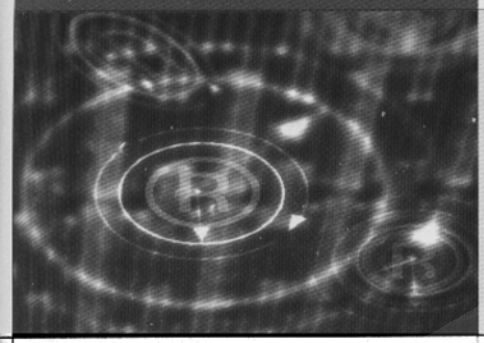
数字水印移动 Agent 系统

Digital Watermark Mobile Agents System

王 峰（郑州华北水电学院信息工程系 450008）
魏秀然（河南农业大学 现代教育技术部 450002）



摘 要：数字水印是数据安全技术中最有发展前景的技术之一。但是如何有效在大型网络中检测数字水印，是一个具有挑战性的问题。我们在本文中提出一种基于移动agent的数字水印模型，移动agent可以自动在网络中的主机间巡游，检测水印和收集证据，并可以在发现非法使用时采取相应行动。

关键词：数字水印 移动代理

1 引言

多媒体数据的数字化，使得多媒体信息的交流已达到了前所未有的深度和广度。但是随之而来的是使得作品侵权更加容易，篡改也更加方便。为了有效地保护知识产权，数字水印（digital watermarking）技术已成为多媒体信息安全研究领域的一个热点，它通过在原始数据中嵌入秘密信息——水印（watermark）来证实该数据的所有权。数字水印与原始数据（如图像、音频、视频数据）紧密结合并隐藏其中，成为源数据不可分离的一部分，并可以在经历一些不破坏源数据使用价值或商用价值的操作下而存活下来。

数字水印技术的实现一般包含有两个部分：嵌入部分和检测部分。嵌入部分主要是利用各种变换手段将水印安全地隐藏到原始数据中。在小波变换等新技术出现后，水印的嵌入技术逐渐趋于成熟。检测部分，则主要负责提取和检测多媒体数据中的数字水印，一般是嵌入部分的逆操作。

但是，在国际互联网出现后，盗版及侵权问题日益严重，而对于像国际互联网这样拥有众多主机的大型网络来说，如何在其上收集数据并实施水印检测，是一项繁琐而复杂的工作。

一个简单的解决办法是采用WEB页面水印探测机制。探测软件连接到远程主机后，跟踪每一个HTML链接，并下载多媒体文件到本地文件系统来检测水印。而多媒体文件的容量一般都比较大，所以这种方法只适合于在有一定的目标后，在某台主机或几台主机范围内实施。否则，如此大量频繁的下载，会极大的加重网络的负载，而且也给本地计算机以很大的负担。因此，它并不适合于大批量的水印检测。

为了解决这个问题，可以把数字水印检测技术和移动agent技术相结合，实施分布式处理。

移动agent（Mobile Agent简称MA）可以简单地理解为一段计算机程序，它能够在运行时刻从一台主机移动到另一台主机上继续执行，代表用户完成特定的任务。相对于在客户机服务器机制中，数据移动到程序端进行处理的方法，移动agent是把程序移动到数据端。这种方法可以有效地降低分布式计算中的网络负载，提高通信效率。

把数字水印检测技术和移动agent技术结合起来，就可以更有效地实施版权保护。由于移动agent不需要网络的持续连接，水印检测过程可以在远程主机的空闲时间进行，检测结果可以异步的传送回控制中心。进一步，它可以在检测到非法使用时，采取适当的行动。例如：它可以发送一封警告信给主机的管理员，控告主机对受保护文档的非授权使用。

2 系统架构

数字水印agent系统是一个基于大型计算机网络的分布式计算环境，它可以派遣和执行数字水印agent。为了更好地控制移动agent的运行，系统中除了基本的agent服务器（即agent运行支持环境）和移动agent以外，还增加了控制中心。

当作者想保护他的作品时，可以向控制中心发送一个请求，控制中心将分配一个水印agent到远程主机(可指定主机、主机范围或随机选择)。远程站点上已经安装的agent服务器(agent server)就会开始执行水印agent。

agent将尝试从文件中提取水印，如果提取到了正确水印，并且其赋与的版权与当前环境（位置、时间、用户等）不符，则agent可以按照控制中心的预先设定，采取相应措施，如：发送电子邮件给相关人员提出警告，或者，如果它有权限的话，它可以把文件移动到一个安全地方或直接删除相应文档。然后，agent向控制中心报告相应信息，并复制它自己，自动迁徙到其它站点,继续实施水印检测。

下面分别一下介绍各部分的主要功能：

2.1 控制中心

＊控制中心负责准备并设定一个水印agent，包括水印agent的目标、中止条件、行动策略（发现非法使用时如何处理）和水印安全密码等；

＊ 派遣水印agent到远程主机去执行；

＊ 收集和处理水印agent的报告数据，放入中心数据库（相当于一个知识库）；

＊ 向水印agent提供更新信息来指导水印agent的迁徙。

控制中心在派遣水印agent前，可以设定两种中止条件：设定水印agent的存活时间和水印agent的代数（水印agent每复制一次称为一代）。例如：控制中心可以设定一个水印agent和它的所有复制必须在分派后一周内中止，则在分派一周后，此水印agent和它的所有复制都将中止。或者设置它的最大代数为10，则第10代水印agent将不再复制，它会在完成任务后删除自己。另外，控制中心通过发相应控制送命令，可以随时中止任何它所分派的水印agent。

中心数据库里主要存放与移动agent相关的各种信息，包括：移动agent已经访问过的主机地址；以前查到的存在非法使用的主机地址；一些被怀疑可能存在非法使用的主机地址；对查到的每一非法使用将会记录它的详细侵权信息，时间、地址、所侵权的产品以及其它可能作为侵权证据的信息。所有上述信息也是水印agent迁徙的重要依据。

2.2 agent服务器

远程agent服务器为水印agent提供执行环境务。也称之为MAE(mobile agent enviroments)，水印agent通过它来访问远程主机的本地文件系统。agent服务器还需要提供传送服务，这样水印agent就可以把它自己复制到其它站点。另外，agent服务器也需要对水印agent进行检查和认证，以避免恶意agent对主机的危害。

agent服务器可以采用一些通用的agent平台系统，如：IBM aglets，Mitsubishi Concordia，General Magic Odyssey、以及国内的南京大学开发的MOGENT移动agent平台等。也可以开发专用的水印agent平台，就可以专门针对水印检测作出优化，使运行效率更高。

2.3 水印 agent

水印agent可以被派遣或自动迁徙到远程主机上，通过主机上的agent服务器访问主机的文件系统。在过滤掉不需要处理的文件后，从相应的文档中依次提取水印，如果提取到水印，则进一步验证水印中的版权与环境信息（如：地点，用户，时间）是否相符，若存在非法使用，则根据控制中心预先的设定采取相应的行动。当所有的检测完成后，水印agent向控制中心报告信息，并从中心获得相应指导信息，来更新水印agent。最后根据迁徙模型计算下个目的地，复制自己并迁徙到下一台主机。

3 迁移模型

与其他水印agent不同，水印agent可以不预先设定一个迁徙路线。当水印agent在一台主机上完成水印检测后，它可以自己决定下一个迁徙目标。它主要依赖于以下三种信息：当前主机的WEB服务器的日志文件；控制中心数据库中所记录的曾被检测到有非法使用的主机；一些被怀疑有非法使用的主机；当前的选择算法是对以上三种因素进行加权累加，确定权值最大的主机为迁移对象。

假设H是当前主机，H'是一个可能的目标主机。选择H'可能性（P）按以下公式计算：

P(H') = S*W1 + N*W2 + V*W3 + V/T*W4

如果H'是个可疑站点则S = 1，否则S = 0，N是H'单位时间内访问H的次数，V是H'上已经检测到的违法次数，T是记录在数据库中所有agent访问过H'的次数，W1－W4是相应的权重。这样一个动态路线机制，可以解决死锁现象，即：当一个水印agent不知道哪个主机是已经被访问过的时候，agent可能会在两台主机间反复互相迁徙，产生死锁。通过与控制中心的协调就可以解决死锁问题。控制中心把所有水印agent访问过的主机记录在中心数据库中,这些主机将从以后的个迁徙主机清单上移去，从而避免了死锁的发生。

4 系统安全

由于移动agent系统本身是开放的，所以系统安全是移动agent系统中一个非常关键的问题，主要包括三个方面：移动agent系统中的主机保护，移动agent如何防止恶意主机的攻击以及传输过程中的数据保护。

主机保护方面可采用的方法有：存取控制（认证、授权与资源分配），沙箱机制（Sandboxing），以及携证代码（proof-carrying code）等方法；对于移动agent的自身保护，主要采用的方法有：事前检测、事后分析、加密计算，黑匣子（Blackbox)以及基于硬件的保护方法等；网络传输的安全问题，主要可以通过两种方法解决：一种是保护所有的通信通道，包括agent分派和报告收集，通过一些已经成熟的技术，如SSL（安全套接层）来实现，另一种方法是在网络传输前加密敏感数据，并利用数字签名技术，建立agent和服务器之间的信任关系。

5 系统实现

由于Java语言的跨平台性，目前大多数的移动agent平台都是用Java语言实现的。Java平台还提供一些对网络安全的支持策略，而Java的RMI（远程调用方法）则可以支持分布式计算。同基于专用解释性语言实现的移动agent系统相比，基于Java语言实现的移动agent系统具有更强的功能和更大的灵活性。但是，所有基于Java语言的系统都是弱移动系统，原因是系统要利用现有的Java虚拟机，而Java虚拟机不能捕获agent的线程状态，因而要作到强迁移就必须更改虚拟机，具体办法可参考有关文献。

数字水印移动agent系统也采用Java语言平台来实现。为了支持点对点通信，需要开启agent服务器和控制中心的远程调用服务，以便于互相之间可以方便的通信。

系统中的数字水印部分，可采用基于小波变换的水印算法来实现。或者可以通过利用Java本身的接口技术，定义一个标准接口，用来支持外部水印库。使得Java对象可以方便的调用C语言或其它语言的水印函数，从而使得水印agent可以支持其他的水印系统。

控制中心的数据库部分采用Java的JDBC方法访问。Java提供内嵌的ODBC和JDBC的连接，物理数据库可以是任何支持ODBC（开放的数据库互连）的关系型数据库。

目前Java的RMI还不支持安全传输，所以为了在大型网络（如互联网）中保护数据，可以增加一个SSL（安全套接层）来替换Java的标准传输层。一旦在通道两端建立了安全套接层，所有在通道中的数据就可以保证安全了。为了进一步保护agent的静态和动态数据，可以采用Java的序列化机制，在对象的读写方法中执行基于商业加密包的序列化算法来保护数据。

6 总结

数字水印移动agent系统可以较好地解决在大型网络中检测数字水印的问题，且易于实现，网络负载也大大降低。进一步的研究可以考虑融合数据挖掘技术，研究数据混合模式，利用一些多源信息，如相关商业分类和我们的网页搜索引擎的搜索结果，来实现更智能化的迁徙策略。

参考文献

1 易开祥、石教英、孙鑫，数字水印技术研究进展[J]，中国图象图形学报，2001.2。

2 Q Ruanaidh J J, Dowling W J, Boland F M.《Watermarking digital images for copyright protection》IEEE proceeding on Vision, Signal and Image Processing, 1996.8。

3 Cbia T.H Kannapan S.Strategically mobile agents [A].Proc MA'97 Lecture Notesin Computer Science [C].Berlin: Springer Verlag,1997:149-161。

4 刘建勋、李仁发、张申生，移动Agent的安全性问题探讨[J]，沈阳 小型微型计算机系统,2000。

5 冯扬悦、陶先平、吕建，PCC技术在移动agent系统安全中的应用初探[J]，重庆 计算机科学，2002。

6 Torsten I,Frank K. Migration of mobile agents in Java:problems,classification and solutions [A]. proc of MA'2000[C].Australia。