JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER ENGINEERING
ISSN: 0975 – 6760 | NOV 16 TO OCT 17 | Volume 4, Issue 2

SOFTWARE PIRACY THROUGH DIGITAL RIGHTS MANAGEMENT SYSTEM

[1]ROMAN PRANITA DATTATRAYA
[2]JADE TEJAL MANOHAR
[3]MANDHARE POONAM VINOD

[1, 2, 3] Department of Computer Engineering,
Rajgad Dyanpeeth Technical Campus,Pune University,
Dhangwadi Pune 412205,Maharashtra, India.

[1]pranitaroman410@gmail.com, [2]tejaljade2295@gmail.com, [3]poonamm2811997@gmail.com

ABSTRACT *: Software publishers use digital rights management, specifically copy-protection techniques, to prevent unauthorized and illegal copying of their software products. Common forms of prevention are copy-protection techniques based on physical tokens. While physical tokens provide better protection from unauthorized copying than intangible ones, the protected digital content becomes unsuitable for online distribution. This paper investigates the role of copy-protection techniques based on physical and intangible tokens in software piracy prevention. An internationally organized online survey among users of sequencer software, a particular kind of music software, provides the data for the subsequent descriptive analysis and logistic regression. Based on our findings, we present the general implications of our results for a software publisher's anti-piracy and online distribution policy.*

KEYWORDS
Mobile communication, Encryption, Publishing, Servers, Packaging, Internet

1.INTRODUCTION

The advent of digital media and analog-to-digital conversion technologies (especially those that are usable on mass-market general-purpose personal computers) has vastly increased the concerns of copyright-owning individuals and organizations. These concerns are particularly prevalent within the music and movie industries, because these sectors are partly or wholly dependent on the revenue generated from such works. While analog media inevitably loses quality with each copy generation, and in some cases even during normal use, digital media files may be duplicated an unlimited number of times with no degradation in the quality of subsequent copies.The advent of personal computers as household appliances has made it convenient for consumers to convert media (which may or may not be copyrighted) originally in a physical, analog or broadcast form into a universal, digital form (this process is called ripping) for portability or viewing later. This, combined with the Internet and popular file-sharing tools, has made unauthorized distribution of copies of copyrighted digital media (also called digital piracy) much easier.

DRM technologies enable content publishers to enforce their own access policies on content, such as restrictions on copying or viewing. These technologies have been criticized for restricting individuals from copying or using the content legally, such as by fair use. DRM is in common use by the entertainment industry(e.g., audio and vid publishers) many online music stores, such as Apple's iTunes Store, and e-book publishers and vendors, such as OverDrive, also use DRM, as do cable and satellite service operators, to prevent unauthorized use of content or services..

2.COMMON DRM TECHNIQUES

Digital Rights Management Techniques include:

- Restrictive Licensing Agreements: The access to digital materials, copyright and public domain is controlled. Some restrictive licenses are imposed on consumers as a condition of entering a website or when downloading software.

- Encryption,Scrambling of expressive material and embedding of a tag: This technology is designed to control access and reproduction of information. This includes backup copies for personal use.

3.ENVIRONMENTAL ISSUES

DRM can accelerate hardware obsolescence, turning it into electronic waste sooner:

- DRM-related restrictions on capabilities of hardware can artificially reduce the range of potential uses of the device (to the point of making a device consisting of general-purpose components usable only for a purpose approved, or with "content" provided, by the vendor), limit upgradeability and repairability.
- Users may be forced to buy new devices for compatibility with DRM, i.a. through having to upgrade an operating system to one with different hardware requirements.

4.WHAT IS DRM ?

"Digital Rights Management", it is a standard term used for access control technologies used by hardware/software companies to impose limitations on the usage of digital content and devices.

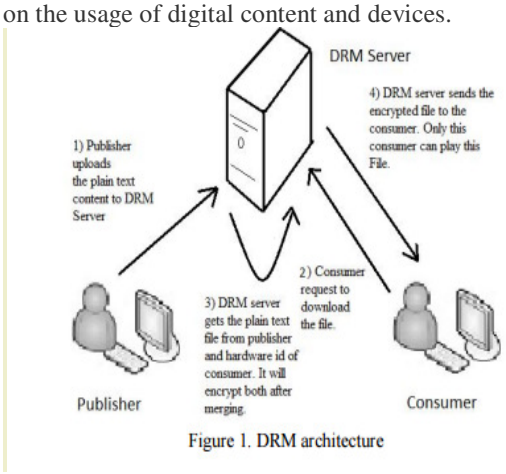


Figure 1. DRM architecture

5. Watermarking Algorithm

Digital images are distributed in encrypted format and watermarking of these images for authentication and copyright protection. We need media authentication in encrypted domain to enhance security. So sometimeese necessary to watermarking in encrypted media for copyright management and authentication.

The working of the Watermarking Algorithm can be explained in the following 2 methods.

A. RC5 Encryption

The input image to be transmitted is first divided into wavelet sub-bands. We choose LL band for encryption since the largest part of the image energy is concentrated at lower frequency sub- bands .The RC5 algorithm is represented as RC5-w/r/b where r=number of rounds, w=word size in numbers of 8- bit byte in the key.
To reduce the computation time, particular region input image can selected encryption without doing Image. RC5 uses following parameters A variable block size (w). Block size may 64, and128 bits. A variable key size (k). Key size can range from 0 bits to 2040 bits in size.

1) Key Expansion

In this module, the password key k is expanded. For thisexpansion table (t) is used. The size of table t is 2(r+1), where r denotes the number of rounds. The key-expansion process must be performed before encryption or decryption processes..

2) Encryption Algorithm:

The two w-bit words inputs are denoted as M and N

```
M=M + S[0]; .
N = N + S[1]; .
for i = 1 to r do .
M = (( M ⊕N) <<< N ) + S[ 2 * i ];
N = (( N ⊕M) <<< M ) + S[ 2 * i + 1];
```

3) Decryption Algorithm:

Decryption is done at receiver side for the same sub-band which is used for encryption. RC5 is a symmetric cipher, so encryption and decryption key are same. The decryption algorithm is the reverse of encryption algorithm. The two w-bit word inputs are denoted as M and N.

```
for i = r down to 1 do
N = (( N –S[ 2 * i + 1 ]) >>> M) ⊕M;
M = (( M –S[ 2 * i ] >>> N) ⊕N;
N = N -S[1];
M = M -S[0];
```

B. Watermarking (LSB Method)

The digital watermarking system fundamentally consists of a watermark embedder and a watermark detector. The watermark embedder inserts a watermark image onto the

cover image and the watermark detector detects the presence of watermark image.

1)Watermark embedding:

The largest part of the image energy is concentrated at The lower frequency sub-band.Therefore embedding watermarks in these sub-bands may corrupt the image a lot. Also, changing the high frequency sub-band HH is not sensitive to human eye. So, many DWT based water marking algorithm uses middle frequency sub-bandHL and HL for embedding the watermark where acceptable performance of imperceptibility and robustness could be achieved . In proposed scheme, for embedding the watermark first step is to choose the high frequency sub-bands which is most sensitive to human visual system i.e. LH sub-band and second step is to apply LSB watermarking in LH sub-band. The Watermarking technique LSB (Least Significant Bit) substitution digital watermarking is invisible watermarking technique in which we embed information which is not visible. In digital watermarking, the watermark bits are spread in the image in such a way that they cannot be recognized and show toughness against attempts to remove the hidden data. In a digital image, information can be inserted directly into every bit of cover image or the more busy areas of an image. We insert information into every bit of cover image.
Example of least significant bit watermarking :-
Image:

10001010 01110100 00011011 01000001 ...
Watermark:

1 0 0 1 ...

Watermarked Image:

10001011 01110100 00011010 01000001…

2) Watermark Extraction :

The extraction of watermarking process will be reverse of embedding. We retrieve watermark bit by extracting LSB of watermarked image.

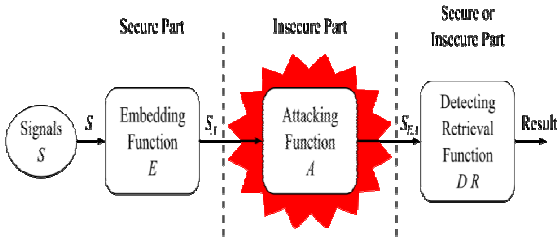
Algorithm for LSB (n bit):-

1: For each pixel in image.

2: Converting the image pixel into binary.

3: Selection of the last n bits from the binary converted code and replacing it with the secret image binary sequence.

4:End.



6.HOW DOES DRM WORKS?

DRM s DRM stands for Digital Rights Management and it is now (spring 2002) the hot topic among content owners and technology companies alike.
DRM, which is most commonly found in movies and music files, doesn't mean just basic copy-protection of video, audio and ebooks, but it basically means full protection for digital content, ranging from delivery to end user's ways to use the content. We can remove the DRM from video and audio files legally by quick recording.
DRM doesn't mean just basic copy-protection of digital content (like ebooks, MP3s or DivX videos), but it basically means full protection for digital content, ranging from delivery to end user's ways to use the content.
Typically, authorized recipients or users must acquire a license in order to consume the protected material: files, music, movies, according to the rights or business rules set by the content owner. DRM plays a very important role in the battle of cracking down on pirated compact discs and contents, however, To some extent, it also hurts the consumers' legitimate rights and takes much unconvenience to user.

7.ADVANTAGES

1)DRM technology focuses on making it impossible to steal web content.
2)Digital right management is a method for managing different kinds of contents .
3)It helps in protecting content against illegal copying and allows control consumption of media.
4)DRM covers the description,identification,trading,protection,monitoring and tracking of all forms of rights usages over both tangible and intangible assests including management of rights holder relationship.

8. CONCLUSIONS

In this paper, we presented a DRM framework to protect digital multimedia content and which can be extended to software applications. The framework can also be extended to support multiple content formats. We found it flexible and efficient to manage user rights, reasonably secure in design and interoperable with the open or third-party clients. Future scope of this work includes the investigation on extending this framework to a cloud environment.

9.REFERENCES

[1] Privacy-Preserving Digital Rights Management based 978-1-4799-3223-8/14/$31.00 ©2014 IEEE [2] A Robust Approach to Prevent Software Piracy 978-1-4673-0455-9/12/$31.00 ©2012 IEEE [3] A P2P Cultural Multimedia Network – Maximizing Cultural Dissemination and supporting Copyright Protection and Management, ©2014 IEEE [4] ADRMS: Active Directory Digital Rights Management Overview. Available: http://msdn.microsoft.com/enus/library/cc530389(v=vs.85).aspx. [5] Adobe Content Server, In http://www.adobe.com/products/ [6] WebGuard: A System for Web Content Protection. Available: http://domino.watson.ibm.com/comm/research_projects.nsf/pages/labasec.WebGuard.htm [7] DRM-JVM: Digital-Rights-Management-Enabled Java Virtual Machine. Available: http://domino.watson.ibm.com/comm/research_projects.nsf/pages/labasec.DRM-JVM.html [8] New Method of Hardware Encryption against Piracy 978-0-7695-3600-2/09 $25.00 © 2009 IEEE [9] Enterprise Digital Rights Management System based on Smart Card. 978-1-61284-842-6/11/$26.00 ©2011 IEEE [10] A DRM Framework Towards Preventing Digital Piracy. 978-1-4577-2155-7/11/$26.00 c_2011 IEEE [11] Unifying Broadcast Encryption and Traitor Tracing for Content Protection. 1063-9527/09 $26.00 © 2009 IEEE [12] Annoyance Maximization for Digital Cinema Anti-piracy Applications 978-0-7695-3959-1/09 $26.00 © 2009 IEEE