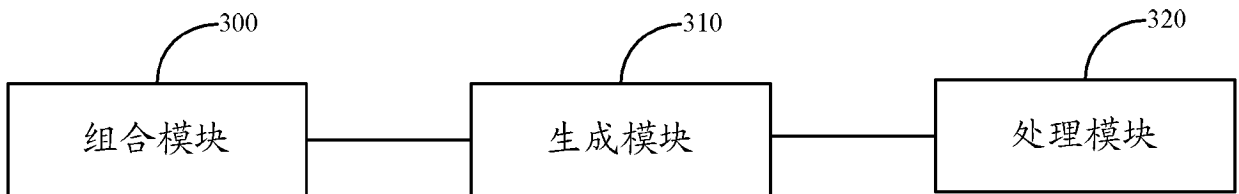


图3

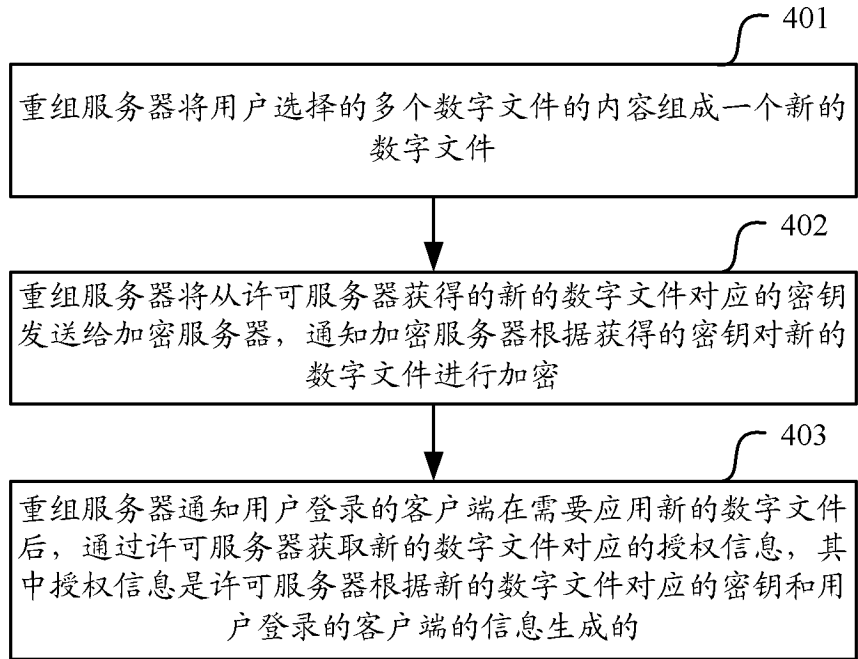


图4

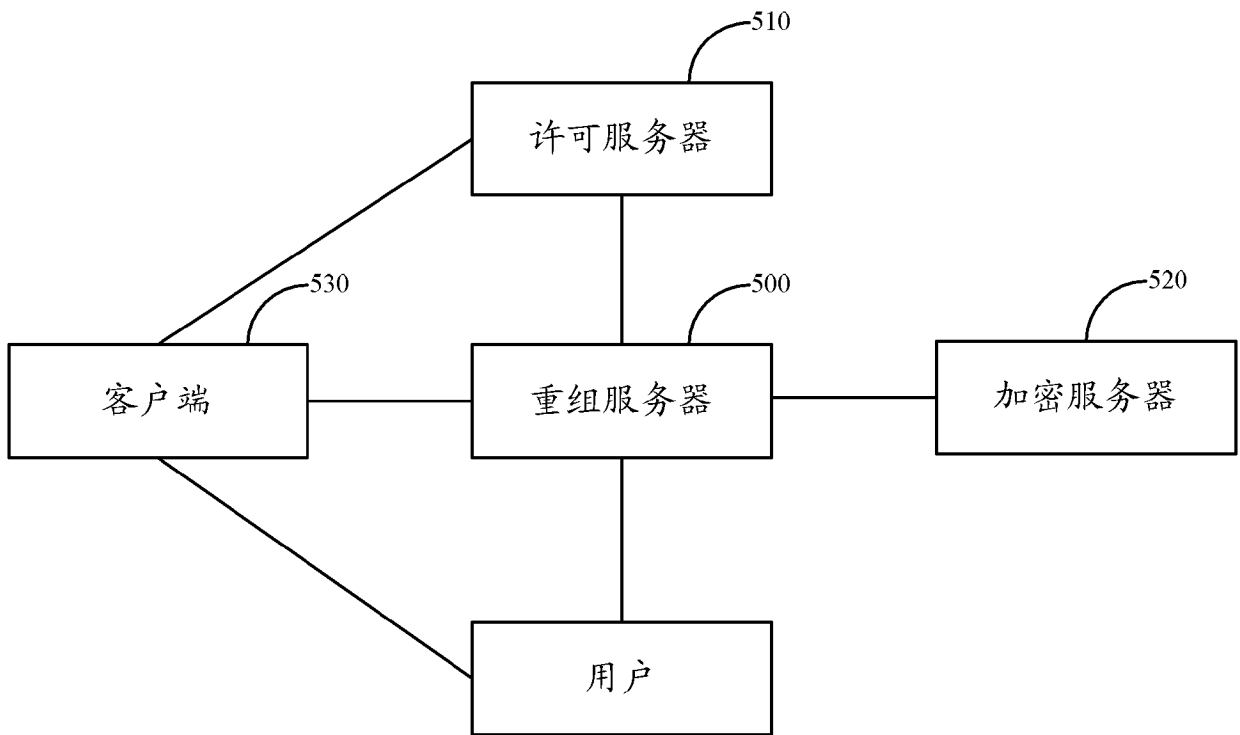


图5

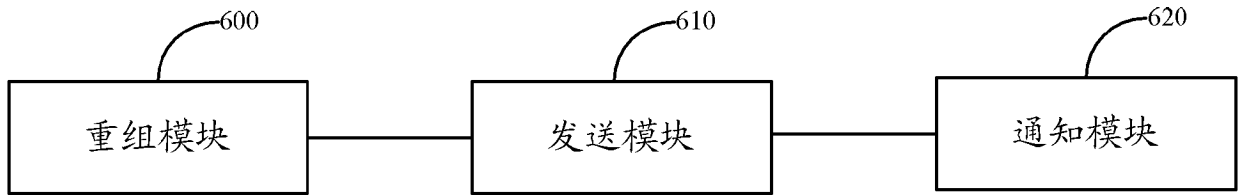


图6