Constructing a Wrapper-based DRM System for Digital Content Protection in Digital Libraries

Jen-Hao Hsiao[1,2], Jenq-Haur Wang[1],

Ming-Syan Chen[2], Chu-Song Chen[1], Lee-Feng Chien[1]

[1] Institute of Information Science, Academia Sinica, Taiwan,
{jenhao, jhwang, song, lfchien}@iis.sinica.edu.tw
[2] Department of Electrical Engineering, Nation Taiwan University, Taiwan
mschen@cc.ee.ntu.edu.tw

Abstract. Conventional digital libraries utilize access control and digital watermarking techniques to protect their digital content. These methods, however, have drawbacks. First, after passing the identity authentication process, authorized users can easily redistribute the digital assets. Second, it is impractical to expect a digital watermarking scheme to prevent all kinds of attack. Thus, how to enforce property rights after digital content has been released to authorized users is a crucial and challenging issue. In this paper, we propose a wrapper-based approach to digital content protection that integrates digital watermarking, cryptography, information protection technology, and a rights model. In this rights enforcement environment, the behavior of all content players is monitored and digital content can only be accessed after certain usage rules have been satisfied. Furthermore, the proposed architecture can be easily integrated into any digital content player, or even existing DRM systems in digital libraries. With the protection of the proposed DRM system, the abuse of digital content can be drastically reduced.

Keywords. Digital rights management, digital watermark, content protection, intellectual property, access control

1 Introduction

With rapid development of the Internet and computer technology, digital content, including digital images, video, and music, can be distributed instantaneously across the Internet. However, digital content in digital world differs from objects in real world, since it can be easily copied, altered, and distributed to a large number of recipients. This almost certainly causes copyright infringement and revenue losses to content owners. The National Digital Archives Program (NDAP) in Taiwan has amassed a rich collection of cultural and historical artifacts. These assets have been digitized to enhance their preservation, and make them more accessible to users. The metadata and digital content storage systems are called archival systems, and – like other types of

digital content – they too face the problem of piracy. Thus, content holders are sometimes unwilling to release digital content, because their intellectual property rights could be infringed. To protect high-value digital content and avoid digital piracy, we need a system that prevents unauthorized access and manages content usage rights.

In this paper, we propose a wrapper-based DRM system that enhances the protection of digital content and drastically reduces piracy. The remainder of the paper is organized as follows. In the next section, some previous works are discussed. The architecture of proposed DRM system is described in Section 3. We then present a brief discussion in Section 4, followed by our conclusions in Section 5.

2 Related Work

To prevent the abuse of digital content, most digital libraries and museums adopt digital watermarking [8] techniques to guard their digital images. Though useful, watermark-based image protection systems are still not robust enough to resist a variety of image attacks. Digital Rights Management (DRM) is a protocol of hardware and software services and technologies governing the authorized use of digital content and managing any consequences of that use throughout the entire life-cycle of the content (as defined by IDC). DRM is a new concept that can be used to protect high-value digital assets and control their distribution and usage. The design of a DRM system must address the following key issues: (1) a digital rights enforcement (DRE) environment, (2) digital rights, and (3) standardization for interoperability. In [9], the author proposed a typical DRM system architecture, including several essential components. Then, in 2004, Pramod et al. [7] proposed that DRM should be adopted as a layered framework, whereby various services are offered to users of the digital content at each layer. In addition, Bogdan et al.[1] proposed a security architecture that enables digital rights management of home networks. The concept of an "authorized domain" is used to authenticate compliant devices, instead of relying on expensive public key cryptographic operations. Although the above works suggest novel architectures for a DRM system, they do not fully address the three issues mentioned earlier. For example, in the area of rights enforcement, authorized users could still distribute digital assets easily after they pass the identity authentication process. To overcome this problem, Nicolakis et al. [6] developed a DRM system called MediaRights that protects digital images. However, although this kind of architecture solves the rights management problem, a customized image viewer is not convenient for users. Furthermore, the circulation of digital assets is seriously impaired. Hence, how to enforce the usage rules and protect content owners' property rights after images have been released are the major challenges in DRM research. Several commercial DRM solutions, such as InterTrust, Alpha-Tec, Digimarc, and LTU, are available. But the requirements of digital libraries vary enormously and differ from those of industry. It is very unlikely that existing commercial systems can meet the demands of digital libraries. Building a DRM system for digital libraries based on existing commercial solutions without any modification is therefore impractical.

3 A Wrapper-based DRM System

Multimedia Center (MMC) [2], the core of the archival systems in NDAP, provides an integrated tool that helps content managers store and manage multimedia files efficiently. It also enables users to access digital content in a convenient manner. To protect digital images in MMC, we use the proposed DRM techniques to attach specific restriction on the use of digital content, which effectively reduces illegal copying. The security in MMC could be improved substantially to protect precious digital assets from illegal use.

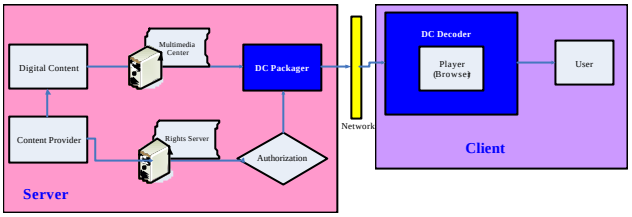

Figure 1. Overview of the Wrapper-based DRM System

3.1 System Architecture

The majority of multimedia files in MMC are digital images, classified as low, middle, and high-resolution images. Figure 1 gives an overview of the wrapper-based DRM system, which consists of two building blocks: the server side preprocessing module and the client side protection module. To facilitate player-independent encapsulation of rights and encryption information, we propose the following wrapper-based approach.

3.2 Rights Model

There are several existing rights models and rights expression languages (RELs), such as XrML and ODRL. XrML is a general purpose REL with good expressive power. For content protection in digital libraries, it is only necessary to consider the following restrictions: play/view, print, save, valid date, and compliant player. A user can only play, print, or save digital images when he authorized to do so. The valid date limits the time that digital images are accessible, while the compliant player ensures that digital images can only be accessed by specific machines.

3.3 DC Packager

The DC Packager envelops digital images in a protected file. An invisible digital watermark representing the copyright of NDAP is then embedded into images prior to release. The usage rules derived from the rights server are then combined with the watermarked image to form a new content package, which is then encrypted for security. The resulting file is called a “protected digital content” file, meaning that the digital image is ready for distribution, and that the usage rules can be enforced with certainty.

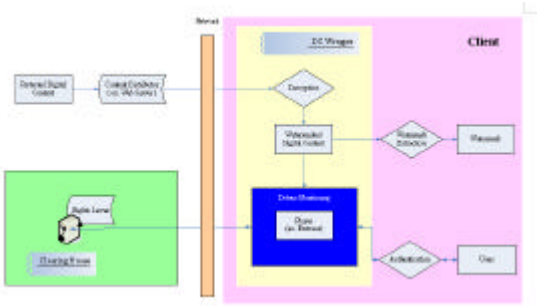

Figure 2. An operational view of the DC Wrapper

3.4 DC Wrapper

DC Wrapper enforces the rules related to the use of digital images. As shown in Figure 2, after a user downloads a protected file from the network and views it on a player (e.g., a browser), DC Wrapper launches automatically and monitors the user's behavior. Furthermore, the digital images are released with specific restrictions on their usage. If these rules are violated, or a user refuses to view images under monitoring by DC Wrapper, the content is rendered unavailable. DC Wrapper is implemented with a binary instrumentation technique called a Detours tool [3][4], which intercepts OS functions by re-writing target function images. Note that the wrapper-based design allows more flexibility in the choice of an underlying content player that is independent of the DRM modules. DC Wrapper's mechanisms decode encrypted digital content based on predefined rules, and transform the content into a readable format for the content player. Note that DC Wrapper monitors the behavior of the player rather than acting as a multimedia player itself. Hence, there is no need to use a customized player to play digital content. The rights information provided by the rights server is employed by DC Wrapper to determine the kind of access a user is allowed to have.

4 Discussions

Our proposed architecture has three major advantages. First, the wrapper-based approach can be a stand-alone system, or it can be integrated into existing content players, even commercial DRM systems. Second, the difficult problem of enforcing usage rules when digital content is playing is addressed by DC Wrapper. It monitors the behavior of the content player, and prevents illegal access to digital content. Third, the proposed architecture enables two or more intellectual property rights protection systems to cooperate and complement each other.

Since the DC Wrapper is implemented using a binary interceptor approach, it is kind of OS dependent. This is a trade-off between better control and platform independence when considering the integration with various existing DRM systems. After all, intercepting the message in the OS level is more robust and compatible than in the unstandardized application level. Just like any other system security tools, there is no 100% secure DRM system which can always survive all kinds of attacks. For example,

a malicious media player could possibly bypass all the usage rules. However, the development of such a malicious player is so complicated and time-consuming that is not technically feasible for an average user. It is also what we try to do to raise the barrier for the abuse of digital content.

5 Conclusions

The distribution of digital content requires content protection and rights management in order to engender trust between the parties involved. Trusted computing platforms and the integration of DRM components into the digital libraries would probably encourage content providers to release precious digital assets. In this paper, we have proposed a novel rights enforcement environment that provides stronger protection for digital images, and thereby drastically reduces the piracy of digital content.

6 Acknowledgements

This work was partially supported by the following grants: NSC 94-2422-H-001-006, 94-2422-H-001-007, and 94-2422-H-001-008. The authors would like to thank Dr. L. F. Chien and various professional parties in NDAP Research & Development of Technology Division for their contributions to this paper.

References

1. Bogdan C. Popescu, Frank L.A.J. Kamperman, "A DRM security architecture for home networks", Proceedings of the 4th ACM workshop on Digital rights management, 2004. pp 1 –10
2. Chen, Hsin Yu, Ho, Jan-Ming, "Multimedia Center: A Novel Multimedia File Management System in NDAP", The Second Workshop on Digital Archives Technologies, 22-23 July 2002. Pages:89-96
3. G. Hunt and D. Brubacher. "Detours: Binary interception of win32 functions". Proceedings of the 3rd USENIX Windows NT Symposium, July 1999 , pages 135-143
4. Lin, Tzung-Bo, Huang, Shih-Kun, "OpenDReaMS: A Generic DRM Wrapper for COTS Readers, The Third Workshop on Digital Archives Technologies", 5-6 Aug 2004, Pages: 289-295
5. Liu, Qiong; Reihaneh, Safavi-Naini; Sheppard, Nicholas Paul, "Digital rights management for content distribution", Proceedings of the Australasian information security workshop conference on ACSW frontiers 2003
6. Nicolakis, Theo; Pizano, Carlos E.; Prumo, Bianca; Webb, Mitchell, "Protecting Digital Archives at the Greek Orthodox Archdiocese of America", Proceedings of the 2003 ACM workshop on Digital rights management, October 2003
7. Pramod A. Jamkhedkar, Gregory L. Heileman, "DRM as a layered system", Proceedings of the 4th ACM workshop on Digital rights management, 2004, Pages: 11 - 21.
8. Serrao, C. Marques, J., "DIGIPIPE - a pipeline methodology for digital image production and protection", 4th EURASIP-IEEE Region 8 International Symposium on VIPromCom, 16-19 June 2002
9. Susanne Guth, A Sample DRM System, Lecture Notes in Computer Science, Volume 2770, November 2003, pp. 150 - 161