# 多媒体数字产品版权保护模型研究与设计

孟芳慧[1,2] 曹宝香[1] 杨义先[2] 钮心忻[2]
(曲阜师范大学计算机科学学院 日照 276826)[1]
(北京邮电大学网络与交换技术国家重点实验室信息安全中心 北京 100876)[2]

**摘 要** 非法的盗版行为侵害了创作者的合法权益,使得多媒体信息的版权保护问题变得十分重要。通过分析一般的版权保护管理系统,提出了一种有效保护多媒体信息版权的模型。该模型综合利用鲁棒水印和脆弱水印对多媒体信息进行4次水印嵌入;采用全文件加密的方式对多媒体信息加密;使用基于双缓冲机制及安全存储机制的专门的客户端软件对信息解密。最后通过性能分析可知,在没有降低系统的权威性、公平性、实用性的前提下,该模型提高了整个DRM系统的安全性。

**关键词** 数字版权管理,鲁棒水印,脆弱水印,多媒体文件加/解密,数字签名

**中图法分类号** TP309.2 **文献标识码** A

## Research and Design of Multimedia Digital Products Copyright Protection Model

MENG Fang-hui[1,2] CAO Bao-xiang[1] YANG Yi-xian[2] NIU Xin-xin[2]
(College of Computer Science, Qufu Normal University, Rizhao 276826, China)[1]
(Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China)[2]

**Abstract** Illegal acts of piracy violate the legitimate interests of creators, making copyright protection of multimedia information to become very important. Based on the analysis about the general copyright protection management system, we proposed an efficient model for copyright protection of multimedia information. In the model, watermarking is embedded four times with comprehensive utilization of robust watermarking and fragile watermarking for multimedia; multimedia information is encrypted by the method of full file encryption; special client software, which adopts double buffering mechanism and secure storage mechanism, is used for information decryption. Finally, performance analysis shows that the model improves the security of the DRM system under the premise of not reducing its authority, fairness, and practice.

**Keywords** Digital rights management (DRM), Robust watermarking, Fragile watermarking, Encryption/Decryption for multimedia, Digital signature

## 1 引言

近几年来,数字多媒体发展如日中天。键盘鼠标替换了纸笔,许多创作与生产成果以数字方式进行存储和传输;多媒体网上交易为数字产品的宣传推广以及进一步的利用和转化提供了便利的途径。

数字化使多媒体的表示、存储和传播变得简单灵活,同时计算机、打印机和扫描仪等设备质量的提高,使得数字产品副本可以保持很好的质量,在未经作品所有者的许可下非法用户很容易复制和传播有版权的数字媒体内容。另外,部分网络运营商出于商业目的,大量非法上传未经授权的数字产品,极大地侵害了数字产品创作者的合法权益。由此带来了知识产权(Intellectual Property Right, IPR)的保护问题。若得不到可靠的保障,很多版权所有者都不愿轻易公开其所拥有的数字产品,阻碍了数字产品自身的发展及传播。

为了从技术上解决数字作品的这些版权保护问题,出现了数字版权管理技术DRM(Digital Rights Management)。目前,比较流行的是基于密码学的数字版权管理技术;基于数字水印的版权保护技术也被广泛研究。鉴于两种技术各有不足,本文的模型是在密码学技术与数字水印技术相结合的基础上实现对数字产品版权的保护。

## 2 数字版权管理技术研究现状

数字版权管理是在制作、发布和使用数字作品的过程中,

到稿日期:2012-03-01 返修日期:2012-07-05 本文受国家973项目(2007CB311203),国家自然科学基金(60803157,90812001),国家242项目(2009A105),国家标准制定计划(20080200-T-339),国家质检公益性科研专项(10-126),山东省自然科学基金项目(ZR2009GM009,ZR2012FQ011),山东省高等学校科技计划项目(J12LN06)资助。

**孟芳慧**(1989—),女,硕士生,主要研究方向为多媒体数字水印等,E-mail:mf_hui_2008@163.com;**曹宝香**(1955—),男,教授,硕士生导师,主要研究方向为企业信息化与系统集成;**杨义先**(1961—),男,博士,教授,主要研究方向为密码学、计算机网络与信息安全;**钮心忻**(1963—),女,博士,教授,主要研究方向为数字水印、信息隐藏、隐写分析。

保护数字内容提供者、发行商和消费者的合法利益[1]。数字版权保护是采取信息安全技术手段在内的系统解决方案，在保证合法的、具有权限的用户对数字信息(如数字图像、音频、视频等)正常使用的同时，保护数字信息创作者和拥有者的版权，根据版权信息获得合法收益，并在版权受到侵害时能够鉴别数字信息的版权归属及版权信息的真伪。数字版权保护技术就是对各类数字内容的知识产权进行保护的一系列软硬件技术，用以保证数字内容在整个生命周期内的合法使用，平衡数字内容价值链中各个角色的利益和需求，促进整个数字化市场的发展和信息的传播。

目前，已有很多关于 DRM 的研究项目在多媒体、电子书籍、P2P 和移动终端等不同领域内展开。一些著名国外公司也已分别推出了一些商业 DRM 系统解决方案，如 Apple 公司的 FairPlay 技术[2]；Microsoft 公司的 Windows Media Rights Manager (WMRM)[3]；IBM 的 Electronic Media Management System (EMMS)；RealNetworks 的 RealSystems Media Commerce Suite(RMCS)；Adobe 公司用于 PDF 格式的 Adobe Content Server(ACS)电子书籍版权保护方案；开放移动联盟(Open Mobile Alliance)推出的面向手机等领域的 DRM 2.0 标准[4]等等。国内也有公司推出了包含 DRM 技术的产品，如方正技术研究院的 Apabi 数字版权保护技术；书生公司的 SureDRM 版权保护系统等。

然而，当前数字版权管理的技术仍存在许多的不足和局限性，各厂商的产品存在互不兼容的问题。且由于 DRM 本身的复杂性，对于其系统结构、数字内容的安全交换及权利语言等关键方面并未达成一致的标准，尚未有统一的技术模型。传统的密码学技术在身份认证和权限控制阶段普遍存在着的缺点和漏洞，使得数字产品一旦遭到破解便很难再对其版权进行有效的保护；而新兴的数字水印技术，虽然可以在发现盗版侵权行为后进行取证或追踪，但却难以在事前防止盗版。这些问题极大地制约了电子商务及各种数字内容相关的商务活动的发展。

因此，本文提出的新的数字版权保护模型是以传统密码学技术与数字水印技术相结合为基础，分别利用它们的优点和长处对版权保护技术进行了深入研究。其中包含版权注册、版权转让、在线交易、验证和仲裁等功能模块，能满足各个实体的需求，可以抵抗各种密码和水印攻击，具有较好的实用性和安全性。

## 3 已有模型及其缺陷

数字版权保护系统的一般框架包括 4 大部分：数字内容拥有者、授权中心、内容分发服务器和授权用户。它们的关系如图 1 所示。

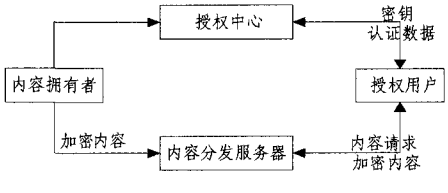


图 1 DRM 系统一般框架

服务器端首先用对称密钥加密算法对数字内容进行加密，然后将解密密钥放入内容许可证中，获取用户公钥后用其加密内容许可证，最后传送给用户加密的数字内容和内容许可证。

在用户端，授权用户获得加密的数字内容和用自己的公钥加密的内容许可证，用自己的私钥解密内容许可证，从而获得内容解密密钥。用户用它解密数字内容并根据许可证设定的权限使用数字内容。

数字内容授权中心是版权保护的核心，它采用密码学技术，经过加密、授权和认证来保护数字内容版权。密钥的安全性决定了版权保护的成功与否。通过授权的方式将密钥传递给用户，从而使授权用户能解密相应的数字内容。

但是一般版权管理系统存在以下缺点：

(1)较少或较弱防范授权用户的非法行为

上面的版权保护系统的一般应用框架描述了端到端的安全通信。但是该框架仅仅考虑了在服务器上的安全存储和密钥传输过程的安全性，防范了网络窃听者和入侵者。但在盗版猖獗的今天，存在着这样的用户，他们拥有媒体授权中心的授权用户身份，可以将解密后的媒体数据进行复制拷贝，进而进行非法传播并谋取利益。简而言之，这些用户以合法的身份进行非法的活动，更具有隐蔽性和不可控性，我们称之为不良用户。该现象的存在使得防范盗版和最大限度地方便用户访问成为矛盾。

(2)采用公钥证书体制

从一般版权保护系统框架的描述中可以看到，该系统在身份认证和权限控制阶段通常都采用公钥证书体制。特别是权限控制阶段，含有数字内容解密密钥的许可证的安全传输和完整性是采用公钥加密私钥解密和私钥签名公钥验证来保证的。

公钥证书体制一方面无法消除用户购买商品的匿名性。另一方面这种机制只适用于大型用户，对于零买用户而言，为买一个数字商品，需特意到 CA 认证中心注册一个证书是极其不情愿的。

(3)系统缺乏通用性

目前，各个应用领域有不同的 DRM 系统，如电子文档、流媒体、ebook 的 DRM 系统。但这些数字版权保护系统都是针对某个具体的应用领域，不能同时处理和保护电子文档、多媒体、ebook 和应用程序等各种数字内容的版权，因此系统缺乏通用性。

下一节提出的多媒体数字版权保护模型可以有效地解决一般版权管理系统存在的问题，该模型主要是在密码技术、数字水印技术上做了改进。

## 4 多媒体数字水印版权保护模型

### 4.1 考虑的主要问题

1. 国家批准的权威机构——密钥管理中心。数字版权保护模型中各实体间通过网络传递信息或进行网上交易，但是交互的双方相对对方而言是隐形的，传递的信息和对方身份便缺乏可靠性和真实性。密钥管理中心解决了以上问题，它为实体分发密钥对，进行数字签名和身份认证。

2. 国家批准的权威机构——版权认证中心。它的作用是为数字产品加载水印，用来判定作品的版权归属。另外作为一个可信实体，版权认证中心也可以在网上交易时接收实体真实身份及交易帐号。

3. 法律权威机构——仲裁机构。该机构受理版权纠纷案

件，裁决盗版侵权行为。

4. 数字版权保护模型中还需要考虑非权威机构的其它实体的需求，在该模型中，提出了 3 个实体，即作者 A、内容发行商 CP 和购买者 B。他们各自的需求如下：

(1)作者最关心的是自己的创作作品不会被剽窃、盗用，也不会被非法复制和篡改；同时，作者还关心作品的实际销售情况；还能提出申请来验证和仲裁作品的真实性和版权。

(2)内容发行商关心的是发行的数字产品不会被剽窃、分发，也不会被非法复制和篡改；还要考虑能够统一管理和跟踪数字产品，能为用户提供多种服务，并且能保证合法购买者按规定的权限使用数字产品，禁止非法用户访问或修改数字产品。

(3)购买者关心的是付费后能否得到合法产品，因为网上交易难以确定商家身份的真实性以及产品的可靠性，购买者最关心能否买到真实的合法的数字产品；购买者还希望在不同设备上可以公平使用购买的数字产品。

### 4.2 模型的关键技术

1. 加解密技术

加密技术是实现信息安全的重要手段。所谓加密就是使用数学方法来重新组织数据，使得除了合法的接收者外，任何其他人要想得到明文或读懂密文是非常困难的。

本文模型中对多媒体(图像、音频和视频)的加密采用全文件加密的方法，即把多媒体文件整体视作一个二进制文件，完全不考虑原始文件的结构，直接对全文件按字节进行加密。由于部分音视频文件的体积可能比较大，因此对多媒体文件加密按段进行，即每次加密 $N$ 个字节。通常选取 $N=2^n$，$n$ 为大于等于 2 的正整数。$N$ 的选择一般与密钥的长度相适应。本文的加密算法采用 Rijndael，并且由于采用了 128 位加密密钥，因此 $N$ 为 128。多媒体文件加密流程如图 2 所示。

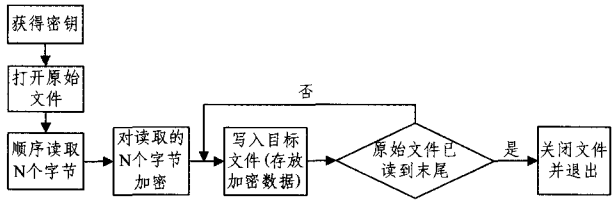


图 2 多媒体文件加密流程图

经过全文件加密法加密后的文件由于已经完全失去了多媒体文件本身的头信息和格式信息而无法用常规的关联软件打开，因此要实现对加密多媒体文件的使用，需要编写专门的代码来实现对加密内容的解密。

本文设计了专门的客户端软件来对加密的文件进行解密。特别是对于音视频流文件，客户端软件采用双缓冲机制，将加密的多媒体一段一段地读入一个空闲缓冲区，然后另一个固定大小的缓冲区抽取解密后的流文件进行播放。当播放下一段时，用下一段的内容覆盖前一段的内容。这保证了音视频流的播放速度。另一方面，由于缓冲区采用了安全存储机制，因此用户无法得到缓冲区中解密后的多媒体内容，从而保护了多媒体的版权。

2. 数字水印技术

当发现非法传播的数字作品时，DRM 可以通过提取出的水印来确认其版权所属或跟踪非法散播者。根据数字水印的特性，可将其分为鲁棒水印和脆弱水印。

该模型根据应用目的，采用了两类鲁棒水印：

(1) 身份标示：标示多媒体内容的所有者(创建者、销售者)和/或内容提供者的身份代码、商标等。在发生版权纠纷时，版权信息用来确认内容的所有者。

(2) 指纹(序列号)：标示多媒体内容的购买者，使之对应于每个购买者，其购买的多媒体中的水印各不相同。在发生版权纠纷时，序列号用于追踪违反协议而非法为盗版提供多媒体内容的购买者。

脆弱水印主要用于完整性保护，它必须对信息的变化非常敏感，我们可以根据脆弱水印的状态来确定数据是否被篡改。

该模型通过综合利用鲁棒水印和脆弱水印，对数字作品共加载 4 次水印，从而加强了多媒体版权的安全性。

### 4.3 模型的组成部分

本文提出的模型综合考虑了多媒体信息的统一管理问题和安全隐患，以及各实体的需求和利益，它包括 6 个实体：密钥管理中心 KM(Key Management)、版权认证中心 CA(Copyright Authenticator)、仲裁机构 MA(Mediation Authority)、作者 A(Author)、内容发行商 CP(Content Publisher)、购买者 B(Buyer)，如图 3 所示。

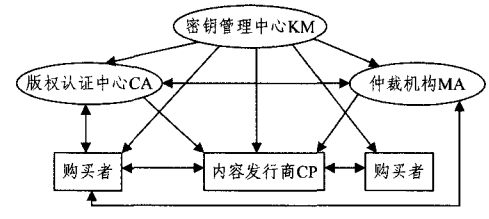


图 3 数字版权管理模型

1. 密钥管理中心 KM 负责建立密钥系统，设置系统参数，产生、分发通信实体的密钥对，选用对称密码算法、签名协议和一些 hash 函数。

2. 版权认证中心 CA 负责给数字产品嵌入不同的水印，以及验证作品的真伪。版权认证中心设有专门的数据库来保存作者、内容发行商和购买者的信息及水印算法，具体内容如下：

(1)作者 A 的身份标识 ID_A、作品 W、作品元数据(包括作品标识 ID_W)、嵌入/提取水印算法等；

(2) 内容发行商 CP 的身份标识 ID_CP、交易账号、作品列表、购买者列表等；

(3) 购买者的身份标识 ID_B、交易账号和 Email 地址；

(4) 若干不可见性的鲁棒性多媒体数字水印算法及脆弱性多媒体数字水印算法。

3. 仲裁机构 MA 负责监视数字作品的非法复制，受理版权纠纷案件，裁决盗版侵权行为。

4. 作者 A 是数字产品的创作人，他在 CP 注册数字产品，得到一定费用之后，根据 CP 的销售情况提取利润。

5. 内容发行商 CP 负责注册、发行和销售数字产品，为用户提供各种服务。

6. 购买者 B 主要是数字产品使用者。使用者不能非法复制和篡改数字产品。

### 4.4 工作流程

模型的具体工作流程为：

1. 版权注册

作者 A 创作完数字作品 W，为保护 W 的版权，向版权管理机构 CA 申请注册 W。

(1)A 将身份标识 ID_A、交易账号、数字作品 W 及其基本元数据信息等签名、加密后分别得到 $s_0$、$c_0$，将($s_0$，$c_0$ ‖ $ID_A$)发送给 CA。

(2)CA 解密 $c_0$ 提取 $\overline{W}$，由 $\overline{W}$ 计算得到$\overline{s_0}$；若$\overline{s_0}\neq s_0$，拒绝服务，结束；若$\overline{s_0}=s_0$，验证通过，CA 接受 $\overline{W}=W$。CA 检测 $W$ 是否已经进行了版权注册，如果 $W$ 已经被注册，则拒绝注册，同时查看数据库中 $W$ 的对应作者 A 的身份标识 ID_A，若存在该 A 的 ID_A，则认为 A 是误操作；若不存在 A 的 ID_A，则初步判定 A 有侵权行为。如果 W 未被注册，则继续注册。根据注册信息生成数字水印 M，然后从数字水印候选算法库中选一个有效水印算法 Embed，在 W 中加载水印：$W_M=Embed(W,M,K)$ ($K$ 为水印算法密钥)。

2. 版权转让

将含有版权水印的数字作品的部分或全部权利转让给内容发行商 CP。

(1)内容发行商对个人信息 $I$，包括 CP 的身份标识 ID_CP、交易账号、给作者的补偿、关于数字产品的各种服务等信息，签名、加密后，分别得到 $s_1$、$c_1$，并将($s_1$，$c_1$ ‖ $ID_{CP}$)发送给 CA。

(2)CA 解密 $c_1$ 提取 $\overline{I}$，由 $\overline{I}$ 计算得到$\overline{s_1}$：若$\overline{s_1}\neq s_1$，拒绝服务，结束；若$\overline{s_1}=s_1$，验证通过，完成注册。

(3)CA 要求 CP 向作者进行支付版权使用/转让费。

(4)完成支付后，CA 根据 CP 的身份标识 ID_CP 和原水印进行重新计算生成第二个水印信息 $M_1$，并加在 W 中：$W_{M_1}=Embed(W_M,M_1,K)$，然后将 $W_{M_1}$ 加密后传给 CP：$CA\rightarrow CP:E(W_{M_1})$。内容发行商获得加密的数字产品后解密得到 $W_{M_1}$，在自己的网页上公布数字产品 W 的内容简介并说明可以为购买者提供的服务类型及收费标准。

3. 网上交易

购买者 B 从网上获得有合法版权信息的数字作品的广告信息，向 CP 申请购买。

(1)B 向 CP 申请购买数字产品 W 及相关服务。

(2)CP 将申请转给 CA。

(3)CA 要求购买者 B 注册身份标识 ID、Email 和交易账号等信息。

(4)B 对个人信息 I 签名、加密后分别得到 $s_2$、$c_2$，将($s_2$，$c_2$ ‖ $ID_B$)发给 CA。

(5)CA 解密 $c_2$ 提取 $\overline{I}$，由 $\overline{I}$ 计算得到$\overline{s_2}$：若$\overline{s_2}\neq s_2$，拒绝服务，结束；若$\overline{s_2}=s_2$，验证通过，完成注册。要求购买者完成支付。

(6)CA 根据 B 身份标识 ID_B 进行计算生成第三个水印信息 $M_2$，并加在 $W_{M_1}$ 中：$W_{M_2}=Embed(W_{M_1},M_2,K)$，最后将 $W_{M_2}$ 加密后传给 CP，即：$CA\rightarrow CP:E(W_{M_2})$。

(7)CP 解密后，嵌入随机生成的完整性标识水印 O：$W_O=Embed(W_{M_2},O,K)$，并加密 $W_O$；再根据购买者的申请生成相应的内容许可证 $L$，最后将已加密的数字产品与内容许可证 $L$ 打包生成最终数字产品：$W_P=Package(E(W_O),L)$。然后在购买者 Email 中给出一次性链接供购买者点击下载。

(8)购买者通过验证来确信自己获得合法产品及相应权限，从而完成网上交易过程。

4. 仲裁过程

仲裁过程如图 4 所示。

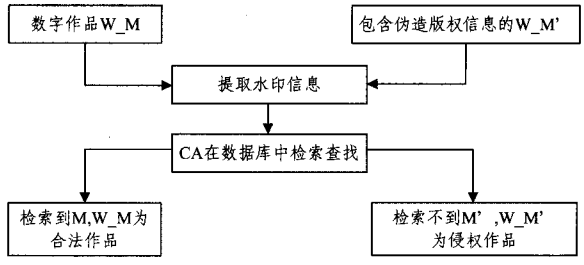


图 4　仲裁过程示意图

(1)A 或 CP 将$(W,\hat{W})$传给 MA，对侵权行为提出申诉。

(2)MA 将$(W,\hat{W})$传给 CA，请求验证。

(3)CA 分别提取$(W,\hat{W})$中的水印 $M,M'$，CA 在数据库中分别检索两者，若有检索不到者，其对应的数字产品被视为侵权。把验证结果发给 MA。

(4)MA 依法对盗版侵权行为进行制裁。

### 4.5　性能优势分析

该多媒体数字水印版权保护模型结合数字水印和密码学两种技术，在没有降低系统的权威性、公平性、实用性的前提下，提高了整个 DRM 系统的安全性。

1. 公平性

作者权益的保护：在该框架中，作者完成数字作品创作后，在 CA 对数字作品的版权进行注册，并将版权水印嵌入到数字作品中，得到版权转让费后，将带有版权水印的数字作品转让给 CP，作者的版权利益得以保障。

内容发行商权益的保护：(1) CP 出售的产品中均嵌入了可以标识其合法身份的水印。(2) 由于产品中嵌入了购买者序列号的指纹水印，CP 一旦发现一个非法拷贝，他就能够识别出非法拷贝源自哪个购买者，若侵权者抵赖，无需提交侵权者任何信息，便可以上诉仲裁机构。

购买者权益的保护：由于购买者所购买的产品中嵌入了作者的版权水印，他可以借助 CA 来证实其购买的产品的真实性。

2. 密码安全性

该模型应用了对称加密算法、公钥密码算法、数字签名、数字身份认证和单向 Hash 函数等密码技术。

使用对称加密算法加密一些敏感信息的签名，如数字产品密文、数字产品摘要、身份标识等，以保证这些信息的机密性。用公钥密码算法为每个实体提供密钥对，双方通信时，用接收方的公钥加密对称加密算法的解密密钥，接收方可以用自己的私钥解密得到对称加密算法的解密密钥。另外实体密钥对也为实现数字签名和身份认证提供了依据。

在该模型中，数字签名几乎每次在交换过程中都要用到，发送方一般先用单向 Hash 函数计算信息的摘要，再用自己的私钥签名，接收方用发送方的公钥验证签名，再用同样的 Hash 函数计算信息的摘要，若相等，则验证成功。Hash 函数和签名保证了传送信息的真实性、完整性和可靠性。

3. 水印安全性

在模型中，数字产品共加载 4 次水印：

第一次水印信息主要包含作者基本信息、作品相关信息，

该水印用来标识作品版权信息，防止对数字产品的非法拷贝和篡改；并且可鉴别数字作品的所有者。嵌入水印可以采用不同的水印保护方案，同时也要考虑不同类型的多媒体数字作品需要不同的水印嵌入算法。

第二次水印信息是根据内容发行商 CP 身份标识 ID 进行计算而来。该水印信息可用于标识 CP 的合法身份。

第三次水印信息与第二次类似，是根据购买者 B 身份标识 ID 进行计算而来。该水印可用来追查非法为盗版提供数字内容的购买者。

第四次水印为随机生成的完整性标识水印。该水印用来保护数字作品的完整性，防止非法篡改。

前三次水印选用鲁棒性水印，可以抵抗各种水印算法的攻击；根据不同的应用目的，采用了两类鲁棒水印，前两次水印用于内容拥有者的身份标识，第三次水印则是作为用户指纹；第四次水印选用脆弱水印算法，可以抵抗各种"伪鉴别"攻击。

4. 实用性

基于数字水印技术的数字版权管理系统极大程度上依赖于数字水印的特性。模型中既包含鲁棒性水印，也需要脆弱水印。框架比较全面地考虑并解决了数字作品版权管理存在的问题，适合于各种网络环境，它选取合适的水印算法，还可用于各类多媒体数字产品的版权保护，所以可以应用于实际的 DRM 工程实现。

**结束语** 多媒体数据在网络上的发布、传播过程中，容易受到剽窃、盗用，严重地侵犯了数字产品所有者或者数字媒体出版商的利益。针对这样的问题，出现了数字版权管理技术和方案。但是，传统的基于密码学的 DRM 系统及新兴的基于数字水印技术的 DRM 系统都存在缺陷。

研究分析一般的数字作品版权保护系统后，本文提出了基于加密和数字水印两种技术的多媒体版权保护模型，它包含版权注册、版权转让、在线交易、验证和仲裁等功能模块，能满足各个实体的需求，可以抵抗各种水印和密码攻击，具有较好的实用性和安全性。

在该模型中，带有版权的数字作品先后共加载 4 次水印，其中包括鲁棒水印和脆弱水印。将数字水印用作版权保护手段，利用数字水印技术的一些特性，不仅能保护版权不受侵犯，还能追踪侵权者，发现盗版者。客户端对多媒体信息加密时采用全文件加密方式；解密时为保证音视频流畅播放，采用双缓冲区机制；同时为防止授权用户获得数字内容明文，缓冲区采用安全存储机制。

本文提出的多媒体数字水印版权保护模型，为解决版权管理系统中的一些问题提供了一种可行的方案，在公平性、安全性、实用性等方面具有一定的优势。为使该系统更加完善，今后还可从以下方面进行进一步的深入研究：数字水印算法；DRM 中关键技术与其他领域先进技术的结合。

## 参 考 文 献


[1] Stamp M. Digital Rights Management: The Technology behind the Hype[J]. Journal of Electronic Commerce Research, 2003, 4(3): 102-112

[2] Jobs S. Thoughts on Music[Z]. February 2007

[3] Microsoft Windows Media—Digital Rights Management(DRM)[OL]. http://www.microsoft.com/windows/windowsmedia/forpros/drm/default.mspx

[4] Irwin J. Digital Rights Management: The Open Mobile Alliance DRM Specifications[J]. Information Security Technical Report, 2004, 9(4): 22-31

[5] 宋永豪，谷大武. 数字版权管理技术的安全性综述[J]. 信息安全与通信保密，2007(9)：140-142

[6] Jiang Xue-hua. Digital Watermarking and Its Application in Image Copyright Protection[C]//2010 International Conference on Intelligent Computation Technology and Automation. Volume 02, 2010: 114-117

[7] 钮心忻. 信息隐藏与数字水印 [M]. 北京：北京邮电大学出版社，2004

[8] 申丽珍. 多媒体信息版权保护新技术——数字水印[J]. 计算机仿真，2005, 22(8): 73-76

[9] 张向华，韦鹏程. 基于信息论的数字水印研究[J]. 计算机科学，2009(3)：248-249

[10] 吕建勋，贾世杰. 基于图像的数字水印技术[J]. 计算机技术与发展，2009, 19(2)

[11] Zhang Hong-bin, Yang Cheng, Quan Xiao-mei. Image Authentication Based on Digital Signature and Semi-Fragile Watermarking [J]. Comput. Sci. &Technol, 2004, 19(6): 752-759

[12] 俞银燕，汤帜. 数字版权保护技术研究综述[J]. 计算机学报，2005, 28(12)

[13] 范科峰. 数字版权管理技术及应用研究进展[J]. 电子学报，2007, 35(6)

[14] 桑军，廖晓峰. 数字图像水印与版权保护——概念与方法[J]. 计算机科学，2005, 32(1)

[15] 汪保友，王俊杰，胡运发. 数字水印与版权保护[J]. 计算机应用与软件，2004(1)

[16] 胡军全，王继武，张龙军，等. 结合数字签名和数字水印的多媒体认证系统[J]. 软件学报，2003, 14(6): 1157-1163

[17] 何佳鸣，张鸿宾. 基于数字水印和传统加密技术的数字版权管理系统框架的研究[J]. 计算机科学，2008, 35(4A): 254-256

[18] 陈晓苏，胡蕾，肖道举. 一个基于 PKI 和数字水印的数字版权保护框架模型[J]. 计算机工程与科学，2005(6)：12-14


(上接第 87 页)


[5] Wang X, Wu K, Wang J, et al. CAPF: Coded anycast packet forwarding for wireless mesh networks[J]. Wireless Networks, 2011, 17(5): 1273-1285

[6] Kim J, Lin X, Shroff N B, et al. Minimizing delay and maximizing lifetime for wireless sensor networks with anycast[J]. IEEE/ACM Transactions on Networking, 2010, 18(2): 515-528

[7] Ashraf F, Vaidya N H, Kravets R H. Any-MAC: Extending any asynchronous MAC with anycast to improve delay in WSN[A]// Proc of 8th Annual IEEE Communications Society Conference on SECON[C]. 2011: 19-27

[8] Chen J C, Chan S H, Li V. Multipath routing for video delivery over bandwidth-limited networks[J]. IEEE Journal on Selected Areas in Communications, 2004, 22(10): 1920-1932

[9] Xuan D, Jia W, Tu W Q, et al. Distributed Admission Control for Anycast Flows [J]. Transactions on Parallel and Distributed Systems, 2004, 15(8): 673-686