International Journal of Information Movement *Vol.I Issue XI* *(March 2017)*
Website: www.ijim.in *ISSN: 2456-0553 (online)* **Pages 11-17**

COPYRIGHT PROTECTION OF SCHOLARLY CONTENT IN THE DIGITAL ENVIRONMENT: POSSIBLE TECHNOLOGICAL MEASURES

Mani Bhusan Roy,
Ex-student of Department of Library and Information Science
North Bengal University
Email - **manibhusanroy84@gmail.com**

Abstract: The spreading of internet and web technologies changed the way of information communication and the mode of information access. Digital content is still valuable and it should be protected. The protection of copyright or intellectual right of digital content is concerned to be one of the big problems of the digital environment. The content providers are investing to new ways of making profits and offering new services concerning digital products. Thus, how to enforce property rights after digital content has been released to authorized users is a crucial and challenging issue. Digital copyright protecting/Digital right management systems have been proposed to address this issue by enforcing the rights access policies in a trusted computing environment. However, DRM systems can only be useful if the computing environment can be protected and compliant to the common rights policy throughout the lifecycle of digital objects. This paper presents a technical overview of the capabilities and characteristics of technologies proposed for use as a means of providing copyright protection for digital Scholarly content.

Keywords: Content Protection, Digital Rights Management, digital signature, digital watermarking, Encryption.

1.0 Introduction

With rapid development of the web technology, computer technology and 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 could cause copyright infringement and revenue losses to content owners. Thus, protection of the copyrights and revenues of content owners has become increasingly important in the present day. To protect high-value digital content and avoid digital piracy, we need a system that prevents unauthorized access and manages content usage rights. For digital content protection, a number of approaches have been proposed. Basic cryptographic schemes are commonly used to encrypt sensitive content. Access control mechanisms are widely deployed to block unauthorized access in archival systems. However, these only address part of the issues. The security of encrypted content depends on the strength of encryption scheme and the privacy of encryption keys. The content would still be redistributed after it's decrypted. Access control schemes could become useless if the system accounts were hacked. Digital watermarking is the most widely used technique in content protection.

2.0 What is Digital Rights Management (DRM)?

Digital Rights Management is a collective name for technologies or a range of techniques that prevent one from using a copyrighted digital work beyond the degree to which the copyright owner (or a publisher who may not actually hold a copyright) wishes to allow one to use it. It is actually a range of techniques that use information about rights and rights holders to manage copyright material and the terms and conditions on which it is made available to users.
In terms that are more formal DRM has been described as 'a way of addressing the description, identification, trading, protection, monitoring and tracking of all forms of rights usages over tangible and intangible assets, including management of rights holders' relationships.

Two possible interpretations of the term digital rights management are:

Management of digital rights: The responsibility of expressing and managing the rights to content in electronic or digital form, as a corollary to content in print.
Digital management of rights: The ability to physically manage intellectual property and proprietary rights in content by way of an electronic system or process associated with copyright management systems.
Digital refers not to rights in information but to the medium in which the information is expressed. The rights one is managing are not digital. It is the content of the work that is in digital form.
Digital Rights Management systems can be used to protect high-value digital assets and control their distribution and usage. A DRM system offers a persistent content protection against unauthorized access to the digital content, limiting access to only those with the proper authorization. It should be flexible to manage usage rights for different kinds of digital content (e.g. music files, video streams, digital books, images) across different platforms (e.g. PCs, laptops, I pad, Tablet, PDAs, mobile phones) and control access to content delivered on physical media or any other distribution method (e.g., CD-ROMs, DVDs, flash memory).

3.0 DRM for Various People

3.1 Creators

A major challenge faced by creators such as writers, illustrators, designers, and animators, is how to keep track of work in the digital environment. Adopting some form of DRM can help them to manage the material online to ensure that their work is protected and that its commercial use is paid for. As individual creators, DRM offers a way of making works commercially available in a relatively safe and protected environment. Done well it should allow creators to reach more potential customers than through normal distribution channels.

As part of a DRM system, creators can:

a) Make their works available on selected terms and conditions
b) Access other works available for use and re-use
c) Make all or part of work/s available on a fee or free basis
d) Make use of whatever technological protection is offered by the system.

- **Publishers**

When publishers prepare content for delivery to customers they may choose to manage the content in a protected format aimed at preventing unauthorised copying. This may be in the form of watermarking, encryption, or password access. They may also contract with users to provide access to the works on a fee or free basis, depending on the rights associated with the work being accessed. Granularity is important here, as the works provided to users may be collections of content from many different sources bundled together into a single product. An MP3 file is a common example of one such bundle.

- **Content Traders**

Digital technology has brought with it an enormous extension in the potential market for content traders (including producers and publishers).
DRM may be helpful to content traders in the following way:

a) Use technology to protect works from unauthorised and unpaid use
b) Use the internet as the marketplace to provide access to more users/consumers
c) Provide an opportunity to deliver new products that would not be cost effective in traditional forms or channels
d) Streamline rights management to provide better remuneration to creators and producers
e) Implement managed payment systems such as pay per use, subscription or micro payments that enable the content to be marketed and priced differently and in more innovative ways
f) Track and record payment and usage for royalty payments and information to rights Holders manage security issues

4.0 Functional Aspects of DRM

Thus DRM has two functional areas:
i) The identification and description of intellectual property, rights pertaining to works and to parties involved in their creation of administration (digital rights management).

ii) The (technical) enforcement of usage restrictions (digital management of rights).

DRM may therefore refer to the technologies and/or processes that are applied to digital content to describe and identify it and /or to define, apply and enforce usage rules in a secure manner.
It is also important to distinguish between "access control", "copy protection" and "the management of intellectual property rights" highlighting their respective boundaries.

An ***access control*** system manages a user's access to content, usually achieved through some kind of password protection. However, once access to the content has been granted, no further protection is applied.
A ***copy protection*** system is designed to signal the extent of allowed copying and serial copying, if any, that is defined by the associated "usage information" with respect to any instance of delivered content , and to implement and enforce the signaled behavior in consumer equipment. The notion of copy protection can be extended to control the movement of content within and outside the user domain, encompassing re-distribution over the internet.

A fully enabled ***Intellectual property rights management system*** covers the processing of all rights information for the electronic administration of rights, sometime including contractual and personal information, to enable end-to-end rights management throughout the value chain.

5.0 Benefits of DRM

- Protection of digital content
- Secure e-book distribution
- Content authenticity
- Transaction non-repudiation
- Market participant identification

5.1 DRM Provides Protection of Digital Content

By scrambling, or ***encrypting***, content, DRM enables authors and publishers to send digital content across an unsecured network, like the Internet, so that the content can be read only by the intended recipients' e-book consumers. DRM uses a computer program called a *cryptographic algorithm* to encrypt e-book content. The cryptographic algorithm needs a secret key, a particular phrase or string of numbers, to encrypt the content. Only the holder(s) of this key can later unlock the content and read it. Since all key holders can readily access the encrypted content, it is quite important to properly manage keys, and much of DRM is concerned with this.

5.2 DRM Enables Secure E-book Distribution

Once e-book content is protected via DRM encryption, the proper key is needed to decrypt the content and render it readable. Without the key, the file is unintelligible. Anyone can have access to the encrypted content, but it will be of no use without the decryption key. Long keys are better than short keys, just like a combination lock using three numbers, say "36-27-12," is better than one that unlocks anytime "12" is selected on the dial. Today, 128-bit keys are in common use.

5.3 DRM Ensures Content Authenticity

It is not very easy to modify the content of a physical book and pass it off to unsuspecting consumers as an original. In contrast, tainted e-book content could be made to blend seamlessly with the original bits. To protect content authenticity, the content provider creates a message digest when the original, authentic e-book content is published.

This "official" message digest is then stored in a safe place, but made available to consumers who want to verify the authenticity of acquired e-book content.

5.4 DRM Provides for Transaction Non-repudiation

In both physical and electronic markets, it is important for participants to be able to prove that any given transaction actually took place. In practice, two mathematically related keys are used, one private and one public. The private key is owned by a transaction participant and kept secret. A participant "signs" the transaction when he encrypts (a piece of) it with his private key. Anyone interested in verifying the authenticity of the transaction can obtain the participant's public key and attempt to decrypt the signature. If the decryption operation is successful, market participants trust that the private key holder participated in the original transaction.

5.5 DRM Supports Participant Identification

In the physical world, it is fairly easy to determine who the participants in a transaction are. On the Internet, of course, it is not so simple. Without much difficulty, anyone can create a web site that appears to be entirely legitimate. Most are; some are not. DRM provides the ability to identify market participants using *digital certificates*. A digital certificate functions much the same way as a birth certificate or a social security number. A digital certificate is created using a cryptographic technique that binds a person's identity with his or her public cryptographic key. A digital certificate is created by combining an individual's public key, other identity information and one or more digital signatures.

5.6 DRM Technology

DRM systems are software packages or technological restraints that restrict the use of digital files in order to protect the interests of copyright holders. DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device.DRM systems take at least three approaches to securing content.

i) The first is "containment" or the wrapper, an approach where the content is encrypted in a shell so that it can only be accessed by authorized users.

ii) The second is "marking" or using an encrypted header, such as the practice of placing a watermark, flag, XML or XrML tag on content as a signal to a device that the media is copy protected.

iii) The third is the secure container, such as a dedicated reading device.

Some technologies (such as watermarking and fingerprinting) are emerging that attempt to provide copyright owners with the desired degree of protection, and to act as a disincentive to data piracy. Others, such as digital signatures, are familiar from cryptography, and provide services for origin authentication and content integrity.
In brief, the three technologies under consideration in this paper can be described as follows:

a) **Watermarking:** A technique for embedding hidden data that attaches copyright protection information to a digital object. This provides an indication of ownership of the object, and possibly other information that conveys conditions of use.

b) **Fingerprinting:** A type of watermark that identifies the recipient of a digital object as well as its owner (i.e. a 'serial number' assigned by the vendor to a given purchaser). This is intended to act as a deterrent to illegal redistribution by enabling the owner of the data object to identify the original buyer of the redistributed copy.

c) **Digital signatures**: A mechanism employed in public-key cryptosystems (PKCS) that enables the originator of an information object to generate a signature, by decipherment (using a private key) of a compressed string derived from the object. The digital signature can provide a recipient with proof of the authenticity of the object's originator.

Digital watermarks are intended to confer properties on digital objects similar to those that traditional watermarks confer on printed objects. Paper watermarks were first produced in the manufacturing process from the pattern of the mould left when paper slurry is pressed between frames to expel moisture. These have been used at various times to record the manufacturer's trademark and certify the composition of the paper. Today, most countries use

watermarked paper for printing currency, to act as a safeguard against forgery. While this does not provide foolproof protection, it makes forgery that much more difficult.

With the growth in the importance of digital media, accessed over computer networks, much interest has been shown in the development of techniques for embedding digital data in information objects to convey copyright information. The technology is relatively immature, and the extent to which it can satisfy this requirement is not yet proven. A diverse range of requirements have been proposed for watermarking. For example

a) Erasing the watermark should be difficult.
b) Adding a new watermark should be difficult.
c) The watermark should survive routine transformations such as filtering, compression, re-sampling, cropping, channel noise, digital/analogue conversion, and other signal processing artifacts.
d) It should be proof against well-known forms of attack (e.g., collusion attacks, where multiple versions of the same content, stamped with different watermarks, are compared).
e) The watermark should be unobtrusive, and should not impede proper use of the object.
f) The watermark should be pervasive and locally contained, to permit its recovery from a small portion of the data object. Other requirements, apparently contradictory, have been proposed that vary according to the needs of specific applications:
g) Watermarks should be perceptually visible, to reduce the commercial value of a stolen data object (though it could be argued that an authenticated object will have higher street value than an object of unknown provenance);
h) Watermarks should be invisible, so that a thief will be unaware that evidence of his illegal copying exists. As with any emerging technology that is both technically attractive and commercially relevant, many workers have entered the field, proposing different analyses of requirements and different technical solutions.

6.0 Software based Technologies

Software based technologies rely only on software mechanisms to defend against tampering. Some common software based approaches include code obfuscation in which the software is transformed into a functionally equivalent form which is difficult to understand and analyze, code encryption that prevents hackers from seeing and accessing the software, and self-modifying code that generates other code at run time. Another possible approach to ensure tamper resistance is for the software to require taking control at the operating system (OS) level. For example, to prevent a screen capture program from capturing unencrypted data on the screen, DRM systems can employ anti-screen capture method that operate at the OS level to disable unauthorized attempts. Deployment of DRM is still at an early stage. There are a number of DRM solutions on the market. Among these solutions, Microsoft's Windows Media Rights Manager (WMRM), IBM's Electronic Media Management System (EMMS), InterTrust's Rights System, and RealNetworks's RealSystems Media Commerce Suite (RMCS) are the most promising ones. Apart from the above major DRM providers, there are many other companies delivering DRM solutions including Adobe (www.adobe.com), IPR Systems (iprsystems.com), Liquid Audio (liquidaudio.com), Alchemedia (alchemedia.com), Digital World Services (dwsco.com), ContentGuard (contentguard.com), SealedMedia (sealedmedia.com) and many more.

7.0 Hardware Based Technologies

Hardware based technologies rely on secured hardware devices for protection. The hardware-based DRM approach is to provide a hardware trusted space, the execution space protected from external software attacks, for hosting protected content and in which only approved applications can execute. DRM services such as content decryption, authentication and rights rendering take place only in this trusted space.

For example, Microsoft is currently developing the "Palladium" architecture for trusted computing in future versions of Windows. While Microsoft says that DRM is not Palladium's stated purpose, the "Palladium" architecture provides a trusted environment upon which a DRM system could be implemented. In this proposed architecture, the nexus, a component of the Windows kernel running in trusted space, is in charge of booting and maintaining trusted space and authenticating user applications that need to run in trusted space. Every machine has a unique embedded private key in hardware and never exposed. This secret hardware key will be used to encrypt data within the trusted space. "Palladium" will offer a way to protect DRM applications against snooping and modification by other software and ensure that only software trusted by the person granting access to the content or service has access to the

enabling secrets. However, some people fear that they will completely lose control of their computers and are concerned that Microsoft could use Palladium to exert monopoly control over the desktop and the IT industry. Whether "Palladium" itself is secure and whether Microsoft will eventually succeed is a very complicated economic issue. Microsoft recognizes that industry support will play a big role if Palladium is to ever succeed and plans to develop "Palladium" as a collaborative consumer and industry initiative.

8.0 Conclusion

With well-designed system architecture and security technologies, copyright protection seems to be good news for content providers who want to develop digital services without fear of losing control over their valuable digital assets. However, to deploy a successful digital online service, it is not sufficient to apply cryptographic primitives and security measures to encrypt and distribute digital content online. This paper has highlighted the technical details of watermarking and PKCS technologies, and where these technologies might be effective. It is our professional duty to take part in the development of emerging technologies by participating in the discussions taking place nationally and internationally in standards organizations and the research arena which will affect the future of reading and information access as a whole.

9.0 References

1. Andra, Kishore., Chakrabarti, Chaitali., and Acharya, Tinku. (2002), A VLSI Architecture for Lifting-Based Forward and Inverse Wavelet Transform, IEEE Transactions on signal Processing, volume 50, No. 4, pp 966-977. Retrieved March 5, 2017 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=992147&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D992147

2. Berrani, S. A., Amsaleg, L., and Gros, P. (2003). Robust Content-based Image Searches for Copyright Protection, Proceedings of the1st ACM International Workshop on Multimedia Databases, 70-77. Retrieved March 5, 2017 https://dl.acm.org/purchase.cfm?id=951690&CFID=783882458&CFTOKEN=56948083

3. Bhat, D. N. and Nayar, S. K. (1998). Ordinal Measures for Image Correspondence, IEEE Transactions on Pattern Analysis and Machine Intelligence, 20 (4), 415-423. Retrieved Feb. 23, 2017 *ieeexplore.ieee.org/iel4/34/14891/00677275.pdf*

4. Chang, E.Y., Wang, J. Z., Li, C.,and Wiederhold, G.(1998). RIME: a Replicated Image Detector for the World Wide Web, Proceedings of the SPIE Multimedia Storage and Archiving Systems, 58- 67 Retrieved Feb 17, 2017. http://proceedings.spiedigitallibrary.org/proceeding.aspx?articleid=967415

5. Figueiredo, M. A. F. and Jain, A.K. (2002).Unsupervised Learning of Finite Mixture Models, IEEE Transactions on Pattern Analysis and Machine Intelligence, 24 (3), 381-396. Retrieved Feb 15, 2017 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=990138&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F34%2F21341%2F00990138.pdf%3Farnumber%3D990138

6. Guth, S. (2003). A Sample DRM System, Proceedings of the Digital Rights Management Conference, 150-161. Retrieved Feb 10, 2017 http://dl.acm.org/citation.cfm?id=947380&picked=prox

7. Hah-lin sieh, Lung-ao Hsu, I-Ju Tsai, (Dec 2005), A copy right protection scheme for color images using secret sharing and wavelet transform, Transaction engineering computing and Technology, volume 10, ISSN 1305-5313. Retrieved March 5, 2017.

8. Kesavan Pillai, (2005), A New Watermark Extraction from Watermarked Images and Videos, International conference on Enabling Technologies for Smart Appliances (ETSA) IEEE, Hyderabad. Retrieved Feb 21, 2017

9. www.watermarkingworld.com Retrieved March 01, 2017.

10. Petitcolas, F. (2000).Watermarking Schemes Evaluation, IEEE Signal Processing Magazine, 17 (5), 58-64. Retrieved Feb16 2017, https://www.google.co.in/#q=Watermarking+++Schemes+Evaluation%2C+IEEE+Signal+Processing+Magazine%2C+