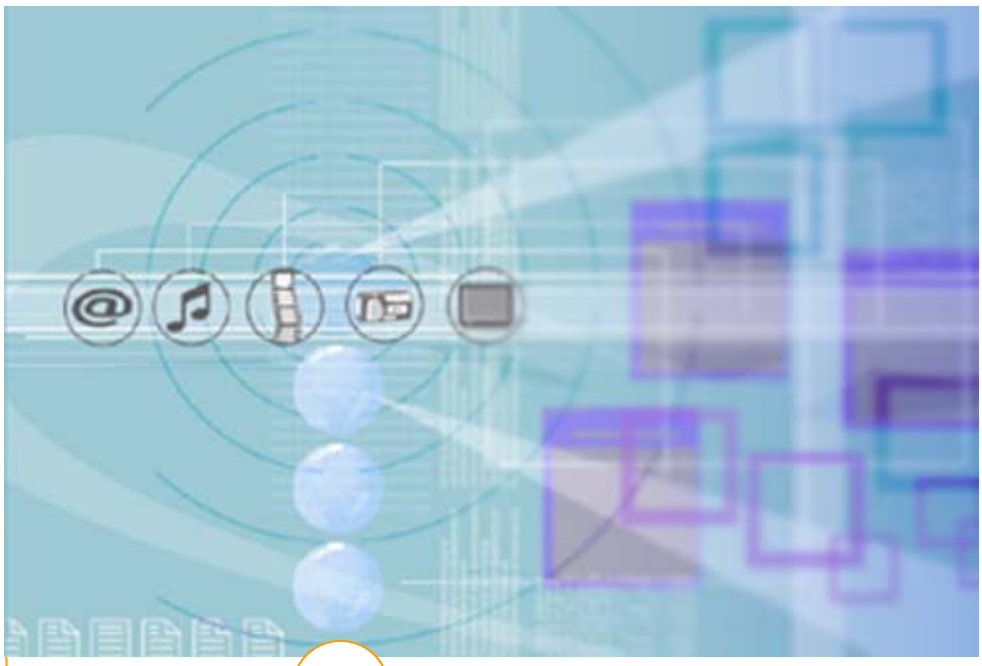


Technical aspects of Digital Rights Management

Emilija Arsenova
MI, RWTH-Aachen

Table of content

1 Introduction

Shifting from traditional content, such as paper documents, to digital media is due to several advantages of digital media over the traditional media. Digital content (audio, video, graphics, and images) can be easily copied, transmitted and distributed over networks. The expansion of the Internet, making it the most powerful toll for information exchange today, as well as the numerous file sharing tools have made the distribution of copyrighted digital media files simple nowadays. A very important aspect of why digital media is superior compared to analog is the improved quality. Analog media looses quality with each copy generation, and often even during normal use.

Exact copies of digital data can be easily made. On one hand this represents a very important property, but on the other it also creates a problem as copies cannot be distinguished from the original. This is one of the main factors which hinders the growth of multimedia networked services because it has a negative impact on the willingness of authors, publishers and providers of multimedia data to endorse distribution of their documents in a networked environment. Easy reproduction of digital data in their exact original form is likely to encourage problems such as copyright violation, unauthorized use and abuse. This is perceived by many as a threat to the content value, particularly in the music and movie industries. It prevents digital media publishers from receiving payment for each copy made out of a digital work, or for example for each time a video is played on a TV or radio channel.
Although online content is protected by copyright laws, policing the Web and identifying and punishing law-breakers is very difficult. The need of a technology that will focus on making it impossible to steal Web content in the first place, is becoming more and more obvious.

2 Digital Rights Management (DRM)

Digital Rights Management is important to creators and publishers of electronic media since it helps ensure profits for their products. Since the advent of personal computers, it has become easy to copy digital media files in an unlimited number of times and at the same time maintaining the same quality level in each subsequent copy. By controlling the trade, protection, monitoring, and tracking of digital media, DRM helps publishers limit the illegal circulation of copyrighted works. Typically, a DRM system protects intellectual property by either encrypting the data so that it can only be accessed by authorized users or marking the content with a digital watermark, so that the content can not be freely distributed. Whatever method publishers choose to deploy, DRM ensures that their digital content is only used by those who have paid for it and have thus gained the right a DRM system protects intellectual property by either encrypting the data so that it can only be accessed by authorized users or marking the content with a digital watermark, so that the content can not be freely distributed. In this sense, DRM represents a concept for managing and controlling the access and utilization of digital

assets. As the name itself implies, it is solely applicable to digital media (and analog media that has been released in digital form).
Digital rights management is sometimes referred to as digital *restriction* management. The latter was given by users who had negative experience with DRM and consider the DRM systems to be nothing else than systems that obstruct them from doing things they feel they have a right to do or violating their privacy by insisting on their identification before they do them. The main conflict is arising from the actual concept of DRM and its purpose. The word 'rights' implies that these measures are enforcing legal rights of a publisher or owner of intellectual property. The publishers and creators of intellectual property, including software, movies, and music, have rights that can and should be enforced [1]. In general, however, the purpose of DRM is perceived as a way of preventing people via technological means from using copyrighted material in ways that are unacceptable to the publisher. In some countries, including the United States, bypassing DRM is almost always a crime, no matter how unreasonable are the restrictions it imposes.
It is important to consider the user's points of view in order to understand the benefits, as well as the various problems and conflicts that the DRM systems lead to.

2.1 DRM Architecture

There is no standard DRM architecture – there are many different frameworks offered by different vendors. The overall functional DRM framework presented in Fig.1 is suited to building digital rights-enabled systems [2].

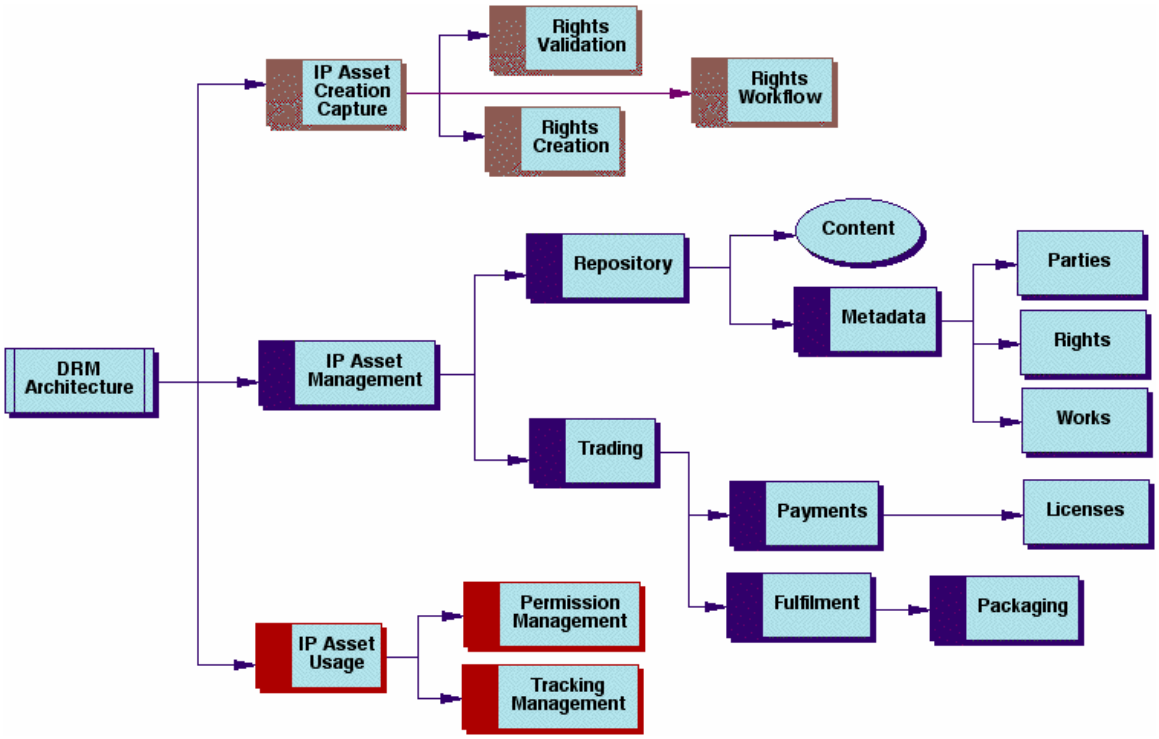


Fig. 1 DRM functional architecture

The DRM framework can be modeled in three areas:

Intellectual Property (IP) Asset Creation and Capture: refers to the process of managing and creation of content in order to simplify its trading. This includes asserting rights when content is created for the first time (or reused and extended with appropriate rights to do so) by various content creators/providers.
This module supports:

- Rights Validation: ensuring that content being created from existing content includes the rights to do so.
- Rights Creation: allowing rights to be assigned to new content, such as specifying the rights owners and allowable usage permissions.
- Rights Workflow: allowing for content to be processed through a series of workflow steps for review and/or approval of rights (and content).

IP Asset Management: refers to the process of managing and enablement the trade of content. This includes receiving content from creators and using it as an input for an asset management system. The data managed in this system includes the descriptive metadata and rights metadata (e.g., parties, usages, payments, etc.).
This module supports:

- Repository functions**:** enabling the access/retrieval of content in potentially distributed databases and the access/retrieval of metadata. The metadata covers Parties, Rights and descriptions of the Works.
- Trading functions: enabling the issuing of licenses to parties who have traded agreements for rights over content.

IP Asset Usage: refers to the process of usage of content after it has been traded. This includes supporting constraints over traded content in specific desktop systems/software.
The IP Asset Usage module supports:

- Permissions Management: enabling enforcement of the rights associated with the content in the usage environment (e.g. if the user only has the right to view the document, then printing will not be allowed).
- Tracking Management: enabling the monitoring of the usage of content where such tracking is part of the agreed to license conditions (e.g., the user has a license to play a video ten times).

Together, these three modules provide the core functionality for DRM systems.

2.2 DRM Techniques

DRM systems typically include the following techniques:

- Encryption
- Public / private keys
- Digital certificates

- Watermarking
- Access control
- Secure communications protocols
- Fingerprinting
- Rights specification language
- Trust infrastructure
- Hashing

Encryption

DRM uses a cryptographic algorithm to encrypt content that needs a secret key - a particular phrase or string of numbers. Only the holder(s) of this key can later unlock the content and read it. The algorithm ‘scrambles’ data hence making it unreadable to everyone except the recipient (for ex. secure sites use encryption). Decryption is the process of decoding data that has been *encrypted* into a secret format and it requires a secret *key* or *password*. However, encrypting the content is merely one of the important aspects of securing the data. Another very important aspect is managing the decryption key. The creation of the key, its transferring to the customers, ways of enforcing time limitations (for ex. making the software license valid only for 3 months) and preventing theft or transfer of a key are the properties of the encryption that have to be considered at all times.
In summary, encryption is the technology that supports electronic document management and control. It must be noted that great care need to be undertaken in its implementation in order to comply with the security standards foreseen to be met.

Public / private keys

They belong to a family of cryptographic techniques that make use of the one-way nature of certain mathematical functions, resulting in a system where two separate keys are used. They are usually called "public" and "private" keys and each key can be used to encrypt or decrypt data. If one of the keys is used to encrypt content then the other one must be used to decrypt it, and knowing one key does help in discovering the other. That key can enable reading messages sent by the sender, or encrypt messages that only the sender can read; only the sender can create messages using private key. Asymmetric cryptography is extremely powerful; it can provide functions in addition to confidentiality (such as digital signatures), and is highly appreciated in large user communities. However it is also extremely compute-intensive. This is why in practical systems such as SSL and most DRM systems it is usually used in combination with symmetric cryptography, also known as "secret key" cryptography. It belongs to a family of cryptographic techniques where the same key is used to both encrypt and decrypt messages. The main weakness of this type of cryptography is in key management.

Digital certificates

Similar to the physical reality where a person has to identify himself upon payment, a person has to prove his virtual identity in the e-market with the help of a *digital certificate*. A digital certificate is actually the link between the person and his virtual

identity. It is created using a cryptographic technique that connects a person's identity with his/her public cryptographic key. The digital signatures are issued by ***certificate authorities*** that offer guarantees that the public key belongs to the person whose name is in the certificate.

Watermarking

Watermarking is the process of secretly embedding information into a data source in such a way its very existence is hidden. In digital sense, it represents a method of embedding a copyright stamp into an image, sound or a video. The watermark is embedded in a way that the quality of the host media is practically maintained and it cannot be captured by a human eye (for images) or ear (for audio content). Only the knowledge of a secret key allows extracting the watermark from the original image.

Access control

Copy protection attempts to find ways for limiting the access to copyrighted material and/or inhibiting the copy process itself. Examples of copy protection include encrypted digital TV broadcast, access controls to copyrighted software through the use of license servers and technical copy protection mechanisms on the media. DRM systems not only have to provide prevention from copying, but also access control. This way intellectual property will be protected by, for example, encrypting the data so that they can only be accessed by authorized users.

Secure communications protocols

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are cryptographic protocols that provide secure communications on the Internet. The protocols allow client/server applications to communicate in a way designed to prevent eavesdropping (intercepting of conversations by unintended recipients), tampering and message forgery.
IPsec (short for IP security) is a standard for securing Internet Protocol (IP) communications by encrypting and/or authenticating all IP packets. IPsec provides security at the network layer.

Fingerprinting

Another method to protect digital media is to fingerprint each copy with the purchaser's information. If the purchaser makes illegitimate copies, they will contain his name. Fingerprints present an extension to watermarking and can be both visible and invisible.

Rights specification language

Rights Specification Language presents the mechanism for describing the author or publisher rights. This data dictionary of rights terms gives a standard vocabulary to describe the DRM and other relevant issues.

Trust infrastructure

To support the market, DRM has to do more than simply provide a secure package containing content and accompanying metadata. DRM must also support transport of this package from the author and through the market all the way to the consumer. The term "trust infrastructure" refers to the technologies that support transport, opening, displaying and disposing the package.

Hashing

DRM can protect the digital content from being manipulated by using a so called *one-way hash function*. A one-way hash function takes digital content of any length as input and produces an output message called a *message digest*. Any change to the content will produce a completely different message digest. Upon purchasing a digital content on the WEB, in presence of a doubt a customer should be able to check if the content is authentic by performing the one-way hash function and comparing his result with the message digest provided to him from the content provider. If both outputs are the same, the customer can be sure that the obtained content has not been tampered and is authentic.

2.3 DRM goals

The DRM systems must have and achieve certain goals in order to give a trusted platform for users who want to participate in the e-market. These goals also have to be advantageous to content providers, who have to trust the system and get assurances that they will be properly compensated if they release content into the market. DRM systems should also assure the authenticity of every content they provide the customers with. DRM will enable a robust digital content e-commerce by accomplishing the following goals:

1. ***DRM should provide protection of digital content***. This type of protection is typically provided by the encrypting technique, which enables authors and publishers to send digital content across an unsecured network, such as the Internet; this way the content can only be read by the intended recipients.
2. ***DRM should enable secure distribution***. Once the content is protected via DRM encryption, the proper key is needed to decrypt the content and make it readable. Without this key, the file is useless. Anyone can have access to the encrypted content, but it will be of no use without the decryption key. Today, 128-256 bit keys are in common use and they are resistant to attack.
3. ***DRM should ensure content authenticity*.** Nowadays a one-way hash function is most widely used in order to provide this functionality.
4. ***DRM should provide for transaction non-repudiation*.** Both in the physical and electronic world, it is important for participants to be able to prove that any given transaction actually took place. In the physical market, the customers would receive a receipt which will be sufficient as a proof of payment. The

analogy to the above in the digital world is the **digital signature**. Two keys are used:

a. A *private key*, which is owned by a transaction participant and kept secret. A participant "signs" the transaction when he encrypts a part of it with his private key.
b. If someone would like to verify the authenticity of the transaction, he 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. ***DRM should support participant identification.*** In order to identify a participant, *digital certificates* are necessary. They prove the connection between the person in the physical world and other personal information provided by this person (for example on the Internet).

3 Watermarks

The watermarking technique takes its name from the watermarking of paper as a security measure, where the paper producer would stamp its logo on the paper. *Digital* watermarking protects digital documents against unauthorized use and distribution. This method however does not prevent copying; what it does is it embeds hidden information, which becomes inseparable with the watermarked data, even after copying and redistribution. Digital watermarking can be applied to digital audio, video, image signals and documents. For images, the hidden information can be a picture (e.g. publisher's logo, carrying copyright information) or it can be a group of bits spread around the image according to a certain algorithm.

A motivation for the use of watermarking techniques are the numerous properties of digital media, that make copyrights violations easy. The simple replication and transmission, as well as file sharing, are just some examples. The major problem for the content providers is the possibility of generating exact copies of digital data. With the dissemination of the World Wide Web, authors of digital media have at their disposal inexpensive means to distribute their works to a much broader audience. Many authors are skeptical when it comes to distributing their works, fearing that it may be copied illegally or that someone else might claim the copyright for works they have not created. Digital watermarks provide means of inserting additional information within the digital media, thus if copies are made, the rightful ownership can be determined. This makes watermarking an effective technology that solves many problems within a digitisation project. By embedding intellectual property data (e.g. the creator, licence model, creation date or other copyright information) within the digital object, the digitiser can demonstrate who the creator is and disseminate this information with each copy, even when the digital object has been uploaded to a third party site. It can also be used to determine if a work has been tampered with or copied.
A watermark is designed to permanently reside in the host data, which enables preservation of the digital data value. In the sections below, the focus will be put on watermarking techniques for images as a media type.

3.1 Different Types of Watermarks

This section describes some of the current types of watermarks, and defines some commonly used watermarking terms. The list below shows some of the different types of watermarks that have been developed in the past few years:

- ***Visible*** watermarks are designed to be easily seen by the viewer, and clearly identify the owner (Fig.2). However, the watermark must not affect the image content itself.
- ***Invisible*** watermarks are imperceptible under normal viewing conditions. Invisible watermarking is a branch of the growing discipline of "data hiding" or steganography. Multimedia objects, particularly sounds and images, inevitably contain bits which can be altered unnoticeably, and this can be exploited in many different ways to encode external information within the object, below the level of

audible or visual detection. However, embedding information in the least significant bits, by taking into account for the human visual system properties, is not resistant to image compressions, as they are also focusing on these bits. These bits will be removed in order to compress the image, as compression techniques are also exploiting the bits that are least noticeable to the human eye.

Fig.2 An example for visible watermarking (‘Lena’) [3]

- A watermark may be ***fragile*** or ***robust***. Fragile watermarks are designed to be distorted or "broken" under the slightest changes to the image. Robust watermarks survive severe signal processing attacks (compression, rescaling, etc.) on an image. The aims of such watermarks are completely different: a fragile watermarking scheme should be able to detect any change in the signal and identify where it has taken place and possibly what the signal was before modification. It serves for proving the authenticity of a document. On the opposite, a robust watermark should be stuck to the document it has been embedded in, in such a way that any signal transform of reasonable strength cannot remove the watermark. Hence, a pirate willing to remove the watermark

will not succeed unless they degrade the document too much so it is no longer of commercial interest.

- ***Blind*** watermarking techniques can perform verification of the mark without use of the original image. Other techniques rely on the original to detect the watermark and these are so-called ***non-blind*** watermarking techniques. ***Semi-blind*** watermarking techniques do not use the original signal but some side information and/or the original watermark.

3.2 Requirements of an ideal watermarking system

The most important requirement would be **imperceptibility**. If the watermarking system distorts the cover image to the point of being useless, or even highly distracting, it will not serve its main purpose. Ideally the watermarked imaged should be indistinguishable from the original, preferably even on the highest quality equipment.

The ideal watermark must also be highly **robust**, entirely resistant to distortion introduced during either normal use (unintentional attack), or a deliberate attempt to disable or remove the watermark present (intentional, or malicious attack). In malicious attacks, an attacker deliberately tries to disable the watermark, often through a geometric distortion or the addition of noise. Unintentional attacks involve transforms that are commonly applied to images during normal use, such as cropping, resizing, contrast enhancement and etc.

The most interesting form of unintentional attack is that of **image compression**. As already pointed out, watermarking aims at encoding information in extra bits that compression hopes to remove. Thus, ideal watermarking and compression systems are most likely essentially exclusive.

Slightly less important requirements of an ideal watermarking system are **capacity** and **speed**. As for capacity, a watermarking system must allow for a useful amount of information to be embedded into the image. This can range from a single bit all the way up to multiple paragraphs of text. Speed is important to those applications that require real time embedding and/or detection.

3.3 Watermarking systems

Watermarking systems would generally involve two processes: watermark embedding (Fig.3) and watermark decoding (Fig.4).

With the help of an encoder, the watermark is applied to the original media signal. First, a list of data elements is selected from the original media signal that will be modified during the encoding of the watermark. The watermark consists of noise-like signals, which are generated pseudo-randomly based on secret keys.

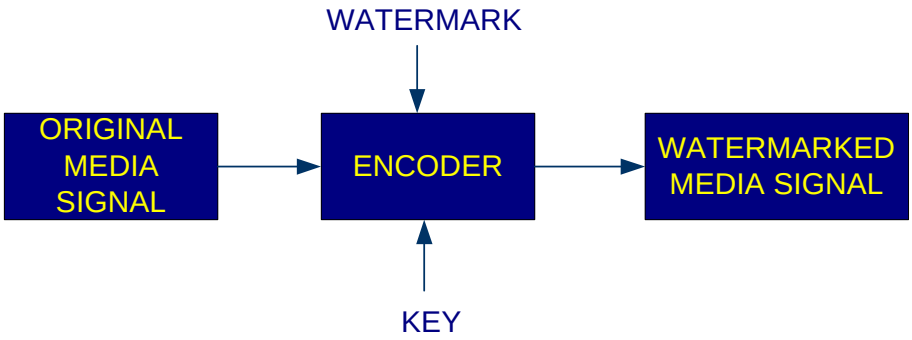


Fig.3 Watermark embedding process [4]

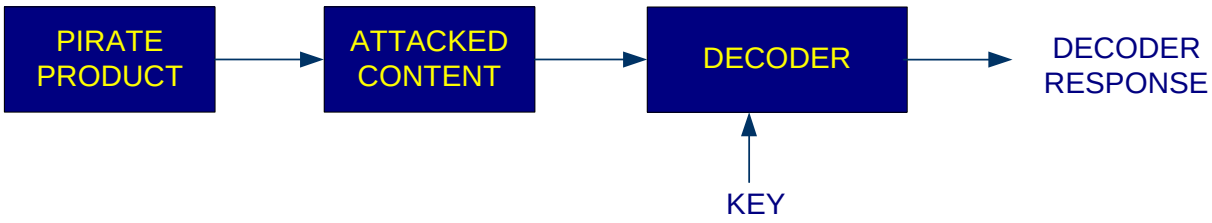


Fig.4 Watermark embedding process [4]

The same key is required for the watermark **decoding** process, where a decoder checks the possibly attacked content for the presence of a watermark. The extracted watermark is compared with the original watermark by using a correlation measure and threshold. The decoder response gives a binary result, stating if the compared and extracted watermarks are the same.

3.4 Watermarking application domain

Digital watermarking has a broad range of uses across many industries. Some of those are given below.

Proof of ownership
Multimedia owners may want to use watermarks not just to *identify* copyright ownership, but to actually *prove* ownership. If a person creates an image and puts it on his website

with a copyright notice, it can then be stolen and with the help of an image processing program the original copyright notice can be replaced with another one. The person who has stolen the image is now able to claim to own the copyright himself. Traditionally, the dispute could be resolved if the image creator already registered the image with the Copyright Office by sending a copy to them. The Copyright Office would have archived the image, together with information about the rightful owner. In the case of a dispute, the Copyright Office can be contacted to provide proof regarding the rightful owner. If the image was not registered, then showing the film negative would have the same effect. However, with the rapid acceptance of digital photography, there may have never been a negative. In theory, it is possible for the image creator to use a watermark embedded in the image to prove that he owns it.

Broadcast monitoring

There are several types of organizations and individuals interested in broadcast monitoring. Advertisers want to ensure that they receive the air time purchased from broadcasting firms. Musicians and actors want to ensure that they receive accurate royalty payments for broadcasts of their performances. Copyright owners want to ensure that their property is not illegally rebroadcast by pirate stations.
Watermarks can be used for broadcast monitoring by putting a unique watermark in each video or sound clip prior to broadcast. Automated monitoring stations can then receive broadcasts and look for these watermarks, identifying when and where each clip appears.

Owner identification

Although a copyright notice is no longer necessary to guarantee copy rights, it is still considered as recommended. The form of the copyright notice is usually "© *date, owner*". On books and photographs, the copyright is placed in plane sight. In movies, it is appended to the end of the credits. And on prerecorded music, it is placed on the packaging. One disadvantage of such text copyright notices is that they can often be removed from the protected material. Packaging can be lost, movies can have the credits cut off, and images can be spatially cropped. A digital watermark can be used to provide complementary copyright marking functionality because it becomes an integral part of the content, i.e. the copyright information is embedded in the music to supplement the text notice printed on the packaging (ex. the **Digimarc** corporation has marketed a watermarking system designed for this application, bundled with Adobe Photoshop. When the detector finds a watermark, it contacts a central database to identify the watermark's owner).

Transactional watermarks (Fingerprinting)

Monitoring and owner identification applications place the same watermark in all copies of the same content. However, electronic distribution of content allows each copy distributed to be customized for each recipient. This capability allows a unique watermark to be embedded in each individual copy. Transactional watermarks, also called fingerprints, allow a content owner or content distributor to identify the source of an illegal copy. This is potentially valuable both as a prevention to illegal use and as a technological aid to investigation. One possible application of transactional watermarks is in the distribution of movie dailies. During the course of making a movie, the result of each day's photography is often distributed to a number of people involved in its production. These dailies are highly confidential, yet occasionally, a daily is leaked to the

press. When this happens, studios quickly try to identify the source of the leak. Clearly, if each copy of the daily contains a unique transactional watermark that identifies the recipient, then identification of the source of the leak is much easier.

Filtering/Classification
Digital watermarks enable content to be identified, classified and filtered. Therefore, systems are enabled to selectively filter potentially inappropriate content, such as corporations and parents restricting viewing of pornographic or other objectionable material. The digital watermark carries the classification codes, or identifies the content and links to a remote database with the classification codes. Classification/Filtering is applicable to images, audio, and video (Implementation examples: Digimarc).

Authentication
As both still and video cameras increasingly embrace digital technology, the ability for undetectable tampering also increases. The content of digital photographs can easily be altered in such a way that it is very difficult to detect what has been changed. In this case there is not even an original negative to examine. This is especially important in legal cases and medical imaging.
When using digital watermarking with an image, it eliminates the problem of ensuring that the signature stays with the image. It also opens up the possibility to learn more about what tampering has occurred, since any changes made to the image will also be made to the watermark.

3.5 Digital watermarking techniques

Current watermarking techniques can be grouped into three main classes. A brief description is given below.

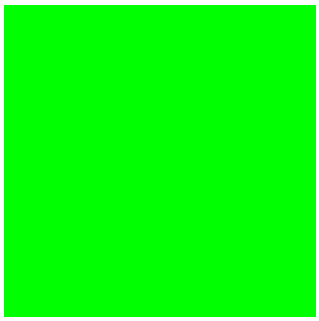
3.5.1 Spatial domain techniques

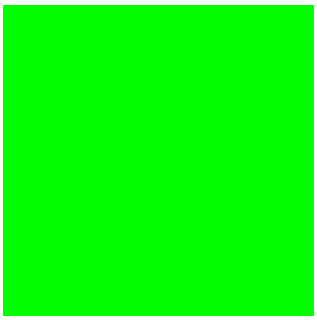
Spatial watermarks are constructed in the image spatial domain, and embedded directly into an image's pixel data. There are several techniques used in this domain.

1. Addition of **pseudo-random noise**. Many spatial techniques are based on adding fixed amplitude pseudo noise sequences to an image. To retrieve the watermark, the same pseudo-random noise generator algorithm is seeded with the same key, and the correlation between the noise pattern and possibly watermarked image computed. If the correlation exceeds a certain threshold T, the watermark is detected, and a single bit is set.

2. Probably one of the simplest techniques used in the spatial domain is the LSB modification. This method encodes a signal in the least significant bits. The invisibility of the watermark is achieved on the assumption that the LSB data are visually insignificant. There are two ways of doing an LSB modification:

a. The LSB of each pixel can be replaced with the secret message;
b. The pixels may be chosen (pseudo) randomly according to a key.





(R,G,B) = (00000000, 11111111, 00000000) (R,G,B) = (00000001, 11111111, 00000000)

Fig.5 Example of LSB modification

For example, if the chosen pixel is green (Fig. 4), and that 8 bits are used for coding color. Its red, green, and blue components in binary are 00000000, 11111111, and 00000000. Now if the program wants to hide the bit value 1 in this pixel's red component. The new pixel value has components 00000001, 11111111, 00000000 and the new image is to the human eye undistinguishable from the original one.

Although this technique can be easily applied to almost every image, it does have some drawbacks. It is highly sensitive to signal processing operations and can be easily corrupted. For example, lossy compression could completely defeat the watermark. Setting the LSB bits of each pixel to one would also completely 'crush' the watermark.

3.5.2 Transform domain techniques

To embed a watermark in the transform domain, a mathematical transformation (DCT, DFT, wavelet) is first applied to the host data. Then modifications are made to the transform coefficients by the watermark. The inverse transform is finally applied to obtain watermarked image [5].

1. Wavelet based watermarking

The wavelet domain provides good space-frequency localization for analyzing image features such as edges or textured areas. To a large extent these features are represented by the large coefficients in the detail sub bands at various resolutions. Some watermarking schemes benefit from the locality of the transform coefficients to implement the region-of-interest coding. One of the many advantages over the wavelet transform is that that it is believed to more accurately model aspects of the human visual system as compared to the FFT or DCT. This allows us to use higher energy watermarks in regions that the HVS is known to be less sensitive to, such as the high

resolution detail bands. Embedding watermarks in these regions increases the robustness of the watermark, at little to no additional impact on image quality.
The wavelet domain is considered to be the most efficient domain for watermark embedding.

2. DCT-based watermarking

The *discrete cosine transform* allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (the low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies).

3. Fractal domain techniques

The word "fractal" denotes a shape that is recursively constructed or self-similar, that is, a shape that appears similar at all scales of magnification and is therefore often referred to as "infinitely complex."
In fractal analysis, similar patterns are identified in an image and only a limited amount of binary code can be embedded using this method. Because of the fact that not every image has a large self-similar pattern makes this technique not suitable for general use. Beside from this disadvantage, it is also computationally expensive.

3.5.3 Feature domain techniques

First generation methods have been mainly focused on applying the watermarking on the entire image domain [4]. However, as new compression standards for images came along, such as the JPEG 2000, the watermarking methods faced a compatibility issue, simply because these compression approaches are region- or object-based. This means that the algorithms from the previous generation do not satisfy the watermarking requirements.
Second generation watermarking (2WG) was developed in order to increase the robustness and invisibility and to overcome the weakness of the algorithms of the previous generation [4]. They improve the 1GW methods in a sense that they take into account region, boundary and object characteristics. This provides an additional advantage in terms of detection and recovery from geometric attacks compared to the first generation methods.

3.6 Testing watermarking algorithms

To find out how resistant and robust the watermarking algorithms, we first have to look at the common processing operations that a media document can undergo.

A watermarked image is likely to be subjected to certain manipulations, some unintentional (compression and transmission noise) and some intentional (geometric transformations).
They are summarized below.

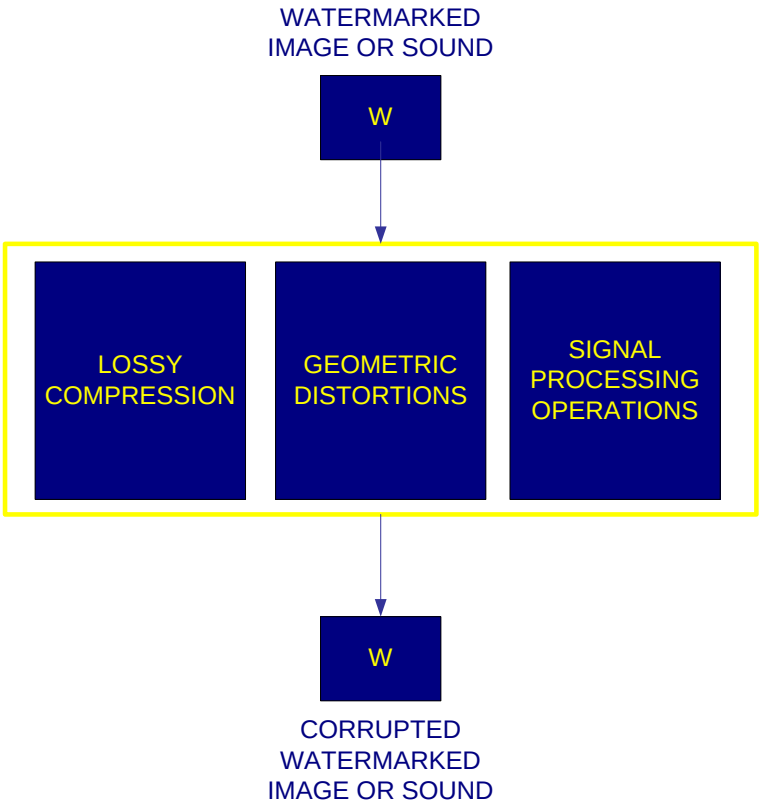


Fig. 6 Manipulations, a watermarked image is likely to be subjected to

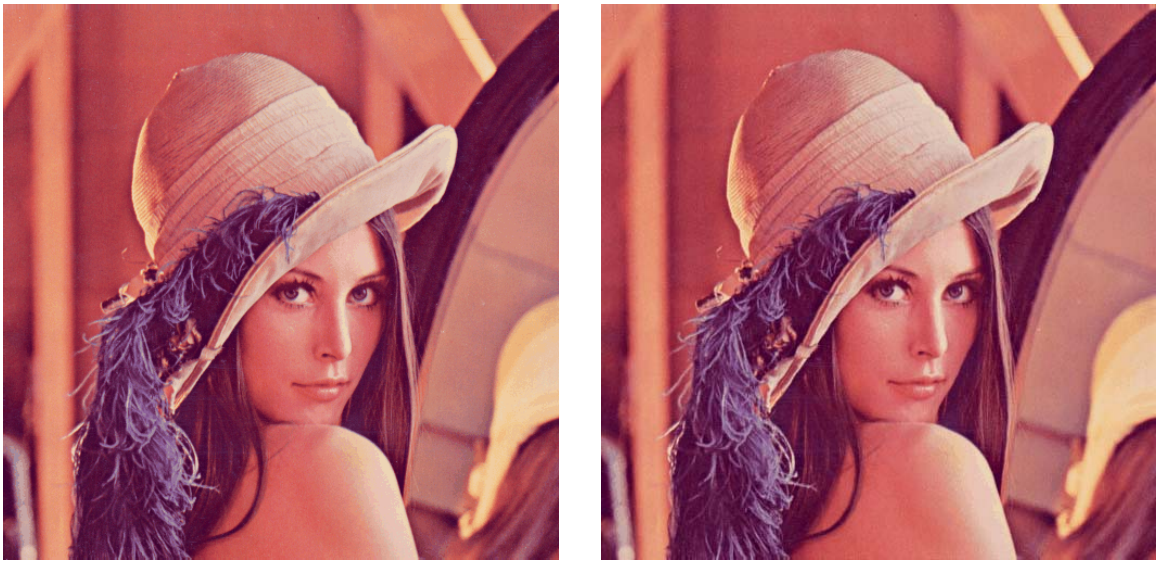
- Lossy compression: JPEG, MPEG can degrade the quality of the data through irretrievable loss of data.
- Geometric distortions: rotation, scaling, cropping, etc…
- Signal processing operations: D/A conversion, resampling, color reduction, filtering.

Image watermarking algorithms must survive robustness attacks and geometric distortions. Many of today's proposed watermarking schemes could survive basic manipulations (manipulations that can be done easily with standard tools, such as rotation, shearing, resampling, resizing and lossy compression). The motivation for creating the *StirMark* tool was the fact that almost none of the schemes would handle combinations of them [6].

3.6.1 StirMark

StirMark is a generic tool for basic robustness testing of image watermarking algorithms. First it applies a minor unnoticeable geometric distortion: the image is slightly stretched, sheared, shifted, bent and rotated by an unnoticeable random amount. Then a slight random low frequency deviation, which is greatest at the centre of the picture, is applied to each pixel. A higher frequency displacement of the form $\lambda \sin(\omega_x x)\sin(\omega_y y)+n(x,y)$ is added, where n is a random number. Finally a transfer function that introduces a small and smoothly distributed error into all sample values is applied. This emulates the small non-linear analogue/digital converter imperfections typically found in scanners and display devices. Finally a transfer function that introduces a small and smoothly distributed error into all sample values is applied. This emulates the small non-linear analogue/digital converter imperfection typically found in scanners and display devices. Quality loss is unnoticeable and watermarking algorithms may not survive this kind of cover-image changing.

In general, the purpose of StirMark is, given an image as a target and a proper set of different distortions, to destroy the watermark without loosing any perceptual quality. The authors of [6] suggest that image watermarking tools which survive StirMark (with default parameters) should be considered unacceptably easy to break.



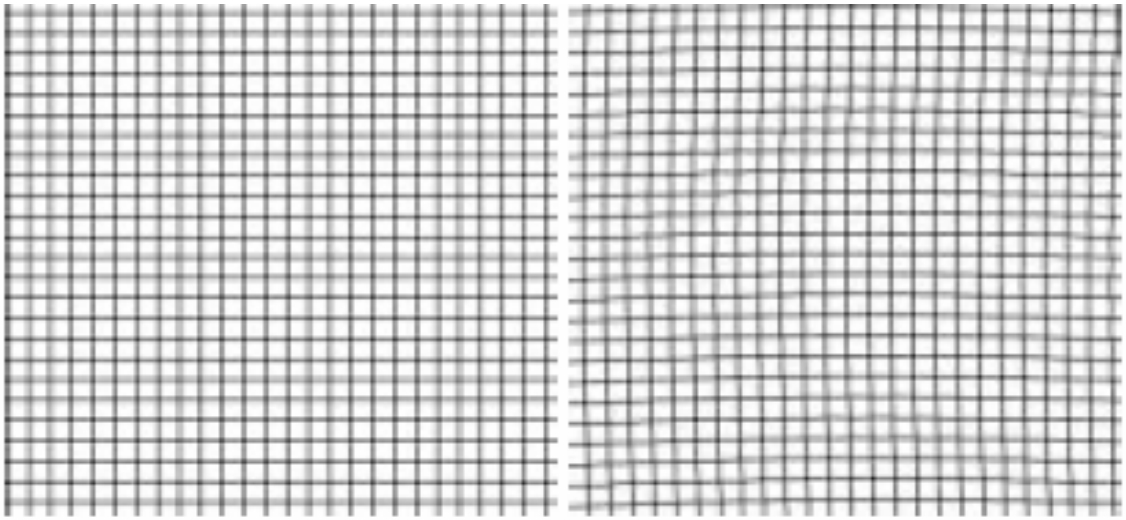
a) Before StirMark b) After StirMark

Fig. 5 Applying StirMark to images ((a) before and b) after) [1]

When applied to images, the distortions introduced by Stir-Mark are almost unnoticeable: before (a) and after (b) StirMark with default parameters. For comparison,

[1] Copyright image courtesy of Kevin Odhner (jko@home.com)

the same distortions have been applied to a grid (c and d). Both images have the same size: 256 *x* 256 pixels.



c) Grid d) Grid after StirMark

Fig.6 StirMark applied to a grid (c) before and d) after) [7]

It turns out to be hard to resist a chosen distortion attack, in which the attacker who understands the marking scheme ‘crushes’ the content in such a way as to cause maximum damage to the mark while doing minimal damage to the marked content.

4 Conclusion

The rapid evolution of digital media and the Internet has had a big influence on the way how today media is used, distributed, shared, copied and managed. Although this progress has brought numerous advantages in handling digital content, it has also been responsible for introducing changes in electronic data trading and data distribution over networks such as the Internet. Customers, content owners, publishers and others involved in e-markets, are now facing different rules than the ones applied in the physical world. Digital rights management systems enable robust e-commerce, copyright protection, secure distribution and protection of digital data by means of encryption, watermarking, fingerprints, secure communication protocols, trust infrastructures, etc. Digital watermarks as a way of preserving the digital data value are designed to permanently reside in the host data (images, audio data, video). The robustness of watermarking algorithms is evaluated by tools such as StirMark, whose purpose is to destroy the watermark in an image without loosing any perceptual quality.
There is still no standard for developing and implementing DRM systems; however it is a necessary tool for protecting intellectual property and its implementation world wide on a very broad level is foreseeable.

5 References

A guide to digital rights management, http://www.dcita.gov.au/drm/1976.html
AAP Digital Rights Management for Ebooks: *Publisher Requirements*
An Overview of Steganography for the Computer Forensics Examiner, http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm
[1] Bret Dunbar, *A detailed look at Steganographic Techniques and their use in an Open-Systems Environment*
[4] Chun-Shien Lu, Multimedia security: Steganography and digital watermarking techniques for protection of intellectual property
Computer Forensics, Cybercrime and Steganography Resources, http://www.forensics.nl/digital-watermarking
[5] D. Taskovski, S. Bogdanova, M. Bogdanov, *Digital Watermarking in wavelet domain*
Digital right management and the crumbling norms of copyright, http://www.firstmonday.org/issues/issue8_11/may/#m4
Digital Rights Management - Part 2. By Karen Coyle, http://www.kcoyle.net/drm_basics2.html
[2] Digital Rights Management (DRM) Architectures, http://www.dlib.org/dlib/june01/iannella/06iannella.html
Digital Watermarking FAQ, http://www.watermarkingworld.org/faq.html
Digital Watermarking Solutions, http://www.digimarc.com/watermark/
Digital Watermarking: a solution to Electronic Copyright Management Systems Requirements, http://www.medicif.org/dig_library/StateArt/Ipr/Piva/piva_doc.html
Digital watermarking: an overview and requirements for successful implementation, http://www.isoc.org/inet2000/cdproceedings/8g/8g_4.htm#s6
DRM - Digital Rights Management, http://www.birds-eye.net/definition/d/drm-digital_rights_management.shtml
DRM Technologies, http://www.info-mech.com/drm_technology.html#watermark
eBooks - The stony road to success and the role of DRM, http://www.indicare.org/tiki-read_article.php?articleId=127
E-Books and DRM, http://www.gripe2ed.com/scoop/story/2004/2/19/0515/77045
[6] Fabien A.P. Petitcolas, Ross J. Anderson, and Markus G. Kuhn, *Attacks on Copyright Marking Systems*
[7] Fabien A. P. Petitcolas and Ross J. Anderson, *Evaluation of copyright marking systems*
Frank Hartung, Student Member, IEEE, and Martin Kutter, *Multimedia Watermarking Techniques*
Guoyou He, *Analysis of E-book Security*
Hannes Federrath, Scientific evaluation of DRM systems
Henry Maitre, *Image watermarking*
Hidden Bits: A Survey of Techniques for Digital Watermarking, http://www.vu.union.edu/~shoemakc/watermarking/watermarking.html
Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom, *Watermarking applications and their properties*
Ingemar J.C., Tom L. Talal S., *A secure, robust watermark for multimedia*
Jonathan Watkins, *Steganography - Messages Hidden in Bits*
LockLizard Ltd 2005, *Encryption is not enough for DRM*
[3] M. Kankanahalli, et. al., *Adaptive Visible Watermarking of Images*, Proc. of IEEE Int. Conf. on Multimedia Computing Systems, ICMCS-99, Cento Affari, Florence, Italy, June 1999.
M.Kutter, S.K. Bhattacharjee, T. Ebrahimi, *Towards Second generation watermarking schemes*
Microsoft Research DRM talk, http://www.dashes.com/anil/stuff/doctorow-drm-ms.html
N. Nikolaidis, I. Pitas, *Digital Image Watermarking: an Overview*

Peter M., Andreas U., *A survey of Wavelet-domain watermarking algorithms*
Prof. Dr.-Ing. Bernd Girod, Dr. Jonathan K. Su, Dipl.-Ing. Joachim Eggers, Dipl.-Ing. Frank Hartung, *Digital Watermarking*
R. Chandramoul, Nasir Memon, *How many pixels to watermark?*
Ravi K.S., Steve D., *Practical challenges for digital watermarking applications*
Rüdiger G., Stefan P., Michael M., *privacy4DRM*
S. A. M. Gilani and A. N. Skodras, *Multiple channel watermarking of color images*
Saraju P. Mohanty, *Digital Watermarking, A Tutorial Review*
Saraju P. Mohanty, K.R. Ramakrishnan, Mohan S Kankanhalli, *A DCT Domain Visible Watermarking Technique for Images*
Soldatov Nikolay, *Information hiding*
Stephen R Lewis, *How much is stronger DRM worth?*
StirMark - Image Watermarking Robustness Test, http://www.cl.cam.ac.uk/~mgk25/stirmark.html
The DRM Dictionary, http://www.info-mech.com/drm_dictionary.html
The end of e-books, http://www.evilgeniuschronicles.org/wordpress/2004/02/29/the-end-of-drm-ebooks-for-me/
The Technology of Rights: Digital Rights Management, http://www.kcoyle.net/drm_basics1.html
The Virtual Display Case, http://www.chin.gc.ca/English/Intellectual_Property/Virtual_Display_Case/varieties.html
What makes ebooks work, http://blogs.adobe.com/worldbehindtheglass/2005/10/what_makes_eboo.html
WWW References on Multimedia Watermarking and Data Hiding Research & Technology, http://www-nt.e-technik.uni-erlangen.de/~hartung/watermarkinglinks.html