第34卷 第24期 计 算 机 工 程 2008年12月
Vol.34 No.24 Computer Engineering December 2008
·安全技术· 文章编号：1000—3428(2008)24—0134—03 文献标识码：A 中图分类号：TP309+.2

基于DRM证书机制的数字作品分发方案

张 金，李庆诚，张振华，赵 亮
(南开大学计算机科学与技术系，天津 300071)

摘 要：针对消费者分发需求多样化与数字版权管理系统中严格限定传播范围之间的矛盾，建立分发模型描述各种分发问题，其中，用户之间的分发和设备之间的分发得以区别描述。在该模型的基础上提出一种采用双证书机制的分发方案。将数字作品分割后，通过使用独立密钥并配合相关的链型证书机制和分发权限管理，使消费者成为分发过程的参与人。分发权限的继承性赋予了消费者在分发过程中的控制权利。

关键词：数字版权管理；分发模型；独立密钥链

Digital Works Distribution Scheme Based on DRM License Mechanism

ZHANG Jin, LI Qing-cheng, ZHANG Zhen-hua, ZHAO Liang
(Department of Computer Science, Nankai University, Tianjin 300071)

【Abstract】 This paper builds a distribution model for describing distribution problems between consumers' diversified distribution demands and strictly restricted scope of the spread in Digital Rights Management(DRM). A related distribution mechanism based on the model, which takes different licenses for different distribution, is substituted. And consumers can configure distribution rights inherited with distribution processing with the help of separate keys chain, license chain mechanism and distribution rights management.

【Key words】 Digital Rights Management(DRM); distribution model; separate keys chain

1 概述

各种数字化技术的飞速发展带来了数字作品的繁荣兴盛。同时，数字作品便于复制、可利于网络快速传播等特点使得对其版权的处理成为数字产业中的关键问题，消费者购买作品后的分发问题更是其中的焦点。在传统的音像和纸质出版行业中，由于磁带和纸张存在自然成本与复制损耗等诸多因素，分发带来的问题并不突出。在新生的网络环境下，数字作品的无损复制和网络渠道的高速传播使这一问题日渐突出。数字版权管理(Digital Rights Management, DRM)的主要目的是保护数字作品内容，维护版权所有者和用户的合法权益[1]，即解决数字产业中的版权问题。分发问题是DRM的关注重点之一。而通过严格限制或者禁止分发的方法处理这一问题却遭到广大消费者的抵制和声讨，因为这影响到消费者权利的转移和继承。文献[2]对相关问题进行了较为深入的分析。

2 分发模型与问题描述

2.1 基本概念与相关研究

分发问题中的一个重要概念是超级分发(Superdistribution)[3]，它通常指消费者通过从服务器获取证书的方式将作品分发给其他消费者的行为。本文将分发行为分解为2种行为：自发与转发。同一用户将其所购买的数字作品在自己拥有的设备间转移的行为称为自发，用户间转移数字作品的行为称为转发(转借)。

针对传统方案中分发必须在网络环境下进行的情况，Kwok等人提出通过建立本地的证书生成组件Local DRM Service Center和External DRM Service Center来解决[4]。而Cheung等人则以嵌入数字水印的方式进行分发的标记[5]。但实际上，数字水印过高的计算代价和多水印叠加导致的鲁棒性下降问题成为这一方案的弊端。OMA是移动通信领域的版权管理体系方案。设定环境的特殊性使其分发设置中允许作品携带一个内容样本。

本文针对当前DRM分发机制的缺点，提出一种利用传播的分发机制。本设计方案基于以下基本观点：

(1)分发机制应当支持分发行为的进行。在一定程度上，消费者可以参与分发规则的制订。

(2)以干扰取代禁止。随着分发过程的不断深入，非厂商授权的副本中将会出现越来越多的干扰。当这些干扰被广告信息取代时，新的商业模式即可诞生。

2.2 分发模型

文献[6]用传播树的形式描述数字作品的分发问题。本文的模型以其为基础，以设备为基本节点进行分析。因为数字作品的播放、呈现和分发都是通过设备进行的，所以任何一种分发行为均可以建立如图1所示的类似模型，其中，实线表示数字作品的实际传输路径；虚线表示数字作品传输的逻辑路径。在模型中，消费者的第一个获得数字作品副本的设备称为基点设备，发起分发的设备称为上位设备，设备持有人称为发起人；接受分发的设备称为下位设备，设备持有人称为接收人。从上位到下位的方向为分发方向。

基金项目：天津市科技发展计划基金资助项目(06YFGZGX04000)
作者简介：张 金(1979－)，男，博士，主研方向：信息安全，数字水印；李庆诚，教授、博士；张振华、赵 亮，硕士
收稿日期：2008-04-30 **E-mail：**hustzhangjin@163.com

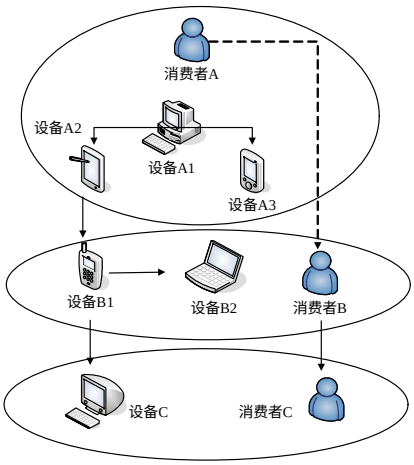

图 1　分发模型

模型中的任意一个设备沿分发的反方向到达最远设备路径上经过的设备数为该设备处的分发深度。而忽略路径方向，该设备能够不经过其他设备直接到达的设备数称为该设备处的分发广度。由于转发的收敛性，基点设备的分发深度表示当前设备持有者与购买数字作品消费者的距离。同理，基点设备的分发广度用于表示当前消费者在分发过程中的影响，即分发范围。

可利用极限假设的方式逼近分发模型的上确界：全局共有N个购买了数字作品的消费者，每个消费者每分发周期与F人共享数字作品，那么在T个分发周期后，全局最大副本数S^*为

$$S^* = N + \sum_{j=1}^{N} \sum_{i=0}^{T-1} (T-i) F^{i+1},\ T>0, F>0, N>1 \qquad (1)$$

3　方案综述

如第 2 节所述，分发行为可以分解为自发和转发。由于数字作品副本的获得大多由原作进行复制所得，因此本方案用证书对数字作品的访问和浏览进行控制，使用 2 种证书应对这 2 种不同的分发行为。

在消费者的自发行为中，必须将自发证书导入设备才能不受干扰地浏览完整的数字作品。而导入转发证书的设备只能浏览数字作品的部分内容，且不得不浏览商家所提供的广告。随着转发次数的增多，可浏览的内容将逐渐减少，广告则逐渐增多。

3.1　设计目标

综上所述，本文机制的具体设计目标如下：

(1)支持消费者的自发和转发 2 种分发行为。用户在一定程度上可以参与分发规则的制订。分发行为可以在离线环境下进行，而不依赖于第三方设备。

(2)在转发过程中，强制下位用户在观看数字作品副本的同时，浏览作为干扰的广告信息。随着转发过程的深入，数字作品中出现的广告信息越来越多，而数字作品的原始内容则递减。

3.2　方案假设

本文的方案基于下述假设：

(1)适用的数字作品对象为文件格式相对宽松、不存在严格校验的数字作品。当数字作品体积较小时，如数字读物、数字音乐，本机制能发挥较好的效果。而在数字作品体积较大的情况下，例如高清晰数字电影，机制的表现将受用户设备的性能影响。

(2)所有相关设备和对象必须兼容于同一个 DRM 框架内。兼容性问题不属于本文的论述范畴。

(3)所有参与分发的用户设备必须具有公私密钥机制和数字签名组件等基本安全保障功能，以保证本机制的运行。同时，设备中具有可靠的计时和文件访问控制机制。

在不符合上述假设的情况下，本文机制不一定能达到预计的效果。

3.3　机制运行流程

本方案的基本实现思路是：将原始数字作品预分割为 N 段，再使用独立的密钥分别加密，组成供用户购买的实体。每个用户获取的数字作品实体都需要不同的密钥链进行解密。自发证书由于绑定用户个人信息，因此给予用户较宽松的使用权限。而在转发过程中，用户可以指定利用该转发证书所许可派生的证书数量。同时，下位设备必须下载与分发证书相应的数字作品副本才能正确浏览。每经历一次转发，证书中的密钥链就会被裁减一定的长度。数字作品播放中因此产生的空位被相应的广告信息所取代。由于证书的导入不需要第三方设备参与，因此分发过程可以在离线环境下实现。分发流程如图 2 所示。

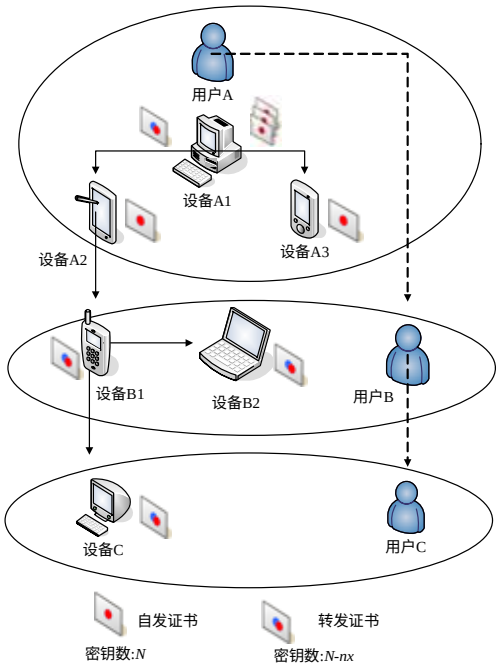

图 2　分发流程

(1)用户 A 付费购买了某款数字产品，根据用户的选择，服务器向用户颁发 m 份包含全部 N 个解密密钥的自发证书和一份可供 p 个用户使用的包含 N-x 个解密密钥的转发证书。这些证书都被存储在设备 A1 上。

(2)用户 A 将 2 份自发证书导入自己的设备 A2,A3 中，并输入自己的个人重要信息将 2 份证书激活，例如注册的真实姓名，产品就可以在 A2, A3 上被用户 A 无限制地浏览了。由于自发证书的激活需要用户的个人重要信息，用户不会将之与其他用户共享，因此对自发证书的数量可以作出较为宽松的规定。

(3)用户 A 将转发证书导入设备 A2 中，并向用户 B 进行新转发证书的发布。新的转发证书中存在 N-x 个密钥。用户 A 使用自己的公私密钥系统对这些密钥加密。同时，新证书中的转发用户许可在用户 A 的制订下变为 q 个。这份用户许可使用 A 的数字签名进行确认。

(4)将 A 颁发的转发证书导入设备 B1 后，用户 B 即可播放浏览数字作品 DC 了。但是，用户 B 所浏览的并不是完整的 DC，只是他能有效解密的内容和一部分厂商所提供的广告。数字作品的结构设置使用户 B 不得不在浏览数字作品的同时观看广告。

(5)同步骤(3)、步骤(4)，用户 B 向用户 C 的设备 C1 颁发转发证书。这个证书中含有的有效密钥数将减少为 N-2x。用户 C 所能浏览的数字作品中将包括更多的广告信息和更少的原始内容。如果 C 希望获得数字作品中缺失的部分，则必须购买一份完整的数字作品。

(6)如果用户 B 希望向自己的另一台设备 B2 进行自发，由于无法获得自发证书，因此只能通过颁布转发证书来实现。

4 机制实现要点

根据第 3 节，本方案的设计要点在于：

(1)数字作品的封装

一方面保证原始数字作品被分割后可以被有效还原组合并顺利插入广告内容；另一方面保证广告内容不会被用户轻易屏蔽。

(2)证书结构的设计

自发证书中需要添加进与用户个人信息相关的部分，以防止用户间的随意共享。转发证书则需要在防止篡改的同时保证其中的有效密钥呈递减趋势。

4.1 数字作品封装

原始数字作品是以文件格式存在的，将文件格式脱离之后可以获取仅承载原始信息的元数据体。数字作品封装的处理顺序如下：

(1)将原始数字作品文件解析为元数据体和文件格式信息。

(2)将元数据体分割成大小不等的 N 块，保证这些块的体积都是广告数据块体积的公倍数。根据对称加密算法，利用 N 个独立密钥对其加密，得到 N 个数据段。将这些数据块连同广告数据块和文件格式信息一起封装成为供用户下载的数字作品实体。

(3)根据元数据体的情况，将用到的加密密钥生成长度为 N 的密钥链。再将实体信息和此密钥链传递给证书服务器，供生成证书使用。

考虑到实现的代价问题，不需要每一个付费消费者都有完全不同的实体。对某一个数字作品而言，可以对其片段采用有限次数的加密，而后通过对其进行组合来达到接近完全独立加密的效果。

由于被加密的是脱离格式的元数据体，因此广告内容只要根据元数据体的形式安排就可以被顺利地加入，与被解密的数据一起生成带有广告内容的数字作品。另一方面，由于被裁减掉的加密块体积是不等的，因此被加入的不等长广告内容也无法用固定长度跳转等方式被用户过滤掉。

4.2 分发证书结构

本方案中涉及的自发证书 SL 和转发证书 DL 具有类似的结构。其中，转发证书由于可以被用户的设备生成，因此更加复杂。转发证书由上位设备的数字签名进行验证，其结构如下：

$$DL=\{\{BR\}_{signS},E(Keys_{N-nx},Idx)_{host},LU\}_{signhost} \quad (2)$$

其中：

(1)BR 表示对数字作品的基本访问权限，例如有效时间、许可访问次数。这个部分由服务商的数字签名进行验证。

(2)$E(Keys_{N-nx},\ Idx)_{host}$表示将含有$N$-$nx$个密钥链及其索引$Idx$用上位设备的私钥进行非对称加密。每一次转发，密钥链中都将有x个密钥被删除，由等长的空字符取代。当$nx+x>N$时，不再允许生成转发证书。Idx用来对密钥链的修改情况作说明，以便设备在播放数字产品时知道广告内容应该插入的位置。但如果转发证书由服务商签发，将不对密钥链的长度进行裁减。

(3)LU是关于允许转发人数的用户许可，如式(3)是一个类似递归的结构，由颁发它的上位设备进行数字签名，包括转发链上从服务商签名的初始LU开始的所有记录。LU由上位用户设定，表示颁发证书设备对所继承LU的修正，$\{lux\}_x$是一个递减序列：

$$LU=\{\{\{\{LU\}_{signS},lu1\}_{signhost1},lu2\}_{signhost2},\cdots,lun\}_{signhostn} \quad (3)$$

自发证书的结构类似于式(3)，但要由服务商的数字签名验证。其中，密钥链是完整的，不存在$\{lux\}_x$这样的修正序列，但是要由结合用户个人重要信息的组合密码进行解密。

5 结束语

数字版权管理是为了保护商家和作者的版权而出现的。虽然在技术层面上对版权的保护起到了促进作用，但在一定程度上限制了数字作品的传播。数字作品传播的重要方式是分发过程，只要 DRM 对分发问题处理得当，就能挽回消费者的信心。

本文正是出于这样的考虑，在建立分发模型的基础上，提出了基于证书机制的双证书分发处理方案。让消费者参与到传播过程中，并赋予其一定的控制分发权利。同时，以作为干扰的广告信息取代严格的禁止拷贝。随着分发的深入，广告信息将不断增多。本方案在缓和消费者对抗情绪的同时，开辟了新的商业模式。

参考文献

[1] Bechtold S. The Present and Future of Digital Rights Management——Musings on Emerging Legal Problems[M]//Becker E. Digital Rights Management: Technological, Economic, Legal and Political Aspects. Berlin: Springer-Verlag, 2003: 597-654.

[2] Petkovic M, Li Hong. Digital Inheritance of Personal and Commercial Content Using DRM[C]//Proceedings of Consumer Communications and Networking Conference. [S. l.]: IEEE Press, 2007.

[3] Ryoichi M, Masaji K. Superdistribution: The Concept and the Architecture[J]. Transactions on IEICE, 1990, E73(7):1133-1146.

[4] Sai Ho Kwok, Lui Siu Man. A License Management Model for Peer-to-Peer Music Sharing[J]. International Journal of Information Technology and Decision Making, 2002, 1(3): 541-558.

[5] Cheung S C, Curreem H. Rights Protection for Digital Content Redistribution over the Internet[C]//Proceedings of the 26th Annual International Computer Software and Applications Conference. [S. l.]: IEEE Computer Society, 2002: 105-110.

[6] 李庆诚, 毛永康, 张 金, 等. 基于 D2RM 数字作品转借问题研究[J]. 计算机工程与设计, 2007, 28(6): 1402-1404.