Major Challenges in Digital Contents Copyright Protection

André Fontes

Lusófona University of Porto,
R. Augusto Rosa 24, 4000-098 Porto, Portugal

arkelogen98@gmail.com

Abstract. The advances of technology can put the Digital Content creators in a bad position because how easy it is for "pirates" to make illegal perfect copies of videos, images, artistic work, literature, documents and among other subjects. This is a violation of copy right ownership therefor there are some people that focus on protecting the copyrights like Digital Rights Management (DRM). The DRM focus on restricting the digital copy while securing and administering copyrights and their trademarks to the extent permitted by copyright laws. It is currently possible to customize the retail spread of a commercialized file, for example by limiting the number of times that file can be opened or the duration of its validity. This Paper reports how DRM is used by content holders, how DRM try to ease the practice of piracy, other types of protection that content holders can do, discuss the fair use and not fair use of digital content. This paper will also report about watermark and security of content.

Keywords: Copyright, Digital Content, DRM, Fair use, Licenses, Progressive download, Piracy

1 Introduction

The increase of digital content and the advance of multimedia bring opportunities for content creators to publish their work and to be recognized.[1] The problem behind the digital content now is how easy it is to make perfect illegal copies and to distribute to others through internet. The internet now is used for everything, publish works from school, articles, artist work, among others which make more vulnerable the content that is private, that someone has ownership like producers. That's why it should be license control of downloads and copying copyright content because now it's more difficult to producers to sell their information and content at a profitable price. The digital information its not only distributed in the internet but may be also distributed by email, even people can use spoofing to capture information that is not theirs and use it to is on benefit.

10.11228/dpsc.02.01.008

Nowadays authors request copyright protection of digital content so that web users can be restricted and not distribute the digital content as he like and to protect the originality and creativity of their intellectual properties.[1]

One way to protect the copyright is to use the Digital Rights Management (DRM) which use the laws to enforce the copyrights and restricting the use of digital content. The DRM can have problems related to "fair use" and privacy because the DRM need a specific legal measures and contractual mechanisms in order to regulate the "fair use" and minimize privacy conflits.

The second topic will report about copyright, piracy, fair use and how these 3 topics are related.

The third topic will report about Digital Rights Management, how it works, what are the advantages and disadvantages.

The fourth topic will report about solutions to the copyright protection and to complement the DRM systems.

2 Copyrights

Copyright is the exclusive right that a creator or a producer have over of a type of work or content like a music, video games, movies among others.

The term of copyright for a work depends on several factors, including whether it has been published, and, if so, the date of first publication. As a rule, for works created after January 1, 1978, copyright protection lasts for the life of the author plus an additional 70 years.[2]

The term Copyright came with the objective to reward a content creator for his work and his originality but with the internet in the mix also came the pirates, who use content from the copyright owners to his own benefit because now is easy to create copies of a type of content and distribute them like copies of a music.

Copyright protection rules are similar worldwide, due to several international copyright treaties, the most important of which is the Berne Convention. Under this treaty, all member countries — and there are more than 100, including virtually all industrialized nations — must afford copyright protection to authors who are nationals of any member country. This protection must last for at least the life of the author plus 50 years and must be automatic without the need for the author to take any legal steps to preserve the copyright.[3]

2.1 Piracy and Fair Use

Piracy is an illegal act that people do to obtain content that is not theirs and by doing that they violate de laws of copyright.

10.11228/dpsc.02.01.008

There are two basic ways in which piracy can occur [4]:

- Unauthorized acquisition. This form of piracy occurs when a consumer obtains copyrighted content illegitimately, for example, by an unauthorized download of content from a peer-to-peer file sharing service, such as Gnutella, or by obtaining illegitimate CDs or DVDs from a street vendor of friend.

- Unauthorized use. This form of piracy occurs when a consumer obtains a piece of copyrighted content legitimately and then attempts to use it in an unauthorized way.

Namely all forms of digital piracy are, to some extent, associated because they are inversely correlated to wider measures of socioeconomic development, the richer the country, the lower its piracy rate.[5]

Economic models of piracy in general study the impact of piracy on profits and the effect of enforcing copyright. Conventional wisdom suggest that piracy represents a drain to publisher profits and reducing piracy forces consumer to legitimately acquire software. We then identify various scenarios including the existence of domestic software industry and study their effect on government incentive for increased copyright enforcement and publisher profits.[6]

The importance of ethics in modelling software piracy is a recurring theme that is just beginning to be tapped. The decision to copy or not copy intellectual property is influenced by ethical reasons. Ethics is the study of moral systems. It is important to note that the moral philosophers do not make moral judgments about right or wrong but attempts to discover truth about the meanings of concepts and justification of judgments.[6]

In the digital environment, the consumer's right to be anonymous in purchasing music, products or services has been severely hampered. The Digital Rights Management software requires users to register their email addresses and other personal information as part of authorization and verification.[7]

The history of "fair use" extends far back before PD 49 and the 1997 Copyright Law.US and Philippine courts, in the past, allowed certain, limited uses of copyrighted material without permission from the copyright owner. Consequently, in the process, these courts, by precedent, firmed up the practice of fair use privilege. The doctrine provides freedom to make copies and publish quotations beyond the special privileges granted to libraries and archives. In time, "fair use" became a convenient excuse for copying, and served as a defence against copyright infringement, when invoked. The doctrine also permits libraries to supply multiple copies of materials for classroom teaching, for purposes of scholarship, research and private study, criticism and review, news reporting, and similar purposes.[8]

10.11228/dpsc.02.01.008

3 Digital Rights Management

The goal of a distributed DRM system is for content authors to be able to project policies governing their content into remote environments with confidence that those policies will be respected by the remote nodes.[9]

First, DRM is about managing the policies under which material will be made available, and then it is about ensuring that these policies are respected.[9]

Unfortunately, today, with a simple browser plug-in, in many sites you can download available material, so it's not uncommon to find courses, movies, and music being marketed illegally or in districts.

DRM can be used to detect and verify ownership of data and to control access to the data in accordance with a policy determined by the content creator or distributor. A further approach frequently incorporated in a DRM system to embed a digital watermark in the digital media file.[10]

DRM removes usage control from the person in possession of digital content and puts it in the hands of a computer program. The applications and methods are endless, here are just a few examples of digital rights management [11]:

- A company sets its servers to block the forwarding of sensitive e-mail.
- An e-book server restricts access to, copying of and printing of material based on constraints set by the copyright holder of the content.
- A movie studio includes software on its DVDs that limits the number of copies a user can make to two.
- A music label releases titles on a type of CD that includes bits of information intended to confuse ripping software.

DRM systems must also facilitate the delivery of content offline on CDs and DVDs, deliver content on-demand over peer-to-peer networks, enterprise networks, or the Internet and provide ways of determining the authenticity of content and of rendering devices.[12]

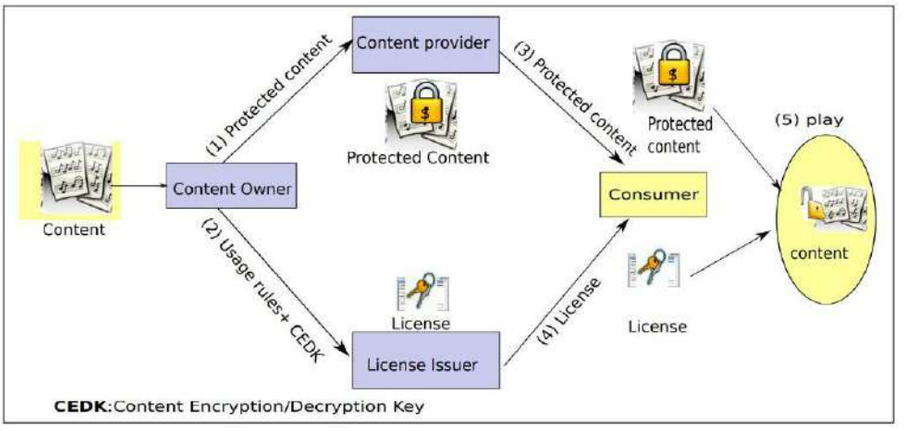

Fig 1. Typical DRM system architecture [13]

10.11228/dpsc.02.01.008

The digital content is packaged (encrypted and metadata enriched) and then provided through distribution channels. Users need special controllers (client-side s/w) in order to be authenticated and gain access through the decryption of content. License servers may be used to manage licenses describing access rights and conditions.[14]

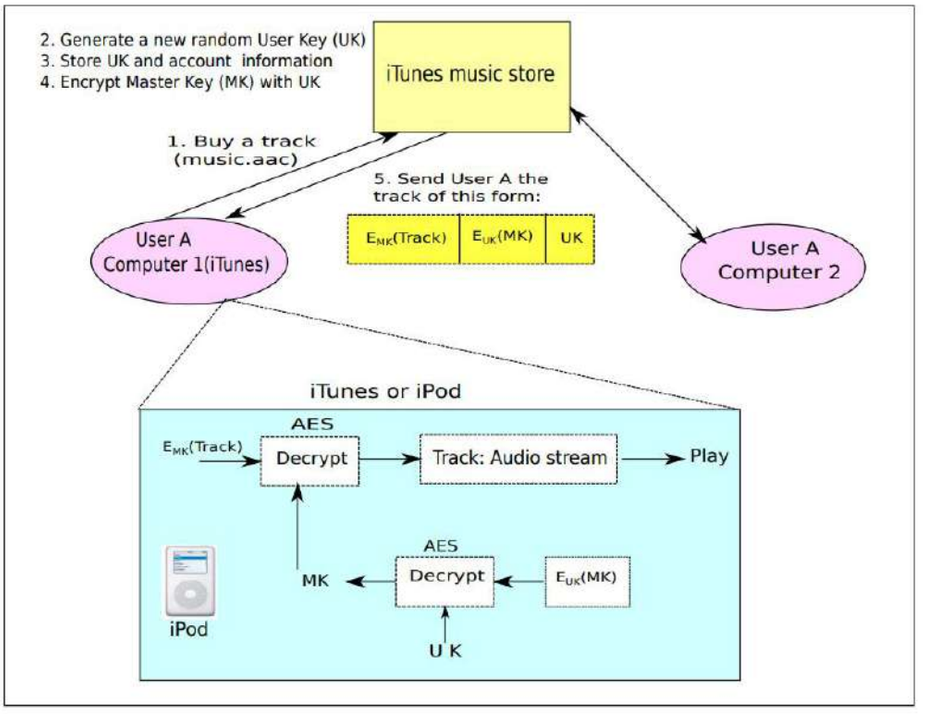

Fig 2. Dataflow of Apply Fair Play DRM [13]

Apple enforced DRM despite not being the actual creator or owner of the intellectual property it licensed. This placed it in the awkward position of maintaining the DRM despite having only marginal, or tangential stake in that IP beyond its role as a gate-keeper. This ultimately contributed to its decision to back down from its DRM scheme.[15]

The big problem of DRM its that it takes control of the content and places a lot of processing issues but brings security to the content providers and tries to end the piracy although its impossible to end that.

10.11228/dpsc.02.01.008

4 Solutions that improve copyright protection

4.1 Watermark and fingerprint

Other type of solutions for digital content protection is the scheme of watermark. A watermark is a signal added to some form of digital data (music, video, image) that can make you prove that you are the owner of that product, its very hard to remove the watermark by distorting the image and its difficult to find the watermark if you don't know the secret key.

The Watermark tactic it's an attribution of a private key to an original digital data that if other people try to claim that digital data, the owner can produce the unmarked original and demonstrate the presence of her watermark in the image that the other people are trying to claim.

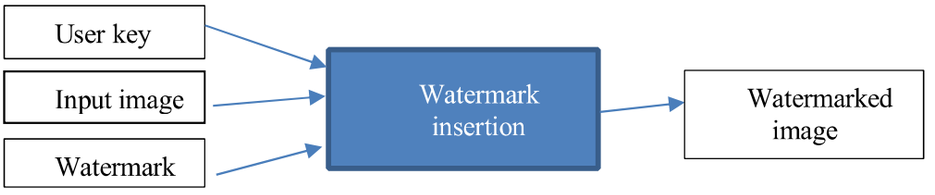

Fig 3. Representation of watermark insertion

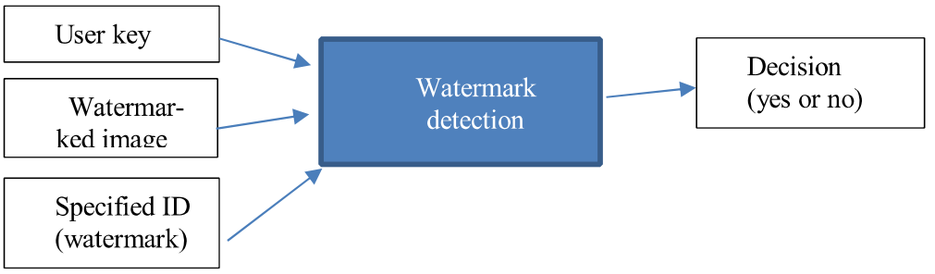

Fig 4. Representation of watermark detection

The digital watermarking system essentially consists of a watermark encoder and a watermark decoder. The watermark encoder inserts a watermark onto the host signal and the watermark decoder detect the presence of watermark signal.

The encoder process is the attribution of a private key to the image and generate de image with the watermark posted. The decoder process is the opposite it takes the image with or without the watermark and compares with the other image.

10.11228/dpsc.02.01.008

For this technique you can make an algorithm that helps you restrain and detect if people are stealing your content.

The watermark can also be used to content protection, when a content creator wants to sell his product, this technique can be used to protect the work. It can also be used, with some software, to limit the number of copies permitted. Every time a copy is made, the watermark can be modified by the hardware and at some point the hardware would not create any more copies of the data. An example is the digital video disc (DVD).

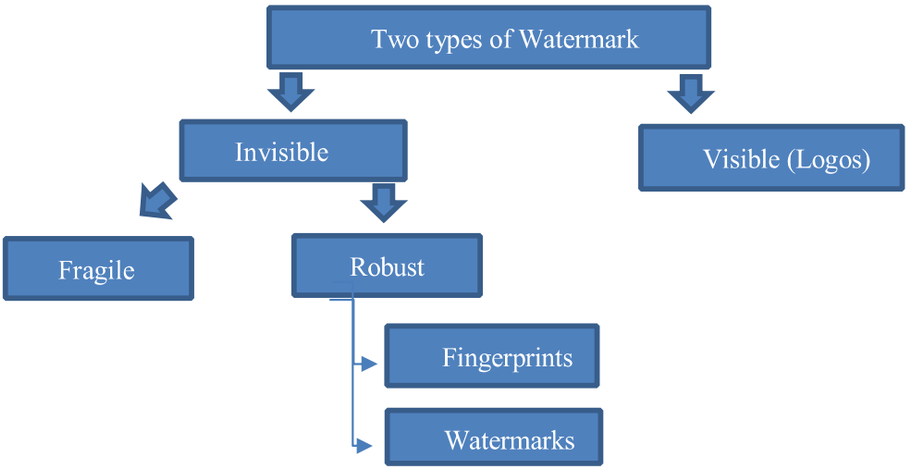

Fig 5. Representation the two types of Watermark

There are two types of watermark, the visible watermark corresponds to logos that you usually see during the video or an image, the invisible watermark corresponds to the watermark that are in embedded on the image that only with software can you see the watermark. In the invisible watermarks there are the fragile watermark which is used for detecting the smallest alteration of an image, while the robust watermark is specially designed to withstand a wide range of "attacks", which basically are trying to remove the watermark, but without destroying the image/video.

Fingerprinting is different of the basic watermark that embed information on the digital data, the fingerprinting analyses the image or video and determine the unique characteristics. These characteristics when are identified they are put on a database and then are use for recognizing the content in the future. Normally it only is few samples of the video that are store in the database because if it was a full video it would make a lot of samples that you would have to store, and it would make it heavier and take a lot of time to verify the fingerprint. The fingerprinting can be often use in forensics for detecting if the video footage was manipulated.

YouTube permit that content owners to fingerprint their own media and then upload to the database of YouTube. That way YouTube can compare with central fingerprinting database before the video can be viewed. If someone uploads a piece of content that its original owner requested be blocked, then YouTube will not allow this video to be shown. Copyright owners get to decide what happens when content in a video on

10.11228/dpsc.02.01.008

YouTube matches a work they own. They can block it, monetize the video by running ads against it or track the video's viewership statistics.

An easy way to watermark an image is to change the position of the pixels, that alone creates a new image. Digital Watermarking doesn't stop piracy but at least brings some protection for content holders and providers because it needs some knowledge to take the watermark out from an image or a video.

I decided to talk about watermarking because nowadays is very common to use this technique, for example on the platform YouTube there is a section that can create your watermark and you also can modify the watermark at your own taste.

There is also, to protect your own work, companies that takedown websites that use content that is not theirs, but those companies need proves that you are the content creator and for that you can use watermark as your evidence.

4.2 Protection of files

Nowadays streaming also has a big problem because there is no way to completely prevent online video from being stolen. If it can be viewed on a computer, it can be stolen. The best you can do is make it harder for thieves and minimize the number of times the video is stolen.

The transfer of media file from server to a client is termed as Progressive Download. There is low protection via Progressive Download, if it is used an embedded media player such as QuickTime or Windows Media player, the user can access the file directly by looking at the HTML code, by HTML code can be used to determine the location of the video file. To add a little security to progressive download, in the code the JavaScript should be on a JS file to be in a different location of the HTML file, so that becomes harder to thieves to find the files and you should use flash video because creates a SWF file that hides his location.

SWF file is an Adobe flash file format which contains videos and vector-based animations. The full abbreviation of SWF is Small Web Format but sometimes it is referred as Shockwave Format. SWF files are generally used for efficient delivery of multimedia contents over the web. This format can also contain ActionScript's, which come in handy in small web-based applications. This type of file is harder to open and see the information but only add a little security.

5 Conclusion

The objective of this paper is to present some tools to copyright protection and to bring some security to content holders.

With the advance of technology, it became easy for people to use other people content to their benefit, so that's why in this paper I present the DRM systems and watermarking. The DRM systems are more sophisticated but more secure that watermarking because DRM implements watermarking and more types of techniques to secure the

10.11228/dpsc.02.01.008

content but for DRM to work it needs to take control of the content as it is refereed in the paper.

Watermarking and Fingerprinting it's easier to implement and it is effective because removes many people for trying to steal content. With these techniques you can provide a secure environment for people to be in like YouTube.

The paper presents solutions for copyright, but the society will always be the factor that controls everything because there are always people that can break the barriers so it will depend of the ethic of the society.

Piracy will always exist no matter what because systems always have flaws.

References

1. Dan Jerker B. Svantesson & Stanley Greenstein (editors), Data protection vs. copyright, Internationalisation of Lawin the Digital Information Society, Nordic Yearbook of Law and Informatics 2010-2012, https://ssrn.com/abstract=2350131
2. copyright.gov,https://www.copyright.gov/help/faq/faq-duration.html,consulted 20/10/2019
3. Stanford University Libraries, https://fairuse.stanford.edu/overview/faqs/copyright-protection/,consulted 22/10/2019
4. M. Campidoglio, F. Frattolillo, F. Landolfi, The Copyright Protection Problem: Challenges and Suggestions, Publisher: IEEE, https://doi.org/10.1109/ICIW.2009.84 (2009)
5. Antoni Terra, Copyright Law and Digital Piracy: An Econometric Global Cross-national Study. North Carolina Journal of Law & Technology. 18. 69. , 2006
6. Mrs. D. Seema Dev Aksatha, MCA, M. Blessing Marshal, Software Piracy Protection, https://doi.org/10.31142/ijtsrd21705 (2019)
7. Thishya Weragoda, Pirates of the Internet: The Curse of the Digital Age" Balancing and Protecting the Rights of Music Owners and Music Users in the Digital Environment, https://www.academia.edu/38153599/_Pirates_of_the_Internet_The_Curse_of_the_Digital_Age_Balancing_and_Protecting_the_Rights_of_Music_Owners_and_Music_Users_in_the_Digital_Environment (2016)
8. Fe Angela M. Verzosa, Copyright Protection for Philippine Publications, In 12th Congress of Southeast Asian Librarian (CONSAL) on Information Resources Empowerment, Brunei Darussalam (Philippines),19-23 October 2003.[Conference paper], http://hdl.handle.net/10760/11219
9. Charles Duncan, Ed Barker, Peter Douglas, Martin Morrey, Charlotte Waelde, Digital Rights Management, https://www.academia.edu/567801/Digital_rights_management (2004)
10. Ahmed Gomaa, Global Music Asset Assurance Digital Currency : A DRM Solution for Streaming Content Using Blockchain, Conference: 6th International Conference of Advanced Computer Science & Information Technology, https://airccj.org/CSCP/vol8/csit88801.pdf (2018)
11. JULIA LAYTON, https://computer.howstuffworks.com/drm1.htm consulted 19/11/2019
12. S.R. Subramanya and B.K. Yi, Digital rights management, Publisher: IEEE, https://doi.org/10.1109/MP.2006.1649008 (2006)
13. Tarek Gaber, Digital Rights Management: Open Issues to Support E-Commerce, DOI: 10.4018/978-1-4666-3954-6.ch005 (2013)

10.11228/dpsc.02.01.008

14. Athanassios Skodras,Vassilis Fotopoulos, Decentralising the Digital Rights Management value chain by means of distributed license catalogues, Publisher: Springer Boston MA, https://doi.org/10.1007/0-387-34224-9_81
15. Timothy J. Wade and S.R. Subramanya, Digital Rights Management in 3D Printing: A Proposed Reference Architecture for Design-to-Fabrication Security and Licensing, https://www.academia.edu/33225875/Digital_Rights_Management_in_3D_Printing_A_Proposed_Reference_Architecture_for_Design-to-Fabrication_Security_and_Licensing

10.11228/dpsc.02.01.008