

数字产品版权保护认证机制^{*}

程卫东¹, 刘红梅²

(1. 成都信息工程学院电子系, 四川 成都 610041;

2. 中山大学电子与通信工程系, 广东 广州 510275)

摘 要: 提出了一种基于数字水印技术和应用密码学的数字产品版权保护认证机制。该数字产品版权保护认证机制通过引入中介机构的方式, 可以公正有效的对数字产品版权进行销售/消费注册和证据提供, 实现对数字产品的版权保护认证。

关键词: 数字水印; 公开密钥加密; 数字产品版权保护

中图分类号: TP391 **文献标识码:** A **文章编号:** 0529-6579 (2004) S2-0091-03

随着数字技术和网络技术的发展, 快捷准确廉价的数字传输手段在为无数商家带来无限机遇的同时, 也给技术界提出了新的挑战, 即解决数字产品(如电子出版物, 电子绘画, 音视频产品等)的版权保护问题。数字水印^[1-3]技术通过将不可见的数字标记隐藏在数字产品中, 证明原创者对作品的所有权并作为起诉非法侵权者的证据, 是一种新的数字产品著作权保护技术。

现有的数字产品版权保护技术分为基于水印的标记法^[4]和基于加密、认证的安全协议法。若干公司提供了相关的技术产品^[5-8], 主要有 IBM 公司的 Cryptolope 技术, InterTrust 公司的 DigiBox 技术, Breaker 技术公司的 SoftSeal, 中国科学院 SKCC 模型以及欧洲电子产业界和有关大学协作开发的采用数字水印技术来监视复制音像软件的监视系统《TALISMAN》等。单一的依靠原创者在自己的数字产品中加入数字水印尚不能从技术上解决非法侵权, 盗版等问题。本文结合数字水印及现代密码学, 提出了一种具有公证性的数字产品版权保护认证机制。在版权所有者和消费用户中引入一个信用度较高的中介认证机构, 由该中介认证机构对版权所有者的有效数字产品版权进行销售/消费注册, 并在版权发生纠纷时充当证据提供者。

1 数字产品版权保护认证机制的设计

本文提出的数字产品版权保护认证机制分为注册过程, 证据提供过程两个部分。

1.1 数字产品版权保护认证机制的消费注册过程

图 1 是数字产品版权保护认证机制的销售/消费注册过程描述框图。

数字产品的原创者在公开发布自己的数字产品前, 对于一般的数字产品, 可自行嵌入数字水印, 同时将含有数字水印, 水印算法 ID, 或数字产品原始数据 ID 送于中介认证机构。由中介认证机构对数字水印、水印算法 ID 和数字产品原始数据 ID 进行加密。加密算法采用公开密钥算法^[9], 也叫非对称算法, 加密密钥 K1 和解密密钥 K2 不同。其中公开密钥 K1 由中介认证机构保留, 私有密钥 K2 由原创者保留。最后, 将加密后的数字水印、水印算法 ID 和数字产品原始数据 ID 存放于中介机构的存储中心。这一过程在本文所述的数字产品版权保护认证机制中称为销售/消费注册过程。

对于销售的某些特殊的数字产品, 或者提供在线有赏服务方式的各种数字产品, 除按销售注册过程操作外, 还可以要求将消费用户 ID (包含用户的基本信息, 消费的时间等) 同时嵌入到要消费的数字产品中, 以此来控制非法用户使用该数字产品。另外, 将用户 ID, 数字水印、水印算法 ID 和数字产品原始数据 ID 送于中介认证机构进行加密保存, 用于防止该消费者的盗卖。中介认证机构采用非对称算法加密, 就象顾客将有效证据存储于银行的保险箱一样, 银行总管全局, 顾客保管自己保险箱的钥匙, 缺少其中的任意一方都打不开保险箱得不到箱内的物品。这样也杜绝了中介机构内部“偷梁换柱”偷换已备份的用户的各种数据。

* 收稿日期: 2004-09-11

基金项目: 四川省科技厅重点资助项目 (01GG007-13); 广东省自然科学基金资助项目 (021758)

作者简介: 程卫东 (1958 年生), 男, 教授; E-mail: chengwd@cuit.edu.cn

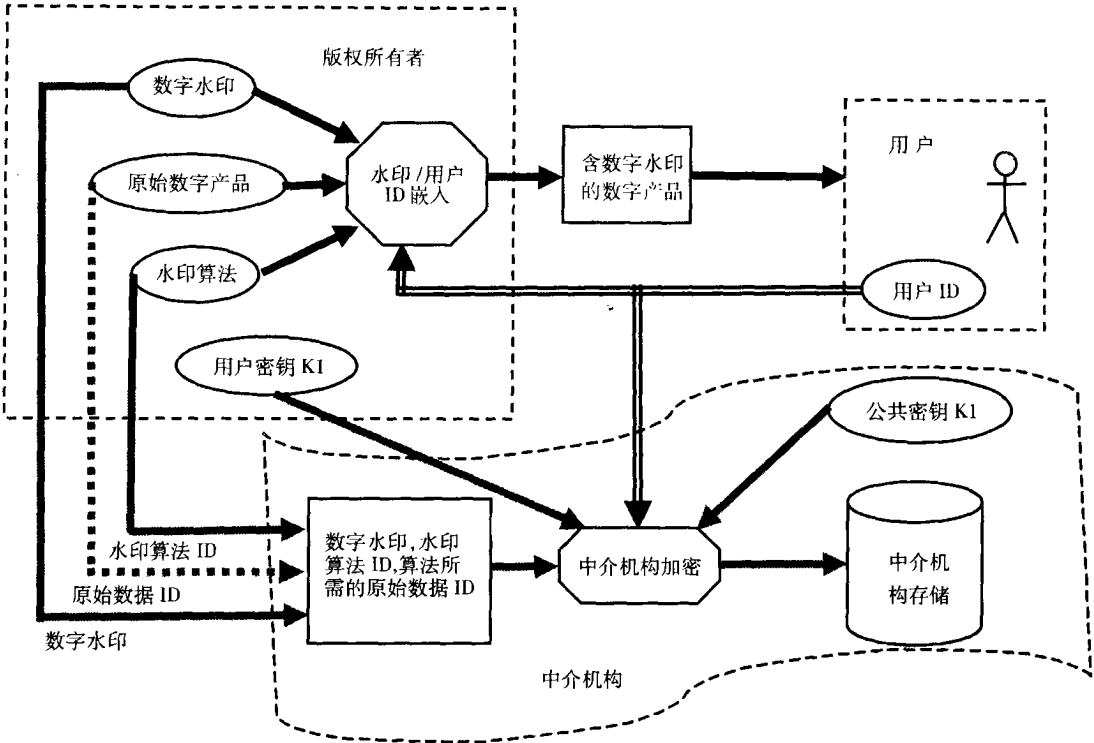


图 1 销售/消费注册过程描述框图

Fig 1 Block diagram of distribution/consumption registration

在图 1 中，虚线表示该水印算法的水印检测需要数字产品原始数据，双实线表示对于销售的某些特殊的数字产品，或者提供在线对于某些服务方式的各种数字产品时，要求将消费用户 ID 同时嵌入到要消费的数字产品中，以此来控制非法用户使用该数字产品和防止该消费用户的盗卖。

1.2 数字产品版权保护认证机制的证据提供过程

图 2 是数字产品版权保护认证机制的证据提供过程描述框图。

当数字产品发生产权纠纷时，中介机构将存储中心加密备份的数字水印、水印算法 ID 和数字产品原始数据 ID，通过版权所有者用户提供的私钥 K1 对这些数据进行解密。将解密所得到的水印算法 ID 和数字产品原始数据 ID 与版权所有者为检验产权纠纷再次提供的水印算法 ID 和数字产品原始数据 ID 进行比较，比较结果将作为是否继续进行数字水印/用户 ID 提取的控制参量和。二者的比较结果正确，继续进行数字水印/用户 ID 提取，否则，将终止数字水印/用户 ID 提取。在数字水印/用户 ID 提取后，再与解密所得到的数水印/用户 ID，数据 ID 比较结果，以及水印算法 ID 比较结果进行综合比较，以便司法部门提供数字产品产权归属证据。这一过程本文称为数字产品版权保护认证机制的证据提供过程。

1.3 该数字产品保护机制的性能评价

该系统在储存版权所有者的数字水印，水印算法 ID，或数字产品原始数据 ID，或用户 ID 时，中介认证机构采用公开密钥加密提高了单纯数字水印的安全性。因为在大多数数字水印应用中，特别是版权保护，必须要确保嵌入的信息的保密性。通过与现代密码学的结合，在嵌入和提取水印的过程中使用密钥，可以提高信息的保密性。在本系统中要解决用户对中介机构的不信任问题。由前所述，本系统中采用的是公开密钥加密，只有版权所有者才有私钥，而中介要想提取数字水印，水印算法 ID，或数字产品原始数据 ID，或用户 ID 必须要私钥，否则是没有能力完成的。

当然系统中也存在不少的缺陷，比如中介认证机构在存储备份文件数据时采用的存储空间必须比较大的，因为这种认证机构做的是长期的工作，也就是说备份的数据是要长时间存放在存储空间中的。这样就造成存储数据时花费较高的问题。

2 结 论

本文设计的数字产品版权保护机制中引入了一个中介认证机构，该中介认证机构可以比较公证的完成全部认证过程，并且具有很高的可信度。比以往双方纠缠更具有说服力，特别是在水印证据提供

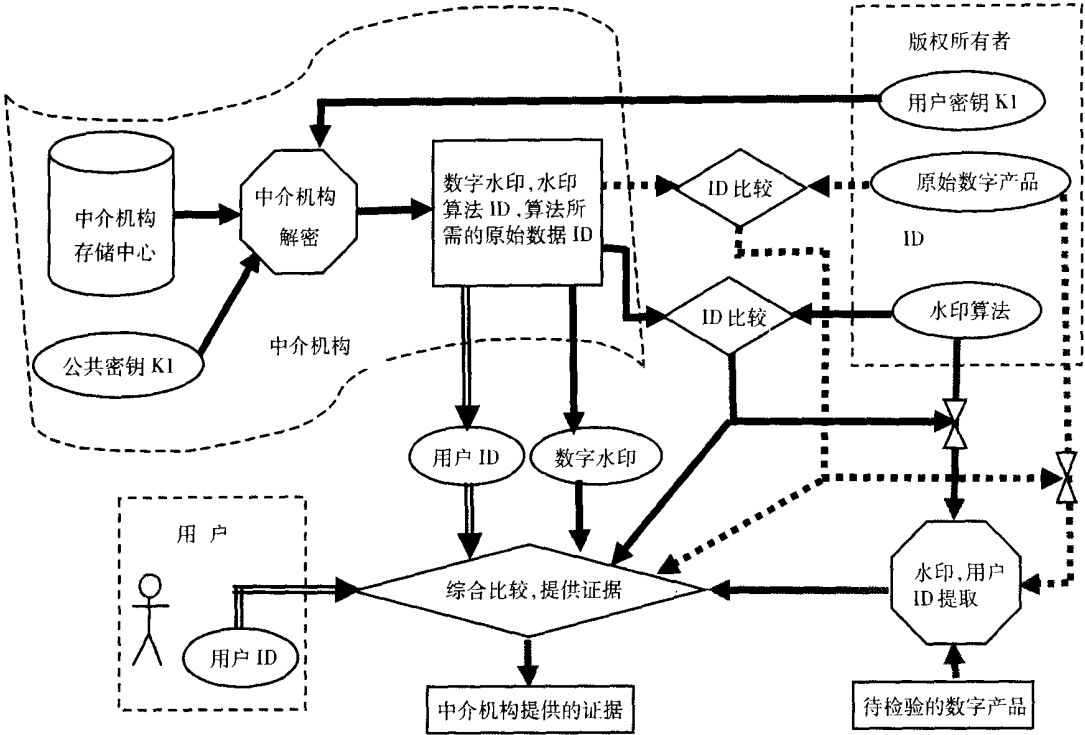


图 2 证据提供过程描述框图

Fig. 2 Block diagram of producing evidence

过程中的两个“比较”，即将解密所得到的水印算法 ID 和数字产品原始数据 ID 与版权所有者为检验产权纠纷再次提供的水印算法 ID 和数字产品原始数据 ID 进行比较，将检测所得的数字水印/用户 ID 与解密所得到的数水印/用户 ID，数据 ID 比较，据此综合做出结论，是很有说服力的。同时在目前没有嵌入数字水印的算法标准，数字水印嵌入的质量参差不齐的情况下，可以说该系统是数字产品版权保护比较简洁的适用的系统。

参考文献:

[1] COX I J, KILLIAN J, LEIGHTON F T, et al. Secure spread spectrum watermarking for multimedia[J] . IEEE Trans on Image Processing, 1997, 6(12) : 1673—1687.

[2] YEUNG M M. Digital watermarking[J] . Communications of the ACM, 1998, 41(7) : 31—33.
[3] 黄继武, 谭铁牛. 图像隐形水印综述[J] . 自动化学报, 2002, 26(5) : 645—655.
[4] PETICOLAS F, ANDERSON R J, KUHN M G. Information Hiding: A Survey[J] . Proc IEEE, 1999, 87(7) : 1062—1078.
[5] IBM Cryptolope[EB/OL] . <http://www.cryptolope.ibm.com/white.com>
[6] InterTrust Digibox[EB/OL] . <http://www.interttrust.com>
[7] ZHUANG C. Network secure content distribution and copy-right protection technology[J] . Computer Engineering, 2000, 26(6) : 50—52.
[8] <http://www.igd.fhg.de/igd-a8/index.html?projects/talisman/index.html>
[9] BRACE S. 应用密码学[M] . 北京: 机械工业出版社.

Authentication Scheme for Copyright Protection of Digital Product

CHENG Wei dong¹, LIU Hong mei²

(1. Department of Electronics, Chengdu University of Information Technology, Chengdu 610041, China;
(2. Department of Electronics, Sun Yat set University, Guangzhou 510275, China)

Abstract: Based on digital watermarking and applied cryptology, an authentication scheme for copyright protection of digital product is proposed. By introducing an intermediary agent, this scheme can provide distribution/consumption registration and evidence for copyright of digital product fairly and effectively, resulting in copyright protection of digital product,

Key words: digital watermarking; public key encryption; copyright protection of digital product