第33卷 第13期 计 算 机 工 程 2007年7月
Vol.33 No.13 Computer Engineering July 2007
·安全技术· 文章编号：1000—3428(2007)13—0173—03 文献标识码：A 中图分类号：TP308

基于数字水印的P2P协同工作环境信息认证技术

陈 军[1]，夏 旭[2]，朱从旭[2]
(1. 惠州学院计算机科学系，惠州 516015；2. 中南大学信息科学与工程学院，长沙 410083)

摘 要：分析了P2P应用中的协同工作所存在的安全问题，结合数字水印在认证方面的特点，提出了一种基于数字水印的解决方法，该方法可以防止非法用户伪装成协作者对其他用户进行欺骗，也能保证资源的完整性。
关键词：P2P；协同工作；数字水印；JXTA

P2P Collaboration Work Information Evidence Theory Based on Digital Watermark

CHEN Jun[1], XIA Xu[2], ZHU Congxu[2]
(1. Dept. of Computer Science, Huizhou University, Huizhou 516015;
2. College of Information Science and Engineering, Central South University, Changsha 410083)

【Abstract】 This paper analyzes the security problem of P2P collaboration work, combining with the characteristics of digital watermark, and puts forward a solution based on the digital watermark. This solution may prevent the illegal user from carrying on the deceit to other users, at the same time also maintain the integrity of resources.
【Key words】 P2P; collaboration work; digital watermark; JXTA

对等网络(Peer-to-Peer，P2P)是近年来广受IT业界关注的一个概念。它的出现改变了互联网上以网站服务器为中心的模式，网络中的参与者既是资源（服务和内容）提供者，又是资源（服务和内容）获取者。目前P2P的主要应用包括：对等计算，协同工作，文件共享和搜索引擎等。其中，协同工作是指对等点为完成某一特定的任务形成的一个群组，它们相互共享资源、即时交互，而且协作系统中的一个用户可以在同一时刻将一个信息多点传送到若干个用户。本文主要分析协同工作的安全特性，介绍基于数字水印实现认证的原理，并利用数字水印提出解决方法，将其应用到JXTA的平台上，对相关算法进行了分析。

1 P2P协同工作的安全需求与数字水印认证原理

1.1 P2P协同工作的安全需求

随着项目规模的不断扩大，“协同工作”的概念日益受到重视。目前已有的软件支持一般是基于C/S模型的。P2P技术实现的协同工作无需Server支持，而且同样可以组合成Workgroup，在之上共享信息、商讨解决方案等，提供更好的“协同工作”能力。根据国际标准化组织的开放系统互联模型的分层原则，认为协同工作的应用中主要成员有制作者、消费者和管理者[1]。协同工作的各个成员根据职责的不同，对安全的要求也不同。

协同工作的安全需求主要包括：

(1)系统成员信任关系管理。应该能够根据节点交易的历史记录，得到成员信任度；

(2)灵活多样的认证机制。同时支持多种认证方式，支持节点间的双向认证；

(3)系统用户之间的安全通信。保证交互、共享的信息和数据的机密性、完整性和不可否认性。

(4)可信协作关系的建立。为系统用户建立唯一的、可认证的合法身份。

本文主要解决第4个问题，即身份认证和信息认证问题。该问题在实际应用中经常可以遇到，人们使用传统的加密技术来解决这两个问题。在身份认证方面许多方法只是单纯的使用密钥机制来实现，但是密钥一旦泄露，攻击者就可以伪装成发送方或接收方。在信息认证方面，许多算法多借鉴密码学中的方法，一般是利用一个Hash函数来生成一个信息认证码，但此认证码需另外存储。这种方法增加了存储空间，并且不容许一个比特的失真。对于P2P这样的无中心的网络，不可能提供一个存储空间来存储认证码。而数字水印的认证算法，是直接将认证信息嵌入到原始信息中，不需要另外的存储空间。

本文提出利用数字水印技术，在发送的信息中嵌入与双方信息及传输内容相关的水印，可以防止第三方伪装成通信的任何一方进行欺骗行为，同时也能保证信息的完整性。

1.2 数字水印认证原理

数字水印[2,3]是信息隐藏的一种方法，它是利用载体中的信息冗余，在不破坏或尽量少破坏原始载体的情况下，将信息隐藏其中。数字水印一般可分为用于版权保护的鲁棒水印和用于防篡改的认证水印。

现有的认证水印算法很多，主要包括易损水印和半易损水印两大类。基于数字水印的认证系统通常包括3部分：水印的产生，水印的嵌入和水印的检测认证。认证水印系统的一般结构可用图1来表示。

基金项目：教育部高校博士点基金资助项目(20040533036)；国家自然科学基金资助项目(60573127)
作者简介：陈 军(1962－)，男，副教授，主研方向：计算机网络；夏 旭，硕士研究生；朱从旭，博士、副教授
收稿日期：2006-08-24 **E-mail：**czg@mail.csu.edu.cn

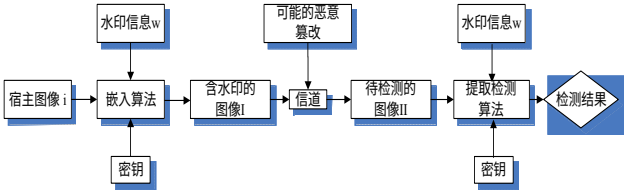


图 1　认证水印系统的一般结构

认证水印系统首先利用一定的算法将来自宿主图像或外界的信息转变成水印信号，通过嵌入算法将其嵌入宿主图像 i 中，得到含有水印的图像 I。其中 i 和 I 在人的知觉上没有明显差别。将含有水印的图像 I 经过信道传输到信宿端，通过水印检测对接收到的图像进行认证，得到检测结果。检测时，要求仅仅通过可能被篡改的图像 II，或者再加上水印信息 w，即可判断图像 II 是否遭受到篡改，从而检验其完整性。

2　一种基于 JXTA 平台的协同工作认证方案

2.1　水印的嵌入与提取

JXTA协议是由SUN公司于 2001 年 2 月推出的一项新技术，主要用于提供P2P程序所需的基础服务支持[4]。JXTA采用统一的对等节点寻址机制(Peer ID)。在JXTA中一个对等点(peer)是网络中一个独立的、异步运行的拥有一个Peer ID的实体，一个对等点的能力依赖于它所属的对等组，对等组内每一个对等点都有唯一的ID号。

由于目前数字水印的载体以图像居多，因此假设 P2P 协同工作的合法用户都具有能表明身份的图像，如徽章、印章等，而且考虑到 P2P 的动态性，为了加快水印处理速度，提高工作效率，在方案中采用直接在图像的空域嵌入水印的算法。原理如图 2。

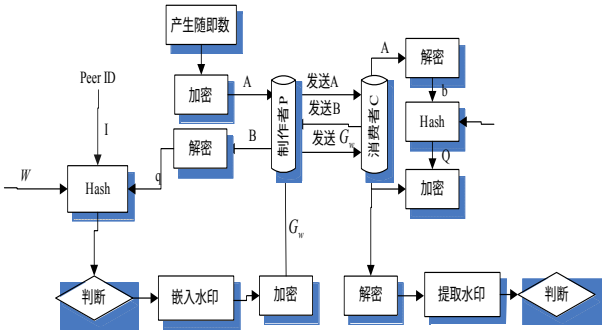


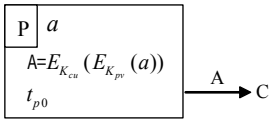
图 2　算法原理

希望加入 P2P 协作工作的节点将协议的信息摘要作为水印信息嵌入到数字印章中，用于协作关系建立时的身份验证，采用的是对称的盲水印方案。如果直接采用对称水印技术，会存在一些问题，因为对称水印方案中水印嵌入的密钥同样用于水印检测，如果攻击者窃取了水印嵌入密钥，就可以用该密钥来检测、甚至除去信息中的水印，为了避免这种情况的发生，在整个通信过程中采用非对称密钥体制予以辅助。加密和解密使用不同的密钥，所以不需要安全的信道来传送密钥，而只需要利用本地的密钥发生器（比如 PGP）产生。因为有两对密钥，所以可以对嵌入水印的信息进行两次加密，弥补了对称水印技术方案的不足。

本算法采用非对称密钥体制，设协作的发起方，即制作者为P，其公钥为K_{pu}，私钥为K_{pv}；协作的接受方，即消费者为C，其公钥为K_{cu}，私钥为K_{cv}。双方的ID号可以用JXTA平台的group.getPeerID()函数获取。

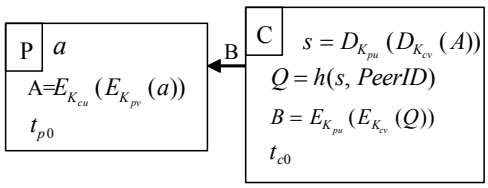
算法描述如下：

第 1 步　由制作者 P 进行处理：



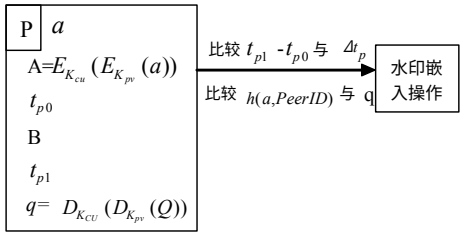
制作者 P 生成一随机数 α，利用自己的私钥对其签名（加密），即 $E_{K_{pv}}(a)$，然后用消费者 C 的公钥进行加密得到 A，即 $A=E_{K_{cu}}(E_{K_{pv}}(a))$，将 A 发送给消费者，同时记录时间 t_{p0} 和 α。

第 2 步　由消费者 C 进行处理：



消费者 C 收到 A，利用自己的私钥进行解密，即 $D_{K_{cv}}(A)$，然后制作者 P 的公钥进行验证签名（解密）得到 s，即 $s=D_{K_{pu}}(D_{K_{cv}}(A))$；将 s 和自己的 Peer ID 进行 Hash 运算得到 Q，即 $Q=h(s, PeerID)$；再对 Q 用消费者的私钥签名（加密），用制作者的公钥加密得到 B，即 $B=E_{K_{pu}}(E_{K_{cv}}(Q))$；把 B 发送给制作者，并记录发送时间 t_{c0}。

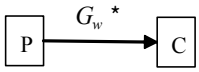
第 3 步　由制作者进行处理：



制作者 P 收到 B，并记录接收到的时间 t_{p1}，对 B 进行解密和验证签名，得到 q，即 $q=D_{K_{CU}}(D_{K_{pv}}(Q))$，为了不占用过多时间，必须设定一个时间的阈值，这里设阈值为 Δt_p，为制作者允许的最大时间间隔，表示如下：

if (t_{p1} - $t_{p0} \le \Delta t_p$ and $h(a, PeerID)$=q)
　then (下一步操作)
else 中断此次通信

第 4 步　由制作者 P 对将要传输的协议内容（设为 G）进行处理：



(1)计算 G 的 MD5 值，作为水印信息 W；

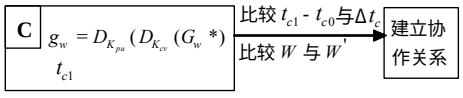
(2)用 q 作为水印密钥，对水印信息 w 加密得到 W_q；

(3)对载体图像 I（在本算法中假设是表明用户身份的数字公章图像）作预处理，将 W_q 嵌入，得到 I_w；

(4)将 I_w 插入到要传输的 G 中，得到 G_w，对 G_w 进行加密得到 G_w*，即 G_w*= $E_{K_{cu}}(E_{K_{pv}}(G_w))$；

(5)将 G_w*发送给消费者。

第 5 步　由消费者 C 进行处理：



消费者 C 收到 G_w*，对其进行解密，得到 g_w，即 $g_w=D_{K_{pu}}(D_{K_{cv}}(G_w*))$，并记录收到 G_w*的时间 t_{c1}，为了不浪费资源，必须根据网络情况设定一个时间的阈值，这里设

阈值 Δt_c 为消费者允许的最大时间间隔，可以表示如下：

if (t_{c1} - t_{c0} $\leq \Delta t_c$ and W= W') then (建立协作关系)

else 中断此次通信

其中，通过水印提取，得到 W_q ，利用 Q 从 W_q 中提出 W，而 W' 则是计算所收到的文件内容的信息摘要得到。

在协议中嵌入水印的基本算法如图 3 所示。

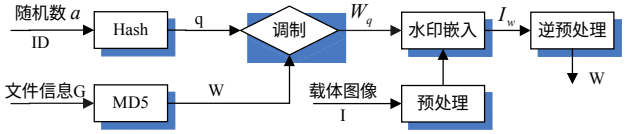


图 3　水印嵌入原理

先用MD5 算法计算出要传输信息的信息摘要W，把W作为水印信息，发送方产生一随机数α，用散列函数生成密钥q，用q对水印信息进行调制得到 W_q ，再将 W_q 嵌入到经过处理的载体图像（采用能表明用户身份的数字公章图像）上去，得到含水印的图像 I_w。这里的预处理是指经过某种变换域变换，如DTF、DCT和DWT变换。

双方的身份确认后，就可以进行协同工作，因为本文重在解决可信协作关系的建立问题，具体方法这里不在叙述。

2.2　水印的认证

本算法因为采用传输协议文件内容的信息摘要作为水印信息嵌入到数字公章图像中，它可以有效防止篡改，文件内容稍加改动，其 MD5 值就会与水印信息中的原值不同。协作的双方通过对提取出的水印进行检测，就可以判断出协议的内容是否被篡改了，同时可以确认对方身份。

比如多个节点之间要建立协作关系，协作的发起方向合法的协作者传送文件，对外是保密的。发起方相当于制作者P，合法协作者相当于消费者C，若有非法用户想窃取该机密文件（相当于攻击者E），用不法手段窃取了合法协作者的私钥 K_{cv}，伪装成合法协作者（消费者C），然后截取了P发送过来的A，用合法协作者的私钥 K_{cv}和发起方的公钥 K_{pu}可以解密得到b，但是不知道Peer ID，因此无法获得正确的 Q，设其生成 Q'，当P收到 Q'，解密得到 q'，然后再用正确的ID和α进行Hash运算，显然这个值不等于 q'，此时，P就可以知道对方不是要通信的对象，攻击者E伪装为合法的协作者失败。若攻击者E想伪装成制作者P，向合法协作者提供虚假资料进行欺骗，同样，攻击者先截获合法协作者所生成的Q，直接将Q作为水印信息，但不具备P的私钥 K_{dv}，合法协作者C对接收到的 G_w 解密后，计算得到的W不可能和 W' 相同，即合法协作者会认为信息无效，攻击者伪装成协作发起者失败。该算法还可以防止不可否认性，即协作发起者P否认信息是由他发出的，以及否认资料是由他所提供的。因为C可以向公证机构出示P的随即数b和其ID，计算q，通过水印检测算法利用q可以把水印提取出来，从而验证传输的信息中存在与P对应的水印，这就说明随机数b确实由P生成，这样P就不能否认其之前的行为。所以，协作的发起者必须对自己的行为负责，从而维护协作双方的利益。

3　小结

本文提出了一种将数字水印与加密算法相结合应用到P2P 的协同工作中的算法，该算法主要是针对 P2P 无中心，不可能提供存储空间来存储认证码的缺陷，利用数字水印可以将认证信息嵌入到原始信息中，不需要存储空间的特点，从而使身份认证过程更为严密。

参考文献

1 张铁军, 张玉清, 战守义, 等. Peer-to-Peer 典型应用安全需求分析[J]. 计算机工程, 2004, 30(20): 56-58.

2 Wang Xianpei, You Wenxia, Wang Quande. A Solution to Electronic Stamping for Documents[C]//Proceedings of International Symposium on Future Software Technology, Wuhan. 2002.

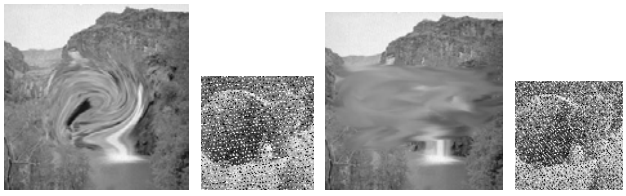
3 Katzenbeisser S, Petitcolas F. 信息隐藏技术——隐写术与水印[M].

4 Project JXTA: A Technology Review[Z]. http//www.jxta.org/pmject/www/ docs/TechOverview.pdf.

5 Li Gong. Get Connected with Jxta[C]//Proc. of Sun Microsystems Java One Conference. 2001.

（上接第 172 页）

如果用 photoshop 对嵌入水印的图像进行涂抹处理，则提取出的水印如图 6 所示。



(a)　(b)　(c)　(d)

图 6　嵌入水印的图像用 photoshop 进行涂沫处理后提取水印

5　结论

考虑人为地对水印植入图像进行一些切除、测试提取的水印图像，以此来考察算法的鲁棒性。从恢复的水印图像可以看到，此算法对剪切及涂抹操作具有较强的鲁棒性，因为通过基于 Arnold 变换和新型反变换，水印图像的信息已经尽可能地分散到原始图像的整个空间域中，所以当图像受到局部攻击时，仍然可以很好地提取出水印。

感谢　本文得到了贾振红博士的悉心指导，在此表示衷心的感谢!

参考文献

1 徐迎庆, 刘慎权, 齐东旭. 织物纹理的计算机生成技术[J]. 软件学报, 1998, 9(6): 409-413.

2 李昌刚, 韩正之, 张浩然. 图像加密技术综述[J]. 计算机研究与发展, 2002, 39(10): 1317-1324.

3 丁　玮, 齐东旭. 数字图像变换及信息隐藏与伪装技术[J]. 计算机学报, 1998, 21(9): 838-843.

4 齐东旭. 矩阵变换及其在图像信息隐藏中的应用研究[J]. 北方工业大学学报, 1999, 11(1): 24-28.

5 陈　伟. 关于 Arnold 变换的周期性[J]. 北方工业大学学报, 1999, 3(11): 29-31.

6 孔　涛, 张　亶. Arnold 反变换的一种新算法[J]. 软件学报, 2004, 15(10): 1558-1564.

7 王剑林, 福　宗. Matlab 在数字水印技术研究中的应用[J]. 计算机工程与应用, 2003, 39(7): 156-158.

8 齐东旭, 邹建成, 韩效宥. 一类新的置乱变换及其在图像信息隐藏中的应用[J]. 中国科学(E 辑), 2000, 30(5): 440-447.