Digital Watermark Mobile Agents*

Jian Zhao and Chenghui Luo
Fraunhofer Center for Research in Computer Graphics, Inc.
321 South Main Street
Providence, RI 02903

Abstract

Digital watermarking has emerged as an enabling technology for protecting intellectual property rights of digital information. However, the effectiveness of digital watermarking relies on the efficient detection of watermarks from huge amount of documents in cyberspace. Digital watermark agent provides an efficient solution. A digital watermark agent travels from host to host on a network and acts like a "detective" that detects watermarks and collects evidence of any misuse. Furthermore, we developed an active watermark method which allows the watermarked documents themselves to report their own usage to an authority if detected.

1. Introduction

Recently, digital watermarking has emerged as a promising technology for intellectual property rights protection [Zhao et al. 1998, Memon & Wong 1998]. Industries from Hollywood studios to computer and consumer electronics manufacturers are embracing the technology. To protect their rights in multimedia works, authors, photographers, publishers, and service providers embed digital watermarks into the text, video, and audio of their works to identify copyright related information such as origin, ownership, use-control, integrity, or destinations. A digital watermark is integrated with the multimedia and tightly bound with the quality of the content.

The effectiveness of digital watermarks relies on the evidence extracted from the watermarks that reveal illicit copying and dissemination of stolen digital documents. On a large computer network such as the Internet with millions of hosts, searching watermarks from the data distributed over the network is a challenging task. A straightforward approach is watermark web spider. A watermark web spider follows HTML links and downloads them to the local file system for watermark detection. The frequent downloading of huge amount of data greatly increases network traffic and enforces a heavy burden to local computation. As a result, the web spider approach is not appropriate for large-scale watermark-based detection of copyright infringement.

Contrary to the client-server scheme where data is moved to a program for computation, a mobile agent system moves a program to data [Chess et al. 1997]. This paradigm solves the problem in watermark spider. First, migration of mobile agents to the remote host reduces

* This project is funded by the Army Research Lab and DARPA under Agreement #DAAL01-98-3-0035 and Fraunhofer TRADE program.

network load because the agent code is much smaller than the files to be checked on the host. Second, a watermark mobile agent distributes the computation on the hosts over the network, since watermark detection will be performed on remote hosts. Finally, a watermark mobile agent does not require ongoing network connectivity. The watermark detection process can run during the idle time on the remote hosts and the detection results can be sent to the agent owner asynchronously.

An additional power of digital watermark mobile agents is that they can take proper actions if an infringement is detected. For example, an agent can charge the host for unauthorized use of copyrighted documents, send a warning to a webmaster, or move a document to a secure place if the agent has privileges to do so.

However, watermark mobile agents introduce critical security and privacy issues just like other mobile agent applications. Moreover, mobile agent paradigm requires the host to install an environment (called agent server in this paper) for the execution of the agents. To satisfy this requirement, appropriate social and business models are needed to support the popularity of the mobile agents.

We will first present several application scenarios of the watermark mobile agents in section 2, in order to better describe the motivation of this work. Then we will describe the system architecture, security features, and implementation details in section 3-5, respectively. Finally in section 6, we present our conclusion and plans for future work.

2. Application Scenarios

Digital watermark has found a multitude of potential applications other than the originally motivation for copyright protection [Zhao et al. 1998]. Similarly, the various types of uses of the watermark agents create many spectrums and great business opportunities. We will present several such examples in this section.

Detection of Unauthorized Use on the Internet

The original goal of the watermark agents is to efficiently search watermarks in millions of copyrighted information on the Internet in order to detect any unauthorized use of such information. In this case watermarks embedded in web documents identify copyright policies such as ownership or authorized users.

For this scenario, it is a problem for web sites to accept watermark agents. One way to enforce web sites to do so is through a contractual agreement. Another approach to motivate web sites is through marketing promotion.

Royalty Collection

This model extends the above scheme by adding payment functions into watermark agents or handling the payment in collaboration with an external online billing entity.

The watermark for such application needs to include price information. The watermark agents, on behalf of copyright owners, charge a user for any unpaid use of copyrighted web documents.

Document Trace and Security Enforcement

Electronic distribution and storage of sensitive information creates serious security problems. Even in a trusted network such as a corporate Intranet, the security policy on the sensitive documents is extremely difficult to enforce and control. The reasons range from the ignorance and carelessness of the recipients to the curiosity of inside hackers.

By attaching permanently a security policy watermark to each sensitive document, we can use watermark agents to monitor and trace a document and to enforce the security policy. For example, a security policy watermark can represent level of confidentiality, scope of distribution, and time of availability. To enable such an environment, a trusted entity in an organization needs to enforce the acceptance of the watermark agent on each host on the organization's network.

Protection of Organization from Unauthorized Use of Copyrighted Documents

Nowadays, employees often carelessly download audio, video, and images from the web for both personal as well as corporate use. Rather than attempting to monitor organization's sensitive information, the goal of this scenario is to protect a decent organization from illegal use of copyrighted information.

In the following sections, our discussion will be limited to the first and second scenarios.

3. System Architecture

A digital watermark agent system is a distributed computing environment on a large computer network which supports the dispatch and execution of a digital watermark agent. As shown in Figure 1, it consists of a central digital watermark agency, agent servers on the remote hosts, and digital watermark agents. For simplicity, a digital watermark agent is hereafter referred to as an agent, and a digital watermark agency as an agency.

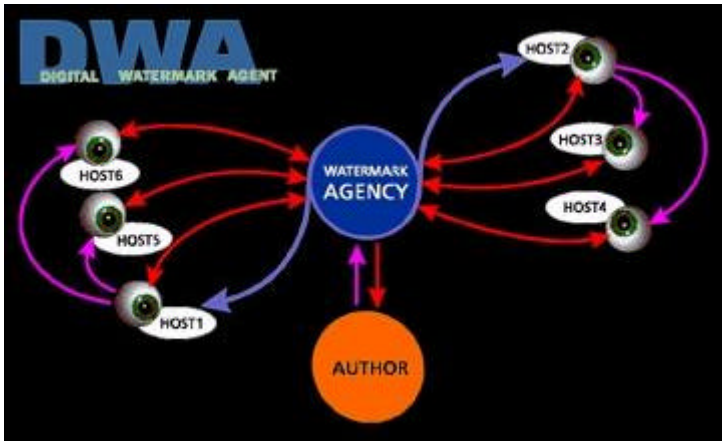

Figure 1. System Overview

The general scenario of the digital watermark agent system is illustrated in Figure 1. After receiving a contract from a content author who wants to protect his/her content, the watermark

agency dispatches a watermark agent to remote hosts. The agent first detects watermarks from the document files which the author intends to protect. If a watermark is found and the security or copyright policy encoded in this watermark does not match the present circumstance or contractual agreement, the watermark agent takes appropriate action specified by the agency, such as sending e-mails, issuing warnings, or even destroying the documents if the agent has been authorized to do so. Afterwards, it reports back to the watermark agency and continues its mission by cloning itself and traveling to other hosts. In Figure 1, the single arrow lines represent the migrations of mobile agents, while the double arrow lines indicate message exchanges, including the reports from the agents to the agency.

Digital Watermark Agency

A digital watermark agency dispatches agents, collects and processes information reported from agents. To guide an agent's navigation and traveling, the digital watermark agency analyzes watermark reports and incrementally builds up a centralized knowledge base.

In detail, the watermark agency has the following functions:

- Preparing and specifying an agent's parameter package, called *suitcase*, which contains the objective, termination condition, action policies of an agent, and secret watermark keys.
- Dispatching agents to remote hosts.
- Collecting and processing reports from agents.
- Guiding agents' travel by providing agents with updated information.

Two types of termination conditions can be specified by the agency before the dispatch. An agent can terminate itself based on the time deadline or the number of clone generations set by the agency. For example, an agency can specify that an agent and all its clones must terminate within one week after dispatch, or a 10th generation agent will stop migration if the maximum clone generation specified by the agency is 10. In addition, the agency can terminate any dispatched agent at anytime by issuing a command. This can be done by a double click on the agent icon on the agency's GUI monitoring area.

Digital Watermark Agent Server

The remote agent server provides an environment and services for the execution of an agent. An agent server also provides agent transportation service so that an agent can send its clones to other hosts for continuos execution. The third function component is a security manager for the authentication between the agency and the host and for access control of resources on the host. Compared to other agent systems, such as the IBM aglets [Lange & Oshima 1998] or Mitsubishi Concordia [Wong et al. 1997], our agent server is very compact yet application-independent.

Each agent server offers a profile for mobile agents. This profile describes the resources which are available on the current host. Each item in the profile represents a resource which consists of resource symbolic name, resource type (e.g., data or program), and resource location in the local file system. Typical resources for watermark agents include the directory of the web site root on the host, the operating system type of the host, the name of the web server log file, and the cache location for mobile agents.

Digital Watermark Agent

In order to keep the agent server application-independent, we have encapsulated all semantic parts into the watermark agent. The workflow of an agent consists of the following steps as shown in Figure 2:

- Traversing a remote host's local file system.
- Filtering the files to be checked.
- Retrieving watermarks from the selected documents (images or video), if any.
- Detecting information about the present circumstance (e.g., IP domain address, present time).
- Matching the security/copyright policy encoded in the watermark with the present circumstance and the contractual information from the agency.
- Taking action if any mismatch (violation) occurs.
- Determining future destinations for migration.
- Reporting the results to the digital watermark agency.
- Receiving information from the agency to update the suitcase of the agent.
- Duplicating itself and traveling to next destination hosts.

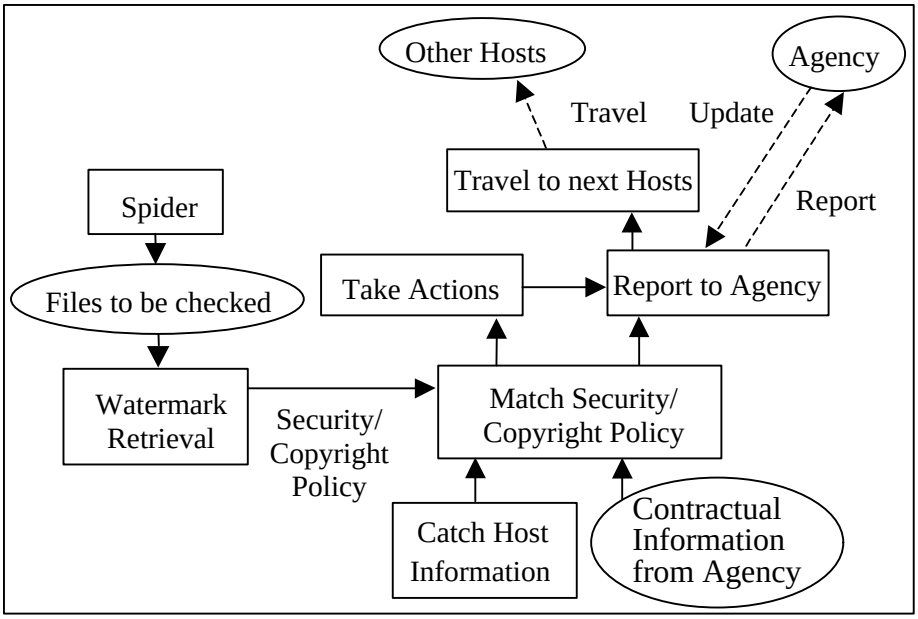

Figure 2. Workflow of Watermark Agent

Types of Watermarks

To support various application scenarios of the watermark agents as discussed in section 2, we have designed three types of watermarks:

- Copyright watermark, which specifies the copyright owner and/or the authorized user. Each document can have two copyright watermarks which identifies ownership and authorized user, respectively.
- Security watermark, which contains encoded security policies, including the place of storage, the time range, and the confidential rank of the document.
- Active watermark, which gives the content owner a control to response to any detected violation of copyright/security policy.

An active watermark is an encoded segment of scripts which is interpretable by the host. Three types of scripts are supported: Java bytecode, UNIX Shell, or DOS command. Active watermark often accompanies with a copyright watermark or a security watermark. For example, a photographer can embed an active watermark which sends an email to him when a watermark agent detects a copyright violation. This active watermark mechanism makes documents become "active".

Dynamic Itineraries

One difference of our watermark agents from others is that there are no predefined itineraries for migration. After an agent completes watermark checking on one host, it needs to make decision by itself on next migration destinations. Presently, the agent uses three sources of information in migration: the web server log files on the current host, the hosts whose violations of copyright/security policy have been detected and recorded in agency's database, and any suspicious sites specified by the agency before dispatch of the agent. The current selection algorithm simply combines these three factors by adding weights. Assume that H is the current host and H' is a potential destination host. The probability (P) to select H' for next host is calculated in the following equation.

$$P(H') = S*W_1 + N*W_2 + V*W_3 + V/T*W_4,$$

where S=1 if H' is a suspicious host specified by the agency, N is the total number of visits to H by H', V is the total number of violations detected on H', T is the total number of visits to H' by the watermark agent ever recorded in the agency's database, and W_1-W_4 are the weights.

Such a dynamic itinerary scheme is subject to deadlock if a clone agent does not know which hosts have been visited by its precedents. We solve the deadlock problem through the coordination of the central agency. An agency records all hosts that have been visited by all cloned agents in a central database. These hosts are removed from the list of the selected hosts for next migrations.

4. Security Features

Security has been recognized as one of the main impediments towards the wide acceptance of mobile agent [Chess et al. 1998, Gong 1997]. Among the three threats, namely, network eavesdroppers, malicious agent, and malicious host, the first two have been concentrated. A new mechanism to detect malicious hosts has been proposed and is under development. The discussion of this mechanism is beyond this paper and will be presented in a separate paper.

Secure transmission

Sensitive data, such as the watermark keys and search reports, may be subject to attack while an agent travels on an insecure network, for instance, the Internet. Therefore, we secure our network transmission of agents using two techniques: the first is to secure all communication channels, including agent dispatching and report collecting, by well-known technologies, such as SSL (Secure Socket Layer). Another technique we applied is to encrypt the sensitive data before network travelling and decrypt it after an agent arrives at an agent server. This way, even the network channel is not secure, the sensitive data is still secured.

Secure invocation

In distributed computing, remote methods to be invoked should be protected in some sense so that only validated parties can invoke it. In our system, some communications between an agent and an agency or server is also secured, for example, only agents with a valid agent identification can insert a report to an agency's database.

Authentication

The agent code and the static data of the agent are signed by the agency who dispatches the agent. When an agent arrives on a host, the host verifies agency's signature. This ensures the authentication and integrity of the agent's behavior.

With the current implementation of security features, the applicable scenarios of the watermark agent are restricted to trusted network environment (e.g., in a military network or a corporate). The example of a watermark agency is the official in a corporation who is responsible for security (facilities, network, documents, etc.).

5. Implementation

To make use of Java's system consistency and network security feature, the watermark agent system has been implemented using Java. The distributed computing environment is built based on Java's RMI (Remote Method Invocation) package. To support peer-to-peer communication, we have enabled both the server and the agency to provide invocation services so that they can conveniently communicate with each other.

An interface has been defined in the watermark agent to the external watermark retrieval library. This interface employs Java's native interface technology to allow Java objects to call watermark retrieval functions written in C. At present, SysCoP [Zhao and Koch 1995] is the only digital watermarking mechanism that has been supported in the watermark agent. However, the watermark agent can easily support any other watermarking system.

The database part at the agency has been implemented based on Java's JDBC (Java Database Connectivity) approach. Since Java provides the built-in bridge between ODBC and JDBC, the physical database can be any relational database which supports ODBC (Open Database Connectivity). In our implementation, we have adopted Microsoft Access database for the simplicity and wide availability.

Java's RMI so far does not support secure transmission. To secure data transmission over a large computer network, such as the Internet, we add an SSL (secure socket layer) layer to replace Java's classical transport layer. Once such a layer is established at the two ends of the communication, all the data in the channel is secured. To further protect an agent's static and dynamic data, we use Java's object serialization mechanism by implementing our own serialization algorithm in the object reading and writing methods based on commercial encryption packages.

Graphical user interfaces (GUI) have been developed to visualize the activities on agency and agent server. The agency's GUI window consists of three areas: the monitoring area to graphically monitor the agent mobility and execution process by animated icons, the message area to show the execution and migration status of mobile agents, and the buttons area. The *dispatch* button activates a window allowing the agent owner to specify agent parameters and dispatch the agent. The *report* button pops up a window for the display of report details and retrieval of reports from the database.

6. Conclusion

This paper presents a complete digital watermark agent system to effectively put the digital watermark technology into practice. This system enables an agency to dispatch digital watermark agents to agent servers and agent can perform various tasks on the server. Once all the actions have been taken, a report will be sent to an agency's database and an agent can continue to travel to another agent server.

Our digital watermark agent system is the first mobile computing approach towards enforcement of digital watermark. Digital watermark agent development is an important step toward technical management of copyrighted and secured documents, it contributes to fundamental knowledge in the areas of digital security, intelligent agent, and collaboration technology.

Several additional components are under development, which are critical towards the success of watermark agents. The first one is a novel approach against malicious host attack, currently we are exploring techniques such as secret sharing, time limited constraints and assertions, Java bytecode obfuscation and watermarking. The second component that we are developing is a data-mining and data-fusion module to intelligently select the next migration hosts based on multiple sources of information such as related business categories and results of web search engines.

References

1. Chess, D., Harrison, C., and Kershenbaum, A. (1997). *Mobile agents: Are they a good idea?* In: Mobile Object Systems: Towards the Programmable Internet, pp. 25-45. Springer-Verlag, 1997. Lecture Notes in Computer Science No. 1222.
2. Chess, D. (1998). *Security Issues in Mobile Code Systems*. In: Mobile Agents and Security. pp. 1-14. Springer-Verlag, Berlin, 1998.
3. Gong, L. (1997). *Surviveable Mobile Code is Hard to Build*. In: Proc. of the DARPA Workshop on Foundations for Secure Mobile Code Workshop, 26 - 28 March 1997.

4. Lange, D.; Oshima, M. (1998). *Programming and Deploying Java Mobile Agents with Aglets*. Addison-Wesley, 1998. See also IBM Aglets web site at http://www.trl.ibm.co.jp/aglets.
5. Memon, N. and Wong, P. (1998). *Protecting Digital Media Content*. In: Communications of ACM, pp. 35-43, Vol. 41, No. 7, July 1998.
6. Wong, D., Paciorek, N., Walsh, T., DiCelie, J., Young, M., Peet, B. (1997). *Concordia: An Infrastructure for Collaborating Mobile Agents*. In First International Workshop on Mobile Agents, Lecture Notes in Computer Science, Vol. 1219, Springer-Verlag, Berlin, Germany, 1997. Also see Concordia web site at http://www.meitca.com/HSL/Projects/Concordia.
7. Zhao, J. and Koch, E. (1995). *Embedding Robust Labels Into Images For Copyright Protection*. In: Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge and New Technologies, Vienna, Austria, August 21-25, 1995.
8. Zhao, J., Koch, E. and Luo, C. (1998). *Digital Watermarking In Business Today and Tomorrow*. In: Communications of ACM, pp. 67-72, Vol. 41, No. 7, July 1998.

Dr. Jian Zhao

Dr. Jian Zhao is Director for Digital Security Technology and a Senior Scientist at Fraunhofer Center for Research in Computer Graphics, Inc. He is also a co-founder of MediaSec Technologies LLC. He has more than 12 years experiences in software research and development. Prior to joining Fraunhofer-CRCG and founding MediaSec, he held research, system analysis and design, software development, and project coordination positions at the Fraunhofer Institute for Computer Graphics and at the German National Research Center for Information Technology, Darmstadt, Germany.

He is one of the inventors and the principal developer of SysCoP, a digital watermarking system. He had been involved in projects in the fields of concurrency control and recovery in distributed database systems, Management Information Systems, User Interface Management Systems, construction tools for database interfaces, computer-mediated and -supported classroom, cooperative user interfaces, and face and voice recognition.

Dr. Zhao is the project manager of Digital Watermark Agents project funded by the US Army Research Laboratory (ARL) and Defense Advanced Research Projects Agency (DARPA) at Fraunhofer-CRCG. He also coordinated and participated several European projects in digital copyright management and protection such as TALISMAN and OCTALIS.

He received his Ph.D. in Computer Science from the Technical University Darmstadt, Germany, his M.Sc. in Computer Science from the East China Normal University, Shanghai, China, and his B.Sc. in Computer Science from Hefei University of Technology, Hefei, China.

Dr. Zhao published about 25 papers and is a member of ACM - the Association for Computing Machinery and the IEEE Computer Society.