实现DRM系统的一种新方案

程春玲[1],张登银[2]
(1.南京邮电大学 计算机学院,江苏 南京 210003;
2.南京邮电大学 科技处,江苏 南京 210003)

摘 要:版权保护一直是困扰创作者和发行商的重大问题,现有的技术和协议在防止盗版上都存在着一定程度的缺陷。数字版权管理(DRM)系统综合使用各种技术和协议寻求买卖双方的利益平衡,保证创作者的版权和用户端的安全。本文提出基于模块化实现DRM系统的全面解决方案。该实现方案对DRM模型进行了改进,将水印的嵌入移交给权威机构来处理,买卖双方只需对水印的存在性进行检验。最后,对整体安全性能进行了分析。该方案利用现有的技术和协议,实现了对作品的整个生命期的安全访问控制。

关键词:数字版权管理;数字水印;访问控制
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)07-0166-04

A New Implementation Scheme for Secure DRM System

CHENG Chun-ling[1], ZHANG Deng-yin[2]
(1. College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China;
2. Division of Science and Technology, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: Copyright is disturbing the authors and issuers. DRM system combines all kinds of techniques and protocols, so as to balance the benefits of the buyers and sellers, and to assure the authors' copyright and users' security. In this paper, the integrate implementation scheme based on the functional architecture for DRM is proposed. The DRM model is improved on relegating the work of implanting digital watermark to authoritative organization, so the buyers and sellers only need to check the presence of watermark. At last, the analysis about the security of the scheme is also given. Secure access control can be achieved in the writing's whole life period.

Key words: digital rights management; digital watermark; access control

0 引 言

随着计算机网络和多媒体技术的发展,越来越多的作品以电子版的形式在网络上发布。但由于对数字内容的拷贝十分容易,使创作者和发行商的利益受到极大损害。防止网上盗版常用的一种技术是加密,但是一旦获取了密钥,就可以对作品解密并任意复制和传播。版权保护主要依赖水印技术[1],但其安全性尚未得到理论证明,对于篡谋攻击更是束手无策。为了提高水印技术的安全性,人们提出了一系列配套协议。例如,buyer-seller协议[2]是一个包括买方、卖方和权威机构的三方协议,可以防止篡谋性攻击,但它没有考虑二手市场情况。buyer-reseller协议[3]在此基础上进行了改进。不过,上述技术和协议主要考虑卖方利益,忽视了买方权益。用户从某个网站下载应用软件时,不会主动验证其版权信息和来源途径。如果这些软件本身不能提供完美的服务,甚至被人恶意设计(带有病毒),那么终端用户和版权所有者将面临工作不便或潜在危害。近年来出现的数字版权管理(DRM)系统[4,5],考虑了卖买双方的利益。介绍现有DRM的功能框架,进而提出基于模块化的DRM系统的完整实现方案。该方案实现了对作品整个生命期(包括作品的生产、传播、销售和使用)的安全访问控制。在实现知识产权的创建和证明模块时,对DRM模型进行了改进。与现有方案相比,文中提出的方案更具公平性和安全性,在考虑卖方的作品权益基础上,真正考虑了消费者的利益。

收稿日期:2008-10-31;**修回日期**:2008-12-25
基金项目:国家自然科学基金资助项目(60573141);国家863计划(2008AA701202)
作者简介:程春玲(1972-),女,陕西西安人,副教授,研究方向为网络技术和信息安全、数据库技术;张登银,博士,研究员,研究方向为信号与信息处理、IP网络技术、信息安全。

1 DRM系统框架模型

DRM系统对数字内容的知识产权进行保护,涉及

对数字版权的描述、认证、交易、保护、监控和跟踪等各个过程[6]。DRM 系统一方面向作品的创作者和发布者提供版权保护,对非授权用户进行访问控制;另一方面向终端用户提供安全保证,以防非法程序访问系统资源,导致系统崩溃。DRM 系统的功能结构主要包括知识产权的创建和证明、知识产权管理、作品使用这三个模块,如图 1 所示。

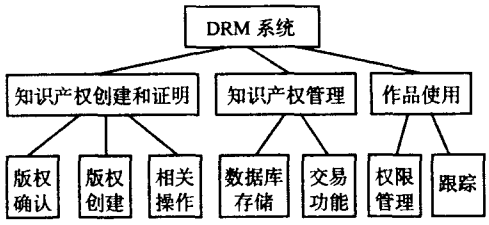

图 1　DRM 功能结构

●知识产权的创建和证明模块完成:

1)版权确认:作品创建者向权威认证机构提出申请,声明对作品的所有权关系;

2)版权创建:将版权及其他信息如用户信息、用户的访问权限、使用期限等嵌入到作品中;

3)与版权相关的操作,如用户查询作品的版权,创作者提取或检测版权信息等。

●知识产权管理模块包括两部分功能:

1)数据库存储:在分布式数据库中存储和检索作品内容和相应数据元。数据元包括与作品相关的各方(作品的创作者、发布者及使用者)、各方拥有的存取权限和对作品的描述等;

2)交易功能:当买方和卖方对作品的存取权限达成一致时,卖方将向买方颁发通行证,同时买方向卖方支付相应的费用。

●作品使用模块的功能需要由终端设备如 PC 机和手机等来实现,包括:

1)权限管理:终端设备根据被授予的访问控制权限对作品进行操作;下载安装的数字作品只能访问终端设备的部分资源和调用部分接口函数,防止恶意程序破坏系统资源;

2)跟踪管理:跟踪内容的使用情况,如果每次使用内容时买方都要向卖方交付费用,那么该模块可以通过交易系统跟踪用户的使用,记录交易过程。

2　DRM 系统实现方案

文中提出的 DRM 系统实现方案是基于 DRM 功能模块的,这种模块化的设计便于扩展。本方案并不对作品的具体内容作区分,更具有通用性。另外,本方案重点考虑了终端设备对应用程序的资源访问控制,而这一点恰恰是现有解决方案所忽略的。下面将按模块来讨论 DRM 系统的具体实现。

2.1　知识产权的创建和证明模块

该模块的实现采用一些协议模型[7],如 ECMS 模型。为了简化实现过程,将作品的创作者与发布者合二为一,于是可以采用 buyer－seller 模型。但是 buyer－seller 模型增加了买方和卖方的负担,给双方带来了极大的不便。因此对该模型进行了改进,将水印的嵌入工作移交给权威机构来处理,卖方和买方只需对水印的存在性进行检验。该模块的实现包括商家 A、客户 B、身份认证机构 C_{ID} 和数字水印颁发机构 C_W,他们之间的交互如图 2 所示。

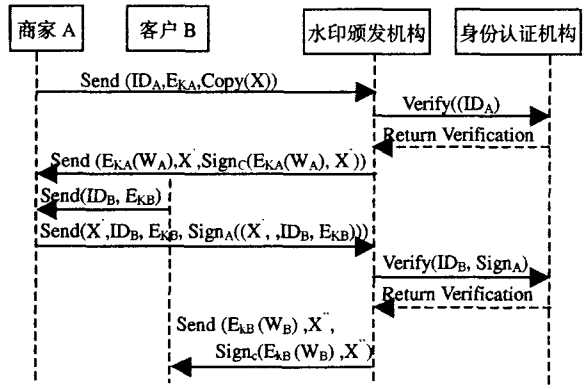

图 2　交互图

商家 A 为了保护自己产品的版权,向数字水印颁发机构 C_W 发送自己的身份标识 ID、公钥 E_{kA} 和产品 X 的一份拷贝。其中身份标识 ID 由身份认证机构 C_{ID} 颁发。C_W 向身份认证机构确认了 A 的身份后,将随机生成水印 W_A,并嵌入到作品中。然后 C_W 将加密后的水印 $E_{kA}(W_A)$、嵌入水印的作品 $X'(X+W_A)$,以及 C_W 的签名 $Sign_c(E_{kA}(W_A),X')$一起发送给 A,同时 C_W 将这些信息保存在数据库。

A 得到 C 发送的加密水印 $E_{kA}(W_A)$后,用自己的私钥 E_{kA} 进行解密,并将解密后的水印 W_A 与 X' 进行相似性检验,即:

$$\mathrm{sim}(W_A,X')=\frac{W_AX'}{\sqrt{X'X'}} \tag{1}$$

如果 $\mathrm{sim}(W_A,X')$大于某个界限值,则证明 X' 中包含了水印 W_A。

当客户 B 想要购买 A 的产品 X 时,必须将自己的 ID_B 和公钥 E_{kB} 发送给 A。若 A 和 B 对这次交易达成一致,A 将加了自己水印的作品 X'、B 的信息(ID_B、E_{kB})以及 A 的签名发送给 C_W。C_W 证明签名的有效性后,为 B 产生水印 W_B 并嵌入 X'。同样 C_W 将加密后的水印 $E_{kB}(W_B)$、嵌入水印的作品 $X''(X''+W_B)$,以及 C_W 的签名 $Sign_c(E_{kB}(W_B),X'')$一起发送给 B。C_W 将这次交易记录下来。

B 验证了 C_W 的签名后，按式(1)检验作品中是否包含了自己的水印 W_B。如果检验成功，则此次交易顺利完成。

独立的水印颁发机构 C_W 可以利用自身数据库中的原始信息验证每件作品及其嵌入水印是否一致，从而追查盗版来源。当 A 发现盗版产品时，也可将该盗版产品发送给数字水印颁发机构 C_W。C_W 将提取出来的水印与数据库中的数据进行对照，如果发现该水印为 B 的水印，即可证明 B 将自己购买的作品进行了非法传播。

这个协议，一方面可以由 B 的水印来判断 B 是否有盗版行为，另一方面也可以防止商家 A 做手脚，借机陷害客户 B，因为 A 无法知道 B 所获得的水印。而且，由于 C_W 中记录了该产品每次交易生成的水印，B 也无法将水印 W_B 嵌入到其他作品中。

2.2 知识产权管理模块

该模块由权威机构，即水印颁发机构 C_W 和身份认证机构 C_{ID} 实现。也可以看作同一个机构，既进行水印颁发，又进行身份认证。这里，以服务器的形式代表这两个机构，图 3 显示了每台服务器上所建立的数据库以及它们之间的交互。

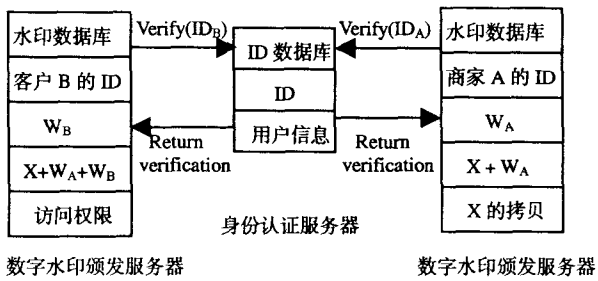

图 3 数据库之间的交互

一个合法的商业机构会将自己的信息发送给身份认证机构 C_{ID}，请求身份认证。C_{ID} 在对客户信息进行验证后，将向该商业机构颁发身份标识号 ID 和数字签名 $Sign_C(ID)$，并在自己的数据库中进行记录。这样，当该商业机构想要保护自己商品的版权时，它会将 ID、$Sign_C(ID)$ 、公钥 E_{kA} 和产品的一份拷贝发送给 C_W。C_W 向 C_{ID} 确认了 ID 的合法性后，给商家颁发水印，并将商家的 ID、颁发的水印 W_A、嵌入水印的作品 $X+W_A$ 和作品的拷贝存储在数据库中。同样，当客户要购买商家的产品时，也要向 C_W 发送自己的 ID 和公钥 E_{kB}，C_W 验证 ID 的合法性后将为该客户生成的水印嵌入到作品中并发送给客户，并将客户的 ID、W_B、嵌入水印的作品 $X+W_A+W_B$ 存储在数据库中。

客户和商家可以对商品的存取权限达成一致，商家将客户信息发送给 C_W 的同时，将颁发给客户的通行证也发送给 C_W。C_W 记录在数据库中，用于对客户进行访问控制。

2.3 作品使用模块

该模块既要实现终端用户对作品访问权限的控制，还要实现作品对终端设备资源访问的控制。有关终端用户对作品访问权限的问题，已有文献[8,9]涉及，这里着重考虑作品对终端设备资源访问的控制。由于应用程序对终端设备的危害大，本方案将作品具体化为应用程序，通过设备对应用程序的下载、安装和运行实施安全控制。该模块由认证、下载/安装控制、运行控制三部分组成。

为了使终端设备能够对下载的应用程序进行安全控制，设备制造商和应用程序的开发商首先要进行认证，具体方法是：

1) 应用程序开发商向身份认证机构 C_{ID} 发送自己的信息，请求身份标识号 ID。身份认证机构进行调查，确认有效性后，向开发商发送 ID 以及数字签名 $Sign_C(ID)$。

2) 应用程序开发商向设备制造商申请认证，并将自己的 ID、$Sign_C(ID)$、所要访问的资源和自己的公钥发送给设备制造商。设备制造商将要求 C_{ID} 证明 ID 的有效性。获得确认后，设备制造商向开发商颁发通行证，包括开发商的 ID、授予的资源访问权限和该通行证的有效期，并用开发商的公钥进行加密，最后设备制造商进行数字签名。同时，开发商在设备出厂前，将这些信息加入到系统中。

下载和安装应用程序时，终端设备系统根据下载软件包的内容，将应用程序划分为不信赖、第三方和可信赖三类。其开发商没有从身份认证机构获得合法 ID 的为不信赖程序。下载和安装此类程序时，系统将给出警告并且不推荐安装此类程序；第三方程序的开发商已经获得了合法的 ID，但缺少设备制造商的数字签名。在下载和安装此类程序时，系统会检查这个 ID 的合法性，并向用户出示该 ID；可信赖程序的开发商既拥有合法 ID，又拥有设备制造商发给他的经过数字签名的通行证。终端设备将根据这三类程序实施不同的安全控制措施。

应用程序在运行时的访问控制过程如下：

1) 应用程序向安全管理器发送资源访问信息，包括：开发商的 ID 或设备制造商的签名、资源名、访问权限等；

2) 安全管理器验证 ID 和签名的合法性，对于可信赖程序，安全管理器检查开发商的通行证；

3) 安全管理器检查用户对资源访问权限的设置；

4) 如果应用程序通过了上述检查，安全管理器为

该程序产生一个证书,包括应用程序的ID、资源名、访问权限,并将其存储在证书库中。

5) 给应用程序发放证书,程序凭证书访问资源。

6) 被访问的资源对证书进行验证,然后应用程序才能进行访问。

至此,给出了DRM系统的一个完整实现方案。本方案既保护了作者和发布商对作品拥有的合法权利,也确保了终端设备的安全性,避免了应用程序对系统资源的破坏。

3 系统安全性分析

上述DRM系统采用模块化方法实现,因此为了确保系统的安全性,就必须保证每个模块在运行过程中是安全的。

在知识产权的创建和证明模块中,采用了改进的buyer-seller协议,由公认的权威机构对每次交易的买卖双方身份进行认证、为双方产生不同的水印,并完成水印的嵌入,同时记录买卖双方的特征信息和交易内容,为识别和打击可能出现的盗版行为预先保留必要的证据。在协议实施过程中,权威机构采用签名技术对发给买卖双方的内容进行签名,以证明其身份的合法性,防止其它非法机构冒充权威机构的行为发生。权威机构采用合适的水印嵌入算法,恶意攻击者在无法获得水印的前提下,很难确认作品中水印的存在,也无法在确保作品质量的前提下,将水印删除。权威机构向买卖双方发送水印时,采用RSA加密技术,只有拥有私钥的用户才能将水印解密出来。为了进一步确保发送消息的机密性,还可以采用SSL安全传输协议。

在知识产权管理模块中,认证服务器之间或者不同的权威机构之间要进行信息的交互。为了防止其他服务器冒充,将在它们之间建立安全通道,使用合适的安全协议,如SSL和SET,从而保证通信的秘密性。同时双方通信时要对传送的信息进行签名,以确保信息的发送方是可靠的。

在作品使用模块中,对终端用户的访问权限进行控制,可以采用外部仓库外部控制模型。该模型实现了信息和控制的完全分离,分别用两种数字容器存放信息和控制集,从作品下载和作品访问权限两方面加强了对信息发布的控制能力。为有效控制作品对系统资源的访问,从下载、安装和运行的全过程实施控制,将下载的程序分成三类分别处理。对不可信赖的程序,系统将警告用户最好不要下载和安装此程序,并且限制此类程序只能访问通用的接口函数;对第三方程序,允许其访问有限的保护类接口函数;而对可信赖的程序,采用颁发通行证的方式,系统只有在确认了通行证的有效性后才允许作品访问通行证中所允许访问的资源。这样,作品创作者的利益和终端的使用安全分别得到保证。

4 结束语

提出了基于模块化实现DRM系统的全面解决方案。该实现方案对DRM模型进行了改进,将水印的嵌入移交给权威机构来处理,买卖双方只需对水印的存在性进行检验。这种方案具有更好的公平性和安全性,在考虑卖方的作品权益基础上,真正考虑了消费者的利益。

对系统整体安全性能的分析表明,该方案利用现有技术和协议实现了对作品整个生命期的安全访问控制。

参考文献:

[1] 陈佳萍,张登银.基于矢量量化的数字图像水印技术研究[J].计算机技术与发展,2008,18(7):139-142.

[2] Memon N, Wong Ping Wah. A Buyer-Seller Watermarking Protocol[J]. IEEE Tranctions on Image Processing, 2001, 10(4):643-649.

[3] Cheung S C, Curreem H. Rights Protection for Digital Contents Redistribution Over the Internet[C]//Proceedings of the 26th Annual International Computer Software and Applications Conference (COMPSAC'02). Washington, DC, USA: IEEE Computer Society, 2002:105-110.

[4] 程文青,邓婉婷,刘清堂.数字媒体版权管理平台研究与实现[J].计算机应用与软件,2007,24(7):27-29.

[5] 朱兴东,罗万伯,柏　银,等.DRM技术及其在电子书发行平台构建中的应用[J].四川大学学报:自然科学版,2006,43(1):84-88.

[6] 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):1957-1968.

[7] Yuan Zhonglan, Xia Guangssheng, Wen Qiaoyan. Copyright protection protocol for digital media[J]. Journal of Beijing University of Posts and Telecommunications, 2005, 28(1):102-106.

[8] 马兆丰,顾　明,孙家广.基于角色的可信数字版权安全许可授权模型[J].清华大学学报:自然科学版,2006,46(4):534-538.

[9] 李　丹,金　庆,吴国新.基于DRM的版权管理系统的研究[J].计算机技术与发展,2008,18(3):188-191.