Pakistan Journal of Information and Technology 2(1): 30-34, 2003

Towards Developing Watermarking Standards for Collaborative eLearning Systems

Jinan A.W. Fiaidhi and Sabah M.A. Mohammed
Department of Computer Science, Lakehead University, 955 Oliver Road
Thunder Bay, Ontario P7B 5E1, Canada

Abstract: There's a lot of talk in e-learning circles these days about the arrival of the "second wave". The marketplace is shifting in maturity. The second wave signals the arrival of greater standardization and the emergence of replicable processes. This paper proposes a watermarking standards for collaborative eLearning systems within a university teaching environments.

Key Words: Watermarking, Collaborative eLearning Systems

Introduction

Collaboration is a concept that makes sense from virtually any perspective - business,, education, technology and personal life. Businesses have been experimenting with enlarging the network of collaboration to include vendor and even competitors - harnessing shared experiences and processes to improve efficiency and quality. Within education, collaboration is critical. Online, many students lack the contact of a face-to-face classroom. Activities that require collaborative work can put students in touch with each other, eliminating the sense of isolation that is common for elearners. At it's simplest level, collaboration may be simply sharing information with another person, department, or organization...at it's most advanced level, collaboration involves unifying communication processes and content and establishing forums for accessing resources and building content and value together.

At the age of the internet knowledge is expanding at lightening speed. Students need to learn more, better and faster. "eLearing" technology is a new internet-based educational system that can empower both students and teachers to improve active participation and achieve faster and effective learning. Certainly, eLearning systems are not dedicated only for virtual institutions, but they are used also within many On-Campus traditional educational institutions. There are many situations that require an On-Campus eLearning system (Fiaidhi Mohammed and AlKhanjari 2001). For example, when teachers are faced with very large classes with little or no support, then teachers are not always able to provide all students with the help that they need. One way of decreasing the load on teachers is for students to help each other. Unfortunately, in a large class or students may not know who to ask. Another example an On-Campus eLearning system can act as an Advisory or as a Teaching Assistant Agent helping in correcting assignments, helping students to dig through the information fog, or as tool aiding to monitor student progress and detect plagiarism cases, thus helping to produce more qualified graduates. Today, the amount of knowledge that students need to master has increased exponentially. They need help. Missing a few basic concepts can result in a very frustrating learning experience. Moreover, tutors need better automated tools that help them deliver their courses/tutorials, schedule assignments submission, automatically correct assignments and monitor student progress. Thus there is an obvious need for On-Campus learning systems.

Hence eLearning moves the learning experience out of the traditional classroom and into your world. It's learning anytime, anywhere ... without geographical or scheduling barriers. It's learning that relies on the Internet for accessing learning materials and interacting with experts and fellow learners. It facilitate:

- Taking courses in the comfort of your home, workplace or when traveling.
- Receiving a quality education without giving up quality time.
- Learning when and where it is convenient for you.
- Learn from experts practicing in their fields.
- Learning collaboratively with other learners.

With good design and delivery, eLearning does all these things. Unfortunately, universities and colleges across the world have jumped on the eLearning bandwagon because it is a new paradigm and to let students too far from campus to reap the benefits of a university education and potentially increase their future opportunities and all they need is a computer, an Internet account, tuition and a book budget to start their distance/Off-Campus learning.

However, The World Wide Web is, in many respects, a world without barriers. Its openness is highly appealing, if not downright noble. Unfortunately, unscrupulous people can take advantage of this electronic latitude to unlawfully take what is not theirs. On the web, hard-won Intellectual Property (IP) becomes a pirate's booty for hackers and less-than-ethical businesses. Efforts aimed at protecting IP are limited to pop-up windows and gateways that show lengthy legal documents establishing ownership of digital files and prove to be very expensive. The lack of online security for IP has many of the world's consumer electronics, computer and entertainment companies nervous. To this end, a digital watermarking has been proposed as a last line of defence. As with the internet itself, digital watermarking is a new technology that is still finding its legs not only for IP protection but as a mechanism for internet security as whole. Indeed, a university environment is an extremely complex one and planning an effective e-infrastructure represents particular challenges in such an environment (Colace, 2001). This article attempts to address the issue of developing standard watermarking (text, images and videos) primitives for a collaborative eLearning system within a university environment.

Table 1: Differences between Collaborative eLearing and WBT

WBT	Collaborative eLearning Systems
It has the advantage of being anytime, anyplace for individual learners.	It requires learners to complete assignments by specific deadlines, rather than simultaneously.
There's no collaboration among students.	Collaboration, voting, and outcomes are determined soley by students.
SME-centered; authority for learning is not transferred.	Learner-centered. Learners understand that it is up to them to learn, not the teacher to teach.
The instructor (or subject matter expert) is the center of knowledge and learning.	The learner group connected via the Internet is the center of knowledge and learning.
Students are directed by an instructor or software to answer predetermined questions.	Learners are empowered by source knowledge to formulate and answer questions.
The authority figure is the subject matter expert and the associated content.	Authority transfers from the subject matter expert to the students.
Content is transmitted to students.	A transaction occurs between learners to determine content relevance and application.

Collaborative eLearning Versus Web Based Training: Before we address the issue of establishing a proper infrastructure for collaborative eLearning systems, we would like to shade the light on its differences with the Web Based Training Systems. Simple one can highlight one main difference, that collaborative learning represents a transfer of authority for learning from instructors to learners connected via the Internet. Table 1 illustrates other differences (Horn, 2000):

For the collaborative eLearing environment, the role of the instructor/facilitator is straightforward. Such role may include the following tasks:

- sets up the assignments for the team and follows up with indiviudal learners
- controls the collaborative process if questions or issues arise (e.g. via email)
- guides the authoring process (e.g via email)
- determines the roles and privileges of participants.

Standardization Effects on International Education: Dr. Kathern Barker (2001) president of Future Education indicated by her recent report the massive potential of Information and Communication Technology for post secondary education. She indicated that there is a growing international competition for eStudents. Moreover, Dr. Julie Kaufman (2002) at her resent seminar on the State of the eLearning Industry said "although 48% of Post-Secondary Institutions utilizes eLearning solutions, the eLearning infrastructure suffers from fragmentation and requires growing efforts of consolidation and standardisation."

In upstart industries such as elearning, big ideas, experimentation, trial-and-error, excitement, creativity and sometimes disappointment and frustration characterize the first wave of growth. It's all about trying to figure out what works and works best. As we've seen during the past two years, some ideas never succeed--regardless of how much time and money are invested. Bad ideas usually fail. Good ideas gain momentum and support, followers and advocates. From a macro perspective, the culmination of enough good ideas will ultimately reach critical mass and the second wave is beginning to rise.

The second wave signals the arrival of greater standardization and the emergence of replicable processes. More and more people are adopting the good ideas and building on them. However, standardization of eLearning systems has many issues and central to all is the security infrastructure of such systems. eLearning systems utilize the internet which is an open media of communication and collaboration and present difficulties with respect to security. One solution is to use hardwired firewalls to ensure the security aspects. This solution is rather expensive and impractical with such a large mesh of communication between eLearning systems and users. With software solutions we are faced with two technologies: Cryptography and Watermarking. Cryptography is an old technology which can only protect the distribution of content and once a customer decrypts it, all protection is Lost. Such security technologies do not provide persistent security and are open to loss of income and intellectual property poaching (Wayner, 2002).

Watermarking, on the other hand, is a relatively new technology which can compliment cryptography, providing protection after decryption, even when the content has entered the analog world. Watermarking involves embedding data, often imperceptibly, into a data medium or multimedia object to enhance or protect its value. While the watermarking field is relatively new, many applications that could benefit from watermarking have been proposed. The recent work of Mintzer *et al.,* (1997) at the IBM Thomas Watsom Research Centre identified three clusters of applications with similar technical requirements: One uses watermarking to convey ownership information; another uses watermarking to verify that the object content has not changed; and the third, called collaborative watermarking, conveys object-specific information to a community of recipients. According to Mintzer *et al.,* (1998) ACM Invited Paper, the three main emerging classes of applications lack standard marks, standard ways of interacting with systems, benchmarks tests and even a standard terminology, thus presenting opportunities for developing application specific watermarking techniques. This proposal aims at developing collaborative watermarking techniques for collaborative eLearning systems.

Proposing a Watermarking Standards for Collaborative eLearning Systems: Though digital watermarking of various types has been around since at least the early 1990's, the remaining open questions seem to be in a continuous-growth mode. Different Watermarks are not alike. Different techniques are used to embed different types of watermarks into digital media objects to accomplish different goals. In

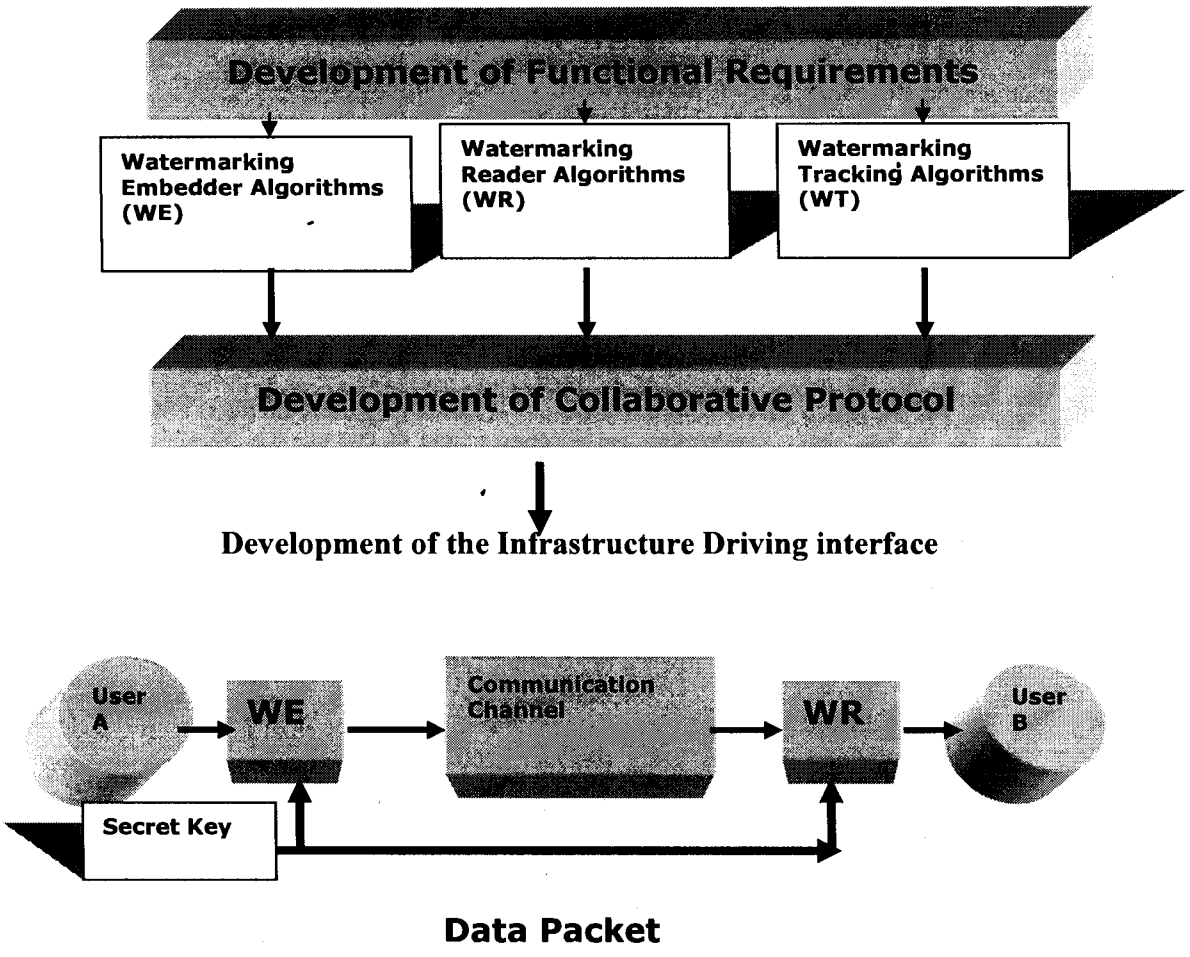

Fig.1: Watermarking Standards Hierarchies for a Collaborative eLearning Systems

this article, we are proposing a methodology for standardising collaborative watermarking for the collaborative eLearning environment. Such methodology will enable the eLearning system to employ multiple watermarks to convey multiple sets of information, intended to satisfy differing or similar goals.

The proposed methodology is illustrated in Fig. 1. The first level addresses the issue of functional requirements of Collaborative Watermarking. Generally, a watermark must convey as much information as possible. This implies that the watermark data rate should be high. A watermark should be a secret and be accessible to authorized parties only. This is can be achieved by the use of cryptographic keys. A watermark is an integral part of the data. It must persist even after signal processing and data manipulation. This also includes malicious manipulation that attempts to remove the watermark. This requirement is known as 'robustness requirement'. A watermark though being irremovable should also be imperceptible. It should not modify or alter the quality of the content. Normally, the degradation in quality is well below one percent. Watermark recovery process may not be allowed to use the original contents of the digital watermark. Most specifically for a collaborative environment, we need to embed several watermarks into the same digital object. Among such watermarks are ownership watermark, content integrity watermark and object-description (caption) watermark. The order of embedding these watermarks should not affect the robustness and fragileness of these watermarks. One safe order (Mintzer, 1997) is to embed the most robust ownership watermark first followed by moderately robust captioning watermark and to embed the most fragile content verification last. The issue of effective watermarking algorithms can be determined from performing an intensive survey of the most recent algorithms and technologies (Yeung, 1998; Cox and Miller, 2002).

In the *second level*, the methodology proposes to construct three generic watermarking utilities(e.g Browser plug-in (Jenkin and Dymond, 1997)) which can manipulates watermarks from within popular document producing applications (e.g. MS Word, Notepad, Adobe, Corel, JBuilder). The *Watermark Embedders* - This software automatically adds the watermark to the digital object (May use Wavelets with appropriate parameters (Dietz and Jassim, 2002)), the *Watermark Readers* - To read and identify an embedded water mark, and the *Watermark Tracking* - This is software assists authorities in searching for watermarks in a particular server domain or in cyberspace. It should utilize the spider technology to search the Web for your water marked objects and report the findings back to you, so that you may take action against any inappropriate usage of your data. Such software is quite important for detecting plagiarism cases which is a major issue in any teaching environment (Fiaidhi and Robinson, 1987). For Java programs watermarking we may need an obfuscating software.

In the *third level* a protocol for collaborative watermarking is proposed. Since every eLearning system utilises the TCP/IP protocol on the internet/intranet/extranet network, then we can think of modifying that protocol to convey watermarks. Handel and Sandford (1996) and Wolf (1989) found that the reserved or unused fields in the packet headers can be used for information hiding. It is the basic layered design principle of the TCP/IP (OSI) network where the IP datagram encapsulate information received from the transport layer. In particular the IP header encapsulates ICMP messages and IGMP report and query messages. Covert channels in the Ipv4 header can, therefore also, be associated with those in the TCP, ICMP or IGMP headers. The Ipv4 header contains fragmentation information especially in the flag field (First bit is reserved, second bit DF (do not fragment and the third bit MF(more fragments)). So in an unfragmented datagram, we can have 13 bit to hide information such as a watermark. Such redundancy provide us with a new venue to develop ICP/IP watermarks and to develop packet filters which can be used by the routers to reinforce its filtering policy.

The *fourth level* represents the driving infrastructure interface. An object content owner approaches a neutral registration authority of the eLearning system. Depending on the nature of object content, the authority allots a unique registration number. It also archives content and the unique registration number for future reference. A content owner generates a suitable watermark using primitives generated in level 2 and using a watermarking algorithm to embed it within the data. Such a watermark should be unobtrusive and secure. To ensure security of embedded digital watermarks, one or several secret and crypto logically secure keys can be used. To ensure robustness against data manipulation and processing, it is helpful to have very small digital watermarks and ensure that they are redundantly distributed in the host data. The digital watermark, public/private key and host data is processed using a watermarking algorithm to generate the watermarked data. To extract (detect) the watermark, the authorized agency requires watermark readers and a secure/public key. All these inputs are processed by the watermark recovery program to extract the watermark or confidence measure. The confidence measure indicates the degree of closeness of the original watermark and recovered watermark. The driving interface can deploy spread-spectrum communication (Viterbi, 1995) using the redundancy bits of the Ipv4 protocol. In such a scheme a watermark is embedded by adding pseudonoise (PN) signal. This PN signal functions as a secret key. This specific PN signal can later on be detected by a correlation receiver or matched filter. The probability of false-positive or false-negative detection can be made low by appropriate amplitude and the number of added samples. It is also possible to subtract the PN signal from the host data. In this case, the correlation receiver will calculate a high-negative correlation in the detection process. Thus, by using an addition or subtraction process it is possible to convey one-bit of information. By the sequential adding of several such bits, it is possible to convey arbitrary information through the internet communication channels.

Conclusion

For compelling evidence of the arrival of e-learning's second wave, look first at the evolution of the standards movement. This article presented a methodology based on watermarking for establishing a standard infrastructure for collaborative eLearning systems. The methodology consists of four levels: Developing Functional Requirements, Constructing Watermarking Utilities, Developing a Collaborative Web-Based Protocol and Developing Collaborative Interfaces.

References

Barker, K., 2001. Status of ICT in International Education in Canada's Post-Secondary Education System, CBIE. (available http://www.cbie.ca/download/ict/Phase%201%20Lit%20Review.pdf)

Colace, F., 2002. Models for eLearning environment evaluation, SSGRR'2002 Int. Conference, Italy.

Cox, I. and M. Miller, 2002. The first 50 years of watermarking, J.Applied Signal Processing, Vol. 2.

Dietze, M. and S. Jassim, 2002. The Choice of Filter Banks for Wavelet-Based Robust Watermarking, ACM Multimedia Workshop,NY.

Fiaidhi, J. and S. Robinson, 1987. Similarity analysis and Plagiarism detection in a Univ. teaching environment, Int. J. Computer and Education, Vol. 11, No. 1.

Fiaidhi, J., S. Mohammed and Z. ALKhanjari, 2001. Designing an On-Campus Learning Portal, J. of Sci. and Technology, Vol 6, No.1.

Horn, R., 2000. The Network is the Teacher: Collaborative eLearning, Learning Circuits J., (available at http://www.learningcircuits.org/2002/june2000

Handel, M. and D. Stanford, 1996. Hiding data in the OSI network, 1st Int. Workshop on Information Hiding, Cambridge,UK, May-June 96.

Jenkin, M. and P. Dymond, 1997. A Plugin-Based Privacy Scheme for WWW file distribution, HICCS'97.

Kaufman, J., 2002. The state of eLearning industry in Canada, Online Education 2002 (available at www.online.nf.ca/final/julie.kaufman.pdf

Mintzer, F., 1997. Safeguarding digital library, DLIB Mag. (www.dlib.org/dlib/december97/ibm/12lotspiech.html)

Mintzer, F., 1998. Opportunities for watermarking Standards, CACM, Vol 41, No. 7.

Mintzer, F. *et al.*, 1997. Effective and Ineffective Image Watermarks, IEEE 1997 In. Conf. On Image Processing, Vol. III, paces 9-12.

Wayner, P., 2002. Disappearing Cryptography, 2nd Edition, Morgan Kaufman.

Wolf, G., 1989. Covert channels in LAN protocols, Proceedings of the Workshop on Local Area Network Security (LANSEC'89),91-102,1989.

Viterbi, A., 1995. CDMA: Principles of Spread-Spectrum Communications, Addison- Wesley.

Yeung, M., 1998. Digital Watermarking, CACM, Vol 41, No. 7, 31-33.