**ECP-2007-DILI-517006**

# EFG – The European Film Gateway

# M 5.4 Digital rights management and watermarking expression

| | |
|---|---|
| **Milestone number** | *M 5.4* |
| **Dissemination level** | *Public* |
| **Delivery date** | *31August 2010* |
| **Status** | *Final* |
| **Author(s)** | *Ñusta Nina (Eye Film Institute Netherlands)* |

***e*Content*plus***

This project is funded under the *e*Content*plus* programme,
a multiannual Community programme to make digital content in Europe more accessible, usable and exploitable.

## Table of Content

# 1 Introduction

This Milestone investigates the use of technical measures to protect archival content online. This report is a document of Work package 5 “IPR management and administration”.

During the research we found that most literature dealt with the more technical and mathematical aspects of protecting content and not so much the with legal aspects. After consulting the project leader of the European Film Gateway (Deutsches Filminstitut), it was decided not to go into the technical aspects in depth, due to the fact that the Work package deals with legal issues and not technical ones. For this reason, the explanation of the various forms of Digital Rights Management may be oversimplified from a technical perspective.

For this research, the European Film Gateway Consortium as well as the members of the Association des Cinémathèques Européennes (ACE) were consulted regarding their experiences with technical protection measures and digital rights management.

# 2 Technical Protection Measures

Technical protection measures have been heralded as the solution for the illegal distribution of media files. They were developed to enable secure distribution of content and came into use in the mid 1990s. A common type of technical protection is Digital Rights Management (DRM), which uses control techniques on the access to digital content or on the use of content. In this chapter, the technical aspects will only be addressed briefly before presenting the several forms of technical protection measures and their practical use.

## *2.1 Lessons Learned From the Music Industry*

In order to stop the widespread sharing of music files, the music industry has been using technical protective measures some time. DRM can control the access to content, an example is the DRM used to protect CDs.

DRM is the catch-all term for any technique to secure the access and use of digital content. The emergence of the internet and file-sharing has made copyright infringement of music common practice. In the past, the music industry focused on improving physical formats for the distribution of music: from vinyl records to cassette to compact disc. The MP3-format has made the distribution of music files far more easy than it had ever been before; anyone can share music online with the ease of a mouse-click. The music industry did not offer the digital distribution of legal MP3s until after the market was flooded by illegal MP3s: i-Tunes was launched in 2003 but MP3s had been available since 1997 already. Consumers had already created networks for distribution themselves via peer-2-peer-networks.

In 2000, the first audio CDs with playback restrictions were released: these CDs could only be played on audio CD-players and were unusable once inserted into CD-Rom drives. The aim of copy protection was to prevent digital audio extraction to limit the file-sharing of ripped music. Consumers were not happy with the limited use copy protected CDs offered: people were neither able to make a private copy of the CD for their own use, nor could they transfer MP3s to their MP3-player.

The music industry abandoned the use of copy protection on audio CDs in 2006. No official press releases were sent out, providing reasons for no longer continuing with this form of DRM. It is safe to say that copy protection did not prevent the enormous growth of file-sharing, the protection was cracked continuously and audio-files were still being made available online.[1]

[1] Halderman, John A. , Evaluating new copy-prevention techniques for audio CDs, In Proceedings of the 2002 ACM Workshop on Digital Rights Management, Washington D.C., 2002.

## *2.2 Digital Watermarking*

Watermarks first appeared in the paper industry in Italy in the 13th century. The purpose of those watermarks is not clear and several theories exist: from signs containing secret messages to watermarks as a way of showing the craftsmanship of the papermaker.[2] Watermarks could also have been utilised to denote in which paper mill a work had been made: that way the papermakers could distinguish which was their own product. Nowadays one can see paper watermarks on a daily basis; e.g. on banknotes.

Digital watermarking was inspired by this tradition of paper-watermarking. Digital watermarks are designed for copyright protection and data-control and are part of DRM-mechanisms.[3] Watermarking can embed rights information into media files. Watermarks exist in various types:

### 2.2.1Perceptible/Imperceptible

Perceptible watermarks are visible to anyone who sees the watermarked items, which are often digital images. Perceptible watermarks can visibly show who the owner of a work is, and make it less attractive to commercially exploit a work at the same time. This is both the strength and the weakness of the perceptible watermark: The incentive to remove perceptible watermarks is far greater than the removal of imperceptible watermarks; visible watermarks distort the image and are visually unattractive.


*Perceptible watermark by Getty Images*

[2] For more information on the history and origin of watermarks please refer to http://www.kunstpedia.com/articles/454/1/History-of-Watermarks/Page1.html

[3] See the paragraph on Digital Cinema in which watermarking is combined with encryption to prevent and discourage piracy.

Imperceptible watermarks are embedded into the data of the digital image and are not visible to the naked eye. Imperceptible watermarks can be extracted via software; anyone wanting to check whether their audiovisual works are being used would need to run specific watermark extracting software to determine whether or not an image is theirs. Imperceptible watermarks do not discourage the use of the work such as perceptible watermarks do, but can be more helpful to identify the origin of the image.

### 2.2.2Robust/ Fragile

For watermarks to resist acts of removal – in literature this is often referred to as “attacks” – the watermark needs to be secure or robust. But a watermark should also be able to remain intact after normal image processing, such as scaling, cropping and compressing. The more fragile a watermark is, the less effort it takes to remove it. Creating a robust imperceptible watermark, however, has proven to be challenging.[4]

The benefit of fragile watermarks is that they are easily damaged or removed, and therefore it is easy to detect whether or not a certain image has been altered. Again, the original image should always be compared to all other images.

### 2.2.3 Spatial Domain-Based Versus Frequency Domain-Based

Watermarks can be embedded into the spatial domain and/or the frequency domain of the image. Adding the watermark to the spatial domain has the advantage of low complexity and easy implementation, a negative aspect is that the watermark may be easily detected using computer analysis as well as removed.

Entering the watermarking data into the frequency domain makes the watermark more robust, however, adding too much data into the frequency domain may have negative effects on the quality of the image.

### 2.2.4 Drawbacks to Digital Watermarking

Visible watermarks have the aim to show the origin of the content, for example they can display the name of the copyright holder or the institution that makes the content available online. A visible watermark distorts the image; invisible watermarks are embedded in the image data itself. While visible watermarks can be seen by anyone, invisible watermarks can only be traced via computers.

Watermarks do not prevent copying of content; they can only identify the right holder of the content. Use of the content still needs to be monitored to end copyright infringement. This is time-consuming and also requires active tracking down of copyright infringers.

[4] Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich and Ton Kalker, "Digital Watermarking and Steganography" (Second Edition), Morgan Kaufmann, 2008

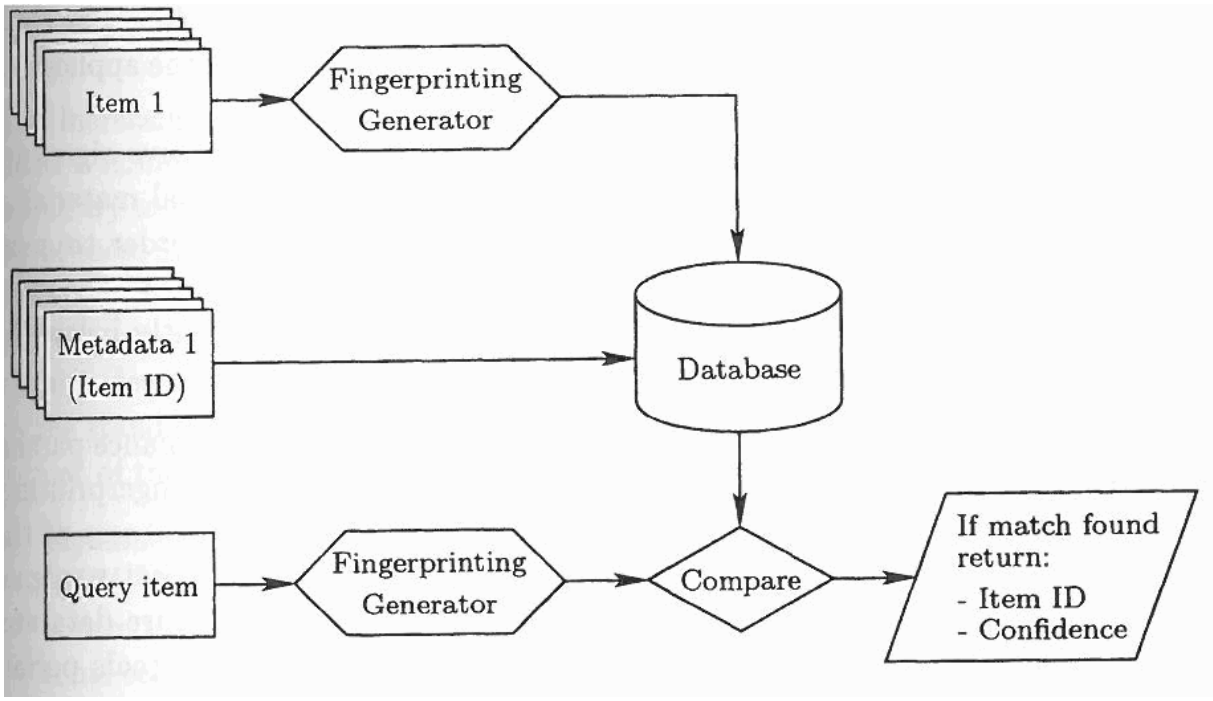
There are free watermarking programmes available online, however, from the survey, which was sent to ACE-members and members of the EFG Consortium, it came forth that none of them has had experience with these programmes.

### 2.2.5 Watermarking Software

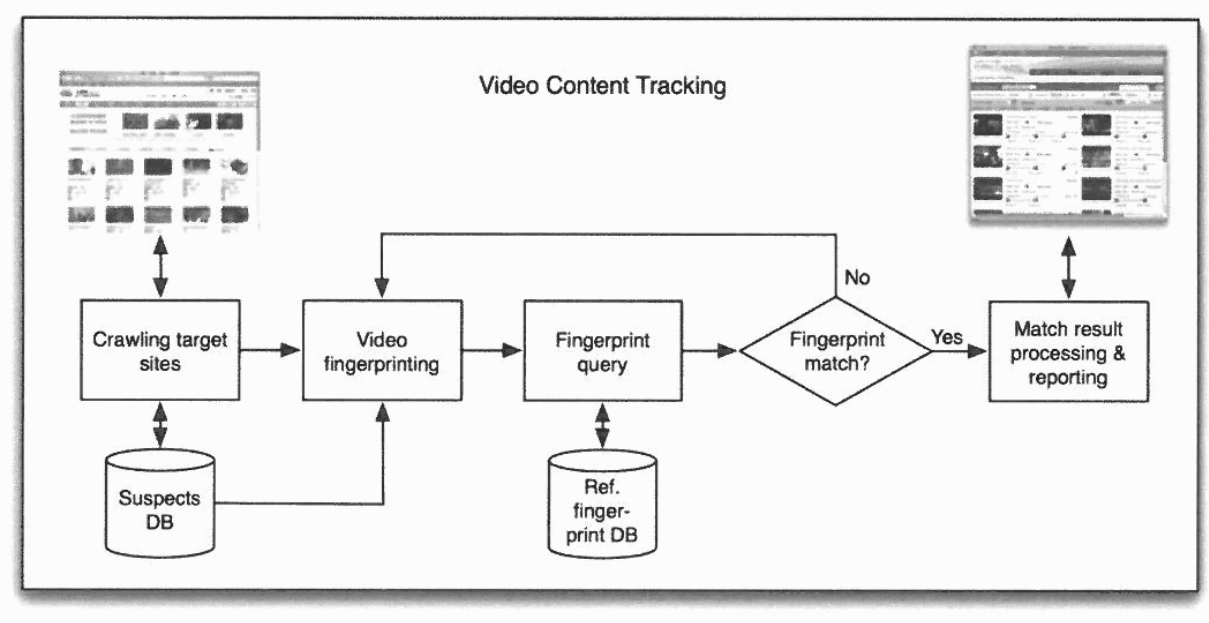
Visible watermarking is simply an overlayed information such as an image or text over the running video. To put an overlay over a respective movie, software or hardware can be used. There are quite a number of different watermarking softwares on the market, part of which are freeware. As it would go beyond the scope of this report, only a small selection of freeware tools will be named, without applying a special recommendation to use one of them:

## *2.3 (Video) Fingerprinting*

Video fingerprinting is a technique in which software extracts characteristic components of a video file. The characteristics can be both visual as well as audio. The fingerprints are highly compressed files and can be stored in databases for comparison.



In contrast to watermarks, fingerprints are not embedded into the audiovisual material. Fingerprinting does not require any modification of the original content. This technique can be used to identify content as your own, in combination with a web crawler[5] it can be used for locating pirated material online.




**Video Content Tracking[6]**

Similar to a human fingerprint, a video fingerprint can identify from which original source a segment was taken from. Video fingerprints are stored in a database and compared to material which needs to be identified. It is often used in broadcasting to track the airing of television programmes and commercials. In contrast to perceptible watermarks, fingerprinting does not visually prevent unlawful use of content.

### 2.3.1 Audio ID/Video ID

YouTube uses video fingerprinting in their video identification system to detect infringing content uploaded by users. YouTube has faced, and is currently facing various lawsuits concerning copyright infringement.[7] Google, the owner of YouTube, has developed Audio ID and Video ID. Right holders can provide fingerprints of content to YouTube, and these are automatically scanned when a user uploads a video. Right holders can indicate whether they want to block the matched content, or they want to allow it but only alongside advertisement. In this way right holders are able to generate income from leaving uploaded videos on YouTube for users to watch.[8]

[5] A web crawler is a computer-programme which browses through websites, they are often used by search-engines (such as Google, Yahoo etc). (unvollständig, daher gelöscht)
[6] Figure taken from Lu, Jian, Video fingerprinting for copy identification: from research to industry applications, 2009
[7] Google is currently being sued by Viacom, for infringing copyright by allegedly not taking down infringing content quickly enough: http://www.usatoday.com/communities/technologylive/post/2010/03/media-morning-the-juicy-details-behind-the-viacom-youtube-lawsuit/1
[8] http://www.guardian.co.uk/technology/2009/nov/01/google-youtube-monetise-content.

### 2.3.2 Ina Signature Project

The Institut national de l'audiovisuel (Ina) has developed their own fingerprinting system to monitor and manage audiovisual content online. Signature[9] was developed by Ina for monitoring the use of their material on television, and has now progressed to the online environment. Signature makes it possible to automatically generate detection reports.

This fingerprinting system is currently being used by Ina, Canal+ and the user-generated content website Dailymotion.[10] Dailymotion lost a court case regarding the making available of copyrighted content and was ordered to pay damages.[11] To prevent any copyright infringement in the future, Dailymotion has already invested thirty four million dollars in content screening technologies.[12]

### 2.3.3 Drawbacks to Fingerprinting

Similar to watermarking, fingerprinting does not prevent the use of the content. Fingerprinting also needs active monitoring: the fingerprints are stored in a database and content can be matched to this database. This technique also requires active monitoring, for online use it can be managed via a web-crawler. This protection measure has similar drawbacks as watermarking.

## *2.4 Encryption*

Encryption is a method of making data unreadable via cryptography, through a specific algorithm (cipher). The only way to make the data comprehensible is by using a specific key which makes it possible to decrypt encrypted data. This technique was first used for secret communication during wars, but is now being used to encrypt all sorts of data. It is now also a method to protect content online.

### 2.4.1 Filmotech.nl

The Dutch mass digitisation project, "Images for the future", will be offering their content as video on demand on the portal Filmotech.nl. The majority of the content is still copyright protected, so licenses are being obtained to make the work available online. Right holders are often rather hesitant to disclose their materials online, due to the ease materials can be distributed without prior authorisation. Filmotech.nl will stream video-on-demand in various resolutions, and this will done via a flash-player,customised with the Filmotech-logo. The content can only be streamed with the player, so no visual watermarks need to be implemented in the audiovisual material; the logo of the website will always be visible on the player itself. This solution could resolve the need for archives to be named as

[9] See also www.ina.fr/signature
[10] See: http://www.dailymotion.com/gb/legal/contentprotection
[11] http://mashable.com/2007/07/17/dailymotion-loses-in-court/
[12] http://mashable.com/2007/10/18/dailymotion-ina/

the source of the audiovisual material, which has proven to be a challenge online. On Filmotech.nl the audiovisual material will be streamed using RTMPE (real time protocol encryption)[13]. The stream is encrypted between the server and the client and sent over a secure tunnel.

### 2.4.2 Drawbacks to Encryption

Encryption can be cracked, it only takes one key which will fit on encrypted data which has been encrypted by the same cipher. If the encryption is advanced, it will of course take more time to find the adequate key. However, Hackers do help each other online in cracking this type of copy protection.[14]

### 2.4.3 Digital Cinema

Although digital cinema is mostly about making feature films available offline , it is worth mentioning how major studios are currently offering their content to theatres. Metro-Goldwyn-Mayer, Paramount Pictures, Sony Pictures Entertainment, 20th Century Fox, Universal Studios, The Walt Disney Company and Warner Brothers started the Digital Cinema Initiatives (DCI) in 2001. The aim of DCI is to create specifications which make digital cinema possible. Digital cinema comprises the distribution of a film in digital format and projection via a digital projector.

Very often motion pictures are released in a staggered manner: copies of the film are sent from country to country. A drawback to this form of release is that pirated copies are able to flood the market before a film is released in cinemas: for instance someone in the USA could be filming in the actual cinema and put this recording online. Thus, the recording can be available to European audiences, where the film has yet to be released. Digital technology enables films to be distributed and projected swift and easily, making a worldwide release more easily possible than it was in the analogue era.

Mostly prior to distribution films are encrypted, and sent to cinemas via hard-discs or electronically (via satellite). The encrypted film is stored on the server of the cinema and should be decrypted and decompressed before it is able to be viewed, which can be done on the server or in the digital projector itself.

To tackle the recording of films in the cinemas itself, watermarking is used. In the watermark, details about the location of screening can be added. This can help to determine where the pirated copy has been recorded and copyright holders may contact the cinema in question to prevent any further illicit recording in their screening rooms. Again watermarking cannot prevent theft, but it can discourage piracy by keeping track of the sources of pirated copies online.[15]

[13] See for more information: http://www.adobe.com/devnet/flashmediaserver/articles/protecting_video_rtmpe.html
[14] An example of a resource for hacking encryption http://www.mycrypto.net/encryption/encryption_crack.html
[15] Bloom, Jeffrey A, Security and rights management in Digital Cinema, IEEE 2003

*Eye* Film Institute Netherlands is currently one of the initiators of the "Project Digitisation Dutch Cinema" which focuses on making digital cinema available in the Netherlands. In this initiative distributors, producers and cinema-owners are co-operating to research in which way digital cinema can be implemented in Dutch cinemas.[16]

## *2.5 Legal Basis for Digital Rights Management*

Directive 2001/29/EC harmonises certain aspects of copyright and related rights in the information society. In this Directive chapter three is devoted entirely to the protection of technical measures and rights management information. The European Union is of the opinion that the protection of technological measures should ensure a secure environment for the making available of on-demand services, so that members of the public may access works online.[17] In this Directive it is acknowledged that right holders may need to use technological measures to prevent copyright-infringement.
Article 6 obligates Member States to provide adequate legal protection against the circumvention of any effective technological measures, as well as against the removal of electronic rights-management information. This information can consist of:

- Author or right holders
- Information about the terms and conditions of use of the work
- Any numbers or codes that represent such information[18]

There has been some criticism of the wording of these articles, commentators have noted that some terms were too vague and not narrowly defined enough.

[16] http://www.eyefilm.nl/en/node/324
[17] (53) Directive 2001/29/EC
[18] Article 7 of Directive 2001/29/EC

# 3 Conclusion

A survey was sent out to ACE-members in April 2010, to gain more insight in the policy of audiovisual archives with regards to copy protection. From the results of the survey we can establish that up until now not many archives have implemented any copy-restrictions on content which they provide online.

Often archives find that their content has been uploaded on user generated content-sites such as YouTube, without reference to their archive. As many archives would like to be credited when their content is published online; a visual watermark could improve their visibility. Our partners Cineteca di Bologna, Cinecitta Luce and the Cinemateca Portuguesa are using visible watermarks for their content to prevent commercial use of the works they make available online.

From the survey it came forth that archives do not have the resources to invest in the rather costly managing and monitoring of their content. They are also rather ambivalent to internet piracy: there usually is only a little chance to prevent the spreading of illegally copied works on the long run, as opposed to considerable costs for following up these matters.[19] Therefore archives prefer to offer their content online at a low-resolution for free, instead of investing in DRM. This investment would often also entail that a fee would have to be asked for viewing the content to compensate for the investment made to protect the content itself.

One should also wonder whether archives should want to close-off their content, when offered online. A combination of perhaps offering low-resolution content for free without any form of protection can be combined with a commercial platform which may offer high-resolution audiovisual material online for a fee. For examples of cultural institutions who are exploring such combinations, please refer to Milestone 5.3 “Open Content Models”. Cinecitta Luce and the Danish Film Institute both offer content online at low-resolution, the latter offers high resolution films on their video-on-demand website for a fee.[20] The Hungarian National Film Archive will be offering their photograph collection at a low resolution, following the example set by the Hungarian Photo Museum.[21]

The weakness of technical protective measures is that they can be circumvented or copy protection can be broken. Only one pirated copy is needed to be distributed in enormous volumes. Anyone who is determined enough and capable will be able to circumvent the implemented copy protection.

The music industry tried to discourage illegal copying by introducing copy protection; however they did not prevent the ripping of music from compact discs. EMI and Sony both stopped adding copy protection to compact discs in 2006.[22] iTunes has been DRM-free since 2009.[23]

[19] According to Martina Werth-Müller, Bundesarchiv-Filmarchiv
[20] See www.filmstriben.dk
[21] Fort he online collection of the Hungarian Photomuseum please see: http://fotomuzeum.hu/hu
[22] EMI Group and Sony BMG both used the Copy Control-system to prevent the copying of audio-cds. Many consumers complained of not being able to play the CDs in CDplayers or their pc’s.

Implementing technical protective measures is costly. Almost every measure can be circumvented or broken: it is prohibited to perform these acts, however illegally copied material is still being made available online. The music industry themselves are also no longer using DRM. Watermarking and fingerprinting both require active monitoring, which also adds costs. Infringing content must be detected online and action has to be taken to stop infringement. Many archives have opted not to implement technical protective measures. A common viewpoint is that effective protection of commercially less attractive content is too costly to outweigh the consequences of possible piracy.

On a final note, there are various archives that do not want to use any form of copy-protection on their publications online. They feel it is the task of the archive to disclose their collection to the public and not restrict its access via technical protection measures.

[23] For a statement from Apple on making Itunes DRM-free please see:
http://www.apple.com/pr/library/2009/01/06itunes.html

# Bibliography

Becker Eberhard, Buhse Willms, Günnewig Dirk, Rump Niels, *Digtal Rights Management: technological, economic, legal and political aspects*, Springer-Verlag, Berlin Heidelberg, 2003

Bloom, Jeffrey A, *Security and rights management in Digital Cinema*, IEEE 2003

Dittmann, Jana & Nack, Frank, *Copyright-Copywrong*, IEEE Multimedia, vol 7, no.4, Oct.-Dec. 2000, p. 14-17

Eskicioglu, A.M.et al., *Security of digital entertainment content from creation to consumption*, Signal Processing: Image Communication 18, 2003, p. 237-262

Gillespie, Tarleton, *Wired Shut: Copyright and the shape of digital culture*, The MIT Press, 2007

Guibault, Lucie et al., *Study on the implementation and effect in Member States'laws of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society,* Insitute for Information Law, University of Amsterdam, The Netherlands February 2007

Helberger, Natali, *Digital Rights Management from a consumer's perspective*, IRIS plus; supplement to IRIS, Legal Observations of the European Audiovisual Observatory, Issue 2005-08, p 1-8

Helberger, Natali et al., Digital Rights Management and consumer acceptability: a multi-disciplinary discussion of consumer concerns and expectations, Indicare-project, December 2004

Hugenholtz, P.B., *Toegang tot de bron: het auteursrecht en het internet*, Ars Aequi, july/august 2008, p. 581-588

Jobs, Steve, Thoughts on music, Apple Inc. 2007 published on http://www.apple.com/hotnews/thoughtsonmusic/

Kunder, Deepa & Karthik, Kannan, *Video Fingerprinting and Encryption Principles for Digital Rights Management*, Proceedings of the IEEE, Vol. 92, No.6, June 2004

Shih, Frank Y., *Digital watermarking and steganography: fundamentals and techniques*, Talylor & Francis Group, Boca Raton, 2008