(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 103942470 B
(45)授权公告日 2017.06.20

(21)申请号 201410189667.0

(22)申请日 2014.05.07

(65)同一申请的已公布的文献号
申请公布号 CN 103942470 A

(43)申请公布日 2014.07.23

(73)专利权人 华中师范大学
地址 430079 湖北省武汉市洪山区珞喻路152号
专利权人 华中科技大学

(72)发明人 王星 刘延申 尤新革 徐端全 胡泉 王哲

(74)专利代理机构 上海硕力知识产权代理事务所 31251
代理人 王法男

(51)Int.Cl.
G06F 21/10(2013.01)
H04L 29/06(2006.01)

(56)对比文件
CN 101202883 A,2008.06.18,
CN 101207794 A,2008.06.25,
EP 1667355 B1,2008.08.20,

审查员 张剑峰

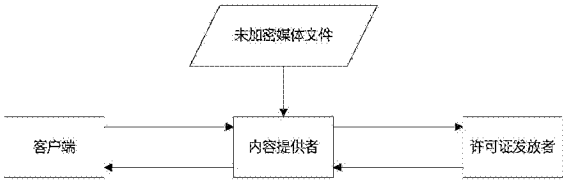
权利要求书2页 说明书11页 附图4页

(54)发明名称

一种具有溯源功能的电子音像制品版权管理方法

(57)摘要

本发明涉及的一种具有溯源功能的电子音像制品版权管理方法，其特征在于：采用由客户端、媒体打包者、许可证发放者三方构成具有溯源功能的电子音像制品版权管理方法框架；由服务器根据用户请求生成用户密钥对，并进行管理和分发；将用户信息利用数字水印技术，嵌入到媒体文件中，实现溯源功能；采用特有文件格式，对电子音像制品进行整体打包，将系统信息、用户信息、媒体文件信息等进行封装；采用分段加密技术，使每段加密密钥与用户信息相关联，媒体文件的权限管理更加灵活。



CN 103942470 B

1.一种具有溯源功能的电子音像制品版权管理方法,其特征在于:

⑴采用由客户端、媒体打包者、许可证发放者三方构成具有溯源功能的电子音像制品版权管理方法框架;媒体打包者承接版权持有者交付的电子音像制品,用户通过客户端在媒体打包者处进行注册、并使用客户端进行登录验证,同时用户经客户端在媒体打包者处购买并下载电子音像制品,在下载过程中由媒体打包者进行打包;许可证发放者生成许可证,对用户权利进行限制;获得许可后的用户经客户端对下载的电子音像制品进行处理;

⑵由服务器根据用户请求进行密钥的生成和分发;

⑶利用数字水印技术,嵌入用户信息,实现溯源功能;

⑷采用自定义格式对纷繁复杂的媒体文件格式进行打包处理,统一成一种文件格式,便于进行系统信息、用户信息、媒体文件信息的验证管理;

⑸采用分段加密对电子音像制品进行打包;

⑹分段加密过程中,每段加密密钥与用户信息相关联;

⑺提供电子音像制品的预览功能。

2.如权利要求1所述的一种具有溯源功能的电子音像制品版权管理方法,其特征在于:所述的电子音像制品版权管理方法框架中,媒体打包者承接版权持有者交付的电子音像制品,用户通过客户端在媒体打包者处进行注册、并使用客户端进行登录验证,同时用户经客户端在媒体打包者处购买并下载电子音像制品,在下载过程中由媒体打包者进行打包;许可证发放者生成许可证,对用户权利进行限制;获得许可后的用户经客户端对下载的电子音像制品进行处理;

所述用户通过服务器生成密钥的流程为:

⑻用户经客户端在服务器端进行注册;

⑹用户经客户端下载客户端软件,安装并登陆;

⑽用户客户端随机生成一对非对称加密密钥:公钥A、私钥A;

⑾用户客户端获取服务器公钥B,并用服务器公钥B加密用户信息、公钥A,然后发送至服务器;

⑿服务器接收数据后,使用服务器私钥B解密数据,获得用户信息、用户硬件信息、公钥A;

⒁服务器对用户信息进行验证,如果用户信息不合法,服务器向客户端发送信息,提示用户;如果用户信息合法,服务器在数据库中对用户硬件信息进行查找、确认;

Ⓖ确认用户信息合法性与否,服务器在数据库中对用户硬件信息进行查找确认用户信息合法性与否,若用户硬件未注册,服务器对当前用户硬件信息进行注册,生成一对非对称密钥:公钥C、私钥C与用户信息进行绑定;若用户硬件信息已注册,服务器从数据库中读取与此硬件信息绑定的私钥C;

⑯服务器使用公钥A,对私钥C进行加密,并发送至客户端;

⑰客户端接收数据后,使用私钥A进行解密,得到私钥C,并存储于本地。

3.如权利要求1所述的一种具有溯源功能的电子音像制品版权管理方法,其特征在于:所述的数字水印技术是:在用户下载电子音像制品过程中,服务器针对不同用户,将用户信息制作成文本、图像、二维码或其它格式的数字水印数据,采用鲁棒隐藏数字水印技术,将数字水印数据实时嵌入用户下载的电子音像制品中。

4.如权利要求1所述的一种具有溯源功能的电子音像制品版权管理方法，其特征在于：自定文件格式包括以下操作步骤：

(a)对原始电子音像制品文件进行整体打包，使不同的电子音像制品封装成统一格式，便于管理；

(b)在文件打包过程中加入系统信息、用户信息、媒体文件信息，使其在播放时进行验证，进行权限管理；

(c)打包后的文件需要在特定的客户端进行解析播放，从而提高安全性。

5.如权利要求1所述的一种具有溯源功能的电子音像制品版权管理方法，其特征在于：所述的分段加密对电子音像制品进行打包的方法为：每段使用的加密密钥由一个特定的种子和用户信息关联生成，由此提高分段加密的安全性。

6.如权利要求1所述的一种具有溯源功能的电子音像制品版权管理方法，其特征在于：所述用户根据分段加密密钥及用户权限对电子音像制品进行部分解密，实现预览。

一种具有溯源功能的电子音像制品版权管理方法

技术领域

[0001] 本发明属于版权管理方法，具体地说是一种具有溯源功能的电子音像制品版权管理方法。

背景技术

[0002] 信息技术的高速发展与网络技术的快速普及不仅提高了信息源传播的速度和广度，同时也极大地降低了电子音像商品盗版的难度；同时也导致盗版音像商品的广泛传播。传统的依赖于电子音像商品的防伪包装以及各类防伪标签进行电子音像商品的防伪防盗对于拷贝、非法下载传播等侵权盗版已经完全失效，而且传统包装防伪等加密防侵权不能为公安机关打击盗版侵权提供有效溯源取证技术支持。

[0003] 目前电子音像制品版权管理通常采用的技术是数字版权管理(DRM，Digital Rights Management)。这是一个系统的概念，它结合硬件和软件存取机制，利用一系列的数字版权保护技术对各类多媒体文件在制作阶段，分发阶段以及使用阶段的全生命周期内的存取进行控制。它包含版权使用的语言描述、识别、交易监控和对使用在有形和无形资产上的各种权限的跟踪和对版权所有人的关系管理等内容。

[0004] DRM的核心技术是数据加密和防拷贝，一个DRM系统需要首先建立数字媒体授权中心，编码已压缩的数字媒体，然后利用密钥对内容进行加密保护，加密的数字媒体头部存放着数字媒体文件唯一标识符和节目授权中心的统一资源定位器地址。用户在点播时，根据节目头部的唯一标识符和统一资源定位器地址信息，通过数字媒体授权中心的验证授权后送出相关的密钥解密，数字媒体方可使用。需要保护的数字媒体是被加密的，即使被用户下载保存并散播给他人，没有得到数字媒体授权中心的验证授权也无法使用，从而严密地保护了数字媒体的版权。

[0005] 数字版权管理系统从提出发展到现在，可以划分为两代：第一代DRM系统主要是加密技术，将数字信息进行加密处理后封装，使得用户只有在付费或满足所要求的条件下，才能获得密钥解开数字信息，保证了只有合法授权的用户才能使用。然而用户在解开数字信息后，数字信息则失去了保护，用户可以随意使用，传播，甚至修改，对于有知识产权的数字信息，还是无法保护其版权。第二代是在第一代的基础上进一步对用户使用数字内容进行控制。即使是合法用户，也必须在允许的范围内使用数字信息，并且还对其操作进行跟踪监测，进一步的保护数字信息的知识版权。

[0006] 然而，虽然DRM技术不断更新发展，其一直没有提供一种有效的溯源方法，同时现有的DRM方案，由于各种限制，使得其用户体验较差，使用较为困难，经常产生各种各样的问题。

[0007] 目前使用规模比较大或研究比较多的DRM系统主要有以下几种：

[0008] 微软公司的WMDRM；

[0009] 苹果公司的FairPlay DRM；

[0010] 开放联盟的OMA DRM。

[0011] 微软WMDRM:采用加密技术,提供SDK开发环境;仅限于Windows系统及微软设备,媒体文件格式为微软非开放格式(WMA,WMV),不提供溯源功能;

[0012] 苹果FairPlay DRM:采用加密技术,系统封闭;仅限于苹果设备,不提供开发接口,仅支持苹果提供的格式,不提供溯源功能;

[0013] 开放联盟OMA DRM:框架及文件结构公开,基于mpeg-4格式,易于实现;仅限于移动设备,不提供溯源功能。

[0014] 综上所述的各DRM系统相比较,可以得出现有电子音像制品版权管理方案的典型缺点:

[0015] 1.不提供有效的溯源功能,在打击盗版上存在空白;

[0016] 2.设备的不统一造成用户与硬件绑定过程复杂,密钥管理混乱;

[0017] 3.文件格式具有一定局限性,对不同的电子音像制品格式支持度不够;

[0018] 4.加密技术不够灵活。

[0019] 由于现有电子音像制品版权管理方法的上述缺点,造成溯源功能的缺失,用户绑定硬件信息与密钥过程繁琐,电子音像制品文件格式的混乱使用,加密技术缺乏一定灵活性。所以发明一种具有防伪溯源功能、易于扩展、灵活方便的电子音像制品版权管理方法是十分有意义的。

发明内容

[0020] 本发明的目的:旨在提供一种具有防伪与溯源功能的电子音像制品版权管理方法,

[0021] 这种具有溯源功能的电子音像制品版权管理方法,其特征在于:

[0022] (1)由客户端、媒体打包者、许可证发放者三方构成具有溯源功能的电子音像制品版权管理方法框架;媒体打包者承接版权持有者交付的电子音像制品,用户通过客户端在媒体打包者处进行注册、并使用客户端进行登录验证,同时用户经客户端在媒体打包者处购买并下载电子音像制品,在下载过程中由媒体打包者进行打包;许可证发放者生成许可证,对用户权利进行限制;获得许可后的用户经客户端对下载的电子音像制品进行处理;

[0023] (2)由服务器根据用户请求进行密钥的生成和分发;

[0024] (3)利用数字水印技术,嵌入用户信息,实现溯源功能;

[0025] (4)采用特有的文件格式,进行系统信息、用户信息、媒体文件信息的验证管理;

[0026] (5)采用分段加密对电子音像制品进行打包;

[0027] (6)分段加密过程中,每段加密密钥与用户信息相关联;

[0028] (7)提供电子音像制品的预览功能。

[0029] 所述用户通过服务器生成密钥的流程为:

[0030] (a)用户经客户端在服务器端进行注册;

[0031] (b)用户经客户端下载客户端软件,安装并登陆;

[0032] (c)用户客户端随机生成一对非对称加密密钥:公钥A、私钥A;

[0033] (d)用户客户端获取服务器公钥B,并用服务器公钥B加密用户信息、用户硬件信息、公钥A,然后发送至服务器;

[0034] (e)服务器接收数据后,使用服务器私钥B解密数据,获得用户信息、用户硬件信

息、公钥A；

[0035] (f)服务器对用户信息进行验证，如果用户信息不合法，进行(g)，如果用户信息合法，进行(h)；

[0036] (g)用户信息不合法，服务器向客户端发送信息，提示用户；

[0037] (h)用户信息合法，服务器在数据库中对用户硬件信息进行查找，若不存在，进行(i)，若存在，进行(j)；

[0038] (i)用户硬件未注册，服务器对当前用户硬件信息进行注册，生成一对非对称密钥：公钥C、私钥C与用户硬件信息进行绑定；

[0039] (j)用户硬件信息已注册，服务器从数据库中读取与此硬件信息绑定的私钥C；

[0040] (k)服务器使用公钥A，对私钥C进行加密，并发送至客户端；

[0041] (l)客户端接收数据后，使用私钥A进行解密，得到私钥C，并存储于本地。

[0042] 所述的数字水印技术是：在用户下载电子音像制品过程中，服务器针对不同用户，将用户信息制作成特定格式的数字水印数据，采用鲁棒隐藏数字水印技术，将数字水印数据实时嵌入用户下载的电子音像制品中。

[0043] 所述的特有文件格式如下：

[0044] (a)对原始电子音像制品文件进行整体打包，使不同的电子音像制品封装成统一格式，便于管理；

[0045] (b)在文件打包过程中加入系统信息、用户信息、媒体文件信息，使其在播放时进行验证，进行权限管理；

[0046] (c)打包后的文件需要在特定的客户端进行解析播放，从而提高安全性。

[0047] 所述的分段加密对电子音像制品进行打包的方法如下：每段使用的加密密钥由一个特定的种子和用户信息关联生成，提高分段加密的安全性；

[0048] 根据以上技术方案提出的这种具有溯源功能的电子音像制品版权管理方法，与目前国内外同类技术相比较，具有以下优点：

[0049] 1.用户密钥的生成管理更加方便；

[0050] 2.能够对盗版电子音像制品进行溯源；

[0051] 3.文件封装成统一格式，便于扩展和管理

[0052] 4.分段加密方式更加灵活。

附图说明

[0053] 图1为管理方法框架示意图；

[0054] 图2为客户端功能结构示意图；

[0055] 图3为内容提供者功能结构示意图；

[0056] 图4为许可证发放者功能结构示意图；

[0057] 图5为基本下载流程示意图；

[0058] 图6为服务器生成和分发用户密钥方法流程图。

具体实施方式

[0059] 以下结合说明书附图进一步阐述本发明，并给出本发明的实施例。

[0060] 这种具有溯源功能的电子音像制品版权管理方法，其发明的核心在于：由服务器根据用户请求生成用户密钥对，并进行管理和分发；将用户信息利用数字水印技术，嵌入到媒体文件中，实现溯源功能；采用特有文件格式，对电子音像制品进行整体打包，将系统信息、用户信息、媒体文件信息等进行封装；采用分段加密技术，使每段加密密钥与用户信息相关联，媒体文件的权限管理更加灵活。其特征在于：采用由客户端、媒体打包者、许可证发放者三方构成具有溯源功能的电子音像制品版权管理方法框架；媒体打包者承接版权持有者交付的电子音像制品，用户通过客户端在媒体打包者处进行注册、并使用客户端进行登录验证，同时用户经客户端在媒体打包者处购买并下载电子音像制品，在下载过程中由媒体打包者进行打包；许可证发放者生成许可证，对用户权利进行限制；获得许可后的用户经客户端对下载的电子音像制品进行处理；

[0061] (2)由服务器根据用户请求进行密钥的生成和分发；

[0062] (3)利用数字水印技术，嵌入用户信息，实现溯源功能；

[0063] (4)采用特有的文件格式，进行系统信息、用户信息、媒体文件信息的验证管理；

[0064] (5)采用分段加密对电子音像制品进行打包；

[0065] (6)分段加密过程中，每段加密密钥与用户信息相关联；

[0066] (7)提供电子音像制品的预览功能。

[0067] 所述的电子音像制品版权管理方法框架中，媒体打包者承接版权持有者交付的电子音像制品，用户通过客户端在媒体打包者处进行注册、并使用客户端进行登录验证，同时用户经客户端在媒体打包者处购买并下载电子音像制品，在下载过程中由媒体打包者进行打包；许可证发放者生成许可证，对用户权利进行限制；获得许可后的用户经客户端对下载的电子音像制品进行处理。

[0068] 由于采用的数字水印嵌入技术具有实时性，不会使用户下载媒体文件的速度显著下降，因而不会影响用户对电子音像制品的正常下载；此外，嵌入的数字水印数据具有隐藏性，不会使电子音像制品的品质有显著下降，因而不会影响用户对电子音像制品的正常使用；同时，这种嵌入的数字水印数据具有鲁棒性，不会使数字水印数据轻易被去除，因而在电子音像制品盗版后，能够提取数字水印数据，进行溯源追踪。

[0069] 所述用户通过服务器生成密钥的流程为：

[0070] (a)用户经客户端在服务器端进行注册；

[0071] (b)用户经客户端下载客户端软件，安装并登陆；

[0072] (c)用户客户端随机生成一对非对称加密密钥：公钥A、私钥A；

[0073] (d)用户客户端获取服务器公钥B，并用服务器公钥B加密用户信息、用户硬件信息、公钥A，然后发送至服务器；

[0074] (e)服务器接收数据后，使用服务器私钥B解密数据，获得用户信息、用户硬件信息、公钥A；

[0075] (f)服务器对用户信息进行验证，如果用户信息不合法，进行(g)，如果用户信息合法，进行(h)；

[0076] (g)用户信息不合法，服务器向客户端发送信息，提示用户；

[0077] (h)用户信息合法，服务器在数据库中对用户硬件信息进行查找，若不存在，进行(i)，若存在，进行(j)；

[0078] (i)用户硬件未注册，服务器对当前用户硬件信息进行注册，生成一对非对称密钥：公钥C、私钥C与用户硬件信息进行绑定；

[0079] (j)用户硬件信息已注册，服务器从数据库中读取与此硬件信息绑定的私钥C；

[0080] (k)服务器使用公钥A，对私钥C进行加密，并发送至客户端；

[0081] (l)客户端接收数据后，使用私钥A进行解密，得到私钥C，并存储于本地。

[0082] 所述的数字水印技术是：在用户下载电子音像制品过程中，服务器针对不同用户，将用户信息制作成特定格式的数字水印数据，采用鲁棒隐藏数字水印技术，将数字水印数据实时嵌入用户下载的电子音像制品中。

[0083] 所述的特有文件格式如下：

[0084] (a)对原始电子音像制品文件进行整体打包，使不同的电子音像制品封装成统一格式，便于管理；

[0085] (b)在文件打包过程中加入系统信息、用户信息、媒体文件信息，使其在播放时进行验证，进行权限管理；

[0086] (c)打包后的文件需要在特定的客户端进行解析播放，从而提高安全性。

[0087] 所述的分段加密对电子音像制品进行打包的方法如下：每段使用的加密密钥由一个特定的种子和用户信息关联生成，达到提高分段加密的安全性。

[0088] 所述用户根据分段加密密钥及用户权限对电子音像制品进行部分解密，实现预览。

[0089] 下面通过具体实施方式对本发明做进一步说明。

[0090] 实例1：

[0091] 1.整体框架设计

[0092] (1)角色和功能实体

[0093] 为了更好的对电子音像制品的版权进行管理，采用用户、内容提供者、许可证发放者三方框架。用户使用客户端对授权的电子音像制品进行播放等操作；内容提供者将得到有具有版权的电子音像制品进行打包加密等操作，同时将其出售给用户；许可证发放者则是与内容提供者无关的第三方，主要对用户购买的电子音像制品的权限进行管理。

[0094] 采用三方的架构，尤其是内容提供者与认可证发放者的分开与独立运行，能够防止内容提供者伪造用户权利，保证用户基本权利不受侵害，同时能够对不同的内容提供者进行管理和约束，防止内容提供者对授权的电子音像制品进行不合理的滥用。

[0095] 用户：用户使用的客户端是经过认证中心认证的软件，其利用系统硬件信息，产生固定的一对公钥私钥。利用这对密钥，客户端可以对根据相应权限对媒体文件进行相应的操作。

[0096] 内容提供者：内容提供者从媒体提供者处获得未加密媒体文件，经过加密打包后，提供给用户，同时申请为用户申请相应许可证，维护用户相应权限信息。

[0097] 许可证发放者：许可证发放者管理不同的内容提供者信息，监控内容提供者的行为；接受内容提供者的许可证请求，验证申请信息，生成许可证，发放许可证。

[0098] 基本流程：(见附图6)

[0099] 未加密媒体文件由打包者进行加密打包，生成打包媒体文件，提供给用户进行购买下载。用户需要在媒体打包者的网站上进行注册，注册成功后即可在媒体打包者网站进

行数字媒体文件的购买。

[0100] 在用户购买成功后，由媒体打包者向许可证发放者申请用户相应的权限的许可证，许可证发放者根据用户的权限及加密媒体文件的密钥，生成用户相应的许可证，并返回给媒体打包者。媒体打包者将为用户申请到的许可证和用户购买的加密媒体文件提供给用户下载。

[0101] 用户下载后，使用认证的客户端，根据其购买的相应权限，使用已下载的数字媒体文件。

[0102] 其中，为了保证用户的权利，防止内容提供者滥用授权的电子音像制品，许可证发放者必须为可靠的无利益关系的第三方机构。其可以通过对内容提供者的管理、监控，保证内容提供者对授权电子音像制品的合理使用。

[0103] 2.信任和安全模型

[0104] 对于所有的DRM系统而言，最关键的部分是如何对具有版权保护的数字媒体文件进行权限的限制和控制。其中，最大的问题是如何保证客户的端的合法性以及许可证发放的限制和保护。

[0105] (1)数字媒体文件的打包

[0106] 每一个数字媒体文件对应一个Content ID，每一个内容打包者对应一个Key Seed。内容打包者使用Content ID和Key Seed生成CEK，采用对称加密算法，对数字媒体文件进行加密，同时生成相应的文件头，然后对文件头与加密数字媒体打包。

[0107] 内容打包者的Key Seed要从可靠的第三方——许可证发放者处申请，许可证发放者要对内容打包者的资质等进行评估，如果合乎安全规范，则可生成唯一的标识符——Key Seed，并将其提供给内容打包者使用。如果内容打包者出现安全问题或者其他违反规定的行为，许可证发放者可以对其进行相应的管控。

[0108] (2)客户端的认证

[0109] 每一个客户端由其唯一硬件标识生成一对唯一的私钥和公钥。客户端将其公钥及一些必要信息，发送给数字认证中心，经数字认证中心认证后发放客户端的数字证书。内容打包者和许可证发放者收到客户端的数字证书，通过数字认证中心的认证后，即可确保数字证书中的公钥是经过认证的客户端的。

[0110] (3)许可证的生成及保护

[0111] 许可证包含了用户购买的权限信息和解密数字媒体文件的密钥，许可证发放者根据这些信息，生成许可证。

[0112] 许可证的生成过程是由许可证发放者进行，其首先要对用户的权利信息和电子音像制品的密钥进行签名处理，防止在传输过程中内容被篡改；其次要对此重要信息进行加密处理，防止在传输过程中被人窃取，而导致用户信息的泄露。

[0113] (4)文件的传输

[0114] 客户端、内容打包者、许可证发放者都经过了数字认证中心的认证，三者之间的公钥传递是安全可靠的。在文件的传输过程中，对于敏感信息都进行了的加密处理，保证了文件传输过程的安全性。

[0115] (5)内容保护

[0116] 由于加密密钥是由Content ID和Key Seed生成，因此保证了不同的数字媒体文件

的加密密钥是不同，确保了媒体文件的加密安全性。

[0117] 同时在传递CEK的过程中，即许可证的发放，对含有CEK的许可证使用相应客户端的公钥进行了加密，保证了只有合法的客户端才能解密，同时对许可证内容使用许可证发放者的私钥进行了数字签名，确保许可证内容不会被篡改。

[0118] 3.文件结构设计

[0119] 文件存储采用box的方式，每个文件都是由必须box和一些可选box构成。每个box中含有特定信息，通过这种文件结构，可以将同一类信息封装在一个box个，便于文件生成及解析。同时，对于较为敏感的box信息可以单独进行处理。

[0120] 为了防止在传输过程中含有用户权利信息的box被篡改，在内容提供者对电子音像制品的基本信息进行打包的同时，要使用其私钥进行签名处理。用户在接收到这一部分信息时，要使用内容提供者的公钥进行签名的验证，这样防止在传输过程中，重要的媒体文件信息被篡改。

[0121] 同样，在许可证发放者将用户权利信息及电子音像制品的解密密钥发放给用户时，也要进行相同的签名验证，防止内容被篡改。同时，由于这一部分的信息较为重要，在进行签名后，还要对其进行必要的加密处理，然后再封装进box中，最后经由内容提供者打包后，传递给用户。

[0122] (1)基本文件单元

[0123] box的主要结构如下表所示：

[0124]

size	4bytes	box大小
type	4bytes	box类型
version	4bytes	box版本
info	size-12bytes	box数据

[0125] size:4字节，表示box的大小；

[0126] type:4字节，表示box的类型；

[0127] version:4字节，表示box的版本，box升级标识；

[0128] info:size-12字节，表示box的数据，不同类型的box数据结构不同。

[0129] 如果size大于4字节能表示的范围，则采用以下结构：

[0130]

size	4bytes	0x0000 0000
type	4bytes	box类型
version	4bytes	box版本
real_size	8bytes	box大小
info	size-12bytes	box数据

[0131] ※所有的sign box均在其签名内容的最后面。

[0132] (2)文件头

[0133] 文件头的必须box为:fdrm,fhdr,sign,其结构分别如下表所示:fdrm主要记录了DRM系统的信息，便于DRM系统的升级及维护。

[0134]

fdrm box		
size	4bytes	fdrm 大小
type	4bytes	fdrm
version	4bytes	fdrm 版本
drm_version	4bytes	drm 系统版本
file_type	4bytes	文件类型

[0135] 其中file_type的取值如下表所示：

[0136]

0x0000 0000	音频mp3
0x0000 0001	视频mp4
0x0000 0002	视频avi

[0137] ※此表可根据具体情况进行扩充。

[0138] fhdr主要记录了电子音像制品的ID及内容提供者的URL。

[0139]

fhdr box		
size	4bytes	fhdr 大小
type	4bytes	fhdr
version	4bytes	fhdr 版本
content_id	4bytes	Content ID
cp_url	size－16bytes	CP URL

[0140] sign主要用来对特定box内信息进行签名。

[0141]

sign box		
size	4bytes	sign 大小
type	4bytes	sign
version	4bytes	sign 版本
algorithm	4bytes	签名算法
signature	由算法确定	数字签名

[0142] 文件头的非必须box——cinf，主要记录了文件的一些基本信息。

[0143]

cinf box		
size	4bytes	cinf 大小
type	4bytes	cinf
version	4bytes	cinf 版本
title_len	4bytes	标题长度
title	title_len	标题
author_len	4bytes	作者长度
author	author_len	作者

[0144] ※此表可根据具体情况进行扩充。

[0145] (3)数据部分

[0146] 数据部分为一个必须box:cont,其结构如下表所示:

[0147] cont主要保存了加密的电子音像制品信息。

[0148]

cont box		
size	4bytes	cont 大小
type	4bytes	cont
version	4bytes	cont 版本
media_data	size - 12bytes	数字媒体文件内容

[0149] 其中,数字媒体文件内容采用加密后的二进制码码流存储。

[0150] (4)许可证

[0151] 许可证的必须box为:robj,sign,其结构如下表所示(sign box结构已在文件头说明中给出):

[0152] robj主要保存了用户的权利信息及电子音像制品的密钥。这一部分信息在打包时要进行签名及加密处理。

[0153]

robj box		
size	4bytes	robj 大小
type	4bytes	robj
version	4bytes	robj 版本

[0154]

play_permission	4bytes	播放许可
play_times	4bytes	播放次数
start_time	4bytes	许可证开始时间
end_time	4bytes	许可证结束时间
ecryption	4bytes	加密方法
key_len	4bytes	密钥长度
data_key	由算法确定	媒体文件解密密钥

[0155] 加密方法如下：

[0156]

0x0000 0000	无加密算法(不推荐使用)
0x0000 0001	AES_128_CBC
0x0000 0002	AES_128_CTR
0x0000 0003	DES
0x0000 0004	RC4

[0157] ※此表可根据具体情况进行扩充。

[0158] 4.数据库表设计

[0159] 用户表(t_user)

id	username	password	gender	email	key_num	reg_time	last_time	last_ip
用户id	用户名	密码	性别	邮箱	注册公钥数	注册时间	最后登陆时间	最后登陆ip

[0160] 媒体内容表(t_content)

id	content_id	name	type	size	path	encryption	time	username	resolution
媒体内容id	媒体文件id	文件名	类型	大小	存储路径	加密算法	上传时间	上传用户	分辨率

[0161] 用户订单表(t_order)

id	content_id	username	right1	right2	right3	.....	state	key_num
订单号	媒体文件id	用户名				.....	当前状态	公钥总数

[0162] 用户公钥表(t_user_key)

username	key	device	reg_time
用户名	用户公钥	设备类别	注册时间

[0163] 5.基本下载流程

[0164] 图6介绍的是基本下载流程，包括用户获得DRM保护的数字媒体文件，以及如何根据相应权限使用数字媒体文件。

[0165] (1)用户在内容打包者处进行注册；

[0166] (2)用户在内容打包者处浏览媒体文件，选定媒体文件并付费；

[0167] (3)内容打包者根据用户的购买情况，向许可证发放者进行许可证的申请；

[0168] (4)许可证发放者根据用户购买权限及CEK，生成许可证；

[0169] (5)媒体打包者收到将媒体文件及许可证提供给用户下载；

[0170] (6)用户使用专用播放器，根据相应权限使用下载的媒体文件。

[0171] 6.实例实现

[0172] 在Windows平台上，采用IIS+PHP+MySQL框架，搭建了内容提供者及许可证发放者测试平台，实现了用户注册、登录、信息管理、购买和下载媒体文件等功能；采用Qt+Mplayer，搭建了测试用客户端，实现了本地播放媒体文件等功能。在用户购买和下载媒体文件的过程中，内容提供者使用鲁棒性数字水印技术，将用户信息嵌入到媒体文件中；使用对称加密技术，对媒体文件进行分段加密；使用非对称加密技术，对用户相应权限信息进行加密。同时，由许可证发放者生成相对应的许可证。用户可通过客户端对所购买和下载的媒体文件进行播放。

[0173] 本系统支持个人电脑、平板电脑、手机等常见设备，支持不同操作系统(Windows、Linux等)；根据购买的媒体文件权限，用户可以在其持有的不同设备上，播放其购买的媒体文件；支持主流的多媒体文件格式，视频格式：mp4、avi、rmvb、mkv等，音频格式：mp3、wav、ape、flac等。

[0174] 本系统使用三方架构，将拥有授权电子音像制品的内容打包者与进行权限管理及许可证发放的许可证发放者进行分离，在系统加框上更好地控制电子音像制品的版权，让电子音像制品的版得到保护的同时，保证用户的基本权利不被侵犯。与此同时，在电子音像制品出现盗版时，提取电子音像制品中的水印信息，确定盗版来源，做到溯源的功能。

[0175] 上述仅为本发明的部分优选实施例，本发明并不仅限于实施例的内容。对于本领域中的技术人员来说，在本发明方法范围内可以有各种变化和更改，所作的任何变化和更改，均在本发明保护范围之内。

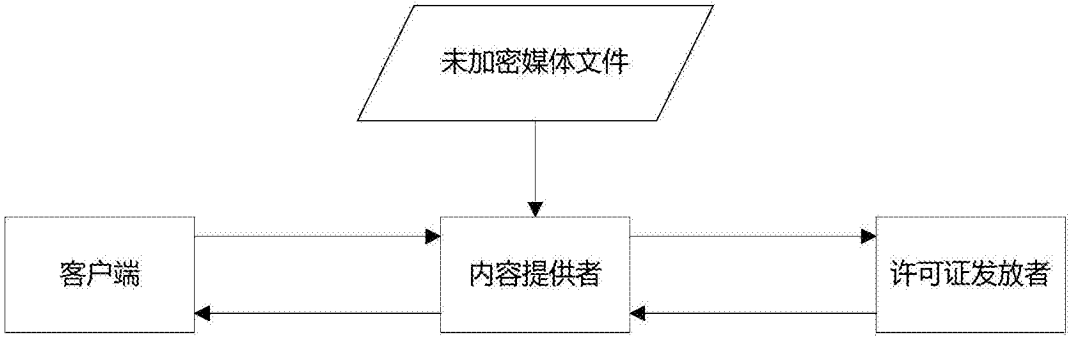

未加密媒体文件
客户端
内容提供者
许可证发放者

图1

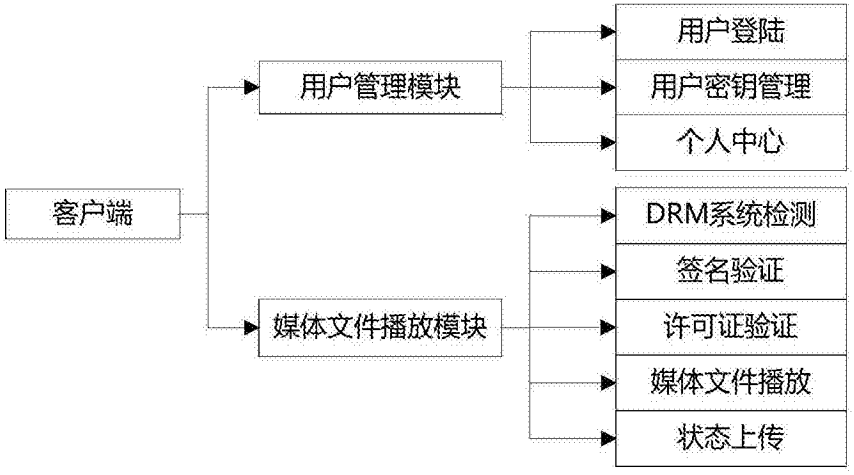

客户端
用户管理模块
媒体文件播放模块
用户登陆
用户密钥管理
个人中心
DRM系统检测
签名验证
许可证验证
媒体文件播放
状态上传

图2

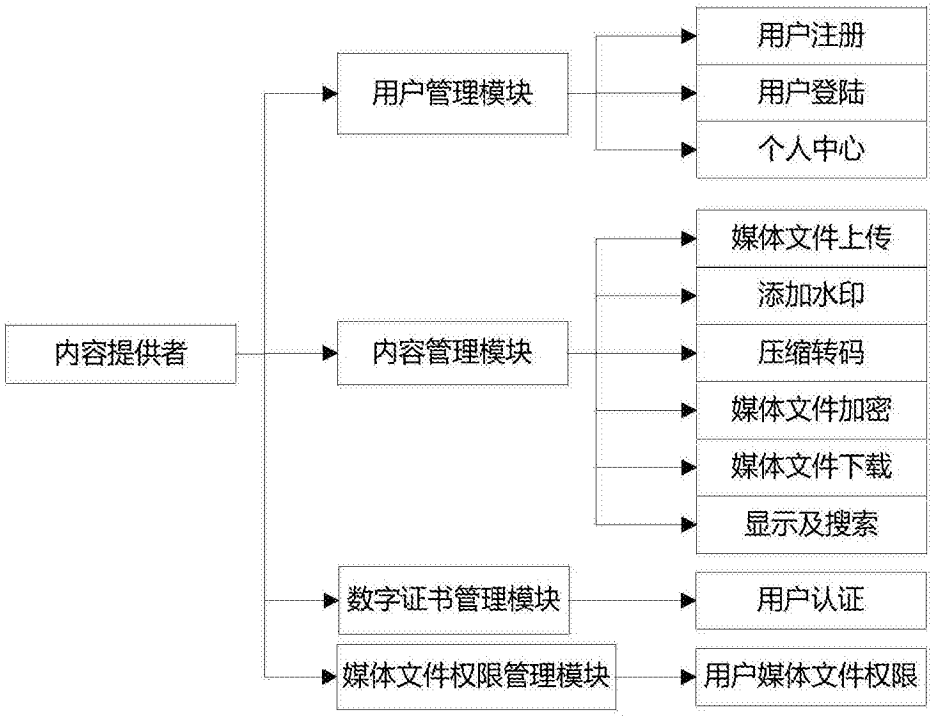

内容提供者
用户管理模块
用户注册
用户登陆
个人中心
内容管理模块
媒体文件上传
添加水印
压缩转码
媒体文件加密
媒体文件下载
显示及搜索
数字证书管理模块
用户认证
媒体文件权限管理模块
用户媒体文件权限

图3

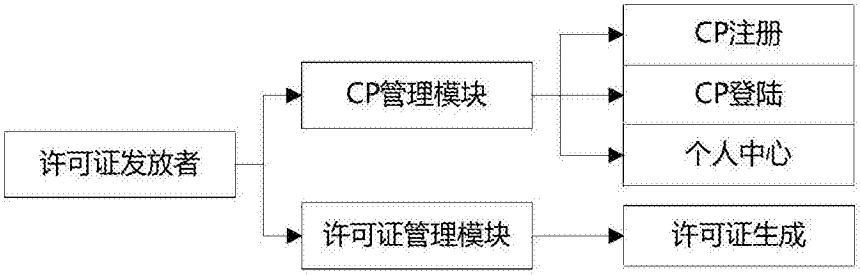

许可证发放者
CP管理模块
CP注册
CP登陆
个人中心
许可证管理模块
许可证生成

图4

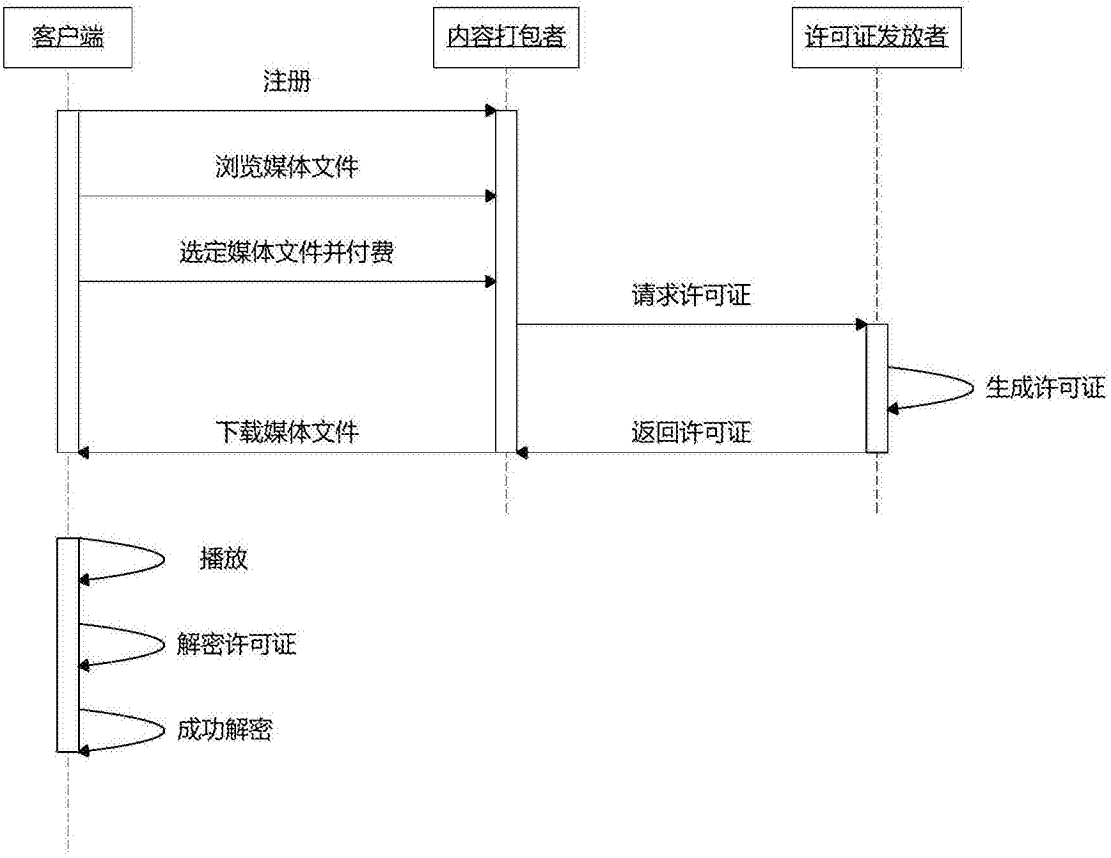

客户端
内容打包者
许可证发放者
注册
浏览媒体文件
选定媒体文件并付费
请求许可证
生成许可证
下载媒体文件
返回许可证
播放
解密许可证
成功解密

图5

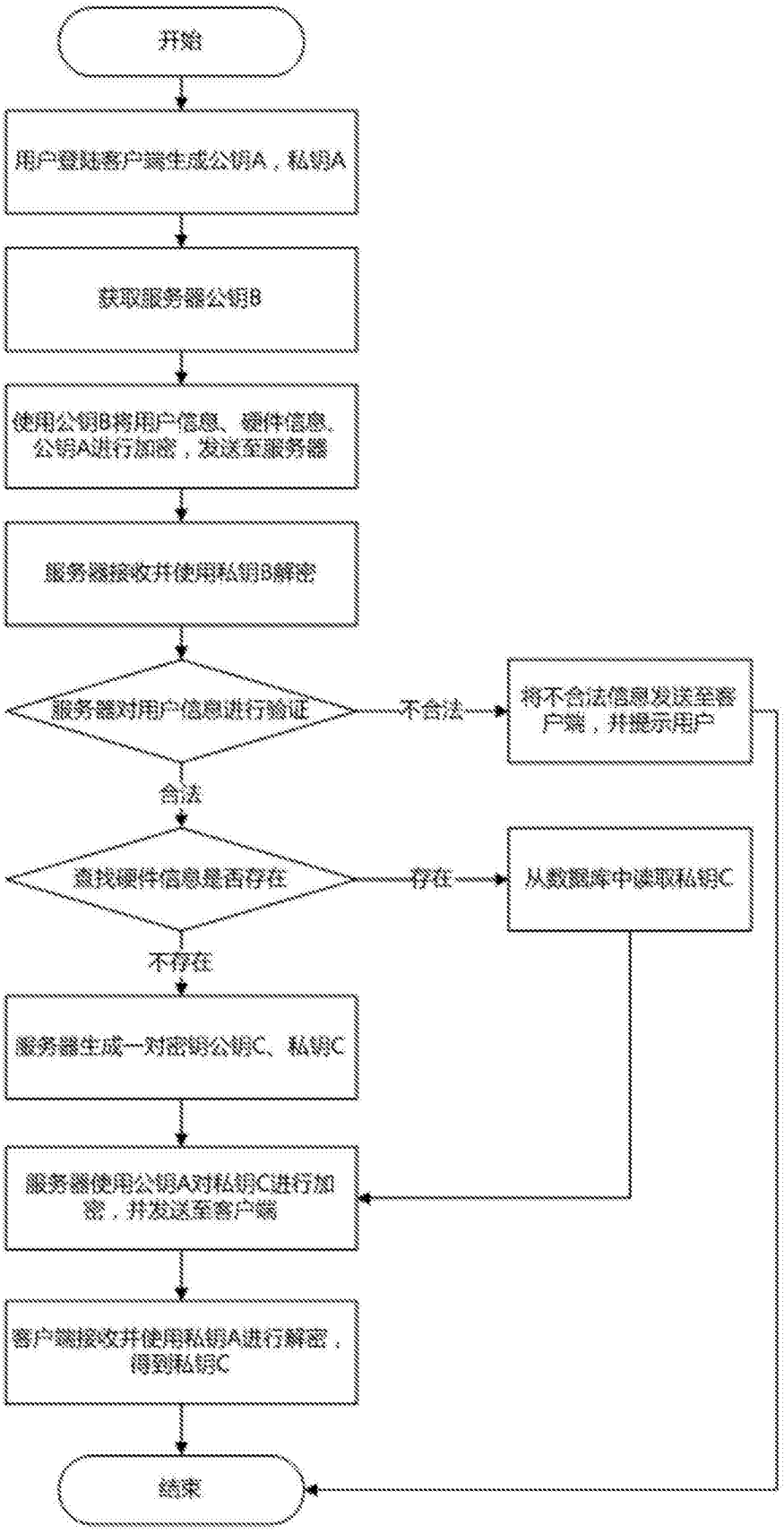

开始
用户登陆客户端生成公钥A，私钥A
获取服务器公钥B
使用公钥B将用户信息、硬件信息、公钥A进行加密，发送至服务器
服务器接收并使用私钥B解密
服务器对用户信息进行验证
不合法
将不合法信息发送至客户端，并提示用户
合法
查找硬件信息是否存在
存在
从数据库中读取私钥C
不存在
服务器生成一对密钥公钥C、私钥C
服务器使用公钥A对私钥C进行加密，并发送至客户端
客户端接收并使用私钥A进行解密，得到私钥C
结束

图6