信息集中存储方式下的水印协议

边杏宾，朱清新

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】提出一种以存储为中心的交易和认证模型(SCTAM)及其水印协议，将信息集中存储在交易中心(TC)，TC自主处理任务不受外部干预，保障了信息的安全和一致性。User不直接和Owner交互，而是与TC交互购买产品。Judge仲裁过程不需Owner和User参与，实现了公平性。不同的水印技术分别用于Owner和User的水印的嵌入和提取，保障了水印的安全。SCTAM能够解决迄今发现的所有水印协议相关的问题，并简化了水印协议的设计。

关 键 词 版权保护； 水印协议； 信息存储； 电子商务

中图分类号 TP309 **文献标识码** A

Watermarking Protocol with Centralized Information Storage

BIAN Xing-bin and ZHU Qing-xin

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract A storage centered transaction and authentication model (SCTAM) is proposed with all information stored in transaction center (TC) where operations are carried out automatically and information security and consistency are ensured. The user does not interact with the owner in transaction; the judge can make decision without the aids from the owner and the user, which is fairer. Different watermark techniques are used to embed and extract watermarks for the owner and for the user to ensure the security of the watermarks. SCTAM can settle all problems discovered so far and make watermarking protocol easy to implement.

Key words copyright protection; ecommerce; information storage; watermarking protocol

在电子商务中，数字产品的版权保护是一个需要解决的问题。虽然数字水印技术能提供版权归属的证据，但因为需要约束交易双方的行为来维护双方的权益，单凭水印技术还不能完全满足交易中的安全要求。结合了加密技术的水印协议正是为了满足这种要求[1-6]。水印协议要实现的基本目标可以归纳为：(1) 数字产品所有者(Owner)认证；(2) 盗版追踪和盗版者识别；(3) 保护用户(user)不受Owner欺骗；(4) 保护User的隐私。除了上述目标，水印协议还需要解决信息(产品信息、水印及交易记录)存储问题。信息存储之所以重要，是因为若所存储的信息被破坏或不一致，水印协议就不能有效维护交易双方的权益。安全一致的信息存储不仅能保障水印协议的有效性，而且能简化水印协议的设计。但目前的水印协议未重视信息存储问题[1-6]。文献[2]最早明确讨论信息存储问题，但只简单地提及。文献[1]中，由TTP和Seller各自存储它们相应的信息。文献[2]和[3]将所有信息由Seller独自存储。然而作为将来处理版权纠纷的依据，信息不应由交易双方的任何一方来保存，因为他们之间存在利益冲突，由任何一方保存信息对对方来说是不公平的。而且文献[1-3]中的信息存储是分散的，容易造成信息的不一致和不利于管理。本文提出一种以存储为中心的交易与认证模型(SCTAM)，将信息集中存储在交易中心(TC)，保障了信息的安全和一致性。SCTAM使用户不直接和所有者交互，而是与TC交互；所有者将产品提交给TC，而不是发送给用户。当发生版权纠纷时，仲裁者(Judge)也只与TC交互并裁决。TC自动与所有者、用户和仲裁者交互，其处理过程及信息存储不受外来干预，提高了安全性。

1 以存储为中心的交易与认证模型的构成

以存储为中心的交易与认证模型 (SCTAM)的功能由3组水印子协议实现。水印协议中有所有者、用户和仲裁者3类参与者，以及TC和CA(数字证书授

收稿日期：2006 – 04 – 25；修回日期：2006 – 09 – 20
基金项目：国家自然科学基金(60671033)；教育部博士点基金(2006061405)
作者简介：边杏宾(1975 –)，男，博士生，主要从事多媒体及数字水印技术方面的研究.

权中心)两个机构。以存储为中心的交易与认证模型如图1所示。由于CA不参与交易和版权纠纷处理，所以不在该图中。TC中存储的信息包括：(1) 数字产品相关信息(存于表$\text{Table}_{\text{pro}}$)；(2) 交易记录(存于表$\text{Table}_{\text{tra}}$)。图1中，SCTAM的参与角色描述如下：(1) 交易中心(TC)：自动交易处理与信息存储机构。(2) 证书授权中心(CA)：负责分发数字证书给所有者、用户和仲裁者。(3) 数字产品所有者将自己的数字产品提交给TC，进行网上交易。(4) 用户从TC购买数字产品。(5) 版权纠纷仲裁者裁决版权纠纷，保护双方的权益。

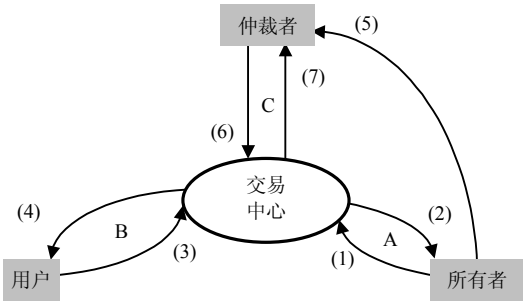

图1　以存储为中心的交易和认证模型

图1中，3组水印子协议分别为：(1) 数字产品提交协议，负责处理所有者将其产品提交到TC的过程。(2) 数字产品交易协议，负责处理数字产品的交易过程。(3) 版权纠纷处理协议，负责处理仲裁者解决版权纠纷的过程。图1中的交互操作包括：(1) 所有者提交其数字产品给TC。(2) TC返回产品的ID给所有者。(3) 用户提交购买数字产品的申请。(4) TC发送数字产品给用户。(5) 所有者发现其产品被盗版；向仲裁者提出指控。(6) 仲裁者查询TC获取解决纠纷的依据。(7) TC返回查询结果给仲裁者。

2　水印协议

水印协议中的符号表示定义如下：u表示用户(User)；o表示版权所有者(Owner)；j表示纠纷仲裁者(Judge)；r表示u、o、j的其中之一；$(\text{sk}_{\text{r}},\text{pk}_{\text{r}})$表示r的私钥－公钥对；$w_{\text{o}}$、$w_{\text{u}}$分别表示Owner和User的水印；$X$、$X'$、$X''$分别表示原始数字产品、嵌入$w_{\text{o}}$的数字产品、同时嵌入$w_{\text{o}}$和$w_{\text{u}}$的数字产品；$f_{w_{\text{e}_{\text{o}}}}(X,w_{\text{o}})$表示Owner的水印嵌入函数；$f_{w_{\text{d}_{\text{o}}}}(X'/X'')$表示Owner的水印盲提取函数，其中"/"表示"或"。$f_{w_{\text{e}_{\text{u}}}}(X',w_{\text{u}})$表示User的叠加水印嵌入函数；$f_{w_{\text{d}_{\text{u}}}}(X'')$表示User的水印盲提取函数；$E_{\text{pk}_{\text{r}}}(\cdot)$表示对加法运算具有自同态特性的加密函数[7]，满足$E_{\text{pk}_{\text{r}}}(a\oplus b)=E_{\text{pk}_{\text{r}}}(a)\oplus E_{\text{pk}_{\text{r}}}(b)$。由$f_{w_{\text{e}_{\text{o}}}}(X,\ w_{\text{o}})$的叠加性和$E_{\text{pk}_{\text{r}}}(\cdot)$对加法运算的自同态特性，得到关系：

$$E_{\text{pk}_{\text{o}}}(f_{w_{\text{e}_{\text{o}}}}(a,b))=f_{w_{\text{e}_{\text{o}}}}(E_{\text{pk}_{\text{o}}}(a),E_{\text{pk}_{\text{o}}}(b)) \tag{1}$$

对User的函数，该关系也成立。根据式(1)和$w_{\text{o}}=f_{w_{\text{d}_{\text{o}}}}(f_{w_{\text{e}_{\text{o}}}}(X/X',w_{\text{o}}))=f_{w_{\text{d}_{\text{o}}}}(X'/X'')$得：

$$E_{\text{pk}_{\text{o}}}(w_{\text{o}})=f_{w_{\text{d}_{\text{o}}}}(E_{\text{pk}_{\text{o}}}(X'/X'')) \tag{2}$$

式中　$D_{\text{sk}_{\text{r}}}(\cdot)$表示对应于$E_{\text{pk}_{\text{r}}}(\cdot)$的解密函数；$\text{Cert}_{\text{CA}}(\text{r})$表示由CA颁发给r的证书，任何人可以使用$\text{pk}_{\text{CA}}$验证，并获得$\text{pk}_{\text{r}}$；$\text{Sign}_{\text{r}}(A)$表示r使用其私钥$\text{sk}_{\text{r}}$对消息$A$的签名；$M_{\text{sub}}$、$M_{\text{buy}}$、$M_{\text{rec}}$、$M_{\text{acc}}$分别表示对应于数字产品提交、购买、接收和盗版指控4种行为的消息，分别规定了4种行为相应的约定。在进行交易或版权仲裁前，交易双方已经选择了密钥对，并且交易双方或Judge已从CA获得了数字证书和pk_{CA}。

2.1　数字产品提交协议

当所有者向TC提交数字产品时，数字产品提交协议规定了所有者和TC间的交互操作：

(1) 所有者选择能够标识其身份的有意义水印w_{o}，然后将$\text{Cert}_{\text{CA}}(\text{o})$、加密后的数字产品$E_{\text{pk}_{\text{o}}}(X)$、以及加密后的水印$E_{\text{pk}_{\text{o}}}(w_{\text{o}})$一起提交给TC。

(2) TC执行$E_{\text{pk}_{\text{o}}}(w_{\text{o}}')=f_{w_{\text{d}_{\text{o}}}}(E_{\text{pk}_{\text{o}}}(X))$，然后以$E_{\text{pk}_{\text{o}}}(w_{\text{o}}')$为关键字搜索数字产品信息表$\text{Table}_{\text{pro}}$，检查是否有匹配的加密后的水印存在，以验证是否已有水印存在于$E_{\text{pk}_{\text{o}}}(X)$中，若存在匹配记录TC将终止提交处理，否则继续步骤(3)。

(3) TC验证$\text{Cert}_{\text{CA}}(\text{o})$，若证书无效则终处理，否则在加密域将水印嵌入数字产品：

$$E_{\text{pk}_{\text{o}}}(X')=f_{w_{\text{e}_{\text{o}}}}(E_{\text{pk}_{\text{o}}}(X),E_{\text{pk}_{\text{o}}}(w_{\text{o}}))=E_{\text{pk}_{\text{o}}}(f_{w_{\text{e}_{\text{o}}}}(X,w_{\text{o}})) \tag{3}$$

并将$E_{\text{pk}_{\text{o}}}(X')$返回给Owner。

(4) Owner使用sk_{o}将$E_{\text{pk}_{\text{o}}}(X')$解密得到$X'$。并通过$w_{\text{o}}=f_{w\text{d}_{\text{o}}}(X')$来验证水印是否已被正确嵌入。若水印已被嵌入，用$\text{sk}_{\text{o}}$将提交消息$M_{\text{sub}}$和加密的水印一起签名得到$\text{Sign}_{\text{o}}(M_{\text{sub}}\,\|\,E_{\text{pk}_{\text{o}}}(w_{\text{o}}))$其中"‖"表示"连接"，然后将$M_{\text{sub}}$、$X'$和$\text{Sign}_{\text{o}}(M_{\text{sub}}\,\|\,E_{\text{pk}_{\text{o}}}(w_{\text{o}}))$提交给TC。

(5) TC验证$\text{Sign}_{\text{o}}(M_{\text{sub}}\,\|\,E_{\text{pk}_{\text{o}}}(w_{\text{o}}))$，若签名无效则终止处理，否则分配一个唯一的$\text{ID}_{X'}$给$X'$，并保存$\text{ID}_{X'}$、$X'$、$M_{\text{sub}}$，$\text{Cert}_{\text{CA}}(\text{o})$、$E_{\text{pk}_{\text{o}}}(w_{\text{o}})$和

$\mathrm{Sign_o}(M_{\mathrm{sub}} \| E_{\mathrm{pk_o}}(w_o))$ 到产品信息表 $\mathrm{Table_{pro}}$ 中。同时将表 $\mathrm{Table_{pro}}$ 中的交易量域置为0。最后将 $\mathrm{ID}_{X'}$ 返回给Owner。

(6) Owner保留 $\mathrm{ID}_{X'}$ 作为其数字产品在产品表中的键值。

数字产品提交协议确保只有Owner拥有没嵌入水印的数字产品。

2.2 交易协议

当User想从TC购买某种数字产品时，首先从TC的交易界面(网页或客户端软件)获得该数字产品的ID，然后执行以下与TC间的交互操作：

(1) User发送 $\mathrm{Cert_{CA}(u)}$、消息 M_{buy}、数字产品的编号 $\mathrm{ID}_{X'}$ 和 $\mathrm{Sign_u}(M_{\mathrm{buy}} \| \mathrm{ID}_{X'})$ 给TC。

(2) TC验证 $\mathrm{Cert_{CA}(u)}$ 和 $\mathrm{Sign_u}(M_{\mathrm{buy}} \| \mathrm{ID}_{X'})$，若任何一项无效，则终止处理；否则产生一个唯一的水印 w_u，并将其返回给User。

(3) User 使用 $\mathrm{sk_u}$ 对水印进行签名得到 $\mathrm{Sign_u}(w_u)$，并将签名提交给TC。

(4) TC验证 $\mathrm{Sign_u}(w_u)$，若签名无效则通知User；否则使用 $f_{w_{\mathrm{e_u}}}(X', w_u)$ 将 w_u 嵌入 X' 得到 X''，然后返回 M_{rec} 给User，通知User准备接收数字产品。

(5) User 将消息 M_{rec} 和 w_u 联合签名得到 $\mathrm{Sign_u}(M_{\mathrm{rec}} \| w_u)$，将其提交给TC。

(6) TC验证 $\mathrm{Sign_u}(M_{\mathrm{rec}} \| w_u)$，若签名无效则通知User；否则返回 X'' 给User。同时保存 $\mathrm{Cert_{CA}}(u)$、M_{rec}、$\mathrm{ID}_{X'}$、w_u、$\mathrm{Sign_u}(w_u)$、$\mathrm{Sign_u}(M_{\mathrm{rec}} \| w_u)$ 和交易时间 $\mathrm{Time_{tra}}$ 到交易记录表 $\mathrm{Table_{tra}}$ 中，并使产品信息表 $\mathrm{Table_{pro}}$ 中 $\mathrm{ID}_{X'}$ 的关联记录中的交易量域增加1。表$\mathrm{Table_{tra}}$和$\mathrm{Table_{tro}}$的访问根权限如表1所示。

表1 访问权限

电子商务参与方	$\mathrm{Table_{pro}}$			$\mathrm{Table_{tra}}$		
	读	写	修改	读	写	修改
所有者	Y	N	N	N	N	N
用户	N	N	N	N	N	N
仲裁者	Y	N	N	Y	N	N

2.3 盗版追踪与鉴别协议

若Owner发现其数字产品被盗版，则向Judge提出指控。盗版追踪与鉴别协议如下：

(1) Owner将被盗版的数字产品 X''、数字证书 $\mathrm{Cert_{CA}(o)}$、指控消息 M_{acc}、产品编号 $\mathrm{ID}_{X'}$、和 $\mathrm{Sign_o}(M_{\mathrm{acc}} \| \mathrm{ID}_{X'})$ 发送给Judge。

(2) Judge使用 $\mathrm{pk_{CA}}$ 验证 $\mathrm{Cert_{CA}(o)}$ 并得到 $\mathrm{pk_o}$，然后用 $\mathrm{pk_o}$ 验证 $\mathrm{Sign_o}(M_{\mathrm{acc}} \| \mathrm{ID}_{X'})$，若两项验证不能全部通过，则拒绝这项指控；否则Judge首先认证指控者是否是 X'' 的Owner，若起诉者是 X'' 的Owner，再进行盗版者识别。(1) Owner鉴定： Judge提取Owner的水印 $w'_o = f_{\mathrm{w_{d_o}}}(X'')$，并使用 $\mathrm{pk_o}$ 将 w'_o 加密得到 $\mathrm{E_{pk_o}}(w'_o)$，然后使用 $\mathrm{E_{pk_o}}(w'_o)$ 作为关键字搜索产品信息表 $\mathrm{Table_{pro}}$。若找到匹配记录，则验证该记录中的 $\mathrm{Sign_o}(M_{\mathrm{sub}} \| \mathrm{E_{pk_o}}(w_o))$，若验证有效，那么断定指控者是Owner；否则拒绝处理该项指控。(2) 盗版者鉴别：Judge从 X'' 中提取水印 $w'_u = f_{\mathrm{w_{d_u}}}(X'')$，然后使用 w'_u 作为关键字搜索交易记录表 $\mathrm{Table_{tra}}$，若找到匹配记录，Judge比较记录中的产品编号 $\mathrm{ID}_{X'}$ 和指控者提交的编号 $\mathrm{ID}'_{X'}$，若 $\mathrm{ID}'_{X'} = \mathrm{ID}_{X'}$ 则从匹配记录中的 $\mathrm{Cert_{CA}}(u)$ 得到 $\mathrm{pk_u}$。Judge使用 $\mathrm{pk_u}$ 验证记录中的 $\mathrm{Sign_u}(M_{\mathrm{rec}} \| w_u)$，并比较 w'_u 和匹配记录中的User水印 w_u，若签名有效且 w'_u 和 w_u 一致，则断定匹配记录中的User是盗版者或者盗版源，从 $\mathrm{Cert_{CA}(u)}$ 中揭示盗版者身份并通知指控者。

3 讨 论

3.1 安全性分析

本节分析SCTAM模型对水印协议的安全问题的处理。

(1) 重提交问题：可能有人先以合法User身份从TC购买某种数字产品，再将此产品作为自己的产品提交给TC来牟利。这是一个SCTAM特有的问题。为了消除该问题，在产品提交协议的步骤(2)中TC检查所提交的数字产品中是否已嵌入了其他某个Owner的水印，若所提取的水印在数字产品表中有匹配记录，则说明该数字产品被重复提交，则TC拒绝处理。

(2) 指控能力问题：Owner有充足的依据对侵权提出指控。在SCTAM中，因为没有人能够得到 X 或者 X'，所以当发生侵权时，Owner能够确信在被盗版的产品中存在自己的水印 w_o 和最初购买者的水印 w_u。

(3) 虚假指控：指某人假冒 X'' 的Owner去诬告无辜User。在SCTAM模型中，由于 w_o 将 X'' 的真实Owner绑定到 X''，Judge在盗版追踪和盗版识别协议中能够鉴别指控者是否是真实的Owner。

(4) 盗版者识别：在SCTAM中，User被 w_u 和所购买的 X'' 绑定在一起，而且除了与TC交互并且执行交易协议规定的操作，没有其他旁路可以获得 X''，因此User的交易记录一定存储在 $\mathrm{Table_{tra}}$ 中。Judge通过验证 $\mathrm{Cert_{CA}(u)}$ 和 $\mathrm{Sign_u}(M_{\mathrm{rec}} \| w_u)$，能够

揭示盗版者的身份，且对方无法否认。

(5) 解绑定问题[2]：指不诚实的Owner将盗版产品中的水印移植到价值更高的数字产品中来伪造盗版的行为。该问题在SCTAM模型中被消除，因为 w_u 和 w_o 都由TC执行嵌入，且交易过程和Owner无关，Owner也不能提取 w_u。因此也就不会发生水印移植的问题。

(6) 匿名问题[1]：指交易系统应能维护User的隐私。SCTAM模型解决了这一问题。首先，User在交易过程中不和Owner发生联系，因此Owner无法获得User的信息；其次，盗版者鉴别过程由Judge独立完成，在没有鉴别出盗版者前，Judge不会泄漏关于User的信息。再有，尽管Owner能够读取 $\text{Table}_{\text{pro}}$ 来了解自己产品的交易量，但没有权限访问记录有User信息的交易记录表 $\text{Table}_{\text{tra}}$，因此也就无法获得User信息。

3.2 性能和可实施性分析

在文献[1]和[3]中，数字产品所有者的水印是针对特定交易的，即每次交易时都嵌入一次水印，这种水印嵌入和使用方式在处理开销方面不可取。该水印协议中，数字产品所有者的水印只在向TC提交数字产品时由TC嵌入一次，所嵌入的水印用于在以后所有的交易中证明版权的归属，这种水印嵌入和使用方式节约了系统开销，提高了系统性能。

在实施方面，数字产品提交子协议、交易协议、盗版追踪和盗版者识别协议，3个水印子协议的划分清晰，易于实现。而且，SCTAM架构及水印协议适合以客户/服务器方式实现，并在互联网环境中部署。

4 结　论

提出以存储为中心的认证模型SCTAM及相应的水印协议。SCTAM将所有信息保存在独立的交易中心TC中。Owner事先将其产品提交到TC，购买方在购买数字产品时不直接与Owner交互，而是与TC交互，而且在处理版权纠纷时，Judge也只与TC交互，不需交易双方参与，保障了仲裁的公平性。SCTAM模型及其水印协议能够解决当前已知的所有水印协议的相关问题，且易于实现和部署。

参 考 文 献

[1] JU H S, KIM H J, LEE D H, et al. An anonymous buyer–seller watermarking protocol with anonymity control[J]. Proc ICISC 2002, 2587: 421-432.

[2] LEI Chin-laung, YU Pei-ling, TSAI Pan-lung, et al. An efficient and anonymous buyer-seller watermarking protocol[J]. IEEE Trans Image Process, 2004, 13(12): 1618-1626.

[3] ZHANG J, KOU W, FAN K. Secure buyer-seller watermarking protocol[J]. IEE Inf Secur, 2006, 153(1): 15-18.

[4] MEMON N, WONG P W. A buyer–seller watermarking protocol[J]. IEEE Trans Image Process, 2001, 10(4): 643-649.

[5] QIAO Lin-tian, NAHRSTEDT K. Watermarking schemes and protocols for protecting rightful ownerships and customer's rights[J]. Journal of Visual Communication and Image Representation, 1998, 9(3): 194-210.

[6] CHOI Jae-gwi, SAKURAI K, PARK JI-Hwan. Does it need trusted third party?[J]. Design of buyer-seller watermarking protocol without trusted third party. Proc Applied Cryptography and Network Security, 2003, 2846: 265-279.

[7] COHEN J D, MICHAEL J F. A robust and verifiable cryptographically secure election scheme[C]//In: Proceedings of 26th Annu Symp Foundations of Computer Science, 1985: 372-382.

[8] LI Qi-ming, CHANG Ee-chien. On the possibility of non-invertible watermark schemes[J]. Lecture Notes in Computer Science, 2004, 3200: 13-24.

编　辑　熊思亮

说明：

(1) 本刊2007年第6期第1 315页《电子采购系统动态身份认证策略研究》的英文题名应为Dynamic Identity Authentication Policy of E-Procurement System Research。

(2) 本刊2008年第3期第428页《网络多级委托授权模型及其应用》一文受到国家863计划(2006AA01Z456)、国家973重点基础研究发展计划(2007CB310704)、国家自然科学基金(60673098)的资助。