DESIDOC Journal of Library & Information Technology, Vol. 34, No. 1, January 2014, pp. 11-15

# Application of Digital Rights Management in Library

Ashis Kumar Pal

*Indian Statistical Institute Library, 203 BT Road, Kolkata-700 108*
*E-mail: ashispal@isical.ac.in*

**ABSTRACT**

Digital rights management (DRM) is emerging as a formidable new challenges and focuces on security like encryption and watermarking. It is a type of access control technology that is used by hardware manufacturers, publishers, copyright holders and individuals with the intent to limit the use of digital content. Libraries may license resources, such as images and videos, which may require a DRM system to protect the files from copying or misuse. The DRM technology is used to limit copying, printing and sharing of e-books. A properly managed DRM system could assist libraries in managing these services.

**Keywords:** Digital rights management, digital libraries, digitisation, copyright, encryption, watermarks, DRM techniques, digital certificate, digital signature

## 1. INTRODUCTION

Information and communication technologies, internet, and particularly the world wide web have revolutionised the information explosion. Now the e-publishing agencies and digital libraries face the challenge to protect the authority rights and fair use of the digitised reading material.

Digital rights management (DRM)[1] is a technique that attributes certain conditions on some digital products to be used and shared in libraries and information centres. The DRM is set up as a system for the protection of digital works, and created or designed to protect the unauthorised duplication and illegal distribution of copyrighted digital products. As the internet is becoming widely used, it is easy to copy and illegally sell a variety of marketed digital information and products. Therefore, this type of technique prevents users from adopting any illegal and unauthorised attempts.

The DRM technology works by allowing distributors of electronic information to control viewing/access to content. Some form of encryption is needed to control access to content. Rights management solutions are based on a wrapper or container placed around a data file which protects and sets the data life-cycle and defines usage rules, payment and redistribution constraints. A license must be acquired to unlock the wrapper and get access to the content. Individual 'keys' for viewing or listening to the content are provided to the end-user who has purchased the rights which generally include limitations on copying, printing and redistribution.

The DRM systems are designed to ensure the harmony of the object so that the object is not intercepted before delivery and to ensure the security of the whole distribution chain, so that objects are transferred only to authorised consumers and devices. The DRM system makes use of the technology and tools to create an end-to-end secured packaging and distribution system for protected contents. The system generally includes the following steps:

- Watermarks and identifiers are used to identify the content uniquely. This identification can also be used for downstream tracing of the content to ensure an authorised use of the content.
- To ensure that only consumers with appropriate keys can access the content and to ensure that the content is unchanged throughout the process.
- To manage the encryption and decryption of the content by authorised entities in the content value chain
- It contains usage rules to decide what conditions must be met for access and how the consumer can use the resource.

The DRM systems have also reached to a stage of maturity and flexibility where libraries can actually consider their adoption to provide integrated access to all digital information. The success of information society depends on digital content being accessible. Libraries must not be prevented by DRM from availing themselves of their lawful rights under national copyright law and must be able to extend their services to the digital environment.

Received 5 February 2013, Online published 17 January 2014

## 2. IMPLEMENTATION OF DRM TECHNOLOGY

For maximum utilisation of the resources, the important part is its implementation in the ground level. Various techniques are used to protect the right of the author. The DRM technologies[2] have enabled publishers to enforce access policies that not only disallow copyright infringements, but also prevent unlawful use of copyrighted works. The DRM is a copy protection tool generally used by the e-book publishers to restrict the user of converting their e-book formats from one to another and limit them to copying, printing, and sharing of e-books.

The fundamental security requirement for a DRM system is that the hardware and/or software used to access the protected data be guaranteed by its manufacturer to behave in accordance with licences. A terminal is an abstract single-user player, editor, or similar that may be implemented as a hardware device, a software application or combination of the two. Figure 1 shows, one reference model of a DRM system. Information is created by a provider and transmitted in a protected (for example, encrypted) form to a user via some distribution channel. To access the protected data, user must obtain a licence from the licence issuer. Licences are written in a machine-readable rights expression language that sets out the terms of use of the data and the information required to access the protected content.

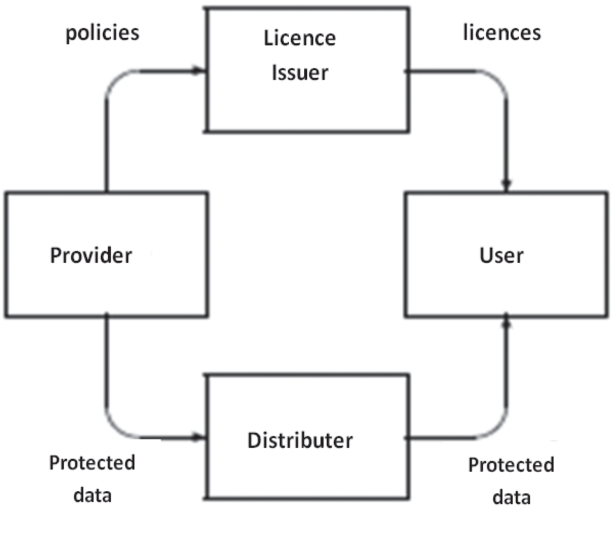


Figure 1. Reference model for DRM systems.

## 3. TOOLS AND COMPONENTS OF DRM

The DRM systems usually comprise of several technologies that enable a transaction of digital documents to the authorised user. Many core technologies involve in DRM that include:

### 3.1 Watermarking

Watermarking[3] inserts information into content that can be used for many purposes, such as provenance (creation and ownership), copyright, and the conditions of use. Watermarks are inserted into contents of a digital file that donot affect the original content. Digital information embedded within any digital media can later be detected and extracted with the watermark recognition software. Watermarks can be measured in terms of capacity and original signal fidelity.

Watermark capacity refers to the amount of information that can be embedded in a watermark. A Signal fidelity measure function measures the distortion between the unmarked file and the watermarked file. Watermarking is often used in data hiding, in which secret information is embedded in a digital file. Watermarks serve the purpose of identification and content use management that generally is a part of DRM system or strategy for safeguarding documents.

*3.1.1 Application of Watermarking[3]*

A number of possible applications of watermarking technologies are there in the field of library and information science which are:

- In the field of data security, watermarks may be used for certification, authentication, and conditional access. Certification is an important issue for official documents, such as identity cards or passports
- Another application of watermarking is on the protected identity card or library card. The identity number is written in clear text on the card and hidden as a digital watermark in the identity photo. Therefore, switching or manipulating the photo, identity will be detected
- Digital watermarks can also be adapted to mark white paper with the goal of authenticating the originator, verify the authenticity of the document content, or to date the document. Such applications are especially of interest for official documents, such as contracts. In the event of a dispute, the digital watermark is then read allowing authentication of key information in the contract.

### 3.2 Encryption

Encryption[4] is based on cryptography. Information security is provided on computers and over the internet by a variety of methods. But the most popular forms of security rely on encryption, the process of encoding information in such a way that only the person (or computer) with the key can decode it. Encryption is a standard method to protect digital content from unauthorised use by scrambling the content, until a key is used to decrypt the content and make it usable by the key holder. The key (code) is the most important component in an encryption system. Encryption systems generally are of two categories:

(a) Symmetric/Private-key encryption; and

(b) Public-key encryption (also known as asymmetric-key encryption).

In symmetric-key encryption, each party (computer) has a secret key (code) that it can use to encrypt a packet of information before it is sent over the network to another computer. Symmetric-key encryption is essentially the same as a secret code that each of the two computers must know to decode the information.

Public-key encryption uses two different keys at once, i.e., combination of a private-key and a public key. The private-key is known only to one's computer, while the public key may be widely distributed, even to unknown users. The public Key and the private-key are related computationally, but the private-key should not derivable from the public key. A message may be encrypted by anyone processing the public key but can only be decrypted by the private-key.

### *3.2.1 Application of Encryption*

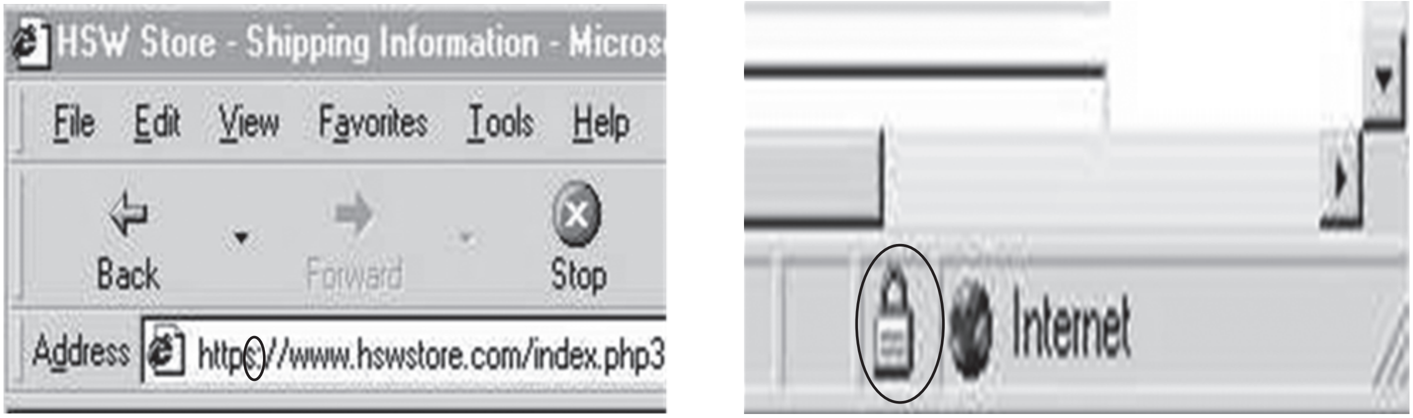
A popular implementation of public-key encryption is the secure sockets layer (SSL) developed by Netscape. It is an Internet security protocol used by Internet browsers and Web servers to transmit sensitive information[4]. The SSL allows authenticating both the client and the server, and also establishing a secure connection between client and server. It is primarily designed to ensure the security of electronic transactions over the internet. This SSL has become part of an overall security protocol known as transport layer security (TLS). Figure 2(a) shows that 's' is given after 'http' in the address whenever someone is about to enter sensitive information, such as a credit-card number. Figure 2(b) also introduces padlock system by the use of encryption system.

## 4. DRM TECHNOLOGY IN LIBRARY

The DRM[5] products are developed in response to the rapid increase in online piracy of commercially marketed material which proliferates through the widespread use of file exchange programs. Typically, DRM is implemented by embedding code that prevents copying, specifies a time period in which the content can be accessed or limits the number of devices the media can be installed on. Although digital content is protected by copyright laws but policing the Web and catching law-breakers is very difficult. The DRM technology focuses on making it impossible to steal content. However, serious breaches of copyright law is there because of the ease with which digital files can be copied and transmitted.

Recently, electronic document delivery services/system[6] libraries have adopted to deliver the documents in the softcopy rather than the physical copy of the same to its user. On this system of delivery, users receive a copy of a required article which is being requested by him from the source, but this system is objectionable by the publisher of the document because when a user receives a document he is free to share it with others without any limitation. To avoid these types of misuses, libraries should have to follow the DRM technologies with the following techniques:

- Many commercially licensed resources are bundled with digital rights licenses or watermarks that may be imperceptible to the libraries as well as to the end users.
- Libraries may license resources, such as images and videos, which may require a DRM system to protect the files from copying or misuse.
- Digital signature or the hand-written signatures are used to regulate the access to digital content, and
- E-books in the library use DRM technology to limit copying, printing, and sharing of e-books. E-books are usually limited to a certain number



https://www.hswstore.com/index.php3

(a)

(b)

**Figure 2. (a) 's' for sensative information and (b) Padlock system used for encryption.**

of reading devices and some e-publishers prevent any copying or printing. Some commentators believe that DRM makes e-book publishing complex.

## 5. FUTURE OF DRM

The DRM is emerging as a formidable new challenge[4]. It is essential for DRM systems to provide interoperable services. Solutions to DRM challenges will enable untold amounts of new content to be made available in safe, open, and trusted environments. The technology can be expected to be heavily used in the future to support digital library collections, software development, distance education, and networking of digital items. Libraries must not be prevented by DRM from availing themselves of their lawful rights under national copyright law and must be able to extend their services to the digital environment.

Evaluation of the DRM implementation with respect to issues such as copyright support, fair use or fair dealing protection, renewability, and degradation of transmission and playback performance should become a standard part of the resource evaluation process. Another issue of concern to libraries is that DRM system may unfairly disadvantage disabled users. Most countries provide exemptions from anti circumvention provisions in law to support access to information for disabled user. Libraries should ensure that DRM bundles with licensed content either includes special provisions for the disabled or can be made accessible to disabled patrons in some manner, perhaps through special certificates or at designated library workstations.

Libraries that routinely purchase DRM-protected content may want to investigate the use of modular hardware components to avoid collisions with operating systems and other application whenever a DRM component is automatically renewed. The best current strategy for dealing with embedded DRM is awareness – studying the system configuration and DRM specification that vendors provide. The DRM components of any given product are marketed to the content rights holder, not to the user.

## 6. DRM AND COPYRIGHT (AMENDMENT) ACT, 2012 IN THE DIGITAL ERA

‘Indian Copyright (Amendment) Bill, 2012’ enacted in the Parliament[7] in May 2012, was largely based on two treaties, i.e., World Intellectual Property Organisation (WIPO) Copyright Treaty, 1996 and the WIPO Performances and Phonograms Treaty (WPPT), 1996. It addresses the challenges posed by digital technology to the protection of copyright and related rights, particularly with regard to the dissemination of protected material over digital networks such as the internet and deals with copyright protection for the authors of literary and artistic works such as writings, computer programs, original databases, musical works, audio-visual works, works of fine art, and photographs.

This Indian copyright Act includes two new Sections 65A and 65B to punish persons found guilty of piracy by using technology to take away somebody’s copyright and then use that material to make profits.

‘Section-65A[7] – Any person who circumvents an effective technological measure applied for the purpose of protecting any of the rights conferred by this Act, with the intention of infringing such rights, shall be punishable with imprisonment which may extend to two years and shall also be liable to fine.’

‘Section-65B[7] – Any person, who knowingly: (a) removes or alters any rights management information without authority, or (b) distributes, imports for distribution, broadcasts or communicates to the public, without authority, copies of any work, or performance knowing that electronic rights management information has been removed or altered without authority, shall be punishable with imprisonment which may extend to two years and shall also be liable to fine’

So, the Copyright (Amendment) Act, 2012, makes substantial progress in filling the gaps in the parent Act (1957) so as to benefit all stakeholders. The act provides a clear picture on the rights of authors for his/her creative works.

## 7. LIBRARIANS AGAINST DRM

The DRM provides media and technology companies the ultimate control over every aspect of what people can do with their media. This essentially moves control of the library's digital collection into the hands of the publishers and intermediary companies which will immediately be implementing DRM. That is why, in 2008, the DRM Elimination Crew stood on the steps of the Boston Public Library (BPL) and demanded that they Kick DRM Out[8].

Back then librarians were somewhat disgruntled with this setup, but, unfortunately, few librarians were willing to take action to get DRM out of their libraries. However, a recent move by the publisher HarperCollins may have just pushed many such librarians over the edge by demanding a 26-checkout limit on many of their titles (i.e., a title can only be checked out 26 times to patrons before it is removed from the library's digital collection and it needs to be re-purchased).

So, the Readers Bill of Rights[9] currently makes the following demands for readers:

- Ability to create a paper copy of the item in its entirety
- Ability to retain, archive and transfer purchased materials

- Digital Books should be in an open format (i.e., one can read on a computer, not just a book reader device)
- Reader information will remain private (what, when and how one reads will not be stored or marketed)

Readers, librarians, and authors need to make their voices against DRM, because it makes them helpless and divided. If one does not ban DRM from libraries then it will be expected that in future librarians and readers may not be able to retain rights into the library.

## 8. CONCLUSIONS

Digital rights management system is a means of delivering content. However, DRM is frequently seen only as a technical protection measure, i.e., technical means of enabling right holders to deliver digital content in a controlled way, preventing users from having access to the content unless they meet the requirements of the right holder, be it financial or otherwise, and preventing users from using the accessed content in ways other than the right holder has given permission for. Libraries are already involved in the clearance and management of rights. A property managed introduction of DRM systems in its widest sense, could assist libraries in managing their services.

## REFERENCES

1. May, Christopher. Digital rights management: Problem of expanding ownership rights. Chandos Publishing, Oxford, 2007.
2. Karen Coyle. The technology of rights: Digital rights management. Talk originally given at the Library of Congress on 19 November 2003, 2003.
3. Hartung, Frank & Ramme, Friedhelm. Digital rights management and watermarking of multimedia content. *IEEE Communications*, 2000, 78-84.
4. Kramer, Elsa F. Digital rights management: Pitfalls and possibilities for people with disabilities. *J. Electr. Pub.*, 2007, **1**(10).
5. Agnew, Garce. Digital rights management: Librarian's guide to technology and practice. Chandos Publishing, Oxford, 2008.
6. Pal, Ashis Kumar. Design and development of Prof. Prasanta Chandra Mohalanobis archives. *IASLIB Bulletin*, 2011, **3**(56), 154-60.
7. The Copyright (Amendment) Bill 2012, passed by Rajya Sabha on 17th May 2012.
8. http://www.defectivebydesign.org/Librarians-Against-DRM. (accessed on 22 October 2012).
9. Eschenfelder, Kristin R. Every library's nightmare? Digital rights management, use restrictions, and licensed scholarly digital resources. *College Res. Lib.*, 2008, **3**(69).

### About the Author

**Mr Ashis Kumar Pal,** MA (Econ.) and MLISc is currently working as Associate Scientist 'A' at Library, Documentation & Information Science Division, Indian Statistical Institute, Kolkata. Besides this, he is working as Guest Faculty, Dept of Library & Information Science, Rabindra Bharati University and Counselor of Indira Gandhi National Open University. He has served the profession for more than 18 years. His research interests include: Institutional repository, digital rights managements, encryption, watermarking, library consortia, library automation, etc. He has published many papers in the national and international journals.