A Multimedia Copyright Protection Protocol Based on Digital Watermarking and Digital Signature

Lu Wei

The First Aeronautic Institute of Air Force, XinYang 464000, China

luwei75@126.com

Abstract: With the fast development of Internet and popularization of the E-Commerce, the importance and urgency of digital media copyright protection is more and more obvious nowadays. How to use the digital watermarking technique to protect the copyright of digital media author or seller and the rights of buyer effectively has become the important research topic of network security area. A new scheme based on digital watermarking to protect the rights of digital media is proposed. In this scheme, the digital watermarking and digital signature can be used to trace the source of the illegal copy. The owner takes charge the embedding of watermark, and the information in watermark include the digital digest of the media and the identity of purchaser, and the information is unreadable to the owner. The three parts in this scheme, owner, purchaser and watermark CA(Certification Authority), keep and maintenance the necessary information in deal, it can be used in dissension.

Keyword: digital watermarking; digital signature; copyright protection; protocol

基于数字水印与数字签名的多媒体版权保护协议研究

卢炜

空军第一航空学院，河南信阳 464000

luwei75@126.com

【摘要】计算机网络技术的飞速发展和电子商务的日益普及使得网络环境下数字媒体的交易日益频繁，与之相关的版权保护就成为非常重要的问题。如何应用数字水印技术保护数字媒体创作者和销售者的版权，保护消费者的正当权益，已经成为网络安全领域的重要研究内容。本文给出了一种保护数字媒体版权的数字水印协议。该协议利用数字水印和数字签名技术，在发生侵犯销售者版权事件时，能追踪到非法拷贝的来源。嵌入水印的过程由销售者控制，嵌入水印的信息中也包含了购买者的身份信息，但此身份信息对销售者而言是不可读的，而且包含了原始图像的一个摘要。在交易过程中，参与交易的三方，即销售者、购买者和数字水印认证中心，分别保留和维护交易过程中收到的必要信息，用于在发生纠纷时解决问题。

【关键词】数字水印；数字签名；版权保护；协议

1 引言

Internet 的飞速普及使得数字产品的广泛传播成为可能，非法拷贝和传播有价值的、受版权保护的数字产品相当容易，而计算机、打印机和扫描仪等设备质量的提高和成本的下降使得复制多媒体数据极其方便，成本也非常低廉，由此带来了知识产权 IPR（Intellectual Property Right）的保护问题[1][2]。

数字水印技术是近年来出现的数字媒体产品版权保护技术，数字水印可以标识数字产品的作者、所有者、发行者或者使用者等，也可以包含版权信息和认证信息，目的是鉴别非法复制和盗用的数字产品，保护数字产品的合法拷贝和传播。

但是仅使用数字水印并不足以解决版权保护中可能出现的各种问题。在数字媒体版权保护协议中可能牵涉到的问题包括：用户身份的可靠识别、安全的产品分发、无二义的版权证明等等，这些问题的解决依赖于现代密码学的技术。必须结合现有的密码技术和电子商务协议才能在复杂的 Internet 环境下构建安全的数字版权保护方案。同时，目前提出的各种数字水印方案中，重

978-1-935068-09-9

点都在于对版权所有者即销售者的版权保护，很少考虑购买者的权益保护，一般都假定销售者是诚实的，从而给中间人攻击提供了机会，也无法保证购买者获得的水印化数字产品是合法的[1]。为此，在交易过程中必须确认双方身份并防止水印被非法使用。

为了在交易过程中让买卖双方能够确认对方的身份，引入水印认证中心 CA；为了防止购买者的水印被销售者非法用于别的数字产品，需要对水印进行置换操作，并要求嵌入的信息必须包含原始数字产品的相关信息。

2 数字媒体版权保护协议

首先给出数字水印协议的基本模型。

现实世界中的版权交易活动比较复杂，参与方较多，可能包括数字产品的创作者、无版权的产品代销商、买断版权的数字产品销售商、数字产品的最终购买者、版权管理机构、交易公证仲裁机构[2]等等，为了协议模型的简洁性和有效性，一般说来数字水印应用协议只包括或部分包括如下参与方：

销售者：数字产品的版权拥有者或拥有版权的数字产品销售商，可能包括数字产品的创作者和代理商。

购买者：数字产品的购买者，不拥有版权，被要求只可自己使用，不能公开或非法传播所购买的数字产品。

数字水印认证中心 CA：负责发放交易参与方用于交易的公钥和私钥，提供交易过程中需要的认证服务，也维护一个与版权交易相关的信息数据库。

仲裁者：任何可信任的第三方 TTP（Trusted Third Party），在出现有关版权的争议时（比如销售者发现有非法拷贝并认定拷贝源）做出最终的裁定，确认有过错的一方。一般而言，CA 也可以担任仲裁者的角色[3][4]。

协议中基本参与方的关系如图 1 所示。

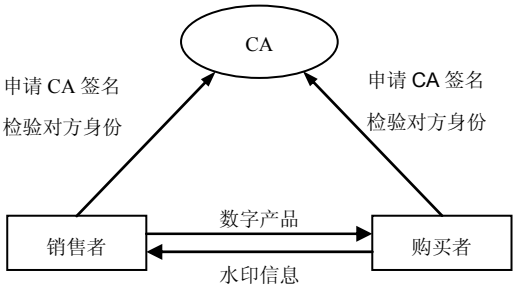

Figure 1. Protocol model
图 1. 协议模型

假设版权所有者即销售者为 A，合法用户即购买者为 B，CA 是数字水印认证中心，X 是 B 想从 A 处购买的数字产品(如一幅图片)，W′是 A 的水印，用于证明 A 的身份和所拥有的版权，W 为 B 用来证明身份的个人信息，H()为一种安全的散列算法，σ 为一个单向的置换函数。

协议具体描述如下：

（1）A→CA：H(X)。A 计算数字产品 X 的摘要 H(X)，发送给水印认证中心 CA，同时发送的还有他的数字证书；CA 对 A 提交的数字证书进行验证，对 H(X)进行数字签名并将 SignCA(H(X))发回给 A，CA 保留 A 的 ID 及 H(X)，如图 2 所示。

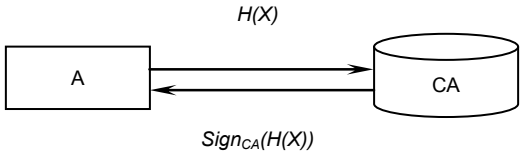

Figure 2. A send H(X) to CA and apply for CA′s signature
图 2. A 向 CA 提交 H(X)并申请 CA 签名

（2）A→B：(SignCA(H(X)), SignA(H(X)), H(X))。A 将 H(X)以及自己和 CA 对 H(X)的数字签名发送给 B；B 通过对签名的真实性进行校验来确认所收到的信息是从 A 那里发来的，而且所收到的信息的确是自己所要购买的数字产品的一个摘要，如图 3 所示。

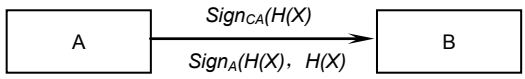

Figure 3. A send H(X) which CA signed to B
图 3. A 将经 CA 签名的 H(X)发送给 B

（3）B→CA：σ(W)。B 选定一个用于表明自己身份的信息 W，选择一个单向的置换函数 σ，用 σ 对 W 进行处理得到 σ(W)，然后 B 将置换过的信息 σ(W)发送给水印认证中心 CA，同时发送的还包括他的数字证书；在 CA 对 B 提交的数字证书进行验证之后，对 σ(W)进行数字签名，然后将 SignCA(σ(W))发回给 B，B 的身份就被确认了，如图 2.4 所示。

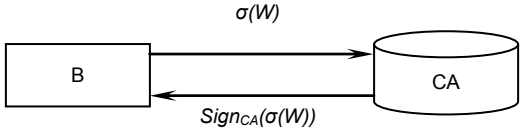

Figure 4. B sendσ(W) to CA and apply for CA′s signature
图 4. B 向 CA 提交 σ(W)并申请 CA 签名

（4）B→A：(SignCA(σ(W))，SignB(σ(W))，σ(W)，SignB(σ(W),H(X)))。B 将置换过的水印 σ(W)和 CA 的数字签名 SignCA(σ(W))、B 自己对 σ(W)和(σ(W),H(X))的数字签名 SignB(σ(W))和 SignB(σ(W),H(X))一起发送给 A，A 通过对签名的真实性进行校验来确认所收到的数据的确是由 B 生成的一个有效的水印，并且的确是 B 发送过来的。B 保留 σ(W)，如图 5 所示。

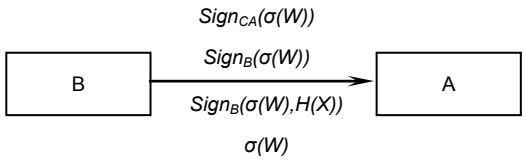

Figure 5. B send his watermark to A

图 5. B 将自己的水印发送给 A

（5）A：X′=X⊕W′⊕σ(W)⊕SignB(σ(W),H(X))。A 选择一个安全的水印嵌入算法，将 W′、σ(W)和 W′以及 B 对(σ(W),H(X))的签名嵌入到 X 中，得到 X′，如图 6 所示。

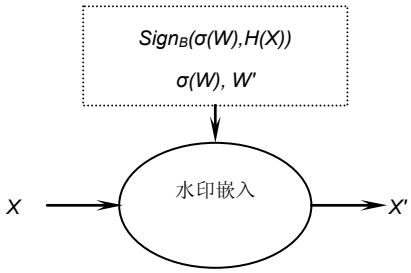

Figure 6. A embed the two watermark into X

图 6. A 将双方水印嵌入数字产品 X

（6）A→B：X′。销售者 A 保留 B 的 ID、W′、σ(W)、SignCA(σ(W))和 SignB(σ(W))，对 X′进行摘要得到 H(X′)，然后用他的私钥加密这个摘要。A 将水印化的作品 X′用 B 的公钥加密之后发送给 B，同时发送的还有加密的摘要。购买者 B 对从销售者 A 接收到的加密数据进行解密，得到水印化的数字作品 X′，然后用销售者的公钥解密接收到的摘要，并与自己计算出来的 X′的摘要进行比较，如果两个数值相等，则说明 X′的确就是自己所购买的数字产品。如图 7 所示。

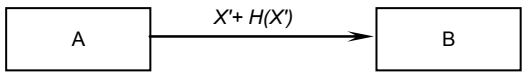

Figure 7. A send the embed X′ to B

图 7. A 将已嵌入水印的数字产品 X′发送给 B

如果发现了数字产品 X′的未经授权的拷贝 X″，销售者 A 就可以通过对原来由他嵌入的水印进行检测来确定这个拷贝是从哪个购买者流失出来的。水印提取算法可以从 X″中提取出水印 σ(W)，然后根据 σ(W)，销售者 A 就能从他所保留的数据表里查出购买者 B 是这份拷贝的购买者，并对 B 提出指控。如果 B 否认指控，A 可以公布他从 B 那里收到的 σ(W)、SignCA(σ(W))和 SignB(σ(W))，仲裁方可以由此校验水印的真实性，从而确定 B 是否与此未经授权的拷贝有关。

3 版权保护协议的安全性分析

3.1 Hash 函数的运用和伪造水印攻击

在加强版权保护方面，水印技术应能提供合理的证据，证明销售者所拥有的版权。但是，由于伪造水印攻击的存在，上述过程往往变得无效。伪造水印攻击的方式可能有[5]：

假设 1：攻击者 T 将自己的水印加入图像 X′，得到水印化图像 X″，并宣称其拥有图像 X″的版权。在销售者 A 所采用的数字水印算法满足健壮性要求的前提下，水印化图像 X″中现在包含了两个水印，一个是 A 所嵌入的，一个是 T 所嵌入的，而且都可验证，在这种情况下，如何决定其真正的版权归属？

假设 2：攻击者并不采取向 X′中加入自己的水印的方式，而是采取从 X′中去除水印 WT 的方式，伪造出一份假的原始图像 XT。

上述的两种假设情况都会导致版权之争。

针对第一种情况，虽然销售者 A 和攻击者 T 都声称对同一图像都拥有版权。但是销售者 A 可以要求攻击者 T 提供他的原始图像给验证方，以检查 T 所提供的所谓原始图像是否包含 A 的数字水印 WA；按照假设，实际情况是攻击者 T 在销售者 A 的水印化图像 X′中加入了 WT，那么，攻击者 T 的“原始图像”X′和“水印化图像”X″中必定包含销售者 A 的水印（除非销售者 A 所采用的水印算法不具有健壮性），而销售者 A 提供的原始图像 X 和水印化图像 X′中并不包含攻击者 T 的水印。所以，如果销售者 A 严格管理原始图像 X，那么就算攻击者 T 可以得到水印化图像 X′，但是他无法获取原始图像 X，从而使得这一类攻击失效。所以本文所提出的版权保护协议的一个基本要求就是销售者 A 要保证原始图像的安全。

针对第二种假设，导致版权之争的原因是：即使真正的原始图像 X 不可获取，攻击者 T 仍然可以伪造出假的原始图像 XT，从而形成两个原始图像 X 和 XT

978-1-935068-09-9 © 2010 SciRes.

的局面，而且其中任一方提供的原始图像中都含有另外一方的水印。

伪造攻击方法利用了可逆的水印算法的性质，从而可以证明 X′中包含水印 WT。由此可见，即使在协议中采用的数字水印算法满足健壮性的要求，也不一定能保证整个协议的安全性。

为了防止此类伪造攻击，应该使水印成为一个不可逆的值，且与原始图像 X 相关，而密码技术中的单向 Hash 函数完全满足要求。

在协议中，通过在嵌入的水印信息中加入原始图像的一个信息摘要来防止了上述的伪造攻击。由于在嵌入图像的数字水印中包含了购买者 B 对原始图像信息摘要 H(X)的数字签名 SignB(σ(W),H(X))，从而使得水印与原始图像相关，并且由数字签名算法的性质保证了攻击者 T 不可能由 SignB(σ(W),H(X))获取 H(X)，而攻击者 T 无法获取原始图像 X，所以不可能伪造出与真正的原始图像 X 有关的数字水印。

在验证过程中，即便可以通过攻击者 T 提供的 X′和水印提取算法获得 WT，但攻击者 T 无法证明 WT 与原始图像 X 有关。而真正的版权所有者即销售者 A 可以提供 WA 中包含了购买者对原始图像 X 的一个信息摘要 H(X)的数字签名信息 SignB(σ(W),H(X))的证据，从而证明自己所拥有的版权。

3.2 中间人攻击

所谓中间人攻击（Man-in-the-middle Attack）一般是指攻击者 T 不试图直接获取某种秘密而是秘密介入到协议双方 A 和 B 之间的通信中，使得 A 和 B 认为自己在与对方通信而实际上在与 T 通信[3]。

下面用攻击检验方法来分析第 2 节提出的数字水印协议的安全性。

经过对协议过程的分析，可以对该版权保护协议提出以下中间人攻击方式：

（1）攻击者 T 截获并篡改销售者 A 出售给购买者 B 的数字图像 X′（用 B 的公钥加密过的）；

（2）攻击者 T 截获并篡改销售者 A 发送给数字水印认证中心 CA 的请求认证的信息；

（3）攻击者 T 截获并篡改数字水印认证中心 CA 发送给销售者 A 的认证信息；

（4）攻击者 T 截获并篡改购买者 B 发送给数字水印认证中心 CA 的请求认证的信息；

（5）攻击者 T 截获并篡改数字水印认证中心 CA 发送给购买者 B 的认证信息；

（6）攻击者 T 假扮销售者 A 并向购买者 B 出售非法拷贝的数字图像 X〞；

（7）攻击者 T 假扮购买者 B 从销售者 A 处得到数字图像 X′；

（8）攻击者 T 窃取销售者 A 和购买者 B 的交易信息（比如窃取 B 的隐私和 A 的商业秘密）。

对于（1）-（5）类的攻击，本文提出的数字水印协议提供了有效机制来防止这些攻击。对（1）类攻击，由于水印化图像 X′在传输过程中是用购买者 B 的公钥加密的，同时传输的还有销售者 A 对 X′的一个摘要的签名，目前的公钥密码系统和数字签名技术已经可以提供足够的安全度以保证加密的数据被破解的概率足够小。对于（2）-（5）类攻击，攻击者截获的数据中都包含数字证书或者 CA 的签名，现有的 PKI 体系架构和技术可以保证签名是不可伪造的，因此也可以抵抗这些类型的中间人攻击。

对于（6）-（8）这些类型的中间人攻击，只要在数字水印协议开始阶段销售者 A 和购买者 B 之间执行某种身份认证协议，确定通信所需的密钥，而后续过程中的通信信息都用协商所得的密钥加密即可保证安全。如果使用的身份认证协议和密钥协商过程都对中间人攻击免疫，那么整个数字水印协议无疑可以抵抗（6）-（8）这些类型的中间人攻击。

4 结束语

本文在对现有版权保护协议的分析基础上，结合数字水印技术和数字签名技术提出了一种用于版权保护的数字水印协议，在发生侵犯销售者版权事件时，能追踪到非法拷贝的来源，确认盗版者的身份。在协议中利用散列函数和数字签名技术，有效地防止了中间人攻击，保证了协议的安全性和公平性。

参考文献

[1] N Memon and P.W Wong. A Buyer-Seller Watermarking Protocol. IEEE Transactions on Image Processing, 2001, 10(4), P643-649

[2] C.C Chang, C.Y Chung, An Enhanced Buyer-Seller Watermarking Protocol. IEEE Proceedings of ICCT 2003, P1779-1783.

[3] Hui-Mei Chao, Chin-Ming Hsu, Shaou-Gang Miaou. A Data-Hiding Technique with Authentication, Integration, and Confidentiality for Electronic Patient Records. IEEE Transactions on Information Technology, 2002, 6(1),P46～53.

[4] Wu Y T., Multimedia security, morphological processing, and applications, Ph.D. Dissertation, New Jersey Institute Technology, Newark, 2005. D.

[5] M.U. Celik, G. Sharma, E. Saber and A.M. Tekalp, Hierarchical watermarking for secure image authentication with localization, IEEE Trans. Image Process. 11 (6) (2002), pp. 585–595.