版权保护系统的安全水印协议设计

任旭峰[1],张贵仓[1],张 旭[2]
REN Xu-feng[1],ZHANG Gui-cang[1],ZHANG Xu[2]

1.西北师范大学 数学与信息科学学院,兰州 730070
2.中国人民解放军炮兵学院,合肥 230031
1.College of Mathematics and Information,Northwest Normal University,Lanzhou 730070,China
2.Artillery Academy of PLA of China,Hefei 230031,China
E-mail:renxuf@163.com

REN Xu-feng,ZHANG Gui-cang,ZHANG Xu.Design for secure protocol of digital right management.Computer Engineering and Applications,2008,44(34):72-74.

Abstract: Based on the analysis of security threat and using watermarking technology and encryption technology,a protocol security model of copyright marking system is proposed.Through protocol mechanism with digital watermarking technology,the proposed protocol security model can resistant to the protocol attack effectively,and protects not only the benefit of the copyright owners but also the benefit of the purchasers.The design of the protocol security model reflects the effectiveness and the convenience of making use of protocol techniques to counteract protocol attacks.

Key words: digital rights management;digital watermarking;protocol design;protocol attacks;protocol layer security

摘 要:根据安全威胁分析和利用水印技术和密码技术,研究对象是版权保护系统的安全协议设计。在协议设计上引入认证机制、时间戳机制和可信第三方的公钥跟踪机制以及多播机制,设计了一个安全可靠的版权保护协议,避免了现有协议的缺陷,实验证明本协议满足版权所有者和购买者的应用需求,可以抵抗现有的协议层安全隐患,并对其性能做出分析,说明了其实际可行性。

关键词:版权保护;数字水印;协议设计;协议攻击;协议层安全
DOI:10.3778/j.issn.1002-8331.2008.34.021 **文章编号**:1002-8331(2008)34-0072-03 **文献标识码**:A **中图分类号**:TP391

1 引言

计算机网络环境下,数字作品的侵权行为泛滥使得版权保护技术的研究成为热点。版权保护系统的商业化要求决定了它必须具有良好的安全特性,这些安全特性不仅体现在版权保护算法对稳健性攻击的安全性上,还体现在系统设计实现对协议层攻击的安全性上。此外,随着电子商务的迅速发展,版权保护系统的协议必须能够满足二手交易和多方交易的需求。

版权保护系统的安全性一方面取决于算法本身,另一方面取决于协议设计。此外,现有的协议除了安全问题,还具有两个缺陷:一是过分关注版权所有者的权益,因此,在二手交易中保护原始购买者的权益,现有的协议困难重重;二是现有协议均由创作者嵌入水印和指纹,在多方交易情况下不能保证多方提供的拷贝一致。因此有必要设计一个新的版权保护协议。文章的创新所在,在前人研究的基础上,引入了新的协议设计机制,设计了一个协议模型。值得指出的是,本文重新归纳了应用需求的分类,说明了安全隐患中只需要解决解释攻击和复制攻击就可以解决其他协议攻击带来的安全隐患。

2 版权保护系统的安全水印协议设计

安全水印协议设计是对版权保护系统的需要及其对策的讨论,设计了水印技术、密码技术和协议设计机制所应当采用的算法,提出了一个协议层安全版权标记系统模型。一方面它能够有效地限制解释攻击和拷贝攻击等安全隐患,提高系统协议层安全性,另一方面可以满足所有权证明、跟踪非法拷贝并鉴别非法拷贝源等应用需求,同时也可以同时满足版权所有者和版权购买者的利益。通过效用分析和时空复杂度分析显示,该模型在系统有效性与可行性之间取得了较好的平衡。

版权保护系统的协议层安全协议的整体结构如图 1 所示,该系统主要包括版权所有者(C0)、购买者(B)、注册机关(RA)、时间戳服务中心(TSS)和证书机关(CA)等 5 个参与者。

该协议层安全模型的简要工作流程如下:

(1)购买者与所有者交互——Bob 向 Alice 提出购买请求;

(2)购买者、所有者与 CA、RA 交互——CA 向 RA 确认Bob 和 Alice 的身份;

(3)所有者生成水印——Alice 向作品中嵌入水印,生成水印作品;

(4)所有者与时戳中心交互——Alice 向水印作品中嵌入时间戳;

(5)所有者与 CA 交互——CA 向含有时间戳的水印作品中嵌入指纹,加密并签名后返回给 Alice;

作者简介:任旭峰(1980-),男,硕士研究生,主要研究方向:数字水印、图像处理、信息安全等;张旭(1980-),男,硕士研究生。
收稿日期:2008-05-16 **修回日期**:2008-08-21

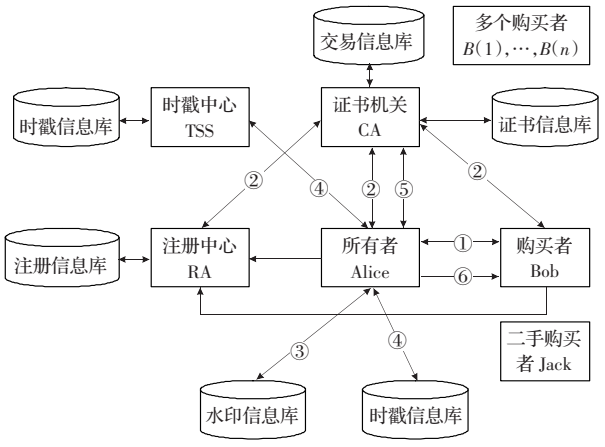

图 1　协议模型整体结构设计

(6)所有者与购买者交互——Alice 对指纹作品签名,将签名和指纹作品发送给 Bob;

(7)购买者验证——Bob 对收到的作品进行解密,得到嵌入了版权所有者标记水印、时间戳和指纹的数字作品,同时也得到了 Alice 的数字签名;

(8)二手交易、多方交易限于复杂性,将在后文具体描述,它们都不包括和 Alice 以及时间戳中心交互。

其中指纹 W 和水印 P 采用相同的水印嵌入算法被嵌入到不同的位置,以防止不同算法间的相互干扰。因此它们之间不会相互干扰,可以将它们联合起来看作一个水印。协议实现步骤如下:

(1)购买者与所有者交互

买方 Bob 生成一对用于匿名交易的公钥和私钥(PKB^*,SKB^*)和一对用于身份证明的公钥和私钥(PKB,SKB),并生成自己的指纹 W,同时进行如下处理:

$e_1=E_{PKB}{}^*(W)$,$P=P(SKB^*)$,$e_2=E_{PKC}(PKB^*)$,$S_B=Sig_{SKB}(e_1,e_2,P)$

式中,e_1 表示使用 *Bob* 的匿名公钥 PKB^* 对 W 进行加密;P 是匿名私钥 SKB^* 的证明;e_2 表示使用可信任第三方认证中心(CA)的公钥 PKC 对 PKB^* 进行加密;$Sign_{SKB}(e_1,e_2,P)$ 表示用 SKB 对 e_1,e_2,P 进行数字签名。

BOB 先向所有者 Alice 发送(PKB^*,e_1),提出购买数字产品的要求。Alice 收到请求后,向 Bob 发送确认信息,并等待 CA 对 Bob 的认证结果。

(2)购买者、所有者与 CA 以及 RA 交互

Bob 收到确认消息后,将(PKB,e_1,P,e_2,S_B)发送给 CA。CA 首先使用 PKB 对 S_B 进行确认,确认后,使用 PKB^* 检查 P,然后检查 Bob 的指纹 W 以确定其有效性。如果所有验证均通过,则 CA 将(PKB、PKB^*、e_1、e_2)存储进记录交易信息的数据库。

认证完 Bob 发送来的信息后,CA 向 Alice 发送($S_C=Sign_{SKC}(PKB^*,e_1)$,$PKB^*$,$e_1$)告知 Alice 对 Bob 的认证已经通过,交易可以继续。否则,协议终止。

(3)所有者生成水印

Alice 用 PKC 对收到的($S_C=Sign_{SKC}(PKB^*,e_1)$,$PKB^*$,$e_1$)予以确认,并与 Bob 发送来的($PKB^*$,$e_1$)比较,确认后,Alice 生成一对公钥和私钥($PKA$,$SKA$)和所有者标记水印 V,使用嵌入算法 g_1,将水印嵌入到数字产品 I 中,生成水印作品 $I_{A1}=g_1(I,V)$。

(4)所有者与时戳中心交互

接着 Alice 计算水印作品 I_{A1} 的哈希函数 $H_{A1}=SHA-1(I_A)$,并使用线状时间戳机制向 H_{A1} 加入自己的时间戳 t_1,然后向时戳服务中心(TSS)申请为 H_{A1} 添加时戳 t_2,得到时间戳证明 $T=H_{A1}\oplus t_1\oplus t_2$。将 T 嵌入水印作品 I_{A1} 得到含有时间戳 T 的水印作品 I_{A2}。

(5)所有者与 CA 交互

Alice 用 PKB^* 对 I_{A2} 进行加密,得到加密后的 $E_{PKB}{}^*(I_{A2})$,然后选择一个随机排列函数 f,将($E_{PKB}{}^*(I_{A2})$,f)发送给 CA。CA 收到($E_{PKB}{}^*(I_{A2})$,f)后,进行如下处理:

$I_{A3}=g_2(E_{PKB}{}^*(I_{A2}),f(E_{PKB}{}^*(W)))=g_2(E_{PKB}{}^*(I_{A2}),E_{PKB}{}^*(f(W)))=E_{PKB}{}^*(g_2(I_{A2},f(W)))$

这就将指纹 W 嵌入了水印作品 I_{A2},然后对其签名 $S_{C3}=Sign_{PKC}(I_{A3})$。最后将($I_{A3}$,$S_{C3}$)发送给 Alice。

(6)所有者与购买者交互

Alice 确认后,计算 I_{A3} 的哈希函数 $H_3=SHA-1(I_{A3})$,使用 ECC 算法用自己的私钥 SKA 对 I_{A3} 签名 $S_{A3}=Sign_{SKA}(I_{A3})$,然后将($I_{A3}$,$S_{A3}$)发送给 Bob。

Bob 使用 SKB^* 对 I_{A3} 进行解密,得到嵌入了 Alice 的版权所有者标记水印 V 和自己的指纹 W 的数字作品 $I_{A4}=g_2(I_{A2},f(W))$,同时也得到了对 I_{A3} 的 Alice 的数字签名。

(7)二手交易实现协议

二手购买者 Jack 向 Bob 提出购买申请,并获得其交易公钥 PKB^*。Jack 生成一对证明自己身份的公钥和私钥(PKJ,SKJ),以及生成水印 U,并进行如下处理:

$e_1'=E_{PKJ}(U)$,$Sign_{SKJ}(PKB^*,e_1')$

e_1' 表示使用 PKJ 对 U 进行加密,$Sign_{SKJ}(PKB^*,e_1')$ 表示使用 SKJ 对(PKB^*,e_1')进行签名。

Jack 将(PKB^*,e_1',PKJ、$S_J=Sign_{SKJ}(PKB^*,e_1')$)发送给 CA,CA 使用 PKJ 对 S_J 进行确认,确认后,对 e_1'进行有效性确认,之后通过 PKB^* 查找相应的交易信息数据库,获取前次交易的信息($E_{PKB}{}^*(W)$,f)然后向 Bob 发送确认信息,告之交易继续。

Bob 获得继续交易的确认信息后,将(I_{A3},$Sign_{SKB}(I_{A3})$)发送给 CA。CA 用 PKB 对 $Sign_{SKB}(I_{A3})$进行确认,确认后,使用 $E_{PKB}{}^*(W)$,f,$E_{PKB}{}^*(U)$进行如下处理:在公式 $I_{A3}=g_2(E_{PKB}{}^*(I_{A2}),f(E_{PKB}{}^*(W)))=g_2(E_{PKB}{}^*(I_{A2}),E_{PKB}{}^*(f(W)))=E_{PKB}{}^*(g_2(I_{A2},f(W)))$ 中使用 $f(E_{PKB}{}^*(U))$代替 $f(E_{PKB}{}^*(W))$,得到 $I_{A4}=g_2(E_{PKB}{}^*(I_{A2}),E_{PKB}{}^*(f(U)))=E_{PKB}{}^*(g_2(I_{A2},f(U)))$,这样就将 Jack 的指纹 U 嵌入了水印作品 I_{A2},然后对其签名 $S_{C4}=Sign_{PKC}(I_{A4})$。最后将($I_{A4}$,$S_{C3}$)发送给 Bob。

Bob 确认后,计算 I_{A4} 的哈希函数 $H_4=SHA-1(I_{A4})$,使用 ECC 算法用自己的私钥 SKB 对 I_{A4} 签名 $S_{A4}=Sign_{SKA}(I_{A4})$,然后将($I_{A4}$,$S_{A4}$)以及自己的公钥 PKB 发送给 Jack。Jack 使用 PKB 便可对 I_{A4} 进行解密,从而获取嵌有自己指纹 U 以及最初版权提供者水印的数字产品,同时也得到了 Bob 的签名。

CA 将把 e_1'、PKJ 与前次交易的信息储存在同一张数据库表中,保存前后两次交易的所有信息,并将(E_{PKB}、e_1'、PKJ)发送给 Alice。

(8)多方交易实现协议

应用协议进行多方交易的具体步骤和方法如下:

N 个购买者 $B(1),B(2),\cdots,B(n)$ 使用几个对应的 $PKB_1{}^*$,$PKB_2{}^*,\cdots,PKB_N{}^*$ 和 $e_1,e_2,\cdots,e_n$ 向 Alice 提出购买数字产品的要求。

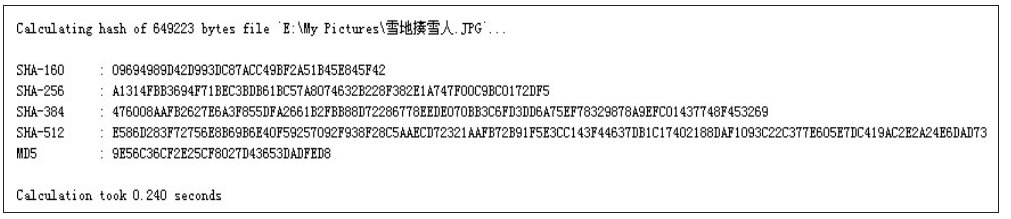

图2 实现协议模型的数字签名功能图

Alice 生成水印 V 和选择一个随机排列函数 f,并将水印 V 嵌入到数字产品 I 中,得到水印作品 I_A,再用 PKC 对 I_A 进行加密,表示为 $E_{PKC}(I_A)$。然后,Alice 使用 SKA 对 $E_{PKC}(I_A)$进行数字签名,表示为 $S=Sign_{SKA}(E_{PKC}(I_A))$,并将 S 以多播的形式发送给 $B(1),B(2),\cdots,B(n)$。

n 个购买者收到 S 后,使用 PKA 对其进行确认。然后,用 PKC 对 $e_1,e_2,\cdots,e_n$ 进行加密,表示为 $E_{PKC}(E_{PKB}(W))$,以及用 PKB^* 对 $E_{PKC}(I_A)$进行加密。这里采用的交互式加密方法可以实现:

$E_{PKB}{}^*(E_{PKC}(I_A))=E_{PKC}(E_{PKB}{}^*(I_A))$。$PKB^*$ 和 W 分别指与 $B(1),B(2),\cdots,B(n)$相对应的 $PKB_1{}^*,PKB_2{}^*,\cdots,PKB_n{}^*$ 和指纹 $W_1,W_2,\cdots,W_n$。

$B(1),B(2),\cdots,B(n)$分别将各自的 $E_{PKC}(E_{PKB}{}^*(W))=E_{PKC}{}^*(E_{PKC}(I_{A2}))$和 $PKB_1,PKB_2,\cdots,PKB_n$ 以及 $P_1,P_2,\cdots,P_n$ 发送给 CA,CA 确认 $B(1),B(2),\cdots,B(n)$的身份和水印的有效性后,向 Alice 获得 f,并就以上信息分别进行 $g_2(E_{PKC}{}^*(E_{PKC}(I_{A2}))$,$f(E_{PKB}{}^*(W))=E_{PKC}(E_{PKB}{}^*(g_2(I_{A2},f(W))))$。

CA 分别将 n 个嵌有买卖双方水印和加密了的数字产品,以及 n 个不同的 $KEY_1,KEY_2,\cdots,KEY_n$ 发送给指定的 $B(1),B(2),\cdots,B(n)$,它们可以分别使用指定 $KEY_1,KEY_2,\cdots,KEY_n$ 的对外层加密 $E_{PKC}(\,)$进行解密,再使用各自的匿名私钥 $SKB_1{}^*,SKB_2{}^*,\cdots,SKB_n{}^*$ 对内层加密 $E_{PKB}{}^*(\,)$进行解密,从而获取嵌有买卖双方水印的数字产品。

3 安全水印协议设计模型的效用和时空复杂度分析

3.1 效用分析

首先,二手交易:由可信第三方嵌入指纹,避免了二手交易必须找到原始创作者的弊端。

(1)购买者将自己购买的含有原始所有者水印 V、自己指纹 W 以及时间戳 T 的作品发送给 CA。

(2)CA 利用 Bob 的公钥解密,提取 Bob 的指纹,并将二手购买者 Jack 的指纹 U 嵌入其中,得到含有原始所有者水印 V、Jack 的指纹 U 以及时间戳 T 的作品,并返回给 Bob。

(3)Bob 确认后,同样的对上述作品签名后一起发送给 Jack;Jack 便获取了嵌有自己指纹 U 以及最初版权提供者水印的数字产品,同时也得到了 Bob 的签名。

其次,多方交易:引入 Qiao L T 的多播机制以及 Boneh D 提出的公钥追踪机制。

(1)多播机制允许将一个作品以多个相同的拷贝发送给不同的接收者,同时一个公钥可以有多个不同的私钥,保证了不同购买者都可以用自己的私钥解密作品,得到相同的拷贝。

(2)公钥跟踪机制使得同样可以使用上述的多个私钥以及数字产品中嵌入的不同指纹进行非法拷贝源的追踪。

3.2 时空复杂度分析

主要在 Memon N 提出的版权保护的数字水印协议模型基础上添加了两个交互。

(1)所有者与时间戳中心的交互:关键的时空消耗在于所有者对提交作品进行 Hash 运算。

(2)所有者与证书机关的交互:关键的时空消耗在于所有者向证书机关提交水印作品时进行公钥加密。

总之,模型的时空消耗取决于采用的 Hash 处理和公钥加密体系的效率。

4 安全水印协议设计模型的部分实现

(1)要实现上述版权保护协议模型,本文建议选择OpenSSL的应用软件包,实现了协议模型的数字签名功能,如图 2。

(2)测试了关于 Hash算法的性能,见图 3,图 4。

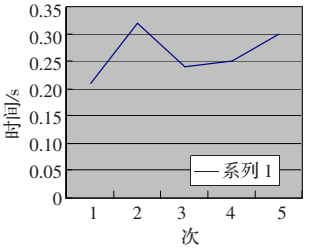

图3 同一数据进行 Hash 运算时间消耗图

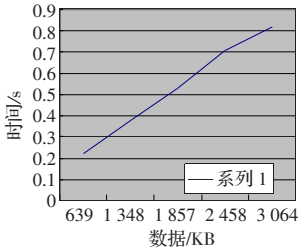

图4 时间消耗随数据变化大小曲线图

5 结束语

综合利用水印技术和密码技术,设计了一个安全可靠的版权保护协议,避免了现有协议的缺陷,可以满足版权所有者和购买者的应用需求,可以抵抗现有的协议层安全隐患。并对其性能做出分析,证明了其实际可行性。总的来说,研究设计了一个可以满足以下要求的版权保护水印协议:一是保护版权所有者的权益,可以进行所有权证明,可以对非法拷贝进行跟踪和鉴别非法拷贝源;二是抵抗了解释攻击和复制攻击等协议层安全隐患,提高了版权保护系统的安全性;三是保护版权购买者的权益,可以进行真伪作品鉴别,进行有条件的二次分发和多方交易等应用。

参考文献:

[1] Cox I J,Miller M L,Mckellips A L.Watermarking'as communications with side information[J].Proceedings of the IEEE,1999,87(7).

[2] Petitmlas F A P,Anderson R J,Kuhn M G.Information hiding:a survey[J].Proceedings of IEEE,1999:1062-1078.

[3] Fridrich J,Goljan M,Du R.Detecting LSB steganography in color and gray-scale images[J].Magazine of IEEE Multimedia Special Issue on Security,2001(10/11):22-28.

[4] Johnson N F,Duric Z,Jajodia S.Information hiding:steganography and watermarking—attacks and countermeasures[M].[S.l.]:Kluwer Academic Publishers,2001.

(下转 92 页)